Tel: +44 (0)1279 408 777
Email: sales@gocomsys.com
Website: www.gocomsys.com

Refurbished CISCO MGBBX1 Datasheet

CISCO > SWITCHES

Cisco 550X Series Stackable Managed Switches

Product specifications

Layer 2 switching	
Spanning Tree Protocol	Standard 802.1d spanning tree support Fast convergence using 802.1w (Rapid Spanning Tree [RSTP]), enabled by default Multiple spanning tree instances using 802.1s (MSTP); 16 instances are supported
Port grouping/link aggregation	Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP) Up to 32 groups Up to 8 ports per group with 16 candidate ports for each (dynamic) 802.3ad LAG
VLAN	Support for up to 4,094 active VLANs simultaneously; port-based and 802.1Q tag-based VLANs; MAC-based VLAN Management VLAN Private VLAN with promiscuous, isolated, and community port Guest VLAN, unauthenticated VLAN, protocol-based VLAN, IP subnet-based VLAN, CPE VLAN Dynamic VLAN assignment using RADIUS server along with 802.1x client authentication
Voice VLAN	Voice traffic is automatically assigned to a voice-specific VLAN and treated with appropriate levels of QoS. Auto voice capabilities deliver networkwide zero-touch deployment of voice endpoints and call control devices
Multicast TV VLAN	Multicast TV VLAN allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. This feature is also known as Multicast VLAN Registration (MVR)
VLAN translation	Support for VLAN One-to-One Mapping. In VLAN One-to-One Mapping, on an edge interface C-VLANs are mapped to S-VLANs and the original C-VLAN tags are replaced by the specified S-VLAN
Q-in-Q	VLANs transparently cross over a service provider network while isolating traffic among customers
Selective Q-in-Q	Selective Q-in-Q is an enhancement to the basic Q-in-Q feature and provides, per edge interface, multiple mappings of different C-VLANs to separate S- VLANs Selective Q-in-Q also allows configuring of Ethertype (TPID) of the S-VLAN tag
GVRP/GARP	Generic VLAN Registration Protocol (GVRP) and Generic Attribute Registration Protocol (GARP) enable automatic propagation and configuration of VLANs in a bridged domain
Unidirectional Link Detection (UDLD)	UDLD monitors physical connection to detect unidirectional links caused by incorrect wiring or port faults to prevent forwarding loops and blackholing of traffic in switched networks
DHCP relay at Layer 2	Relay of DHCP traffic to DHCP server in a different VLAN. Works with DHCP option 82
IGMP (versions 1, 2, and 3) snooping	Internet Group Management Protocol (IGMP) limits bandwidth-intensive multicast traffic to only the requesters; supports 4K multicast groups (source-specific multicasting is also supported)
IGMP querier	IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router
Layer 3	
IPv4 routing	Wirespeed routing of IPv4 packets Up to 7,168 routes and up to 256 IP interfaces
Wirespeed IPv6 static routing	Up to 1,792 routes and up to 256 IPv6 interfaces
Layer 3 interface	Configuration of Layer 3 interface on physical port, LAG, VLAN interface, or loopback interface
CIDR	Support for classless interdomain routing
RIP v2	Support for Routing Information Protocol version 2 for dynamic routing
VRRP	Virtual Router Redundancy Protocol (VRRP) delivers improved availability in a Layer 3 network by providing redundancy of the default gateway servicing hosts on the network. VRRP versions 2 and 3 are supported. Up to 255 virtual routers are supported

Policy-Based Routing (PBR)	Flexible routing control to direct packets to different next hop based on IPv4 or IPv6 ACL
IP Service-Level Agreement (SLA) object tracking	IP SLA object tracking relies on IP SLA ICMP echo operation to detect connectivity to a certain network destination IP SLA object tracking for VRRP provides a mechanism to track the connectivity to the VRRP router default route next hop IP SLA object tracking for static routes provides a mechanism to track the connectivity to the destination network via the next hop specified in the static route
DHCP server	Switch functions as an IPv4 DHCP server serving IP addresses for multiple DHCP pools/scopes Support for DHCP options
DHCP relay at Layer 3	Relay of DHCP traffic across IP domains
Stacking	
Hardware stack	Up to 8 units in a stack. Up to 400 ports managed as a single system with hardware failover
High availability	Fast stack failover delivers minimal traffic loss. Support link aggregation across multiple units in a stack
Plug-and-play stacking configuration/ management	Master/backup for resilient stack control Autonumbering Hot swap of units in stack Ring and chain stacking options, auto stacking port speed, flexible stacking port options
High-speed stack interconnects	Cost-effective high-speed 10G fiber and copper interfaces. Support LAG as stacking interconnects for even higher bandwidth
Security	
SSH	SSH is a secure replacement for Telnet traffic. SCP also uses SSH. SSH versions 1 and 2 are supported
SSL	Secure Sockets Layer (SSL) encrypts all HTTPS traffic, allowing secure access to the browser-based management GUI in the switch
IEEE 802.1X (authenticator role)	RADIUS authentication and accounting, MD5 hash, guest VLAN, unauthenticated VLAN, single/ multiple host mode, and single/multiple sessions Supports time-based 802.1X dynamic VLAN assignment
IEEE 802.1X supplicant	A switch can be configured to act as a supplicant to another switch. This enables extended secure access in areas outside the wiring closet (such as conference rooms)
Web-based authentication	Web-based authentication provides network admission control through web browser to any host devices and operating systems
STP BPDU Guard	A security mechanism to protect the networks from invalid configurations. A port enabled for Bridge Protocol Data Unit (BPDU) Guard is shut down if a BPDU message is received on that port. This avoids accidental topology loops
STP Root Guard	This prevents edge devices not in the network administrator’s control from becoming Spanning Tree Protocol root nodes
DHCP snooping	Filters out DHCP messages with unregistered IP addresses and/or from unexpected or untrusted interfaces. This prevents rogue devices from behaving as a DHCP server
IP Source Guard (IPSG)	When IP Source Guard is enabled at a port, the switch filters out IP packets received from the port if the source IP addresses of the packets have not been statically configured or dynamically learned from DHCP snooping. This prevents IP address spoofing
Dynamic ARP Inspection (DAI)	The switch discards ARP packets from a port if there are no static or dynamic IP/MAC bindings or if there is a discrepancy between the source or destination address in the ARP packet. This prevents man-in-the-middle attacks
IP/MAC/Port Binding (IPMB)	The preceding features (DHCP Snooping, IP Source Guard, and Dynamic ARP Inspection) work together to prevent DoS attacks in the network, thereby increasing network availability
Secure Core Technology (SCT)	Makes sure that the switch will receive and process management and protocol traffic no matter how much traffic is received
Secure Sensitive Data (SSD)	A mechanism to manage sensitive data (such as passwords, keys, and so on) securely on the switch, populating this data to other devices, and secure autoconfig. Access to view the sensitive data as plaintext or encrypted is provided according to the user-configured access level and the access method of the user
Private VLAN	Private VLAN provides security and isolation between switch ports, which helps ensure that users cannot snoop on other users’ traffic; supports multiple uplinks
Port security	Ability to lock source MAC addresses to ports and limit the number of learned MAC addresses
RADIUS/TACACS+	Supports RADIUS and TACACS authentication. Switch functions as a client

