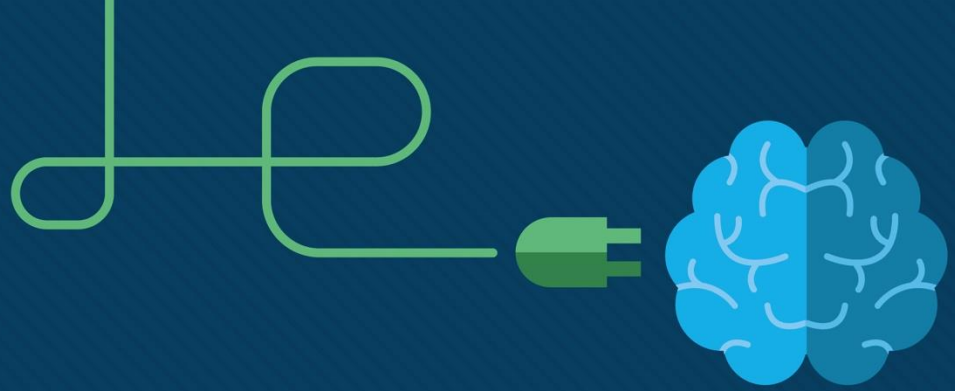
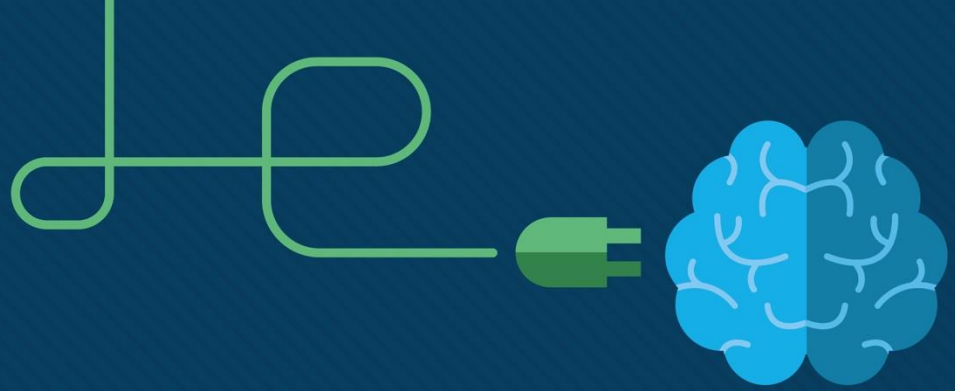


Module 11 : Configuration de la sécurité du commutateur

Contenu Pédagogique de l'instructeur

Notions de base sur la commutation, le routage et le sans fil v7.0 (SRWE)



Module : Configuration de la sécurité du commutateur

Notions de base sur la commutation, le routage et le sans fil v7.0 (SRWE)

Objectifs de ce module

Titre du module : Configuration de la sécurité du commutateur

Objectif du module: configurer la sécurité des commutateurs pour atténuer les attaques LAN

Titre du rubrique	Objectif du rubrique
Mise en œuvre de la sécurité des ports	Implémentez la sécurité des ports pour atténuer les attaques de table d'adresses MAC.
Atténuer les attaques VLAN	Expliquez comment configurer le DTP et le VLAN natif pour atténuer les attaques de VLAN.
Atténuer les attaques DHCP	Expliquez comment configurer la suveillance DHCP pour atténuer les attaques DHCP.
Atténuer les attaques ARP	Expliquez comment configurer l'inspection ARP pour atténuer les attaques ARP.
Atténuer les attaques STP	Expliquez comment configurer PortFast et BPDU Guard pour atténuer les attaques STP.

.1 Mettre en oeuvre la sécurité des ports

Ports inutilisés sécurisés

Les attaques de couche 2 sont parmi les plus faciles à déployer pour les pirates, mais ces menaces peuvent également être atténuées avec certaines solutions de couche 2 courantes.

- Tous les ports (interfaces) du commutateur doivent être sécurisés avant que le commutateur ne soit déployé pour une utilisation en production. La façon dont un port est sécurisé dépend de sa fonction.
- Une méthode simple que de nombreux administrateurs utilisent pour protéger le réseau contre les accès non autorisés consiste à désactiver tous les ports inutilisés d'un commutateur. Naviguez vers chaque port inutilisé et émettez la commande **shutdown** de Cisco IOS. Si un port doit être réactivé plus tard, il peut être activé avec la commande **no shutdown** .
- Pour configurer une portée de ports, utilisez la commande **interface range** .

```
Switch(config)# interface range type module/first-number - last-number
```

Atténuer les attaques de table d'adresses MAC

La méthode la plus simple et la plus efficace pour empêcher les attaques par débordement de la table d'adresses MAC consiste à activer la sécurité des ports.

