

Cisco 350X Series Stackable Managed Switches

Easy-to-Use 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 Cisco 350XG models provide 12, 24, or 48 ports of 10 Gigabit Ethernet, providing a solid foundation for your current business applications as well as those you are planning for the future. At the same time, these switches are easy to deploy and manage without a large IT staff. The 350X 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 troubleshot 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.

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 www.cisco.com/go/findit.)

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 a maximum of 48⁺ 192 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.

Network-wide 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. For example, 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.

Additionally, Cisco 350X models provide static Layer 3 routing features. With these capabilities, 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 protect 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 350X 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 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[®] Support Service, 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

Feature	Description
Performance	
Switching capacity and forwarding rate All switches are wire-speed and nonblocking.	Product Name
	Capacity in mpps (64-byte packets)
	Switching Capacity (Gbps)
	SG350XG-24T
	SG350XG-24F
SG350XG-48T	
SG350XG-2F10	
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) <ul style="list-style-type: none"> 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 4096 VLANs simultaneously Port-based and 802.1Q tag-based VLANs MAC-based VLAN Management VLAN Private VLAN Edge (PVE), also known as Protected Port, with multiple uplinks Guest VLAN Unauthenticated VLAN Protocol-based VLAN CPE VLAN Dynamic VLAN assignment via 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 network-wide 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.
Jumbo Frames	Frames up to 10K bytes in length.
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 2K (2048) static 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

Feature	Description
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.
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
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 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, etc.) 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.
Layer 2 isolation (PVE) with community VLAN	Private VLAN Edge 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	Levels 1, 7, and 15 privilege levels.

Feature	Description
in CLI	
ACLs	Support for up to 3K (3072). 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. 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 based
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 802.3x Flow Control, IEEE 802.3ad LACP, 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, RFC 768, RFC 783, RFC 791, RFC 792, RFC 793, RFC 813, RFC 879, RFC 896, RFC 826, RFC 854, RFC 855, RFC 856, RFC 858, RFC 894, RFC 919, RFC 922, RFC 920, RFC 950, RFC 951, RFC 1042, RFC 1071, RFC 1123, RFC 1141, RFC 1155, RFC 1157, RFC 1350, RFC 1533, RFC 1541, RFC 1542, RFC 1624, RFC 1700, RFC 1867, RFC 2030, RFC 2616, RFC 2131, RFC 2132, RFC 3164, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 2576, RFC 4330, RFC 1213, RFC 1215, RFC 1286, RFC 1442, RFC 1451, RFC 1493, RFC 1573, RFC 1643, RFC 1757, RFC 1907, RFC 2011, RFC 2012, RFC 2013, RFC 2233, RFC 2618, RFC 2665, RFC 2666, RFC 2674, RFC 2737, RFC 2819, RFC 2863, RFC 1157, RFC 1493, RFC 1215, RFC 3416
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	

Feature	Description	
Web user interface	Built-in switch configuration utility for easy browser-based device configuration (HTTP/HTTPS). Supports configuration, system dashboard, system maintenance, and monitoring.	
SNMP	SNMP versions 1, 2c, and 3 with support for traps and SNMP v3 user-based security model (USM)	
Standard MIBs	lldp-MIB lldpextdot1-MIB lldpextdot3-MIB lldpextmed-MIB rfc2674-MIB rfc2575-MIB rfc2573-MIB rfc2233-MIB rfc2013-MIB rfc2012-MIB rfc2011-MIB RFC-1212 RFC-1215	rfc2665-MIB rfc2668-MIB rfc2737-MIB rfc3621-MIB rfc4668-MIB rfc4670-MIB trunk-MIB tunnel-MIB udp-MIB draft-ietf-bridge-8021x-MIB draft-ietf-bridge-rstpmib-04-MIB draft-ietf-hubmib-etherif-mib-v3-00-MIB ianaaddrfamnumbers-MIB
Standard MIBs (continued)	SNMPv2-CONF SNMPv2-TC p-bridge-MIB q-bridge-MIB rfc1389-MIB rfc1493-MIB rfc1611-MIB rfc1612-MIB rfc1850-MIB rfc1907-MIB rfc2571-MIB rfc2572-MIB rfc2574-MIB rfc2576-MIB rfc2613-MIB	ianaifty-MIB ianaprot-MIB inet-address-MIB ip-forward-MIB ip-MIB RFC1155-SMI RFC1213-MIB SNMPv2-MIB SNMPv2-SMI SNMPv2-TM RMON-MIB rfc1724-MIB dcb-raj-DCBX-MIB-1108-MIB rfc1213-MIB rfc1757-MIB
Private MIBs	CISCOB-lldp-MIB CISCOB-brgmulticast-MIB CISCOB-bridgemibobjects-MIB CISCOB-bonjour-MIB CISCOB-dhcpcl-MIB CISCOB-MIB CISCOB-wrandomtaildrop-MIB CISCOB-traceroute-MIB CISCOB-telnet-MIB CISCOB-stormctrl-MIB CISCOBssh-MIB CISCOB-socket-MIB CISCOB-sntp-MIB CISCOB-smon-MIB CISCOB-phy-MIB CISCOB-multisessionterminal-MIB CISCOB-mri-MIB CISCOB-jumboframes-MIB CISCOB-gvrp-MIB CISCOB-endofmib-MIB CISCOB-dot1x-MIB CISCOB-deviceparams-MIB CISCOB-cli-MIB CISCOB-cdb-MIB	CISCOB-iprouter-MIB CISCOB-ipv6-MIB CISCOB-mnginf-MIB CISCOB-lcli-MIB CISCOB-localization-MIB CISCOB-mcmngr-MIB CISCOB-mng-MIB CISCOB-physdescription-MIB CISCOB-PoE-MIB CISCOB-protectedport-MIB CISCOB-rmon-MIB CISCOB-rs232-MIB CISCOB-SecuritySuite-MIB CISCOB-snmp-MIB CISCOB-specialbpdu-MIB CISCOB-banner-MIB CISCOB-syslog-MIB CISCOB-TcpSession-MIB CISCOB-traps-MIB CISCOB-trunk-MIB CISCOB-tuning-MIB CISCOB-tunnel-MIB CISCOB-udp-MIB CISCOB-vlan-MIB

