Chapter special: Authentication, Authorization, and Accounting

Lektor: Jaroslav Dočkal

Chapter Zero

0.0 Metody šifrování

Type 0 – bez šifrování

enable password cisco123

Type 7 – Vigenerova šifra

ena password cisco123

service password-encryption

Type 5 na bázi MD5

enable secret 5 00271A5307542A02D22842

nebo

enable secret cisco123

Type 4 od IOS 15.3(3) – obecný SHA-256

enable secret 4 Rv4kArhts7yA2xd8BD2YTVbts

Type 8 od IOS 15.3(3) solený pbkdf2-hmac-sha256

R1(config)#**enable algorithm-type sha256 secret cisco**

R1(config)#**do sh run | i enable**
enable secret 8
8mTj4RZG8N9ZDOk$elY/asfm8kD3iDmkBe3hD2r4xcA/0oWS5V3o
s.O91u.

R1(config)# **username dockal algorithm-type sha256 secret class**

R1# **show running-config | inc username**
username dockal secret 8
8dsYGNam3K1SIJO$7nv/35M/qr6t.dVc7UY9zrJDWRVqncHub1PE
9UlMQFs

Type 9 od IOS 15.3(3)- SHA256 pro hesla

SHA256, ale speciálně zaměřené na hesla

R1(config)#**ena algorithm-type scrypt secret cisco**

R1(config)#do sh run | i enable
enable secret 9
9WnArItcQHW/uuE$x5WTLbu7PbzGDuv0fSwGKS/KURsy5a3WC
QckmJp0MbE:

R1(config)# **username dockal algorithm-type scrypt secret cisco**

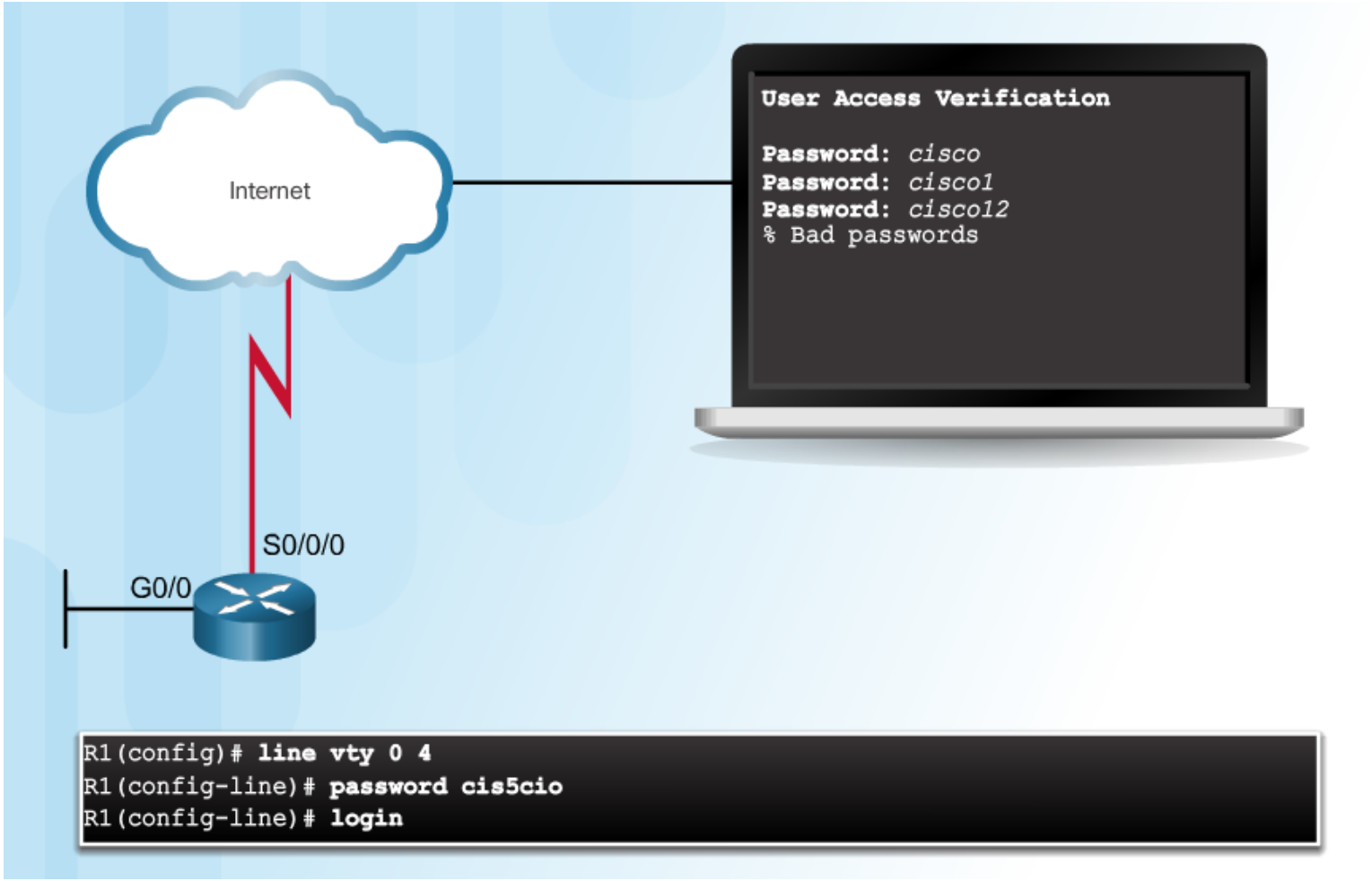
R1# show running-config | inc username
username dockal secret 9
9nhEmQVczB7dqsO$X.HsgL6x1il0RxkOSSvyQYwucySCt7qFm4v
7pqCxkKM

