Cisco 350X Series Stackable Managed Switches

10-Gigabit Managed Switches That Provide the Ideal Combination of Features and Affordability

To stay ahead in a competitive marketplace, small businesses need to make every dollar count. That means getting the most value from your technology investments, but it also means making sure that employees have fast, reliable access to the business tools and information they need. Every minute an employee waits for an unresponsive application – and every minute your network is down – has an impact on your bottom line. The importance of maintaining a strong and dependable business network only grows as your business adds more employees, applications, and network complexity.

When your business needs advanced security and features but value is still a top consideration, you're ready for the new generation of Cisco® Small Business managed switches: the Cisco 350X Series.

Cisco 350X Series Stackable Managed Switches

The Cisco® 350X Series Stackable Managed Switches (Figure 1) are a new line of stackable managed Ethernet switches that provide the rich capabilities you need to support a more demanding network environment at a very affordable price. The SG350X models provide 24 or 48 ports of Gigabit Ethernet connectivity with 10 Gigabit uplinks. The Cisco 350XG models provide 12, 24, or 48 ports of all 10 Gigabit Ethernet, providing a solid foundation for your current business applications as well as those you are planning for the future. In addition, these switches are easy to deploy and manage without a large IT staff. The SG350X platforms are Cisco's most cost-effective platforms with 10 Gigabit Ethernet and stacking.

Figure 1. Cisco 350X Series Stackable Managed Switches

Cisco 350X Series switches are designed to protect your technology investment as your business grows. Unlike switches that claim to be stackable but have elements that are administered and troubleshot separately, the Cisco 350X Series provides true stacking capability, allowing you to configure, manage, and troubleshoot multiple physical switches as a single device and more easily expand your network.

A true stack delivers a unified data and control plane, in addition to management plane, providing flexibility, scalability, and ease of use because the stack of units operate as a single entity constituting all the ports of the stack members. The switches also protect your technology investment with an enhanced warranty, dedicated technical support, and the ability to upgrade equipment in the future. Overall, the Cisco 350X Series provides the ideal technology foundation for a growing business.

Features and Benefits

Cisco 350X Series switches provide the advanced feature set that growing businesses require and that high-bandwidth applications and technologies demand. These switches can improve the availability of your critical applications, protect your business information, and optimize your network bandwidth to more effectively deliver information and support applications. The switches provide the following benefits.

High-Performance 10 Gigabit Ethernet

Cisco 350X Series switches break the barrier of 10 Gigabit Ethernet adoption by providing affordable and flexible configurations customized for the demanding network requirements of small and medium businesses.

With 10G copper ports on SG350XG switches, you can easily and cost-effectively enable 10G connections to servers and network storage devices with standard RJ45 Ethernet cable. You can also connect your SG350X access switches to the SG350XG aggregation with 10G SFP+ fiber connections, building a high-performance backbone to speed up the overall operation of your network.

Easy Deployment and Use

Cisco 350X Series switches are designed to be easy to use and manage by commercial customers or the partners that serve them. They feature:

- Simple-to-use graphical interfaces reduce the time required to deploy, troubleshoot, and manage the network and allow you to support sophisticated capabilities without increasing IT head count.
- The switches also support Textview, a full command-line interface (CLI) option for partners that prefer it.
- Using Auto Smartports intelligence, the switch can detect a network device connected to any port and automatically configure the optimal security, quality of service (QoS), and availability on that port.
- Cisco Discovery Protocol discovers Cisco devices and allows devices to share critical configuration information, simplifying network setup and integration.
- Support for Simple Network Management Protocol (SNMP) allows you to set up and manage your switches and other Cisco devices remotely from a network management station, improving IT workflow and mass configurations.
- The Cisco FindIT utility, which works through a simple toolbar on the user's web browser, discovers Cisco devices in the network and displays basic information, such as serial numbers and IP addresses, to aid in configuration and deployment. (For more information and to download this free utility, visit http://www.cisco.com/go/findit.)

Power over Ethernet Plus (PoE+) and 60W PoE

PoE capabilities simplify the deployment of advanced technologies by allowing you to connect and power network endpoints over a single Ethernet cable, without having to install separate power supplies. Cisco 350X Series switches are also fully backward compatible with IEEE 802.11af PoE and Cisco legacy PoE protocols.

Cisco 350X Series switches support the Power over Ethernet Plus (PoE+) standard (IEEE 802. at), providing up to 30 watts per port. The switches also support 60W PoE on select ports to power compact switches, high-power wireless access points, or connected lighting. The PoE power is intelligently managed in a way such that only the amount of power needed by endpoints is delivered to it and not wasted. As a result, the switches can support devices that require more power, such as 802.11ac wireless access points, video-based IP phones, surveillance cameras, and more.

