Cisco Networking Academy
Mind Wide Open

Chapitre 6:

Sécuriser le réseau local

CCNA Security v2.0

Samir DIABI

Sommaire

6.0 Introduction

6.1 Sécurité de point final

6.2 Menaces de sécurité de couche 2

6.3 Résumé

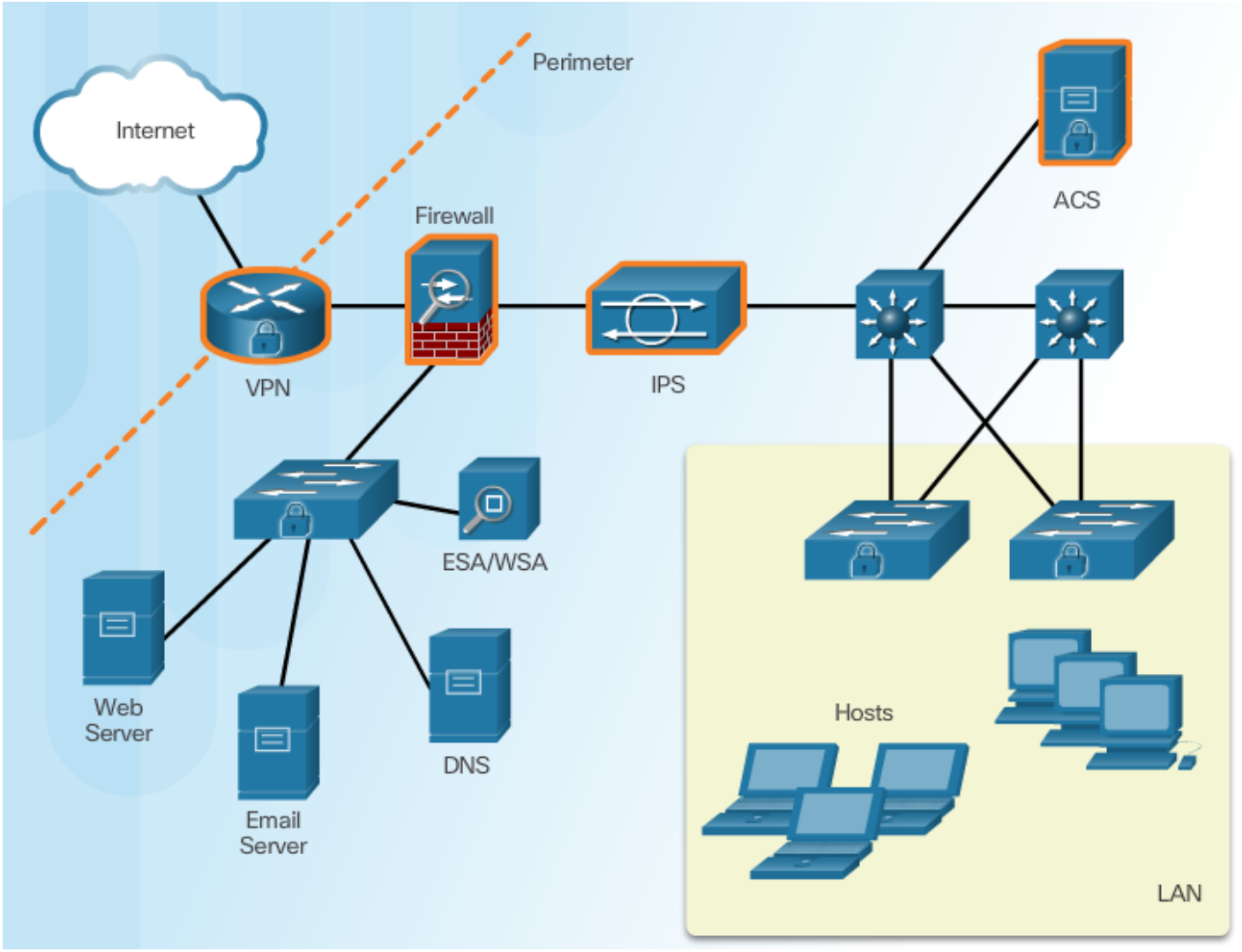
Section 6.1: Sécurité de point final

À la fin de cette section, vous devriez pouvoir:

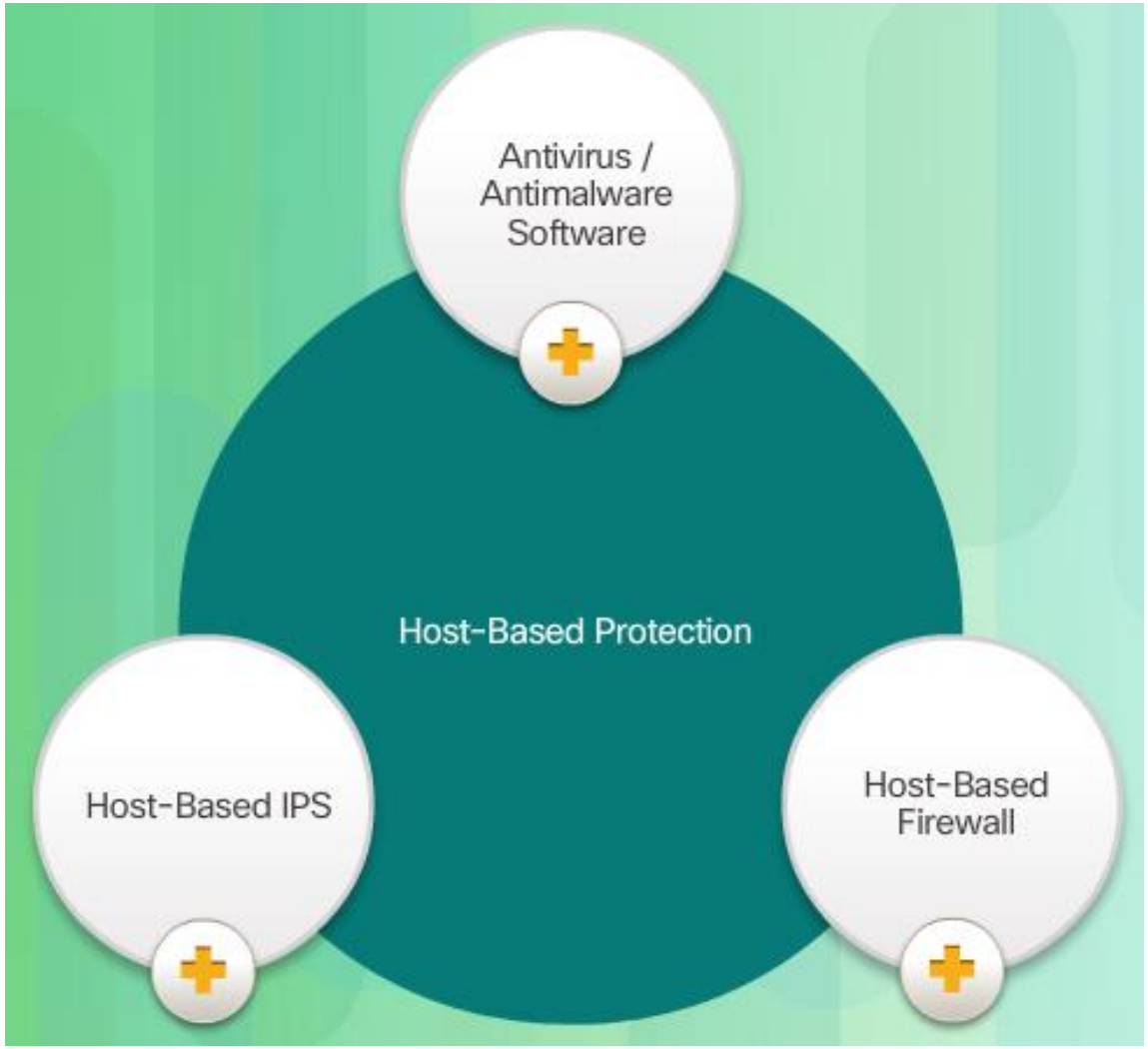
- Décrire la sécurité des points d'extrémité et les technologies habilitantes.
- Expliquer comment Cisco AMP est utilisé pour assurer la sécurité des terminaux.
- Expliquer comment Cisco NAC authentifie et applique la politique de sécurité du réseau.

Sujet 6.1.1:
Présentation du sécurité Endpoint

Sécurisation des éléments LAN



Sécurité de point final traditionnel



Le réseau sans bordure

Sécurisation des points d'extrémité dans le réseau sans bordure

Poste les questions d'attaque sur les logiciels malveillants:

- D'où vient-il?
- Quelle était la méthode de menace et le point d'entrée?
- Quels systèmes ont été affectés?
- Qu'a fait la menace?
- Puis-je arrêter la menace et la cause racine?
- Comment en récupérons-nous?
- Comment l'empêchons-nous de se reproduire?

Protection par hôte:

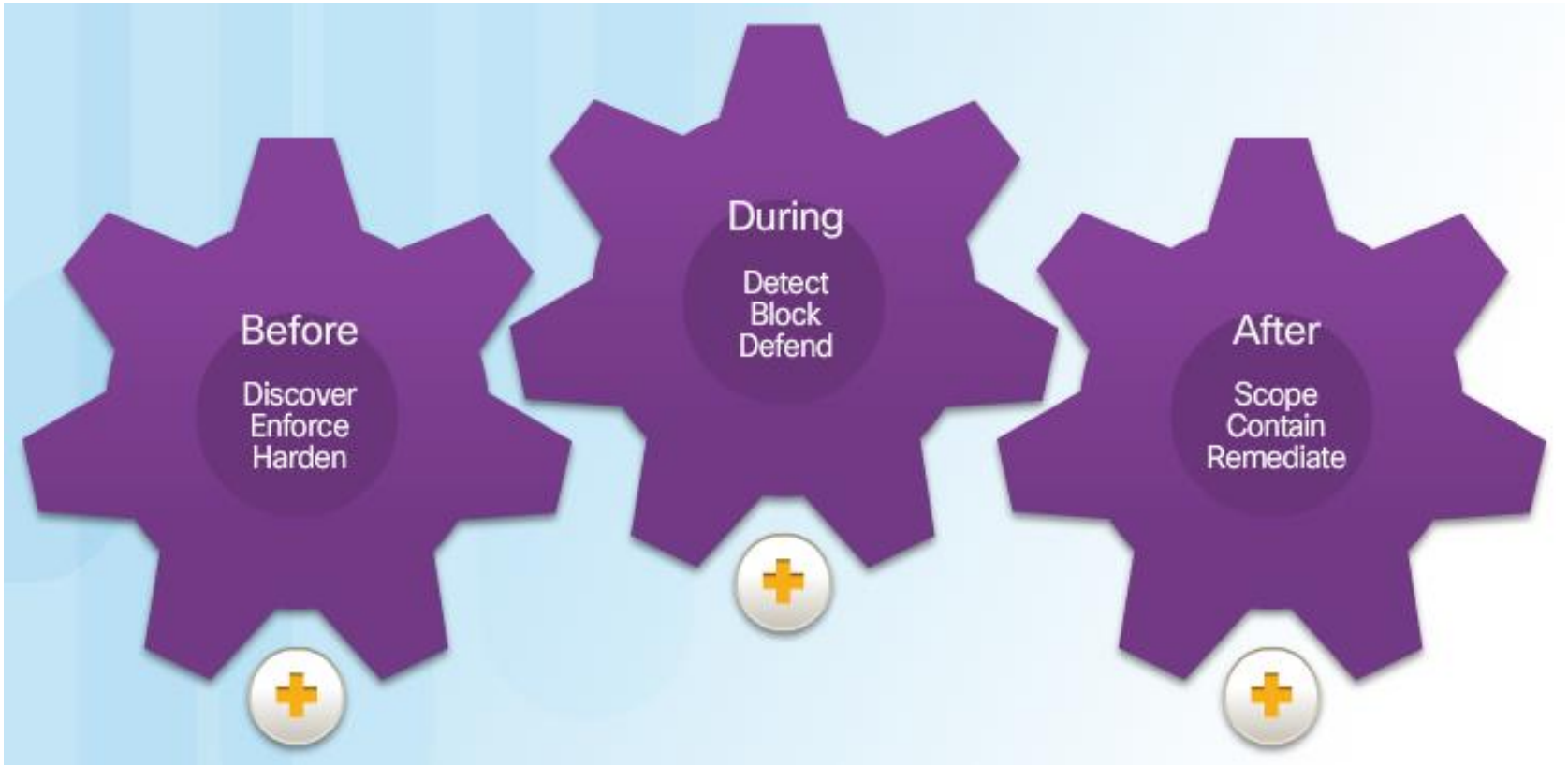
- Antivirus / Antimalware
- Filtrage SPAM
- Filtrage d'URL
- Liste noire
- Prévention des pertes de données (DLP)

Modernes solutions de sécurité de point final

Cryptage matériel et logiciel des données locales

Sujet 6.1.2:
Protection antimalware

Protection avancée contre les logiciels malveillants



AMP et gestion de la menace de défense

Les équipes de Talos rassemblent des informations sur les menaces en temps réel provenant de diverses sources:

- 1,6 million de dispositifs de sécurité déployés, y compris les pare-feu, IPS, Web et les appliances de messagerie
- 150 millions de points d'extrémité
- Ils analysent ensuite ces données:
- 100 TB de l'intelligence de sécurité par jour
- 13 milliards de demandes Web par jour
- 35% du trafic mondial de courrier électronique d'entreprise

AMP pour les points finaux

- **AMP for Endpoints** - AMP for Endpoints s'intègre avec Cisco AMP pour les réseaux pour offrir une protection complète sur les réseaux étendus et les points d'extrémité.
- **AMP for Networks** - Fournit une solution basée sur le réseau et est intégrée dans les appliances de sécurité Cisco ASA Firewall et Cisco FirePOWER dédiées.
- **AMP pour la sécurité du contenu** - Ceci est une fonctionnalité intégrée dans Cisco Cloud Web Security ou Cisco Web et Email Security Appliances pour protéger contre les courriels et les attaques de logiciels malveillants avancées basées sur le Web.

Sujet 6.1.3:
Email et sécurité Web

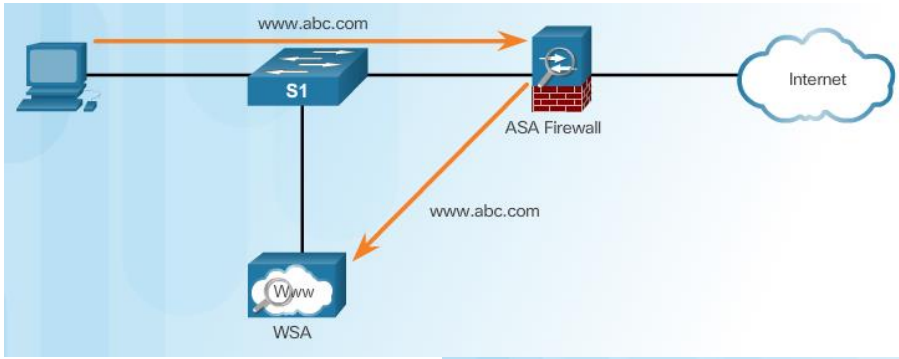
Sécurisation du courrier électronique et du Web

Appareil Cisco de la sécurité par courrier électronique

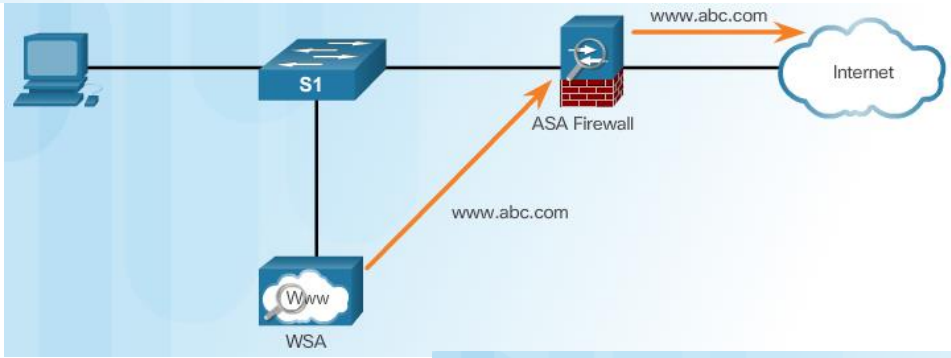
Caractéristiques et avantages des solutions Cisco Email Security:

- Intelligence globale contre les menaces
- Blocage de spam
- Protection avancée contre les logiciels malveillants
- Contrôle des messages sortants

