Configurer la liste de contrôle d'accès MAC (ACL) et l'entrée de contrôle d'accès (ACE) sur un commutateur géré

Objectif

Une liste de contrôle d’accès (ACL) est une liste de filtres de trafic réseau et d’actions corrélées utilisées pour améliorer la sécurité. Il 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. La liste de contrôle d'accès (ACL) basée sur MAC (Media Access Control List) est une liste d'adresses MAC source qui utilisent les informations de couche 2 pour autoriser ou refuser l'accès au trafic. Si un paquet provient d’un point d’accès sans fil vers un port LAN (Local Area Network) ou vice versa, ce périphérique vérifie si l’adresse MAC source du paquet correspond à une entrée de cette liste et vérifie les règles de la liste de contrôle d’accès par rapport 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. Une entrée de contrôle d'accès (ACE) contient les critères de règle d'accès réels. Une fois l'ACE créée, elle est appliquée à une liste de contrôle d'accès. Vous devez utiliser des listes d'accès pour fournir un niveau de sécurité de base pour accéder à votre réseau. Si vous ne configurez pas de listes d'accès sur vos périphériques réseau, tous les paquets passant par le commutateur ou le routeur peuvent être autorisés sur toutes les parties de votre réseau.

Cet article fournit des instructions sur la configuration de la liste de contrôle d'accès et de l'ACE basées sur MAC sur votre commutateur géré.

Périphériques pertinents | Version du logiciel

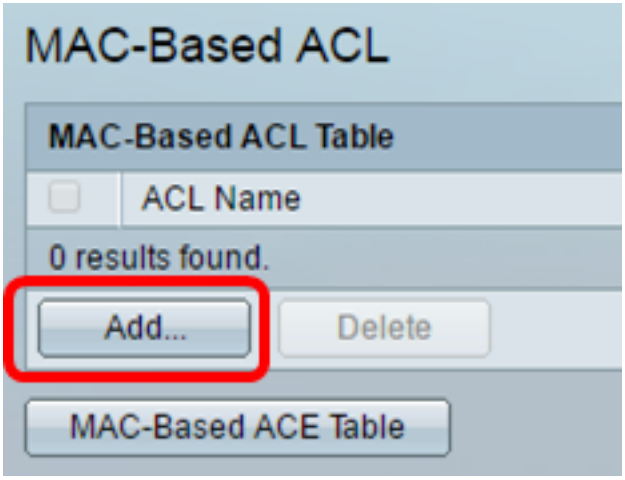
- Gamme Sx350 | 2.2.0.66 (Télécharger la dernière version)
- Gamme SG350X | 2.2.0.66 (Télécharger la dernière version)
- Série Sx500 | 1.4.5.02 (Télécharger la dernière version)
- Gamme Sx550X | 2.2.0.66 (Télécharger la dernière version)

Configurer ACL et ACE basées sur MAC

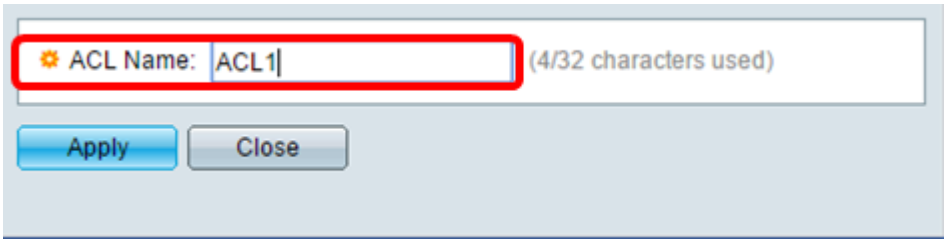
Configurer une liste de contrôle d’accès basée sur MAC

Étape 1. Connectez-vous à l'utilitaire Web, puis accédez à **Access Control > MAC-Based ACL**.

