

# Chapitre 2:

## Sécurisation des périphériques réseau

CCNA Security v2.0

Samir DIABI



# Sommaire

2.0 Introduction

2.1 sécurisation de dispositif d'accès

2.2 assigner des rôles administratifs

2.3 surveillance et gestion des périphériques

2.4 à l'aide de sécurité automatisée dispose d'assurer le contrôle avion

2.6 Résumé

# Section 2.1 : Sécurisation de l'accès de l'appareil

À la fin de cette section, vous devriez être en mesure de :

- Expliquer comment sécuriser un réseau de périmètre.
- Configurer un accès administratif sécurisé aux routeurs Cisco.
- Configurer la sécurité améliorée pour les connexions d'accès virtuelles.
- Configurer un démon SSH pour l'administration à distance sécurisée.

## Rubrique 2.1.1 : Sécuriser le routeur de périphérie



# Sécurisation de l'Infrastructure réseau

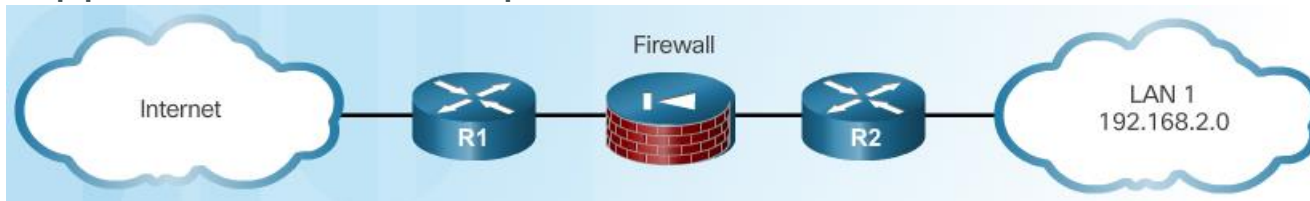


# Approches de sécurité routeur de périphérie

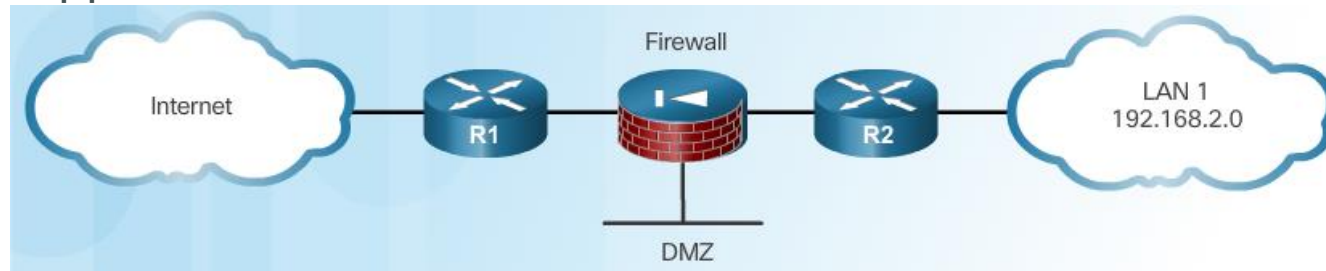
## Approche routeur seul



## Approche Défense en profondeur



## Approche DMZ



# Trois domaines de la sécurité du routeur

Sécurité  
physique

Sécurité de  
l'IOS et du  
fichier de  
configuration

Durcissement  
du routeur



# Sécuriser les accès administratifs

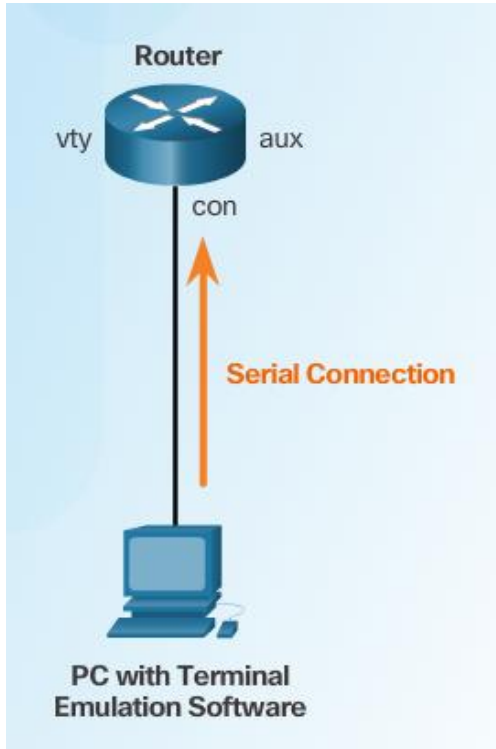
## Tâches:

- Restriction des accès aux équipements
- Comptes et journaux d'accès
- Accès authentique
- Actions autorisés
- Présence des notifications légale
- Assurer la confidentialité

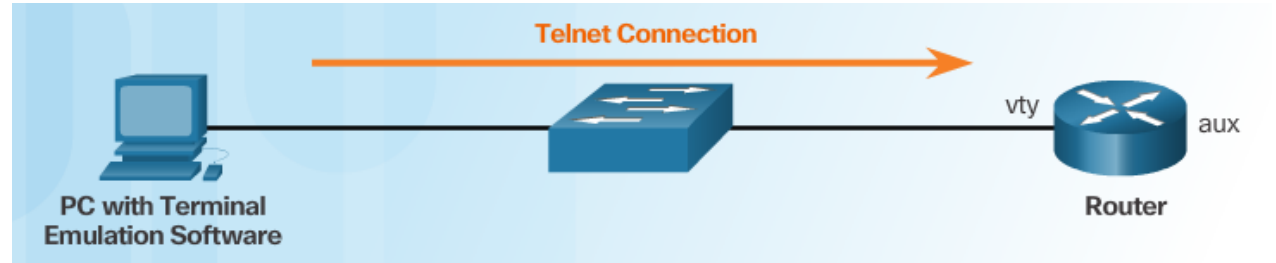


# Sécuriser l'accès Local et distant

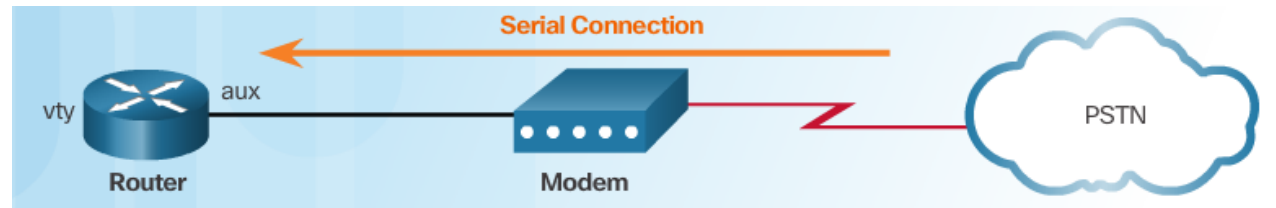
## Accès local



## Accès à distance à l'aide de Telnet

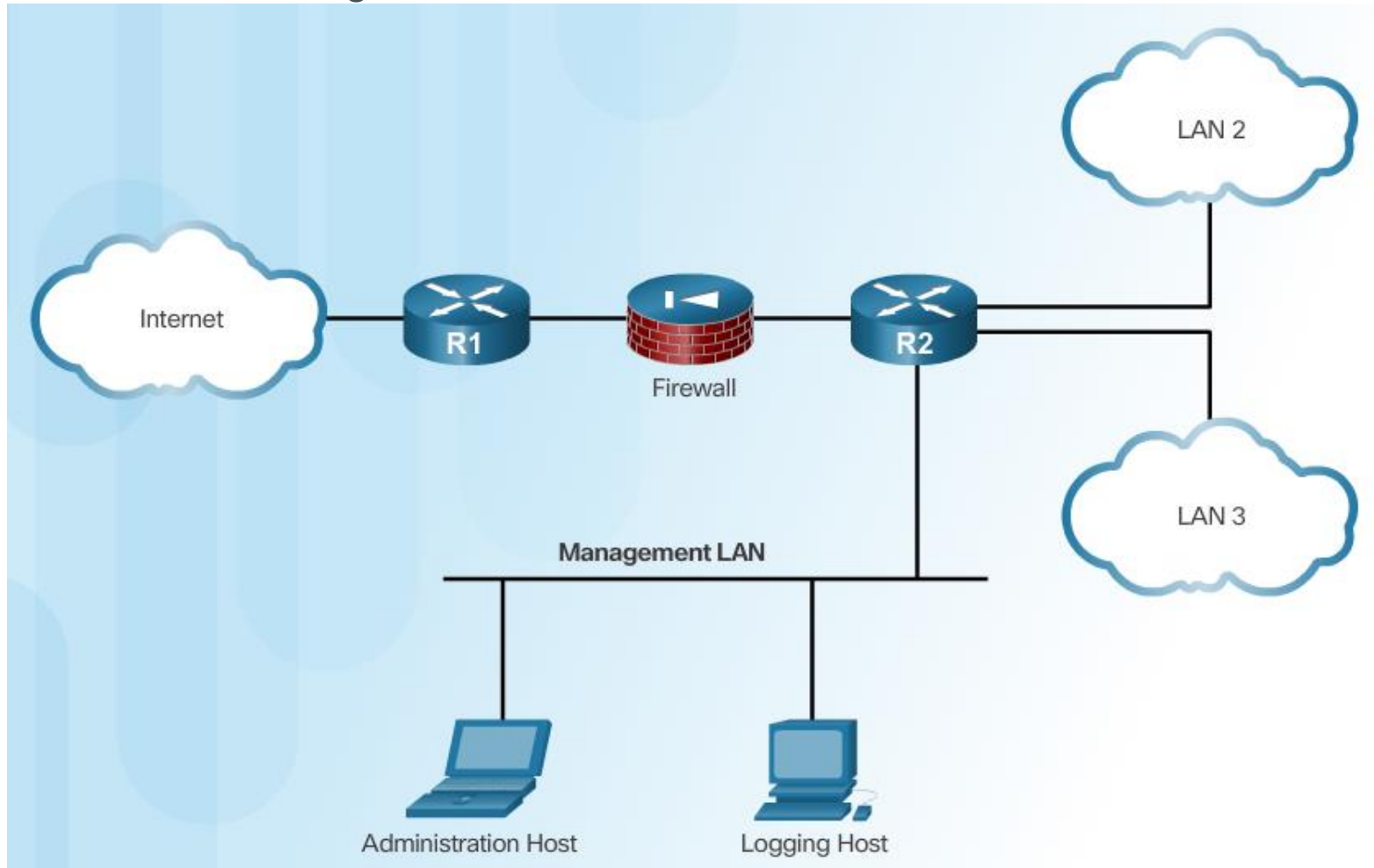


## Accès à distance à l'aide de Modem et Port Aux



# Sécuriser l'accès Local et distant (Cont.)

Réseau de management dédié



## Rubrique 2.1.2 : Configuration sécurisée accès administratif



# Mots de passe forts

## Guide:

- Utiliser des mots de passe de plus de 10 caractères.
- Inclure minuscule, majuscule, caractères spéciaux chiffres et espace.
- Eviter les mots de passes basés sur des pièces d'information facilement identifiables.
- Dicter différemment un mot de passe (Smith = Smyth = 5mYth).
- Changer régulièrement de mot de passe.
- Ne pas écrire les mots de passe pour les laisser dans des endroits accessibles.