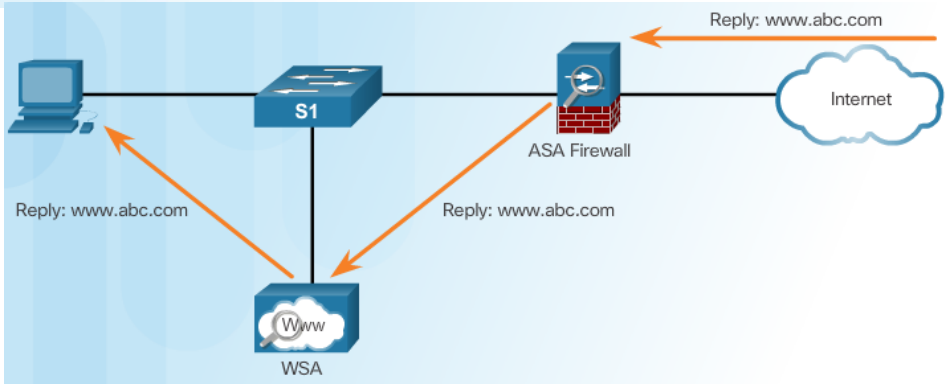
Appareil Cisco de la sécurité Web



Le client lance une demande Web



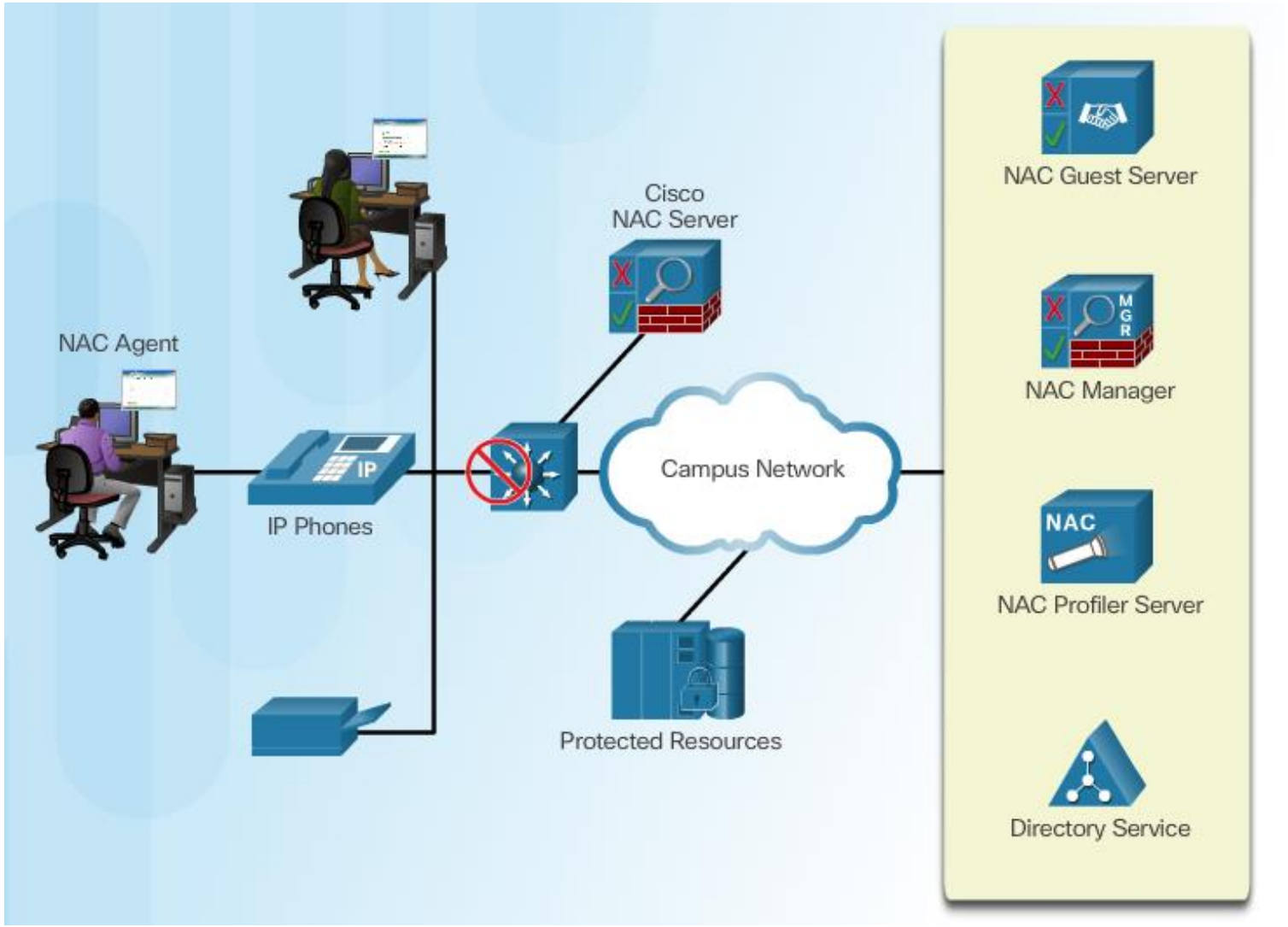
WSA lance une demande



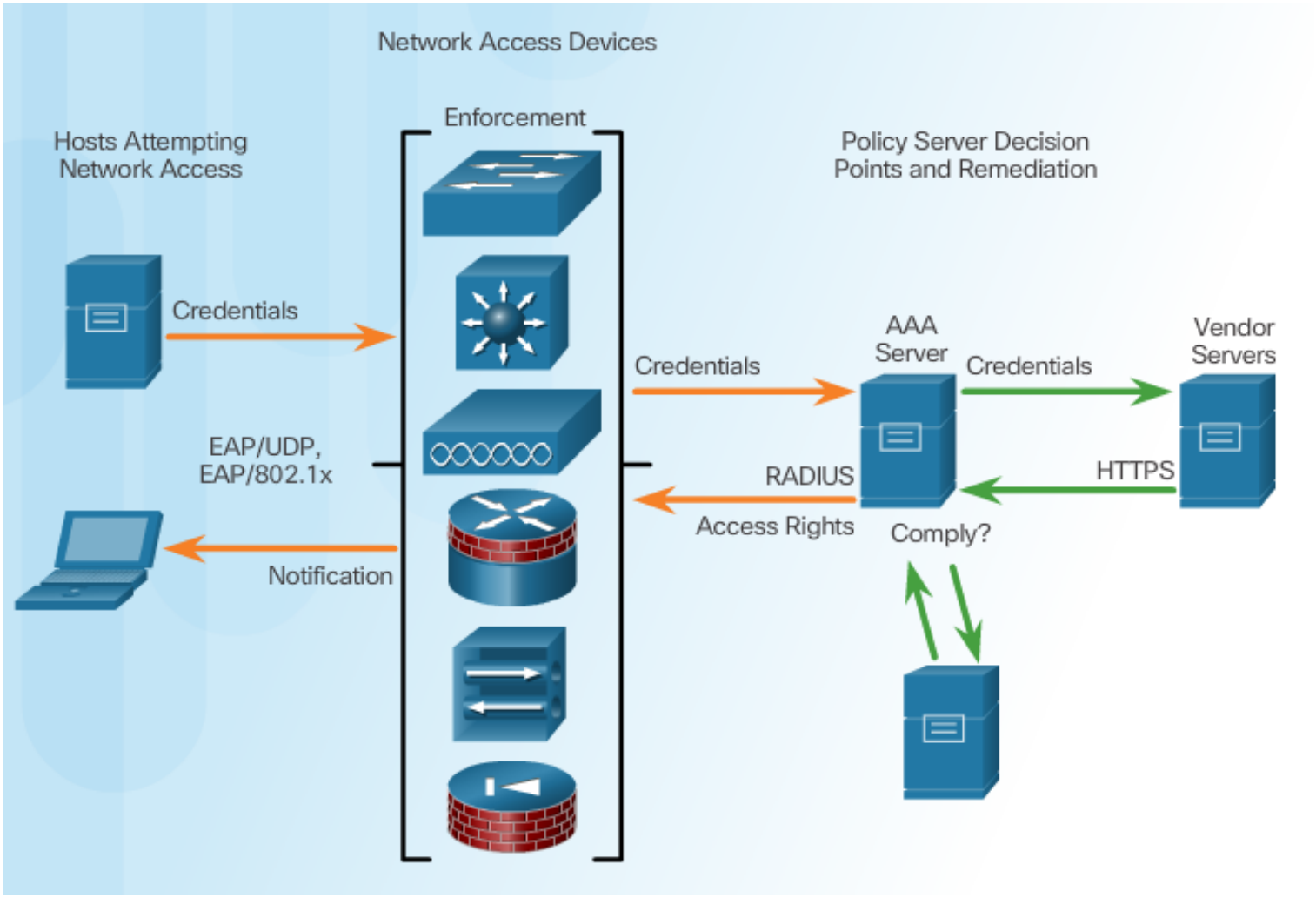
Réponse envoyée à WSA et ensuite au client

Sujet 6.1.4:
Contrôle du réseau d'accès

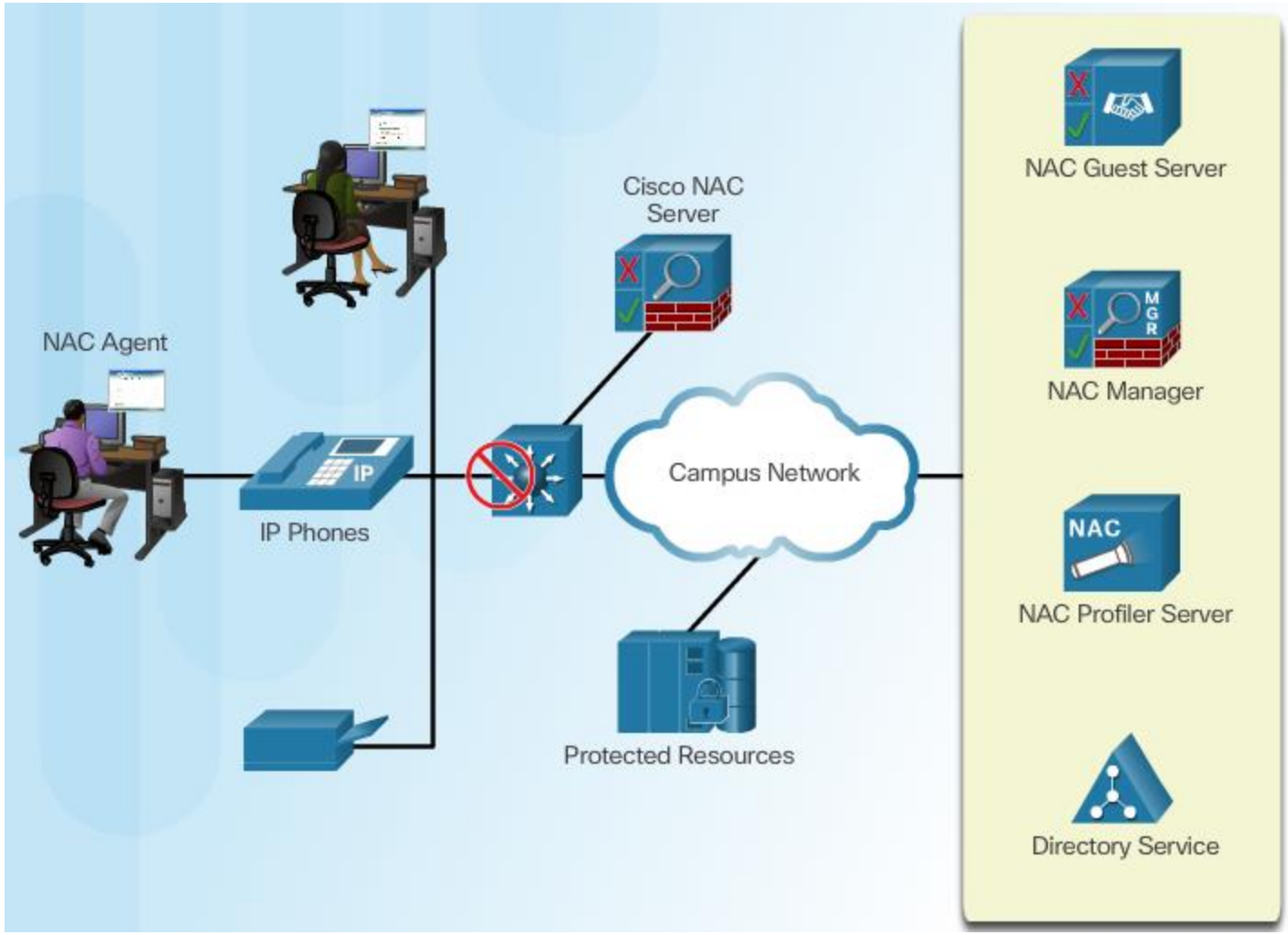
Contrôle d'admission au réseau Cisco



Fonctions Cisco NAC



Composants Cisco NAC

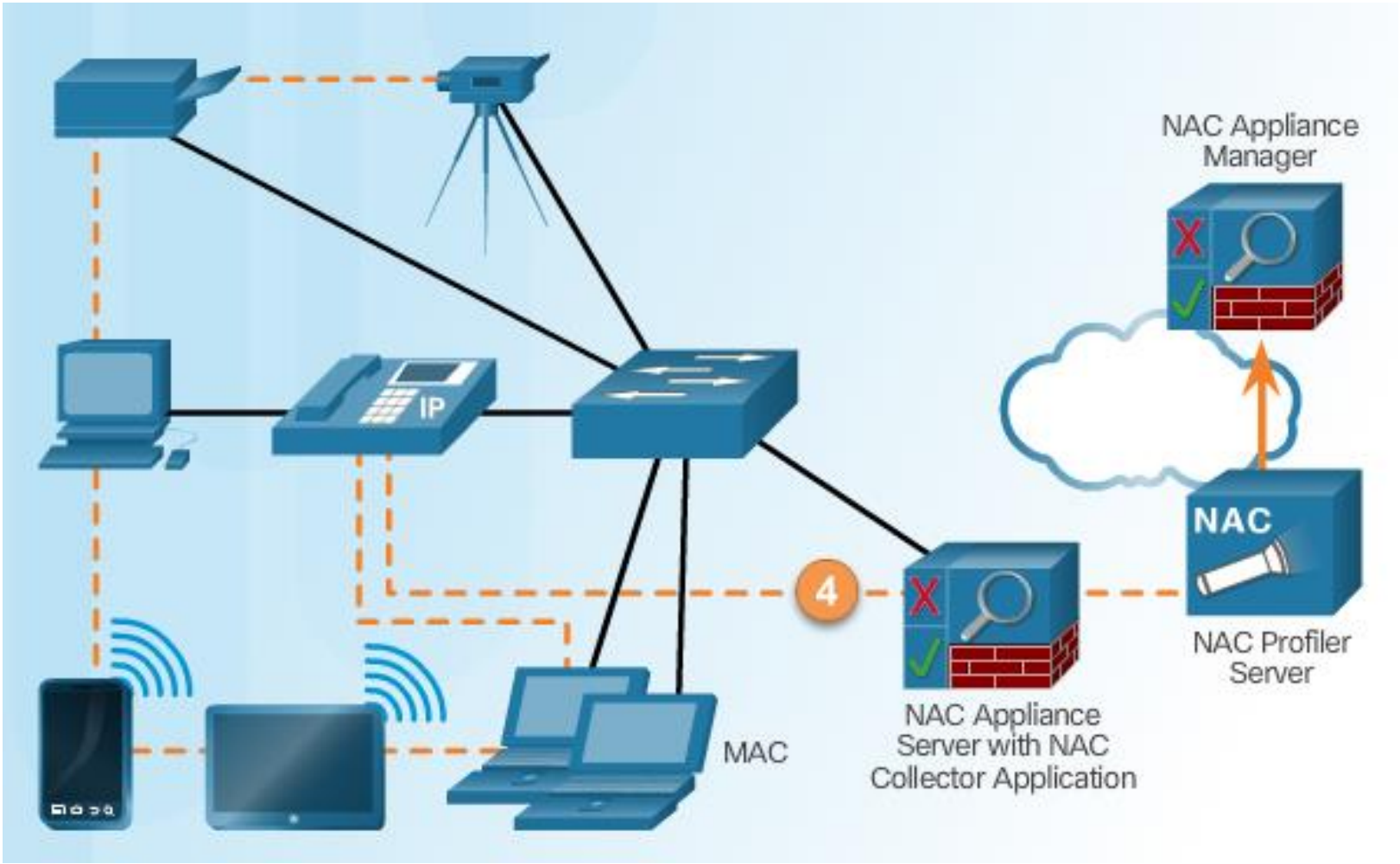


Accès réseau aux invités

Trois façons d'accorder des autorisations de parrainage:

- À seulement les comptes créés par le parrain
- À tous les comptes
- Sans compte (c.-à-d., Ils ne peuvent pas modifier d'autorisations)

Cisco NAC Profiler



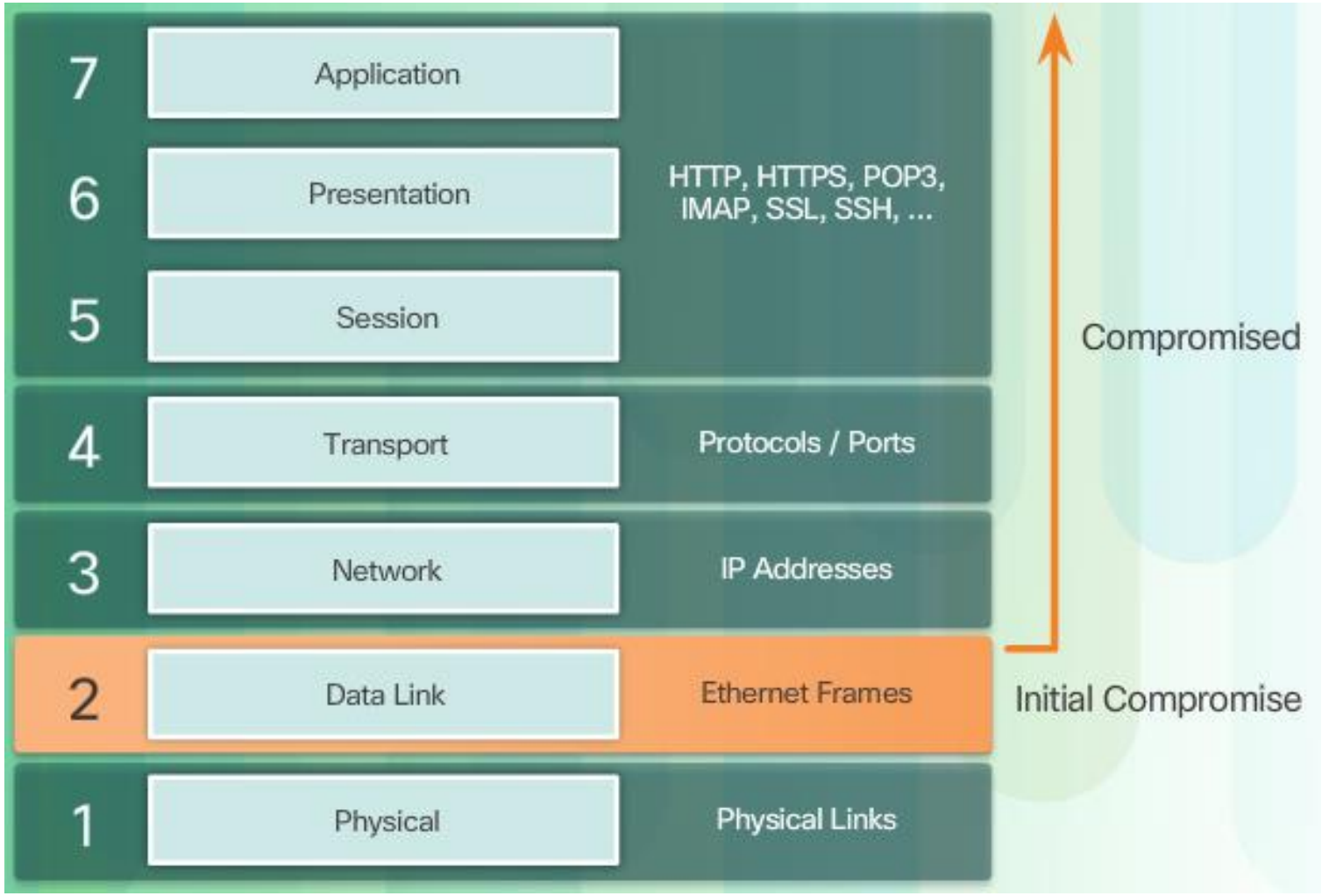
Section 6.2: Considérations relatives à la sécurité de couche 2

Une fois la section terminée, vous devriez pouvoir:

- Décrire les vulnérabilités de la couche 2.
- Décrire les attaques de dépassement de table CAM.
- Configurer la sécurité des ports pour atténuer les attaques de dépassement de table CAM.
- Configurer la sécurité du camion VLAN pour atténuer les attaques de sauts VLAN.
- Mettre en place DHCP Snooping pour atténuer les attaques DHCP.
- Mettre en place une inspection Arp dynamique pour atténuer les attaques ARP.
- Mettre en place IP Source Guard pour atténuer les attaques de falsification d'adresse.

Sujet 6.2.1:
Menaces de sécurité de couche 2

Décrivez les vulnérabilités de la couche 2



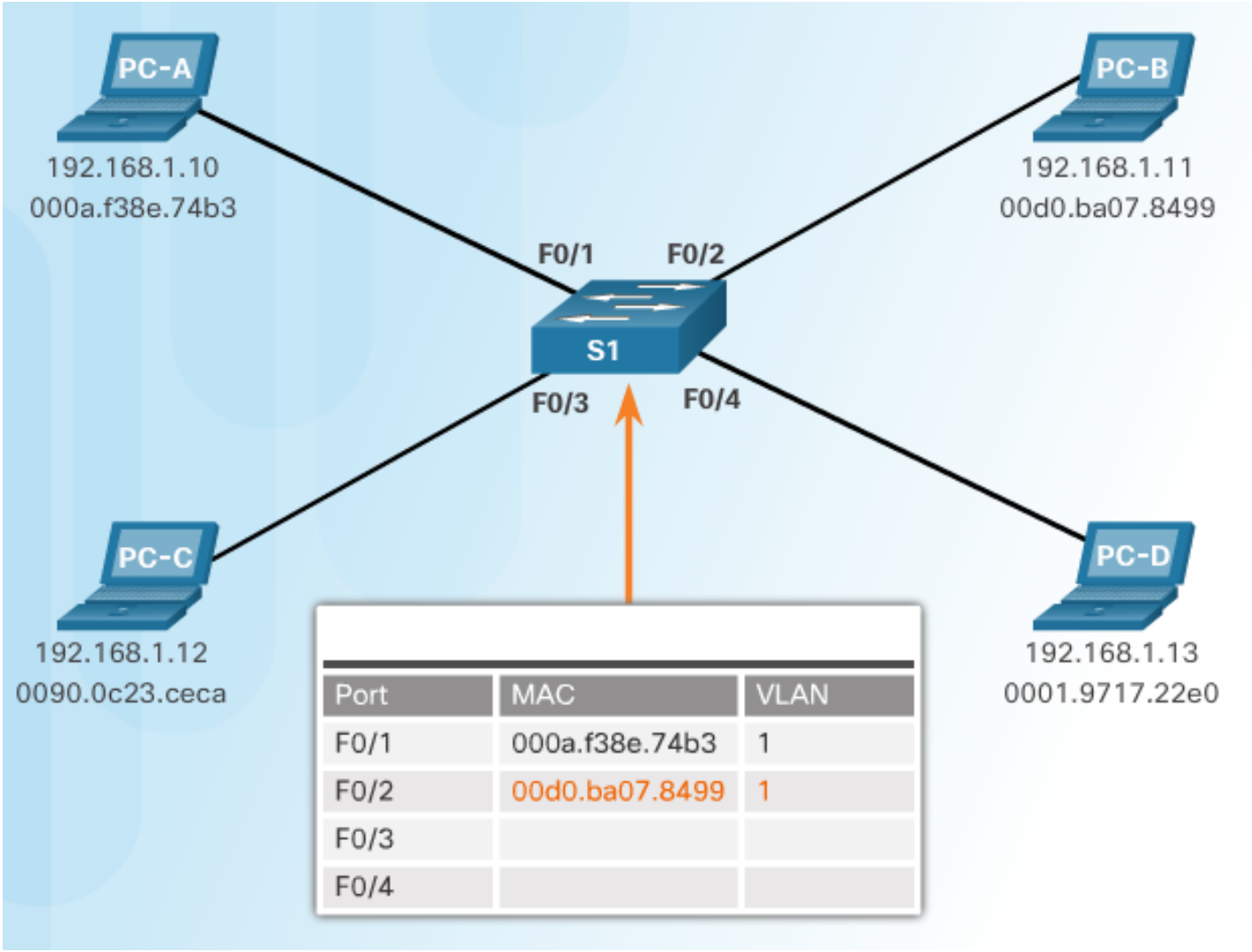
Catégories d'attaque par commutateur

Sujet 6.2.2:
Attaques de table CAM

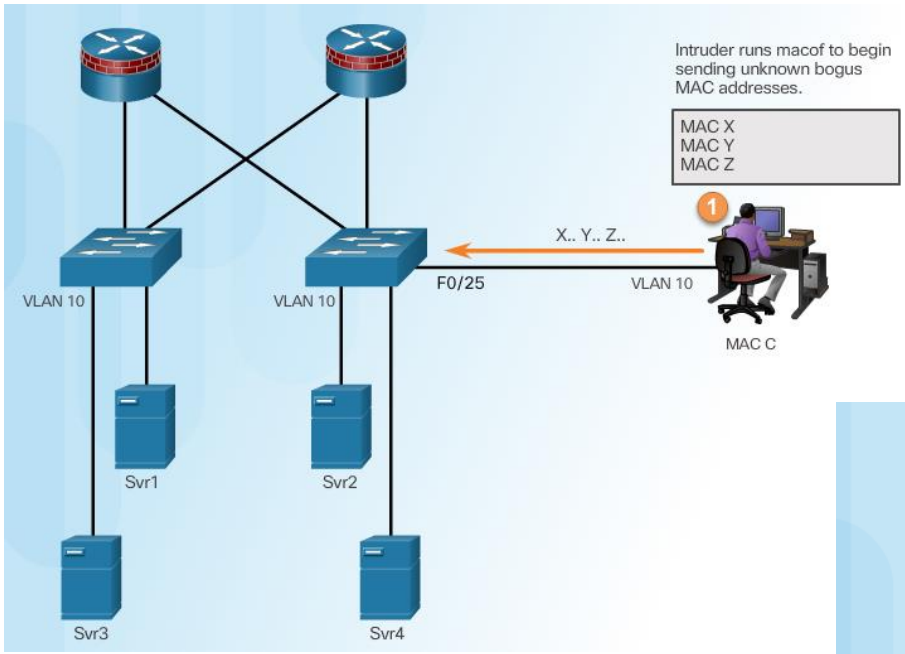
Fonctionnement de commutation de base

```
S1# show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
Sw1#
```

