Basic Device Hardening

Cisco IOS includes various commands to configure security access on network devices. The configuration of user authentication is required to verify user identity. That is required before any access is allowed. There are encryption services as well to protect against password hacking. The options to configure authentication is based on local and remote access.

Enable Password

Cisco network devices are configured and managed directly from the command-line interface (CLI). The first level of defense is to configure an enable password. By default, there is no enable password on any Cisco device. The enable password only allows authorized users to access privileged EXEC mode (or enable mode).

enable password [*password*] [*level*]

The default security level that is assigned to enable mode is privilege level 15 (highest). That is a user authorization access level permitted to commands and functions. Anyone with enable password has full authorization to the network devices. From enable mode you can enter global configuration mode and all sub-modes.

Table 1 Command-Line Interface Modes

CLI Mode	Command Prompt
user EXEC mode	device >
privileged EXEC mode	device#
global configuration mode	device(config)#
ROMmon mode	rommon >
routing configuration mode	device(config-router)#

The following IOS global commands configure an enable password on a Cisco device. The enable password will be required before access to privileged EXEC mode prompt is allowed. You can specify a security privilege level as well for more granular user authorization.

```
device> enable
device# configure terminal
device(config)# enable password cisco
```

Enable Secret Password

Cisco devices also support enable passwords based on an MD5 hash algorithm that is uncrackable. That makes them more secure than standard enable plain-text passwords. The enable secret password is encrypted automatically and does not require service password-encryption command.

The following IOS global commands configure a secret enable password on a Cisco device. The secret enable password will be required before access to privileged EXEC mode prompt is allowed. It is not necessary to specify **secret 5** (MD5) since that is the Cisco default encryption level for secret passwords.

```
device(config)# enable secret cisco
```

Service Password-Encryption

The purpose of password encryption is to encrypt passwords in the running configuration script. The same passwords are also encrypted in the startup configuration as well. It applies to all except enable secret passwords. The purpose is to make passwords unreadable for security purposes. Cisco default is to display configured passwords as plain-text format. It applies to enable, console, VTY line passwords, and authentication keys.

The following IOS global command is used to encrypt all plain-text passwords in a configuration script. That applies to all existing plain-text passwords and newly created passwords.

```
device(config)# service password-encryption
```

Local Authentication

User identity requires that you create accounts with username and password credentials. There is no user authentication provided with an enable password. Anyone with knowledge of that password is granted access. Cisco local authentication allow network administrators to create local accounts on the network device.

It is a local security database with user accounts that are comprised of username/password credentials. Each account can be assigned unique security level authorization as well based on roles. The following IOS global command creates a new local account on a Cisco device. It assigns username **admin** and assigns password **cisco.**

The security authorization level 15 configured is privileged EXEC mode. It is the highest user authorization with access to all commands.

```
device(config)# username admin privilege 15 password cisco
```

The following IOS global command creates a local authentication account with username **cisco** and password **cisco.** The user authorization level 1 configured is user EXEC mode. That is the lowest authorization with access to only user mode prompt commands. You can however start a Telnet session with only privilege level 1.

```
device(config)# username cisco privilege 1 password cisco
```

Table 2 Local Authentication Security Options

Security	**Description**
privilege 0	disable, enable, help, exit, logout
privilege 1	user EXEC mode (lowest)
privilege 15	privileged EXEC mode (highest)
password 5	hidden secret password
password 7	hidden password

It is a common practice to copy/paste encrypted passwords between similar network devices. The following command would include the encrypted password that was generated from the previous command.

The following IOS global command creates a new local account on a Cisco device. It assigns username **admin** and privilege level 15. The **password 7** designates that you are copying a hidden (encrypted) password instead of a new password. The encrypted password is copy/pasted from configuration script of another device.

```
username admin privilege 15 password 7 [encrypted password]
```

The **service password-encryption** command must be enabled on the network device for type 7 encryption. The following IOS global command creates a new local account on a Cisco device. It assigns username **admin** and privilege level 15.

