UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Chapter 3: Authentication, Authorization, and Accounting

KATEDRA INFORMAČNÝCH SIETÍ * FAKULTA RIADENIA A INFORMATIKY ŽU *

CCNA Security v2.0 / Network Security v1.0

Chapter 2 / Modules 7

cisco
Networking Academy

Bezpečnosť informačných sietí – KIS FRI UNIZA
Aktualizované v rámci projektu KEGA 026TUKE-4/2021.

Access control

- Essential part of cybersecurity
  - Apply selective restriction of access to a place, resource or assets
- Many types
  - Physical control
  - Logical control
  - Administrative control
  - ….
- How the access is controlled => AAA (authorization, authentication and accounting)

Physical Access Control

- Barriers deployed to prevent direct physical contact with systems.
- The goal => prevent unauthorized users from gaining physical access to facilities, equipment and other organizational assets
- Examples
  - Guards to monitor the facility
  - Fences to protect the perimeter
  - Motion detectors to detect moving objects
  - Laptop locks to safeguard portable equipment
  - Locked doors to prevent unauthorized access
  - Swipe cards to allow access to restricted areas
  - Guard dogs to protect the facility
  - Video cameras to monitor a facility by collecting and recording images
  - Mantrap-style entry systems to stagger the flow of people into the secured area and trap any unwanted visitors
  - Alarms to detect intrusion

Logical Access Control

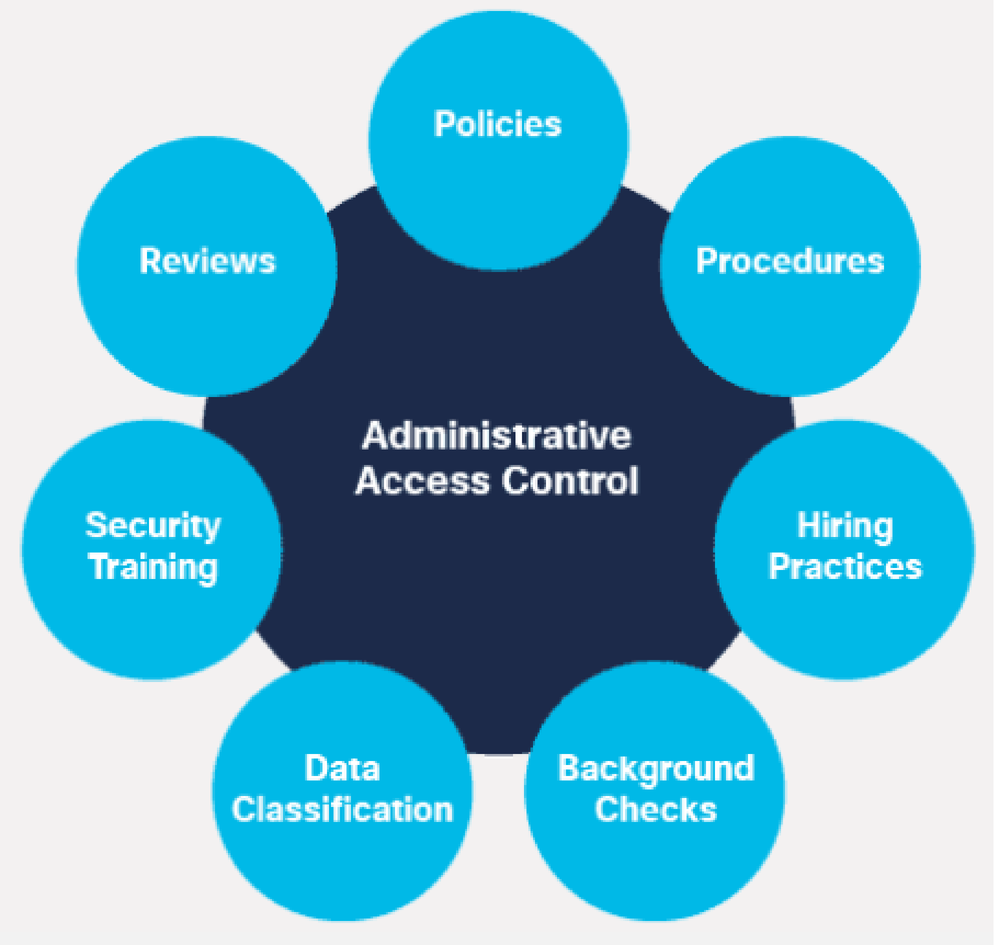
- Hardware and software solutions used to manage access to resources and systems

- Examples
  - Encryption is the process of taking plaintext and creating ciphertext.
  - Smart cards have an embedded microchip.
  - Passwords are protected strings of characters.
  - Biometrics are users' physical characteristics.
  - Access control lists (ACLs) define the type of traffic allowed on a network.
  - Protocols are sets of rules that govern the exchange of data between devices.
  - Firewalls prevent unwanted network traffic.
  - Routers connect at least two networks.
  - Intrusion detection systems monitor a network for suspicious activities.
  - Clipping levels are certain allowed thresholds for errors before triggering a red flag

Administrative Access Controls

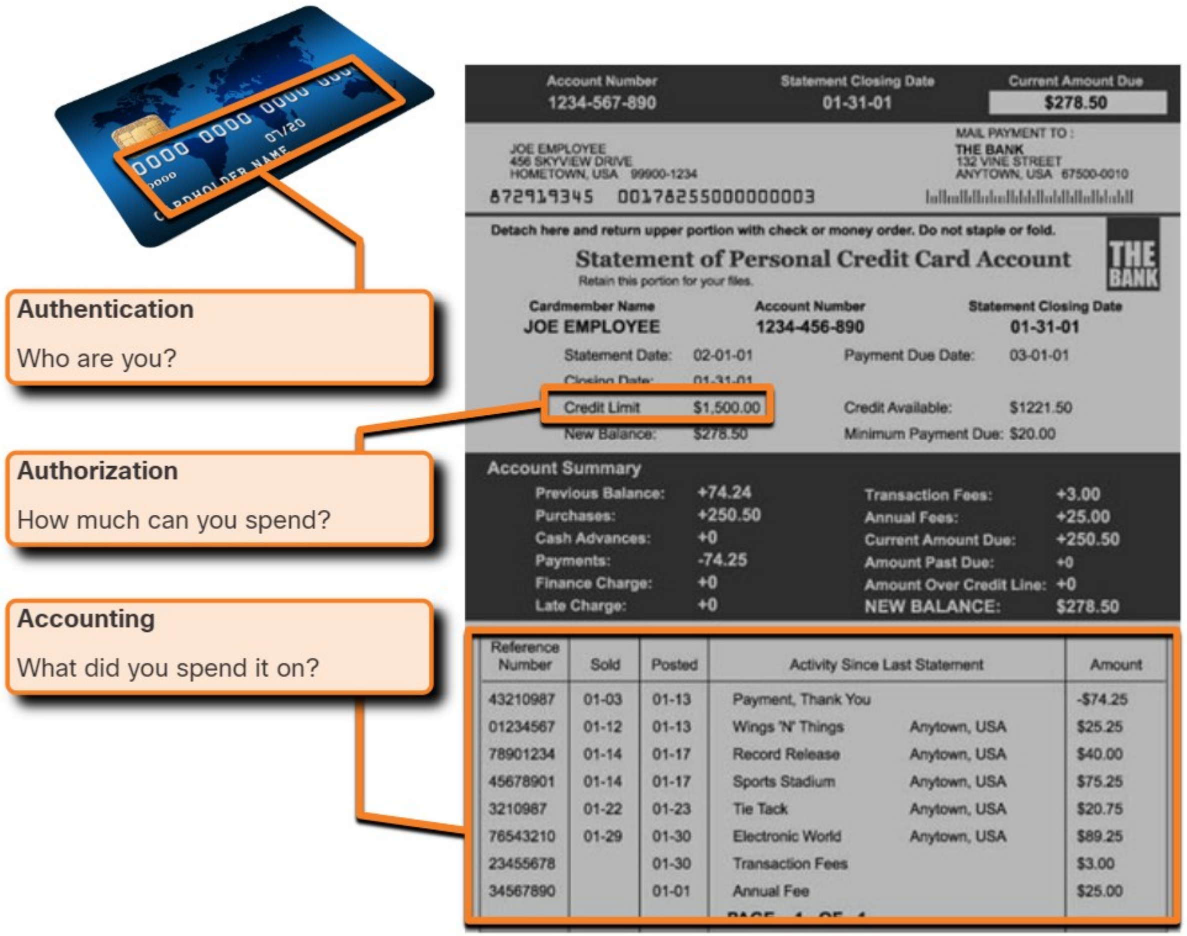
- Policies and procedures defined by organizations
  - Implement and enforce all aspects of controlling unauthorized access

- AC => typically implemented using AAA services



AAA overview and components

- AAA is a set of mechanisms (framework) for authentication, authorization, and accounting (billing)
  - Authentication
  - Authorization
  - Accounting (Reporting and auditing)
- Purpose of the AAA
  - Who is allowed to connect to
    - admins, corporate users, remote users, visitors, groups, business partners ..
  - When they are allowed to
  - What they are allowed to do



Authentication

Who are you?

Authorization

How much can you spend?

Accounting

What did you spend it on?

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

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA 99900-1234

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

872919345 0017825500000003

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

THE BANK

Statement of Personal Credit Card Account

Retain this portion for your files.

Cardmember Name	Account Number	Statement Closing Date
JOE EMPLOYEE	1234-456-890	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	NEW BALANCE:	$278.50

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		

AAA

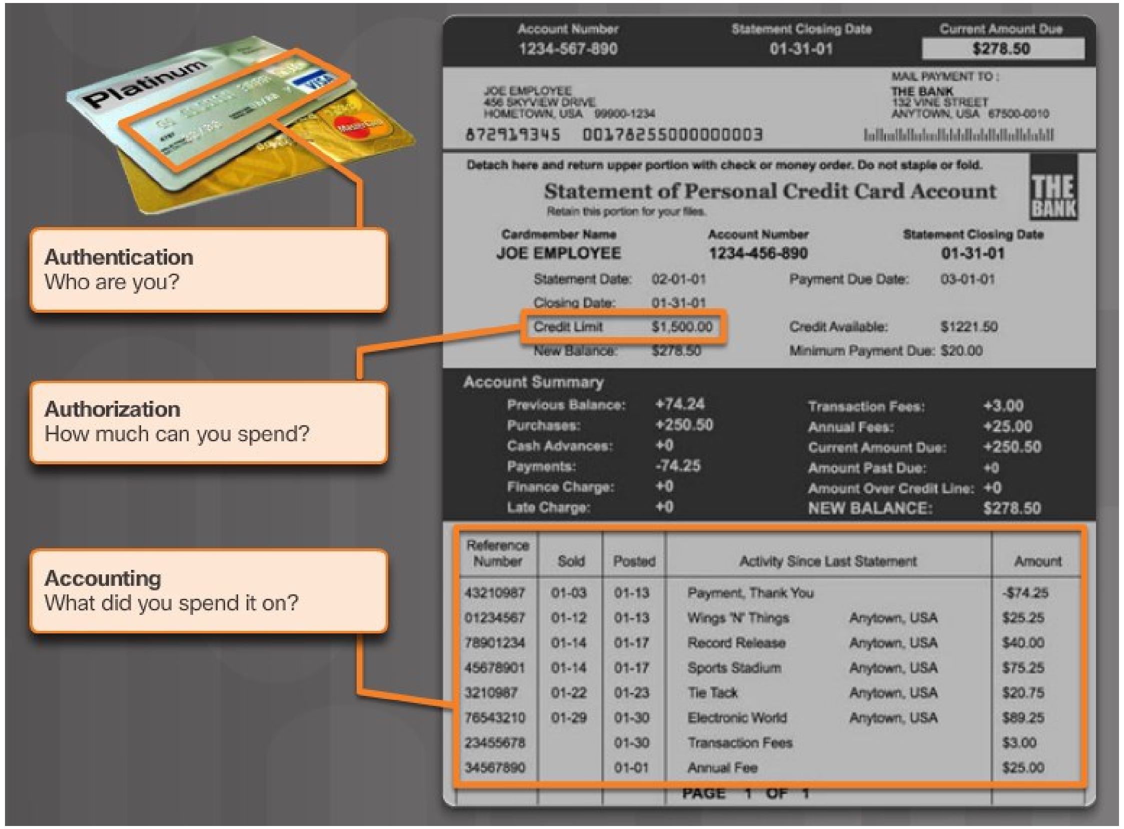
- **Authentication**
  - Verifies the identity to prevent unauthorized access
  - Users authentication
    - By username/UID
    - and one of
      - Something they **know**
        - Password, passphrases, PIN, …
      - Something they **have**
        - Token, card, key fob,
      - Something **they are**
        - Physiological characteristics
          - fingerprints, DNA, face, hands, the retina or ear features.
        - Behavioral characteristics
          - gestures, voice, gait or typing rhythm.
  - Two or multi-factor authentication

- **Authorization**
  - Tight with auth
  - Determine
    - Which resources can be accessed
    - or which operations can be performed
    - When
    - And by who

- **Accounting**
  - Keeps track of activities
    - What was done
    - What was accessed
    - The amount of time resources were accessed
    - Changes were made
  - My account
    - Network acc, EXEC, System, Command, resource

AAA overview and components

- In our course context
  - AAA is usually specified by the network security policy document
- On Cisco devices, AAA is used for various purposes
  - Administrative Access Control (EXEC)
  - 802.1X on switches
  - WPA or WPA2 Enterprise on WiFi Access Points
  - PPP, IPSec …



Authentication
Who are you?

Authorization
How much can you spend?

Accounting
What did you spend it on?

