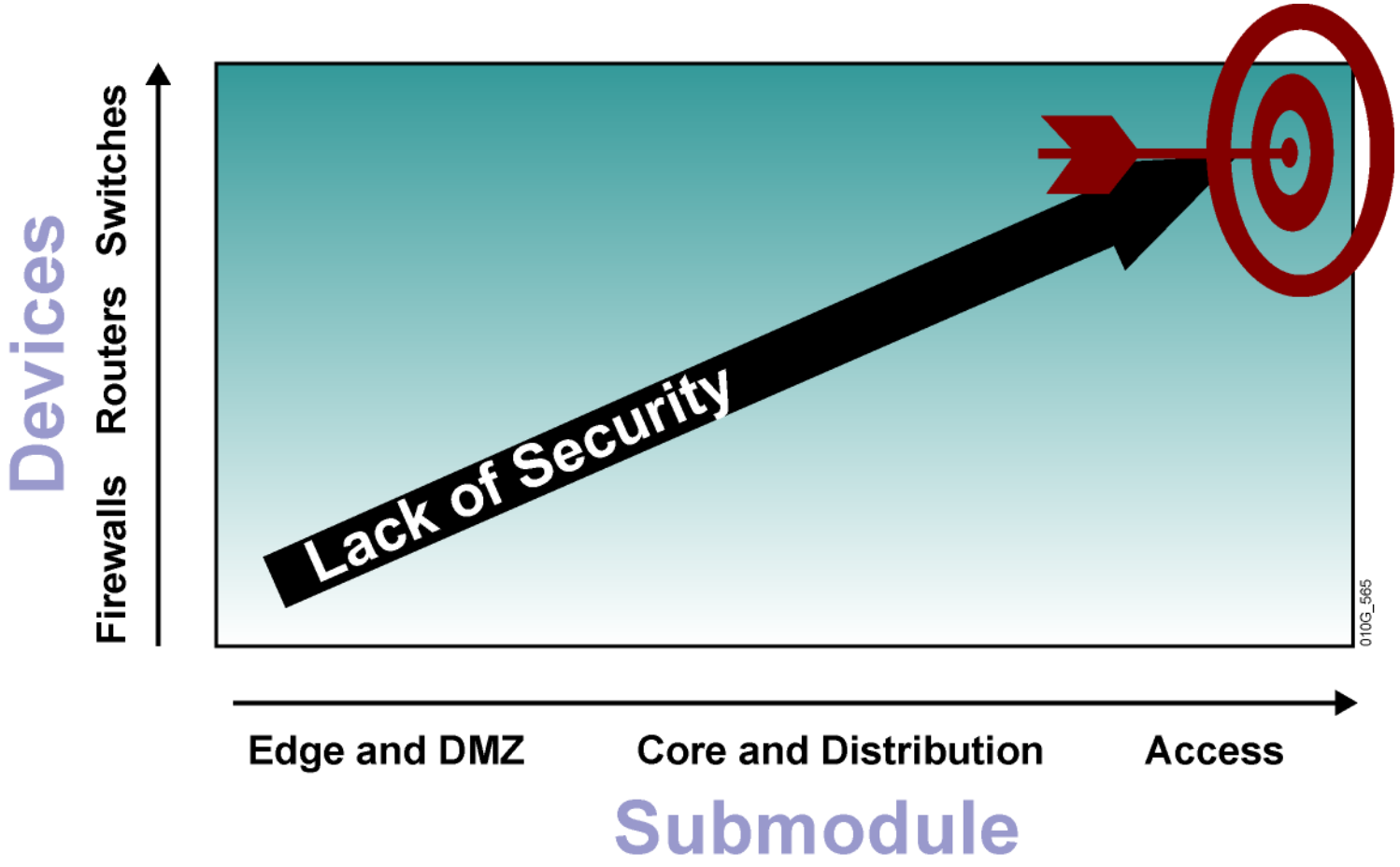
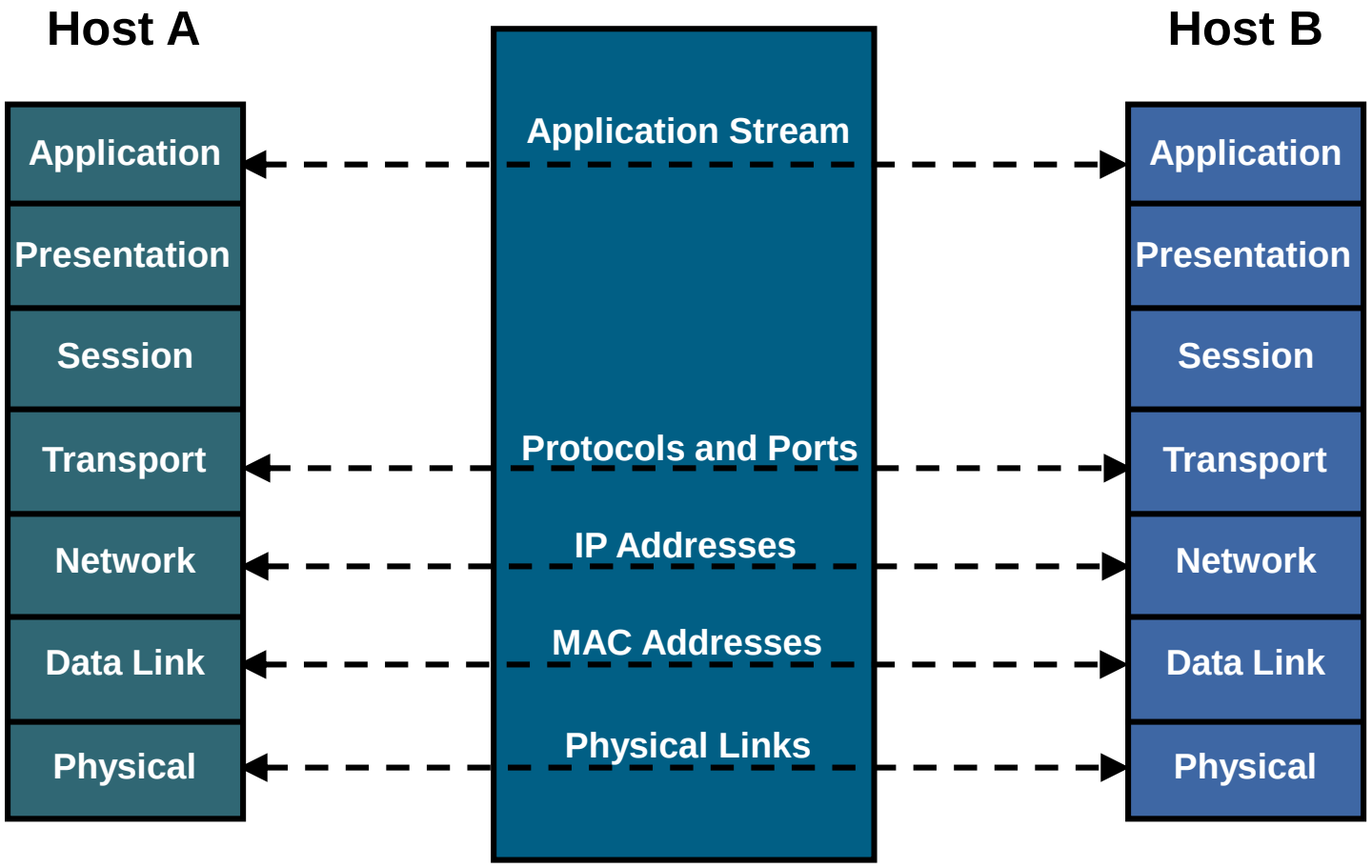
Layer 2 Security

