

# Chapitre 5 : sécurité et surveillance du réseau

CCNA Routing and Switching  
Connecting Networks v6.0



# Chapitre 5 – Sections et objectifs

## ■ 5.1 Sécurité du réseau local

- Expliquer comment atténuer les attaques de sécurité LAN courantes.
- Décrire les attaques de sécurité LAN courantes.
- Expliquer comment utiliser les bonnes pratiques de sécurité pour réduire les attaques de sécurité LAN courantes.

## ■ 5.2 SNMP

- Configurer SNMP de manière à surveiller les opérations réseau sur un réseau de PME.
- Expliquer le fonctionnement du protocole SNMP.
- Configurer le protocole SNMP pour compiler des données de performance du réseau.

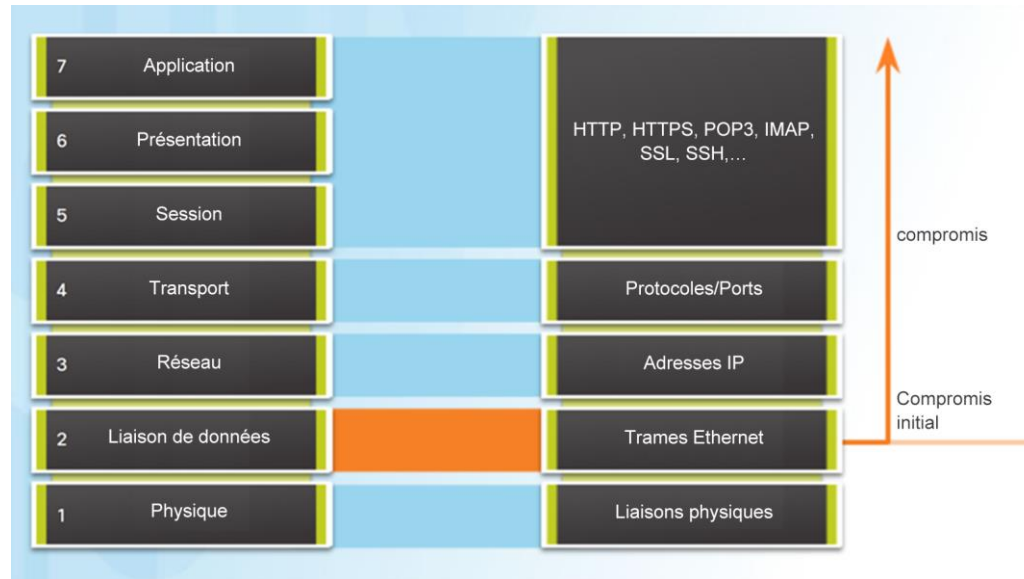
## ■ 5.3 Analyseur de port de commutateur Cisco (SPAN)

- Dépanner un problème réseau à l'aide de la fonction SPAN.
- Expliquer les fonctionnalités et les caractéristiques du protocole SPAN.
- Configurer une session SPAN locale
- Résoudre les problèmes liés à un trafic LAN suspect à l'aide du protocole SPAN.

# 5.1 Sécurité du réseau local

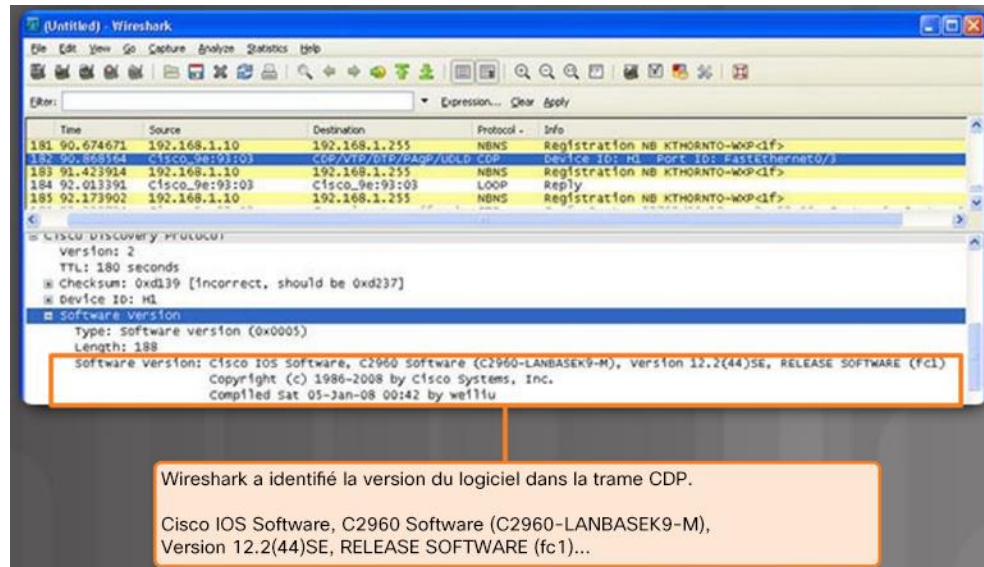
# Attaques LAN courantes

- Les solutions de sécurité classiques reposant sur des routeurs, des pare-feu, des systèmes de prévention des intrusions (IPS) et des périphériques VPN protègent les couches 3 à 7 du réseau.
- Mais la couche 2 doit également être protégée.
- Quelques exemples d'attaques de couche 2 courantes :
  - Attaque de reconnaissance de CDP
  - Attaques Telnet
  - Attaque par inondation (flooding) de table d'adresse MAC
  - Attaques de VLAN
  - Attaques DHCP



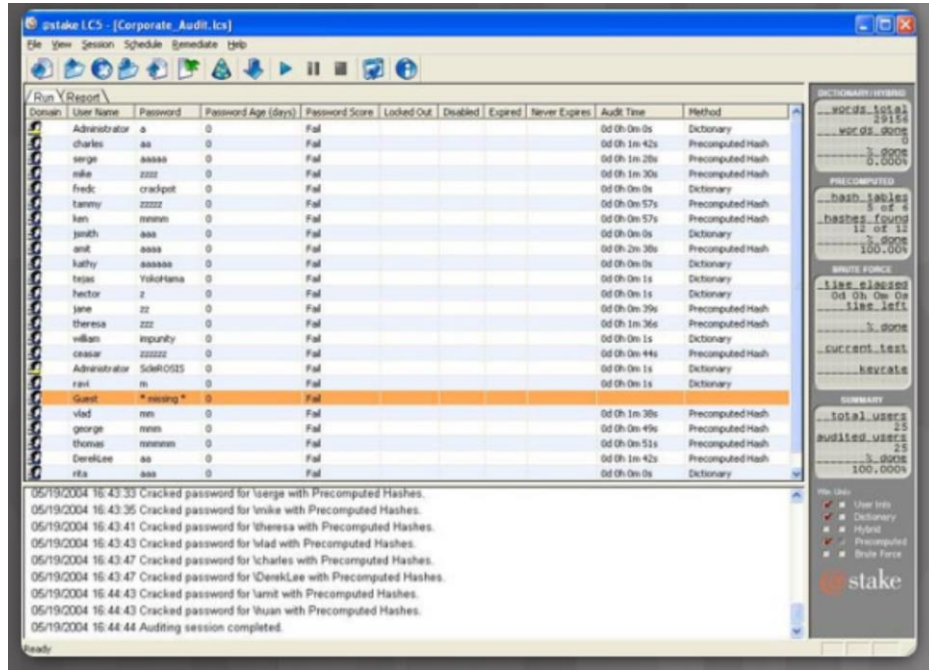
# Attaque de reconnaissance de CDP

- Le protocole CDP (Cisco Discovery Protocol) est un protocole propriétaire de découverte de liaison de couche 2 qui est activé par défaut.
- Le protocole CDP permet de détecter automatiquement d'autres périphériques CDP.
- Les informations relatives à CDP peuvent être utilisées par un hacker.
- Utilisez la commande **no cdp run** en mode de configuration globale pour désactiver le protocole CDP de manière globale.
- Utilisez la commande **no cdp enable** en mode de configuration d'interface pour désactiver le protocole CDP sur un port.



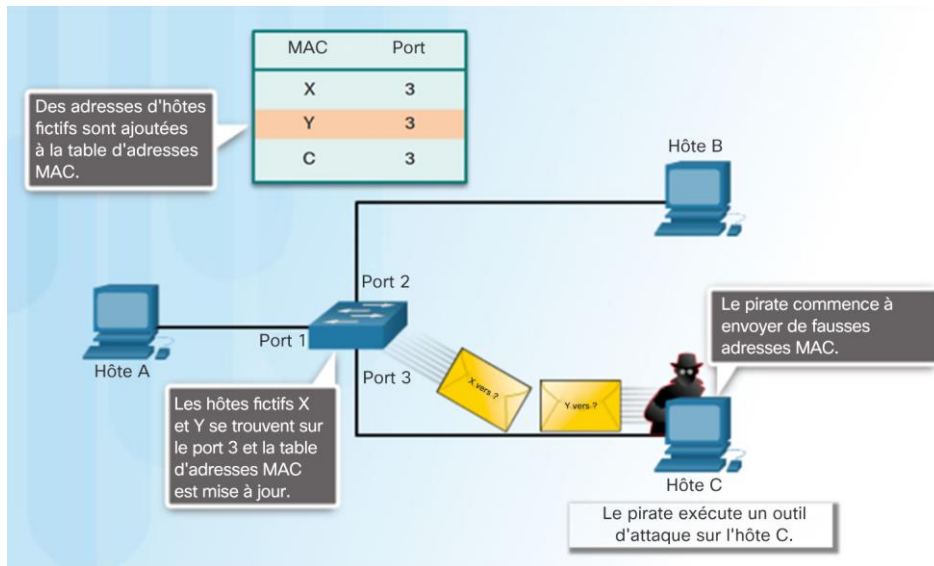
# Attaques de sécurité LAN

## Attaques Telnet



- On distingue deux types d'attaques Telnet :
  - Attaque de mot de passe par force brute** : attaque par force brute utilisée pour obtenir le mot de passe d'administrateur.
  - Attaque DoS Telnet** : un hacker envoie sans cesse des demandes de connexion Telnet pour tenter de rendre le service Telnet indisponible.
- Pour neutraliser ces attaques :
  - Utiliser SSH
  - Utilisez des mots de passe forts que vous modifierez fréquemment.
  - Limitez l'accès aux lignes vty à l'aide d'une liste de contrôle d'accès.
  - Utilisez AAA avec le protocole TACACS+ ou RADIUS.

