

Spécifications produit des commutateurs entièrement gérés de la gamme Cisco Sx350

Objectif

Les commutateurs entièrement gérés de la gamme Cisco Sx350 sont des commutateurs autonomes qui fournissent des ports Fast Ethernet (FE)/Gigabit Ethernet (GE) et SFP (Small Form-Factor Pluggable) 2 combinés + PoE sur des modèles spécifiques. Les commutateurs sont équipés d'un nouveau processeur de paquets hautement intégré pour les applications Carrier Ethernet et Small-Medium Enterprise (SME) avec des performances à vitesse maximale du médium.

L'utilitaire Web vous permet de déployer et de gérer efficacement votre réseau. La configuration et le dépannage peuvent être effectués facilement grâce à des outils faciles à utiliser tels que Cisco Discovery Protocol (CDP), FindIT Network Management et Cisco Smartports, qui permettent à votre réseau de détecter et de configurer automatiquement tous les périphériques Cisco connectés.

Cet article vise à présenter les spécifications produit et matériel des commutateurs entièrement gérés de la gamme Sx350. Pour en savoir plus sur les commutateurs entièrement gérés de la gamme Sx350, cliquez [ici](#).

Spécifications du produit

Performances

Fonctionnalité	Description	
Capacité de commutation et débit de transfert Tous les commutateurs sont à vitesse filaire et non bloquants	N	
	o	
	m	
	d	
	u	
	Taux de transfert en millions de paquets par seconde (mpps); Paquets de 64 octets)	Capacité de commutation en gigabits par seconde
	è	
	l	
	e	
	SF35 0-48	13.10 17.6
	SF35 0-48P	13.10 17.6
	SF35 0-48M	13.10 17.6
	P	
	SG35	14.88 20.0

0-10		
SG35		
0-	14.88	20.0
10P		
SG35		
0-	14.88	20.0
10M		
P		
SG35		
5-	14.88	20.0
10M		
P		
SG35	41.67	56.0
0-28		
SG35		
0-	41.67	56.0
28P		
SG35		
0-	41.67	56.0
28M		
P		

Commutation de couche 2

Fonctionnalité	Description
Protocole Spanning Tree (STP)	<ul style="list-style-type: none"> • Prise en charge du protocole Spanning Tree 802.1d standard • Convergence rapide utilisant 802.1w ou Rapid Spanning Tree (RSTP), activée par défaut • 8 instances sont prises en charge • Instances Spanning Tree multiples utilisant la norme 802.1s (MSTP)
Regroupement de ports	Prise en charge du protocole LACP (Link Aggregation Control Protocol) IEEE 802.3ad <ul style="list-style-type: none"> • Jusqu'à 8 groupes • Jusqu'à 8 ports par groupe avec 16 ports candidats pour chaque agrégation de liaisons 802.3ad (dynamique) • Prise en charge simultanée de 4 096 VLAN maximum • VLAN basés sur les ports et les balises 802.1Q • VLAN basé sur MAC (Media Access Control) • VLAN de gestion
Réseau local virtuel (VLAN)	<ul style="list-style-type: none"> • PVE (Private VLAN Edge), également appelé ports protégés, avec plusieurs liaisons ascendantes • VLAN invité • VLAN non authentifié • Attribution dynamique de VLAN via le serveur RADIUS avec authentification client 802.1x • VLAN Équipement client (CPE)
VLAN voix	<ul style="list-style-type: none"> • Le trafic vocal est automatiquement attribué à un