- La sécurité des ports limite le nombre d'adresses MAC valides autorisées sur un port. Il permet à un administrateur de configurer manuellement les adresses MAC d'un port ou de permettre au commutateur d'apprendre dynamiquement un nombre limité d'adresses MAC. Lorsqu'un port configuré avec la sécurité de port reçoit une trame, l'adresse MAC du source de la trame est comparée à la liste des adresses MAC des source sécurisées qui ont été configurées manuellement ou apprises dynamiquement sur le port.
- En limitant le nombre d'adresses MAC autorisées sur un port à un, la sécurité du port peut être utilisée pour contrôler l'accès non autorisé au réseau.

Activer la sécurité des ports

La sécurité des ports est activée avec la commande de configuration de l'interface **switchport port-security** .

Notez que dans l'exemple, la commande **switchport port-security** a été rejetée. C'est parce que, la sécurité des ports ne peut être configurée que sur des ports d'accès configurés manuellement ou des ports de trunk de réseau configurés manuellement. Par défaut, les ports de commutateur de couche 2 sont réglés sur l'auto dynamique (trunking activée). Par conséquent, dans l'exemple, le port est configuré avec la commande de configuration de l'interface **switchport mode access** .

Remarque: la sécurité des ports trunc dépasse le cadre de ce cours.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

Activer la sécurité des ports (Suite)

Utilisez la commande **show port-security interface** pour afficher les paramètres de sécurité de port actuels pour FastEthernet 0/1.

- Remarquez comment la sécurité des ports est activée, le mode de violation est arrêté et comment le nombre maximal d'adresses MAC est 1.
- Si un périphérique est connecté au port, le commutateur ajoute automatiquement l'adresse MAC du périphérique en tant que MAC sécurisé. Dans cet exemple, aucun périphérique n'est connecté au port.

```
S1# show port-security interface f0/1
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   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

Remarque: si un port actif est configuré avec la commande **switchport port-security** et que plusieurs périphériques sont connectés à ce port, le port passera à l'état désactivé par erreur.

Activer la sécurité des ports (Suite)

Une fois la sécurité des ports est activée, d'autres spécificités de sécurité des ports peuvent être configurées, comme illustré dans l'exemple.

```
S1(config-if)# switchport port-security ?
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addresses
  violation     Security violation mode
  <cr>
S1(config-if)# switchport port-security
```

Limiter et apprendre les adresses MAC

Pour définir le nombre maximal d'adresses MAC autorisées sur un port, utilisez la commande suivante:

```
Switch(config-if)# switchport port-security maximum value
```

- La valeur de sécurité du port par défaut est 1.
- Le nombre maximal d'adresses MAC sécurisées pouvant être configurées dépend du commutateur et de l'IOS.
- Dans cet exemple, le maximum est 8192.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security maximum ?
  <1-8192>  Maximum addresses
S1(config-if)# switchport port-security maximum
```

Limiter et apprendre les adresses MAC (Suite)

Le commutateur peut être configuré pour en savoir plus sur les adresses MAC sur un port sécurisé de trois manières:

1. Configuration manuelle: l'administrateur configure manuellement une ou des adresses MAC statiques à l'aide de la commande suivante pour chaque adresse MAC sécurisée sur le port:

```
Switch(config-if)# switchport port-security mac-address mac-address
```

2. Apprentissage dynamique: lorsque la commande **switchport port-security** est entrée, le MAC source actuel du périphérique connecté au port est automatiquement sécurisé mais n'est pas ajouté à la configuration en cours. Si le commutateur est redémarré, le port devra réapprendre l'adresse MAC du périphérique.

3. Apprentissage dynamique - Sticky: l'administrateur peut activer le commutateur pour apprendre dynamiquement les adresses MAC et les «coller» à la configuration en cours en utilisant la commande suivante:

```
Switch(config-if)# switchport port-security mac-address sticky
```

L'enregistrement de la configuration en cours valide l'adresse MAC apprise dynamiquement dans la NVRAM.

