

# Chapitre 3:

## Authentication Authorization Accounting

CCNA Security v2.0  
Samir DIABI



# Sommaire

3.0 Introduction

3.1 Objectifs d' AAA

3.2 Authentification Locale AAA

3.3 Authentification AAA basée sur un serveur

3.4 Authentification basée sur un serveur

3.5 Autorisation et journalisation basées sur un serveur AAA

3.6 Résumé

# Section 3.1:

## Les objectifs de l'approche AAA

A la fin de cette section, vous serez en mesure de :

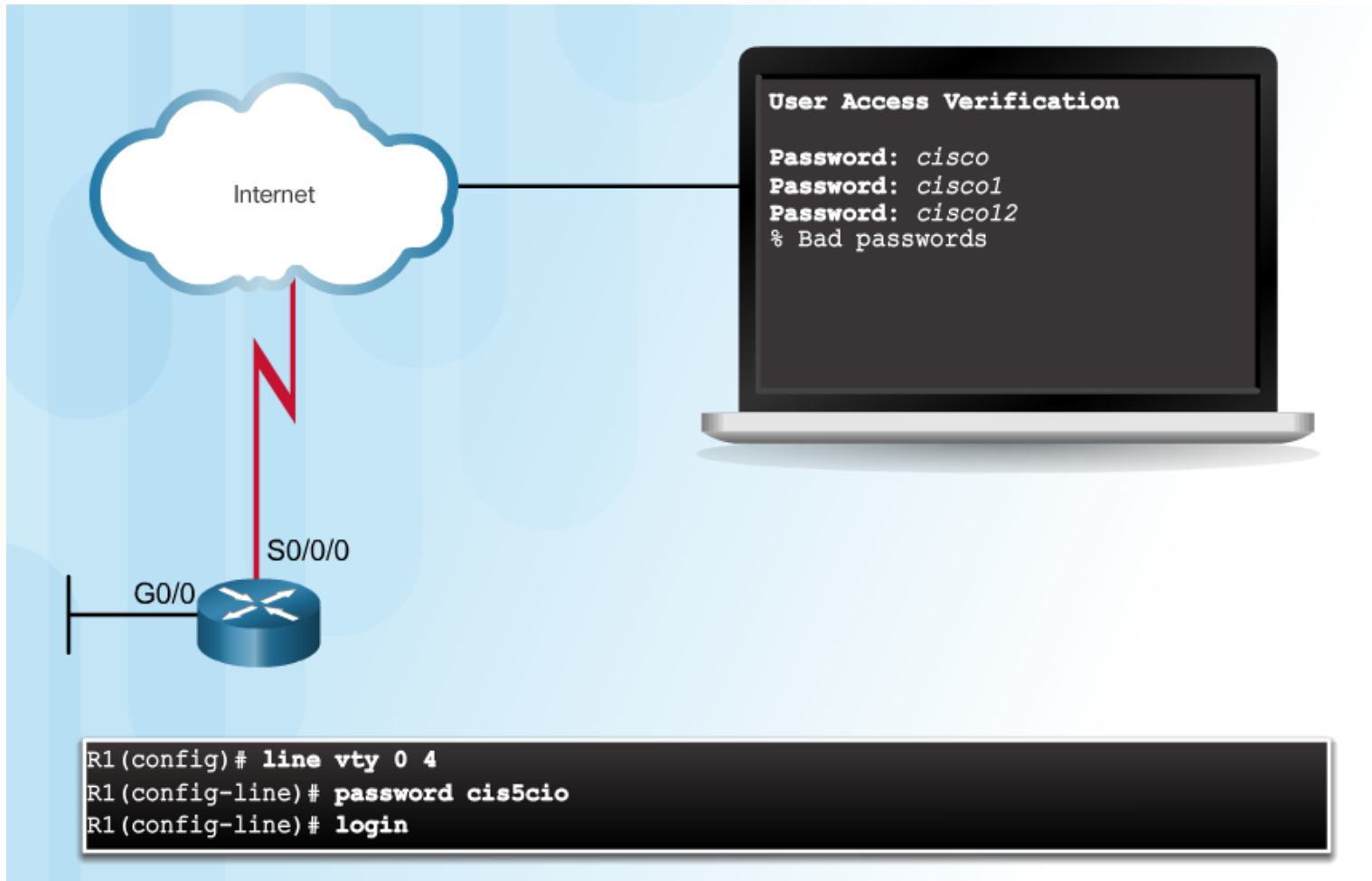
- Expliquez pourquoi AAA est essentiel pour la sécurité du réseau.
- Décrire les caractéristiques de AAA.

## Rubrique 3.1.1: AAA aperçu



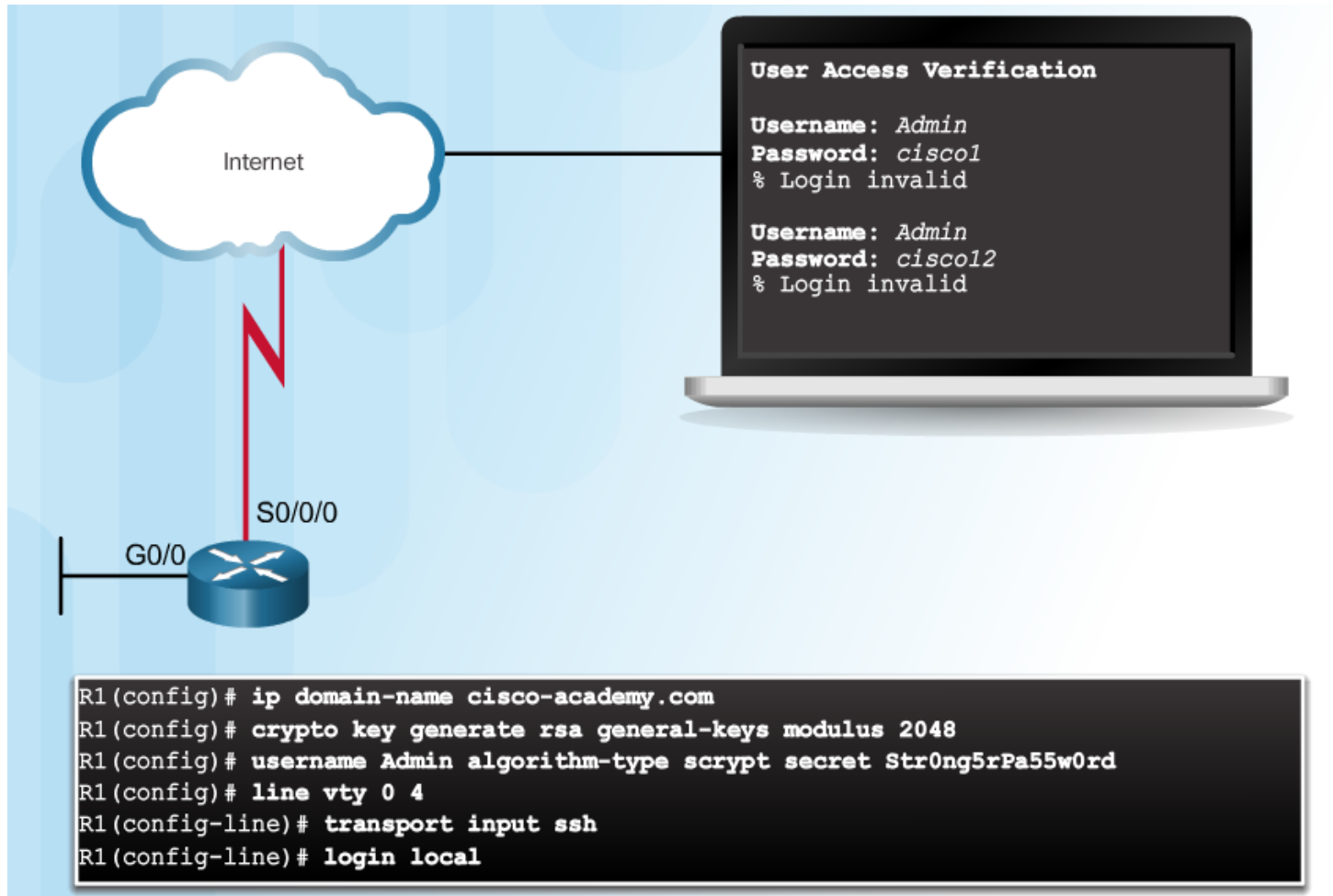
# Authentication sans AAA

Telnet est vulnérable aux attaques de force brute



# Authentication sans AAA (Cont.)

## SSH et la base de données locale



# Composants d'AAA

The diagram illustrates the AAA components (Authentication, Authorization, Accounting) mapped to a credit card statement. Three callout boxes on the left point to specific sections of the statement:

- Authentication** (Who are you?): Points to the Cardmember Name and Account Number.
- Authorization** (How much can you spend?): Points to the Credit Limit.
- Accounting** (What did you spend it on?): Points to the Account Summary and Transaction Table.

