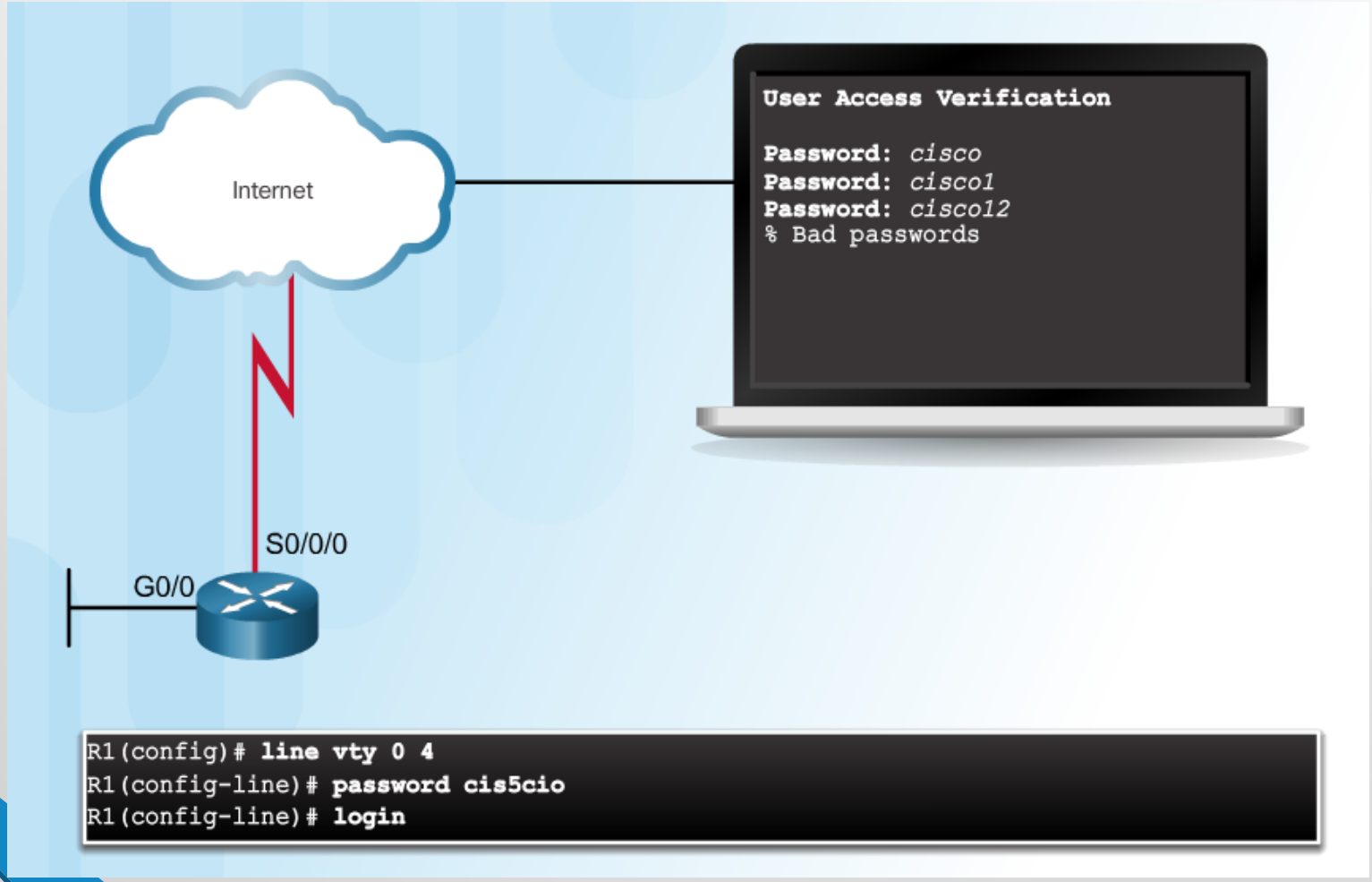
Лекция 4
Аутентификация, авторизация и учет

