Cisco Systems
Networking Academy

Cisco.com

Module 10 – Configure Filtering on a Switch

10.1 Introduction to Layer 2 Attacks

CCNA CISCO CERTIFIED

Högskolan Halmstad

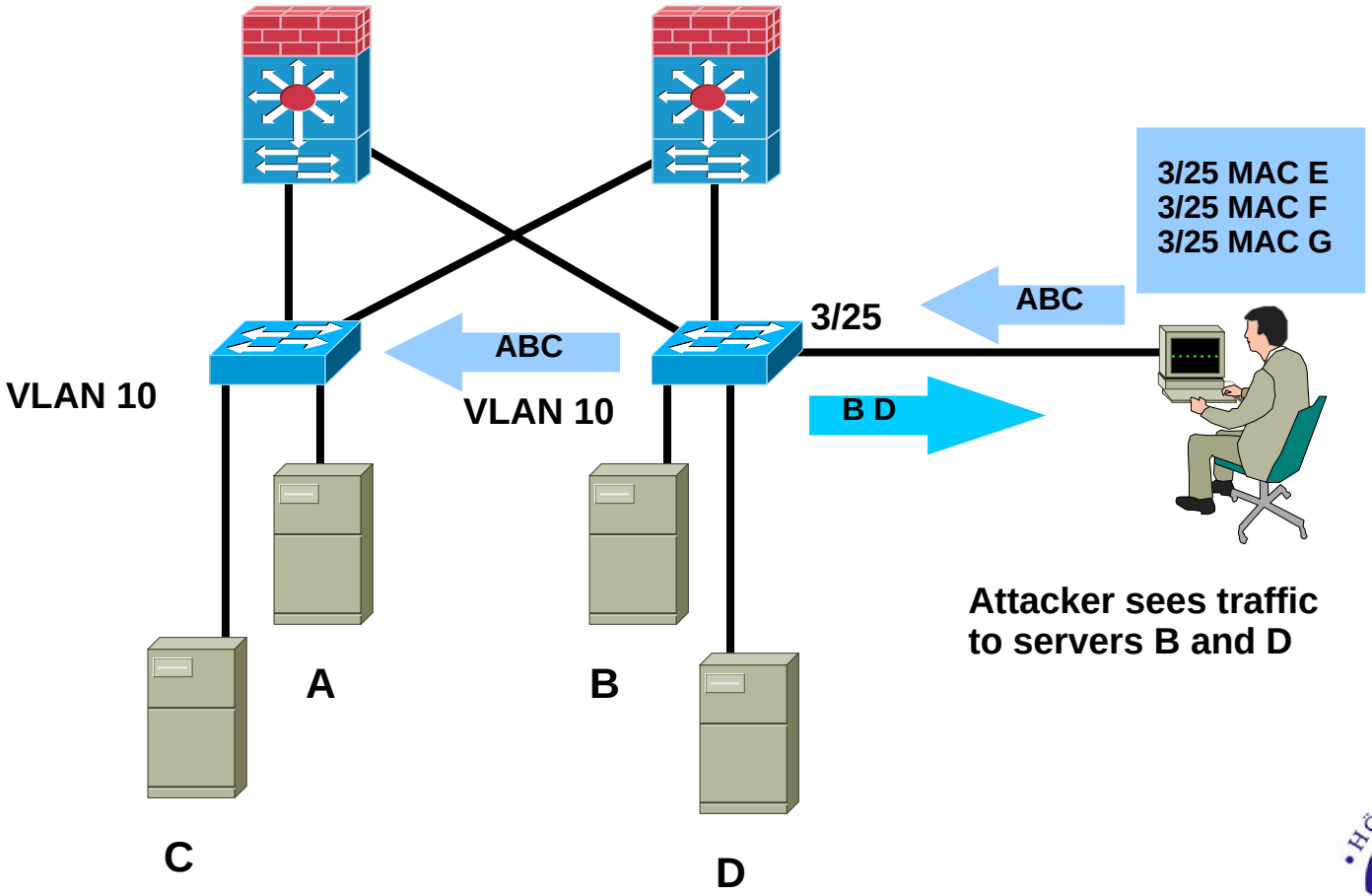
Types of Attacks

- CAM table overflow
- Media Access Control (MAC) address spoofing
- DHCP starvation

