Addressing ARP-related Security Risks

Jim Rizzo
NETWORK ENGINEER AND SECURITY LEADER

Overview

ARP & Denial of Service (DoS)

- ARP broadcast storms
- ARP Poisoning Blackhole

Switch CAM Table Flooding

ARP Spoofing, Man in the Middle (MITM) Attacks

Mitigation techniques

Overview

ARP broadcast storm

- Hardware problems
- Software misconfigurations
- Hacker Denial of Service (Dos)

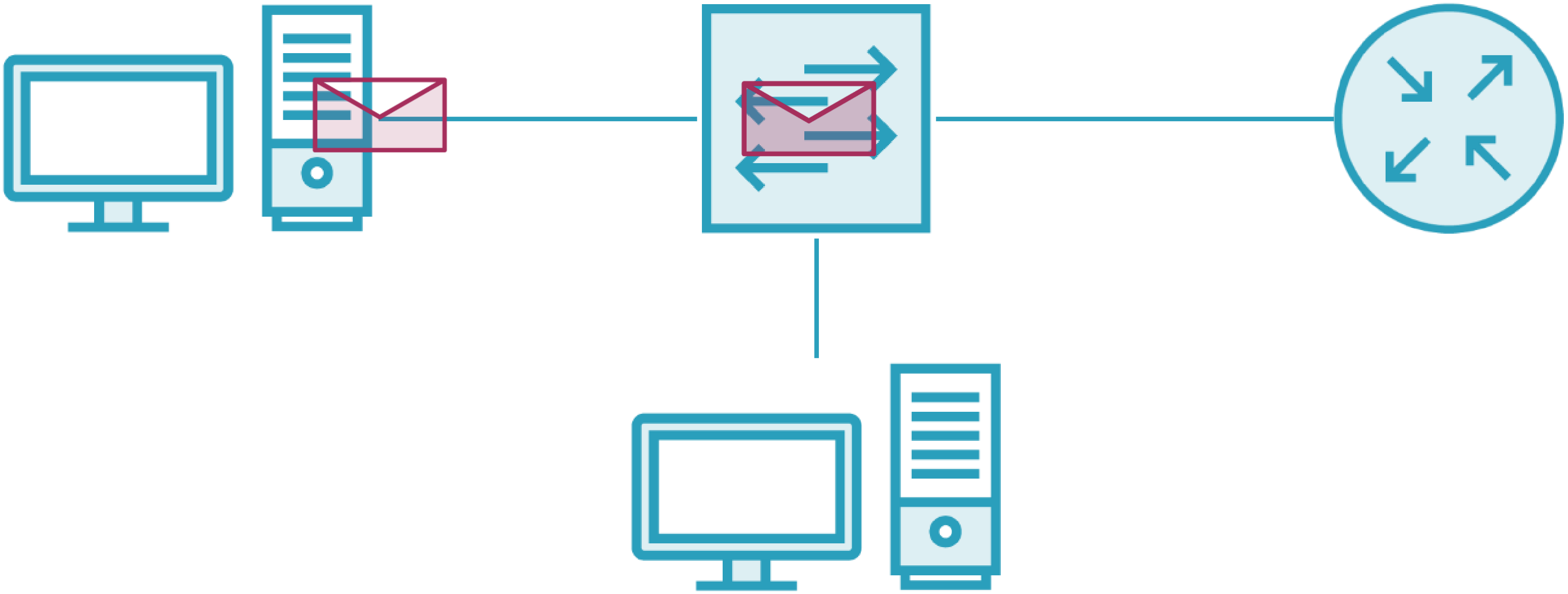
Mitigations

- Broadcast storm control
- Intrusion detection/prevention
- Network authentication

ARP Broadcast Scope

ARP Broadcast Packet

Destination ffff.ffff.ffff



Denial of Service

Too much broadcast traffic is called a broadcast storm

As broadcast storms worsen, they negatively impact network systems

Denial of Service disrupts normal use making resources unavailable to intended users