Account Number	Statement Closing Date	Current Amount Due
1234-567-890	01-31-01	$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

Cardmember Name	Account Number	Statement Closing Date
JOE EMPLOYEE	1234-456-890	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	NEW BALANCE:	$278.50

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

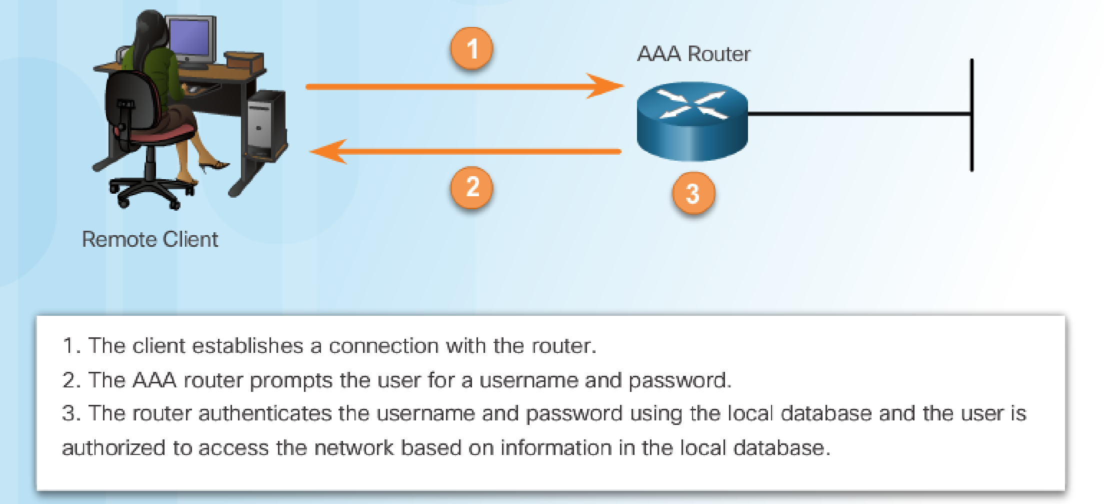
Cisco AAA modes

Local AAA

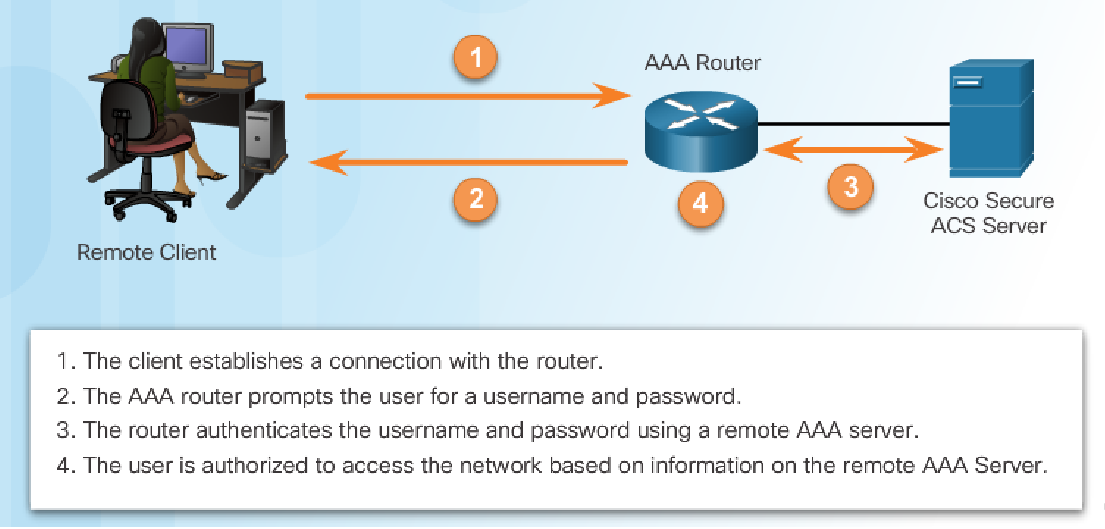
- Older method
- Uses a local database
  - database is the same one as required for establishing role-based CLI.
  - Stores names and passwords
- Supports authentication and authorization
- Accounting is very limited

Server-Based AAA

- Newer method
- Uses an AAA server
  - Username and passwords for authentication
  - Rights and cmds for authorization
  - Activity logging for accounting
  - For example Cisco Secure Access Control System (ACS)
- Better flexibility
  - allows different services to target AAAs to different databases



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.



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.

Cisco IOS
Local AAA Authentication

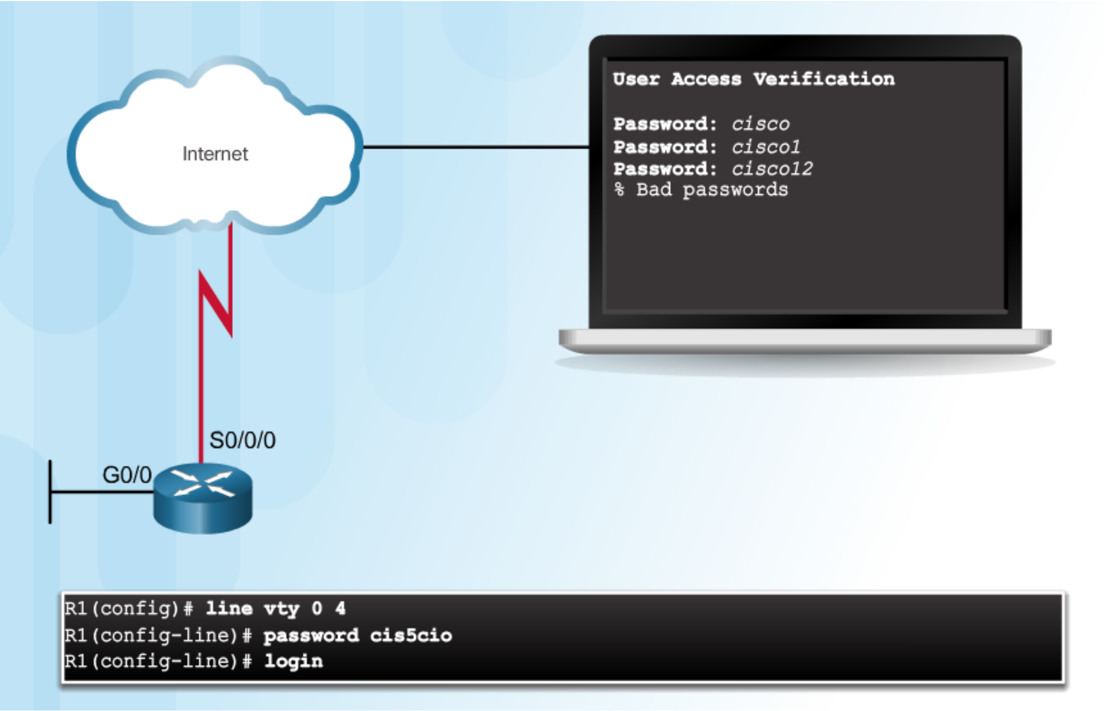
Upon completion of this section, you should be able to:

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

Authentication without AAA

Telnet with shared pass

- Simplest method
- Must be configured on each device
- Telnet is Vulnerable to Brute-Force Attacks
- Weakest
  - No encryption,
  - No accounting
  - Shared pass

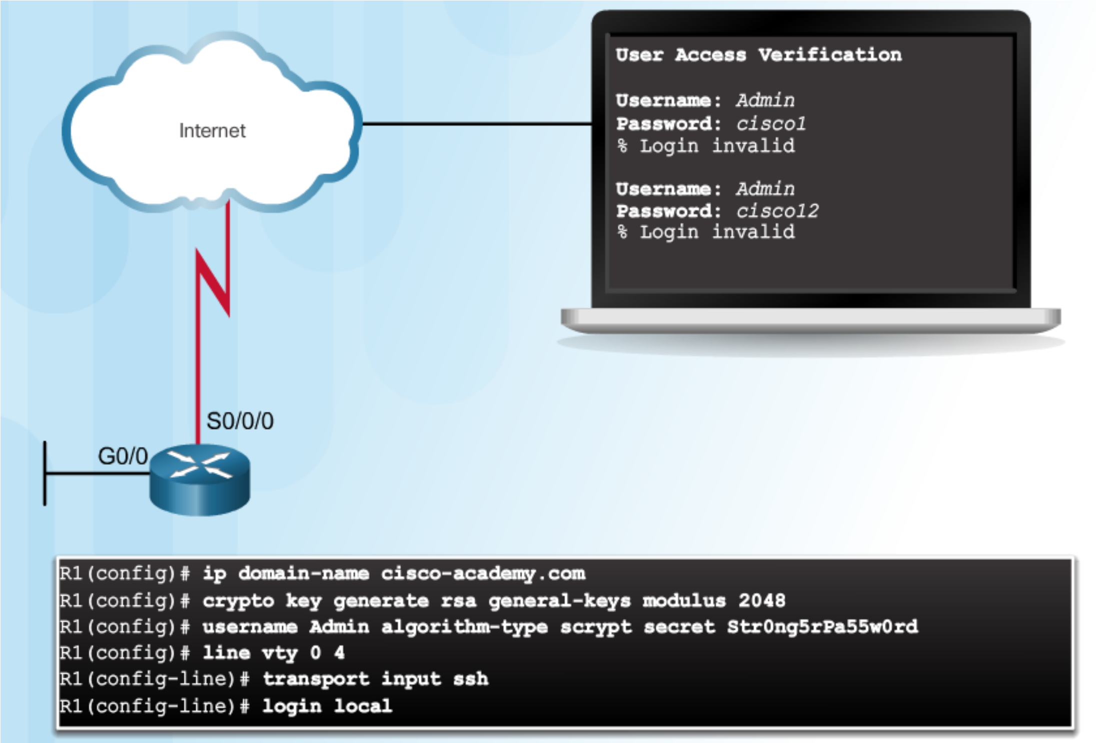


```
User Access Verification

Password: cisco
Password: cisco1
Password: cisco12
% Bad passwords
```

```
R1(config)# line vty 0 4
R1(config-line)# password cis5cio
R1(config-line)# login
```

SSH using Local DB

- More secure
  - Encryption, user passwords
  - Login recording
- Must be configured on each device



```
User Access Verification

Username: Admin
Password: cisco1
% Login invalid

Username: Admin
Password: cisco12
% Login invalid
```

```
R1(config)# ip domain-name cisco-academy.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

New AAA model

- The new AAA model is based on these assumptions
  - On the one hand, we have certain types of services that can control access through a certain mechanism (dot1x, enable, login, ppp)
  - On the other hand, we have various databases with user records and their rights (RADIUS, TACACS, lokálna databáza)
  - We want to be able to explain the specific service in which database should search for a user
- For example:
  - Console logins authenticate against local database
  - SSH logins against RADIUS server available at IP 1.2.3.4
  - PPP logins authenticate against RADIUS server at IP 5.6.7.8
  - Ethernet clients authenticate against RADIUS server at IP 9.8.7.6

Configuring AAA authentication – 1.

- 1) Define sources of authentication

```
! Define local DB entries only
Router(config)# username USERNAME password PASSWORD

! Radius - potlacana froma specifikacie servera
Router(config)# radius-server host {HOSTNAME | IP-ADDRESs} [key STRING]

! Tacacs  - potlacana froma specifikacie servera
Router(config)# tacacs-server host {HOSTNAME | IP-ADDRESS} [key STRING]

! Preferovane
Router(config)# address {ipv4 | ipv6} ADDRESS

! Mozme formovat grupu ako list zdrojov
Router(config)# aaa group server {radius | tacacs+} GROUP-NAME
Router (config-sg)# server IP-ADDRESS
```

- 2) Activate support for the new AAA:

```
Router(config)# aaa new-model
```

Configuring AAA Authentication – 2.

- 3) Define the list of authentication methods (databases) that will be tried for specific service:

```
Router(config)# aaa authentication { ppp | dot1x | enable | login } {default |
  MENO_DB} db1 [db2 …]
```

  - DB
    - tacacs+: try out every TACACS server in the order how it is defined
    - radius: try out every Radius server in the order how it is defined
    - local: use local *Usernames*.
    - line: line pass authenticates whoever uses it, usernames will not be used

- 4) Apply authentication methods to console / vty / aux lines and verify

```
Router(config)# line con 0 OR vty 0 15 OR aux
Router(config-line)# login authentication {default | MENO_DB}
```

Authenticating Administrative Access – example default and named with Local DB

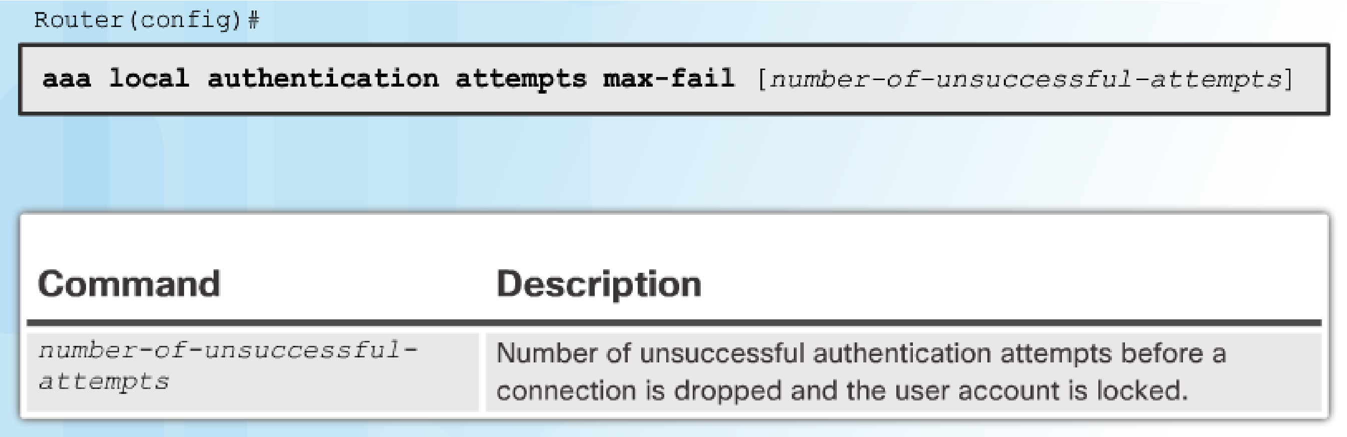
- An example for smaller networks
  - Add usernames and passwords to the local router database for users that need administrative access to the router.
  - Enable AAA globally on the router.
  - Configure AAA parameters on the router.
  - Confirm and troubleshoot the AAA configuration.

