Executing Spoofing Attacks

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

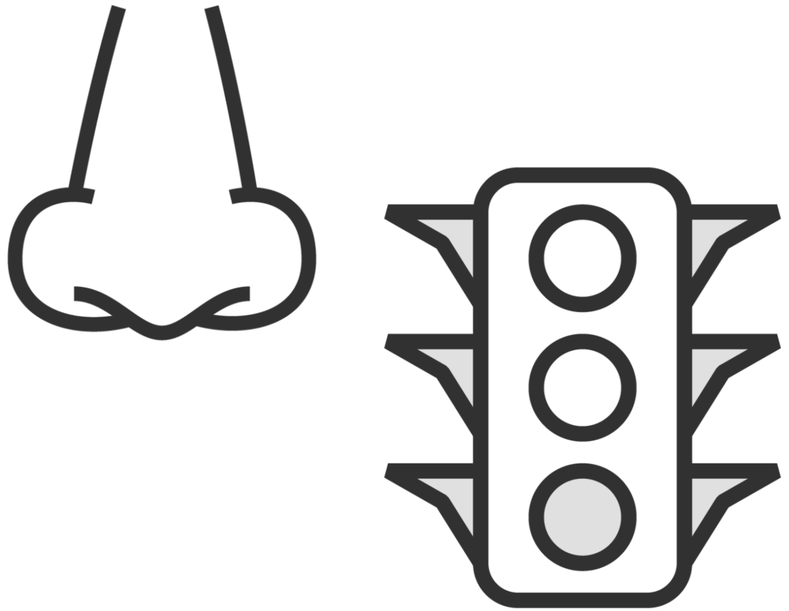
dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

“He imitated me so well that I couldn't stand myself any longer.”

Georges Pompidou

Spoofing Techniques

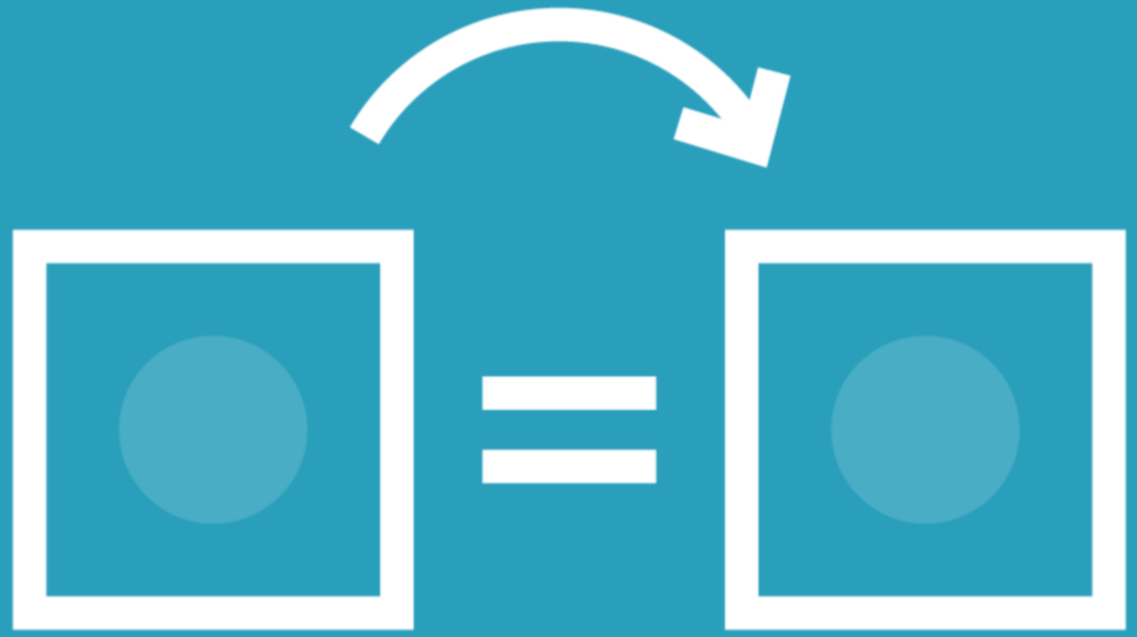
- ARP spoofing
- MAC spoofing
- IRDP spoofing
- VLAN hopping
- STP attacks