Weak Password	Why it is Weak	Strong Password	Why it is Strong
secret	Simple dictionary password	b67n42d39c	Combines alphanumeric characters
smith	Mother's maiden name	12^h u4@1p7	Combines alphanumeric characters, symbols, and includes a space
toyota	Make of car		
bob1967	Name and birthday of user		
Blueleaf23	Simple words and numbers		

# Améliorer la sécurité des accès

```
R1(config)# security passwords min-length 10
R1(config)# service password-encryption
R1(config)# line vty 0 4
R1(config-line)# exec-timeout 3 30
R1(config-line)# line console 0
R1(config-line)# exec-timeout 3 30
```

```
R1(config)# service password-encryption
R1(config)# exit
R1# show running-config

<output omitted>
line con 0
  exec-timeout 3 30
  password 7 094F471A1A0A
  login
line aux 0
  exec-timeout 3 30
  password 7 094F471A1A0A
  login
line vty 0 4
  password 7 094F471A1A0A
  login
```

Cisco Cracker

094F471A1A0A

Crack it

Password = Cisco

# Algorithmes des mots de passes secrets

## Guidelines:

- Configurer tous les mots de passe secrets à l'aide de type 8 ou mots de passe de type 9
- La syntaxe de la commande *enable algorithm-type* permet d'entrer un mot de passe non crypté

```
Router(config) #
```

```
enable algorithm-type {md5 | scrypt | sha256 } secret unencrypted-password
```

- Utilisez la commande *username algorithm-type* pour spécifier cryptage du type 9

```
Router(config) #
```

```
username name algorithm-type {md5 | scrypt | sha256 } secret unencrypted-password
```

# Securing Line Access

```
R1(config)# username Bob algorithm-type scrypt secret cisco54321
R1(config)# line con 0
R1(config-line)# no password
R1(config-line)# login local
R1(config-line)# exit
R1(config)# line aux 0
R1(config-line)# no password
R1(config-line)# login local
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
```

## Rubrique 2.1.3 : Configuration de sécurité renforcée pour les connexions virtuelles





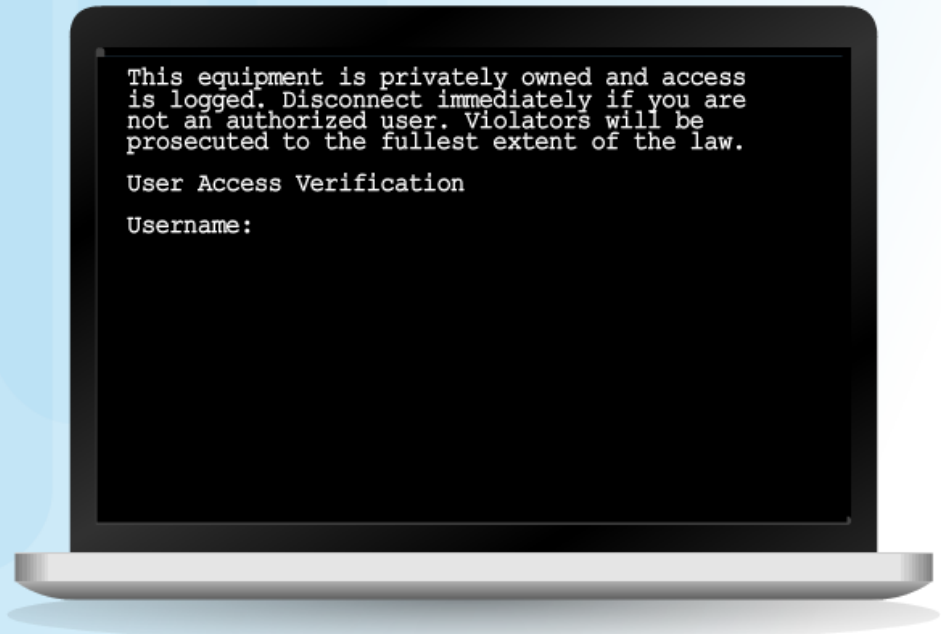
# Améliorer le processus de Login

Améliorations de sécurité de connexion virtuelle :

- Configurer des délais entre les tentatives de connexion successives
- Permettre l'arrêt de la connexion si des attaques DoS sont soupçonnés.
- Générer des messages de journalisation système pour la détection de connexion

R1 (config) #

```
banner {motd | exec | login} delimiter message delimiter
```



```
This equipment is privately owned and access  
is logged. Disconnect immediately if you are  
not an authorized user. Violators will be  
prosecuted to the fullest extent of the law.
```

```
User Access Verification
```

```
Username:
```

# Configurez des fonctionnalités de mise en valeur de Login

R1(config)#

```
login block-for seconds attempts tries within seconds
```

R1(config)#

```
login quiet-mode access-class {acl-name|acl-number}
```

R1(config)#

```
login delay seconds
```

R1(config)#

```
login on-success log [every login]
```

R1(config)#

```
login on-failure log [every login]
```

# Activer le renforcement des Login

Syntaxe de la commande : *login block-for*

```
router(config)#
```

```
login block-for seconds attempts tries within seconds
```

```
R1(config)# login block-for 120 attempts 5 within 60
```

Exemple: *login quiet-mode access-class*

```
R1(config)# ip access-list standard PERMIT-ADMIN  
R1(config-std-nacl)# remark Permit only Administrative hosts  
R1(config-std-nacl)# permit 192.168.10.10  
R1(config-std-nacl)# permit 192.168.11.10  
R1(config-std-nacl)# exit  
R1(config)# login quiet-mode access-class PERMIT-ADMIN
```

Exemple: *login delay*

```
R1(config)# login delay 3
```

# Journaliser les accès infructueux

## Générer des Messages Syslog Login

```
R1(config)# login on-success log [every login]
R1(config)# login on-failure log [every login]
R1(config)# security authentication failure rate threshold-rate log
```

## Exemple: *show login failures*

```
R1# show login failures
Total failed logins: 22
Detailed information about last 50 failures
```

Username	SourceIPAddr	lPort	Count	TimeStamp
admin	1.1.2.1	23	5	15:38:54 UTC Wed Dec 10 2008
Admin	10.10.10.10	23	13	15:58:43 UTC Wed Dec 10 2008
admin	10.10.10.10	23	3	15:57:14 UTC Wed Dec 10 2008
cisco	10.10.10.10	23	1	15:57:21 UTC Wed Dec 10 2008

```
R1#
```

## Rubrique 2.1.4 : Configuration de SSH



# Étapes de configuration SSH

## Exemple configuration de SSH

```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R1(config)#
*Feb 16 21:18:41.977: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# ip ssh version 2
R1(config)# username Bob algorithm-type scrypt secret cisco54321
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# end
R1#
```

## Exemple vérification de SSH

```
R1# show crypto key mypubkey rsa
% Key pair was generated at: 21:18:41 UTC Feb 16 2015
Key name: R1.span.com
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
 30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CF35DB
A58A1BDB F7C7E600 F189C2F3 2EC6E584 D923EE5B 71841D98 B5472A03 D19CD620
ED125825 5A58412B B7F29234 DE2A1809 6C421AC3 07F298E6 80BE149D 2A262E13
74888DAF CAC8F187 B11111AF A413E76F 6C157CDF DFEF0D82 2961B58C BE1CAD21
176E82B9 6D81F893 06E66C93 94E1C508 887462F6 90AC63CE 5E169845 C1020301 0001

% Key pair was generated at: 21:18:42 UTC Feb 16 2015
Key name: R1.span.com.server
Key type: RSA KEYS
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00AB914D 8172DFBE
DE57ACA9 7B844239 1F3B5942 3943AC0D F54E7746 3895CF54 606C3961 8A44FEB3
1A019F27 D9E71AAE FC73F423 A59CB8F5 50289272 3392CEBC 4C3CBD6D DB9233DE
9DDD9DAD 79D56165 4293AA62 FD1CBAB2 7AB859DC 2890C795 ED020301 0001

R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# crypto key zeroize rsa
% All keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
R1(config)#
```

# Modifier la configuration de SSH

```
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 120 secs; Authentication retries: 3
<output omitted>

R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip ssh time-out 60
R1(config)# ip ssh authentication-retries 2
R1(config)# ^Z
R1#
*Feb 16 21:23:51.237: %SYS-5-CONFIG_I: Configured from console by console
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 60 secs; Authentication retries: 2
<output omitted>
```

# Utiliser SSH sur un routeur

Deux façons pour se connecter :

- Activer SSH et utiliser un routeur Cisco comme client ou serveur SSH.
  - En tant que serveur, le routeur peut accepter des connexions client SSH
  - En tant que client, le routeur peut se connecter via SSH à un autre routeur SSH
- Utiliser un client SSH en cours d'exécution sur un ordinateur hôte, comme le mastic, OpenSSH ou TeraTerm.



# Section 2.2 :

## Assigner des rôles d'administration

À la fin de cette section, vous devriez être en mesure de :

- Configurer les niveaux de privilèges d'administrateur pour la disponibilité de commande de contrôle.
- Configurer l'accès CLI basé sur les rôles de contrôle des commandes de disponibilité.

## Rubrique 2.2.1 : Configuration des niveaux de privilège



# Limiter la disponibilité des commandes

## Niveaux de privilèges:

- Niveau 0: rarement utilisé, mais inclut 5 commandes: disable, enable, exit, help et disconnect.
- Niveau 1: Niveau d'accès par défaut (invite router>).
- Niveaux 2-14: peuvent être personnalisés pour différents niveaux de privilèges.
- Niveau 15: Réservé pour le mode enable (privilegié).

## Levels of access commands:

- User EXEC mode (privilege level 1)  
Lowest EXEC mode user privileges  
Only user-level command available at the router> prompt
- Privileged EXEC mode (privilege level 15)  
All enable-level commands at the router# prompt

## Syntaxe des niveaux des privilèges

Router(config)#

```
privilege mode {level level | reset} command
```

### Command

### Description

<i>mode</i>	Specifies the configuration mode. Use the <b>privilege ?</b> command to see a complete list of router configuration modes available on your router.
<b>level</b>	(Optional) Enables setting a privilege level with a specified command.
<i>level</i>	(Optional) The privilege level that is associated with a command. You can specify up to 16 privilege levels, using numbers 0 to 15.
<b>reset</b>	(Optional) Resets the privilege level of a command.
<i>command</i>	(Optional) Argument to use when you want to reset the privilege level.

# Configurer et attribuer des niveaux de privilège

```
R1# conf t
R1(config)# !Level 5 and SUPPORT user configuration
R1(config)# privilege exec level 5 ping
R1(config)# enable algorithm-type scrypt secret level 5 cisco5
R1(config)# username SUPPORT privilege 5 algorithm-type scrypt
secret cisco5
R1(config)# !Level 10 and JR-ADMIN user configuration
R1(config)# privilege exec level 10 reload
R1(config)# enable algorithm-type scrypt secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 algorithm-type scrypt
secret cisco10
R1(config)# !Level 15 and ADMIN user configuration
R1(config)# enable algorithm-type scrypt secret level 15 cisco123
R1(config)# username ADMIN privilege 15 algorithm-type scrypt secret
cisco123
```

# Limite les niveaux de privilège

- Aucun contrôle d'accès aux interfaces spécifiques, des ports, des interfaces logiques et machines à sous sur un routeur
- Commandes disponibles aux niveaux de privilèges inférieurs sont toujours exécutables à des niveaux plus élevés de privilège
- Commandes spécifiquement fixés à un niveau de privilège plus élevé ne sont pas disponibles pour les utilisateurs de privilège inférieurs
- Affectation d'une commande avec plusieurs mots clés permet d'accéder à toutes les commandes qui utilisent ceux

## Rubrique 2.2.2 : Configuration basée sur les rôles CLI



# Accès basé sur les rôles CLI

Par exemple:

