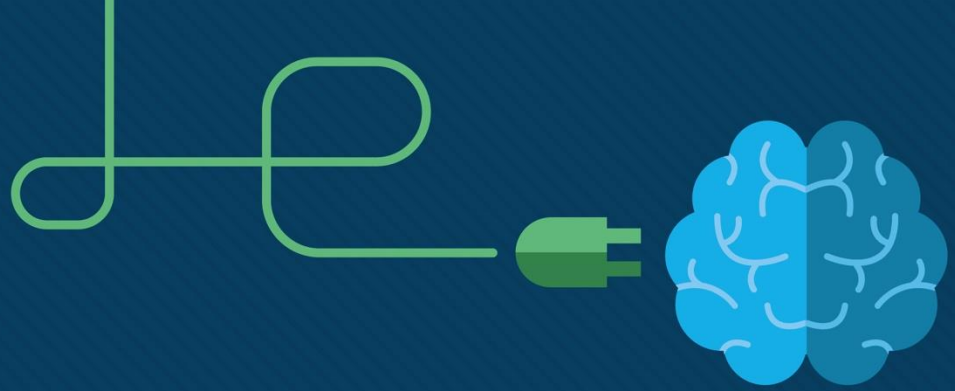


Module 10: Gestion du réseau

Réseau, Sécurité et Automatisation D'entreprise v7.0 (ENSA)

Objectifs du module

Titre du module : Gestion du réseau

Objectif du module : Mettre en œuvre des protocoles pour gérer le réseau.

Titre du Rubrique	Objectif du Rubrique
Détection de périphériques avec le protocole CDP	Utiliser le protocole CDP pour élaborer une topologie du réseau.
Détection de périphériques avec le protocole LLDP	Utiliser le protocole LLDP pour élaborer une topologie du réseau.
NTP	Mettre en œuvre le protocole NTP entre un client NTP et un serveur NTP.
SNMP	Expliquer le fonctionnement du protocole SNMP.
Syslog	Expliquer le fonctionnement de Syslog.
Maintenance des fichiers du routeur et du commutateur	Utiliser les commandes pour sauvegarder et restaurer un fichier de configuration IOS.
Gestion des images IOS	Mettre en œuvre des protocoles pour gérer le réseau.

10.1 : Détection des périphériques avec le protocole CDP

Aperçu du CDP

Le CDP est un protocole de couche 2 propriétaire de Cisco qui est utilisé pour recueillir des informations sur les appareils Cisco qui partagent la même liaison de données. CDP fonctionne indépendamment des supports et protocoles et s'exécute sur tous les périphériques Cisco, tels que routeurs, commutateurs et serveurs d'accès.

Le périphérique envoie des annonces CDP périodiques aux périphériques connectés. Ces annonces partagent des informations sur le type de périphérique détecté, le nom des périphériques, ainsi que le nombre et le type d'interfaces.

Configurer et vérifier le CDP

- Pour les périphériques Cisco, le protocole CDP est activé par défaut. Pour vérifier le statut du CDP et afficher des informations sur la CDP, entrez la commande **show cdp** .
- Pour désactiver le CDP sur une interface spécifique, saisissez **no cdp enable** dans le mode de configuration de l'interface. Le protocole CDP est toujours activé sur le périphérique; cependant, il n'envoie aucune annonce CDP via cette interface. Pour réactiver le CDP sur l'interface spécifique, saisissez **cdp enable.**
- Pour activer CDP globalement pour toutes les interfaces prises en charge sur le périphérique, saisissez **cdp run** comme mode de configuration globale. Le CDP peut être désactivé pour toutes les interfaces de l'appareil avec la commande **no cdp run** en mode de configuration globale.
- Utilisez la commande **show cdp interface** pour afficher les interfaces compatibles CDP d'un périphérique. L’état de chaque interface est également affiché.

Découvrir des appareils en utilisant le CDP

- Lorsque la CDP est activée sur le réseau, la commande **show cdp neighbors** peut être utilisée pour déterminer la configuration du réseau, comme indiqué dans la sortie.
- La sortie montre qu'il existe un autre périphérique Cisco, S1, connecté à l'interface G0/0/1 sur R1. En outre, S1 est connecté via son F0/5

```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID Local Intrfce Holdtme Capability Platform Port ID
S1 Gig 0/0/1 179 S I WS-C3560- Fas 0/5
```

Découvrir des appareils en utilisant le CDP (suite)

L'administrateur réseau utilise **show cdp neighbors detail** pour découvrir l'adresse IP de S1. Comme indiqué dans la sortie, l'adresse de S1 est 192.168.1.2.

```
R1# show cdp neighbors detail
-------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.2
Platform: cisco WS-C3560-24TS, Capabilities: Switch IGMP
Interface: GigabitEthernet0/0/1, Port ID (outgoing port): FastEthernet0/5
Holdtime : 136 sec

(output omitted)
```

Packet Tracer - Utiliser CDP pour cartographier un réseau

Un administrateur réseau principal vous demande de mapper le réseau distant d'une filiale et de déterminer le nom d'un commutateur récemment installé nécessitant une adresse IPv4 à configurer. Votre tâche consiste à créer une carte du réseau de la filiale. Pour mapper le réseau, vous devrez utiliser SSH pour l'accès à distance et le protocole CDP (Cisco Discovery Protocol) pour rechercher des informations sur les périphériques réseau voisins, comme des routeurs et des commutateurs.

10.2 Détection des périphériques avec le protocole LLDP

Aperçu du LLDP

Le protocole LLDP (Link Layer Discovery Protocol) est un protocole de détection voisin ouvert semblable au protocole CDP. LLDP fonctionne avec des périphériques réseau, tels que des routeurs, des commutateurs et des points d'accès LAN sans fil. Ce protocole fait connaître son identité et ses capacités à d'autres appareils et reçoit les informations d'un appareil de couche 2 physiquement connecté.

Configurer et vérifier le LLDP

- Le LLDP peut être activé par défaut. Pour activer LLDP globalement sur un appareil réseau Cisco, saisissez la commande **lldp run** en mode de configuration globale. Pour désactiver le protocole LLDP, entrez la commande **no lldp run** en mode de configuration globale.
- LLDP peut être configuré sur des interfaces spécifiques. Cependant, le LLDP doit être configuré séparément pour transmettre et recevoir des paquets LLDP.
- Po… …e **sh**

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
Switch# show lldp
Global LLDP Information:
   Status: ACTIVE
   LLDP advertisements are sent every 30 seconds
   LLDP hold time advertised is 120 seconds
   LLDP interface reinitialisation delay is 2 seconds
```

Découvrir des périphériques en utilisant le LLDP

Lorsque le protocole LLDP est activé, les voisins de l'appareil peuvent être détectés à l'aide de la commande **show lldp neighbors**.

```
S1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID Local Intf Hold-time Capability Port ID
R1 Fa0/5 117 R Gi0/0/1
S2 Fa0/1 112 B Fa0/1
Total entries displayed: 2
```

Découvrir des dispositifs en utilisant le LLDP (suite)

Pour plus d'informations sur les voisins, utilisez la commande **show lldp neighbors detail** qui permet d'obtenir la version IOS et l'adresse IP des voisins ainsi que la capacité de l'appareil.

```
S1# show lldp neighbors detail
------------------------------------------------
Chassis id: 848a.8d44.49b0
Port id: Gi0/0/1
Port Description: GigabitEthernet0/0/1
System Name: R1
System Description: Cisco IOS Software [Fuji], ISR Software(X86_64_LINUX_.....,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 18:09 by mcpre

Time remaining: 111 seconds
System Capabilities: B,R
Enabled Capabilities: R
Adresses de gestion - non annoncées
(output omitted)
```

Packet Tracer - Utiliser LLDP pour cartographier un réseau

Dans cette activité Packet Tracer, vous remplirez les objectifs suivants:

- Création du réseau et configuration des paramètres de base des périphériques
- Détection de réseaux avec le protocole CDP
- Détection de réseaux avec le protocole LLDP

10.3 NTP

Services de temps et de calendrier

- L'horloge logicielle d'un routeur ou d'un commutateur se déclenche au démarrage du système. C'est la principale source de temps pour le système. Il est important de synchroniser l'heure sur tous les appareils du réseau. Si l'heure n'est pas synchronisée entre les différents périphériques, il vous sera impossible de déterminer l'ordre des événements et leurs causes.
- En règle générale, les paramètres de la date et de l'heure sur un routeur ou un commutateur peuvent être définis en utilisant l'une des deux méthodes suivantes Vous pouvez configurer manuellement la date et l'heure, comme indiqué dans l'exemple, ou configurer le Network Time Protocol (NTP).