DoS conditions may cause unstable network or machines to crash

ARP Broadcast Storm Sources

Hardware

Bad NIC or
Physical loop

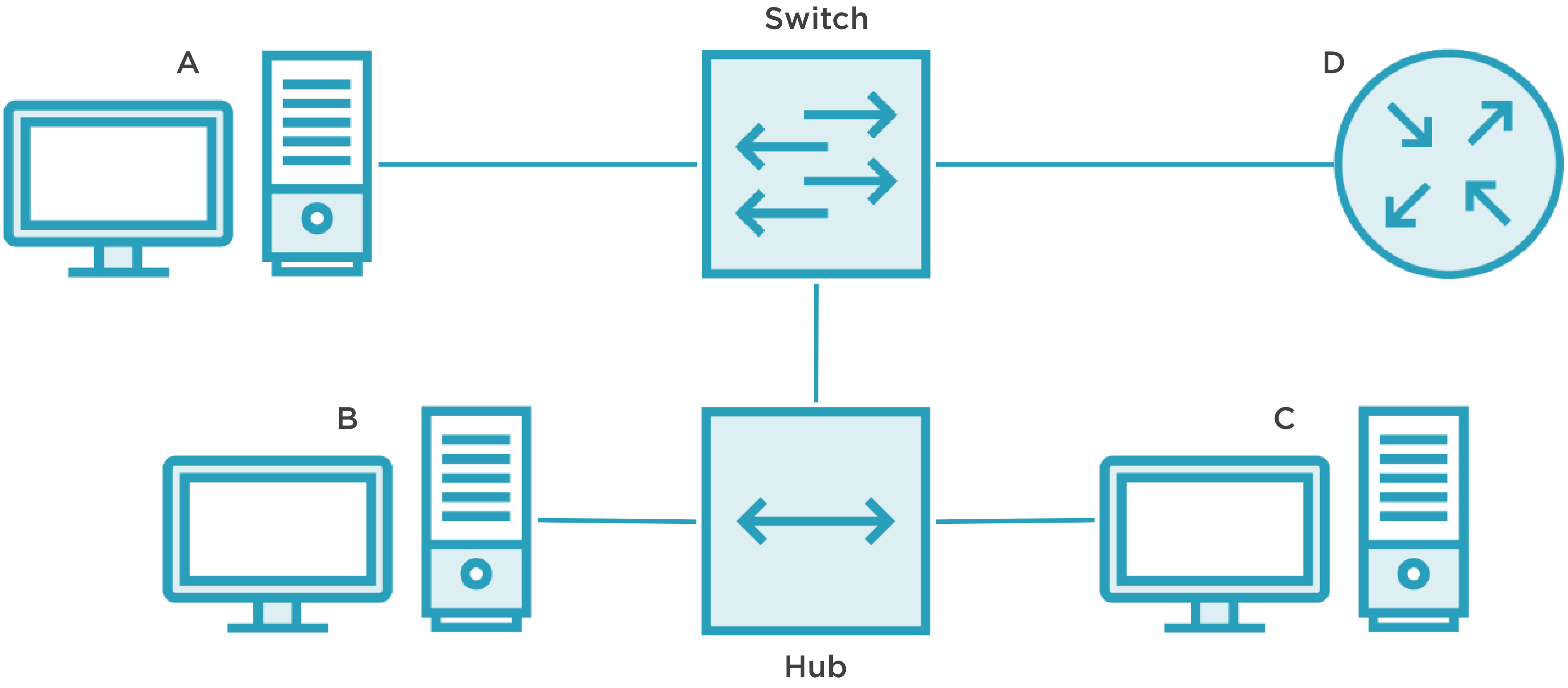
Software

Spanning Tree Protocol loop
or Device misconfiguration

Malicious attack

Malware (virus/worms)
or Live software attack

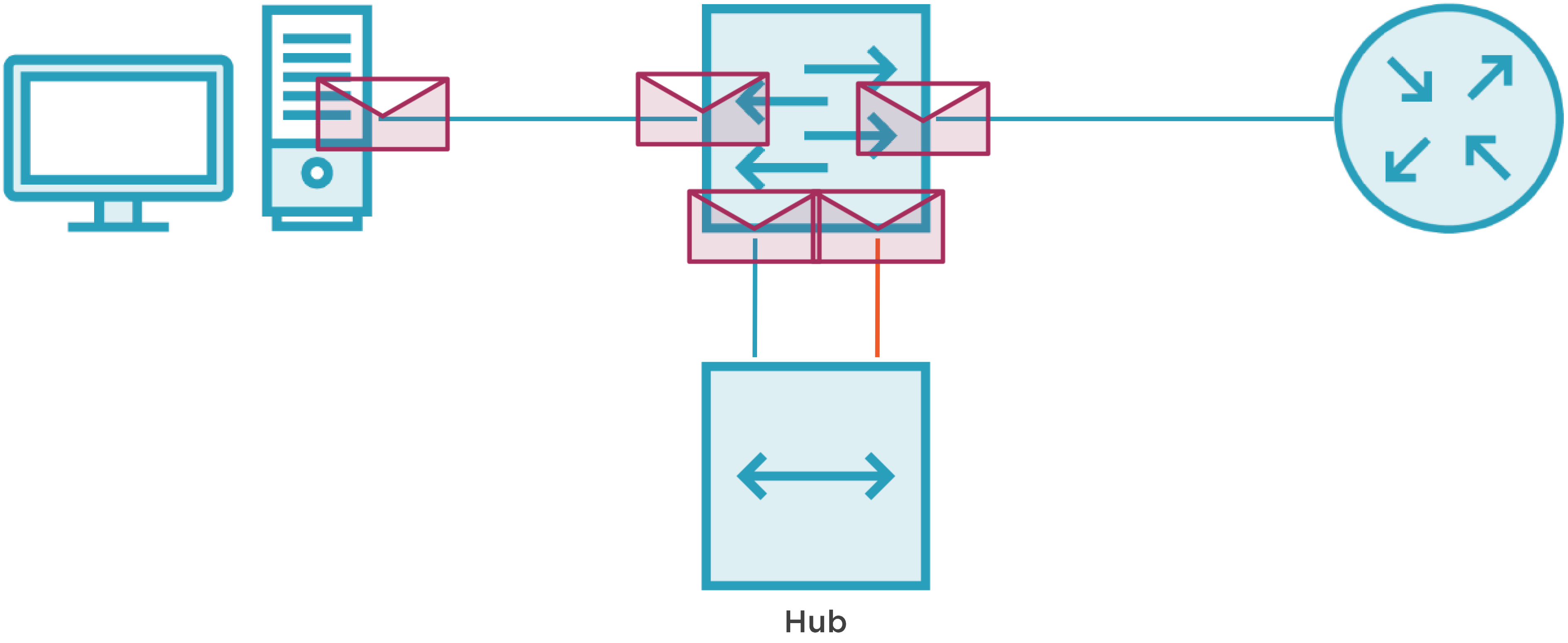
