Glossaire des termes relatifs aux commutateurs

Objectif

Cet article contient la liste des termes utilisés dans la configuration et le dépannage des commutateurs Cisco Small Business.

Périphériques pertinents

- Série Sx200
- Gamme Sx250
- Gamme Sx300
- Gamme Sx350
- Série SG300X
- Gamme Sx500
- Gamme Sx550X

Liste des termes

- 802.1X Supplicant : le demandeur est l'un des trois rôles de la norme IEEE 802.1X. La norme 802.1X a été développée pour assurer la sécurité de la couche 2 du modèle OSI. Il se compose des éléments suivants : Demandeur, authentificateur et serveur d'authentification. Un demandeur est le client ou le logiciel qui se connecte à un réseau afin de pouvoir accéder aux ressources de ce réseau. Il doit fournir des informations d’identification ou des certificats pour obtenir une adresse IP et faire partie de ce réseau particulier. Un demandeur ne peut pas accéder aux ressources du réseau tant qu'il n'a pas été authentifié.
- ACL : une liste de contrôle d'accès (ACL) est une liste de filtres de trafic réseau et d'actions corrélées utilisées pour améliorer la sécurité. Elle bloque ou permet aux utilisateurs d'accéder à des ressources spécifiques. Une liste de contrôle d’accès contient les hôtes auxquels l’accès au périphérique réseau est autorisé ou refusé. Le routeur ou le commutateur examine chaque paquet pour déterminer s’il doit le transférer ou l’abandonner, sur la base des critères spécifiés dans les listes d’accès. Les critères de la liste d’accès peuvent être l’adresse source du trafic, l’adresse de destination du trafic, le protocole de couche supérieure ou d’autres informations.

- IGMP Snooping : le protocole IGMP (Internet Group Management Protocol) est un protocole qui fonctionne sur des commutateurs et qui leur permet d'en apprendre dynamiquement sur le trafic de multidiffusion. La surveillance IGMP est une fonctionnalité qui permet à un commutateur réseau d'écouter la conversation IGMP entre les hôtes et les routeurs. La surveillance IGMP exécute un mécanisme de filtrage qui est activé dans le routeur pour transférer le trafic de multidiffusion d'un groupe uniquement aux ports qui ont rejoint le groupe. Ainsi, avec la surveillance IGMP, le trafic sur le réseau est réduit et l'amélioration des performances des hôtes derrière le routeur est possible. Les multidiffusions peuvent être filtrées à partir des liens qui n'en ont pas besoin.

- IPv4 : IPv4 est un système d'adressage 32 bits utilisé pour identifier un périphérique dans un réseau. Il s'agit du système d'adressage utilisé dans la plupart des réseaux informatiques, y compris Internet.

- IPv6 : IPv6 est un système d'adressage 128 bits utilisé pour identifier un périphérique dans un réseau. Il s'agit du successeur d'IPv4 et de la version la plus récente du système d'adressage utilisé dans les réseaux informatiques. IPv6 est actuellement déployé dans le monde entier. Une adresse IPv6 est représentée par huit champs de nombres hexadécimaux, chaque champ contenant 16 bits. Une adresse IPv6 est divisée en deux parties, chacune composée de 64 bits. La première partie correspond à l'adresse réseau et la seconde à l'adresse hôte.

- Link Flap : le « Link Flap » est une situation dans laquelle une interface physique du commutateur s'active et s'arrête en permanence, trois fois ou plus par seconde pendant au moins 10 secondes. La cause la plus fréquente est généralement liée à un câble défectueux, non pris en charge ou non standard, à un câble SFP (Small Form-Factor Pluggable) ou à d'autres problèmes de synchronisation de liaison. La cause du battement de la liaison peut être intermittente ou permanente.

- ACL basée sur MAC : la liste de contrôle d'accès basée sur MAC (Media Access Control) est une liste d'adresses MAC source. Si un paquet provient d'un point d'accès sans fil vers un port de réseau local (LAN) ou vice versa, ce périphérique vérifie si l'adresse MAC source du paquet correspond à une entrée de cette liste et compare les règles de liste de contrôle d'accès au contenu de la trame. Il utilise ensuite les résultats correspondants pour autoriser ou refuser ce paquet. Cependant, les paquets du LAN au port LAN ne seront pas vérifiés.