Chapter Outline

Section 3.1:
Purpose of the AAA

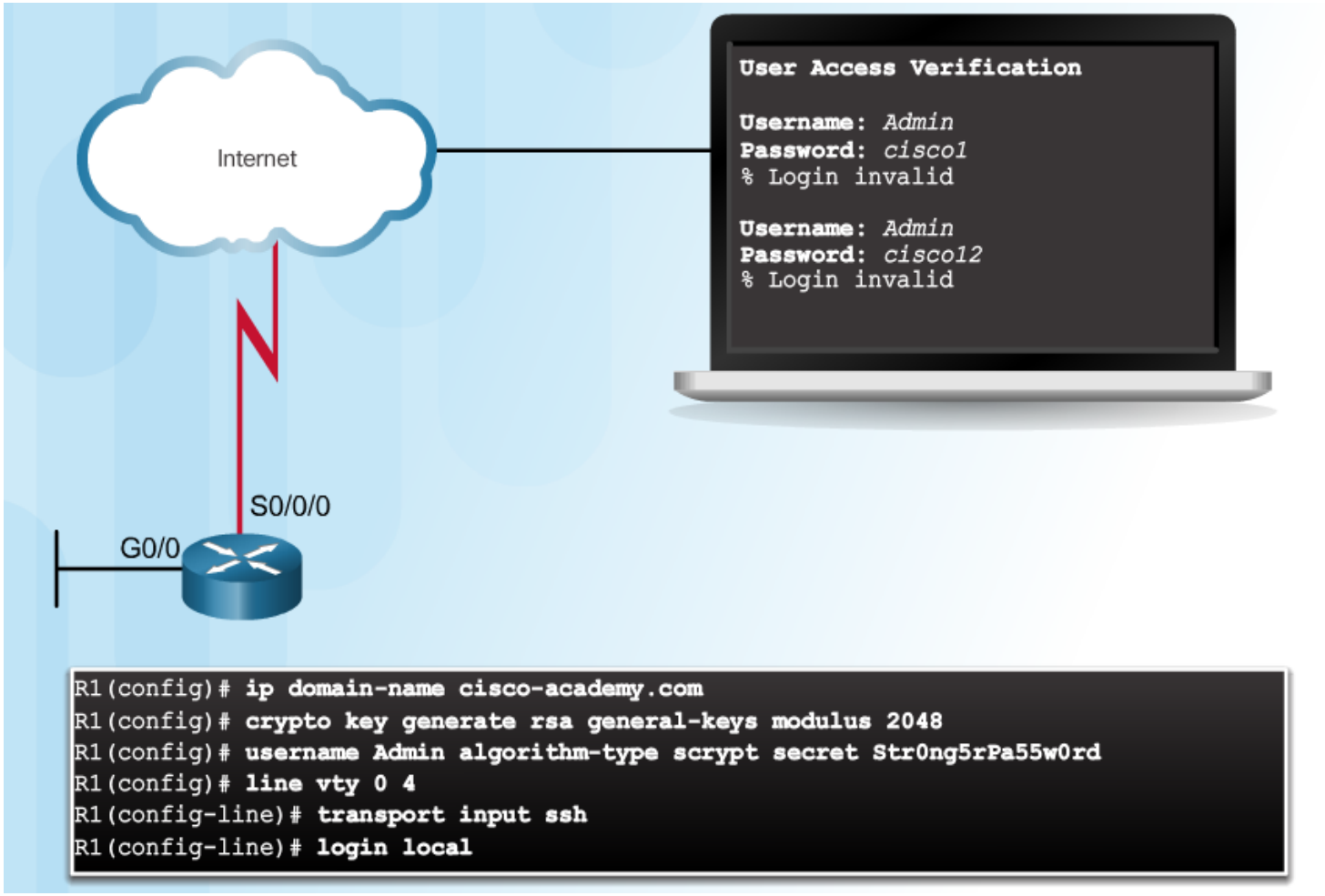
Authentication without AAA

Telnet is Vulnerable to Brute-Force Attacks



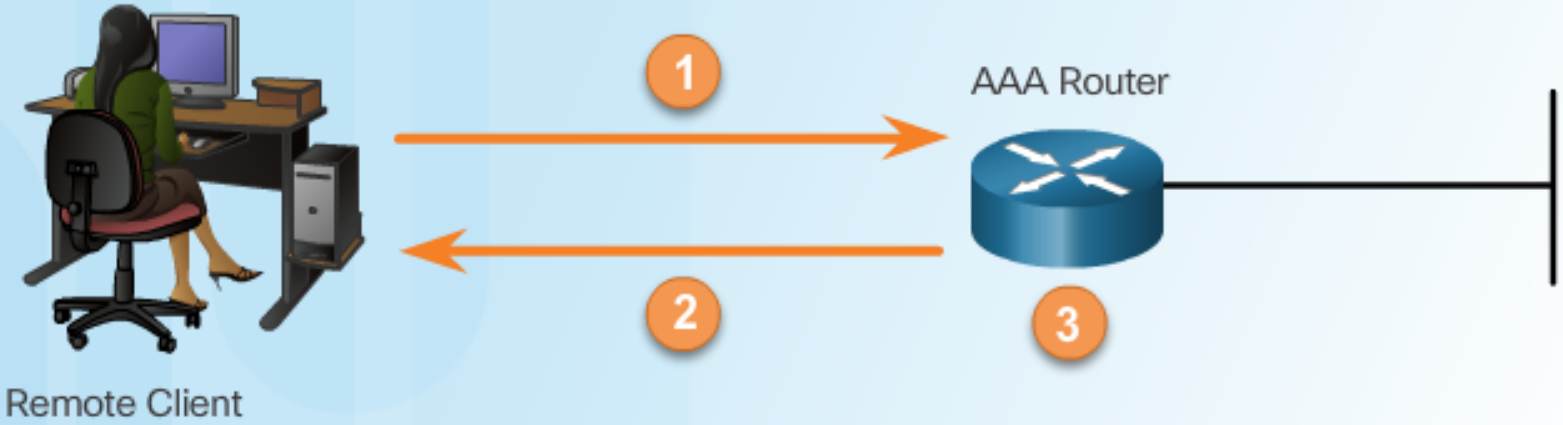
Authentication without AAA (Cont.)

SSH and Local Database Method



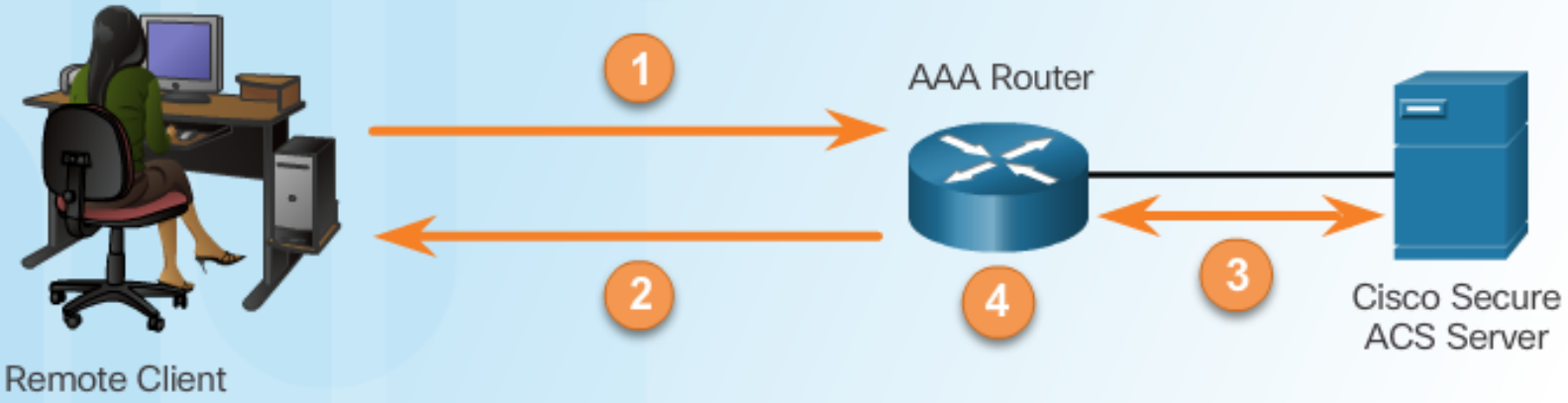
Topic 3.1.2:
AAA Characteristics

Local AAA Authentication



1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using the local database and the user is authorized to access the network based on information in the local database.

