Cisco 350 Series Managed Switches

Easy-to-Use Managed Switches That Provide the Ideal Combination of Features and Affordability

To stay ahead in a competitive marketplace, 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 effect on your profits. 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 350 Series (Figure 1).

Figure 1. Cisco 350 Series Managed Switches

Cisco 350 Series Switches

The Cisco 350 Series, part of the Cisco Small Business line of network solutions, is a portfolio of affordable managed switches that provides a reliable foundation for your business network. These switches deliver the features you need to improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth to deliver information and applications more effectively. Easy to set up and use, the Cisco 350 Series provides the ideal combination of affordability and capabilities for small businesses and helps you create a more efficient, better-connected workforce.

The Cisco 350 Series is a broad portfolio of fixed-configuration managed Ethernet switches. Models are available with 48 ports of Fast Ethernet and 10 to 28 ports of Gigabit Ethernet connectivity, providing optimal flexibility to create exactly the right network foundation for your business. However, unlike other small business switching solutions that provide managed network capabilities only in the costliest models, all Cisco 350 Series Switches support the advanced security management capabilities and network features you need to support business-class data, voice, security, and wireless technologies. At the same time, these switches are simple to deploy and configure, allowing you to take advantage of the managed network services your business needs.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Business Applications

Whether you need a basic high-performance network to connect employee computers or a solution to deliver data, voice, and video services, the Cisco 350 Series offers a solution to meet your needs. Possible deployment scenarios include:

- **Secure desktop connectivity:** Cisco 350 Series Switches can simply and securely connect employees working in small offices with each other and with all of the servers, printers, and other devices they use. High performance and reliable connectivity help speed file transfers and data processing, improve network uptime, and keep your employees connected and productive.
- **Secure wireless connectivity:** With its advanced security features, Power over Ethernet, Auto Smartports, QoS, VLAN, and access control features, the Cisco 350 Series Switches are the perfect foundation to add business-grade wireless to a business network.
- **Unified communications:** As a managed network solution, the Cisco 350 Series provides the performance and advanced traffic-handling intelligence you need to deliver all communications and data over a single network. Cisco offers a complete portfolio of IP telephony and other unified communications products designed for businesses. Cisco 350 Series Switches have been rigorously tested to help ensure easy integration and full compatibility with these and other products, providing a complete business solution.
- **Highly secure guest connectivity.** Cisco 350 Series Switches let you extend highly secure network connectivity to guests in a variety of settings, such as a hotel, an office waiting room, or any other area open to nonemployee users. Using powerful but easy-to-configure security and traffic segmentation capabilities, you can isolate your vital business traffic from guest services and keep guests' network sessions private from each other.

Features and Benefits

Cisco 350 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 350 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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

- 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.)

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. The Cisco 350 Series 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.

Strong Security

Cisco 350 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 predesignated 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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Power over Ethernet

Cisco 350 Series Switches are available with up to 48 PoE ports of Fast Ethernet or up to 24 ports of Gigabit Ethernet connectivity. This capability simplifies advanced technology deployments such as IP telephony, wireless, and IP surveillance by allowing you to connect and power network endpoints over a single Ethernet cable. With no need to install separate power supplies for IP phones or wireless access points, you can take advantage of advanced communications technologies more quickly and at a lower cost. Models support 802.3af PoE, 802.3at PoE+, and 802.3xx 60W PoE.

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 350 Series can support the transition to the next generation of networking and operating systems such as Windows 8, 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 350 Series switches have successfully completed rigorous IPv6 testing and have received the USGv6 and IPv6 Gold certification.

Advanced Layer 3 Traffic Management

The Cisco 350 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 350 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 350 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 350 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

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

- 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

Expansion Ports

The Cisco 350 Series provides more ports per Gigabit Ethernet switch than traditional switch models, giving you more flexibility to connect and empower your business. Gigabit Ethernet models offer up to 28 ports to give you more value, versus the 24-port variety with four shared ports that's common in the market. The Cisco 350 Series also offers mini gigabit interface converter (mini-GBIC) expansion slots that give you the option to add fiber-optic or Gigabit Ethernet uplink connectivity to the switch. With the ability to increase the connectivity range of the switches, you have more flexibility to design your network around your unique business environment and to easily connect switches on different floors or across the business.