Module 10 – Configure Filtering on a Switch

10.2 MAC Address, ARP, and DHCP Vulnerabilities

CAM Table Overflow Attack



Mitigating the CAM Table Overflow Attack


```
switch(config-if)#
```

```
switchport port-security
```

- **Enable port security on interface.**

```
switch(config-if)#
```

```
switchport port-security [mac_addr]
```

- **Enable port security and set specific MAC address (H.H.H).**

Mitigating the CAM Table Overflow Attack


```
switch(config-if)#
```

```
switchport port-security maximum (1-132)
```

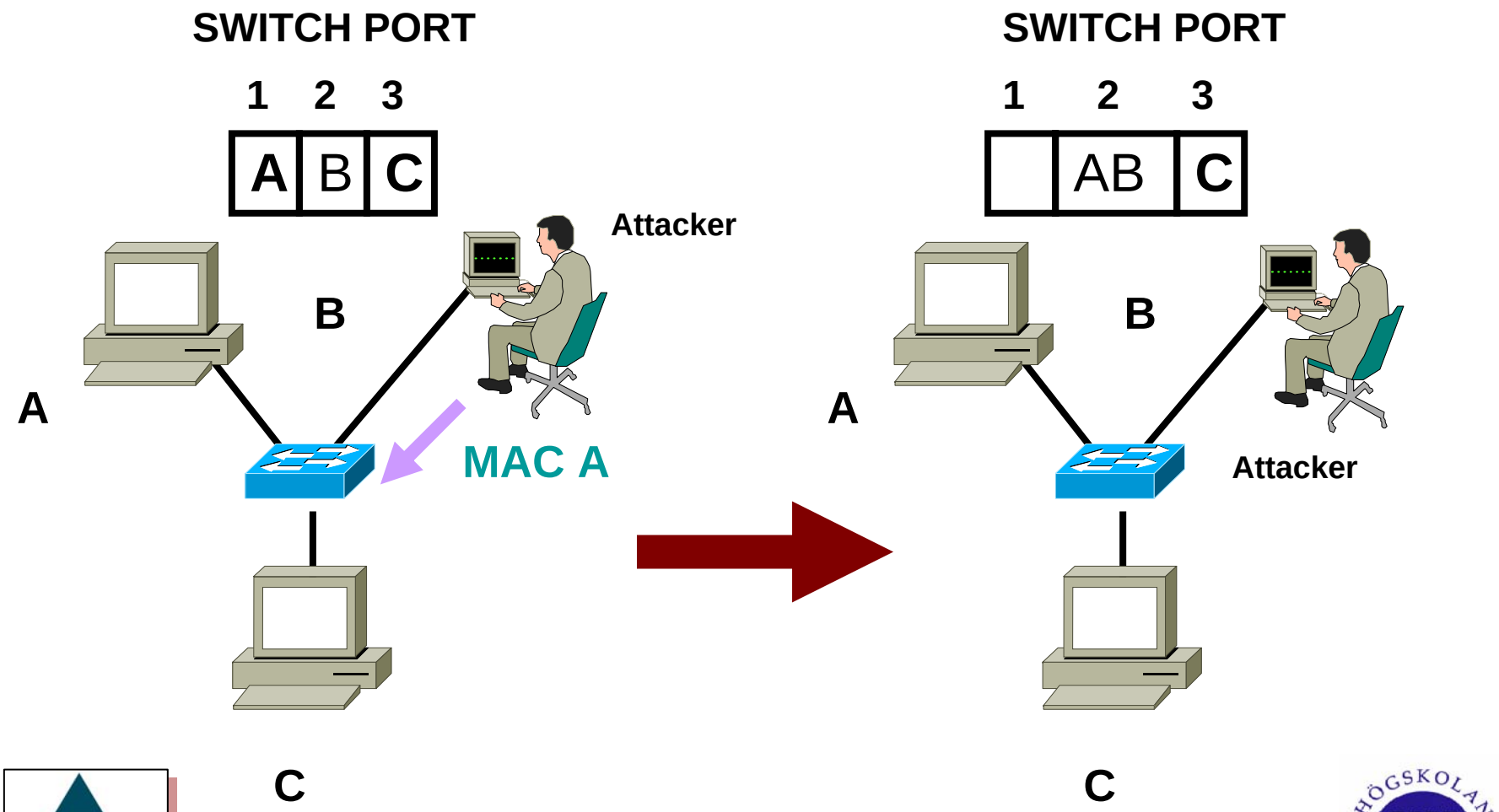
- **Set maximum number of MAC addresses.**

```
switch(config-if)#
```

```
switchport port-security violation shutdown [protect |
restrict | shutdown]
```