	VLAN spécifique à la voix et traité avec les niveaux de QoS appropriés.
	<ul style="list-style-type: none"> • Les fonctionnalités vocales automatiques permettent un déploiement automatique des terminaux vocaux et des périphériques de contrôle des appels à l'échelle du réseau.
VLAN TV multidiffusion	Le VLAN TV multidiffusion permet de partager le VLAN multidiffusion unique dans le réseau, tandis que les abonnés restent dans des VLAN distincts, également appelés MVR (Multicast VLAN Registration)
VLAN Q-in-Q	Les VLAN traversent en toute transparence un réseau de fournisseur de services tout en isolant le trafic entre les clients
GVRP (Generic VLAN Registration Protocol) et GARP (Generic Attribute Registration Protocol)	Protocoles pour la propagation et la configuration automatiques de VLAN dans un domaine ponté
Unidirectional Link Detection (UDLD)	UDLD surveille la connexion physique pour détecter les liaisons unidirectionnelles provoquées par des erreurs de câblage ou de câble/port incorrectes afin d'empêcher les boucles de transfert et la mise en veille du trafic dans les réseaux commutés
Relais DHCP (Dynamic Host Configuration Protocol) au niveau de la couche 2	Relais du trafic DHCP vers le serveur DHCP dans différents VLAN ; fonctionne avec DHCP Option 82
Surveillance IGMP (Internet Group Management Protocol) versions 1, 2 et 3	IGMP limite le trafic de multidiffusion gourmand en bande passante aux seuls demandeurs ; prend en charge des groupes de multidiffusion de 1000 bits (la multidiffusion spécifique à la source est également prise en charge)
Requête IGMP	Le demandeur IGMP est utilisé pour prendre en charge un domaine multicast de couche 2 de commutateurs de surveillance en l'absence d'un routeur multicast
Blocage en tête de ligne (HOL) Trame étendue	Prévention du blocage HOL Jusqu'à 9 216 octets

Couche 3

Fonctionnalité	Description
Routage IPv4	<ul style="list-style-type: none"> • Routage à distance des paquets IPv4 • Jusqu'à 512 routes statiques et jusqu'à 128 interfaces IP
Routage interdomaine sans classe (CIDR)	Prise en charge du routage CIDR
Interface de couche 3	Configuration de l'interface de couche 3 sur le port physique, le LAG, l'interface VLAN ou l'interface de bouclage
Relais DHCP au niveau de la	Relais du trafic DHCP sur les domaines IP

couche 3

Relais UDP (User Datagram Protocol)	Relais des informations de diffusion sur les domaines de couche 3 pour la détection d'applications ou le relais de paquets bootP/DHCP
Serveur DHCP	<ul style="list-style-type: none">• Le commutateur fonctionne comme un serveur DHCP IPv4 qui sert des adresses IP pour plusieurs pools/étendues DHCP• Prise en charge des options DHCP

Sécurité

Fonctionnalité	Description
Protocole SSH (Secure Shell)	SSH est un remplacement sécurisé du trafic Telnet. Le protocole SCP (Secure Copy Protocol) utilise également SSH. SSH v1 et v2 sont pris en charge.
SSL (Secure Sockets Layer)	Prise en charge SSL : Chiffre tout le trafic HTTPS, ce qui permet un accès hautement sécurisé à l'interface utilisateur graphique de gestion basée sur navigateur du commutateur. <ul style="list-style-type: none">• 802.1X : Authentification et comptabilité RADIUS, hachage MD5 ; VLAN invité ; VLAN non authentifié, mode hôte unique/multiple et sessions simples/multiples
IEEE 802.1X (rôle d'authentificateur)	<ul style="list-style-type: none">• Prise en charge de la norme 802.1X basée sur le temps• Affectation de VLAN dynamique
Authentification basée sur le Web	L'authentification basée sur le Web offre un contrôle d'admission réseau via un navigateur Web à tous les périphériques hôtes et systèmes d'exploitation.
Protection des unités BPDU (Bridge Protocol Data Unit) STP	Mécanisme de sécurité permettant de protéger le réseau des configurations non valides. Un port activé pour la protection BPDU est arrêté si un message BPDU est reçu sur ce port.
Protection de la racine STP	Cela empêche les périphériques périphériques qui ne sont pas sous le contrôle de l'administrateur réseau de devenir des noeuds racine du protocole Spanning Tree.
Surveillance DHCP	Filtre les messages DHCP avec des adresses IP non enregistrées et/ou à partir d'interfaces inattendues ou non approuvées. Cela empêche les périphériques indésirables de se comporter en serveurs DHCP.
Protection de la source IP (IPSG)	Lorsque la protection de la source IP est activée sur un port, le commutateur filtre les paquets IP reçus du port si les adresses IP source des paquets n'ont pas été configurées de manière statique ou apprises dynamiquement à partir de la surveillance DHCP. Cela empêche l'usurpation d'adresse IP.
Inspection ARP	Le commutateur rejette les paquets ARP