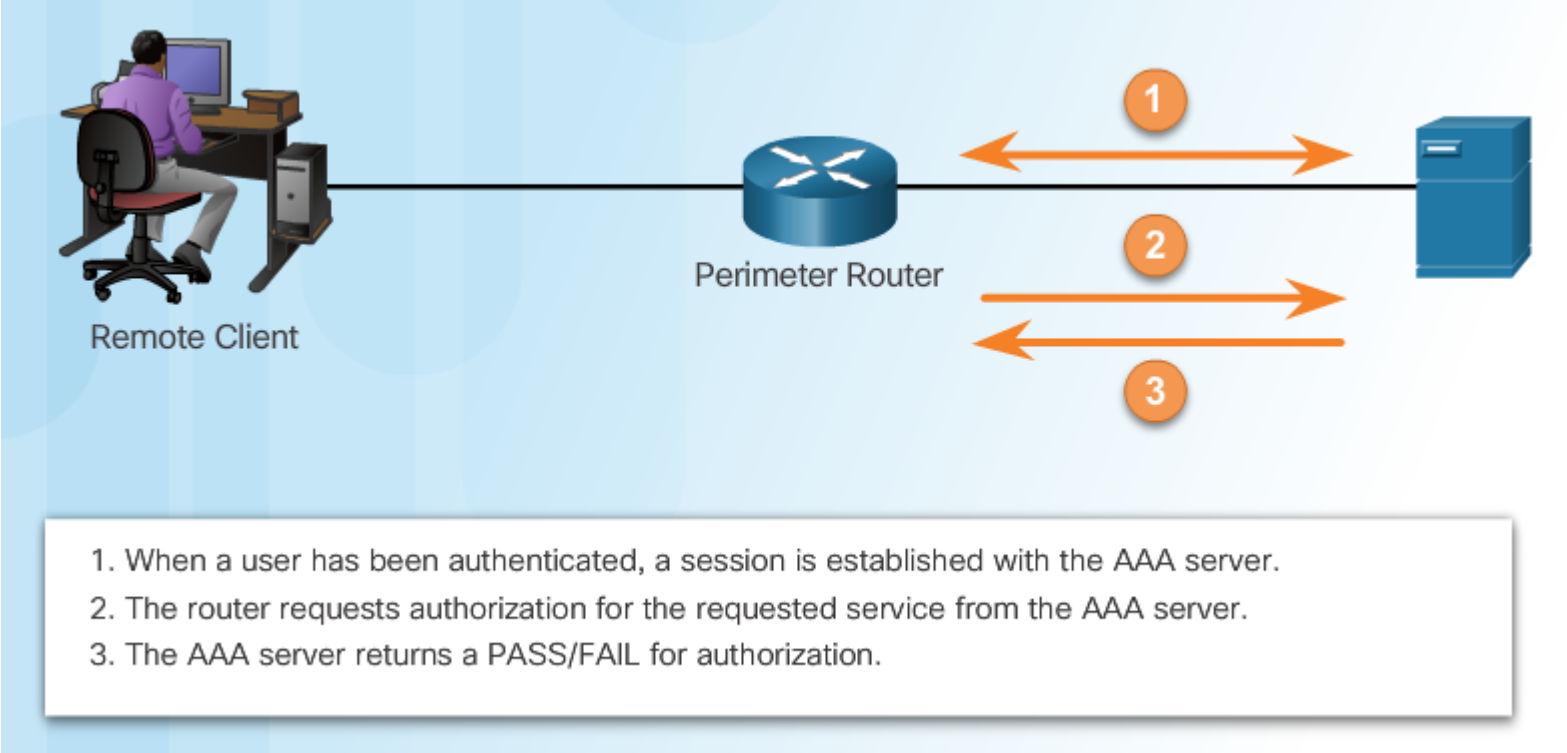
Server-Based AAA Authentication



1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a remote AAA server.
4. The user is authorized to access the network based on information on the remote AAA Server.

Authorization

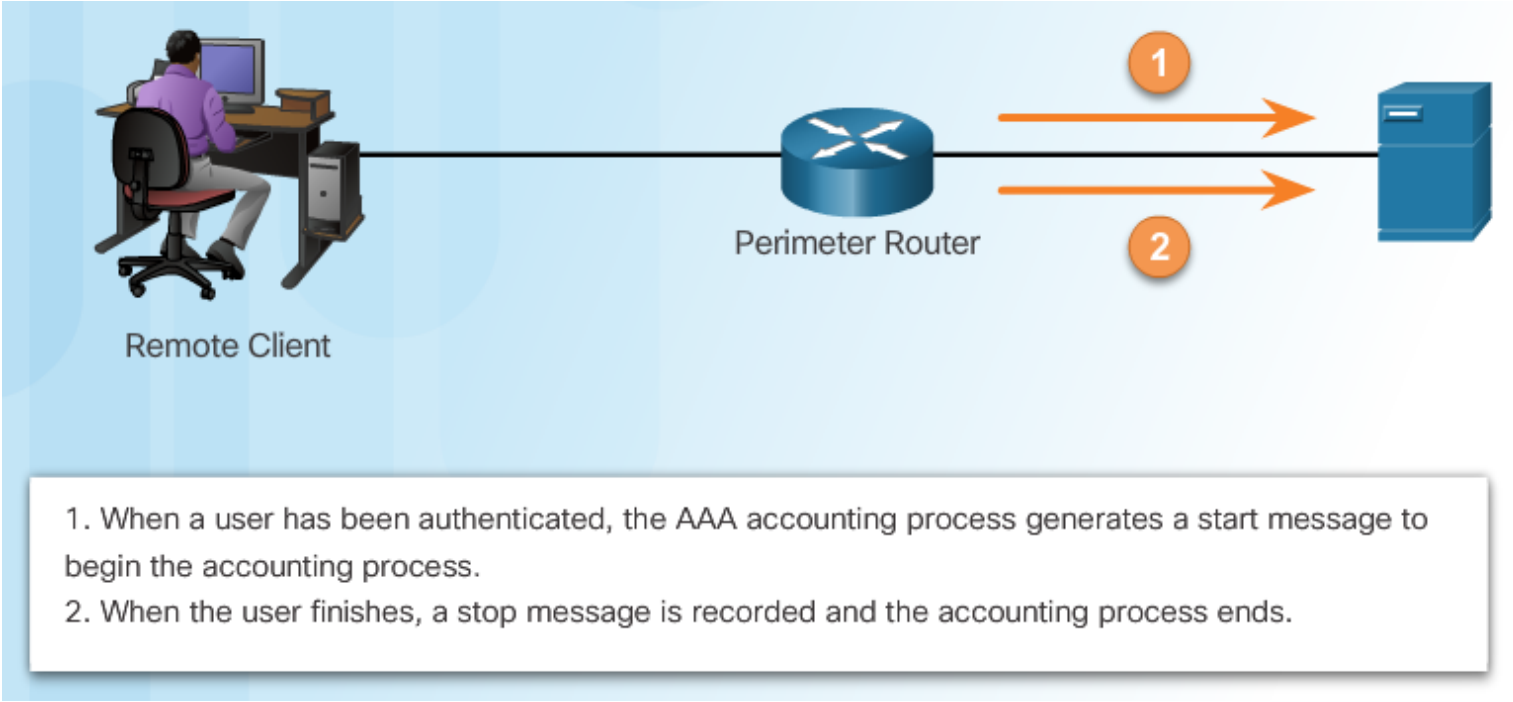
AAA Authorization



Accounting

Types of accounting information:

- Network
- Connection
- EXEC
- System
- Command
- Resource



Section 3.2: Local AAA Authentication

Upon completion of this section, you should be able to:

- Configure AAA authentication, using the CLI, to validate users against a local database.
- Troubleshoot AAA authentication that validates users against a local database.

Topic 3.2.1:
Configuring Local AAA Authentication with CLI

Authenticating Administrative Access

1. Add usernames and passwords to the local router database for users that need administrative access to the router.
2. Enable AAA globally on the router.
3. Configure AAA parameters on the router.
4. Confirm and troubleshoot the AAA configuration.

```
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)#
```

Authentication Methods

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

Authentication Command

```
router(config-line)#
aaa authentication login {default | list-name} method1…[method4]
```

Command	Description
default	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in.
method1...[method4]	Identifies the list of methods that the AAA authentication process will query in the given sequence. At least one method must be specified. A maximum of four methods may be specified.

Default and Named Methods

Example Local AAA Authentication

```
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
```

Fine-Tuning the Authentication Configuration

Command Syntax

```
Router(config)#
aaa local authentication attempts max-fail [number-of-unsuccessful-attempts]
```

Command	Description
number-of-unsuccessful-attempts	Number of unsuccessful authentication attempts before a connection is dropped and the user account is locked.

Fine-Tuning the Authentication Configuration

Display Locked Out Users

```
R1# show aaa local user lockout
                Local-user          Lock time
                JR-ADMIN            04:28:49 UTC Sat Dec 27 2015
```

Fine-Tuning the Authentication Configuration
Show Unique ID of a Session

```
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
```

Topic 3.2.2:
Troubleshooting Local AAA Authentication

Debug Options

Debug Local AAA Authentication

```
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

Understanding Debug Output

```
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

Upon completion of this section, you should be able to:

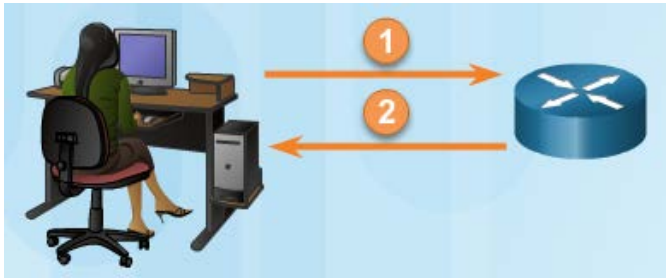
- Describe the benefits of server-based AAA.
- Compare the TACACS+ and RADIUS authentication protocols.

