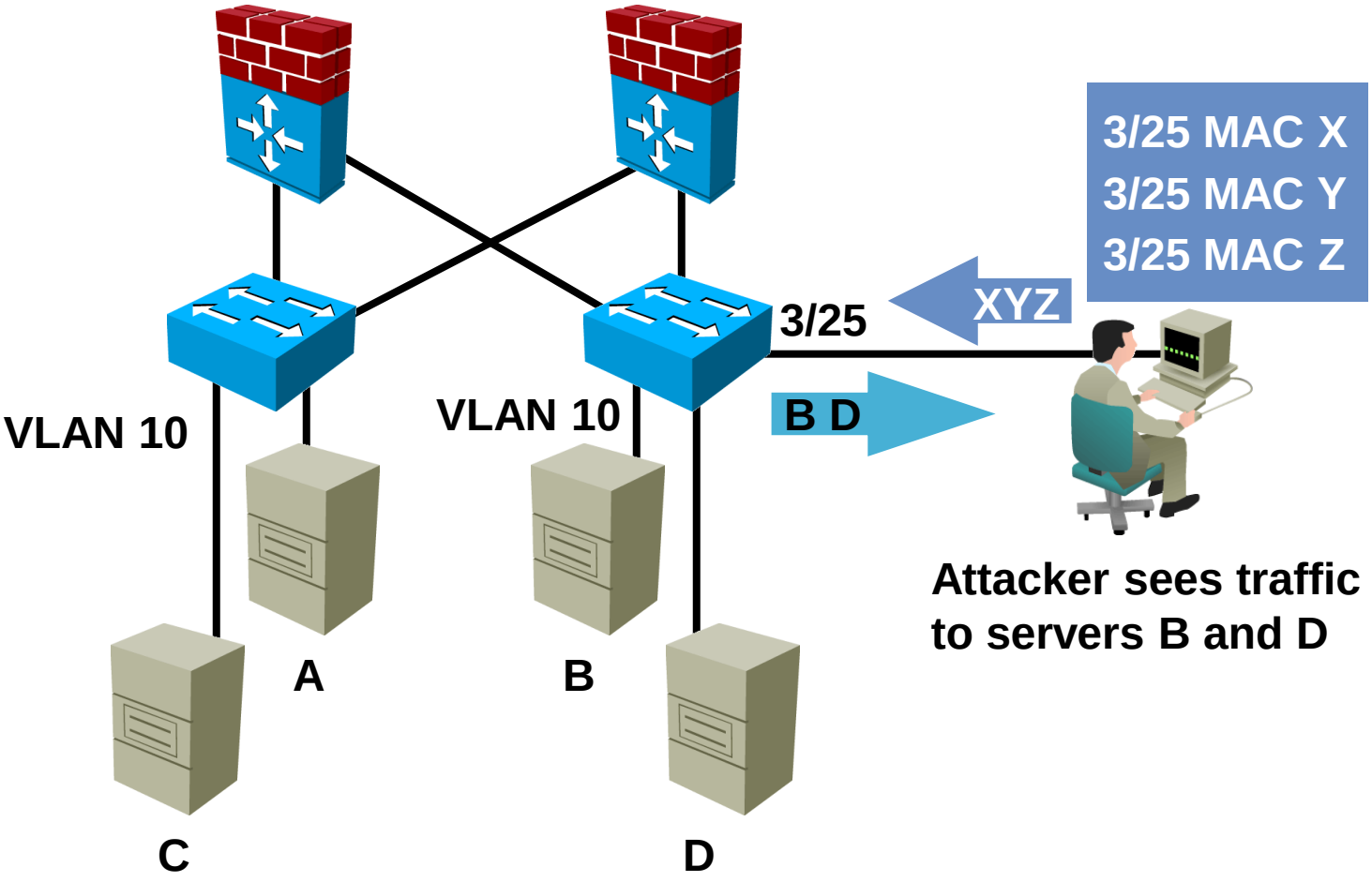
Switch Security

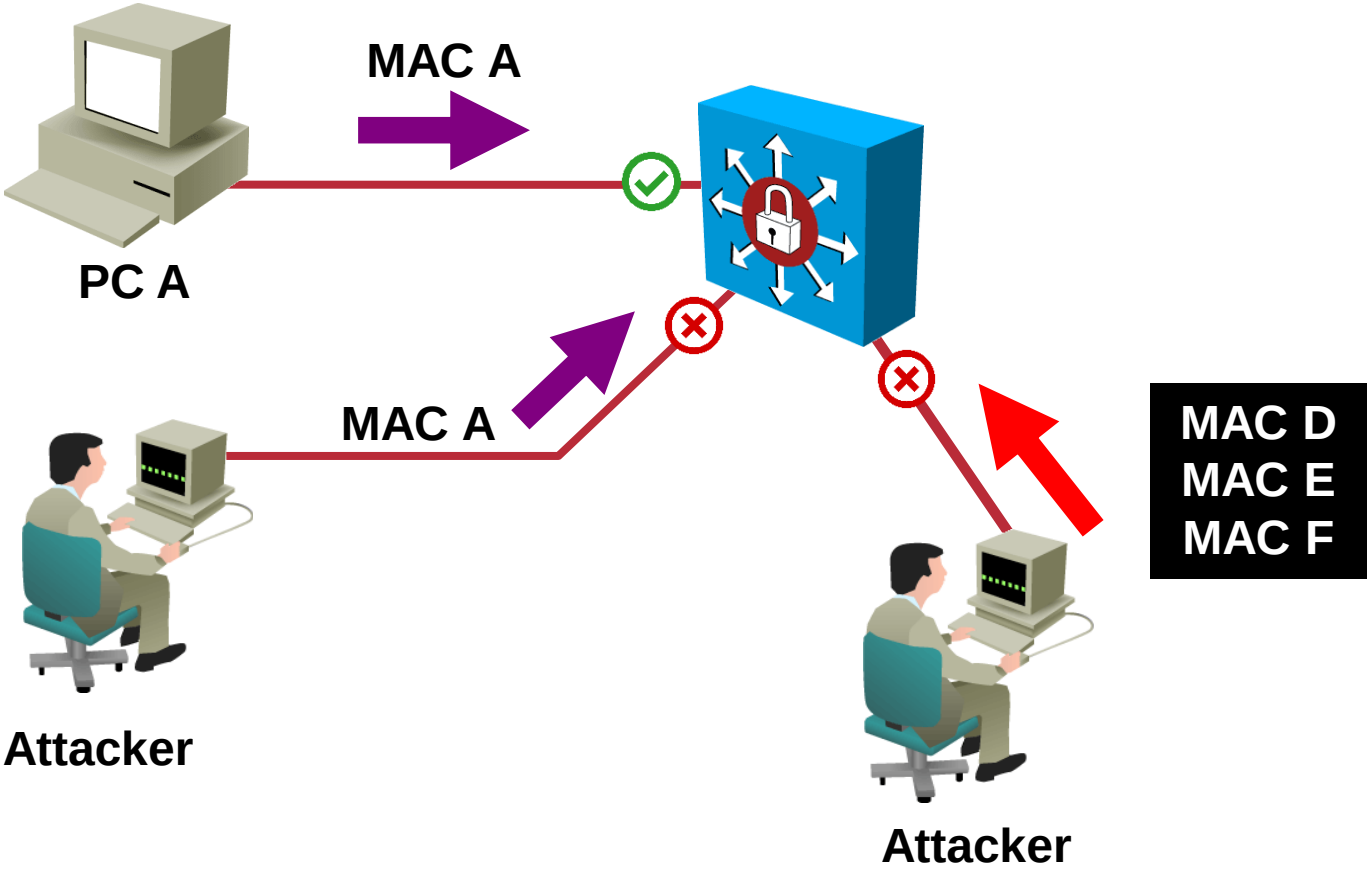
Types of Attacks

- CAM (Content Addressable Memory) table overflow
- VLAN hopping
- Spanning Tree manipulation
- MAC address spoofing
- DHCP attacks

CAM Table Overflow Attack



Port Security



- Port security allows you to configure Layer 2 interfaces that allow inbound traffic from only a restricted set of MAC addresses.
- The MAC addresses in the restricted set are called secure MAC addresses.

Secure MAC Addresses

- **Static**
  - Manually configure secure MAC addresses for an interface
  - Stored in the address table & added to running configuration
- **Dynamic** (default)
  - Dynamically learned and configure secure MAC addresses with the MAC addresses of connected devices
  - Stored **only** in the address table & removed when the switch restarts (or when the aging time expires)
- **Sticky**
  - Dynamically learned
  - Stored in the address table & added to running configuration
  - If these addresses are saved in the configuration file, the interface does not need to dynamically relearn them when the switch restarts

Port Security Violation Modes

- **Protect**: Frames from the non-allowed address are dropped, but there is no log of the violation.
- **Restric**: Frames from the non-allowed address are dropped, a log message is created and SNMP trap sent.
- **Shutdown** (default): If any frames are seen from a non-allowed address, the interface is **err-disabled**, a log entry is made, SNMP trap sent.

Violation Mode	Forwards Traffic	Sends Syslog Message	Increases Violation Counter	Shutdown Port
Protect	No	No	No	No
Restric	No	Yes	Yes	No
Shutdown	No	Yes	Yes	Yes

Configuration Guidelines

- Only on static access ports
- Not on trunk or dynamic access ports
- Not on SPAN port
- Not on EtherChannel port
- Not configurable on per-VLAN basis
- No aging of sticky addresses