Feature	Description
	<p>CISCOB-brgmacswitch-MIB CISCOB-3sw2swtables-MIB CISCOB-smartPorts-MIB CISCOB-tbi-MIB CISCOB-macbaseprio-MIB CISCOB-env_mib-MIB CISCOB-policy-MIB CISCOB-sensor-MIB CISCOB-aaa-MIB CISCOB-application-MIB CISCOB-bridgesecurity-MIB CISCOB-copy-MIB CISCOB-CpuCounters-MIB CISCOB-Custom1BonjourService-MIB CISCOB-dhcp-MIB</p>
	<p>CISCOB-ipstdacl-MIB CISCOB-eee-MIB CISCOB-ssl-MIB CISCOB-digitalkeymanage-MIB CISCOB-qosclimib-MIB CISCOB-vrrp-MIB CISCOB-tbp-MIB CISCOB-stack-MIB CISCOB-MIB CISCOB-secsd-MIB CISCOB-draft-ietf-entmib-sensor-MIB CISCOB-draft-ietf-syslog-device-MIB CISCOB-rfc2925-MIB CISCOB-vrrpv3-MIB CISCO-SMI-MIB</p>
Private MIBs (continued)	<p>CISCOB-dif-MIB CISCOB-dnscl-MIB CISCOB-embweb-MIB CISCOB-fft-MIB CISCOB-file-MIB CISCOB-greeneth-MIB CISCOB-interfaces-MIB CISCOB-interfaces_recovery-MIB CISCOB-ip-MIB</p>
	<p>CISCOB-DebugCapabilities-MIB CISCOB-CDP-MIB CISCOB-vlanVoice-MIB CISCOB-EVENTS-MIB CISCOB-sysmng-MIB CISCOB-sct-MIB CISCO-TC-MIB CISCO-VTP-MIB CISCO-CDP-MIB</p>
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	<ul style="list-style-type: none"> • 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 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.
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 and a menu CLI are supported.
Cloud Services	Support for Cisco Small Business and Cisco OnPlus.
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; BOOTP; Simple Network Time Protocol (SNTP); Xmodem upgrade; cable diagnostics; Ping; syslog; Telnet client (SSH secure support); Automatic time settings from Management Station.
Green (Power Efficiency)	