# Attaque par inondation (flooding) de la table d'adresses MAC

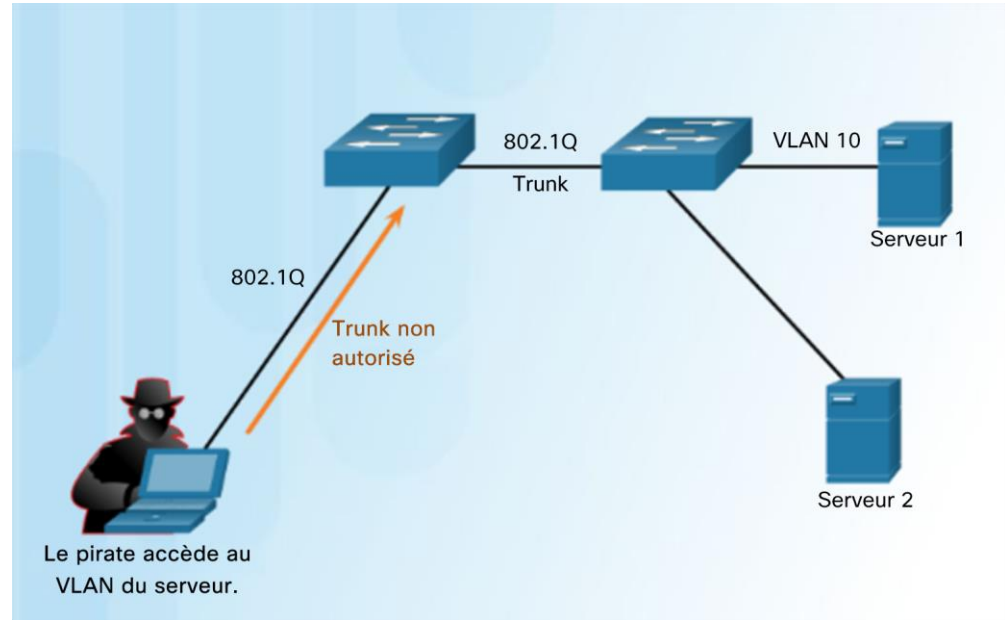


- L'attaque par inondation de la table d'adresses MAC est une attaque de commutateur LAN courante.
  - Un hacker envoie de fausses adresses MAC source jusqu'à ce que la table d'adresses MAC du commutateur soit pleine et que le commutateur arrive à saturation.
  - Le commutateur finit par entrer en mode « fail-open » et diffuse toutes les trames que le hacker peut alors capturer.
- Configurez la sécurité des ports pour contrer ces attaques.

# Attaques de sécurité LAN

## Attaques VLAN

- L'attaque par usurpation du commutateur est un exemple d'attaque de VLAN.
  - Le hacker peut accéder au VLAN en configurant un hôte afin qu'il se fasse passer pour un commutateur utilisant le protocole de trunk 802.1Q ainsi que le protocole DTP pour établir une liaison trunk avec le commutateur.
- Méthodes pour réduire les attaques VLAN :
  - Configurer explicitement les liens d'accès.
  - Désactiver le trunking automatique.
  - Activer manuellement les liaisons trunk.
  - Désactiver les ports inutilisés, les convertir en ports d'accès et les attribuer au VLAN black hole.
  - Modifier le VLAN natif par défaut.
  - Configurer la sécurité des ports.

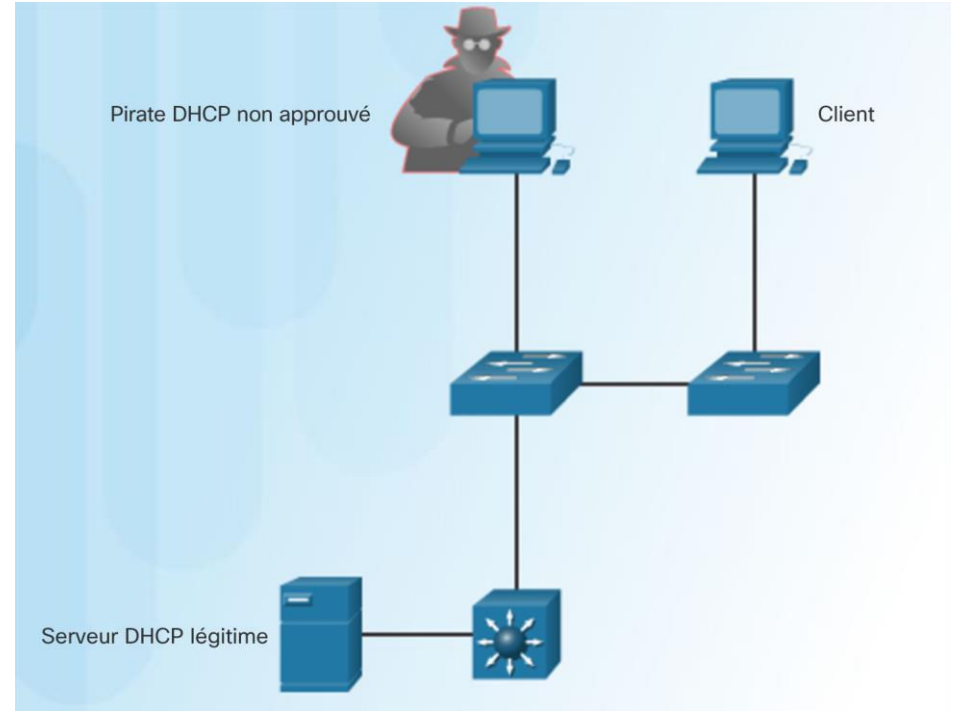




# Attaques de sécurité LAN

## Attaques DHCP

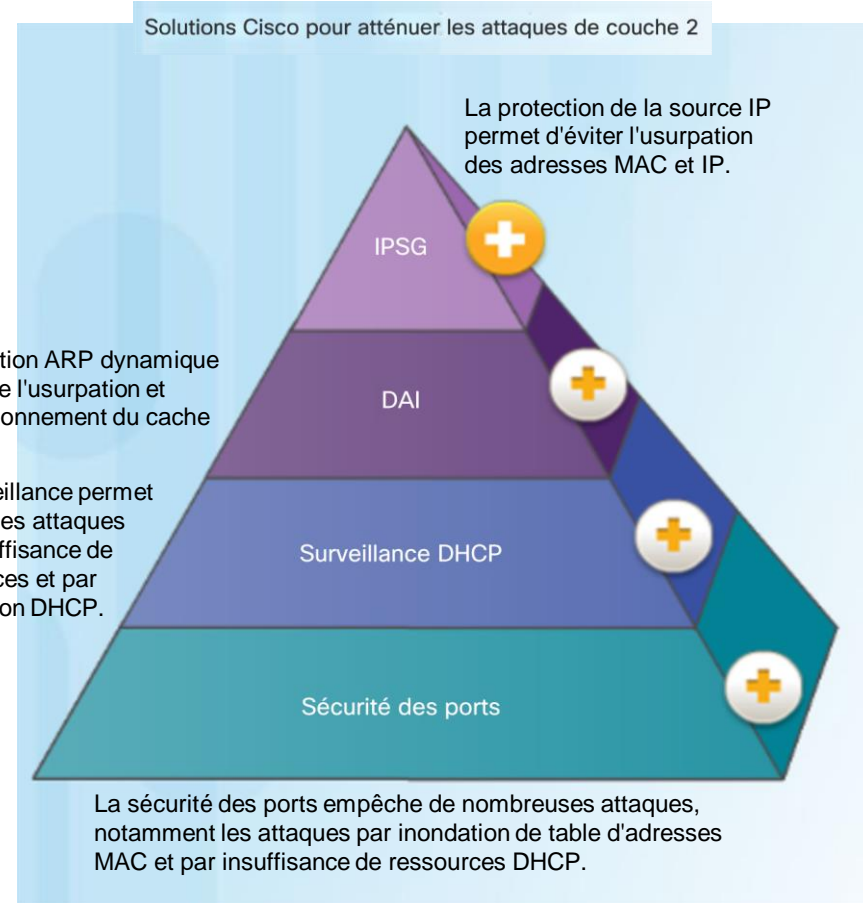
- **Attaque par usurpation DHCP (ou spoofing)** : un hacker configure un faux serveur DHCP sur le réseau pour attribuer des adresses IP aux clients.
- **Attaque par insuffisance de ressources DHCP** : un hacker inonde le serveur DHCP de fausses requêtes DHCP et réserve ensuite toutes les adresses IP disponibles. Cela se traduit par une attaque par déni de service (DoS) qui empêche l'attribution d'adresse IP aux nouveaux clients.
- Méthodes pour limiter les attaques DHCP :
  - Configurer la surveillance DHCP
  - Configurer la sécurité des ports



