Cisco Networking Academy
Mind Wide Open

Wykład 6: Uwierzytelnianie, autoryzacja i konta użutkowników

dr inż. Maciej Sobieraj

Plan wykładu

6.0 Wprowadzenie

6.1 Zastosowania protokołu AAA

6.2 Lokalne uwierzytelnianie AAA

6.3 AAA oparte na serwerze

6.4 Uwierzytelnianie AAA oparte na serwerze

6.5 Uwierzytelnianie I konta użytkowników na serwerze

6.6 Monitorowanie i zarządzanie urządeniami

6.7 Podsumowanie

Rozdział 6.1: Zastosowanie protokołu AAA

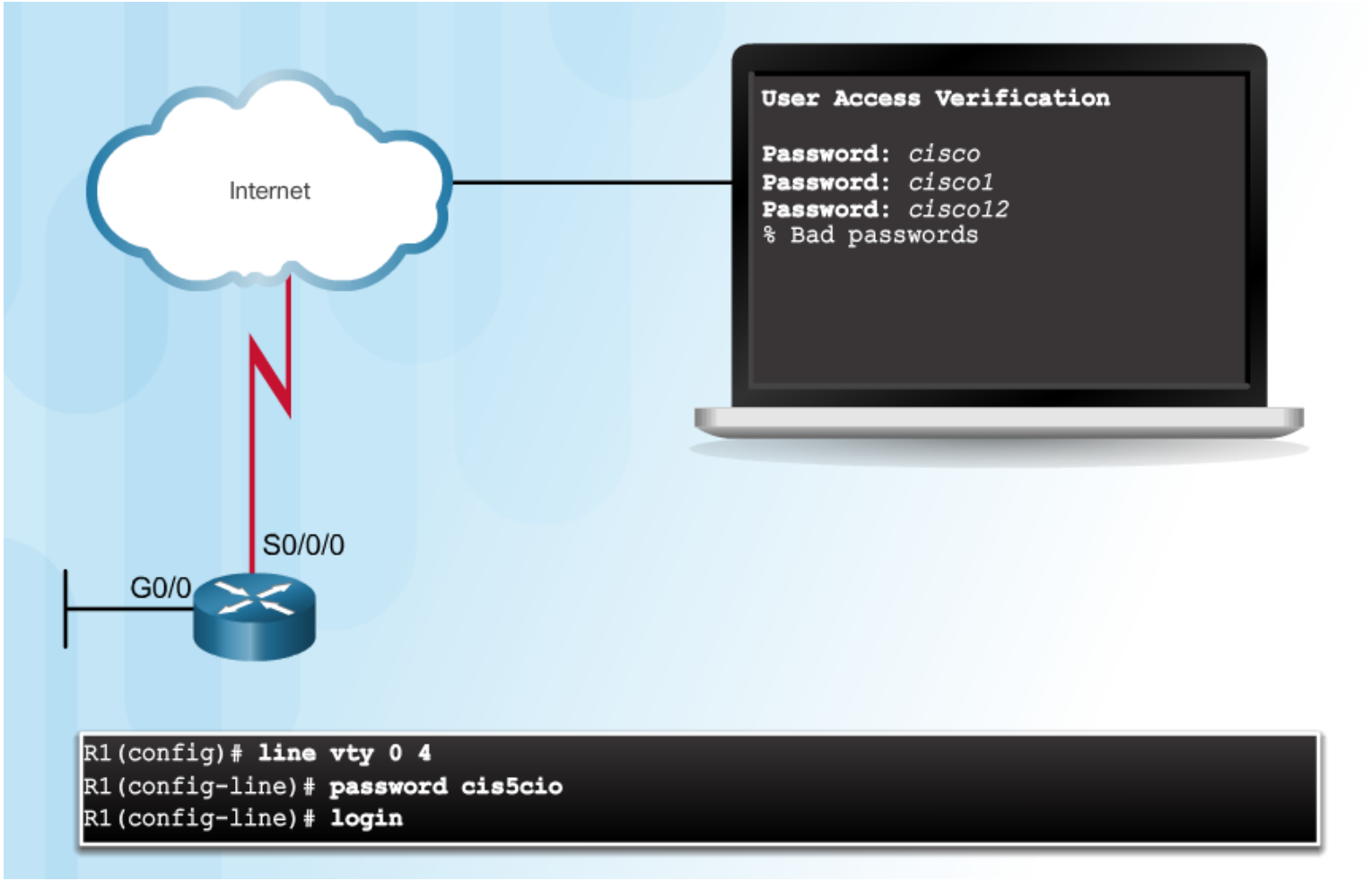
Po zakończeniu tej części, powinieneś być w stanie:

- Dlaczego protokół AAA jest tak istotny w bezpieczeństwie sieci.
- Opisać charakterystykę AAA.