- **Set action on violation.**

MAC Spoofing – Man in the Middle Attacks



Mitigating MAC Spoofing Attacks – Cisco IOS


```
switch(config-if)#
port security max-mac-count {1-132}
```

- **Enable port security and set maximum MAC address.**

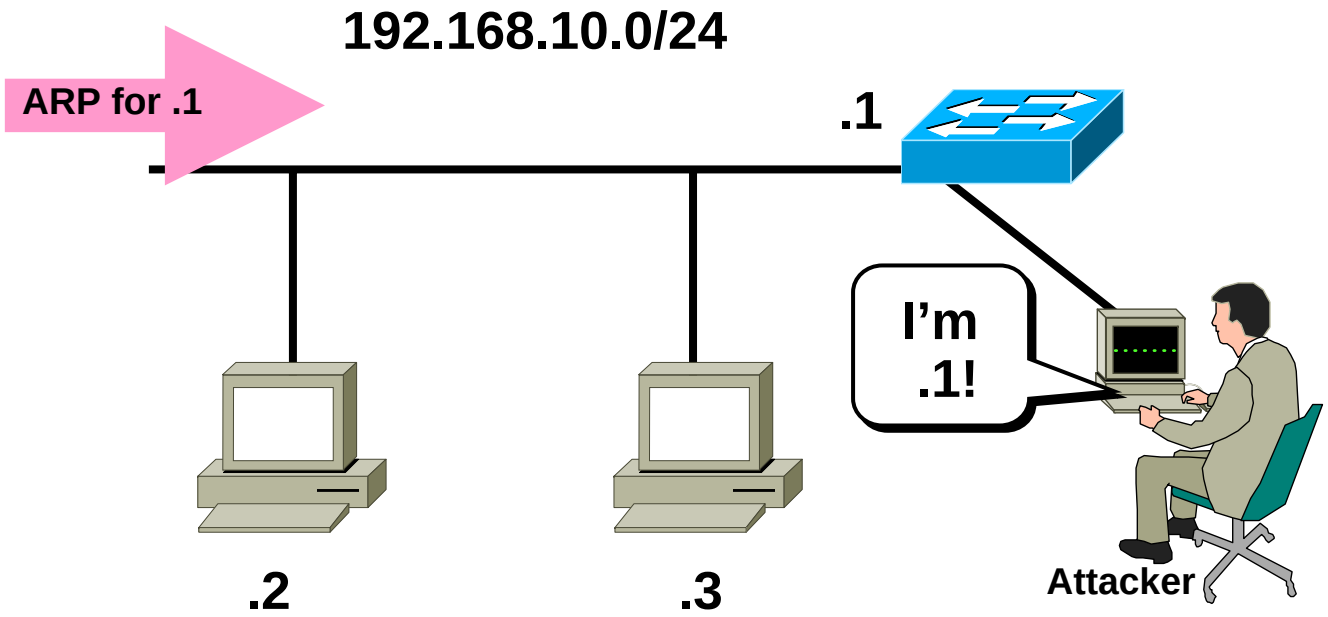
```
switch(config-if)#
port security action {shutdown|trap}
```

- **Specify action to take when violation occurs.**

```
switch(config-if)#
arp timeout seconds
```

- **Specify ARP timeout.**

ARP Spoofing



Mitigating ARP Spoofing with DHCP Snooping


```
switch(config)#
ip dhcp snooping
```

- **Enable DHCP Snooping.**

```
switch(config)#
ip dhcp snooping vlan vlan_id {,vlan_id}
```

- **Enable DHCP Snooping for specific VLANs.**

```
switch(config-if)#
ip dhcp snooping trust
```