Topic 3.3.1:
Server-Based AAA Characteristics

Comparing Local AAA and Server-Based AAA Implementations

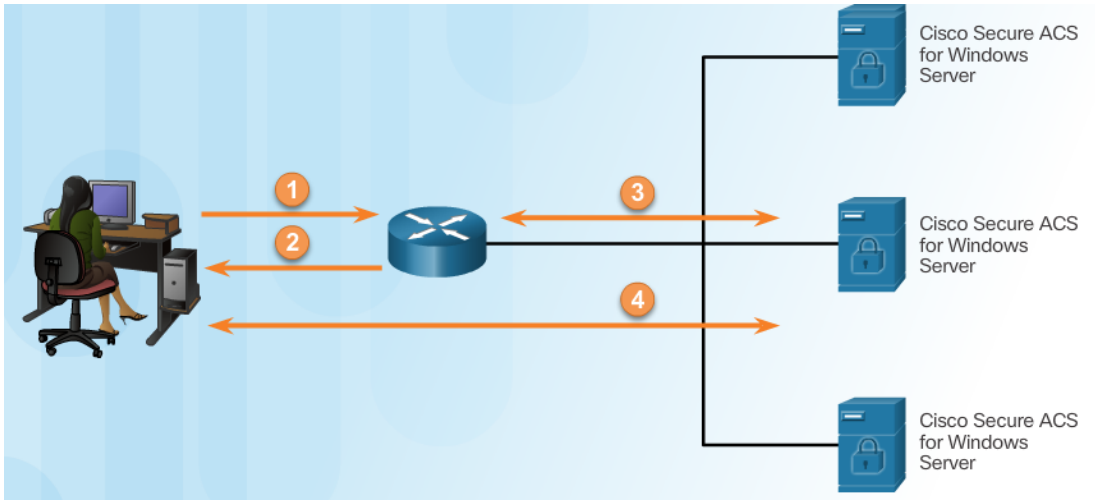
Local authentication:

1. User establishes a connection with the router.
2. Router prompts the user for a username and password, authentication the user using a local database.

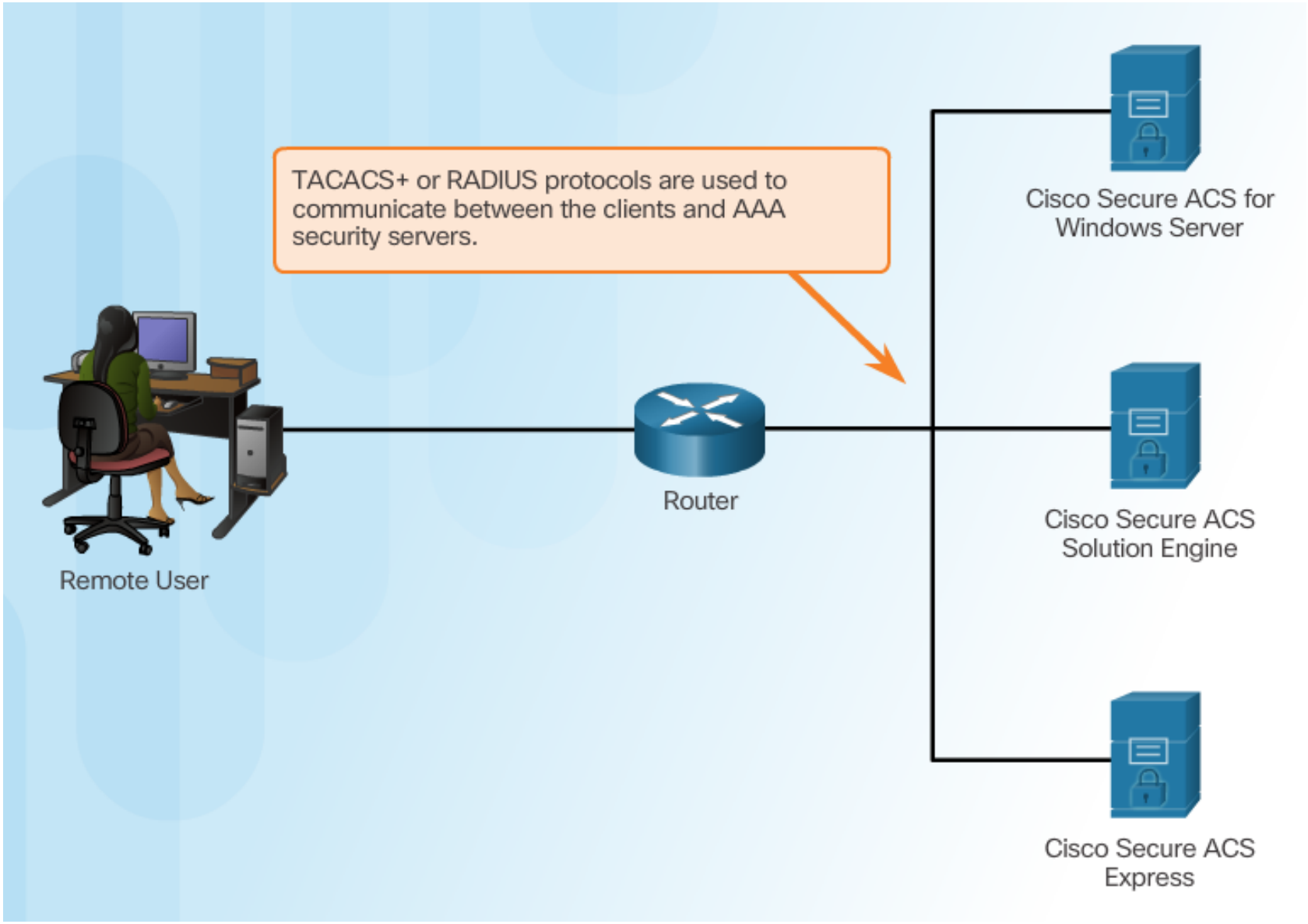


Server-based authentication:

1. User establishes a connection with the router.
2. Router prompts the user for a username and password.
3. Router passes the username and password to the Cisco Secure ACS (server or engine)
4. The Cisco Secure ACS authenticates the user.