Temat 6.1.1: Protokół AAA

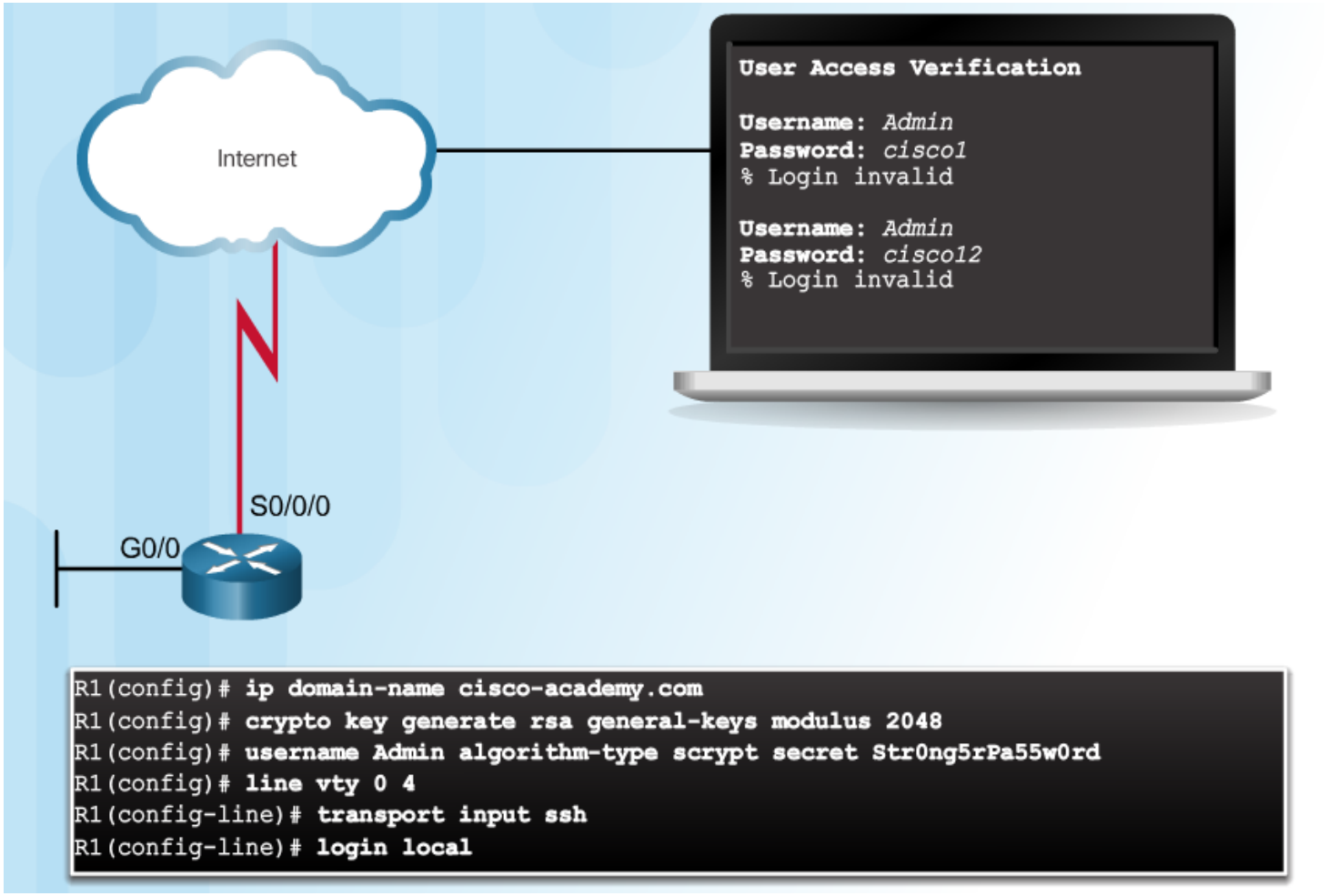
Uwierzytelnianie bez użycia AAA

Telnet jest narażony na ataki typu Brute-Force

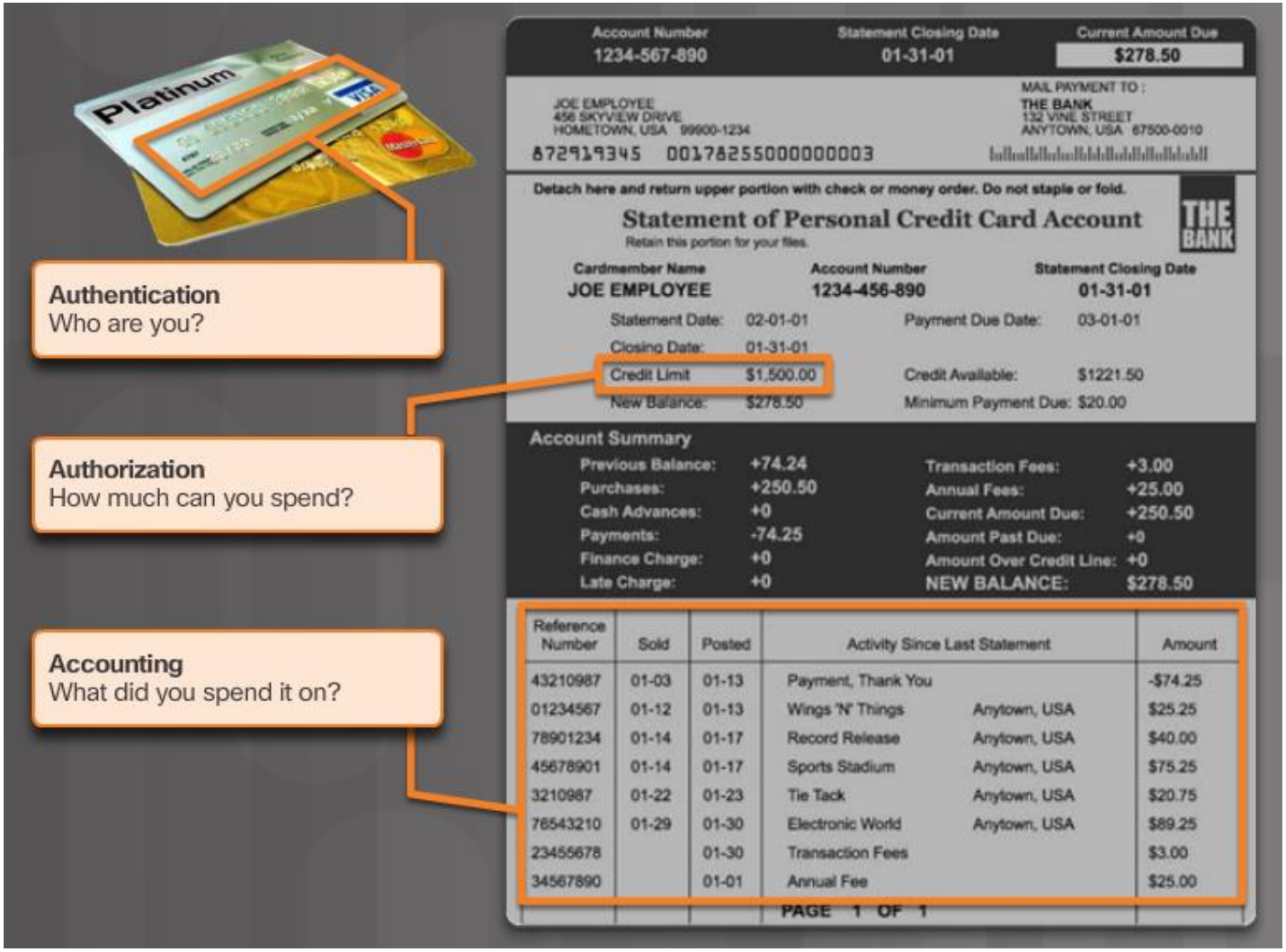


Uwierzytelnianie bez użycia AAA

SSH i lokalna baza użytkowników



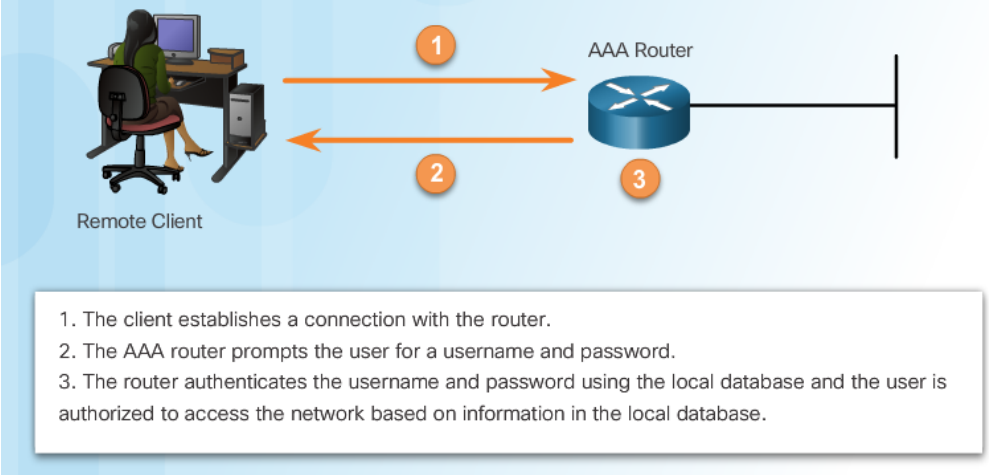
Składniki AAA



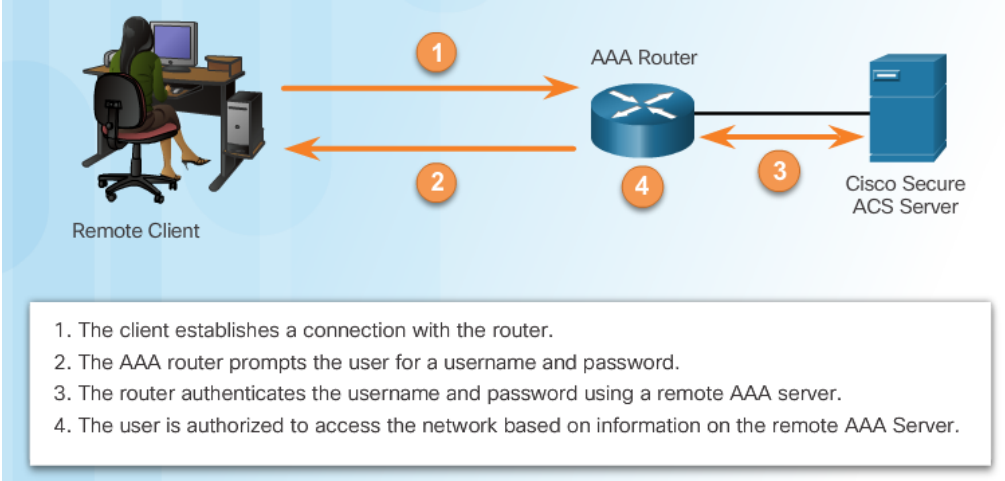
Temat 6.1.2: Charamkterystyka AAA

Tryby uwierzytelniania

Lokalne uwierzytelnianie AAA

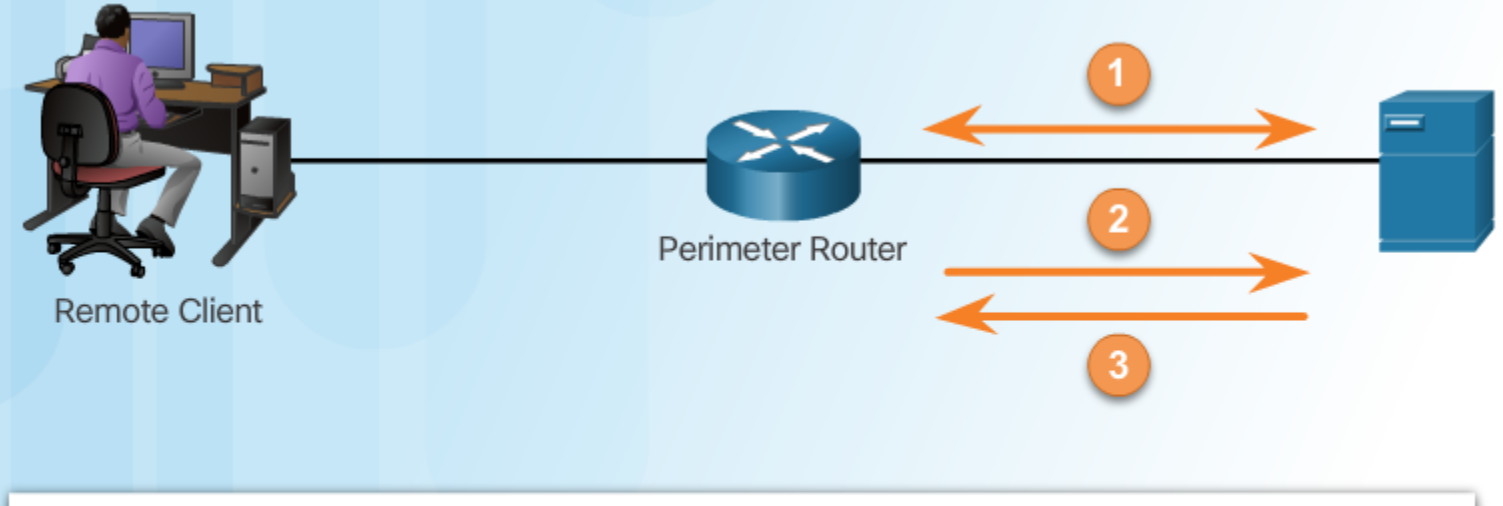


Uwierzytelnianie AAA z serwerem



Autoryzacja

Autoryzacja AAA



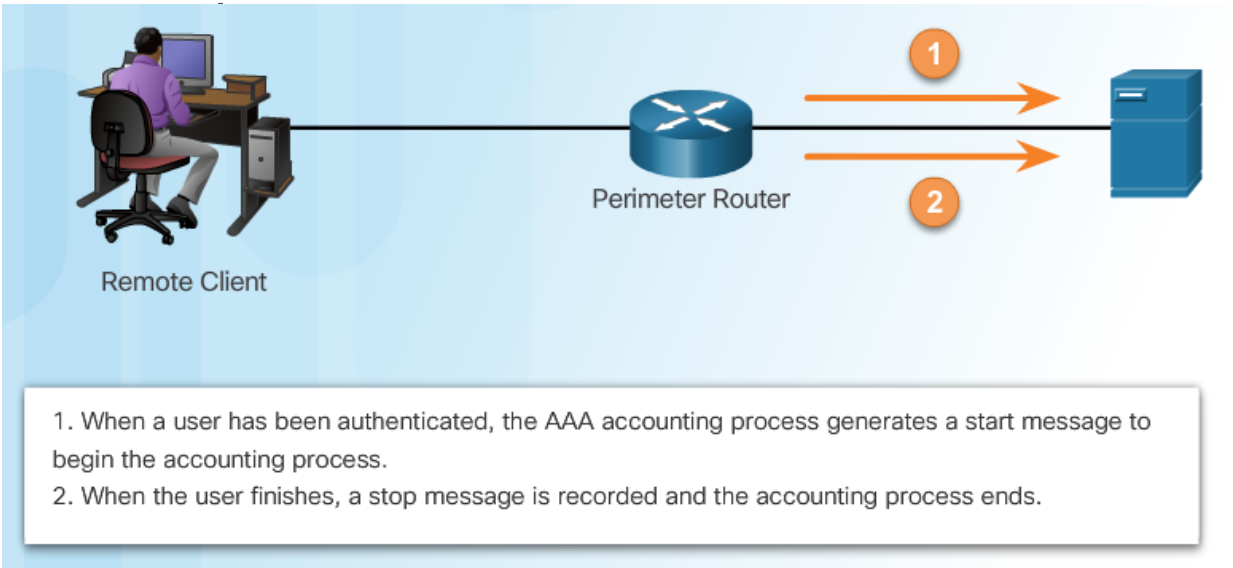
1. When a user has been authenticated, a session is established with the AAA server.
2. The router requests authorization for the requested service from the AAA server.
3. The AAA server returns a PASS/FAIL for authorization.

Konto użytkownika/śledzenie

Rodzaje informacji przesyłane podczas pracy z urządzeniem:

- Sieć
- Połączenie
- EXEC
- System
- Polecenie
- Zasoby

Proces nazwiązywania połączenia



Rozdział 6.2: Lokalne uwierzytelnainie AAA

Po zakończeniu tej części, powinieneś być w stanie:

- Konfigurować uwierzytelnianie AAA, wykorzystując wiersz poleceń weryfikować użytkowników na podstawie lokalnej bazy.
- Rozwiązywać problemy z autoryzacją AAA użytkowników w lokalnej bazie danych.

Temat 6.2.1:
Konfiguracja lokalnego uwierzytelniania AAA przez CLI

Uwierzytelnianie dostępu administracyjnego

1. Dodaj nazwy użytkowników i hasła w lokalnej bazie danych dla użytkowników, którzy wymagają dostępu administracyjnego do routera.
2. Włącz AAA globalnie na routerze.
3. Skonfiguruj parametry AAA na routerze.
4. Potwierdź rozwiąż ewentualne problemy z konfiguracją 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)#
```

Metody uwierzytelniania

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.

```
router(config-line)#
aas 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.

Domyślne metody z nazwami

Przykład lokalnego uwierzytelniania 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
```

Dostosowywanie konfiguracji uwierzytelniania

Składnia polecenia

```
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.

Wyświetlanie zablokowanych użytkowników

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

Wyświetlania identyfikatora sesji

```
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
```

Temat 6.2.2:
Rozwiązywanie problemów z lokalnym uwierzytelnianiem AAA

Opcje debug

Debug lokalnego uwierzytelniania AAA

```
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
```

Debug uwierzytelniania AAA

Wynik Debug

```
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
```

Rozdział 6.3: AAA z serwerem

Po zakończeniu tej części, powinieneś być w stanie:

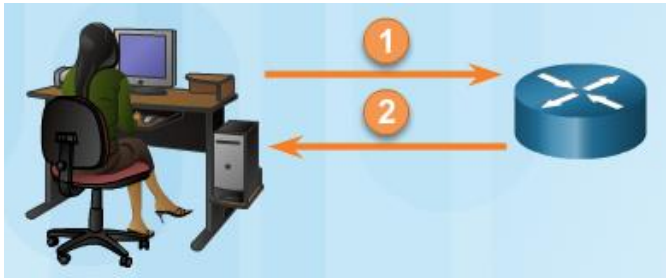
- Opisać zalety stosowania AAA z serwerem.
- Porównać protokoły uwierzytelniania TACACS+ i RADIUS.

Temat 6.3.1:
Charakterystyka AAA z serwerem

Porównanie implementacji lokalnego AAA i AAA z serwerem

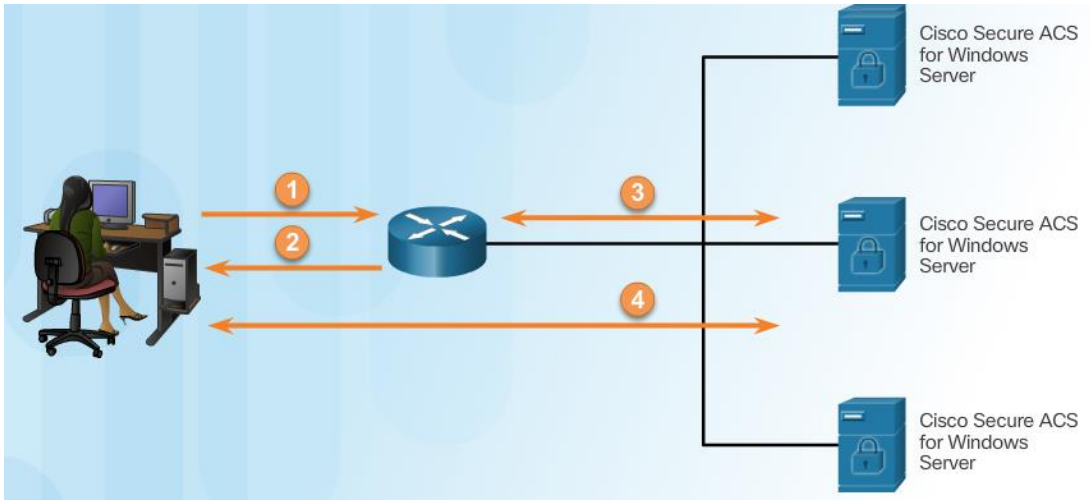
Lokalne uwierzytelnianie:

1. Użytkownik ustanawia połączenie z routerem.
2. Router prosi o podanie nazwy użytkownika i hasła, uwierzytelnia użytkownika wykorzystując lokalną bazę.

