Chapitre 5 : Sécurisation d'un commutateur

Routing and Switching Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™

Chapitre 5 – Sections et objectifs

Sécurité du commutateur : gestion et implémentation

- Configurer l'interface virtuelle de gestion sur un commutateur.
- Configurer la fonction de sécurité des ports pour restreindre l'accès au réseau.

Sécurité du commutateur : gestion et implémentation

Cisco | Networking Academy®
Mind Wide Open™

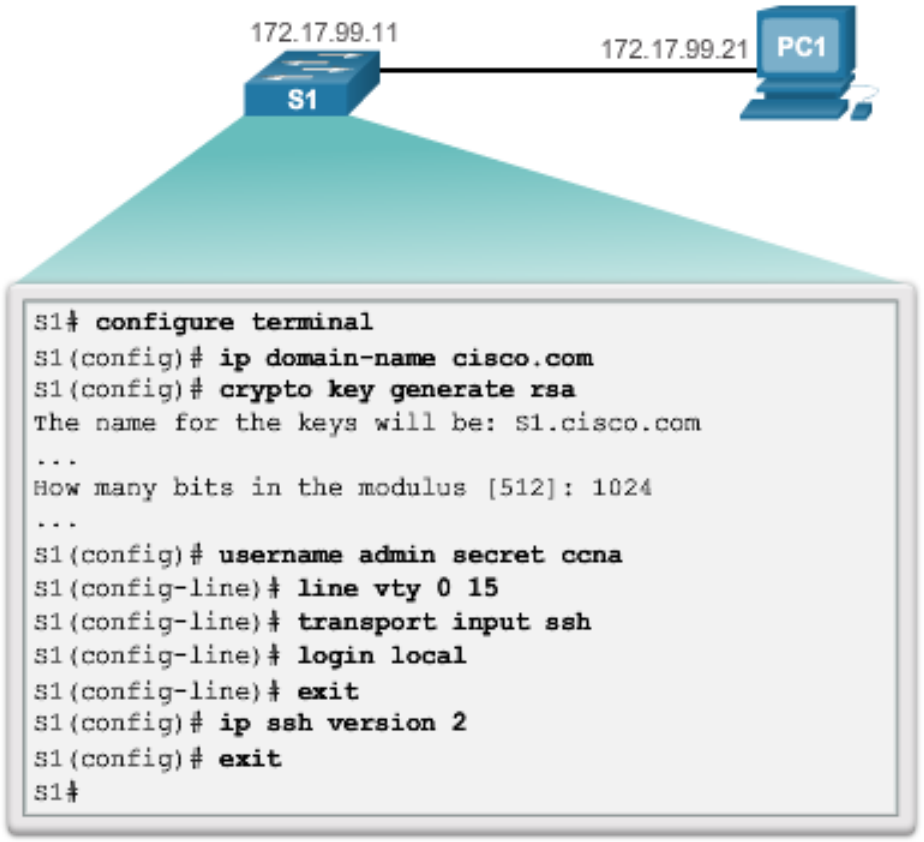
Le fonctionnement de SSH

- Secure Shell (SSH) est un protocole qui permet de se connecter de manière sécurisée (connexion chiffrée) à un appareil distant via une ligne de commande.
- En raison de la fiabilité de ses fonctions de chiffrement, SSH devrait remplacer Telnet pour les connexions de gestion.
- SSH utilise le port TCP 22 par défaut.
- Telnet utilise le port TCP 23.
- Il faut disposer d'une version du logiciel IOS comprenant des fonctions et des fonctionnalités chiffrées pour pouvoir utiliser SSH sur les commutateurs Catalyst 2960.