- No simultaneous enabling of protect and restrict options

Default Settings

Feature	Default Setting
Port security	Disabled
Maximum MAC addresses	1
Violation mode	Shutdown
Sticky address learning	Disabled
Port security aging	Disabled. Aging time is 0. When enabled, the default type is absolute.

Configuring Port Security

```
SW(config-if)# switchport mode access
```

- Set the interface mode as access

```
SW(config-if)# switchport port-security
```

- Enable port security on the interface

```
SW(config-if)# switchport port-security maximum value
```

- Set the maximum number of secure MAC addresses for the interface (optional)

Configuring Port Security (Cont.)

```
SW(config-if)# switchport port-security violation
{protect | restrict | shutdown}
```

- Set the violation mode (optional)

```
SW(config-if)# switchport port-security mac-address
mac-address
```

- Enter a static secure MAC address for the interface (optional)
- MAC Address example: AAAA.BBBB.CCCC

```
SW(config-if)# switchport port-security mac-address
sticky
```

- Enable sticky learning on the interface (optional)

Configuring Port Security Aging

```
SW(config-if)# switchport port-security aging
{static | time time | type {absolute | inactivity}}
```

- Enable or disable static aging for the secure port, or set the aging time or type
  - static: enable aging for statically configured secure addresses on this port
  - time *time*: specify the aging time (mins)
  - type absolute: age out exactly after the specified time period
  - type inactivity: age out only if there is no data traffic for the specified time period

Verifying Port Security

```
SW# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)          (Count)
---------------------------------------------------------------------------
Fa0/12              1             0                 0          Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Verifying Port Security (Cont.)