```
! username MENO algorithm-type scrypt secret HESLO
username JR-ADMIN-JOZEF algorithm-type scrypt secret T4t1lBr5t@1P@ssw4rd
!
aaa new-model
!
! Use a default schema, be case sensitive
! aaa authentication login default local-case

! use an authentication database named
aaa authentication login AE_L_LOCAL local
!
! Apply for line vty
line vty 0 15
! login authentication default
 login authentication AE_L_LOCAL
```

Fine-Tuning the Authentication Configuration

- Provides additional security
  - Locking out users with excessive attempts
  - Locked users must be explicitly unlocked

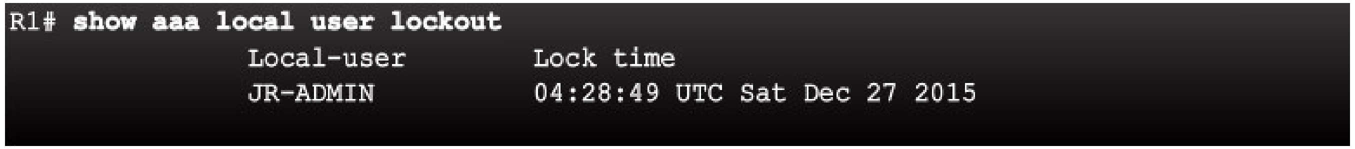
Command Syntax



```
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.

Display Locked Out Users

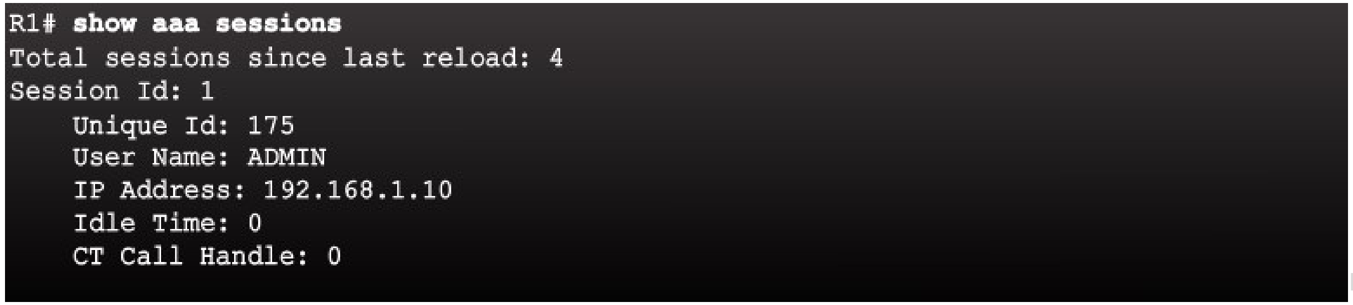


```
R1# show aaa local user lockout
               Local-user        Lock time
               JR-ADMIN          04:28:49 UTC Sat Dec 27 2015
```

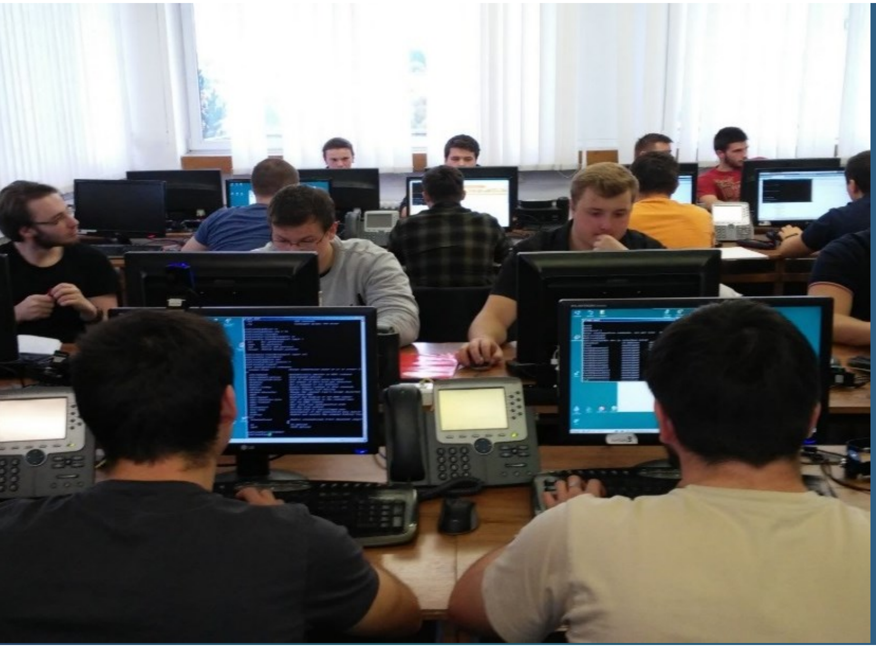
Unlock

```
clear aaa local user lockout
```

Show Unique ID of a Session



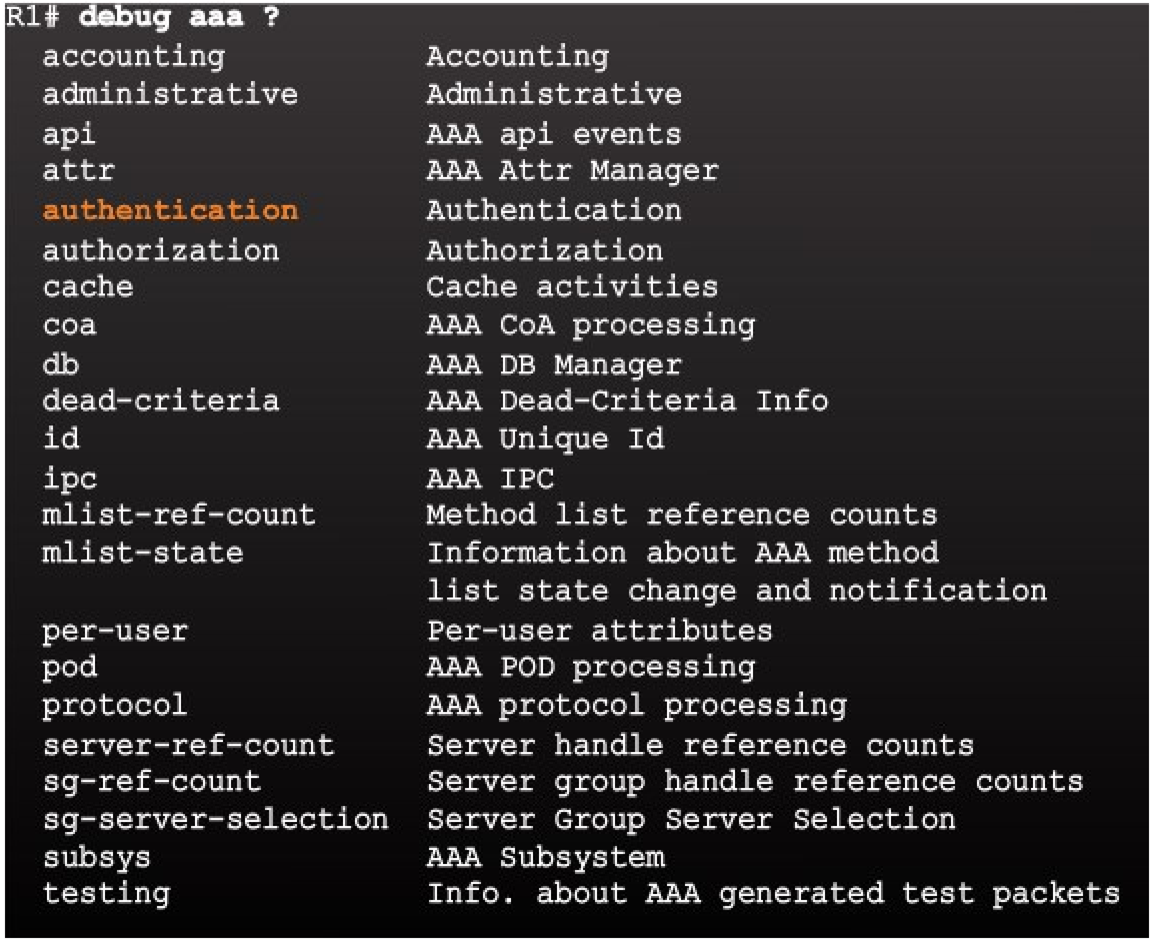
```
R1# show aaa sessions
Total sessions since last reload: 4
Session Id: 1
    Unique Id: 175
    User Name: ADMIN
    IP Address: 192.168.1.10
    Idle Time: 0
    CT Call Handle: 0
```



Troubleshooting Local AAA Authentication

Debug AAA Options

Debug Local AAA Authentication

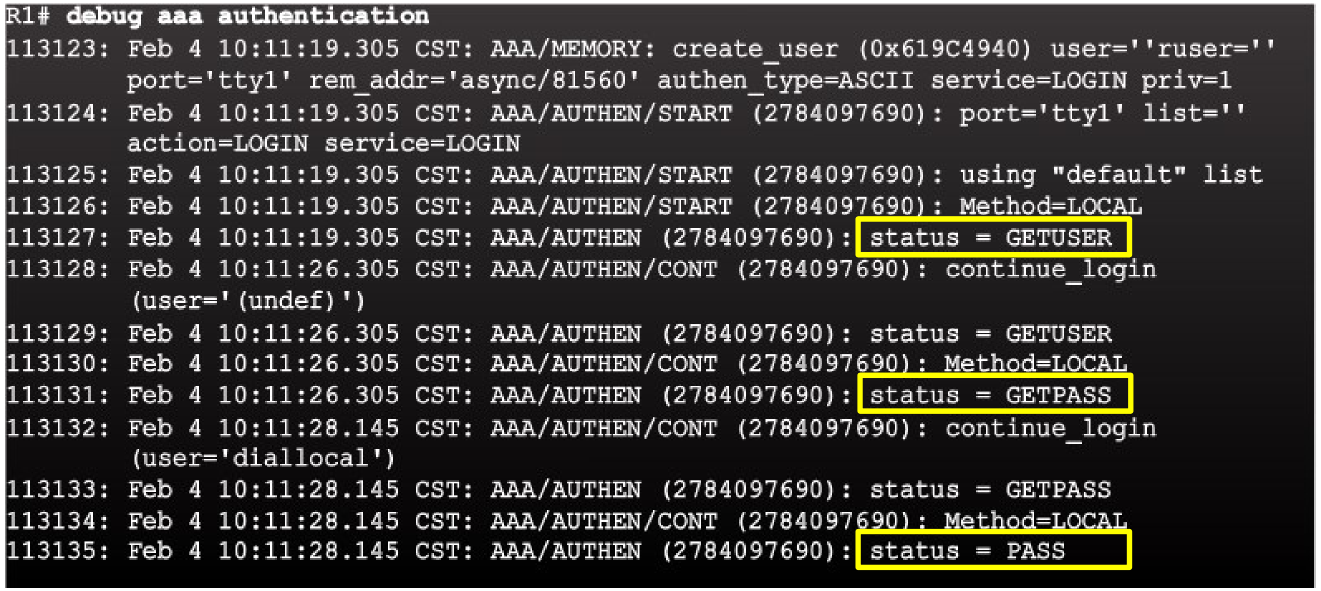


```
R1# debug aaa ?
  accounting            Accounting
  administrative        Administrative
  api                   AAA api events
  attr                  AAA Attr Manager
  authentication        Authentication
  authorization         Authorization
  cache                 Cache activities
  coa                   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

```
! On
debug aaa authentication
! Off
no debug aaa authentication
undebug all
```

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
```

- Look for status messages (GETUSER and GETPASS)
  - Username and pass exchange
- And final status
  - Final decision

Server-Based AAA

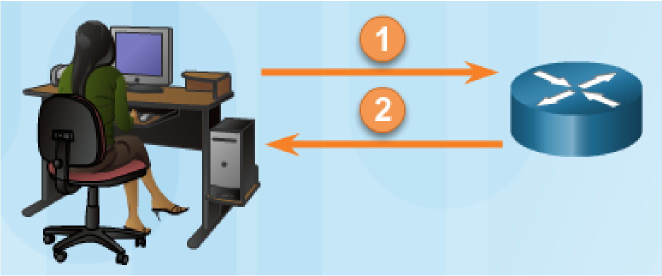
Upon completion of this section, you should be able to:

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

Comparing Local AAA and Server-Based AAA Implementations

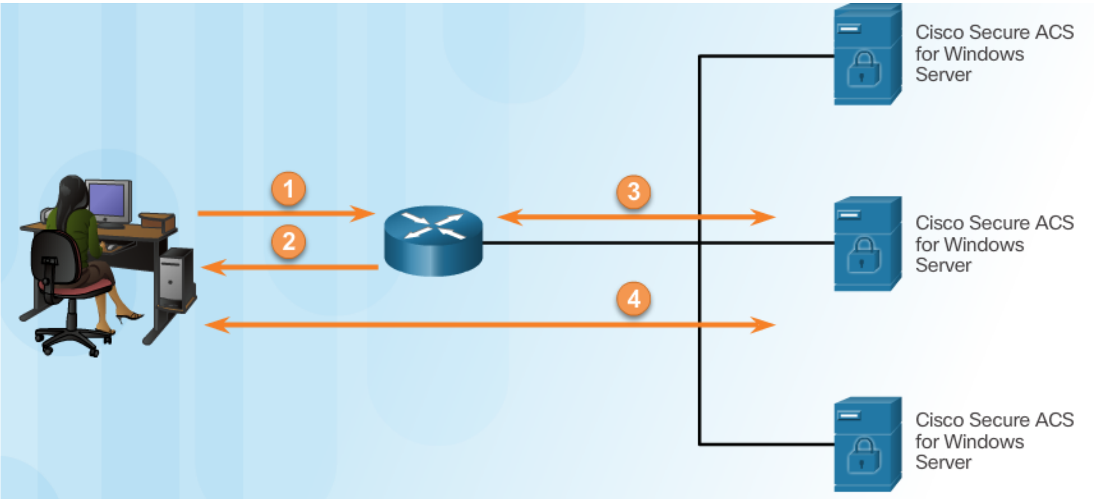
Local authentication:

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.