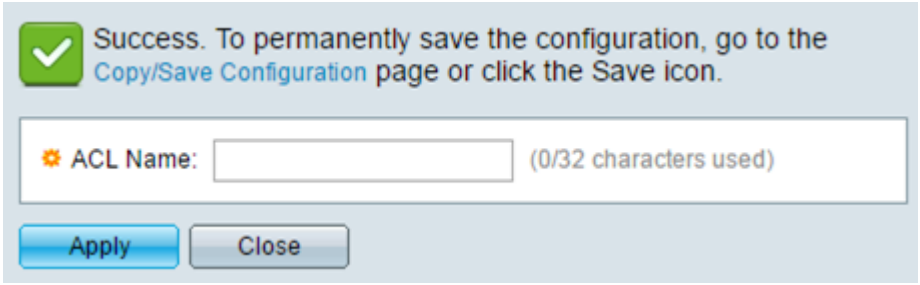
Étape 2. Cliquez sur le bouton **Add.**



Étape 3. Saisissez le nom de la nouvelle liste de contrôle d'accès dans le champ ACL Name.



Étape 4. Cliquez sur **Appliquer** puis sur **Fermer**.



Étape 5. (Facultatif) Cliquez sur **Enregistrer** pour enregistrer les paramètres dans le fichier de configuration initiale.

Vous devez maintenant avoir configuré une liste de contrôle d'accès basée sur MAC sur votre commutateur.

Configurer ACE basé sur MAC

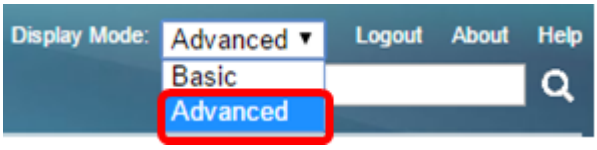
Lorsqu'une trame est reçue sur un port, le commutateur traite la trame via la première liste de contrôle d'accès. Si la trame correspond à un filtre ACE de la première liste de contrôle d'accès, l'action ACE a lieu. Si la trame ne correspond à aucun des filtres ACE, la liste de contrôle d'accès suivante est traitée. Si aucune correspondance n'est trouvée avec une entrée ACE dans toutes les listes de contrôle d'accès pertinentes, la trame est abandonnée par défaut.

Dans ce scénario, une ACE sera créée pour refuser le trafic envoyé à partir d'une adresse MAC source définie par l'utilisateur spécifique vers n'importe quelle adresse de destination.

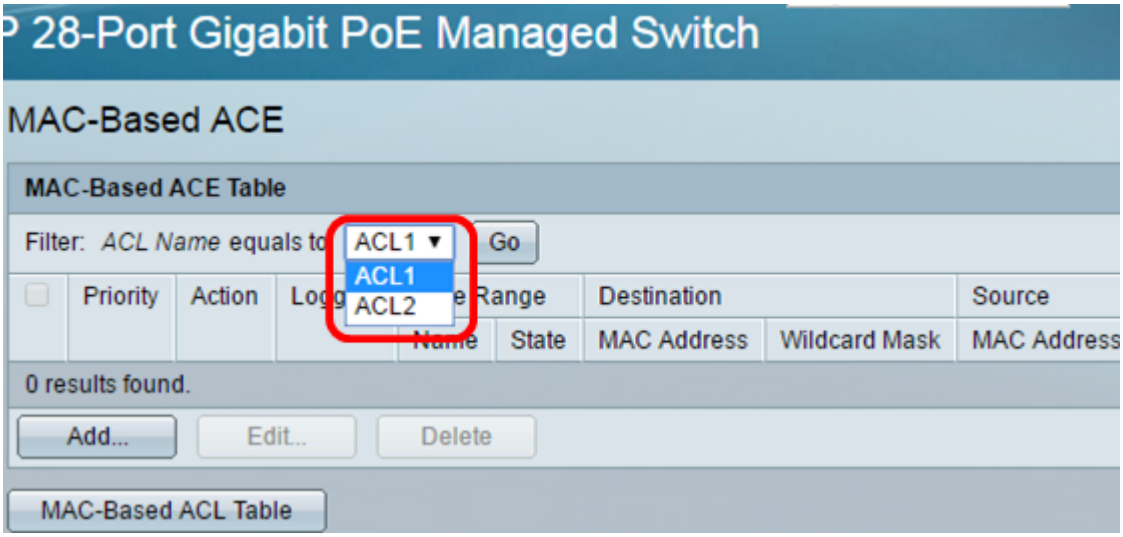
Note: Cette action par défaut peut être évitée par la création d'une ACE de faible priorité qui autorise tout le trafic.