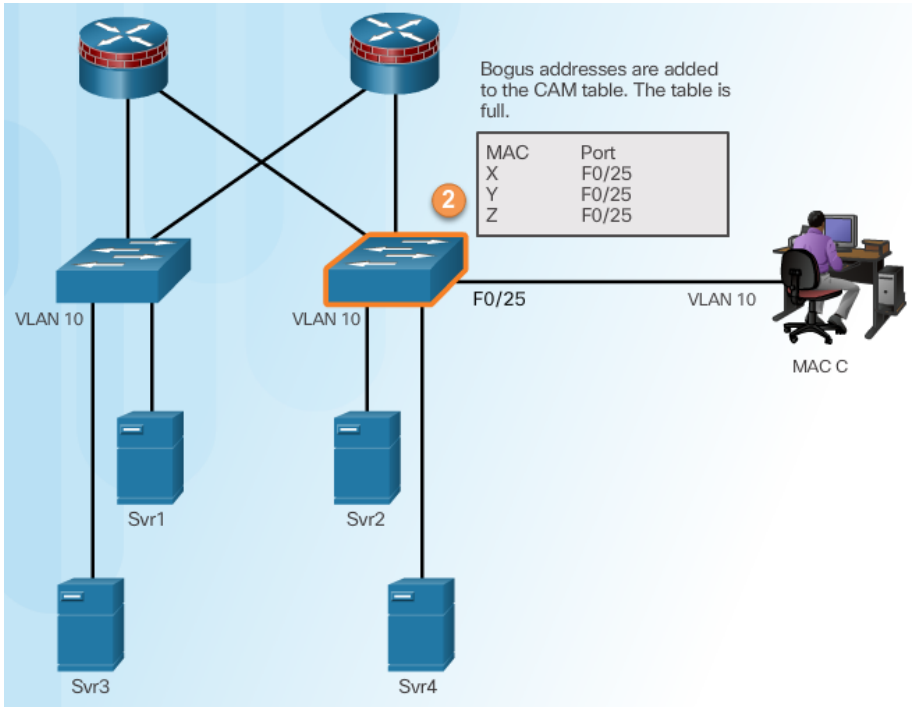
Exemple d'opération de la table CAM



Attaque de la table CAM

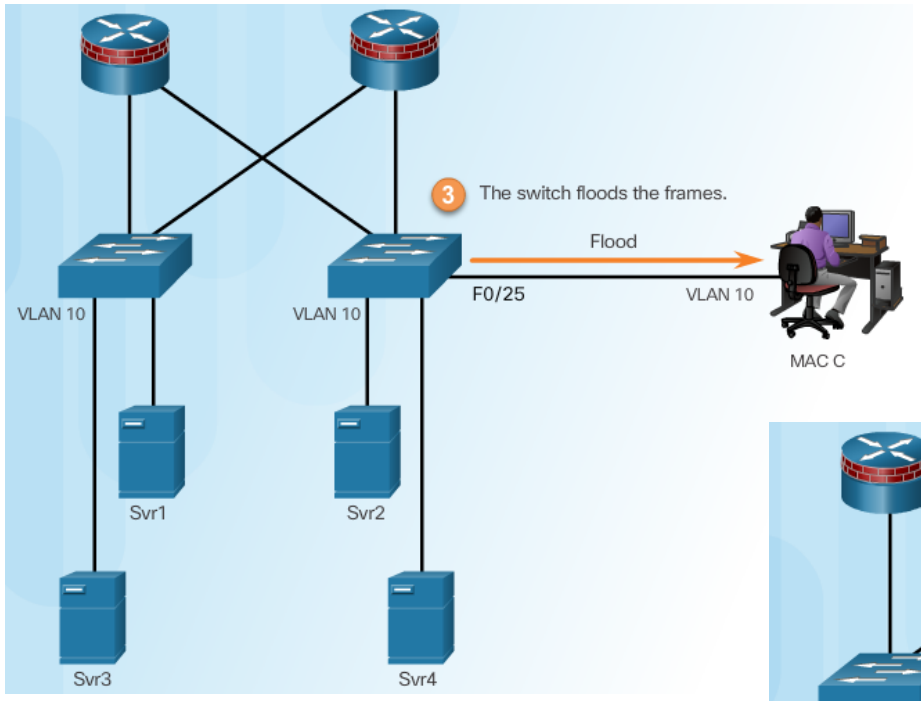


L' intrus lance un outil d'attaque

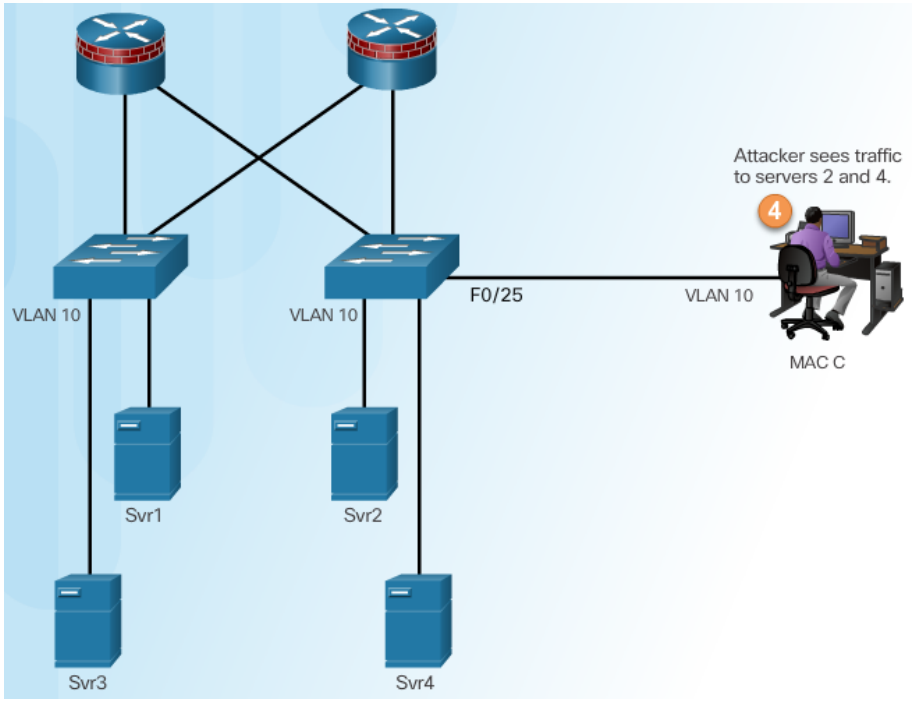


Remplir la table CAM

Attaque de la table CAM



Changer les inondations de tout le trafic



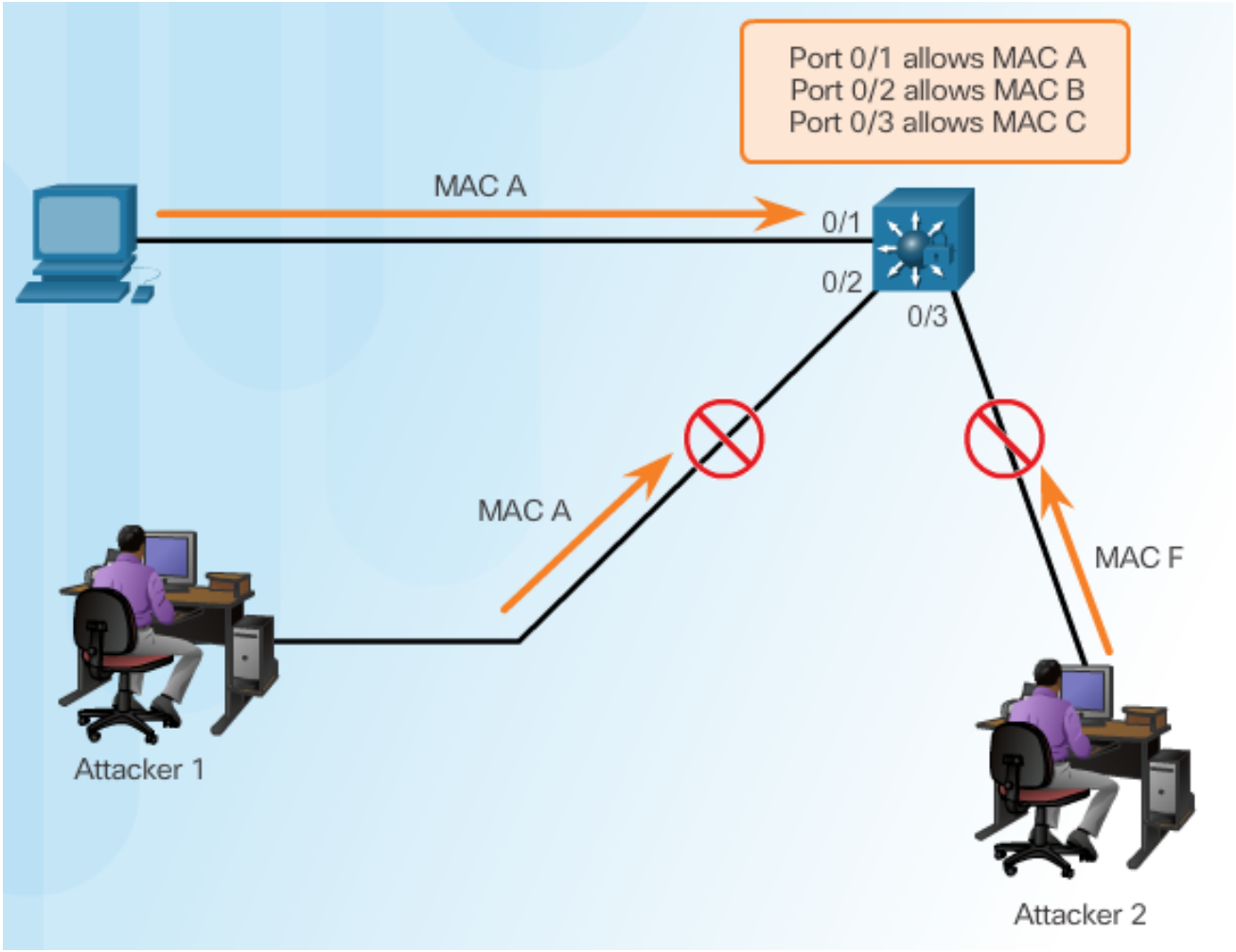
L'attaquant capture le trafic

Outils d'attaque de table CAM

```
macof -i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```

Sujet 6.2.3:
Mitigation des attaques de la CAM

Contre-mesure pour les attaques de table CAM



Port de Sécurité

```
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#
```

Activation de la sécurité des ports

Vérification de la sécurité des ports

```
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#
```

Options de sécurité du port

```
S1(config)# interface f0/1
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
```

Activation des options de sécurité du port

Définition du nombre maximal d'adresses Mac

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

Configuration manuelle des adresses MAC

```
Switch(config-if)
switchport port-security mac-address mac-address {vlan | {access | voice}}
```

Apprendre les adresses Mac connectées dynamiquement

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

Violations de sécurité des ports

Modes de violation de sécurité:

- Protéger
- Restreindre
- Fermer

Security Violation Modes

Violation Mode	Forwards Traffic	Sends Syslog Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No
Restrict	No	Yes	Yes	No
Shutdown	No	Yes	Yes	Yes

Vieillissement de la Sécurité du port

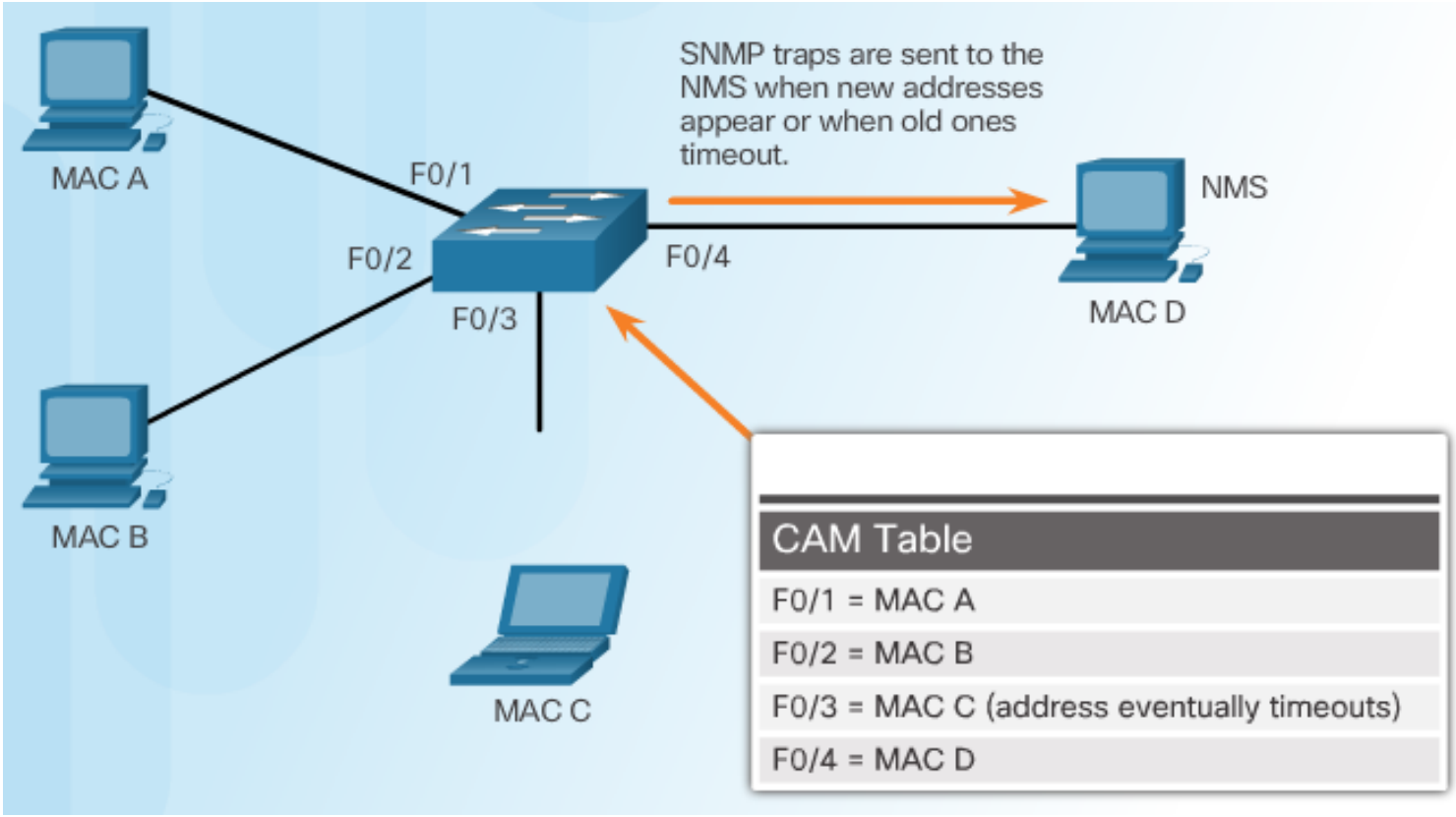
```
Switch(config-if)
switchport port-security aging {static | time time| type {absolute | inactivity}}
```

Parameter	Description
static	• Enable aging for statically configured secure addresses on this port.
time time	• Specify the aging time for this port. • The range is 0 to 1440 minutes. • If the time is 0, aging is disabled for this port.
type absolute	• Set the absolute aging time. All the secure addresses on this port age out exactly after the time (in minutes) specified and are removed from the secure address list.
type inactivity	• Set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Sécurité du port avec téléphones IP

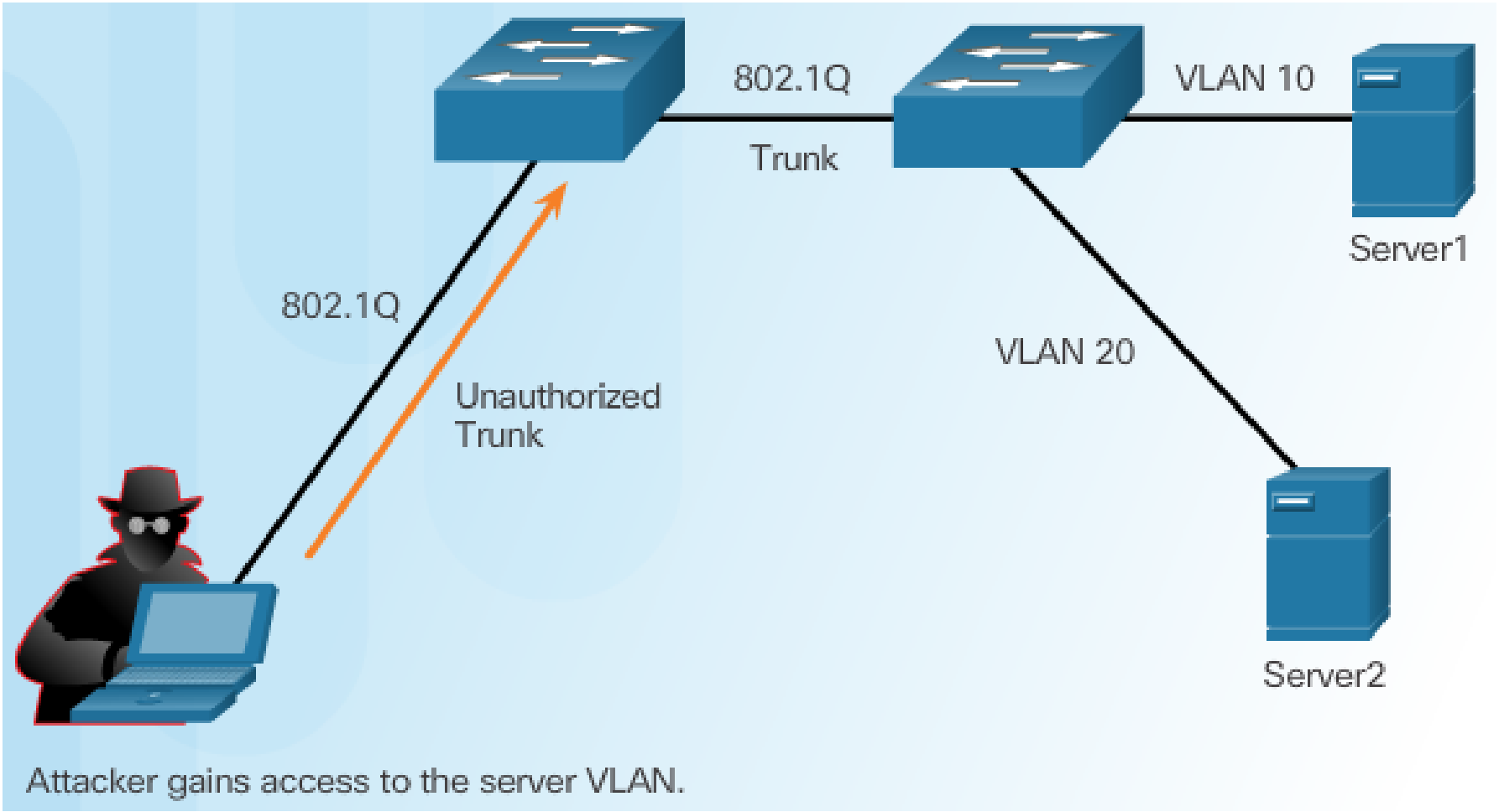

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 3
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# switchport port-security aging time 120
S1(config-if)#
```