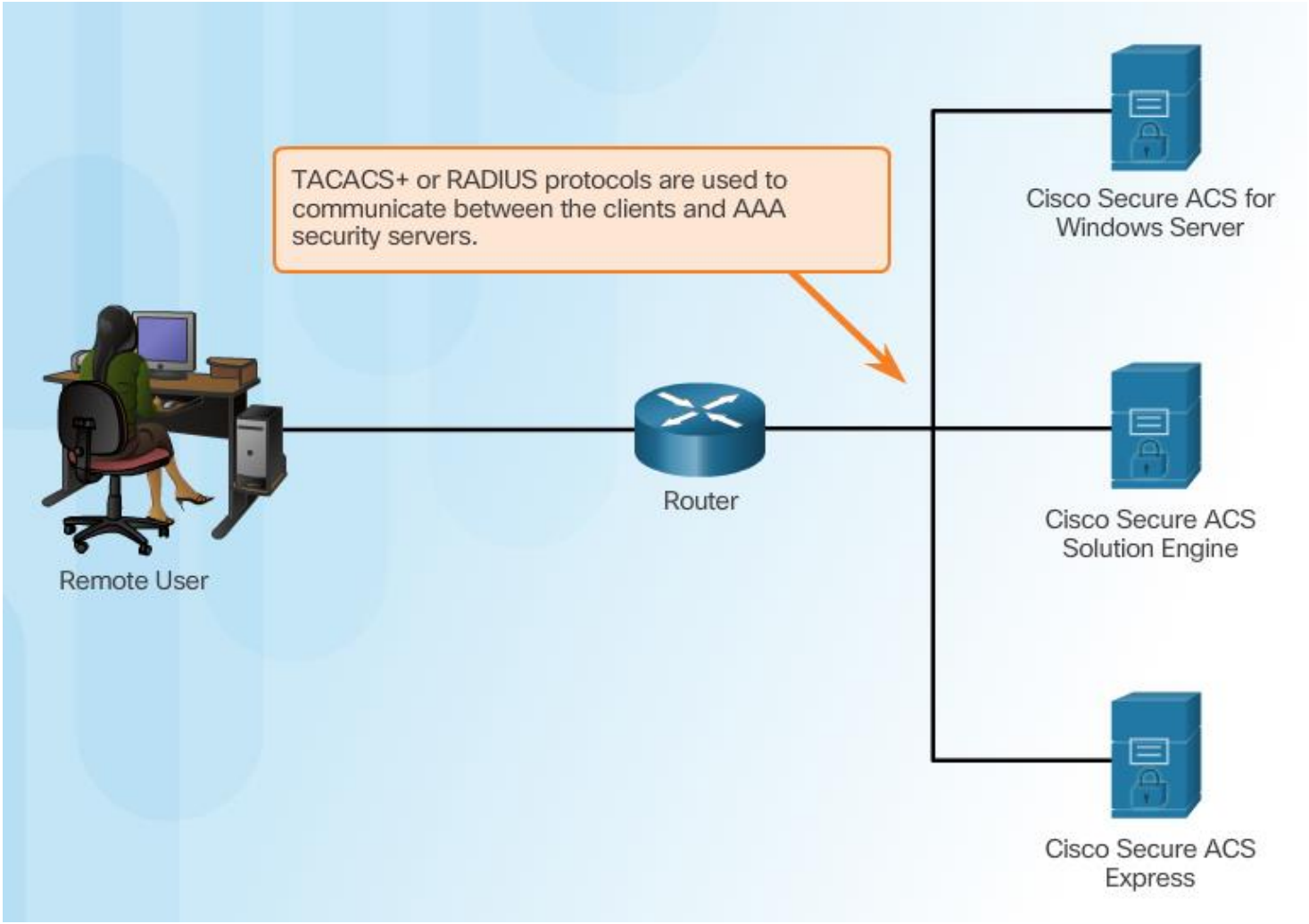


Uwierzytelnianie z serwerem:

1. Użytkownik ustanawia połączenie z routerem.
2. Router prosi o podanie nazwy użytkownika i hasła.
3. Router przesyła dalej nazwę użytkownika i hasło do Cisco Secure ACS (serwer)
4. Cisco Secure ACS uwierzytelnia użytkownika.



System sterowania bezpieczym dostępem Cisco



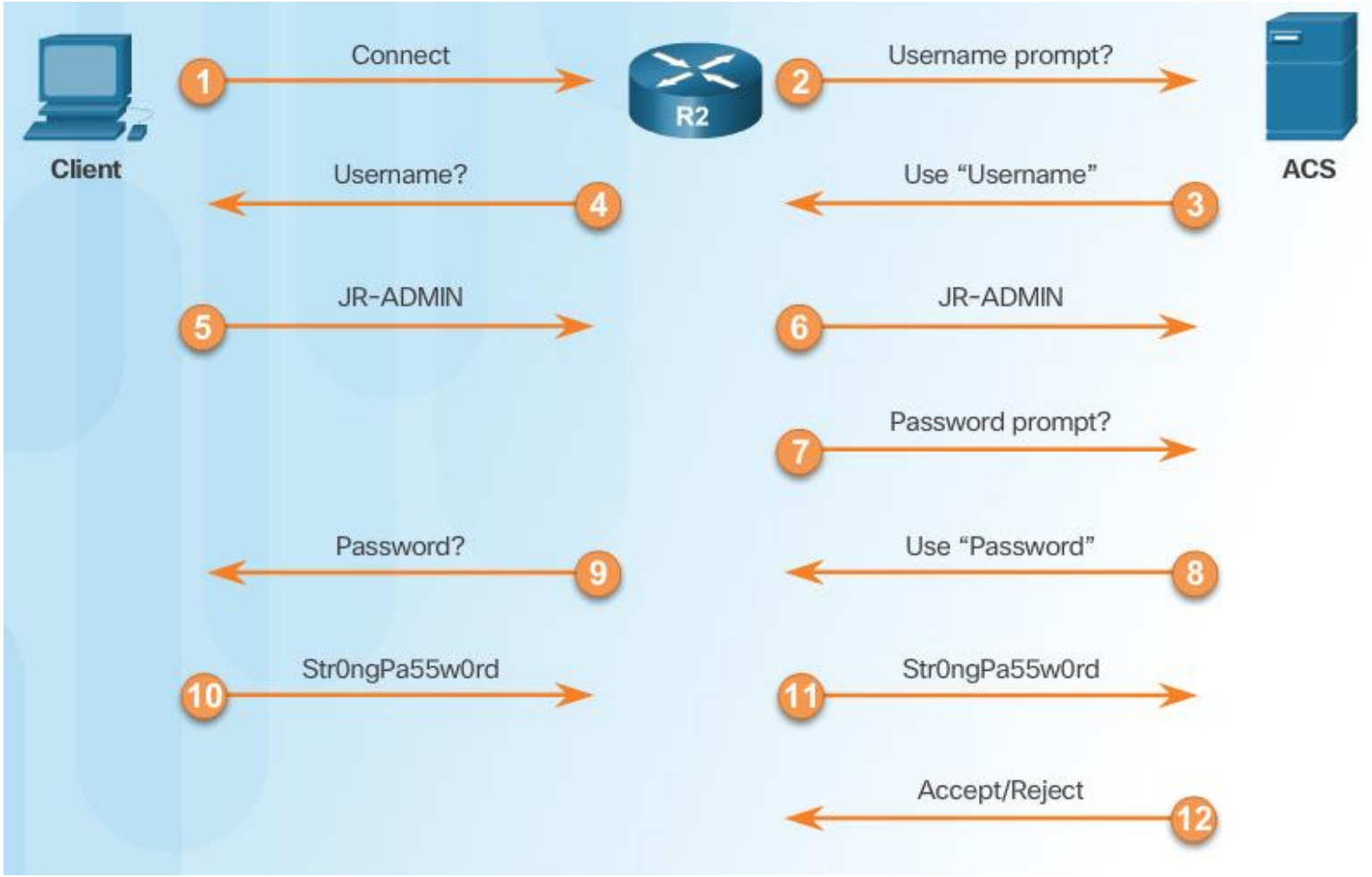
Temat 6.3.2:
Protokoły komunikacyjne w AAA z serwerem

