CCNA Security

Chapter Three
Authentication, Authorization, and Accounting
AAA Access Security

**Authentication**
Who are you?

**Authorization**
which resources the user is allowed to access and which operations the user is allowed to perform?

**Accounting**
What did you spend it on?
Authentication – Password-Only

Password-Only Method

- Uses a login and password combination on access lines
- Easiest to implement, but most unsecure method
- Vulnerable to brute-force attacks
- Provides no accountability

User Access Verification
Password: cisco
Password: cisco1
Password: cisco12
% Bad passwords

R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
Authentication – Local Database

- Creates individual user account/password on each device
- Provides accountability
- User accounts must be configured locally on each device
- Provides no fallback authentication method

```
R1(config)# username Admin secret Strong5rPa55w0rd
R1(config)# line vty 0 4
R1(config-line)# login local
```

User Access Verification
Username: Admin
Password: cisco1
% Login invalid

Username: Admin
Password: cisco12
% Login invalid

Local Database Method
Local Versus Remote Access

**Local Access**

- LAN 1
- R1
- Internet
- Console Port
- Administrator

Requiring a direct connection to a console port using a computer running terminal emulation software.

**Remote Access**

- Internet
- R1
- Firewall
- R2
- LAN 2
- LAN 3
- Management LAN
- Administration Host
- Logging Host

Uses Telnet, SSH, HTTP or SNMP connections to the router from a computer.
To increase the security of passwords, use additional configuration parameters:

- Minimum password lengths should be enforced
- Unattended connections should be disabled
- All passwords in the configuration file should be encrypted
An acceptable password length is 10 or more characters

Complex passwords include a mix of upper and lowercase letters, numbers, symbols and spaces.

Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, or biographical information.

Deliberately misspell a password (Security = 5ecur1ty)

Change passwords often

Do not write passwords down and leave them in obvious places.
Access Port Passwords

Command to restrict access to privileged EXEC mode

R1(config)# enable secret cisco

Commands to establish a login password on incoming Telnet sessions

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

Commands to establish a login password for dial-up modem connections

R1(config)# line aux 0
R1(config-line)# password cisco
R1(config-line)# login

R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login

Commands to establish a login password on the console line

PC with Terminal Emulation Software

Router

Vty

Aux

Con

Modem

PSTN
username  name  secret  {[0]password|5encrypted-secret}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>name</strong></td>
<td>This parameter specifies the username.</td>
</tr>
<tr>
<td><strong>0</strong></td>
<td>(Optional) This option indicates that the plaintext password is to be hashed by the router using MD5.</td>
</tr>
<tr>
<td><strong>password</strong></td>
<td>This parameter is the plaintext password to be hashed using MD5.</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>This parameter indicates that the encrypted-secret password was hashed using MD5.</td>
</tr>
<tr>
<td><strong>encrypted-secret</strong></td>
<td>This parameter is the MD5 encrypted-secret password that is stored as the encrypted user password.</td>
</tr>
</tbody>
</table>
Self-Contained AAA Authentication

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

- Used for small networks
- Stores usernames and passwords locally in the Cisco router
Server-Based AAA Authentication

- Uses an external database server
  - Cisco Secure Access Control Server (ACS) for Windows Server
  - Cisco Secure ACS Solution Engine
  - Cisco Secure ACS Express
- More appropriate if there are multiple routers

Server-Based AAA
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.
AAA Authorization

- Typically implemented using an AAA server-based solution
- Uses a set of attributes that describes user access to the network

1. When a user has been authenticated, a session is established with an 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.
AAA Accounting

- Implemented using an AAA server-based solution
- Keeps a detailed log of what an authenticated user does on a device

1. When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
2. When the user finishes, a stop message is recorded ending the accounting process.
Local AAA Authentication Commands

To authenticate administrator access (character mode access)