Peace of Mind and Investment Protection

Cisco 350 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 benefits 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.
- Complimentary software updates for bug fixes for the warranty term. To download software updates, go to http://www.cisco.com/cisco/web/download/index.html.
- Telephone technical support at no charge for the first 12 months following the date of purchase.
- Product warranty terms and other information applicable to Cisco products are available at http://www.cisco.com/go/warranty.
- Cisco Small Business products are supported by professionals in Cisco Small Business Support Center locations worldwide who are specifically trained to understand your needs. The Cisco Small Business Support Community, an online forum, enables you to collaborate with your peers and reach Cisco technical experts for support information.

Cisco Limited Lifetime Hardware Warranty

Cisco 350 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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

World-Class Service and Support

Your time is valuable, especially when you have a problem affecting your business. Cisco 350 Series switches are backed by Cisco SMARTnet® Total Care™ which provides affordable peace-of-mind coverage. 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 gives the product specifications for the Cisco 350 Series Switches.

Table 1. Product Specifications

Feature	Description		
Performance			
Switching capacity and forwarding rate **All switches are wire speed and nonblocking**	**Model Name**	**Capacity in Millions of Packets per Second (mpps) (64-byte packets)**	**Switching Capacity in Gigabits per Second (Gbps)**
	SF350-48	13.10	17.6
	SF350-48P	13.10	17.6
	SF350-48MP	13.10	17.6
	SG350-10	14.88	20.0
	SG350-10P	14.88	20.0
	SG350-10MP	14.88	20.0
	SG355-10MP	14.88	20.0
	SG350-28	41.67	56.0
	SG350-28P	41.67	56.0
	SG350-28MP	41.67	56.0
USB slot	For file-management purposes		
Layer 2 Switching			
Spanning Tree Protocol	Standard 802.1d Spanning Tree support Fast convergence using 802.1w (Rapid Spanning Tree [RSTP]), enabled by default 8 instances are supported Multiple Spanning Tree instances using 802.1s (MSTP)		
Port grouping	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 link aggregation		
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 ports, with multiple uplinks Guest VLAN Unauthenticated VLAN Dynamic VLAN assignment via RADIUS server along with 802.1x client authentication CPE VLAN		