```
R1# clock set 20:36:00 nov 15 2019
R1#
*Nov 15 20:36:00.000: %SYS-6-CLOCKUPDATE: System clock has been
updated from 21:32:31 UTC Fri Nov 15 2019 to 20:36:00 UTC Fri Nov 15
2019, configured from console by console.
```

Services de temps et de calendrier (suite)

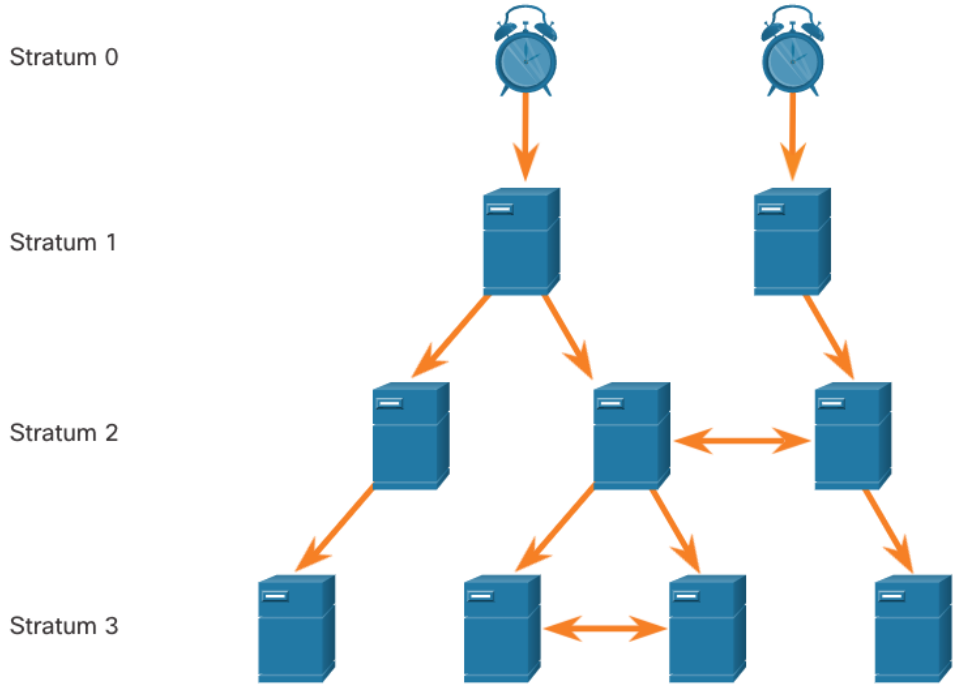
À mesure qu'un réseau se développe, il devient difficile de s'assurer que tous les appareils de l'infrastructure fonctionnent avec un temps synchronisé en utilisant la méthode manuelle.

La meilleure solution consiste à configurer le protocole NTP sur le réseau. Ce protocole permet aux routeurs du réseau de synchroniser leurs paramètres de temps avec un serveur NTP, qui fournit des paramètres de temps plus cohérents. Le NTP peut être configuré pour se synchroniser avec une horloge maîtresse privée, ou il peut se synchroniser avec un serveur NTP accessible au public sur l'internet. Le protocole NTP utilise le port UDP 123 et est décrit dans le document RFC 1305.

Opération NTP

Les réseaux NTP utilisent un système de sources temporelles hiérarchique. Chaque niveau de ce système hiérarchique est appelé strate. Le niveau de strate correspond au nombre de sauts à partir de la source faisant autorité. Le temps synchronisé est distribué à travers le réseau en utilisant NTP.

Le nombre de sauts maximal est de 15. La strate 16, le niveau de strate le plus bas, indique qu'un périphérique n'est pas synchronisé.



Opération NTP (suite)

- **Strate 0:** Ces sources de temps faisant autorité sont des dispositifs de chronométrage de haute précision supposés être précis et associés à peu ou pas de retard.
- **Strate 1:** Dispositifs directement connectés aux sources de temps faisant autorité. Ils représentent la principale référence temporelle du réseau.
- **Strate 2 et inférieure:** les serveurs de la strate 2 sont connectés aux appareils de la strate 1 par des connexions réseau. Les périphériques de strate 2, tels que les clients NTP, synchronisent leur horloge à l'aide des paquets NTP des serveurs de la strate 1. Ils peuvent également servir de serveurs pour les périphériques de la strate 3.

Les serveurs temporels de même niveau de strate peuvent être configurés de manière à agir en tant qu'homologues avec d'autres serveurs temporels de la même strate en vue de la sauvegarde ou de la vérification de l'heure.

Configurer et vérifier le NTP

- Avant que NTP ne soit configuré sur le réseau, la commande **show clock** affiche l'heure actuelle sur l'horloge du logiciel. Avec l'option **detail** , notez que la source de temps est la configuration utilisateur. Cela signifie que l'heure a été configurée manuellement avec la commande **clock** .
- La commande **ntp server** *ip-address* est émise en mode de configuration globale pour configurer le 209.165.200.225 comme serveur NTP pour R1. Pour vérifier si la source temporelle est définie sur NTP, utilisez à nouveau la commande **show clock detail**. Notez que maintenant la source de temps est NTP.

```
R1# show clock detail
20:55:10 .207 UTC ven nov. 15 2019
Time source is user configuration
R1# config t
R1(config)# ntp server 209.165.200.225
R1(config)# end
R1# show clock detail
21:01:34 .563 UTC ven. nov. 15 2019
Time source is NTP
```

Configurer et vérifier le NTP (suite)

Les commandes **show ntp associations** and **show ntp status** sont utilisées pour vérifier que R1 est synchronisé avec le serveur NTP au 209.165.200.225. Notez que R1 est synchronisé avec un serveur NTP de strate 1 à l'adresse 209.165.200.225, qui est synchronisée avec une horloge GPS. La commande **show ntp status** indique que R1 est maintenant un appareil de strate 2 qui est synchronisé avec le serveur NTP au 209.165.220.225.

```
R1# show ntp associations

address ref clock st when poll each delay offset disp
*~209.165.200.225 .GPS.       1 61 64 377 0.481 7.480 4.261
• sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**19
(output omitted)
```

Configurer et vérifier le NTP (suite)

- L'horloge sur S1 est configurée pour se synchroniser sur R1 avec la commande **ntp server** et la configuration est vérifiée avec la commande **show ntp associations** .
- Le résultat de la commande **show ntp associations** vérifie que l'horloge sur S1 est désormais synchronisée avec R1 sur 192.168.1.1 via NTP. R1 est un dispositif de strate 2, ce qui fait que S1 est un dispositif de strate 3 qui peut fournir un service NTP à d'autres dispositifs du réseau.

```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations
address ref clock st when poll reach delay offset disp
*~192.168.1.1 209.165.200.225 2 12 64 377 1.066 13.616 3.840
• sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
(output omitted)