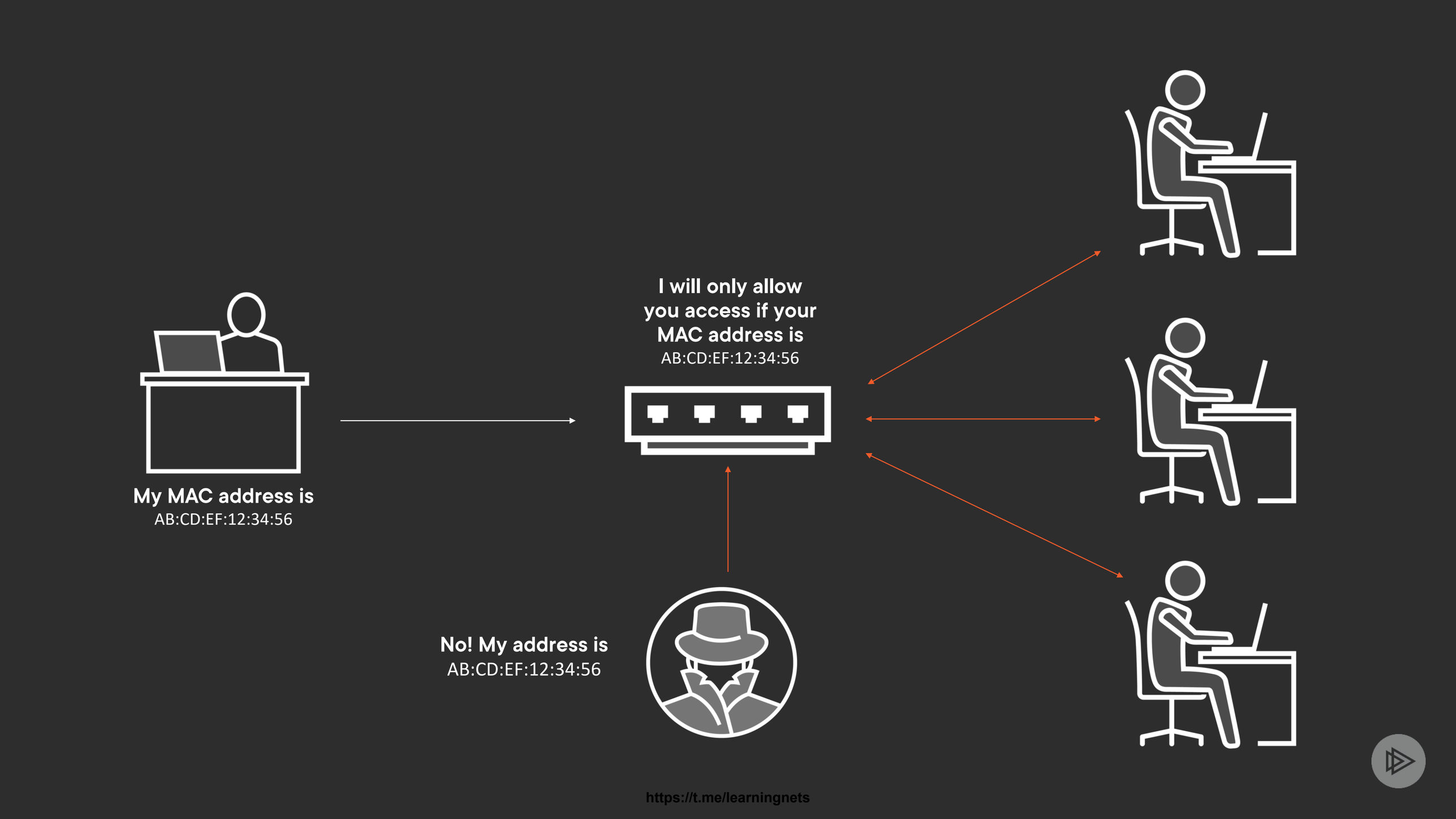


MAC Spoofing

IDS (Intrusion Detection System)

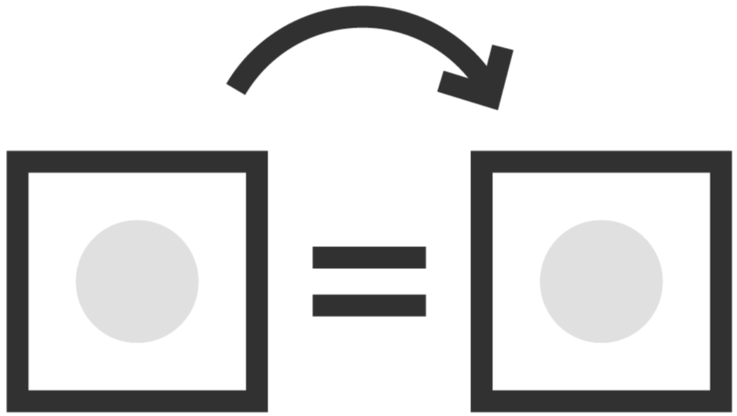
IPS (Intrusion Prevention System)





