802.1X

802.1x forces devices that connect to a switchport to authenticate prior to wider use of the net.

AAA (Authentication Authorization and Accounting) Server—Performs centralized authentication. Holds the user names and passwords. Provides a yes/no response when an authenticator asks if a username/password combination is legitimate.

Supplicant—802.1x software on the client device that handles authentication from the user

Authenticator—The switch. Usernames and passwords from the supplicant are passed to the AAA server for verification before the switch is authenticated and non-802.1x frames are allowed.

EAP (Extensible Authentication Protocol)—Protocol used for authentication messages from the supplicant to the authenticator (switch) and on to the AAA server. EAP messages are encapsulated either in EZPoL or RADIUS, depending on which leg of the journey they're in.

RADIUS—An AAA communication protocol over IP and UDP between the switch and the AAA server.

EAPoL (EAP over Lan)—an encapsulation that allows EAP packets to travel directly in an Ethernet frame from the supplicant to the switch. Traffic between the authenticator (switch) and the authentication server (AAA) is encapsulated in ordinary IP packets, just like any other RADIUS message.

AAA AUTHENTICATION

As mentioned above, AAA servers can centralize authentication. For example, the "login local" username and password entries on hundreds of routers and switches could be replaced by a AAA server, ensuring consistency. When presented with a username and password, the router or switch would ask the AAA server if the login is correct.

Cisco ACS (Access Control Server)—An example of AAA software that can be installed on a server.

TACACS+—A Cisco AAA protocol, like RADIUS, which operates over TCP instead of UDP between the Cisco device and the authentication server. Authorization and accounting can also be provided by a TACACS+ server, for example only giving a user access to certain IOS commands. Configuring this on one AAA server instead of every device can be a huge savings over Radius.

AAA Server Feature	RADIUS	TACACS+
Primary Use	Users	Network Devices
Transport Protocol	UDP	TCP
TCP/UDP Port Numbers (for authentication)	1645, 1812	49
Encryption	Just Password	Entire Packet
CLI Command Subset Authorization		•
Defined by	RFC 2865	Cisco

AAA Configuration—The test only asks only that you "describe device security using AAA with TACACS+ and RADIUS." Therefore, commands are simply a narrative device.

- Turn on AAA authentication—this changes which IOS commands are available

```
R5(config)# aaa new-model
```

Default is "no aaa …"

- Define each AAA server

```
R5(config)# tacacs server myServer
R5(config-server-tacacs)# address ipv4 10.0.1.5
R5(config-server-tacacs)# key mySharedSecretKey
R5(config-server-tacacs)# port 49
```

- Define a group of AAA servers—many commands will reference the entire group rather than an individual server

```
R5(config)# aaa group server tacacs+ myTacacsGroup
R5(config-sg-tacacs+)# server name myServer
R5(config-sg-tacacs+)# server name myOtherServer
```

- Set up a default list of authentication methods to be used for the console port, the aux port, and vty lines. If IOS can't get an authentication answer from the first method on the list it'll try the second, etc. This could happen if the network is down and the AAA server is unreachable.

```
R5(config)# aaa authentication login default group myTacacsGroup local line
```

The first option "group myTacacsGroup" refers to the list of Tacacs servers we created
The second option"local" refers to username/password combinations on the router
The third option "line" refers to passwords without usernames that can be define on the console port, vty lines, etc.

DHCP SNOOPING

This is an L2 switch feature, not an L3 router feature.

MITM (Man In The Middle) Attack—An attacker with a spurious (fake) DHCP server can cause hosts to configure themselves with the attacker as their default gateway.

Trusted Ports—Those from which legitimate DHCP server traffic (offer and ack messages) can be expected.

Untrusted ports—Those where an attacker can easily connect. Here, DHCP snooping will

- Discard server messages
- Maintain state information based on observed DHCP traffic in a DHCP binding table (interface, MAC, IP) to identify the traffic from a malicious client
- Prevent a client on another port from using the same MAC or IP address
- Optionally rate-limit DHCP messages to prevent DoS attacks