- Surveillance MLD : la multidiffusion est la technique de couche réseau qui transmet des paquets de données d'un hôte aux hôtes sélectionnés dans un groupe. Au niveau de la couche inférieure, le commutateur diffuse le trafic de multidiffusion sur tous les ports, même si un seul hôte souhaite le recevoir. La surveillance MLD (Multicast Listener Discovery) est utilisée pour transférer le trafic de multidiffusion IPv6 uniquement aux hôtes souhaités. Lorsque la surveillance MLD est activée sur le commutateur, il détecte les messages MLD échangés entre le routeur IPv6 et les hôtes de multidiffusion connectés à l'interface. Il gère ensuite une table qui restreint le trafic de multidiffusion IPv6 et le transfère dynamiquement aux ports qui souhaitent le recevoir.

- MSTP - Multiple Spanning Tree Protocol (MSTP) est un protocole qui crée plusieurs

Spanning Tree (instances) pour chaque réseau local virtuel (VLAN) sur un réseau physique unique. Cela permet à chaque VLAN d'avoir un pont racine configuré et une topologie de transfert. Cela réduit le nombre d'unités BPDU (Bridge Protocol Data Unit) sur le réseau et réduit la contrainte sur les unités centrales (CPU) des périphériques réseau.

- Mise en miroir des ports/VLAN : la mise en miroir est une méthode utilisée pour surveiller le trafic réseau. Avec la mise en miroir des ports ou des VLAN, les copies des paquets entrants et sortants au niveau des ports (ports source) d'un périphérique réseau sont transférées vers un autre port (port cible) où les paquets sont étudiés. Il est utilisé comme outil de diagnostic par l'administrateur réseau.

- Sécurité des ports : la configuration de la sécurité des ports est un moyen d'améliorer la sécurité du réseau. Il peut être configuré sur un port spécifique ou un groupe d'agrégation de liaisons (LAG). Un LAG combine des interfaces individuelles en une seule liaison logique, ce qui fournit une bande passante totale pouvant atteindre huit liaisons physiques. Vous pouvez limiter ou autoriser l'accès à différents utilisateurs sur un port/LAG donné. La sécurité des ports peut également être utilisée avec des adresses MAC statiques et apprises dynamiquement pour limiter le trafic entrant d'un port.

- VLAN basé sur le protocole : les groupes basés sur le protocole peuvent être définis et liés à un port ; par conséquent, chaque paquet provenant des groupes de protocoles est attribué au VLAN configuré sur la page. Le VLAN basé sur un protocole divise le réseau physique en groupes VLAN logiques pour chaque protocole requis. Dans le paquet entrant, la trame est vérifiée et l'appartenance au VLAN peut être déterminée en fonction du type de protocole. Le mappage des groupes basés sur des protocoles sur le VLAN permet de mapper un groupe de protocoles sur un seul port.

- QoS : la qualité de service (QoS) vous permet de hiérarchiser le trafic pour différentes applications, utilisateurs ou flux de données. Il peut également être utilisé pour garantir des performances à un niveau spécifié, affectant ainsi la qualité de service du client. La qualité de service est généralement affectée par les facteurs suivants : gigue, latence et perte de paquets.

- RADIUS Server : le service RADIUS (Remote Authentication Dial-In User Service) est un mécanisme d'authentification permettant aux périphériques de se connecter et d'utiliser un service réseau. Il est utilisé à des fins d'authentification, d'autorisation et de comptabilité centralisées. Un serveur RADIUS régule l'accès au réseau en vérifiant l'identité des utilisateurs à l'aide des informations d'identification saisies. Par exemple, un réseau Wi-Fi public est installé dans un campus universitaire. Seuls les étudiants disposant du mot de passe peuvent accéder à ces réseaux. Le serveur RADIUS vérifie les mots de passe entrés par les utilisateurs et accorde ou refuse l'accès selon le cas.