La configuration de SSH

1. **Vérifiez que SSH est pris en charge : show `ip ssh`.**
2. **Configurez le domaine IP.**
3. **Générez des paires de clés RSA.**
4. **Configurez l'authentification utilisateur.**
5. **Configurez les lignes vty.**
6. **Activez SSH version 2.**

Configuration de SSH pour la gestion à distance



La vérification de SSH

Accès à distance sécurisé

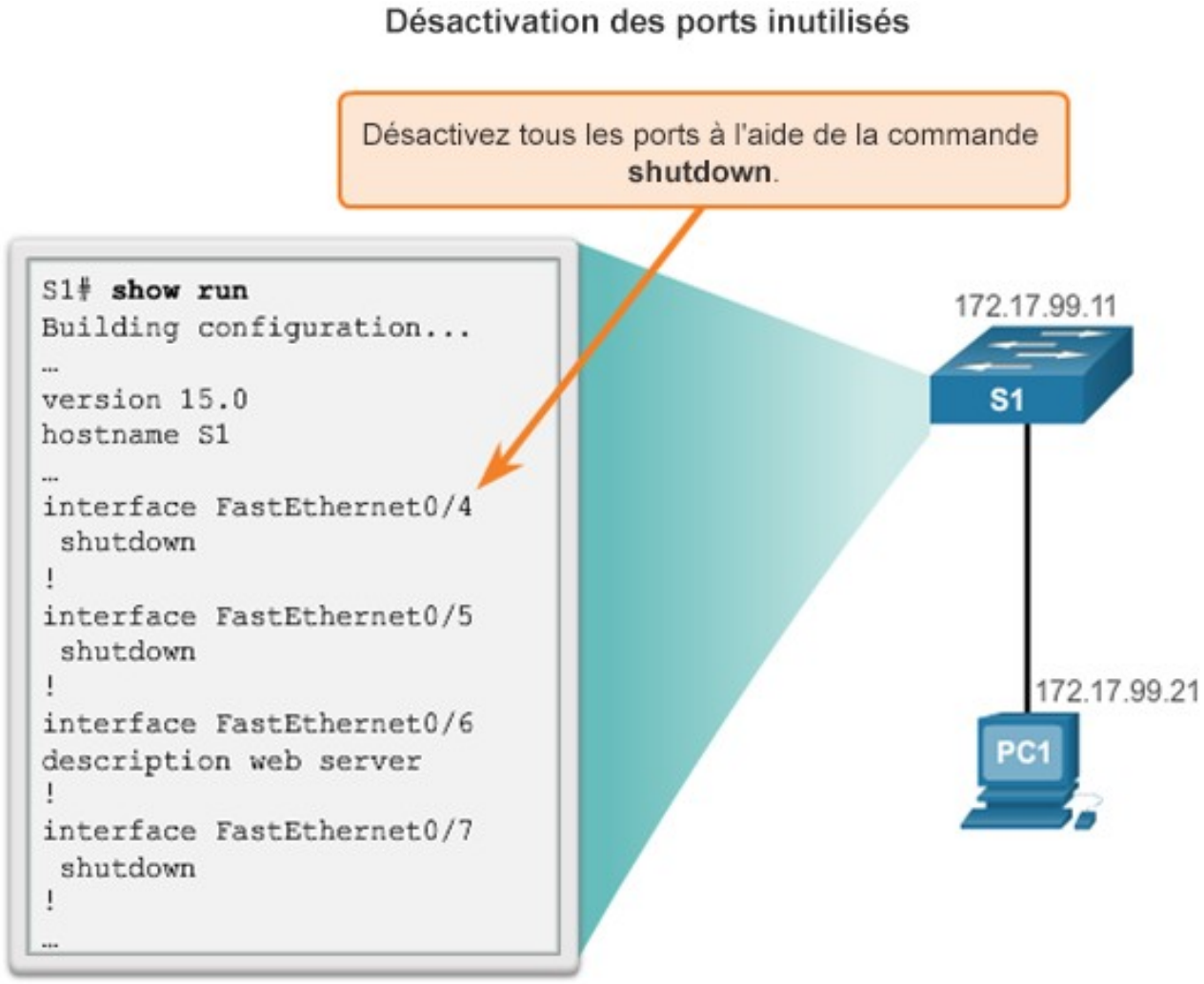
La vérification de SSH (suite)

Vérification de l'état et des paramètres de SSH


```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAa
P3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==

S1# show ssh
Connection Version Mode Encryption  Hmac       State         Username
0          2.0     IN   aes256-cbc  hmac-sha1 Session started admin
0          2.0     OUT  aes256-cbc  hmac-sha1 Session started admin
%No SSHv1 server connections running.
S1#
```