**Statement of Personal Credit Card Account**

Account Number: 1234-567-890 | Statement Closing Date: 01-31-01 | Current Amount Due: \$278.50

JOE EMPLOYEE  
456 SKYVIEW DRIVE  
HOMETOWN, USA 99900-1234

MAIL PAYMENT TO:  
THE BANK  
132 VINE STREET  
ANYTOWN, USA 87500-0010

872919345 001782550000000003

Detach here and return upper portion with check or money order. Do not staple or fold.

**Statement of Personal Credit Card Account**  
Retain this portion for your files.

Cardmember Name: JOE EMPLOYEE | Account Number: 1234-456-890 | Statement Closing Date: 01-31-01

Statement Date: 02-01-01 | Closing Date: 01-31-01 | Payment Due Date: 03-01-01

Credit Limit: \$1,500.00 | Credit Available: \$1221.50

New Balance: \$278.50 | Minimum Payment Due: \$20.00

**Account Summary**

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	<b>NEW BALANCE:</b>	<b>\$278.50</b>

Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43210987	01-03	01-13	Payment, Thank You	-\$74.25
01234567	01-12	01-13	Wings 'N' Things Anytown, USA	\$25.25
78901234	01-14	01-17	Record Release Anytown, USA	\$40.00
45678901	01-14	01-17	Sports Stadium Anytown, USA	\$75.25
3210987	01-22	01-23	Tie Tack Anytown, USA	\$20.75
76543210	01-29	01-30	Electronic World Anytown, USA	\$89.25
2345678		01-30	Transaction Fees	\$3.00
34567890		01-01	Annual Fee	\$25.00

PAGE 1 OF 1

Les services de sécurité réseau AAA fournissent le cadre principal pour configurer le contrôle d'accès sur un périphérique réseau. AAA est un moyen de contrôler qui est autorisé à accéder à un réseau (authentifier), ce qu'ils peuvent faire pendant qu'ils sont là (autoriser) et de vérifier quelles actions ils ont effectué lors de l'accès au réseau (comptabilité)

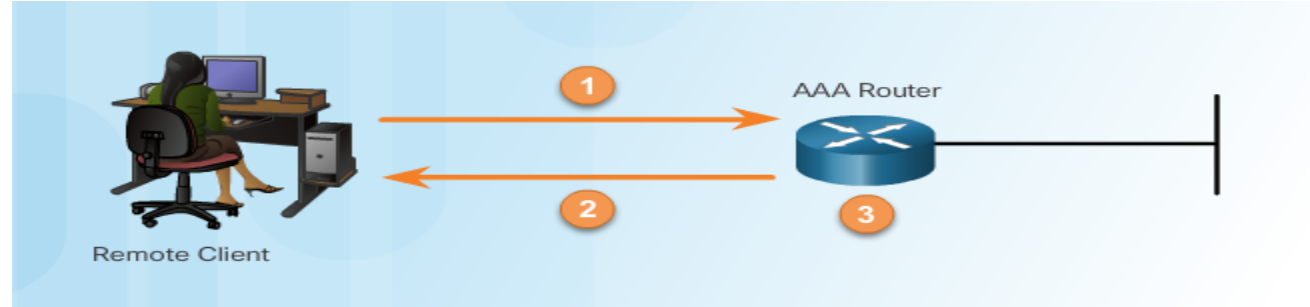
## Rubrique 3.1.2: Caractéristiques d'AAA





# Modes d'Authentification

## Authentification Local AAA



1. Le client établit une connexion avec le routeur.
2. Le routeur AAA invite l'utilisateur à saisir un nom d'utilisateur et un mot de passe.
3. Le routeur authentifie le nom d'utilisateur et le mot de passe à l'aide de la base de données locale et l'utilisateur dispose d'un accès au réseau basé sur des informations contenues dans la base de données locale.

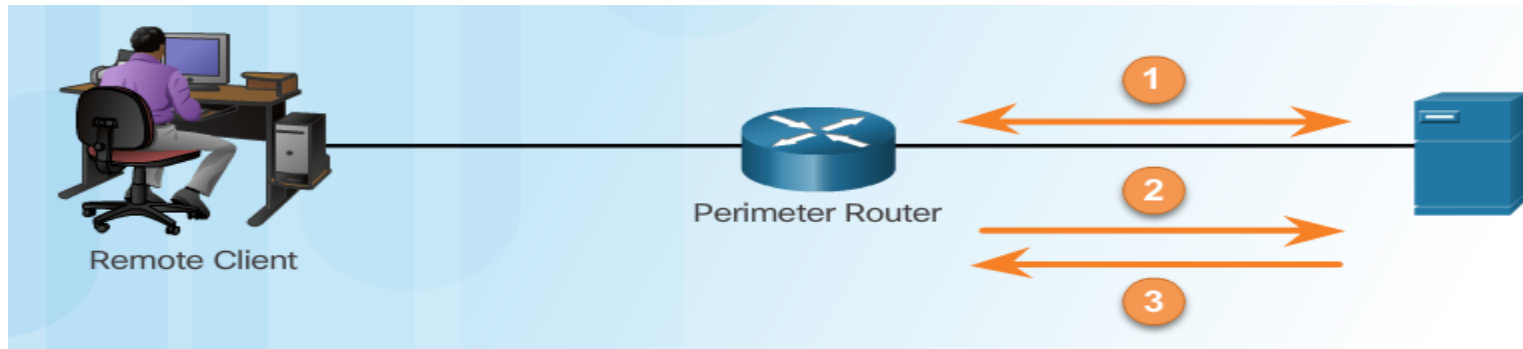
## Authentification Server-Based AAA



1. Le client établit une connexion avec le routeur.
2. Le routeur AAA invite l'utilisateur à saisir un nom d'utilisateur et un mot de passe.
3. Le routeur authentifie le nom d'utilisateur et le mot de passe à l'aide d'un serveur AAA distant.

# Autorisation

## L' autorisation AAA

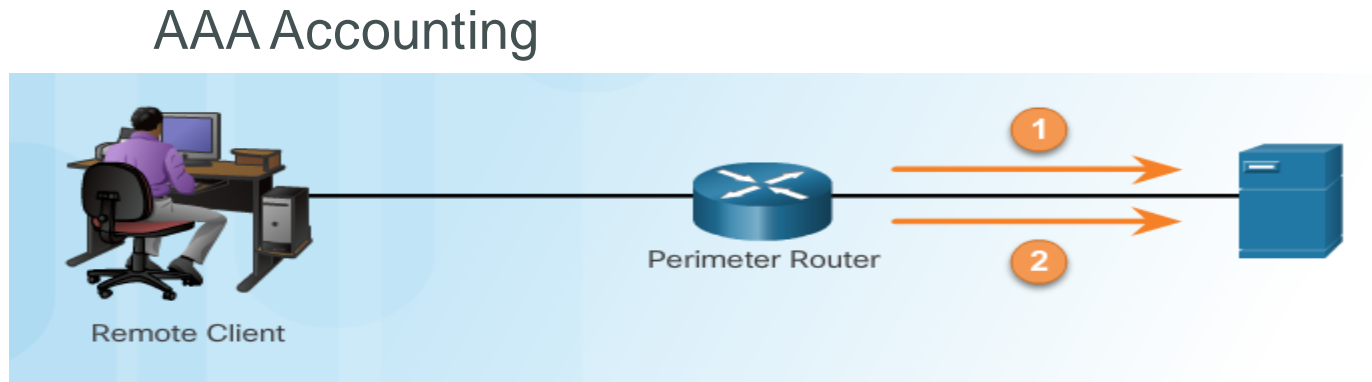


1. Lorsqu'un utilisateur a été authentifié, une session est établie entre le routeur et le serveur AAA.
2. Le routeur demande l'autorisation du serveur AAA pour le service demandé par le client.

# Accounting

Types d'information d'Accounting:

- Réseau
- Connexion
- EXEC
- Système
- Commande
- Ressource



1. Lorsqu'un utilisateur a été authentifié, le processus d'accounting AAA génère un message de début pour commencer le processus d'accounting.

# Section 3.2:

## Authentication Local AAA

A la fin de cette section, vous serez en mesure de :

- Configurez l'authentification AAA, à l'aide de la CLI, pour valider les utilisateurs en utilisant une base de données locale.
- Dépannage de l'authentification AAA, qui valide les utilisateurs par rapport à une base de données locale.