High Reliability and Resiliency

In a growing business where availability 24 hours a day, 7 days a week is critical, you need to assure that employees can always access the data and resources they need. In these environments, stackable switches can play an important role in eliminating downtime and improving network resiliency. For example, if a switch within a Cisco 350X Series stack fails, another switch immediately takes over, keeping your network up and running. You can also replace individual devices in the stack without taking your network offline or affecting employee productivity.

The Cisco 350X Series also supports dual images, allowing you to perform software upgrades without having to take the network offline or worry about the network going down during the upgrade.

Simplified IT Operation

Cisco 350X Series switches help optimize your IT operations with built-in features that simplify and streamline day-to-day network operation:

- True stacking allows you to troubleshoot, configure, and manage multiple physical switches as a single entity.
- Cisco switches use common chipsets/software across all switching portfolios, so all Cisco switches within a category support the same feature set, making it easier to manage and support all switches across the network.

True Stacking

Some switches claim to support stacking but in practice support only “clustering,” meaning that each switch must still be managed and configured individually. Cisco 350X Series switches provide true stacking capability, allowing you to configure, manage, and troubleshoot all switches in a stack as a single unit, with a single IP address, for up to 4 units and a maximum of 208 Ethernet ports.

A true stack delivers a unified data and control plane, in addition to management plane, providing flexibility, scalability, and ease of use because the stack of units operate as a single entity constituting all the ports of the stack members. This capability can radically reduce complexity in a growing network environment while improving the resiliency and availability of network applications. True stacking also provides other cost savings and administrative benefits through features such as cross-stack QoS, VLANs, LAGs, and port mirroring, which clustered switches can’t support.

Strong Security

Cisco 350X Series switches provide the advanced security features you need to protect your business data and keep unauthorized users off the network:

- Embedded Secure Sockets Layer (SSL) encryption protects management data traveling to and from the switch.
- Extensive access control lists (ACLs) restrict sensitive portions of the network to keep out unauthorized users and guard against network attacks.
- Guest VLANs let you provide Internet connectivity to nonemployee users while isolating critical business services from guest traffic.
- Support for advanced network security applications such as IEEE 802.1X port security tightly limits access to specific segments of your network. Web-based authentication provides a consistent interface to authenticate all types of host devices and operating systems, without the complexity of deploying IEEE 802.1X clients on each endpoint.
- Advanced defense mechanisms, including dynamic Address Resolution Protocol (ARP) inspection, IP Source Guard, and Dynamic Host Configuration Protocol (DHCP) snooping, detect and block deliberate network attacks. Combinations of these protocols are also referred to as IP-MAC port binding (IPMB).
- IPv6 First Hop Security extends the advanced threat protection to IPv6. This comprehensive security suite includes ND inspection, RA guard, DHCPv6 guard, and neighbor binding integrity check, providing unparalleled protection against a vast range of address spoofing and man-in-the-middle attacks on IPv6 networks.
- Time-based ACLs and port operation restrict access to the network during pre-designated times such as business hours.
- Uniform MAC address-based security can be applied automatically to mobile users as they roam between wireless access points.
- Secure Core Technology (SCT) helps ensure that the switch is able to process management traffic in the face of a denial-of-service (DoS) attack.
- Private VLAN Edge (PVE) provides Layer 2 isolation between devices on the same VLAN.
- Storm control can be applied to broadcast, multicast, and unknown unicast traffic.
- Protection of management sessions occurs using RADIUS, TACACS+, and local database authentication as well as secure management sessions over SSL, SSH, and SNMPv3.
- DoS attack prevention maximizes network uptime in the presence of an attack.

Networkwide Automatic Voice Deployment

Using a combination of Cisco Discovery Protocol, LLDP-MED, Auto Smartports, and Voice Services Discovery Protocol (or VSDP, a unique Cisco protocol), customers can deploy an end-to-end voice network dynamically. The switches in the network automatically converge around a single voice VLAN and QoS parameters and then propagate them out to the phones on the ports, where they are discovered. For example, automated voice VLAN capabilities let you plug any IP phone (including third-party phones) into your IP telephony network and receive an immediate dial tone. The switch automatically configures the device with the right VLAN and QoS parameters to prioritize voice traffic.

IPv6 Support

As the IP address scheme evolves to accommodate a growing number of network devices, the Cisco 350X Series can support the transition to the next generation of networking and operating systems such as Windows 7, Vista, and Linux. These switches continue to support previous-generation IPv4, allowing you to evolve to the new IPv6 standard at your own pace, and helping ensure that your current network will continue to support your business applications in the future. Cisco 350X Series switches have successfully completed rigorous IPv6 testing and have received the USGv6 and IPv6 Gold certification.

Advanced Layer 3 Traffic Management

The Cisco 350X Series enables a more advanced set of traffic management capabilities to help growing businesses organize their networks more effectively and efficiently. The switches provide static LAN Layer 3 routing, allowing you to segment your network into workgroups and communicate across VLANs without degrading application performance. With these capabilities, you can boost the efficiency of your network by offloading internal traffic-handling tasks from your router and allowing it to manage primarily external traffic and security. You can minimize the need to manually configure routing devices and simplify the ongoing operation of the network.