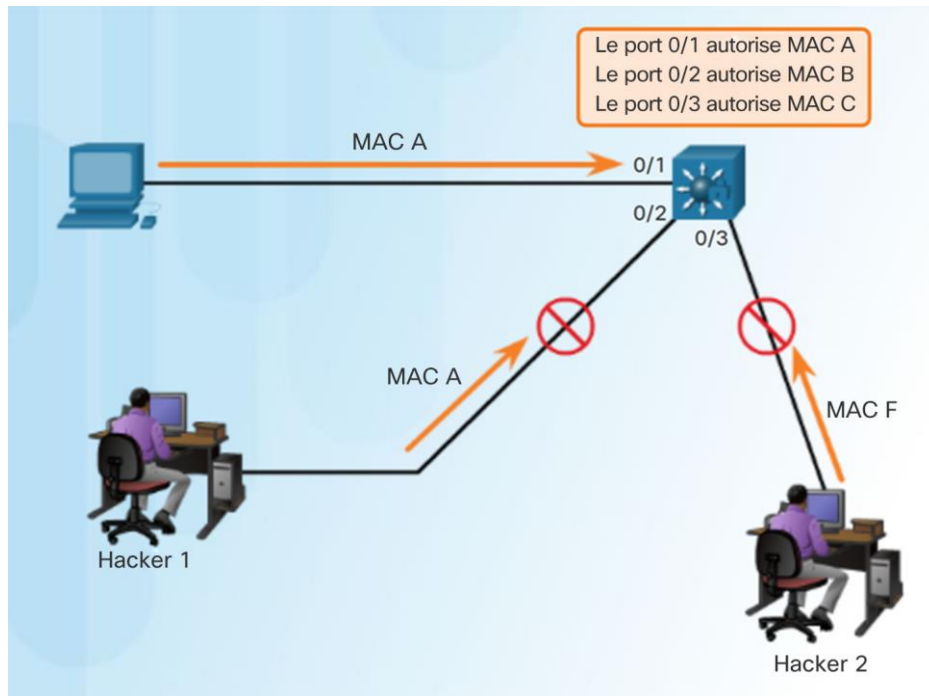
# Bonnes pratiques en matière de sécurité LAN

## Sécuriser le LAN

- Stratégies permettant de sécuriser la couche 2 d'un réseau :
  - Utilisez toujours les variantes sécurisées des protocoles, comme SSH, SCP et SSL.
  - Utilisez des mots de passe forts et modifiez-les souvent.
  - Activez CDP sur certains ports seulement.
  - Sécurisez l'accès Telnet.
  - Utilisez un VLAN de gestion dédié.
  - Utilisez des listes de contrôle d'accès pour filtrer tout accès non souhaité.



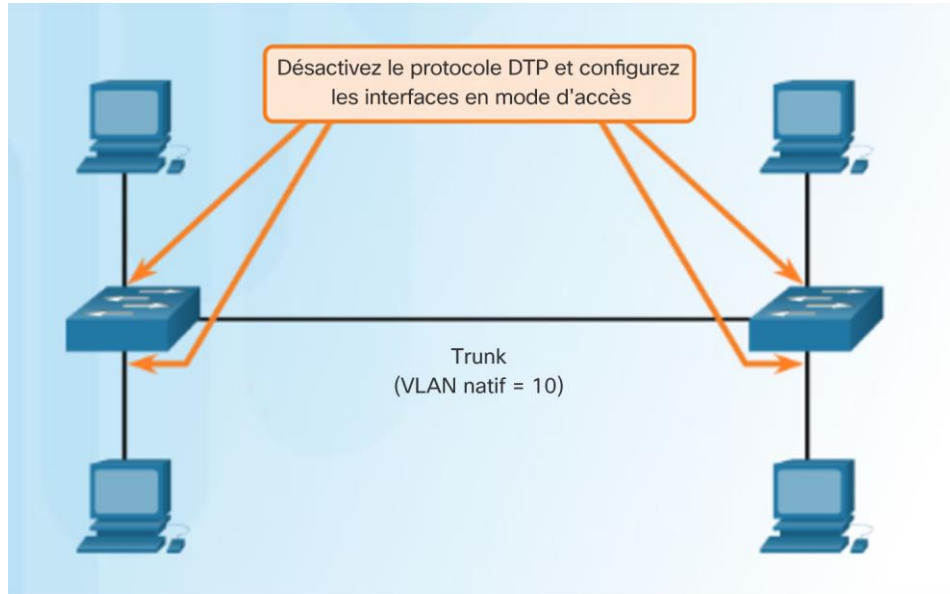
# Limiter les attaques par flooding de la table d'adresses MAC



- Activez la sécurité des ports pour empêcher les attaques par inondation de la table d'adresses MAC.
- Grâce à la sécurité des ports, un administrateur peut :
  - spécifier les adresses MAC pour un port de manière statique.
  - autoriser le commutateur à détecter de manière dynamique un nombre limité d'adresses MAC.
  - Lorsque le nombre maximum d'adresses MAC est atteint, toute tentative de connexion supplémentaire réalisée depuis une adresse MAC inconnue générera une violation de sécurité.

# Bonnes pratiques en matière de sécurité LAN

## Réduire les attaques VLAN

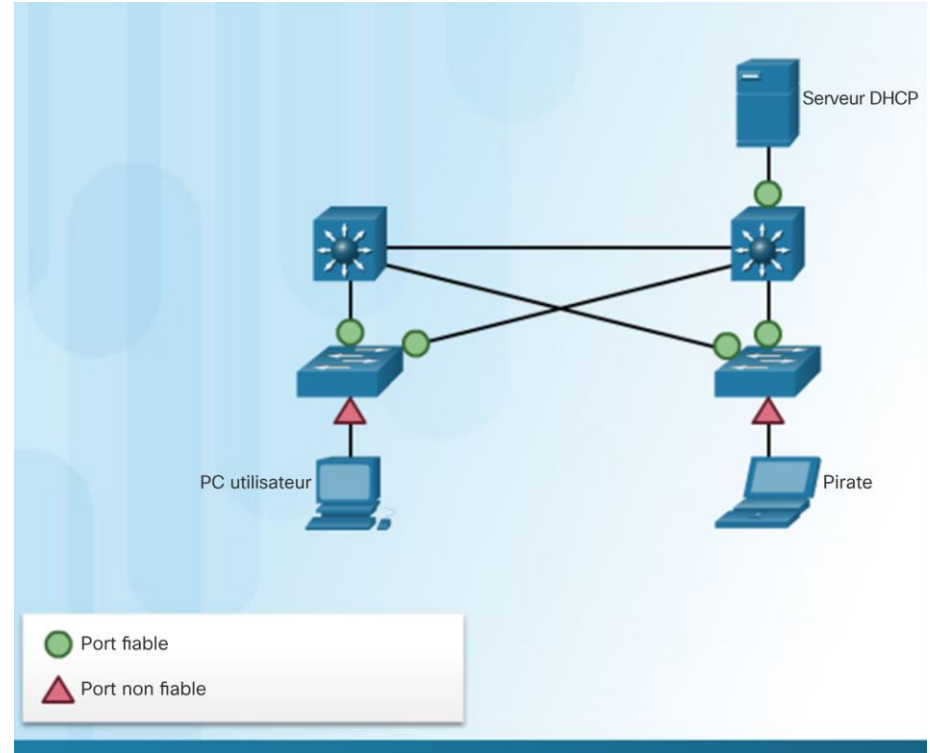


- Pour empêcher les attaques de VLAN de base :
  - Désactivez les négociations DTP (trunking automatique) sur les ports non trunk et exécutez la commande **switchport mode access**.
  - Activez manuellement les liaisons trunk à l'aide de la commande **switchport mode trunk**.
  - Désactivez les négociations DTP (trunking automatique) sur les ports trunk et non trunk en exécutant la commande **switchport nonegotiate**.
  - Définissez comme VLAN natif un VLAN autre que le VLAN 1.
  - Désactivez les ports inutilisés et affectez-les dans un VLAN inutilisé.

# Bonnes pratiques en matière de sécurité LAN

## Réduire les attaques DHCP

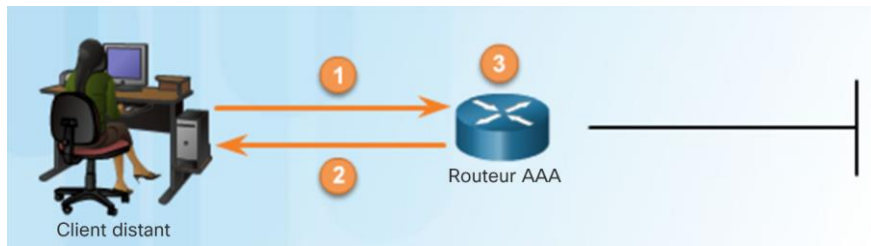
- Pour empêcher les attaques DHCP, activez la surveillance DHCP.
- Lorsque la surveillance DHCP est activée sur une interface, le commutateur refuse les paquets contenant les éléments suivants :
  - Messages de serveurs DHCP non autorisés provenant d'un port non approuvé.
  - Messages de clients DHCP non autorisés ne respectant pas les limitations de débit ou celles indiquées dans la base de données de la surveillance DHCP.
- La surveillance DHCP reconnaît deux types de ports :
  - **Les ports DHCP approuvés** : seuls les ports se connectant aux serveurs DHCP en amont peuvent être approuvés.
  - **Les ports non approuvés** : ces ports se connectent à des hôtes qui ne doivent pas envoyer de messages de serveurs DHCP.