## Rubrique 3.2.1: Configurer Authentication AAA Local avec CLI



# Authenticating Administrative Access

1. Ajoutez des noms d'utilisateur et des mots de passe à la base de données du routeur local pour les utilisateurs qui ont besoin d'un accès administratif au routeur.
2. Activer AAA globalement sur le routeur.
3. Configurez les paramètres AAA sur le routeur.
4. Confirmez et dépannez la configuration AAA.

```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case
R1(config)#
```

# Méthodes d'authentification

Method Type Keywords	Description
<code>enable</code>	Uses the enable password for authentication.
<code>local</code>	Uses the local username database for authentication.
<code>local-case</code>	Uses case-sensitive local username authentication.
<code>none</code>	Uses no authentication.
<code>group radius</code>	Uses the list of all RADIUS servers for authentication.
<code>group tacacs+</code>	Uses the list of all TACACS+ servers for authentication.
<code>group group-name</code>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <code>aaa group server radius</code> or <code>aaa group server tacacs+</code> command.

`aaa authentication login [default| list-name] method1.. method4`

- **Enable** : Utilise le mot de passe ENABLE pour l'authentification
- **Local** : Utilise des noms d'utilisateurs de la base de données locale pour l'authentification
- **Local-case** : Utilise l'authentification de nom d'utilisateur local sensible à la casse
- **None** : N'utilise aucune authentification
- **Group radius** : Utilise la liste de tous les serveurs RADIUS pour l'authentification.
- **Group tacacs+** : Utilise la liste de tous les serveurs TACACS + pour l'authentification.
- **Group group-name** : Utilise un sous-réseau de serveurs RADIUS ou TACACS + pour l'authentification tel que défini par la commande **aaa group server radius** ou **aaa group server tacacs+**

# Méthodes par défaut et nommées

## Exemple Authentification Local AAA

```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case enable
R1(config)# aaa authentication login SSH-LOGIN local-case
R1(config)# line vty 0 4
R1(config-line)# login authentication SSH-LOGIN
```



# Optimisation de la configuration d'authentification

Syntaxe des commandes

Router (config) #

```
aaa local authentication attempts max-fail [number-of-unsuccessful-attempts]
```

Command	Description
<i>number-of-unsuccessful-attempts</i>	Nombre de tentatives infructueuses avant qu'une connexion soit abandonnée et que le compte d'utilisateur soit verrouillé

R1# **show aaa local user logout**

Local-user	Lock time
JR-ADMIN	04:28:49 UTC Sat Dec 27 2015

R1# **show aaa sessions**

Total sessions since last reload: 4

Session Id: 1

Unique Id: 175

User Name: ADMIN

IP Address: 192.168.1.10

Idle Time: 0

CT Call Handle: 0

Afficher l'ID unique d'une session

## Rubrique 3.2.2: Dépannage de l'authentification AAA locale.



# Options de débogage

## Dépannage de l'Authentification AAA locale

```
R1# debug aaa ?
accounting          Accounting
administrative      Administrative
api                AAA api events
attr               AAA Attr Manager
authentication     Authentication
authorization       Authorization
cache              Cache activities
coa                AAA CoA processing
db                 AAA DB Manager
dead-criteria       AAA Dead-Criteria Info
id                 AAA Unique Id
ipc                AAA IPC
mlist-ref-count     Method list reference counts
mlist-state         Information about AAA method
                   list state change and notification
per-user            Per-user attributes
pod                AAA POD processing
protocol            AAA protocol processing
server-ref-count    Server handle reference counts
sg-ref-count        Server group handle reference counts
sg-server-selection Server Group Server Selection
subsys             AAA Subsystem
testing             Info. about AAA generated test packets
```

# Debugging AAA Authentication

## Comprendre la sortie de débogage

```
R1# debug aaa authentication
113123: Feb 4 10:11:19.305 CST: AAA/MEMORY: create_user (0x619C4940) user=''ruser=''
      port='tty1' rem_addr='async/81560' authen_type=ASCII service=LOGIN priv=1
113124: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): port='tty1' list=''
      action=LOGIN service=LOGIN
113125: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): using "default" list
113126: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): Method=LOCAL
113127: Feb 4 10:11:19.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113128: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): continue_login
      (user='(undef)')
113129: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113130: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113131: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETPASS
113132: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): continue_login
      (user='diallocal')
113133: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = GETPASS
113134: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113135: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = PASS
```

# Section 3.3:

## Server-Based AAA

A la fin de cette section, vous serez en mesure de :

- Décrire les avantages de server-based AAA.
- Comparez les protocoles d'authentification TACACS + et RADIUS.

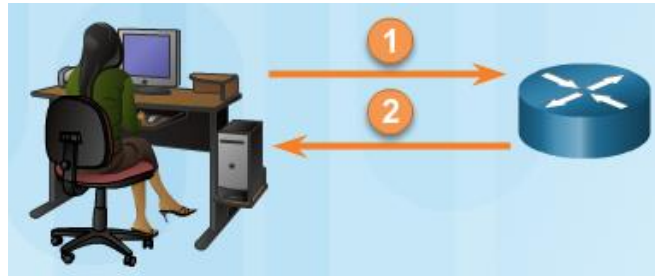
## Rubrique 3.3.1: Les caractéristiques Server-Based AAA



# Comparaison des implémentations : Local AAA and Server-Based AAA

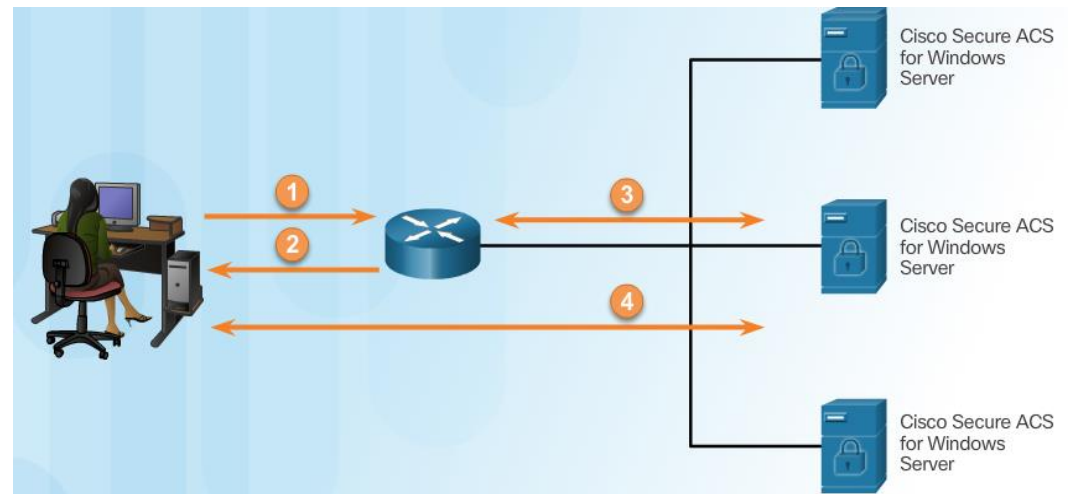
## Authentication Local :

1. L'utilisateur établit une connexion avec le routeur.
2. Le routeur demande à l'utilisateur un nom d'utilisateur et un mot de passe, l'authentification de l'utilisateur à l'aide d'une base de données locale.



