

Refurbished CISCO CSS5-CABLX-LCSC Datasheet

CISCO > SWITCHES

Cisco Catalyst 3750 Metro Series Switches

Features and Benefits

Service Breadth

Triple-Play Services	Advanced QoS functionalities to provide differentiated class of service treatment to support triple-play service. Multicast VLAN Registration (MVR) reduces overall bandwidth requirement for multicast distribution in ring based networks. Comprehensive security solution to provide protection of subscribers, switch, and network at the network edge. Source Specific Multicast (SSM) reduces the need for IP Multicast address management and prevents DoS attacks against receivers. SSM mapping provides a mapping of source to group, which allows listeners to find/connect to multicast sources dynamically, reducing dependencies on the application.
Intelligent Ethernet Demarcation	Industry standard OAM&P 802.1ag (CFM) feature supports end-to-end network monitoring and troubleshooting. This greatly reduces OpEx for service providers by reducing the numbers of site visits needed to troubleshoot network problems. E-LMI enables the service provider to automatically configure the customer-edge and CPE devices to match the subscribed service.
Layer 2 VPN Service	Standard 802.1Q Tunneling creates a hierarchy of 802.1Q tags. This feature helps service providers use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and segregating traffic from different customers within the service provider infrastructure even when they appear to be on the same VLAN. Selective QinQ gives service providers more flexibility in segregating customer traffic in the network. L2PT allows for transport of the customers' control protocols, thereby allowing for a true virtual-circuit service across service providers' shared infrastructure.

Availability and Scalability

Superior Redundancy for Fault Backup	IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) provides rapid spanning-tree convergence independent of spanning-tree timers and offers the benefit of distributed processing. Per-VLAN Rapid Spanning Tree (PVRST+) allows rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances. Cisco Hot Standby Router Protocol (HSRP) is supported to create redundant, fail-safe routing topologies. Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD allow unidirectional links caused by incorrect fiber-optic connections or port faults to be detected and disabled on fiber-optic interfaces. Flex-Link provides fast failover of ports without overhead of control protocols such as the Spanning Tree Protocol. VLAN Flex-Link Load Balancing provides high availability and load balancing based on VLAN. Switch-port autorecovery (errdisable) automatically attempts to reactivate a link that is disabled because of a network error. Equal-cost routing provides for load balancing and redundancy. Bandwidth aggregation up to 800 Mbps through Cisco Fast EtherChannel ® technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches and to routers and individual servers. Accelerate Layer 3 reconvergence through the use of Link-State Tracking by taking down associated downstream ports when all the corresponding upstream ports are down. Customer switches that are connected to the downstream ports can then take the appropriate failover action. Resilient Ethernet Protocol (REP) provides fast Layer 2 reconvergence in a ring network and offers an alternative to Spanning Tree Protocol. Pseudowire redundancy enables service providers to configure their Multiprotocol Label Switching) MPLS network to detect a failure in the network and reroute Layer 2 service to another endpoint that can continue to provide service.
---	--

Multicast

Efficient Multicast Distribution	Multicast VLAN Registration provides efficient multicast distribution in ring networks by dedicating a single VLAN for multicast traffic, thereby removing duplicate multicast traffic in other VLANs. PIM-SM provides efficient routing of multicast traffic by establishing distribution trees across WANs. Source Specific Multicast (SSM) reduces the need for IP Multicast address management and prevents DoS attacks against receivers. SSM mapping provides a mapping of source to group, which allows listeners to find/connect to
---	---

multicast sources dynamically, reducing dependencies on the application.

QoS and Control

Advanced QoS

Standard 802.1p class of service (CoS) and differentiated services code point (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, VLAN ID, or Layer 4 TCP/User Datagram Protocol (TCP/UDP) port number.

Cisco control-plane and data-plane QoS ACLs on all ports help ensure proper marking on a per-packet basis.

Shaped Round Robin (SRR) scheduling helps ensure differential prioritization of packet flows by intelligently servicing the queues.

Weighted Tail Drop (WTD) provides per QoS class congestion avoidance at the queues before a disruption occurs.

Priority queue rate limiting provides optional protection against lower priority queue starvation.

The ES ports offer the following additional functionalities:

- Hierarchical QoS with traffic classification, policing, queuing, shaping, and scheduling at the class, VLAN, and interface level
- Traffic classification based on MPLS experimental (EXP) bits
- 2 Rate 3 Color policing
- WRED (Weighted Random Early Detection) for congestion avoidance
- Class-Based Weighted Fair Queuing (CBWFQ) for bandwidth management
- Low-Latency Queue provides strict-priority queuing for delay sensitive data
- Configurable control plane queue assignment allows service providers to assign control plane traffic to specific egress queue.
- Prioritization of control plane traffic enables service providers to set QoS markings globally for CPU-generated traffic so these protocol packets will receive priority in the network.
- There is no performance penalty for advanced QoS functionalities.