Overview of Switch Security



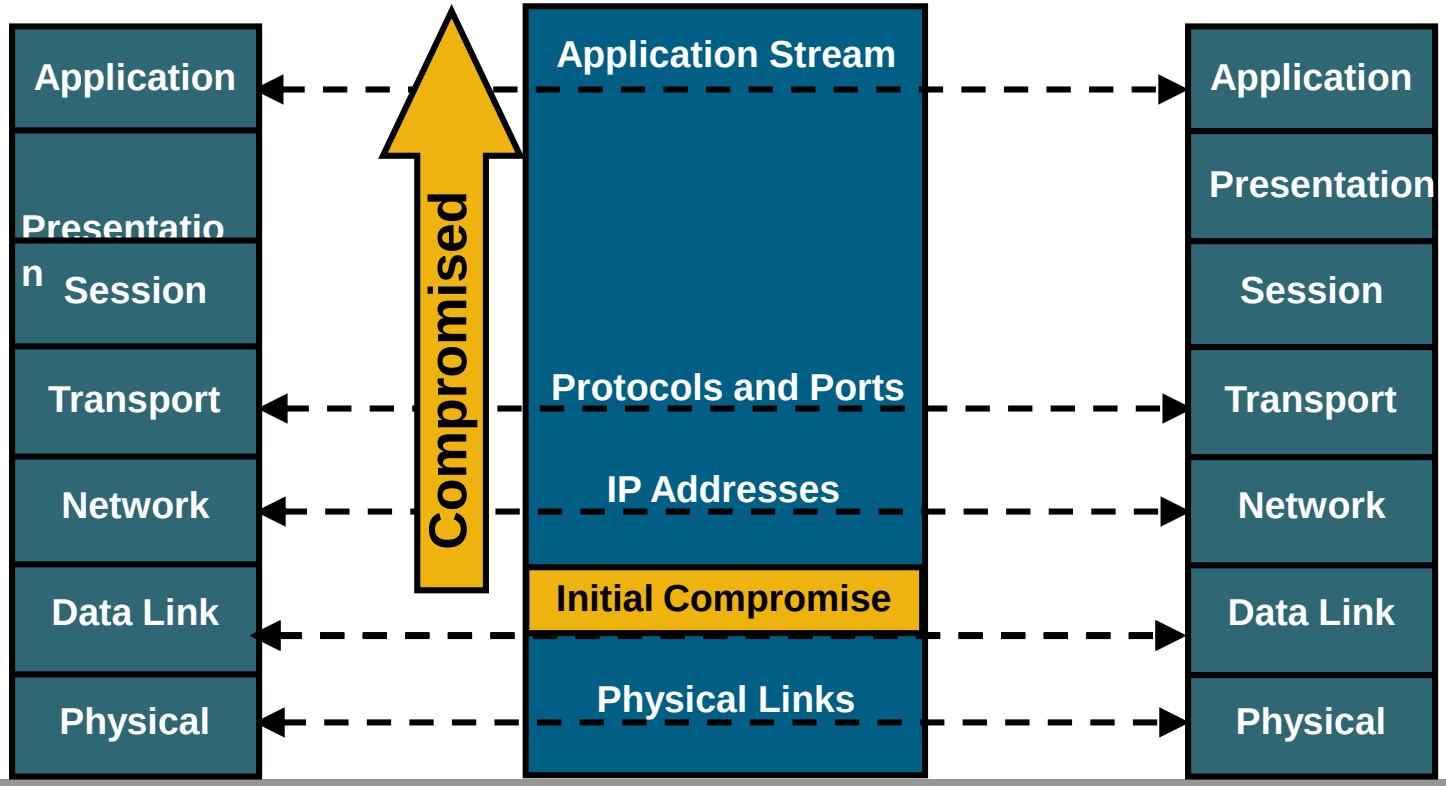
Why Worry About Layer 2 Security?



OSI was built to allow different layers to work without knowledge of each other.