# Sécuriser l'accès administratif à l'aide d'AAA

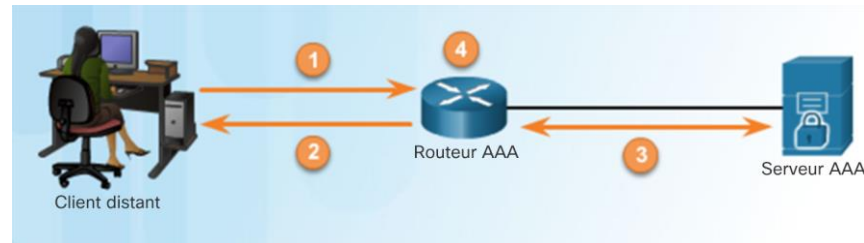
### ■ Authentification AAA locale

1. Le client établit une connexion avec le routeur.
2. Le routeur AAA invite l'utilisateur à saisir un nom d'utilisateur et un mot de passe.
3. Le routeur authentifie le nom d'utilisateur et le mot de passe à l'aide de la base de données locale et autorise l'accès de l'utilisateur.



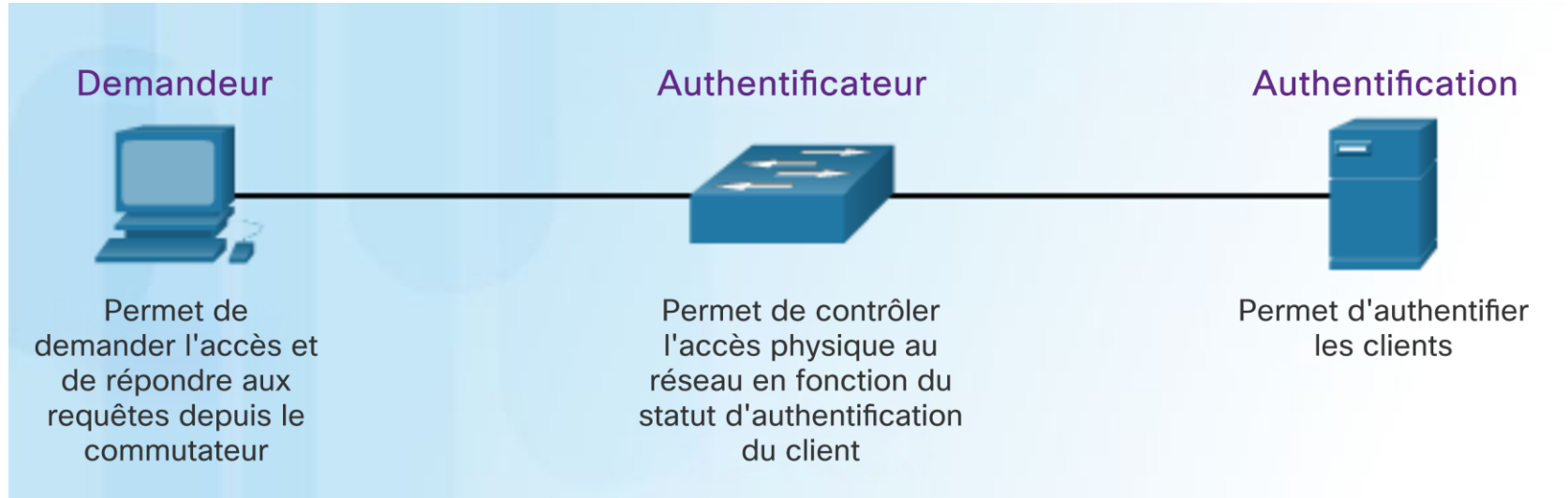
### ■ Authentification AAA basée sur le serveur

1. Le client établit une connexion avec le routeur.
  2. Le routeur AAA invite l'utilisateur à saisir un nom d'utilisateur et un mot de passe.
  3. Le routeur authentifie le nom d'utilisateur et le mot de passe à l'aide d'un serveur AAA distant.
- Le routeur AAA utilise le protocole TACACS+ (Terminal Access Controller Access Control System) ou le protocole RADIUS (Remote Authentication Dial-In User Service) pour communiquer avec le serveur AAA.



# Sécuriser l'accès aux équipements à l'aide de 802.1X

- Le standard IEEE 802.1x définit un protocole de contrôle d'accès et d'authentification basé sur les ports.
  - Il empêche les postes de travail non autorisés de se connecter à un réseau local.
  - Le serveur d'authentification authentifie chaque poste de travail connecté à un port de commutateur avant d'autoriser l'accès aux services.

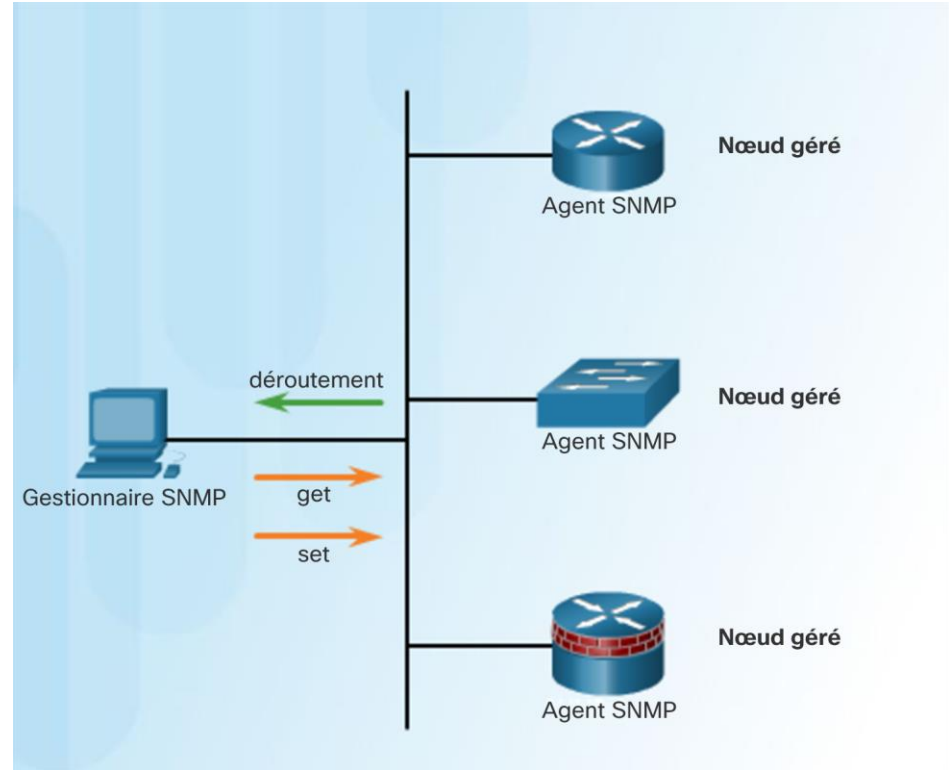


## 5.2 SNMP



# Présentation de SNMP

- Le protocole SNMP (Simple Network Management Protocol) permet aux administrateurs de réseau de surveiller et de gérer les nœuds du réseau.
- Le système SNMP se compose de trois éléments :
  - **Le gestionnaire SNMP**, qui recueille des informations auprès d'un agent SNMP via l'action « get ». Il modifie les configurations sur un agent à l'aide de l'action « set ».
  - **Des agents SNMP** (nœud géré)
  - **Une base d'informations de gestion (MIB)**, qui stocke les données relatives aux périphériques gérés et à leur fonctionnement.



# Fonctionnement de SNMP

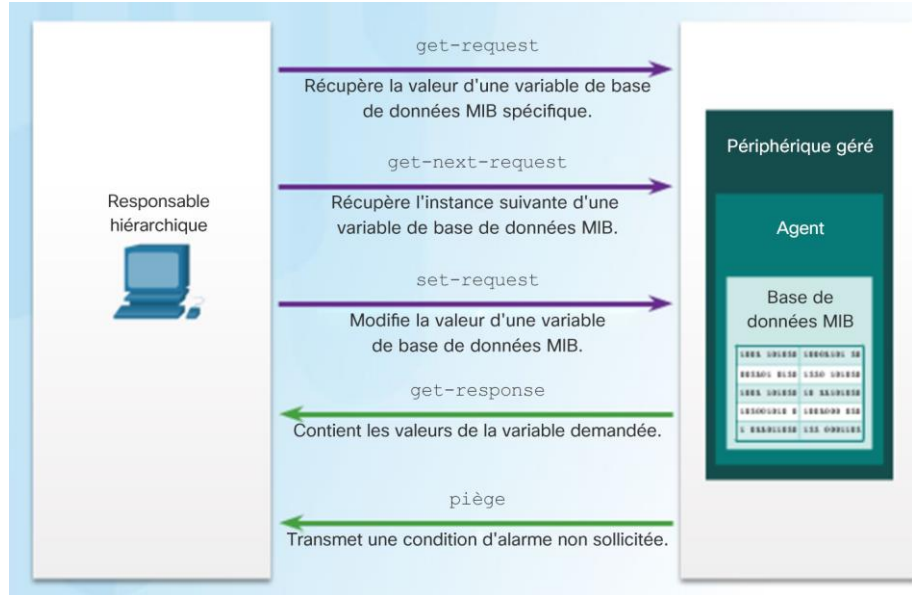
## Fonctionnement de SNMP

- Les agents SNMP qui résident sur des périphériques gérés collectent et stockent les informations relatives aux périphériques.
- Ces informations sont stockées localement par l'agent dans la base de données MIB.
- Le gestionnaire SNMP utilise ensuite l'agent SNMP pour accéder aux informations contenues dans la base de données MIB.
- L'agent SNMP répond comme suit aux requêtes du gestionnaire SNMP :
  - Obtenir une variable MIB** : l'agent SNMP procède à cette opération en réponse à une requête de type GetRequest-PDU envoyée par le gestionnaire du réseau.
  - Définir une variable MIB** : l'agent SNMP procède à cette opération en réponse à une requête de type SetRequest-PDU envoyée par le gestionnaire du réseau.