Power Efficiency

The Cisco 350X Series integrates a variety of power-saving features across all models, providing the industry's most extensive energy-efficient switching portfolio. These switches are designed to conserve energy by optimizing power use, which helps protects the environment and reduce your energy costs. They provide an eco-friendly network solution without compromising performance. Cisco 350X Series switches feature:

- Support for the Energy Efficient Ethernet (IEEE 802.3az) standard, which reduces energy consumption by monitoring the amount of traffic on an active link and putting the link into a sleep state during quiet periods
- The latest application-specific integrated circuits (ASICs), which use low-power 65/40-nanometer technology and low-power, high-performance ARM CPUs
- Automatic power shutoff on ports when a link is down
- LEDs that can be turned off to save power
- Embedded intelligence to adjust signal strength based on the length of the connecting cable

Peace of Mind and Investment Protection

Cisco 350X Series switches offer the reliable performance and peace of mind you expect from a Cisco switch. When you invest in the Cisco 350 Series, you gain the benefit of:

- Limited lifetime warranty with next-business-day (NBD) advance replacement (where available; otherwise same day ship)
- A solution that has been rigorously tested to help ensure optimal network uptime to keep employees connected to primary resources and productive
- A solution designed and tested to easily and fully integrate with other Cisco voice, unified communications, security, and networking products, as part of a comprehensive technology platform for your business

Cisco Limited Lifetime Hardware Warranty

Cisco 350X Series switches offer a limited lifetime hardware warranty with NBD advance replacement (where available; otherwise same day ship) and a limited lifetime warranty for fans and power supplies.

In addition, Cisco offers software application updates for bug fixes for the warranty term and telephone technical support at no charge for the first 12 months following the date of purchase. To download software updates, go to http://software.cisco.com/download/navigator.html.

Product warranty terms and other information applicable to Cisco products are available at http://www.cisco.com/go/warranty.

World-Class Service and Support

Your time is valuable, especially when you have a problem affecting your business. Cisco 350X Series switches are backed by the Cisco SMARTnet® Total Care, which provides affordable peace-of-mind coverage. This subscription-based service helps you protect your investment and derive maximum value from Cisco SMB products. Delivered by Cisco and backed by your trusted partner, this comprehensive service includes software updates and access to the Cisco Support Center, and it extends technical service to three years.

Cisco SMB products are supported by professionals in the Cisco Support Center, a dedicated resource for small business customers and networks, with locations worldwide that are specifically trained to understand your needs. You also have access to extensive technical and product information through the Cisco Support Community, an online forum that enables you to collaborate with your peers and reach Cisco technical experts for support information.

Product Specifications

Table 1 describes product specifications.

Table 1. Specifications

Performance			
Switching capacity and forwarding rate **All switches are wire speed and nonblocking**	**Product Name**	**Capacity in Mpps (64-Byte Packets)**	**Switching Capacity (Gbps)**
	SG350X-24	95.23	128
	SG350X-24P	95.23	128
	SG350X-24MP	95.23	128
	SG350X-48	130.94	176
	SG350X-48P	130.94	176
	SG350X-48MP	130.94	176
	SG350XG-2F10	178.56	240
	SG350XG-24F	357.12	480
	SG350XG-24T	357.12	480
	SG350XG-48T	714.24	960

Layer 2 switching	
Spanning Tree Protocol	Standard 802.1d spanning tree support Fast convergence using 802.1w (Rapid Spanning Tree Protocol [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 8 groups ● Up to 8 ports per group with 16 candidate ports for each (dynamic) 802.3ad LAG
VLAN	Support for up to 4094 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. Autovoice 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).
Q-in-Q	VLANs transparently cross over a service provider network while isolating traffic among customers.
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.
HOL blocking	Head-of-line (HOL) blocking.
Layer 3	
IPv4 routing	Wirespeed routing of IPv4 packets Up to 8K static routes and up to 256 IP interfaces
Wirespeed IPv6 static routing	Up to 4K static routes and up to 200 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
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
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
User Datagram Protocol (UDP) relay	Relay of broadcast information across Layer 3 domains for application discovery or relaying of BOOTP/DHCP packets
Stacking	
Hardware stack	Up to 4 units in a stack. Up to 208 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, autostacking 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.
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.
ACLs	Support for up to 2K entries. Drop or rate limit based on source and destination MAC, VLAN ID or IP address, protocol, port, DSCP/IP precedence, TCP/User Datagram Protocol (UDP) source and destination ports, 802.1p priority, Ethernet type, Internet Control Message Protocol (ICMP) packets, Internet Group Management Protocol (IGMP) packets, TCP flag; ACL can be applied on both ingress and egress sides. Time-based ACLs supported.
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.