Wireless and MAC Spoofing

MAC Spoofing



MAC flooding

Man-in-the-middle attacks

Phishing attacks

MAC Spoofing Tools

SMAC

MAC address changer

Change MAC address

Easy MAC changer

Spoof-me-now

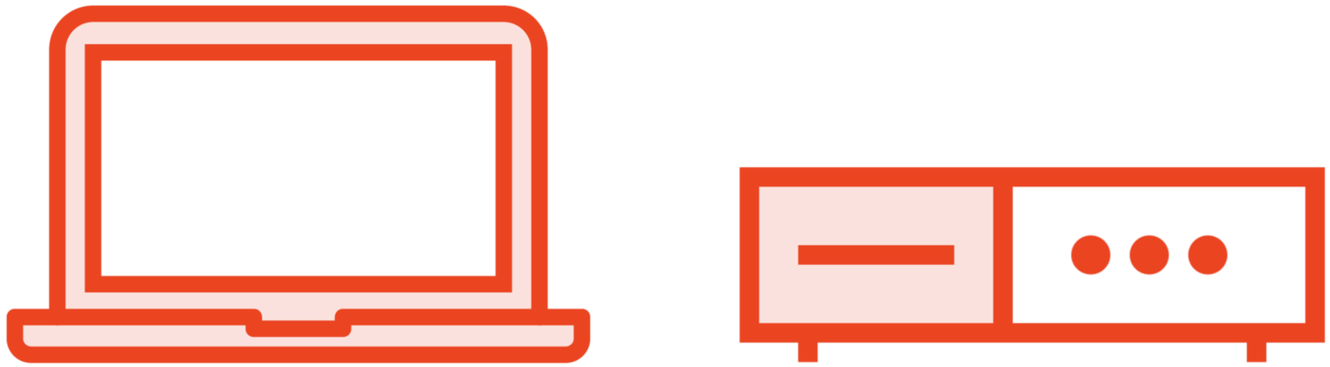
Demo

MAC Spoofing

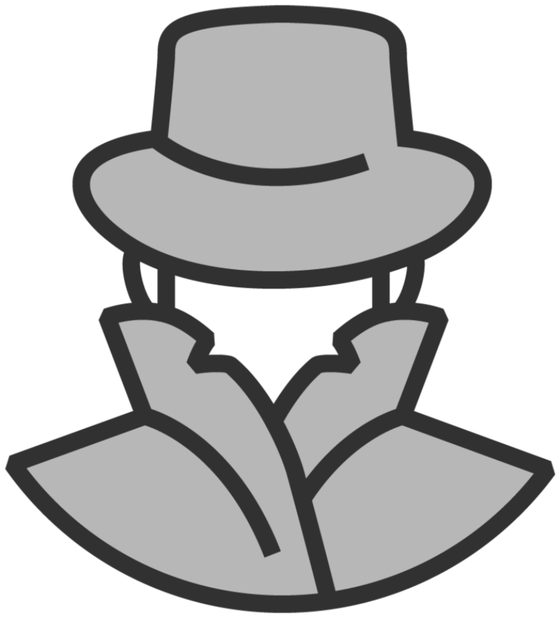
IRDP Spoofing

IRDP (ICMP Router Discovery Protocol)

A routing protocol for systems to detect routers on their own subnets.