Domino Effect

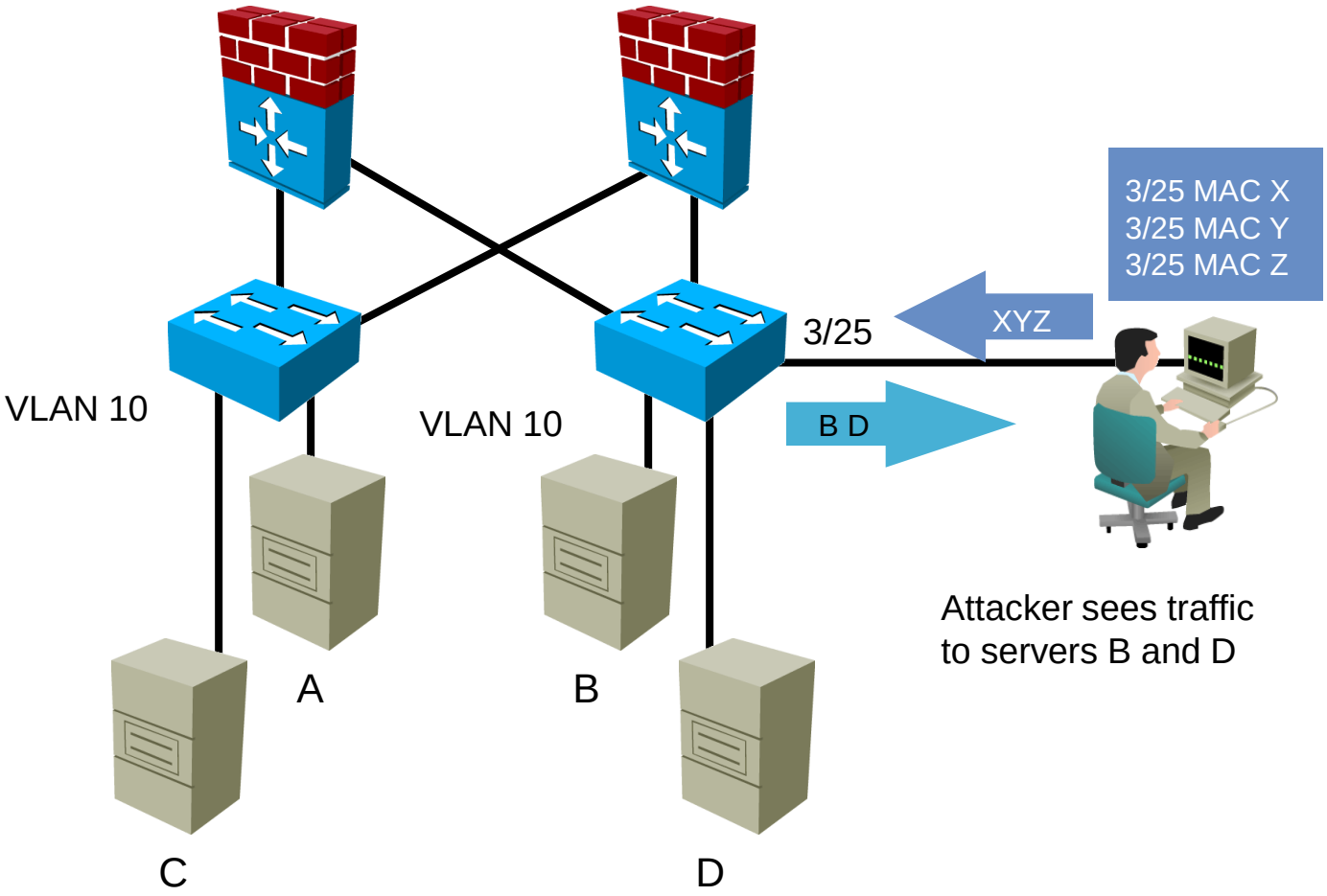
- If one layer is hacked, communications are compromised without the other layers being aware of the problem.
- Security is only as strong as your weakest link.
- When it comes to networking, Layer 2 can be a very weak link.