- **Configure an interface as trusted for DHCP snooping purposes.**

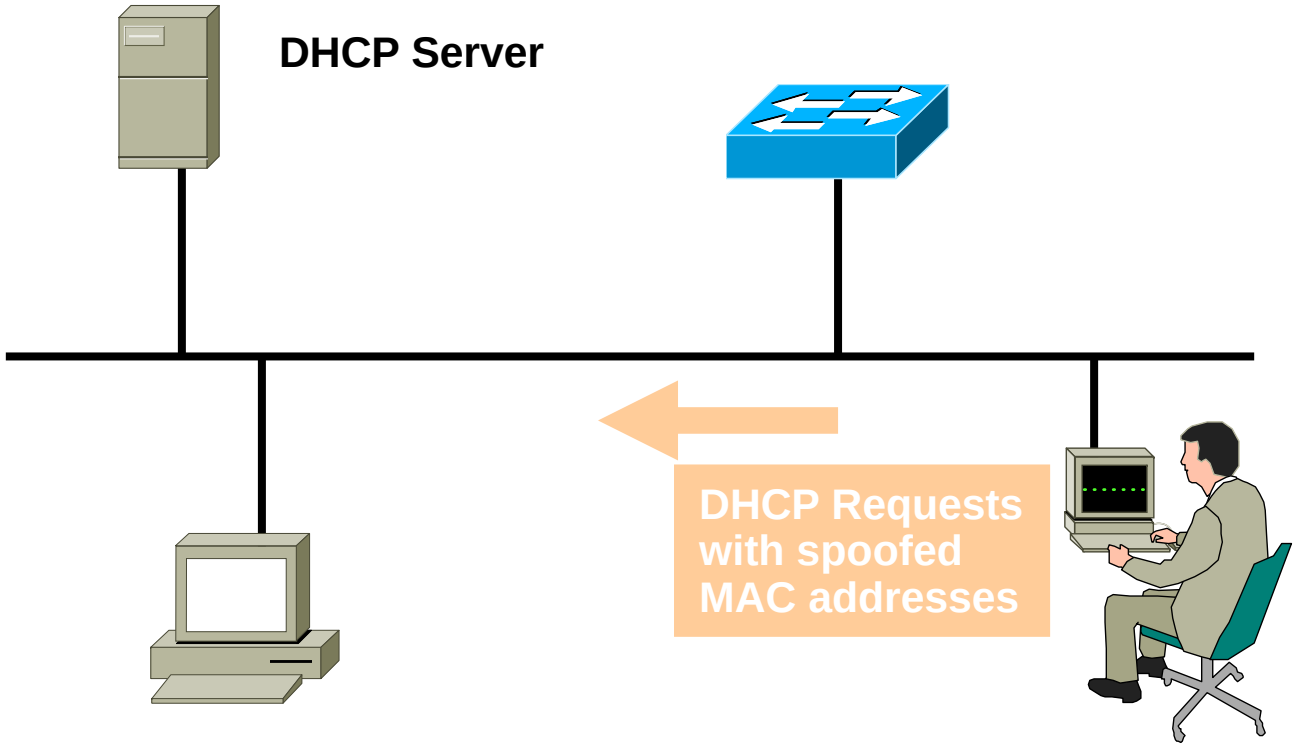
Mitigating ARP Spoofing with DHCP Snooping


```
switch(config-if)#
```

```
ip dhcp snooping limit rate rate
```

- **Set rate limit for DHCP Snooping.**

DHCP Starvation



Attacker attempting to set up rogue DHCP Server

Commands to Mitigate DHCP Starvation Attacks


```
switch(config)#
```

```
ip dhcp snooping
```

- **Enable DHCP Snooping.**

```
switch(config)#
```

```
ip dhcp snooping vlan vlan_id {,vlan_id}
```

- **Enable DHCP Snooping for specific VLANs.**

```
switch(config-if)#
```

```
ip dhcp snooping trust
```

- **Set interface to trusted state.**

Commands to Mitigate DHCP Starvation Attacks (Cont.)


```
switch(config-if)#
```

