

Commutateurs administrables et empilables Cisco 350X

Des commutateurs administrables faciles à utiliser qui allient à la perfection fonctionnalités et prix compétitif

Pour garder une longueur d'avance sur leurs concurrents, les petites entreprises doivent rentabiliser chacune de leurs dépenses. Elles doivent donc tirer pleinement parti de leurs investissements technologiques, mais également s'assurer que leurs collaborateurs accèdent rapidement et en toute sécurité aux outils et aux données dont ils ont besoin. Chaque minute qu'un employé passe à attendre la réponse d'une application, et chaque minute d'indisponibilité de votre réseau, a un impact sur vos résultats. Votre réseau devra être performant et stable à mesure que votre entreprise multipliera son nombre de collaborateurs et d'applications, et que votre réseau gagnera en complexité.

Si votre entreprise a besoin de fonctionnalités avancées et d'une sécurité poussée, mais que le prix reste une préoccupation de taille, vous êtes prêt à adopter les commutateurs administrables Cisco® Small Business de nouvelle génération : la gamme Cisco 350X.

Commutateurs administrables et empilables Cisco 350X

La nouvelle gamme Cisco 350X de commutateurs Ethernet administrables et empilables (Figure 1) offre les fonctionnalités avancées dont vous avez besoin pour prendre en charge un environnement réseau plus exigeant, à un prix abordable. Les modèles Cisco 350XG disposent de 12, 24 ou 48 ports 10 Gigabit Ethernet. Ils fournissent ainsi une base solide à vos applications actuelles, comme à celles que vous envisagez de déployer. Leur grande simplicité de déploiement et de gestion signifie par ailleurs des besoins réduits en collaborateurs IT. Les plates-formes Cisco 350X sont les plus économiques du marché, proposent une connectivité 10 Gigabit Ethernet et disposent d'une capacité d'empilage.

Figure 1. Commutateurs administrables et empilables Cisco 350X



Les commutateurs Cisco 350X sont conçus pour protéger vos investissements technologiques alors que votre entreprise se développe. Contrairement aux commutateurs soi-disant empilables, mais dont certains éléments requièrent une administration et un dépannage distincts, les commutateurs Cisco 350X offrent une véritable capacité d'empilage qui vous permet de configurer, de gérer et de dépanner plusieurs commutateurs physiques comme s'il n'y en avait qu'un, et ainsi d'étendre votre réseau plus facilement.

Une véritable pile fournit un plan de données et de contrôle unifié, en plus d'un plan de gestion flexible, évolutif et facile à utiliser, puisque la pile de commutateurs fonctionne comme une seule entité rassemblant tous les ports des membres de la pile. Les commutateurs protègent également vos investissements technologiques avec une meilleure garantie, une assistance technique dédiée et la possibilité de mettre à niveau l'équipement à l'avenir. En bref, la gamme Cisco 350X constitue la base technologique idéale pour une entreprise en pleine croissance.

Caractéristiques et avantages

Les commutateurs Cisco 350X offrent les fonctionnalités avancées dont les entreprises en plein essor ont besoin, et que les applications et les technologies gourmandes en bande passante requièrent. Ces commutateurs améliorent la disponibilité de vos applications stratégiques, protègent les informations de votre entreprise et optimisent la bande passante de votre réseau pour garantir une mise à disposition plus efficace des informations et une meilleure prise en charge des applications. Ils offrent les avantages détaillés ci-dessous.

Simplicité de déploiement et d'utilisation

Les commutateurs Cisco 350X sont conçus pour être faciles à utiliser et à gérer par les entreprises commerciales et leurs partenaires. Ils offrent les fonctionnalités suivantes :

- Des interfaces graphiques faciles à utiliser réduisent le temps de déploiement, de dépannage et de gestion du réseau, et permettent la prise en charge de fonctionnalités sophistiquées, sans personnel IT supplémentaire.
- Les commutateurs prennent également en charge Textview, une interface de ligne de commande (CLI) complète pour ceux qui préfèrent cette option.
- Grâce aux fonctionnalités intelligentes Auto Smartports, le commutateur est capable de détecter un périphérique réseau connecté à tout port et de configurer automatiquement les paramètres optimaux de sécurité, de qualité de service (QoS) et de disponibilité au niveau de ce port.
- Le protocole CDP (Cisco Discovery Protocol) détecte les appareils Cisco et leur permet de partager des informations de configuration critiques, simplifiant ainsi l'installation et l'intégration du réseau.
- La prise en charge du protocole SNMP (Simple Network Management Protocol) vous permet de configurer et de gérer vos commutateurs et d'autres périphériques Cisco à distance, à partir d'une station de gestion réseau, ce qui améliore le flux de travail IT et les configurations de masse.
- À l'aide d'une simple barre d'outils dans le navigateur Web de l'utilisateur, l'utilitaire Cisco FindIT détecte les périphériques Cisco du réseau et affiche les informations élémentaires, comme les numéros de série et les adresses IP, afin de faciliter la configuration et le déploiement. (Pour obtenir plus d'informations et télécharger gratuitement cet utilitaire, rendez-vous sur www.cisco.com/go/findit.)

Une fiabilité et une résilience élevées

Pour les entreprises en plein développement pour lesquelles une disponibilité 24h/24 et 7j/7 est cruciale, il est fondamental de s'assurer que les employés disposent d'un accès permanent aux données et aux ressources dont ils ont besoin. Dans ces environnements, les commutateurs empilables peuvent jouer un rôle important en éliminant les temps d'arrêt et en améliorant la résilience du réseau. Par exemple, en cas de défaillance d'un commutateur Cisco 350X dans une pile, un autre prend immédiatement le relais, garantissant ainsi la disponibilité totale du réseau. Chaque entité de la pile peut par ailleurs être remplacée sans déconnexion du réseau ni impact sur la productivité des employés.

Les commutateurs Cisco 350X prennent également en charge les doubles images, ce qui vous permet d'effectuer des mises à niveau logicielles sans déconnecter le réseau, ni vous soucier d'une coupure du réseau pendant ce processus.

Des opérations IT simplifiées

Les commutateurs Cisco 350X optimisent vos opérations IT grâce à des fonctionnalités intégrées qui simplifient et rationalisent l'exploitation quotidienne de votre réseau :

- Une véritable capacité d'empilage vous permet de configurer, de gérer et de dépanner plusieurs commutateurs physiques comme une seule entité.
- Les commutateurs Cisco partagent des jeux de composants et des logiciels, de sorte que tous les commutateurs d'une catégorie donnée prennent en charge le même jeu de fonctionnalités, ce qui simplifie la gestion et la prise en charge de l'ensemble des commutateurs sur le réseau.

Une véritable capacité d'empilage

Certains commutateurs qui se disent empilables ne permettent en pratique qu'un « regroupement », chaque entité devant être configurée et gérée individuellement. Les commutateurs Cisco 350X offrent, quant à eux, une véritable capacité d'empilage : vous pouvez configurer, gérer et dépanner tous les commutateurs d'une pile comme une seule entité, avec une adresse IP unique pour un maximum de $48 * 4 = 192$ ports Ethernet.

Une véritable pile fournit un plan de données et de contrôle unifié, en plus d'un plan de gestion flexible, évolutif et facile à utiliser, puisque la pile de commutateurs fonctionne comme une seule entité rassemblant tous les ports des membres de la pile. Dans un environnement réseau en plein développement, cette capacité peut considérablement réduire la complexité, tout en améliorant la résilience et la disponibilité des applications réseau. Cet empilage réel, au travers de fonctionnalités telles que la QoS interpile, les VLAN, les LAG et la mise en miroir des ports, que ne prennent pas en charge les commutateurs en grappe, offre encore bien des bénéfices en termes de réduction des coûts et de gestion.