dynamique (DAI)	(Address Resolution Protocol) d'un port s'il n'existe aucune liaison IP/MAC statique ou dynamique ou s'il existe une différence entre les adresses source ou de destination dans le paquet ARP. Cela empêche les attaques de l'homme du milieu.
Liaison IP/MAC/port (IPMB)	Les fonctions précédentes (surveillance DHCP, protection de la source IP et inspection ARP dynamique) fonctionnent ensemble pour empêcher les attaques DOS sur le réseau, augmentant ainsi la disponibilité du réseau.
Technologie Secure Core (SCT)	Assurez-vous que le commutateur recevra et traitera le trafic de gestion et de protocole, quel que soit le volume de trafic reçu.
SSD (Secure Sensitive Data)	Mécanisme permettant de gérer les données sensibles (mots de passe, clés, etc.) de manière sécurisée sur le commutateur, en renseignant ces données sur d'autres périphériques et en sécurisant la configuration automatique. L'accès pour afficher les données sensibles en texte clair ou chiffré est fourni en fonction du niveau d'accès configuré par l'utilisateur et de la méthode d'accès de l'utilisateur.
Isolation de couche 2 Périphérie de VLAN privé (PVE) avec VLAN de communauté	PVE (également appelé ports protégés) assure l'isolation de couche 2 entre les périphériques du même VLAN, prend en charge plusieurs liaisons ascendantes.
Sécurité de port	Possibilité de verrouiller les adresses MAC source sur les ports et de limiter le nombre d'adresses MAC acquises.
Service utilisateur de numérotation d'authentification à distance (RADIUS), Système de contrôle d'accès aux contrôleurs d'accès aux terminaux (TACACS+)	Prend en charge l'authentification RADIUS et TACACS ; commutateur fonctionne comme client
Contrôle des tempêtes	Diffusion, multidiffusion et monodiffusion inconnue
Gestion des comptes RADIUS	Les fonctions de comptabilité RADIUS permettent d'envoyer des données au début et à la fin des services, en indiquant la quantité de ressources (temps, paquets, octets, etc.) utilisées pendant la session.
Protection contre les dénis de	Prévention des attaques DoS

service (DoS)

Listes de contrôle d'accès (ACL)

- Prise en charge de 512 règles maximum
- Limite de débit ou d'abandon basée sur l'adresse MAC source et de destination, l'ID de VLAN ou l'adresse IP, le protocole, le port, la priorité DSCP (Differentiated Services Code Point)/IP, les ports source et de destination TCP/UDP, la priorité 802.1p, le type Ethernet, les paquets ICMP (Internet Control Message Protocol), les paquets IGMP, l'indicateur TCP, les listes de contrôle d'accès temporelles prises en charge.

Qualité de service

Fonctionnalité Description

Niveaux de priorité	8 files d'attente matérielles par port
Planification	Attribution de priorité stricte et de file d'attente WRR (Weighted Round-Robin) basée sur DSCP et classe de service (802.1p/CoS)
Classe de service	Basé sur les ports ; VLAN 802.1p basé sur la priorité ; Priorité IP IPv4/v6, type de service (ToS) et DSCP ; Services différenciés (DiffServ); classification et marquage des listes de contrôle d'accès, qualité de service (QoS) de confiance
Limitation de débit	Police d'entrée ; formatage des sorties et contrôle de la vitesse ; par VLAN, par port et basé sur le flux
Évitement de la congestion	Un algorithme d'évitement de congestion TCP est requis pour réduire et empêcher la synchronisation globale des pertes TCP

Normes

Fonctionnalité Description

Normes	IEEE 802.3 10BaseT Ethernet, IEEE 802.3u 100BaseTX Fast Ethernet, IEEE 802.3ab 1000BaseT Gigabit Ethernet, IEEE 802.3ad LACP, IEEE 802.3z Gigabit Ethernet, IEEE 802.3 Contrôle de flux 3x, IEEE 802.1D (STP, GARP et GVRP), VLAN IEEE 802.1Q/p, RSTP IEEE 802.1w, STP multiple IEEE 802.1s, Authentification d'accès aux ports IEEE 802.1X, 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 8888 6, RFC 858, RFC 894, RFC 919, RFC 922, RFC 920, RFC 950, RFC 1042, RFC 1071, RFC 1123, RFC 1141, RFC 155 , 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,
--------	---