Hub – Multiport Repeater



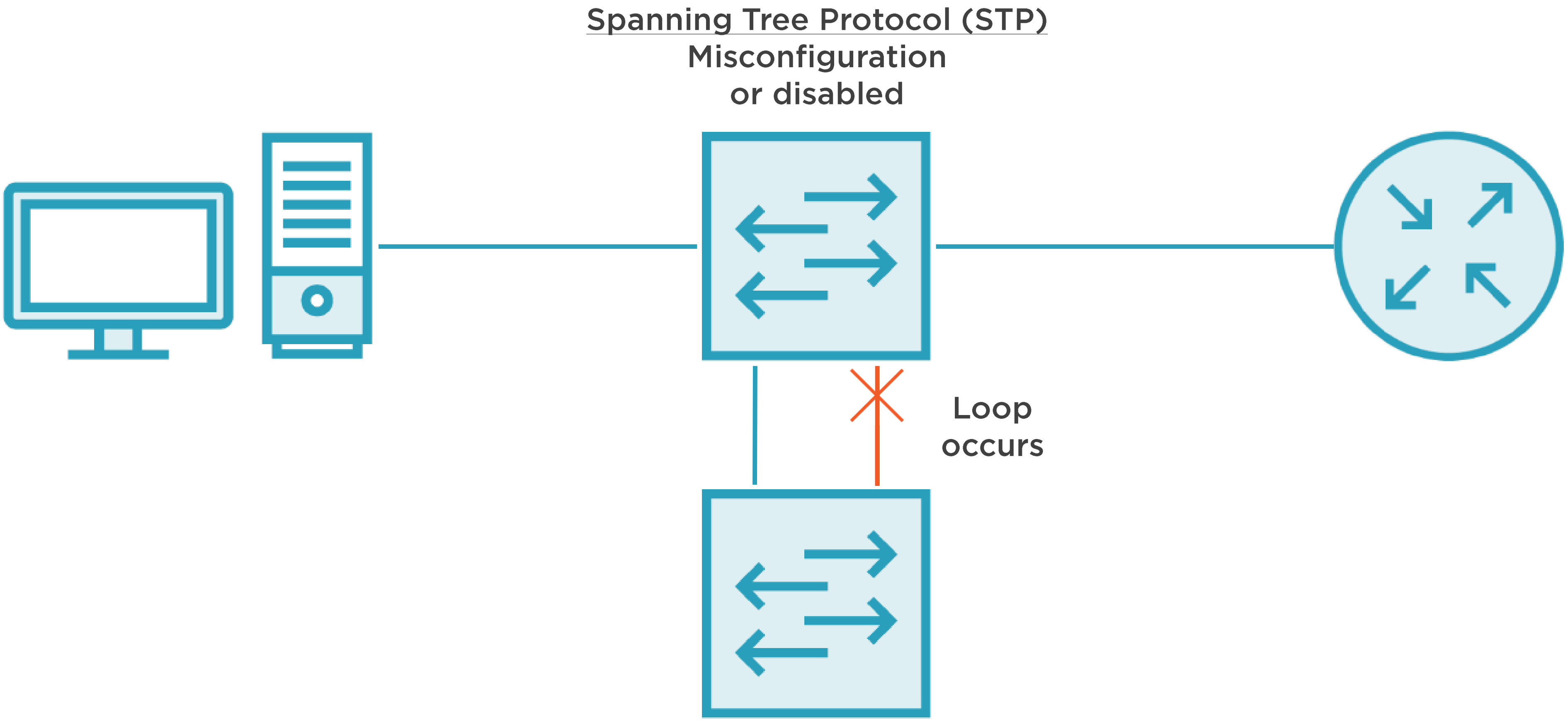
ARP Broadcast Storm – Hardware Loop

ARP Broadcast Packet

Destination ffff.ffff.ffff



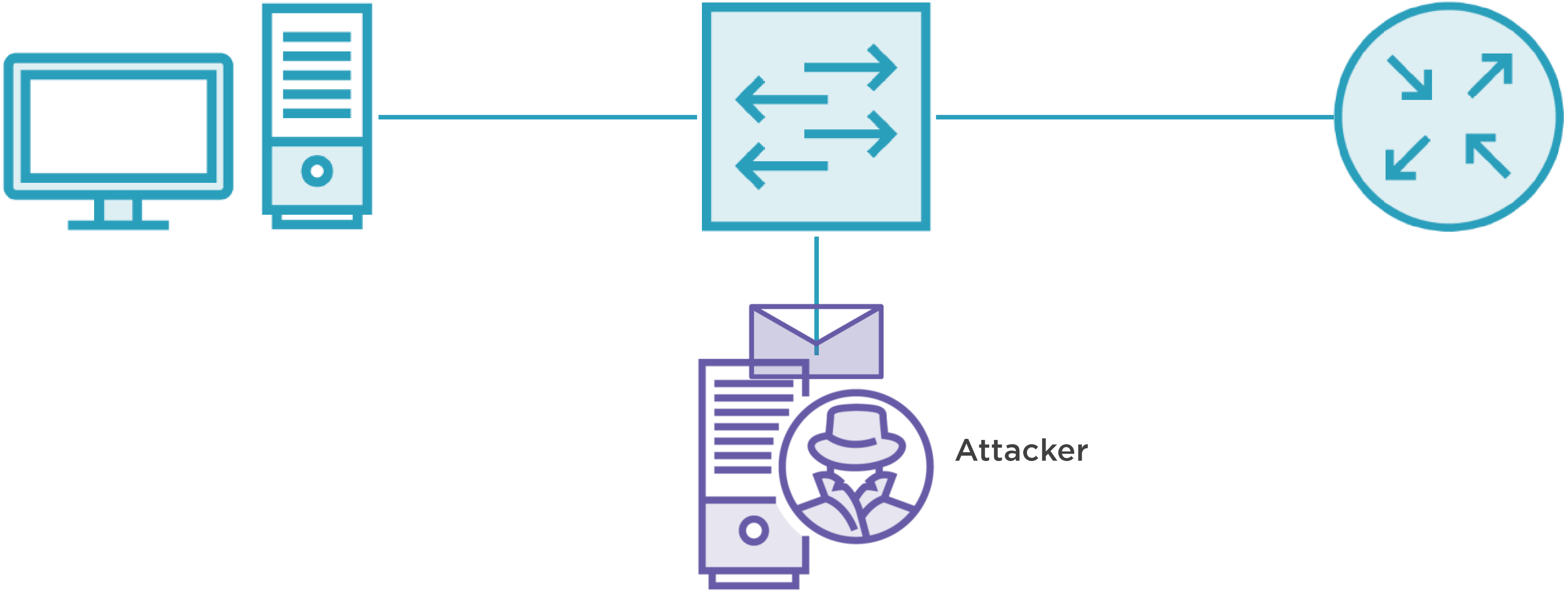
ARP Broadcast Storm – Software Loop



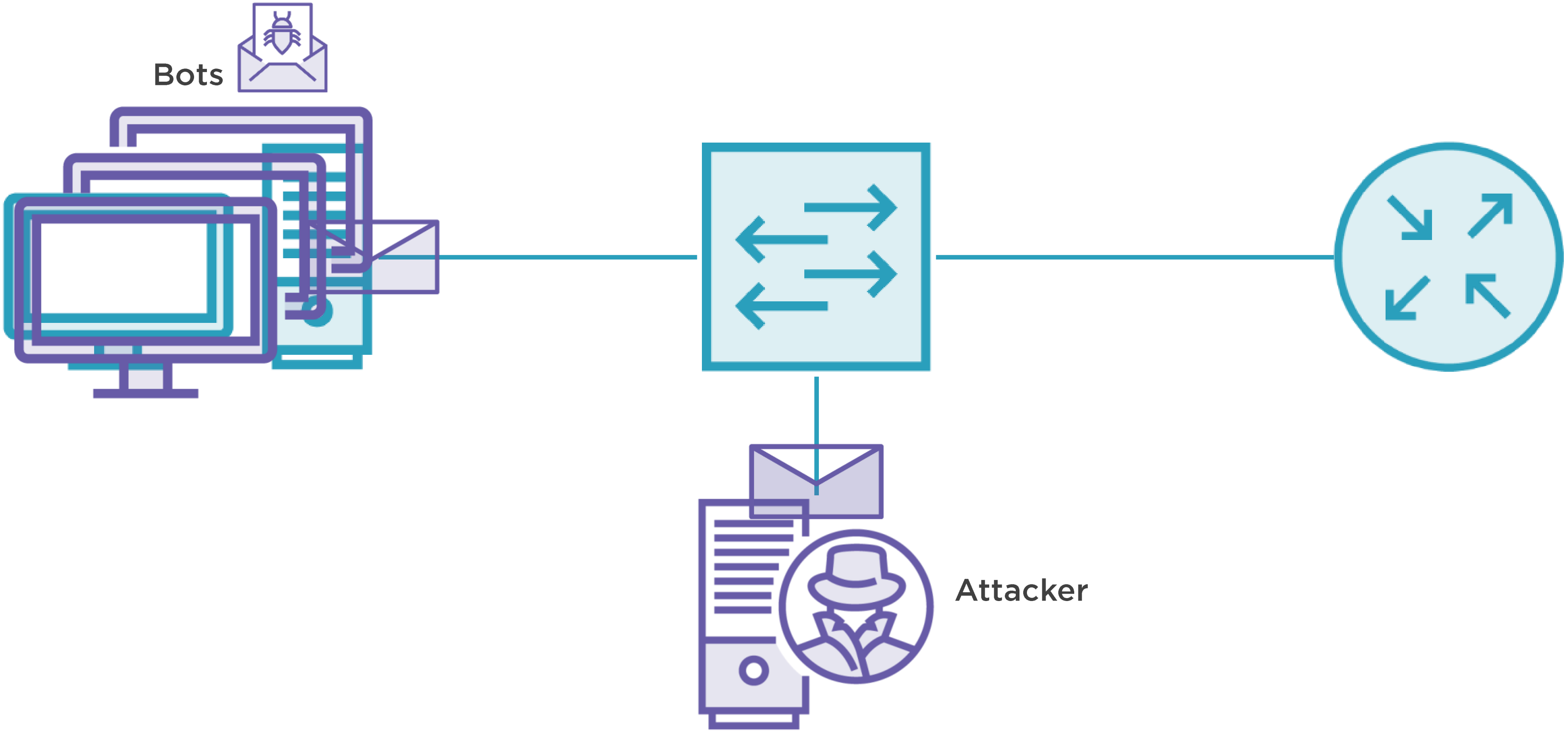
Spanning Tree Protocol (STP) Misconfiguration or disabled