- Security operator privileges

- Configure AAA

- Issue **show** commands

- Configure firewall

- Configure IDS/IPS

- Configure NetFlow

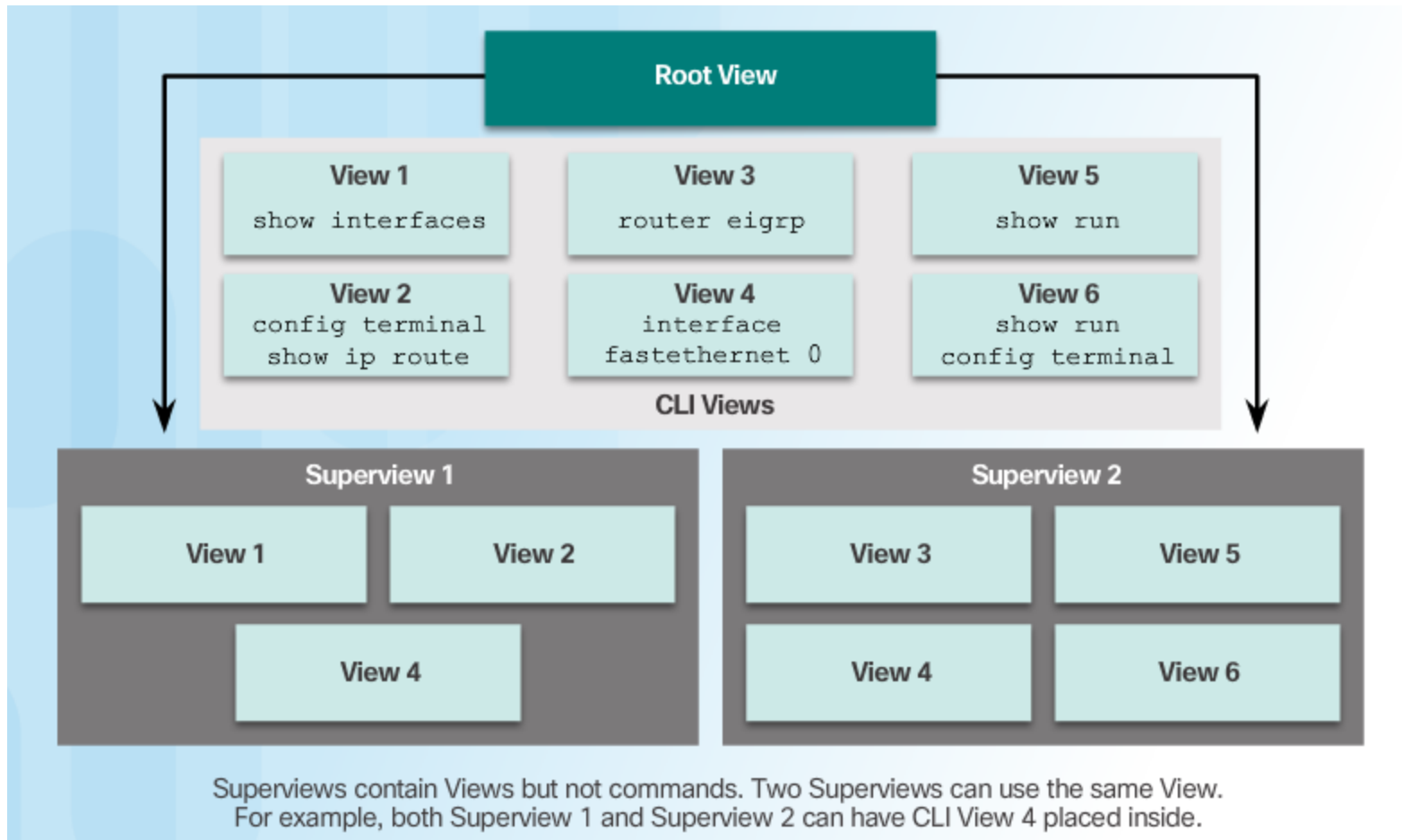
- WAN engineer privileges

- Configure routing

- Configure interfaces

- Issue **show** commands

# Role-Based Views





# Configuration basée sur les rôles CLI

## root view

- ***Une root view ou vue racine :***
  - Il s'agit de la vue permettant la gestion des View et Superview.
  - Il est nécessaire de disposer d'un niveau de privilège 15 pour accéder à la vue root.
  - Il est naturellement conseillé d'appliquer un mot de passe à l'accès de la vue racine.

# Configuration basée sur les rôles CLI view

- ***Une View ou vue est un profil disposant des caractéristiques suivantes :***
  - Une vue dépend toujours de la vue root ou d'une super vue
  - Une vue contient la liste des différentes commandes pouvant être exécutées par l'exploitant.
  - La création d'une vue ne nécessite pas obligatoirement l'application d'un niveau de privilège.
  - Le niveau de privilège est tout simplement régi par les commandes pouvant être exécutées.
  - Il est fortement conseillé d'appliquer un mot de passe à l'ensemble des vue.
  - Les vues sont indépendantes les unes des autres.

# Configuration basée sur les rôles CLI Superview

- ***Une superview ou super-vue est un profil disposant des caractéristiques suivantes :***
  - Une super-vue dépend toujours de la vue root
  - Une super-vue contient la liste des différents profils (view) appartenant par exemple à une entité administrative de l'organisation.
  - La création d'une super-vue ne nécessite pas l'application d'un niveau de privilège.
  - Il est fortement conseillé d'appliquer un mot de passe à l'ensemble des super- vue.
  - Les super-vue sont indépendantes les unes des autres.
  - Une vue peut appartenir à plusieurs super vues.
  - Il n'est pas possible d'associer des commandes à une super vues, ceci est le rôle d'une vue

# Configuration basée sur les rôles CLI View

## Étape 1

Router#

```
enable [view view-name]
```

## Étape 2

Router(config)#

```
parser view view-name
```

## Étape 3

Router(config-view)#

```
secret encrypted-password
```

## Étape 4

Router(config-view)#

```
commands parser mode {include | include-exclusive | exclude} [all]  
[interface interface-name | command]
```

# Configuration basée sur les rôles CLI Superview

## Étape 1

```
Router(config)#
```

```
parser view view-name superview
```

## Étape 2

```
Router(config-view)#
```

```
secret encrypted-password
```

## Étape 3

```
Router(config-view)#
```

```
view view-name
```

# Vérifier les CLI basée sur les rôles vues

Activer l'affichage de la vue racine et de vérifier toutes les vues

```
R1# show parser view
Current view is 'JR-ADMIN'

R1# enable view
Password:

R1# show parser view
Current view is 'root'

R1# show parser view all
Views/SuperViews Present in System:
  SHOWVIEW
  VERIFYVIEW
  REBOOTVIEW
  USER *

  SUPPORT *

  JR-ADMIN *

----- (*) represent superview-----
R1#
```

# Article 2.3 :

## Surveillance et gestion des périphériques

À la fin de cette section, vous devriez être en mesure de :

- Utilisez la fonctionnalité de configuration résiliente de Cisco IOS pour sécuriser les fichiers d'image et de configuration Cisco IOS.
- Comparer les accès de gestion intrabande et hors de bande.
- Configurer syslog pour la consignation des événements système.
- Configurer à l'aide d'un accès sécurisé SNMPv3
- Configurer NTP pour activer un horodatage précis entre tous les périphériques.

## Rubrique 2.3.1 : Sécuriser l'image Cisco IOS et les fichiers de Configuration





# Fonctionnalité de Configuration résiliente

## Cisco IOS

- Un des soucis majeurs pour un administrateur est de réduire le temps d'arrêt lorsqu'un ou plusieurs routeurs ont été compromis et que l'image IOS ou le fichier de configuration ont été supprimés.
- La fonctionnalité Cisco IOS Resilient configuration accélère le processus de récupération.
- Le fichier de configuration dans le jeu de démarrage primaire est une copie du fichier de configuration en cours d'exécution quand la fonctionnalité a été activée.
- Cette fonctionnalité ne peut être désactivée qu'à travers une connexion par console.
- La fonctionnalité n'est disponible que sur les systèmes supportant une mémoire flash PCMCIA.

# Activation de la fonctionnalité de résilience Image IOS

```
R1# conf t
R1(config)# secure boot-image
R1(config)#
*Feb 18 17:57:29.035: %IOS_RESILIENCE-5-IMAGE_RESIL_ACTIVE:
Successfully secured running image
R1(config)# secure boot-config
R1(config)#
*Feb 18 18:02:29.459: %IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE:
Successfully secured config archive [flash0:.runcfg-20150218-180228.ar]
R1(config)# exit
R1# show secure bootset
IOS resilience router id FTX1636848Z

IOS image resilience version 15.4 activated at 18:02:04 UTC Wed Feb
18 2015
Secure archive flash0:c1900-universalk9-mz.SPA.154-3.M2.bin type is
image (elf) []
  file size is 75551300 bytes, run size is 75730352 bytes
  Runnable image, entry point 0x81000000, run from ram

IOS configuration resilience version 15.4 activated at 18:02:29 UTC
Wed Feb 18 2015
Secure archive flash0:.runcfg-20150218-180228.ar type is config
configuration archive size 2182 bytes

R1#
```

# L'image principale de la Bootset

```
Router# reload
<Issue Break sequence, if necessary>
rommon 1 > dir flash0:
program load complete, entry point: 0x80803000, size: 0x1b340
Directory of flash0:

4          75551300  -rw-      c1900-universalk9-mz.SPA.154-3.M2.bin
<output omitted>
rommon 2 > boot flash0:c1900-universalk9-mz.SPA.154-3.M2.bin
<Router reboots with specified image>
Router> enable
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# secure boot-config restore flash0:rescue-cfg
ios resilience:configuration successfully restored as flash0:rescue-cfg

Router(config)# end
Router# copy flash0:rescue-cfg running-config
Destination filename [running-config]?
%IOS image resilience is already active
%IOS configuration resilience is already active

2182 bytes copied in 0.248 secs (8798 bytes/sec)

R1#
```

# Configuring Secure Copy

Configurer le routeur pour SCP côté serveur avec AAA locale :

1. Configurer SSH
2. Configurer au moins un utilisateur avec le niveau de privilège 15
3. Activer AAA
4. Préciser que la base de données locale doit être utilisé pour l'authentification
5. Configure command authorization
6. Activer la fonctionnalité de serveur-côté SCP

# Récupérer un mot de passe routeur

1. Se connecter sur le port de la console.
2. Enregistrement de la configuration de Registre paramètre.
3. Cycle d'alimentation du routeur.
4. Numéro de la séquence de rupture.
5. Modifiez le registre de configuration par défaut avec la commande `confreg 0x2142`.
6. Redémarrer le router.
7. Appuyez sur Ctrl-C pour ignorer la procédure de configuration initiale.
8. Mettre le routeur en mode privilégié.
9. Copier la configuration de démarrage de la configuration en cours d'exécution.
10. Vérifier la configuration.
11. Changer le mot de passe enable secret.
12. Activer les interfaces.
13. Modifier le registre, config avec le `configuration_register_setting config-register`.
14. Enregistrez les modifications de configuration.