Une haute sécurité

Les commutateurs Cisco 350X offrent les fonctionnalités de sécurité avancées dont vous avez besoin pour protéger les données de votre entreprise et interdire aux utilisateurs non autorisés l'accès à votre réseau :

- Le cryptage SSL (Secure Sockets Layer) intégré protège les données administratives acheminées vers et depuis le commutateur.
- Des listes de contrôle d'accès (ACL) étendues restreignent l'accès à des parties sensibles du réseau pour tenir à l'écart les utilisateurs non autorisés et prévenir les attaques contre le réseau.
- Des réseaux VLAN invités (VLAN) vous permettent d'offrir une connectivité Internet aux utilisateurs non-employés tout en isolant les services stratégiques de l'entreprise du trafic invité.

- Une prise en charge des applications avancées de sécurité réseau, comme la sécurité de port IEEE 802.1X, permet de restreindre strictement l'accès à des segments spécifiques de votre réseau. Une solution d'authentification basée sur le Web offre une interface homogène pour l'authentification de tous les types d'appareils hôte et de systèmes d'exploitation, sans avoir recours au déploiement complexe de clients IEEE 802.1X sur chaque terminal.
- Des mécanismes de défense avancés, notamment l'inspection ARP (Address Resolution Protocol) dynamique, la protection de la source IP et la surveillance DHCP (Dynamic Host Configuration Protocol) détectent et bloquent les attaques réseau délibérées. Les combinaisons de ces protocoles sont également appelées IPMB (liaison IP-MAC).
- La sécurité IPv6 First Hop étend une solution avancée de protection contre les menaces à l'IPv6. Cette solution de sécurité complète intègre l'inspection ND, la protection RA, la protection DHCPv6 et le contrôle de l'intégrité des liaisons avec les appareils voisins afin de protéger vos réseaux IPv6 contre toutes sortes d'attaques, notamment l'usurpation d'adresses et les attaques par intermédiaire (man-in-the-middle).
- Des listes de contrôle d'accès (ACL) et un fonctionnement des ports tous deux basés sur l'heure permettent de limiter l'accès au réseau pendant des durées prédéfinies (heures d'ouverture, par exemple).
- Une sécurité uniforme basée sur l'adresse MAC peut être appliquée automatiquement aux utilisateurs mobiles lorsqu'ils se déplacent entre les points d'accès sans fil.
- La technologie SCT (Secure Core Technology) permet au commutateur de traiter le trafic de gestion en cas d'attaque par refus de service (DoS).
- La technologie PVE (Private VLAN Edge) fournit une isolation de couche 2 entre les périphériques situés sur le même VLAN.
- Le contrôle des débordements peut être appliqué au trafic de diffusion, de multideestination et de monodiffusion inconnue.
- Les sessions de gestion sont protégées à l'aide d'authentifications RADIUS, TACACS+ et via la base de données locale, et de sessions de gestion sécurisées sur SSL, SSH et SNMPv3.
- La prévention des attaques par refus de service (DoS) optimise le temps de disponibilité du réseau en cas d'attaque.

Un déploiement automatique de systèmes voix sur l'ensemble du réseau

À l'aide d'une combinaison des protocoles CDP, LLDP-MED, Auto Smartports et VSDP (Voice Services Discovery Protocol, un protocole unique de Cisco), les clients peuvent déployer un réseau voix de bout en bout de manière dynamique. Les commutateurs sur le réseau convergent automatiquement autour d'un VLAN voix unique et de paramètres QoS, puis les diffusent vers les téléphones sur les ports où ils sont détectés. Par exemple, les fonctionnalités de VLAN voix automatisées vous permettent de brancher n'importe quel téléphone IP (y compris des téléphones tiers) sur votre réseau de téléphonie IP et d'entendre immédiatement une tonalité. Le commutateur configure automatiquement le périphérique et applique les paramètres VLAN et QoS appropriés pour hiérarchiser le trafic voix.

Prise en charge d'IPv6

Le schéma d'adressage IP évoluant pour s'adapter à un plus grand nombre d'appareils réseau, les commutateurs Cisco 350X prennent en charge la transition vers les réseaux et les systèmes d'exploitation de nouvelle génération tels que Windows 7, Vista et Linux. Ces commutateurs prennent toujours en charge l'ancien protocole IPv4, ce qui vous permet d'évoluer vers la nouvelle norme IPv6 à votre rythme, avec l'assurance que votre réseau actuel sera toujours capable de prendre en charge vos applications métier à l'avenir. Les commutateurs Cisco 350X ont réussi de rigoureux tests IPv6 et ont obtenu les certifications USGv6 et IPv6 Gold.

Une gestion avancée du trafic de couche 3

La gamme Cisco 350X intègre un jeu plus avancé de fonctionnalités de gestion du trafic, qui aide les entreprises en pleine croissance à organiser leur réseau de manière plus efficace. Ces commutateurs assurent par exemple le routage LAN statique de couche 3, ce qui vous permet de segmenter votre réseau en groupes de travail et de communiquer entre plusieurs réseaux VLAN sans que cela n'affecte la performance des applications.

Grâce à ces fonctionnalités, vous pouvez optimiser l'efficacité de votre réseau en déchargeant votre routeur des tâches de gestion du trafic interne afin qu'il gère prioritairement le trafic externe et la sécurité.

Les modèles Cisco 350X offrent par ailleurs des fonctionnalités de routage statique de couche 3. Celles-ci réduisent la nécessité de configuration manuelle des périphériques de routage et simplifient le fonctionnement continu du réseau.

Efficacité énergétique

Les nombreuses fonctionnalités écoénergétiques intégrées sur tous les modèles Cisco 350X en font la plus vaste gamme de commutateurs écoénergétiques disponible sur le marché. Ces commutateurs sont conçus pour conserver l'énergie en optimisant sa consommation, afin de protéger l'environnement et de réduire vos coûts énergétiques. Ils offrent une solution réseau écologique, sans que cela n'affecte les performances.

Les commutateurs Cisco 350X offrent les atouts suivants :

- Une prise en charge de la norme Energy Efficient Ethernet (IEEE 802.3az), qui favorise la réduction de la consommation d'énergie par la surveillance du volume de trafic sur une liaison active et par la mise en veille lors des périodes calmes.
- Les derniers circuits ASIC (Application-Specific Integrated Circuit), qui s'appuient sur une technologie à faible consommation de 65/40 nanomètres et des processeurs ARM à faible consommation hautes performances.
- L'arrêt automatique de l'alimentation sur les ports PoE lorsqu'une liaison est en panne.
- La possibilité de désactiver les voyants pour économiser de l'énergie.
- Des fonctionnalités intelligentes intégrées pour ajuster la puissance du signal selon la longueur de câble.

La tranquillité d'esprit et la protection des investissements

Les commutateurs Cisco 350X offrent les performances fiables et la tranquillité d'esprit que l'on attend d'un commutateur Cisco. Lorsque vous investissez dans la gamme Cisco 350X, vous profitez des bénéfices suivants :

- Une garantie limitée à vie avec remplacement anticipé le jour ouvrable suivant (sous réserve de disponibilité, sinon expédition le jour même).
- Une solution soumise à des tests rigoureux pour garantir un temps de disponibilité du réseau optimal et maintenir la productivité des employés en assurant leur accès permanent aux ressources stratégiques.