Limiter et apprendre les adresses MAC(Suite)

L'exemple illustre une configuration de sécurité de port complète pour FastEthernet 0/1.

- L'administrateur spécifie un maximum de 4 adresses MAC, configure manuellement une adresse MAC sécurisée, puis configure le port pour apprendre dynamiquement des adresses MAC sécurisées supplémentaires jusqu'à 4 adresses MAC sécurisées au maximum.
- Utilisez les commandes **show port-security interface** et **show port-security address** pour vérifier la configuration.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 4
S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1# show port-security address
            Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    aaaa.bbbb.1234    SecureConfigured              Fa0/1        -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

S1#
```

Obsolescence de la sécurité des ports (suite)

L'obsolescence de la sécurité des ports peut être utilisée pour définir le temps d'obsolescence des adresses sécurisées statiques et dynamiques sur un port.

- **Absolue** - Les adresses sécurisées sur le port sont supprimées après le temps d'obsolescence spécifié.
- **Inactivité** - Les adresses sécurisées sur le port sont supprimées si elles sont inactives pendant une durée spécifiée.

Utilisez l'obsolescence pour supprimer les adresses MAC sécurisées sur un port sécurisé sans supprimer manuellement les adresses MAC sécurisées existantes.

- l'obsolescence des adresses sécurisées configurées statiquement peut être activé ou désactivé par port.

Utilisez la commande **switchport port-security aging** pour activer ou désactiver l'obsolescence statique pour le port sécurisé, ou pour définir le temps ou le type d'obsolescence.

```
Switch(config-if)# switchport port-security aging {static | time time | type {absolute | inactivity}}
```

Obsolescence de la sécurité des ports (suite)

L'exemple montre un administrateur configurant le type d'obsolescence à 10 minutes d'inactivité.

La commande **show port-security** confirme les modifications. la commande

```
S1(config)# interface fa0/1
S1(config-if)# switchport port-security aging time 10
S1(config-if)# switchport port-security aging type inactivity
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Restrict
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.56be.e4dd:1
Security Violation Count   : 1
```

Modes de violation de la sécurité des ports

Si l'adresse MAC d'un périphérique connecté à un port diffère de la liste des adresses sécurisées, une violation de port se produit et le port entre dans l'état désactivé par erreur.

- Pour définir le mode de violation de sécurité du port, utilisez la commande suivante:

```
Switch(config-if)# switchport port-security violation {shutdown | restrict | protect}
```

Le tableau suivant montre comment un commutateur réagit en fonction du mode de violation configuré.

Mode	Description
shutdown (par défaut)	Le port passe immédiatement à l'état désactivé par erreur, éteint la LED du port et envoie un message Syslog. Il incrémente le compteur de violations. Lorsqu'un port sécurisé est dans l'état désactivé par erreur, un administrateur doit le réactiver en entrant les commandes **shutdown** and **no shutdown**
restreindre	Le port supprime les paquets dont l'adresse source est inconnue jusqu'à ce que vous supprimiez un nombre suffisant d'adresses MAC sécurisées pour passer en dessous de la valeur maximale ou augmenter la valeur maximale. Ce mode entraîne l'incrémentation du compteur de violation de sécurité et génère un message syslog.
protéger	Il s'agit du mode de violation de sécurité le moins sécurisé. Le port supprime les paquets avec des adresses source MAC inconnues jusqu'à ce que vous supprimiez un nombre suffisant d'adresses MAC sécurisées pour descendre en dessous de la valeur maximale ou augmenter la valeur maximale. Aucun message Syslog n'est envoyé.

Modes de violation de la sécurité des ports (suite)

L'exemple montre un administrateur remplaçant la violation de sécurité par «Restreindre».

La sortie de la commande **show port-security interface** confirme que la modification a été effectuée.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security violation restrict
S1(config-if)# end
S1#
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.56be.e4dd:1
Security Violation Count   : 1
S1#
```

Ports en état désactivé par erreur

Quand un port est fermé et placé dans l'état error-disabled, aucun trafic n'est envoyé ou reçu sur ce port

Une série de messages liés à la sécurité des ports s'affiche sur la console, comme illustré dans l'exemple suivant.