Three Methods to use IRDP

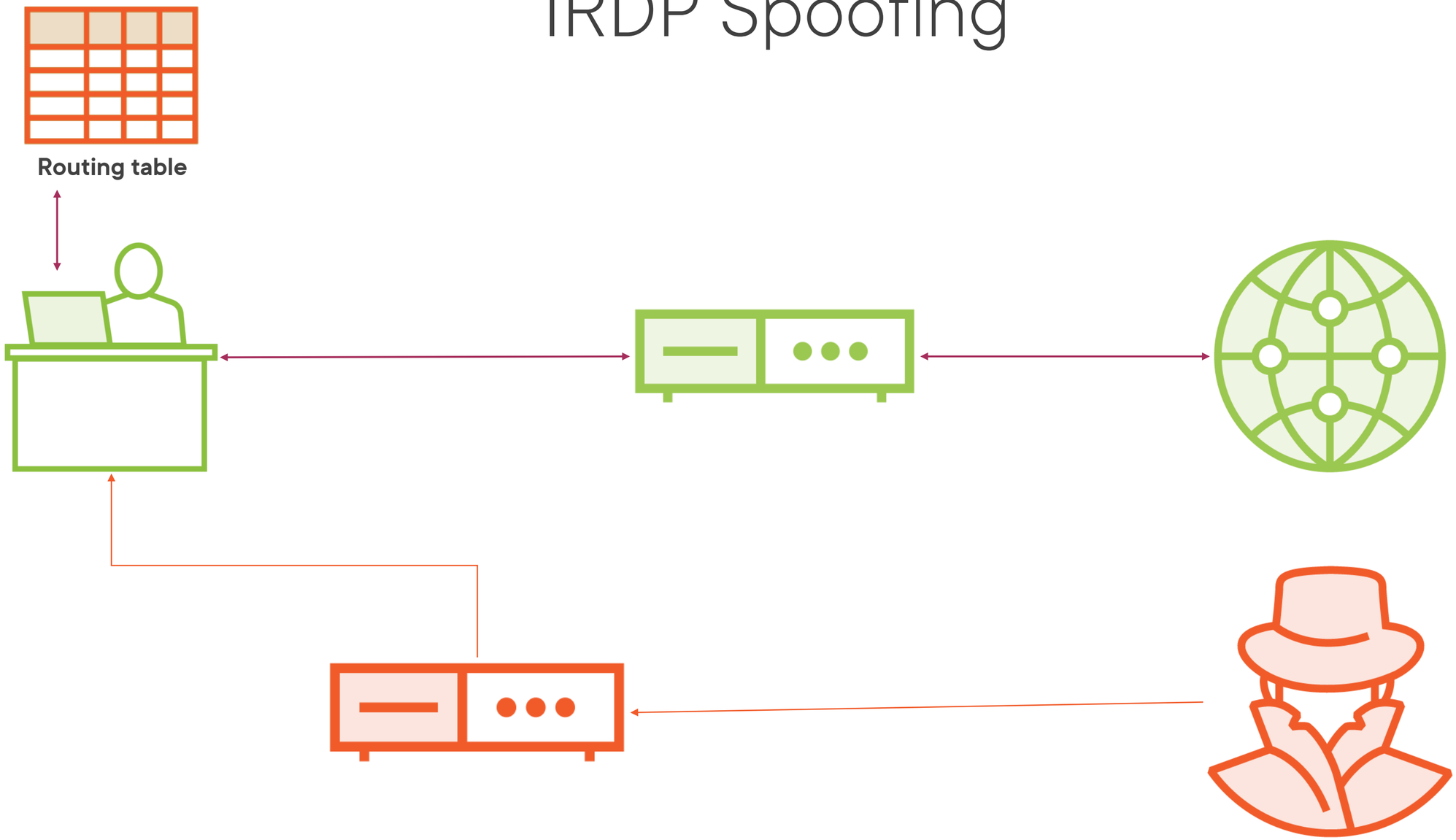


Passive sniffing

Man-in-The-Middle (MiTM)

Denial of Service (DoS)

IRDP Spoofing



IRDP doesn’t require any type of authentication

VLAN Hopping

VLAN Hopping

VLAN Hopping is used to gain access to traffic flowing in other VLANs in the same network