S1# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2088 Hz, precision is 2**17
(output omitted)
```

Packet Tracer - Configurer et vérifier NTP

Dans ce Packet Tracer, vous allez configurer NTP sur R1 et R2 pour permettre la synchronisation du temps.

10.4 - SNMP

Introduction au SNMP

Le protocole SNMP permet aux administrateurs de gérer les périphériques sur un réseau IP. Ces derniers peuvent ainsi contrôler et gérer les performances du réseau, identifier et résoudre les problèmes et anticiper la croissance du réseau.

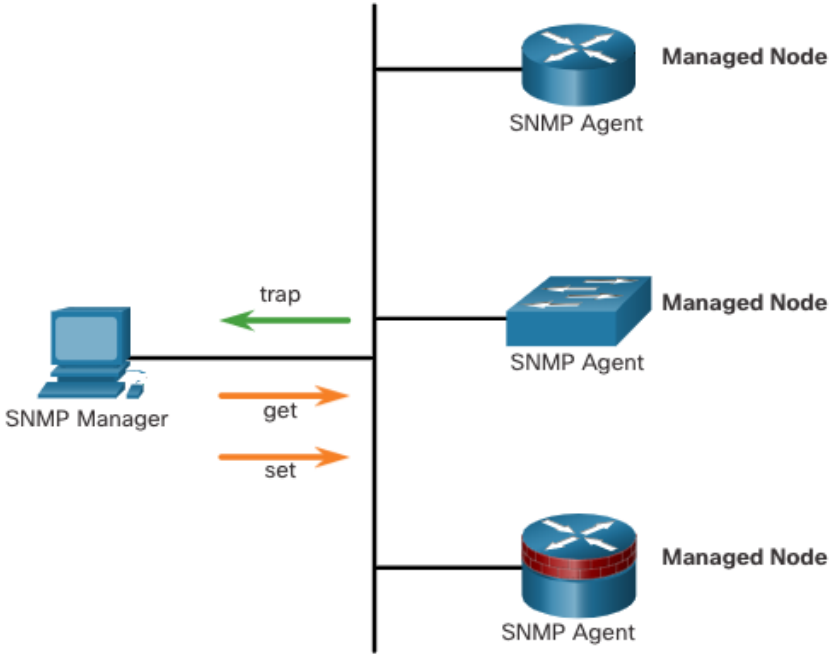
SNMP est un protocole de couche Application qui procure un format pour les messages de communication entre les gestionnaires et les agents. Le système SNMP se compose de trois éléments :

- Gestionnaire SNMP
- Agents SNMP (nœud géré)
- Base d'informations de gestion (MIB)

Le protocole SNMP définit la manière selon laquelle les informations de gestion sont échangées entre les applications de gestion du réseau et les agents de gestion. Le gestionnaire SNMP interroge les agents et envoie des requêtes à la base de données MIB des agents sur le port UDP 161. Les agents SNMP envoient les déroutements SNMP au gestionnaire SNMP sur le port UDP 162.

Introduction au SNMP (suite)

- Le gestionnaire SNMP fait partie d'un système de gestion du réseau (NMS). Le gestionnaire SNMP peut collecter des informations à partir d'un agent SNMP à l'aide de l'action «get» et modifier des configurations sur un agent à l'aide de l'action «set». Les agents SNMP peuvent transmettre des informations directement à un gestionnaire de réseau en utilisant des "pièges".
- L'agent SNMP et la base de données MIB sont présents sur tous les périphériques client SNMP. Les MIB contiennent les données relatives aux périphériques et à leur fonctionnement. Elles peuvent être consultées par tout utilisateur distant authentifié. C'est l'agent SNMP qui est chargé de fournir l'accès à la MIB locale



Opération SNMP

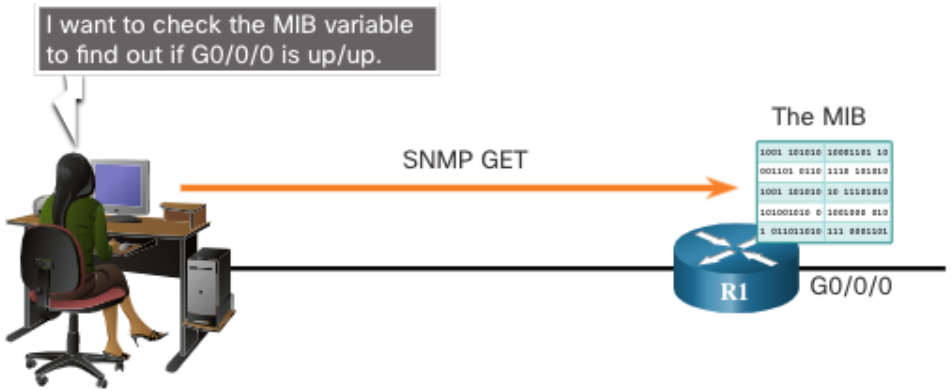
- Les agents SNMP qui résident sur les appareils gérés collectent et stockent des informations sur l'appareil et son fonctionnement localement dans le MIB. Le gestionnaire SNMP utilise ensuite l'agent SNMP pour accéder aux informations contenues dans la base de données MIB.
- Il existe deux types principaux de requêtes de gestionnaire SNMP, à savoir get et set. En plus de la configuration, un ensemble peut provoquer une action, comme le

Operation	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	Réponses aux **get-request, get-next-request,** and **set-request** par un NMS.
set-request	Stocke une valeur dans une variable spécifique.

Opération SNMP (suite)

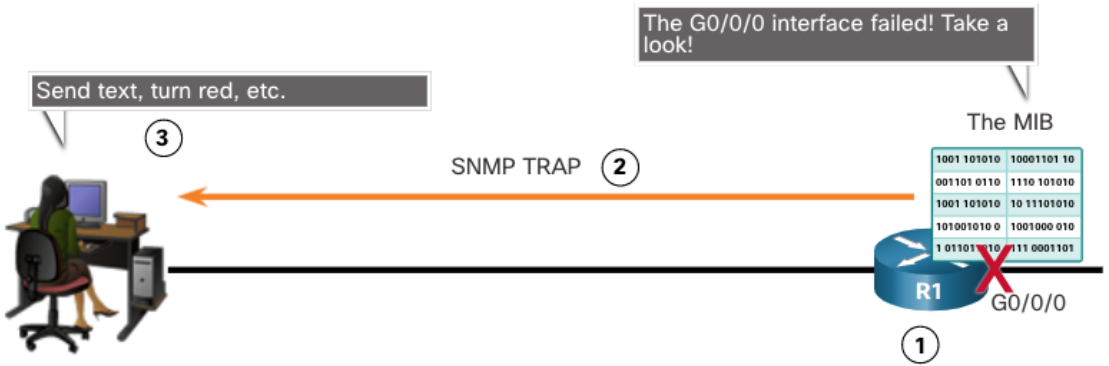
L'agent SNMP répond comme suit aux requêtes du gestionnaire SNMP:

- **Obtenir une variable MIB** - L'agent SNMP exécute cette fonction en réponse à une demande GetRequest-PDU du gestionnaire de réseau. L'agent récupère la valeur de la variable MIB demandée et la transmet au gestionnaire du réseau.
- **Définir une variable MIB** - L'agent SNMP exécute cette fonction en réponse à une SetRequest-PDU du gestionnaire de réseau. L'agent SNMP remplace la valeur de la variable MIB par la valeur spécifiée par le gestionnaire du réseau. Une réponse d'agent SNMP à une requête set inclut les nouveaux paramètres définis dans le périphérique.



Pièges à agents SNMP

- Les déroutements sont des messages non sollicités alertant le gestionnaire SNMP d'une condition ou d'un événement sur le réseau. Les notifications par pièges réduisent les ressources du réseau et des agents en éliminant la nécessité de certaines demandes de sondage SNMP.
- La figure illustre l'utilisation d'un piège SNMP pour alerter l'administrateur réseau que l'interface G0/0/0 a échoué. Le logiciel du système de gestion de réseau (NMS) peut envoyer à l'administrateur réseau un message textuel, faire apparaître une fenêtre contextuelle dans ce logiciel ou faire passer l'icône du routeur au rouge dans l'interface g



Versions SNMP

- SNMPv1 - Standard hérité défini dans la RFC 1157. Utilise une méthode d'authentification basée sur une chaîne de communauté simple. Ne doit pas être utilisé en raison de risques de sécurité.
- SNMPv2c - Défini dans les RFCs 1901-1908. Utilise une méthode d'authentification basée sur une chaîne de communauté simple. Fournit des options de récupération en bloc, ainsi que des messages d'erreur plus détaillés.
- SNMPv3 - Défini dans les RFCs 3410-3415. Utilise l'authentification par nom d'utilisateur, assure la protection des données à l'aide de HMAC-MD5 ou HMAC-SHA et le chiffrement à l'aide du chiffrement DES, 3DES ou AES.

Cordes communautaires

Les protocoles SNMPv1 et SNMPv2c utilisent des identifiants de communauté qui contrôlent l'accès à la base de données MIB. Les identifiants de communauté sont des mots de passe qui circulent en clair (plain text). Les identifiants de communauté SNMP authentifient l'accès aux objets MIB.

Il existe deux types d'identifiants de communauté:

- **Lecture seule (ro)** - Ce type donne accès aux variables MIB, mais ne permet pas de modifier ces variables, seulement de les lire. La sécurité étant minimale dans la version 2c, de nombreuses entreprises utilisent le protocole SNMPv2c en mode lecture seule.
- **Lecture/écriture (rw)** - Ce type fournit un accès en lecture et en écriture à l'ensemble des objets de la base de données MIB.

Pour afficher ou définir des variables MIB, l'utilisateur doit spécifier l'identifiant de communauté approprié pour l'accès en lecture ou en écriture.

ID d'objet MIB

La base de données MIB organise les variables de manière hiérarchique. De manière formelle, la base de données MIB définit chaque variable comme étant un objet avec un identifiant (OID). Les ID d'objet identifient de manière unique les objets gérés. La base de données MIB organise les OID sur la base des RFC au sein d'une hiérarchie d'ID d'objet, généralement affichée sous la forme d'une arborescence.