Opération	Description
get-request	Récupère une valeur à partir d'une variable spécifique.
get-next-request	Récupère une valeur à partir d'une variable dans une table ; le gestionnaire SNMP ne doit pas connaître le nom exact de la variable. Une recherche séquentielle est effectuée afin de trouver la variable requise dans une table.
get-bulk-request	Récupère des blocs importants de données, comme plusieurs lignes dans une table, qui autrement nécessiteraient la transmission de nombreux petits blocs de données. (Fonctionne uniquement avec SNMPv2 ou version ultérieure.)
get-response	Répond aux requêtes <b>get-request</b> , <b>get-next-request</b> et <b>set-request</b> envoyées par un système de gestion de réseau (NMS).
set-request	Stocke une valeur dans une variable spécifique.



# Déroutement par agent SNMP



- Un système de gestion du réseau interroge régulièrement les agents SNMP à l'aide de la requête **get**.
- À l'aide de ce processus, le protocole SNMP peut collecter des informations permettant le contrôle des charges de trafic et la vérification des configurations des périphériques gérés.
- Les agents SNMP peuvent générer et envoyer des déroutements visant à informer immédiatement le système de gestion du réseau de l'occurrence de certains événements.
  - Les déroutements sont des messages non sollicités qui informent le gestionnaire SNMP d'une situation ou d'un événement spécifique, tel qu'une authentification utilisateur non valide ou un mauvais état de la liaison.

# Fonctionnement de SNMP

## Versions de SNMP

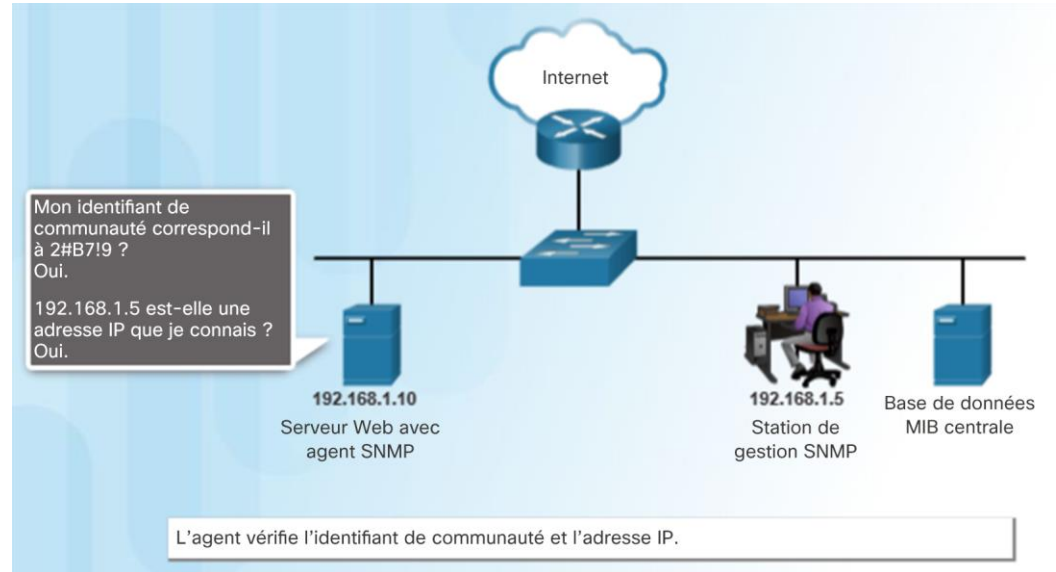
Modèle	Niveau	Authentification	Gestion	Résultat
SNMPv1	noAuthNoPriv	Chaîne de communauté	Non	Utilise une correspondance de chaîne de communauté pour l'authentification.
SNMPv2c	noAuthNoPriv	Chaîne de communauté	Non	Utilise une correspondance de chaîne de communauté pour l'authentification.
SNMPv3	noAuthNoPriv	Nom d'utilisateur	Non	Utilise une correspondance de nom d'utilisateur pour l'authentification (amélioration par rapport à la version SNMPv2c).
SNMPv3	authNoPriv	MD5 (Message Digest 5) ou algorithme de hash sécurisé (SHA)	Non	Fournit une authentification basée sur les algorithmes HMAC-MD5 ou HMAC-SHA.
SNMPv3	authPriv (nécessite l'image logicielle de cryptographie)	MD5 ou SHA	Algorithme DES (Data Encryption Standard) ou AES (Advanced Encryption Standard)	Fournit une authentification basée sur les algorithmes HMAC-MD5 ou HMAC-SHA. Permet la spécification du modèle USM (User-based Security Model) avec ces algorithmes de chiffrement : <ul style="list-style-type: none"><li>• Chiffrement DES 56 bits en plus de l'authentification basée sur le standard CBC-DES (DES-56).</li><li>• Chiffrement 3DES 168 bits.</li><li>• Chiffrement AES 128 bits, 192 bits ou 256 bits.</li></ul>

- Toutes les versions utilisent des agents, des gestionnaires SNMP et des MIB. Ce cours se concentre sur les versions 2c et 3.
- Un administrateur réseau doit configurer l'agent SNMP de manière à utiliser la version SNMP prise en charge par la station de gestion.

# Fonctionnement de SNMP

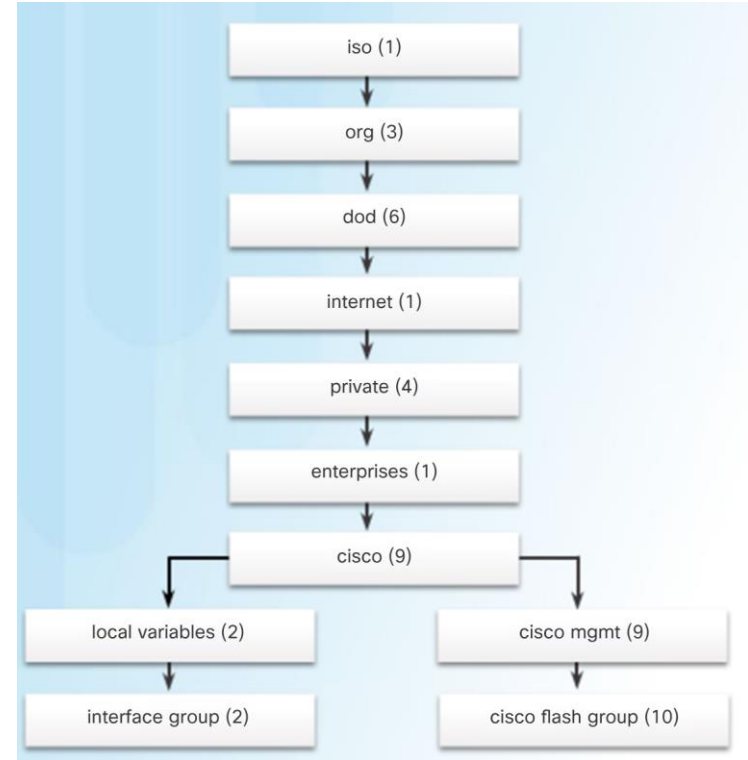
## Chaînes de communauté

- Les protocoles SNMPv1 et SNMPv2c utilisent des identifiants de communauté qui contrôlent l'accès à la base de données MIB.
- On distingue deux types de chaînes de communauté :
  - **Lecture seule (ro)** : permet d'accéder aux variables MIB, mais pas d'effectuer des modifications.
  - **Lecture/écriture (rw)** : fournit un accès en lecture et en écriture à l'ensemble des objets de la base de données MIB.



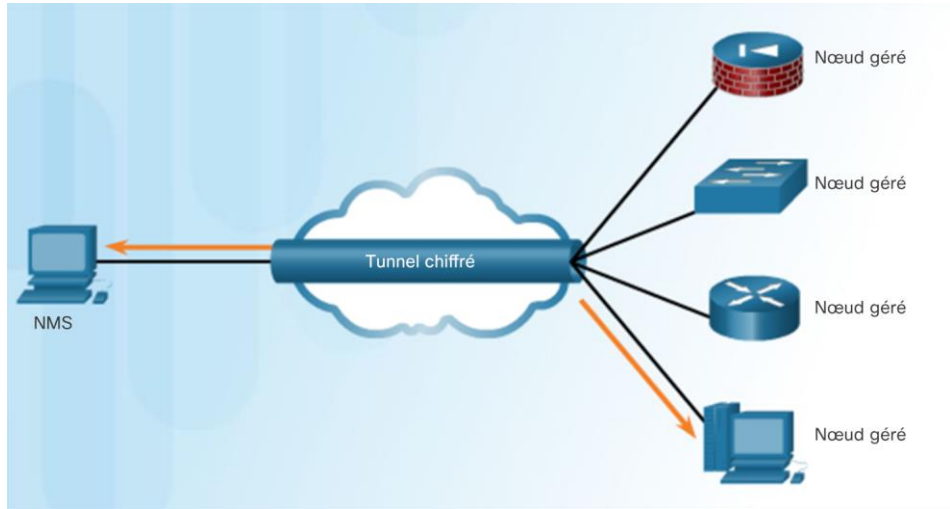
# Base d'informations de gestion (ID d'objet)

- La base de données MIB définit chaque variable comme ID d'objet.
  - Les ID d'objet identifient de manière unique les objets gérés.
  - Les ID d'objet sont organisés en hiérarchie ou en arborescence selon des normes RFC.
- La plupart des périphériques déploient des variables publiques courantes définies par RFC.
  - Les fournisseurs tels que Cisco peuvent définir des branches privées dans l'arborescence pour prendre en charge leurs propres variables.
- Le processeur est l'une des ressources clés et doit être mesuré de manière continue.
  - Un outil graphique SNMP permet d'interroger périodiquement des agents SNMP et d'afficher graphiquement les valeurs collectées.
  - Les données sont récupérées via l'utilitaire snmpget.