Sécuriser les ports inutilisés



La sécurité des ports : fonctionnement

- Les adresses MAC des périphériques légitimes sont ainsi autorisées. Toutes les autres adresses MAC sont refusées.
- Toute autre tentative de connexion avec des adresses MAC inconnues constitue une violation des règles de sécurité.
- Les adresses MAC fiables peuvent être configurées de différentes manières :
  - Adresses MAC statiques sécurisées : configurées et ajoutées manuellement à la configuration en cours : **`switchport port-security mac-address`** *`mac-address`*
  - Adresses MAC dynamiques sécurisées : supprimées au redémarrage du commutateur
  - Adresses MAC sécurisées rémanentes : ajoutées à la configuration en cours et apprises dynamiquement : commande du mode de configuration d'interface **`: switchport port-security mac-address sticky`**

La sécurité des ports : modes de violation

- L'IOS détecte une violation des règles de sécurité si :
  - Le nombre maximal d'adresses MAC sécurisées a été ajouté dans la table CAM et un appareil dont l'adresse MAC ne figure pas dans cette table tente d'accéder à l'interface.
- Trois actions peuvent être entreprises en cas de violation :
  - Protéger : aucune notification reçue
  - Limiter : notification relative à une violation de sécurité reçue
  - Arrêter
  - Commande du mode de configuration d'interface **`switchport port-security violation {`*`protect`*` | `*`restrict`*` | `*`shutdown`*`}`**

La sécurité des ports : modes de violation (suite)

Les modes de violation de sécurité incluent les modes Protect, Restrict et Shutdown.

Modes de violation de sécurité

Mode de violation	Acheminement du trafic	Envoi d'un message syslog	Affichage d'un message d'erreur	Incrémentation du compteur de violation	Arrêt du port
Protect	Non	Non	Non	Non	Non
Restrict	Non	Oui	Non	Oui	Non
Shutdown	Non	Non	Non	Oui	Oui

La sécurité des ports : configuration

Paramètres par défaut de la sécurité des ports

Fonctionnalité	Paramètre par défaut
Sécurité des ports	Désactivée sur un port
Nombre maximal d'adresses MAC sécurisées	1
Mode de violation	Shutdown. Le port est désactivé en cas de dépassement du nombre maximal d'adresses MAC sécurisées.
Apprentissage des adresses rémanentes	Désactivé

Configuration de la sécurité du port dynamique

Commandes de l'interface en ligne de commande de Cisco IOS	
Spécifiez l'interface à configurer pour la sécurité des ports.	`S1(config)# interface fastethernet 0/18`
Définissez le mode d'interface sur accès.	`S1(config-if)# switchport mode access`
Activez la sécurité des ports sur l'interface.	`S1(config-if)# switchport port-security`

Configuration la sécurité des ports rémanents

Commandes de l'interface en ligne de commande de Cisco IOS	
Spécifiez l'interface à configurer pour la sécurité des ports.	`S1(config)# interface fastethernet 0/19`
Définissez le mode d'interface sur accès.	`S1(config-if)# switchport mode access`
Activez la sécurité des ports sur l'interface.	`S1(config-if)# switchport port-security`
Définissez le nombre maximal d'adresses sécurisées autorisées sur le port.	`S1(config-if)# switchport port-security maximum 10`
Activez l'apprentissage rémanent.	`S1(config-if)# switchport port-security mac-address sticky`

La sécurité des ports : vérification

Vérification des adresses MAC : dynamiques

```
S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0025.83e6.4b01:1
Security Violation Count   : 0
```

Vérification des adresses MAC : rémanentes

```
S1# show port-security interface fastethernet 0/19
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 10
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0025.83e6.4b02:1
Security Violation Count   : 0
```

Sécurité des ports de commutateur

La sécurité des ports : vérification (suite)

Vérification des adresses MAC rémanentes : configuration en cours

```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 10
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

Vérification des adresses MAC sécurisées