Standards	
Standards	IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbit/s Ethernet over fiber for LAN, IEEE 802.3an 10GBase-T 10 Gbit/s Ethernet over copper twisted pair cable, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient Ethernet, RFC 768, RFC 783, RFC 791, RFC 792, RFC 793, RFC 813, RFC 826, RFC 879, RFC 896, RFC 854, RFC 855, RFC 856, RFC 858, RFC 894, RFC 919, RFC 920, RFC 922, RFC 950, RFC 951, RFC 1042, RFC 1071, RFC 1123, RFC 1141, RFC 1155, RFC 1157, RFC 1213, RFC 1215, RFC 1286, RFC 1350, RFC 1442, RFC 1451, RFC 1493, RFC 1533, RFC 1541, RFC 1542, RFC 1573, RFC 1624, RFC 1643, RFC 1700, RFC 1757, RFC 1867, RFC 1907, RFC 2011, RFC 2012, RFC 2013, RFC 2030, RFC 2131, RFC 2132, RFC 2233, RFC 2576, RFC 2616, RFC 2618, RFC 2665, RFC 2666, RFC 2674, RFC 2737, RFC 2819, RFC 2863, RFC 3164, RFC 3176, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 4330
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 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
IPv6 RFC supported	RFC 4443 (which obsoletes RFC 2463): ICMPv6 RFC 4291 (which obsoletes RFC 3513): IPv6 address architecture RFC 4291: IP Version 6 Addressing Architecture RFC 2460: IPv6 Specification RFC 4861 (which obsoletes RFC 2461): Neighbor Discovery for IPv6 RFC 4862 (which obsoletes RFC 2462): IPv6 Stateless Address Autoconfiguration RFC 1981: Path MTU Discovery RFC 4007: IPv6 Scoped Address Architecture RFC 3484: Default address selection mechanism RFC 5214 (which obsoletes RFC 4214): ISATAP tunneling RFC 4293; MIB IPv6: Textual Conventions and General Group RFC 3595; Textual Conventions for IPv6 Flow Label
Management	
Web user interface	Built-in switch configuration utility for easy browser-based device configuration (HTTP/HTTPS). Supports simple and advanced mode, configuration, wizards, customizable dashboard, system maintenance, monitoring, online help, and universal search.
SNMP	SNMP versions 1, 2c, and 3 with support for traps, and SNMP v3 User-based Security Model (USM)

Standard MIBs	lldp-MIB	rfc2668-MIB
	lldpextdot1-MIB	rfc2737-MIB
	lldpextdot3-MIB	rfc2925-MIB
	lldpextmed-MIB	rfc3621-MIB
	rfc2674-MIB	rfc4668-MIB
	rfc2575-MIB	rfc4670-MIB
	rfc2573-MIB	trunk-MIB
	rfc2233-MIB	tunnel-MIB
	rfc2013-MIB	udp-MIB
	rfc2012-MIB	draft-ietf-bridge-8021x-MIB
	rfc2011-MIB	draft-ietf-bridge-rstpmib-04-MIB
	RFC-1212	draft-ietf-hubmib-etherif-mib-v3-00-MIB
	RFC-1215	draft-ietf-syslog-device-MIB
	SNMPv2-CONF	ianaaddrfamnumbers-MIB
	SNMPv2-TC	ianaifty-MIB
	p-bridge-MIB	ianaprot-MIB
	q-bridge-MIB	inet-address-MIB
	rfc1389-MIB	ip-forward-MIB
	rfc1493-MIB	ip-MIB
	rfc1611-MIB	RFC1155-SMI
	rfc1612-MIB	RFC1213-MIB
	rfc1850-MIB	SNMPv2-MIB
	rfc1907-MIB	SNMPv2-SMI
	rfc2571-MIB	SNMPv2-TM
	rfc2572-MIB	RMON-MIB
	rfc2574-MIB	rfc1724-MIB
	rfc2576-MIB	dcb-raj-DCBX-MIB-1108-MIB
	rfc2613-MIB	rfc1213-MIB
	rfc2665-MIB	rfc1757-MIB
Private MIBs	CISCOSB-lldp-MIB	CISCOSB-iprouter-MIB
	CISCOSB-brgmulticast-MIB	CISCOSB-ipv6-MIB
	CISCOSB-bridgemibobjects-MIB	CISCOSB-mnginf-MIB
	CISCOSB-bonjour-MIB	CISCOSB-lcli-MIB
	CISCOSB-dhcpcl-MIB	CISCOSB-localization-MIB
	CISCOSB-MIB	CISCOSB-mcmngr-MIB
	CISCOSB-wrandomtaildrop-MIB	CISCOSB-localization-MIB
	CISCOSB-traceroute-MIB	CISCOSB-mcmngr-MIB
	CISCOSB-telnet-MIB	CISCOSB-mng-MIB
	CISCOSB-stormctrl-MIB	CISCOSB-physdescription-MIB
	CISCOSBssh-MIB	CISCOSB-PoE-MIB
	CISCOSB-socket-MIB	CISCOSB-protectedport-MIB
	CISCOSB-sntp-MIB	CISCOSB-rmon-MIB
	CISCOSB-smon-MIB	CISCOSB-rs232-MIB
	CISCOSB-phy-MIB	CISCOSB-SecuritySuite-MIB
	CISCOSB-multisessionterminal-MIB	CISCOSB-snmp-MIB
	CISCOSB-mri-MIB	CISCOSB-specialbpdu-MIB
	CISCOSB-jumboframes-MIB	CISCOSB-banner-MIB
	CISCOSB-gvrp-MIB	CISCOSB-syslog-MIB
	CISCOSB-endofmib-MIB	CISCOSB-TcpSession-MIB
	CISCOSB-dot1x-MIB	CISCOSB-traps-MIB
	CISCOSB-deviceparams-MIB	CISCOSB-trunk-MIB
	CISCOSB-cli-MIB	CISCOSB-tuning-MIB
	CISCOSB-cdb-MIB	CISCOSB-tunnel-MIB
	CISCOSB-brgmacswitch-MIB	CISCOSB-udp-MIB
	CISCOSB-3sw2swtables-MIB	CISCOSB-vlan-MIB