Introducing Cisco Secure Access Control System



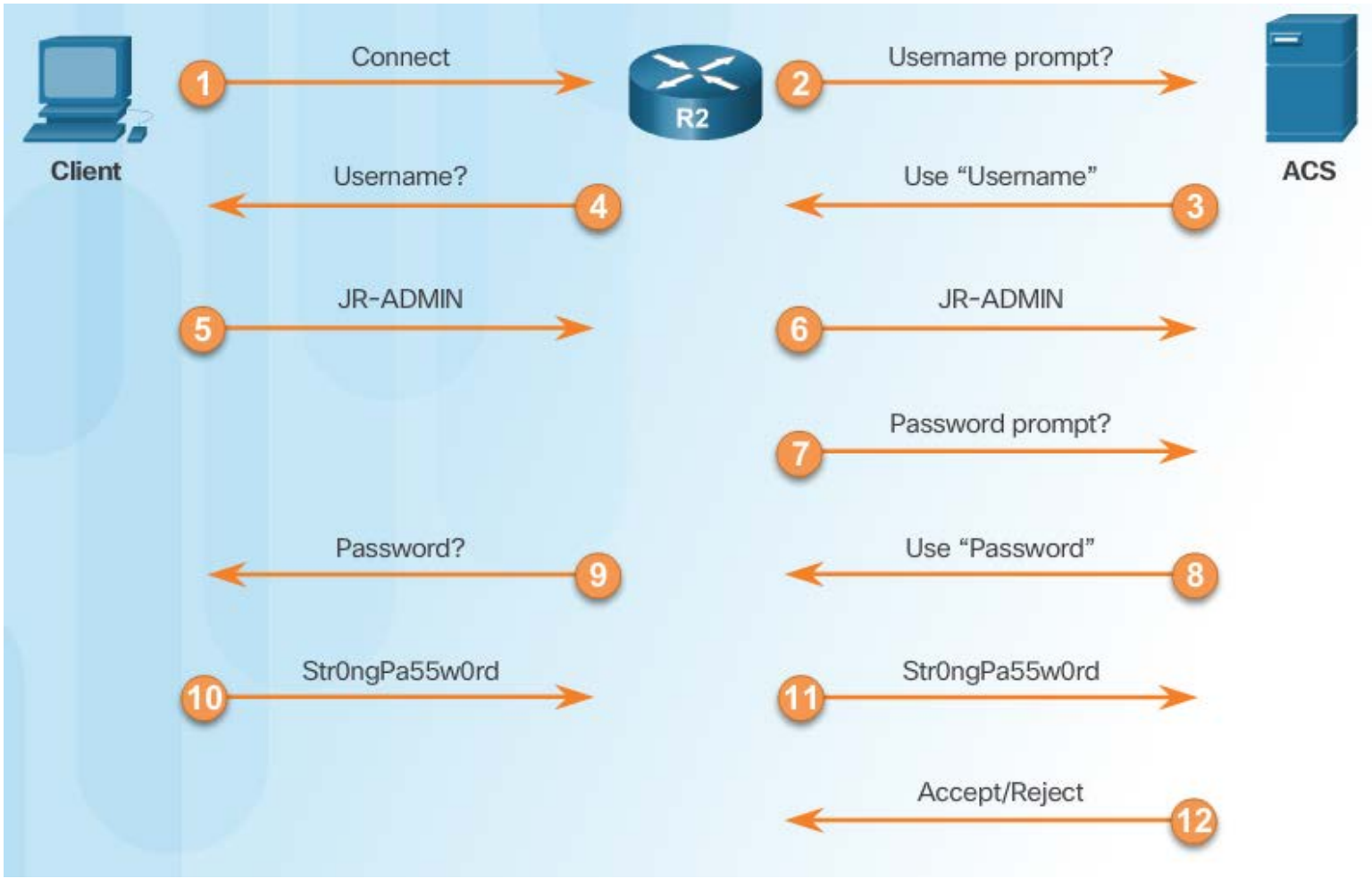
Topic 3.3.2:
Server-Based AAA Communication Protocols

Introducing TACACS+ and RADIUS

	TACACS+	RADIUS
Functionality	Separates AAA according to the AAA architecture, allowing modularity of the security server implementation	Combines authentication and authorization but separates accounting, allowing less flexibility in implementation than TACACS+
Standard	Mostly Cisco supported	Open/RFC standard
Transport Protocol	TCP	UDP
CHAP	Bidirectional challenge and response as used in Challenge Handshake Authentication Protocol (CHAP)	Unidirectional challenge and response from the RADIUS security server to the RADIUS client
Protocol Support	Multiprotocol support	No ARA, no NetBEUI
Confidentiality	Entire packet encrypted	Password encrypted
Customization	Provides authorization of router commands on a per-user or per-group basis	Has no option to authorize router commands on a per-user or per-group basis
Accounting	Limited	Extensive