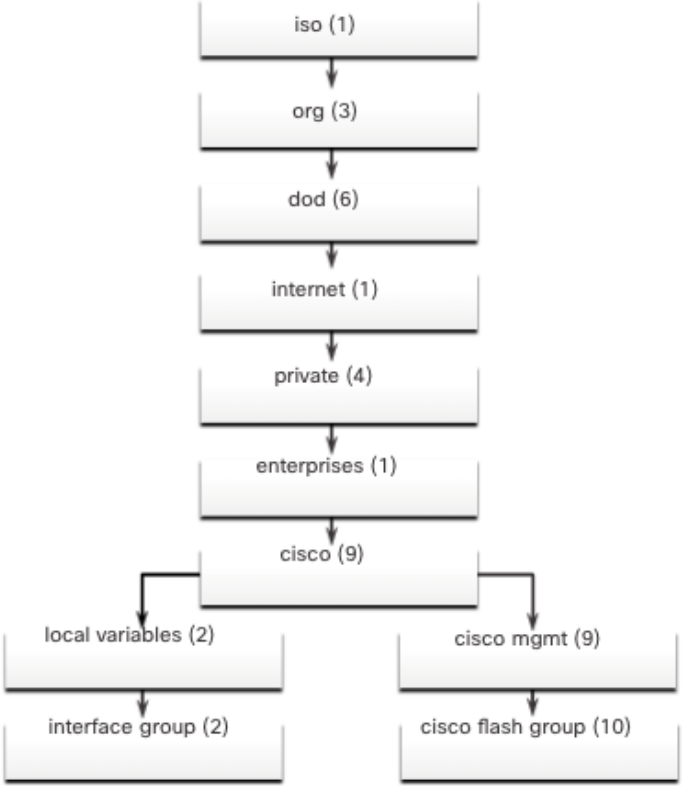
- L'arborescence de la base de données MIB de tout type de périphérique donné inclut certaines branches avec des variables communes à de nombreux périphériques réseau, ainsi que quelques branches avec des variables spécifiques à ce périphérique ou au fournisseur.
- Les RFC définissent certaines variables publiques courantes. La plupart des périphériques implémentent ces variables MIB. De plus, les fournisseurs d'équipements réseau, tels que Cisco, peuvent définir leurs propres branches privées de l'arborescence afin d'accueillir de nouvelles variables spécifiques pour leurs périphériques.

ID d'objet MIB (suite)

La figure montre des parties de la structure MIB définie par Cisco. Notez comment l'OID peut être décrit en mots ou en chiffres pour aider à localiser une variable particulière dans l'arbre.

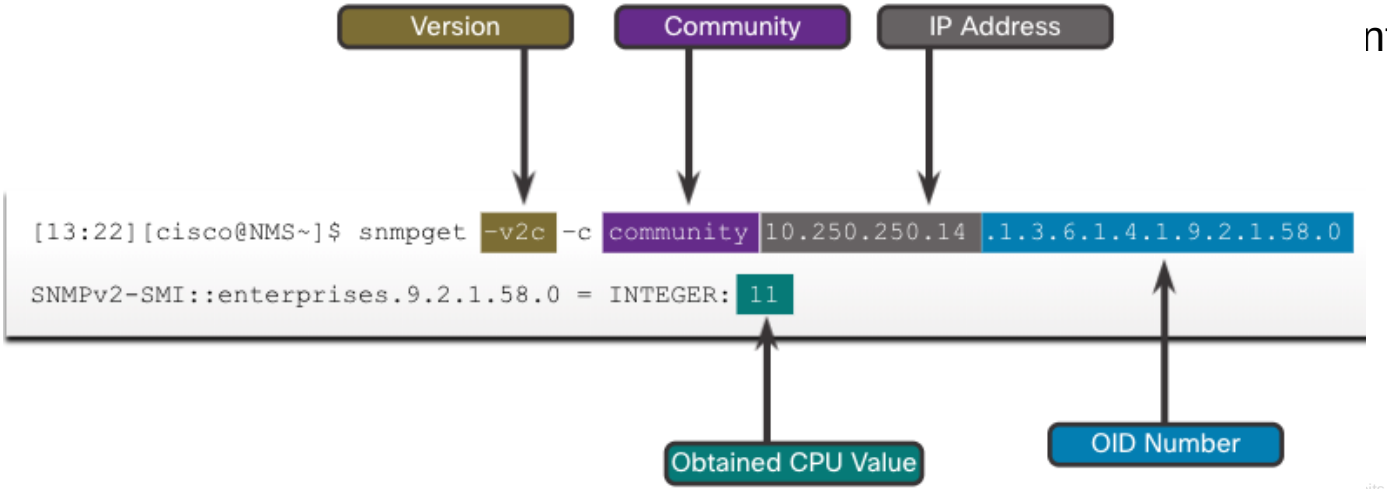
Les OID Cisco sont numérotés comme suit: .iso (1).org (3).dod (6).internet (1).private (4).enterprises (1).cisco (9).

L'OID d'objet est donc 1.3.6.1.4.1.9.



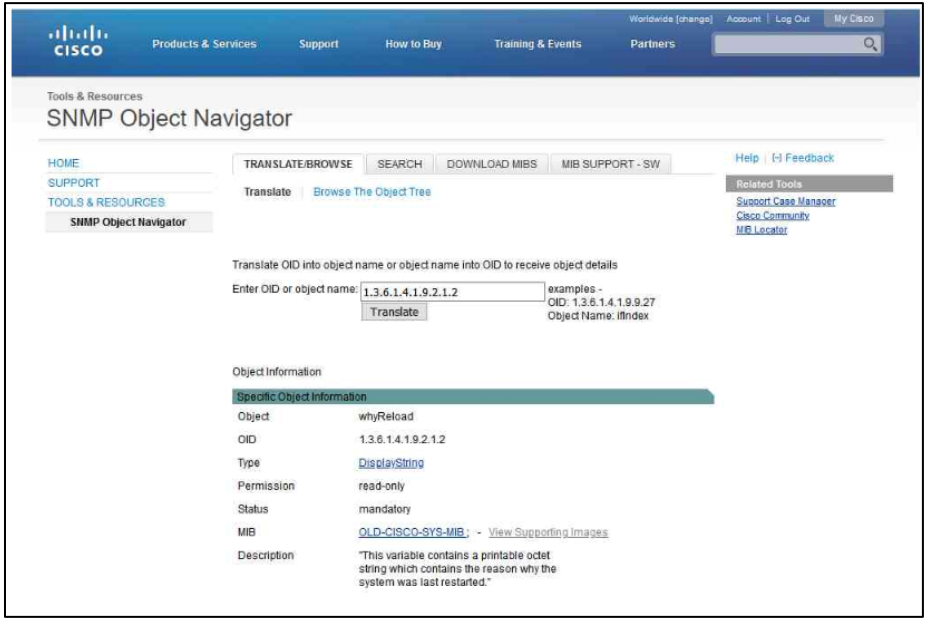
Scénario d'interrogation SNMP

- SNMP peut être utilisé est d'observer l'utilisation du CPU sur une période de temps par des périphériques d'interrogation. Les statistiques du processeur doivent être compilées sur le système de gestion de réseau (NMS) et affichées graphiquement. Cela crée une ligne de base pour l'administrateur réseau.
- Les données sont récupérées par l'intermédiaire de l'utilitaire snmpget, exécuté sur le système de gestion de réseau (NMS). À l'aide de l'utilitaire snmpget, vous pouvez récupérer manuellement des données en temps réel ou demander au NMS d'exécuter nt laquelle vous



Navigateur d'objets SNMP

L'utilitaire snmpget permet de comprendre le fonctionnement de base du protocole SNMP. Toutefois, l'utilisation de longs noms de variable MIB tels que 1.3.6.1.4.1.9.2.1.58.0 peut s'avérer problématique pour un utilisateur moyen. Le plus souvent, le personnel chargé de l'exploitation du réseau utilise un produit de gestion de réseau doté d'une interface graphique facile à utiliser, qui rend transparente pour l'utilisateur la dénomination de l'ensemble des variables de données de la MIB.



Le navigateur SNMP de Cisco sur le site http://www.cisco.com permet à un administrateur réseau de rechercher des

Travaux pratiques - Logiciel de surveillance des réseaux de recherche

Au cours de ces travaux pratiques, vous aborderez les points suivants :

- Partie 1 : évaluation de vos connaissances relatives à la surveillance du réseau
- Partie 2 : recherche d'outils de surveillance du réseau
- Partie 3 : sélection d'un outil de surveillance du réseau

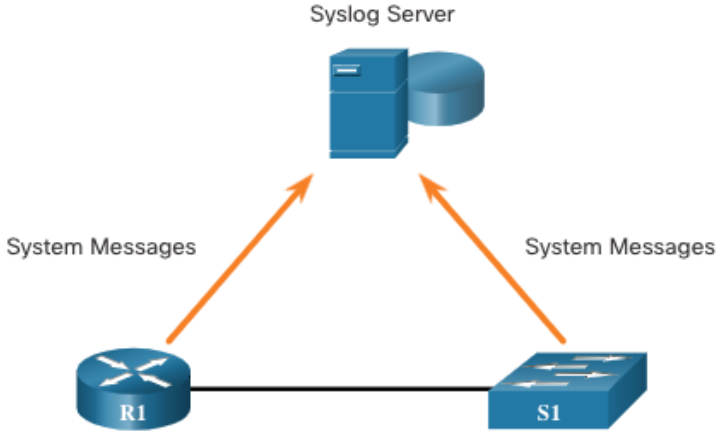
10.5 Syslog

Introduction à Syslog

Syslog utilise le port UDP 514 pour envoyer des messages de notification d'événements sur les réseaux IP aux collecteurs de messages d'événements, comme le montre la figure.

Le service de consignation syslog assure trois fonctions principales, comme suit :

- La capacité à collecter les informations de journalisation pour la surveillance et le dépannage
- La capacité de sélectionner le type d'information de journalisation capturée
- La capacité es Syslog capturés



Opération Syslog

Le protocole syslog commence par envoyer des messages système et une sortie de **debug** à un processus d'enregistrement local. La configuration Syslog peut envoyer ces messages sur le réseau à un serveur syslog externe, où ils peuvent être récupérés sans avoir besoin d'accéder au périphérique réel.

De même, des messages Syslog peuvent également être envoyés vers un tampon interne. Les messages envoyés vers le tampon interne ne peuvent être affichés que par l'intermédiaire de l'interface en ligne de commande du périphérique.

Enfin, l'administrateur réseau peut spécifier que seuls certains types de messages sont envoyés à différentes destinations. Les destinations populaires des messages Syslog sont les suivantes:

- Tampon de consignation (RAM à l'intérieur d'un routeur ou d'un commutateur)
- Ligne de console
- Ligne de terminal
- Serveur Syslog

Format de message Syslog

Les périphériques Cisco génèrent des messages Syslog à la suite des événements réseau. Chaque message Syslog contient un niveau de gravité et une capacité.

Plus les numéros des niveaux sont petits, plus les alarmes Syslog sont critiques. Il est possible de définir le niveau de gravité des messages de manière à contrôler l'emplacement d'affichage de chaque type de message (par exemple sur la console ou d'autres destinations). La liste complète des niveaux Syslog est illustrée au tableau.

Gravité	Niveau de gravité	Explication
Urgence	Niveau 0	Système inutilisable
Alerte	Niveau 1	Action immédiate requise
Essentiel	Niveau 2	Condition critique
Erreur	Niveau 3	Condition d'erreur
Avertissement	Niveau 4	Condition d'avertissement
Notification	Niveau 5	Événement normal mais important
Informatif	Niveau 6	Message informatif
Débogage	Niveau 7	Message de débogage

Installations Syslog

En plus de spécifier la gravité du problème, les messages Syslog contiennent également des informations de capacité. Les capacités Syslog sont des identificateurs de service permettant de déterminer et de catégoriser les données d'état du système pour les rapports des messages d'événement et d'erreur. Les options de consignation disponibles sont spécifiques à l'appareil de réseau.

Les capacités classiques des messages Syslog signalées sur les routeurs Cisco IOS sont les suivantes:

- IP
- Protocole OSPF
- Système d'exploitation SYS
- IPsec (IP Security)
- Adresse IP d'interface (IF)

Installations Syslog (suite)

Par défaut, le format des messages Syslog du logiciel Cisco IOS est le suivant:

%facility-severity-MNEMONIC: description

Exemple de résultat sur un commutateur Cisco en ce qui concerne la modification d'état à la valeur «up» d'une liaison EtherChannel:

```
%LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

Dans ce cas, la capacité est LINK et le niveau de gravité est égal à 3, avec une valeur mnémonique UPDOWN.

Configurer l'horodatage Syslog

Par défaut, les messages de journal ne sont pas horodatés. Les messages de journal doivent être horodatés de sorte que lorsqu'ils sont envoyés à une autre destination, comme un serveur Syslog, il reste une trace du moment où le message a été généré. Utilisez la commande **service timestamps log datetime** pour forcer les événements journalisés à afficher la date et l'heure.

```
R1# configure terminal
R1(config)# interface g0/0/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to down
R1(config-if)# exit
R1(config)# service timestamps log datetime
R1 (config) # interface g0/0/1
R1(config-if)# no shutdown
*Mar 1 11:52:42: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Mar 1 11:52:45: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Mar 1 11:52:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
R1(config-if)#
```

10.6 - Maintenance des fichiers de routeurs et de commutateurs

Systèmes de fichiers de routeurs

Le Cisco IFS (IOS File System) permet à l'administrateur de naviguer dans différents répertoires et d'établir la liste des fichiers d'un répertoire. L'administrateur peut également créer des sous-répertoires en mémoire flash ou sur un disque. Les répertoires disponibles dépendent du périphérique.

L'exemple affiche la sortie de la commande **show file systems** , qui répertorie tous les systèmes de fichiers disponibles sur un routeur Cisco 4221.

```
Router# show file systems
File Systems:
      Size(b)       Free(b)      Type  Flags  Prefixes
            -             -    opaque     rw   system:
            -             -    opaque     rw   tmpsys:
*   7194652672    6294822912      disk     rw   bootflash: flash:
    256589824     256573440      disk     rw   usb0:
   1804468224    1723789312      disk     ro   webui:
            -             -    opaque     rw   null:
            -             -    opaque     ro   tar:
            -             -   network     rw   tftp:
            -             -    opaque     wo   syslog:
     33554432      33539983     nvram     rw   nvram:
            -             -   network     rw   rcp:
            -             -   network     rw   ftp:
            -             -   network     rw   http:
            -             -   network     rw   scp:
            -             -   network     rw   sftp:
            -             -   network     rw   https:
            -             -    opaque     ro   cns:
Router#
```

Il indique qu'il s'agit du système de fichiers par défaut actuel. Le signe dièse (#) indique un disque de démarrage. Les deux sont assignés au système de fichiers flash par défaut

Systèmes de fichiers de routeurs (suite)

Comme flash est le système de fichiers par défaut, la commande **dir** liste le contenu de flash. La dernière liste présente un intérêt particulier. Il s'agit du nom de l'image en cours des fichiers Cisco IOS qui s'exécute dans la mémoire vive.

```
Router# dir
Directory of bootflash:/
   11  drwx            16384   Aug 2 2019 04:15:13 +00:00  lost+found
370945  drwx             4096    Oct 3 2019 15:12:10 +00:00  .installer
338689  drwx             4096    Aug 2 2019 04:15:55 +00:00  .ssh
217729  drwx             4096    Aug 2 2019 04:17:59 +00:00  core
379009  drwx             4096   Sep 26 2019 15:54:10 +00:00  .prst_sync
80641  drwx              4096   Aug 2 2019 04:16:09 +00:00  .rollback_timer
161281  drwx             4096    Aug 2 2019 04:16:11 +00:00  gs_script
112897  drwx           102400    Oct 3 2019 15:23:07 +00:00  tracelogs
362881  drwx             4096   Aug 23 2019 17:19:54 +00:00  .dbpersist
298369  drwx             4096    Aug 2 2019 04:16:41 +00:00  virtual-instance
   12  -rw-               30    Oct 3 2019 15:14:11 +00:00  throughput_monitor_params
 8065  drwx             4096    Aug 2 2019 04:17:55 +00:00  onep
   13  -rw-               34    Oct 3 2019 15:19:30 +00:00  pnp-tech-time
249985  drwx             4096   Aug 20 2019 17:40:11 +00:00  Archives
   14  -rw-            65037    Oct 3 2019 15:19:42 +00:00  pnp-tech-discovery-summary
   17  -rw-          5032908   Sep 19 2019 14:16:23 +00:00
isr4200_4300_rommon_1612_1r_SPA.pkg
   18  -rw-        517153193   Sep 21 2019 04:24:04 +00:00  isr4200-
universalk9_ias.16.09.04.SPA.bin
7194652672 bytes total (6294822912 bytes free)
Router#
```

Systèmes de fichiers de routeurs (suite)

Pour visualiser le contenu de la NVRAM, vous devez modifier le système de fichiers actuel par défaut en utilisant la commande **cd** (change directory), comme indiqué dans l'exemple.

La commande actuelle du répertoire de travail est **pwd**. Cette commande verifie que nous affichons le répertoire NVRAM. Enfin, la commande **dir** affiche la liste du contenu de la mémoire non volatile NVRAM. Parmi les différents fichiers affichés, le seul qui présente un intérêt pour nous est le fichier nommé «startup-config» qui définit la configuration de démarrage

```
Router#
Router# cd nvram:
Router# pwd
nvram:/
Router# dir
Directory of nvram:/
32769  -rw-             1024                    startup-config
32770  ----               61                    private-config
32771  -rw-             1024                    underlying-config
    1  ----                4                    private-KS1
    2  -rw-             2945                    cwmp_inventory
    5  ----              447                    persistent-data
    6  -rw-             1237                    ISR4221-2x1GE_0_0_0
    8  -rw-               17                    ecfm_ieee_mib
    9  -rw-                0                    ifIndex-table
   10  -rw-             1431                    NIM-2T_0_1_0
   12  -rw-              820                    IOS-Self-Sig#1.cer
   13  -rw-              820                    IOS-Self-Sig#2.cer
33554432 bytes total (33539983 bytes free)
Router#
```

Systèmes de fichiers de commutation

Avec le système de fichiers Flash du commutateur Cisco 2960, vous pouvez copier les fichiers de configuration et archiver (charger et télécharger) des images logicielles.