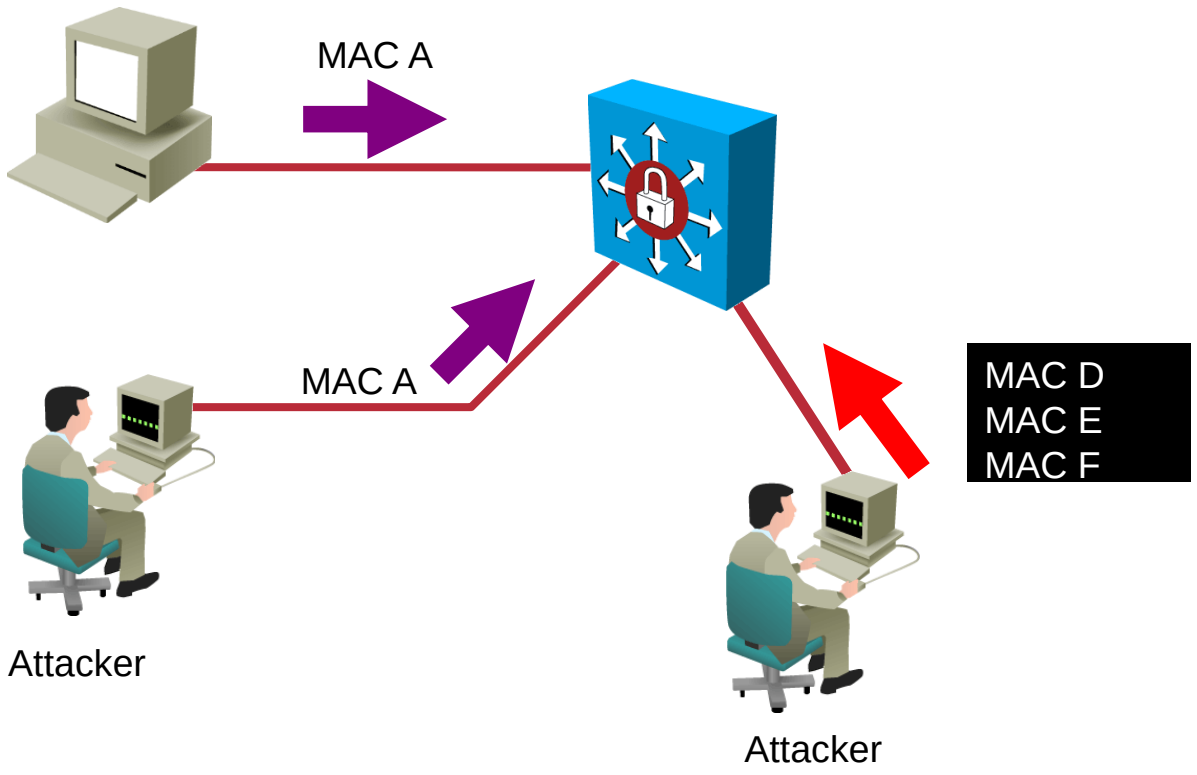
Switch Attack Categories

- **STP attacks**
- **CAM table (MAC address table) overflows**
- **DHCP spoofing**
- **ARP spoofing**
- **Address spoofing**

CAM Table Overflow Attack



Port Security



Secure MAC Addresses

- **Static**
- **Dynamic**
- **Sticky**

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.

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**

Configuring Port Security

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

- Set the interface mode as access

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

- Enable port security on the interface

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

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

Configuring Port Security (Cont.)

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

- Set the violation mode (optional)

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

- Enter a static secure MAC address for the interface (optional)

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

- Enable sticky learning on the interface (optional)

Configuring Port Security Aging

```
switch(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

Verifying Port Security

```
sw-class# 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-class# 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-class# show port-security address
          Secure Mac Address Table
-----------------------------------------------------------------------
Vlan    Mac Address       Type                  Ports    Remaining Age
                                                          (mins)
----    -----------       ----                  -----    -------------
   1    0000.ffff.aaaa    SecureConfigured      Fa0/12         -
-----------------------------------------------------------------------
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

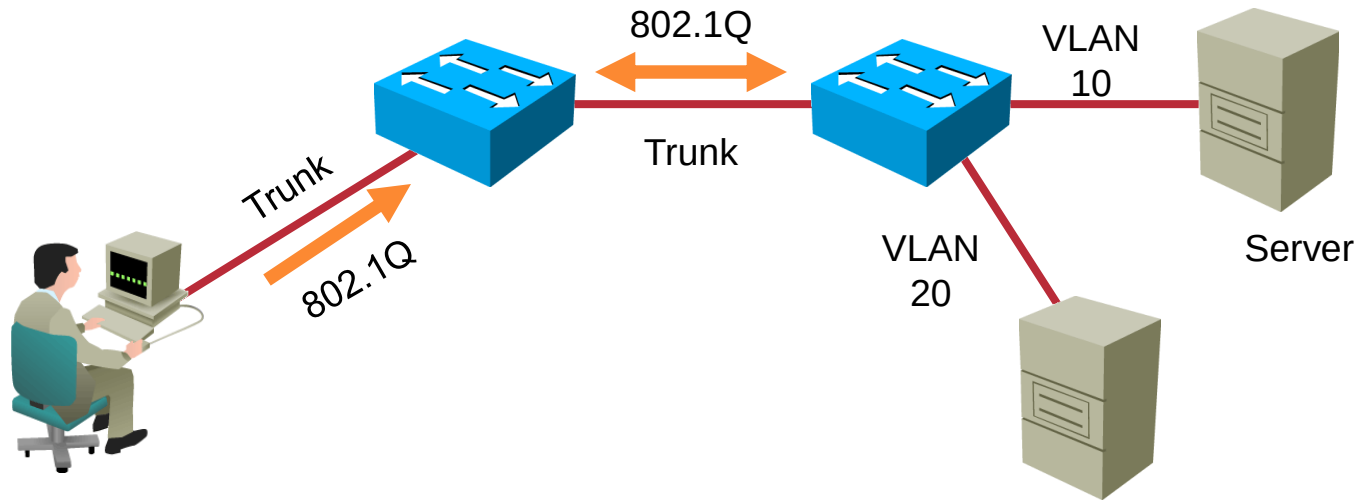
- **If the port – security feature has shutdown a port, the port can be restored to an operational state using the error-disable recovery procedure.**
- **Enable recovery cause is port – security:**