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Feature	Description
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 (also known as MVR)
Q-in-Q VLAN	VLANs transparently cross a service provider network while isolating traffic among customers
Generic VLAN Registration Protocol (GVRP)/Generic Attribute Registration Protocol (GARP)	Protocols for automatically propagating and configuring VLANs in a bridged domain
Unidirectional Link Detection (UDLD)	UDLD monitors physical connection to detect unidirectional links caused by incorrect wiring or cable/port faults to prevent forwarding loops and blackholing of traffic in switched networks
Dynamic Host Configuration Protocol (DHCP) Relay at Layer 2	Relay of DHCP traffic to DHCP server in different VLAN; works with DHCP Option 82
Internet Group Management Protocol (IGMP) versions 1, 2, and 3 snooping	IGMP limits bandwidth-intensive multicast traffic to only the requesters; supports 1K 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
Head-of-line (HOL) blocking	HOL blocking prevention
Jumbo frames	Up to 9K (9216) bytes
Layer 3	
IPv4 routing	Wirespeed routing of IPv4 packets Up to 512 static routes and up to 128 IP interfaces
Classless Interdomain Routing (CIDR)	Support for CIDR
Layer 3 Interface	Configuration of Layer 3 interface on physical port, LAG, VLAN interface, or loopback interface
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
DHCP Server	Switch functions as an IPv4 DHCP server serving IP addresses for multiple DHCP pools/scopes Support for DHCP options
Security	
Secure Shell (SSH) Protocol	SSH is a secure replacement for Telnet traffic. SCP also uses SSH. SSH v1 and v2 are supported
Secure Sockets Layer (SSL)	SSL support: Encrypts all HTTPS traffic, allowing highly secure access to the browser-based management GUI in the switch
IEEE 802.1X (Authenticator role)	802.1X: 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 Bridge Protocol Data Unit (BPDU) Guard	A security mechanism to protect the network from invalid configurations. A port enabled for BPDU Guard is shut down if a BPDU message is received on that port.
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 DHCP Servers.
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 addresses in the ARP packet. This prevents man-in-the-middle attacks.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Feature	Description
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.
Layer 2 isolation Private VLAN Edge (PVE) with community VLAN	PVE (also known as protected ports) provides Layer 2 isolation between devices in the same VLAN, supports multiple uplinks.
Port security	The ability to lock source MAC addresses to ports and limits the number of learned MAC addresses.
RADIUS/TACACS+	Supports RADIUS and TACACS authentication. Switch functions as a client.
Storm control	Broadcast, multicast, and unknown unicast
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.
DoS prevention	Denial-of-service (DOS) attack prevention
ACLs	Support for up to 512 rules Drop or rate limit based on source and destination MAC, VLAN ID or IP address, protocol, port, differentiated services code point (DSCP)/IP precedence, TCP/UDP source and destination ports, 802.1p priority, Ethernet type, Internet Control Message Protocol (ICMP) packets, IGMP packets, TCP flag, time-based ACLs supported.
Quality of Service	
Priority levels	8 hardware queues
Scheduling	Strict priority and weighted round-robin (WRR) Queue assignment based on DSCP and class of service (802.1p/CoS)
Class of service	Port based; 802.1p VLAN priority based; IPv4/v6 IP precedence/type of service (ToS)/DSCP based; differentiated services (DiffServ); classification and remarking ACLs, trusted QoS.
Rate limiting	Ingress policer; egress shaping and 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 LACP, IEEE 802.3z Gigabit Ethernet, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w RSTP, 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 1042, RFC 1071, RFC 1123, RFC 1141, RFC 1155, RFC 1157, RFC 1350, RFC 1533, RFC 1541, 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 maximum transmission unit (MTU) discovery Duplicate address detection (DAD) ICMP version 6 IPv6 over IPv4 network with Intrasite Automatic Tunnel Addressing Protocol (ISATAP) support USGv6 and IPv6 Gold Logo certified
IPv6 QoS	Prioritize IPv6 packets in hardware
IPv6 ACL	Drop or rate limit IPv6 packets in hardware

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Feature	Description	
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, Simple Network Time Protocol (SNTP), Trivial File Transfer Protocol (TFTP), SNMP, RADIUS, syslog, DNS client, Telnet Client, DHCP Client, DHCP Autoconfig, IPv6 DHCP Relay, TACACS	
IPv6 RFCs supported	RFC 4443 (which obsoletes RFC2463): ICMP version 6 RFC 4291 (which obsoletes RFC 3513): IPv6 address architecture RFC 4291: IPv6 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 configuration, system dashboard, system maintenance, and monitoring.	
SNMP	SNMP versions 1, 2c, and 3 with support for traps, and SNMP version 3 user-based security model (USM)	
Standard MIBs	draft-ietf-bridge-8021x-MIB draft-ietf-bridge-rstpmib-04-MIB draft-ietf-hubmib-etherif-MIB-v3-00-MIB draft-ietf-syslog-device-MIB ianaaddrfamnumbers-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.my dcb-raj-DCBX-MIB-1108-MIB rfc1724-MIB RFC-1212.my_for_MG-Soft rfc1213-MIB rfc1757-MIB RFC- 1215.my SNMPv2- CONF.my SNMPv2-TC.my rfc2674-MIB rfc2575-MIB rfc2573-MIB rfc2233-MIB rfc2013-MIB rfc2012-MIB	rfc2011-MIB draft-ietf-entmib-sensor-MIB lldp-MIB lldpextdot1-MIB lldpextdot3-MIB lldpextmed-MIB 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 rfc2665-MIB rfc2668-MIB rfc2737-MIB rfc2925-MIB rfc3621-MIB rfc4668-MIB rfc4670-MIB trunk-MIB tunnel-MIB udp-MIB