```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------
Vlan    Mac Address       Type             Ports   Remaining Age
                                                     (mins)
----    -----------       ----             -----   -------------
1       0025.83e6.4b01    SecureDynamic    Fa0/18       -
1       0025.83e6.4b02    SecureSticky     Fa0/19       -
------------------------------------------------------------
```

Ports désactivés en raison d'une erreur

- Une violation des règles de sécurité des ports peut entraîner la désactivation d'un commutateur suite à une erreur.
- Le port est alors arrêté.
- Le commutateur signale ces événements via les messages de console.

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to down
```

Ports désactivés en raison d'une erreur (suite)

LED

```
S1# show interface fa0/18 status
Port Name  Status        Vlan  Duplex  Speed   Type
Fa0/18     err-disabled  1     auto    auto    10/100BaseTX

S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000c.292b.4c75:1
Security Violation Count   : 1
```

La commande **show interface** permet également de détecter un port de commutateur désactivé suite à une erreur.

Il faut utiliser la commande du mode de configuration d'interface **shutdown** ou **no shutdown** pour réactiver le port.

Réactivation d'un port en mode de désactivation des erreurs

```
S1(config)# interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface
FastEthernet0/18, changed state to administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to up
```

5.3 Synthèse du chapitre

Cisco | Networking Academy®
Mind Wide Open™

Synthèse du chapitre

Synthèse

- Séquence d'amorçage des commutateurs LAN Cisco
- Modes des voyants des commutateurs LAN Cisco
- Comment accéder à distance à un commutateur LAN Cisco et le gérer via une connexion sécurisée
- Modes duplex des ports des commutateurs LAN Cisco
- Sécurité des ports, modes de violation et actions pour les commutateurs LAN Cisco
- Bonnes pratiques relatives aux réseaux commutés

Synthèse du chapitre

Synthèse

- Lorsqu'un commutateur LAN Cisco est mis sous tension pour la première fois, il exécute la séquence de démarrage suivante :
  1. D'abord, le commutateur exécute un programme de Power-On Self Test (POST) stocké dans la mémoire ROM. Le POST contrôle le sous-système du processeur. Il teste le processeur, la mémoire vive dynamique et la partie du périphérique flash qui compose le système de fichiers flash.
  2. Le commutateur exécute ensuite le bootloader. Le bootloader est un petit programme stocké dans la mémoire morte et exécuté immédiatement après la réussite du POST.
  3. Il effectue l'initialisation de bas niveau du processeur. Il initialise les registres du processeur qui contrôlent l'emplacement auquel la mémoire physique est mappée, la quantité de mémoire et sa vitesse.
  4. Le bootloader initialise le système de fichiers flash sur la carte système.
  5. Finalement, le chargeur de démarrage localise et charge dans la mémoire une image par défaut du logiciel du système d'exploitation IOS et donne le contrôle du commutateur à l'IOS.
- Si les fichiers du logiciel Cisco IOS sont manquants ou endommagés, le bootloader peut être utilisé pour procéder au redémarrage ou à la récupération à la suite d'un problème.
- L'état opérationnel du commutateur est affiché par une série de LED sur le panneau avant. Ces LED affichent des informations telles que l'état des ports, la bidirectionnalité et la vitesse.

Synthèse

- Une adresse IP est configurée sur l'interface SVI du VLAN de gestion afin de permettre la configuration à distance du périphérique. Une passerelle par défaut appartenant au VLAN de gestion doit être configurée sur le commutateur à l'aide de la commande **ip default-gateway**. Si la passerelle par défaut n'est pas correctement configurée, la gestion à distance est impossible.
- Il est recommandé d'utiliser Secure Shell (SSH) pour créer une connexion de gestion sécurisée (chiffrée) vers un périphérique distant, afin d'éviter que les noms d'utilisateur et les mots de passe non chiffrés ne soient interceptés. Certains protocoles, notamment Telnet, ne permettent pas de se prémunir contre ces interceptions.
- Les commutateurs présentent l'avantage de prendre en charge les communications bidirectionnelles simultanées entre les périphériques, doublant ainsi le débit effectif des communications. Bien qu'il soit possible de spécifier les paramètres de vitesse et de bidirectionnalité d'une interface de commutateur, il est recommandé de laisser le commutateur procéder à ces réglages automatiquement afin d'éviter toute erreur.
- La sécurité des ports ne constitue qu'une des méthodes permettant de se prémunir contre les attaques sur le réseau.