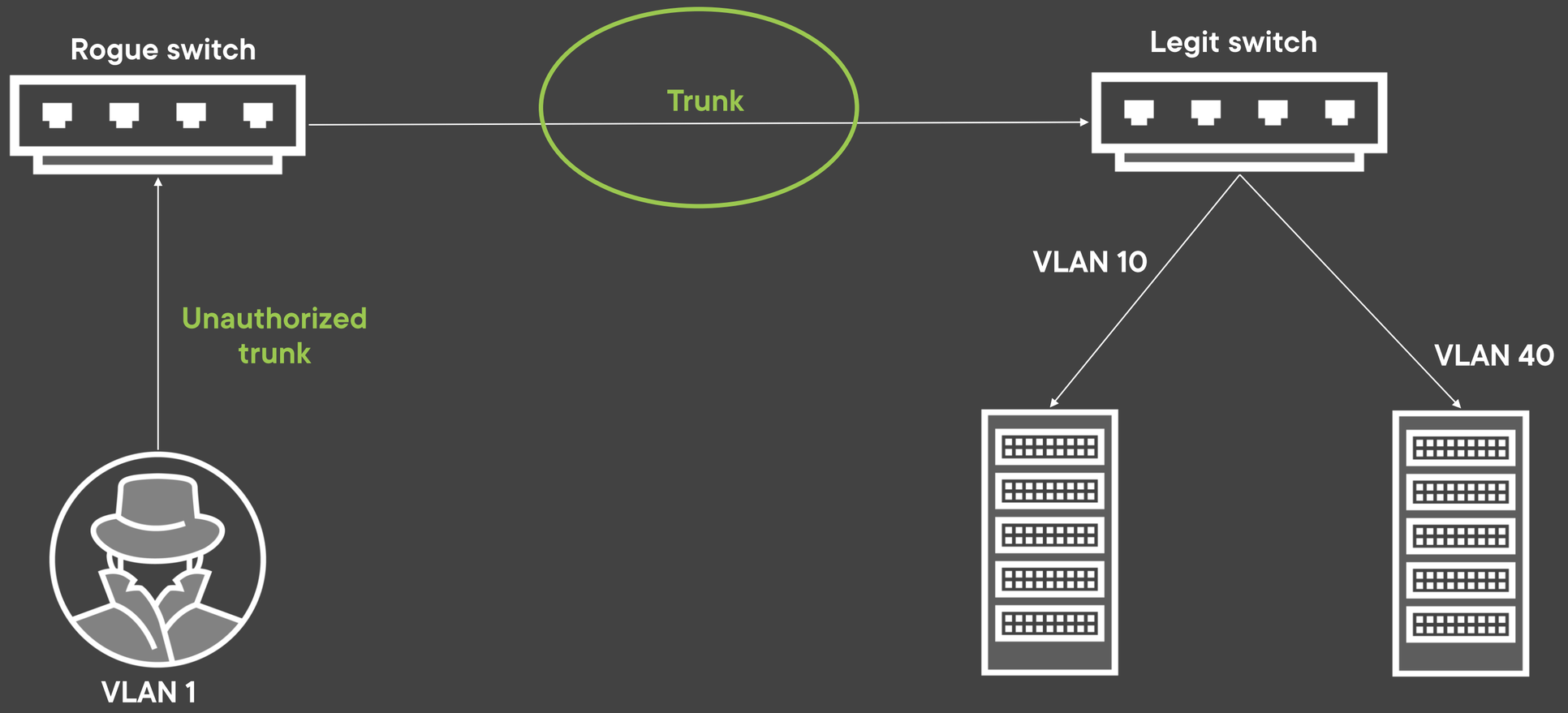
Switch spoofing

Attacker creates a trunk line by connecting a rogue switch into the network

Double tagging

Attacker adds and modifies tags in the Ethernet frame

Switch Spoofing

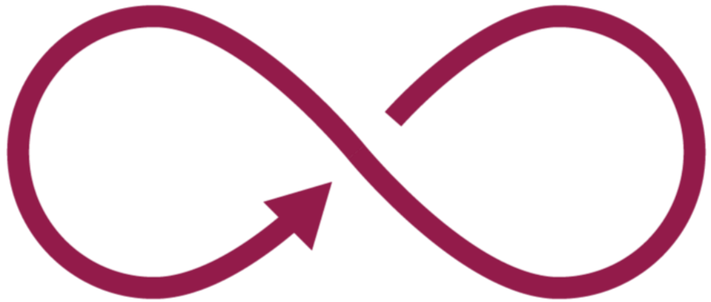


Double Tagging

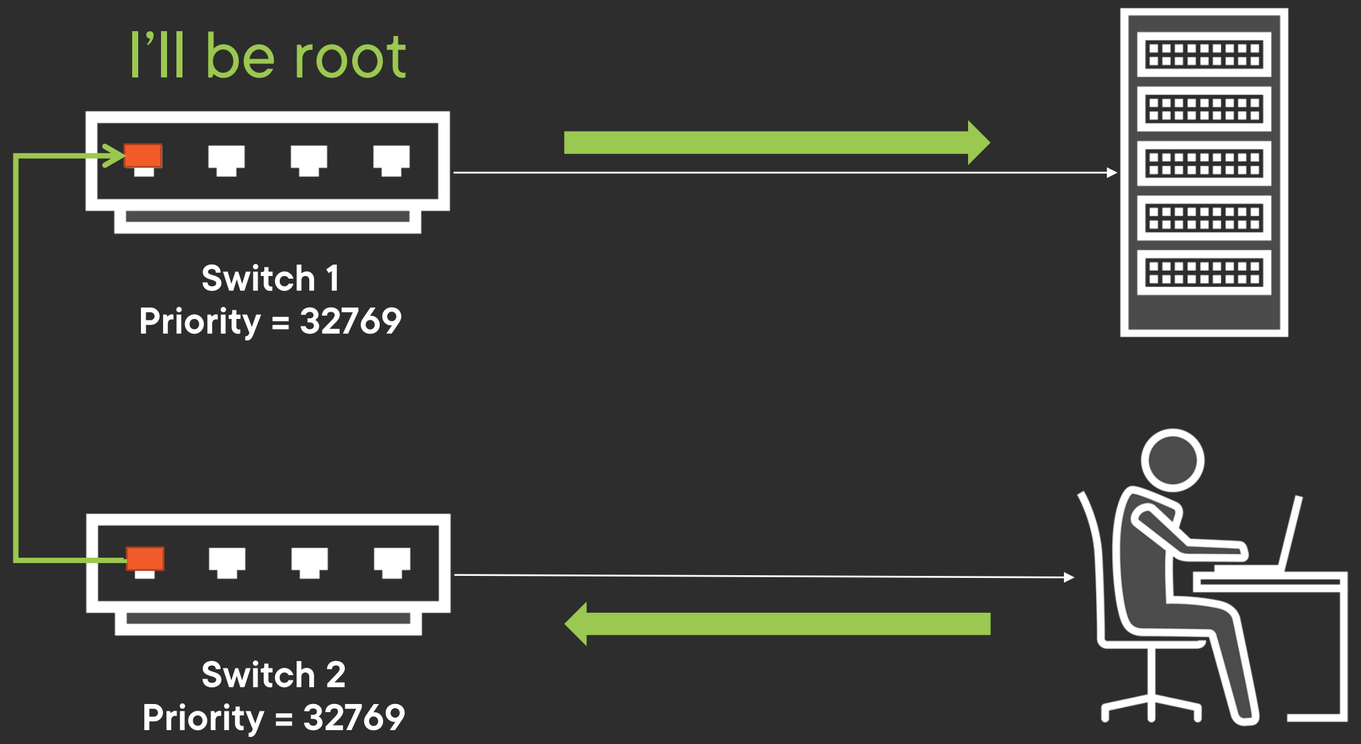
STP Attack

STP (Spanning Tree Protocol)