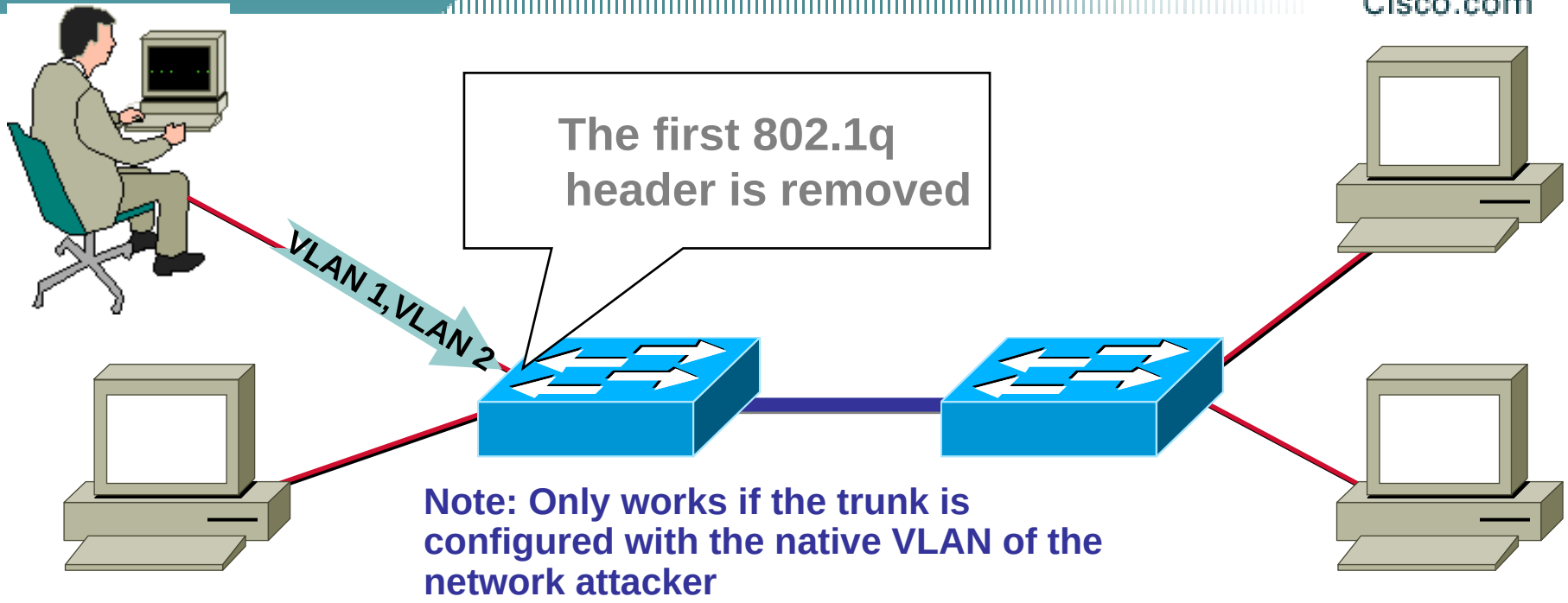
```
ip dhcp snooping limit rate rate
```