# Fonctionnement de SNMP

## SNMPv3



- Le protocole SNMPv3 permet d'authentifier et de chiffrer les paquets sur un réseau afin de sécuriser l'accès aux appareils.
- SNMPv3 offre trois fonctionnalités de sécurité :
  - **Authentification et intégrité des messages** : les messages transmis par le gestionnaire SNMP (NMS) aux agents (nœuds gérés) peuvent être authentifiés.
  - **Chiffrement** : les messages SNMPv3 peuvent être chiffrés pour en garantir la confidentialité.
  - **Contrôle d'accès** : limite les actions du gestionnaire SNMP sur certaines parties de données.

# Travaux pratiques : recherche de logiciel de surveillance du réseau

 Cisco Networking Academy<sup>®</sup>Mind Wide Open<sup>™</sup>

---

### Lab – Researching Network Monitoring Software

#### Objectives

- Part 1: Survey Your Understanding of Network Monitoring
- Part 2: Research Network Monitoring Tools
- Part 3: Select a Network Monitoring Tool

#### Background / Scenario

Network monitoring is needed for any sized network. Proactively monitoring the network infrastructure can assist network administrators with their day-to-day duties. The wide variety of networking tools available vary in cost, depending on the features, number of network locations and number of nodes supported.

In this lab, you will conduct research on available network monitoring software. You will gather information on software products and features of those products. You will investigate one product in greater detail and list some of the key features available.

#### Required Resources

- PC with Internet access

#### Part 1: Survey Your Understanding of Network Monitoring

Describe network monitoring as you understand it. Give an example of how it might be used in a production network.

#### Part 2: Research Network Monitoring Tools

**Step 1: Research and find three network monitoring tools.**

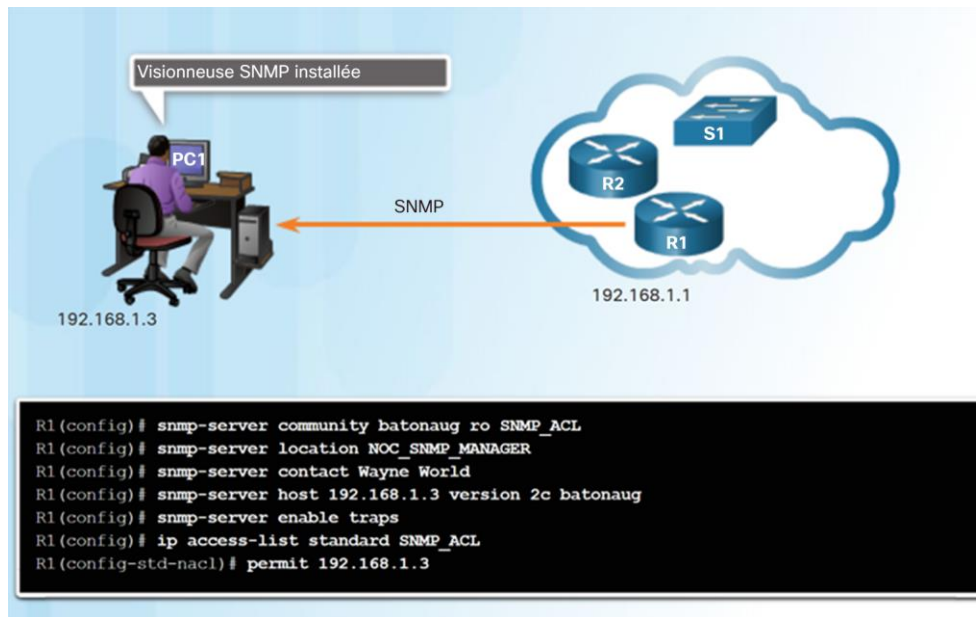
List the three tools that you found.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Page 1 of 2



# Étapes de configuration du protocole SNMP



### ■ Étapes de configuration de base du protocole SNMP :

1. Configurez l'identifiant de communauté et le niveau d'accès à l'aide de la commande **snmp-server community chaîne ro | rw**.
2. (Facultatif) Documentez l'emplacement du périphérique à l'aide de la commande **snmp-server location texte**.
3. (Facultatif) Documentez le contact du système à l'aide de la commande **snmp-server contact texte**.
4. (Facultatif) Utilisez une liste de contrôle d'accès pour limiter l'accès SNMP aux hôtes NMS (gestionnaires SNMP). Référez la liste de contrôle d'accès à l'aide de la commande **snmp-server community chaîne nom-ou-numéro-liste-accès**.

# Vérification de la configuration SNMP

```
R1# show snmp
Chassis: FTX1636848Z
Contact: Wayne World
Location: NOC_SNMP_MANAGER
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
  0 Input queue packet drops (Maximum queue size 1000)
19 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
19 Trap PDUs
SNMP Dispatcher:
  queue 0/75 (current/max), 0 dropped
SNMP Engine:
  queue 0/1000 (current/max), 0 dropped

SNMP logging: enabled
  Logging to 192.168.1.3.162, 0/10, 19 sent, 0 dropped.
```

- Le serveur Syslog Kiwi fait partie des solutions qui affichent les résultats du protocole SNMP.
- Les déroutements SNMP sont envoyés au gestionnaire SNMP et affichés sur le serveur syslog.
- Pour vérifier la configuration SNMP, exécutez la commande **show snmp**.
- Utilisez la commande **show snmp community** pour afficher la chaîne de communauté SNMP et les informations relatives à la liste de contrôle d'accès.

```
R1# show snmp community

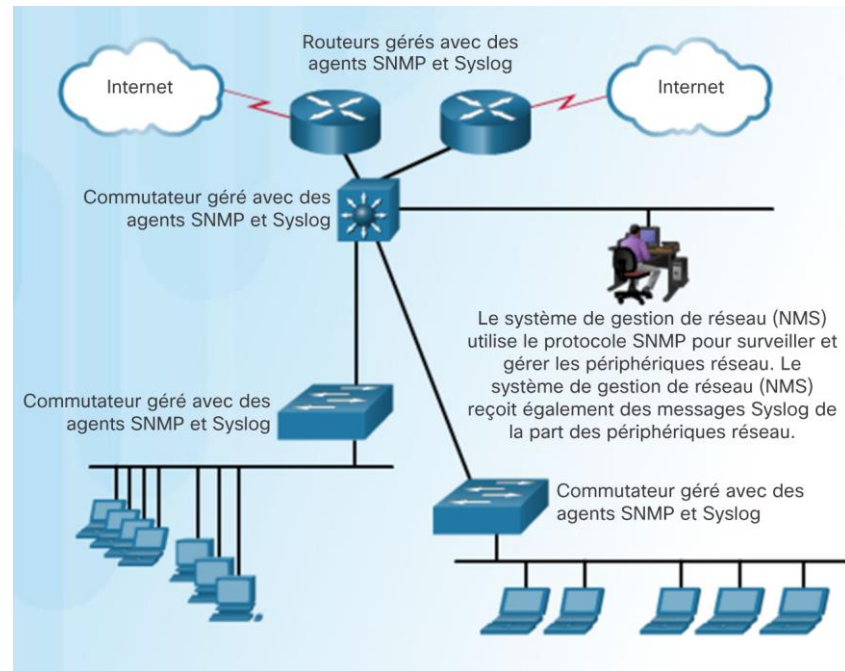
Community name: ILMI
Community Index: cisco0
Community SecurityName: ILMI
storage-type: read-only      active

Community name: batonaug
Community Index: cisco7
Community SecurityName: batonaug
storage-type: nonvolatile    active      access-list: SNMP_ACL

Community name: batonaug@1
Community Index: cisco8
Community SecurityName: batonaug@1
storage-type: nonvolatile    active      access-list: SNMP_ACL
```

# Bonnes pratiques relatives à SNMP

- Le protocole SNMP peut créer des failles de sécurité.
- Pour SNMPv1 et SNMPv2c, les chaînes de communauté doivent être sécurisées et modifiées régulièrement.
- Il est nécessaire d'utiliser des listes de contrôle d'accès afin d'empêcher la diffusion des messages SNMP au-delà des périphériques requis et de limiter l'accès aux périphériques surveillés.
- L'utilisation du protocole SNMPv3 est recommandée, car il permet l'authentification et le chiffrement.
  - La commande **snmp-server group** *nomdegroupe* {v1 | v2c | v3 {auth | noauth | priv}} crée un nouveau groupe SNMP sur le périphérique.
  - La commande **snmp-server user** *nomutilisateur nomdegroupe* est utilisée pour ajouter un nouvel utilisateur au groupe.



# Étapes de configuration du protocole SNMPv3

### ■ Étapes de configuration du protocole SNMPv3 :

1. Configurez une liste de contrôle d'accès standard permettant uniquement l'accès aux gestionnaires SNMP autorisés.
2. Configurez une vue SNMP pour identifier les ID d'objet que le gestionnaire SNMP pourra lire.
3. Configurez le groupe SNMP et ses caractéristiques, y compris le nom, la version, le type d'authentification et de chiffrement, la vue associée au groupe, l'accès en lecture ou en écriture, et le filtrage par liste de contrôle d'accès.
4. Configurez un utilisateur et ses caractéristiques, y compris le nom d'utilisateur, la vue associée au groupe, la version, le type d'authentification, le type de chiffrement et le mot de passe.