# Récupération du mot de passe

```
R1(config)# no service password-recovery
WARNING:
Executing this command will disable password recovery
mechanism.
Do not execute this command without another plan for
password recovery.
Are you sure you want to continue? [yes/no]: yes
R1(config)#
```

Désactiver la récupération du mot de passe

Aucune Service de récupération de mot de passe

```
R1# show running-config
Building configuration...

Current configuration : 836 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service password-recovery
```

```
System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.
PLD version 0x10
GIO ASIC version 0x127
c1841 platform with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

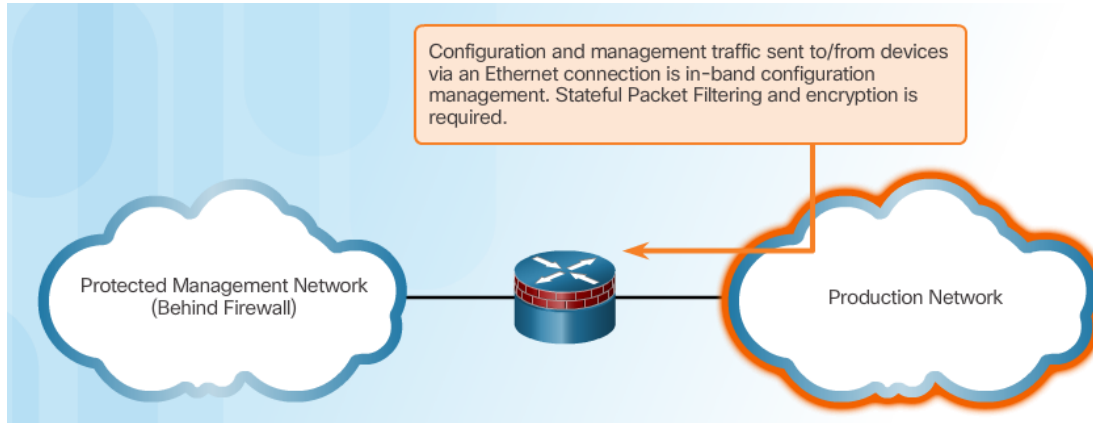
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x8000f000, size:0xcb80
```

Récupération du mot de passe désactivée

## Rubrique 2.3.2 : Gestion sécurisée et rapports



# Déterminer le Type d'accès à l'administration

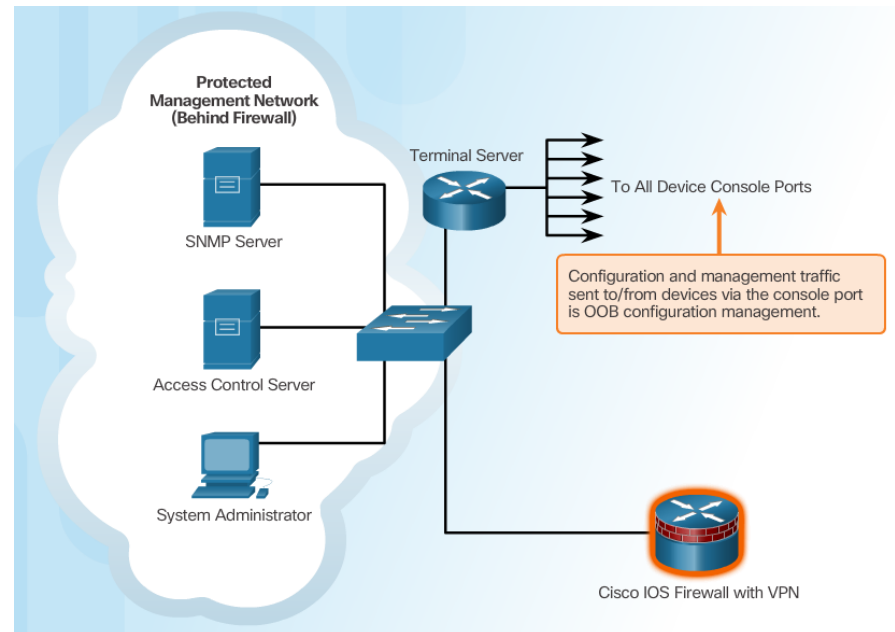


## In-Band Management:

- Apply only to devices that need to be managed or monitored
- Use IPsec, SSH, or SSL when possible
- Decide whether the management channel need to be open at all time

## Out-of-Band (OOB) Management:

- Provide highest level of security
- Mitigate the risk of passing management protocols over the production network

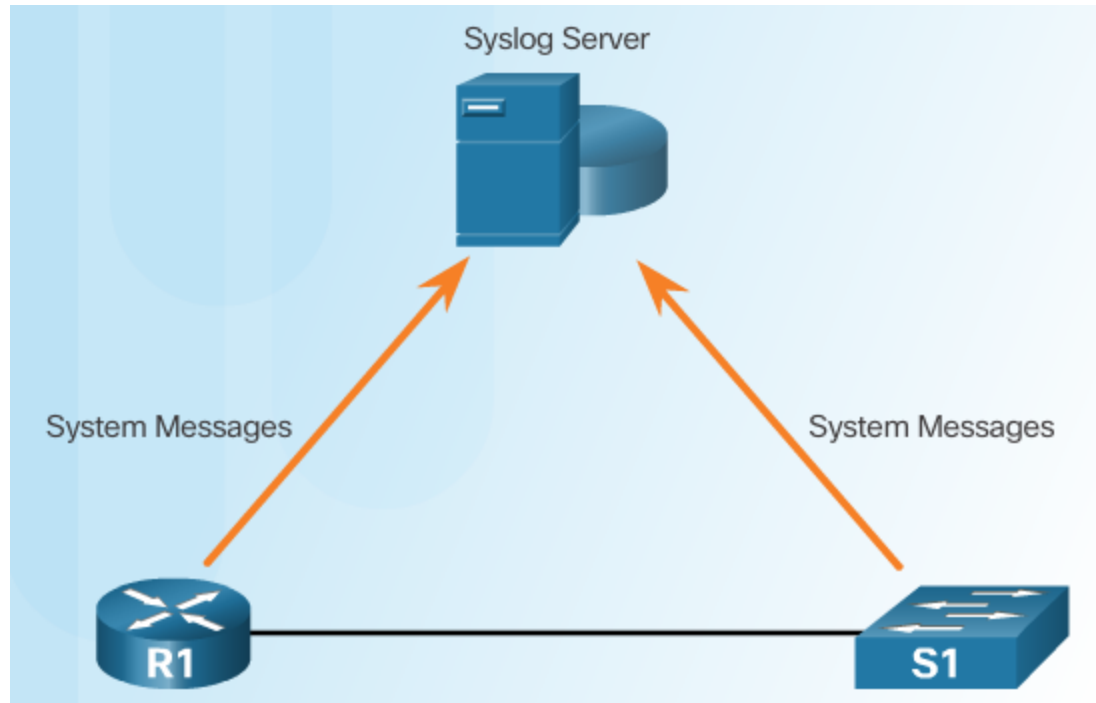




## Rubrique 2.3.3 : À l'aide de Syslog pour sécurité de réseau

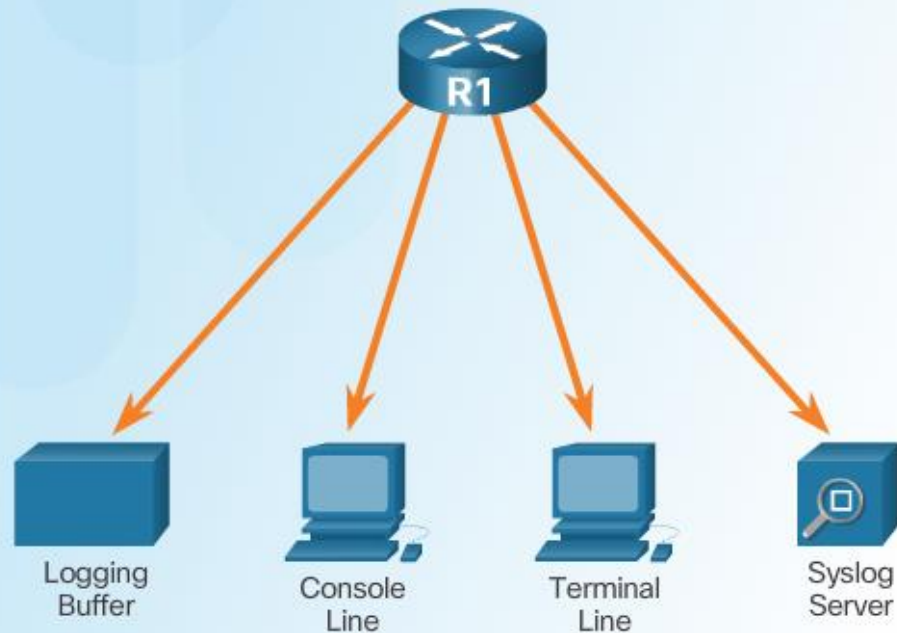


# Introduction to Syslog



# Syslog Operation

```
R1(config-if)# no shutdown
R1(config-if)#
000047: *Feb 19 11:36:47.779: %LINK-3-UPDOWN: Interface Serial0/0/0, changed
state to up
000048: *Feb 19 11:36:48.779: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
```



# Syslog Message

## Security Levels

	Level	Keyword	Description	Definition
Highest Level	0	emergencies	System is unusable	LOG_EMERG
	1	alerts	Immediate action is needed	LOG_ALERT
	2	critical	Critical conditions exist	LOG_CRIT
	3	errors	Error conditions exist	LOG_ERR
	4	warnings	Warning conditions exist	LOG_WARNING
	5	notifications	Normal but significant condition	LOG_NOTICE
	6	informational	Informational messages only	LOG_INFO
Lowest Level	7	debugging	Debugging messages	LOG_DEBUG

## Example Severity Levels

Syslog Level and Name	Definition	Example
0 LOG_EMERG	A panic condition normally broadcast to all users	Cisco IOS software could not load
1 LOG_ALERT	A condition that should be corrected immediately, such as a corrupted system database	Temperature too high
2 LOG_CRIT	Critical conditions; for example, device errors	Unable to allocate memory
3 LOG_ERR	Errors	Invalid memory size
4 LOG_WARNING	Warning messages	Crypto operation failed
5 LOG_NOTICE	Non-error conditions that may require special handling	Interface changed state, up or down
6 LOG_INFO	Informational messages	Packet denied by ACL
7 LOG_DEBUG	Messages that contain information that is normally used only when debugging a program	Packet type invalid

# Syslog Message (Cont.)

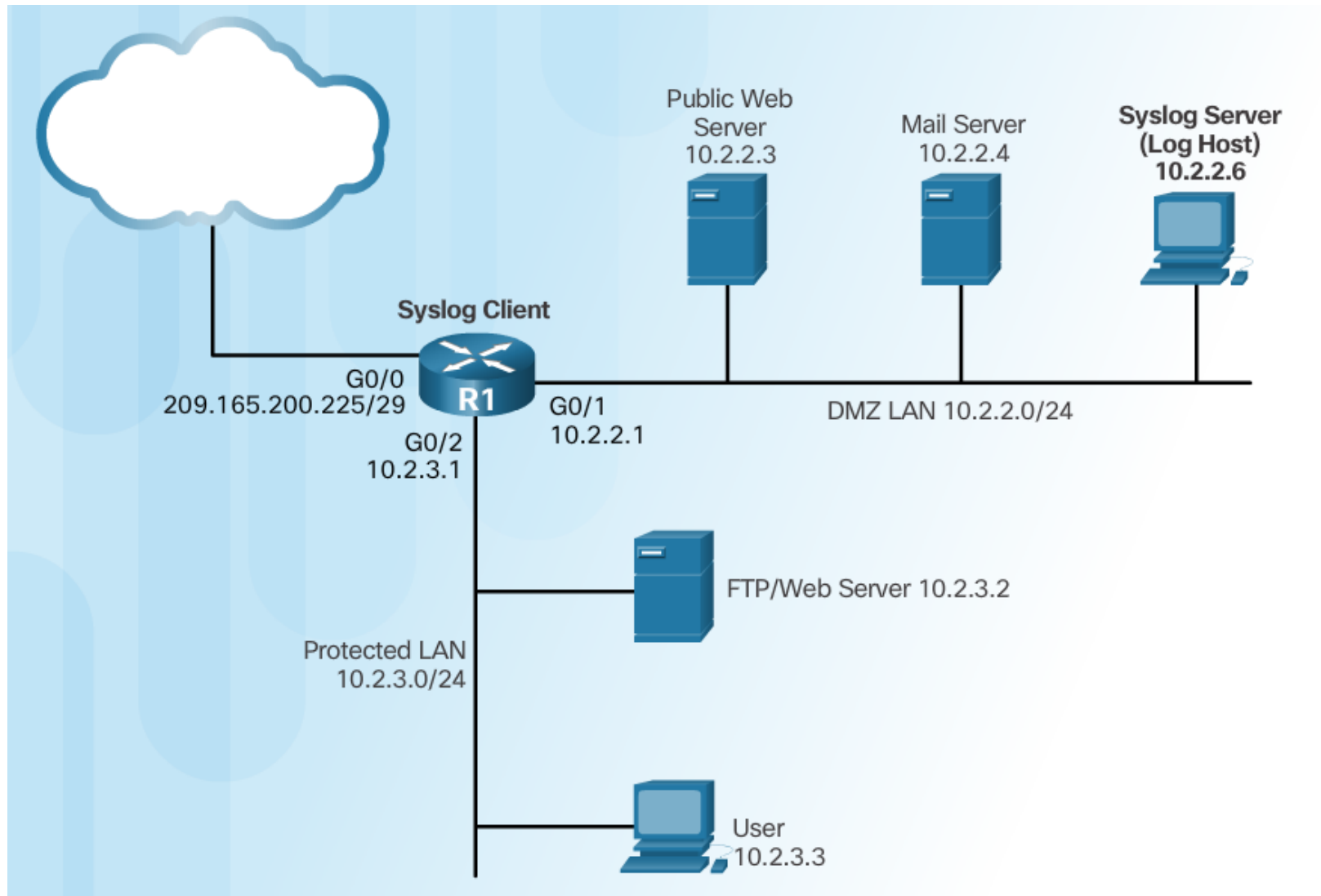
1                      2                      3                      4                      5

```
000048: *Feb 19 11:36:48.779: %LINEPROTO-5-UPDOWN:
Line protocol on Interface Serial10/0/0, changed state to up
```