Feature	Description					
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 cable shorter than 10m. Supported on Gigabit Ethernet models.					
EEE compliant (802.3az)	Supports IEEE 802.3az on all Gigabit copper ports.					
Disable port LEDs	LEDs can be manually turned off to save on energy.					
General						
Jumbo frames	Frame sizes up to 10K 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 via Cisco Discovery Protocol.					
Product Specifications						
Power consumption (worst case)	Model Name	Green Power (mode)	System Power Consumption	Power Consumption (with PoE)	Heat Dissipation (BTU/hr)	
	SG350XG-24T	Energy Detect	110V=72.3W 220V=71.8W	N/A	288.67	
	SG350XG-24F	N/A	110V=42.81W 220V=43.1W	N/A	264.44	
	SG350XG-48T	Energy Detect	110V=131.7W 220V=130.5W	N/A	491.01	
	SG350XG-2F10	Energy Detect	110V=50.1W 220V=50.5W	N/A	902.17	
Ports	Model Name	Total System Ports	RJ-45 Ports	Combo Ports (RJ-45 + SFP)		
	SG350XG-24T	22 XG copper + 2 combo XG copper/SFP+ plus 1 GE OOB management	22 XG	2 combo XG copper/SFP+		
	SG350XG-24F	22 XG SFP+ slots + 2 combo XG copper/SFP+ plus 1 GE OOB management	2 XG combo	22 SFP+ slots plus 2 XG copper/SFP+ combo		
	SG350XG-48T	46 XG copper + 2 combo XG copper/SFP+ plus 1 GE OOB management	46 XG	2 combo XG copper/SFP+		
	SG350XG-2F10T	10 XG copper + 2 combo XG copper/SFP+ plus 1 GE OOB management	10 XG	2 combo XG copper/SFP+		
USB slot	For file-management purposes					
Buttons	Reset button					
Cabling type	Unshielded twisted pair (UTP) Category 6e 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, as the buffers are dynamically shared:					
	Model Name	Packet Buffer				
	SG350XG-24T	16Mb				

Feature	Description				
Supported SFP/SFP+ modules	SG350XG-24F		16Mb		
	SG350XG-48T		32Mb		
	SG350XG-2F10		8Mb		
	SKU	Media	Speed	Maximum Distance	
	MGBBX1	Single-mode fiber	1000 Mbps	10 km	
	MGBSX1	Multimode fiber	1000 Mbps	500 m	
	MGBLH1	Single-mode fiber	1000 Mbps	40 km	
	MGBLX1	Single-mode fiber	1000 Mbps	10 km	
	MGBT1	UTP cat 5e	1000 Mbps	100 m	
	SFP-H10GB-CU1M	Copper coax	10G	1 m	
	SFP-H10GB-CU3M	Copper coax	10G	3 m	
	SFP-H10GB-CU5M	Copper coax	10G	5 m	
SFP-10G-SR	Multimode fiber	10 Gig	26 m - 400 m		
SFP-10G-LR	Single-mode fiber	10 Gig	10 km		
Environmental					
Unit Dimensions (W x H x D)	Model Name		Unit Dimensions		
	SG350XG-24T		440 x 44 x 350 mm		
	SG350XG-24F		440 x 44 x 350 mm		
	SG350XG-48T		440 x 44 x 450 mm		
	SG350XG-2F10		440 x 44 x 257 mm		
Unit weight	Model Name		Unit Weight		
	SG350XG-24T		5.57 kg		
	SG350XG-24F		4.16 kg		
	SG350XG-48T		7.43 kg		
	SG350XG-2F10		4.03 kg		
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-24T, SG350XG-24F, SG350XG-48T, SG350XG-2F10 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 @ 40°C (Hours)
	SG350XG-24T		4	0°C-30°C: 40.7dB 50°C: 51.7dB	229,393
	SG350XG-24F		4	0°C-25°C: 36.4dB	121,050
	SG350XG-48T		4	0°C-30°C: 47.7dB 50°C: 58.9dB	131,767
	SG350XG-2F10		3	0°C-30°C: 38.9dB 50°C: 49.7dB	291,863
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
10-Gigabit		
SG350XG-24T	SG350XG-24T-K9	<ul style="list-style-type: none"> • 24 10 Gigabit Ethernet 10GBASE-T copper port • 2 10 Gigabit Ethernet SFP+ (combo with 2 copper ports) • 1 Gigabit Ethernet management port
SG350XG-24F	SG350XG-24F-K9	<ul style="list-style-type: none"> • 24 10 Gigabit Ethernet SFP+ • 2 10 Gigabit Ethernet 10GBASE-T copper port (combo with 2 SFP+) • 1 Gigabit Ethernet management port
SG350XG-48T	SG350XG-48T-K9	<ul style="list-style-type: none"> • 48 10 Gigabit Ethernet 10GBASE-T copper port • 2 10 Gigabit Ethernet SFP+ (combo with 2 copper ports) • 1 Gigabit Ethernet management port
SG350XG-2F10	SG350XG-2F10-K9	<ul style="list-style-type: none"> • 12 10 Gigabit Ethernet 10GBASE-T copper port • 2 10 Gigabit Ethernet SFP+ • 1 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.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. [Learn more.](#)

For More Information

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

To learn about other products and solutions in the Cisco Small Business portfolio, visit 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.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)