Тема Обзор AAA

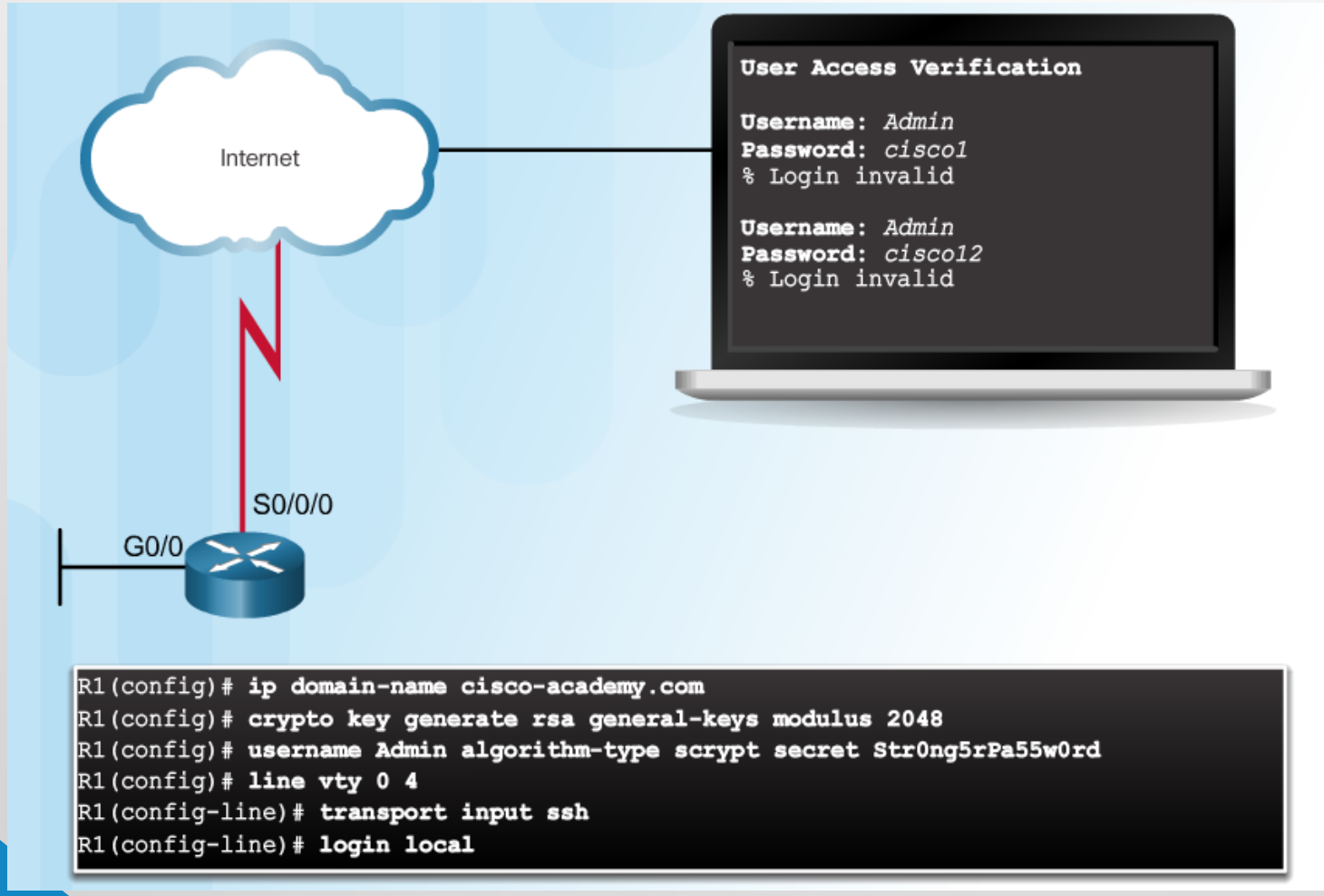
Аутентификация без AAA

Telnet уязвим перед атаками подбора паролей

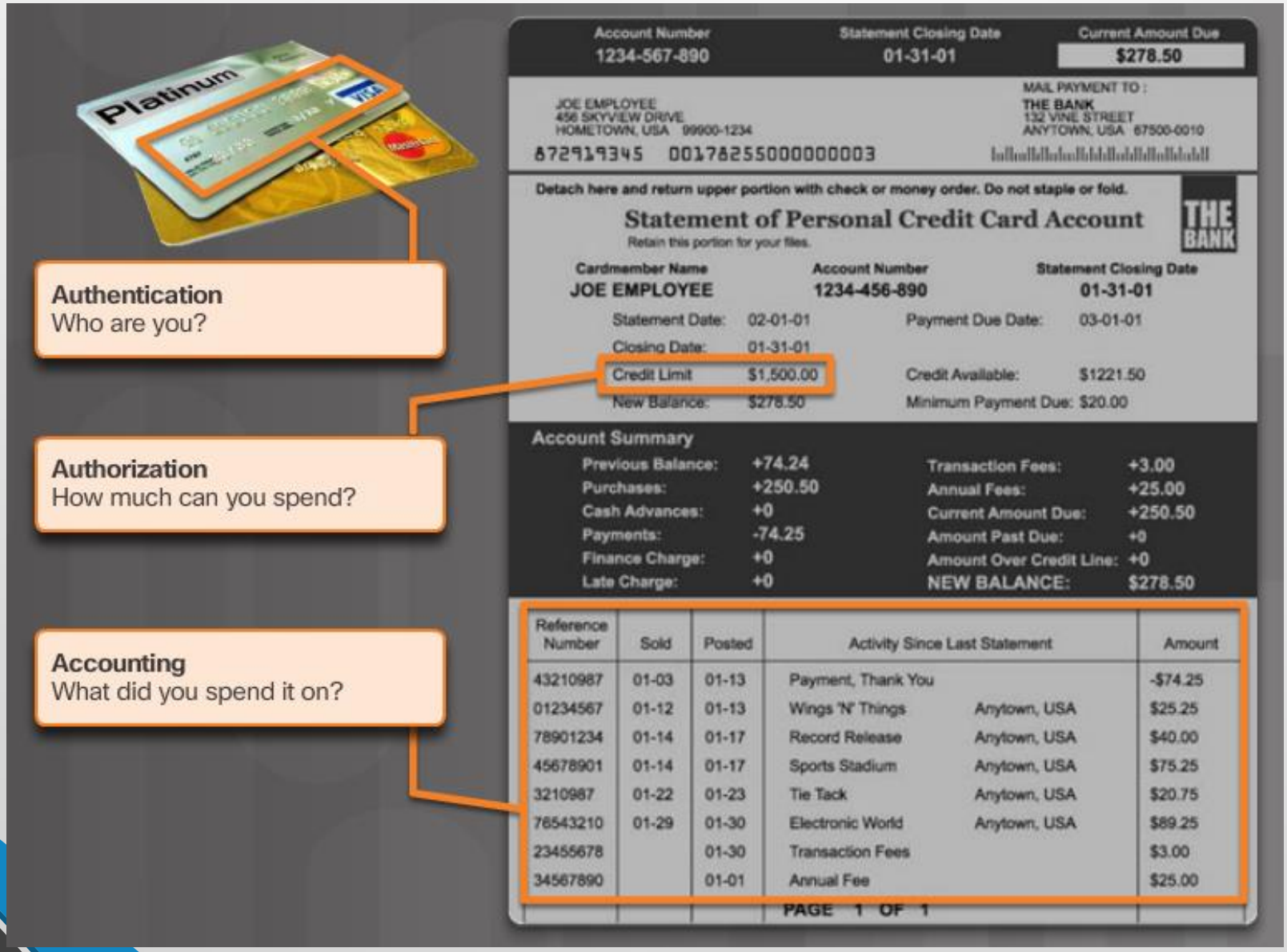


Аутентификация без AAA (продолжение)