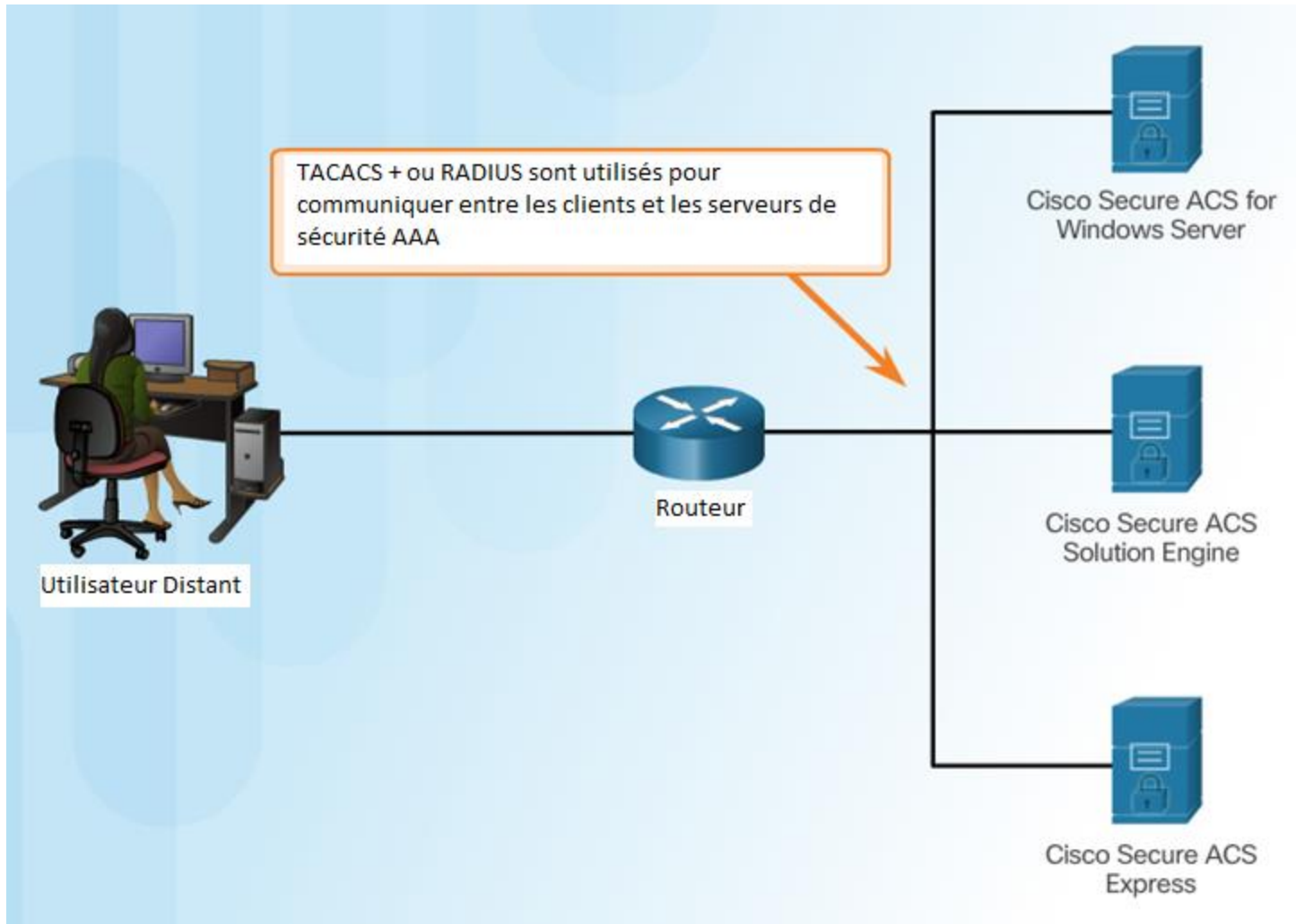
## Server-based authentication:

1. L'utilisateur établit une connexion avec le routeur.
2. Le routeur demande à l'utilisateur un nom d'utilisateur et un mot de passe.
3. Le routeur transmet le nom d'utilisateur et le mot de passe au système Cisco Secure ACS
4. Cisco Secure ACS authentifie l'utilisateur.





# Présentation de Cisco Secure Access Control System





## Rubrique 3.3.2: Protocoles de communication Server-Based AAA

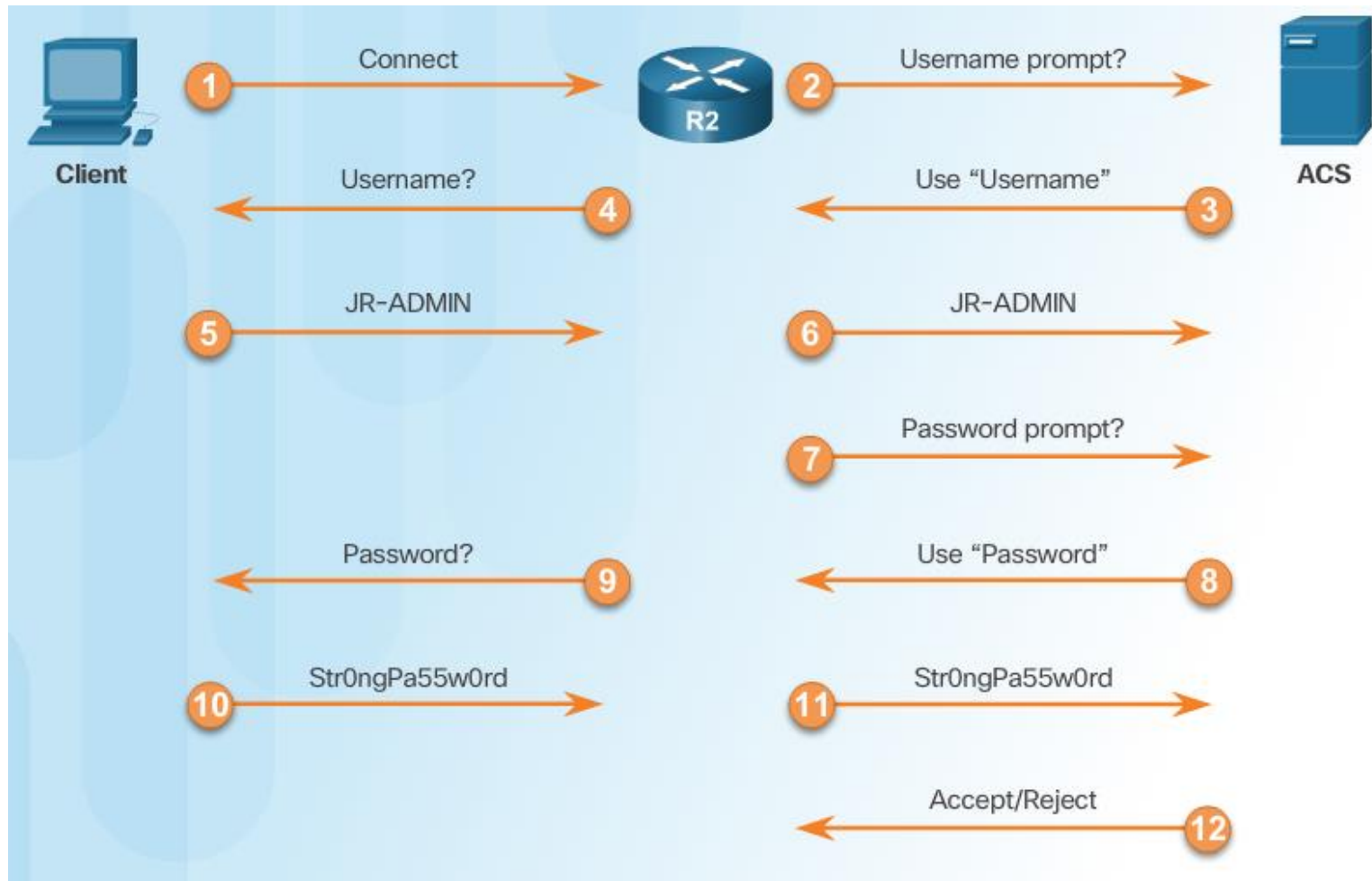


# Introduction de TACACS+ et RADIUS

	TACACS+	RADIUS
Fonctionnalité	Sépare AAA selon l'architecture AAA, permettant la modularité de la mise en œuvre du serveur de sécurité	Combine l'authentification et l'autorisation, mais sépare le suivi, permettant moins de souplesse dans la mise en œuvre que TACACS +
Standard	Pris en charge Principalement par cisco	Open/RFC standard
Protocole de transport	TCP	UDP
CHAP	Défi et réponse bidirectionnels utilisés dans le protocole d'authentification de prise de contact Challenge (CHAP)	Défi et réponse unidirectionnel du serveur de sécurité RADIUS au client RADIUS
Protocol support	Multiprotocol support	No ARA, no NetBEUI
confidentialité	Paquet entier crypté	Mot de passe crypté
Adaptation	Fournit l'autorisation des commandes de routeur par utilisateur ou par groupe	N'a aucune option pour autoriser les commandes de routeur sur une base par utilisateur ou par groupe
Accounting	limité	Etendu