SNMP MAC Adresse de Notification

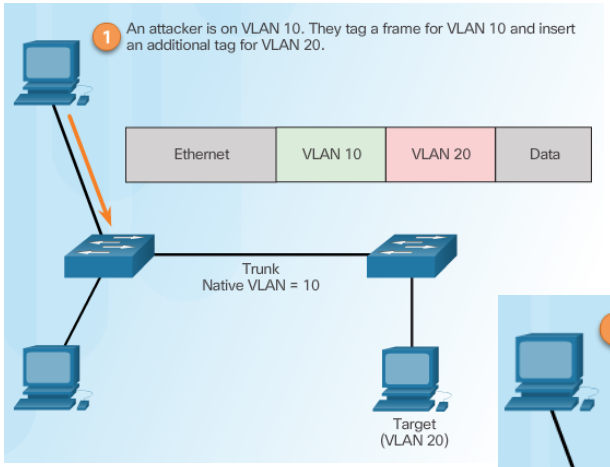


Sujet 6.2.4:
Atténuer les attaques VLAN

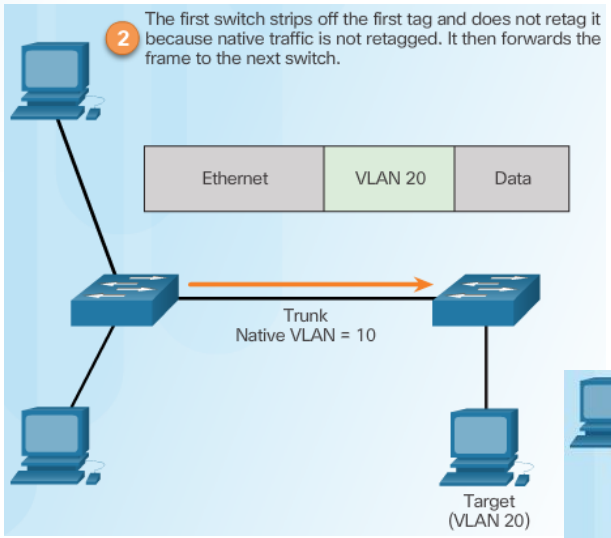
Attaques de VLAN Hopping



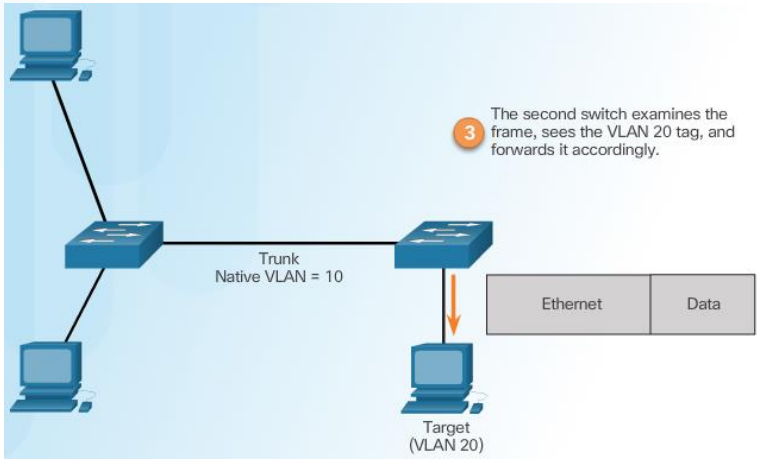
Les attaques VLAN Double-Tagging



Étape 1 - Double attaque de marquage

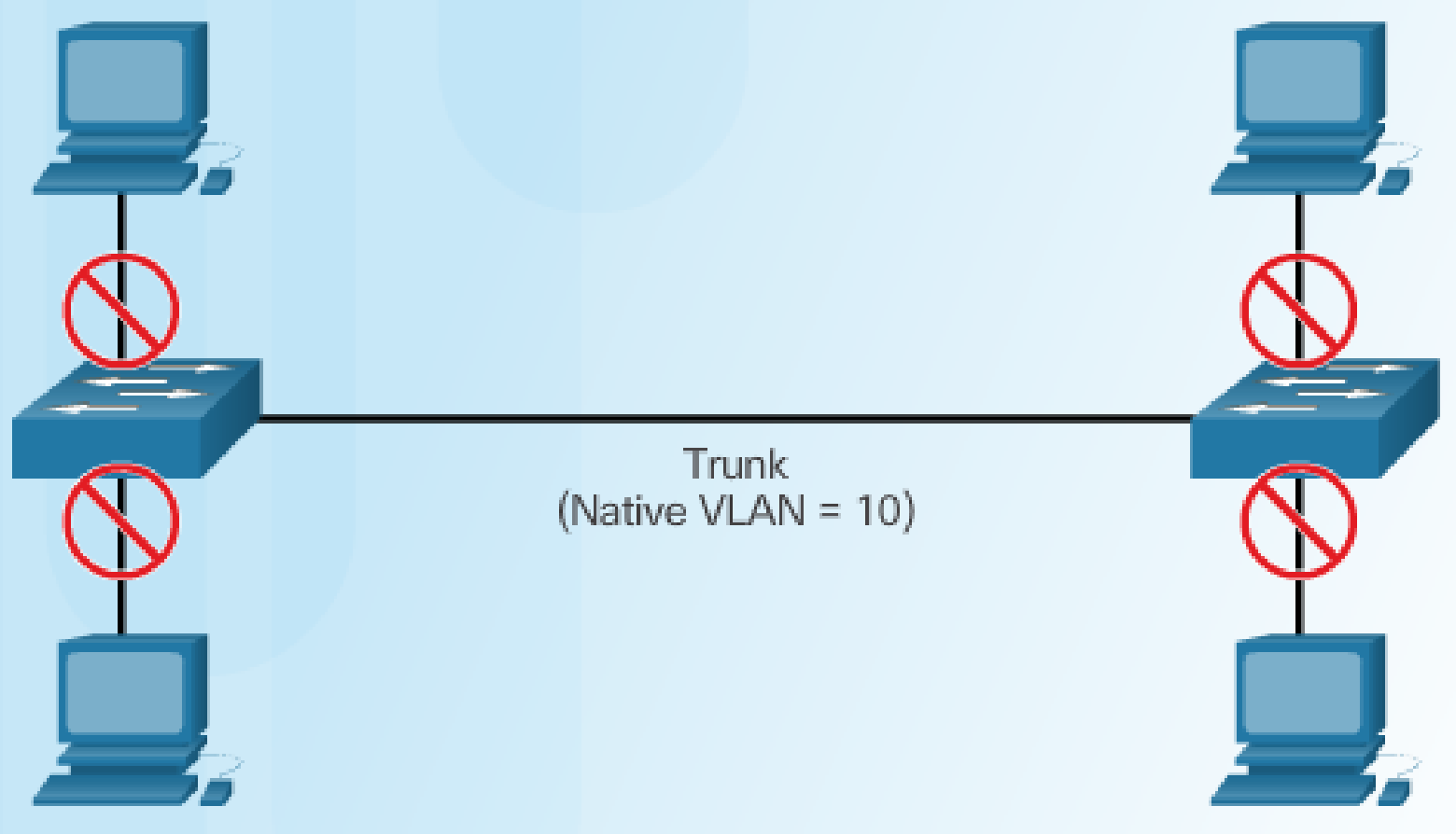


Étape 2 - Double attaque de marquage

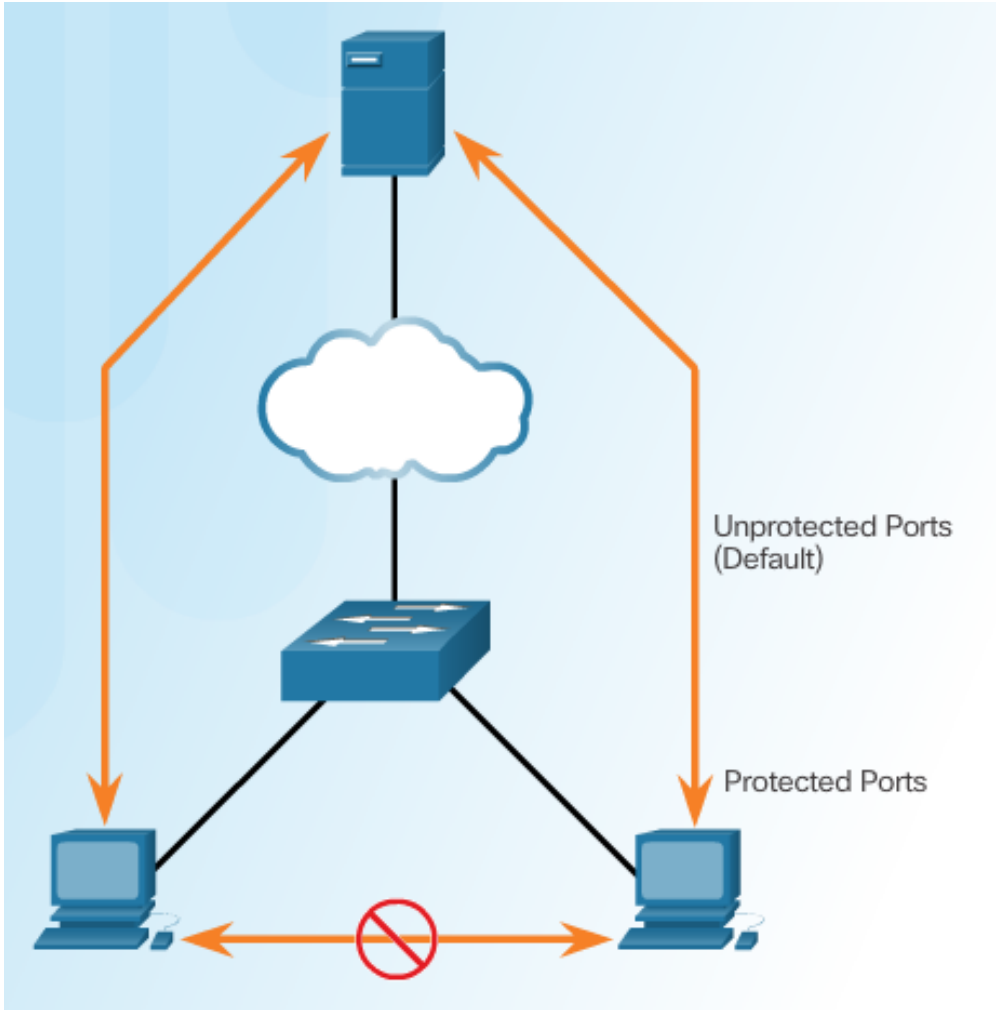


Étape 3 - Double attaque de marquage

Atténuer les attaques de VLAN Hopping



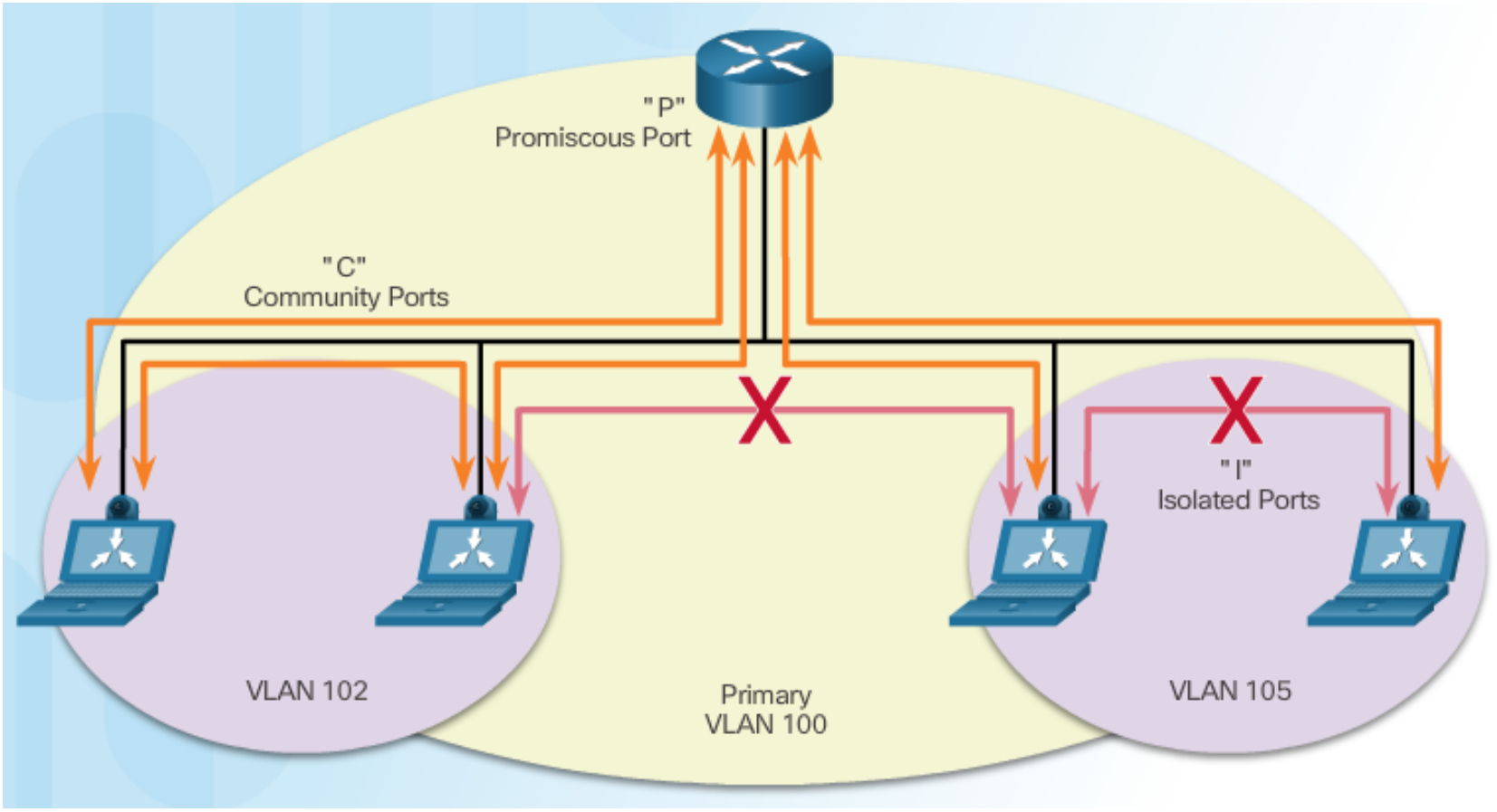
Caractéristique de bord PVLAN



Vérification des ports protégés

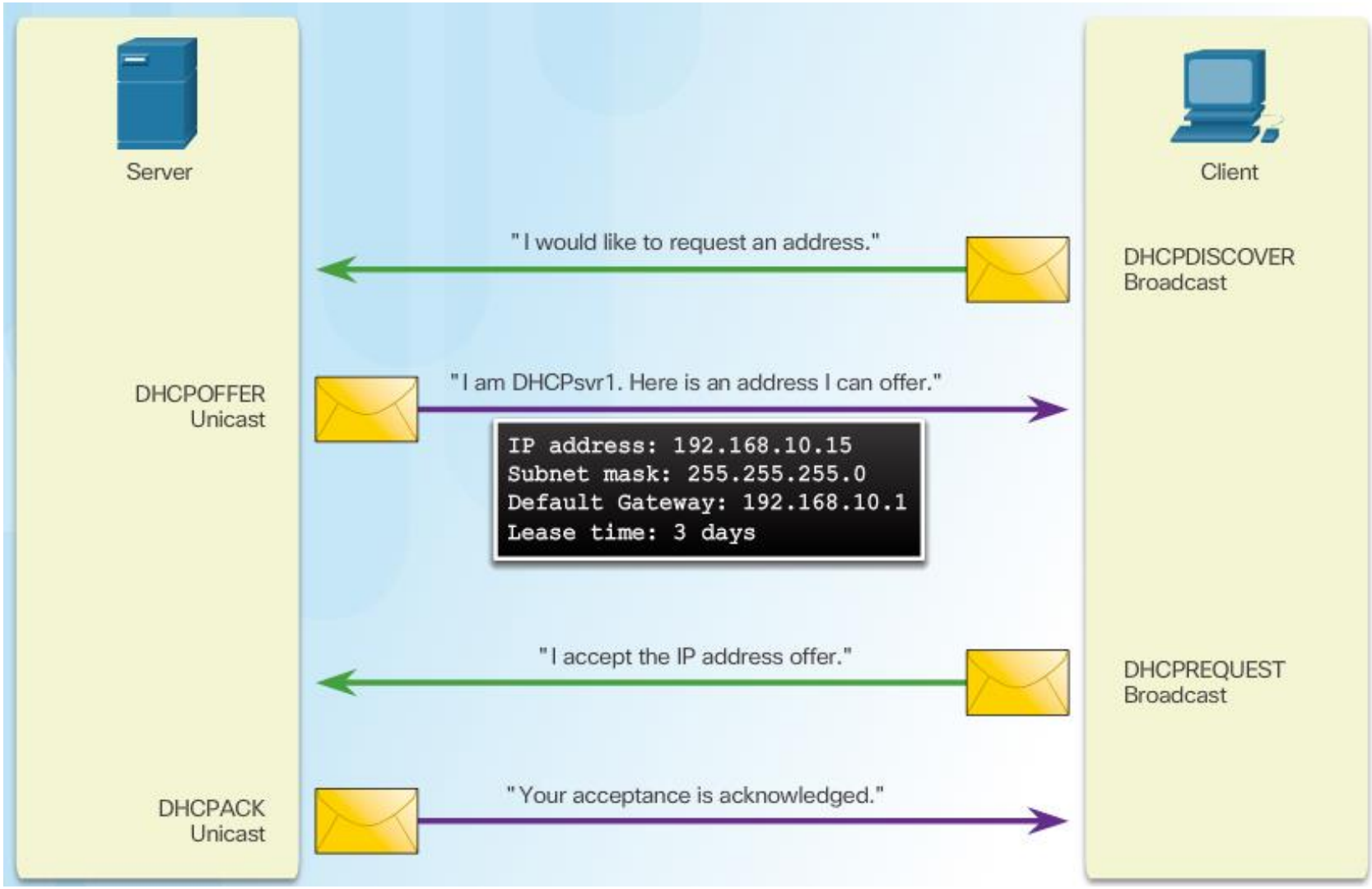
```
Switch# show interfaces gigabitethernet1/0/1 switchport
Name: G1/0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
<output omitted >
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

Voice VLAN: none (Inactive)
Appliance trust: none
```