Remarque: Le protocole de port et l'état de la liaison passent à l'état bas et le voyant du port est éteint.

```
*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 en état désactivé par erreur (suite)

- Dans l'exemple, la commande **show interface** identifie l'état du port comme étant **err-disabled**.. La sortie de la commande **show port-security interface** affiche désormais l'état du port comme étant **secure-shutdown**. Le compteur de violation de sécurité incrémente de 1.
- L'administrateur doit déterminer la cause de la violation de sécurité. Si un périphérique non autorisé est connecté à un port sécurisé, la menace de sécurité est éliminée avant de réactiver le port.
- Pour réactiver le port, utilisez d'abord la commande **shutdown** puis utilisez la commande **no shutdown** .

```
S1# show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
(output omitted)
S1# show port-security interface fa0/18
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        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : c025.5cd7.ef01:1
Security Violation Count   : 1
S1#
```

Vérifier la sécurité des ports

Après avoir configuré la sécurité des ports sur un commutateur, vérifiez chaque interface pour vérifier que la sécurité des ports est correctement définie et assurez-vous que les adresses MAC statiques ont été correctement configurées.

Pour afficher les paramètres de sécurité des ports pour le commutateur, utilisez la commande **showport-security** .

- L'exemple indique que les 24 interfaces sont configurées avec la commande **switchport port-security** car le maximum autorisé est 1 et le mode de violation est arrêté.
- Aucun périphérique n'est connecté, par conséquent, le CurrentAddr (Count) est 0 pour chaque interface.

```
S1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-----------------------------------------------------------------------------
      Fa0/1            1            0                  0         Shutdown
      Fa0/2            1            0                  0         Shutdown
      Fa0/3            1            0                  0         Shutdown
(output omitted)
     Fa0/24            1            0                  0         Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

Vérifier la sécurité des ports(suite)

Utilisez la commande **show port-security interface** pour afficher les détails d'une interface spécifique, comme indiqué précédemment et dans cet exemple.

```
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
S1#
```

Vérifier la sécurité des ports(suite)

Pour vérifier que les adresses MAC «collent» à la configuration, utilisez la commande **show run** comme indiqué dans l'exemple pour FastEthernet 0/19.

```
S1# show run | begin interface FastEthernet0/19
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
(output omitted)
S1#
```

Vérifier la sécurité des ports(suite)

Pour afficher toutes les adresses MAC sécurisées configurées manuellement ou apprises dynamiquement sur toutes les interfaces de commutateur, utilisez la commande **show port-security address** comme indiqué dans l'exemple.

```
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          -
------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

.2 Atténuer les attaques VLAN

Revue des attaques VLAN

Une attaque par saut de VLAN peut être lancée de trois manières:

- Usurpation des messages DTP de l'hôte attaquant pour que le commutateur passe en mode de jonction. À partir de là, l'attaquant peut envoyer du trafic étiqueté avec le VLAN cible, et le commutateur délivre ensuite les paquets à la destination.
- Présentation d'un commutateur escroc et activation de la jonction. L'attaquant peut alors accéder à tous les VLAN sur le commutateur victime à partir du commutateur non autorisé.
- Un autre type d'attaque par saut de VLAN est une attaque à double marquage (ou à double encapsulation). Cette attaque tire parti du fonctionnement du matériel sur la plupart des commutateurs.

Étapes pour atténuer les attaques de saut de VLAN

Utilisez les étapes suivantes pour atténuer les attaques par saut de VLAN:

Étape 1: désactivez les négociations DTP (jonction automatique) sur les ports sans jonction à l'aide de la commande de configuration de l'interface **switchport mode access** .

Étape 2: désactivez les ports inutilisés et placez-les dans un VLAN inutilisé.

Étape 3: Activez manuellement la liaison de jonction sur un port de jonction à l'aide de la commande **switchport mode trunk** .

Étape 4: désactivez les négociations DTP (trunking automatique) sur les ports de jonction à l'aide de la commande **switchport nonegotiate** .

Étape 5: définissez le VLAN natif sur un VLAN autre que VLAN 1 à l'aide de la commande **switchport trunk native vlan** *vlan_number* .