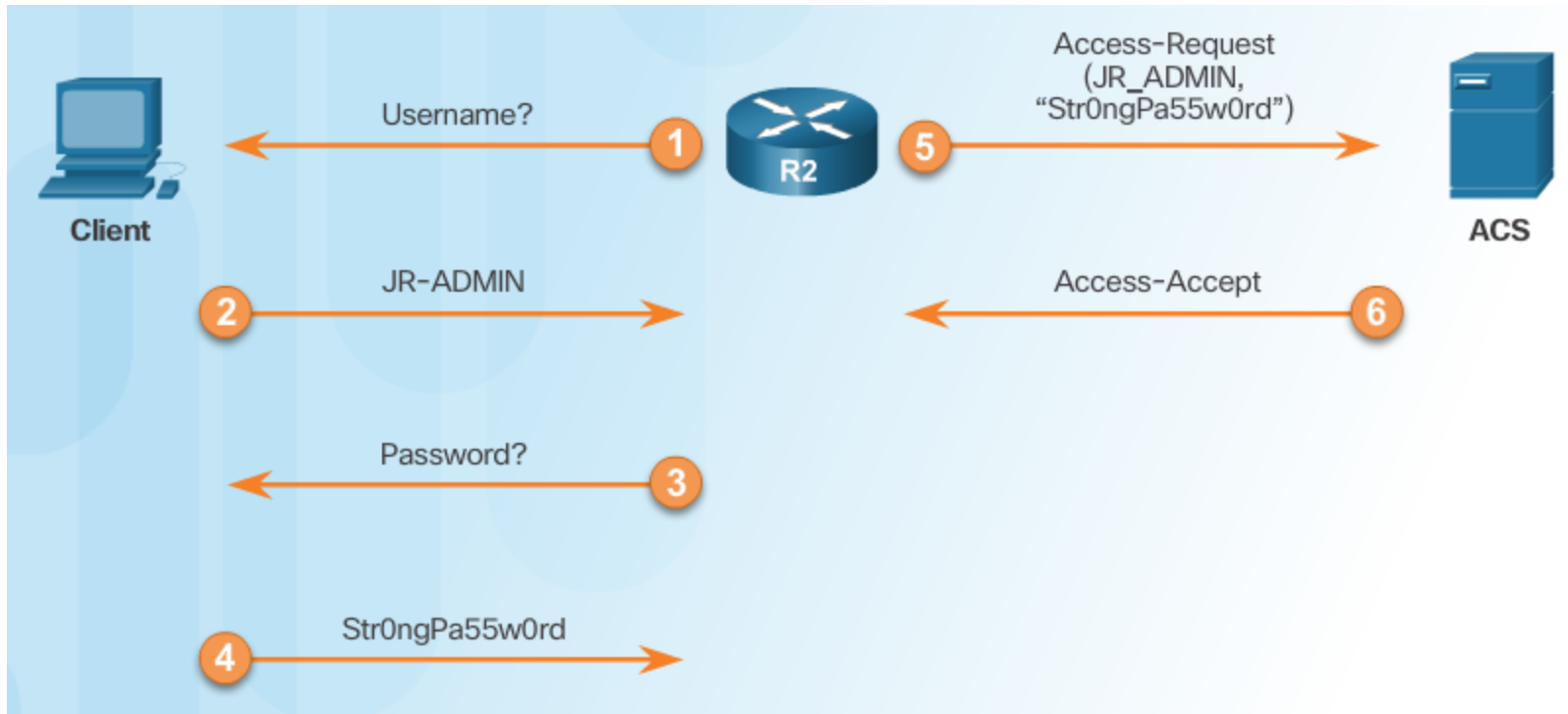
# Authentication TACACS+

## Processus d'authentification TACACS +



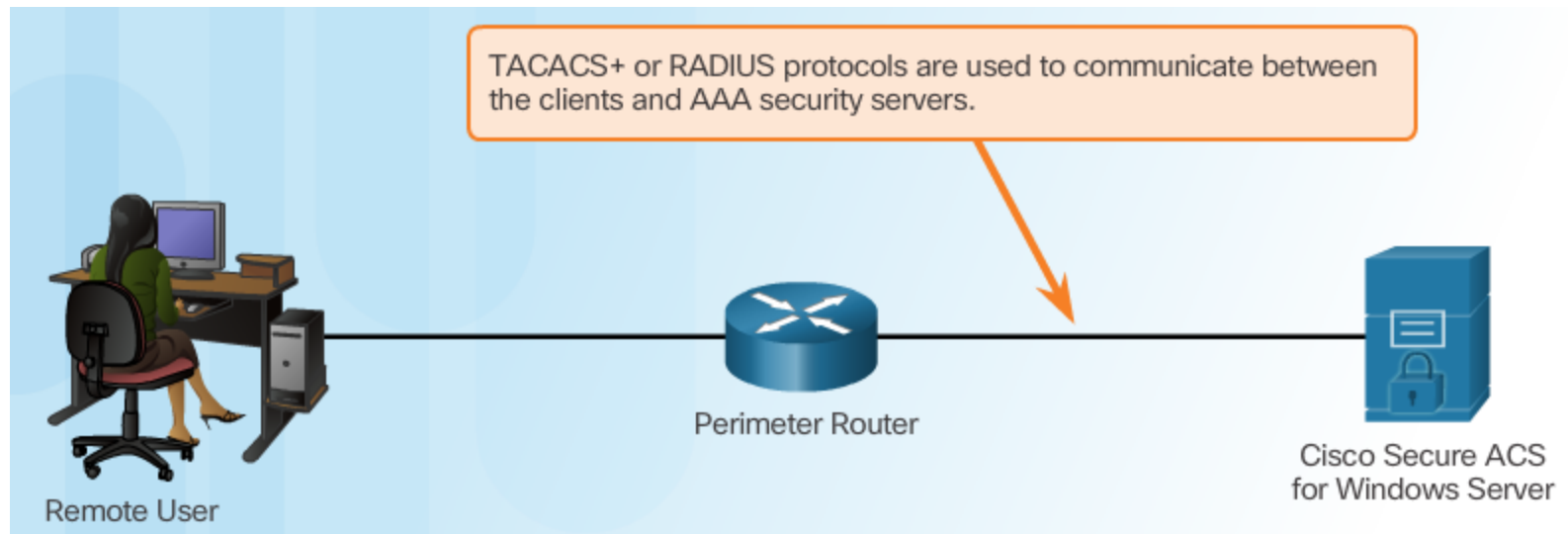
# Authentication RADIUS

## Processus d'authentification RADIUS

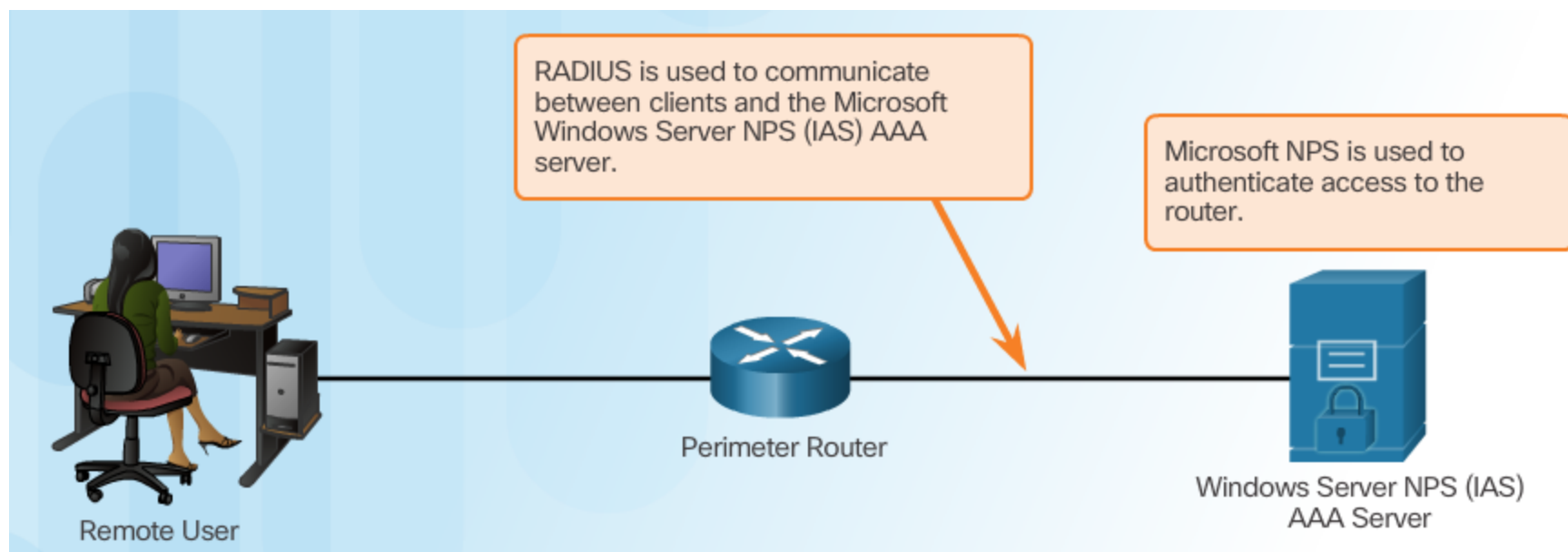


# Intégration de TACACS+ et ACS

## Cisco Secure ACS



# Intégration de AAA sur l'Active Directory



# Section 3.4:

## Authentication Server-Based AAA

A la fin de cette section, vous serez en mesure de :

- Configurez l'authentification server-based AAA , à l'aide de la CLI, sur les routeurs Cisco.
- Dépanner authentification server-based AAA.