**Étape 1 :** Configurer une liste de contrôle d'accès pour autoriser l'accès au réseau de gestion protégé.

```
Router(config)# ip access-list standard acl-name  
Router(config-std-nacl)# permit source_net
```

**Étape 2 :** Configurer une vue SNMP.

```
Router(config)# snmp-server view view-name oid-tree
```

**Étape 3 :** Configurer un groupe SNMP.

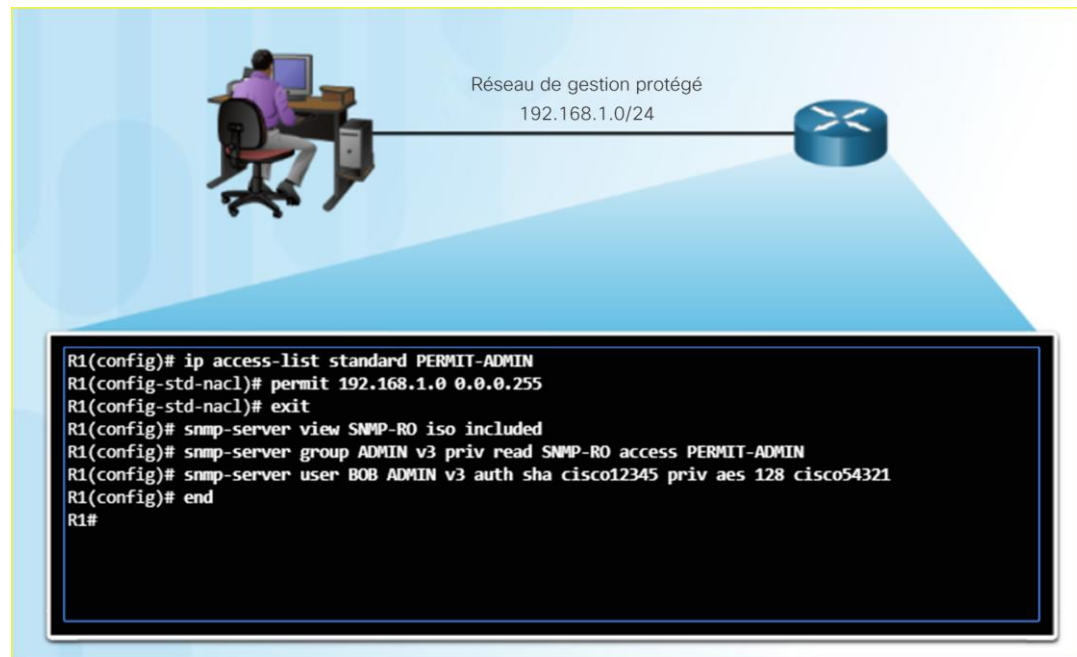
```
Router(config)# snmp-server group group-name v3 priv read view-name access [acl-  
number | acl-name]
```

**Étape 4 :** Configurer un utilisateur en tant que membre du groupe SNMP.

```
Router(config)# snmp-server user username group-name v3 auth {md5 | sha} auth-  
password priv {des | 3des | aes (128 | 192 | 256)} privpassword
```


# Configuration du protocole SNMPv3

- L'exemple illustre la configuration d'une liste de contrôle d'accès standard nommée PERMIT-ADMIN. Celle-ci est configurée pour autoriser uniquement le réseau 192.168.1.0/24. Ainsi, tous les hôtes connectés à ce réseau peuvent accéder à l'agent SNMP s'exécutant sur R1.
- Une vue SNMP nommée SNMP-RO est configurée pour inclure l'arborescence ISO complète de la base de données MIB.



# Configuration de SNMP

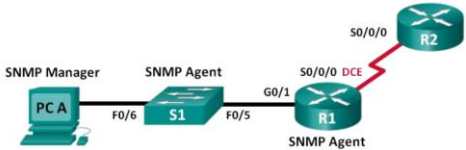
## Travaux pratiques : configuration de SNMP

 Cisco Networking Academy

Mind Wide Open

Lab – Configuring SNMP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.252	N/A
R2	S0/0/0	192.168.2.2	255.255.255.252	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure an SNMPv2 Manager and Agent

Part 3: Configure an SNMPv3 Manager and Agent

Background / Scenario

Simple Network Management Protocol (SNMP) is a network management protocol and an IETF standard which can be used to both monitor and control clients on the network. SNMP can be used to get and set variables related to the status and configuration of network hosts like routers and switches, as well as network client computers. The SNMP manager can poll SNMP agents for data, or data can be automatically sent to the SNMP manager by configuring traps on the SNMP agents.

In this lab, you will download, install, and configure SNMP management software on PC-A. You will also configure a Cisco router and Cisco switch as SNMP agents. After capturing SNMP notification messages from the SNMP agent, you will convert the MIB/Object ID codes to learn the details of the messages using the Cisco SNMP Object Navigator.

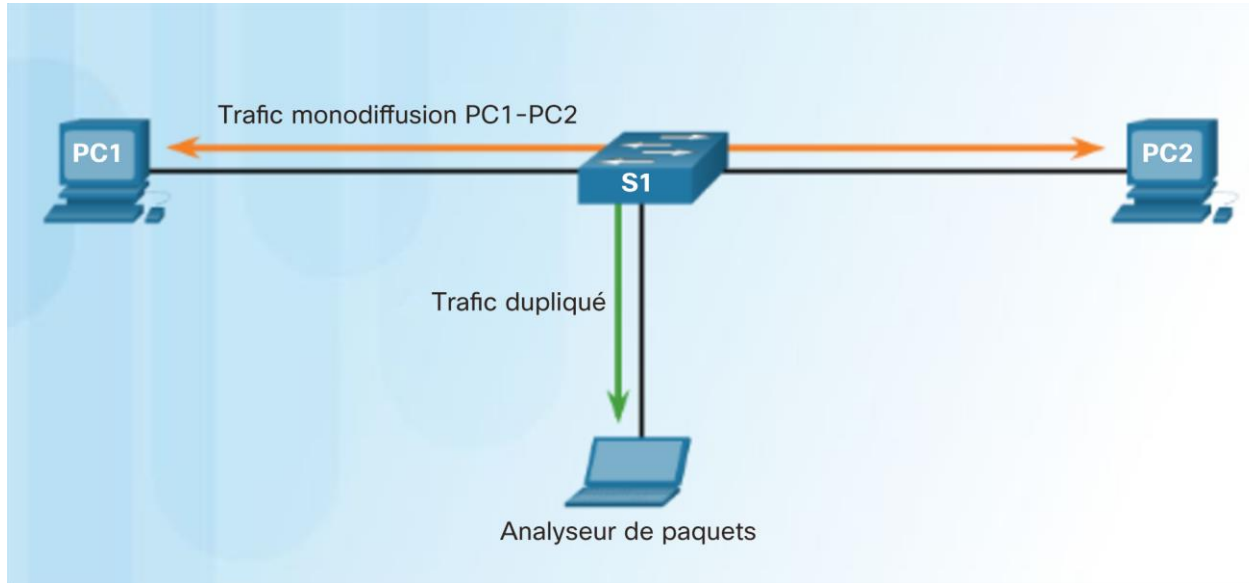
**Note:** The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.4(3) (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public. Page 1 of 12

# 5.3 Analyseur de ports de commutateur Cisco

# Mise en miroir des ports

- Grâce à la mise en miroir des ports, un commutateur peut copier et envoyer des trames Ethernet depuis des ports spécifiques vers un port de destination sur lequel est connecté un analyseur de paquets.





# Analyse du trafic suspect

- La mise en miroir de ports SPAN permet aux administrateurs ou aux périphériques de collecter et d'analyser le trafic.
- La fonction SPAN est généralement mise en œuvre pour acheminer le trafic vers divers périphériques spécialisés :
  - Analyseurs de paquets : inclut l'utilisation d'un logiciel tel que Wireshark pour capturer et analyser le trafic à des fins de dépannage.
  - Systèmes de prévention des intrusions (IPS) : les systèmes IPS veillent à la sécurité du trafic en détectant les attaques réseau au moment où elles se produisent.
- La fonction SPAN peut être mise en œuvre en local ou à distance.

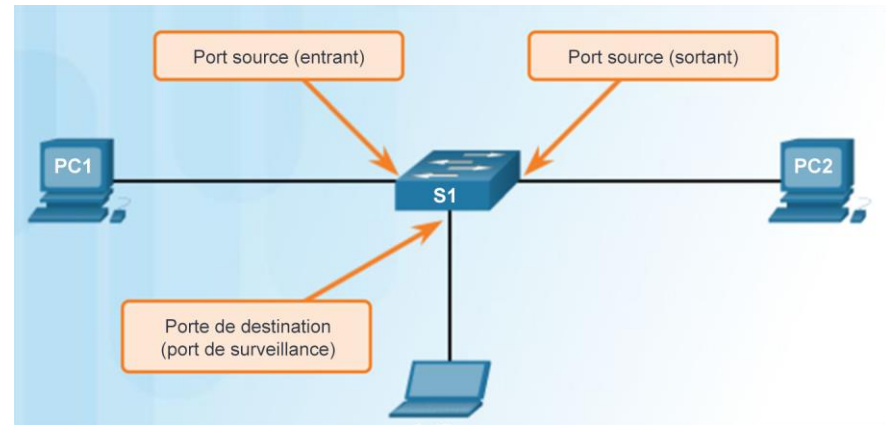


# Présentation de SPAN

## Fonction SPAN locale

- On parle de fonction SPAN locale lorsque le trafic sur un commutateur est mis en miroir sur un autre port du même commutateur.
- Une session SPAN est l'association entre les ports sources (ou VLAN) et un port de destination.
- Trois éléments importants à prendre en considération lors de la configuration de la fonction SPAN :
  - Le port de destination ne peut pas être un port source et le port source ne peut pas être un port de destination.
  - Le nombre de ports de destination dépend de la plate-forme utilisée.
  - Le port de destination n'est plus un port de commutation normal. Seul le trafic surveillé transite par ce port.