Étape 1. Dans l'utilitaire Web, accédez à **Access Control > MAC-Based ACE**.

Important : Pour utiliser pleinement les fonctions et fonctions disponibles du commutateur, passez en mode Avancé en sélectionnant **Avancé** dans la liste déroulante Mode Affichage dans le coin supérieur droit de la page.



Étape 2. Choisissez une liste de contrôle d'accès dans la liste déroulante Nom de la liste de contrôle d'accès, puis cliquez sur **Go**.

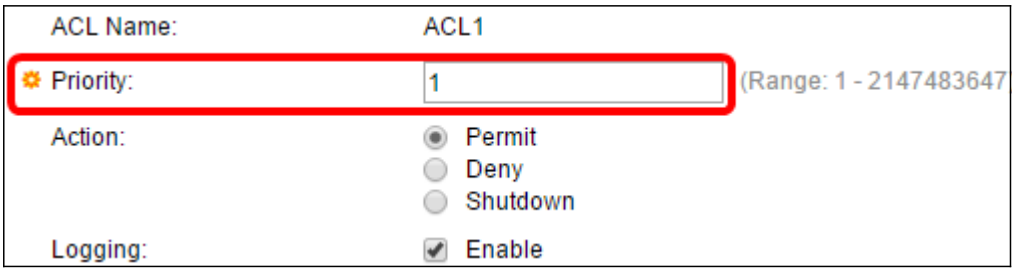


Note: Les ACE déjà configurés pour la liste de contrôle d'accès s'affichent dans le tableau.

Étape 3. Cliquez sur le bouton **Ajouter** pour ajouter une nouvelle règle à la liste de contrôle d'accès.

Note: Le champ *Nom de la liste de contrôle d'accès* affiche le nom de la liste de contrôle d'accès.

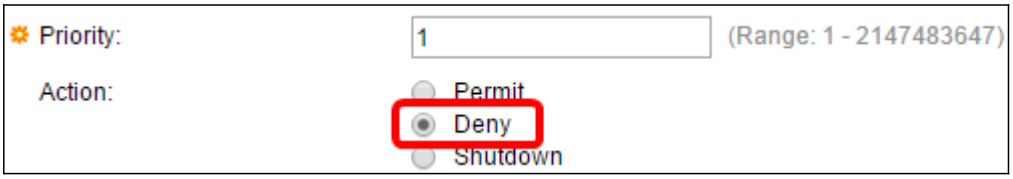
Étape 4. Entrez la valeur de priorité de l'ACE dans le champ *Priorité*. Les ACE ayant une valeur de priorité supérieure sont traités en premier. La valeur 1 est la priorité la plus élevée.



Étape 5. (Facultatif) Cochez la case Activer la journalisation pour activer la journalisation des flux ACL qui correspondent à la règle ACL.

Étape 6. Sélectionnez la case d'option correspondant à l'action souhaitée qui est effectuée lorsqu'une trame répond aux critères requis de l'ACE.

Note: Dans cet exemple, Deny est sélectionné.



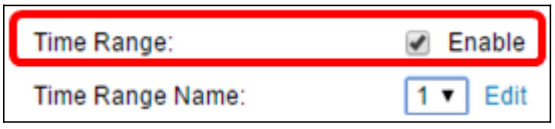
Permit : le commutateur transfère les paquets qui répondent aux critères requis de l'ACE.

Deny : le commutateur abandonne les paquets qui répondent aux critères requis de l'ACE.

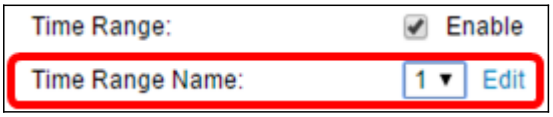
Arrêt : le commutateur abandonne les paquets qui ne répondent pas aux critères requis de l'ACE et désactive le port où les paquets ont été reçus.

Note: Les ports désactivés peuvent être réactivés sur la page Port Settings.