6

Column 1		Column 2
1	seq no	Stamps log messages with a sequence number if <code>service sequence-numbers</code> is configured.
2	timestamp	displays if <code>service timestamps log</code> is configured
3	facility	denotes the source or the cause of the system message
4	severity	levels 0 - 7
5	MNEMONIC	text string that uniquely describes the message
6	description	text string containing detailed information about the event being reported

# Syslog Systems



# Configuring System Logging

## Step 1

Router(config) #

```
logging host [hostname | ip-address]
```

## Step 2 (optional)

Router(config) #

```
logging trap level
```

## Step 3

Router(config) #

```
logging source-interface interface-type interface-number
```

## Step 4

Router(config) #

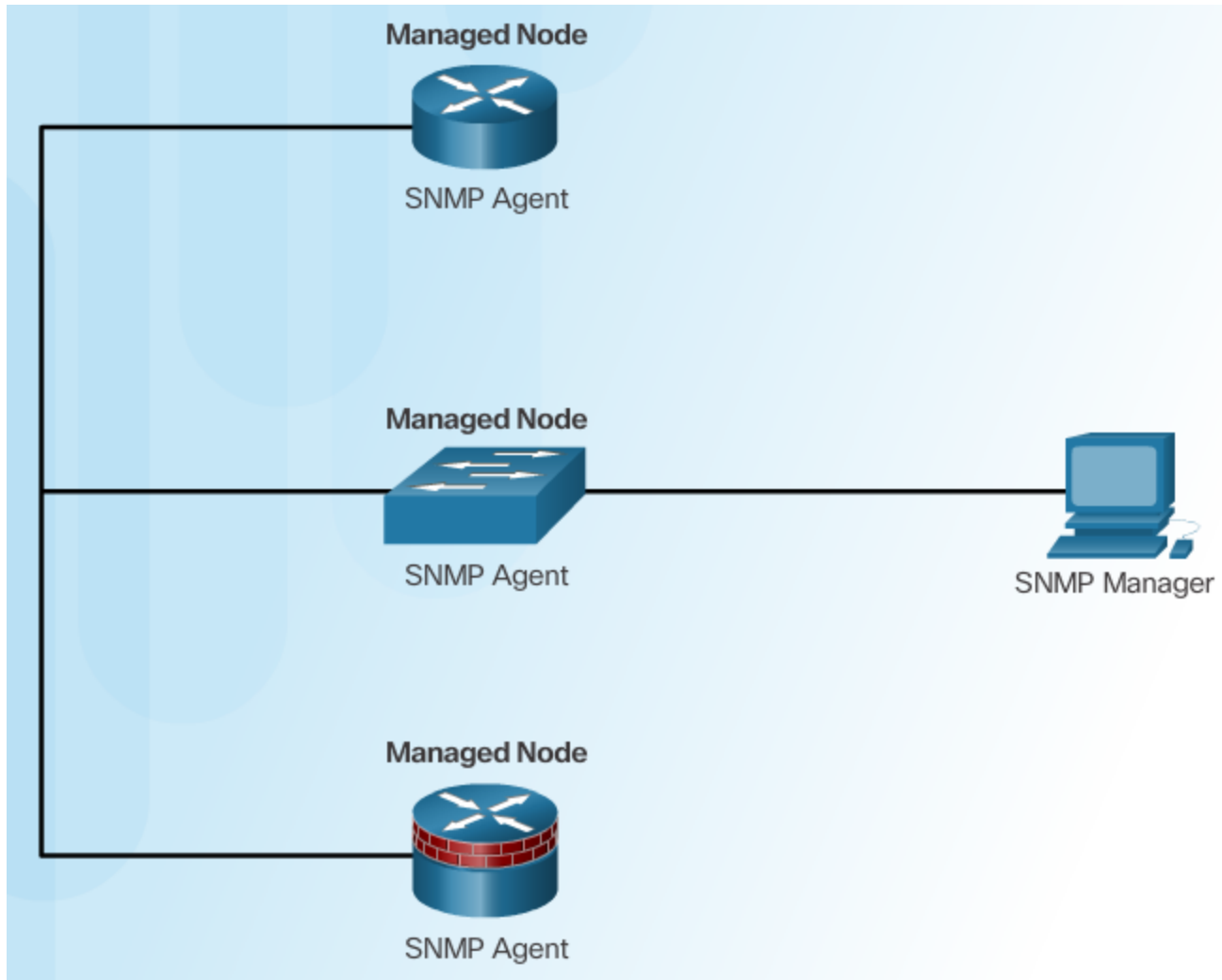
```
logging on
```

## Rubrique 2.3.4 : À l'aide de SNMP pour la sécurité du réseau

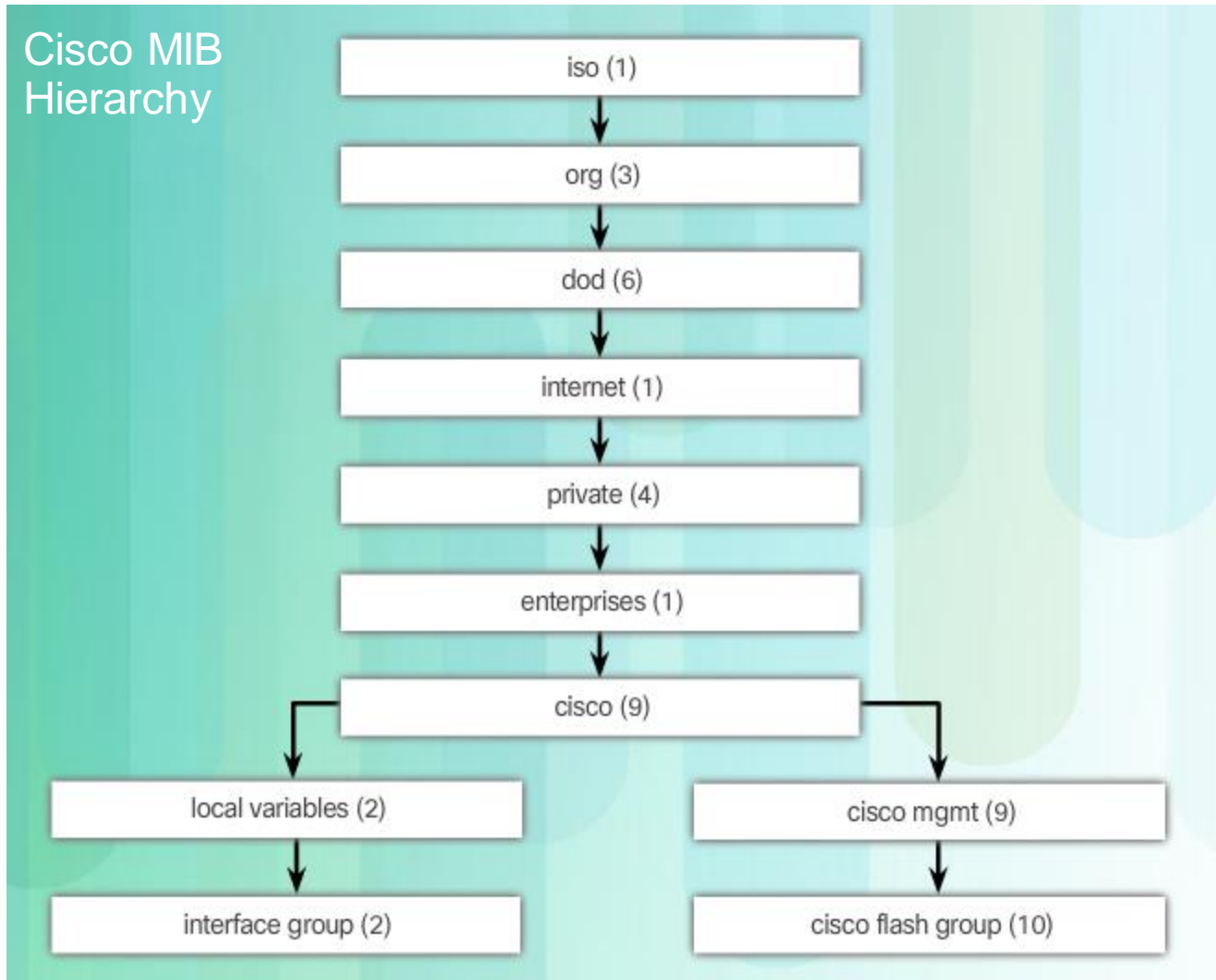




# Introduction to SNMP



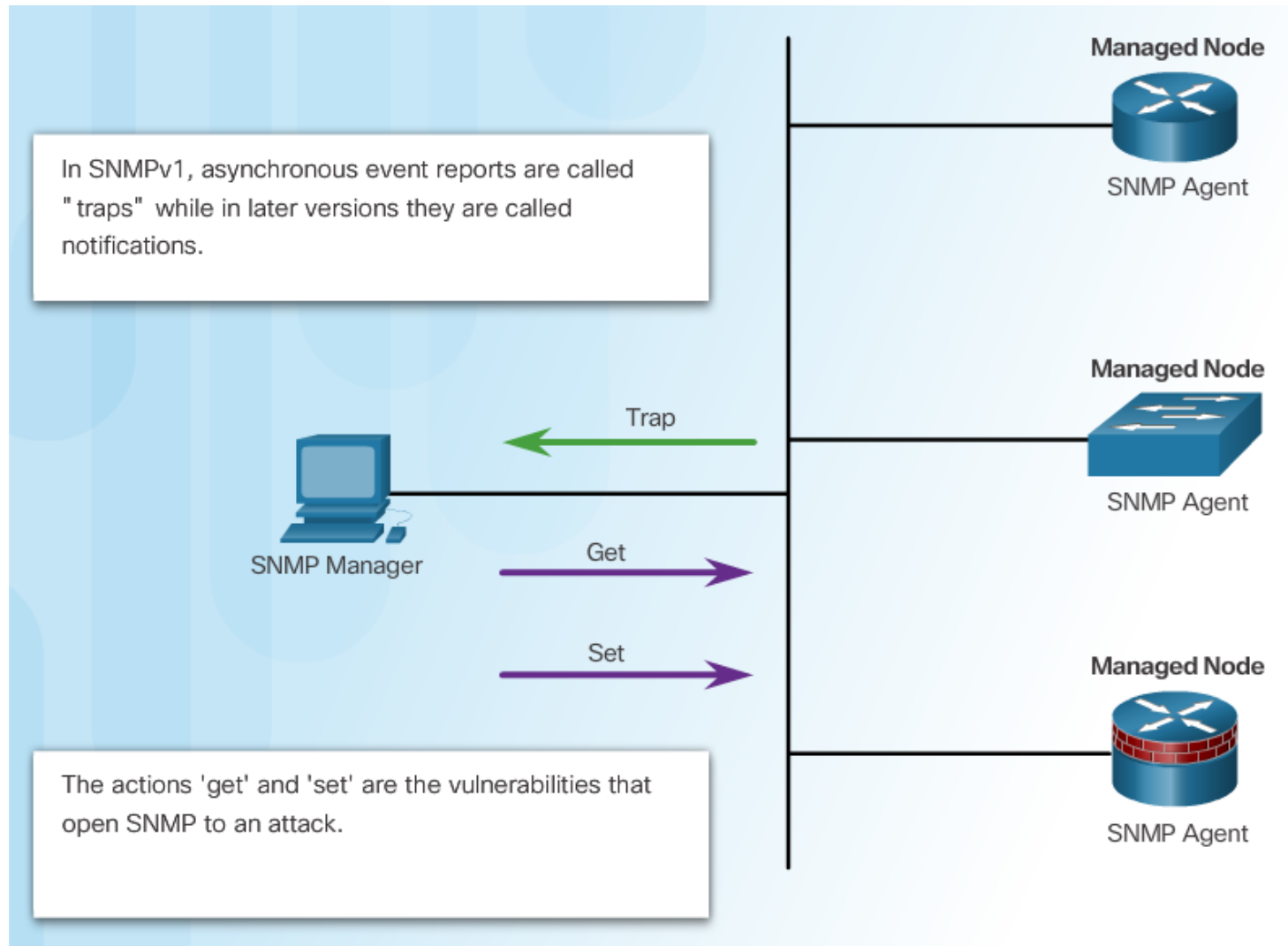
# Management Information Base



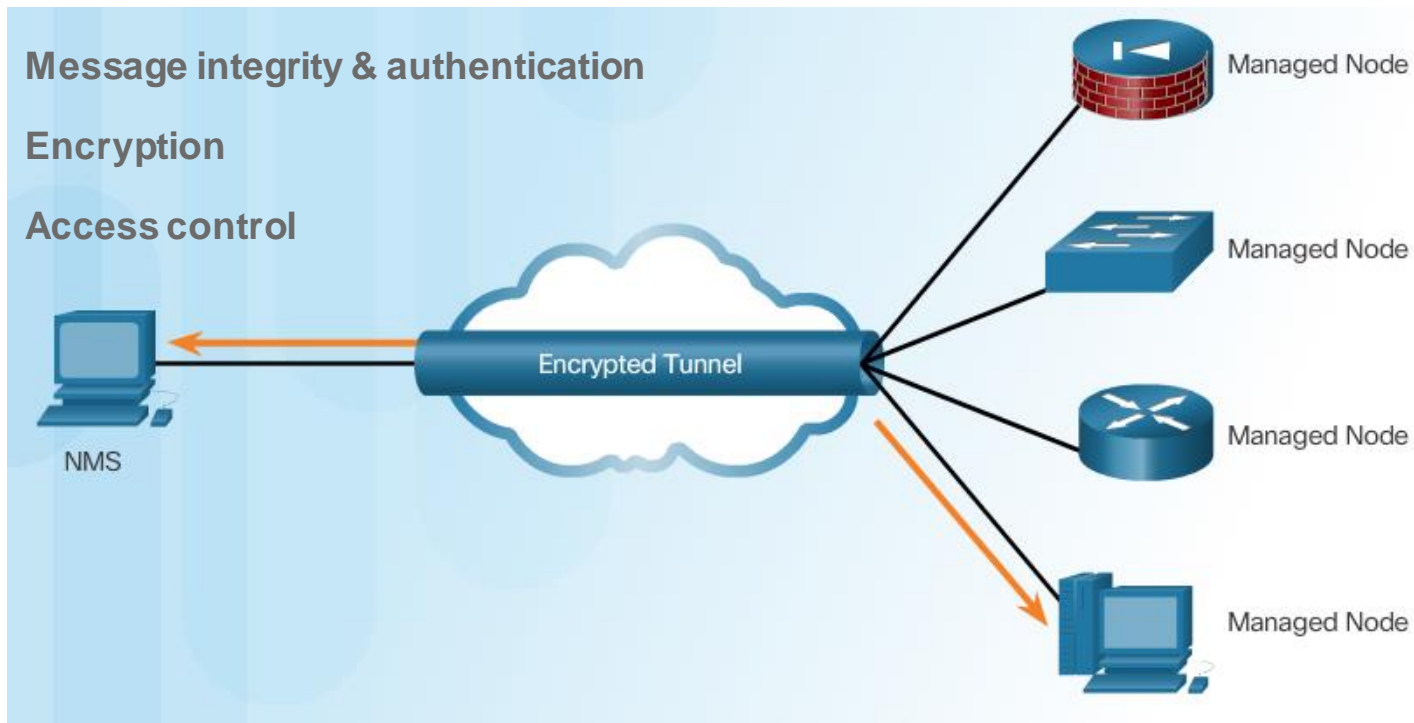
# SNMP Versions

Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication (an improvement over SNMPv2c).