1. Add usernames and passwords to the local router database
2. Enable AAA globally
3. Configure AAA parameters on the router
4. Confirm and troubleshoot the AAA configuration

```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case
R1(config)# aaa local authentication attempts max-fail 10
```
AAA Authentication Command Elements

```
router(config)#

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in</td>
</tr>
<tr>
<td>list-name</td>
<td>Character string used to name the list of authentication methods activated when a user logs in</td>
</tr>
<tr>
<td>password-expiry</td>
<td>Enables password aging on a local authentication list.</td>
</tr>
<tr>
<td><code>method1</code></td>
<td>Identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods.</td>
</tr>
</tbody>
</table>
## Method Type Keywords

<table>
<thead>
<tr>
<th>Keywords</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication. This keyword cannot be used.</td>
</tr>
<tr>
<td>krb5</td>
<td>Uses Kerberos 5 for authentication.</td>
</tr>
<tr>
<td>krb5-telnet</td>
<td>Uses Kerberos 5 telnet authentication protocol when using Telnet to connect to the router.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>local-case</td>
<td>Uses case-sensitive local username authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>cache <em>group-name</em></td>
<td>Uses a cache server group for authentication.</td>
</tr>
<tr>
<td>group radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>group tacacs+</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
<tr>
<td>group <em>group-name</em></td>
<td>Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <strong>aaa group server radius</strong> or <strong>aaa group server tacacs+</strong> command.</td>
</tr>
</tbody>
</table>
router(config)\#

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

R1# show aaa local user lockout

<table>
<thead>
<tr>
<th>Local-user</th>
<th>Lock time</th>
</tr>
</thead>
<tbody>
<tr>
<td>JR-ADMIN</td>
<td>04:28:49 UTC Sat Dec 27 2008</td>
</tr>
</tbody>
</table>

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
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case enable
R1(config)# aaa authentication login TELNET-LOGIN local-case
R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET-LOGIN
Troubleshooting

- The `debug aaa` Command
- Sample Output
### The debug aaa Command

```
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

R1# debug aaa
```
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
Local Versus Server-Based Authentication

Local Authentication

1. The user establishes a connection with the router.
2. The router prompts the user for a username and password authenticating the user using a local database.

Server-Based Authentication

1. The user establishes a connection with the router.
2. The router prompts the user for a username and password.
3. The router passes the username and password to the Cisco Secure ACS (server or engine).
4. The Cisco Secure ACS authenticates the user. The user is authorized to access the router (administrative access) or the network based on information found in the Cisco Secure ACS database.
TACACS+ or RADIUS protocols are used to communicate between the clients and AAA security servers.
# TACACS+/RADIUS Comparison

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

- Provides separate AAA services
- Utilizes TCP port 49
RADIUS Authentication Process

- Works in both local and roaming situations
- Uses UDP ports 1645 or 1812 for authentication and UDP ports 1646 or 1813 for accounting
Cisco Secure ACS Benefits

• Extends access security by combining authentication, user access, and administrator access with policy control

• Allows greater flexibility and mobility, increased security, and user-productivity gains

• Enforces a uniform security policy for all users

• Reduces the administrative and management efforts
Advanced Features

• Automatic service monitoring
• Database synchronization and importing of tools for large-scale deployments
• Lightweight Directory Access Protocol (LDAP) user authentication support
• User and administrative access reporting
• Restrictions to network access based on criteria
• User and device group profiles
### Installation Options

#### Cisco Secure ACS for Windows
Cisco Secure ACS for Windows can be installed on:
- Windows 2000 Server with Service Pack 4
- Windows 2000 Advanced Server with Service Pack 4
- Windows Server 2003 Enterprise Edition

#### Cisco Secure ACS Solution Engine
- A highly scalable dedicated platform that serves as a high-performance ACS
- 1RU, rack-mountable
- Preinstalled with a security-hardened Windows software, Cisco Secure ACS software
- Support for more than 350 users

#### Cisco Secure ACS Express 5.0
- Entry-level ACS with simplified feature set
- Support for up to 50 AAA device and up to 350 unique user ID logins in a 24-hour period
• Consider Third-Party Software Requirements
• Verify Network and Port Prerequisites
  - AAA clients must run Cisco IOS Release 11.2 or later.
  - Cisco devices that are not Cisco IOS AAA clients must be configured with TACACS+, RADIUS, or both.
  - Dial-in, VPN, or wireless clients must be able to connect to AAA clients.
  - The computer running ACS must be able to reach all AAA clients using ping.
  - Gateway devices must permit communication over the ports that are needed to support the applicable feature or protocol.
  - A supported web browser must be installed on the computer running ACS.
  - All NICs in the computer running Cisco Secure ACS must be enabled.
• Configure Secure ACS via the HTML interface
Cisco Secure ACS Homepage

- add, delete, modify settings for AAA clients (routers)
- set menu display options for TACACS and RADIUS
- configure database settings
1. Click **Network Configuration** on the navigation bar

2. Click Add Entry

3. Enter the hostname

4. Enter the IP address

5. Enter the secret key

6. Choose the appropriate protocols

7. Make any other necessary selections and click **Submit and Apply**
1. Click the External User Databases button on the navigation bar

2. Click Database Configuration

3. Click Windows Database
1. Click External User Databases on the navigation bar

2. Click Unknown User Policy

3. Place a check in the box

4. Choose the database in from the list and click the right arrow to move it to the Selected list

5. Manipulate the databases to reflect the order in which each will be checked

6. Click Submit
Database group mappings - Control authorizations for users authenticated by the Windows server in one group and those authenticated by the LDAP server in another.

1. Click Group Setup on the navigation bar.

2. Choose the group to edit and click Edit Settings.

3. Click Permit in the Unmatched Cisco IOS commands option.

4. Check the Command check box and select an argument.

5. For the Unlisted Arguments option, click Permit.
1. Globally enable AAA to allow the user of all AAA elements (a prerequisite)

2. Specify the Cisco Secure ACS that will provide AAA services for the network access server

3. Configure the encryption key that will be used to encrypt the data transfer between the network access server and the Cisco Secure ACS

4. Configure the AAA authentication method list
aaa authentication Command

R1(config)# aaa authentication type { default | list-name } method1 ... [method4]

R1(config)# aaa authentication login default ?
   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
   radius Use list of all Radius hosts.
   tacacs+ Use list of all Tacacs+ hosts.

R1(config)# aaa authentication login default group
Sample Configuration

- Multiple RADIUS servers can be identified by entering a radius-server command for each.

- For TACACS+, the single-connection command maintains a single TCP connection for the life of the session.