- Une solution conçue et testée pour permettre une intégration simple et une entière compatibilité avec les autres produits Cisco pour la voix, les communications unifiées, la sécurité et la mise en réseau, au sein d'une plate-forme technologique complète.

Garantie matérielle à vie limitée Cisco

Les commutateurs Cisco 350X offrent une garantie matérielle limitée à vie avec remplacement anticipé le jour ouvrable suivant (sous réserve de disponibilité, sinon expédition le jour même) et une garantie limitée à vie sur les ventilateurs et les blocs d'alimentation.

De plus, Cisco propose des mises à jour logicielles pour la correction de bugs selon les conditions de la garantie ainsi qu'une assistance téléphonique gratuite les 12 premiers mois suivant la date de l'achat. Pour télécharger les mises à jour logicielles, accédez à la page <http://software.cisco.com/download/navigator.html>.

Pour en savoir plus sur les conditions de garantie et obtenir des informations supplémentaires sur les produits Cisco, rendez-vous sur www.cisco.com/go/warranty.

Service et assistance performants

Votre temps est précieux, surtout lorsqu'un problème affecte vos activités. Les commutateurs Cisco 350X bénéficient du service d'assistance Cisco SMARTnet[®], qui garantit votre tranquillité d'esprit à un prix abordable. Ce service disponible sur abonnement vous aide à protéger votre investissement et à exploiter pleinement les produits Cisco SMB. Mis en place par Cisco et soutenu par votre partenaire de confiance, ce service complet propose des mises à jour logicielles et un accès au centre d'assistance Cisco, et prolonge le service technique à trois ans.

Les produits Cisco SMB bénéficient du soutien de professionnels spécifiquement formés pour comprendre vos besoins, qui travaillent au sein du centre d'assistance Cisco, un service dédié aux petites entreprises avec des locaux dans le monde entier. Vous pouvez également accéder à des informations techniques et produit complètes via la communauté d'assistance Cisco, un forum en ligne qui vous permet de collaborer avec vos pairs et joindre des experts techniques Cisco.

Spécifications techniques

Le tableau 1 présente les caractéristiques du produit.

Tableau 1. Caractéristiques techniques

Fonction	Description		
Performances			
Capacité de commutation et débit de transfert Tous les commutateurs fonctionnent à la vitesse du câble sans blocage.	Nom de produit		
	Capacité en Mp/s (paquets de 64 octets)		
	Capacité de commutation (Gbit/s)		
	SG350XG-24T	357,12	480
	SG350XG-24F	357,12	480
SG350XG-48T	714,24	960	
SG350XG-2F10	178,56	240	
Commutation de couche 2			
Protocole STP (Spanning Tree Protocol)	Prise en charge de la norme 802.1d Spanning Tree Convergence rapide en utilisant 802.1w (Rapid Spanning Tree [RSTP]), activé par défaut Instances MSTP (Multiple Spanning Tree) utilisant 802.1s. 16 instances sont prises en charge		
Regroupement de ports / Agrégation de liaisons	Prise en charge du protocole LACP (Link Aggregation Control Protocol) IEEE 802.3ad <ul style="list-style-type: none"> • Jusqu'à 32 groupes • Jusqu'à 8 ports par groupe avec 16 ports candidats pour chaque LAG 802.3ad (dynamique) 		

Fonction	Description
VLAN	Prise en charge simultanée de 4 096 VLAN VLAN basés sur les ports et les balises 802.1Q Réseau VLAN basé sur MAC. VLAN de gestion PVE (Private VLAN Edge), également appelé « port protégé », avec plusieurs liaisons montantes Réseau VLAN invité ; réseau VLAN non authentifié ; réseau VLAN basé sur protocole ; réseau VLAN CPE Affectation de VLAN dynamique via un serveur RADIUS avec authentification client 802.1x
VLAN voix	Le trafic voix est automatiquement affecté à un réseau VLAN voix spécifique et traité avec les niveaux QoS appropriés. Des fonctionnalités de voix automatique permettent de déployer sans intervention des terminaux voix et des terminaux de commande d'appel à l'échelle du réseau.
VLAN TV multidestination	Permet de partager le réseau VLAN multidestination unique au sein du réseau tandis que les abonnés restent sur des réseaux VLAN séparés. Cette fonctionnalité est également appelée « enregistrement VLAN multidestination » (MVR).
Q-in-Q	Les VLAN franchissent le réseau d'un prestataire de services de façon transparente, tout en isolant le trafic parmi les utilisateurs.
GVRP/GARP	Les protocoles GVRP (Generic VLAN Registration Protocol) et GARP (Generic Attribute Registration Protocol) assurent la propagation et la configuration automatiques des VLAN dans un domaine de pont.
Détection de liaison unidirectionnelle (UDLD - Unidirectional Link Detection)	L'UDLD contrôle la connexion physique pour détecter des liaisons unidirectionnelles causées par un câblage incorrect ou des ports défectueux afin d'éviter les boucles d'acheminement et les trous noirs dans le trafic des réseaux commutés.
Relais DHCP au niveau de la couche 2	Relais de trafic DHCP vers un serveur DHCP sur un réseau VLAN différent. Fonctionne avec DHCP option 82.
Surveillance IGMP (versions 1, 2 et 3)	Le protocole IGMP (Internet Group Management Protocol) limite le trafic multidestination à forte consommation de bande passante aux seuls demandeurs. Il prend en charge 4 000 groupes de multidestination (le protocole SSM [Source Specific Multicast] est également pris en charge).
Demandeur IGMP	Le demandeur IGMP est utilisé pour prendre en charge un domaine de diffusion multipoint de couche 2 de commutateurs de surveillance en l'absence d'un routeur multipoint.
Blocage HOL	Blocage en tête de ligne (HOL).
Trames géantes	Trames jusqu'à 10 000 octets.
Couche 3	
Routage IPv4	Routage à vitesse filaire des paquets IPv4 Jusqu'à 8 000 routes statiques et 256 interfaces IP
Routage statique IPv6 à vitesse du câble	Jusqu'à 2 048 routes statiques et 256 interfaces IPv6
Interface de couche 3	Configuration de l'interface de couche 3 sur un port physique, un LAG, une interface VLAN ou une interface de bouclage
CIDR	Prise en charge du routage CIDR (Classless Inter-Domain Routing)
Serveur DHCP	Fonctions de commutation, sous la forme d'un serveur DHCP IPv4, traitant des adresses IP pour de nombreux regroupements/périmètres DHCP Prise en charge des options DHCP
Relais DHCP au niveau de la couche 3	Relais du trafic DHCP sur les domaines IP.
Relais UDP (User Datagram Protocol)	Relais des informations de diffusion sur les domaines de couche 3 pour la détection d'applications ou relais de paquets BOOTP/DHCP
Empilage	
Pile matérielle	Jusqu'à 4 unités par pile. Jusqu'à 208 ports gérés comme un seul système avec basculement matériel.
Haute disponibilité	Le basculement rapide entre les piles garantit une perte de trafic minimale.
Configuration/Gestion de l'empilage « plug-and-play »	Maître/Sauvegarde pour un contrôle des piles résilient Numérotation automatique Remplacement à chaud des unités de la pile Options d'empilage en anneau et en chaîne Débit de port à empilage automatique Options de port d'empilage flexibles.