Использование SSH и локальной базы данных



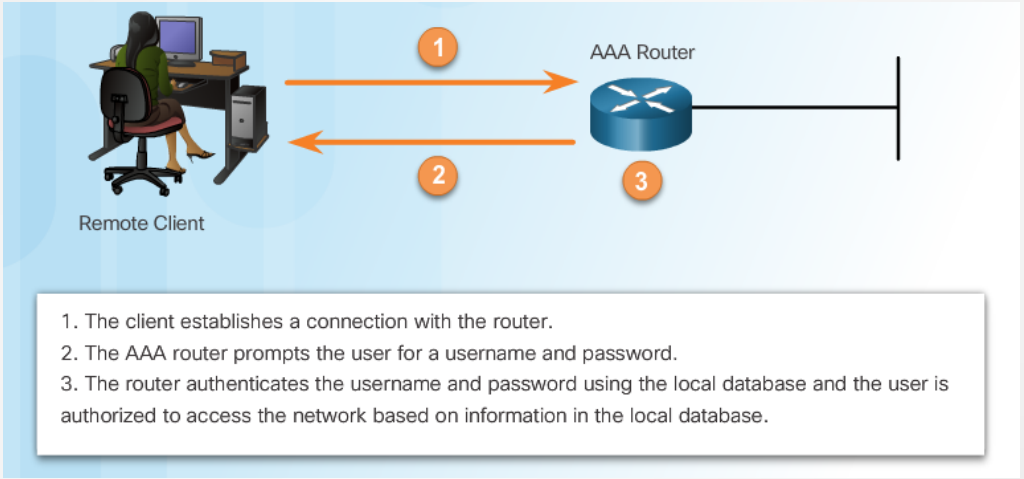
Компоненты AAA



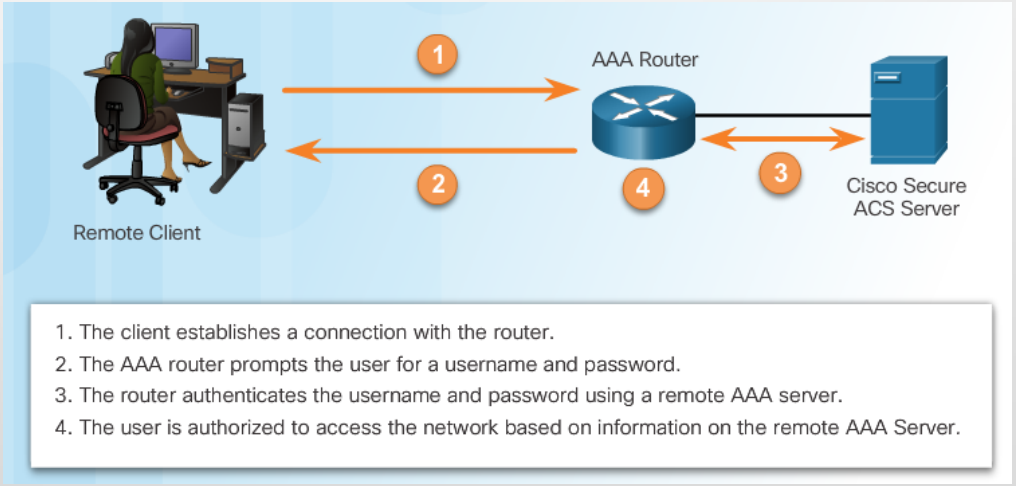
Тема Характеристики ААА

Режимы аутентификации

Локальная аутентификация AAA

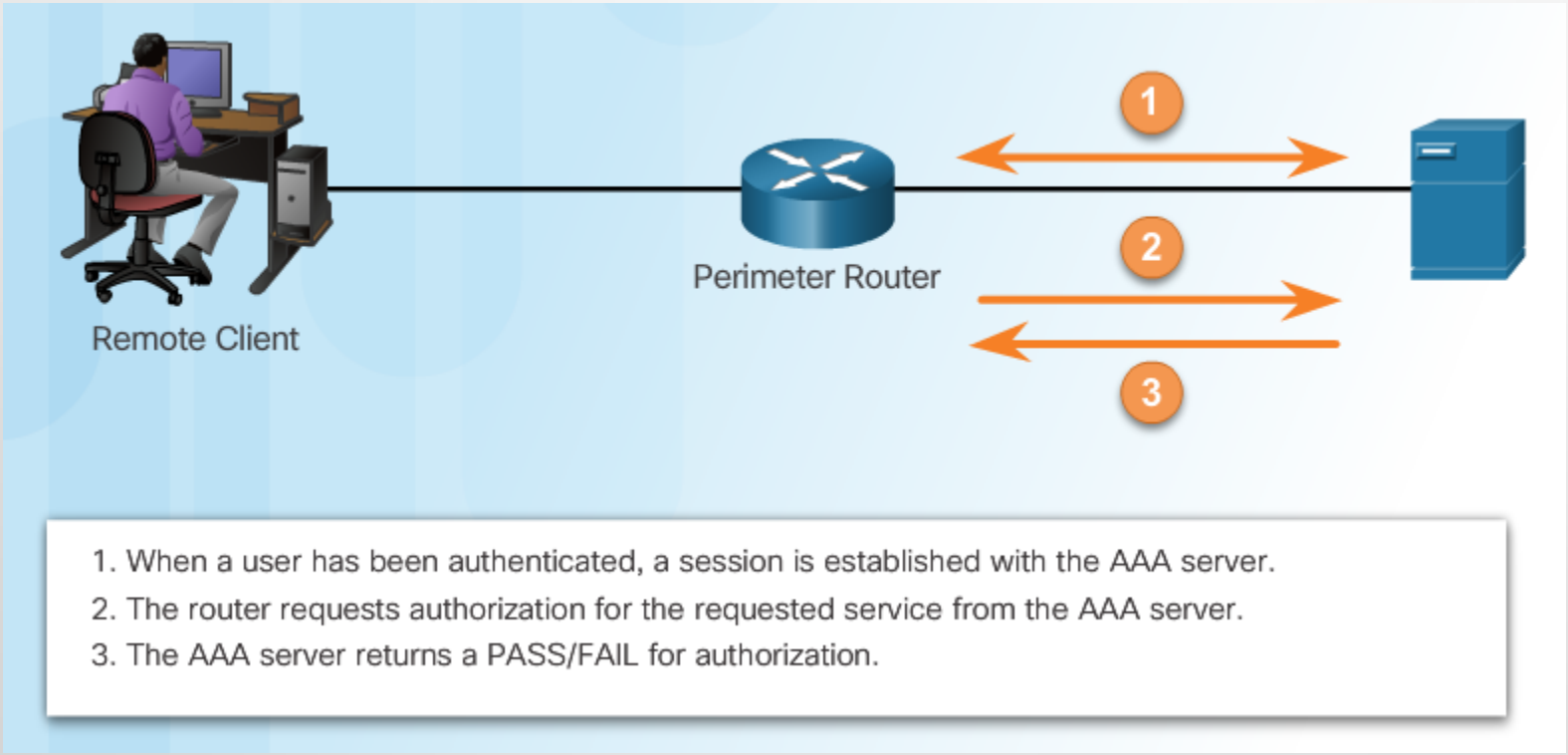


Серверная аутентификация AAA



Авторизация

Авторизация AAA

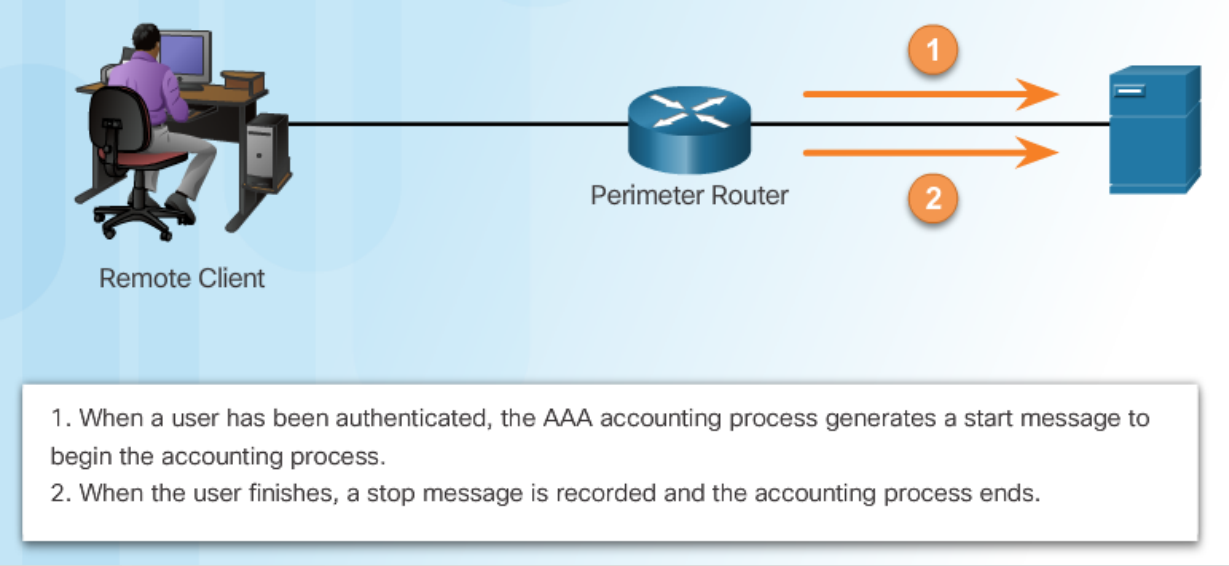


Учет

Типы учетной информации

- Сеть
- Подключение
- Режим ввода
- Система
- Команда
- Ресурс

Учет AAA



Тема Конфигурирование локальной аутентификации AAA с помощью интерфейса командной строки (CLI)

Аутентификация административного доступа

1. Добавьте имена пользователей и пароли в локальную базу данных маршрутизатора для пользователей, которым необходим административный доступ к этому маршрутизатору.
2. Включите AAA в глобальном режиме на маршрутизаторе.
3. Настройте параметры AAA на маршрутизаторе.
4. Подтвердите конфигурацию AAA и устраните неисправности.

```
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)#
```

Методы аутентификации

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)#
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.

Стандартный и именованный методы

Пример локальной аутентификации 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
```

Точная настройка конфигурации аутентификации

Синтаксис команды

```
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.