VLAN privés



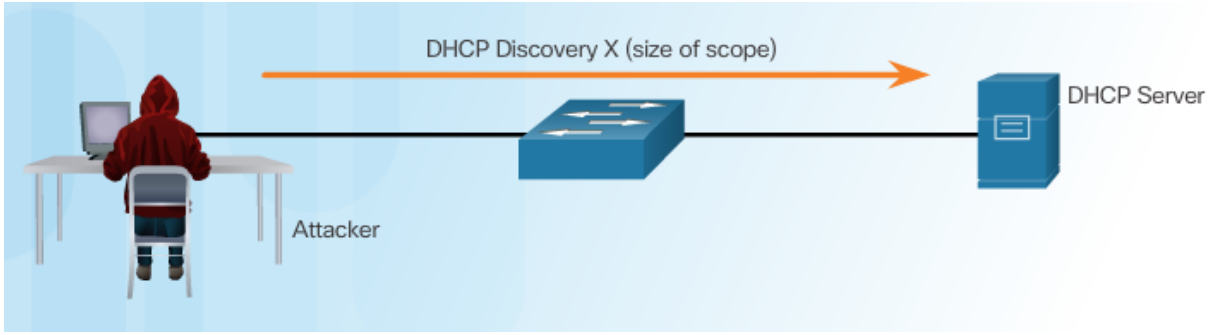
Sujet 6.2.5:
Atténuer les attaques DHCP

Les attaques de DHCP Spoofing

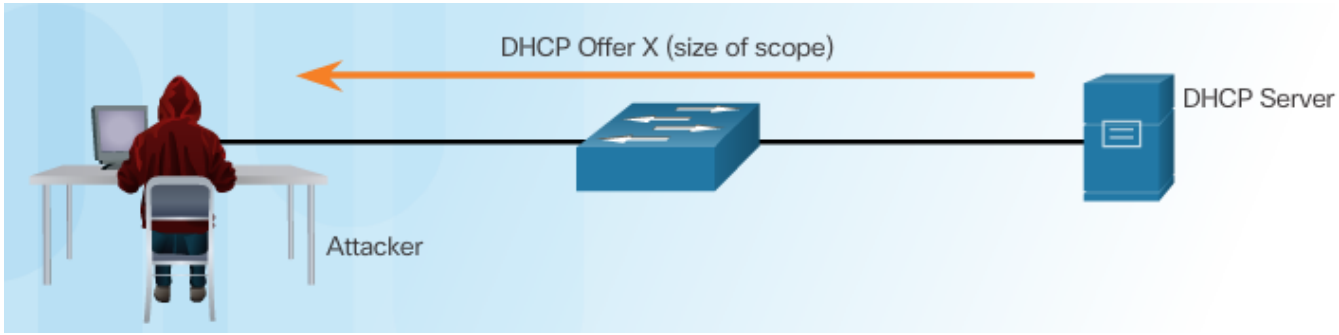


Attaque DHCP Starvation

L'attaquant lance une attaque de famine

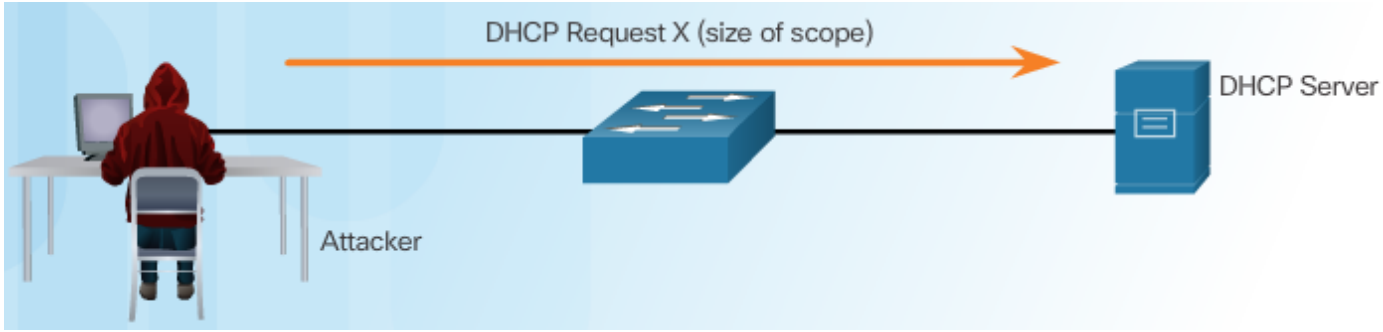


Le serveur DHCP offre des paramètres

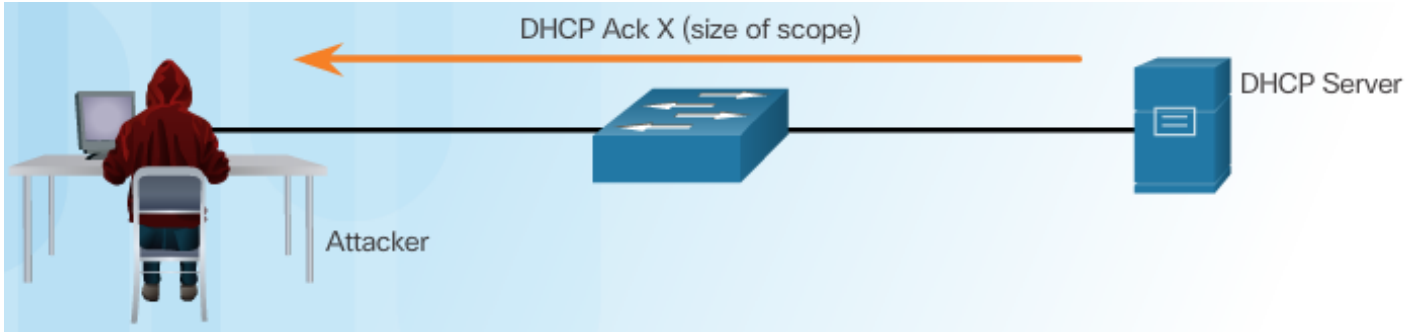


Attaque DHCP Starvation

Le client demande toutes les offres



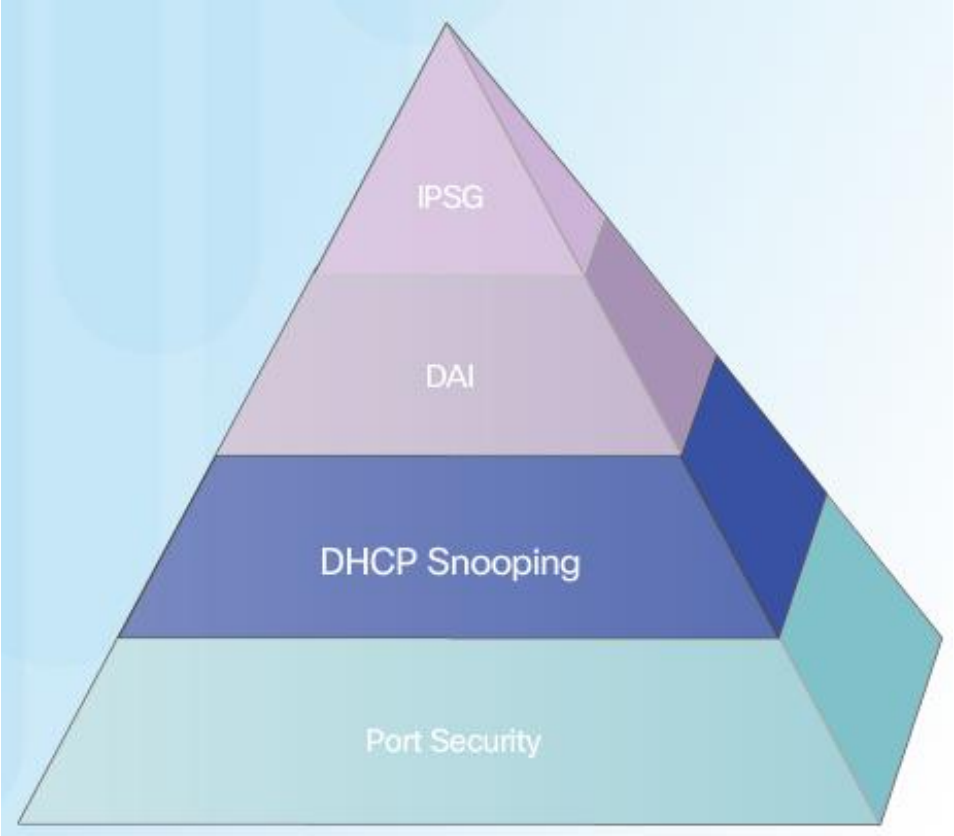
Le serveur DHCP reconnaît toutes les demandes



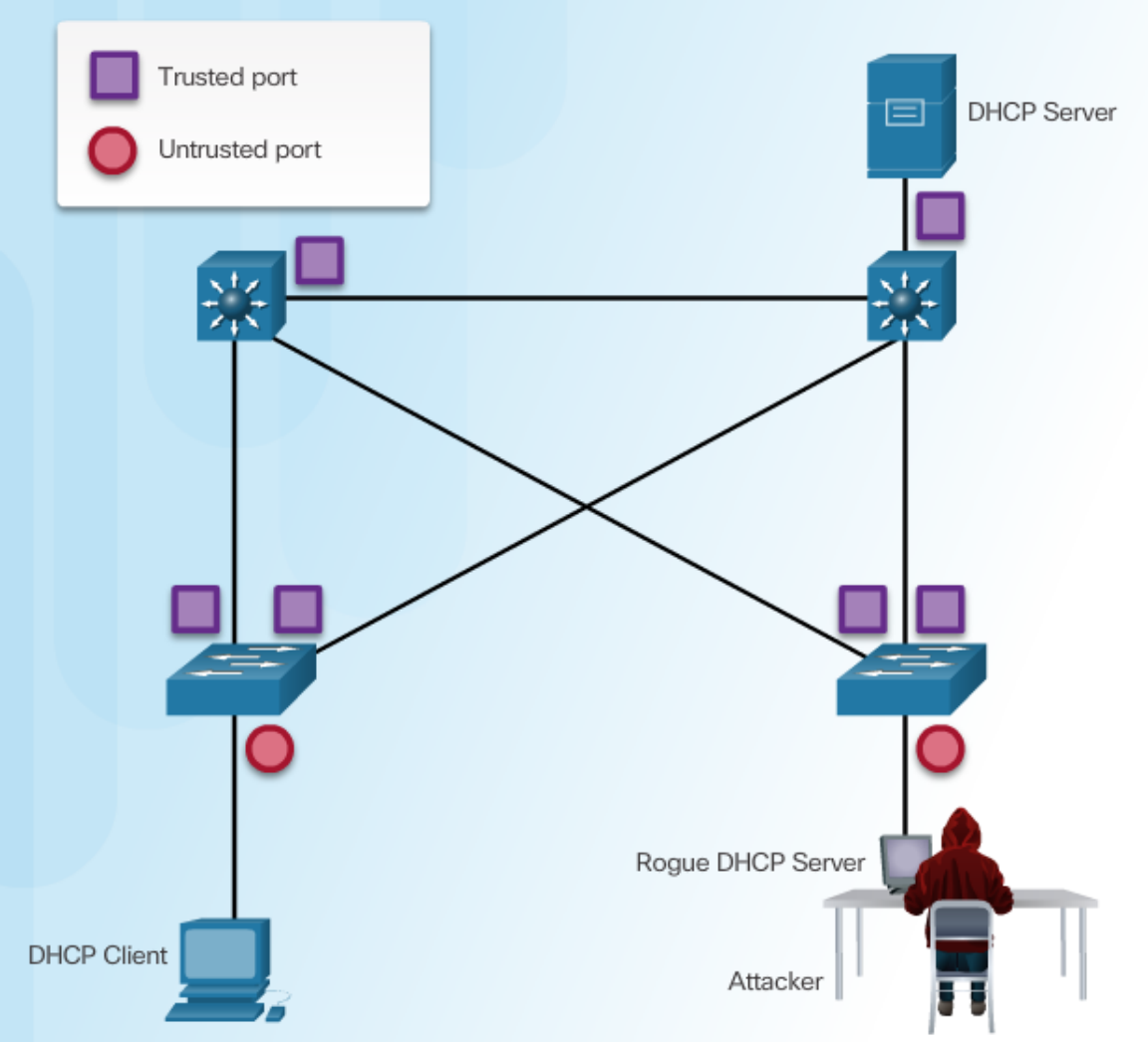
Atténuer les attaques VLAN

Le commutateur refuse les paquets contenant des informations spécifiques:

- Messages du serveur DHCP non autorisés à partir d'un port non approuvé
- Les messages client DHCP non autorisés ne respectent pas la table de liaison de snooping ou les limites de taux
- Paquets de relais-agent DHCP qui incluent des informations d'option-82 sur un port non approuvé

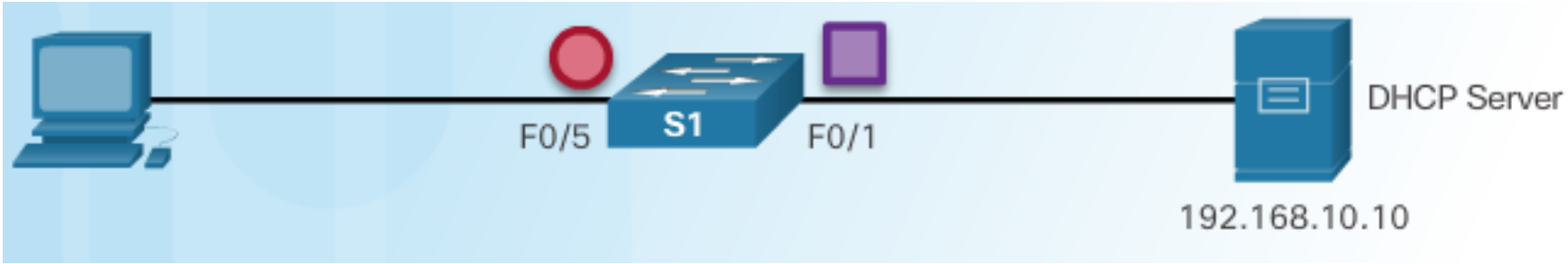


Configuration du snooping DHCP



Configuration de l'exemple de Snooping DHCP

La topologie de reference du DHCP Snooping



Configuration d'un nombre maximal d'adresses MAC

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

Configuration de l'exemple de Snooping DHCP

Vérification du snooping DHCP

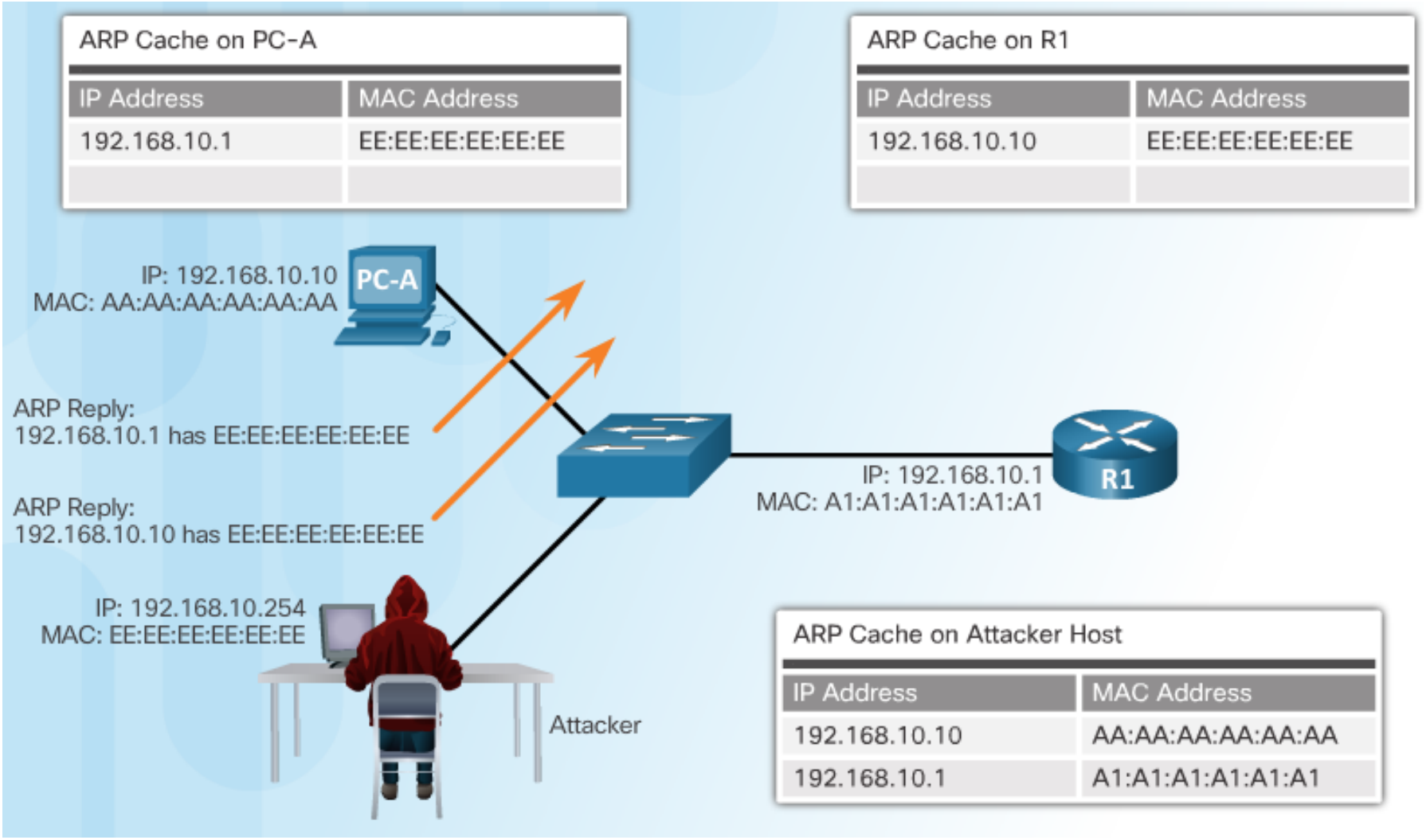
```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

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:

<output omitted>
```

Configuration d'un nombre maximal d'adresses MAC

```
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
```

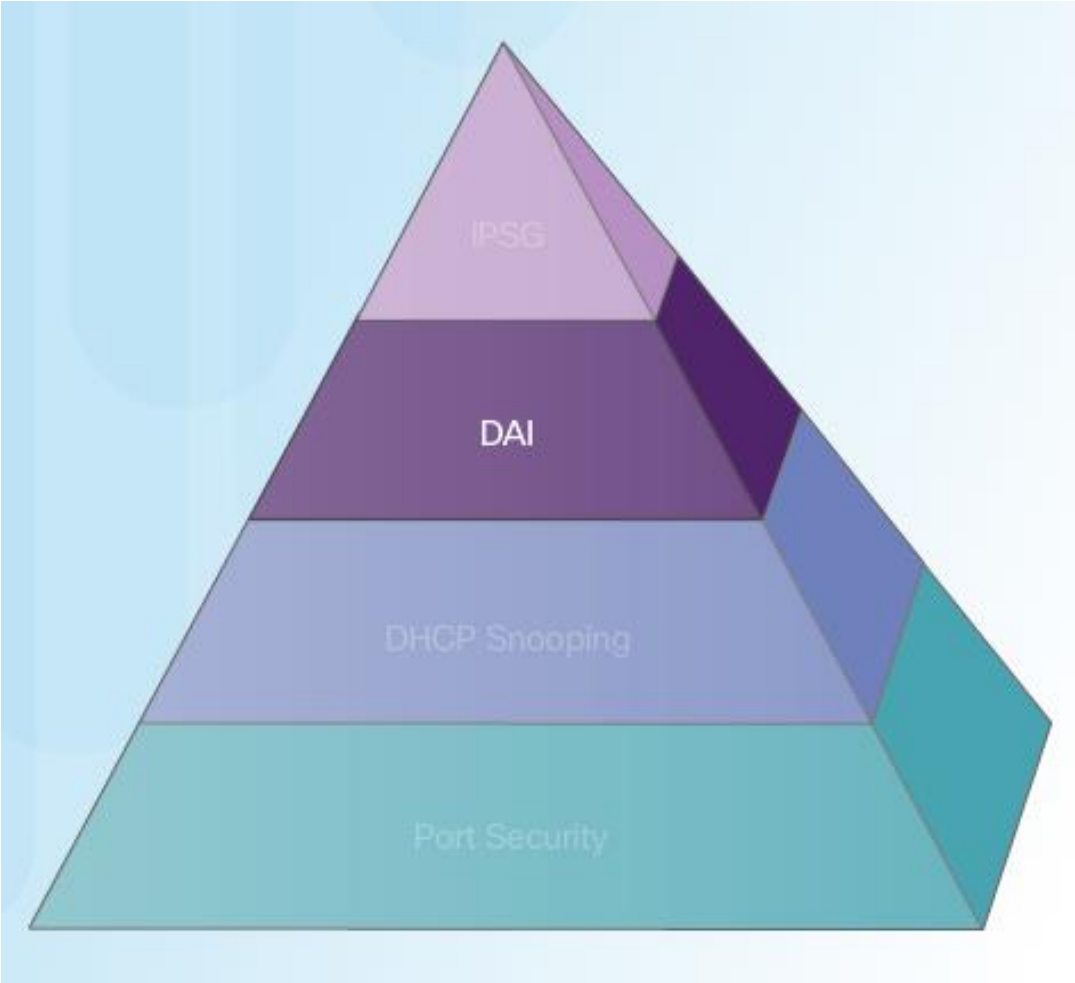
Sujet 6.2.6:
Atténuer les attaques ARP

ARP Spoofing et ARP Intoxication Attaque

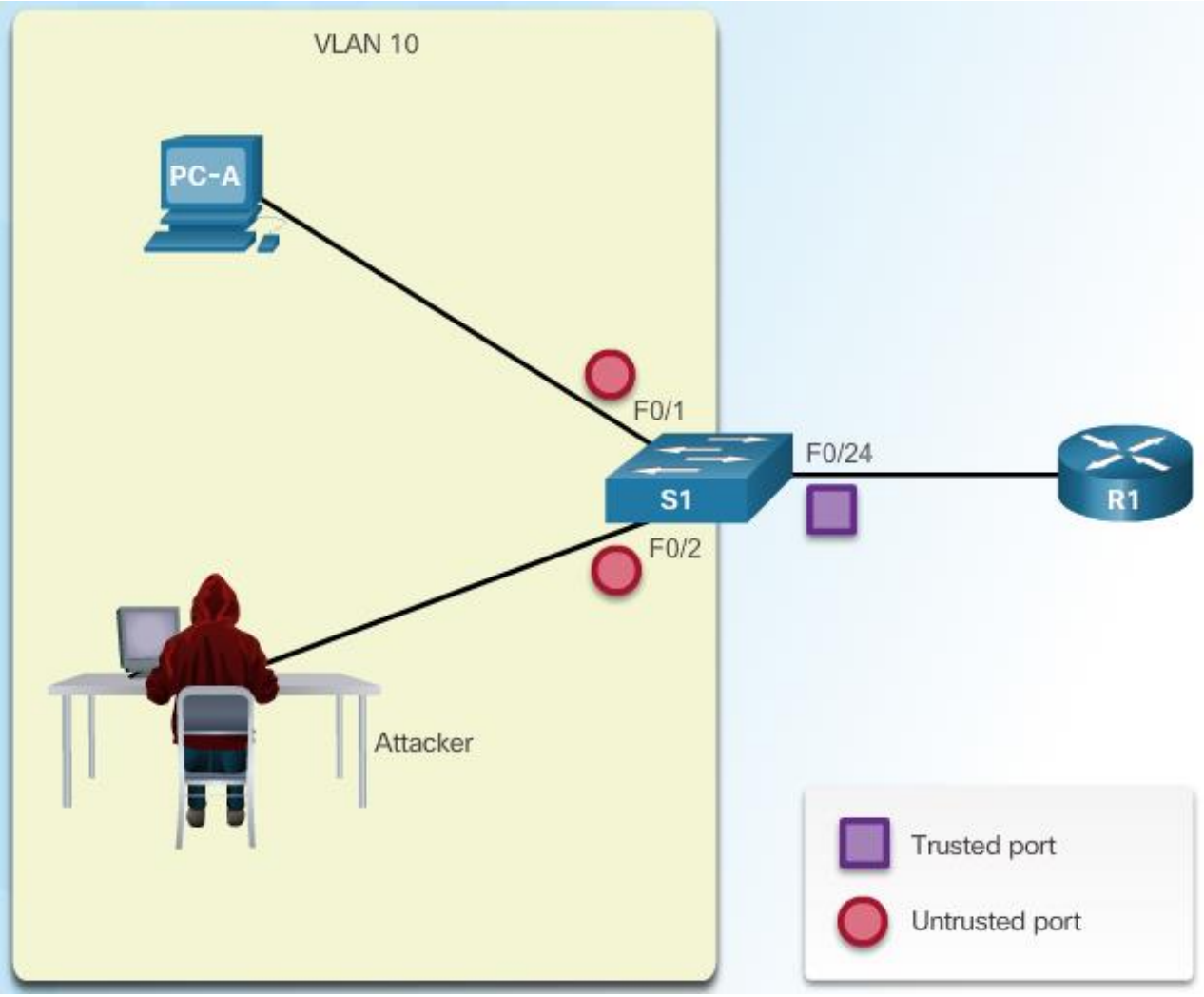


Atténuer les attaques ARP

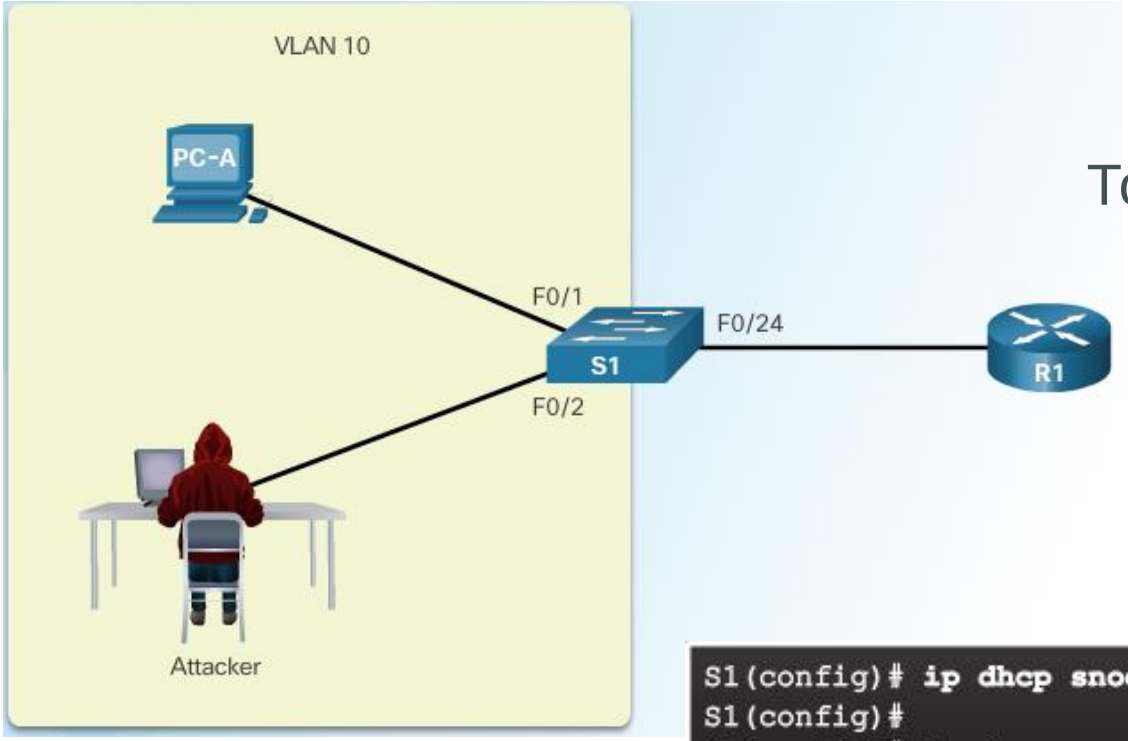
Inspection Dynamique ARP:



Configuration de l'inspection Dynamique ARP



Configuration de l'exemple de Snooping DHCP



Topologie de référence ARP

Configuration de l'inspection Dynamique ARP

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

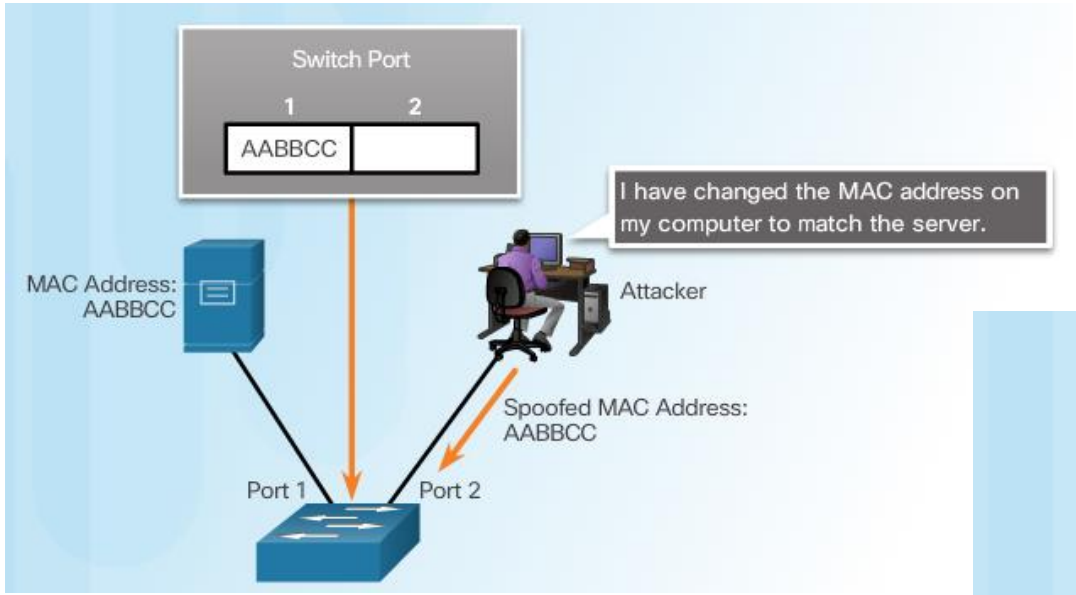
Configuration de l'exemple de Snooping DHCP