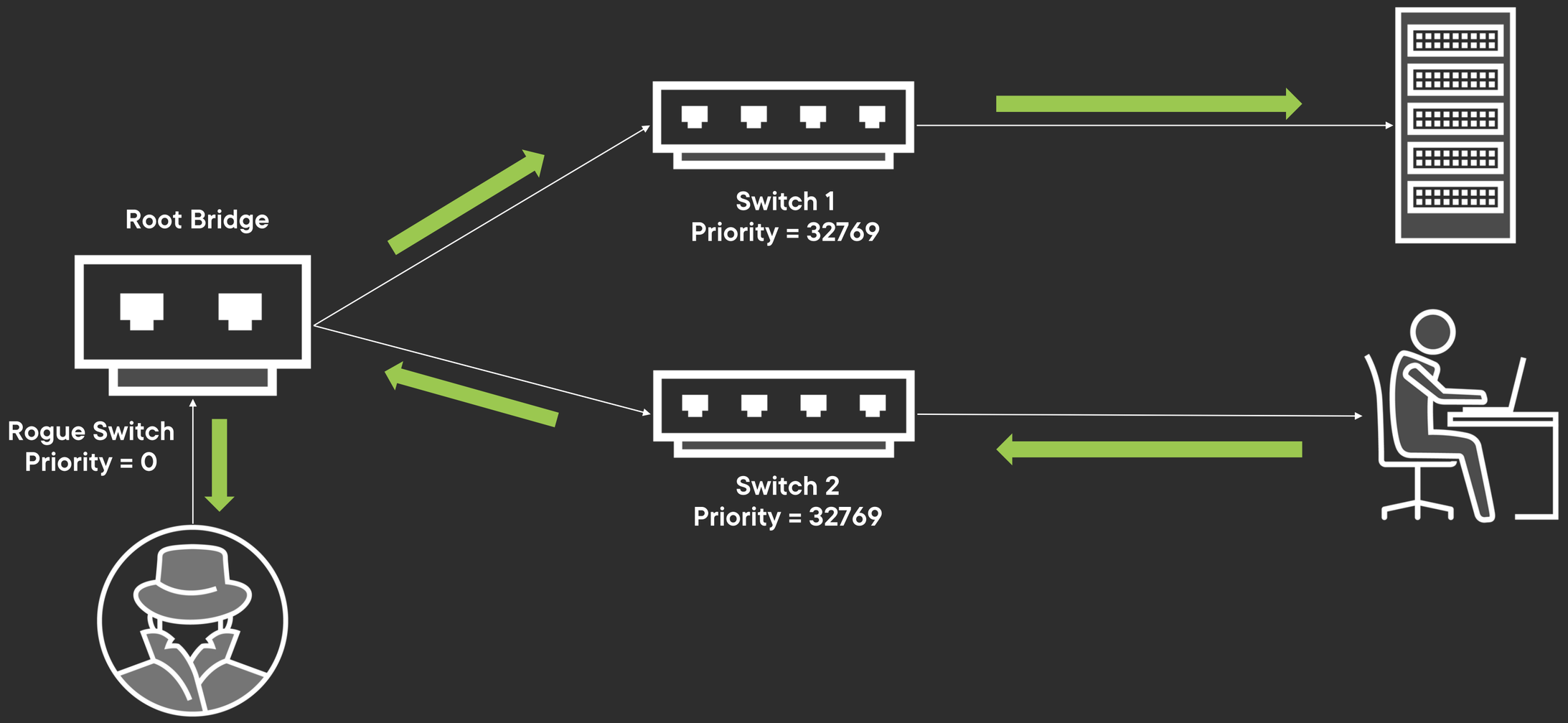
A protocol for preventing loops in network topologies that can slow down or crash a network.