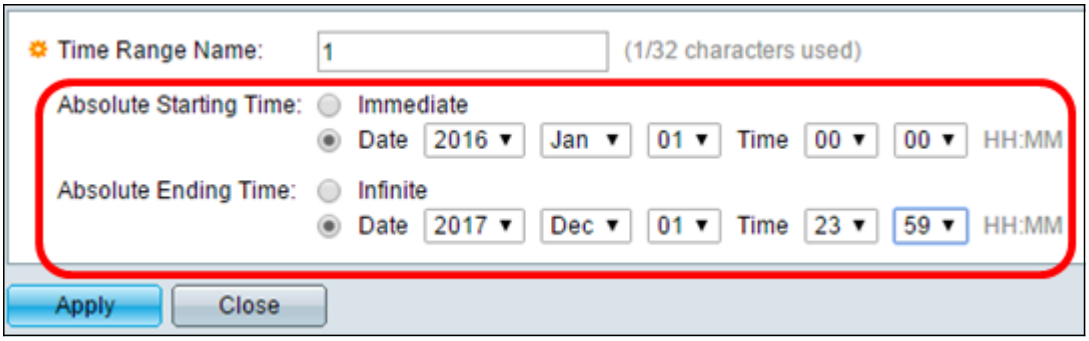
Étape 7. (Facultatif) Cochez la case **Activer** la plage de temps pour autoriser la configuration d'une plage de temps à l'ACE. Les plages de temps sont utilisées pour limiter la durée de validité d'une ACE.



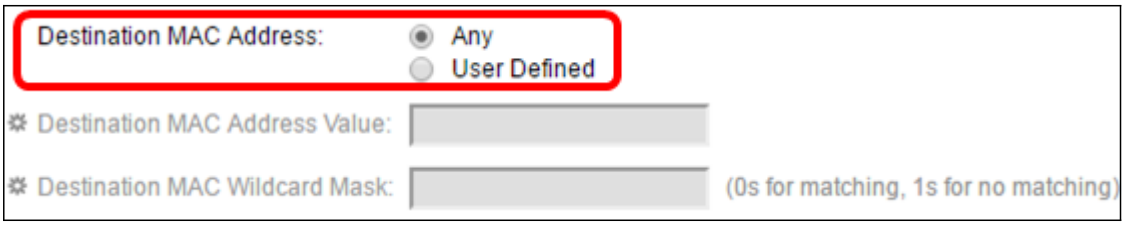
Étape 8. (Facultatif) Dans la liste déroulante Nom de la plage de temps, sélectionnez une plage de temps à appliquer à l'ACE.



Note: Vous pouvez cliquer sur **Modifier** pour accéder à la page Plage de temps et en créer une.



Étape 9. Cliquez sur la case d'option qui correspond aux critères souhaités de l'ACE dans la zone Adresse MAC de destination.