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	authPriv (requires the cryptographic software image)	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms: <ul style="list-style-type: none"><li>• DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.</li><li>• 3DES 168-bit encryption</li><li>• AES 128-bit, 192-bit, or 256-bit encryption</li></ul>

# SNMP Vulnerabilities



# SNMPv3



- Transmissions de gestionnaire à l'agent peuvent être authentifiées afin de garantir l'identité de l'expéditeur et l'intégrité et l'actualité d'un message.
- SNMPv3 messages peuvent être chiffrés pour assurer l'intimité.
- Agent peut exécuter un contrôle d'accès pour limiter chaque entité à certaines actions effectuées sur des éléments précis de données.

# Configuring SNMPv3 Security

Step 1: Configure an ACL to permit the protected management network.

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

Step 2: Configure an SNMP view.

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

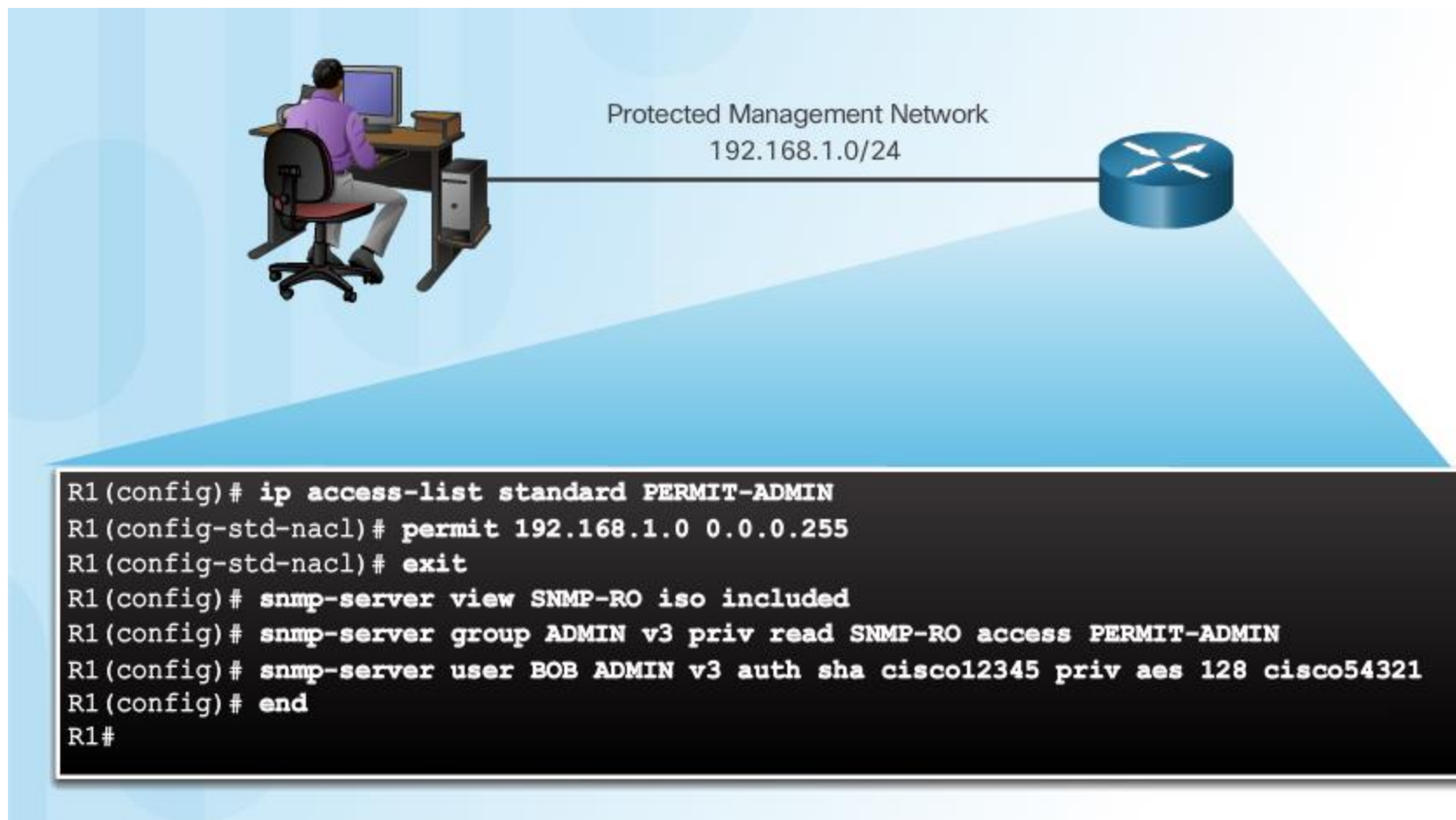
Step 3: Configure an SNMP group.

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

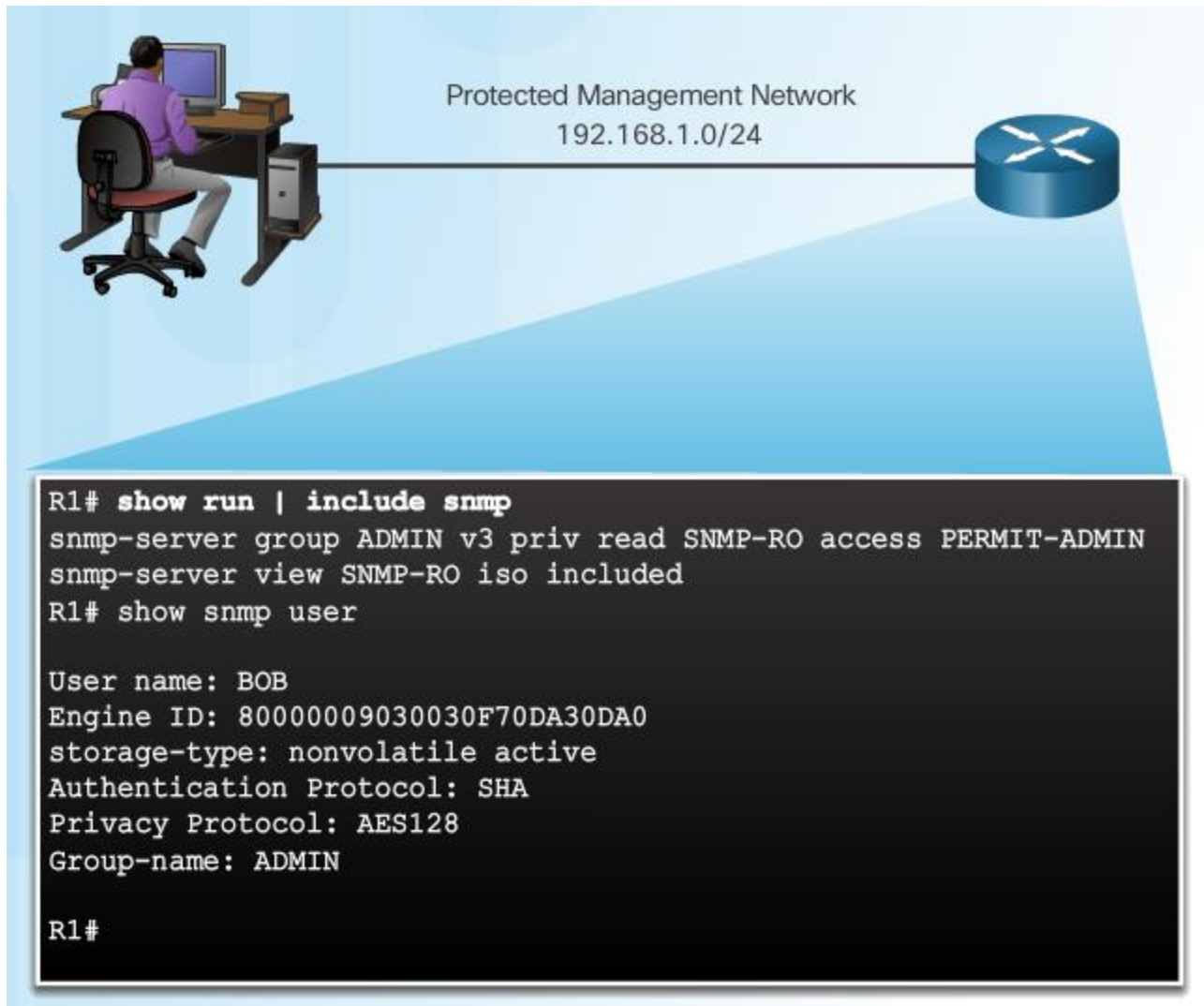
Step 4: Configure a user as a member of the SNMP group.