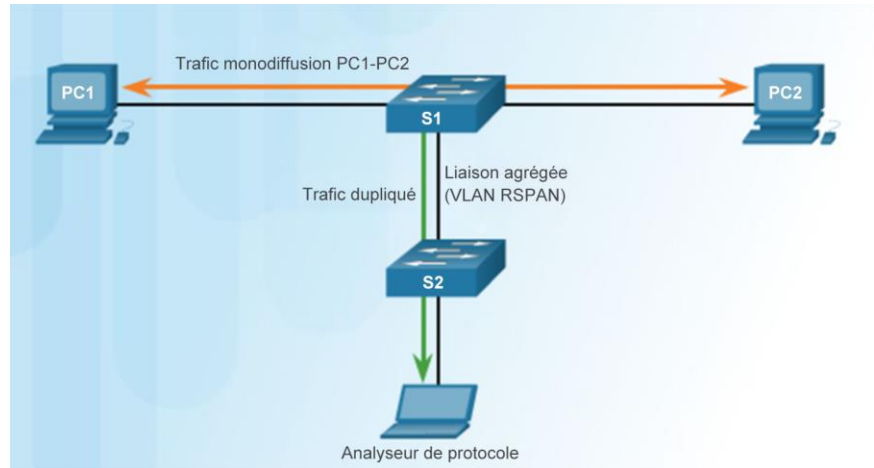
Terme	Définition
Trafic entrant	Le trafic qui entre dans le commutateur.
Trafic sortant	Le trafic qui sort du commutateur.
Port source (SPAN)	Port surveillé à l'aide de la fonction SPAN.
Port de destination (SPAN)	Port qui surveille les ports sources, généralement en cas de connexion d'un analyseur de paquets, d'un IDS ou d'un IPS. Ce port est également appelé « port de surveillance ».
Session SPAN	Association d'un port de destination avec un ou plusieurs ports sources.
VLAN source	Le VLAN surveillé à des fins d'analyse du trafic.



# Fonction SPAN distante (Remote SPAN ou RSPAN)

- Remote SPAN (RSPAN) permet aux ports source et de destination d'être sur des commutateurs différents.
- RSPAN utilise deux sessions.
  - Une des sessions est utilisée comme source et l'autre sert à copier ou à recevoir le trafic d'un VLAN.
  - Le trafic de chaque session RSPAN est acheminé via des liaisons trunk dans un VLAN RSPAN spécifié par l'utilisateur.

Terme	Définition
Session RSPAN source	Le port/VLAN source dont vous souhaitez copier le trafic.
Session RSPAN de destination	Le port/VLAN de destination vers lequel envoyer le trafic.
VLAN RSPAN	<ul style="list-style-type: none"><li>• Un VLAN unique est requis pour transporter le trafic d'un commutateur à un autre.</li><li>• Le VLAN est configuré avec la commande de configuration de VLAN <code>remote-span</code>.</li><li>• Ce VLAN doit être défini sur tous les commutateurs du chemin et doit également être autorisé sur les ports de trunk entre la source et la destination.</li></ul>



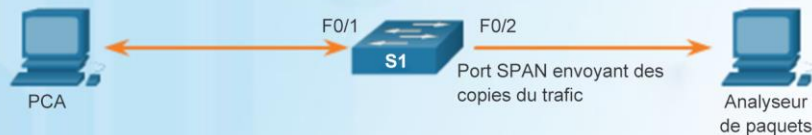
# Configuration de la fonction SPAN locale



```
S1(config)# monitor session 1 source interface fastethernet 0/1
S1(config)# monitor session 1 destination interface fastethernet 0/2
```

- Un numéro de session permet d'identifier une session SPAN locale.
- Utilisez la commande **monitor session** pour associer un port source et un port de destination à une session SPAN.
- Une commande monitor session distincte doit être utilisée pour chaque session.
- Vous pouvez utiliser un VLAN comme source au lieu d'un port physique.

# Vérification de la fonction SPAN locale




- Utilisez la commande **show monitor** pour vérifier les paramètres de la session SPAN. Elle affiche le type de la session, les ports source pour chaque sens du trafic et le port de destination.

```
S1# show monitor
Session 1
-----
Type                : Local Session
Source Ports        :
    Both            : Fa0/1
Destination Ports   : Fa0/2
Encapsulation       : Native
Ingress             : Disabled
```

```
S1#
```

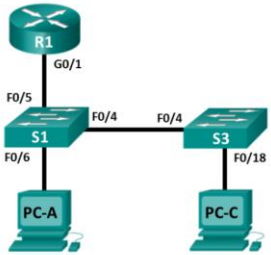
## Travaux pratiques : mise en œuvre d'une fonction SPAN locale

 Cisco Networking Academy®Mind Wide Open®

---

### Lab – Implement Local SPAN

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.3	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.254	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

**Objectives**

**Part 1: Build the Network and Verify Connectivity**

**Part 2: Configure Local SPAN and Capture Copied Traffic with Wireshark**

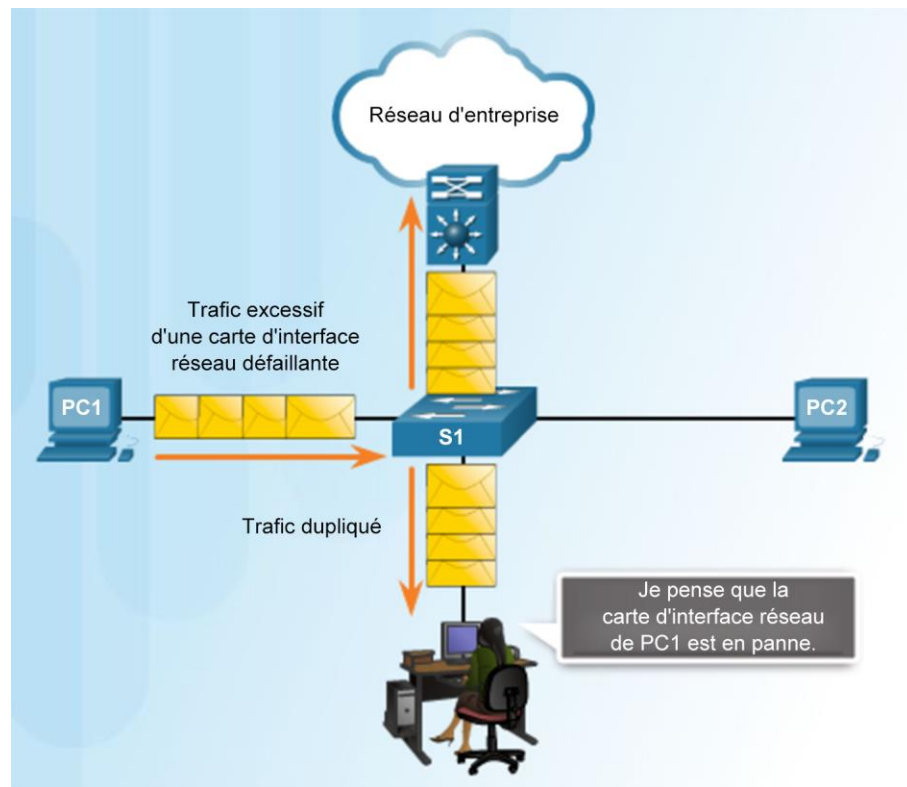
**Background / Scenario**

As the network administrator you want to analyze traffic entering and exiting the local network. To do this, you will set up port mirroring on the switch port connected to the router and mirror all traffic to another switch port. The goal is to send all mirrored traffic to an intrusion detection system (IDS) for analysis. In this initial implementation, you will send all mirrored traffic to a PC which will capture the traffic for analysis using a port sniffing program. To set up port mirroring you will use the Switched Port Analyzer (SPAN) feature on the Cisco switch. SPAN is a type of port mirroring that sends copies of a frame entering a port, out another port on the same switch. It is common to find a device running a packet sniffer or Intrusion Detection System (IDS) connected to the mirrored port.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.Page 1 of 6


# Résolution de problèmes à l'aide de la fonction SPAN

- La fonction SPAN permet aux administrateurs de résoudre les problèmes de réseau.
  - Pour identifier la source d'un problème de performance applicative sur le réseau, l'administrateur réseau peut utiliser la fonction SPAN pour dupliquer et rediriger le trafic vers un analyseur de paquets tel que Wireshark.
  - Les systèmes plus anciens dont les cartes réseaux sont défectueuses peuvent également générer des problèmes. Si la fonction SPAN est activée, un technicien réseau peut détecter et isoler le périphérique à l'origine du problème.



# Configuration du SPAN

## Travaux pratiques : dépannage du trafic LAN à l'aide de la fonction SPAN

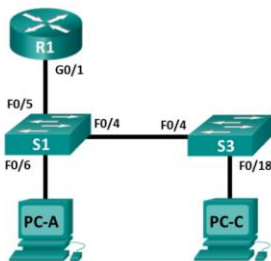


Cisco Networking Academy®

Mind Wide Open™

### Lab – Troubleshoot LAN Traffic Using SPAN

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.3	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.254	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure Local SPAN and Capture Copied Traffic with Wireshark

Background / Scenario

As the network administrator you decide to analyze the internal local area network for suspicious network traffic and possible DoS or reconnaissance attacks. To do this, you will set up port mirroring on all active switchports and mirror/copy all traffic to a designated switchport where a PC running Wireshark can analyze the captured traffic. The goal is to identify the source of suspicious traffic. To set up port mirroring you will use the Switched Port Analyzer (SPAN) feature on the Cisco switch. It is common to find a device running a packet sniffer or Intrusion Detection System (IDS) connected to the mirrored port.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco



# 5.4 Synthèse du chapitre

## Chapitre 5 : sécurité et surveillance du réseau

- Expliquer comment atténuer les attaques de sécurité LAN courantes
- Configurer SNMP de manière à surveiller les opérations réseau sur un réseau de PME
- Dépanner un problème réseau à l'aide de la fonction SPAN