IPv6

Fonctionnalité	Description
IPv6	<ul style="list-style-type: none"> • Mode hôte IPv6 • IPv6 sur Ethernet • Double pile IPv6/IPv4 • Détection de routeur et de voisin IPv6 (ND) • Configuration automatique de l'adresse sans état IPv6 • Découverte MTU (Path Maximum Transmission Unit) • Détection des adresses en double (DAD) • ICMP version 6
QoS IPv6	Hiérarchiser les paquets IPv6 dans le matériel
ACL IPv6	Supprimer ou réduire la limite de débit des paquets IPv6 dans le matériel
<ul style="list-style-type: none"> • Sécurité du premier saut IPv6 	<ul style="list-style-type: none"> • Gardien de la RA • Inspection ND • Protection DHCPv6 • Table de liaison de voisinage (entrées statiques et de surveillance) • Vérification de l'intégrité de la liaison de voisinage
Surveillance de la détection de l'écouteur multidiffusion (MLD v1/2)	Livraison des paquets de multidiffusion IPv6 uniquement aux récepteurs requis
Applications IPv6	<p>Web/SSL, serveur Telnet/SSH, client DHCP (Dynamic Host Configuration Protocol), configuration automatique DHCP, CDP (Cisco Discovery Protocol), LLDP (Link Layer Discovery Protocol)</p> <ul style="list-style-type: none"> • RFC 4443 (obsolète RFC2463) - ICMP version 6 • RFC 4291 (obsolète RFC 3513) - Architecture d'adresses IPv6 • RFC 4291 - Architecture d'adressage IPv6 • RFC 2460 - Spécification IPv6 • RFC 4861 (obsolète RFC 2461) - Détection de voisins pour IPv6 • RFC 4862 (obsolète RFC 2462) - Configuration automatique des adresses sans état IPv6 • RFC 1981 - Découverte de MTU de chemin • RFC 4007 - Architecture d'adresses IPv6 étendues • RFC 3484 - Mécanisme de sélection d'adresse par défaut
Requêtes de commentaires IPv6 (RFC) prises en charge	

Gestion

Fonctionnalité	Description
Interface utilisateur Web	Utilitaire de configuration de commutateur intégré pour une configuration de périphérique basée sur navigateur (HTTP/HTTPS) aisée. Prend en charge la

configuration, le tableau de bord système, la maintenance et la surveillance du système

Protocole de gestion de réseau simple (SNMP)

SNMP versions 1, 2c et 3 avec prise en charge des interruptions et SNMP version 3 User-Based Security Model (USM)

	draft-ietf-bridge-8021x-MIB	rfc2011-MIB
	draft-ietf-bridge-rstpmib-04-MIB	draft-ietf-entmib-capteur-MIB
	draft-ietf-hubmib-etherif-MIB-v3-00-MIB	Ildp-MIB
	draft-ietf-syslog-device-MIB	Ildpextdot1-MIB
	ianaaddrfamNuméros-MIB	Ildpextdot3-MIB
	ianaifty-MIB	Ildpextmed-MIB
	lanaport-MIB	p-bridge-MIB
	inet-address-MIB	q-bridge-MIB
	ip-forward-MIB	rfc1389-MIB
	ip-MIB	rfc1493-MIB
	RFC1155-SMI	rfc1611-MIB
	RFC1213-MIB	rfc1612-MIB
Base MIB (Standard Management Information Base)	SNMPv2-MIB	rfc1850-MIB
	SNMPv2-SMI	rfc1907-MIB
	SNMPv2-TM	rfc2571-MIB
	RMON-MIB.my	rfc2572-MIB
	dcb-raj-DCBX-MIB-1108-MIB	rfc2574-MIB
	rfc1724-MIB	rfc2576-MIB
	RFC-1212.my_for_MG-Soft	rfc2613-MIB
	rfc1213-MIB	rfc2665-MIB
	rfc1757-MIB RFC-1215.mon	rfc2668-MIB
	SNMPv2-CONF.my	rfc2737-MIB
	SNMPv2-TC.my	rfc2925-MIB
	rfc2674-MIB	rfc3621-MIB
	rfc2575-MIB	rfc4668-MIB
	rfc2573-MIB	rfc4670-MIB
	rfc2233-MIB	trunk-MIB
	rfc2013-MIB	tunnel-MIB
	rfc2012-MIB	MIB udp
	CISCOB-Ildp-MIB	CISCOB-ip-MIB
	CISCOB-brgmulticast-MIB	CISCOB-lprouter-MIB
	CISCOB-bridgemibobject-MIB	CISCOB-ipv6-MIB
	CISCOB-bonjour-MIB	CISCOB-Mnginf-MIB
	CISCOB-dhcpcl-MIB	CISCOB-lcli-MIB
	MIB CISCOB	CISCOB-MIB-localisation
	CISCOB-wrandomtaildrop-MIB	CISCOB-mcmngr-MIB
MIB privés	CISCOB-MIB-traceroute	CISCOB-mng-MIB
	CISCOB-telnet-MIB	CISCOB-physdescription-MIB
	CISCOB-stormctrl-MIB	CISCOB-POE-MIB
	CISCOB-ssh-MIB	MIB de port protégé par CISCOB
	CISCOB-socket-MIB	CISCOB-rmon-MIB
	CISCOB-sntp-MIB	CISCOB-rs232-MIB
	CISCOB-smon-MIB	CISCOB-SecuritySuite-MIB
	CISCOB-phy-MIB	CISCOB-snmplib-MIB
	CISCOB-MIB multisession-terminal	CISCOB-specialbpdu-MIB