Loop occurs

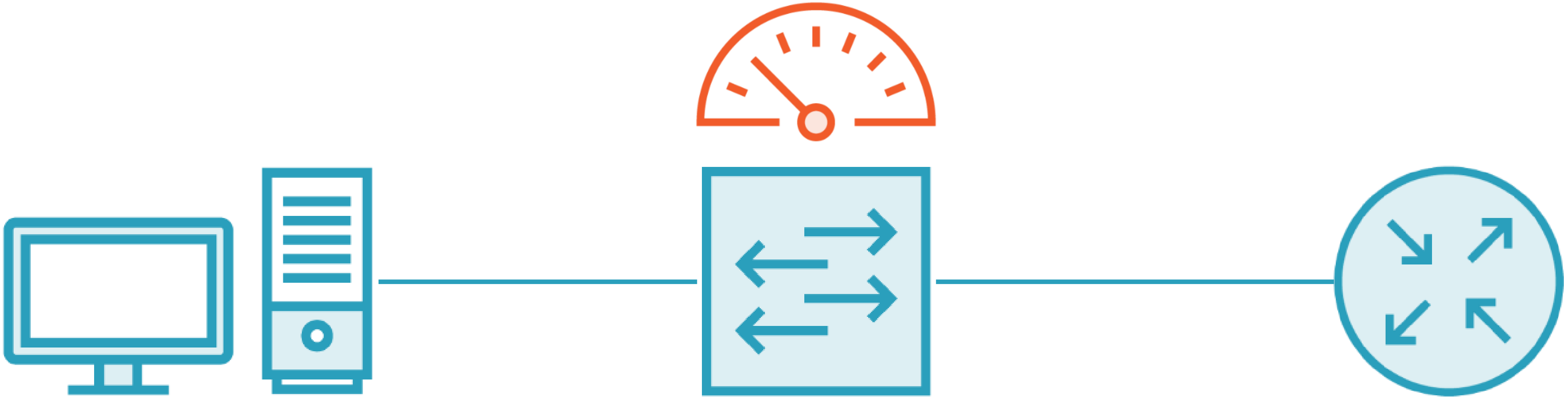
Malicious ARP Broadcast Storm DoS



Malicious ARP Broadcast Storm DDoS



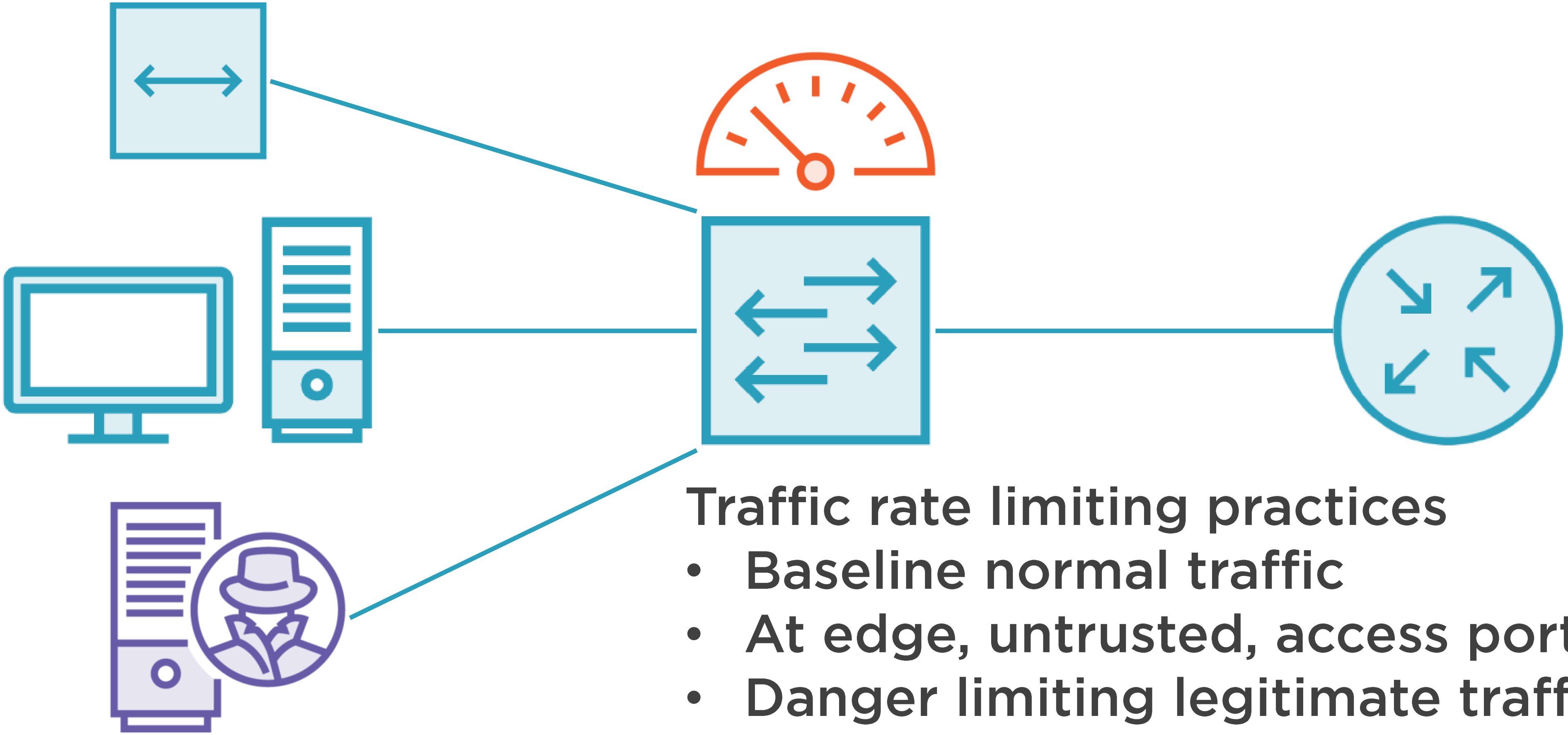
ARP Broadcast Storm Mitigation



Rate limiting traffic

- General: broadcast, multicast, unicast storm control
- Protocol specific: Address Resolution Protocol
- Rate in: packets/second, bits/second, percent of bandwidth