STP Attack



STP Attack



Countermeasures

How to Defend Against MAC Spoofing

How to Defend Against MAC Spoofing

Must know all the MAC addresses

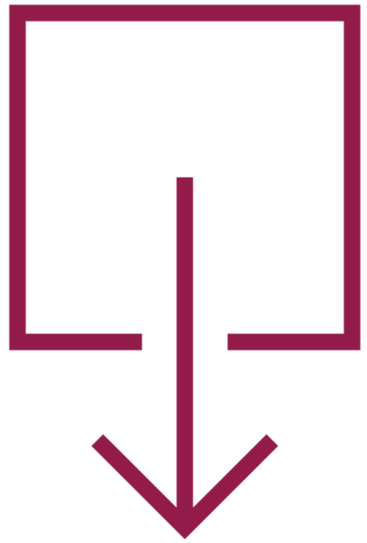
Place the server behind the router

Routers use only IP addresses

Change the port security interface configuration

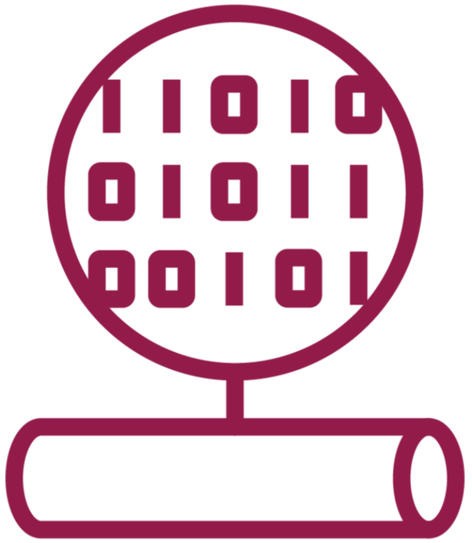
Defending a MAC Spoof

DHCP Snooping Binding Table



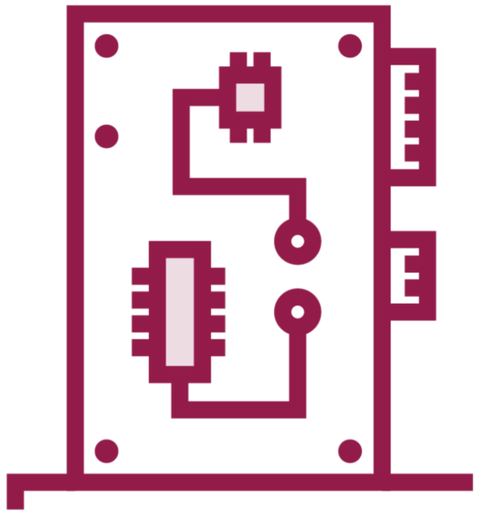
Dynamic ARP Inspection

IP Source Guard



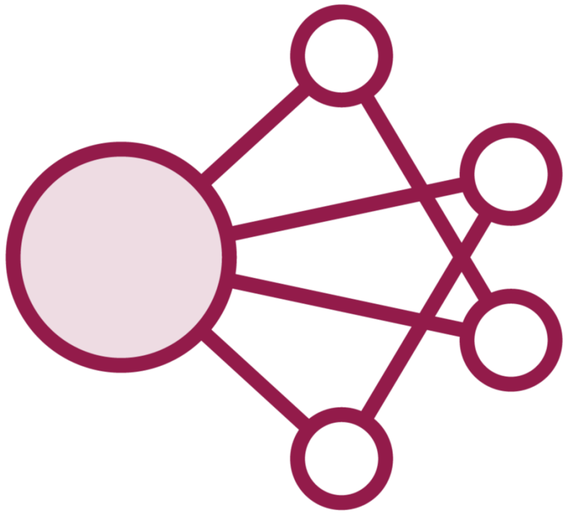
Encryption

Defending a MAC Spoof



Retrieval of MAC Address

Implementation of IEEE 802.1X Suites



AAA Authentication, Authorization, and Accounting

How to Defend Against VLAN Hopping

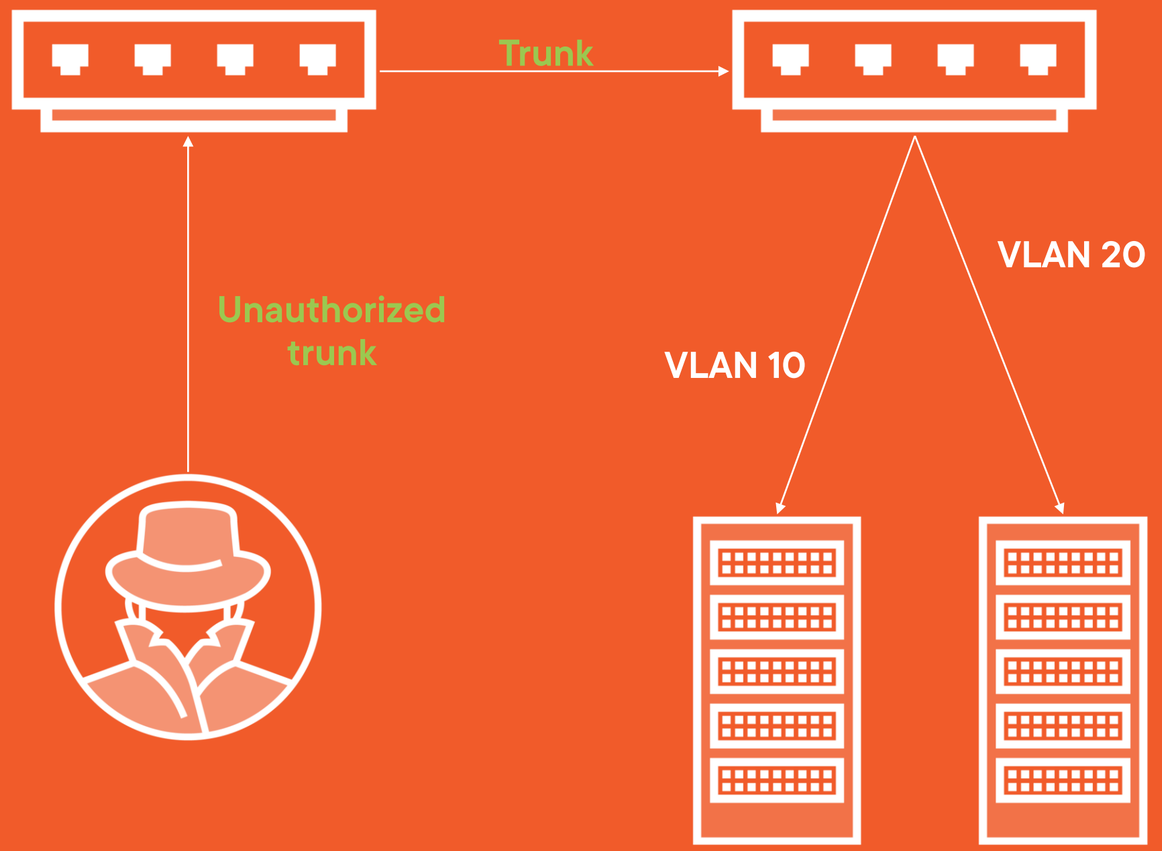
Defend Against Switch Spoofing