CISCOSB-Mri-MIB	MIB-Bannière CISCOSB
CISCOSB-MIB-jumboframes	CISCOSB-syslog-MIB
CISCOSB-gvrp-MIB	CISCOSB-TcpSession-MIB
CISCOSB-endofmib-MIB	CISCOSB-traps-MIB
CISCOSB-dot1x-MIB	CISCOSB-MIB-trunk
CISCOSB-deviceparams-MIB	CISCOSB-MIB de réglage
CISCOSB-cli-MIB	CISCOSB-tunnel-MIB
CISCOSB-cdb-MIB	CISCOSB-UDP-MIB
CISCOSB-MIB-brgmacswitch	CISCOSB-Vlan-MIB
CISCOSB-3sw2swtables-MIB	CISCOSB-ipstdacl-MIB
CISCOSB-smartPorts-MIB	MIB CISCO-SMI
CISCOSB-tbi-MIB	CISCOSB-DebugCapabilities-MIB
CISCOSB-macbaseprio-MIB	CISCOSB-CDP-MIB
CISCOSB-policy-MIB	CISCOSB-vlanMIB voix
CISCOSB-env_mib	CISCOSB-EVENTS-MIB
CISCOSB-capteur-MIB	CISCOSB-MIB-SYSTÈME
CISCOSB-Aaa-MIB	CISCOSB-MIB-STT
CISCOSB-Application-MIB	MIB CISCO-TC
CISCOSB-bridgesecurity-MIB	CISCO-VTP-MIB
CISCOSB-copy-MIB	MIB CDP-CISCO
CISCOSB-CpuCounters-MIB	CISCOSB-eee-MIB
CISCOSB-Custom1BonjourService-MIB	CISCOSB-ssl-MIB
CISCOSB-dhcp-MIB	CISCOSB-Qosclib-MIB
CISCOSB-dlf-MIB	CISCOSB-digitalkeymanage-MIB
CISCOSB-dnscl-MIB	CISCOSB-tbp-MIB
CISCOSB-embweb-MIB	CISCOSMB-MIB
CISCOSB-fft-MIB	CISCOSB-secsd-MIB
CISCOSB-file-MIB	CISCOSB-draft-ietf-entmib-capteur-MIB
CISCOSB-greeneth-MIB	CISCOSB-draft-ietf-syslog-device-MIB
CISCOSB-interfaces-MIB	CISCOSB-rfc2925-MIB
CISCOSB-interfaces_recovery-MIB	