	CISCOSB-smartPorts-MIB CISCOSB-tbi-MIB CISCOSB-macbaseprio-MIB CISCOSB-env_mib-MIB CISCOSB-policy-MIB CISCOSB-sensor-MIB CISCOSB-aaa-MIB CISCOSB-application-MIB CISCOSB-bridgesecurity-MIB CISCOSB-copy-MIB CISCOSB-CpuCounters-MIB CISCOSB-Custom1BonjourService-MIB CISCOSB-dhcp-MIB CISCOSB-dlf-MIB CISCOSB-dnscl-MIB CISCOSB-embweb-MIB CISCOSB-fft-MIB CISCOSB-file-MIB CISCOSB-greeneth-MIB CISCOSB-interfaces-MIB CISCOSB-interfaces_recovery-MIB CISCOSB-ip-MIB CISCOSB-iprouter-MIB CISCOSB-ipv6-MIB CISCOSB-mnginf-MIB CISCOSB-lcli-MIB CISCOSB-ipstdacl-MIB CISCOSB-eee-MIB CISCOSB-ssl-MIB CISCOSB-digitalkeymanage-MIB CISCOSB-qosclimib-MIB CISCOSB-vrrp-MIB CISCOSB-tbp-MIB CISCOSB-stack-MIB CISCOSMB-MIB CISCOSB-secsd-MIB CISCOSB-draft-ietf-entmib-sensor-MIB CISCOSB-draft-ietf-syslog-device-MIB CISCOSB-rfc2925-MIB CISCOSB-vrrpv3-MIB CISCO-SMI-MIB CISCOSB-DebugCapabilities-MIB CISCOSB-CDP-MIB CISCOSB-vlanVoice-MIB CISCOSB-EVENTS-MIB CISCOSB-sysmng-MIB CISCOSB-sct-MIB CISCO-TC-MIB CISCO-VTP-MIB CISCO-CDP-MIB
RMON	Embedded RMON software agent supports 4 RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis.
IPv4 and IPv6 dual stack	Coexistence of both protocol stacks to ease migration.
Firmware upgrade	• Web browser upgrade (HTTP/HTTPS) and TFTP and SCP • Upgrade can be initiated through console port as well • Dual images for resilient firmware upgrades
Port mirroring	Traffic on a port or LAG can be mirrored to another port for analysis with a network analyzer or RMON probe. Up to 8 source ports can be mirrored to one destination port.
VLAN mirroring	Traffic from a VLAN can be mirrored to a port for analysis with a network analyzer or RMON probe. Up to 8 source VLANs can be mirrored to one destination port.
Flow-based redirection and mirroring	Redirect or mirror traffic to a destination port or mirroring session based on flow.
Remote switch port analyzer (RSPAN)	Traffic can be mirrored across Layer 2 domain to a remote port on a different switch for easier troubleshooting.
sFlow agent	Switch can export sFlow sample to external collectors. sFlow provides visibility into network traffic down to flow level.
DHCP (options 12, 66, 67, 82, 129, and 150)	DHCP options facilitate tighter control from a central point (DHCP server), to obtain IP address, autoconfiguration (with configuration file download), DHCP Relay, and host name.
Autoconfiguration with secure copy (SCP) file download	Enables secure mass deployment with protection of sensitive data.
Text-editable configs	Config files can be edited with a text editor and downloaded to another switch, facilitating easier mass deployment.
Smartports	Simplified configuration of QoS and security capabilities.
Auto Smartports	Automatically applies the intelligence delivered through the Smartports roles to the port based on the devices discovered over Cisco Discovery Protocol or LLDP-MED. This facilitates zero-touch deployments.
Secure copy (SCP)	Securely transfer files to and from the switch.
Textview CLI	Scriptable CLI. A full CLI as well as a menu CLI are supported.
Cloud services	Support for Cisco Active Advisor.
Localization	Localization of GUI and documentation into multiple languages.