Configure the ports as access ports and ensure all are configured not to negotiate trunks

```
switchport mode access
switchport mode nonegotiate
```

Configure trunk ports not to negotiate trunks

```
switchport mode trunk
switchport mode nonegotiate
```



Defend Against Double Tagging

Assign all access ports with VLAN except the default (VLAN1)

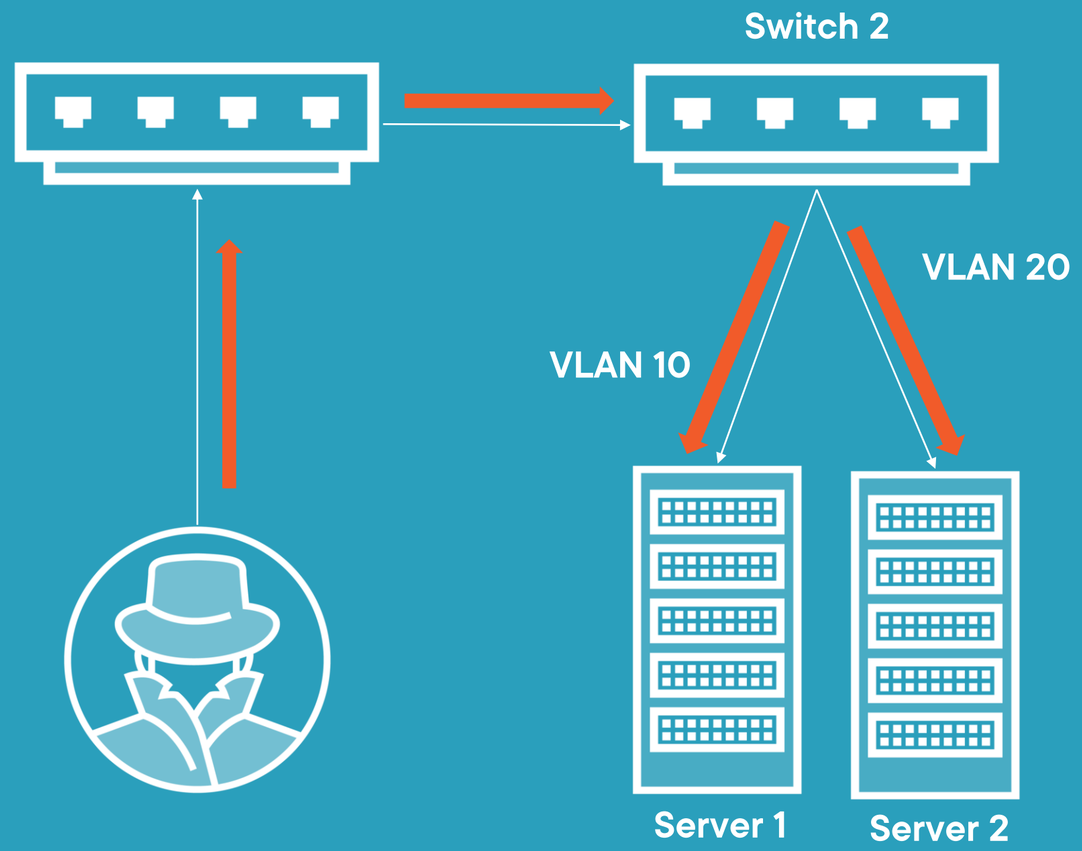
```
switchport access vlan 2
```

Change native VLANs on trunk ports to an unused VLAN ID

```
Switchport trunk native vlan 999
```

Explicitly tag all native VLANs

```
Vlan dot1q tag native
```



How to Defend Against STP Spoofing

STP Defense

- **BPDU Guard**
- **Root Guard**
- **Loop Guard**
- **UDLD**

Learning Checks

Learning Check

- IRDP
- Switch spoofing
- STP
- Double tagging
- BRDU Guard

Up Next:
Playing with DNS Poisoning Attacks