TACACS+ i 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

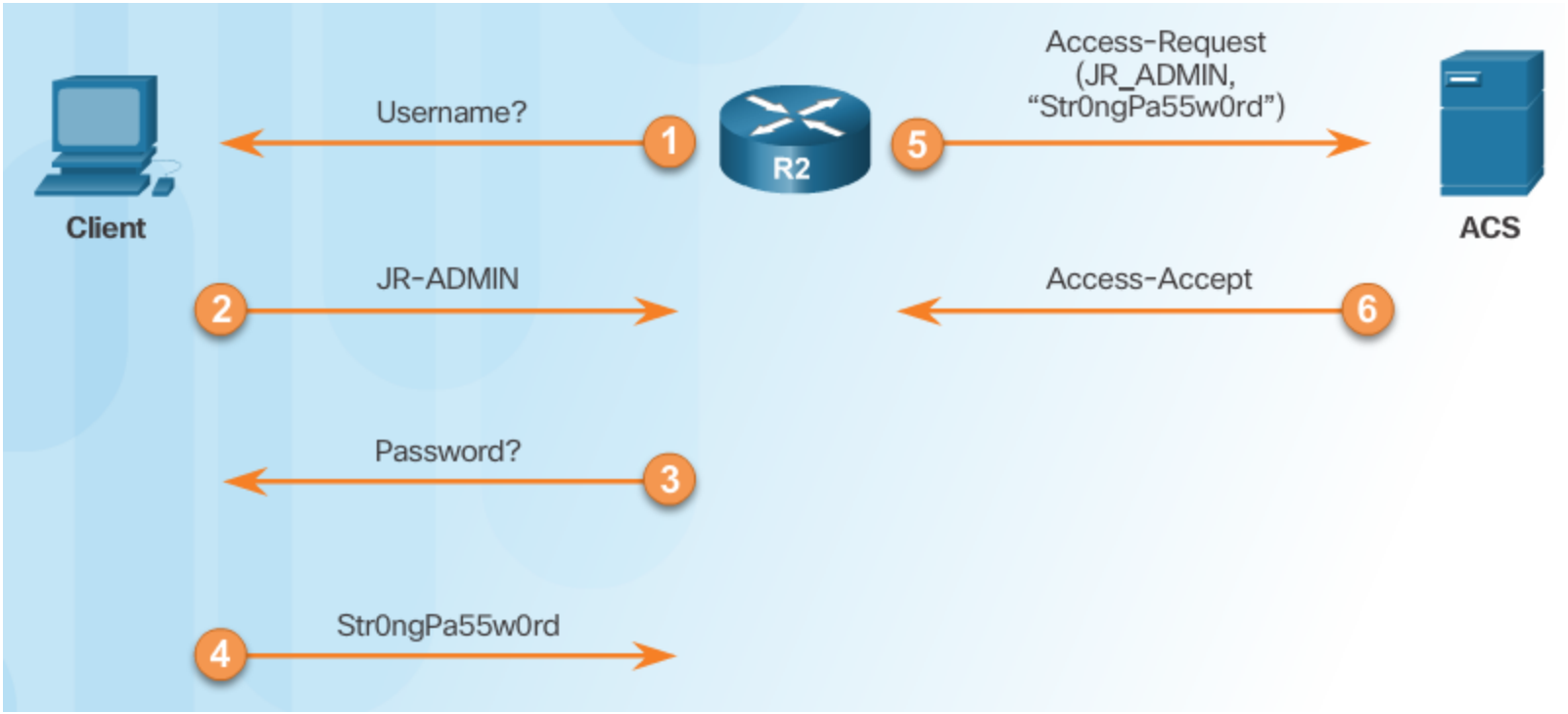
Uwierzytelnianie TACACS+

Proces uwierzytelniania TACACS+



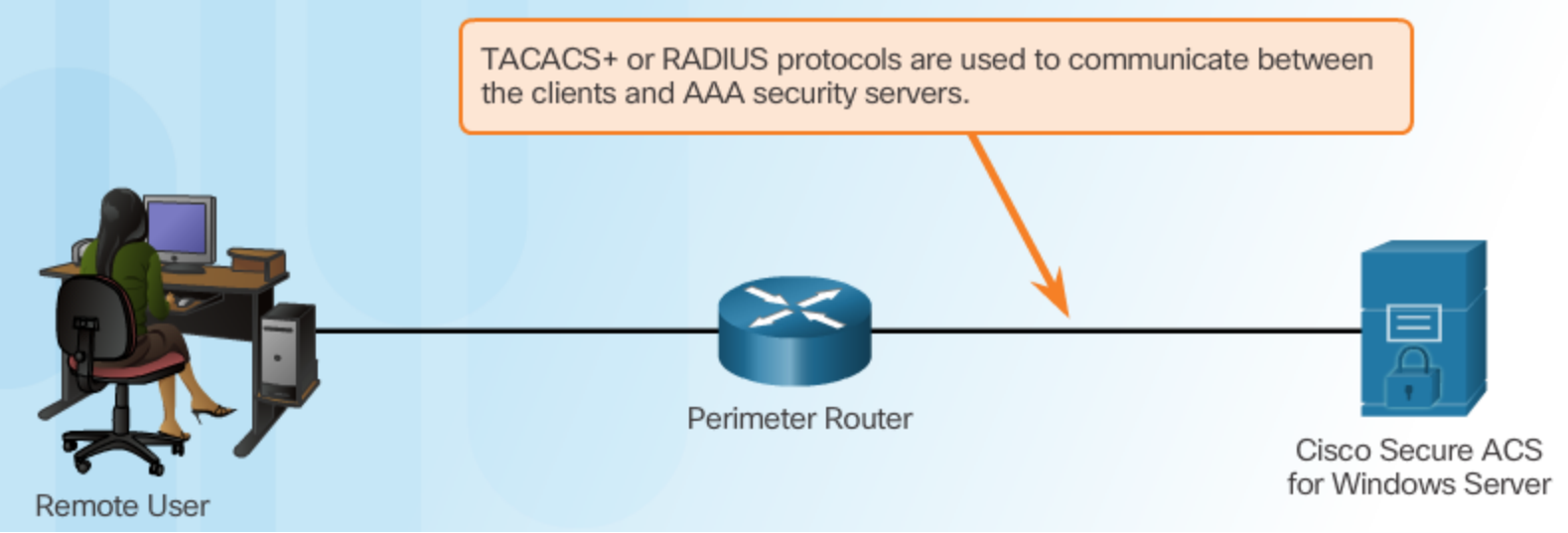
Uwierzytelnianie RADIUS

Proces uwierzytelniania RADIUS

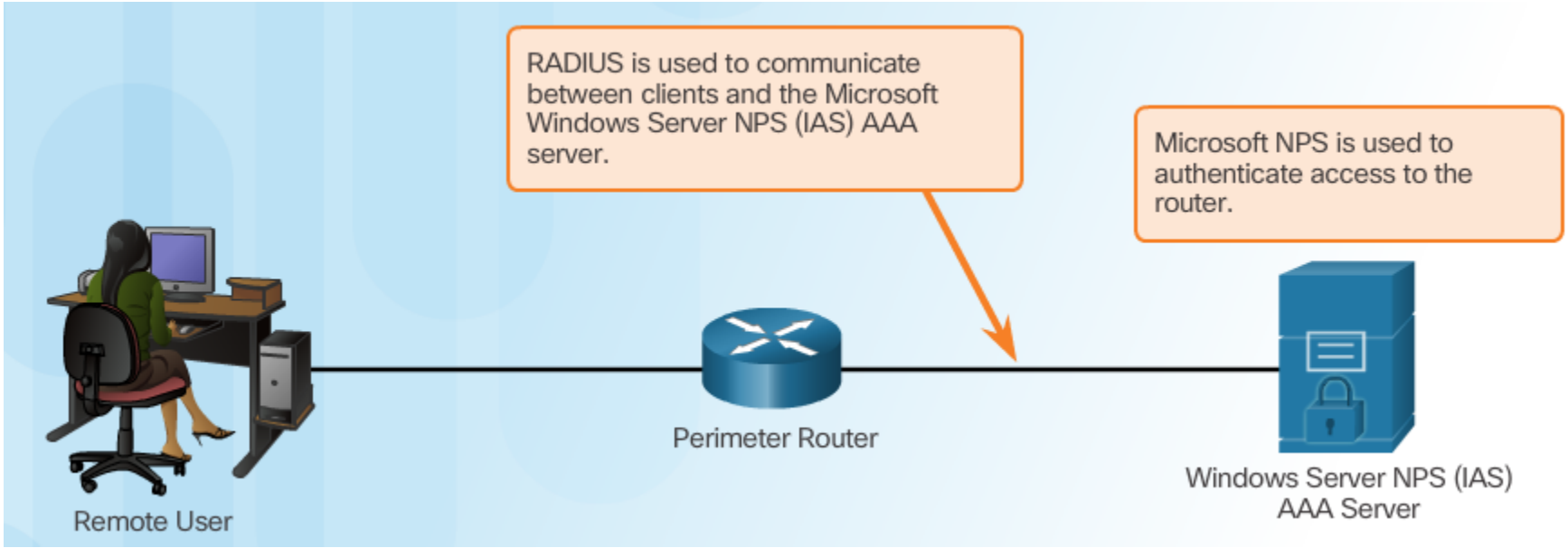


Integracja TACACS+ i ACS

Cisco Secure ACS



Intergracja AAA zvActive Directory



Rozdział 6.4: Uwierzytelnianie AAA z serwerem

Po zakończeniu tej części, powinieneś być w stanie:

- Konfigurować uwierzytelnianie AAA z serwerem, wykorzystując do tego wiersz poleceń CLI.
- Rozwiązywać problemy związane z uwierzytelnianem AAA na serwerze.

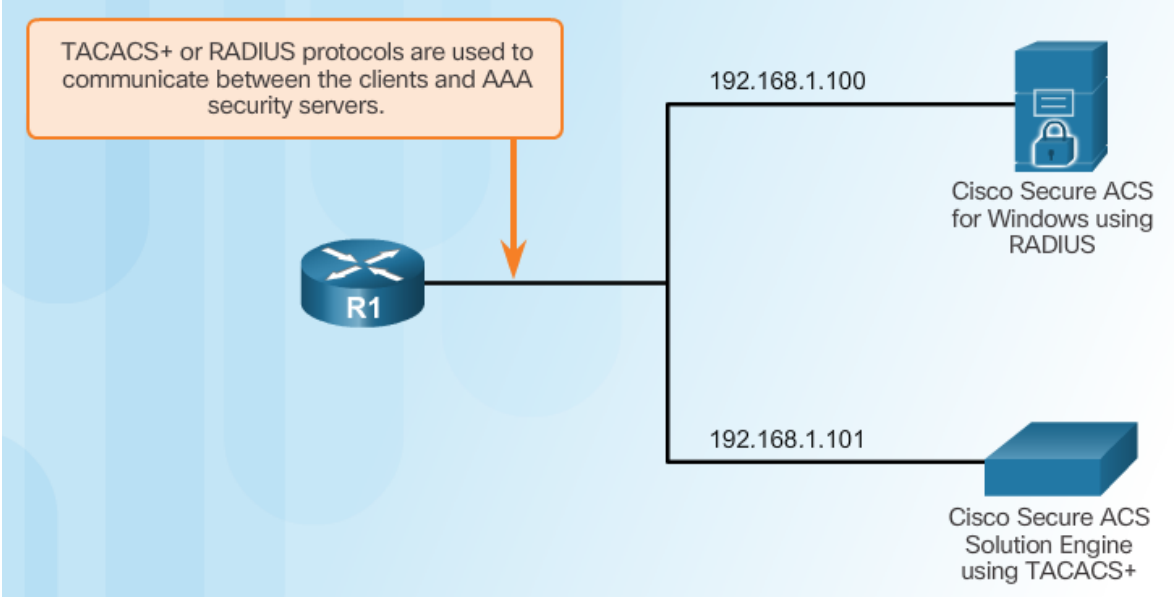
Temat 6.4.1:
Konfiguracja uwierzytelniania z serwerem poprzez CLI

Kroki konfiguracji uwierzytelniania AAA z serwerem poprzez CLI

1. Uruchom AAA.
2. Określ adres IP serwera ACS.
3. Skonfiguruj klucz bezpieczeństwa.
4. Skonfiguruj uwierzytelnianie, w taki sposób, aby korzystało z serwera RADIUS lub TACACS+.

Konfiguracja CLI z serwerami TACACS+

Topologia odniesienia AAA z serwerem



Konfiguracja serwera AAA TACACS+

```
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)#
```

Konfiguracja CLI dla serwerów RADIUS

Konfiguracja serwera AAA RADIUS

```
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)#
```

Konfiguracja uwierzytelniania do używania serwera AAA

Składnia polecenia

```
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.
```

Konfiguracja uwierzytelniania AAA z serwerem

```
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
```

Temat 6.4.2:
Rozwiązywanie problemów z uwierzytelnianiem AAA z serwerem

Monitorowanie ruchu związanego z uwierzytelnianiem

Rozwiązywanie problemów z uwierzytelnainien AAA z serwerem

```
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
```

Debug protokołów TACACS+ i RADIUS

Rozwiązywanie problemów z 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>
```

Rozwiązywanie problemów z TACACS+

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

Debug protokołów TACACS+ i RADIUS

Uwierzytelnianie AAA z serwerem zakończone sukcesem

```
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
```

Uwierzytelnianie AAA z serwerem zakończone niepowodzeniem

```
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
```

Rozdział 6.5: Autoryzacja AAA z serwerem

Po zakończeniu tej części, powinieneś być w stanie:

- Konfigurować autoryzację AAA z serwerem.
- Konfigurować proces tworzenia kont AAA z serwerem.
- Wyjaśnić funkcje składników 802.1x.

Temat 6.5.1:
Konfiguracja autoryzacji AAA z serwerem

Autoryzacja AAA z serwerem

Uwierzytelnianie vs. autoryzacja

- **Uwierzytelnianie** sprawdza, czy urządzenie lub użytkownik końcowy istnieje
- **Autoryzacja** zezwala lub zabrania uwierzytelnionym użytkownikom na dostęp do określonych obszarów i probramów w sieci.

TACACS+ vs. RADIUS

- **TACACS+** oddziela uwierzytelnianie od autoryzacji
- **RADIUS nie** oddziela uwierzytelniania od autoryzacji

Konfiguracja autoryzacji AAA poprzez CLI

Składnia polecenia

```
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.
```

Lista metod autoryzacji

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

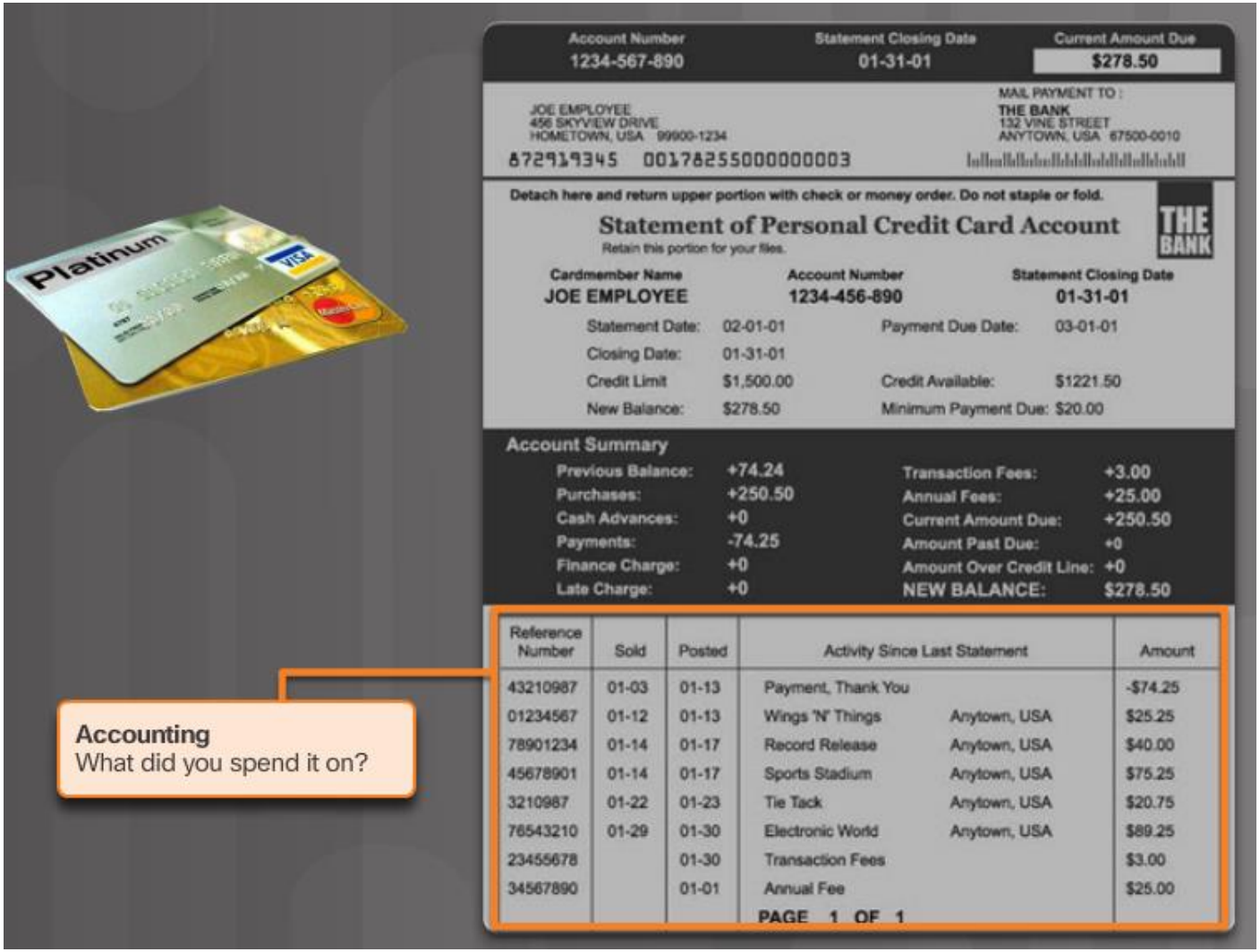
```
R1(config)# aaa authorization exec default ?
  cache             Use Cached-group
  group             Use server-group.
  if-authenticated  Succeed if user has authenticated.
  krb5-instance     Use Kerberos instance privilege maps.
  local             Use local database.
  none              No authorization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

Przykład autoryzacji 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+
```

Temat 6.5.2:
Konfiguracja obsługi połączeń w ramach AAA

Konfiguracja obsługi połaczeń AAA



Konfiguracja obsługi połączeń AAA poprzez CLI

Składnia polecenia