- **Set rate limit for DHCP Snooping.**

Module 10 – Configure Filtering on a Switch

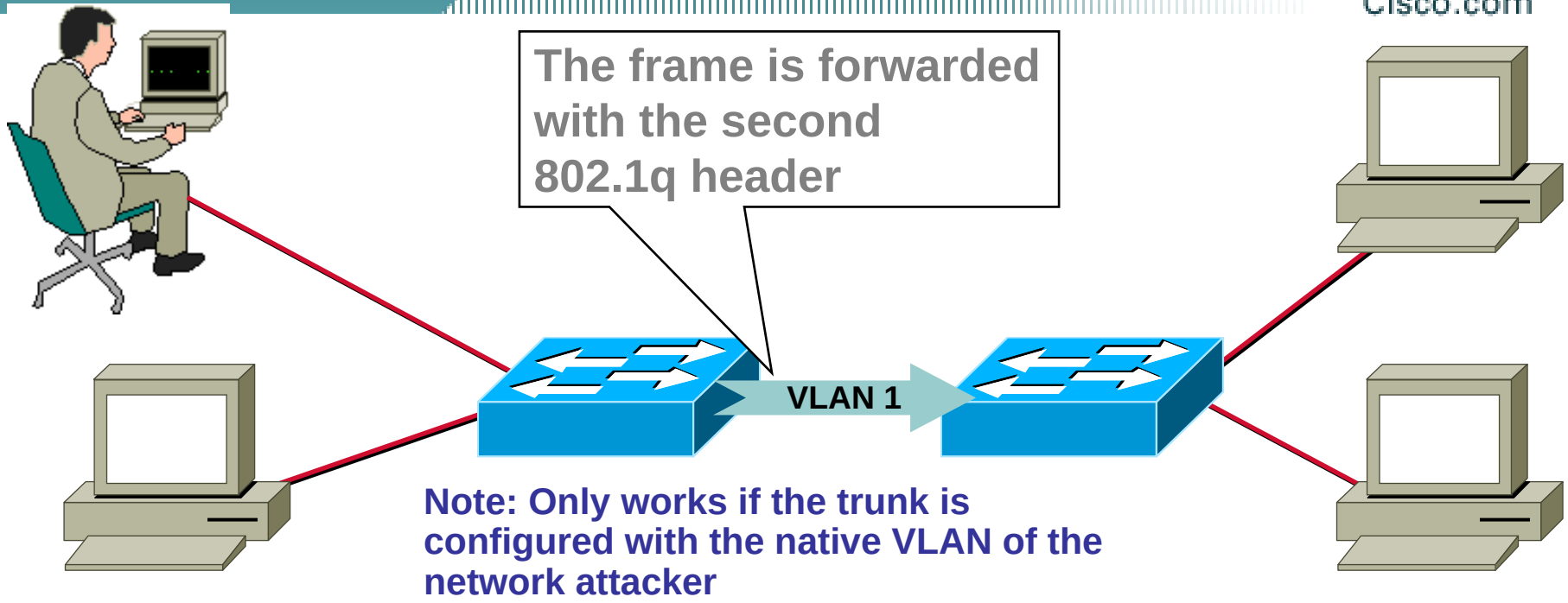
10.3 VLAN Vulnerabilities

Double 802.1q Encapsulation VLAN Hopping Attack



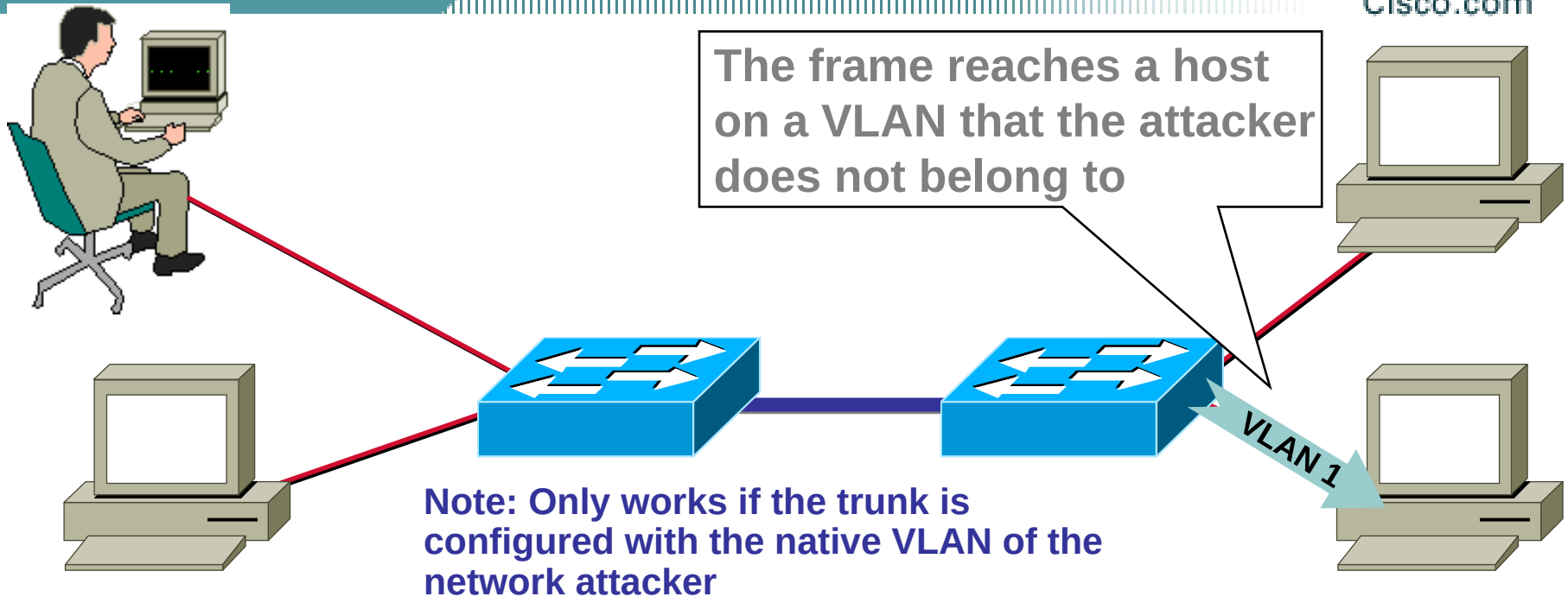
- Send 802.1q double encapsulated frames
- Switch performs only one level of decapsulation
- Unidirectional traffic only
- Works even if trunk ports are set to off