```plaintext
R1(config)# aaa new-model
R1(config)#
R1(config)# radius-server host 192.168.1.100
R1(config)# radius-server key RADIUS-Pa55w0rd
R1(config)#
R1(config)# tacacs-server host 192.168.1.101
R1(config)# tacacs-server key TACACS+Pa55w0rd single-connection
R1(config)#
R1(config)# aaa authentication login default group tacacs+ group radius local-case
R1(config)#
```
The debug aaa authentication command provides a view of login activity.

For successful TACACS+ login attempts, a status message of PASS results.
### Sample Commands

#### 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

```
R1# debug radius
```

#### R1# **debug tacacs** ?
- **accounting**: TACACS+ protocol accounting
- **authentication**: TACACS+ protocol authentication
- **authorization**: TACACS+ protocol authorization
- **events**: TACACS+ protocol events
- **packet**: TACACS+ packets

```
R1# debug tacacs
```
AAA Authorization Overview

- The TACACS+ protocol allows the separation of authentication from authorization.
- Can be configured to restrict the user to performing only certain functions after successful authentication.
- Authorization can be configured for
  - character mode (exec authorization)
  - packet mode (network authorization)
- RADIUS does not separate the authentication from the authorization process.

Command authorization for user JR-ADMIN, command “show version”? Accept

Command authorization for user JR-ADMIN, command “configure terminal”? Reject
AAA Authorization Commands

To configure command authorization, use:

```
aaa authorization service-type {default | list-name} method1 [method2] [method3] [method4]
```

Service types of interest include:

- **commands level** For exec (shell) commands
- **exec** For starting an exec (shell)
- **network** For network services. (PPP, SLIP, ARAP)
AAA Accounting Overview

• Provides the ability to track usage, such as dial-in access; the ability to log the data gathered to a database; and the ability to produce reports on the data gathered.

• To configure AAA accounting using named method lists:

  `aaa accounting {system | network | exec | connection | commands level} {default | list-name} {start-stop | wait-start | stop-only | none} [method1 [method2]]`

• Supports six different types of accounting: network, connection, exec, system, commands level, and resource.
AAA Accounting Commands

- **aaa accounting exec default start-stop group tacacs+**
  Defines a AAA accounting policy that uses TACACS+ for logging both start and stop records for user EXEC terminal sessions.

- **aaa accounting network default start-stop group tacacs+**
  Defines a AAA accounting policy that uses TACACS+ for logging both start and stop records for all network-related service requests.

```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default group tacacs+
R1(config)# aaa authentication login TELNET-LOGIN local-case
R1(config)# aaa authorization exec group tacacs+
R1(config)# aaa authorization network group tacacs+
R1(config)# aaa accounting exec start-stop group tacacs+
R1(config)# aaa accounting network start-stop group tacacs+
R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET-LOGIN
R1(config-line)# ^Z
```