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

# Exemple de Configuration de sécurité SNMPv3



# Vérifier la Configuration de SNMPv3





## Rubrique 2.3.5 : À l'aide de NTP

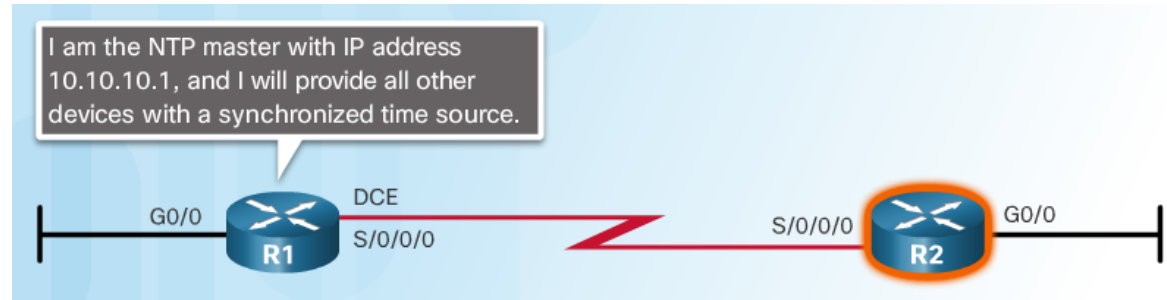


# Network Time Protocol

```
R1# clock set 10:28:00 DEC 16 2008
R1#
*Dec 16 10:28:00.000: %SYS-6-CLOCKUPDATE: System clock
has been updated from 16:07:17 UTC Tue Dec 16 2008 to
10:28:00 UTC Tue Dec 16 2008, configured from console
by console.
R1#
```

# NTP Server

## Sample NTP Topology



## Exemple de Configuration NTP sur R1

```
R1# conf t
R1(config)# ntp master 1
R1(config)# ^Z
R1#
R1# show clock
13:01:15.735 UTC Tue Dec 16 2008
R1#
```

## Exemple de Configuration NTP sur R2

```
R2# conf t
R2(config)# ntp server 10.10.10.1
R2(config)# ^Z
R2# show clock
13:01:41.986 UTC Tue Dec 16 2008
R2# show ntp status
Clock is synchronized, stratum 2, reference is 10.10.10.1
nominal freq is 250.0000 Hz, actual freq is 249.9992 Hz, precision is 2**18
reference time is CCF2253E.5DC2A53B (13:01:50.366 UTC Tue Dec 16 2008) clock
offset is 0.3072 msec, root delay is 23.41 msec
root dispersion is 0.38 msec, peer dispersion is 0.05 msec
R2#
```

# NTP Authentication



```
R1# conf t
R1(config)# ntp authenticate
R1(config)# ntp authentication-key 1 md5 cisco123
R1(config)# ntp trusted-key 1
R1(config)# ^Z
```

# Article 2.4 : À l'aide de fonctions de sécurité automatisés

À la fin de cette section, vous devriez être en mesure de :

- Use security audit tools to determine IOS-based router vulnerabilities.
- Utilisez AutoSecure pour activer la sécurité sur les routeurs IOS.

## Rubrique 2.4.1 : Effectuer un Audit de sécurité



# Protocoles de découverte CDP et LLDP

```
R1(config)# lldp run
R1(config)# end
R1# show cdp neighbors detail
-----
Device ID: S1
Entry address(es):
  IP address: 192.168.1.254
Platform: cisco WS-C2960-24TT-L, Capabilities: Switch IGMP
Interface: GigabitEthernet0/1, Port ID (outgoing port): FastEthernet0/5
Holdtime : 164 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
<output omitted>

R1# show lldp neighbors detail
-----
Local Intf: Gi0/1
Chassis id: 0022.9121.0380
Port id: Fa0/5
Port Description: FastEthernet0/5
System Name: S1

System Description:
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
<output omitted>
```

# Paramètres des protocoles et Services

Il y a une liste détaillée des paramètres de sécurité pour les protocoles et services fournis à la Figure 2 de cette page en cours.

Autres pratiques recommandées pour assurer un dispositif est sécurisé :

- Désactiver les services inutiles et interfaces.
- Désactiver et restreindre les services de gestion généralement configuré.
- Désactiver les sondes et les analyses. Assurer la sécurité d'accès au terminal.
- Disable gratuite et proxy ARP
- Désactiver les diffusions vers IP.



## Rubrique 2.4.2 : Verrouillage d'un routeur à l'aide de AutoSecure



# Cisco AutoSecure

```
R1# auto secure
--- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security
    of the router but it will not make router
    absolutely secure from all security attacks ***

All the configuration done as part of AutoSecure
will be shown here. For more details of why and
how this configuration is useful, and any possible
side effects, please refer to Cisco documentation of
AutoSecure.

At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for
AutoSecure

Is this router connected to internet? [no]:yes
```

# A l'aide de la fonctionnalité AutoSecure de Cisco

Router#

```
auto secure [no-interact | full] [forwarding | management]  
[ntp | login | ssh | firewall | tcp-intercept]
```

Parameter	Description
<b>no-interact</b>	(Optional) The user will not be prompted for any interactive configurations. No interactive dialogue parameters will be configured, including usernames or passwords.
<b>full</b>	(Optional) The user will be prompted for all interactive questions. This is the default setting.
<b>forwarding</b>	(Optional) Only the forwarding plane will be secured.
<b>management</b>	(Optional) Only the management plane will be secured.
<b>ntp</b>	(Optional) Specifies the configuration of the NTP feature in the AutoSecure CLI.
<b>login</b>	(Optional) Specifies the configuration of the Login feature in the AutoSecure CLI.
<b>ssh</b>	(Optional) Specifies the configuration of the SSH feature in the AutoSecure CLI.
<b>firewall</b>	(Optional) Specifies the configuration of the Firewall feature in the AutoSecure CLI.
<b>tcp-intercept</b>	(Optional) Specifies the configuration of the TCP-Intercept feature in the AutoSecure CLI.

# Utiliser l'auto pour fixer commande

1. La commande sûr auto est entrée
2. Assistant recueille des informations sur les interfaces externes
3. AutoSecure secures the management plane by disabling unnecessary services
4. AutoSecure vous invite pour une bannière
5. AutoSecure demande des mots de passe et active les fonctionnalités de mot de passe et login
6. Interfaces are secured
7. Plan de transfert est sécurisé

# Article 2.5 : Obtenir le plan de contrôle

À la fin de cette section, vous devriez être en mesure de :

- Configurer une authentification Protocole routage.
- Expliquer la fonction du plan de contrôle de police.

## Sujet 2.5.1 : Protocole de routage authentification



# Routing Protocol Spoofing

Conséquences de l'usurpation de protocole :

- Rediriger le trafic pour créer des boucles de routage.
- Rediriger le trafic afin qu'il soit contrôlable sur un lien non sécurisé.
- Rediriger le trafic pour jeter.

# Authentication de protocole de routage OSPF MD5



```
R1# conf t
R1(config)# interface s0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 cisco12345
R1(config-if)# ip ospf authentication message-digest
R1(config-if)#
000209: Feb 20 13:59:35.091 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
000210: Feb 20 14:01:09.975 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0/0 from
LOADING to FULL, Loading Done
-----
R2# conf t
000137: Feb 20 13:59:35.091 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Dead timer expired
R2(config)# interface s0/0/0
R2(config-if)# ip ospf message-digest-key 1 md5 cisco12345
R2(config-if)# ip ospf authentication message-digest
R2(config-if)#
000138: Feb 20 14:01:09.975 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done
R2(config-if)#
```



# Authentication du protocole de routage OSPF SHA

Step 1: Specify an SHA authentication key chain.

```
Router(config)# key chain name  
Router(config-keychain)# key key-id  
Router(config-keychain-key)# key-string string  
Router(config-keychain-key)# cryptographic-algorithm hmac-sha-256  
Router(config)# send-lifetime start-time {infinite | end-time | duration seconds}
```

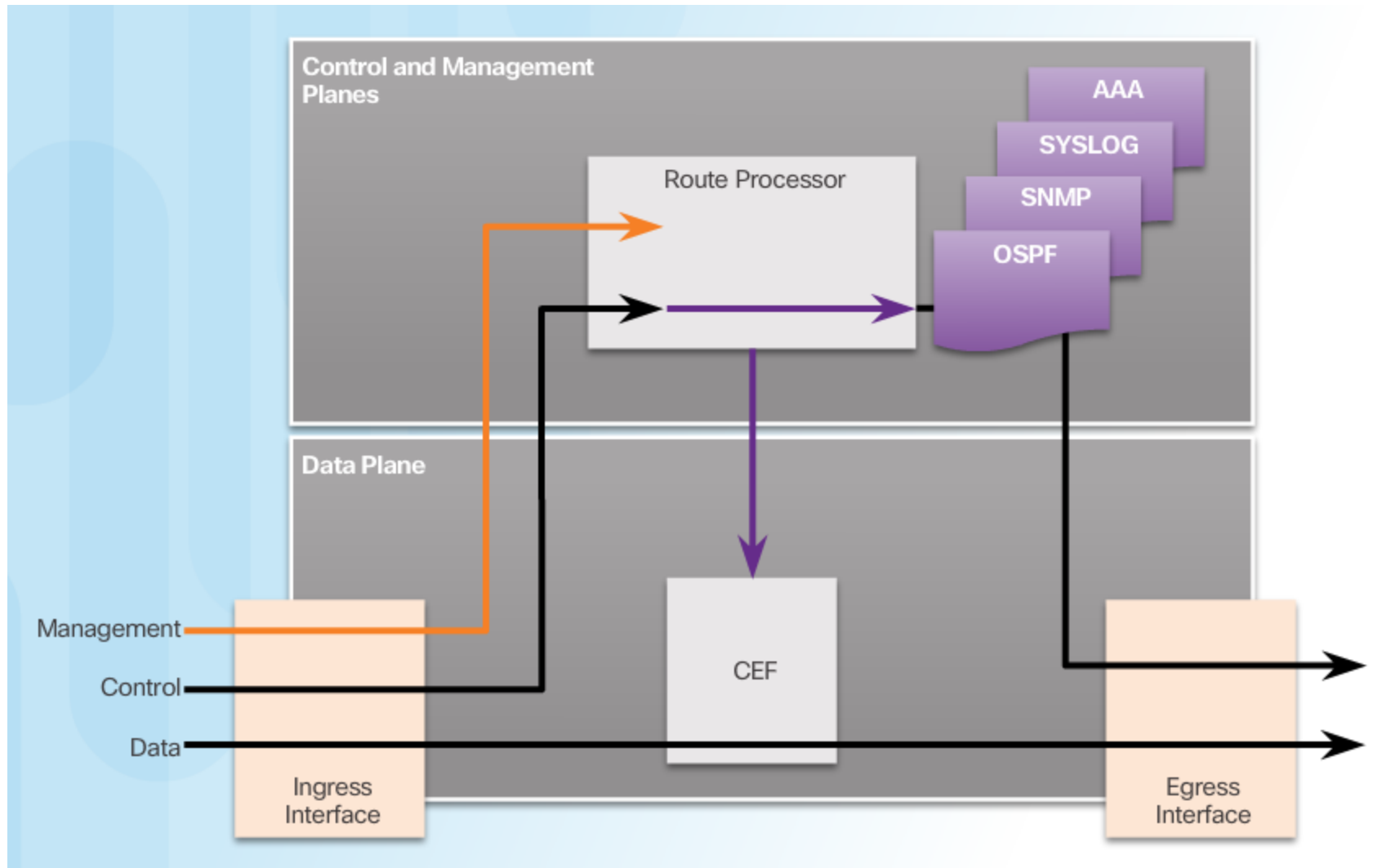
Step 2: Assign the authentication key chain to the desired interfaces.

```
Router(config)# interface type number  
Router(config-if)# ip ospf authentication key-chain name
```