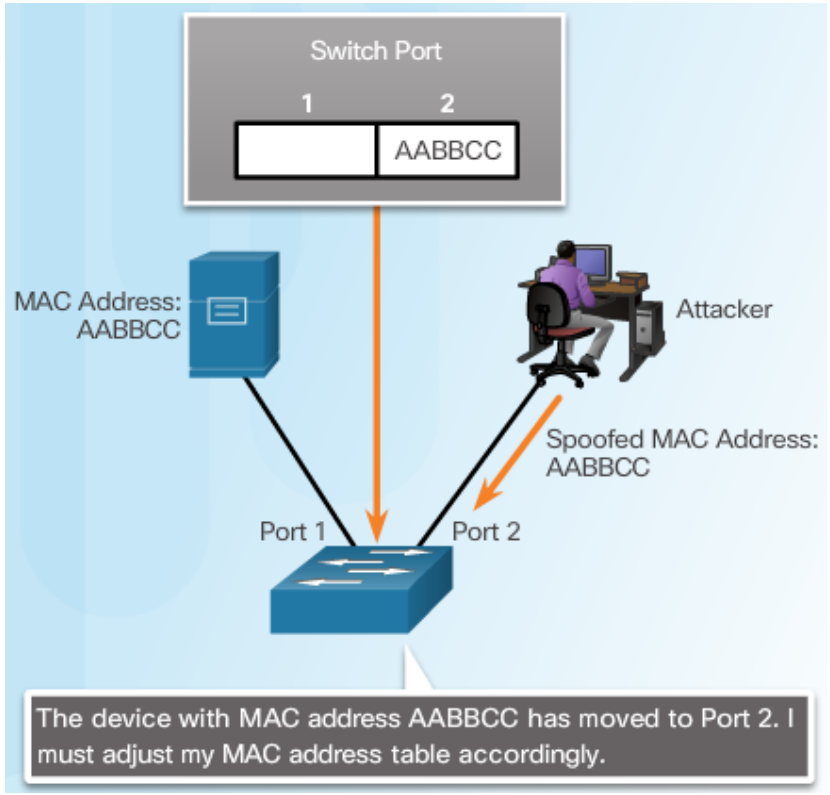
Vérification de la source, de la destination et de l'IP

```
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)#
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)#
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)#
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```

Sujet 6.2.7:
Attaques d'atténuation des attaques d'adresse

Attaque Spoofing d'adresse

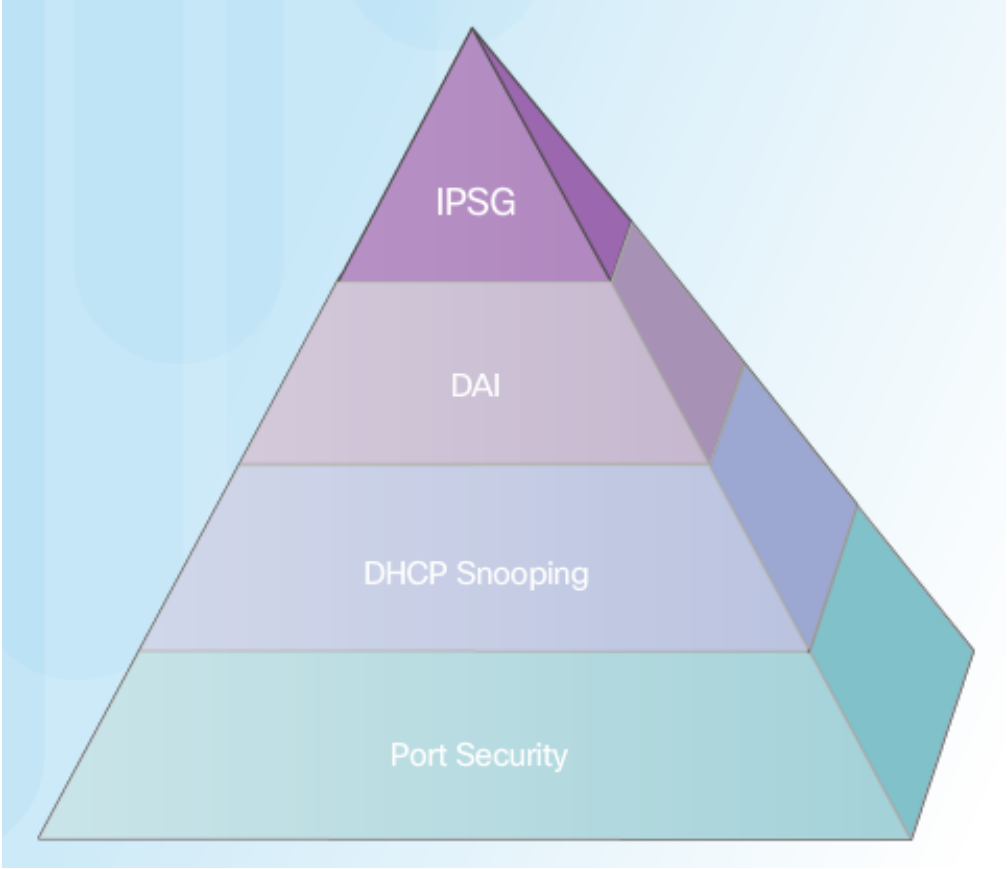




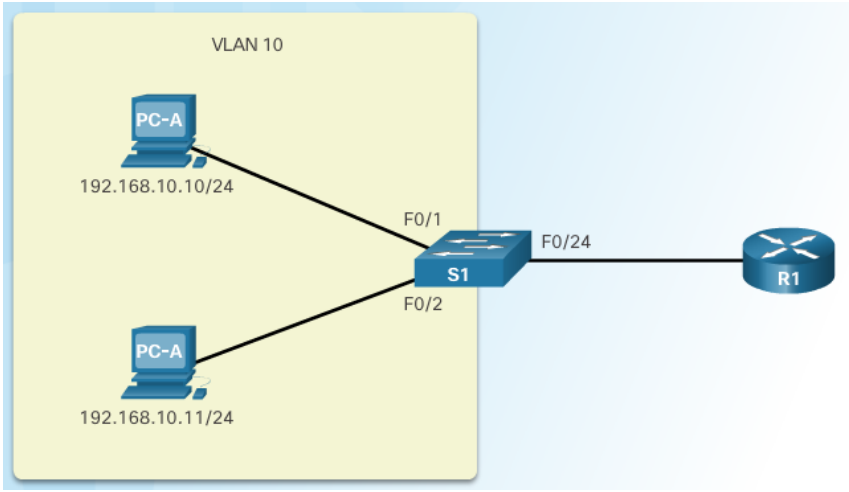
Attaques d'atténuation des attaques d'adresse

Pour chaque port non approuvé, il existe deux niveaux possibles de filtrage de sécurité de trafic IP:

- Filtre d'adresse IP source
- Filtre d'adresse IP et d'adresse MAC



Configurer IP Source Guard



Topologie de référence du IP Source Guard

Configuration du IP Source Guard

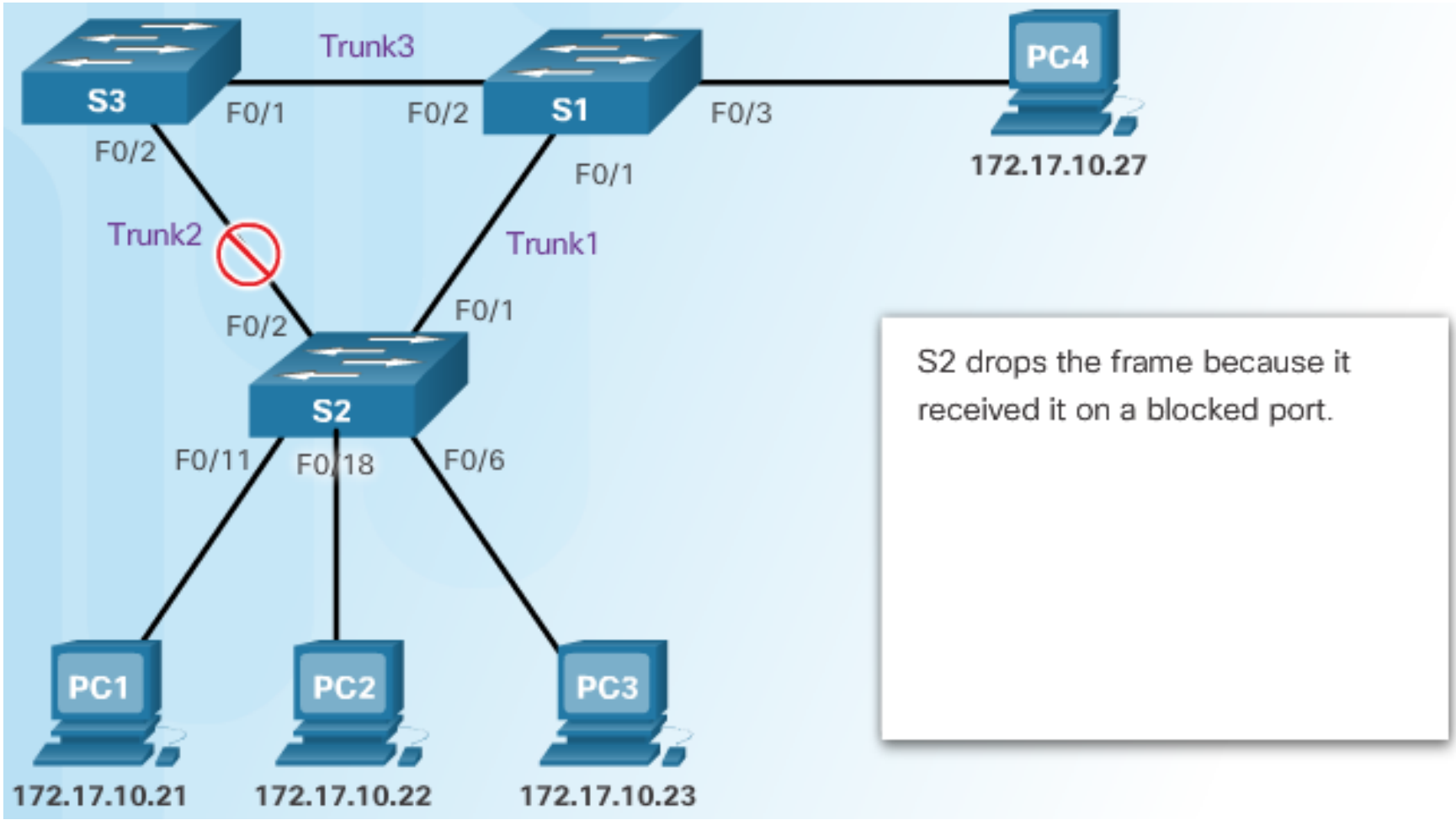
```
S1(config)# interface range fastethernet 0/1 - 2
S1(config-if-range)# ip verify source
S1(config-if-range)# end
S1#
```

Vérification du IP Source Guard

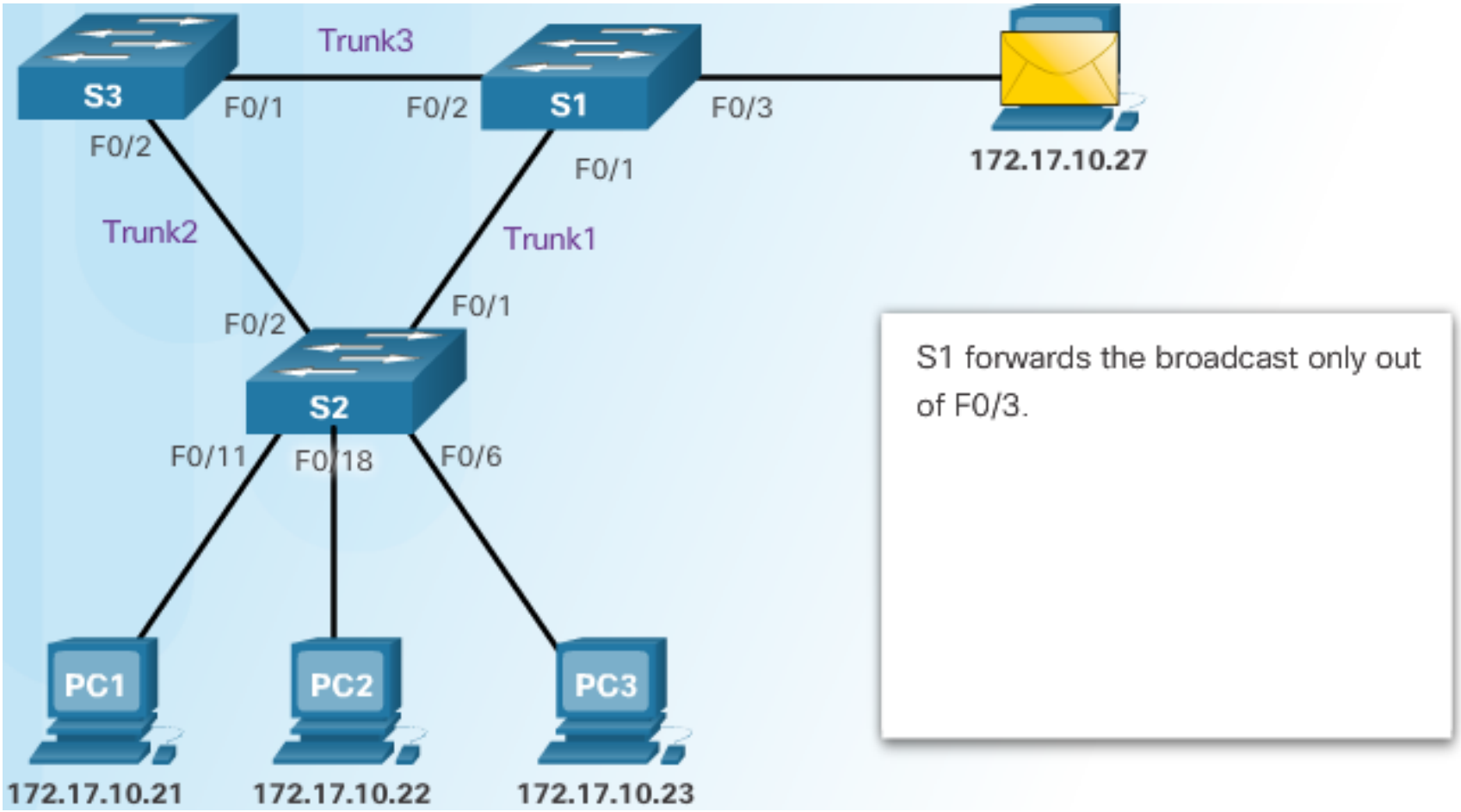
```
S1# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
F0/1       ip           active       192.168.10.10                       10
F0/2       ip           active       192.168.10.11                       10
S1#
```

Sujet 6.2.8:
Spanning Tree Protocol

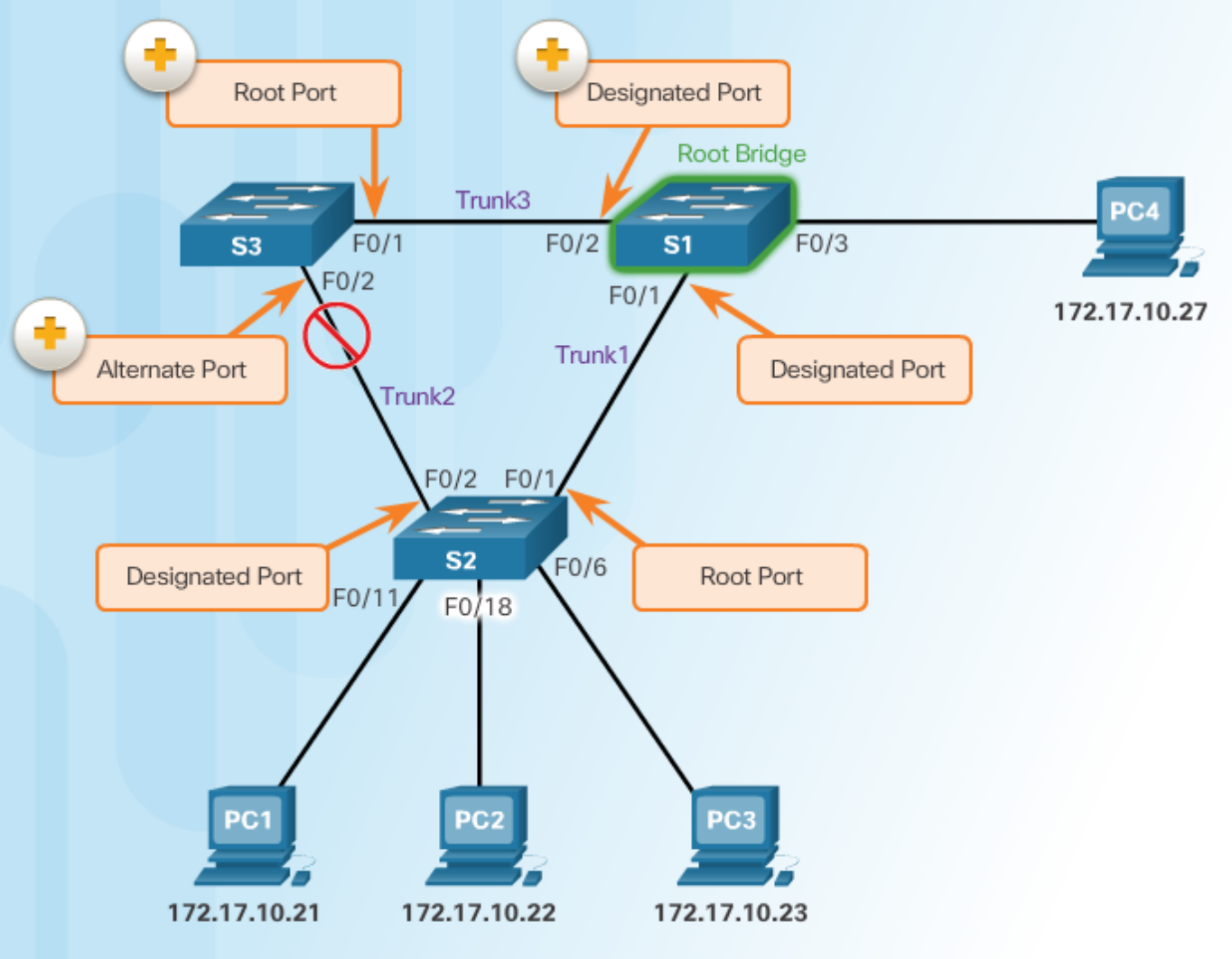
Introduction au protocole Spanning Tree



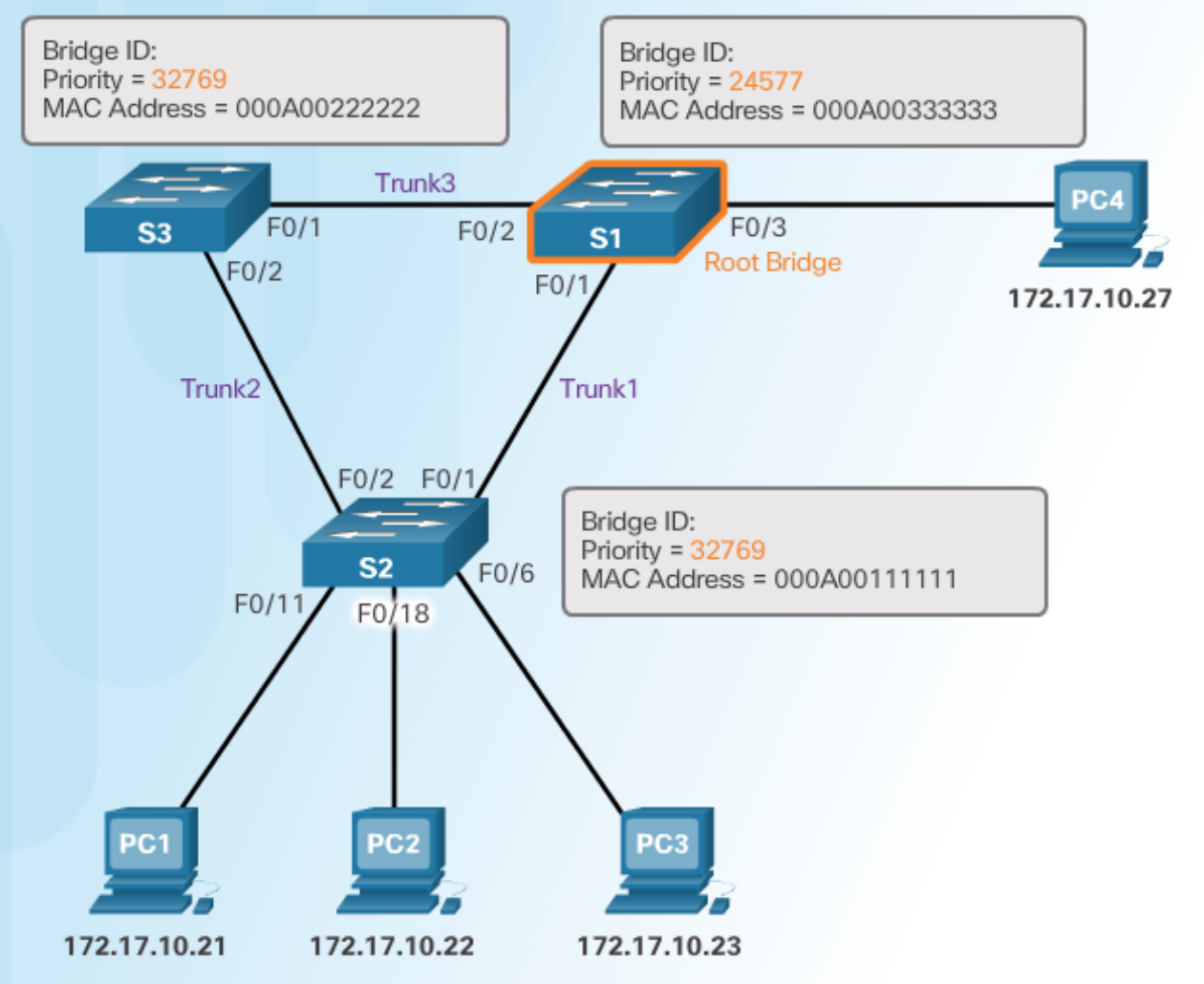
Diverses implémentations de STP



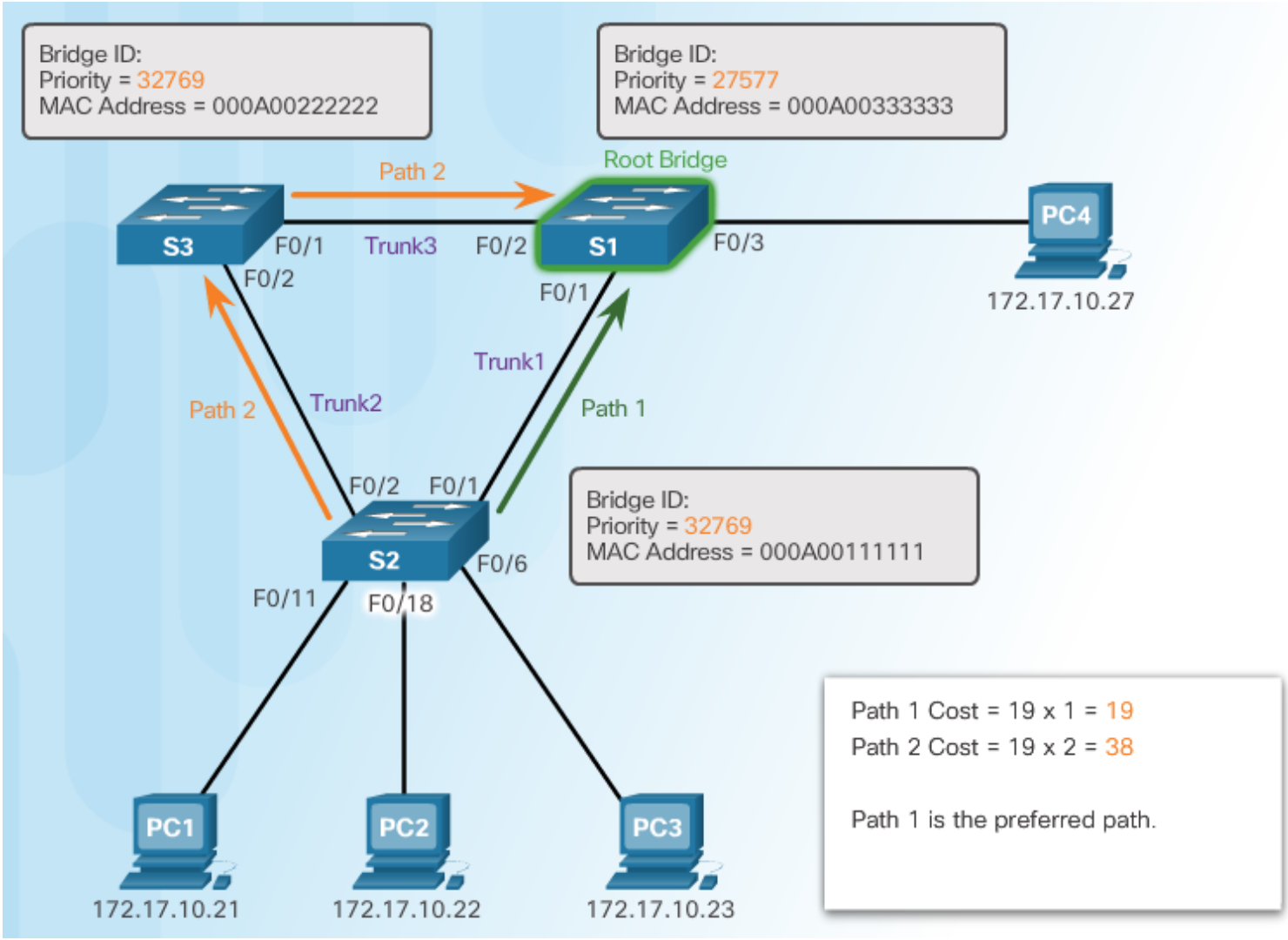
Rôles de port STP



Port racine STP



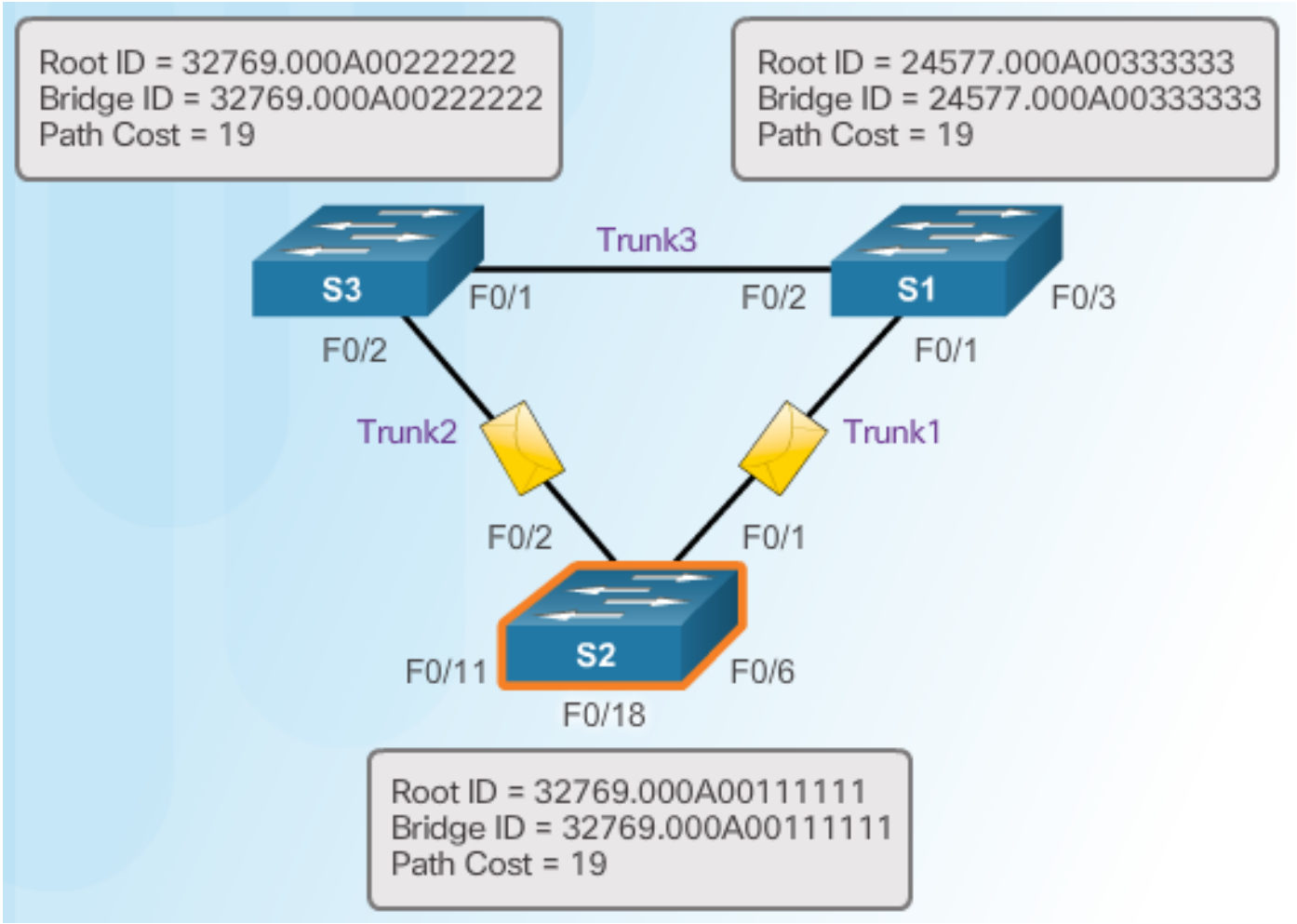
Coût du chemin STP



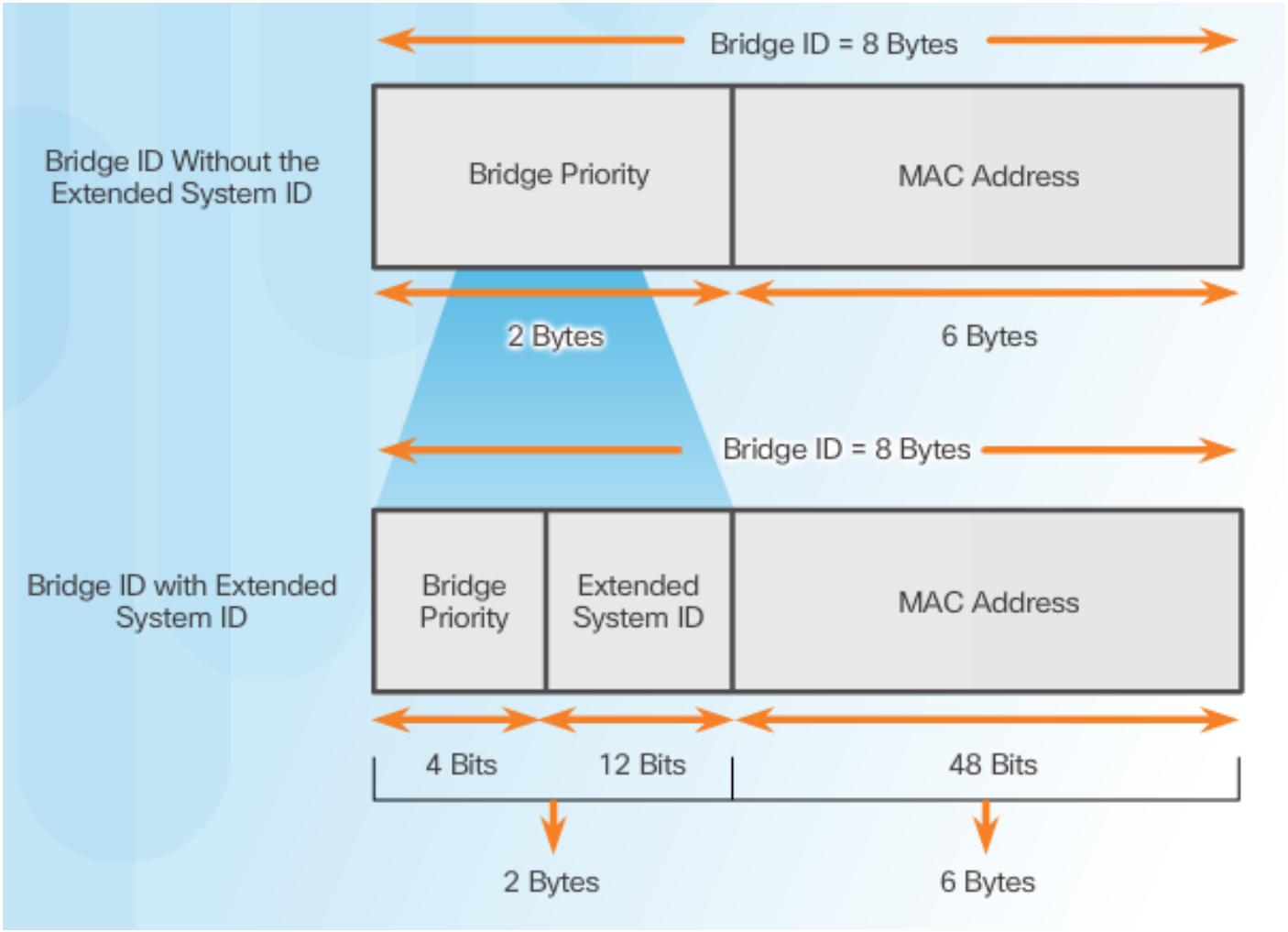