Показ заблокированных пользователей

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

Показ уникального идентификатора сеанса

```
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
```

Тема Устранение ошибок аутентификации AAA

Варианты отладки

Отладка локальной аутентификации 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
```

Отладка аутентификации AAA

Интерпретация результата отладки

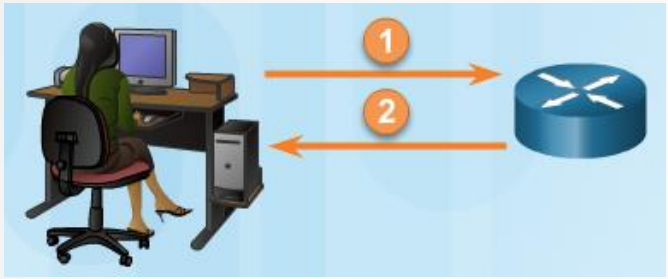
```
R1# debug aaa authentication
113123: Feb 4 10:11:19.305 CST: AAA/MEMORY: create_user (0x619C4940) user=''ruser=''
        port='tty1' rem_addr='async/81560' authen_type=ASCII service=LOGIN priv=1
113124: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): port='tty1' list=''
        action=LOGIN 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
```

Тема Характеристики серверной аутентификации AAA

Сравнение локальной и серверной аутентификации AAA

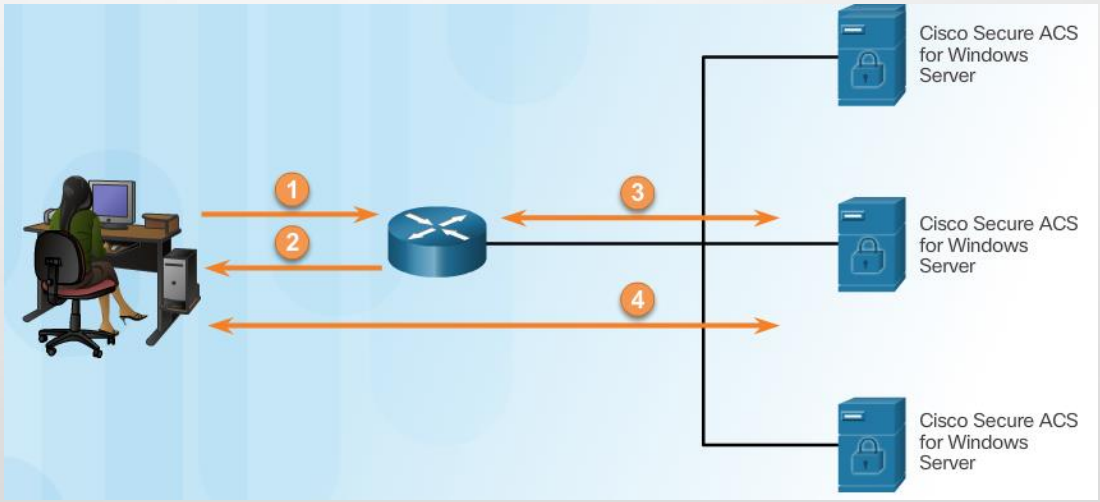
Локальная аутентификация:

1. Пользователь устанавливает подключение к маршрутизатору.
2. Маршрутизатор запрашивает имя пользователя и пароль, аутентифицирует пользователя по локальной базе данных.

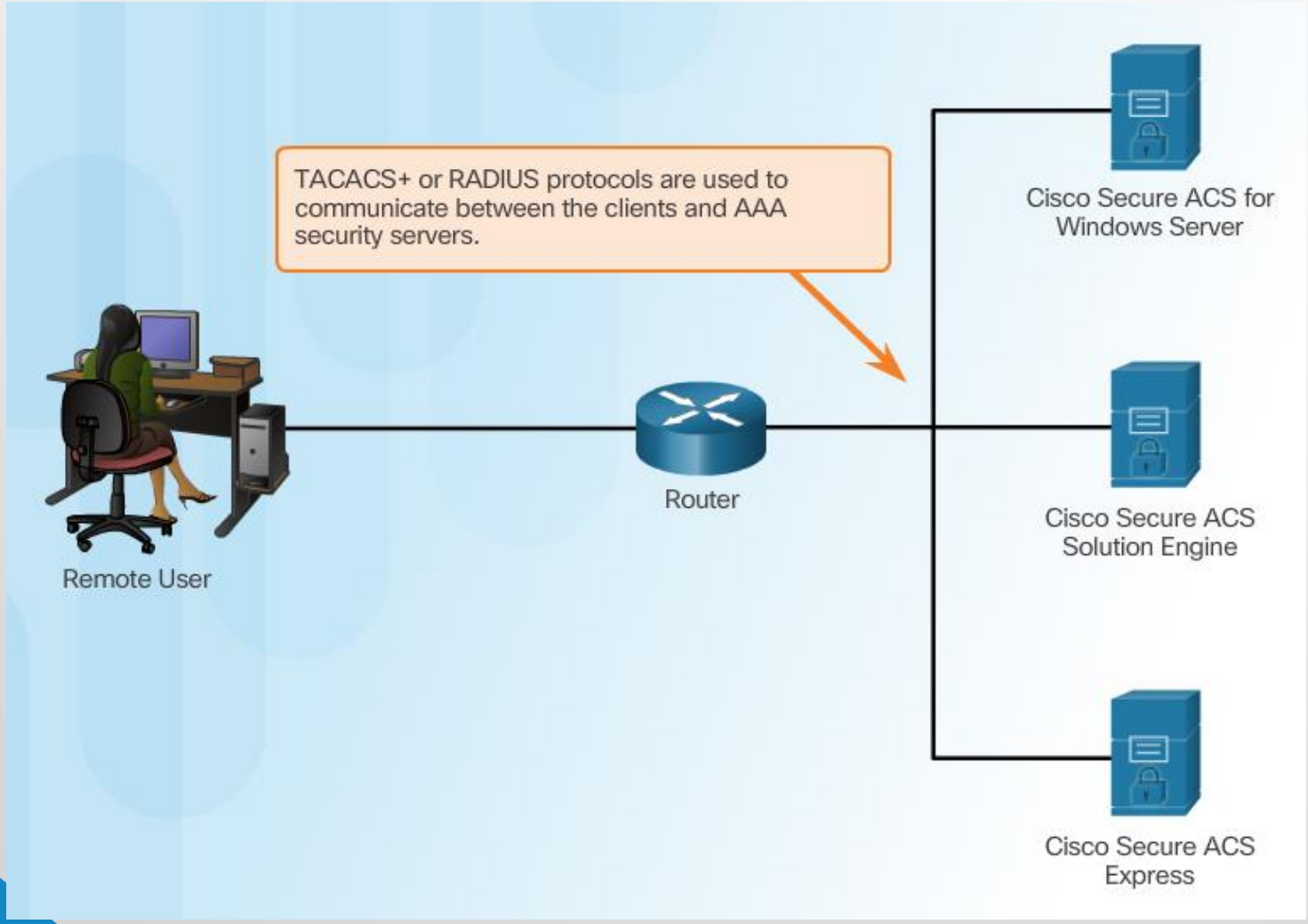


Серверная аутентификация:

1. Пользователь устанавливает подключение к маршрутизатору.
2. Маршрутизатор запрашивает имя пользователя и пароль.
3. Маршрутизатор передает имя пользователя и пароль на Cisco Secure ACS (сервер или модуль).
4. Cisco Secure ACS аутентифицирует пользователя.



Знакомство с системой управления защищенным доступом Cisco (Access Control System, ACS)



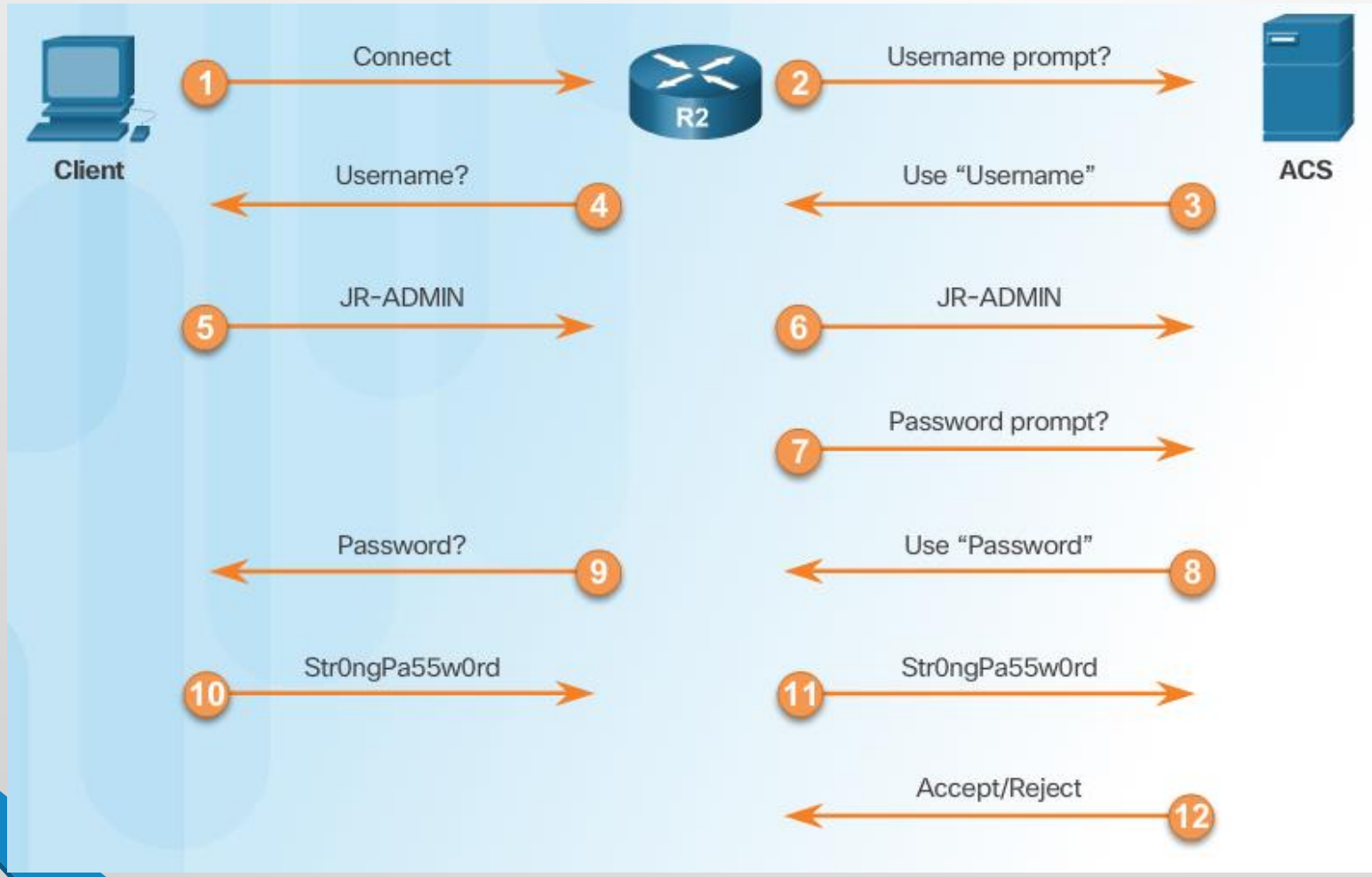
Тема Коммуникационные протоколы серверного AAA

Знакомство с протоколами TACACS+ и 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