Fonction	Description
Interconnexion haut débit des piles	Interfaces cuivre et fibre 10G haut débit économiques
Sécurité	
SSH	Le protocole SSH constitue un substitut sécurisé pour le trafic Telnet. Le protocole SCP utilise également ce protocole. Les versions 1 et 2 du protocole SSH sont prises en charge.
SSL	Le protocole SSL (Secure Sockets Layer) crypte l'ensemble du trafic HTTPS, ce qui permet un accès sécurisé à l'interface utilisateur graphique (IUG) du commutateur de gestion, accessible par navigateur.
IEEE 802.1X (rôle Authentificateur)	Authentification et comptabilité RADIUS, hachage MD5 ; VLAN invité ; VLAN non authentifié, mode hôte simple/multiple et sessions simples/multiples Prise en charge de l'affectation de VLAN dynamique 802.1X basée sur l'heure
Authentification Web	L'authentification basée sur le Web assure via un navigateur Web le contrôle d'admission au réseau des appareils hôte et des systèmes d'exploitation.
Protection BPDU STP	Un mécanisme de sécurité pour protéger le réseau de configurations non valides. Un port activé pour protection des unités BPDU (Bridge Protocol Data Unit) est fermé si un message BPDU est reçu sur ce port. Cela évite les boucles topologiques accidentelles.
Fonction STP Root Guard	Cette fonction empêche les périphériques réseau non contrôlés par l'administrateur réseau de devenir des nœuds racines pour le protocole Spanning Tree.
Surveillance DHCP	Filtre les messages DHCP qui possèdent des adresses IP non enregistrées et/ou qui sont issus d'interfaces imprévues ou non approuvées. Cette fonction empêche les périphériques indésirables de se comporter comme un serveur DHCP.
Protection de la source IP (IPSG)	Lorsque la protection de la source IP est activée au niveau d'un port, le commutateur filtre les paquets IP reçus de sa part si les adresses IP d'origine n'ont pas été configurées de manière statique, ni acquises de manière dynamique depuis la surveillance DHCP. Cette fonction empêche l'usurpation des adresses IP.
Inspection ARP dynamique (DAI)	Le commutateur élimine les paquets ARP issus d'un port si aucune liaison, statique ou dynamique, n'existe entre les adresses IP et MAC, ou s'il existe une divergence entre l'adresse d'origine ou de destination dans le paquet. Cette fonction empêche les attaques par intermédiaire (man-in-the-middle).
Liaison IP/Mac/Port (IPMB)	Les fonctionnalités de surveillance DHCP, de protection de la source IP et d'inspection ARP dynamique collaborent pour empêcher les attaques par refus de service (DoS) sur le réseau, améliorant ainsi sa disponibilité.
Secure Core Technology (SCT)	Garantit que le commutateur recevra et traitera le trafic lié à la gestion et aux protocoles, quel que soit le volume reçu.
Secure Sensitive Data (SSD)	Mécanisme permettant de gérer en toute sécurité les données sensibles (telles que les mots de passe, les clés, etc.) au niveau du commutateur lors de la transmission de ces données vers d'autres périphériques, et de sécuriser la configuration automatique. L'accès à la consultation des données sensibles, sous forme cryptée ou de texte clair, est accordé en fonction du niveau d'accès configuré pour l'utilisateur et son mode de connexion.
Isolation de la couche 2 (PVE) avec le réseau VLAN de la communauté	La technologie PVE (Private VLAN Edge) assure sécurité et isolation entre les ports de commutation, ce qui garantit que les utilisateurs ne peuvent pas surveiller le trafic d'autres utilisateurs. Elle prend en charge de multiples liaisons ascendantes.
Sécurité des ports	Possibilité de verrouiller les adresses MAC source aux ports et de limiter le nombre d'adresses MAC acquises.
RADIUS/TACACS+	Prend en charge l'authentification RADIUS et TACACS. Fonctions de commutation en tant que client.
Comptabilité RADIUS	Les fonctions de comptabilisation RADIUS permettent d'envoyer, au démarrage et à l'arrêt des services, des données indiquant la quantité de ressources (telles que le temps, les paquets, les octets, etc.) utilisées pendant la session.
Contrôle des tempêtes	Diffusion, multidiffusion, et monodiffusion inconnue.
Prévention des attaques par déni de service	Prévention des attaques par déni de service (DoS).
Multi-niveaux de privilèges utilisateurs dans l'interface CLI	Niveaux de privilèges 1, 7 et 15.
Listes de contrôle d'accès (ACL)	Prise en charge de 3 072 entrées. Limite de débit ou d'abandon basé sur l'adresse MAC, ID VLAN ou IP de source et destination, sur le protocole, le port, la priorité IP DSCP (Differentiated Services Code Point), les ports source et de destination TCP/UDP (User Datagram Protocol), la priorité 802.1p, le type Ethernet, les paquets ICMP (Internet Control Message Protocol), les paquets IGMP (Internet Group Management Protocol), l'indicateur TCP. Prise en charge des listes de contrôle d'accès (ACL) basées sur l'heure.

Fonction	Description
Qualité de service	
Niveaux de priorité	8 files d'attente matérielles
Planification	Priorité stricte et « Round Robin » pondérée (WRR)
Classe de service	Basée sur les ports ; basée sur la hiérarchisation VLAN 802.1p ; basée sur DSCP/ToS (type de service)/priorité IP IPv4/v6 ; services différenciés (DiffServ) ; classification et reclassification des listes de contrôle d'accès (ACL), qualité de service (QoS) validée Attribution de files d'attente basée sur un marquage DSCP (Differentiated Services Code Point) et classe de service (802.1p/CoS)
Limitation de débit	Contrôle en entrée ; lissage en sortie et contrôle du débit en entrée ; par VLAN, par port et basé sur le flux
Élimination d'encombrement	Un algorithme d'élimination de congestion TCP est requis pour minimiser et empêcher une perte de synchronisation globale TCP.
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 (Link Aggregation Control Protocol), IEEE 802.3z Gigabit Ethernet, contrôle de flux IEEE 802.3x, IEEE 802.3 ad LACP, IEEE 802.1D (STP, GARP et GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s MSTP (Multiple STP), 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 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	Mode hôte IPv6 ; IPv6 over Ethernet ; double pile IPv4 et IPv6 Détection d'appareils voisins et de routeurs (ND) pour IPv6 ; configuration automatique des adresses statiques IPv6 ; découverte du MTU de chemin Détection d'adresses en double (DAD) ICMPv6 Réseau IPv6 sur IPv4 avec prise en charge de la tunnelisation ISATAP Logo certifié USGv6 et IPv6 Gold
Qualité de service IPv6	Hiérarchiser les paquets IPv6 dans le matériel
ACL IPv6	Limite de débit ou d'abandon des paquets IPv6 dans le matériel
Sécurité du premier saut IPv6	Protection RA Inspection Inspection ND Protection DHCPv6 Table des liaisons avec les périphériques voisins (entrées de surveillance et entrées statiques) Contrôle de l'intégrité des liaisons avec les périphériques voisins
Surveillance MDL (Multicast Listener Discovery v1/2)	Remettre des paquets de diffusion multipoint IPv6 uniquement aux destinataires requis
Applications IPv6	Web/SSL, serveur Telnet/SSH, Ping, Traceroute, protocoles SNMP, TFTP, SNMP, RADIUS, Syslog, client DNS, client DHCP, configuration automatique DHCP, relais DHCP IPv6, TACACS
RFC IPv6 pris en charge	RFC 4443 (en remplacement de RFC 2463) : ICMPv6 RFC 4291 (en remplacement de RFC 3513) : architecture d'adresses IPv6 RFC 4291 : architecture d'adressage IPv6 RFC 2460 : spécification IPv6 RFC 4861 (en remplacement de RFC 2461) : détection d'appareils voisins pour IPv6 RFC 4862 (en remplacement de RFC 2462) : configuration automatique des adresses statiques IPv6 RFC 1981 : Découverte du MTU de chemin. RFC 4007 : architecture d'adressage étendue IPv6 RFC 3484 : mécanisme de sélection de l'adresse par défaut RFC 5214 (en remplacement de RFC 4214) : tunnel ISATAP RFC 4293 : MIB IPv6 : conventions textuelles et groupe général RFC 3595 : conventions textuelles pour étiquette de flux IPv6