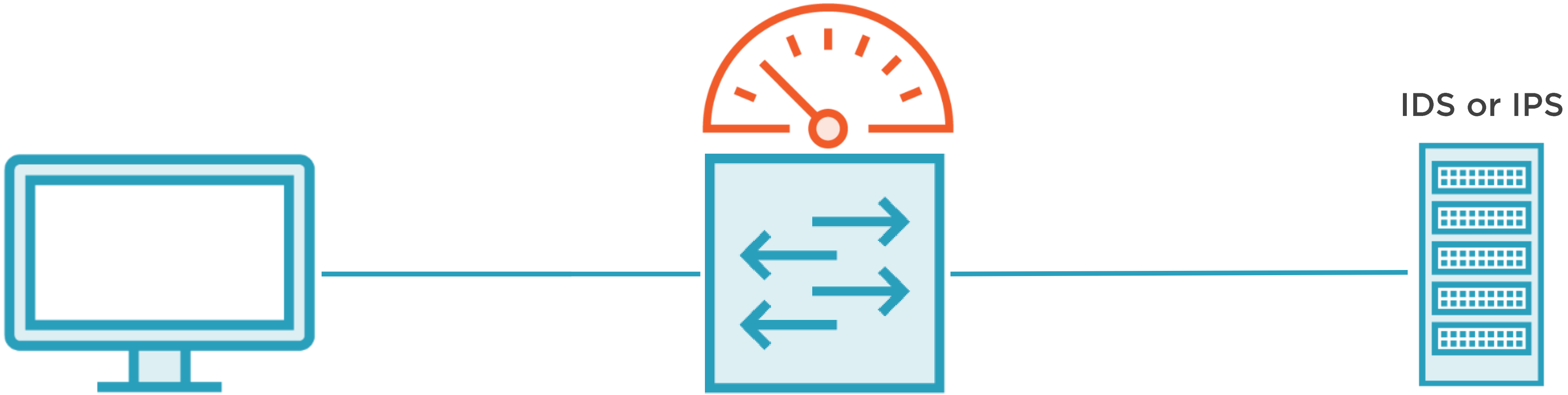
Traffic Rate Limit Best Practices



Traffic rate limiting practices

- Baseline normal traffic
- At edge, untrusted, access ports
- Danger limiting legitimate traffic
- Determine actions: disable ports, filter traffic, alarms and traps

Intrusion Detection/Prevention Systems



Intrusion Detection or Prevention Systems

- Can help baseline and prepare changes
- Can help localize the source of problems
- Can potentially react to help isolate network issues and attacks
- Useful in aggregating alarms and in later forensic analysis

Summary

ARP broadcast storms are a form of DoS

Causes include hardware, software, or malicious users

Solutions include:

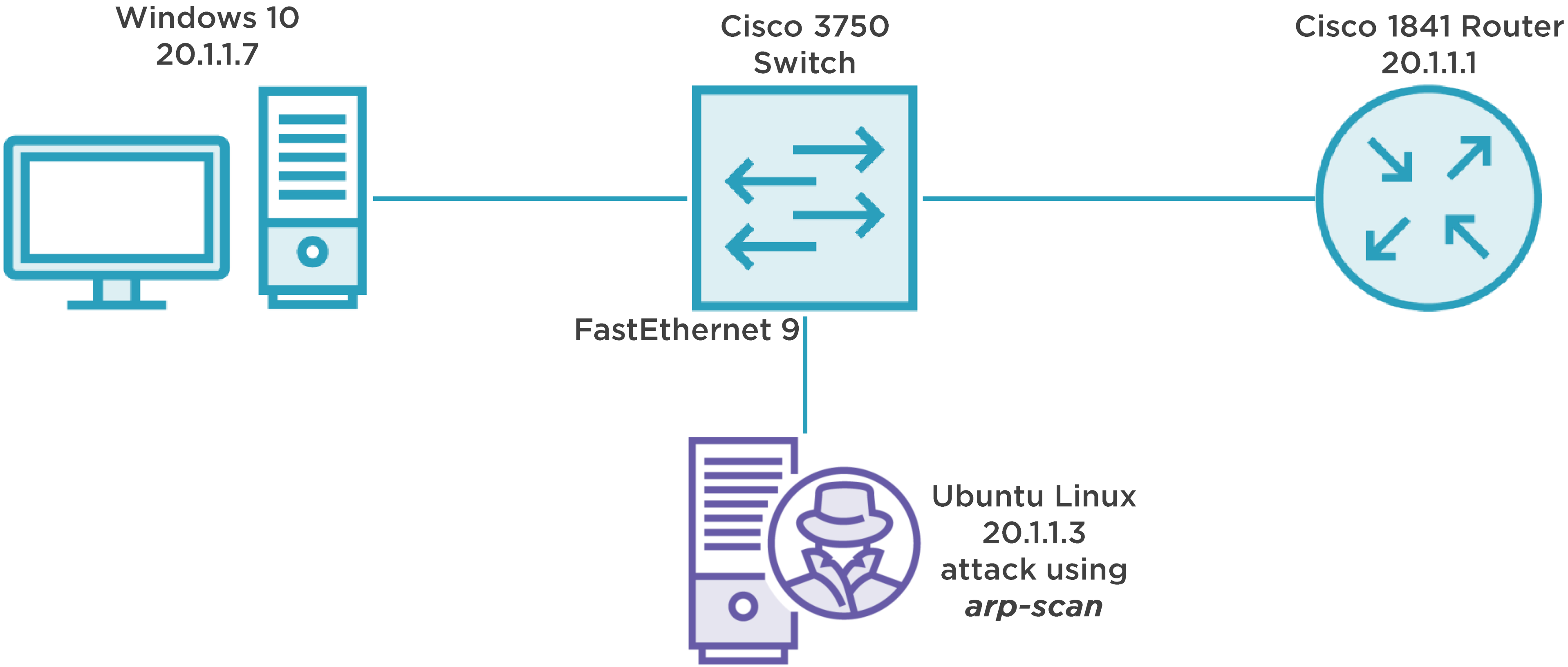
- Rate limiting broadcasts and ARPs
- Intrusion Detection/Prevention Systems
- Validating traffic, users and devices in the network