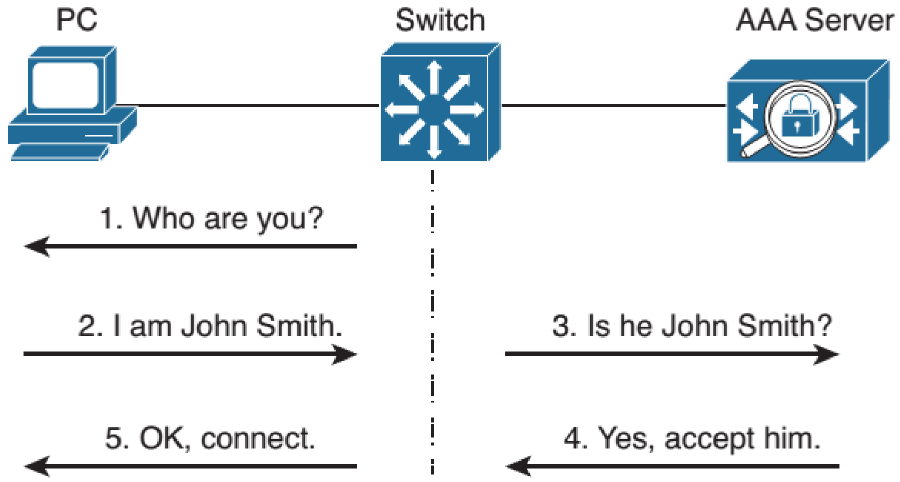


Server-based authentication:

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 server (Cisco Secure ACS (server or engine) here)
4. The server (Cisco Secure ACS) authenticates the user.


1
2
3
4
Cisco Secure ACS for Windows Server
Cisco Secure ACS for Windows Server
Cisco Secure ACS for Windows Server

Možnosti serverovej autentifikácie a autorizácie

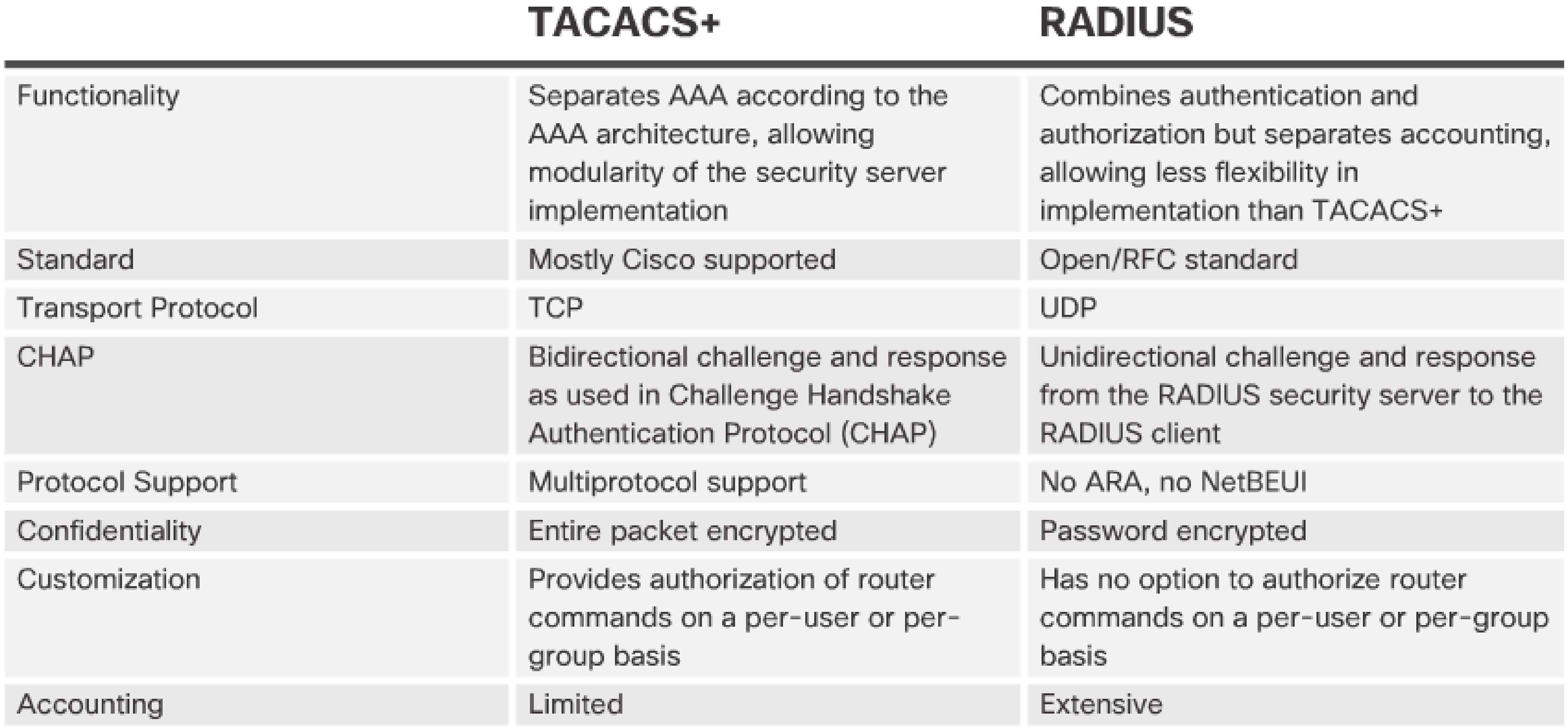


- Common in an enterprise
  - More devices and admins, or admin roles
- AAA network solutions
  - Tacacs+ a Radius
    - Cisco Secure ACS vs. FreeRadius (vs MS NPS – Network Policy Server)

- **Radius (Remote Authentication Dial-In User Service)**
  - Open solution defined in several RFC
  - Uses UDP ports
    - IANA 1812 (auth) / 1813 (account)
    - Cisco def. 1645 (auth) / 1646 (account)
  - Only part of the message containing a password is encrypted
  - Combines authentication and authorization
  - Offers robust account functions
  - Supports remote-access solutions (dot1x)

- **TACACS/TACACS+ (Terminal Access Controller Access Control System+)**
  - Cisco proprietary
  - Robust (heavy) solution
  - Encrypts the whole message
  - Uses TCP port 49
  - Separates authentication and authorization

Introducing TACACS+ and RADIUS

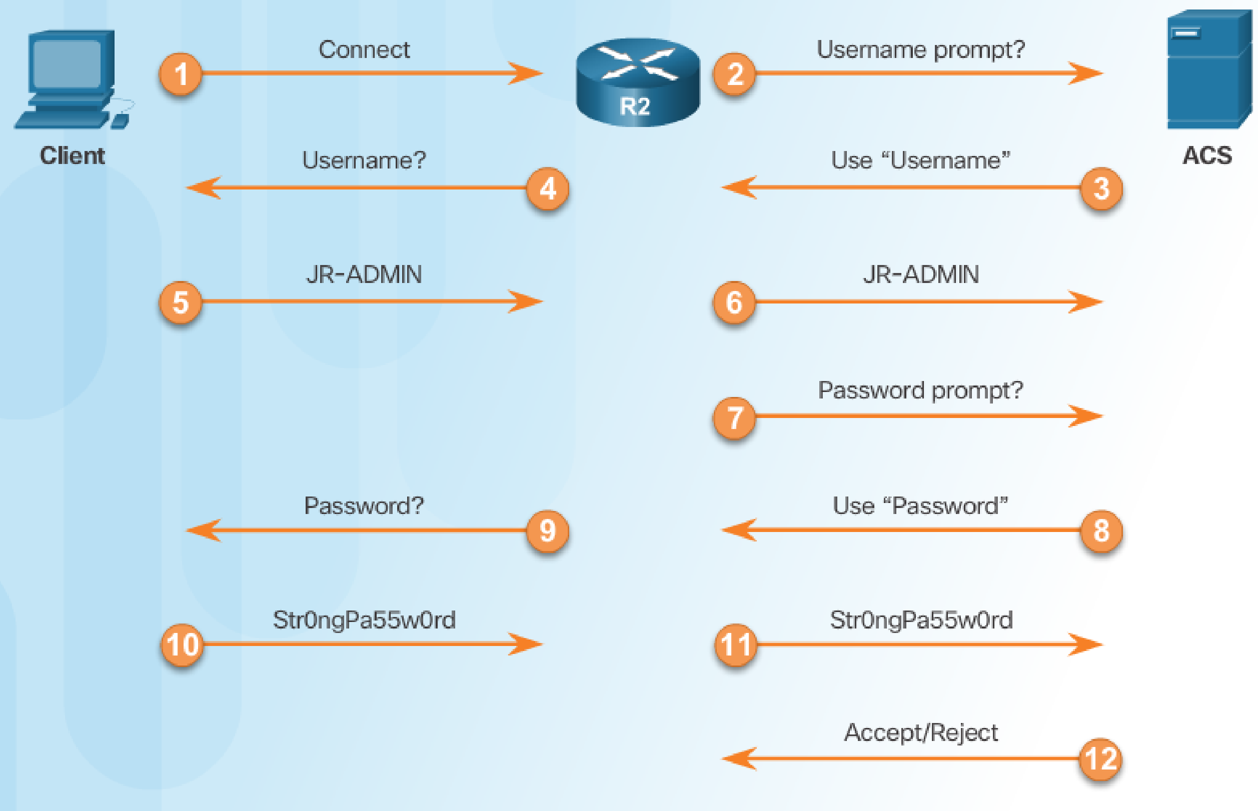


	TACACS+	RADIUS
Functionality	Separates AAA according to the AAA architecture, allowing modularity of the security server implementation	Combines authentication and authorization but separates accounting, allowing less flexibility in implementation than TACACS+
Standard	Mostly Cisco supported	Open/RFC 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

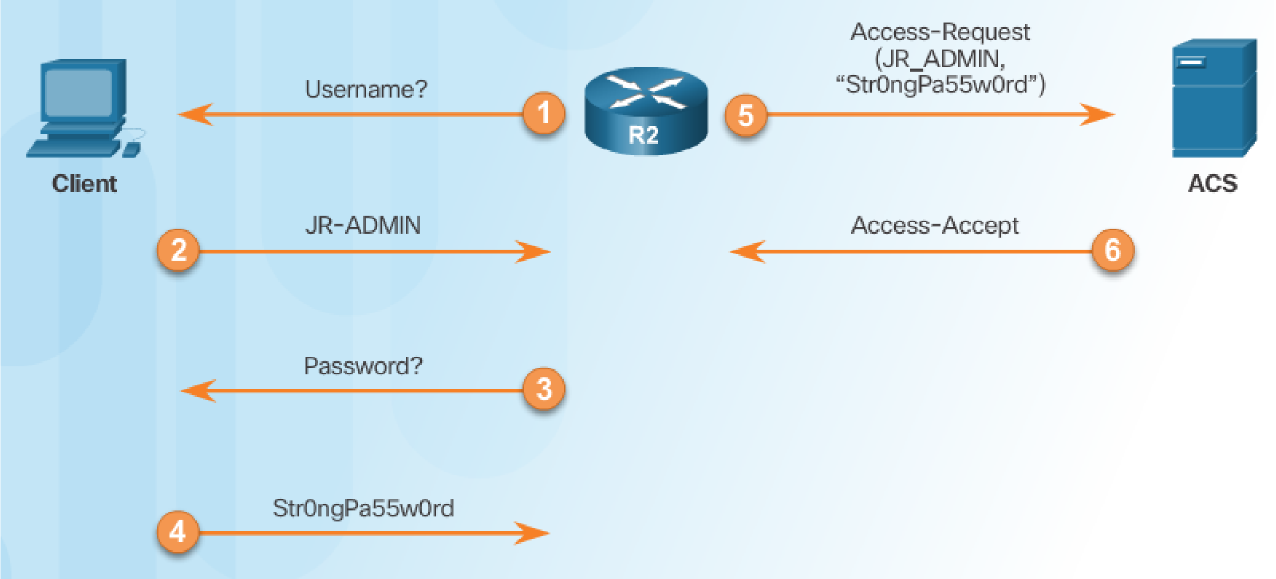
- *Note*. Next-generation AAA protocol alternative to RADIUS is the DIAMETER AAA
  - Uses SCTP and TCP instead of UDP

Server Authentication – communication example

TACACS+ Authentication Process

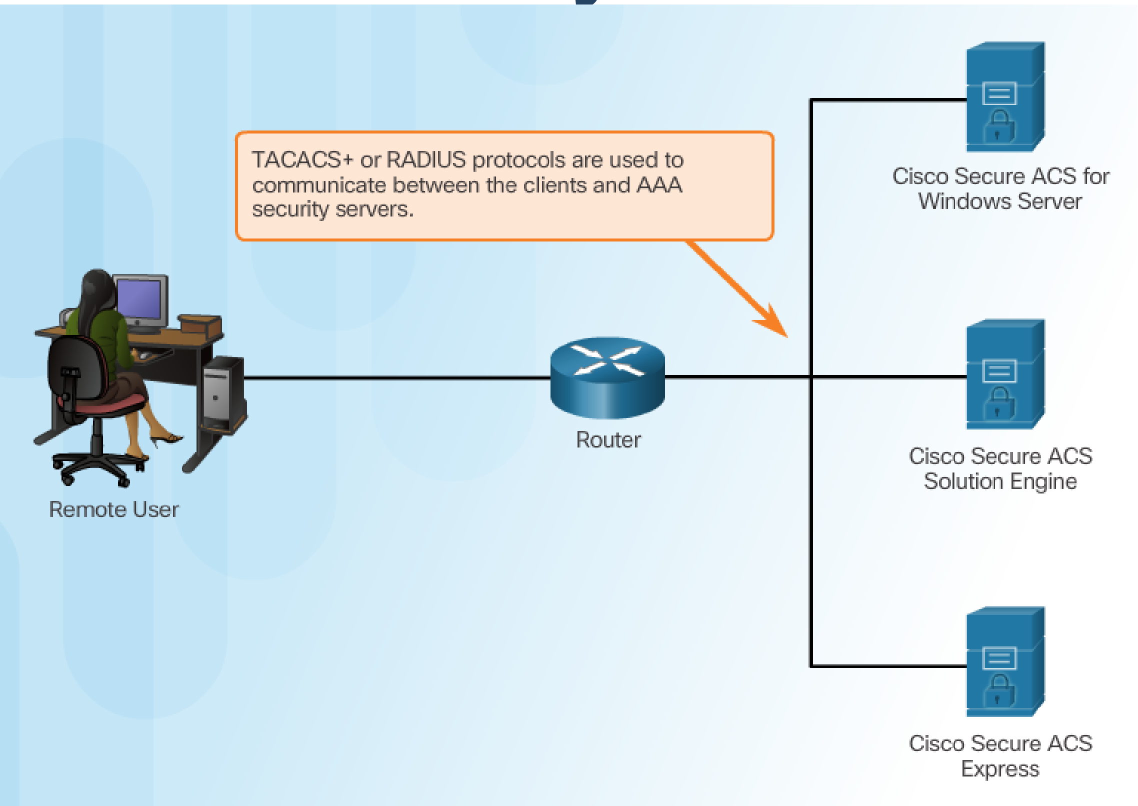


RADIUS Authentication Process



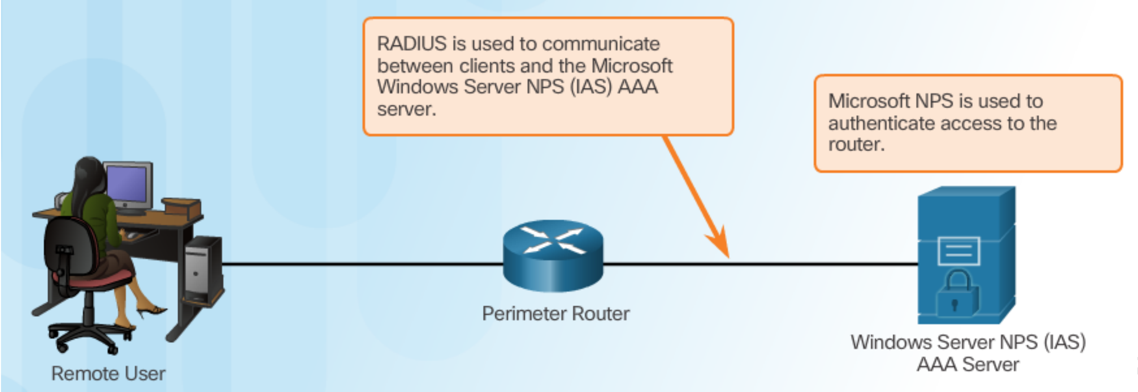
Introducing Cisco Secure Access Control System

- Cisco Secure Access Control System (ACS) for Windows
  - Centralized AAA/policy based solution
  - Includes high-performance access control servers
    - and supports distributed architecture
  - Supports both TACACS+ and RADIUS protocols
  - Supports IPv4/IPv6
  - Provides lightweight web-based GUI
  - Integratable with
    - Windows Active Directory
    - LDAP



TACACS+ or RADIUS protocols are used to communicate between the clients and AAA security servers.