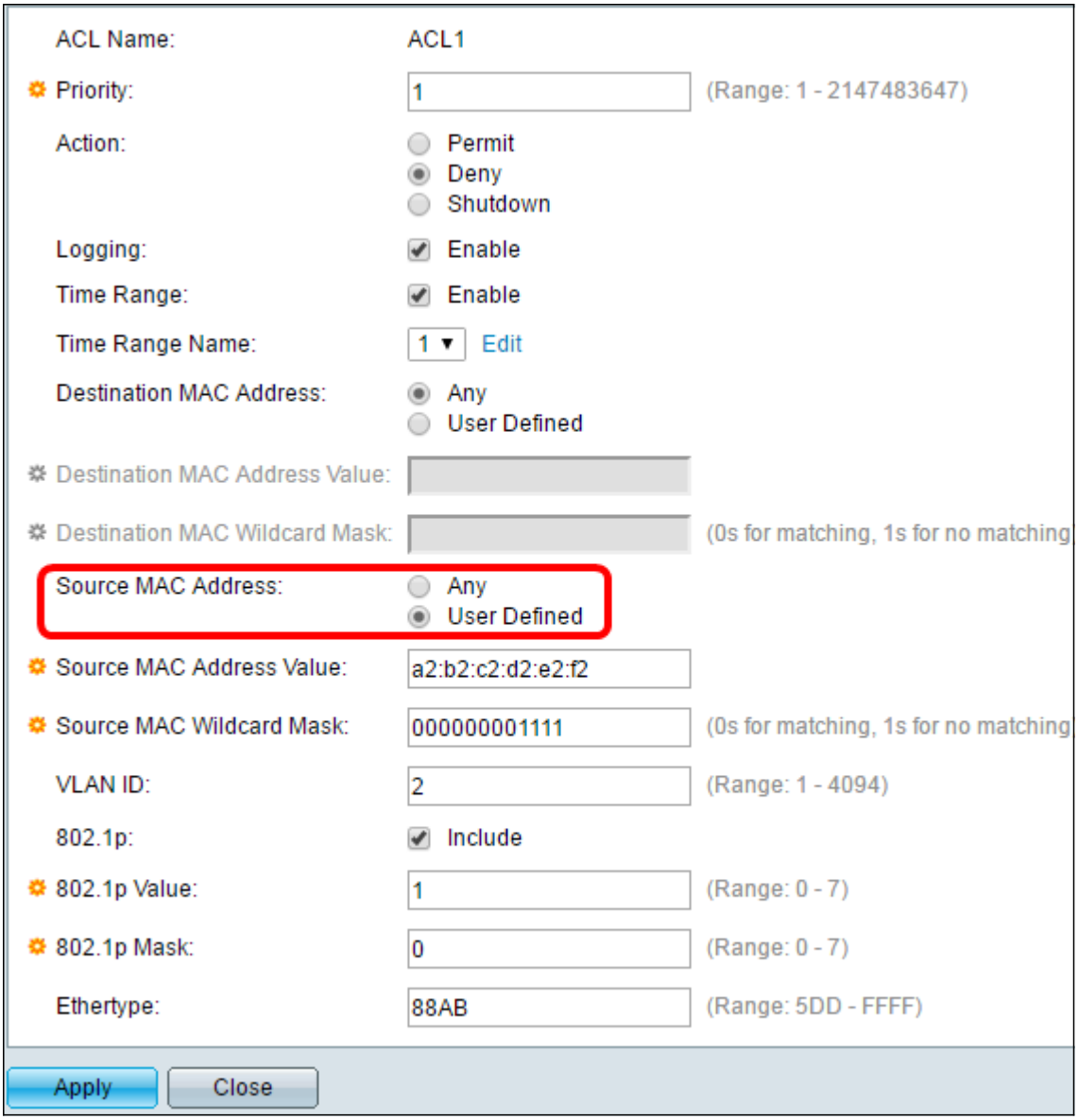
Les options sont les suivantes :

Any : toutes les adresses MAC de destination s'appliquent à l'ACE.

User Defined : saisissez une adresse MAC et un masque générique MAC qui doivent être appliqués à l'ACE dans les champs *Destination MAC Address Value* et *Destination MAC Wildcard Mask*. Les masques génériques sont utilisés pour définir une plage d'adresses MAC.

Note: Dans cet exemple, Any est sélectionné. Si vous choisissez cette option, l'ACE à créer refusera le trafic ACE.

Étape 10. Cliquez sur la case d'option qui correspond aux critères souhaités de l'ACE dans la zone Adresse MAC source.



Les options sont les suivantes :

Any : toutes les adresses MAC source s'appliquent à l'ACE.

User Defined : saisissez une adresse MAC et un masque générique MAC qui doivent être appliqués à l'ACE dans les champs *Source MAC Address Value* et *Source MAC Wildcard Mask*. Les masques génériques sont utilisés pour définir une plage d'adresses MAC.

Note: Dans cet exemple, User Defined est sélectionné.

Étape 11. (Facultatif) Dans le champ *ID de VLAN*, saisissez un ID de VLAN correspondant à l'étiquette VLAN de la trame.

Étape 12. (Facultatif) Pour inclure les valeurs 802.1p dans les critères ACE, cochez la case **Inclure** dans la case 802.1p. La norme 802.1p implique la classe de service (CoS) de la technologie. La CoS est un champ de 3 bits dans une trame Ethernet utilisée pour différencier le trafic.