La commande de visualisation des systèmes de fichiers sur un commutateur Catalyst est la même que sur un routeur Cisco: **show file systems.**

```
Switch# show file systems
File Systems:
       Size(b)     Free(b)      Type  Flags  Prefixes
*     32514048    20887552     flash     rw    flash:
           -           -      opaque     rw       vb:
           -           -      opaque     ro       bs:
           -           -      opaque     rw   system:
           -           -      opaque     rw   tmpsys:
         65536       48897     nvram     rw    nvram:
           -           -      opaque     ro   xmodem:
           -           -      opaque     ro   ymodem:
           -           -      opaque     rw     null:
           -           -      opaque     ro      tar:
           -           -     network     rw     tftp:
           -           -     network     rw      rcp:
           -           -     network     rw     http:
           -           -     network     rw      ftp:
           -           -     network     rw      scp:
           -           -     network     rw    https:
           -           -      opaque     ro      cns:
Switch#
```

Utiliser un fichier texte pour sauvegarder une configuration

Les fichiers de configuration peuvent être enregistrés dans un fichier texte en utilisant Tera Term :

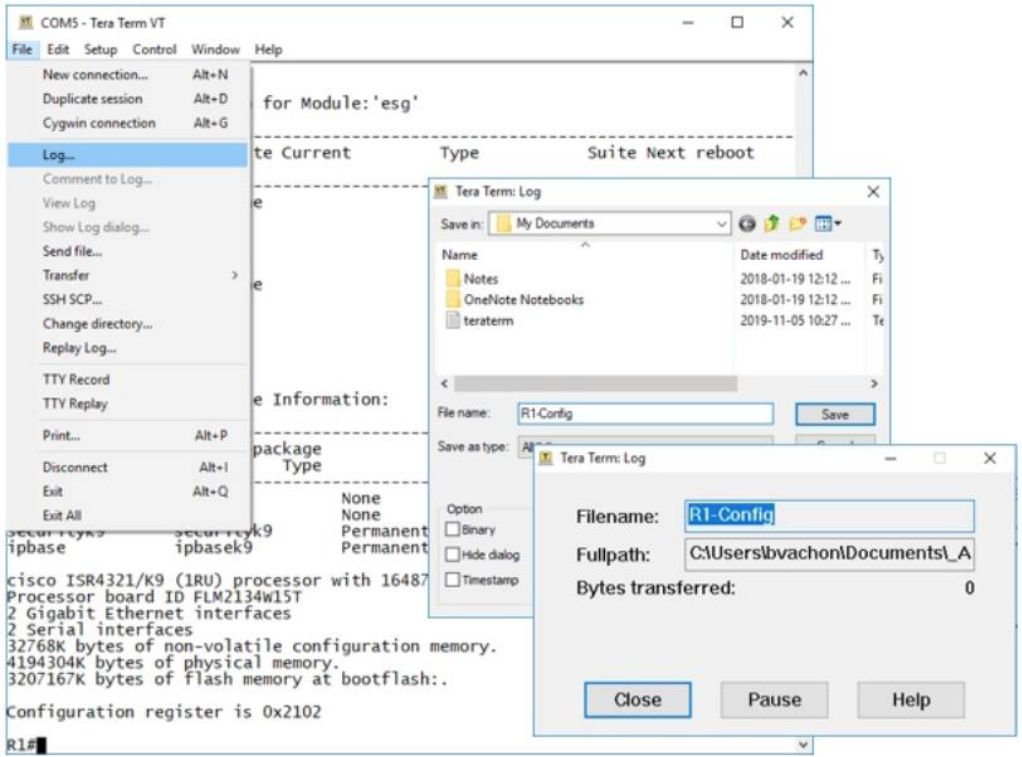
Étape 1. Dans le menu File (Fichier), cliquez sur **Log**(Journal).

Étape 2. Choisissez l'emplacement où vous souhaitez enregistrer le fichier. Tera Term commence à capturer le texte.

Étape 3. Une fois la capture lancée, exécutez la commande **show running-config** ou **show startup-config** à l'invite EXEC privilégiée. Le texte affiché dans la fenêtre du terminal est alors placé dans le fichier choisi.

Étape 4. Lorsque la capture est terminée, sélectionnez **Close** dans le Tera Term: Log window.

Étape 5. Affichez le fichier afin de vérifier qu'il n'a pas été endommagé.



Utiliser un fichier texte pour restaurer une configuration

Une configuration peut être copiée à partir d'un fichier et ensuite directement collée sur un périphérique. Le fichier devra être modifié pour garantir que les mots de passe cryptés sont en texte clair et que les textes non commandés tels que **--More--** et les messages IOS sont supprimés.

En outre, vous pouvez ajouter **enable** et **configure terminal** au début du fichier ou entrer en mode de configuration globale avant de coller la configuration. Au lieu de copier et coller, une configuration peut être restaurée à partir d'un fichier texte à l'aide de Tera Term. En utilisant Tera Term, la procédure est la suivante:

Étape 1. Dans le menu File (Fichier), cliquez sur **Send** (Envoyer).
Étape 2. Recherchez le fichier à copier sur le périphérique et cliquez sur **Open** (Ouvrir).
Étape 3. Tera Term colle alors le fichier dans le périphérique.

Le texte contenu dans le fichier est appliqué sous forme de commandes dans l'environnement CLI et devient la configuration en cours du périphérique.

Utilisation de l'USB pour sauvegarder et restaurer une configuration

Procédez comme suit pour sauvegarder la configuration en cours sur un serveur TFTP:

Étape 1. Saisissez la commande **copy running-config tftp** .
Étape 2. Entrez l'adresse IP de l'hôte sur lequel le fichier de configuration sera stocké.
Étape 3. Entrez le nom à attribuer au fichier de configuration.
Étape 4. Appuyez sur Entrée pour confirmer chaque choix.

Procédez comme suit pour restaurer la configuration en cours à partir d'un serveur TFTP:

Étape 1. Saisissez la commande **copy tftp running-config** .
Étape 2. Saisissez l'adresse IP de l'hôte sur lequel le fichier de configuration est stocké.
Étape 3. Entrez le nom à attribuer au fichier de configuration.
Étape 4. Appuyez sur **Enter** pour confirmer chaque choix.

```
R1# copy running-config tftp
Remote host []?192.168.10.254
Name of the configuration file to write[R1-config]? R1-Jan-2019
Write file R1-Jan-2019 to 192.168.10.254? [confirm]
Writing R1-Jan-2019 !!!!!! [OK]
```

Ports USB sur un routeur Cisco

La fonction de stockage USB (Universal Serial Bus) permet à certains modèles de routeurs Cisco de prendre en charge les disques Flash USB. La fonction Flash USB fournit une capacité de stockage secondaire en option et un périphérique d'amorçage supplémentaire. Les ports USB d'un routeur Cisco 4321 sont illustrés sur la figure.

Utilisez la commande **dir** pour afficher le contenu du disque Flash USB.

Utilisation de l'USB pour sauvegarder et restaurer une configuration

- Exécutez la commande **show file systems** pour vérifier que le lecteur USB est là et confirmer son nom. Dans cet exemple, le système de fichiers USB est nommé **usbflash0 :**.
- Utilisez la commande **copy run usbflash0:/** pour copier le fichier de configuration vers la clé USB. Veillez à utiliser le nom du disque Flash tel qu'il apparait dans le système de fichiers. La barre oblique est facultative et indique le répertoire racine du disque Flash USB.
- L'IOS vous invite à indiquer le nom du fichier. Si le fichier existe déjà sur le lecteur

```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
%Avertissement : Il existe déjà un fichier portant ce nom
Vous voulez sur-écrire ? [confirm]

5024 bytes copied in 1.796 secs (2797 bytes/sec)
R1#
```

Utilisation de l'USB pour sauvegarder et restaurer une configuration

Utilisez la commande **dir** pour afficher le fichier sur le disque USB et la commande **more** pour voir le contenu.

Pour restaurer les configurations avec une clé USB, il sera nécessaire de modifier le fichier USB R1-Config avec un éditeur de texte. En partant du principe que le nom de fichier est **R1-Config**,utilisez la commande **copy usbflash0:/R1-Config** *running-config* pour rétablir une configuration en cours.

```
R1# dir usbflash0:/
Directory of usbflash0:/
    1  drw-      0  Oct 15 2010 16:28:30 +00:00  Cisco
   16  -rw-  5024   Jan 7 2013 20:26:50 +00:00  R1-Config
4050042880 bytes total (3774144512 bytes free)
R1#
R1# more usbflash0:/R1-Config
!
! Last configuration change at 20:19:54 UTC Mon Jan 7 2013 by
admin version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
!
no ipv6 cef
R1#
```

Procédures de récupération des mots de passe

Les mots de passe des périphériques permettent d'empêcher les accès non autorisés. Les mots de passe chiffrés, tels que les mots de passe secrets chiffrés, doivent être remplacés après la récupération. Selon l'appareil, la procédure détaillée de récupération de mot de passe varie.

Cependant, toutes les procédures de récupération des mots de passe pour les périphériques Cisco suivent le même principe:

Étape 1. Activez le mode ROMMON.
Étape 2. Modifiez le registre de configuration.
Étape 3. Copiez la configuration de démarrage dans la configuration d'exécution.
Étape 4. changer le mot de passe.
Étape 5. Enregistrez le running-config comme nouveau startup-config.
Étape 6. Rechargez l'appareil.

Exemple de récupération de mot de passe

Étape 1. Activez le mode ROMMON. La console d'accès permet à l'utilisateur d'accéder au mode ROMMON au moyen d'une séquence de pause pendant le processus de démarrage ou en retirant la mémoire flash externe au moment de la mise hors tension du périphérique.