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Feature	Description	
Private MIBs	CISCOSB-lldp-MIB CISCOSB-brgmulticast-MIB CISCOSB-bridgemibobjects-MIB CISCOSB-bonjour-MIB CISCOSB-dhcpcl-MIB CISCOSB-MIB CISCOSB-wrandomtaildrop-MIB CISCOSB-traceroute-MIB CISCOSB-telnet-MIB CISCOSB-stormctrl-MIB CISCOSB-ssh-MIB CISCOSB-socket-MIB CISCOSB-sntp-MIB CISCOSB-smon-MIB CISCOSB-phy-MIB CISCOSB-multisessionterminal-MIB CISCOSB-mri-MIB CISCOSB-jumboframes-MIB CISCOSB-gvrp-MIB CISCOSB-endofmib-MIB CISCOSB-dot1x-MIB CISCOSB-deviceparams-MIB CISCOSB-cli-MIB CISCOSB-cdb-MIB CISCOSB-brgmacswitch-MIB CISCOSB-3sw2swtables-MIB CISCOSB-smartPorts-MIB CISCOSB-tbi-MIB CISCOSB-macbaseprio-MIB CISCOSB-policy-MIB CISCOSB-env_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-localization-MIB CISCOSB-mcmngr-MIB CISCOSB-mng-MIB CISCOSB-physdescription-MIB CISCOSB-Poe-MIB CISCOSB-protectedport-MIB CISCOSB-rmon-MIB CISCOSB-rs232-MIB CISCOSB-SecuritySuite-MIB CISCOSB-snmp-MIB CISCOSB-specialbpdu-MIB CISCOSB-banner-MIB CISCOSB-syslog-MIB CISCOSB-TcpSession-MIB CISCOSB-traps-MIB CISCOSB-trunk-MIB CISCOSB-tuning-MIB CISCOSB-tunnel-MIB CISCOSB-udp-MIB CISCOSB-vlan-MIB CISCOSB-ipstdacl-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 CISCOSB-eee-MIB CISCOSB-ssl-MIB CISCOSB-qosclimib-MIB CISCOSB-digitalkeymanage-MIB CISCOSB-tbp-MIB CISCOSMB-MIB CISCOSB-secsd-MIB CISCOSB-draft-ietf-entmib-sensor-MIB CISCOSB-draft-ietf-syslog-device-MIB CISCOSB-rfc2925-MIB
Remote Monitoring (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 upgrade over SCP running over SSH • Upgrade can be initiated through console port as well • Dual images for resilient firmware upgrades	

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Feature	Description
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. A single session is supported.
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. A single session is supported.
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 hostname.
Secure Copy (SCP)	Securely transfer files to and from the switch
Autoconfiguration with Secure Copy (SCP) file download	Enables secure mass deployment with protection of sensitive data
Text-editable config files	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	Applies the intelligence delivered through the Smartport roles and applies it automatically to the port based on the devices discovered over Cisco Discovery Protocol or LLDP-MED. This facilitates zero-touch deployments.
Textview CLI	Scriptable command-line interface. A full CLI as well as a menu-based CLI is supported. User privilege levels 1, 7, and 15 are supported for the CLI.
Cloud services	Support for Cisco Small Business FindIT Network
Localization	Localization of GUI and documentation into multiple languages
Other management	Traceroute; single IP management; HTTP/HTTPS; SSH; RADIUS; port mirroring; TFTP upgrade; DHCP client; BOOTP; SNTP; Xmodem upgrade; cable diagnostics; ping; syslog; Telnet client (SSH secure support)
Time-based port operation	Link up or down based on user-defined schedule (when the port is administratively up)
Login banner	Configurable multiple banners for web as well as CLI
Power Efficiency	
EEE Compliant (802.3az)	Supports 802.3az on all copper ports (SG350 models)
Energy Detect	Automatically turns power off on Gigabit Ethernet and 10/100 RJ-45 port when detecting link down Active mode is resumed without loss of any packets when the switch detects the link up
Cable length detection	Adjusts the signal strength based on the cable length for Gigabit Ethernet models. Reduces the power consumption for cables shorter than 10m.
Disable port LEDs	LEDs can be manually turned off to save on energy
General	
Jumbo frames	Frame sizes up to 9K (9216) bytes supported on 10/100 and Gigabit interfaces
MAC table	Up to 16K (16384) MAC addresses
Discovery	
Bonjour	The switch advertises itself using the Bonjour protocol.
Link Layer Discovery Protocol (LLDP) (802.1ab) with LLDP-MED extensions	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.
Power over Ethernet (PoE)	
802.3af PoE, 802.3at PoE+, and 802.3xx 60W power are delivered over any of the RJ-45 ports within the listed power budgets	Switches support 802.3at PoE+, 802.3af, 802.3xx 60W, and Cisco prestandard (legacy) PoE. Maximum power of 60W to any 10/100 or Gigabit Ethernet port for PoE+ supported devices and 15.4W for PoE supported devices, until the PoE budget for the switch is reached. The total power available for PoE per switch is as follows:

Model Name	Power Dedicated to PoE	Number of Ports That Support PoE
SF350-48P	382W	48
SF350-48MP	740W	48
SG350-10P	62W	8
SG355-10P	62W	8
SG350-10MP	124W	8
SG350-28P	195W	24
SG350-28MP	382W	24

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Feature	Description
PoE powered device and PoE passthrough	In addition to AC power, compact switch models can work as PoE powered devices and be powered by PoE switches connected to the uplink ports. The switch can also pass through the power to downstream PoE end devices if required. Maximum of 60W can be drawn per uplink port if the peer PoE switch supports 60W PoE. When multiple uplink ports are connected to PoE switches, the power drawn from these ports is combined. When AC power is connected and functioning properly, it will have priority over the PoE powered device function. The PoE powered device function will then act as a backup power source to the AC power. The PoE powered device function will be the primary power source for the switch if AC power is not connected.

Model	Power Option	Available PoE Power (W)	Can Switch Be Powered with Uplinks?
SG350-10P	1 PoE uplink	0W	Yes
	2 PoE uplink	0W	Yes
	1 PoE+ uplink	0W	Yes
	2 PoE+ uplink	22W	Yes
	1 60W PoE uplink	22W	Yes
	2 60W PoE uplink	50W	Yes
	AC power	62W	Yes
SG350-10MP	1 PoE uplink	0W	Yes
	2 PoE uplink	0W	Yes
	1 PoE+ uplink	0W	Yes
	2 PoE+ uplink	22W	Yes
	1 60W PoE uplink	22W	Yes
	2 60W PoE uplink	50W	Yes
	AC power	128W	Yes
SG355-10P	1 PoE uplink	0W	Yes
	2 PoE uplink	0W	Yes
	1 PoE+ uplink	0W	Yes
	2 PoE+ uplink	22W	Yes
	1 60W PoE uplink	22W	Yes
	2 60W PoE uplink	50W	Yes
	AC power	62W	Yes

Model	Green Power (mode)	System Power Consumption	Power Consumption (with PoE)	Heat Dissipation (BTU/hr)
SF350-48	Energy Detect	110V=23.4W 220V=24.2W	N/A	20.16
SF350-48P	Energy Detect	110V=50.8W 220V=52.1W	110V=464.3W 220V=453.1W	409.96
SF350-48MP	Energy Detect	110V=58.4W 220V=58.5W	110V=866.7W 220V=843.5W	770.8
SG350-10	Energy Detect Short Reach	9.01W	N/A	
SG350-10P	Energy Detect Short Reach	13.0W	84.7W	
SG355-10P	Energy Detect Short Reach	12.37W	83.5W	
SG350-10MP	Energy Detect Short Reach	13.15W	152.6W	

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Feature	Description				
	SG350-28	Energy Detect Short Reach	110V=19.7W 220V=19.9W	N/A	16.4
	SG350-28P	Energy Detect Short Reach	110V=35.7W 220V=36.9W	110V=263W 220V=255.1W	214.2
	SG350-28MP	Energy Detect Short Reach	110V=41.3W 220V=42.1W	110V=261.1W 220V=451.2W	401.2