Fonction	Description																																										
Gestion																																											
Interface utilisateur web	Utilitaire de configuration de commutateurs intégré pour une configuration d'appareil via navigateur (HTTP/HTTPS). Prend en charge la configuration, le tableau de bord du système, la maintenance du système et la surveillance.																																										
SNMP	SNMP versions 1, 2c et 3 avec prise en charge des filtres et USM (User-Based Security Model) pour SNMP version 3																																										
MIB normalisés	<table border="0"> <tr> <td>lldp-MIB</td> <td>rfc2665-MIB</td> </tr> <tr> <td>lldpextdot1-MIB</td> <td>rfc2668-MIB</td> </tr> <tr> <td>lldpextdot3-MIB</td> <td>rfc2737-MIB</td> </tr> <tr> <td>lldpextmed-MIB</td> <td>rfc3621-MIB</td> </tr> <tr> <td>rfc2674-MIB</td> <td>rfc4668-MIB</td> </tr> <tr> <td>rfc2575-MIB</td> <td>rfc4670-MIB</td> </tr> <tr> <td>rfc2573-MIB</td> <td>trunk-MIB</td> </tr> <tr> <td>rfc2233-MIB</td> <td>tunnel-MIB</td> </tr> <tr> <td>rfc2013-MIB</td> <td>udp-MIB</td> </tr> <tr> <td>rfc2012-MIB</td> <td>draft-ietf-bridge-8021x-MIB</td> </tr> <tr> <td>rfc2011-MIB</td> <td>draft-ietf-bridge-rstp-mib-04-MIB</td> </tr> <tr> <td>RFC-1212</td> <td>draft-ietf-hubmib-etherif-mib-v3-00-MIB</td> </tr> <tr> <td>RFC-1215</td> <td>ianaaddrfamnumbers-MIB</td> </tr> </table>	lldp-MIB	rfc2665-MIB	lldpextdot1-MIB	rfc2668-MIB	lldpextdot3-MIB	rfc2737-MIB	lldpextmed-MIB	rfc3621-MIB	rfc2674-MIB	rfc4668-MIB	rfc2575-MIB	rfc4670-MIB	rfc2573-MIB	trunk-MIB	rfc2233-MIB	tunnel-MIB	rfc2013-MIB	udp-MIB	rfc2012-MIB	draft-ietf-bridge-8021x-MIB	rfc2011-MIB	draft-ietf-bridge-rstp-mib-04-MIB	RFC-1212	draft-ietf-hubmib-etherif-mib-v3-00-MIB	RFC-1215	ianaaddrfamnumbers-MIB																
lldp-MIB	rfc2665-MIB																																										
lldpextdot1-MIB	rfc2668-MIB																																										
lldpextdot3-MIB	rfc2737-MIB																																										
lldpextmed-MIB	rfc3621-MIB																																										
rfc2674-MIB	rfc4668-MIB																																										
rfc2575-MIB	rfc4670-MIB																																										
rfc2573-MIB	trunk-MIB																																										
rfc2233-MIB	tunnel-MIB																																										
rfc2013-MIB	udp-MIB																																										
rfc2012-MIB	draft-ietf-bridge-8021x-MIB																																										
rfc2011-MIB	draft-ietf-bridge-rstp-mib-04-MIB																																										
RFC-1212	draft-ietf-hubmib-etherif-mib-v3-00-MIB																																										
RFC-1215	ianaaddrfamnumbers-MIB																																										
MIB normalisés (suite)	<table border="0"> <tr> <td>SNMPv2-CONF</td> <td>ianaifty-MIB</td> </tr> <tr> <td>SNMPv2-TC</td> <td>ianaprot-MIB</td> </tr> <tr> <td>p-bridge-MIB</td> <td>inet-address-MIB</td> </tr> <tr> <td>q-bridge-MIB</td> <td>ip-forward-MIB</td> </tr> <tr> <td>rfc1389-MIB</td> <td>ip-MIB</td> </tr> <tr> <td>rfc1493-MIB</td> <td>RFC1155-SMI</td> </tr> <tr> <td>rfc1611-MIB</td> <td>RFC1213-MIB</td> </tr> <tr> <td>rfc1612-MIB</td> <td>SNMPv2-MIB</td> </tr> <tr> <td>rfc1850-MIB</td> <td>SNMPv2-SMI</td> </tr> <tr> <td>rfc1907-MIB</td> <td>SNMPv2-TM</td> </tr> <tr> <td>rfc2571-MIB</td> <td>RMON-MIB</td> </tr> <tr> <td>rfc2572-MIB</td> <td>rfc1724-MIB</td> </tr> <tr> <td>rfc2574-MIB</td> <td>dcb-raj-DCBX-MIB-1108-MIB</td> </tr> <tr> <td>rfc2576-MIB</td> <td>rfc1213-MIB</td> </tr> <tr> <td>rfc2613-MIB</td> <td>rfc1757-MIB</td> </tr> </table>	SNMPv2-CONF	ianaifty-MIB	SNMPv2-TC	ianaprot-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	SNMPv2-MIB	rfc1850-MIB	SNMPv2-SMI	rfc1907-MIB	SNMPv2-TM	rfc2571-MIB	RMON-MIB	rfc2572-MIB	rfc1724-MIB	rfc2574-MIB	dcb-raj-DCBX-MIB-1108-MIB	rfc2576-MIB	rfc1213-MIB	rfc2613-MIB	rfc1757-MIB												
SNMPv2-CONF	ianaifty-MIB																																										
SNMPv2-TC	ianaprot-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	SNMPv2-MIB																																										
rfc1850-MIB	SNMPv2-SMI																																										
rfc1907-MIB	SNMPv2-TM																																										
rfc2571-MIB	RMON-MIB																																										
rfc2572-MIB	rfc1724-MIB																																										
rfc2574-MIB	dcb-raj-DCBX-MIB-1108-MIB																																										
rfc2576-MIB	rfc1213-MIB																																										
rfc2613-MIB	rfc1757-MIB																																										
MIB privés	<table border="0"> <tr> <td>CISCOB-lldp-MIB</td> <td>CISCOB-iprouter-MIB</td> </tr> <tr> <td>CISCOB-brgmulticast-MIB</td> <td>CISCOB-ipv6-MIB</td> </tr> <tr> <td>CISCOB-bridgemibobjects-MIB</td> <td>CISCOB-mnginf-MIB</td> </tr> <tr> <td>CISCOB-bonjour-MIB</td> <td>CISCOB-lic-MIB</td> </tr> <tr> <td>CISCOB-dhcpcl-MIB</td> <td>CISCOB-localization-MIB</td> </tr> <tr> <td>CISCOB-MIB</td> <td>CISCOB-mcmngr-MIB</td> </tr> <tr> <td>CISCOB-wrandomtaildrop-MIB</td> <td>CISCOB-mng-MIB</td> </tr> <tr> <td>CISCOB-traceroute-MIB</td> <td>CISCOB-physdescription-MIB</td> </tr> <tr> <td>CISCOB-telnet-MIB</td> <td>CISCOB-PoE-MIB</td> </tr> <tr> <td>CISCOB-stormctrl-MIB</td> <td>CISCOB-protectedport-MIB</td> </tr> <tr> <td>CISCOBssh-MIB</td> <td>CISCOB-rmon-MIB</td> </tr> <tr> <td>CISCOB-socket-MIB</td> <td>CISCOB-rs232-MIB</td> </tr> <tr> <td>CISCOB-sntp-MIB</td> <td>CISCOB-SecuritySuite-MIB</td> </tr> <tr> <td>CISCOB-smon-MIB</td> <td>CISCOB-snmplib-MIB</td> </tr> <tr> <td>CISCOB-phy-MIB</td> <td>CISCOB-specialbpdu-MIB</td> </tr> <tr> <td>CISCOB-multisessionterminal-MIB</td> <td>CISCOB-banner-MIB</td> </tr> <tr> <td>CISCOB-mri-MIB</td> <td>CISCOB-syslog-MIB</td> </tr> <tr> <td>CISCOB-jumboframes-MIB</td> <td>CISCOB-TcpSession-MIB</td> </tr> <tr> <td>CISCOB-gvrp-MIB</td> <td>CISCOB-traps-MIB</td> </tr> <tr> <td>CISCOB-endofmib-MIB</td> <td>CISCOB-trunk-MIB</td> </tr> <tr> <td>CISCOB-dot1x-MIB</td> <td>CISCOB-tuning-MIB</td> </tr> </table>	CISCOB-lldp-MIB	CISCOB-iprouter-MIB	CISCOB-brgmulticast-MIB	CISCOB-ipv6-MIB	CISCOB-bridgemibobjects-MIB	CISCOB-mnginf-MIB	CISCOB-bonjour-MIB	CISCOB-lic-MIB	CISCOB-dhcpcl-MIB	CISCOB-localization-MIB	CISCOB-MIB	CISCOB-mcmngr-MIB	CISCOB-wrandomtaildrop-MIB	CISCOB-mng-MIB	CISCOB-traceroute-MIB	CISCOB-physdescription-MIB	CISCOB-telnet-MIB	CISCOB-PoE-MIB	CISCOB-stormctrl-MIB	CISCOB-protectedport-MIB	CISCOBssh-MIB	CISCOB-rmon-MIB	CISCOB-socket-MIB	CISCOB-rs232-MIB	CISCOB-sntp-MIB	CISCOB-SecuritySuite-MIB	CISCOB-smon-MIB	CISCOB-snmplib-MIB	CISCOB-phy-MIB	CISCOB-specialbpdu-MIB	CISCOB-multisessionterminal-MIB	CISCOB-banner-MIB	CISCOB-mri-MIB	CISCOB-syslog-MIB	CISCOB-jumboframes-MIB	CISCOB-TcpSession-MIB	CISCOB-gvrp-MIB	CISCOB-traps-MIB	CISCOB-endofmib-MIB	CISCOB-trunk-MIB	CISCOB-dot1x-MIB	CISCOB-tuning-MIB
CISCOB-lldp-MIB	CISCOB-iprouter-MIB																																										
CISCOB-brgmulticast-MIB	CISCOB-ipv6-MIB																																										
CISCOB-bridgemibobjects-MIB	CISCOB-mnginf-MIB																																										
CISCOB-bonjour-MIB	CISCOB-lic-MIB																																										
CISCOB-dhcpcl-MIB	CISCOB-localization-MIB																																										
CISCOB-MIB	CISCOB-mcmngr-MIB																																										
CISCOB-wrandomtaildrop-MIB	CISCOB-mng-MIB																																										
CISCOB-traceroute-MIB	CISCOB-physdescription-MIB																																										
CISCOB-telnet-MIB	CISCOB-PoE-MIB																																										
CISCOB-stormctrl-MIB	CISCOB-protectedport-MIB																																										
CISCOBssh-MIB	CISCOB-rmon-MIB																																										
CISCOB-socket-MIB	CISCOB-rs232-MIB																																										
CISCOB-sntp-MIB	CISCOB-SecuritySuite-MIB																																										
CISCOB-smon-MIB	CISCOB-snmplib-MIB																																										
CISCOB-phy-MIB	CISCOB-specialbpdu-MIB																																										
CISCOB-multisessionterminal-MIB	CISCOB-banner-MIB																																										
CISCOB-mri-MIB	CISCOB-syslog-MIB																																										
CISCOB-jumboframes-MIB	CISCOB-TcpSession-MIB																																										
CISCOB-gvrp-MIB	CISCOB-traps-MIB																																										
CISCOB-endofmib-MIB	CISCOB-trunk-MIB																																										
CISCOB-dot1x-MIB	CISCOB-tuning-MIB																																										