En cas de succès, l'invite **rommon 1 >** s'affiche, comme indiqué dans l'exemple.

```
Readonly ROMMON initialized

monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

Exemple de récupération de mot de passe (suite)

Étape 2. Modifiez le registre de configuration. La commande **confreg 0x2142** permet à l'utilisateur de régler le registre de configuration sur 0x2142, ce qui fait que le périphérique ignore le fichier de configuration au démarrage pendant le démarrage.

Une fois le registre de configuration défini sur 0x2142, tapez **reset** à l'invite pour redémarrer le périphérique. Saisissez la séquence de pause au moment où le périphérique redémarre et décompresser l'IOS. L'exemple montre la sortie du terminal d'un routeur 1941 en mode ROMMON après l'utilisation d'une séquence de pause au cours du processus de démarrage.

```
rommon 1 > confreg 0x2142
rommon 2 > reset

System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
(output omitted)
```

Exemple de récupération de mot de passe (suite)

Étape 3. Copiez la configuration de démarrage dans la configuration d'exécution. Une fois que l'appareil a fini de se recharger, lancez la commande **copy startup-config running-config** .

AVERTISSEMENT : Ne pas saisir la commande **copy running-config startup-config**. Cette commande efface la configuration initiale.

```
Router# copy startup-config running-config
Destination filename [running-config]?

1450 bytes copied in 0.156 secs (9295 bytes/sec)
R1#
```

Exemple de récupération de mot de passe (suite)

Étape 4. changer le mot de passe. Étant donné que vous êtes en mode d'exécution privilégié, vous pouvez maintenant configurer tous les mots de passe requis.

Remarque: Le mot de passe **cisco** is n'est pas un mot de passe fort et n'est utilisé ici qu'à titre d'exemple

```
R1# configure terminal
Entrez les commandes de configuration, une par ligne. End with
CNTL/Z.
R1(config)#
```

Exemple de récupération de mot de passe (suite)

Étape 5. Enregistrez le running-config comme nouveau startup-config. Une fois que les nouveaux mots de passe sont configurés, modifiez le registre de configuration pour le ramener à 0x2102 en utilisant la commande **config-register 0x2102** dans le mode de configuration globale. Enregistrez le running-config dans startup-config.

```
R1(config)# config-register 0x2102
R1(config)# end
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration... [OK]
R1#
```

Packet Tracer - Sauvegarde des fichiers de configuration

Au cours de cet exercice, vous aborderez les points suivants :

- Partie 1 : Établissement de la connectivité avec le serveur TFTP
- Partie 2 : Transfert du fichier de configuration à partir du serveur TFTP
- Partie 3 : Sauvegarde de la configuration et de l'IOS sur le serveur TFTP

Travaux pratiques - Utiliser le terme Tera pour gérer les fichiers de configuration des routeurs

Au cours de ces travaux pratiques, vous aborderez les points suivants :

- Partie 1: Configurer les paramètres de base des périphériques
- Partie 2: Utiliser un logiciel d'émulation de terminal pour créer un fichier de sauvegarde de configuration
- Partie 3 : Utilisation d'un fichier de sauvegarde de configuration pour restaurer un routeur

Packet Tracer - Utiliser TFTP, Flash et USB pour gérer les fichiers de configuration — Physical Mode
Travaux Pratiques - Utiliser TFTP, Flash et USB pour gérer les fichiers de configuration

Dans cette activité mode physique du Packet Tracer et dans les Travaux Pratiques, vous remplirez les objectifs suivants:

- Partie 1: Câbler le réseau et configurer les paramètres de base des appareils
- Partie 2 : Utiliser TFTP pour sauvegarder et restaurer la configuration de fonctionnement du commutateur
- Partie 3: Utiliser un TFTP pour sauvegarder et restaurer la configuration en cours du routeur
- Partie 4 : Sauvegarde et restauration des configurations en cours d'exécution à l'aide de la mémoire flash du routeur
- Partie 5 : (Facultatif) Utiliser une clé USB pour sauvegarder et restaurer la configuration en cours (Travaux Pratiques uniquement)

Packet Tracer – Procédures de récupération de mot de passe de recherche – Mode Physique

Travaux Pratiques - Procédures de récupération de mot de passe de recherche

Dans cette activité mode physique du Packet Tracer et dans les Travaux Pratiques, vous remplirez les objectifs suivants:

- Partie 1 : Examiner le registre de configuration
- Partie 2 : Documenter la procédure de récupération des mots de passe pour un routeur Cisco spécifique

10.7 - Gestion des images IOS

Vidéo - Gestion des images IOS de Cisco

Cette vidéo démontrera le processus de mise à niveau de l'IOS sur un routeur Cisco.

Serveurs TFTP comme lieu de sauvegarde

À mesure que le réseau se développe, les images du logiciel Cisco IOS et les fichiers de configuration peuvent être stockés sur un serveur TFTP central. Cela permet de contrôler le nombre d'images IOS et les révisions correspondantes, ainsi que les fichiers de configuration à gérer.

Les interréseaux couvrent habituellement de grandes zones et comprennent de multiples routeurs. Pour tout réseau, il est bon de conserver une copie de sauvegarde de l'image du logiciel Cisco IOS au cas où l'image du système sur le routeur serait corrompue ou accidentellement effacée.

Les routeurs largement répartis nécessitent un emplacement source ou de sauvegarde pour les images du logiciel Cisco IOS. Un serveur TFTP permet de télécharger des images logicielles et des configurations par l’intermédiaire du réseau. Le serveur TFTP réseau peut être un autre routeur, une station de travail ou un système hôte.

Exemple de sauvegarde d'une image IOS sur un serveur TFTP

Pour gérer les opérations réseau avec un temps d'indisponibilité minimum, il est nécessaire de mettre en place des procédures de sauvegarde des images Cisco IOS. Ainsi, l'administrateur réseau peut rapidement copier une image sur un routeur en cas d'image corrompue ou effacée. Procédez comme suit :

Étape 1. Envoyez une requête ping au serveur TFTP. Ping sur le serveur TFTP pour tester la connectivité.

Étape 2. Vérifiez la taille de l'image en flash. Vérifiez que le serveur TFTP possède un espace disque suffisant pour accueillir l'image du logiciel Cisco IOS. Utilisez la commande **show flash0:** sur le routeur pour déterminer la taille du fichier image Cisco IOS.

Étape 3. Copiez l'image sur le serveur TFTP Copiez l'image sur le serveur TFTP en utilisant la commande **copy** *source-url destination-url* . Une fois la commande exécutée à l'aide des URL source et de destination spécifiées, l'utilisateur est invité à indiquer le nom du fichier source, l'adresse IP de l'hôte distant et le nom du fichier de destination. Le transfert commence.

Exemple de copie d'une image de l'IOS sur un appareil

Étape 1. Envoyez une requête ping au serveur TFTP. Ping sur le serveur TFTP pour tester la connectivité.

Étape 2. Vérifiez la quantité de flash libre. Assurez-vous qu'il y a suffisamment d'espace de flash sur l'appareil mis à niveau en utilisant la commande **show flash:** Comparez l'espace de mémoire Flash disponible avec la nouvelle taille du fichier d'image.

Étape 3. Copiez le fichier image IOS du serveur TFTP vers le routeur en utilisant la commande **copy tftp: flash:** Une fois la commande exécutée à l'aide des URL source et de destination spécifiées, l'utilisateur est invité à indiquer l'adresse IP de l'hôte distant, le nom du f

```
R1# copy tftp: flash:
Address or name of remote host []? 2001:DB8:CAFE:100::99
Source filename []? isr4200-universalk9_ias.16.09.04.SPA.bin
Destination filename [isr4200-universalk9_ias.16.09.04.SPA.bin]?
Accessing tftp://2001:DB8:CAFE:100::99/ isr4200- universalk9_ias.16.09.04.SPA.bin...
Loading isr4200-universalk9_ias.16.09.04.SPA.bin from 2001:DB8:CAFE:100::99 (via
GigabitEthernet0/0/0): !!!!!!!!!!!!!!!!!!!

[OK - 517153193 bytes]
517153193 bytes copied in 868.128 secs (265652 bytes/sec)
```

La commande boot system

Au démarrage, le code d'amorçage analyse le fichier de configuration de démarrage dans la NVRAM pour les commandes **boot system** qui spécifient le nom et l'emplacement de l'image du logiciel Cisco IOS à charger. Plusieurs commandes **boot system** peuvent être saisies successivement pour créer un plan d'amorçage à tolérance de panne.

En l'absence de commandes **boot system** dans la configuration, le routeur charge par défaut la première image Cisco IOS valide dans la mémoire Flash et l'exécute.

Pour passer à l'image IOS copiée après que cette image ait été enregistrée sur la mémoire flash du routeur, configurez le routeur pour qu'il charge la nouvelle image au démarrage en utilisant la commande **boot system** Enregistrez la configuration. Redémarrez le routeur pour qu'il démarre avec la nouvelle image.