Ports	Model Name	Total System Ports	RJ-45 Ports	Combo Ports (RJ-45 + SFP)
	SF350-48	48 Fast Ethernet + 4 Gigabit Ethernet	48 Fast Ethernet 2 Gigabit Ethernet	2 SFP slots, 2 Gigabit Ethernet
	SF350-48P	48 Fast Ethernet + 4 Gigabit Ethernet	48 Fast Ethernet 2 Gigabit Ethernet	2 SFP slots, 2 Gigabit Ethernet
	SF350-48MP	48 Fast Ethernet + 4 Gigabit Ethernet	48 Fast Ethernet 2 Gigabit Ethernet	2 SFP slots, 2 Gigabit Ethernet
	SG350-10	10 Gigabit Ethernet	8 Gigabit Ethernet	2 Gigabit Ethernet combo
	SG350-10P	10 Gigabit Ethernet	8 Gigabit Ethernet	2 Gigabit Ethernet combo
	SG355-10P	10 Gigabit Ethernet	8 Gigabit Ethernet	2 Gigabit Ethernet combo
	SG350-10MP	10 Gigabit Ethernet	8 Gigabit Ethernet	2 Gigabit Ethernet combo
	SG350-28	28 Gigabit Ethernet	24 Gigabit Ethernet	2 SFP slots, 2 Gigabit Ethernet combo
	SG350-28P	28 Gigabit Ethernet	24 Gigabit Ethernet	2 SFP slots, 2 Gigabit Ethernet combo
	SG350-28MP	28 Gigabit Ethernet	24 Gigabit Ethernet	2 SFP slots, 2 Gigabit Ethernet combo

Buttons	Reset button
Cabling type	Unshielded twisted pair (UTP) Category 5 or better for 10BASE-T/100BASE-TX; UTP Category 5 Ethernet or better for 1000BASE-T
LEDs	System, Link/Act, PoE, Speed, LED power saving option
Flash	32 MB
CPU memory	256 MB
Packet buffer	All numbers are aggregate across all ports as the buffers are dynamically shared:

Model Name	Packet Buffer
SF350-48	24Mb
SF350-48P	24Mb
SF350-48MP	24Mb
SG350-10	12Mb
SG350-10P	12Mb
SG355-10P	12Mb
SG350-10MP	12Mb
SG350-28	12Mb
SG350-28P	12Mb
SG350-28MP	12Mb

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Feature	Description			
Supported SFP modules	**SKU**	**Media**	**Speed**	**Maximum Distance**
	MGBSX1	Multimode fiber	1000 Mbps	350 m
	MGBLH1	Single-mode fiber	1000 Mbps	40 km
	MGBT1	UTP cat 5	1000 Mbps	100 m
Environmental				
Dimensions (W x H x D)	SG350-10, SG350-10P, SG350-10MP 11 x 1.45 x 6.7 in. (279.4 x 44.45 x 170 mm) SG355-10P, SG350-28 17.3 x 1.45 x 10.1 in. (440 x 44.45 x 202 mm) SF350-48, SG350-28P, SG350-28MP 17.3 x 1.45 x 10.1 in. (440 x 44.45 x 257 mm) SF350-48P, SF350-48MP 17.3 x 1.45 x 13.78 in. (440 x 44.45 x 350 mm)			
Unit weight	SF350-48: 7.87 lb (3.57 kg) SF350-48P: 12.34 lb (5.59 kg) SF350-48MP: 12.37 lb (5.61 kg)		SG350-10: 2.40 lb (1.09 kg) SG350-10P: 2.62 lb (1.19kg) SG355-10P: 5.20 lb (2.36 kg) SG350-10MP: 2.62 lb (1.19kg) SG350-28: 6.06 lb (2.75 kg) SG350-28P: 8.44 lb (3.83 kg) SG350-28MP: 7.43 lb (3.37 kg)	
Power	100-240V 50-60 Hz, internal, universal: SF350-48P, SF350-48MP, SG350-28MP, SG350-28, SG350-28P, SG350-28MP 100-240V 50-60 Hz, 0.7A, external: SG350-10 100-240V 50-60 Hz, 1.5A, external: SG350-10P 100-240V 50-60 Hz, internal, universal: SG355-10P 100-240V 50-60 Hz, 2.0A, external: SG350-10MP			
Certification	UL (UL 60950), CSA (CSA 22.2), CE mark, FCC Part 15 (CFR 47) Class A			
Operating temperature	SG350-10, SG350-10P, SG355-10P, SG350-10MP, SG350-28, SG350-28P, SG350-28MP 32° to 104°F (0° to 40°C) SG350-10MP, SG350-10P, SG350-28P 32° to 113°F (0° to 45°C) SF350-48P, SF350-48MP, SG350-28MP 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 MTBF	**Model Name**	**FAN (Number)**	**Acoustic Noise**	**MTBF @40C (hr)**
	SF350-48	Fanless	N/A	277,653
	SF350-48P	3	53.7 dB at 40C	182,270
	SF350-48MP	4	49.8 dB at 40C	191,951
	SG350-10	Fanless	N/A	308,196
	SG350-10P	Fanless	N/A	205,647
	SG355-10P	Fanless	N/A	296,426
	SG350-10MP	Fanless	N/A	80,093
	SG350-28	Fanless	N/A	367,209
	SG350-28P	2	47.9 dB at 40C	396,687
	SG350-28MP	4	49.6dB at 40C 54dB at 50C	213,373
Warranty	Limited lifetime with next business day advance replacement (where available)			