```
SW# show port-security interface fa0/12
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address        : 0000.0000.0000
Security Violation Count   : 0
```

Verifying Port Security (Cont.)

```
SW# show port-security address
           Secure Mac Address Table
-----------------------------------------------------------------------
Vlan    Mac Address       Type                  Ports    Remaining Age
                                                          (mins)
----    -----------       ----                  -----    -------------
   1    0050.7966.6800    SecureConfigured      Fa0/1          -
   1    0050.7966.6801    SecureDynamic         Fa0/2          -
   1    0050.7966.6802    SecureDynamic         Fa0/3          5
   1    0050.7966.6803    SecureSticky          Fa0/4          -
-----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Auto recovery from err-disable state

- If the port – security feature has shutdown a port, the port can be restored to an operational state using the error-disable recovery procedure.

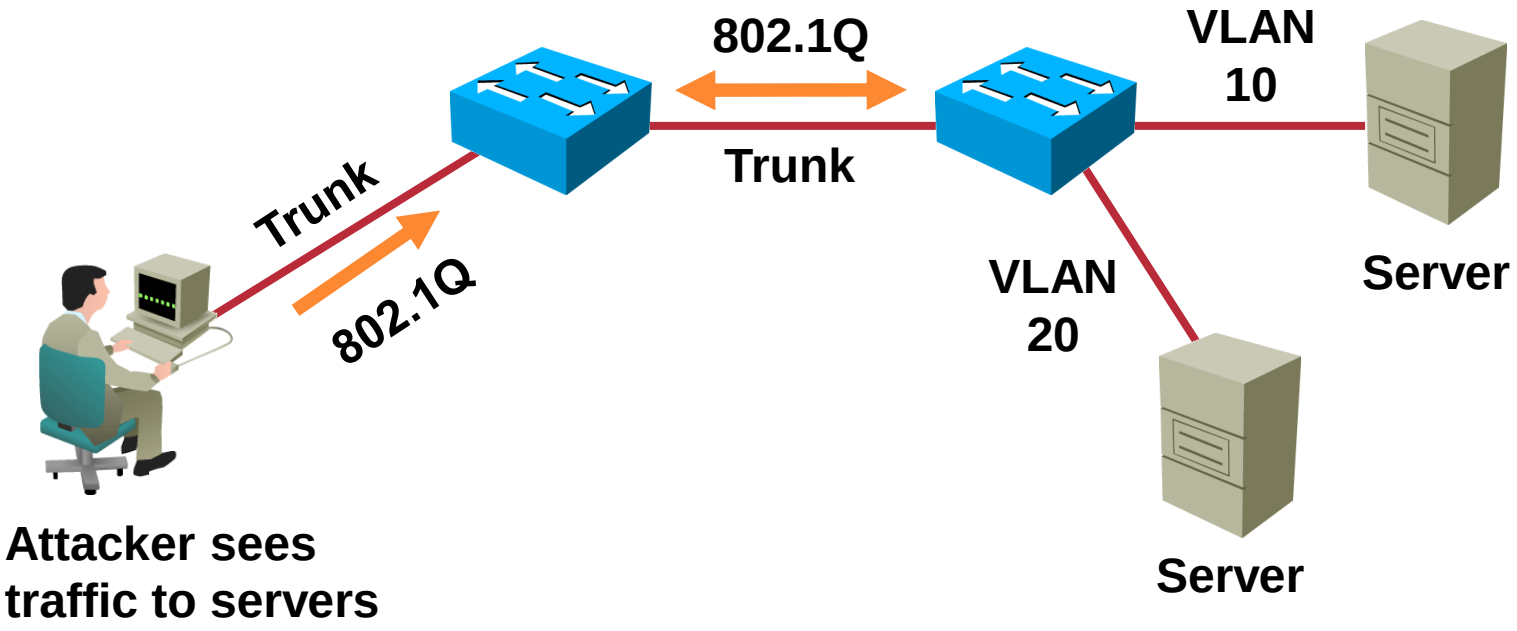
- Enable recovery cause is port – security:

```
Switch(config)#errdisable recovery cause psecure-violation
```

- Set a global recovery timeout by using the command:

```
Switch(config)#errdisable recovery interval seconds
```