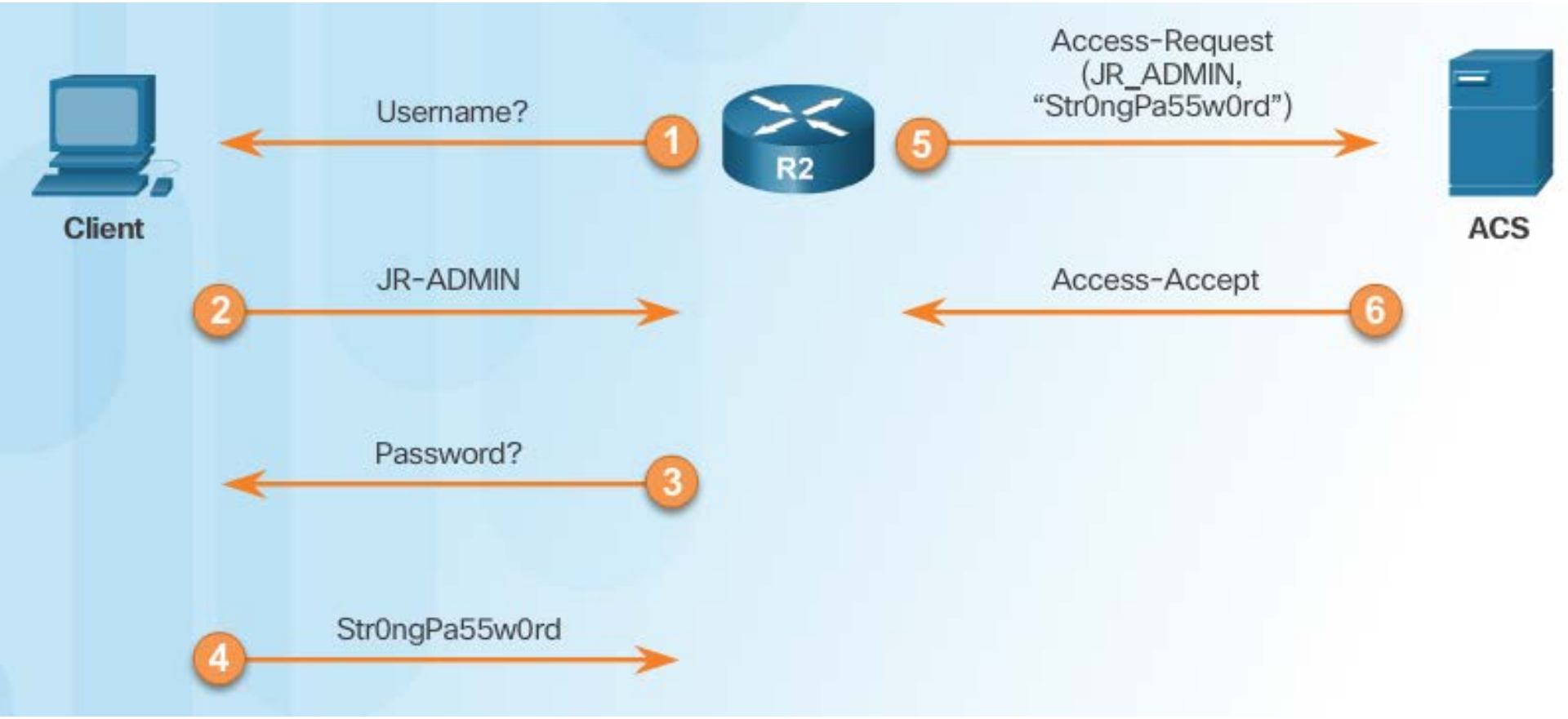
TACACS+ Authentication

TACACS+ Authentication Process



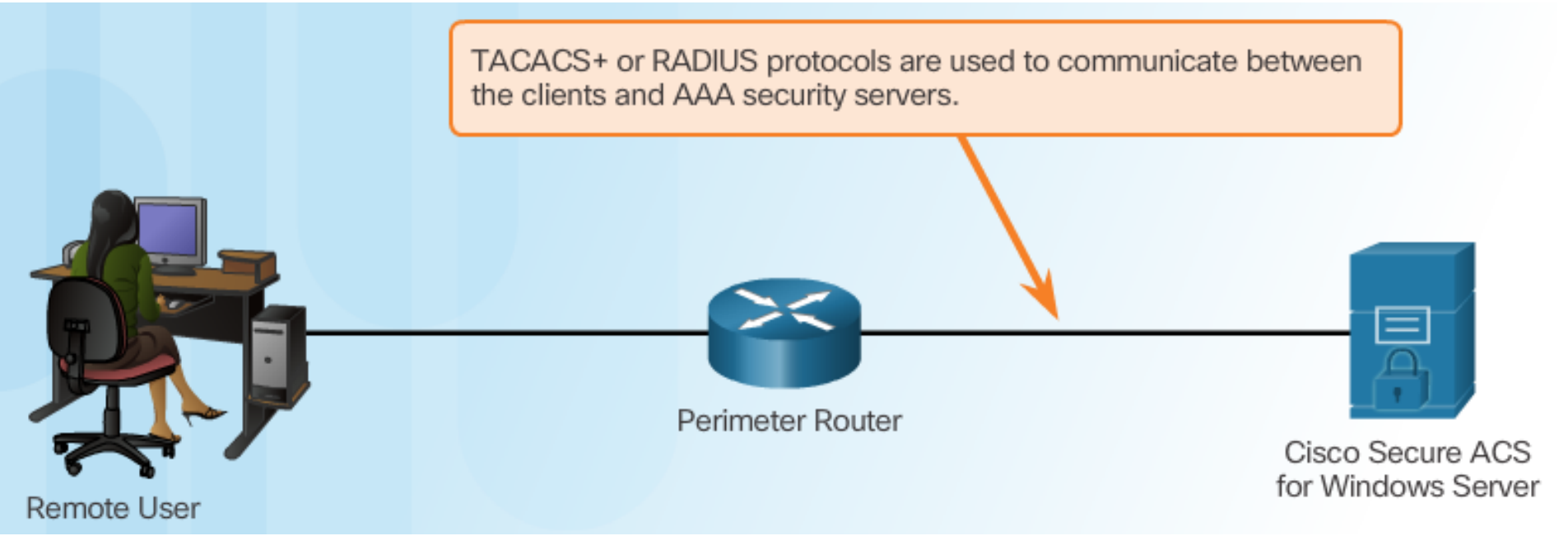
RADIUS Authentication

RADIUS Authentication Process

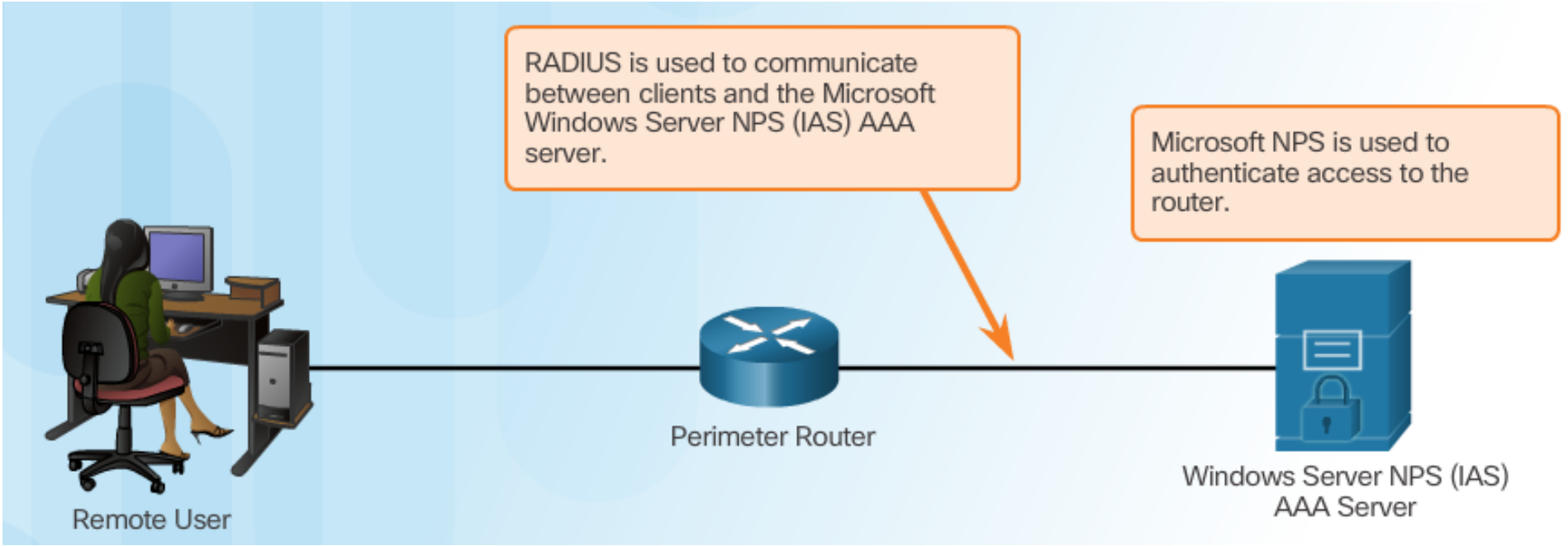


Integration of TACACS+ and ACS

Cisco Secure ACS



Integration of AAA with Active Directory



Internet Authentication Service (*IAS*) byl přejmenován na Network Policy Server (*NPS*).

Section 3.4: Server-Based AAA Authentication

Upon completion of this section, you should be able to:

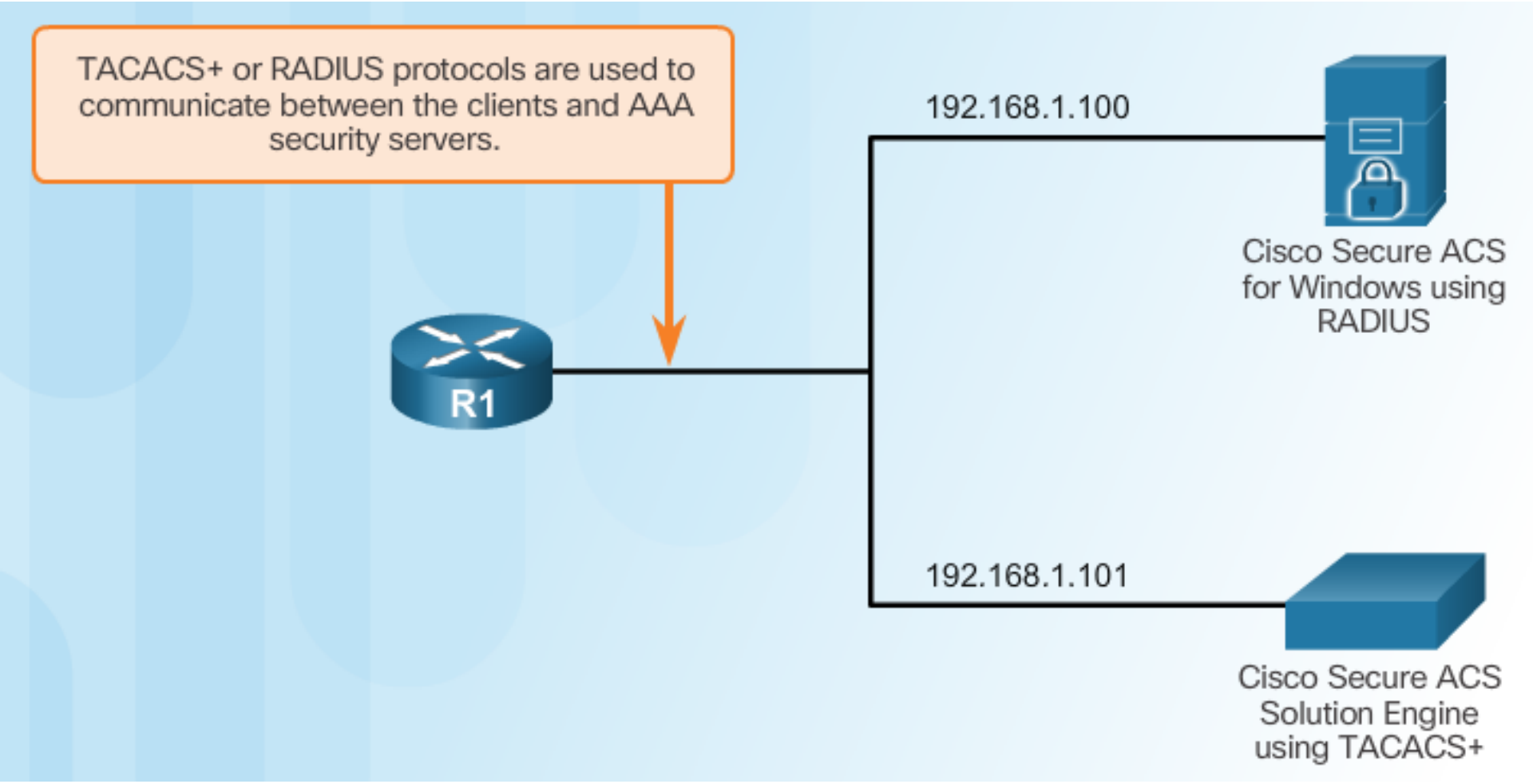
- Configure server-based AAA authentication, using the CLI, on Cisco routers.
- Troubleshoot server-based AAA authentication.