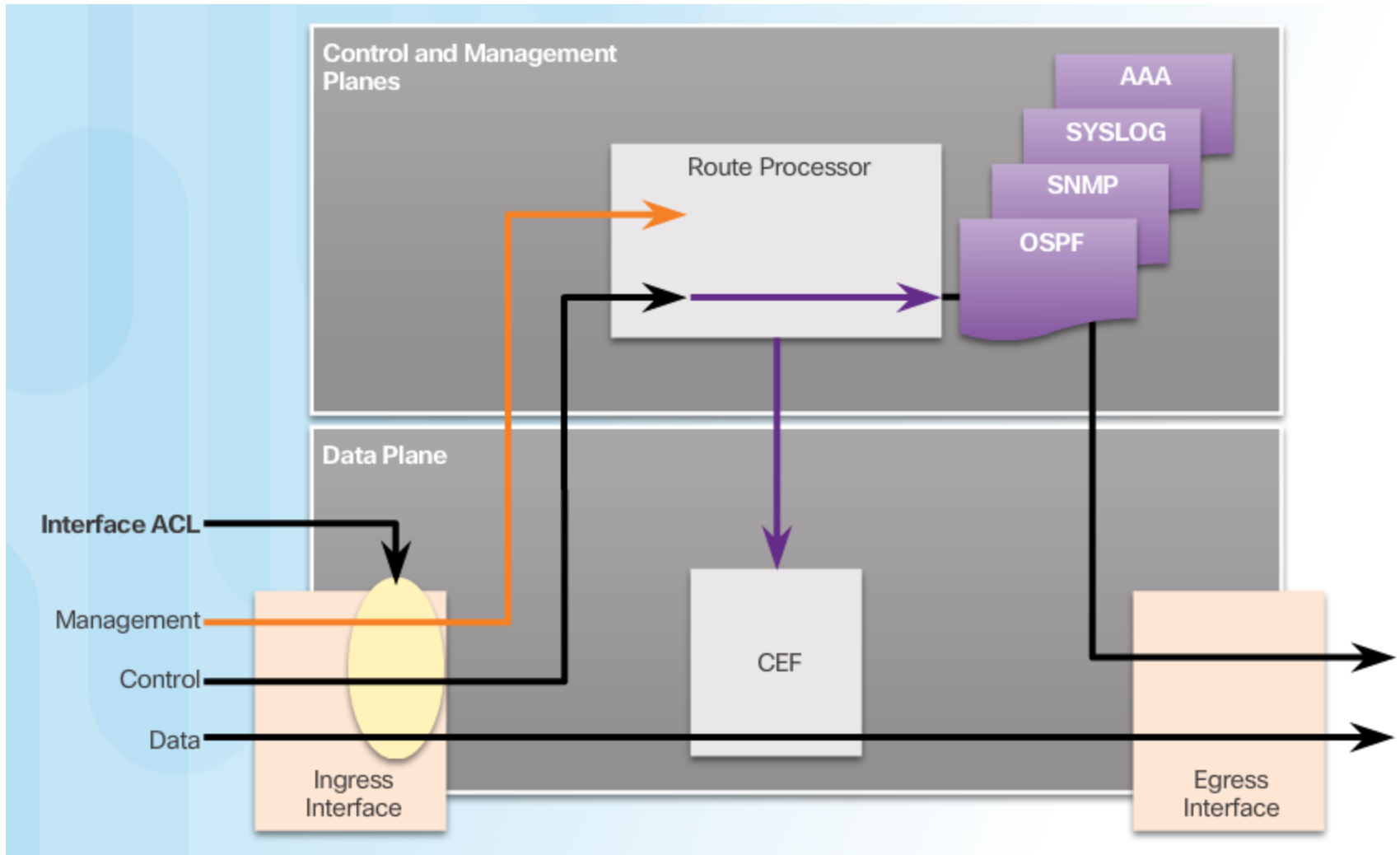
## Rubrique 2.5.2 : Contrôler le plan de police



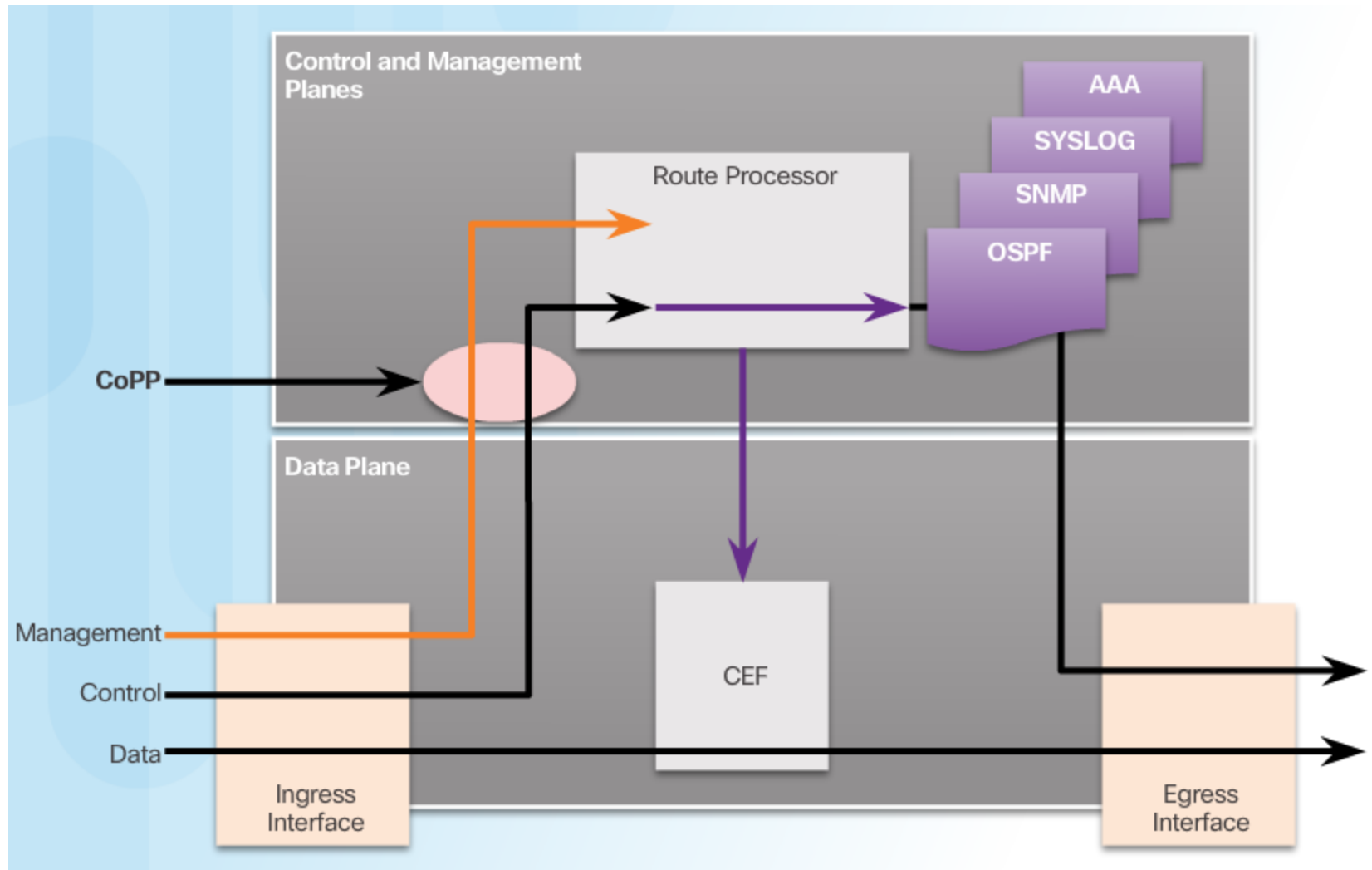
# Network Device Operations



# Contrôle et gestion des vulnérabilités avion



# CoPP Operation



# Section 2.6:

## Summary

### Chapitre Objectives:

- Configurer un accès administratif sécurisé.
- Configurez l'autorisation de commande à l'aide des niveaux de privilège et CLI basée sur les rôles.
- Mettre en œuvre la sécurisation et la surveillance des périphériques réseau.
- Fonctions automatiques permet d'activer la sécurité sur les routeurs IOS.
- Implement control plan sécurité.

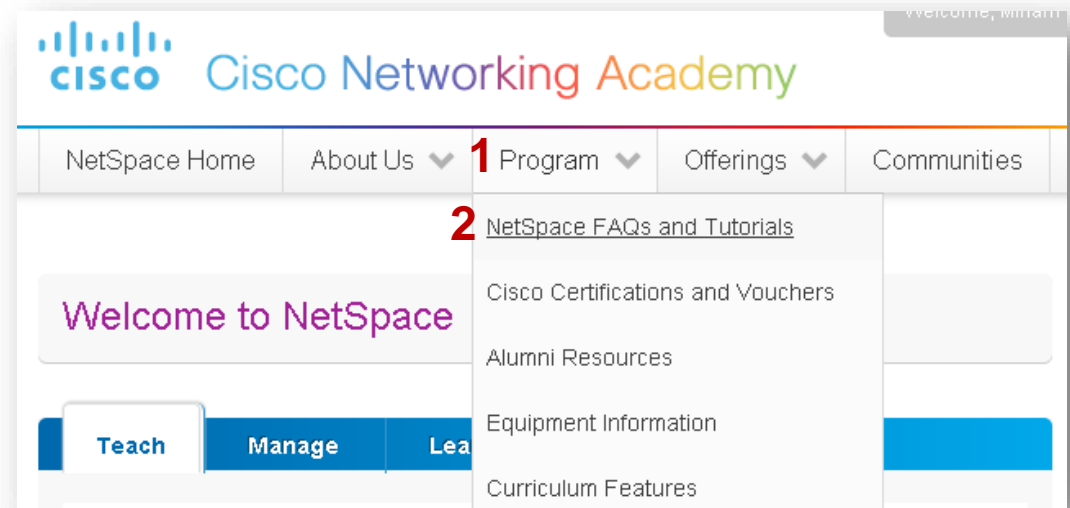
Thank you.



Cisco Networking Academy  
Mind Wide Open

# Instructor Resources

- N'oubliez pas, tutoriels utiles et guides de l'utilisateur sont disponibles via votre page d'accueil de NetSpace. (<https://www.netacad.com>)
- Ces ressources couvrent un éventail de sujets, y compris la navigation, les évaluations et les affectations. Une capture d'écran a été apportée ici mettant en évidence les tutoriels liés à l'activation des examens, gestion des évaluations et la création de quiz.



## Managing Assessments

- Assessment FAQ
  - Assessment Viewer
  - Default Assessments *Revised*
  - Advanced Assessments *Revised*
- Manage Assessments *Revised*
  - Student Performance Assessment Summary
- Activation Tool: Complete Tutorial (13 Minutes)
  - Activation Tool: Bulk Activation
  - Activation Tool: Bulk Deactivation **NEW**
  - Activation Tool: Manage Activations
  - Activation Tool: Creating an Activation Profile *Revised*
  - Packet Tracer Activity Grader