```
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.
```

Lista metod

```
R1(config)#
aaa accounting {network | exec | connection} {default | list-name}
{start-stop | stop-only | none } [broadcast] method1...[method4]
```

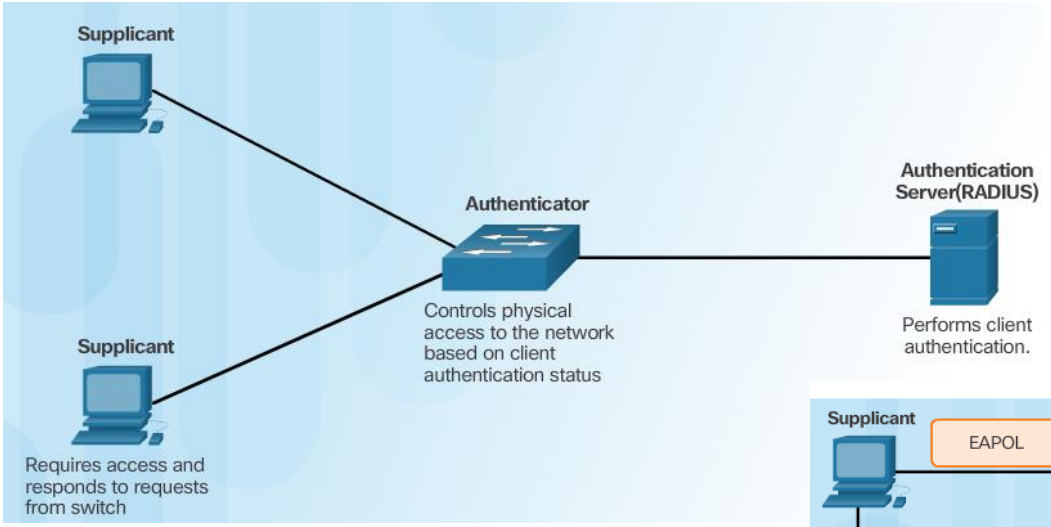
```
R1(config)# aaa accounting exec default start-stop?
  broadcast Use Broadcast for Accounting
  group     Use Server-group

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.
```

Przykład

```
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+
```

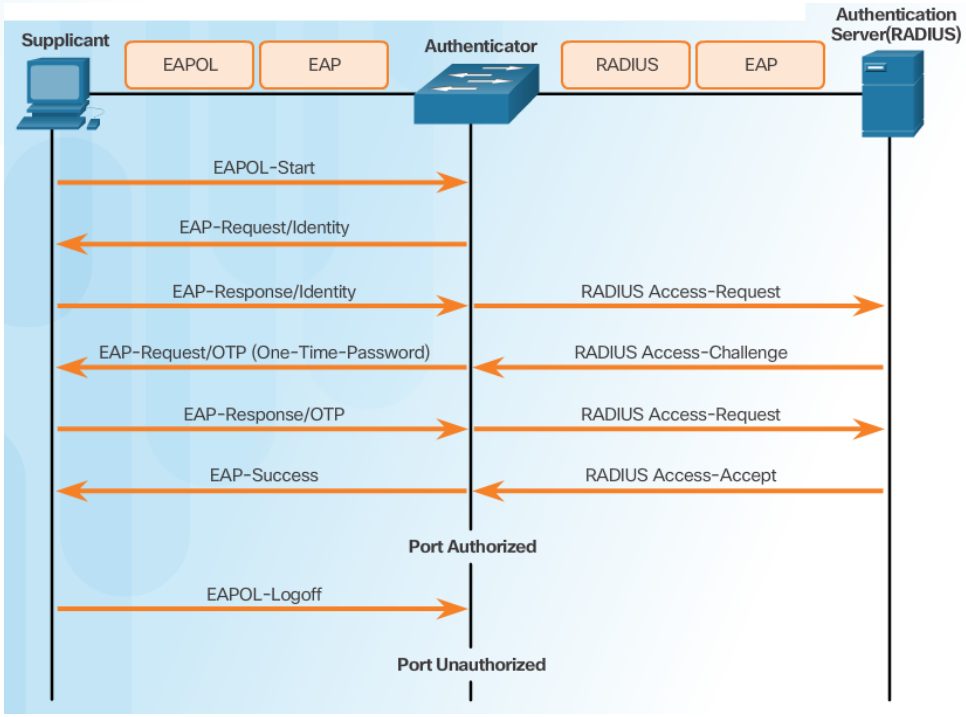
Temat 6.5.3: Uwierzytelnianie 802.1X

802.1X – uwierzytelnianie na podstawie portów



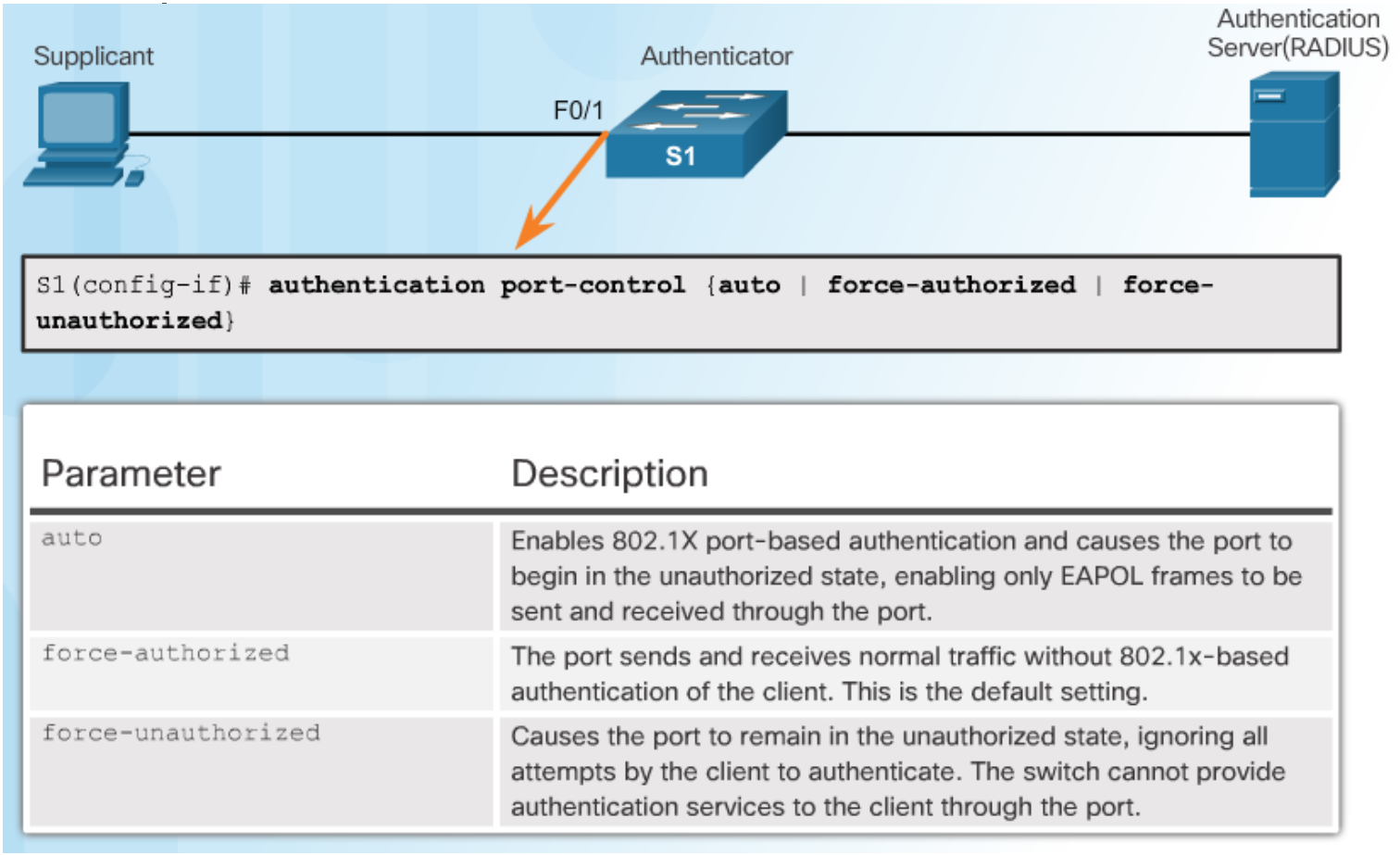
Role 802.1X

Wymiana wiadomości 802.1X



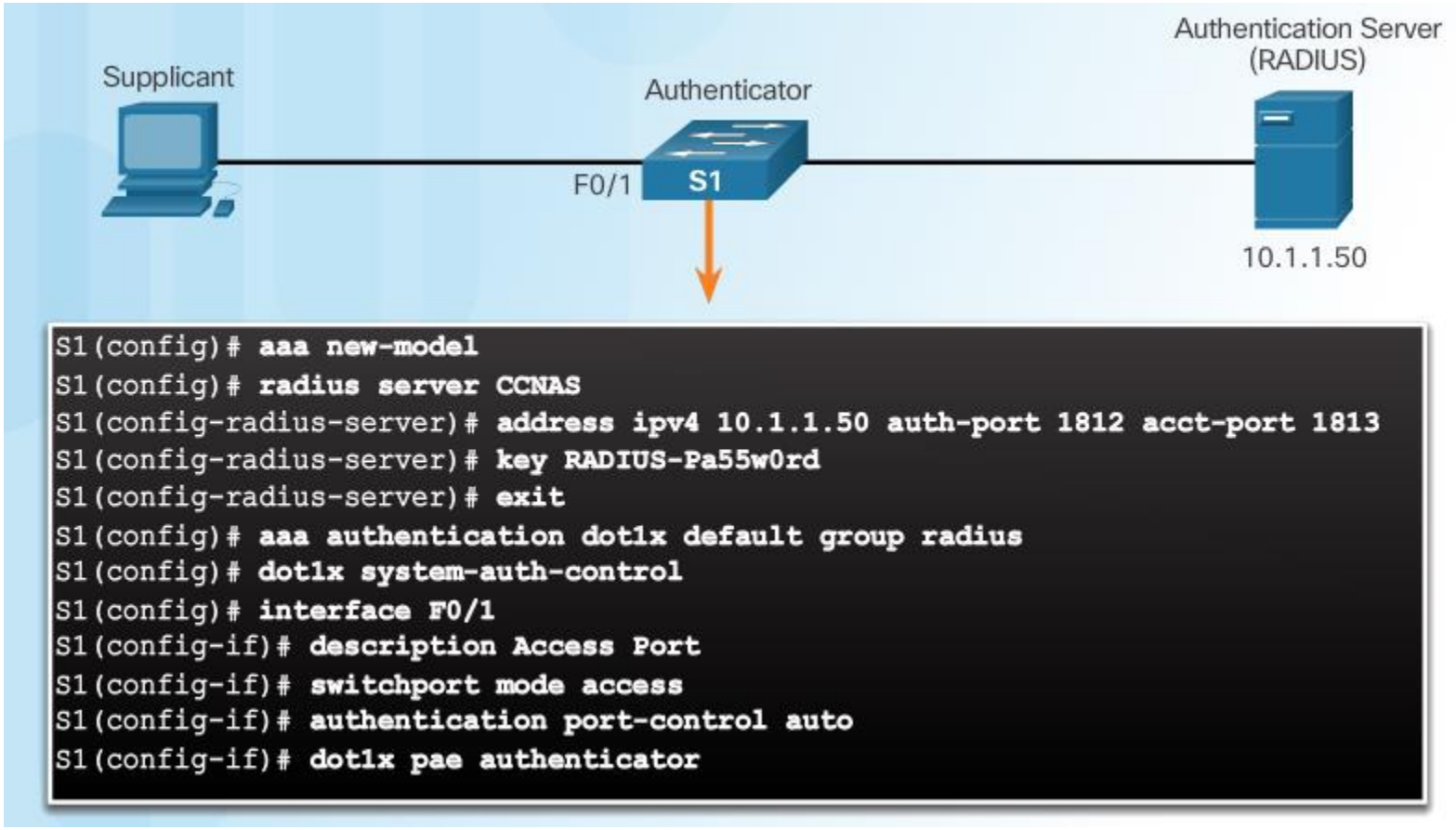
Stan uwierzytelniania portu 802.1X

Składnia polecenia dla dot1x port-



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.

Konfiguracja 802.1X



Rozdział 6.6: Monitorowanie i zarządzanie urządeniami

Po zakończeniu tej części, powinieneś być w stanie:

- Używać konfiguracji Cisco IOS, aby zapewnićbezpieczeństwo obrazom Cisco IOS i plikom konfiguracyjnym.
- Porównać dostęp w paśmie i poza pasmem.
- Skonfigurować serwer syslog do przechwytywania zdarzeń systemowych.
- Skonfigurować bezpieczny dostęp SNMPv3 za pomocą ACL
- Skonfigurować NTP, aby umożliwić dokładną synchronizację pomiędzy wszystkimi urządzeniami.

Temat 6.6.1:
Zabezpieczanie systemu Cisco IOS Image i plików konfiguracyjnych

Elastyczna konfiguracja Cisco IOS

Cisco IOS Resilient Configuration Facts

- The configuration file in the primary bootset is a copy of the running configuration that was in the router when the feature was first enabled.
- The feature secures the smallest working set of files to preserve persistent storage space. No extra space is required to secure the primary Cisco IOS image file.
- The feature automatically detects image or configuration version mismatch.
- Only local storage is used for securing files, eliminating scalability maintenance challenges from storing multiple images and configurations on TFTP servers.
- The feature can be disabled only through a console session.
- The feature is only available for systems that support a PCMCIA Advanced Technology Attachment (ATA) flash interface.

Uruchamianie elastycznej konfiguracji

```
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#
```

Uruchamianie podstawowego obrazu systemu