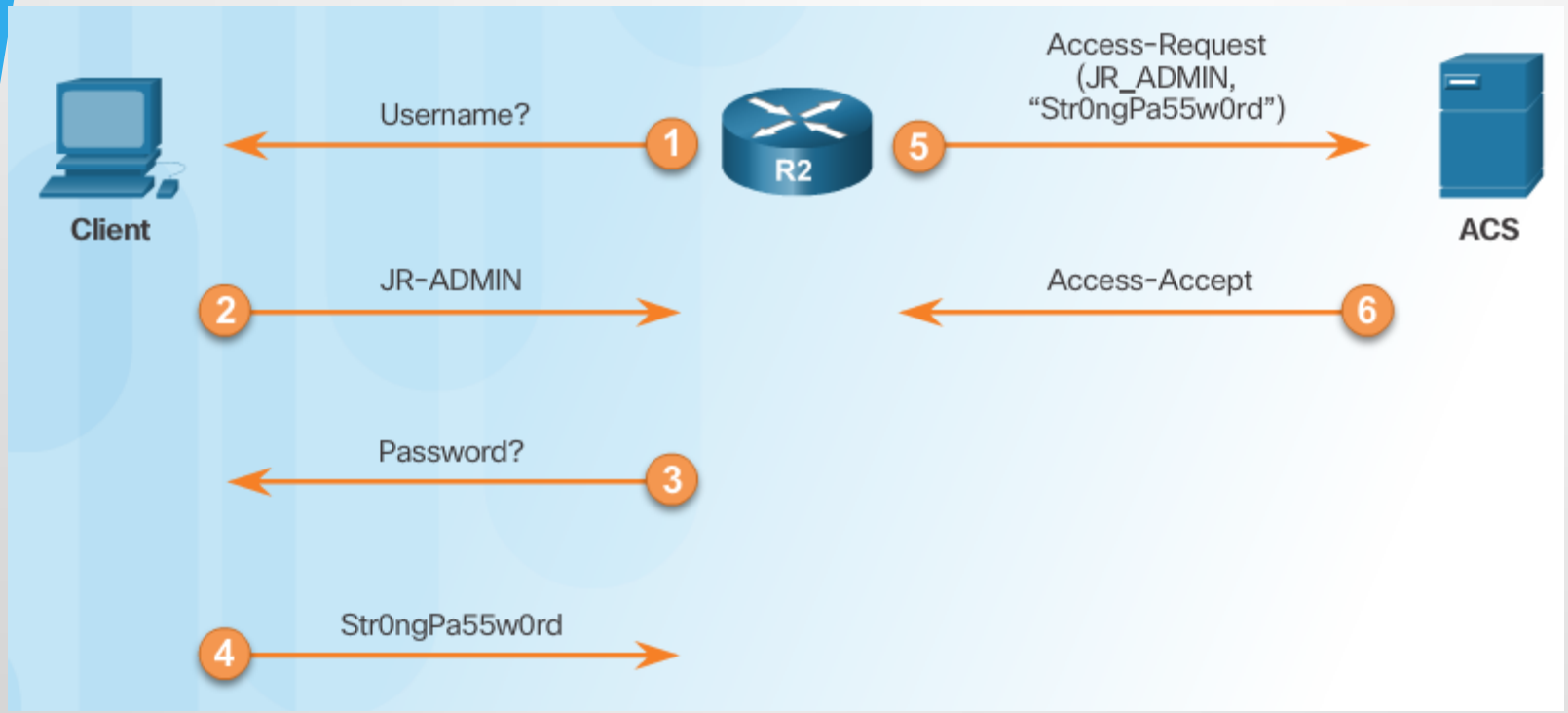
Аутентификация TACACS+

Процесс аутентификации TACACS+



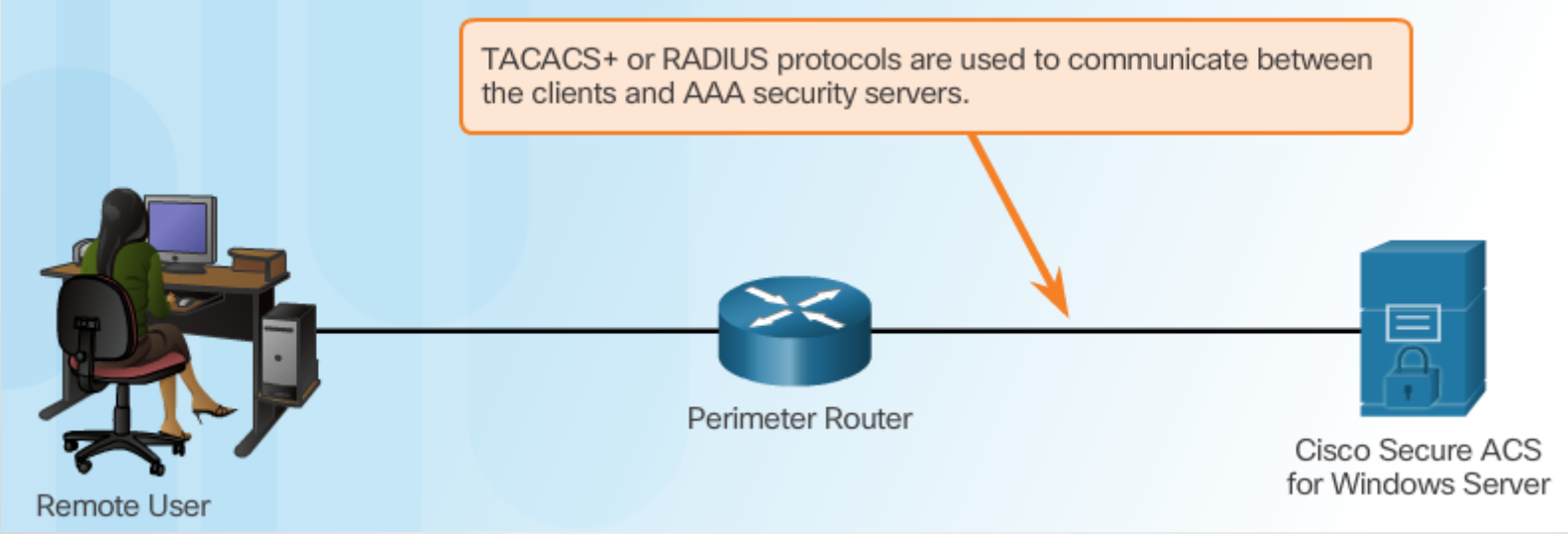
Аутентификация RADIUS

Процесс аутентификации RADIUS

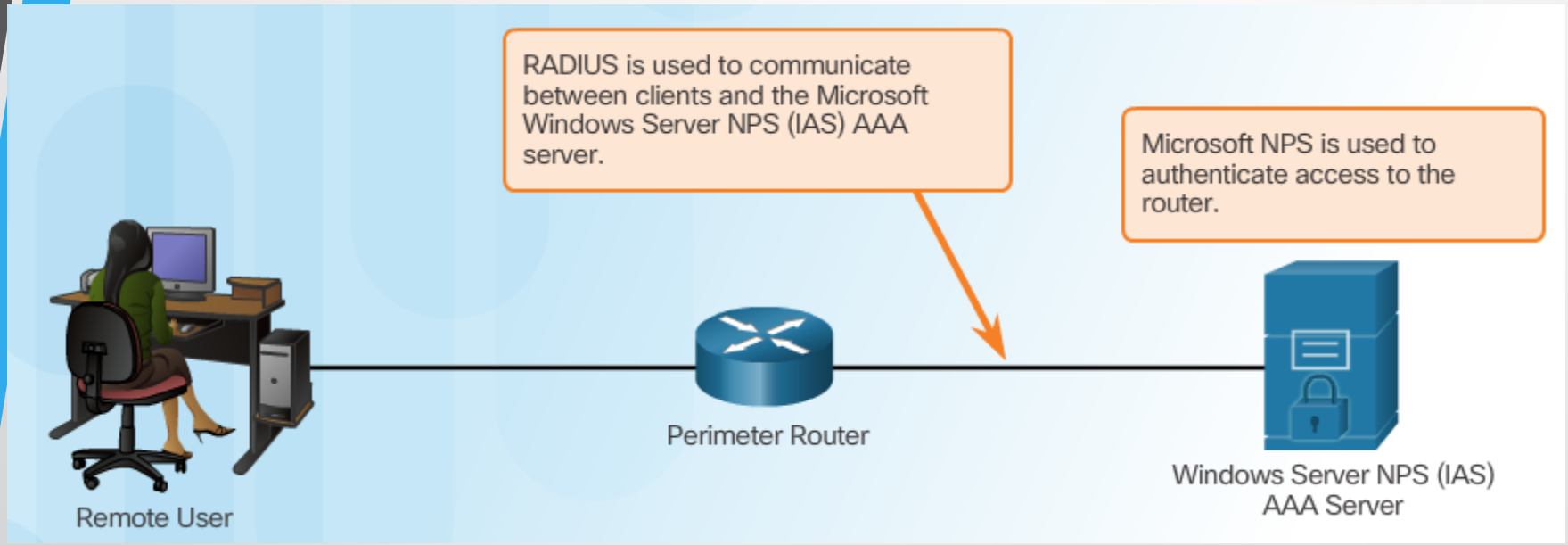


Интеграция TACACS+ и ACS

Cisco Secure ACS



Интеграция AAA с Active Directory



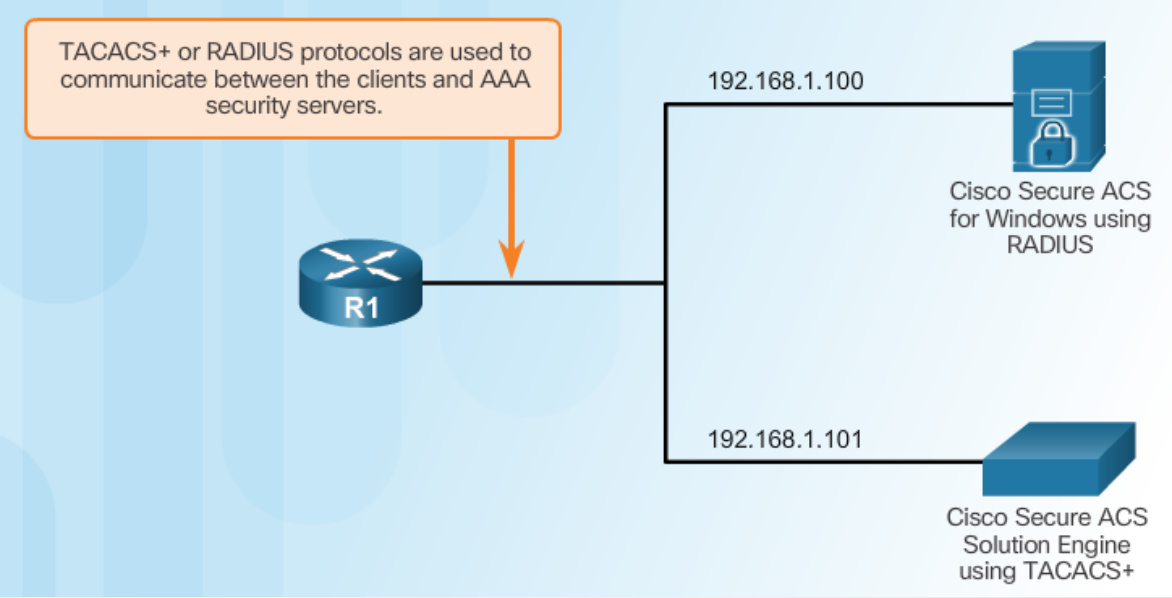
Тема Конфигурирование серверной аутентификации AAA с помощью интерфейса командной строки (CLI)

Процедура настройки серверной аутентификации AAA с помощью интерфейса командной строки (CLI)

1. Включите AAA.
2. Укажите IP-адрес сервера ACS.
3. Настройте секретный ключ.
4. Настройте использование сервера RADIUS или TACACS+ для аутентификации.

Конфигурирование использования серверов TACACS+ через CLI

Эталонная топология серверной AAA



Конфигурирование сервера 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)#
```