Fonction	Description
	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-env_mib-MIB CISCOSB-policy-MIB CISCOSB-sensor-MIB CISCOSB-aaa-MIB CISCOSB-application-MIB CISCOSB-bridgesecurity-MIB CISCOSB-copy-MIB CISCOSB-CpuCounters-MIB CISCOSB-Custom1BonjourService-MIB CISCOSB-dhcp-MIB CISCOSB-tunnel-MIB CISCOSB-udp-MIB CISCOSB-vlan-MIB CISCOSB-ipstdacl-MIB CISCOSB-eee-MIB CISCOSB-ssl-MIB CISCOSB-digitalkeymanage-MIB CISCOSB-qosclimib-MIB CISCOSB-vrrp-MIB CISCOSB-tbp-MIB CISCOSB-stack-MIB CISCOSB-MIB CISCOSB-secsd-MIB CISCOSB-draft-ietf-entmib-sensor-MIB CISCOSB-draft-ietf-syslog-device-MIB CISCOSB-rfc2925-MIB CISCOSB-vrrpv3-MIB CISCO-SMI-MIB
MIB privés (suite)	CISCOSB-dif-MIB CISCOSB-dnscI-MIB CISCOSB-embweb-MIB CISCOSB-fft-MIB CISCOSB-file-MIB CISCOSB-greeneth-MIB CISCOSB-interfaces-MIB CISCOSB-interfaces_recovery-MIB CISCOSB-ip-MIB CISCOSB-DebugCapabilities-MIB CISCOSB-CDP-MIB CISCOSB-vlanVoice-MIB CISCOSB-EVENTS-MIB CISCOSB-symng-MIB CISCOSB-sct-MIB CISCO-TC-MIB CISCO-VTP-MIB CISCO-CDP-MIB
RMON	L'agent logiciel intégré de surveillance à distance ou RMON prend en charge 4 groupes de données (historique, statistiques, alarmes et événements) pour améliorer la gestion, la surveillance et l'analyse du trafic.
Double pile IPv4 et IPv6	Coexistence des deux piles de protocole pour une migration facile
Mise à niveau du micrologiciel	<ul style="list-style-type: none"> Mise à niveau par navigateur Web (HTTP/HTTPS), TFTP et SCP La mise à niveau peut également être initialisée par l'intermédiaire du port de console Doubles images pour des mises à niveau de microprogramme résilientes
Mise en miroir des ports	Le trafic sur un port peut être mis en miroir sur un autre port et analysé à l'aide d'un analyseur réseau ou d'une sonde de surveillance à distance. 8 ports sources maximum peuvent être mis en miroir sur un port de destination.
Mise en miroir de VLAN	Le trafic provenant d'un réseau VLAN peut être mis en miroir sur un port et analysé à l'aide d'un analyseur réseau ou d'une sonde de surveillance à distance. 8 réseaux VLAN sources maximum peuvent être mis en miroir sur un port de destination.
DHCP (options 12, 66, 67, 82, 129 et 150)	Les options DHCP favorisent un contrôle plus étroit depuis un point central (serveur DHCP) afin d'obtenir une adresse IP, une configuration automatique (avec téléchargement du fichier de configuration), un relais DHCP et un nom d'hôte.
Configuration automatique avec téléchargement du fichier de copie sécurisée (SCP)	Permet un déploiement en masse sécurisé avec protection des données sensibles.
Fichiers de configuration au format texte éditable	Les fichiers de configuration peuvent être modifiés avec un éditeur de texte et téléchargés sur un autre commutateur, facilitant le déploiement en masse.
SmartPorts	Configuration simplifiée des fonctionnalités QoS et de sécurité.
Auto Smartports	Applique automatiquement au port les informations fournies par le biais des rôles Smartports, en fonction des appareils détectés avec les protocoles CDP ou LLDP-MED. Cela facilite les déploiements automatiques.
Copie sécurisée (SCP)	Transférer en toute sécurité des fichiers vers et depuis le commutateur.
Interface de ligne de commande (CLI) Textview	Interface de ligne de commande (CLI) pouvant contenir des scripts. Prise en charge d'une interface CLI complète et d'une interface CLI avec menus.
Services cloud	Prise en charge de Cisco Small Business et de Cisco OnPlus.