VLAN Hopping

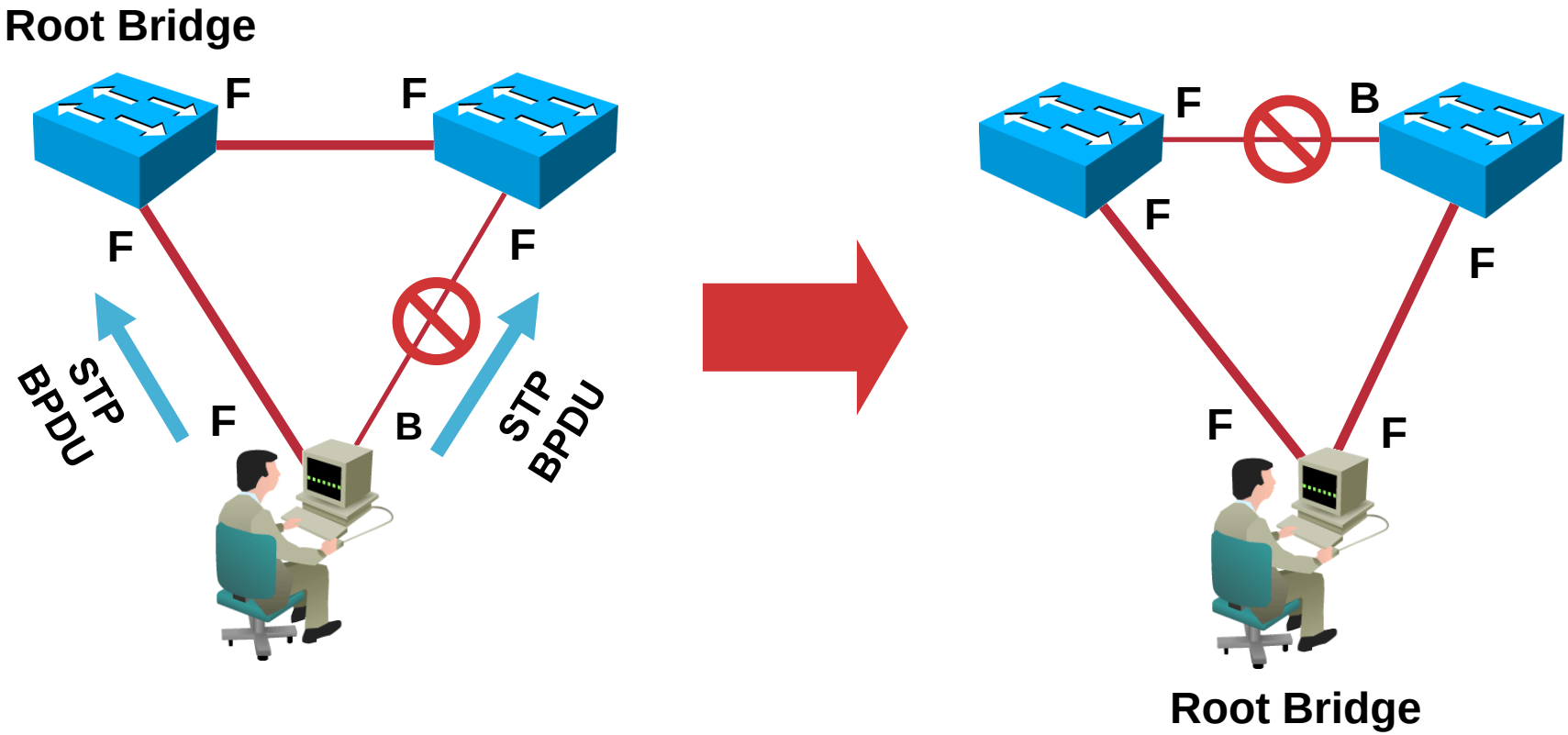


Mitigating VLAN Hopping

```
switch(config-if)# switchport mode access
```

- Configure port as an access port

Spanning Tree Manipulation



Implementing BPDUGuard to Mitigate Spanning Tree Manipulation

```
Switch(config)#spanning-tree portfast bpduguard

or

Switch(config-if)#spanning-tree bpduguard enable
```

- The BPDU – guard feature shuts down ports when ports receive BPDU.

Auto recovery from err-disable state

- If the BPDU – guard feature has shutdown a port, the port can be restored to an operational state using the error-disable recovery procedure.

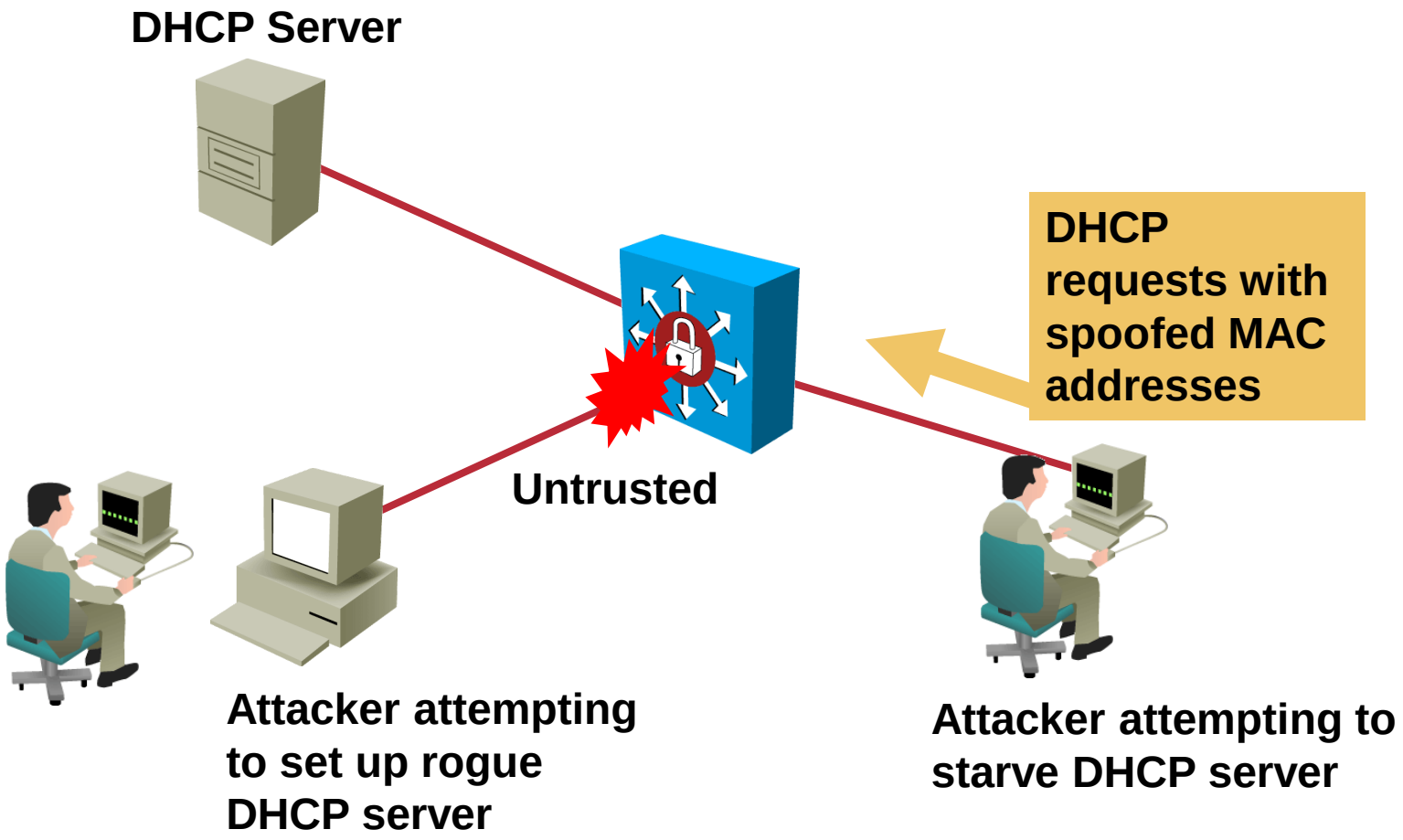
- Enable recovery cause is BPDU – guard :