## Rubrique 3.4.1: Configurez l'authentification server-based AAA , à l'aide de la CLI.



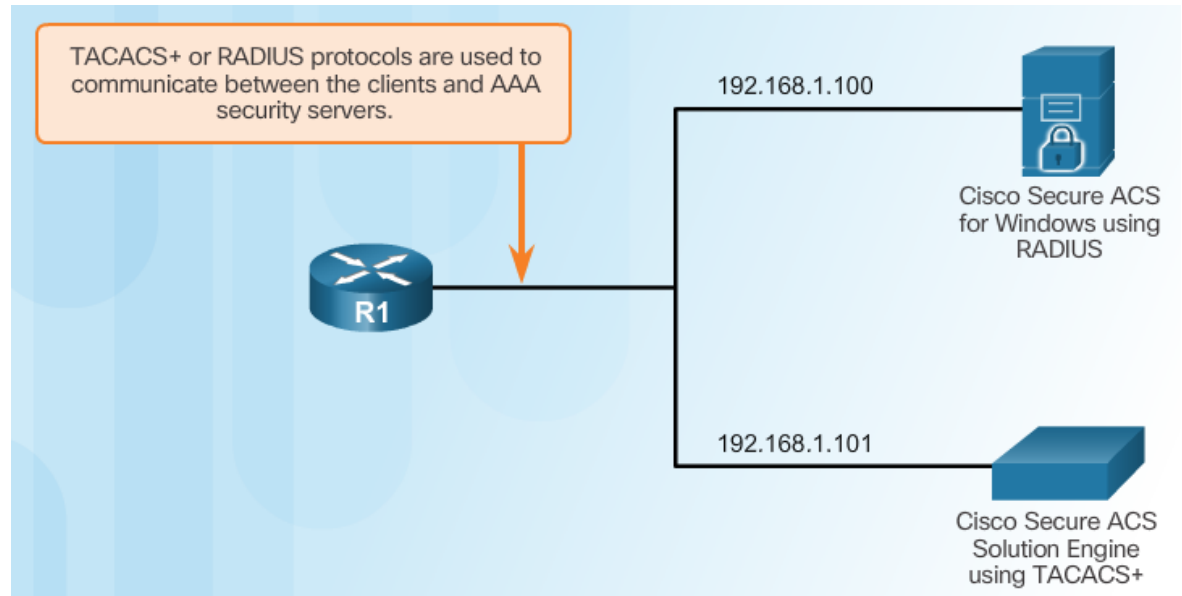


# Etapes pour le configuration d'authentification Server-Based AAA à l'aide de CLI

1. Activé AAA.
2. Spécifié l'adresse IP du serveur ACS.
3. Configurer la clé secrète.
4. Configurer authentification pour utiliser soit RADIUS or TACACS+ server.

# Configuration de l'interface CLI avec les serveurs TACACS +

Topologie de référence pour Server-Based



Configurer AAA TACACS+ Server

```
R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs server Server-T
R1(config-server-tacacs)# address ipv4 192.168.1.101
R1(config-server-tacacs)# single-connection
R1(config-server-tacacs)# key TACACS-Pa55w0rd
R1(config-server-tacacs)# exit
R1(config)#
```

# Configurer le serveur RADIUS à l'aide de CLI

## Configurer AAA RADIUS Server

```
R1(config)# aaa new-model
R1(config)#
R1(config)# radius server SERVER-R
R1(config-radius-server)# address ipv4 192.168.1.100 auth-port 1812 acct-port 1813
R1(config-radius-server)# key RADIUS-Pa55w0rd
R1(config-radius-server)# exit
R1(config)#
```

# Configurer l'Authentification pour Utiliser AAA Server

## Syntaxe des commandes

```
R1(config)# aaa authentication login default ?
cache          Use Cached-group
enable         Use enable password for authentication.
group          Use Server-group
krb5           Use Kerberos 5 authentication.
krb5-telnet    Allow logins only if already authenticated via Kerberos V
               Telnet.
line          Use line password for authentication.
local          Use local username authentication.
local-case     Use case-sensitive local username authentication.
none           NO authentication.
passwd-expiry  enable the login list to provide password aging support

R1(config)# aaa authentication login default group ?
WORD           Server-group name
ldap           Use list of all LDAP hosts.
radius         Use list of all Radius hosts.
tacacs+        Use list of all Tacacs+ hosts.
```

## Configurer l'Authentification Server-Based AAA

```
R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs server Server-T
R1(config-server-tacacs)# address ipv4 192.168.1.100
R1(config-server-tacacs)# single-connection
R1(config-server-tacacs)# key TACACS-Pa55w0rd
R1(config-server-tacacs)# exit
R1(config)#
R1(config)# radius server SERVER-R
R1(config-radius-server)# address ipv4 192.168.1.101 auth-port 1812 acct-port 1813
R1(config-radius-server)# key RADIUS-Pa55w0rd
R1(config-radius-server)# exit
R1(config)#
R1(config)# aaa authentication login default group tacacs+ group radius local-case
```

## Rubrique 3.4.2: Dépannage de l'authentification Server-Based AAA



# Monitoring Authentication Traffic

## Dépannage de l'authentification Server-Based AAA

```
R1# debug aaa authentication
AAA Authentication debugging is on
R1#
14:01:17: AAA/AUTHEN (567936829): Method=TACACS+
14:01:17: TAC+: send AUTHEN/CONT packet
14:01:17: TAC+ (567936829): received authen response status = PASS
14:01:17: AAA/AUTHEN (567936829): status = PASS
```

# Debugging TACACS+ and RADIUS

## Dépanner RADIUS

```
R1# debug radius ?
accounting      RADIUS accounting packets only
authentication  RADIUS authentication packets only
brief           Only I/O transactions are recorded
elog            RADIUS event logging
failover        Packets sent upon fail-over
local-server    Local RADIUS server
retransmit      Retransmission of packets
verbose         Include non essential RADIUS debugs
<cr>
```

## Dépanner TACACS+

```
R1# debug tacacs ?
accounting      TACACS+ protocol accounting
authentication  TACACS+ protocol authentication
authorization   TACACS+ protocol authorization
events          TACACS+ protocol events
packet          TACACS+ packets
<cr>
```



# Débogage de TACACS+ et RADIUS (Cont.)

## Succès de l' Authentification AAA Server-Based

```
R1# debug tacacs
TACACS access control debugging is on
R1#

14:00:09: TAC+: Opening TCP/IP connection to 192.168.1.101 using source 10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.1.101 (AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.1.101 (AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.1.101 (AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15
```

## Échec d'authentification AAA Server-Based

```
R1# debug tacacs
TACACS access control debugging is on
R1#

13:53:35: TAC+: Opening TCP/IP connection to 192.168.1.101 using source 192.48.0.79
13:53:35: TAC+: Sending TCP/IP packet number 416942312-1 to 192.168.1.101 (AUTHEN/START)
13:53:35: TAC+: Receiving TCP/IP packet number 416942312-2 from 192.168.60.15
13:53:35: TAC+ (416942312): received authen response status = GETUSER
13:53:37: TAC+: send AUTHEN/CONT packet
13:53:37: TAC+: Sending TCP/IP packet number 416942312-3 to 192.168.1.101 (AUTHEN/CONT)
13:53:37: TAC+: Receiving TCP/IP packet number 416942312-4 from 192.168.60.15
13:53:37: TAC+ (416942312): received authen response status = GETPASS
13:53:38: TAC+: send AUTHEN/CONT packet
13:53:38: TAC+: Sending TCP/IP packet number 416942312-5 to 192.168.1.101 (AUTHEN/CONT)
13:53:38: TAC+: Receiving TCP/IP packet number 416942312-6 from 192.168.60.15
13:53:38: TAC+ (416942312): received authen response status = FAIL
13:53:40: TAC+: Closing TCP/IP connection to 192.168.60.15
```



# Section 3.5:

## Server-Based AAA Autorisation et Accounting

A la fin de cette section, vous serez en mesure de :

- Configurer l'autorisation sur server-based AAA.
- Configurer l'accounting sur server-based AAA.
- Expliquer les fonctions des composants 802.1x.