Remote User
Router
Cisco Secure ACS for Windows Server
Cisco Secure ACS Solution Engine
Cisco Secure ACS Express

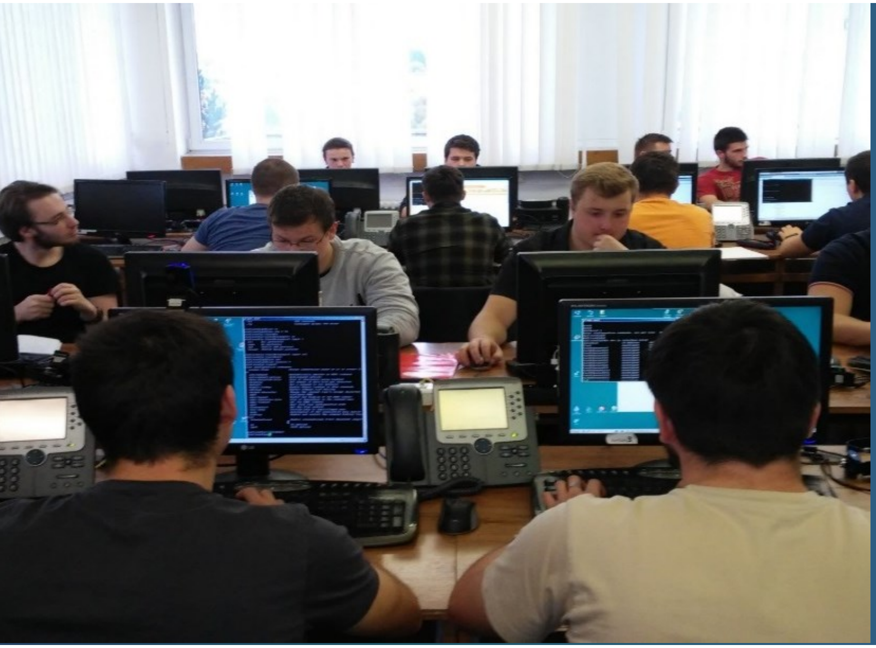


RADIUS is used to communicate between clients and the Microsoft Windows Server NPS (IAS) AAA server.

Microsoft NPS is used to authenticate access to the router.

AAA integration – other sources

- AAA may utilize also other sources
  - Windows AD server
    - using RADIUS, known before as **Internet Authentication Service (IAS)**
    - From Windows Server 2008 renamed to **Network Policy Server (NPS)**
  - Cisco Identity Services Engine (ISE)
    - Cisco identity and access control policy platform (NAC – Network Access Control)
      - control access to devices
      - establish user identity, location, and access history
      - assign services based on the assigned user role, group, and associated policy (job role, location, device type, etc.)
      - grant authenticated users access to specific segments of the network, or specific applications and services, or both
    - Used for BYOD and policy component for Cisco TrustSec arch
    - Features
      - Device profiling
      - Posture assessment
      - Guest management
      - AAA



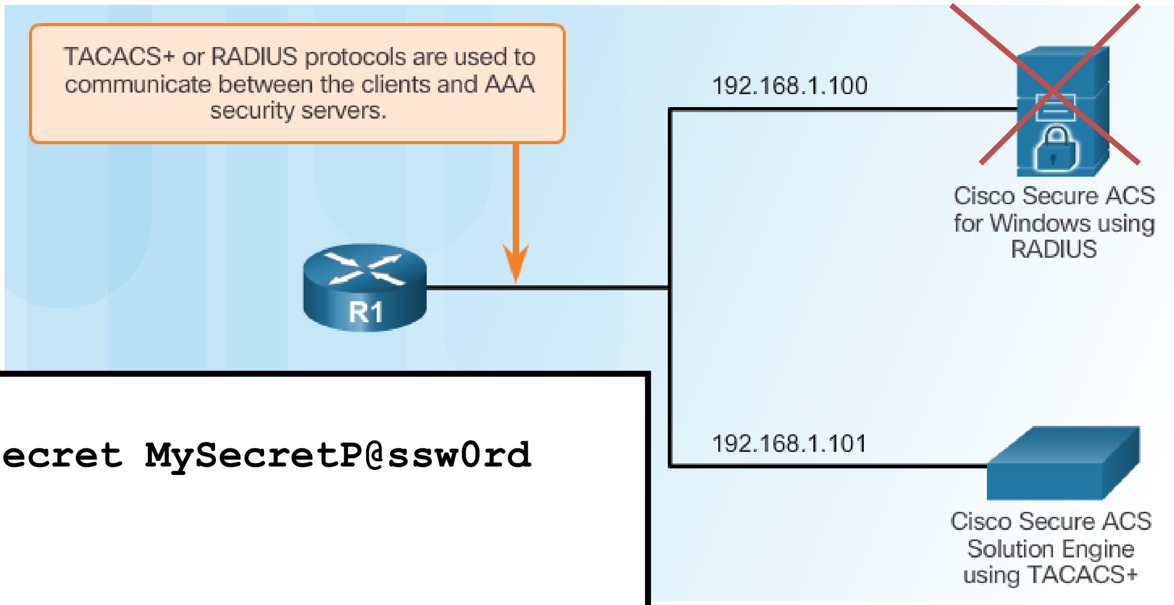
Configuring Server-Based Authentication with CLI

Steps for Configuring Server-Based AAA Authentication with CLI

1. Define sources of authentication - Define AAA server
   - Specify the IP address/es of the ACS server.
   - Configure the secret key
2. Enable AAA
3. Define the list of authentication methods (databases) that will be tried:
   - Configure authentication to use either the RADIUS or TACACS+ server.
4. Apply authentication methods to con / vty / aux and verify

Configuring authentication with one TACACS+ Server

Server-Based AAA Reference Topology

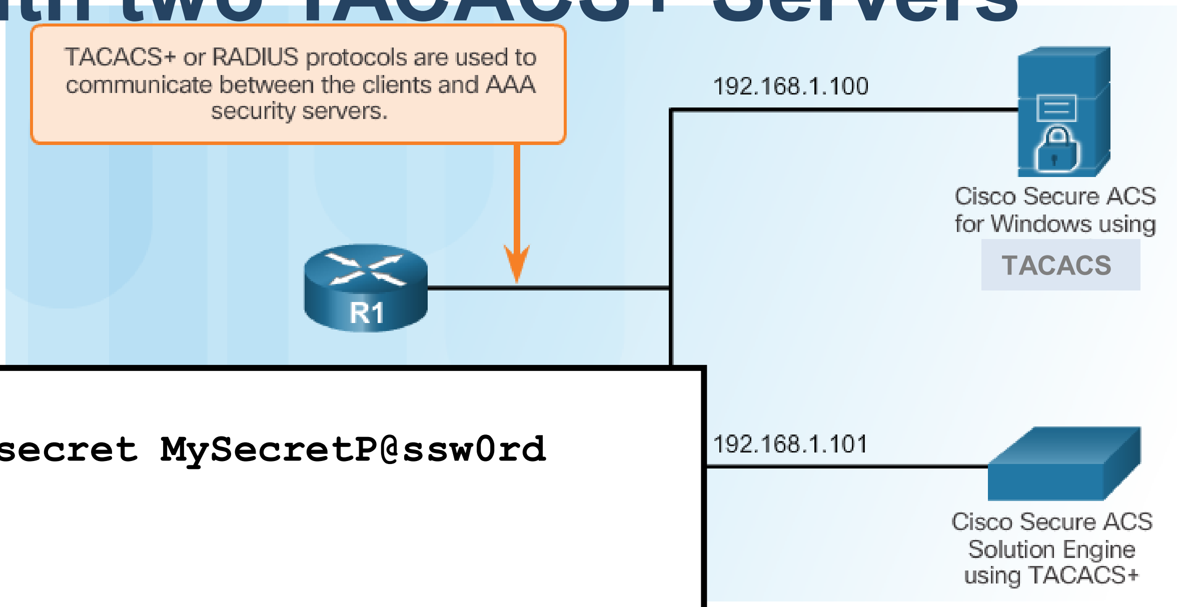

TACACS+ or RADIUS protocols are used to communicate between the clients and AAA security servers.

192.168.1.100
Cisco Secure ACS for Windows using RADIUS
R1
192.168.1.101
Cisco Secure ACS Solution Engine using TACACS+

```
Router(config)# aaa new-model
Router(config)# username JR-ADMIN algorithm-type scrypt secret MySecretP@ssw0rd
Router(config)# tacacs server SERVER-2
! Cmd allows to modify port too
Router(config-radius-server)# address ipv4 192.168.1.101
! Keep TCP connection open for the life of the session,
! otherwise it is opened/closed per each session
Router(config-radius-server)# single-connection
! Specify encryption key
Router(config-radius-server)# key TACACS-pa55w0rd
Router(config-radius-server)# exit
! Modify default database/behavior, usernames are case sensitive
! Router(config)# aaa authentication login default group tacacs+ local-case
!  Or use your own DB name
Router(config)# aaa authentication login MYAUTH group tacacs+ local-case
Router(config)# line vty 0 15
Router(config-line)# login authentication MYAUTH
```

Configuring authentication with two TACACS+ Servers

Server-Based AAA
Reference Topology

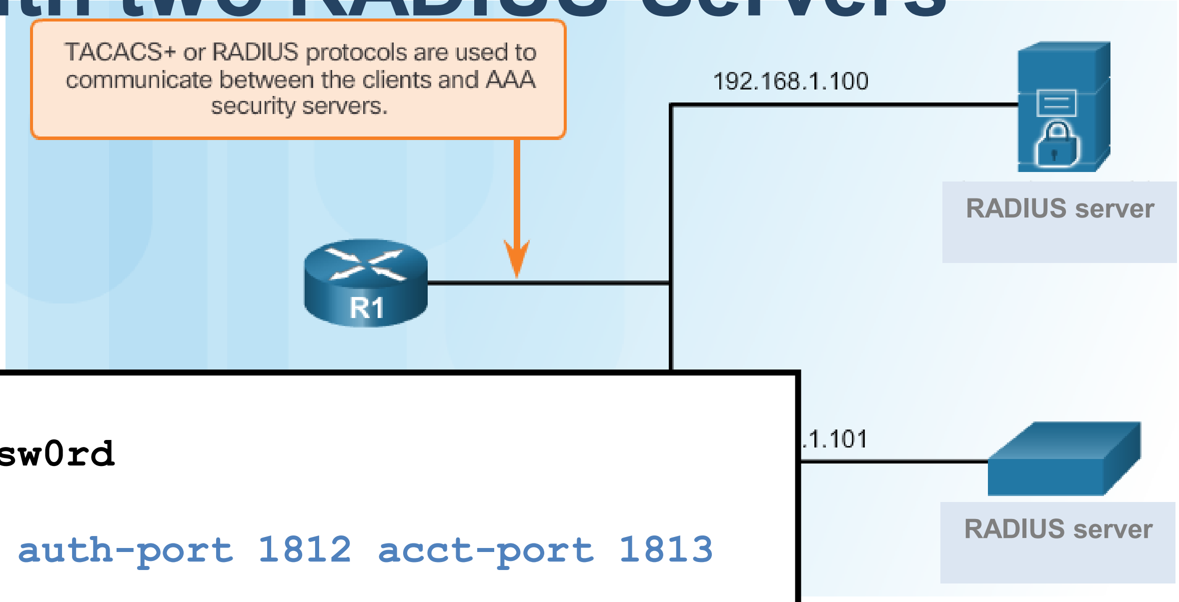

TACACS+ or RADIUS protocols are used to communicate between the clients and AAA security servers.