```
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#
```

Konfigurowanie bezpiecznej kopii

Konfiguracja routera jako serwer SCP z lokalnym AAA:

1. Konfiguracja SSH
2. Konfiguracja przynajmniej jednego użytkownika z poziomem uprawnień 15
3. Włączenie AAA
4. Określenie, że lokalna baza zostanie użyta do uwierzytelnienia
5. Uruchom serwer SCP

Odzyskiwanie hasła routera

1. Podłącz port konsoli.
2. Zapisz ustawnie rejestru konfiguracji.
3. Uruchom ponownie router.
4. Zastosuj sekwencję przerywania bootowania.
5. Zmień domyślną wartość rejestru konfiguracji przy użyciu polecenia **confreg 0x2142**.
6. Uruchom ponownie router.
7. Wciśnij Ctrl-C żeby pominąć wstępną procedurę konfiguracji.
8. Wejdź w trym **privileged EXEC mode**.
9. Skopiuj konfigurację startową do bieżącej.
10. Zweryfikuj konfigurację.
11. Zmień hasło **enable secret**.
12. Włącz wszystkie interfejsy.
13. Zmień wartość rejestru **config-register configuration_register_setting**.
14. Zapisz konfigurację.

Odzyskiwanie hasła

```
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)#
```

Wyłączanie procedury odzyskiwania hasła

Procedura wyłączona

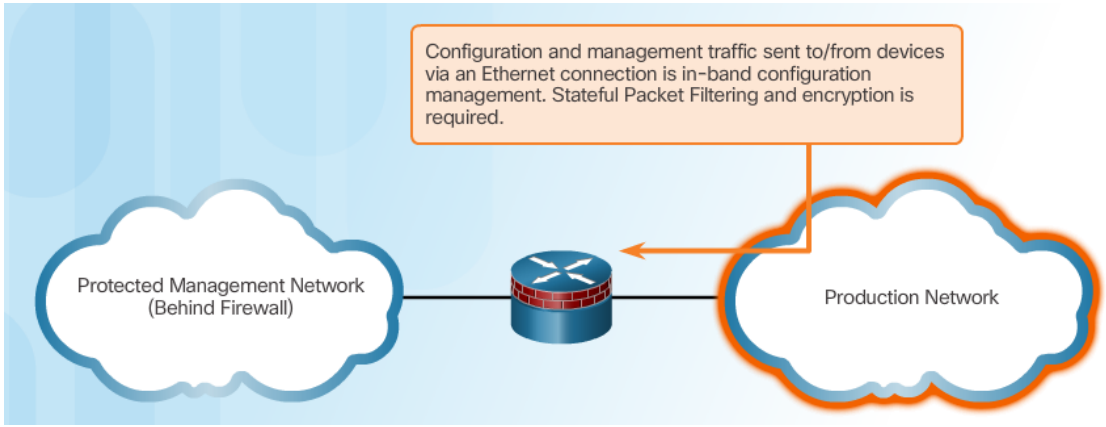
```
R1# show running-config
Building configuration...

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 (fc1)
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
```

Procedura wyłączona

Teamt 6.6.2:
Zabezpieczenie zarządzania i raportowania

Określanie typu dostępu zarządzania

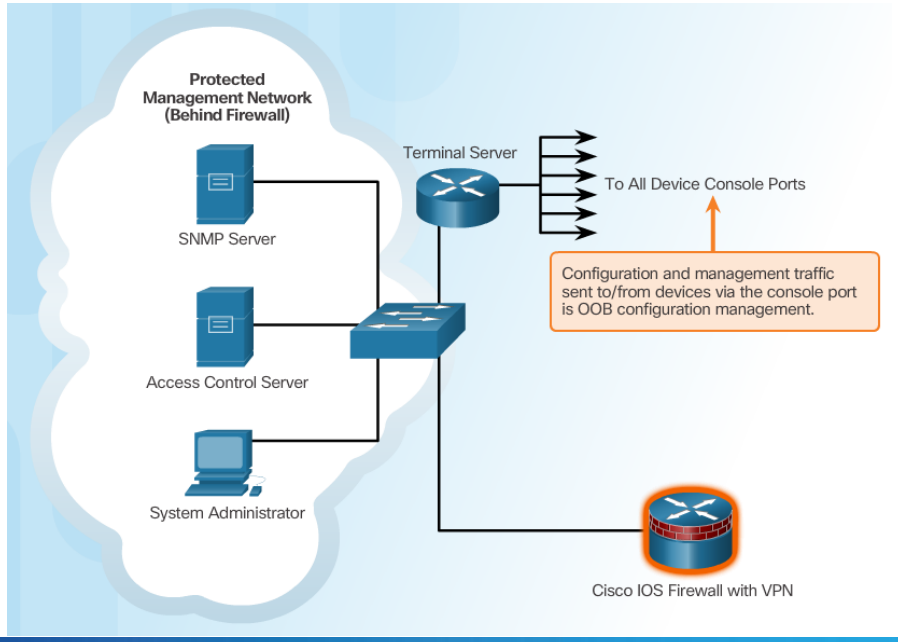


W paśmie:

- Tylko dla urządzeń, które mają być monitorowanie i zarządzane
- Użycie IPsec, SSH, lub SSL jeśli możliwe
- Określenie kiedy kanał zarządzana będzie aktywny

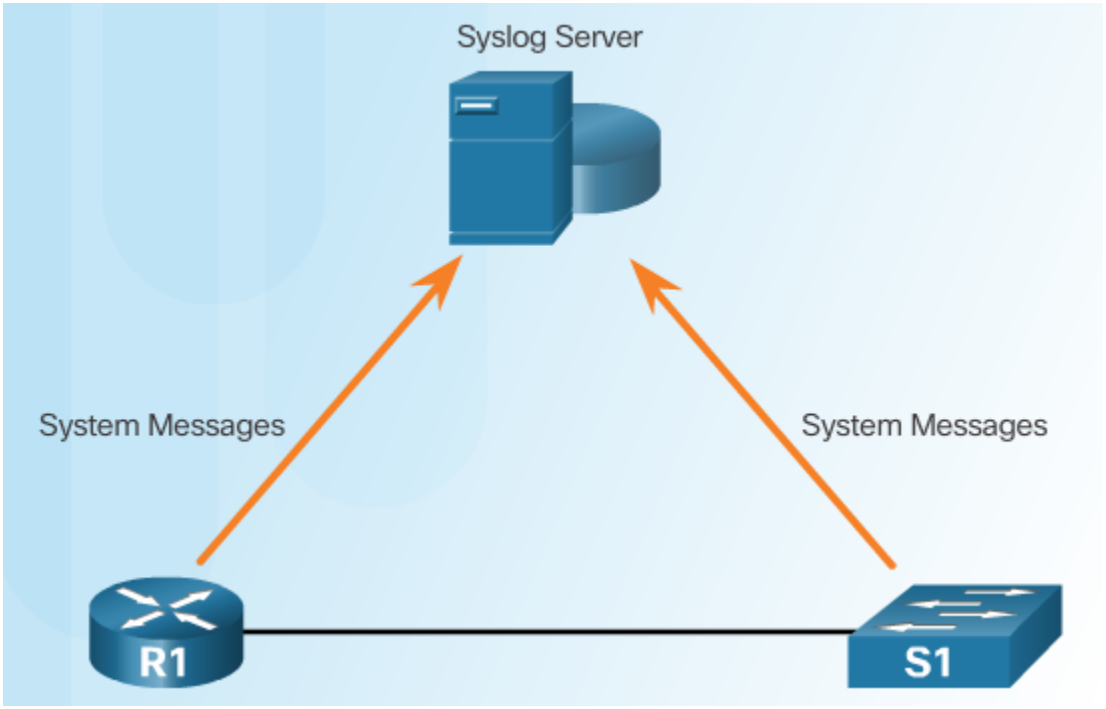
Poza pasmem:

- Zapewnia większy poziom zabezpieczeń
- Minimalizuje ryzyko dostępu do protokołów zarządzania przez sieć produkcyjną



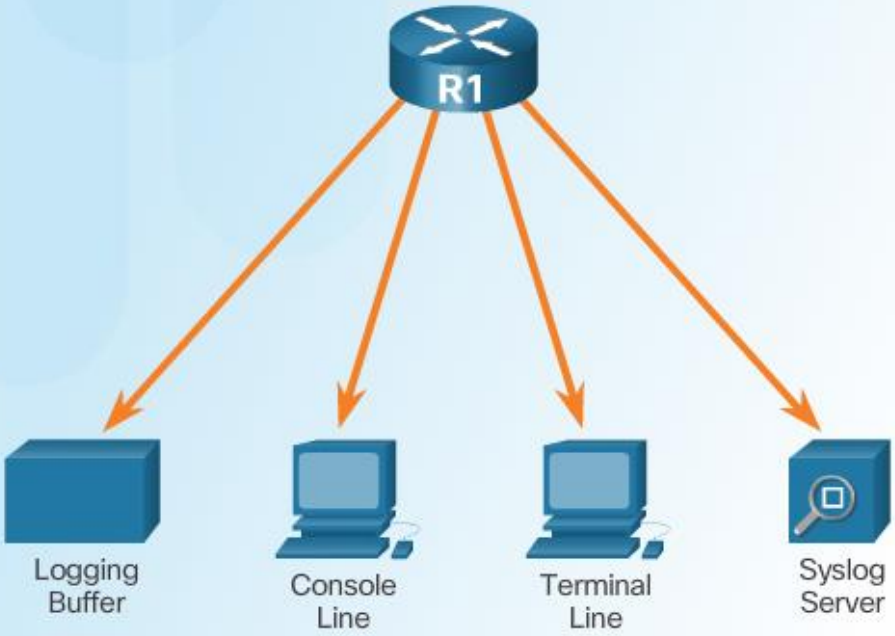
Temat 6.6.3:
Użycie serwera Syslog

Wprowadzenie do Syslog



Operacje Syslog

```
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
```



Wiadomości Syslog

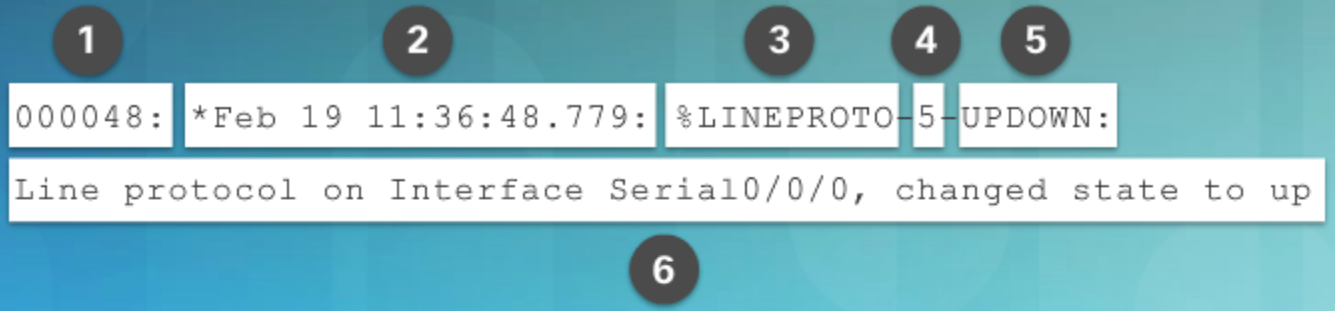
Security Levels

	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

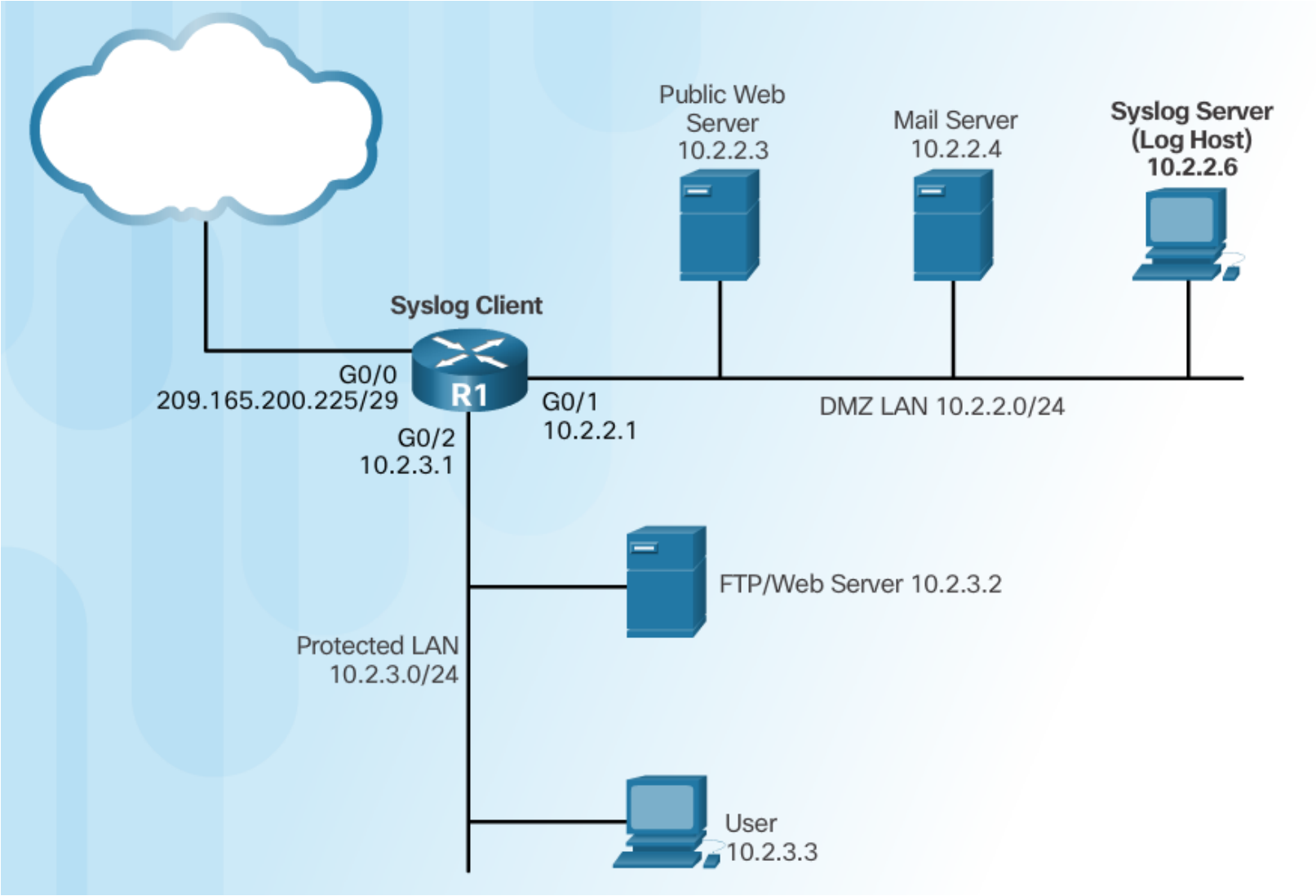
Syslog Level and Name	Definition	Example
0 LOG_EMERG	A panic condition normally broadcast to all users	Cisco IOS software could not load
1 LOG_ALERT	A condition that should be corrected immediately, such as a corrupted system database	Temperature too high
2 LOG_CRIT	Critical conditions; for example, 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

Wiadomości Syslog



	Column 1	Column 2
1	seq no	Stamps log messages with a sequence number if `service sequence-numbers` is configured.
2	timestamp	displays if `service timestamps` log 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

Systemy Syslog



Konfiguracja systemów logowania

Step 1