## Rubrique 3.5.1: Configurer l'autorisation sur server-based AAA.



# Introduction à l' Autorisation Server-Based AAA

## Authentification vs. Autorisation

- **L'authentification** garantit que le périphérique ou l'utilisateur final est légitime
- **L'autorisation** autorise ou interdit aux utilisateurs authentifiés l'accès à certaines zones et programmes du réseau.

## TACACS+ vs. RADIUS

- **TACACS +** sépare l'authentification de l'autorisation
- **RADIUS** ne distingue pas l'authentification de l'autorisation

# Configuration d'Autorisation AAA à l'aide de CLI

## Syntaxe de Commandes

```
R1(config)# aaa authorization {network | exec | commands level}
{default | list-name} method1...[method4]
```

```
R1(config)# aaa authorization exec ?
WORD      Named authorization list.
default    The default authorization list.
```

```
R1(config)# aaa authorization {network | exec | commands level}
{default | list-name} method1...[method4]
```

```
R1(config)# aaa authorization exec default ?
cache      Use Cached-group
group      Use server-group.
if-authenticated Succeed if user has authenticated.
krb5-instance Use Kerberos instance privilege maps.
local      Use local database.
none       No authorization (always succeeds).
```

```
R1(config)# aaa authorization exec default group ?
WORD       Server-group name
ldap       Use list of all LDAP hosts.
radius     Use list of all Radius hosts.
tacacs+    Use list of all Tacacs+ hosts.
```

## Listes de méthodes d'autorisation


## Exemple d'Autorisation AAA

```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
```

## Rubrique 3.5.2: Configurer l'accounting sur server-based AAA.



# Introduction à Server-Based AAA Accounting



**Accounting**  
What did you spend it on?

Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43210987	01-03	01-13	Payment, Thank You	-\$74.25
01234567	01-12	01-13	Wings 'N' Things Anytown, USA	\$25.25
78901234	01-14	01-17	Record Release Anytown, USA	\$40.00
45678901	01-14	01-17	Sports Stadium Anytown, USA	\$75.25
3210987	01-22	01-23	Tie Tack Anytown, USA	\$20.75
76543210	01-29	01-30	Electronic World Anytown, USA	\$89.25
23455678		01-30	Transaction Fees	\$3.00
34567890		01-01	Annual Fee	\$25.00

PAGE 1 OF 1

**Account Number**  
1234-567-890

**Statement Closing Date**  
01-31-01

**Current Amount Due**  
\$278.50

JOE EMPLOYEE  
456 SKYVIEW DRIVE  
HOMETOWN, USA 99900-1234

MAIL PAYMENT TO:  
**THE BANK**  
132 VINE STREET  
ANYTOWN, USA 67500-0010

872919345 00178255000000003

Detach here and return upper portion with check or money order. Do not staple or fold.

**Statement of Personal Credit Card Account**  
Retain this portion for your files.

**THE BANK**

<b>Cardmember Name</b> JOE EMPLOYEE	<b>Account Number</b> 1234-456-890	<b>Statement Closing Date</b> 01-31-01
Statement Date: 02-01-01	Payment Due Date: 03-01-01	
Closing Date: 01-31-01		
Credit Limit: \$1,500.00	Credit Available: \$1221.50	
New Balance: \$278.50	Minimum Payment Due: \$20.00	

**Account Summary**

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	<b>NEW BALANCE:</b>	<b>\$278.50</b>

# AAA Accounting Configuration with CLI

## Syntaxe de Commande

```
R1(config)#
```

```
aaa accounting {network | exec | connection} {default | list-name}  
{start-stop | stop-only | none} [broadcast] method1...[method4]
```

```
R1(config)# aaa accounting exec?
```

```
WORD      Named Accounting list.  
default   The default accounting list.
```

## Listes des Methodes d'Accounting

```
R1(config)#
```

```
aaa accounting {network | exec | connection} {default | list-name}  
{start-stop | stop-only | none} [broadcast] method1...[method4]
```

```
R1(config)# aaa accounting exec default start-stop?
```

```
broadcast Use Broadcast for Accounting  
group      Use Server-group
```

```
R1(config)# aaa accounting exec default start-stop group?
```

```
WORD      Server-group name  
radius     Use list of all Radius hosts.  
tacacs+    Use list of all Tacacs+ hosts.
```

## Exemple AAA Accounting

```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa5w0rd  
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd  
R1(config)# aaa new-model  
R1(config)# aaa authentication login default group tacacs+  
R1(config)# aaa authorization exec default group tacacs+  
R1(config)# aaa authorization network default group tacacs+  
R1(config)# aaa accounting exec default start-stop group tacacs+  
R1(config)# aaa accounting network default start-stop group tacacs+
```