Demo

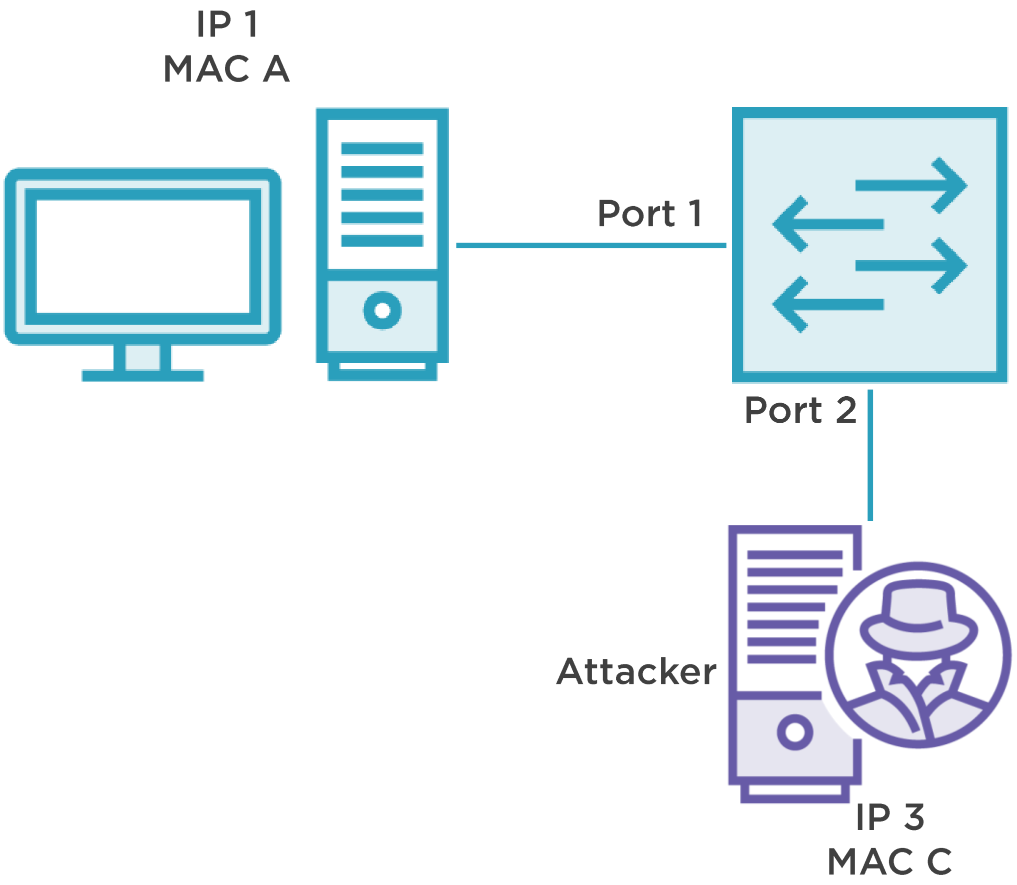
ARP Broadcast Storm Attack

Broadcast Storm Control

Malicious ARP Broadcast Storm DoS

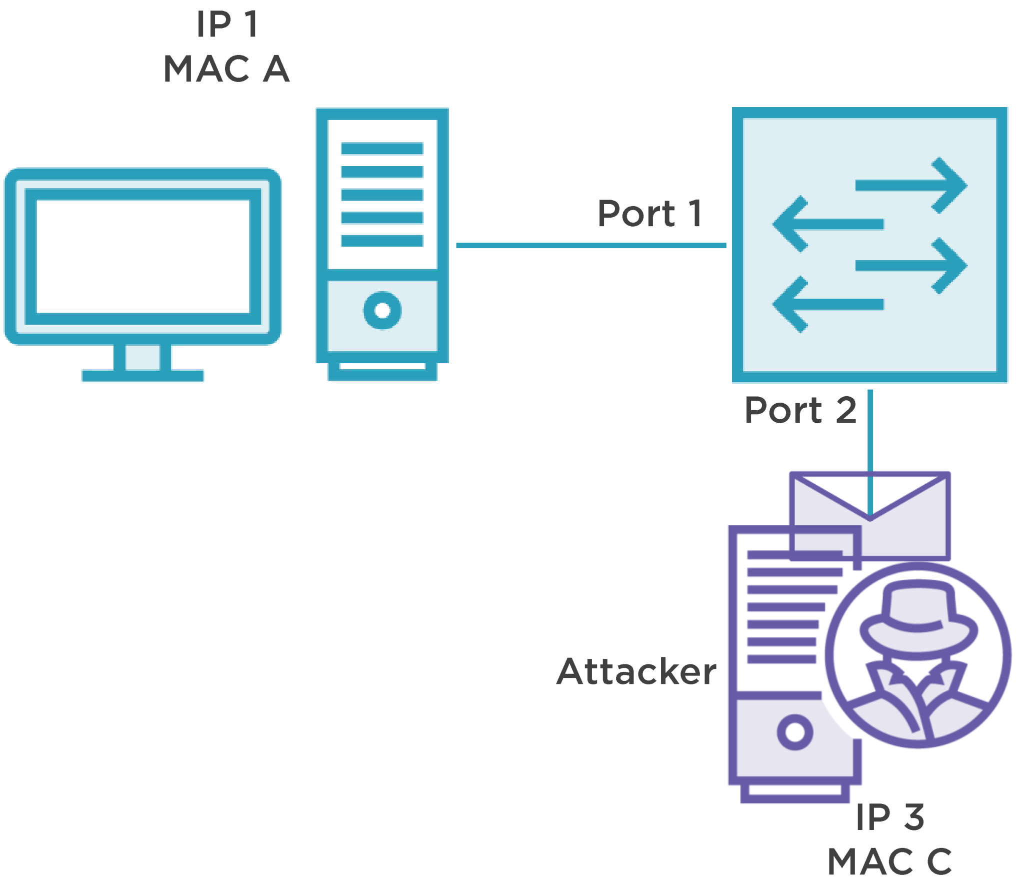


Switch MAC Address Table Learning



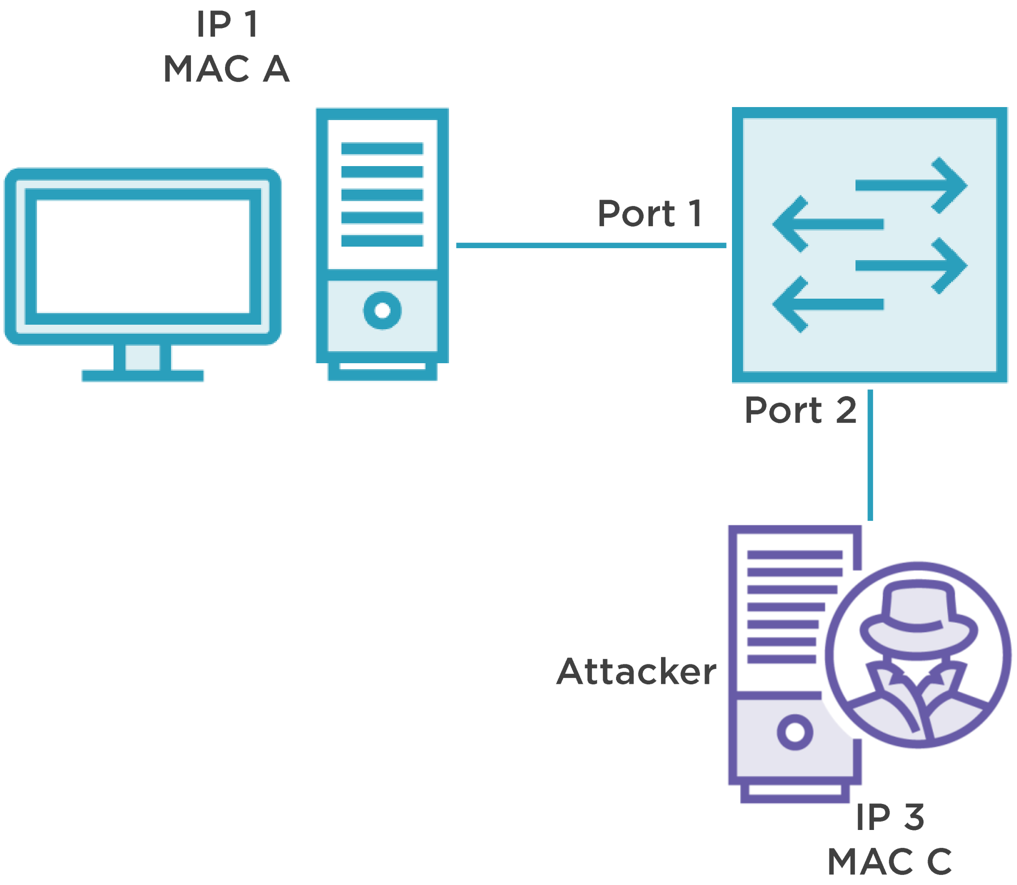
Port	MAC address(es)
1	A
2	C
3	
4…	
Count	2
Max	4196