Login banner	Configurable multiple banners for web as well as CLI.
Time-based port operation	Link up or down based on user-defined schedule (when the port is administratively up).
Other management	Traceroute; single IP management; HTTP/HTTPS; SSH; RADIUS; port mirroring; TFTP upgrade; DHCP client; Simple Network Time Protocol (SNTP); Xmodem upgrade; cable diagnostics; Ping; syslog; Telnet client; SSH client; automatic time settings from Management Station.
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.
Disable port LEDs	LEDs can be manually turned off to save on energy.
General	
Jumbo frames	Frame sizes up to 9K bytes. The default MTU is 2K.
MAC table	64K addresses.
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.
Cisco Discovery Protocol	The switch advertises itself using the Cisco Discovery Protocol. It also learns the connected device and its characteristics using Cisco Discovery Protocol.
Product specifications	
Power over Ethernet	The following switches support 802.3at PoE+, 802.3af PoE, and Cisco prestandard (legacy) PoE on any of the RJ45 network ports. 60W PoE is also supported on selected RJ-45 network ports. Maximum power of 60W is delivered to any of the 60W PoE ports, and maximum power of 30W is delivered to any of the other RJ45 network ports, until the PoE budget for the switch is reached. The total power available for PoE per switch is as follows.

Model	Power Dedicated to PoE	Number of Ports That Support PoE+ and PoE	Number of Ports That Support 60W PoE, PoE+ and PoE
SG350X-24P	195W	16	8
SG350X-24MP	382W	16	8
SG350X-48P	382W	32	16
SG350X-48MP	740W	32	16

Power consumption (worst case)

Model Name	Green Power (Mode)	System Power Consumption	Power Consumption (with PoE)	Heat Dissipation (BTU/hr)
SG350X-24	EEE, Energy Detect, Short Reach	110V=32.5W 220V=32.5W	N/A	83.39
SG350X-24P	EEE, Energy Detect, Short Reach	110V=48.8W 220V=49.3W	110V=269.2W 220V=260.1W	764.18
SG350X-24MP	EEE, Energy Detect, Short Reach	110V=53.8W 220V=54.8W	110V=471.2W 220V=460.4W	1,607.80
SG350X-48	EEE, Energy Detect, Short Reach	110V=52.0W 220V=51.8W	N/A	177.43
SG350X-48P	EEE, Energy Detect, Short Reach	110V=76.3W 220V=76.9W	110V=494.3W 220V=483.1W	1,686.62
SG350X-48MP	EEE, Energy Detect, Short Reach	110V=82.9W 220V=82.9W	110V=893.1W 220V=878.0W	3,047.38
SG350XG-2F10	EEE, Energy Detect, Short Reach	110V=84.3W 220V=84.6W	N/A	288.67

	SG350XG-24F	EEE, Energy Detect, Short Reach	110V=76.6W 220V=77.5W	N/A	264.44
	SG350XG-24T	EEE, Energy Detect, Short Reach	110V=143.9W 220V=142.9W	N/A	491.01
	SG350XG-48T	EEE, Energy Detect, Short Reach	110V=264.4W 220V=255.8W	N/A	902.17
Ports	**Model Name**	**Total System Ports**	**Network Ports**	**Uplink Ports**	
	SG350X-24	24 GE + 4 10GE	24 GE	2 10GE copper/SFP+ combo + 2 SFP+	
	SG350X-24P	24 GE + 4 10GE	24 GE	2 10GE copper/SFP+ combo + 2 SFP+	
	SG350X-24MP	24 GE + 4 10GE	24 GE	2 10GE copper/SFP+ combo + 2 SFP+	
	SG350X-48	48 GE + 4 10GE	48 GE	2 10GE copper/SFP+ combo + 2 SFP+	
	SG350X-48P	48 GE + 4 10GE	48 GE	2 10GE copper/SFP+ combo + 2 SFP+	
	SG350X-48MP	48 GE + 4 10GE	48 GE	2 10GE copper/SFP+ combo + 2 SFP+	
	SG350XG-2F10	10 10G copper + 2 10G SFP+ plus 1 GE OOB management	10 10GE	2 10GE SFP+ (dedicated)	
	SG350XG-24F	22 10G SFP+ slots + 2 combo 10G copper/SFP+ plus 1 GE OOB management	22 10GE SFP+	2 10GE copper/SFP+ combo	
	SG350XG-24T	22 10G copper + 2 combo 10G copper/SFP+ plus 1 GE OOB management	22 10GE	2 10GE copper/SFP+ combo	
	SG350XG-48T	46 10G copper + 2 combo 10G copper/SFP+ plus 1 GE OOB management	46 10GE	2 10GE copper/SFP+ combo	
Console port	Cisco Standard RJ45 console port				
OOB management port	Dedicated Gigabit management port for out-of-band management on SG350XG models				
USB slot	USB Type-A slot on the front panel of the switch for easy file and image management				
Buttons	Reset button				
Cabling type	Unshielded twisted pair (UTP) Category 5 or better; fiber options (SMF and MMF); coaxial SFP+				
LEDs	System, master, stack ID, link/speed per port				
Flash	256 MB				
CPU	800 MHz (dual-core) ARM				
CPU memory	512 MB				
Packet buffer	All numbers are aggregate across all ports because the buffers are dynamically shared:				
	Model Name	**Packet Buffer**			
	SG350X-24	1.5 MB			
	SG350X-24P	1.5 MB			
	SG350X-24MP	1.5 MB			
	SG350X-48	3 MB			
	SG350X-48P	3 MB			
	SG350X-48MP	3 MB			
	SG350XG-2F10	2 MB			
	SG350XG-24F	2 MB			