`Switch(config)#errdisable recovery cause bpduguard`

- Set a global recovery timeout by using the command:

`Switch(config)#errdisable recovery interval` ***`seconds`***

DHCP Attacks



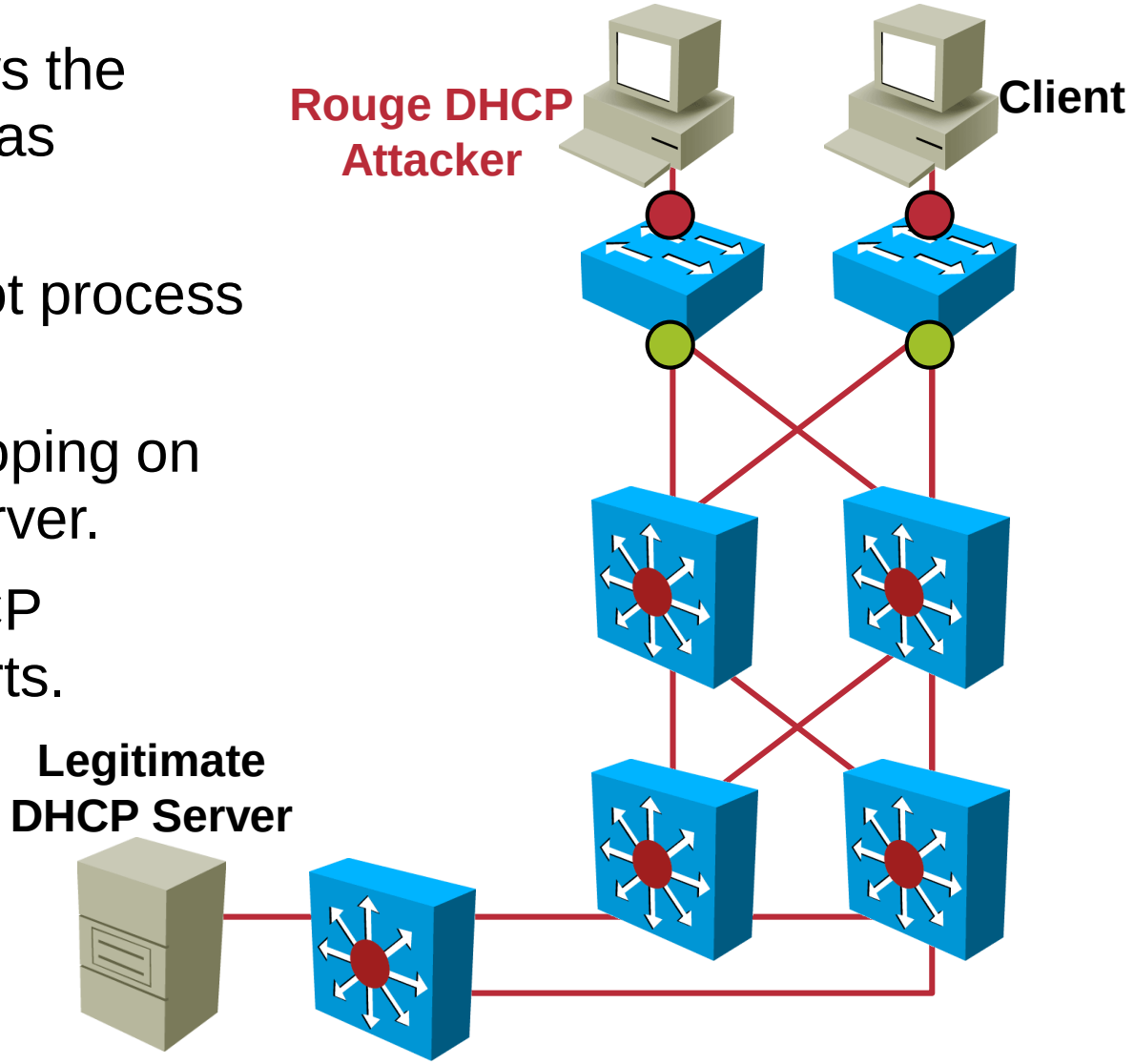
Mitigating DHCP Attacks

Here are two ways to mitigate DHCP spoofing and starvation attacks:

- **Port security**
- **DHCP snooping**

DHCP Snooping

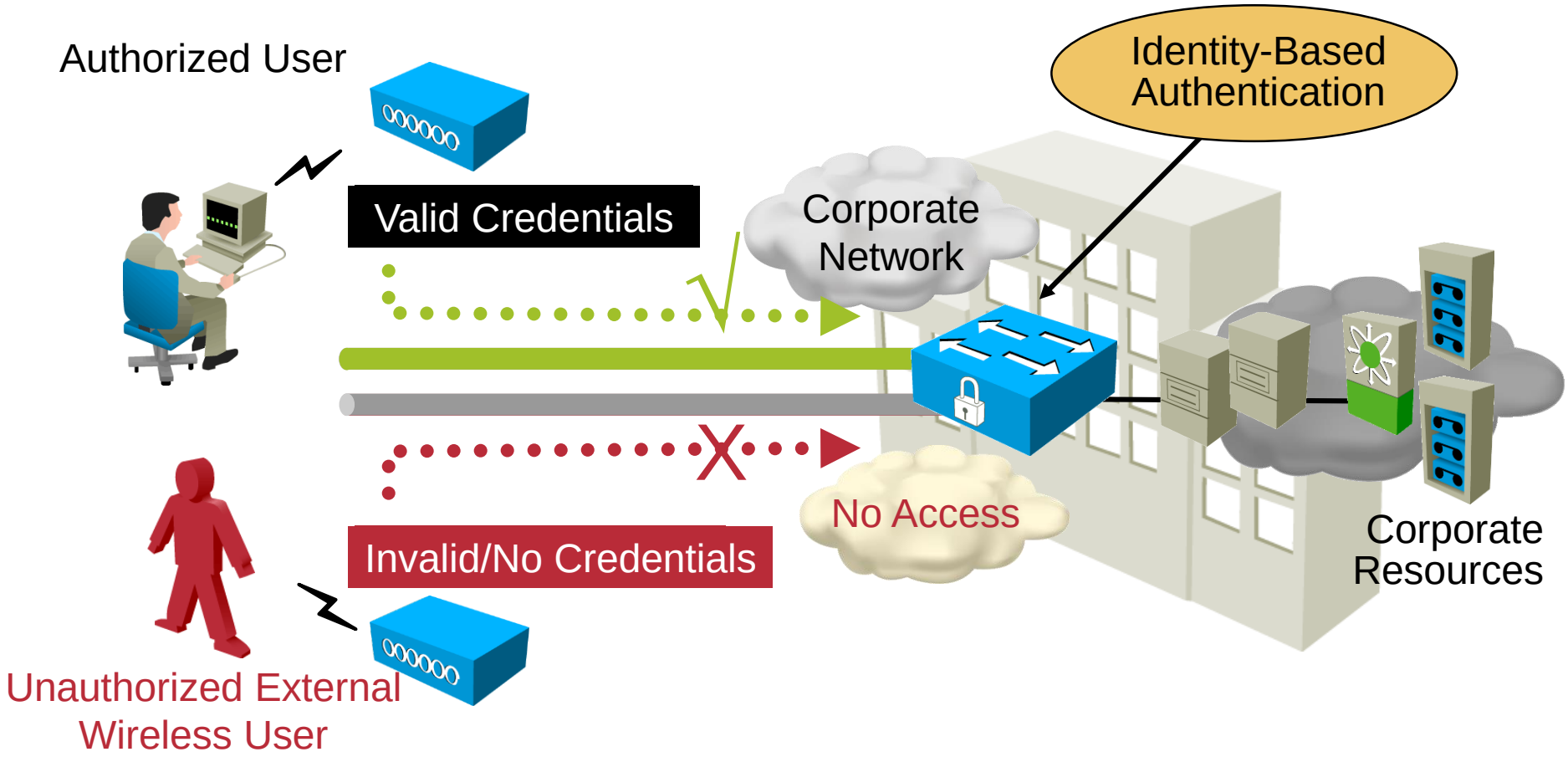
- DHCP snooping allows the configuration of ports as **trusted** or **untrusted**.
- Untrusted ports cannot process DHCP replies.
- Configure DHCP snooping on uplinks to a DHCP server.
- Do not configure DHCP snooping on client ports.