```
Router(config)#
logging host [hostname | ip-address]
```

Step 2 (optional)

```
Router(config)#
logging trap level
```

Step 3

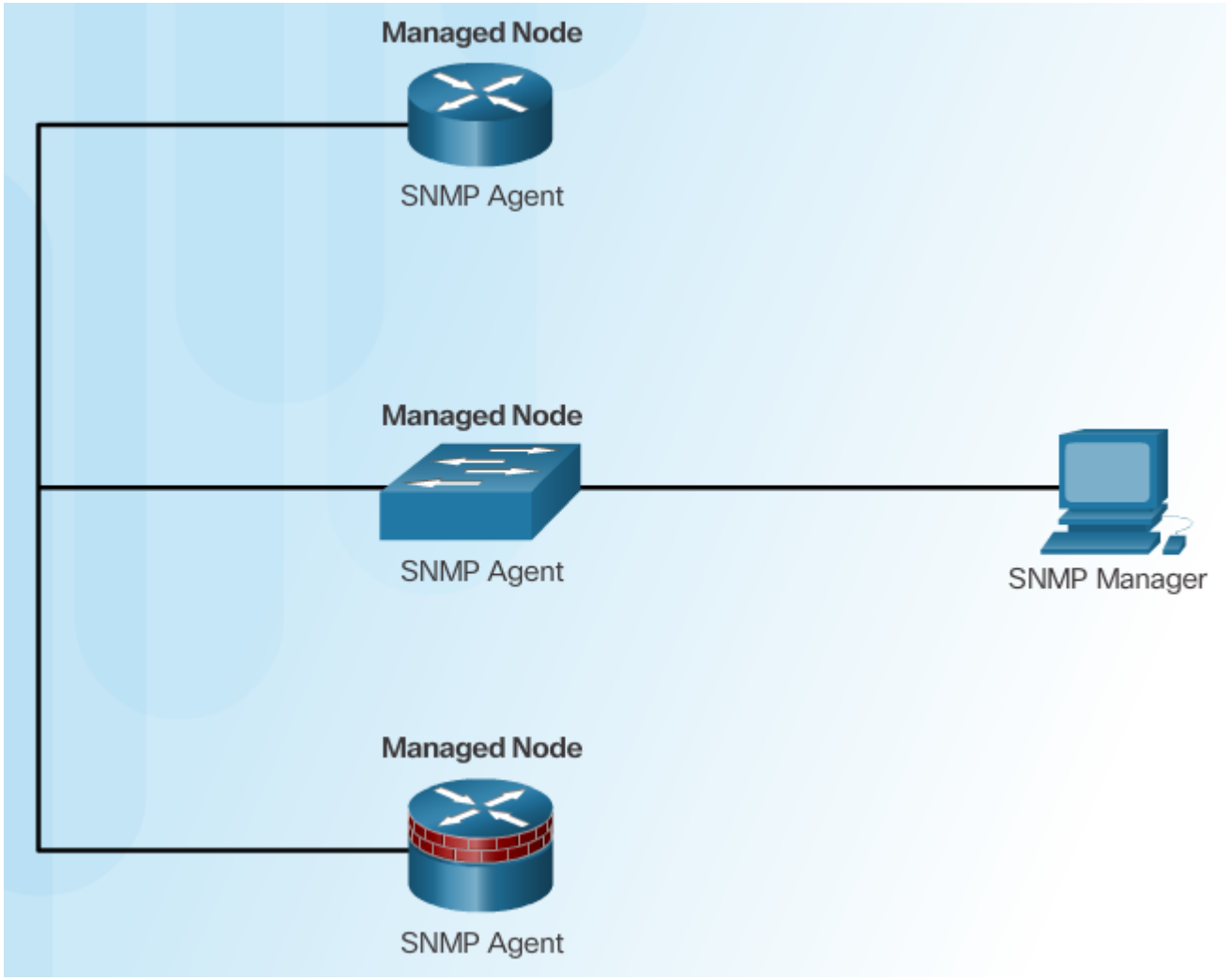
```
Router(config)#
logging source-interface interface-type interface-number
```

Step 4

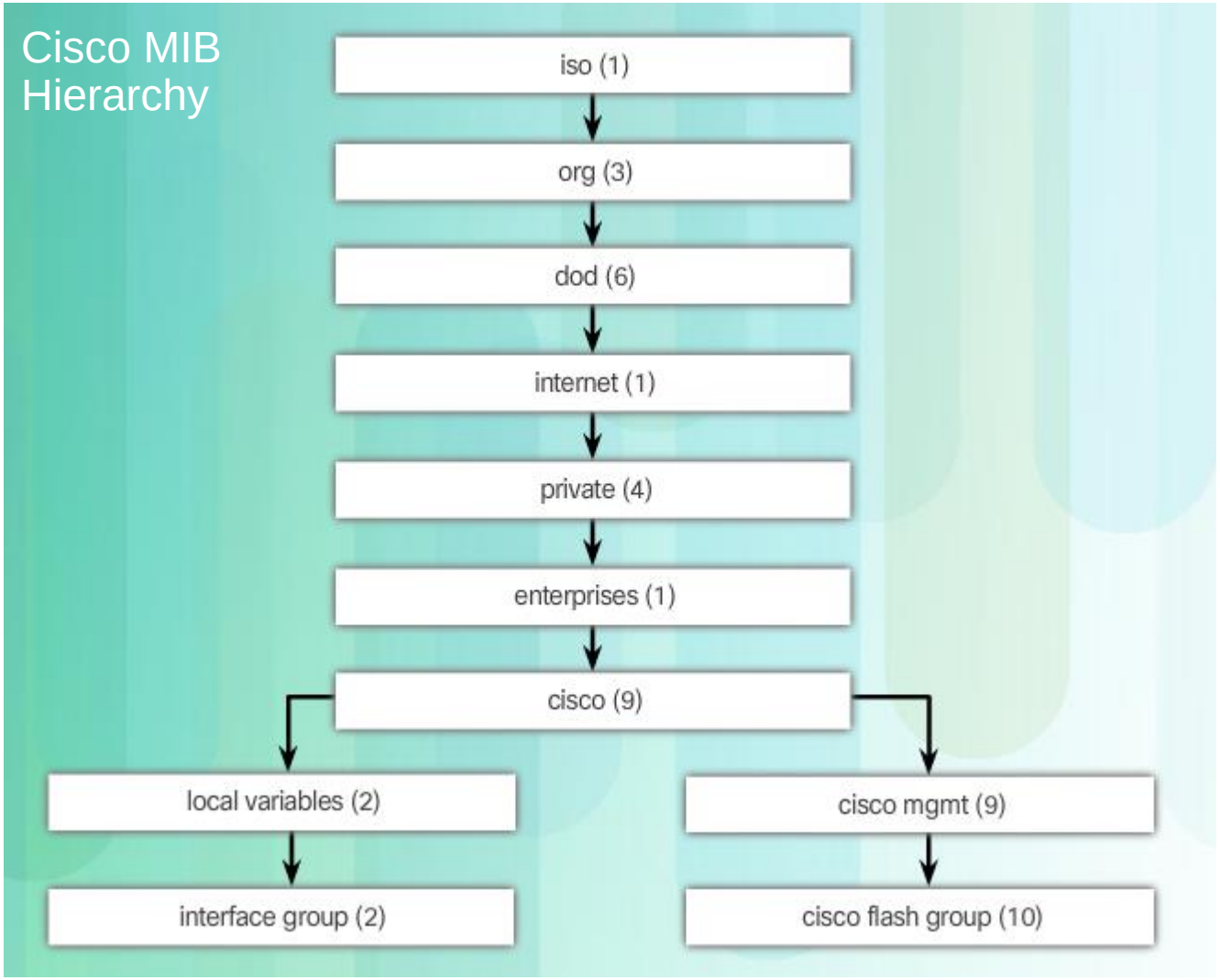
```
Router(config)#
logging on
```

Temat 6.6.4:
Użycie SNMP

Wprowadzenie do SNMP



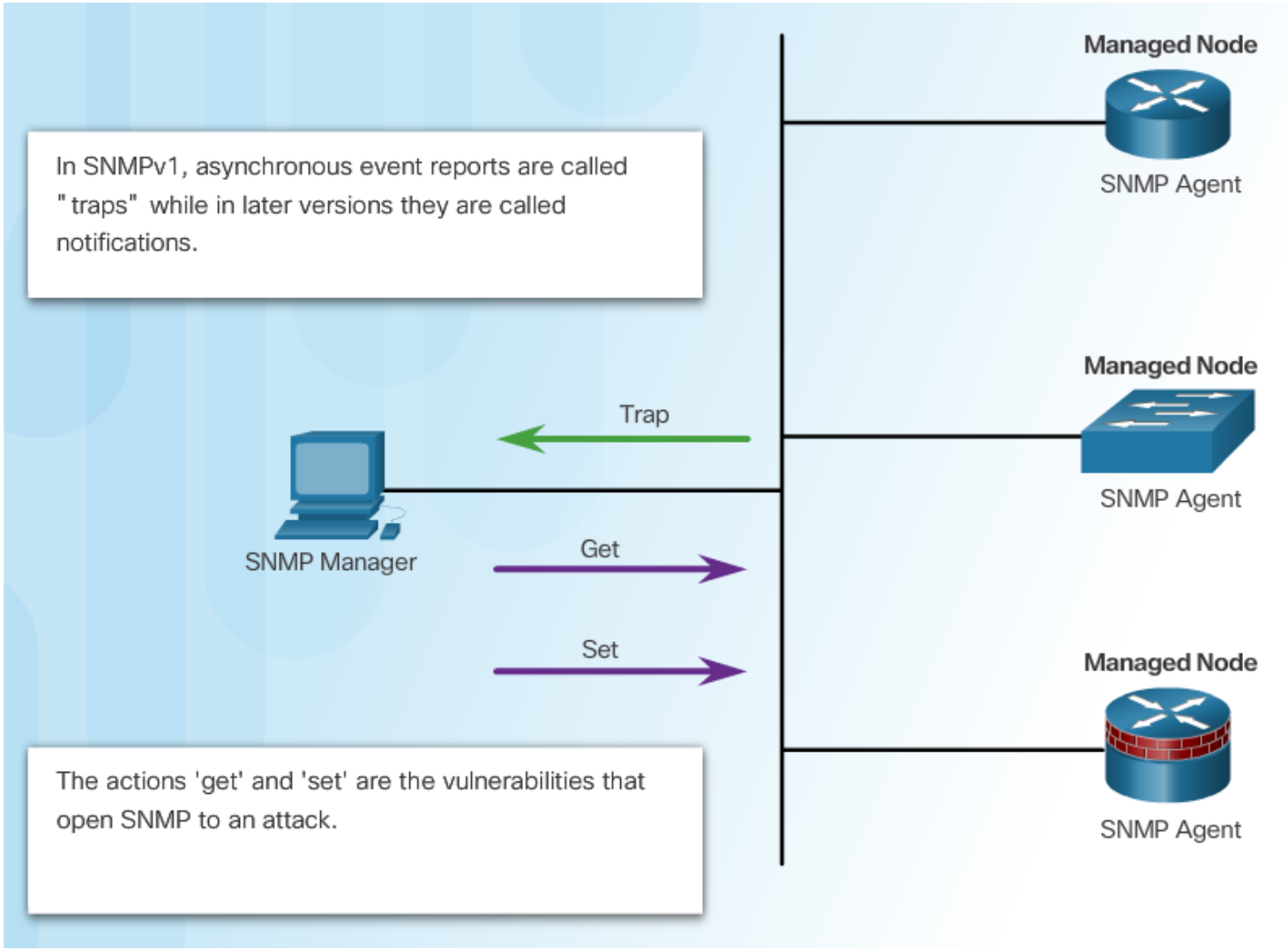
Baza MIB (Management Information Base)



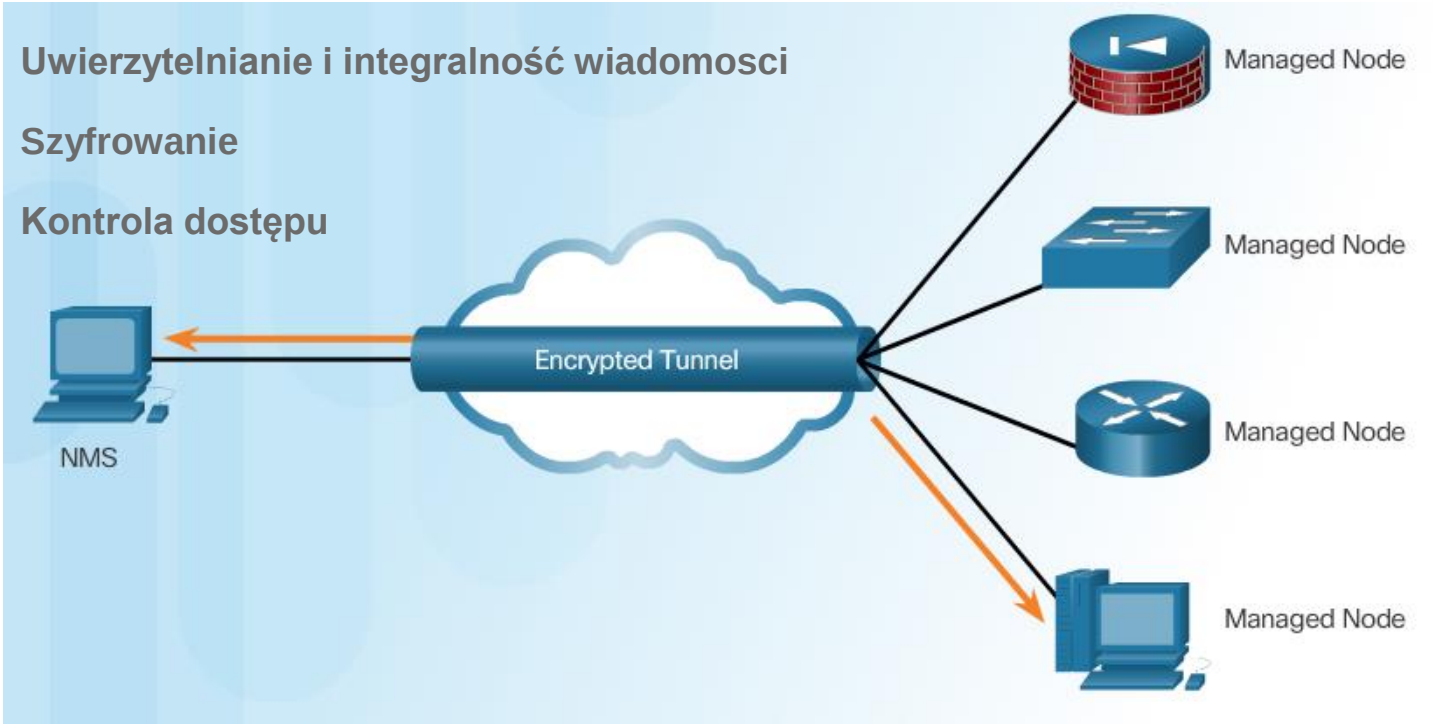
Wersje SNMP

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: • DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. • 3DES 168-bit encryption • AES 128-bit, 192-bit, or 256-bit encryption

Słabości SNMP



SNMPv3



- Transmisje z menedżera do agenta może być uwierzytelniona w celu zagwarantowania tożsamości nadawcy oraz wiarygodności i terminowości wiadomości.
- Komunikaty SNMPv3 mogą być szyfrowane w celu zapewnienia prywatności.
- Agent może wymusić kontrolę dostępu do ograniczenia każdego zleceniodawcy pewnych działań dotyczących poszczególnych danych.

Konfiguracja zabezpieczeń SNMPv3

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.

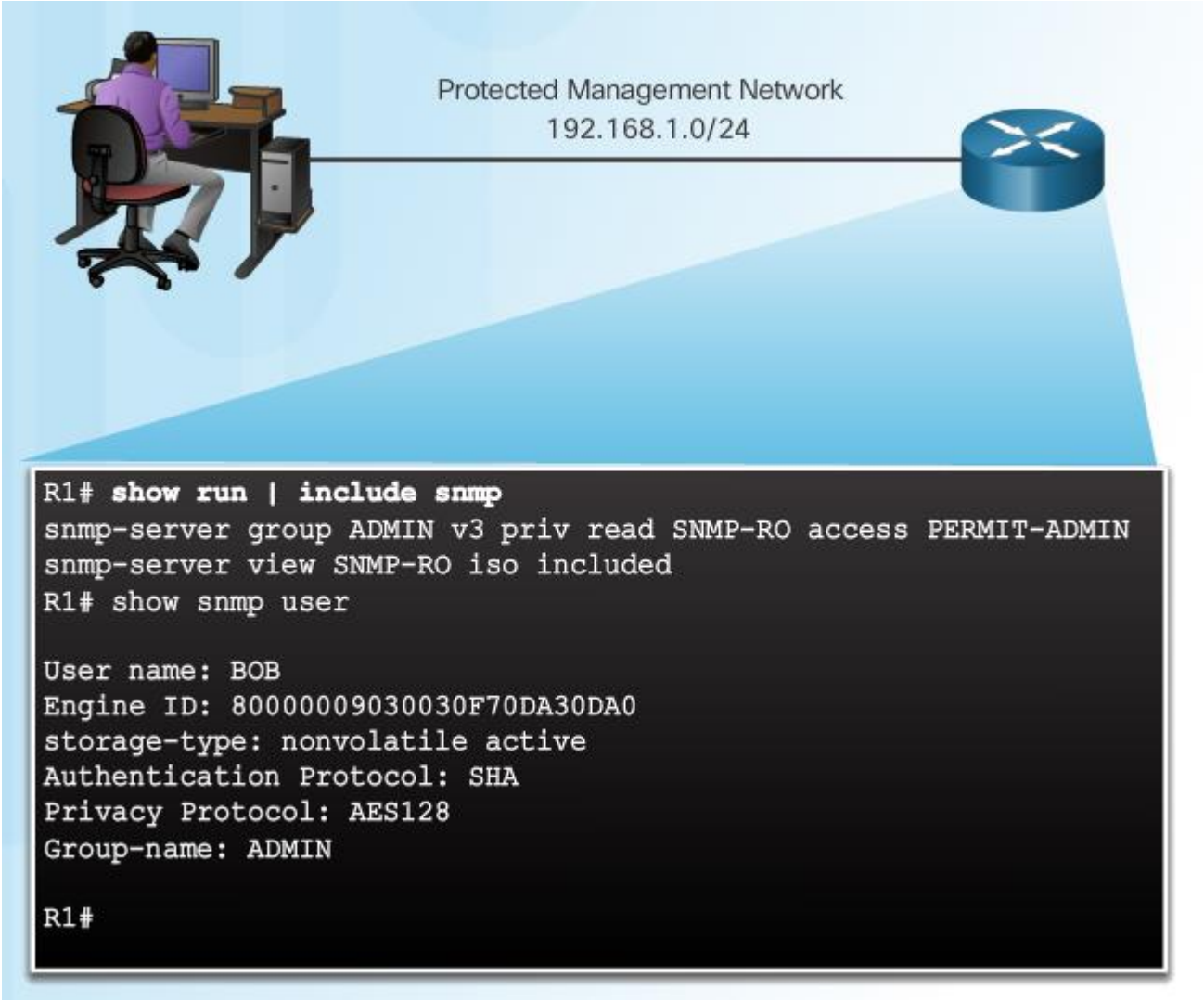
```
Router(config)# snmp-server user username group-name v3
auth {md5 | sha} auth-password priv {des | 3des | aes
{128 | 192 | 256}} privpassword
```

Przykład zabezpieczania SNMPv3

Protected Management Network
192.168.1.0/24