MAC Flooding Attack



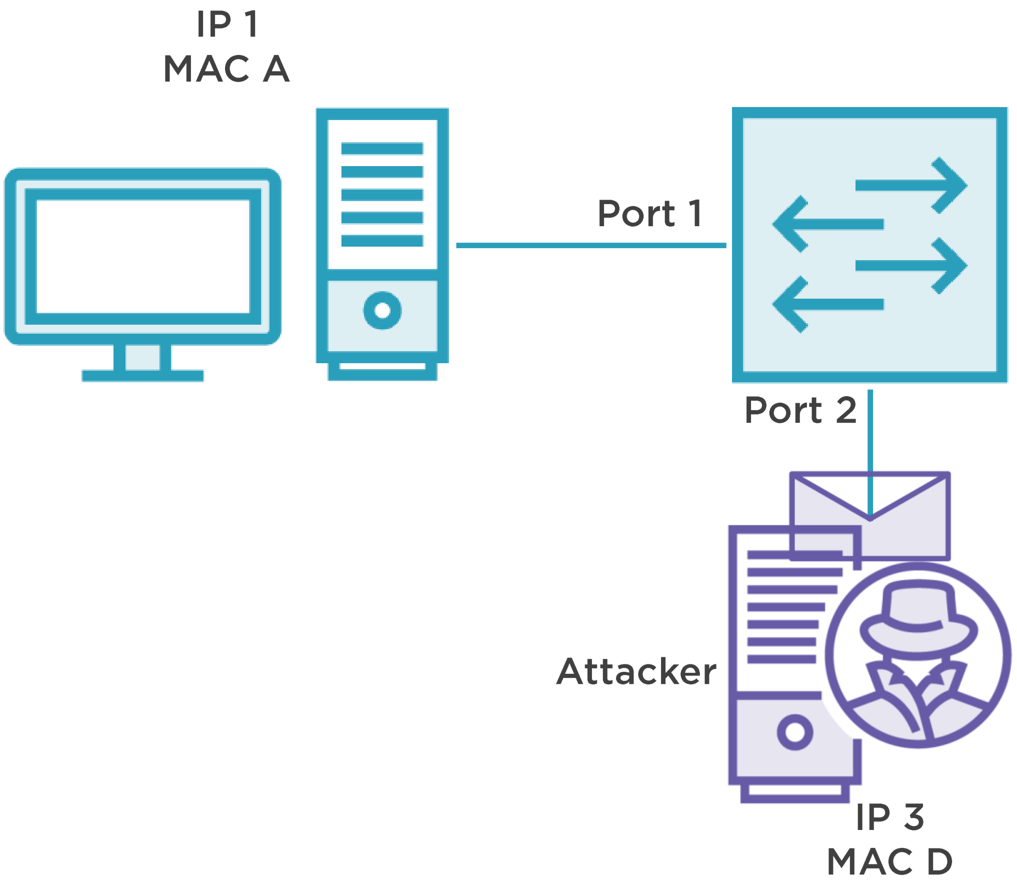
Port	MAC address(es)
1	A
2	NMKJ E B D C F G H I L O...
3	
4...	
Count	4196
Max	4196

Port Security



Port	MAC address	Port Security Enabled	Max. MACs	Action	Persistent	Violation Occurred
1	A	Y	1	Restrict	Yes	No
2	E D	Y	2	Shutdown	Yes	Yes No
3		N	-	N/A	N/A	N/A
4	-	Y	5	Shutdown	No	No
Count	1					
Max	4196					

Port Security



Port	MAC address	Port Security Enabled	Max. MACs	Action	Persistent	Violation Occurred
1	A	Y	1	Restrict	Yes	No
2	E D	Y	2	Shutdown	Yes	Yes
3		N	-	N/A	N/A	N/A
4	-	Y	5	Shutdown	No	No
Count	2					
Max	4196					

Summary

Switch MAC table flooding attacks create privacy issues as switches flood all traffic

Countermeasure is port security

- Network port-based authentication
- Validates based on MAC address
- Maximum allowed MAC addresses
- Violations block ingress traffic
- Can be circumvented through MAC Spoofing