```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# end
S1#
```

.3 Atténuer les attaques DHCP

Revue d'attaque DHCP

Le but d'une attaque de famine DHCP est d'utiliser un outil d'attaque tel que Gobbler pour créer un déni de service (DoS) pour connecter les clients.

Rappelez-vous que les attaques de famine DHCP peuvent être efficacement atténuées en utilisant la sécurité des ports car Gobbler utilise une adresse MAC source unique pour chaque demande DHCP envoyée. Cependant, l'atténuation des attaques d'usurpation DHCP nécessite plus de protection.

Gobbler peut être configuré pour utiliser l'adresse MAC de l'interface réelle comme adresse Ethernet source, mais spécifiez une adresse Ethernet différente dans la charge utile DHCP. Cela rendrait la sécurité du port inefficace car l'adresse MAC source serait légitime.

Les attaques d'usurpation DHCP peuvent être atténuées en utilisant la surveillance DHCP sur les ports approuvés.

Surveillance du DHCP

La surveillance DHCP filtre les messages DHCP et limite le trafic DHCP sur les ports non approuvés.

- Les périphériques sous contrôle administratif (par exemple, les commutateurs, les routeurs et les serveurs) sont des sources fiables.
- Les interfaces sécurisées (par exemple, liaisons de jonction, ports de serveur) doivent être explicitement configurées comme sécurisées.
- Les périphériques en dehors du réseau et tous les ports d'accès sont généralement traités comme des sources non fiables.

Une table DHCP est créée qui inclut l'adresse MAC source d'un périphérique sur un port non approuvé et l'adresse IP attribuée par le serveur DHCP à ce périphérique.

- L'adresse MAC et l'adresse IP sont liées ensemble.
- Par conséquent, cette table est appelée table de liaison d'espionnage DHCP.

Étapes pour implémenter la surveillance DHCP

Utilisez les étapes suivantes pour activer la surveillance DHCP (snooping):

Étape 1. Activez la surveillance DHCP à l'aide de la commande de configuration globale **ip dhcp snooping** .

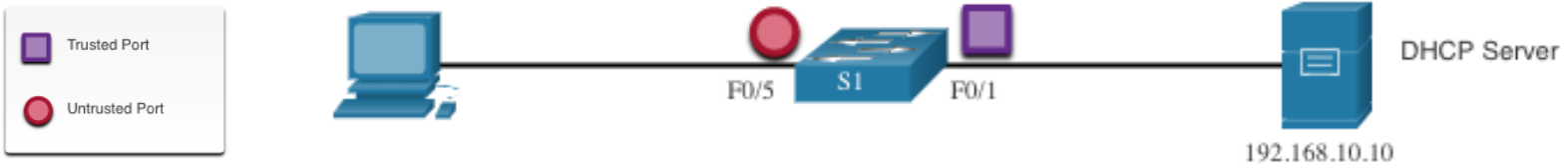
Étape 2. Sur les ports approuvés, utilisez la commande de configuration de l'interface **ip dhcp snooping trust** .

Étape 3: sur les interfaces non fiables, limitez le nombre de messages de découverte DHCP pouvant être reçus à l'aide de la commande de configuration d'interface **ip dhcpsnooping limit rate** *packets-per-second* .

Étape 4. Activez la surveillance DHCP par VLAN, ou par une portée de VLAN, en utilisant la commande de configuration globale **ip dhcp snooping** *vlan* .

Exemple de configuration de surveillance DHCP

Reportez-vous à l'exemple de topologie de surveillance DHCP avec des ports approuvés et non approuvés.



- La surveillance DHCP est d'abord activé sur S1.
- L'interface en amont du serveur DHCP est explicitement approuvée.
- F0 / 5 à F0 / 24 ne sont pas approuvés et sont donc limités à six paquets par seconde.
- Enfin, la surveillance DHCP est activée sur les VLANS 5, 10, 50, 51 et 52.

```
S1(config)# ip dhcp snooping
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
S1#
```

Exemple de configuration de surveillance DHCP

Utilisez la commande EXEC privilégiée **show ip dhcp snooping** pour vérifier les paramètres de surveillance DHCP.

Utilisez la commande **show ip dhcp snooping binding** pour afficher les clients qui ont reçu des informations DHCP.

Remarque:La surveillance DHCP est également requis par l'inspection ARP dynamique (DAI).