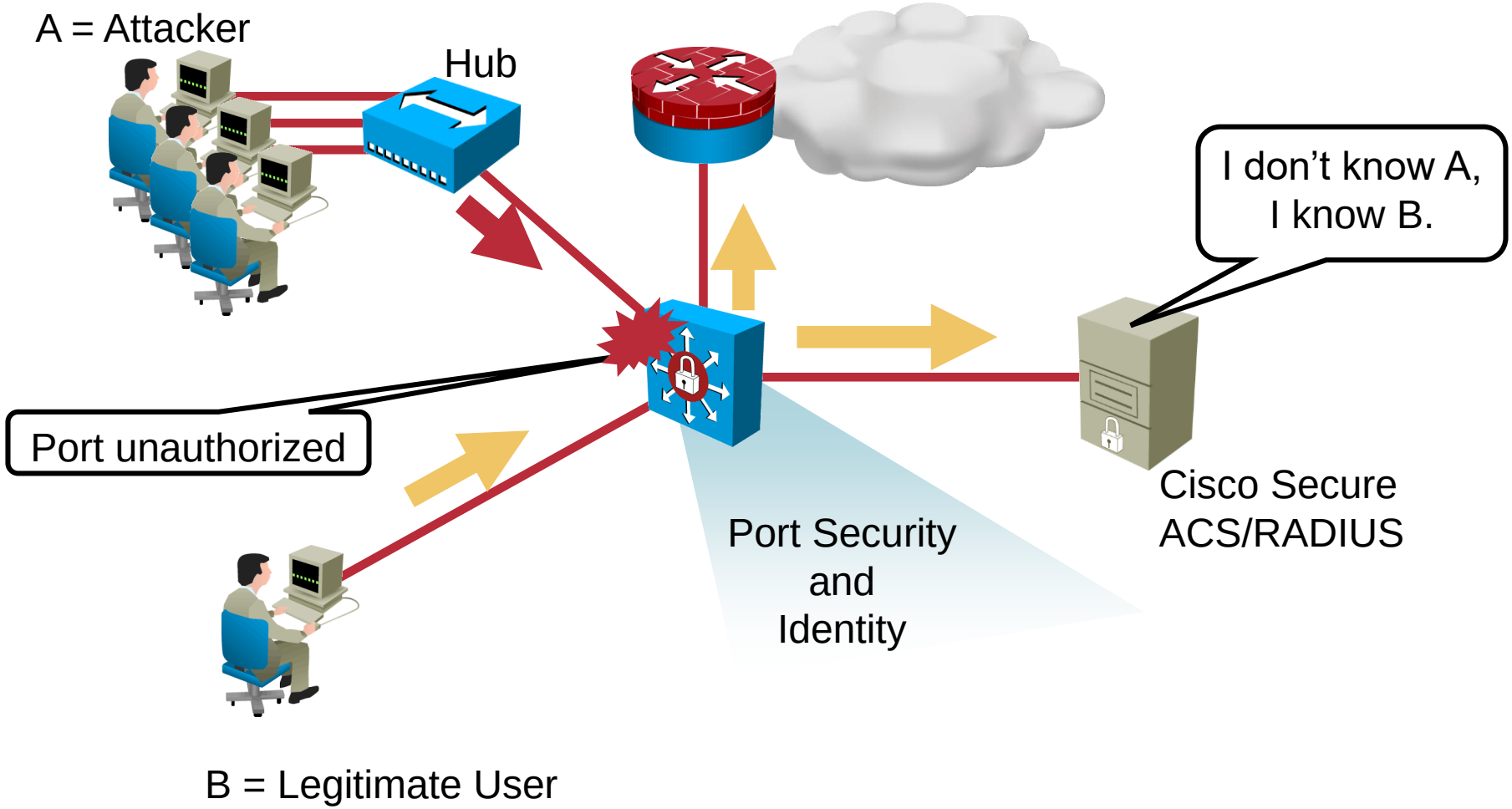
IEEE 802.1x

- Standard set by the IEEE 802.1 working group
- A framework designed to address and provide port-based access control using authentication
- Layer 2 protocol for transporting authentication messages between supplicant (user/PC) and authenticator (switch or access point)
- Actual enforcement is via MAC-based filtering and port-state monitoring