```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)# snmp-server view SNMP-RO iso included
R1(config)# snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
R1(config)# snmp-server user BOB ADMIN v3 auth sha cisco12345 priv aes 128 cisco54321
R1(config)# end
R1#
```

Weryfikacja konfiguracji SNMPv3



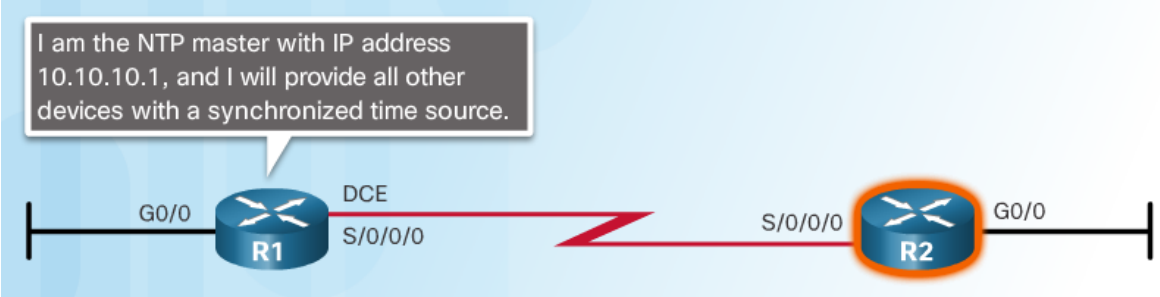
Temat 6.6.5: Użycie NTP

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#
```

Serwer NTP

Topologia NTP



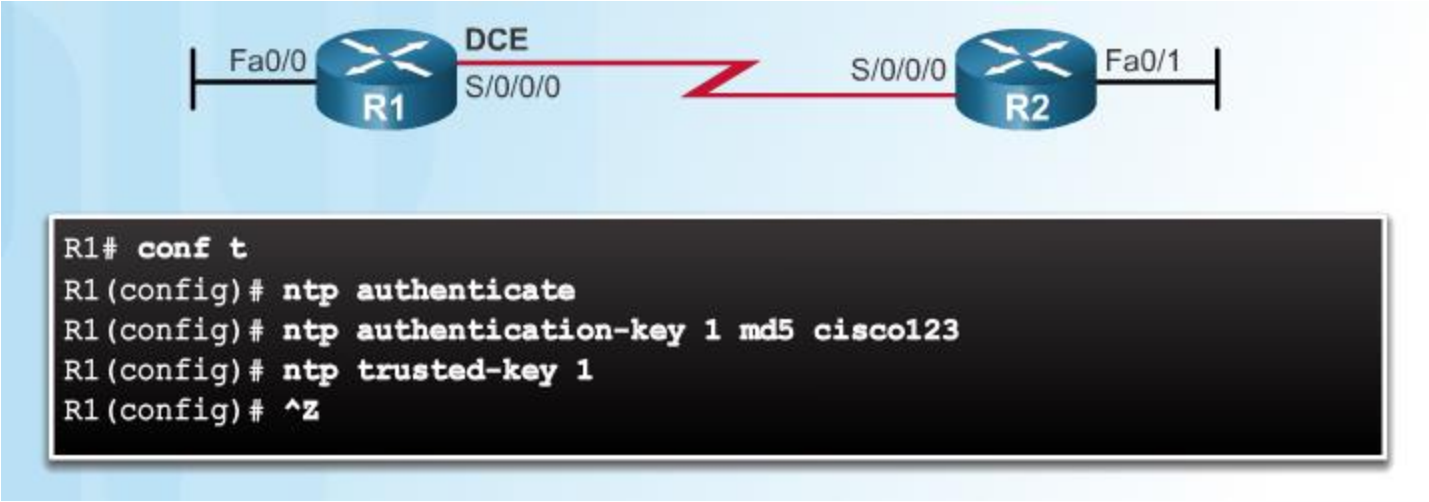
Konfiguracja NTP na R1

```
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#
```

Konfiguracja NTP na 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#
```

Uwierzytelnianie NTP



Rozdział 6.7: Podsumowanie

Zagadnienia:

- Wyjaśnienie jak AAA jest używany w celu zabezpieczenia sieci.
- Implementacja uwierzytelnania AAA w celu weryfikacji użytkowników lokalnej bazie.
- Implementacja uwierzytelniania AAA z serwerem z wykorzystaniem protokołów TACACS+ i RADIUS.
- Konfiguracja autoryzacji AAA.


cisco