```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet0/1            yes        yes             unlimited
  Custom circuit-ids:
FastEthernet0/5            no         no              6
  Custom circuit-ids:
FastEthernet0/6            no         no              6
  Custom circuit-ids:
S1# show ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec) Type           VLAN Interface
------------------ --------------- ---------- -------------- ---- --------------------
00:03:47:B5:9F:AD  192.168.10.10   193185     dhcp-snooping 5    FastEthernet0/5
```

.4 Atténuer les attaques d'ARP

Inspection ARP dynamique

Dans une attaque ARP typique, un acteur de menace peut envoyer des réponses ARP non sollicitées à d'autres hôtes du sous-réseau avec l'adresse MAC de l'acteur de menace et l'adresse IP de la passerelle par défaut. Pour empêcher l'usurpation ARP et l'empoisonnement ARP qui en résulte, un commutateur doit garantir que seules les demandes et réponses ARP valides sont relayées.

L'inspection ARP dynamique (DAI) nécessite la surveillance DHCP et aide à prévenir les attaques ARP en:

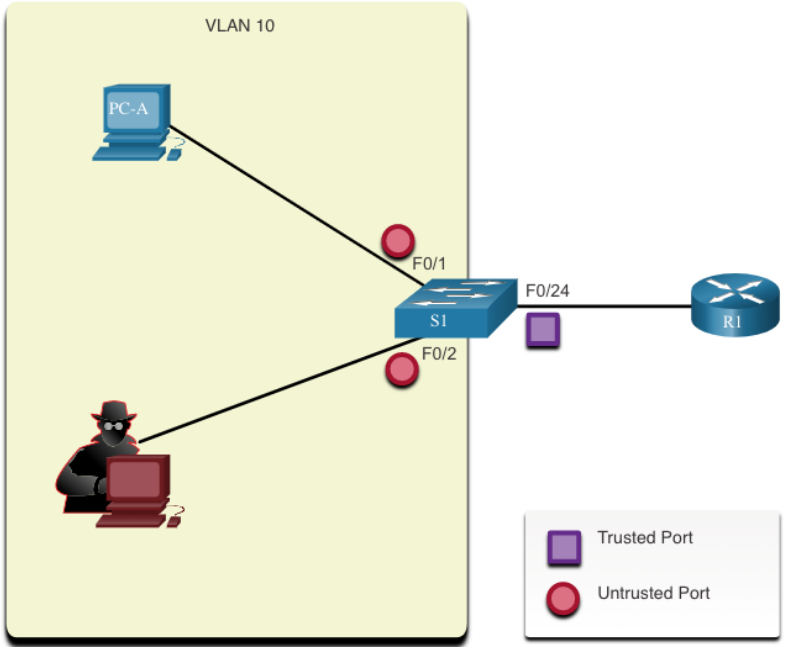
- Ne pas relayer les réponses ARP non valides ou gratuites vers d'autres ports du même VLAN.
- Interception de toutes les demandes et réponses ARP sur des ports non approuvés.
- Vérification de chaque paquet intercepté pour une liaison IP-MAC valide.
- Abandon et journalisation des réponses ARP provenant de non valides pour empêcher l'empoisonnement ARP.
- Erreur-désactivation de l'interface si le nombre DAI de paquets ARP configuré est dépassé.

Directives d'implémentation DAI

Pour atténuer les risques d'usurpation ARP et d'empoisonnement ARP, suivez ces directives d'implémentation DAI:

- Activez globalement la surveillance DHCP.
- Activez la surveillance DHCP sur les VLAN sélectionnés.
- Activez DAI sur les VLAN sélectionnés.
- Configurez des interfaces sécurisées pour la surveillance DHCP et l'inspection ARP.

Il est généralement conseillé de configurer tous les ports de commutateur d'accès comme non approuvés et de configurer tous les ports de liaison montante qui sont connectés à d'autres commutateurs comme approuvés.



Exemple de configuration DAI

Dans la topologie précédente, S1 connecte deux utilisateurs sur le VLAN 10.

- DAI sera configuré pour atténuer les attaques d'usurpation ARP et d'empoisonnement ARP.

- La surveillance DHCP est activée car DAI nécessite la table de liaison de surveillance DHCP pour fonctionner.
- Ensuite, la surveillance DHCP et l'inspection ARP sont activés pour les PC sur VLAN10.
- Le port de liaison montante vers le routeur est approuvé et est donc configuré comme approuvé pour la surveillance DHCP et l'inspection ARP.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection trust
```

Exemple de configuration DAI (suite)

DAI peut également être configuré pour vérifier les adresses MAC et IP de destination ou de source:

- **MAC destination** - vérifie l'adresse MAC de destination dans l'en-tête Ethernet par rapport à l'adresse MAC cible dans le corps ARP.
- **MAC source** -vérifie l'adresse MAC de source dans l'en-tête Ethernet par rapport à l'adresse MAC de l'expéditeur dans le corps ARP.
- **Adresse IP** -Vérifie le corps ARP pour les adresses IP invalides et inattendues, y compris les adresses 0.0.0.0, 255.255.255.255 et toutes les adresses de multidiffusion IP.