R1
192.168.1.100
Cisco Secure ACS for Windows using
TACACS
192.168.1.101
Cisco Secure ACS Solution Engine using TACACS+

```
Router(config)# aaa new-model
Router(config)# username JR-ADMIN algorithm-type scrypt secret MySecretP@ssw0rd
Router(config)# tacacs server SERVER-T1
Router(config-radius-server)# address ipv4 192.168.1.100
Router(config-radius-server)# key TACACS-pa55w0rd
Router(config-radius-server)# exit
Router(config)# tacacs server SERVER-T2
Router(config-radius-server)# address ipv4 192.168.1.101
Router(config-radius-server)# key TACACS-pa55w0rd
Router(config-radius-server)# exit
Router(config)# aaa group server tacacs+ TACACS-SERVERS
Router(config-sg)# server name SERVER-T1
Router(config-sg)# server name SERVER-T2
Router(config-sg)# exit
Router(config)# aaa authentication login MY_TACAC_AUTH group TACACS-SERVERS local-
case
Router(config)# line vty 0 15
Router(config-line)# login authentication MY_TACAC_AUTH
```

Configuring authentication with two RADIUS Servers

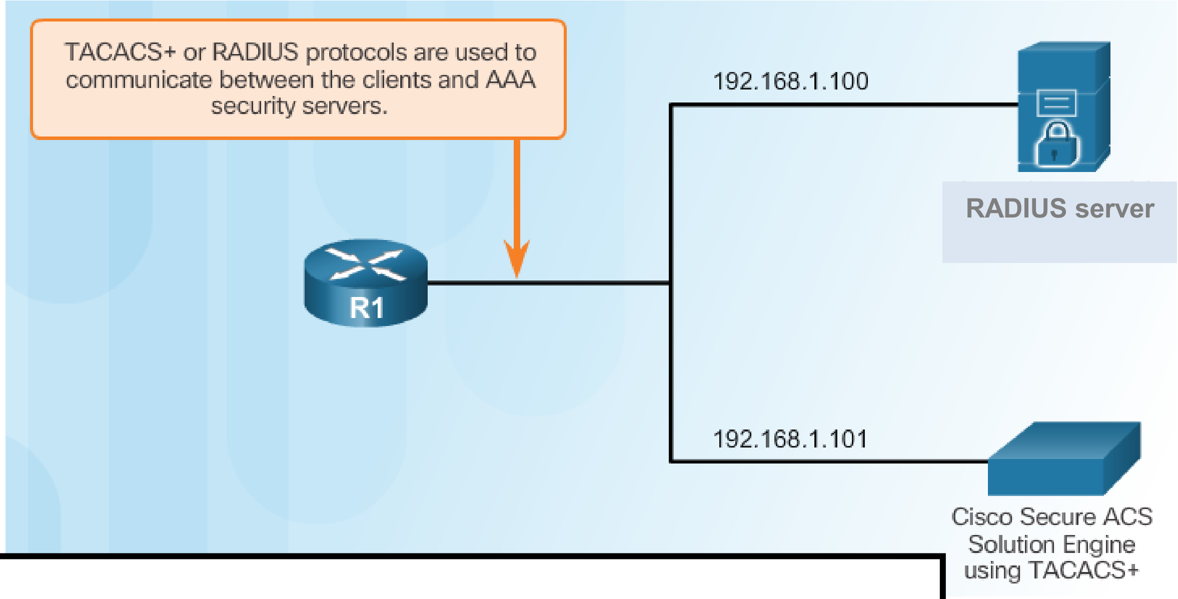
Server-Based AAA
Reference Topology


TACACS+ or RADIUS protocols are used to communicate between the clients and AAA security servers.
192.168.1.100
RADIUS server
R1
.1.101
RADIUS server

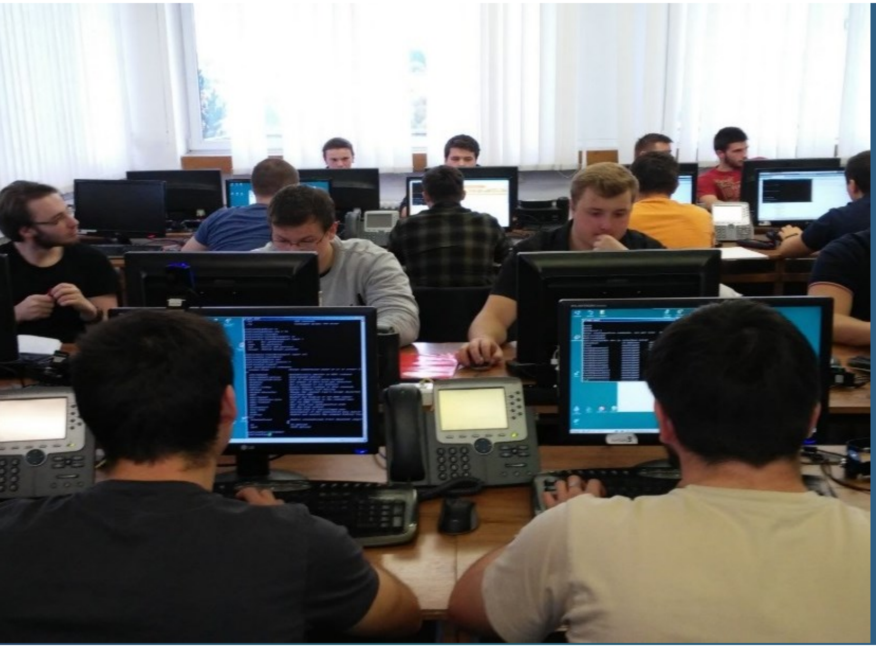
```
Router(config)# aaa new-model
Router(config)# username lastresort password MySecretP@ssw0rd
Router(config)# radius server SERVER-R1
Router(config-radius-server)# address ipv4 192.168.1.100 auth-port 1812 acct-port 1813
Router(config-radius-server)# key RADIUS-pa55w0rd
Router(config-radius-server)# exit
Router(config)# radius server SERVER-R2
Router(config-radius-server)# address ipv4 192.168.1.101 auth-port 1812 acct-port 1813
Router(config-radius-server)# key RADIUS-pa55w0rd
Router(config-radius-server)# exit
Router(config)# aaa group server radius RADIUS-SERVERS
Router(config-sg)# server name SERVER-R1
Router(config-sg)# server name SERVER-R2
Router(config-sg)# exit
Router(config)# aaa authentication login MY_RADIUS_AUTH group RADIUS-SERVERS local-case
Router(config)# aaa authentication enable MY_RADIUS_AUTH group RADIUS-SERVERS local-case
Router(config)# line vty 0 15
Router(config-line)# login authentication MY_RADIUS_AUTH
```

Configuring authentication with TACACS+/RADIUS Servers

Server-Based AAA Reference Topology


TACACS+ or RADIUS protocols are used to communicate between the clients and AAA security servers.
192.168.1.100
RADIUS server
R1
192.168.1.101
Cisco Secure ACS Solution Engine using TACACS+

```
Router(config)# aaa new-model
Router(config)# username lastresort password MySecretP@ssw0rd
Router(config)# radius server SERVER-R
Router(config-radius-server)# address ipv4 192.168.1.100 auth-port 1812 acct-port 1813
Router(config-radius-server)# key RADIUS-pa55w0rd
Router(config-radius-server)# exit
Router(config)# tacacs server SERVER-T
Router(config-radius-server)# address ipv4 192.168.1.101
Router(config-radius-server)# single-connection
Router(config-radius-server)# key TACACS-pa55w0rd
Router(config-radius-server)# exit
Router(config)# aaa authentication login MY_AUTH_RAD+TAC group radius group tacacs+ local-case
Router(config)# line vty 0 15
Router(config-line)# login authentication MY_AUTH_RAD+TAC
```



Troubleshooting Server-Based AAA Authentication

AAA debugging

- For debugging use

```
debug aaa authentication

no debug aaa authentication
```

```
Router# debug aaa authentication
…
…
 6:50:20: AAA/AUTHEN (50996740): Method=TACACS+
 6:50:20: TAC+: send AUTHEN/CONT packet
 6:50:20: TAC+ (50996740): received authen response status = PASS
 6:50:20: AAA/AUTHEN (50996740): status = PASS
```

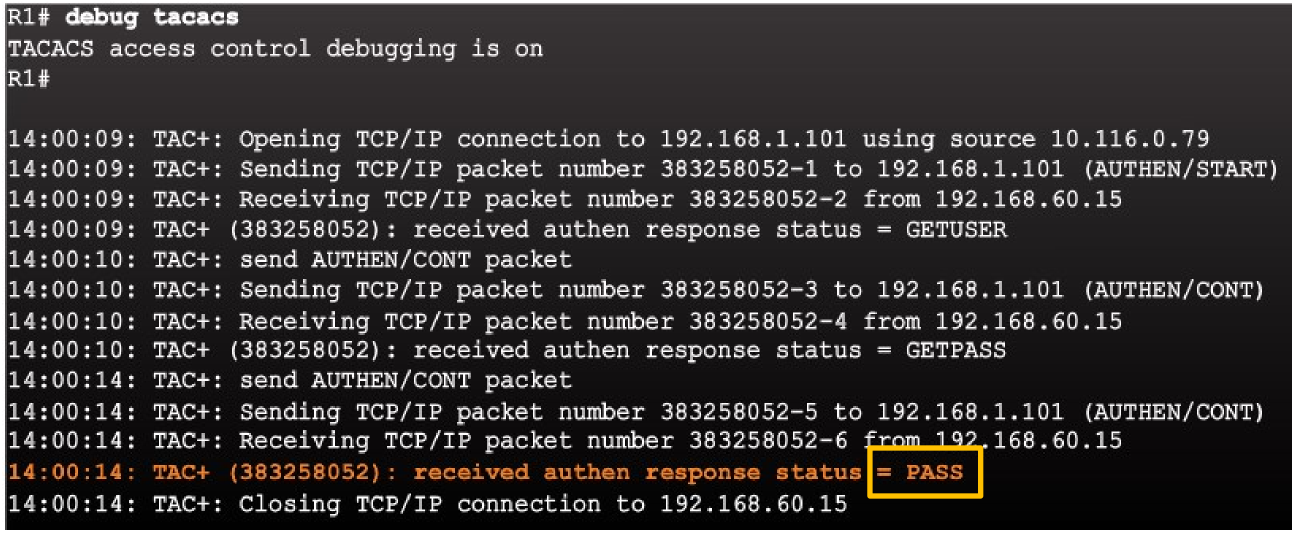
AAA debugging (cont.)

```
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
  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>
```

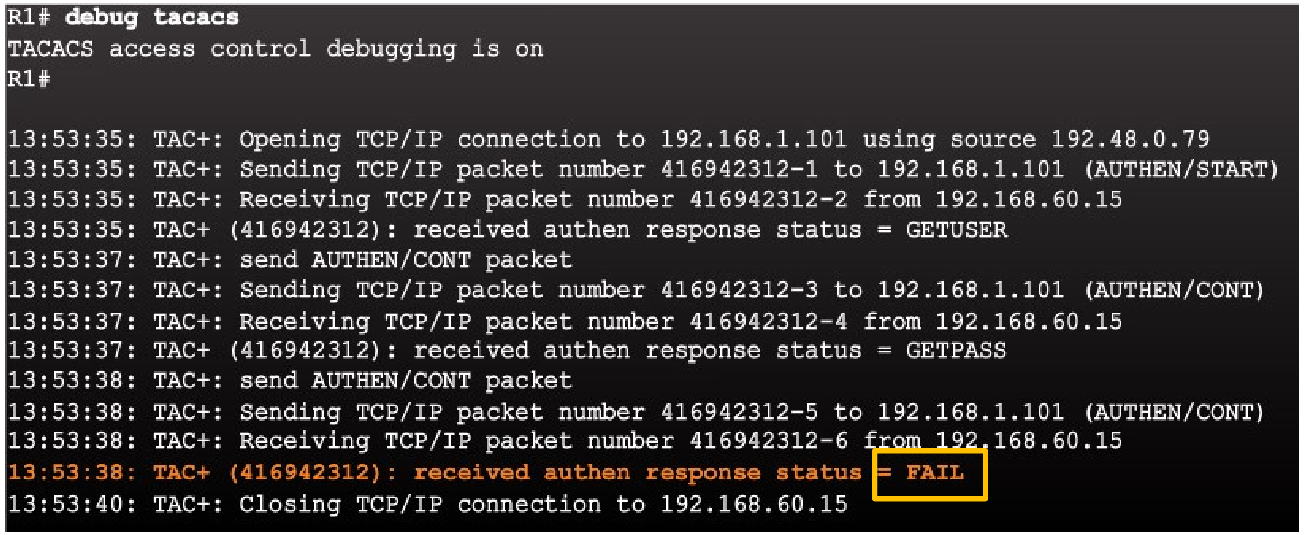
Debugging TACACS+ and RADIUS (Cont.)

AAA Server-Based
Authentication Success

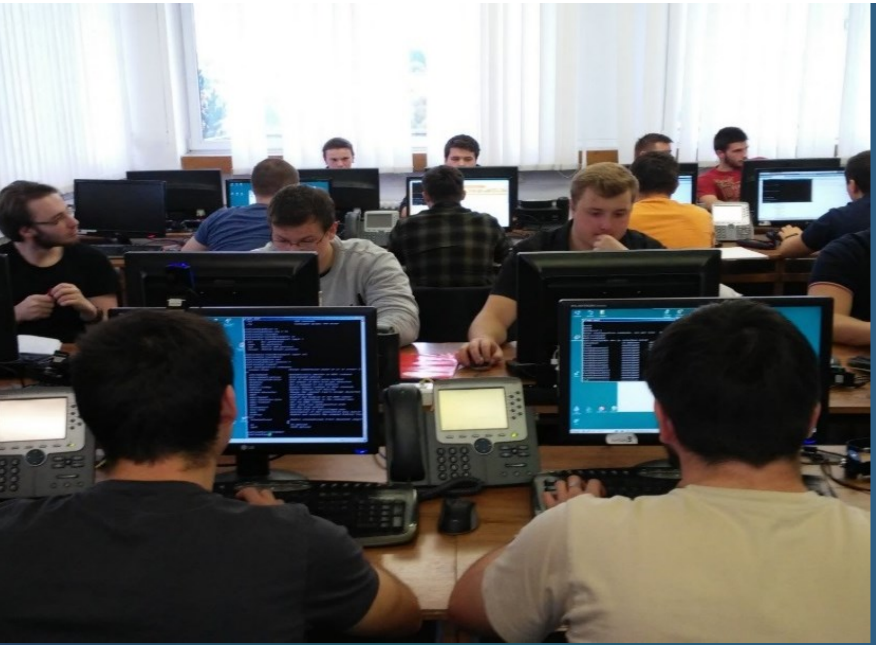


```
R1# debug tacacs
TACACS access control debugging is on
R1#

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
```

AAA Server-Based
Authentication Failure



```
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
```



Configuring Server-Based AAA Authorization

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.

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/programs/services/commands on the network.