Конфигурирование использования серверов RADIUS через CLI

Конфигурирование сервера 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)#
```

Конфигурирование аутентификации с использованием сервера AAA

Синтаксис команды

```
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.
```

Конфигурирование серверной аутентификации 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
```

Тема Устранение ошибок серверной аутентификации AAA

Мониторинг трафика аутентификации

Исправление ошибок серверной аутентификации 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
```

Отладка протоколов TACACS+ и RADIUS

Поиск неисправностей 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>
```

Поиск неисправностей TACACS+

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

Отладка протоколов TACACS+ и RADIUS (продолжение)

Серверная аутентификация AAA прошла успешно

```
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
```

Серверная аутентификация AAA не удалась

```
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
```

Тема Конфигурирование серверной авторизации AAA

Знакомство с серверной авторизацией AAA

Сравнение аутентификации и авторизации

- **Аутентификация** проверяет, что устройство или конечный пользователь являются легитимными.
- **Авторизация** разрешает или запрещает пользователям, прошедшим аутентификацию, доступ к определенным областям и программам в сети.

Сравнение TACACS+ и RADIUS

- **TACACS+** разделяет аутентификацию от авторизации.
- **RADIUS не** разделяет аутентификацию от авторизации.

Настройка авторизации AAA с помощью интерфейса командной строки (CLI)

Синтаксис команды

```
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.
```

Список методов авторизации

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

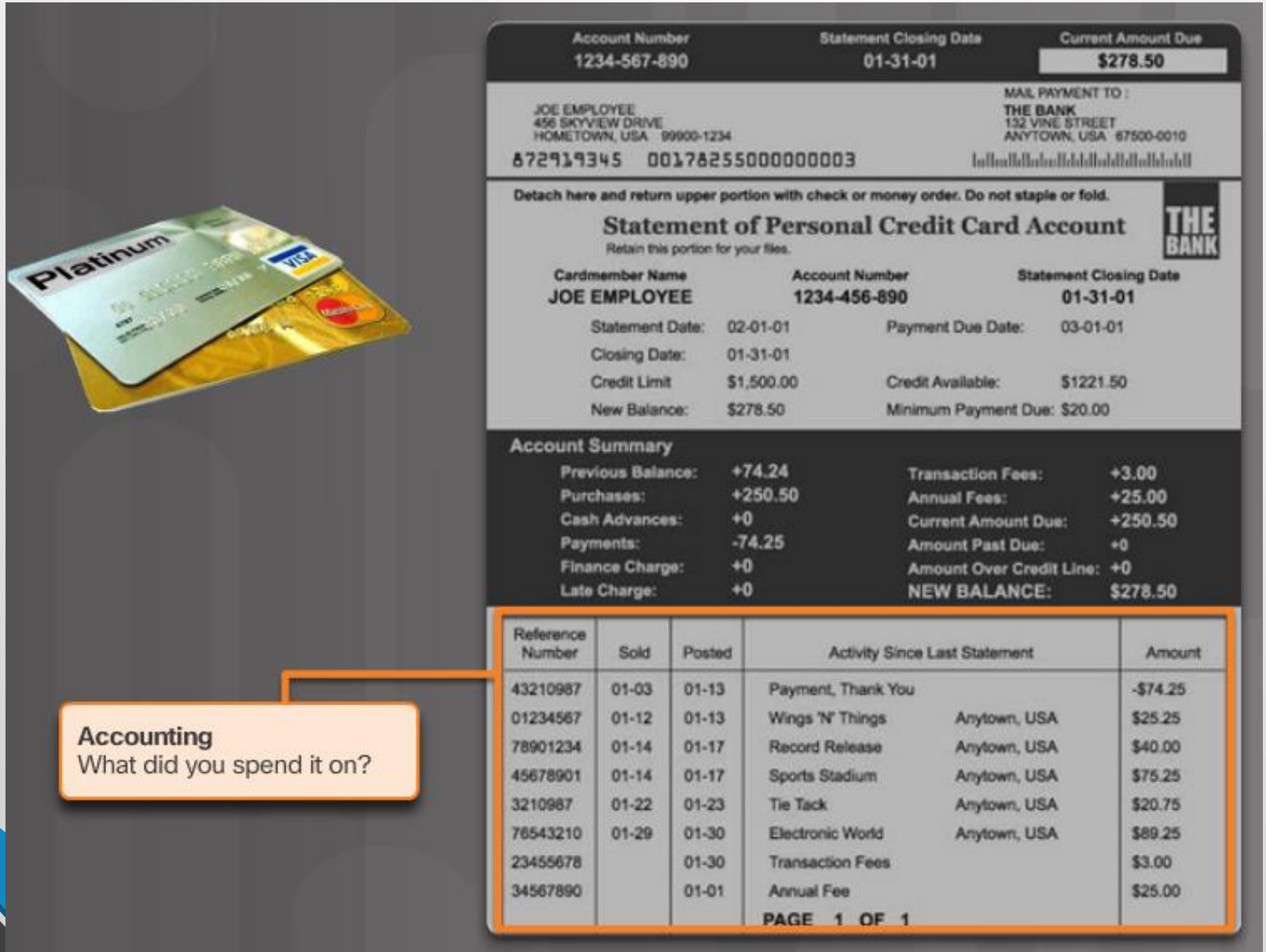
```
R1(config)# aaa authorization exec default ?
  cache             Use Cached-group
  group             Use server-group.
  if-authenticated  Succeed if user has authenticated.
  krb5-instance     Use Kerberos instance privilege maps.
  local             Use local database.
  none              No authorization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

Пример авторизации 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+
```

Тема Конфигурирование серверной авторизации AAA

Знакомство с серверным учетом AAA



Конфигурирование учета AAA с помощью интерфейса командной строки (CLI)

Синтаксис команды

```
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.
```

Список методов учета

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

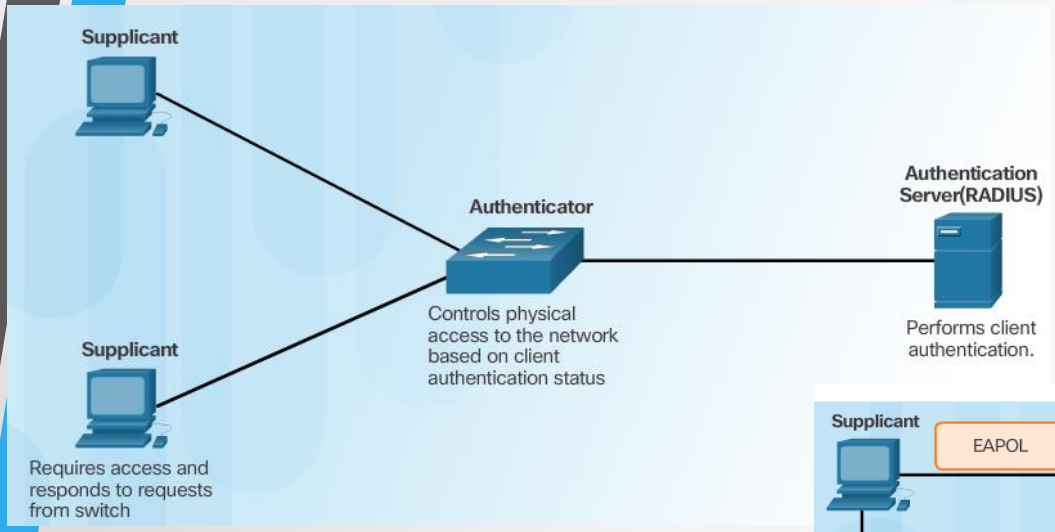
```
R1(config)# aaa accounting exec default start-stop?
  broadcast Use Broadcast for Accounting
  group     Use Server-group

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.
```