Exemple de configuration DAI (suite)

La commande de configuration globale **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} est utilisée pour configurer DAI pour supprimer les paquets ARP lorsque les adresses IP ne sont pas valides.

- Il peut être utilisé lorsque les adresses MAC dans le corps des paquets ARP ne correspondent pas aux adresses spécifiées dans l'en-tête Ethernet.
- Remarquez dans l'exemple suivant comment une seule commande peut être configurée.
- Par conséquent, la saisie de plusieurs commandes **ip arp inspection validate** écrase la commande précédente.
- Pour inclure plusieurs méthodes de validation, saisissez-les sur la même ligne de commande comme indiqué dans la sortie.

```
S1(config)# ip arp inspection validate ?
  dst-mac  Validate destination MAC address
  ip       Validate IP addresses
  src-mac  Validate source MAC address
S1(config)# ip arp inspection validate src-mac
S1(config)# ip arp inspection validate dst-mac
S1(config)# ip arp inspection validate ip
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```

.5 Atténuer les attaques STP

PortFast et BPDU Guard

Rappelez-vous que les attaquants du réseau peuvent manipuler le protocole STP (Spanning Tree Protocol) pour mener une attaque en usurpant le pont racine et en modifiant la topologie d'un réseau.

Pour atténuer les attaques STP, utilisez PortFast et Bridge Protocol Data Unit (BPDU) Guard:

PortFast

- PortFast amène immédiatement un port à l'état de transfert à partir d'un état de blocage, en contournant les états d'écoute et d'apprentissage.
- Appliquer à tous les ports d'accès d'utilisateur final.

BPDU Guard

- BPDU guard – Désactive immédiatement par erreur un port qui reçoit une unité BPDU.
- Comme PortFast, la protection BPDU (BPDU guard) ne doit être configurée que sur les interfaces connectées aux périphériques d'extrémité.

Configurer PortFast

PortFast contourne les états d'écoute et d'apprentissage STP pour minimiser le temps que les ports d'accès doivent attendre pour que STP converge.

- Activez PortFast uniquement sur les ports d'accès.
- PortFast sur les liaisons inter-commutateurs peut créer une boucle de spanning-tree.

PortFast peut être activé:

- **Sur une interface** - Utilisez la commande de configuration d'interface **spanning-tree portfast** .
- **Globalement** - Utilisez la commande de configuration globale **spanning-tree portfast default** pour activer PortFast sur tous les ports d'accès.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet0/1 but will only
 have effect when the interface is in a non-trunking mode.
S1(config-if)# exit
S1(config)# spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
 should now disable portfast explicitly on switched ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.
S1(config)# exit
```

Configurer PortFast (suite)

Pour vérifier si PortFast est activé globalement, vous pouvez utiliser soit:

- **show running-config | begin span** commande
- **S1#** show spanning-tree summary

Pour vérifier si PortFast est activé sur une interface, utilisez la commande **show running-config interface** *type/number* .

La commande **spanning-tree interface** *type/number* **detail** peut également être utilisée pour la vérification.

Configurer BPDU Guard

Un port d'accès pourrait recevoir des BPDU inattendus accidentellement ou parce qu'un utilisateur a connecté un commutateur non autorisé au port d'accès.

- Si une BPDU est reçue sur un port d'accès activé par BPDU Guard, le port est mis en état désactivé par erreur.
- Cela signifie que le port est arrêté et doit être réactivé manuellement ou récupéré automatiquement par la commande globale **errdisable recovery cause psecure_violation** .

BPDU Guard peut être activé:

- **Sur une interface** - Utilisez la commande de configuration d'interface **spanning-tree bpduguard enable** .
- **Globalement** - Utilisez la commande de configuration globale **spanning-tree portfast bpduguard default** pour activer BPDU Guard sur tous les ports d'accès.

```
S1(config)# interface fa0/1
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# spanning-tree portfast bpduguard default
S1(config)# end
S1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short
(output omitted)
S1#
```


CISCO