```
R1# configure terminal
R1(config)# boot system flash0:isr4200-universalk9_ias.16.09.04.SPA.bin
R1(config)# exit
R1# copy running-config startup-config
R1# reload
```

Packet Tracer - Utiliser un serveur TFTP pour mettre à jour une image IOS Cisco

Dans ce Packet Tracer, vous atteindrez les objectifs suivants:

- Partie 1: Mettre à niveau d'une image IOS sur un périphérique Cisco
- Partie 2: Sauvegarder une image IOS sur un serveur TFTP

10.8 Module Practice and Questionnaire

Packet Tracer - Configurer CDP, LLDP et NTP

Dans cette activité Packet Tracer, vous remplirez les objectifs suivants:

- Création du réseau et configuration des paramètres de base des périphériques
- Détection de réseaux avec le protocole CDP
- Détection de réseaux avec le protocole LLDP
- Configuration et vérification du protocole NTP

Travaux pratiques - Configurer CDP, LLDP et NTP

Au cours de ces travaux pratiques, vous aborderez les points suivants:

- Créer le réseau et configurer les paramètres de base des périphériques
- Détection de réseaux avec le protocole CDP
- Détection de réseaux avec le protocole LLDP
- Configuration et vérification du protocole NTP

Qu'est-ce que j'ai appris dans ce module?

- CDP (Cisco Discovery Protocol) est un protocole propriétaire de couche 2 de Cisco qui permet de rassembler des informations sur les périphériques Cisco qui partagent la même liaison de données.
- Le protocole CDP peut être utilisé comme outil de détection réseau pour analyser les données des périphériques voisins. Ces données collectées par le protocole CDP peuvent vous aider à développer une topologie logique d'un réseau lorsque la documentation est manquante ou manque de précision.
- Sur les périphériques Cisco, le protocole CDP est activé par défaut. Pour activer CDP globalement pour toutes les interfaces prises en charge sur le périphérique, saisissez cdp run comme mode de configuration globale. Pour activer CDP sur l'interface spécifique, entrez la commande cdp enable.
- Pour vérifier l'état du protocole CDP et afficher une liste des voisins, utilisez la commande show cdp neighbors en mode d'exécution privilégié.
- Les périphériques Cisco prennent également en charge le protocole LLDP (Link Layer Discovery Protocol), qui est un protocole de détection de voisin indépendant similaire au protocole CDP.
- Pour activer le LLDP globalement sur un périphérique réseau Cisco, entrez la commande lldprun dans le mode de configuration globale.

Qu'est-ce que j'ai appris dans ce module? (Cont.)

- Lorsque le protocole LLDP est activé, les voisins de l'appareil peuvent être détectés à l'aide de la commande show lldp neighbors. Pour plus d'informations sur les voisins, utilisez la commande show lldp neighbors detail qui permet d'obtenir la version IOS et l'adresse IP des voisins ainsi que la capacité de l'appareil.
- Si l'heure n'est pas synchronisée entre les différents périphériques, il vous sera impossible de déterminer l'ordre des événements et leurs causes.
- Vous pouvez configurer manuellement la date et l'heure, ou vous pouvez configurer le NTP, qui permet aux périphériques du réseau de synchroniser leurs paramètres d'heure avec un serveur NTP.
- Les réseaux NTP utilisent un système hiérarchique de sources temporelles et chaque niveau de ce système est appelé une strate. Les sources de temps faisant autorité, également appelées dispositifs de strate 0, sont des dispositifs de chronométrage de haute précision. Les périphériques de strate 1 sont directement connectés aux sources temporelles faisant autorité. Les périphériques de strate 2, tels que les clients NTP, synchronisent leur horloge à l'aide des paquets NTP des serveurs de la strate 1.
- La commande ntp server ip-address est émise en mode de configuration globale pour configurer un périphérique en tant que serveur NTP.

Qu'est-ce que j'ai appris dans ce module? (Cont.)

- Pour vérifier si la source temporelle est définie sur NTP, utilisez à nouveau la commande show clock detail. Les commandes show ntp associations et show ntp status sont utilisées pour vérifier qu'un appareil est synchronisé avec le serveur NTP.
- SNMP est un protocole de couche Application qui procure un format pour les messages de communication entre les gestionnaires et les agents.
- Le système SNMP se compose de trois éléments : gestionnaire SNMP, agents SNMP et MIB.
- Le gestionnaire SNMP peut collecter des informations à partir d'un agent SNMP à l'aide de l'action «get» et modifier des configurations sur un agent à l'aide de l'action «set». Les agents SNMP peuvent transmettre des informations directement à un gestionnaire de réseau en utilisant des "pièges".
- SNMPv1, SNMPv2c et SNMPv3 sont toutes des versions de SNMP. SNMPv1 est une solution héritée. Les deux protocoles SNMPv1 et SNMPv2c utilisent une forme de sécurité basée sur la communauté. Le protocole SNMPv3 fournit des services à la fois pour les modèles et les niveaux de sécurité.
- La base de données MIB organise les variables de manière hiérarchique. Les OID identifient de manière unique les objets gérés au sein de la hiérarchie MIB. Le navigateur SNMP de Cisco sur le site http://www.cisco.com permet à un administrateur réseau de rechercher des détails sur un OID particulier.
- Le protocole Syslog utilise le port 514 pour permettre aux périphériques réseau d'envoyer leurs

Qu'est-ce que j'ai appris dans ce module? (Cont.)

- Le service de journalisation syslog fournit trois fonctions principales : collecter des informations de consignation pour la surveillance et le dépannage, sélectionner le type d'informations de consignation capturées et spécifier les destinations des messages syslog capturés.
- Destinations for syslog messages include the logging buffer (RAM inside a router or switch), console line, terminal line, and syslog server.
- Les capacités Syslog permet de déterminer et de catégoriser les données d'état du système pour les rapports des messages d'événement et d'erreur. Les services de message syslog courants signalés sur les routeurs Cisco IOS comprennent : IP, protocole OSPF, système d'exploitation SYS, IPsec et IF.
- Le format par défaut des messages syslog sur le logiciel Cisco IOS est: %facility-severity-MNEMONIC: description.
- Utilisez la commande service timestamps log datetime pour forcer les événements enregistrés à afficher la date et l'heure.
- Le Cisco IFS permet à l'administrateur de naviguer dans différents répertoires et de répertorier les fichiers dans un répertoire, et de créer des sous-répertoires en mémoire flash ou sur un disque.
- Utilisez la commande "Show file systems" pour visualiser les systèmes de fichiers sur un commutateur Catalyst ou un routeur Cisco.

Qu'est-ce que j'ai appris dans ce module? (Cont.)

- Vous pouvez également utiliser Tera Term pour enregistrer les fichiers de configuration dans un document texte. Une configuration peut être copiée à partir d'un fichier et ensuite directement collée sur un périphérique.
- Les fichiers de configuration peuvent être stockés sur un serveur TFTP (Trivial File Transfer Protocol) ou sur un périphérique de stockage USB.
- Pour enregistrer la configuration d'exécution ou la configuration de démarrage sur un serveur TFTP, utilisez soit la commande copy running-config tftp ou copy startup-config tftp
- Les images du logiciel Cisco IOS et les fichiers de configuration peuvent être stockés sur un serveur TFTP central pour contrôler le nombre d'images IOS et les révisions correspondantes, ainsi que les fichiers de configuration qui doivent être conservés.
- Sélectionnez un fichier d'image Cisco IOS répondant aux exigences en termes de plate-forme, de fonctionnalités et de logiciel. Téléchargez le fichier à partir de cisco.com et transférez-le sur le serveur TFTP.
- Pour passer à l'image IOS copiée après que cette image ait été enregistrée sur la mémoire flash du routeur, configurez le routeur pour qu'il charge la nouvelle image au démarrage en utilisant la commande boot system .

Nouveaux termes et commandes

- Protocole CDP (Cisco Discovery Protocol)
- **cdp run**
- **cdp enable**
- **show cdp**
- **show cdp interface**
- **show cdp neighbors**
- **show cdp neighbors detail**
- Protocole LLDP (Link Layer Discovery Protocol)
- **lldp run**
- **lldp enable**
- **lldp transmit**
- **lldp receive**
- **show lldp**
- **show lldp neighbors**
- **show lldp neighbors detail**
- **clock set hh:mm:ss mm dd yyyy**
- Protocole NTP (Network Time Protocol)
- Strate
- **show clock**
- **show clock detail**
- **ntp server ip-address**
- **show ntp associations**
- **show ntp status**
- Protocole SNMP (Simple Network Management Protocol)
- système de gestion de réseau
- Gestionnaire SNMP
- Agent SNMP
- Base d’informations de gestion (MIB)
- ID d'objet (OID)
- get-request
- get-next-request
- get-bulk-request
- get-response
- set-request

Nouveaux termes et commandes (Suite)

- Variable MIB
- Déroutement par agent SNMP
- SNMPv1
- SNMPv2c
- SNMPv3
- noAuthNoPriv
- authNoPriv
- authPriv
- Identifiants de communauté
- snmpget
- Navigateur d'objets Cisco SNMP
- Syslog
- Fonctions de message Syslog
- **service timestamps log datetime**
- Système de fichiers intégré Cisco (IFS)
- show file systems
- bootflash
- **pwd**
- **copy running-config tftp**
- **copy tftp running-config**
- **copy running-config usbflash0:**
- ROMMON
- **confreg**
- **config-register**
- **copy tftp: flash:**
- **boot system**


CISCO