The **password 5** designates that you are copying a hidden (encrypted) secret password instead of a new password. The encrypted password is copy/pasted from configuration script of another device.

```
username admin privilege 15 secret 5 [encrypted password]
```

The following password types are encrypted:

- SSH session password
- Password type 7
- Enable secret password

Virtual Terminal Lines (VTY)

The following IOS commands enable default VTY lines for remote management access. There is a password of **cisco** assigned and timeout value of 5 minutes for inactivity. Enable password must be configured on the device as well for Telnet to work correctly.

```
line vty 0 4
password cisco
login
exec-timeout 5
```

Login Local

The IOS command **login local** enables user authentication based on a local account. The username and password are manually configured in the local device database. Anyone requesting access would enter a username and password for VTY line access.

```
line vty 0 4
login local
```

Console Port

The following commands will configure password **cisco** to the console port for local management access. Any login attempt to the console port will require that password. Optionally you can configure **login local** for user local authentication.

```
line console 0
password cisco
login
```

Transport Protocols

The following IOS command allows only SSH protocol traffic inbound to the default VTY lines (0 4). It will deny all other protocols inbound access to the VTY lines including Telnet. The Cisco default is to allow all protocols inbound and outbound access.

```
device(config-line)# transport input ssh
```

The following describe usage of the **transport** command to filter protocols. The **input** | **output** keyword determines whether inbound or outbound traffic is permitted with the default to allow all inbound and outbound traffic.

```
transport input all (default)  (allow all protocols (telnet, ssh)
transport input telnet ssh   (allow Telnet and SSH only)
```

The following are options for permit / deny of management protocols. Cisco default is to allow all protocols inbound and outbound access on VTY lines.

```
transport input ssh (allow SSH only)
transport input all (allow all protocols)
transport input telnet ssh (allow Telnet and SSH only)
```

AAA Security Model

AAA is a well-established security framework for controlling and monitoring network access. It is based on authentication, authorization and accounting of all requests to access network services and data.

There are often multiple security solutions that are integrated based on the unique requirements of each company. For example, solutions to manage physical access, surveillance systems, network devices and web servers are all different. The common elements of the AAA model should be included when deploying your security solution. The following describes and compared each element of the AAA security model.

Authentication

This is security control verifies the identity of a device and/or user before authorization to data. Network level access is initially based on some authentication protocol or technique.

The traditional username/password identity credential has been a standard for years. It is being replaced with Multi-Factor Authentication (MFA) for more robust layered authentication.

Authorization

This security control is in effect only after user authentication has been verified. The purpose of user authorization is to permit or deny access to data, services and commands. It is much more complex and involves permission levels for device modes, files and data that exist.

Accounting

This security service includes monitoring, logging and auditing of all security events. Any request for network access generates an event record that is stored for all users and transactions. The transaction would consist of username, time stamp, event type, and resources accessed. In addition, any user access denied is logged and alerts sent based on severity level. It is used for tracking, sending alerts, notifications, attack forensics and auditing.

RADIUS and TACACS+

The most common account servers are TACACS+ and RADIUS. They are deployed for centralized management of user accounts. Each user account is assigned username/password identity credentials for user authentication. They are referred to as AAA servers since they provide authentication, authorization and accounting security.

AAA servers request user credentials and permit or deny authentication request. There are authorization settings assigned to each user account as well that specify access permissions. The level of authorization is often directly associated and determine by role and job responsibilities. Cisco network devices are often managed remotely via Telnet or SSH session based on AAA server security. In contrast, local authentication maintains a separate user account database on each network device.

- Authentication verifies user identity for approving access to the server.
- Authorization allows user access to commands, data and applications.
- Accounting provides audit trail for alerts, security analysis and forensics.

Table 3 RADIUS vs TACACS Server

TACACS+	**RADIUS**
Cisco proprietary	multi-vendor open standard
TCP	UDP
separates authentication, authorization and accounting	integrates authentication and authorization
encrypts all communication	encrypts passwords only

The following is a list of disadvantages with using AAA servers:

- AAA server is a single point of failure
- Local account is required as a backup on network devices
- Same AAA password is used for multiple network devices

The following are three advantages of TACACS+ over RADIUS server.

- TACACS+ supports 15 privilege levels
- TACACS+ enables controls for user authorization levels
- TACACS+ allow for device administration

TACACS+ is a server-based authentication protocol that allows defining of authorization policies per group. As a result TACACS+ is well suited to managing the access security for thousands of network devices. RADIUS is limited to privilege mode with network access and authentication only.