Topic 3.4.1:
Configuring Server-Based Authentication with CLI

Steps for Configuring Server-Based AAA Authentication with CLI

1. Enable AAA.
2. Specify the IP address of the ACS server.
3. Configure the secret key.
4. Configure authentication to use either the RADIUS or TACACS+ server.

Configuring the CLI with TACACS+ Servers



Cisco Access Control Server (ACS) a **Cisco Identity Services Engine (ISE)**
ACS supports only network access/Device admin. ISE has a lot more services.

Configure a 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)#
```

Configuring the CLI for RADIUS Servers

```
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)#
```

Configure Authentication to Use the AAA Server

```
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.
```

Configure Authentication to Use the AAA Server

```
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
```

Topic 3.4.2:
Troubleshooting Server-Based AAA Authentication

Monitoring Authentication Traffic

```
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

```
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>
```

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

Debugging TACACS+

```
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
```

Debugging TACACS+

```
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 Authorization and Accounting

Upon completion of this section, you should be able to:

- Configure server-based AAA authorization.
- Configure server-based AAA accounting.
- Explain the functions of 802.1x components.

Topic 3.5.1:
Configuring Server-Based AAA Authorization

Introduction to Server-Based AAA Authorization

Authentication vs. Authorization

- **Authentication** ensures a device or end-user is legitimate
- **Authorization** allows or disallows authenticated users access to certain areas and programs on the network.

TACACS+ vs. RADIUS

- **TACACS+** separates authentication from authorization
- **RADIUS** does **not** separate authentication from authorization

AAA Authorization Configuration with CLI

Command Syntax

```
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.
```

AAA Authorization Configuration with CLI

Authorization Method Lists

```
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.
```

AAA Authorization Configuration with CLI

Example AAA Authorization

```
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+
```

Topic 3.5.2:
Configuring Server-Based AAA Accounting

AAA Accounting Configuration with CLI

Command Syntax

```
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.
```

AAA Accounting Configuration with CLI

Accounting Method Lists

```
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.
```

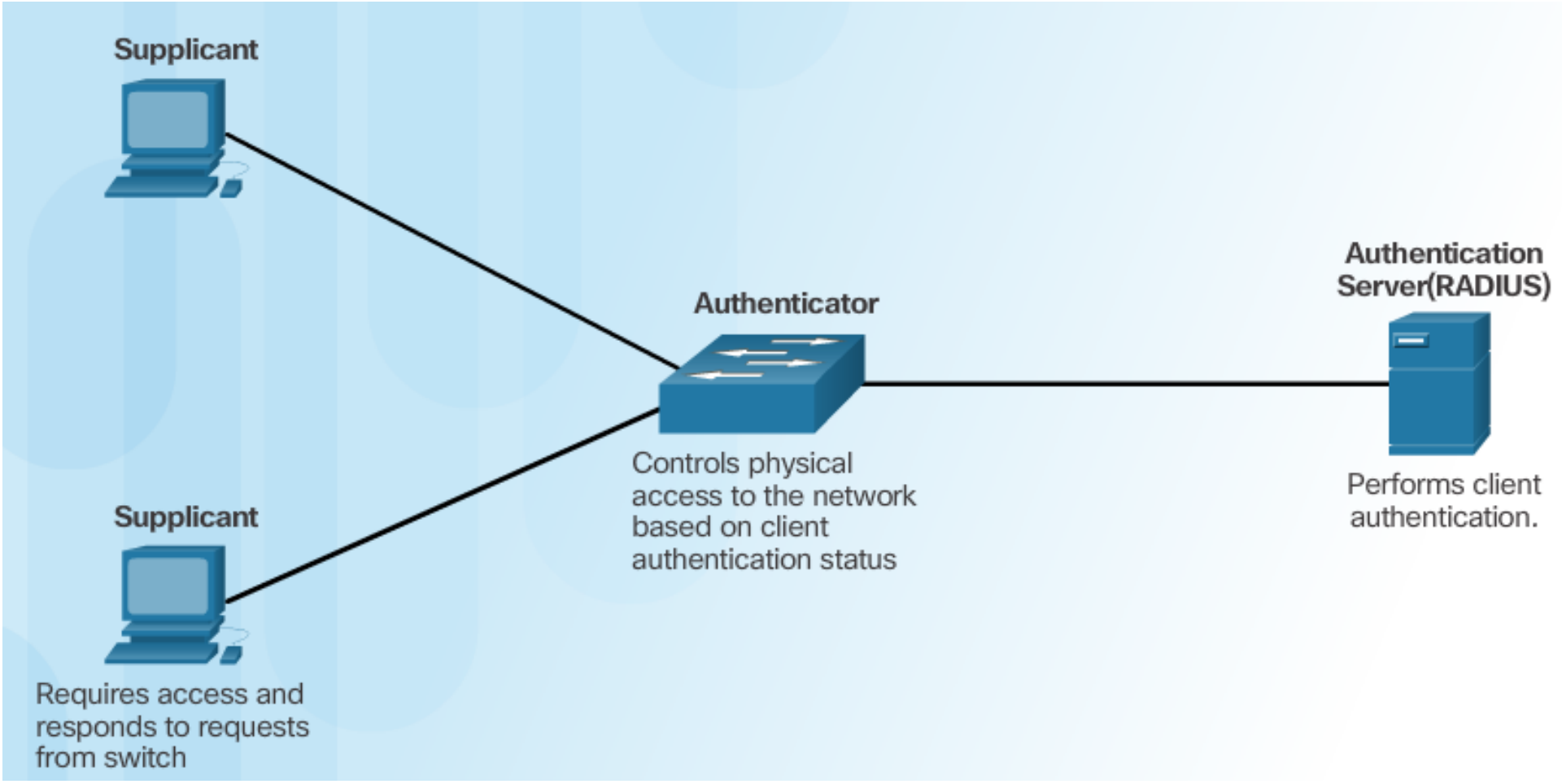
AAA Accounting Configuration with CLI

Example 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+
```