TACACS+ vs. RADIUS

- **TACACS+**
  - separates authentication from authorization
  - establishes a new TCP session for every authorization reques
- **RADIUS** does **not** separate authentication from authorization

Configuring AAA authorization – different steps only

- 1) Define sources – list of authorization servers per service

```
Router(config)# aaa authorization {commands | config-commands | configuration | exec
  | network | reverse-access} {default | LIST-NAME} method1 [method2 ...]
```

  - commands: The server must return permission to use any device command at any privilege level.
  - config-commands: The server must return permission to use any device configuration command.
  - configuration: The server must return permission to *enter* the device configuration mode.
  - exec: The server must return permission for the user to *run a device EXEC session*.
    The server also can return the privilege level for the user so that the user immediately can be put into privileged EXEC (enable) mode without having to type in the enable command.
  - network: The server must return permission to use network-related services (SLIP, PPP, ARAP).
  - reverse-access: The server must return permission for the user to access a reverse Telnet session on the device.
- 2) Activate support for the new AAA:

```
Router(config)# aaa new-model
```

- 3) Apply authorization methods to the line and verify

```
Router(config-line)# authorization {commands level | exec | reverse-access} {default
  | LIST-NAME}
```

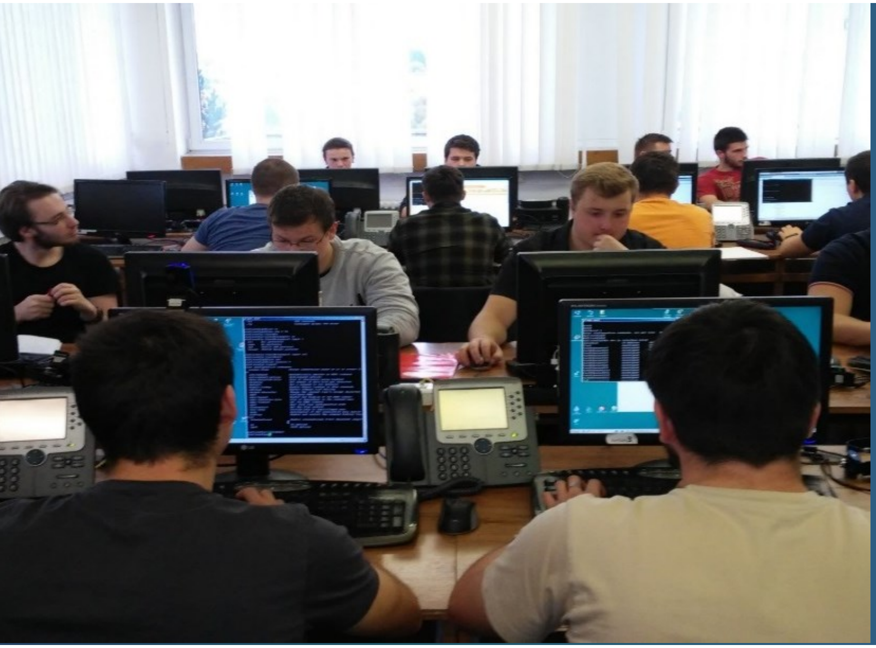
  - Network: For network services such as PPP
  - Exec: For starting an exec (shell)
  - Commands *level*: For exec (shell) commands

Example

Configuring authorization

```
username JR-ADMIN algorithm-type scrypt secret G33dP@ssw4rd
username ADMIN algorithm-type scrypt secret T4t1lBr5t@lP@ssw4rdWrtYU!H3LL&:-)
!
aaa new-model
!
! Use a default schema, case sensitive for running EXEC
aaa authorization exec default local-case
!
! Use own DB name with tacacs+
! tacacs server SERVER-T1
!       address ipv4 192.168.1.100
!       key TACACS-pa55w0rd

! aaa authorization network AUTHOR_NET_T+L group tacacs+ local
!
! Apply for example for vty line
line vty 0 15
  authorization exec default
```

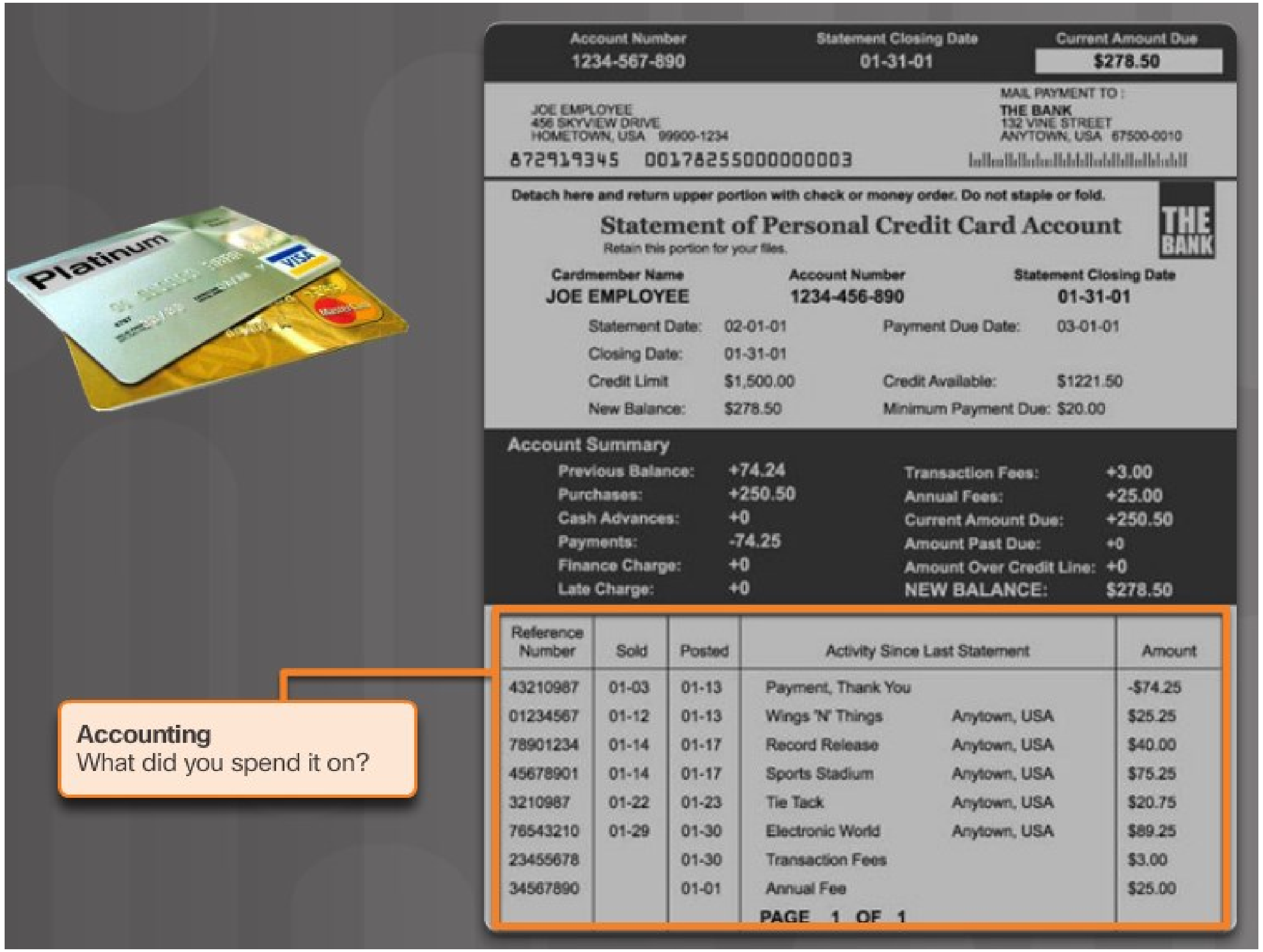
- Note:
  - An administrator must create a user with full access rights before authorization is enabled,
  - do it immediately locks the administrator out of the system the moment the aaa authorization command is entered



Configuring Server-Based AAA Accounting

Introduction to Server-Based AAA Accounting

- Accounting
  - Keep tracks of resource usage
    - For example
      - who call where and how long
      - Who is logged on a console and what he did
      - Track list of config changes
- Cisco uses the Cisco Secure ACS


Platinum
VISA

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

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA 99900-1234

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

872919345 0017825500000003

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

THE BANK

Statement of Personal Credit Card Account

Retain this portion for your files.

Cardmember Name	Account Number	Statement Closing Date
JOE EMPLOYEE	1234-456-890	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	NEW BALANCE:	$278.50

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		

Accounting
What did you spend it on?

Configuring AAA accounting - steps

- 1) Define what will be accounted and account triggers

```
Router(config)# aaa accounting {system | exec | commands level} {default | list-name}
  {start-stop | stop-only | wait-start | none} method1 [method2 ...]
```

  - Network: Runs accounting for all network-related service requests, including PPP
  - Exec: Runs accounting for the EXEC shell session (time, IP address, …)
  - Connection: Runs accounting on all outbound connections such as SSH and Telnet.
  - Commands *level*: Accounts the execution of level commands, user name including
  - Triggers:
    - Start-stop: Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process.
    - Stop-only: Sends a "stop" accounting record for all cases including authentication failures.
    - None: Disables accounting services on a line or interface.
- 2) Activate support for the new AAA:

```
Router(config)# aaa new-model
```

- 3) Apply accounting methods and verify

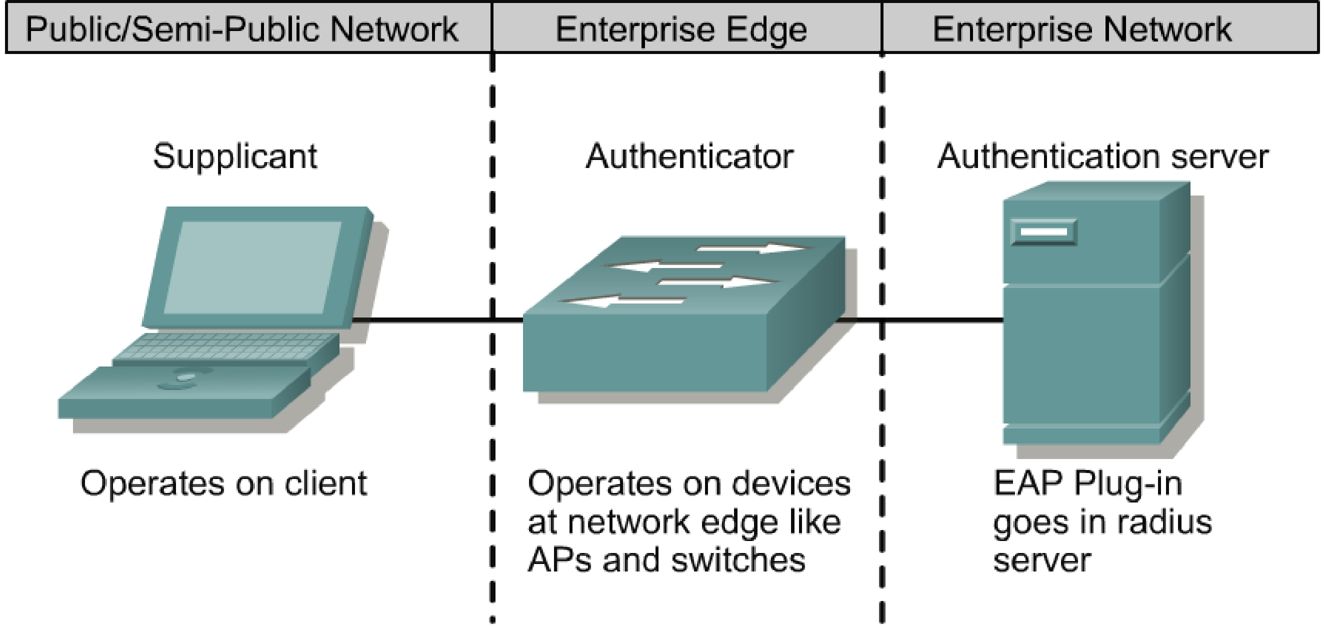
```
Router(config-line)# accounting {commands level | connection | exec} {default | list-
  name}
```

Configuring AAA with accouting

```
username JR-ADMIN algorithm-type scrypt secret G33dP@ssw4rd
username ADMIN algorithm-type scrypt secret T4t1lBr5t@lP@ssw4rdWrtYU!H3LL&:-)
!
aaa new-model
!
aaa authentication login default local-case
aaa authorization exec default local-case
aaa authorization network AUTHOR_NET_T+L group tacas+ local
!
! Define accounting
aaa accouting exec default start-stop local-case
aaa accouting network default start-stop group tacacs+
! apply
line vty 0 15
  authentication login default
  authorization exec default
  accouting exec default
```

802.1X Authentication

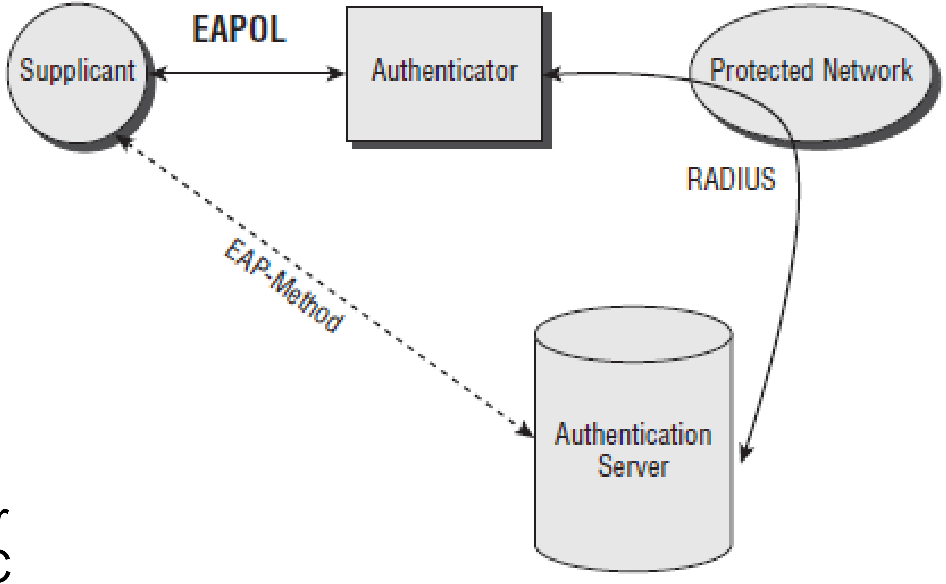
802.1X authentication

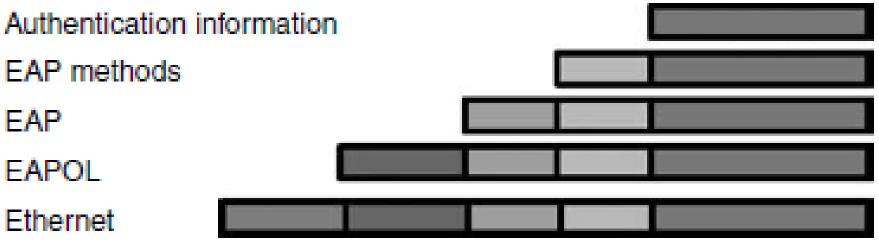

Public/Semi-Public Network
Enterprise Edge
Enterprise Network
Supplicant
Authenticator
Authentication server
Operates on client
Operates on devices at network edge like APs and switches
EAP Plug-in goes in radius server