Network Security

Comprehensive Security Solutions

Subscriber Security

IEEE 802.1x allows dynamic, port-based security by providing user authentication.

IEEE 802.1x with VLAN assignment allows a dynamic VLAN assignment for a specific user regardless of where the user is connected.

IEEE 802.1x and port security are provided to authenticate the port and manage network access for all MAC addresses.

IEEE 802.1x readiness check simplifies deployment by generating a report for end hosts capable of 802.1x.

An absence of local switching behavior provides security and isolation between UNIs, helping ensure that users cannot monitor or access other users' traffic on the same switch.

DHCP Snooping prevents malicious users from spoofing a DHCP server and sending out bogus addresses. This feature also prevents numerous other attacks such as Address Resolution Protocol (ARP) poisoning.

Dynamic ARP Inspection helps ensure user integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.

IP Source Guard prevents a malicious user from spoofing or taking over another user's IP address by creating a binding table between client's IP and MAC address, port, and VLAN.

Switch Security

Control Plane Security prevents DoS attacks on the CPU.

Secure Shell (SSH) Protocol, 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.

Port security secures the access to an access or trunk port based on MAC address. After a specific timeframe, the aging feature removes the MAC address from the switch to allow another device to connect to the same port.

Multilevel security on the console access prevents unauthorized users from altering the switch configuration.

TACACS+ and RADIUS authentication facilitate centralized control of the switch and restrict unauthorized users from altering the configuration.

Configuration File Security helps ensure that only authenticated users have access to the configuration file.

Per VLAN MAC address learning prevents MAC address table overflow attack.

Network Security

Network Security

Cisco security VLAN ACLs on all VLANs prevent unauthorized data flows from being bridged within VLANs.

Cisco standard and extended IP security router ACLs define security policies on routed interfaces for control-plane and data-plane traffic.

Port-based ACLs for Layer 2 interfaces allow for application of security policies on individual switch ports.

MAC address notification allows administrators to be notified of users added to or removed from the network.

Manageability

Superior Manageability

The Cisco IOS Software CLI provides a common user interface and command set with all Cisco routers and Cisco Catalyst desktop switches.

Service Assurance Agent (SAA) provides service-level management throughout the network.

IEEE 802.1ag Connectivity Fault Management provides standard support for transport fault management. It allows for discovery and verification of path for Layer 2 services.

Ethernet Local Management Interface enables auto configuration of CPE by CLE to support Metro Ethernet services.

IEEE 802.3ah Ethernet in the First Mile provides standard support for monitoring, remote failure indication, loopback, and OAM discovery on the link between the customer equipment and service provider network.

ITU-T Y.1731 introduces the support for fault management functions, including alarm indication signal (AIS), remote defect indication (RDI) and locked signal (LCK) to detect and signal a failure in the service path.

Switching Database Manager templates for Layer 2 and Layer 3 deployment allow the administrator to easily optimize memory allocation to the desired features based on deployment-specific requirements.

VLAN trunks can be created from any port, using standards-based 802.1Q tagging. Up to 1005 VLANs per switch and up to 128 spanning-tree instances per switch are supported.

Four thousand VLAN IDs are supported.

RSPAN allows administrators to remotely monitor ports in a Layer 2 switch network from any other switch in the same network.

Manageability

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.

MPLS OAM supports service providers to quickly troubleshoot and monitor MPLS networks.

All nine RMON groups are supported through a SPAN port, permitting traffic monitoring of a single port, a group of ports, or the entire stack from a single network analyzer or RMON probe.

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 Timing Protocol (NTP) provides an accurate and consistent time stamp to all intranet switches.

The Cisco Catalyst 3750 Metro Series supports the Cisco CNS 2100 Series Intelligence Engine and SNMP for networkwide management.

Cisco IP Solution Center (ISC) applications help reduce overall administration and management costs by providing automated resource management and rapid profile-based provisioning capabilities.

Configuration Rollback helps in error recovery by providing the capability to replace the current running configuration with any saved Cisco IOS Software configuration file.

Manageability

Embedded Event Manager (EEM) offers the ability to monitor events and take user-defined action when the monitored events occur or a threshold is reached.

Dynamic Host Configuration Protocol (DHCP) based auto configuration and image update simplifies management of large number of switches by automatically downloading specified configuration and image.

Service Diagnostics automates a set of network diagnostic procedures derived from the vast troubleshooting experiences of Cisco network experts. These diagnostic tools help customers increase network uptime, reduce time to repair and improve service levels.

Digital optical monitoring (DOM) support provides a service provider with the capability to perform in-service transceiver monitoring and troubleshooting operations.

DOM threshold functions allow the monitoring of real time optical parameters on DOM SFPs and the comparison against factory-reset values, generating alarm and warning thresholds.