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

- **Set a global recovery timeout by using the command:**

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

VLAN Hopping



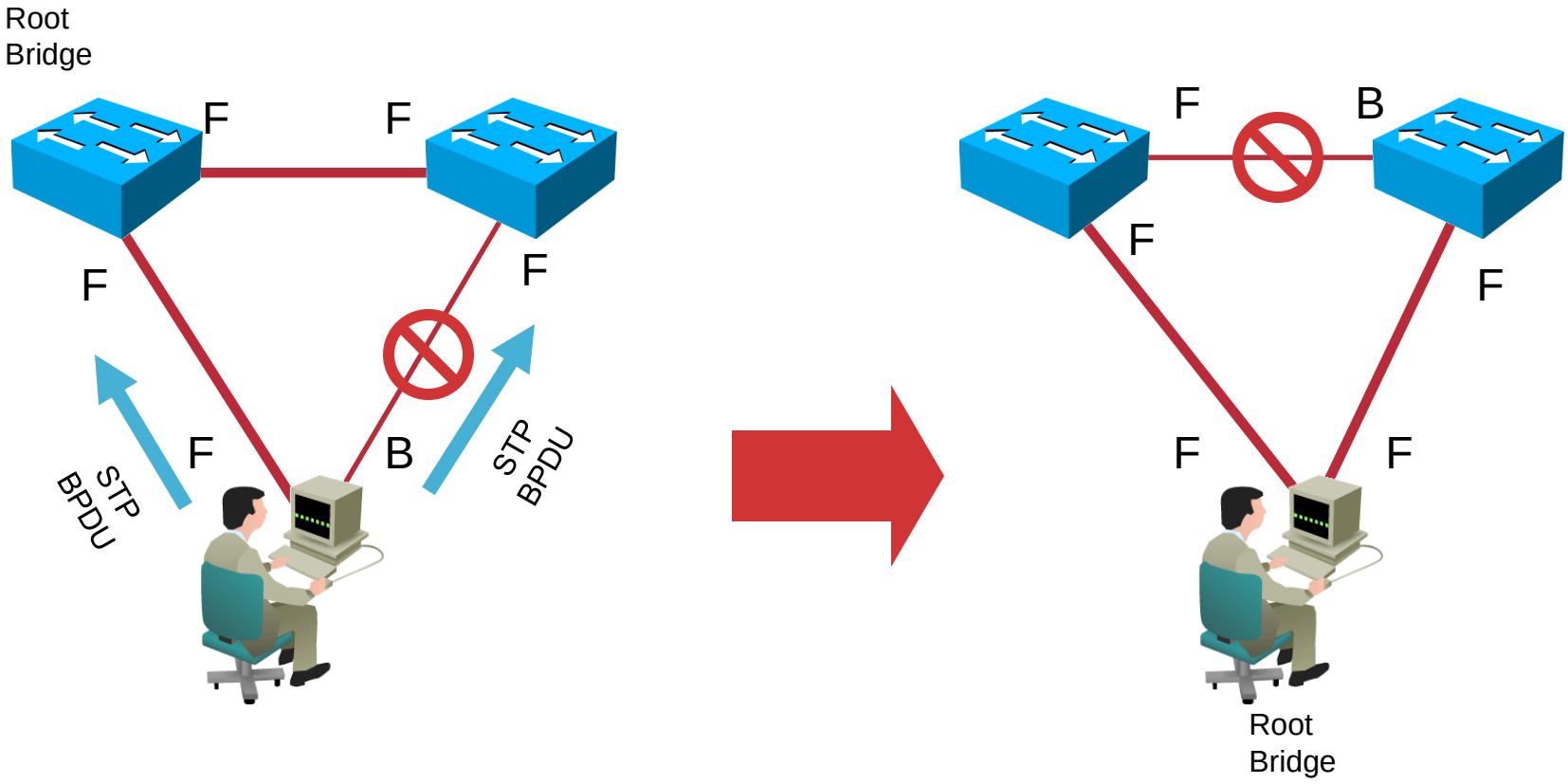
Attacker sees traffic to servers

Mitigating VLAN Hopping

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

- Configure port as an access port

Spanning Tree Manipulation



Mitigating 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

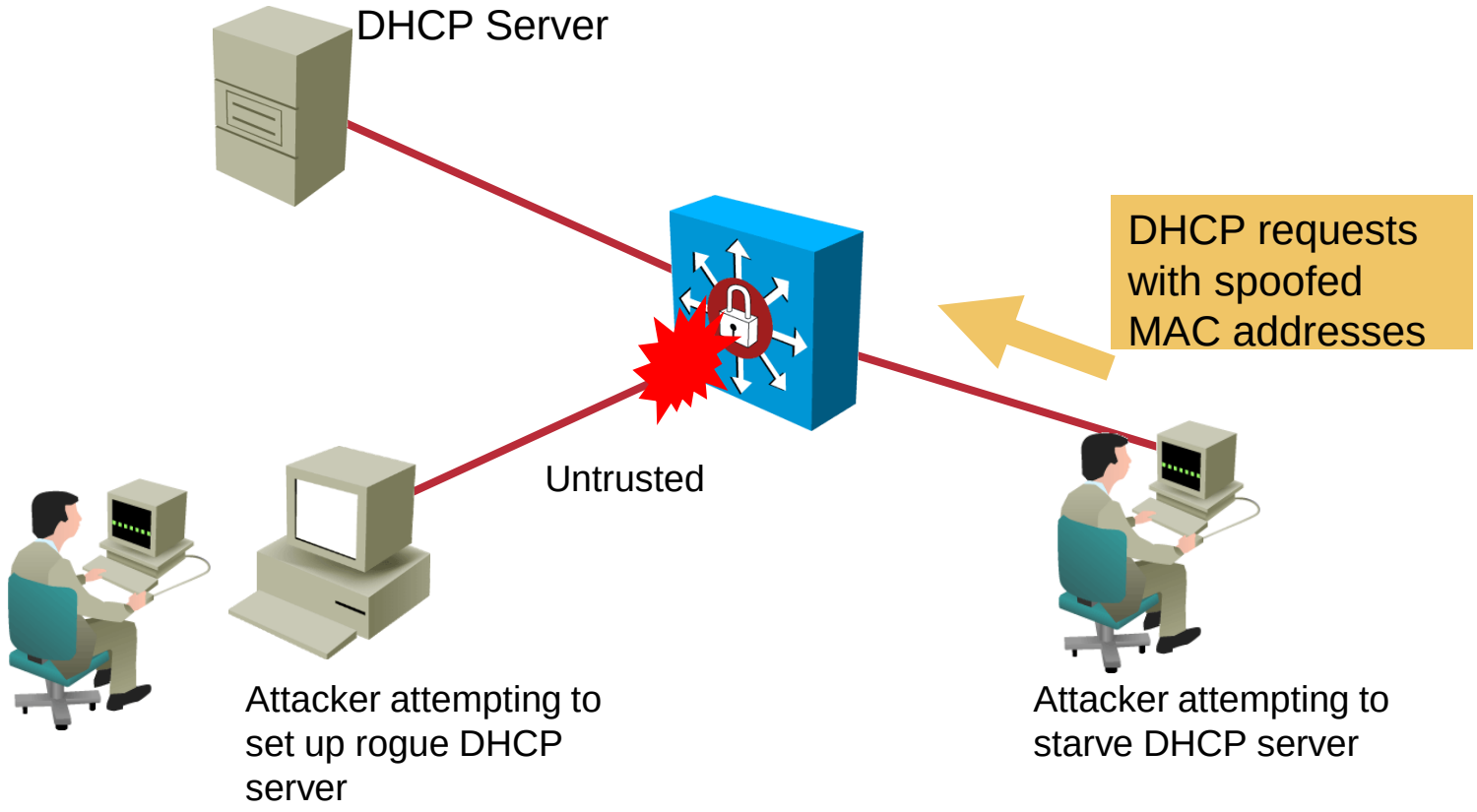
- **If the BPDU – guard feature has shutdown a port, the port can be restored to an operational state using the error-disable recovery procedure.**
- **Enable recovery cause is BPDU – guard :**

```
Switch(config)#errdisable recovery cause bpduguard
```