RADIUS accounting	The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session
Storm control	Broadcast, multicast, and unknown unicast
DoS prevention	Denial-of-Service (DoS) attack prevention
Multiple user privilege levels in CLI	Level 1, 7, and 15 privilege levels
Quality of service	
Priority levels	8 hardware queues
Scheduling	Strict priority and Weighted Round-Robin (WRR)
Class of service	Port based; 802.1p VLAN priority based; IPv4/v6 IP precedence/ToS/DSCP based; DiffServ; classification and remarking ACLs, trusted QoS Queue assignment based on Differentiated Services Code Point (DSCP) and class of service (802.1p/CoS)
Rate limiting	Ingress policer; egress shaping and ingress rate control; per VLAN, per port, and flow base; 2R3C policing
Congestion avoidance	A TCP congestion avoidance algorithm is required to minimize and prevent global TCP loss synchronization
IPv6	
IPv6	IPv6 host mode IPv6 over Ethernet dual IPv6/IPv4 stack IPv6 Neighbor and Router Discovery (ND), IPv6 Stateless Address Autoconfiguration, path MTU Discovery Duplicate Address Detection (DAD) ICMPv6 DHCPv6 stateful client IPv6 over IPv4 network with ISATAP tunnel support USGv6 and IPv6 Gold Logo certified
IPv6 QoS	Prioritize IPv6 packets in hardware
IPv6 ACL	Drop or rate limit IPv6 packets in hardware
IPv6 First Hop Security	RA guard ND inspection DHCPv6 guard Neighbor binding table (snooping and static entries) Neighbor binding integrity check
Multicast Listener Discovery (MLD v1/2) snooping	Deliver IPv6 multicast packets only to the required receivers
IPv6 applications	Web/SSL, Telnet Server/SSH, Ping, Traceroute, SNTP, TFTP, SNMP, RADIUS, Syslog, DNS client, DHCP Client, DHCP Autoconfig, IPv6 DHCP Relay, TACACS
Green (power efficiency)	
Energy detect	Automatically turns power off on RJ-45 port when detecting link down. Active mode is resumed without loss of any packets when the switch detects the link is up
Cable length detection	Adjusts the signal strength based on the cable length. Reduces the power consumption for shorter cables
EEE compliant (802.3az)	Supports IEEE 802.3az on all 10 Gigabit copper ports
General	
Jumbo frames	Frame sizes up to 9000 bytes. The default MTU is 2000
Discovery	
Bonjour	The switch advertises itself using the Bonjour protocol
LLDP (802.1ab) with LLDP-MED extensions	Link Layer Discovery Protocol (LLDP) allows the switch to advertise its identification, configuration, and capabilities to neighboring devices that store the data in a MIB. LLDP-MED is an enhancement to LLDP that adds the extensions needed for IP phones

Country/region suffix for product order ID number

Suffix	Country/region
-NA	USA, Canada, Mexico, Colombia, Chile, and rest of LATAM

-BR	Brazil
-AR	Argentina
-EU	EU, Russia, Ukraine, Israel, UAE, Turkey, Egypt, South Africa, Indonesia, Philippines, Vietnam, Thailand, India, Korea
-UK	United Kingdom, Saudi Arabia, Qatar, Kuwait, Singapore, Hong Kong, Malaysia
-AU	Australia, New Zealand
-CN	China
-JP	Japan

The next steps...

ORDER NOW

VIEW ONLINE

Tel: +44 (0)1279 408 777

Email: sales@gocomsys.com

Website: www.gocomsys.com