Fonction	Description				
Localisation	Traduction de l'interface utilisateur graphique (IUG) et de la documentation en plusieurs langues.				
Bannière d'ouverture de session	Bannières de connexion configurables pour le Web ainsi que des interfaces CLI.				
Fonctionnement des ports basé sur l'heure	Lien actif ou non en fonction de la programmation définie par l'utilisateur (lorsque le port est administrativement activé).				
Autres	Traceroute ; gestion d'IP unique ; HTTP/HTTPS ; SSH ; RADIUS ; mise en miroir des ports ; mise à niveau TFTP ; client DHCP ; BOOTP ; SNTP (Simple Network Time Protocol) ; mise à niveau Xmodem ; diagnostics de câbles ; Ping ; syslog ; client Telnet (prise en charge SSH sécurisée) ; paramètres d'heure automatiques depuis la station de gestion.				
Performances écoénergétiques					
Détection d'énergie	Met automatiquement hors tension le port RJ-45 lors de la détection d'une interruption de liaison. Le mode actif reprend sans perte de paquets lorsque le commutateur détecte que la liaison est de nouveau active.				
Détection de la longueur du câble	Règle la puissance du signal en fonction de la longueur du câble. Réduit la consommation d'énergie pour les câbles d'une longueur inférieure à 10 m. Fonction prise en charge sur les modèles Gigabit Ethernet.				
Conformité à la norme EEE (802.3az)	Prise en charge de la norme 802.3az sur tous les ports Gigabit en cuivre.				
Désactivation des DEL sur les ports	Les DEL peuvent être éteintes manuellement afin d'économiser de l'énergie.				
Général					
Trames géantes	Trames jusqu'à 10 000 octets. La valeur MTU par défaut est 2 000.				
Table MAC	64 000 adresses.				
Détection					
Bonjour	Le commutateur s'annonce en utilisant le protocole Bonjour.				
LLDP (802.1ab) avec extensions LLDP-MED	Le protocole LLDP (Link Layer Discovery Protocol) permet au commutateur d'annoncer son identification, sa configuration et ses fonctionnalités aux périphériques voisins qui stockent les données dans une base de données MIB. Le protocole LLDP-MED est une amélioration du protocole LLDP qui ajoute les postes nécessaires aux téléphones IP.				
Protocole CDP	Le commutateur s'annonce en utilisant le protocole CDP (Cisco Discovery Protocol). Il détecte également la connexion d'un appareil et ses caractéristiques par le biais de ce protocole.				
Spécifications techniques					
Consommation énergétique (maximum)	Nom du modèle	Mode écoénergétique	Consommation énergétique du système	Consommation énergétique (avec PoE)	Dissipation thermique (BTU/h)
	SG350XG-24T	Détection d'énergie	110 V = 72,3 W 220 V = 71,8 W	N/A	288,67
	SG350XG-24F	N/A	110 V = 42,81 W 220 V = 43,1 W	N/A	264,44
	SG350XG-48T	Détection d'énergie	110 V = 131,7 W 220 V = 130,5 W	N/A	491,01
	SG350XG-2F10	Détection d'énergie	110 V = 50,1 W 220 V = 50,5 W	N/A	902,17
Ports	Nom du modèle	Nombre total de ports du système	Ports RJ-45	Ports combinés (RJ-45 + SFP)	
	SG350XG-24T	22 connecteurs XG cuivre, plus 2 connecteurs combinés XG cuivre/SFP+, plus 1 port de gestion OOB GE	22 XG	2 ports combinés XG cuivre/SFP+	
	SG350XG-24F	22 connecteurs XG SFP+, plus 2 connecteurs combinés XG cuivre/SFP+, plus 1 port de gestion OOB GE	2 ports XG combinés	22 connecteurs SFP+, plus 2 connecteurs combinés XG cuivre/SFP+	
	SG350XG-48T	46 connecteurs XG cuivre, plus 2 connecteurs combinés XG cuivre/SFP+, plus 1 port de gestion OOB GE	46 XG	2 ports combinés XG cuivre/SFP+	

Fonction	Description			
	SG350XG-2F10T	10 connecteurs XG cuivre, plus 2 connecteurs combinés XG cuivre/SFP+, plus 1 port de gestion OOB GE	10 XG	2 ports combinés XG cuivre/SFP+
Port USB	À des fins de gestion de fichiers			
Boutons	Bouton Reset			
Type de câblage	Paires torsadées non blindées (UTP) de catégorie 6e ou plus ; options fibre (SMF et MMF) ; SFP+ coaxial			
Voyants	Système, maître, ID de pile, liaison/débit par port			
Flash	256 Mo			
Processeur	ARM 800 MHz (double cœur)			
Mémoire CPU	512 Mo			
Mémoire tampon de paquets	Tous les numéros sont agrégés sur tous les ports car les mémoires tampons sont partagées dynamiquement :			
	Nom du modèle		Mémoire tampon de paquets	
	SG350XG-24T		16 Mbit	
	SG350XG-24F		16 Mbit	
	SG350XG-48T		32 Mbit	
	SG350XG-2F10		8 Mbit	
Modules SFP/SFP+ pris en charge	Référence	Médias	Débit	Distance maximale
	MGBBX1	Câblage par fibre optique mode unique	1 000 Mbit/s	10 km
	MGBSX1	Fibre multimode	1 000 Mbit/s	500 m
	MGBLH1	Câblage par fibre optique mode unique	1 000 Mbit/s	40 km
	MGBLX1	Câblage par fibre optique mode unique	1 000 Mbit/s	10 km
	MGBT1	UTP cat. 5e	1 000 Mbit/s	100 m
	SFP-H10GB-CU1M	Cuivre coaxial	10G	1 m
	SFP-H10GB-CU3M	Cuivre coaxial	10G	3 m
	SFP-H10GB-CU5M	Cuivre coaxial	10G	5 m
	SFP-10G-SR	Fibre multimode	10 Gig	26 m - 400 m
	SFP-10G-LR	Câblage par fibre optique mode unique	10 Gig	10 km
Spécifications environnementales				
Dimensions du produit (l x h x p)	Nom du modèle		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	
Poids de l'unité	Nom du modèle		Poids de l'unité	
	SG350XG-24T		5,57 kg	
	SG350XG-24F		4,16 kg	
	SG350XG-48T		7,43 kg	
	SG350XG-2F10		4,03 kg	
Alimentation	100–240 V 47-63 Hz, interne, universelle			
Certification	UL (UL 60950), CSA (CSA 22.2), marque CE, FCC Partie 15 (CFR 47) Classe A			