Format du trame BPDU 802.1D

Field Number	Bytes	Field
1-4	2	Protocol ID
	1	Version
	1	Message type
	1	Flags
5-8	8	Root ID
	4	Cost of path
	8	Bridge ID
	2	Port ID
9-12	2	Message age
	2	Max age
	2	Hello time
	2	Forward delay

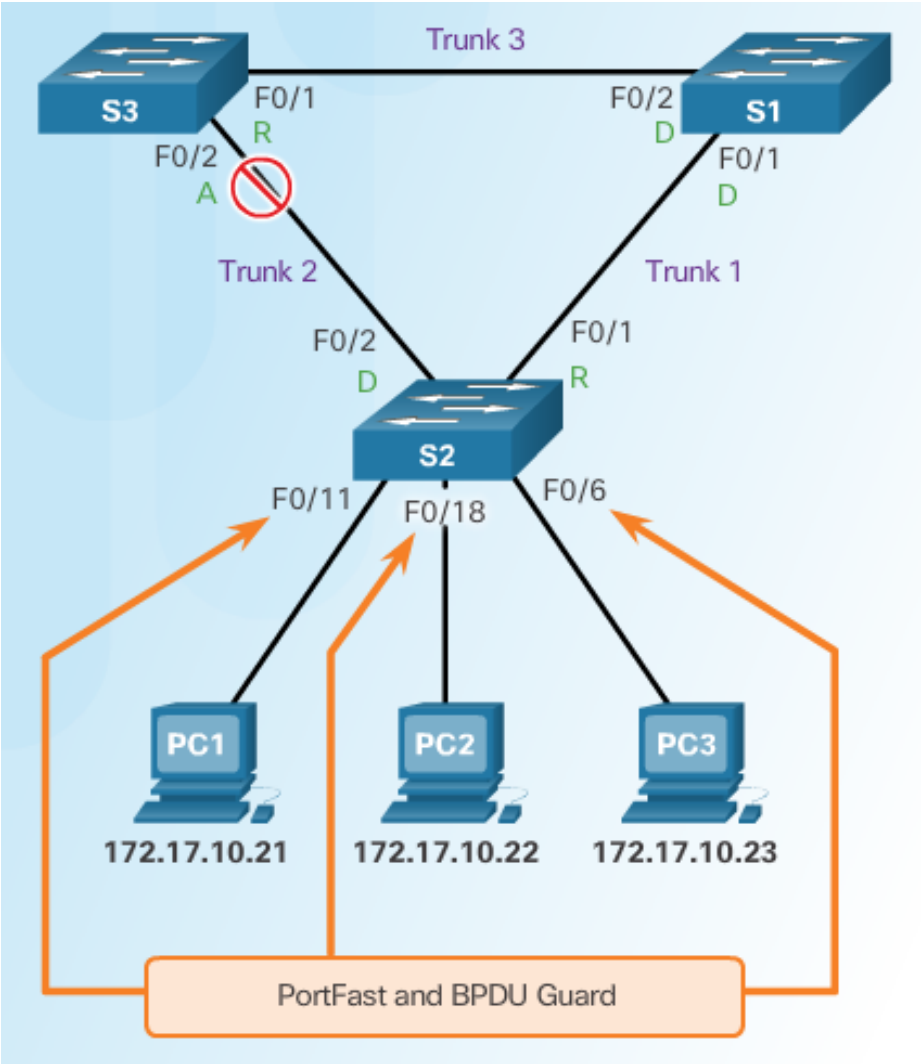
Propagation et processus de BPDU



ID de système étendu

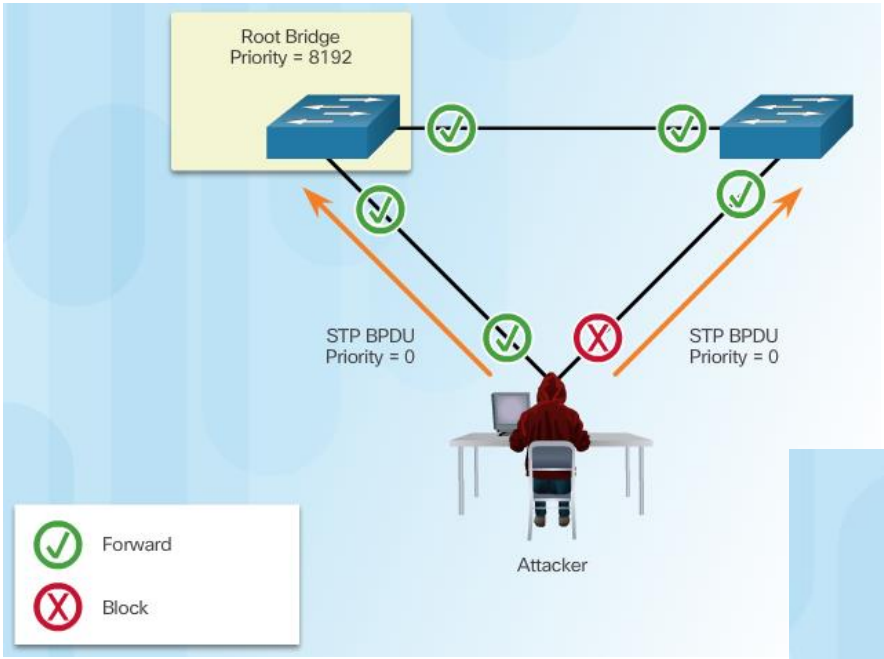


Sélectionnez le pont racine



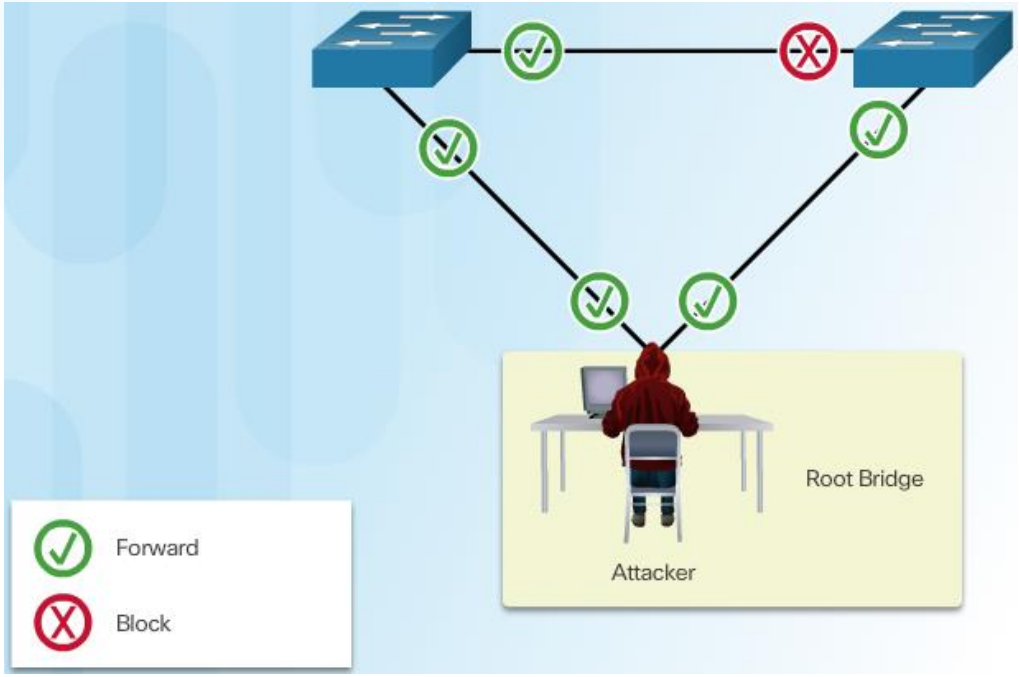
Sujet 6.2.9:
Atténuer les attaques STP

Attaques de manipulation STP

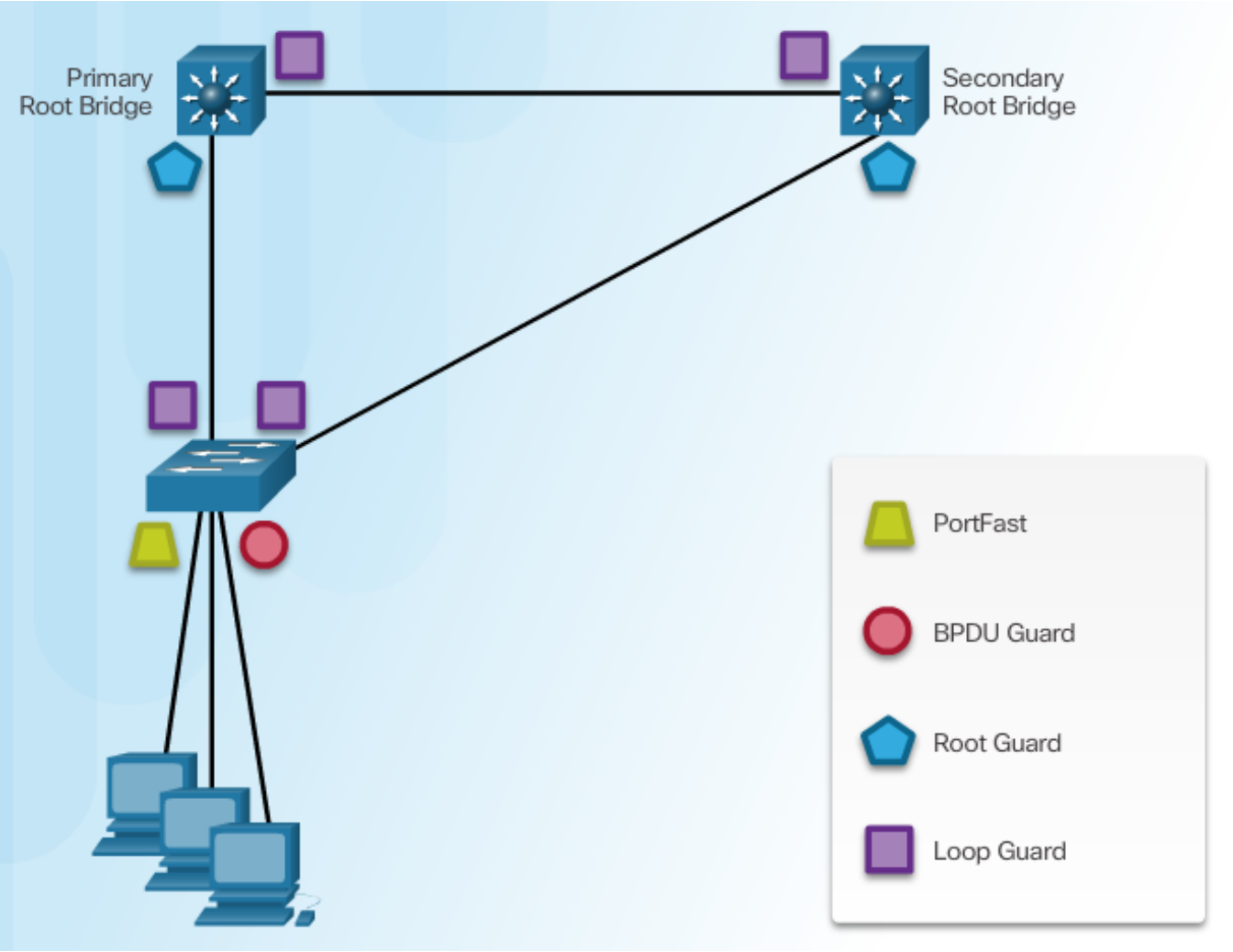


Spoofing le pont racine

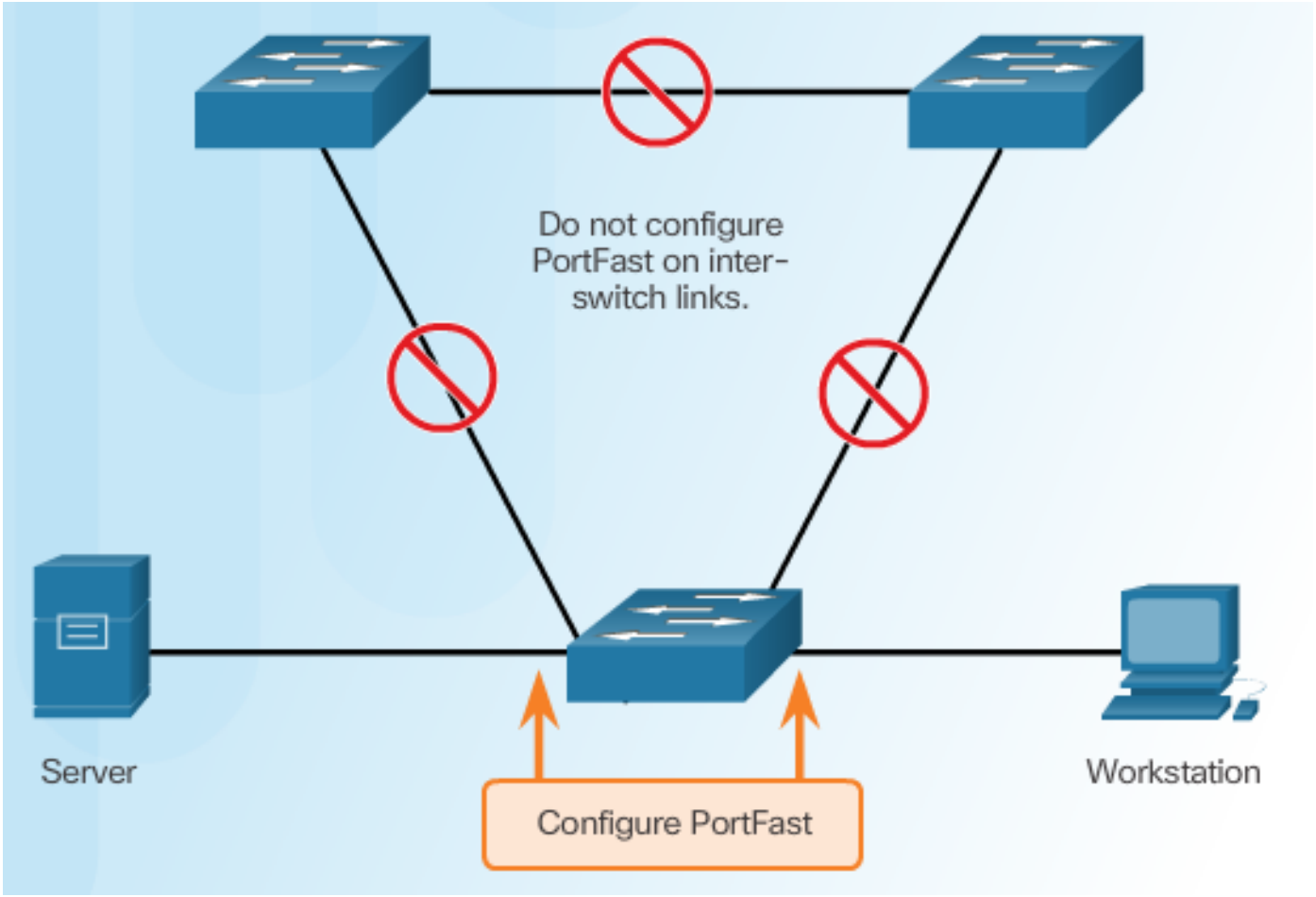
Attaque réussie de manipulation STP



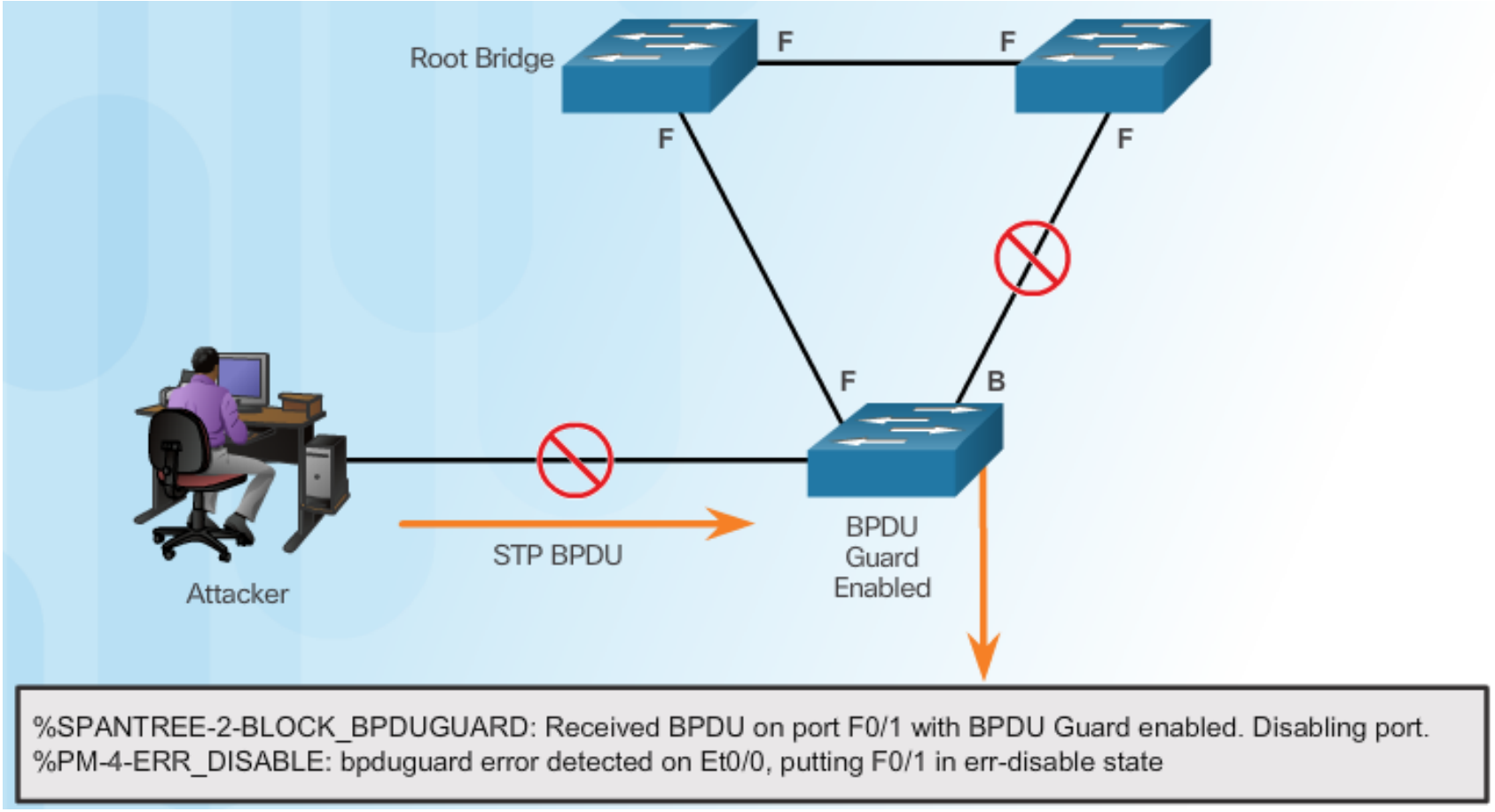
Atténuer les attaques STP



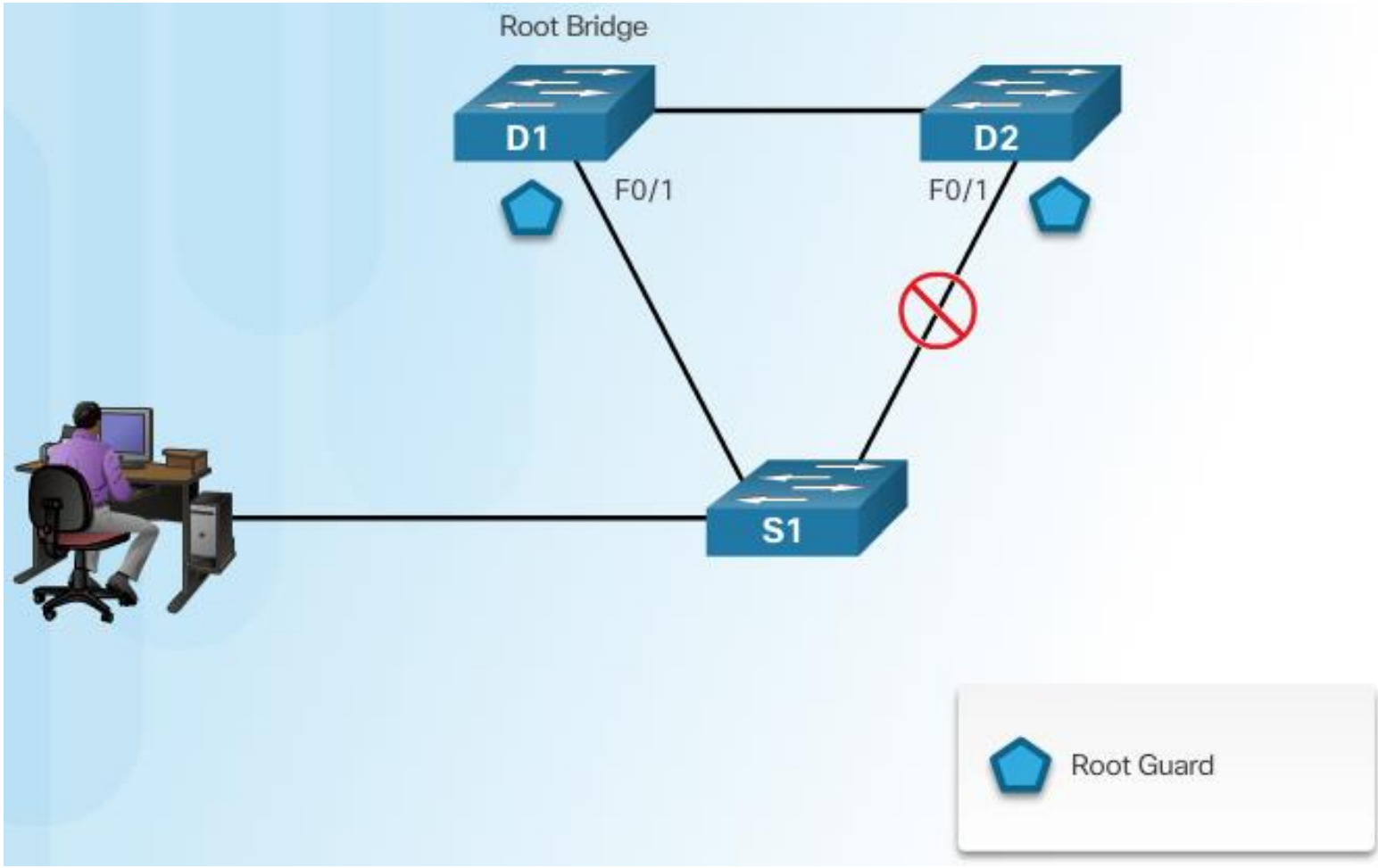
Configuration de PortFast



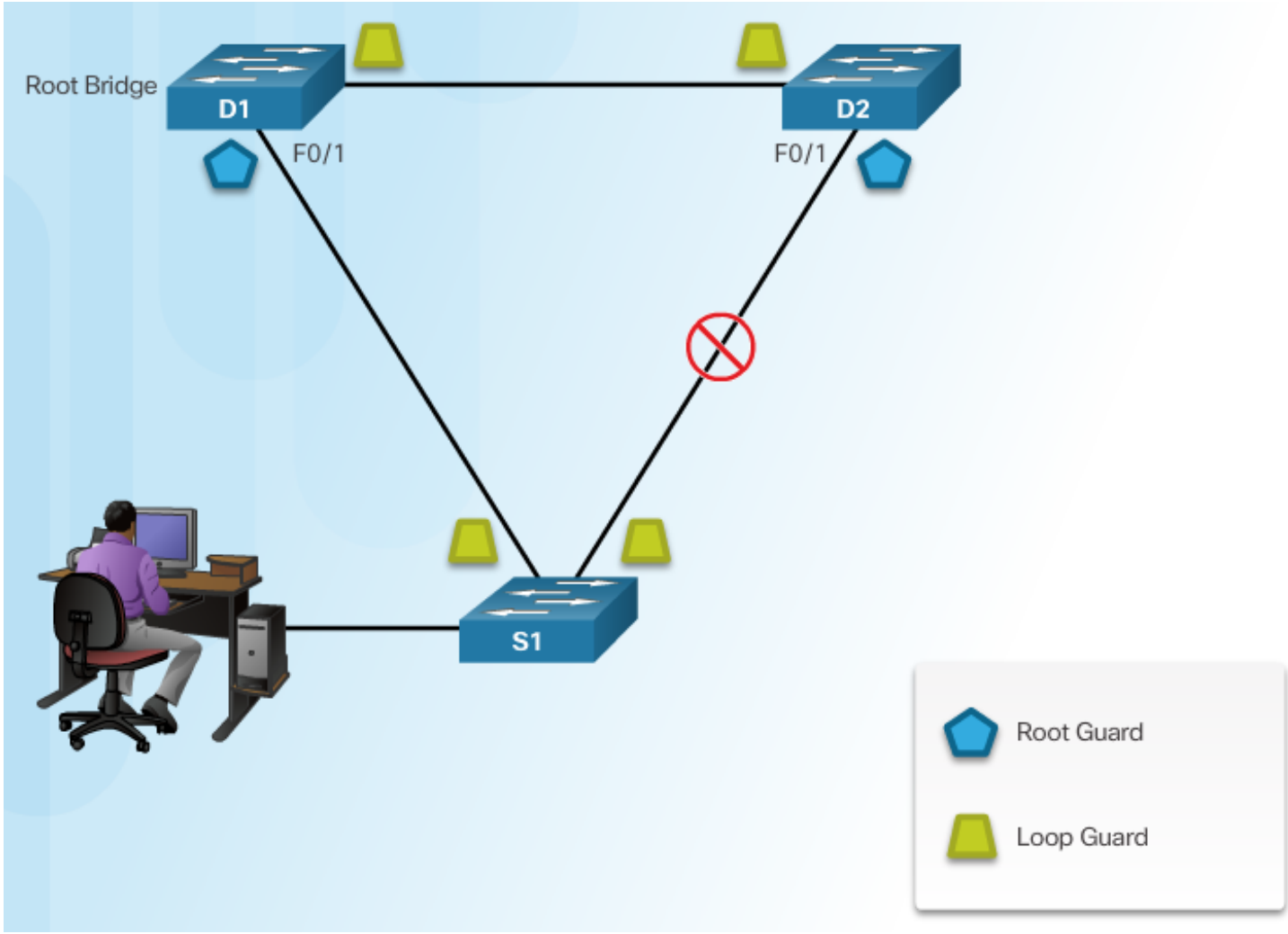
Configuration de BPDU Guard



Configuration de Root Guard



Configuration de Loop Guard



Section 6.3: Résumé

Objectifs du chapitre:

- Expliquez la sécurité des points d'extrémité.
- Décrivez différents types d'applications de sécurité de point d'extrémité.
- Décrivez les vulnérabilités de la couche 2.

Merci .

cisco Cisco Networking Academy

Mind Wide Open

Ressources de l'instructeur

- **Rappelez-vous**, il existe des tutoriels utiles et des guides d'utilisation disponibles via votre page d'accueil NetSpace. (Https://www.netacad.com)
- Ces ressources couvrent une variété de sujets, y compris la navigation, les évaluations et les affectations.
- Une capture d'écran a été fournie ici en soulignant les tutoriels liés à l'activation des examens, à la gestion des évaluations et à la création de quiz.