- **Set a global recovery timeout by using the command:**

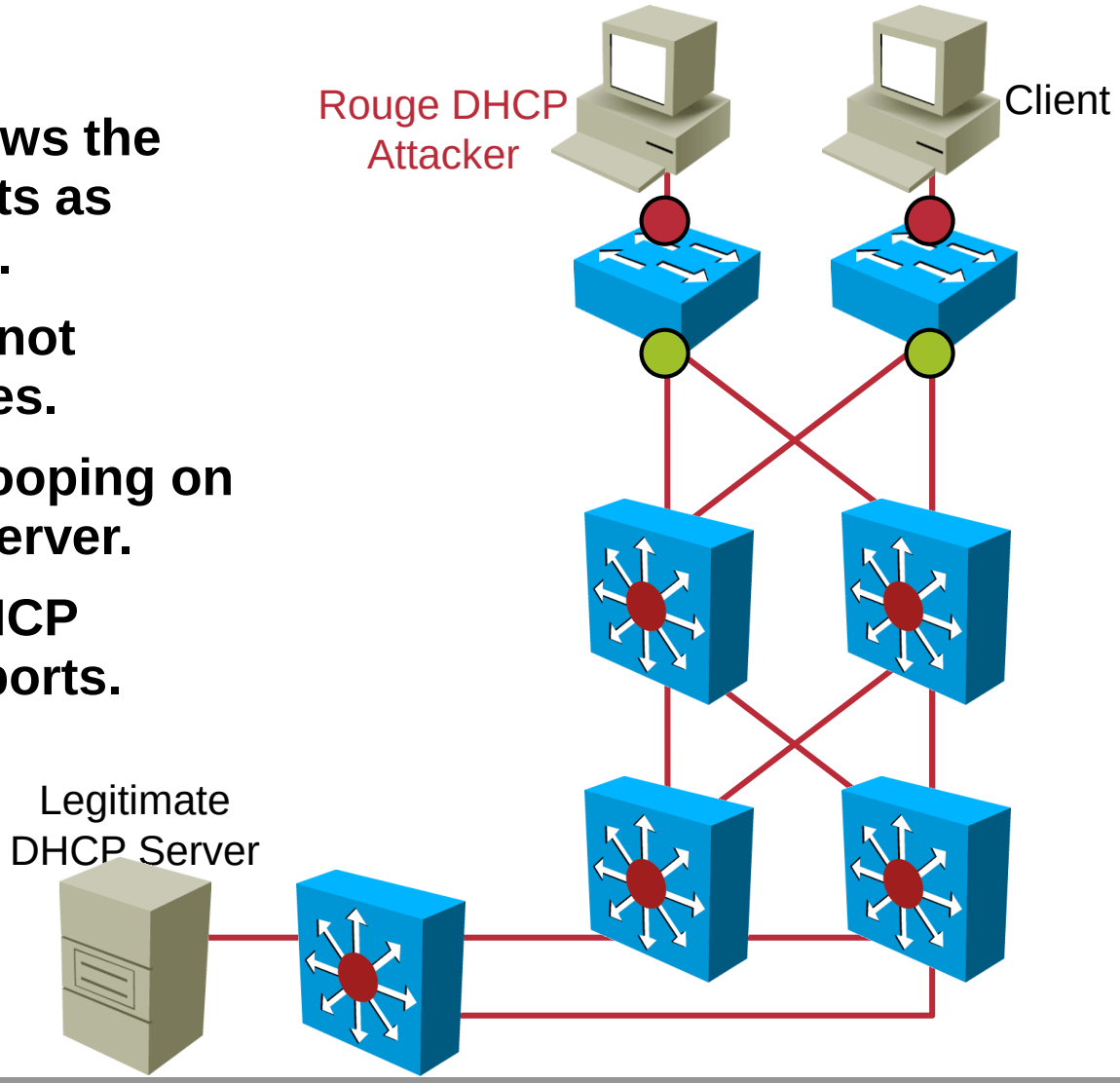
```
Switch(config)#errdisable recovery interval seconds
```