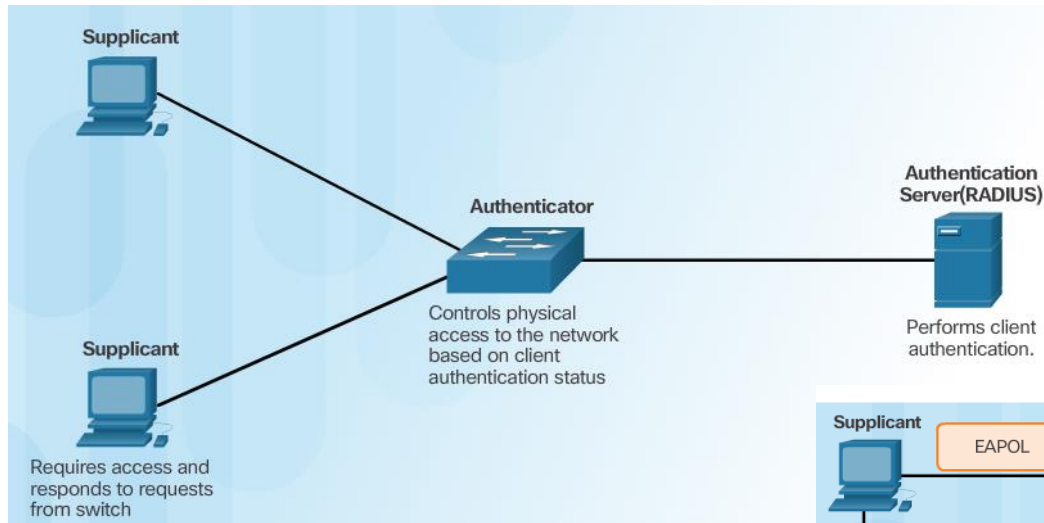


## Rubrique 3.5.3: Authentication 802.1X



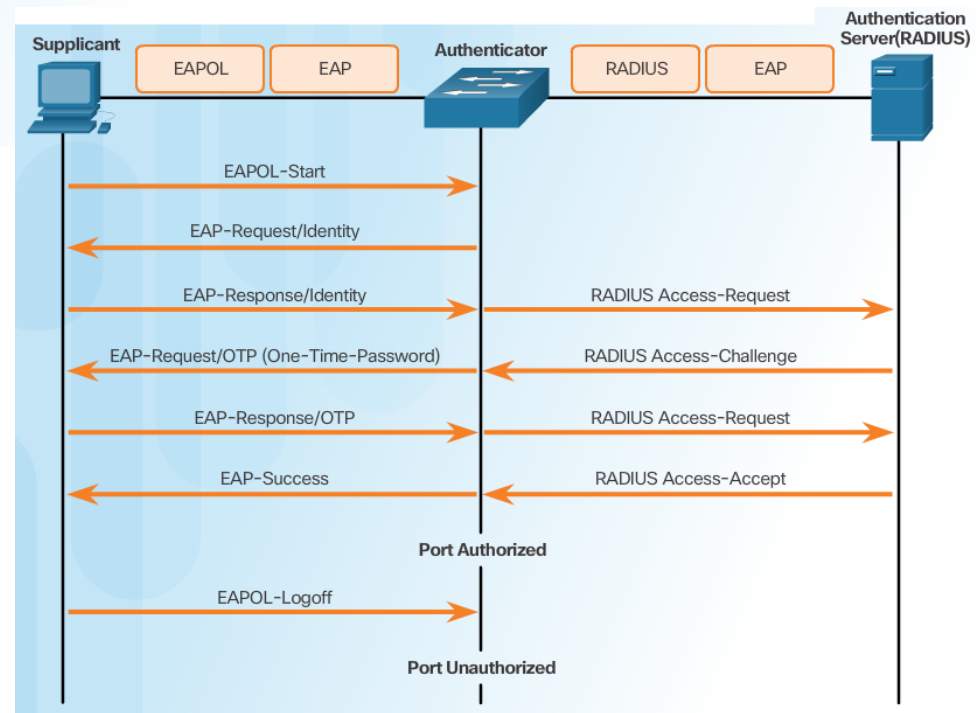


# Sécurité en utilisant l'authentification basée sur le port 802.1X



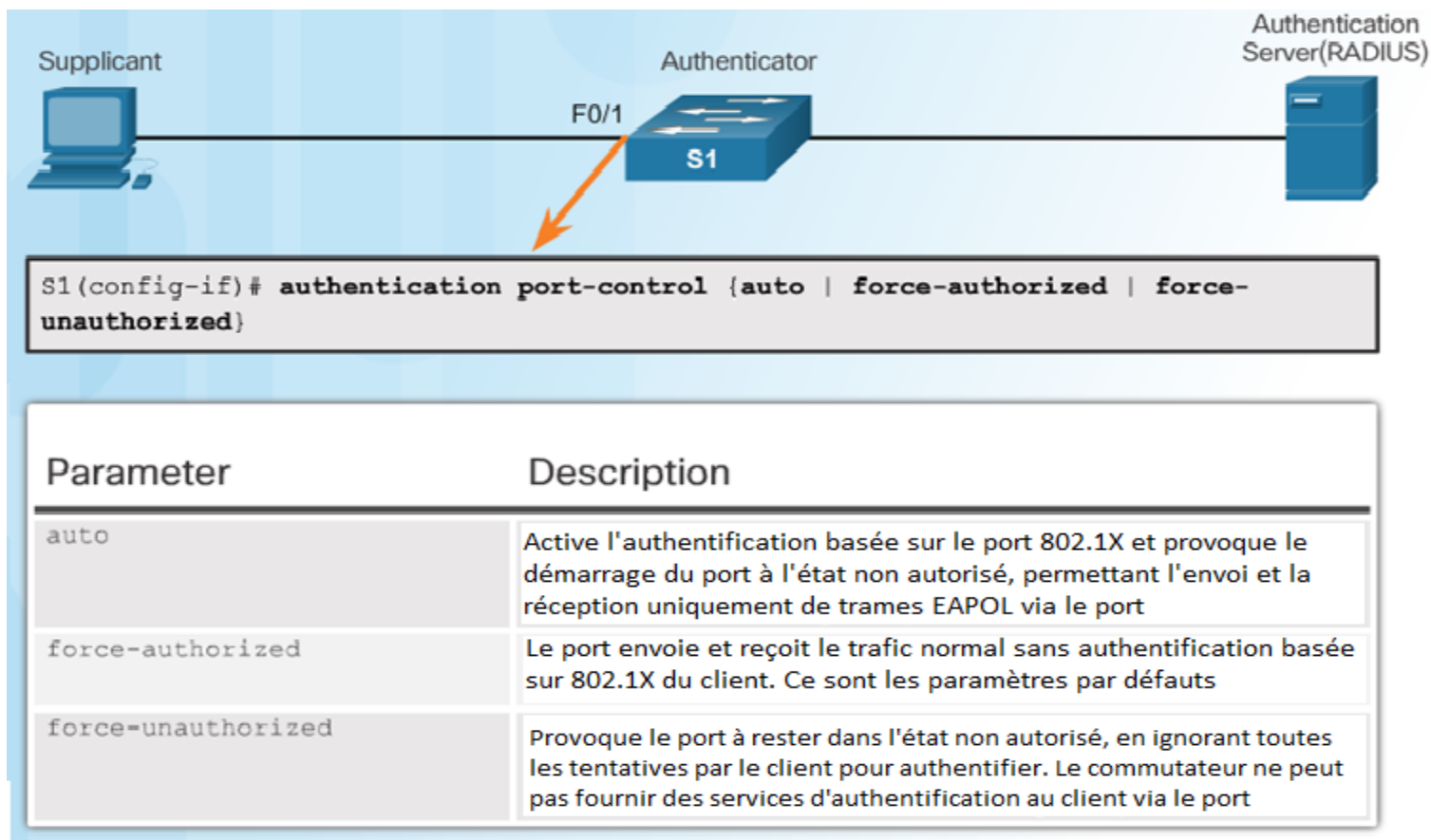
## Rôles 802.1X

## Échange de messages 802.1X

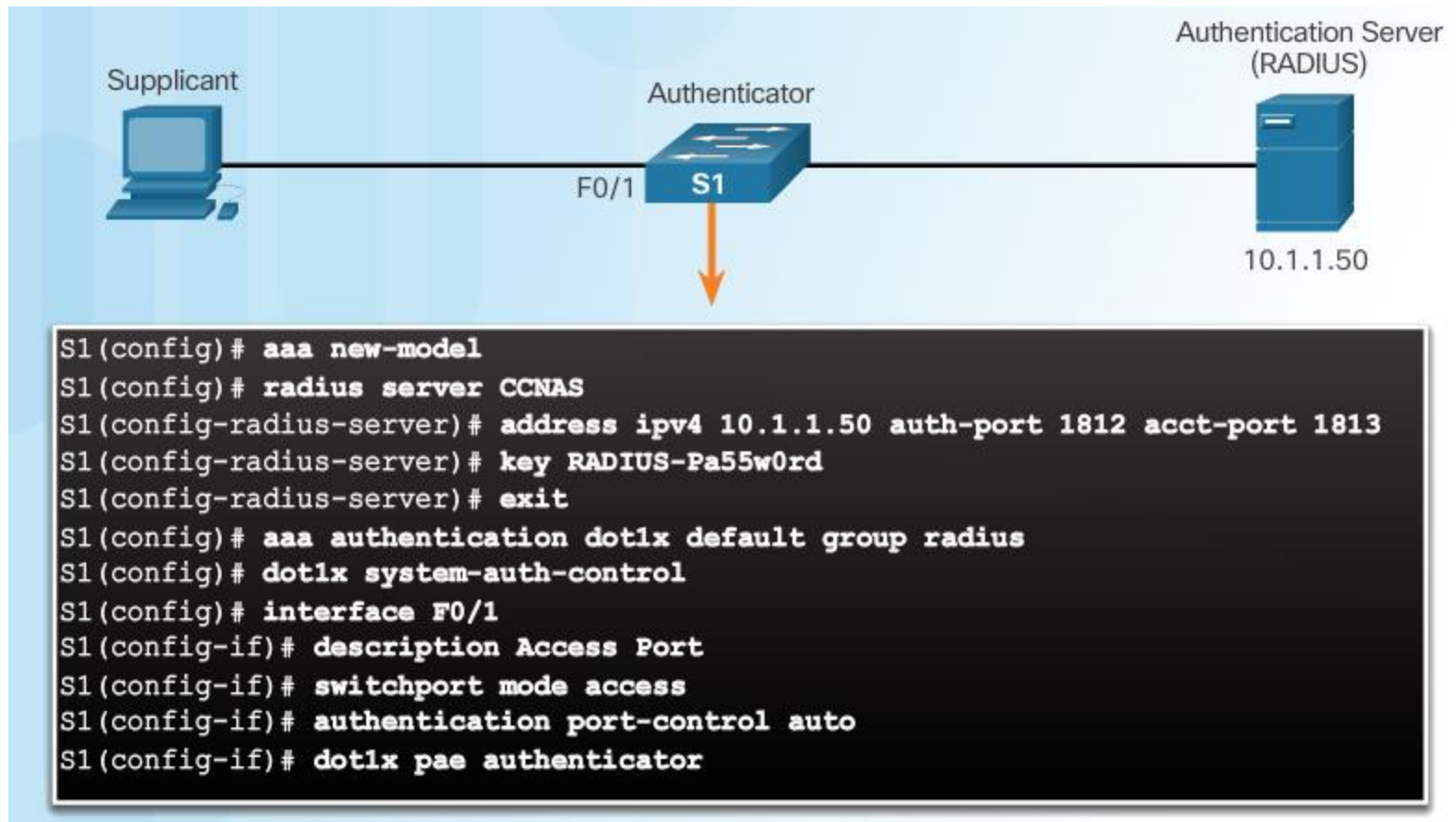


# État d'autorisation de port 802.1X

## Syntaxe de Commande pour dot1x port-control



# Configurer 802.1X



# Section 3.6: Summary

## Objectifs du Chapitre:

- Expliquer comment AAA est utilisé pour sécuriser un réseau.
- Mettre en œuvre l'authentification AAA qui valide les utilisateurs par rapport à une base de données locale.
- Implémentez l'authentification AAA basée sur le serveur en utilisant les protocoles TACACS + et RADIUS.
- Configurer l'autorisation et l'accounting AAA basées sur le serveur.

Thank you.



Cisco Networking Academy  
Mind Wide Open