Пример учета AAA

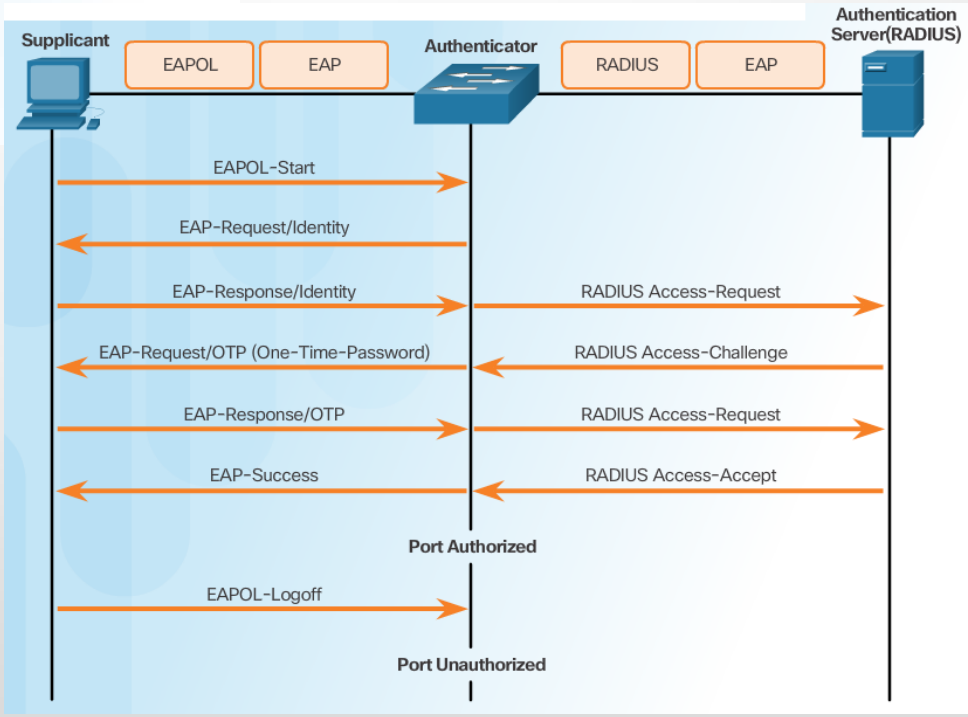
```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa5w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default group tacacs+
R1(config)# aaa authorization exec default group tacacs+
R1(config)#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

Тема
Аутентификация 802.1X

Обеспечение безопасности с использованием аутентификации 802.1X на основе портов



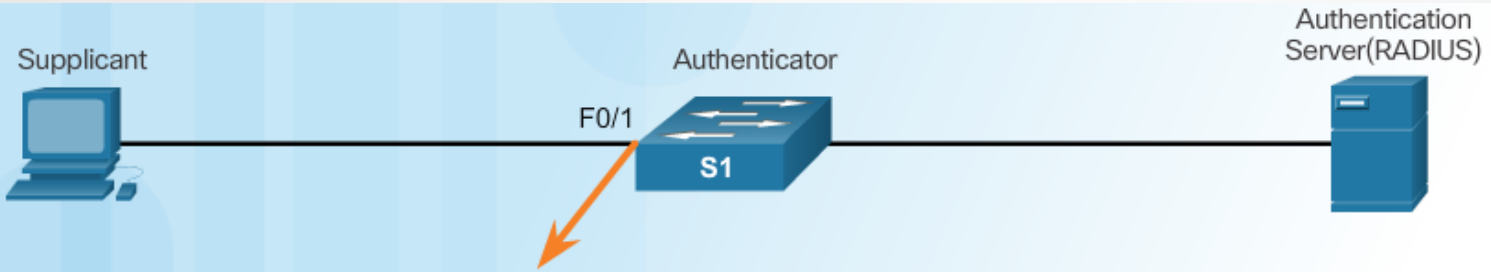
Роли 802.1X



Обмен сообщениями 802.1X

Состояния авторизации портов 802.1X

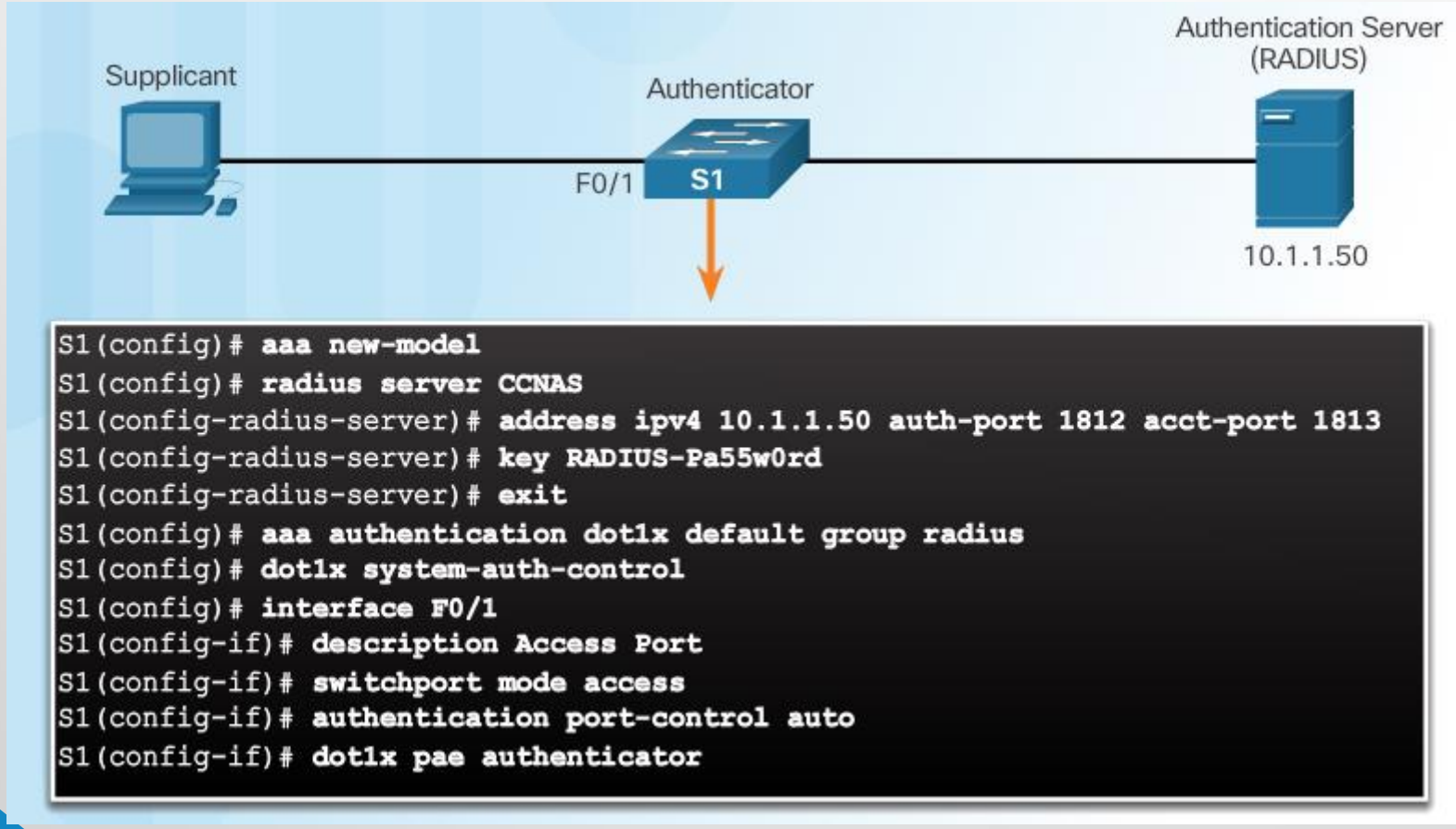
Синтаксис команд для dot1x port-control




```
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.

Конфигурирование 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
```