Fonction	Description																				
Température de fonctionnement	SG350XG-24T, SG350XG-24F, SG350XG-48T, SG350XG-2F10 0 à 50 °C (32 à 122 °F)																				
Température de stockage	De -20 °C à 70 °C (de -4 °F à 158 °F)																				
Taux d'humidité de fonctionnement	Humidité relative (sans condensation) de 10 % à 90 %																				
Taux d'humidité de stockage	Humidité relative (sans condensation) de 10 % à 90 %																				
Bruit acoustique et intervalle moyen entre les défaillances (MTBF, Mean Time Between Failures)	<table border="1"> <thead> <tr> <th>Nom du modèle</th> <th>Ventilateur (nombre)</th> <th>Bruit acoustique</th> <th>MTBF à 40 °C (heures)</th> </tr> </thead> <tbody> <tr> <td>SG350XG-24T</td> <td>4</td> <td>0 °C-30 °C : 40,7 dB 50 °C : 51,7 dB</td> <td>229,393</td> </tr> <tr> <td>SG350XG-24F</td> <td>4</td> <td>0 °C-25 °C : 36,4 dB</td> <td>121,050</td> </tr> <tr> <td>SG350XG-48T</td> <td>4</td> <td>0 °C-30 °C : 47,7 dB 50 °C : 58,9 dB</td> <td>131,767</td> </tr> <tr> <td>SG350XG-2F10</td> <td>3</td> <td>0 °C-30 °C : 38,9 dB 50 °C : 49,7 dB</td> <td>291,863</td> </tr> </tbody> </table>	Nom du modèle	Ventilateur (nombre)	Bruit acoustique	MTBF à 40 °C (heures)	SG350XG-24T	4	0 °C-30 °C : 40,7 dB 50 °C : 51,7 dB	229,393	SG350XG-24F	4	0 °C-25 °C : 36,4 dB	121,050	SG350XG-48T	4	0 °C-30 °C : 47,7 dB 50 °C : 58,9 dB	131,767	SG350XG-2F10	3	0 °C-30 °C : 38,9 dB 50 °C : 49,7 dB	291,863
	Nom du modèle	Ventilateur (nombre)	Bruit acoustique	MTBF à 40 °C (heures)																	
	SG350XG-24T	4	0 °C-30 °C : 40,7 dB 50 °C : 51,7 dB	229,393																	
	SG350XG-24F	4	0 °C-25 °C : 36,4 dB	121,050																	
	SG350XG-48T	4	0 °C-30 °C : 47,7 dB 50 °C : 58,9 dB	131,767																	
SG350XG-2F10	3	0 °C-30 °C : 38,9 dB 50 °C : 49,7 dB	291,863																		
Garantie	Garantie limitée à vie avec remplacement anticipé le jour ouvrable suivant (sous réserve de disponibilité, sinon expédition le jour même)																				
Contenu du coffret																					
<ul style="list-style-type: none"> Commutateur administrable et empilable Cisco Small Business 350X Câble d'alimentation Kit de montage fourni avec tous les modèles Câble série Guide de démarrage rapide 																					
Configuration minimale requise																					
<ul style="list-style-type: none"> Navigateur Web : Mozilla Firefox version 8 ou supérieure, Microsoft Internet Explorer version 7 ou supérieure, Safari, Chrome Câble réseau Ethernet de catégorie 6a pour des vitesses de 10 Gigabit jusqu'à 100 m TCP/IP, carte réseau et système d'exploitation réseau (par ex. Microsoft Windows, Linux ou Mac OS X) installés 																					

Pour commander

Le tableau 2 fournit des informations relatives aux commandes.

Tableau 2. Pour commander

Nom du modèle	Référence de commande du produit	Description
10 Gigabit		
SG350XG-24T	SG350XG-24T-K9	<ul style="list-style-type: none"> 24* Port cuivre 10 Gigabit Ethernet 10GBASE-T 2* 10 Gigabit Ethernet SFP+ (combiné avec 2 ports cuivre) 1 port de gestion Gigabit Ethernet
SG350XG-24F	SG350XG-24F-K9	<ul style="list-style-type: none"> 24* 10 Gigabit Ethernet SFP+ 2* Port cuivre 10 Gigabit Ethernet 10GBASE-T (combiné avec 2 SFP+) 1 port de gestion Gigabit Ethernet
SG350XG-48T	SG350XG-48T-K9	<ul style="list-style-type: none"> 48* Port cuivre 10 Gigabit Ethernet 10GBASE-T 2* 10 Gigabit Ethernet SFP+ (combiné avec 2 ports cuivre) 1 port de gestion Gigabit Ethernet
SG350XG-2F10	SG350XG-2F10-K9	<ul style="list-style-type: none"> 12* Port cuivre 10 Gigabit Ethernet 10GBASE-T 2* 10 Gigabit Ethernet SFP+ 1 port de gestion Gigabit Ethernet

* Chaque port combiné comprend un port Ethernet cuivre 10/100/1 000/10 000 et un connecteur Gigabit Ethernet SFP+, un seul port étant actif à la fois.

Un réseau fédérateur technologiquement avancé pour des entreprises en pleine croissance

La croissance est toujours une bonne chose. Toutefois, plus vous attirez de clients et gagnez en renommée, plus votre entreprise a besoin d'une plate-forme technologique capable de fournir un niveau de service et de fiabilité de pointe. Plus vous ajoutez des utilisateurs, des périphériques et des applications, plus votre sécurité est compromise, et vous ne pouvez tout simplement plus vous contenter d'une plate-forme de commutation conçue pour un fonctionnement plus réduit. Il est temps de vous doter d'un réseau capable de prendre en charge les besoins croissants de votre entreprise et d'évoluer avec elle. Les commutateurs Cisco 350X offrent le jeu de fonctionnalités avancées, la fiabilité et la protection des investissements dont votre entreprise a besoin, aujourd'hui et demain.

Cisco Capital

Un financement pour vous aider à atteindre vos objectifs

Cisco Capital peut vous aider à acquérir la technologie dont vous avez besoin pour atteindre vos objectifs et rester compétitif. Vous pouvez réduire vos CapEx, accélérer votre croissance, et optimiser vos investissements et votre ROI. Les financements octroyés par Cisco Capital vous permettent d'acheter en toute flexibilité du matériel, des logiciels, des services et des équipements tiers complémentaires. Et vous n'avez qu'un seul remboursement à prévoir. Cisco Capital est disponible dans plus de 100 pays. [En savoir plus.](#)

Pour en savoir plus

Pour en savoir plus sur les commutateurs Cisco 350X, rendez-vous sur : www.cisco.com/go/350Xswitches.

Pour en savoir plus sur les autres produits et solutions Cisco Small Business, rendez-vous sur : www.cisco.com/go/smallbusiness



Siège social aux États-Unis
Cisco Systems, Inc.
San José, CA

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site web de Cisco, à l'adresse : www.cisco.com/go/offices.

Cisco et le logo Cisco sont des marques commerciales ou des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques commerciales Cisco, visitez le site : www.cisco.com/go/trademarks. Les autres marques mentionnées dans les présentes sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat commercial entre Cisco et d'autres entreprises. (1110R)