Surveillance à distance (RMON)	L'agent logiciel RMON intégré prend en charge 4 groupes RMON (historique, statistiques, alarmes et événements) pour une gestion, une surveillance et une analyse améliorées du trafic
Double pile IPv4 et IPv6	Coexistence des deux piles de protocoles pour faciliter la migration <ul style="list-style-type: none"> • Mise à niveau du navigateur Web (HTTP/HTTPS) et TFTP et mise à niveau via SCP exécutée sur SSH
Mise à niveau du micrologiciel	<ul style="list-style-type: none"> • La mise à niveau peut également être lancée via le port de console • Deux images pour des mises à niveau résilientes du micrologiciel
Mise en miroir des ports	Le trafic sur un port ou un VLAN peut être mis en miroir sur un autre port pour analyse avec un analyseur de réseau ou une sonde RMON. Jusqu'à 8 ports source peuvent être mis en miroir sur un port de destination. Une seule session est prise en charge
Mise en miroir VLAN	Le trafic d'un VLAN peut être mis en miroir sur un port pour analyse à l'aide d'un analyseur de réseau ou d'une sonde RMON. Jusqu'à 8 VLAN source peuvent être mis en miroir sur un port de destination. Une seule session est prise en charge.
DHCP (réponses 12, 66, 67, 82, 129 et 150)	Les options DHCP facilitent un contrôle plus strict à partir d'un point central (serveur DHCP) pour obtenir l'adresse IP, la configuration automatique (avec téléchargement du fichier de configuration), le relais DHCP et le nom d'hôte
Copie	Transfert sécurisé des fichiers depuis et vers le commutateur

sécurisée (SCP) Configuration automatique avec téléchargement de fichier Secure Copy (SCP) Fichiers de configuration modifiables en texte	Déploiement massif sécurisé avec protection des données sensibles et téléchargés vers un autre commutateur, facilitant ainsi le déploiement en masse
Smartports	Configuration simplifiée de la qualité de service et des fonctionnalités de sécurité
Auto Smartports	Applique l'intelligence fournie par le biais des rôles Smartport et l'applique automatiquement au port en fonction des périphériques détectés via le protocole CDP ou LLDP-MED. Cela facilite les déploiements sans intervention.
CLI Textview	Interface de ligne de commande scriptable. Une interface de ligne de commande complète et une interface de ligne de commande basée sur des menus sont prises en charge. Les niveaux de privilège utilisateur 1, 7 et 15 sont pris en charge pour la CLI.
Services cloud	Prise en charge de l'outil Cisco Small Business FindIT Network
Localisation	Localisation de l'interface utilisateur graphique et de la documentation dans plusieurs langues
Autre gestion	Traceroute ; gestion IP unique ; HTTP/HTTPS ; SSH ; RADIUS; Mise en miroir des ports; Mise à niveau TFTP ; Client DHCP; BOOTP ; SNMP ; Mise à niveau Xmodem ; diagnostic des câbles ; ping ; syslog; Client Telnet (prise en charge sécurisée SSH)
Fonctionnement des ports basé sur le temps	Liaison active ou inactive en fonction du planning défini par l'utilisateur (lorsque le port est administrativement actif)
Bannière de connexion	Plusieurs bannières configurables pour Web et CLI

Efficacité énergétique

Fonctionnalité	Description
Conformité EEE (802.3az)	Prise en charge de la norme 802.3az sur tous les ports cuivre (modèles SG350) <ul style="list-style-type: none"> • Désactiver automatiquement les ports Gigabit Ethernet et RJ-45 10/100 lors de la détection d'une liaison inactive
Détection d'énergie	<ul style="list-style-type: none"> • Le mode actif reprend sans perte de paquets lorsque le commutateur détecte la liaison.
Détection de la longueur des câbles	Ajuste la puissance du signal en fonction de la longueur du câble pour les modèles Gigabit Ethernet. Réduit la consommation électrique des câbles de moins de 10 m.
Désactiver les DEL de	Les DEL peuvent être désactivées manuellement pour économiser de l'énergie

port

Généralités

Fonctionnalité Description

Trames jumbo	Taille des trames pouvant atteindre 9 000 octets (9 216) pris en charge sur les interfaces 10/100 et Gigabit
Table MAC	Jusqu'à 16 000 adresses MAC (16 384)

Découverte

Fonctionnalité Description

Bonjour	Le commutateur s'annonce à l'aide du protocole Bonjour
LLDP (Link Layer Discovery Protocol) (802.1ab) avec les extensions LLDP-MEDE	Le protocole LLDP permet au commutateur d'annoncer son identification, sa configuration et ses fonctionnalités aux périphériques voisins qui stockent les données dans une base MIB. LLDP-MED est une amélioration du protocole LLDP qui ajoute les extensions nécessaires aux téléphones IP.
Cisco Discovery Protocol	Le commutateur s'annonce à l'aide du protocole CDP (Cisco Discovery Protocol). Il apprend également le périphérique connecté et ses caractéristiques via le protocole CDP (Cisco Discovery Protocol).