	SG350XG-24T		2 MB	
	SG350XG-48T		4 MB	
Supported SFP/SFP+ modules	**SKU**	**Media**	**Speed**	**Maximum Distance**
	MGBSX1	Multimode fiber	1000 Mbps	500 m
	MGBLH1	Single-mode fiber	1000 Mbps	40 km
	MGBT1	UTP cat 5e	1000 Mbps	100 m
	SFP-H10GB-CU1M	Copper coax	10 Gig	1 m
	SFP-H10GB-CU3M	Copper coax	10 Gig	3 m
	SFP-H10GB-CU5M	Copper coax	10 Gig	5 m
	SFP-10G-SR	Multimode fiber	10 Gig	26 m - 400 m
	SFP-10G-LR	Single-mode fiber	10 Gig	10 km
	SFP-10G-SR-S	Multimode fiber	10 Gig	26 m - 400 m
	SFP-10G-LR-S	Single-mode fiber	10 Gig	10 km
Environmental				
Unit dimensions (W x H x D)	**Model Name**		**Unit Dimensions**	
	SG350X-24		440 x 44 x 257 mm (17.3 x 1.45 x 10.12 in)	
	SG350X-24P		440 x 44 x 350 mm (17.3 x 1.45 x 13.78 in)	
	SG350X-24MP		440 x 44 x 350 mm (17.3 x 1.45 x 13.78 in)	
	SG350X-48		440 x 44 x 257 mm (17.3 x 1.45 x 10.12 in)	
	SG350X-48P		440 x 44 x 350 mm (17.3 x 1.45 x 13.78 in)	
	SG350X-48MP		440 x 44 x 450 mm (17.3 x 1.45 x 17.72 in)	
	SG350XG-2F10		440 x 44 x 350 mm (17.3 x 1.45 x 13.78 in)	
	SG350XG-24F		440 x 44 x 350 mm (17.3 x 1.45 x 13.78 in)	
	SG350XG-24T		440 x 44 x 450 mm (17.3 x 1.45 x 17.72 in)	
	SG350XG-48T		440 x 44 x 450 mm (17.3 x 1.45 x 17.72 in)	
Unit weight	**Model Name**		**Unit Weight**	
	SG350X-24		4.32 kg (9.52 lb)	
	SG350X-24P		4.93 kg (10.41 lb)	
	SG350X-24MP		5.69 kg (11.75 lb)	
	SG350X-48		3.73 kg (8.22 lb)	
	SG350X-48P		5.82 kg (12.83 lb)	
	SG350X-48MP		6.69 kg (14.75 lb)	
	SG350XG-2F10		4.03 kg (8.88 lb)	
	SG350XG-24F		4.16 kg (9.17 lb)	
	SG350XG-24T		5.57 kg (12.28 lb)	
	SG350XG-48T		7.43 kg (16.38 lb)	
Power	100 - 240V 47 - 63 Hz, internal, universal			
Certification	UL (UL 60950), CSA (CSA 22.2), CE mark, FCC Part 15 (CFR 47) Class A			
Operating temperature	SG350XG-2F10, SG350XG-24F, SG350XG-24T, SG350XG-48T 32° to 122°F (0° to 50°C)			
Storage temperature	-4° to 158°F (-20° to 70°C)			
Operating humidity	10% to 90%, relative, noncondensing			

Storage humidity	10% to 90%, relative, noncondensing
Acoustic noise and mean time between failures (MTBF)	