- 802.1X defines a port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN
  - Authentication server authenticates each workstation that is connected to a switch port before making available any services
  - A switch port is unlocked only after successful logon (default state is unauthorized)
    - In the meantime, only STP, CDP and EAPOL are allowed
  - If not
    - port remains unauthorized or may move in a quarantine or guest VLAN or reauthorize

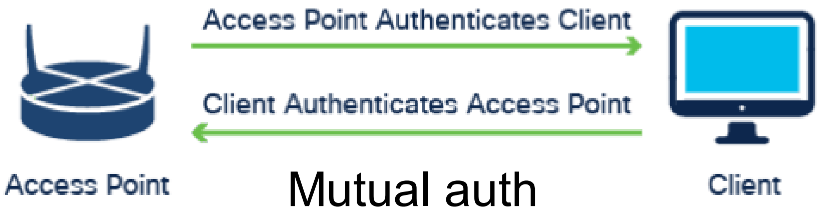
802.1X authentication components

- 802.1X Authentication uses several supporting components and protocols:
  - **Supplicant (Client):** Software client on PC, responsible for uploading client’ authentication data
  - **Authenticator**: The device, to which PC connects and which requires the client to authenticate correctly (switch, AP)
  - **Authentication Server:** Contains user information database. Confirms client identity (TACACS / Radius server)
  - **Extensible Authentication Protocol (EAP**): A generic protocol for transmitting authentication information over a link, specified in RFC 3748
  - **EAPOL (EAP over LAN):** adaptation of EAP protocol for communication over LAN
  - **RADIUS**: authentication communication protocol used between a Network Access Server (or authenticator) and an authentication server.
    - specified in RFC 2865. RADIUS and EAP cooperation in RFC 3579
  - **802.1X**: IEEE standard for Port-Based Authentication using EAP messages over Ethernet frameworks (EAP over LAN = EAPOL) and RADIUS protocol





Extensible Authentication Protocol


Access Point Authenticates Client
Client Authenticates Access Point
Access Point
Client

Mutual auth

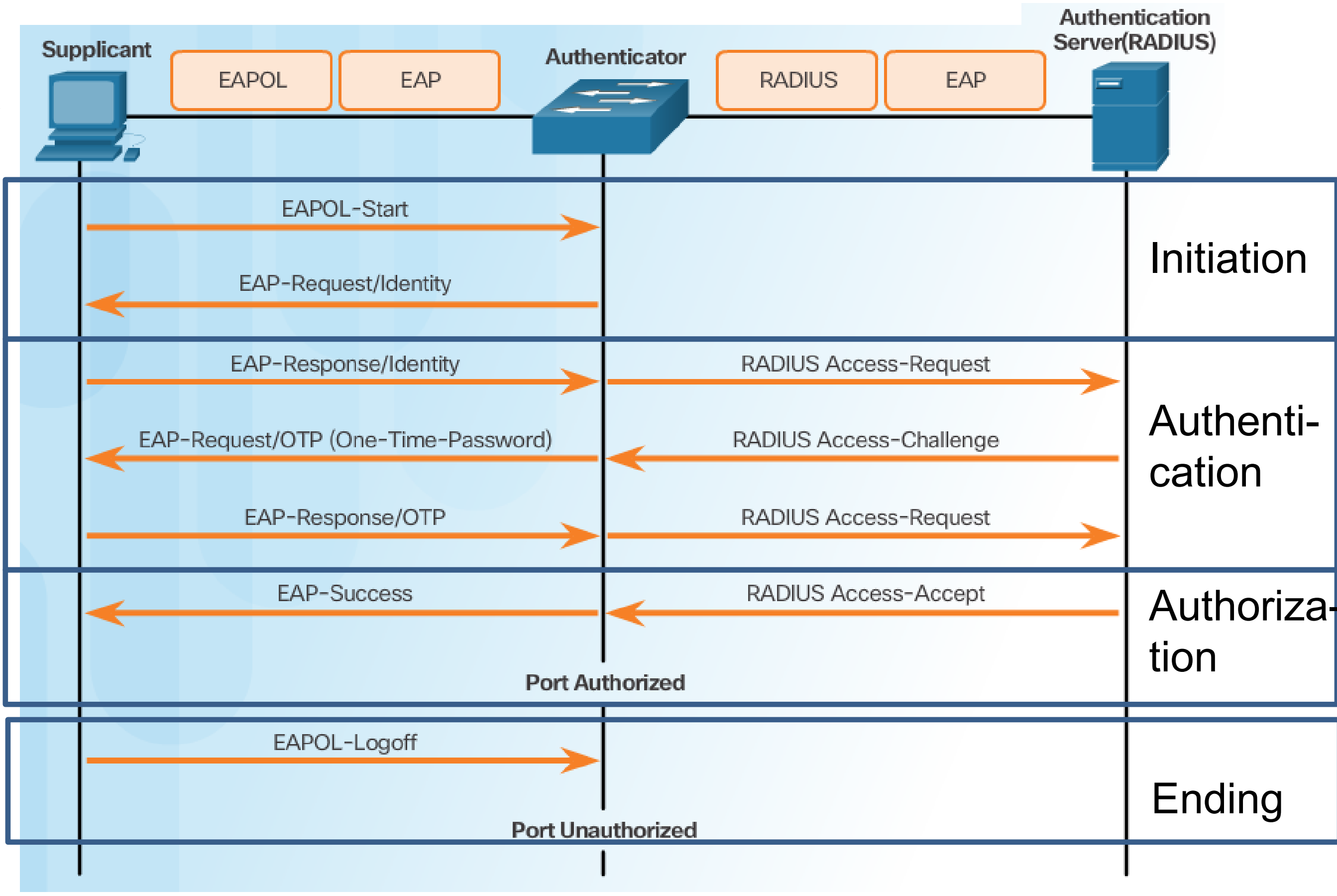
- An authentication framework for wired and wireless networks
- Different methods
  - EAP-TLS
    - Requires Client Certificate: Yes
    - Requires Server Certificate: Yes
    - Easily Deployed: Difficult
    - Security: High
    - Mutual auth (both way): Yes
  - PEAP (Protected EAP)
    - Requires Client Certificate: No
    - Requires Server Certificate: Yes
    - Easily Deployed: Moderate
    - Security: Medium
    - Mutual auth (both way): No

- EAP-TTLS (Tunnelled Transport Layer Security EAP)
  - Requires Client Certificate: No
  - Requires Server Certificate: Yes
  - Easily Deployed: Moderate
  - Security: Medium
  - Mutual auth (both way): No
- EAP-FAST
  - Requires Client Certificate: No
  - Requires Server Certificate: No
  - Easily Deployed: Easy
  - Security: Medium
  - Mutual auth (both way): No

Security Using 802.1X Port-Based Authentication

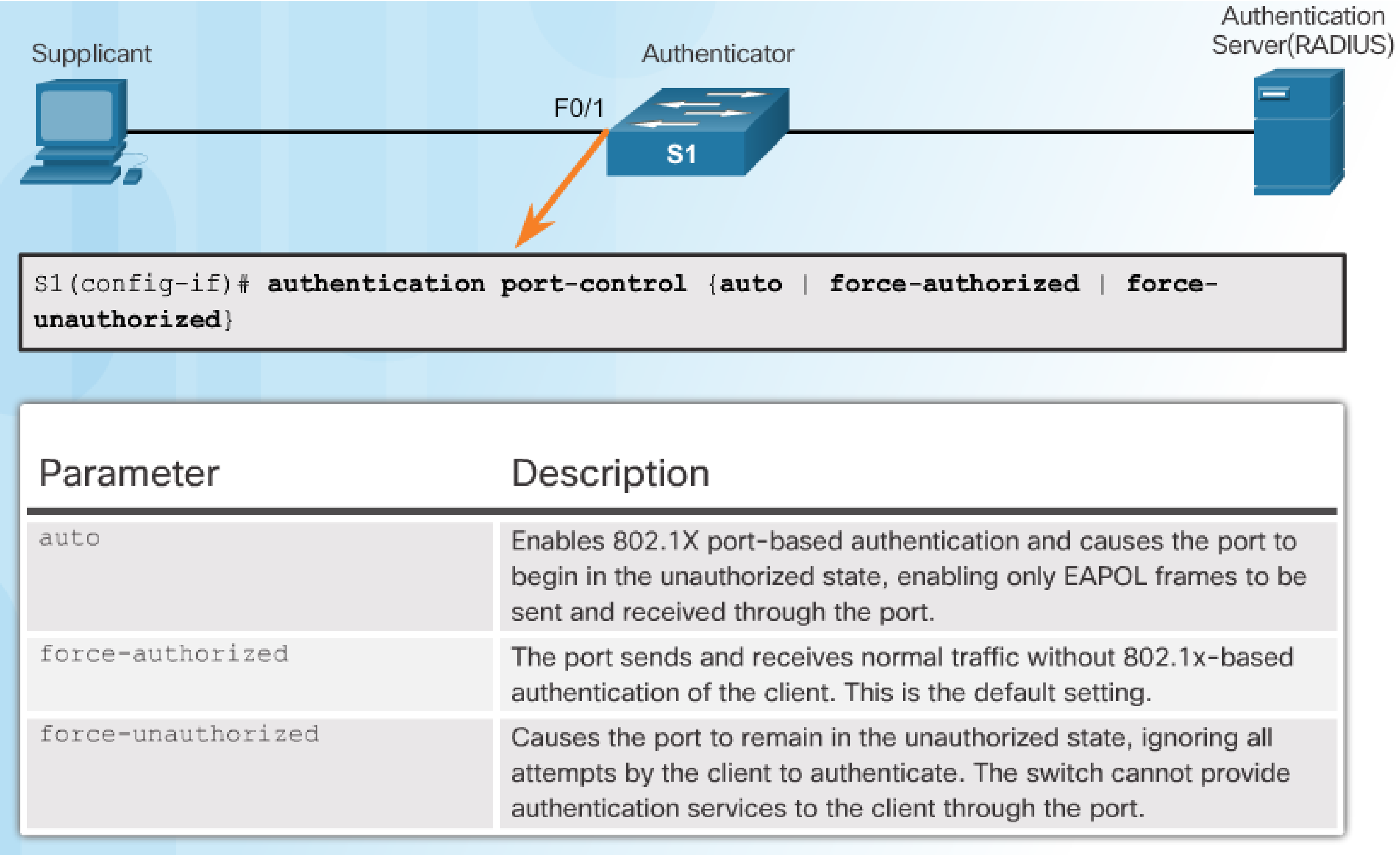
- Client sends the EAPOL-Start message
  - Or just responds to the EAP-request / identity prompt receiver from an authenticator
- Switch from the client requires its primary identification data
  - Only EAPOL messages are allowed through the port
- Switch will re-encapsulates EAP response into a RADIUS message and sent it to the server
- RADIUS server may authenticate immediately
  - or the exchange of several "call-response“ messages will follow
- Once successfully authenticated, RADIUS will send the Access-Accept message
- Switch unlocks the port and informs the client about success

802.1X Message Exchange



802.1X Port Authorization State

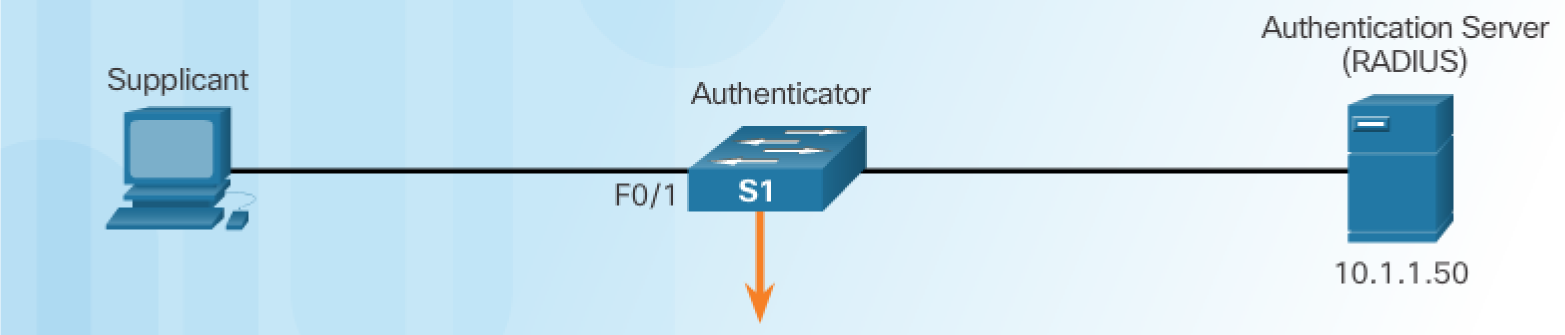
Command Syntax for dot1x port-control



```
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.

Configuring 802.1X – an example



```
aaa new-model
!
radius-server SERVER-R
   address ipv4 10.1.1.50 auth-port 1812 acct-port 1813
   key HESLO
!
aaa authentication dot1x default group radius
! Nasledujúci riadok netreba, ak nechceme dynamicky prideľovať VLAN
aaa authorization network default group radius
!
dot1x system-auth-control
!
interface FastEthernet 0/1
 switchport mode access
! Zapni dot1x na porte
 authentication port-control auto
 dot1x pae authenticator
```

UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

KATEDRA INFORMAČNÝCH SIETÍ * FAKULTA RIADENIA A INFORMATIKY ŽU *

CISCO
Networking Academy

MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Aktualizované v rámci projektu KEGA 026TUKE-4/2021