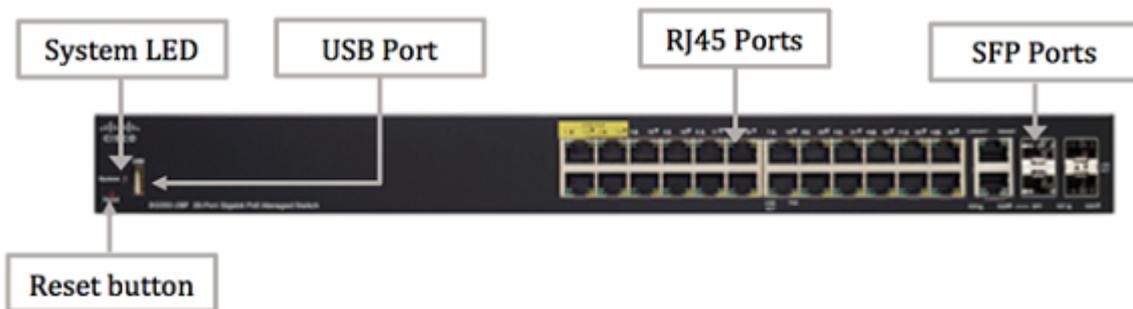
PoE (Power Over Ethernet)

Fonctionnalité Description

PoE 802.3af ou PoE+ 802.3at fournis sur quel port RJ-45 des budgets d'alimentation répertoriés	Les commutateurs prennent en charge les technologies PoE+ 802.3at, 802.3af, 802.3xx 60 W et la prénorme Cisco (ancienne) PoE. Puissance maximale de 60 W sur n'importe quel port 10/100 ou Gigabit Ethernet pour les périphériques pris en charge par PoE+ et de 15,4 W pour les périphériques pris en charge par PoE, jusqu'à ce que le budget PoE du commutateur soit atteint. L'alimentation totale disponible pour PoE par commutateur est la suivante :
--	--

	Nom du modèle	Alimentation dédiée au PoE	Nombre de ports prenant en charge PoE
	SF350-48P	382 W	48
	SF350-48MP	740 W	48
	SG350-10P	62 W	8
	SG350-10MP	62 W	8
	SG355-10P	124 W	8
	SG350-28P	195 W	24
	SG350-28MP	382 W	24

Interfaces physiques



Fonctionnalité Description

Nom du modèle	Nombre total de ports système	Ports RJ-45	Ports combinés (RJ-45 + SFP)
SF350-48	48 Fast Ethernet + 4 Gigabit Ethernet	48 Fast Ethernet 2 Gigabit Ethernet	2 logements SFP, 2 Gigabit Ethernet
SF350-48P	48 Fast Ethernet + 4 Gigabit Ethernet	48 Fast Ethernet 2 Gigabit Ethernet	2 logements SFP, 2 Gigabit Ethernet
SF350-48MP	48 Fast Ethernet + 4 Gigabit Ethernet	48 Fast Ethernet 2 Gigabit Ethernet	2 logements SFP, 2 Gigabit Ethernet
Ports			
SG350-10	10 Gigabit Ethernet	8 Gigabit Ethernet	2 ports combinés Gigabit Ethernet
SG350-10P	10 Gigabit Ethernet	8 Gigabit Ethernet	2 ports combinés Gigabit Ethernet
SG355-10P	10 Gigabit Ethernet	8 Gigabit Ethernet	2 ports combinés Gigabit Ethernet
SG350-10MP	10 Gigabit Ethernet	8 Gigabit Ethernet	2 ports combinés Gigabit Ethernet 2 logements SFP
SG350-28	28 Gigabit Ethernet	24 Gigabit Ethernet	SFP, 2 ports Gigabit Ethernet combinés
SG350-28P	28 Gigabit Ethernet	24 Gigabit Ethernet	2 logements SFP