DHCP Attacks



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.**

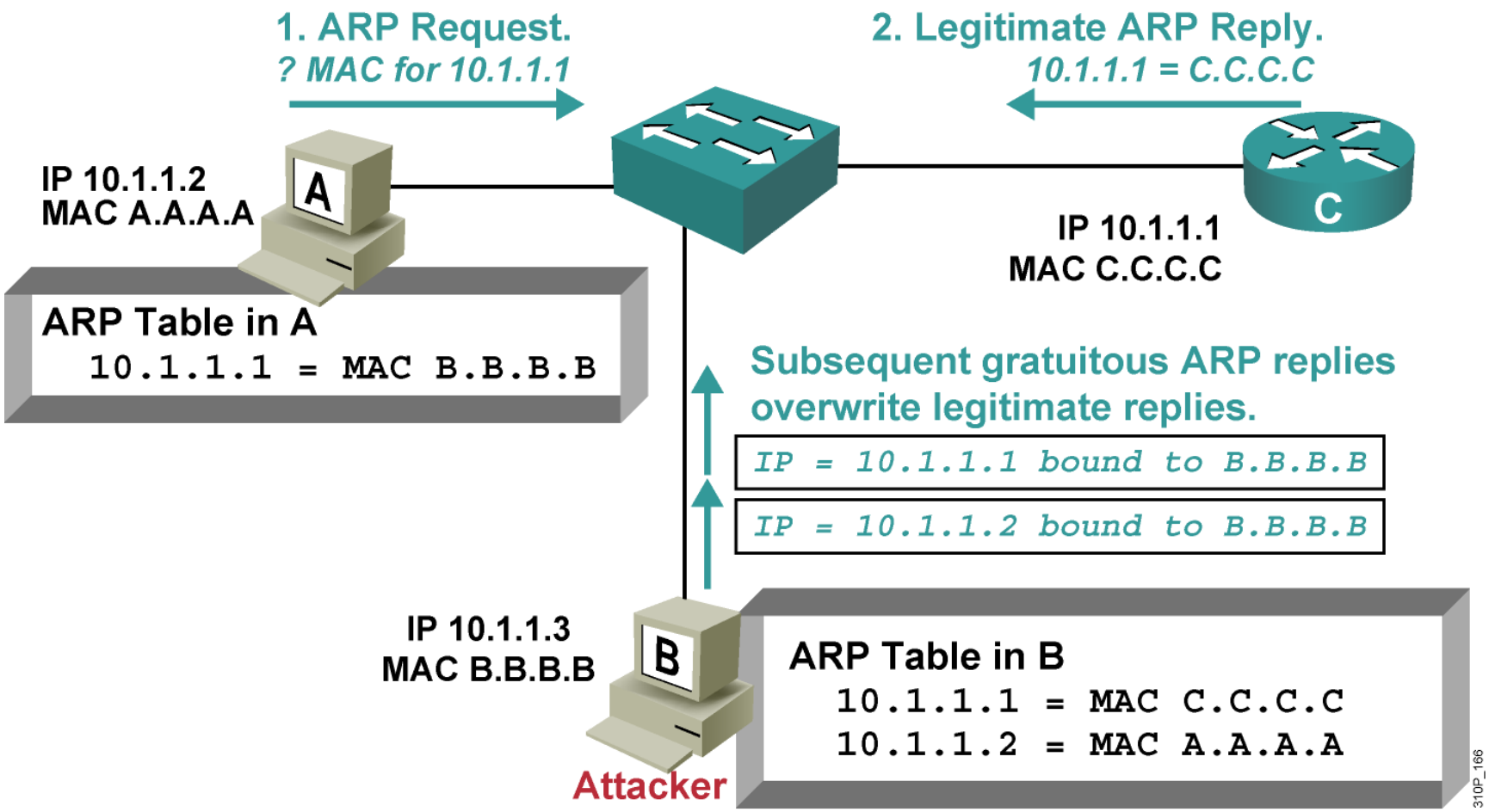


Mitigating DHCP Attacks

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

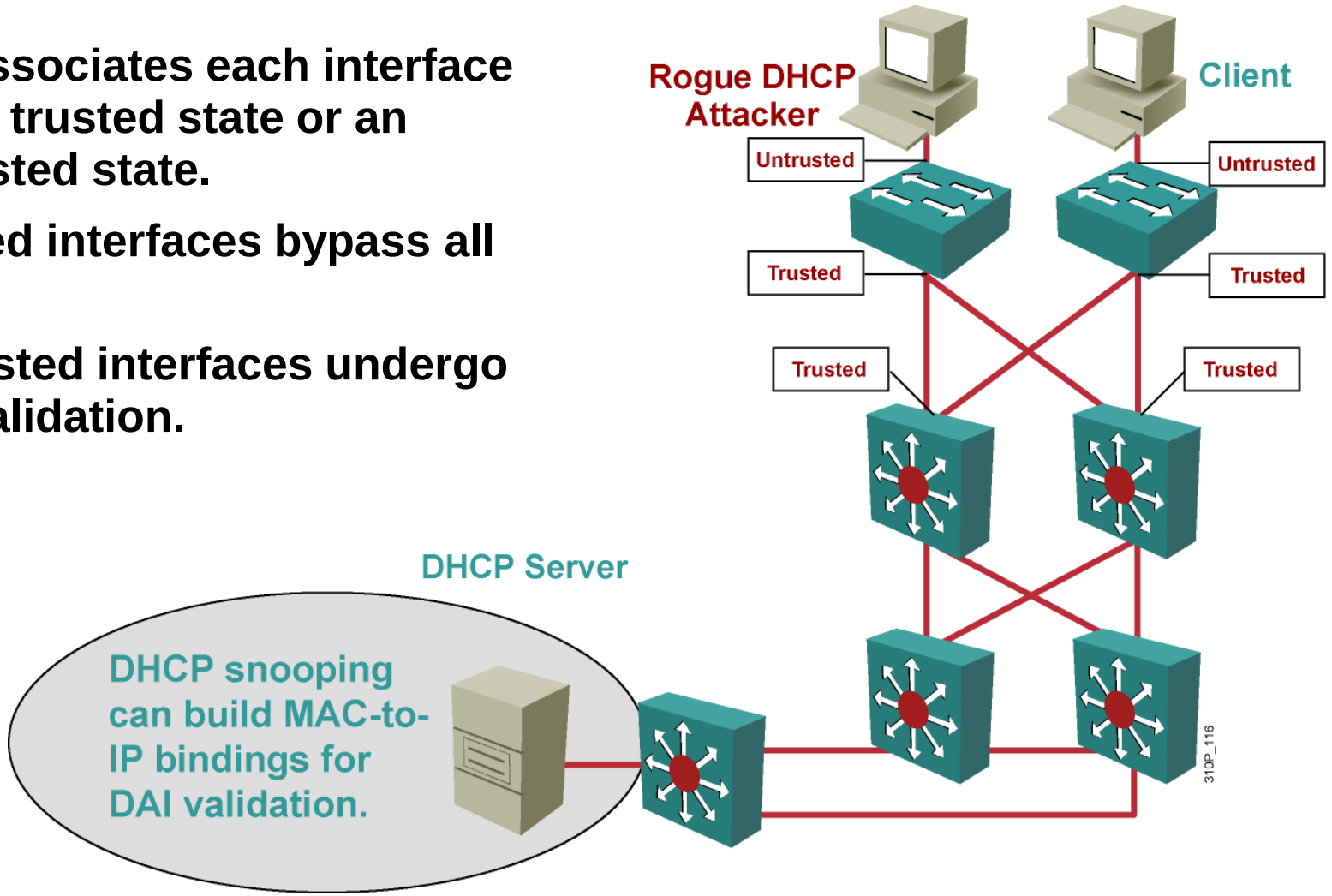
- **Port security**
- **DHCP snooping**

ARP Spoofing



Dynamic ARP Inspection

- DAI associates each interface with a trusted state or an untrusted state.
- Trusted interfaces bypass all DAI.
- Untrusted interfaces undergo DAI validation.



Configuring DAI

```
Switch(config)#ip arp inspection vlan vlan_id[,vlan_id]
```

- **Enables DAI on a VLAN or range of VLANs**

```
Switch(config-if)#ip arp inspection trust
```

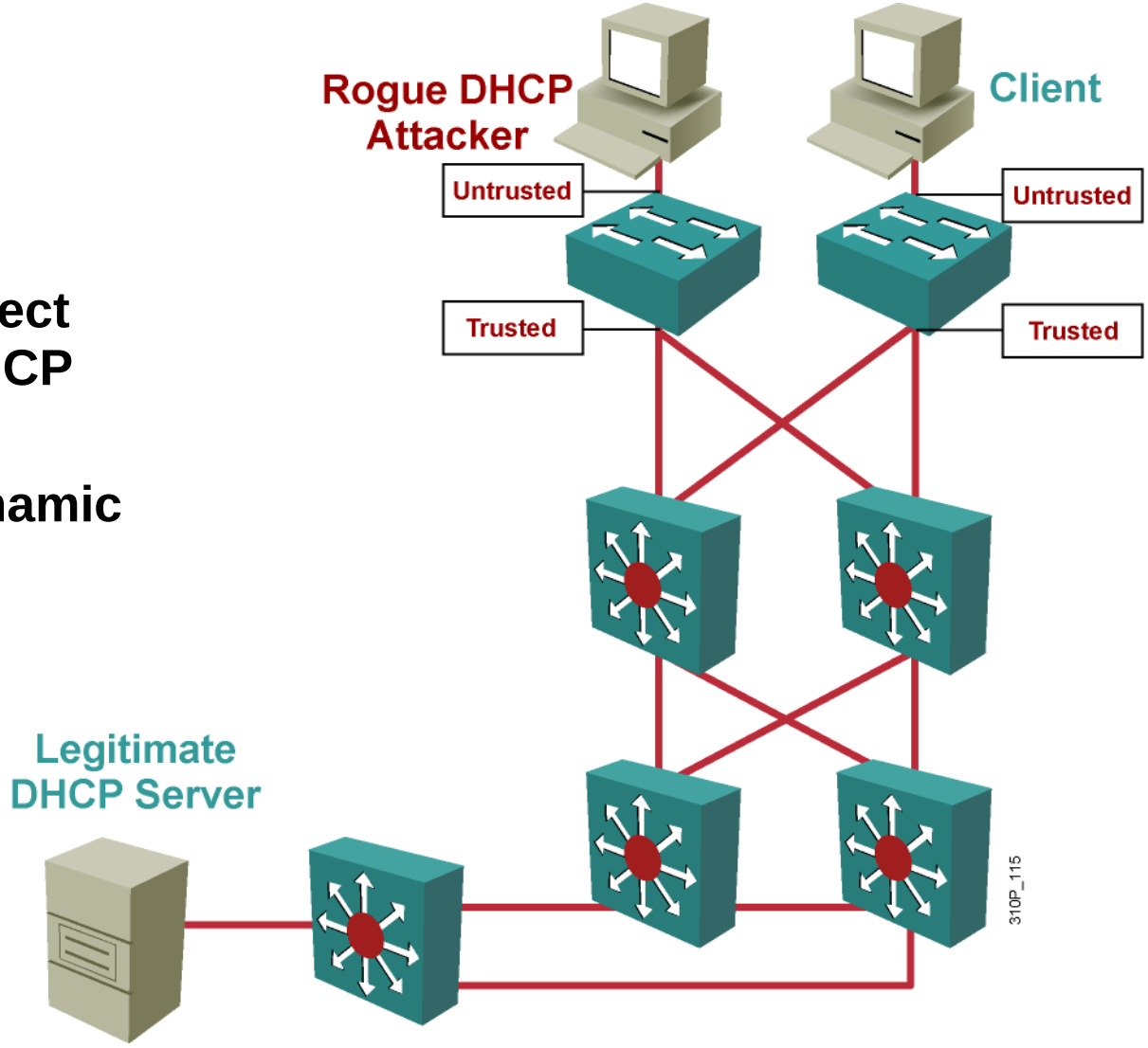
- **Enables DAI on an interface and sets the interface as a trusted interface**

```
Switch(config-if)#ip arp inspection validate {[src-mac]
[dst-mac] [ip]}
```

- **Configures DAI to drop ARP packets when the IP addresses are invalid**

Protection from ARP Spoofing

- **Configure to protect against rogue DHCP servers.**
- **Configure for dynamic ARP inspection.**



Layer 2 Security Best Practices

- **Manage switches in as secure a manner as possible (SSH, OOB, permit lists, etc.).**
- **Do not use VLAN 1 for anything.**
- **Set all user ports to nontrunking (unless you are using Cisco VoIP).**
- **Use port security where possible for access ports.**
- **Enable STP attack mitigation (BPDU guard, root guard).**
- **Use Cisco Discovery Protocol only where necessary—it is useful with phones.**
- **Disable all unused ports and put them in an unused VLAN.**


CISCO