Étape 13. Si les valeurs 802.1p sont incluses, saisissez les champs suivants :

802.1p Value : saisissez la valeur 802.1p qui doit être mise en correspondance. La norme 802.1p permet aux commutateurs de couche 2 de hiérarchiser le trafic et d'effectuer un filtrage multicast dynamique. Les valeurs sont les suivantes :

- 0 — Contexte. Les données les moins prioritaires, comme les transferts en masse, les jeux, etc.

- 1 — Le Meilleur Effort. Les données qui nécessitent une livraison au mieux sur une priorité LAN ordinaire. Le réseau ne fournit aucune garantie lors de la livraison, mais les données obtiennent un débit binaire et un temps de livraison non spécifiés en fonction du trafic.

- 2 — Excellent Effort. Les données qui nécessitent une livraison au mieux pour les utilisateurs importants.

- 3 — Application critique telle que Linux Virtual Server (LVS), protocole SIP (Session Initiation Protocol) téléphonique.

- 4 — Vidéo. Latence et instabilité inférieures à 100 ms.

- 5 — Téléphone IP Cisco vocal par défaut. Latence et instabilité inférieures à 10 ms.

- 6 — Téléphone LVS de contrôle interréseau RTP (Real-time Transport Protocol).

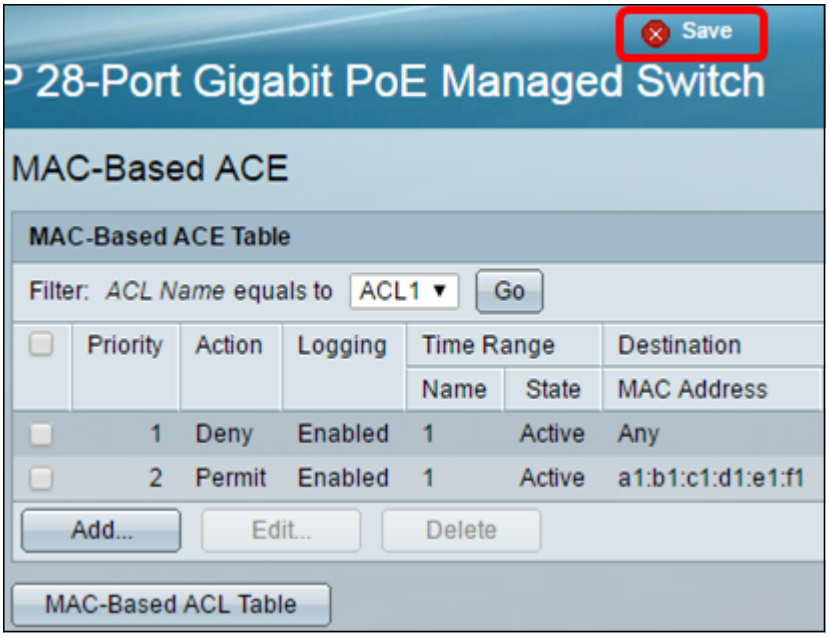
- 7 — Contrôle du réseau. Besoin élevé d'intervention pour la maintenance et la prise en charge de l'infrastructure réseau.

802.1p Mask : saisissez le masque générique des valeurs 802.1p. Ce masque générique est utilisé pour définir la plage de valeurs 802.1p.

Étape 14. (Facultatif) Entrez l'Ethernet de la trame à mettre en correspondance. Ethertype est un champ de 2 octets dans une trame Ethernet qui est utilisé pour indiquer quel protocole est utilisé pour la charge utile de la trame.

Étape 14. Cliquez sur **Appliquer**, puis sur **Fermer**. L'ACE est créée et associée au nom de la liste de contrôle d'accès.

Étape 15. Cliquez sur **Save** pour enregistrer les paramètres dans le fichier de configuration initiale.



Vous devez maintenant avoir configuré un ACE basé sur MAC sur votre commutateur.

Autres liens utiles :

- Page Produit Commutateurs de la gamme 350
- Page produit Commutateurs de la gamme 350X
- Page Produit Commutateurs de la gamme 550
- Page Produit Commutateurs de la gamme 550X

Afficher une vidéo relative à cet article...

Cliquez ici pour afficher d'autres présentations techniques de Cisco