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 versions 1, 2c, and 3 and Telnet provide comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management.

Cisco Discovery Protocol versions 1 and 2 help enable automatic switch discovery for a CiscoWorks network management station.

The CiscoWorks 2000 LAN Management Solution is supported.

Product Specifications

Description	Specification
Performance	Forwarding rate: 8.55 mpps 128-MB DRAM and 32-MB flash memory 64-MB DRAM enhances services port memory Configurable up to 12,000 MAC addresses Configurable up to 11,000 unicast routes Configurable up to 1,000 IGMP groups and multicast routes Configurable maximum transmission unit (MTU) of up to 9000 bytes for bridging on Gigabit Ethernet ports and up to 1998 bytes for bridging and routing on Fast Ethernet ports
Connectors and Cabling	10/100 Ports: 10BASE-T ports: RJ-45 connectors, 2-pair Category 3, 4, or 5 unshielded twisted-pair (UTP) cabling 100BASE-TX ports: RJ-45 connectors, 2-pair Category 5 UTP cabling SFP Ports: 1000BASE-T SFP-based ports: RJ-45 connectors, 2-pair Category 5 UTP cabling 1000BASE-BX: Single-fiber LC receptacle connector (single-mode fiber) 1000BASE-EX: Single Mode Fiber with DOM support 1000BASE-SX, -LX, and -ZX and CWDM and DWDM: Duplex LC receptacle fiber connectors (multimode and single-mode fiber) 100FX SFP on GE SFP ports (only non-ES SFP ports) Management console port: RJ-45-to-DB9 cable for PC connections
Indicators	Per-port status LEDs: Link integrity, port disabled, and activity indications System-status LED

Dimensions (H x W x D)	1.73 x 17.5 x 14.68 in. (4.39 x 44.5 x 37.3 cm)
Weight	12.1 lb (5.49 kg) (Cisco Catalyst 3750 Metro 24-AC or DC)
Mean Time Between Failure (MTBF)	168,231 hours (one power supply) 256,311 hours (two power supplies)

Power Specifications

Description	Specification
Power Consumption	110W (maximum), 374 BTUs per hour (Cisco Catalyst 3750 Metro 24-AC or DC Switch)
AC Input Voltage and Frequency	100 to 127/200 to 240 VAC (autoranging), 50 to 60 Hz (Cisco Catalyst 3750 Metro 24-AC)
DC Input Voltages	-36 to -72 VDC @ 3A (Cisco Catalyst 3750 Metro 24-DC)

Management and Standards

Description	Specification
Management	BRIDGE-MIB (RFC1493) BGP4-MIB (RFC1657) CISCO-BULK-FILE-MIB
Standards and Protocols	IEEE 802.1s IEEE 802.1w BFD for OSPF, IS-IS, BGP, HSRP, EIGRP IEEE 802.1x IEEE 802.3ad IEEE 802.3ah IEEE 802.1ag IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports IEEE 802.1D Spanning Tree Protocol IEEE 802.1p CoS classification IEEE 802.1Q VLAN IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-T IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-X IP routing: Static, RIP versions 1 and 2, EIGRP, OSPF, BGPv4, HSRPv2, PIM-SM, and PIM-DM (metro IP access only) IPv6: RIP, OSPFv3, static routes Management: SNMP versions 1, 2, and 3 IPv6: MLD Snooping v1 and v2

Safety and Compliance

Type	Standards
Electromagnetic Emissions Compliance (EMC)	FCC Part 15 Class A, EN 55022B Class A (CISPR22 Class A) GR-1089 CORE Class A VCCI Class I AS/NZS 3548 Class A or AS/NZS CISPR22 Class A BSMI Class A MIC CE Marking
Safety	UL 60950, Third Edition UL to CAN/CSA 22.2 No.60950, Third Edition TUV/GS to EN 60950 with Amendment A1-A4 and A11 CB to IEC 60950 with all country deviations NOM to NOM-019-SCFI AS/NZS 3260, TS001 CE Marking CLEI Coding
NEBS	GR-63-CORE and GR-1089-CORE - Level 3, Type 2
ETSI	EN 300 019 - Storage: Class 1.2, Transportation: Class 2.3, In-Use: Class 3.2
Noise Specifications	Office product specification: 50dBA
Operating Environment	Temperature: 0 to +45°C

-5 to +55°C (NEBS short-term operation)
Altitude: Up to 10,000 ft (3000m)
Relative humidity:
10 to 85% non-condensing
5 to 95% non-condensing (NEBS short-term operation)

Storage Environment

Temperature:
-25 to 70°C
-40 to 70°C (NEBS short-term operation)
Altitude: 15,000 ft (4570m)

The next steps...

ORDER NOW

VIEW ONLINE

Tel: +44 (0)1279 408 777

Email: sales@gocomsys.com

Website: www.gocomsys.com