Double 802.1q Encapsulation VLAN Hopping Attack



- Send 802.1q double encapsulated frames
- Switch performs only one level of decapsulation
- Unidirectional traffic only
- Works even if trunk ports are set to off

Double 802.1q Encapsulation VLAN Hopping Attack



- Send 802.1q double encapsulated frames
- Switch performs only one level of decapsulation
- Unidirectional traffic only
- Works even if trunk ports are set to off

Security Best Practices for VLANs and Trunking

- Always use a dedicated VLAN ID for all trunk ports
- Disable unused ports and put them in an unused VLAN
- Be paranoid – Do not use VLAN 1 for anything
- Disable auto-trunking on user facing ports (DTP off)
- Explicitly configure trunking on infrastructure ports
- Use all tagged mode for the native VLAN on trunks

Cisco Systems Networking Academy

Cisco.com

Module 10 – Configure Filtering on a Switch

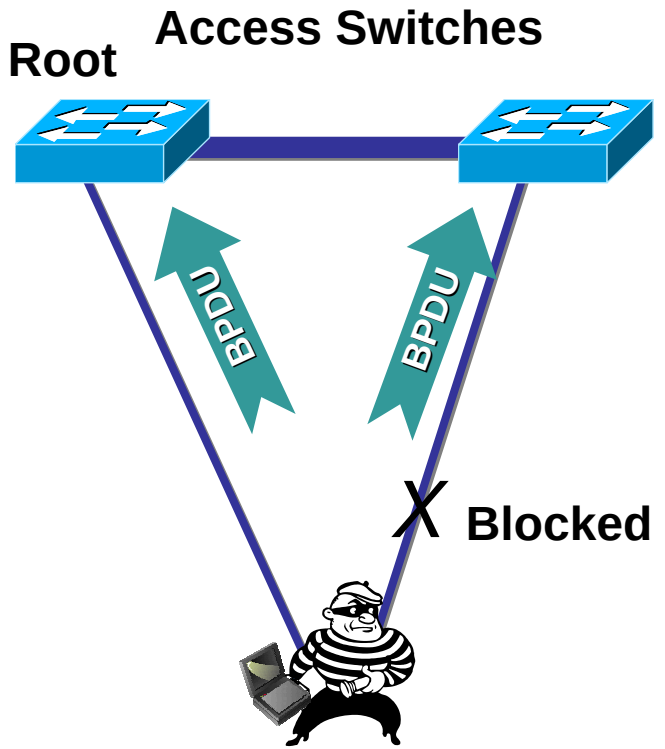
10.4 Spanning-Tree Vulnerabilities

CCNA CISCO CERTIFIED

Högskolan Halmstad

Spanning Tree Attack Example

- The attacker sends BPDU messages to become the root bridge



Spanning Tree Attack Example

- The attacker sends BPDU messages to become the root bridge
  - The attacker then sees frames he shouldn't
    - Man in the middle and DoS attacks become possible
    - This attack requires that the attacker is connected to two different switches. This can be done with either multiple NICs or a with a hub.