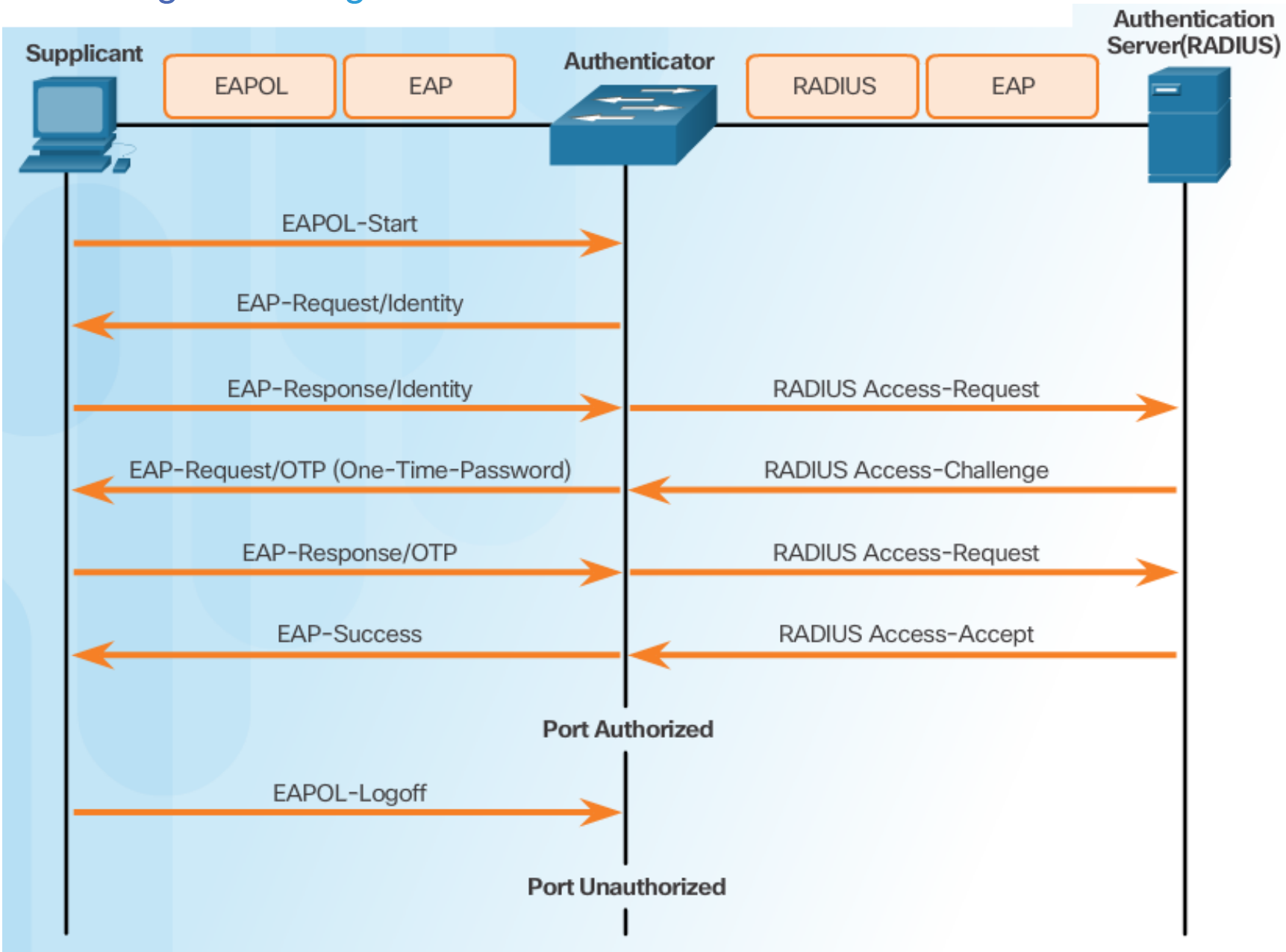
Topic 3.5.3:
802.1X Authentication

Security Using 802.1X Port-Based Authentication

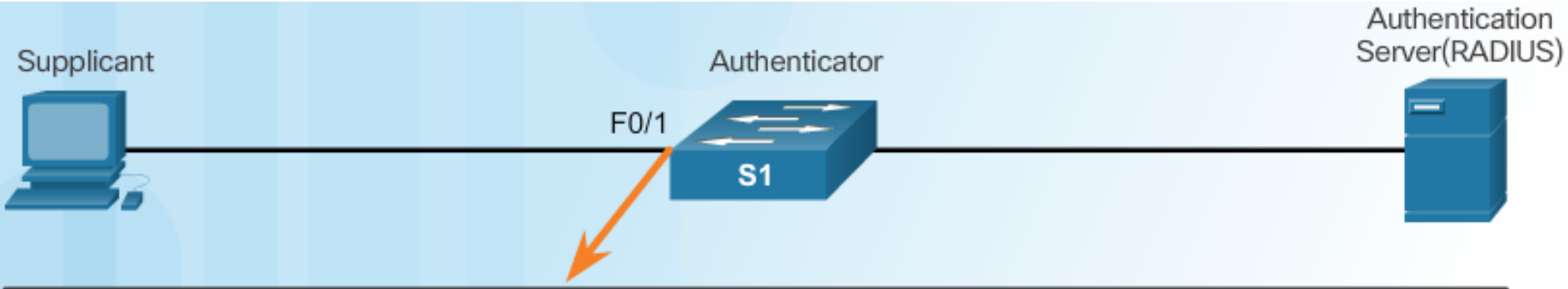


Security Using 802.1X Port-Based Authentication

802.1X Message Exchange



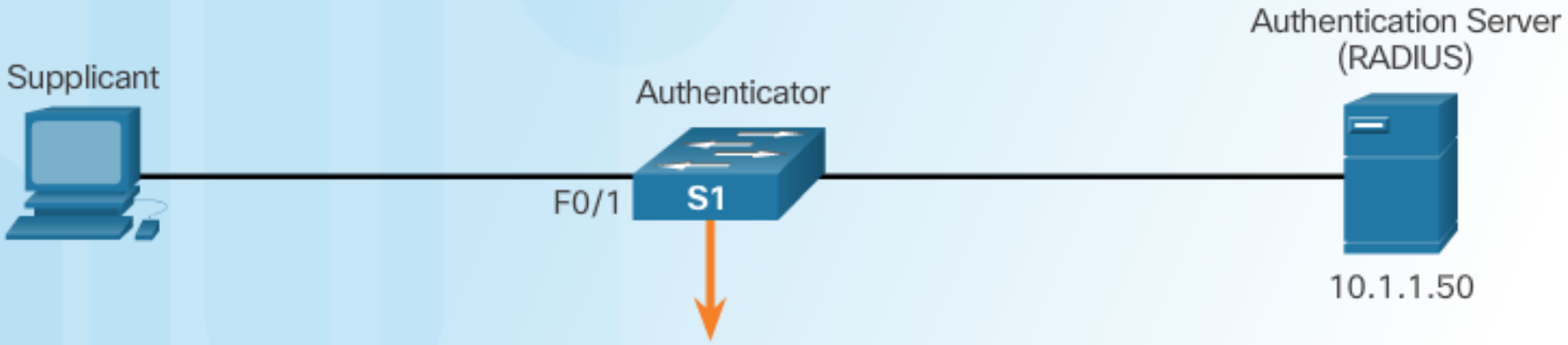
802.1X Port Authorization State




```
S1(config-if)# authentication port-control {auto | force-authorized | force-unauthorized}
```

Parameter	Description
auto	Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, enabling only EAPOL frames to be sent and received through the port.
force-authorized	The port sends and receives normal traffic without 802.1x-based authentication of the client. This is the default setting.
force-unauthorized	Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.

Configuring 802.1X




```
S1(config)# aaa new-model
S1(config)# radius server CCNAS
S1(config-radius-server)# address ipv4 10.1.1.50 auth-port 1812 acct-port 1813
S1(config-radius-server)# key RADIUS-Pa55w0rd
S1(config-radius-server)# exit
S1(config)# aaa authentication dot1x default group radius
S1(config)# dot1x system-auth-control
S1(config)# interface F0/1
S1(config-if)# description Access Port
S1(config-if)# switchport mode access
S1(config-if)# authentication port-control auto
S1(config-if)# dot1x pae authenticator
```