Model Name	Fan (Number)	Acoustic Noise	MTBF at 50°C (Hours)
SG350X-24	1	0°C - 30°C: 36.3dB 50°C: 49.3dB	385,289
SG350X-24P	2	0°C - 30°C: 41.0dB 50°C: 52.9dB	244,654
SG350X-24MP	2	0°C - 30°C: 43.3dB 50°C: 52.3dB	144,617
SG350X-48	1	0°C - 30°C: 35.0dB 50°C: 51.7dB	248,842
SG350X-48P	3	0°C - 30°C: 43.8dB 50°C: 52.1dB	164,614
SG350X-48MP	4	0°C - 30°C: 43.2dB 50°C: 53.2dB	171,530
SG350XG-2F10	3	0°C - 30°C: 38.9dB 50°C: 49.7dB	291,863
SG350XG-24F	4	0°C - 25°C: 36.4dB	194,544
SG350XG-24T	4	0°C–30°C: 40.7dB 50°C: 51.7dB	347,052
SG350XG-48T	4	0°C–30°C: 47.7dB 50°C: 58.9dB	131,767

Warranty	Limited lifetime with next-business-day advance replacement (where available, otherwise same day ship)

Package Contents

- Cisco Small Business 350X Series Stackable Managed Switch
- Power cord
- Mounting kit included with all models
- Serial cable
- Quick Start Guide

Minimum Requirements

- Web browser: Mozilla Firefox version 8 or later; Microsoft Internet Explorer version 7 or later, Safari, Chrome
- Category 6a Ethernet network cable for 10 Gig speeds at up to 100m
- TCP/IP, network adapter, and network operating system (such as Microsoft Windows, Linux, or Mac OS X) installed

Ordering Information

Table 2 provides ordering information.

Table 2. Ordering Information

Model Name	Product Order ID Number	Description
SG350X-24	SG350X-24-K9	• 24 x 10/100/1000 ports • 4 x 10 Gigabit Ethernet (2 x 10GBase-T/SFP+ combo + 2 x SFP+)
SG350X-24P	SG350X-24P-K9	• 24 x 10/100/1000 PoE+ ports with 195W power budget • 4 x 10 Gigabit Ethernet (2 x 10GBase-T/SFP+ combo + 2 x SFP+)
SG350X-24MP	SG350X-24MP-K9	• 24 x 10/100/1000 PoE+ ports with 382W power budget • 4 x 10 Gigabit Ethernet (2 x 10GBase-T/SFP+ combo + 2 x SFP+)
SG350X-48	SG350X-48-K9	• 48 x 10/100/1000 ports • 4 x 10 Gigabit Ethernet (2 x 10GBase-T/SFP+ combo + 2 x SFP+)
SG350X-48P	SG350X-48P-K9	• 48 x 10/100/1000 PoE+ ports with 382W power budget

Model Name	Product Order ID Number	Description
		• 4 x 10 Gigabit Ethernet (2 x 10GBase-T/SFP+ combo + 2 x SFP+)
SG350X-48MP	SG350X-48MP-K9	• 48 x 10/100/1000 PoE+ ports with 740W power budget • 4 x 10 Gigabit Ethernet (2 x 10GBase-T/SFP+ combo + 2 x SFP+)
SG350XG-2F10	SG350XG-2F10-K9	• 10 x 10 Gigabit Ethernet 10GBase-T copper port • 2 x 10 Gigabit Ethernet SFP+ (dedicated) • 1 x Gigabit Ethernet management port
SG350XG-24F	SG350XG-24F-K9	• 24 x 10 Gigabit Ethernet SFP+ • 2 x 10 Gigabit Ethernet 10Gbase-T copper port (combo with 2 SFP+) • 1 x Gigabit Ethernet management port
SG350XG-24T	SG350XG-24T-K9	• 24 x 10 Gigabit Ethernet 10GBase-T copper port • 2 x 10 Gigabit Ethernet SFP+ (combo with 2 copper ports) • 1 x Gigabit Ethernet management port
SG350XG-48T	SG350XG-48T-K9	• 48 x 10 Gigabit Ethernet 10GBase-T copper port • 2 x 10 Gigabit Ethernet SFP+ (combo with 2 copper ports) • 1 x Gigabit Ethernet management port

* Each combo port has one 10/100/1000/10000 copper Ethernet port and one SFP+ Gigabit Ethernet slot, with one port active at a time.

An Advanced Technology Backbone for Growing Businesses

Growth is never a bad thing. But as you gain new customers and a higher profile, you need a business technology platform capable of delivering a higher level of service and reliability. With more users, more devices and applications, and more exposure to security threats, a switching platform designed for a smaller operation simply cannot meet your growing needs. It's time for a network that will support your business as you take it to the next level. Cisco 350X Series switches provide the advanced feature set, reliability, and investment protection your business needs, today and in the future.

For More Information

To find out more about the Cisco 350X Series, visit http://www.cisco.com/go/350Xswitches.

To learn about other products and solutions in the Cisco Small Business portfolio, visit http://www.cisco.com/go/smallbusiness.

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.

Printed in USA C78-735986-01 03/17