		Ethernet	Ethernet	SFP, 2 ports Gigabit Ethernet combinés 2 logements
	SG350-28MP	28 Gigabit Ethernet	24 Gigabit Ethernet	SFP, 2 ports Gigabit Ethernet combinés
Boutons	Bouton Réinitialiser			
Type de câblage	paire torsadée non blindée (UTP) de catégorie 5 ou supérieure pour 10BASE-T/100BASE-TX ; Ethernet UTP de catégorie 5 ou supérieure pour 1000BASE-T			
DEL	Option d'économie d'énergie système, Link/Act, PoE, Speed, LED			
Flash	32 Mo			
Mémoire processeur	256 Mo			

Tampon de paquets

Fonctionnalité	Description			
	Tous les nombres sont agrégés sur tous les ports, car les tampons sont partagés dynamiquement :			
	Nom du modèle	Tampon de paquets		
	SF350-48	24 Mo		
	SF350-48P	24 Mo		
	SF350-48MP	24 Mo		
Tampon de paquets	SG350-10	12 Mo		
	SG350-10P	12 Mo		
	SG355-10P	12 Mo		
	SG350-10MP	12 Mo		
	SG350-28	12 Mo		
	SG350-28P	12 Mo		
	SG350-28MP	12 Mo		
	Référence	Médias	Vitesse	Distance maximale
Modules SFP pris en charge	MGBSX1	Fibre multimode	1000 Mbits/s	350 m
	MGBLH1	Fibre monomode	1000 Mbits/s	40 km
	MGBT1	Fibre monomode	1000 Mbits/s	100 km

Environnement

Fonctionnalité	Description	
Dimensions (L x H x P)	SG350-10, SG350-10P, SG350-10MP : 11 x 1,45 x 6,7 pouces 279,4 x 44,45 x 170 mm	
	SG355-10P, SG350-28 : 17,3 x 1,45 x 10,1 pouces 440 x 44,45 x 202 mm	
	SF350-48, SG350-28P, SG350-28MP : 17,3 x 1,45 x 10,1 pouces 440 x 44,45 x 257 mm	
	SF350-48P, SF350-48MP : 17,3 x 1,45 x 13,78 pouces 440 x 44,45 x 350 mm	
Poids unitaire	SF350-48 : 3,57 kg	SG350-10 : 1,09 kg

SF350-48P : 5,59 kg
 SF350-48MP : 5,61 kg
 SG350-10P : 1,19 kg
 SG355-10P : 2,36 kg
 SG350-10MP : 1,19 kg
 SG350-28 : 2,75 kg
 SG350-28P : 3,83 kg
 SG350-28MP : 3,37 kg

Alimentation 100-240 V 50-60 Hz, interne, universel : SF350-48P, SF350-48MP, SG350-28MP, SG350-28, SG350-28P, SG350-28MP
 100-240 V 50-60 Hz, 0,7 A, externe : SG350-10
 100-240 V 50-60 Hz, 1,5 A, externe : SG350-10P
 100-240 V 50-60 Hz, interne, universel : SG355-10P
 100-240 V 50-60 Hz, 2,0 A, externe : SG350-10MP

Certification UL (UL 60950), CSA (CSA 22.2), marque CE, FCC
 Partie 15 (CFR 47) Classe A
 SG350-10, SG350-10P, SG355-10P, SG350-10MP, SG350-28, SG350-28P, SG350-28MP

Température de fonctionnement 0 à 40 °C
 SG350-10MP, SG350-10P, SG350-28P
 0 à 45 °C
 SF350-48P, SF350-48MP, SG350-28MP
 0 à 50 °C

Température de stockage -20 à 70 °C

Humidité en fonctionnement 10 à 90 %, relatif, sans condensation

Humidité de stockage 10 à 90 %, relatif, sans condensation

	Nom du modèle	VENTILATEUR R (numéro)	Bruit acoustique	MTBF 40 C (h)
Bruit acoustique et MTBF	SF350-48	Sans ventilateur	S/O	277,653
	SF350-48P	3	53,7 dB à 40 C	182,270
	SF350-48MP	4	49,8 dB à 40 C	191,951
	SG350-10	Sans ventilateur	S/O	308,196
	SG350-10P	Sans ventilateur	S/O	205,647
	SG355-10P	Sans ventilateur	S/O	296,426
	SG350-10MP	Sans ventilateur	S/O	80,093
	SG350-28	Sans ventilateur	S/O	367,209
	SG350-28P	2	47,9 dB à 40 C	396,687
	SG350-28MP	4	49,6 dB à 40 C 54 dB à 50 C	213,373