- RSTP : le protocole RSTP (Rapid Spanning Tree Protocol) est une amélioration du protocole STP. Le protocole RSTP assure une convergence Spanning Tree plus rapide après une modification de topologie. Le protocole STP peut prendre de 30 à 50 secondes pour répondre à une modification de topologie, tandis que le protocole RSTP répond dans les trois fois la durée Hello configurée. RSTP est rétrocompatible avec STP.

- SNMP : le protocole SNMP (Simple Network Management Protocol) est une norme réseau permettant de stocker et de partager des informations sur les périphériques réseau. SNMP facilite la gestion, le dépannage et la maintenance du réseau.

- Spanning Tree : le protocole STP (Spanning Tree Protocol) est un protocole réseau utilisé sur un réseau local (LAN). L'objectif du protocole STP est de garantir une topologie sans boucle pour un réseau local. Le protocole STP supprime les boucles via un algorithme qui garantit qu'il n'existe qu'un seul chemin actif entre deux périphériques réseau. Le protocole STP garantit que le trafic emprunte le chemin le plus court possible au sein du réseau. Le protocole STP peut également réactiver automatiquement les chemins redondants en tant que chemins de secours en cas de défaillance d'un chemin actif.

- SSL Server : le protocole SSL (Secure Sockets Layer) est principalement utilisé pour la gestion de la sécurité sur Internet. Il utilise une couche programme située entre les couches HTTP et TCP. Pour l'authentification, SSL utilise des certificats qui sont signés numériquement et liés à la clé publique pour identifier le propriétaire de la clé privée. Cette authentification est utile lors de la connexion. Grâce à l'utilisation de SSL, les certificats sont échangés par blocs au cours du processus d'authentification qui sont au format décrit dans la norme ITU-T X.509. Ensuite, par l'autorité de certification qui est une autorité externe, des certificats X.509 sont émis qui sont signés numériquement.

- Agrégation Syslog : un service Syslog accepte simplement les messages et les stocke dans des fichiers ou les imprime en fonction d'un fichier de configuration simple. L'agrégation Syslog signifie que plusieurs messages Syslog du même type n'apparaîtront pas à l'écran chaque fois qu'une instance se produit. L'activation de l'agrégation de la journalisation vous permet de filtrer les messages système que vous recevrez pendant une période spécifique. Il collecte quelques messages syslog du même type afin qu'ils n'apparaissent pas lorsqu'ils se produisent, mais qu'ils apparaissent plutôt à un intervalle spécifié.

- TACACS+ — Terminal Access Controller Access Control System (TACACS+) est un protocole propriétaire de Cisco utilisé pour la mise en oeuvre d'une sécurité renforcée en fournissant une authentification et une autorisation via un nom d'utilisateur et un mot de passe. Pour configurer un serveur TACACS+, l'utilisateur doit disposer du privilège d'accès 15, qui lui permet d'accéder à toutes les fonctions de configuration du commutateur. Certains commutateurs peuvent faire office de client TACACS+, où tous les utilisateurs connectés peuvent être authentifiés et autorisés sur le réseau via un serveur TACACS+ correctement configuré. TACACS+ prend uniquement en charge IPv4.

- Serveur TFTP - Un serveur TFTP (Trivial File Transfer Protocol) est un serveur utilisé pour transférer automatiquement des fichiers de configuration et de démarrage entre des périphériques sur un réseau local. Le protocole est simple, ce qui permet une faible utilisation de la mémoire ; cependant, cette simplicité permet également de compromettre facilement le protocole. Pour cette raison, le protocole TFTP est rarement utilisé avec Internet.

- VLAN : un réseau local virtuel (VLAN) est un réseau commuté qui est segmenté logiquement par fonction, zone ou application, sans tenir compte des emplacements physiques des

utilisateurs. Les VLAN sont un groupe d’hôtes ou de ports qui peuvent être situés n’importe où sur un réseau, mais qui communiquent comme s’ils se trouvaient sur le même segment physique. Les VLAN simplifient la gestion du réseau en vous permettant de déplacer un périphérique vers un nouveau VLAN sans modifier les connexions physiques.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.