Concepts of 802.1x in Action



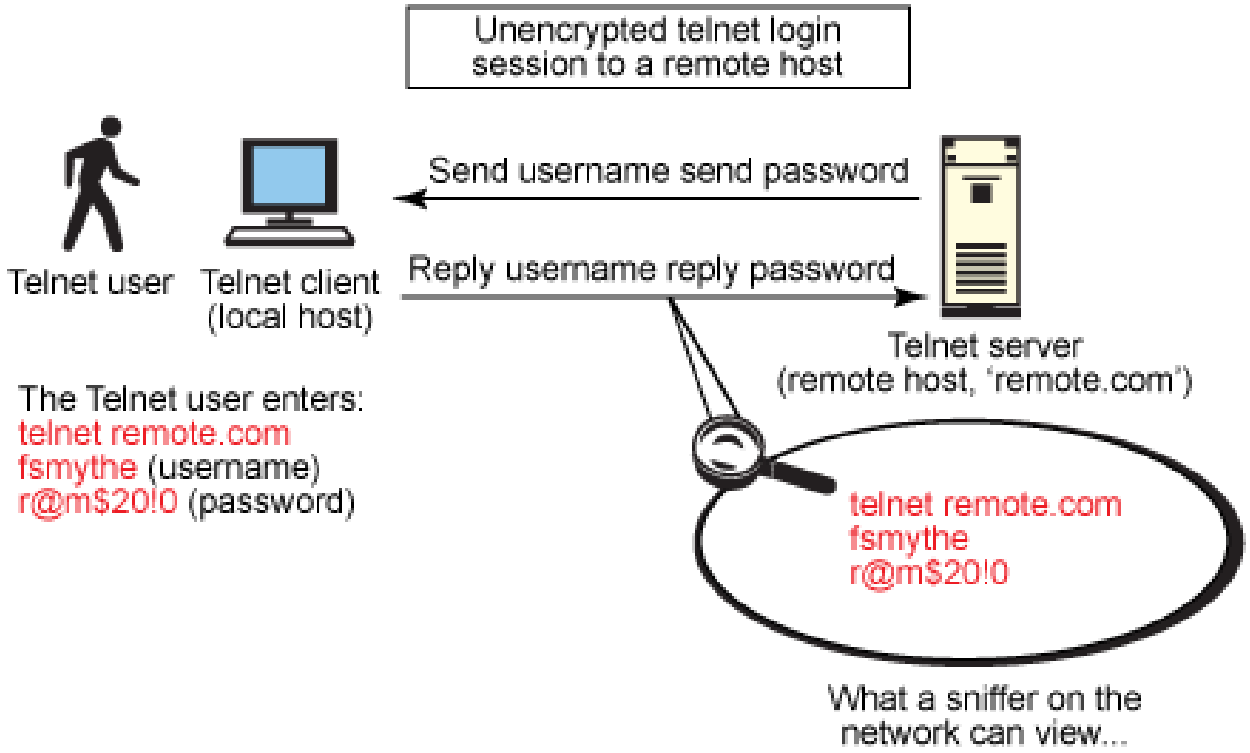
802.1x and Port Security



Local Authentication, SSH

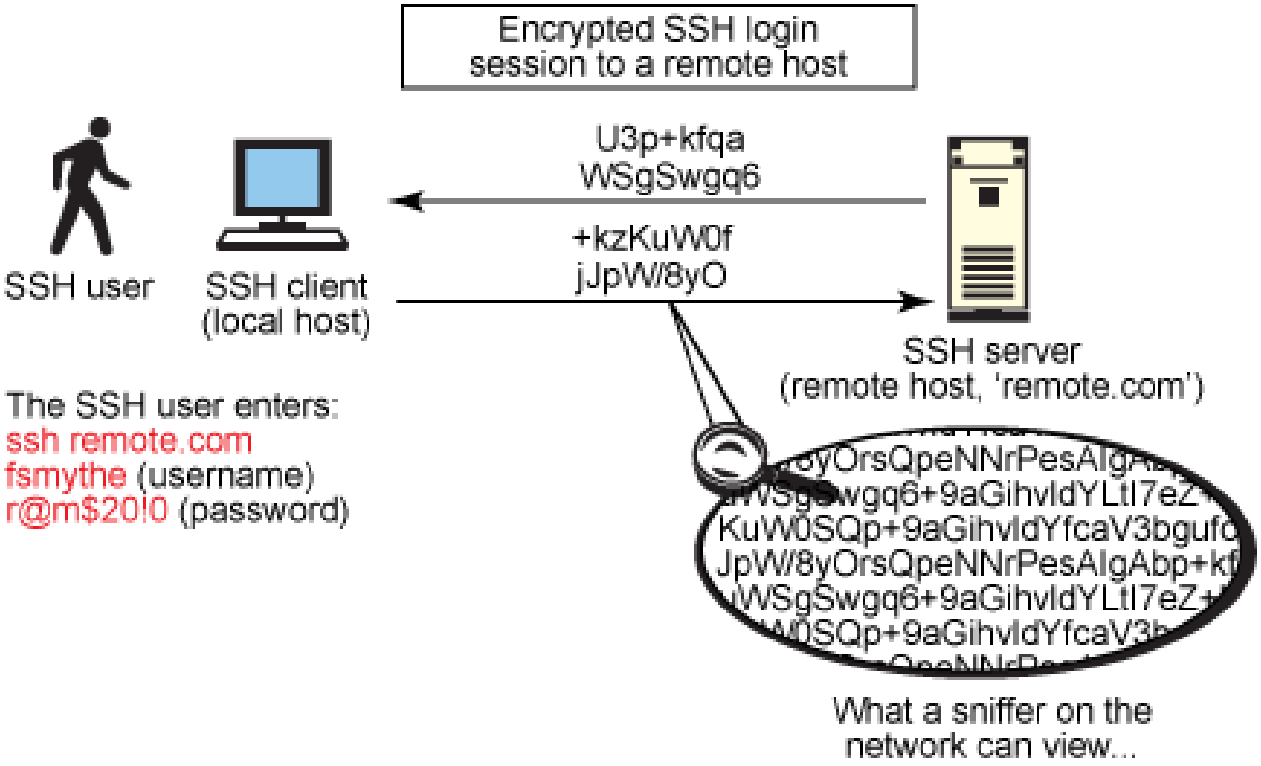
Telnet vs SSH Access

- **Telnet**
  - Most commond access method
  - Insecure
  - TCP, port 23



Telnet vs SSH Access (Cont.)

- **SSH** (**S**ecure **S**hell **P**rotocol)
  - More secure
  - TCP, port 22



Enhanced Username Password Security

```
router(config)#
username name password {[0] password | 7 hidden-password}
```

- Traditional user configuration with plaintext password

```
RouterX(config)#username admin password cisco
RouterX(config)#username admin password 7 070C285F4D06
```

```
router(config)#
username name secret {[0] password | 5 encrypted-secret}
```

- Uses MD5 hashing for strong password protection
- Better than the type 7 encryption found in *service password-encryption* command

```
RouterX(config)#username admin secret 0 cisco
RouterX(config)#username admin secret 5 $1$Opbm$tNrg6DH0ue45LJHCbXaNZ.
```

Local Authentication

- Enters line configuration mode (console or vty)

```
router(config)#
line console 0
line vty 0 4
```

- Enables local authentication

```
Boston(config)#line con 0
Boston(config-line)#login local
```

Configuring an SSH Server for Secure Management

```
Austin2#configure terminal
① Austin2(config)#ip domain-name cisco.com
② Austin2(config)#crypto key generate rsa general-keys modulus 1024
Sept 22 13:20:45: %SSH-5-ENABLED: SSH 1.5 has been enabled
③ Austin2(config)#ip ssh version 2
③ Austin2(config)#ip ssh timeout 120
③ Austin2(config)#ip ssh authentication-retries 4
④ Austin2(config)#username cisco password cisco
⑤ Austin2(config)#line vty 0 4
⑤ Austin2(config-line)#no transport input telnet
⑤ Austin2(config-line)#transport input ssh
⑤ Austin2(config-line)#login local
⑥ Austin2(config)#enable password cisco
```

1. Configure the IP domain name
2. Generate the RSA keys
3. Configure the SSH parameters
4. Create local user
5. Configure line vty
6. Configure enable password


CISCO