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Feature	Description
Package Contents	
	• Cisco 350 Series Switch • Power Cord (Power Adapter for Desktop SKUs) • Mounting Kit included in all SKUs, including desktop models • Console Cable • Quick Start Guide
Minimum Requirements	
	• Web browser: Mozilla Firefox version 8 or later; Microsoft Internet Explorer version 7 or later, Safari, Chrome • Category 5 Ethernet network cable • TCP/IP, network adapter, and network operating system (such as Microsoft Windows, Linux, or Mac OS X) installed on each computer in the network

Ordering Information

Table 2 provides ordering information for the Cisco 350 Series Switches. Table 3 provides MFE and MGE transceiver ordering information.

Table 2. Cisco 350 Series Switches Ordering Information

Model Name	Order Product ID Number	Description
Fast Ethernet		
SF350-48	SF350-48-K9	• 48 10/100 ports • 2 10/100/1000 ports • 2 combo mini-GBIC
SF350-48P	SF350-48P-K9	• 48 10/100 PoE+ ports with 382W power budget • 2 SFP slots • 2 combo mini-GBIC ports
SF350-48MP	SF350-48MP-K9	• 48 10/100 PoE+ ports with 740W power budget • 2 SFP slots • 2 combo mini-GBIC ports
Gigabit Ethernet		
SG350-10	SG350-10-K9	• 8 10/100/1000 ports • 2 combo mini-GBIC ports
SG350-10P	SG350-10P-K9	• 8 10/100/1000 PoE ports with 62W power budget • 2 Combo mini-GBIC ports
SG350-10MP	SG350-10MP-K9	• 8 10/100/1000 PoE ports with 128W power budget • 2 Combo mini-GBIC ports
SG355-10P	SG355-10P-K9	• 8 10/100/1000 PoE+ ports with 62W power budget • 2 Combo mini-GBIC ports
SG350-28	SG350-28-K9	• 26 10/100/1000 ports • 2 SFP slots • 2 combo mini-GBIC ports
SG350-28P	SG350-28P-K9	• 26 10/100/1000 ports (24 PoE ports with 195W power budget) • 2 SFP slots • 2 combo mini-GBIC ports
SG350-28MP	SG350-28MP-K9	• 26 10/100/1000 ports (24 PoE+ ports with 382W power budget) • 2 SFP slots • 2 combo mini-GBIC ports

* Each combo mini-GBIC port has one 10/100/1000 Ethernet port and one mini-GBIC/SFP Gigabit Ethernet slot, with one port active at a time.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Table 3. MFE and MGE Transceiver Ordering Information

MGE Transceivers	
MGBLH1	1000BASE-LH SFP transceiver, for single-mode fiber, 1310 nm wavelength, support up to 40 km
MGBSX1	1000BASE-SX SFP transceiver, for multimode fiber, 850 nm wavelength, support up to 550 m

A Powerful, Affordable Foundation for Your Small Business Network

As you strive to make your employees as productive and effective as possible, your business applications and information and the network that delivers them become ever more vital parts of your business. You need a technology foundation that can meet your business's needs today and in the future and that delivers the right feature set at the right price. The Cisco 350 Series portfolio of managed switches provides the reliability, performance, security, and capabilities you need to power your business.

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 350 Series, visit http://www.cisco.com/go/350switches.

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)

Printed in USA C78-737359-00 06/16

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.