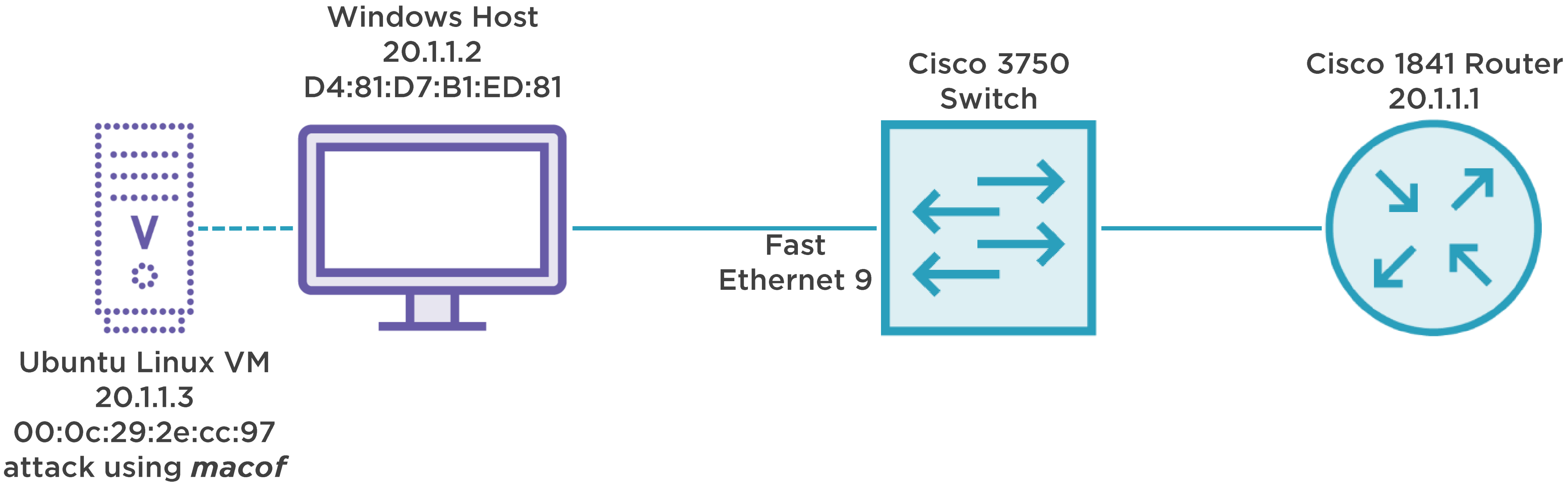
Demo

Switch MAC address table flood attack

Attack MACOF Ubuntu packet flood

Countermeasure port security switch configuration

Switch MAC Address Table Flood



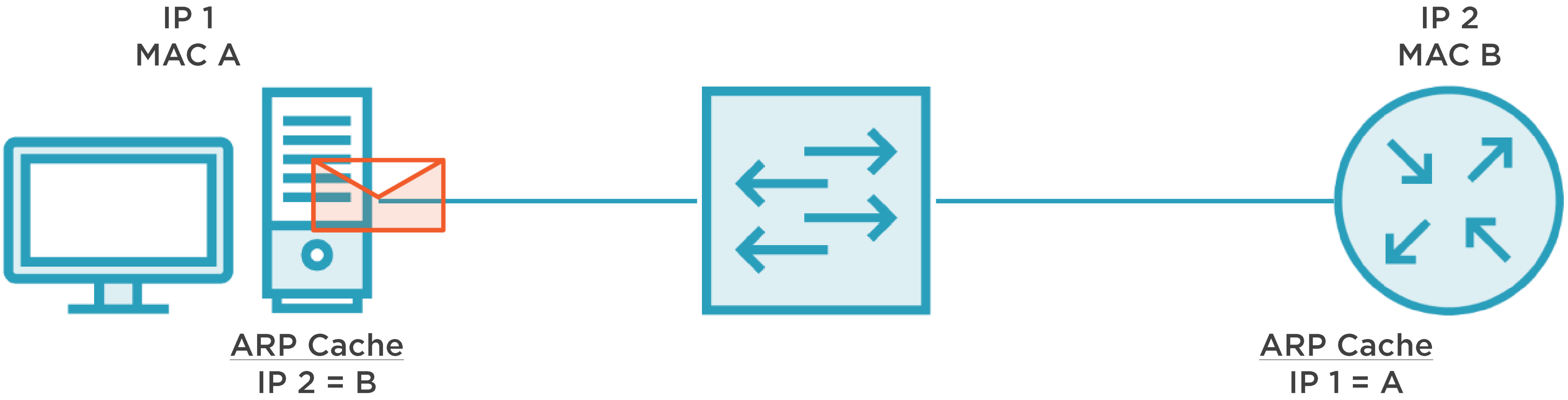
Summary

Switch MAC table flooding attacks create eavesdropping and DoS conditions

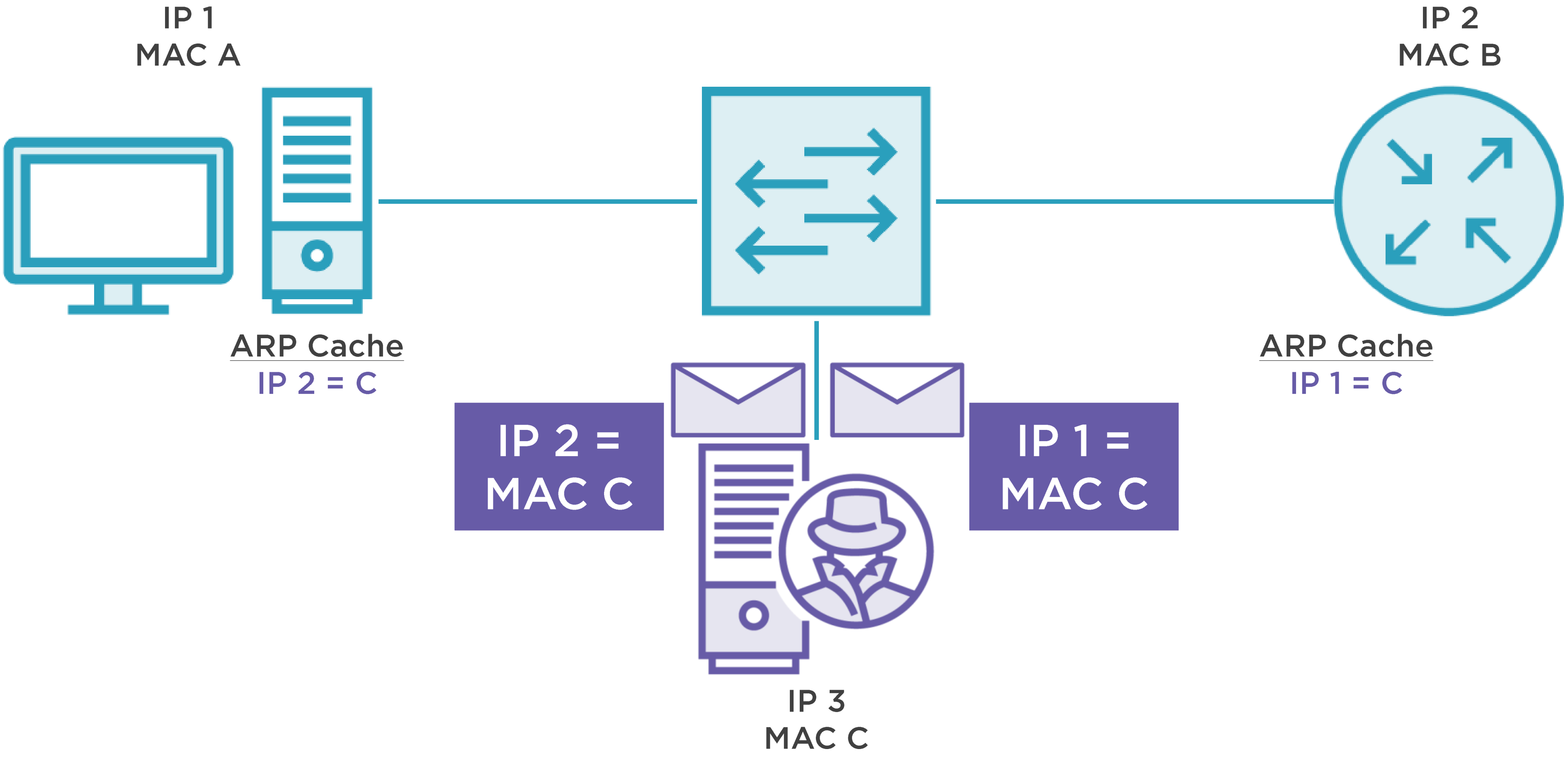
Port security can

- Authenticate devices to the network
- Validate static or dynamic MAC addresses
- Allow for a maximum number of MAC addresses
- Alert administrators to issues
- Be circumvented through MAC Spoofing

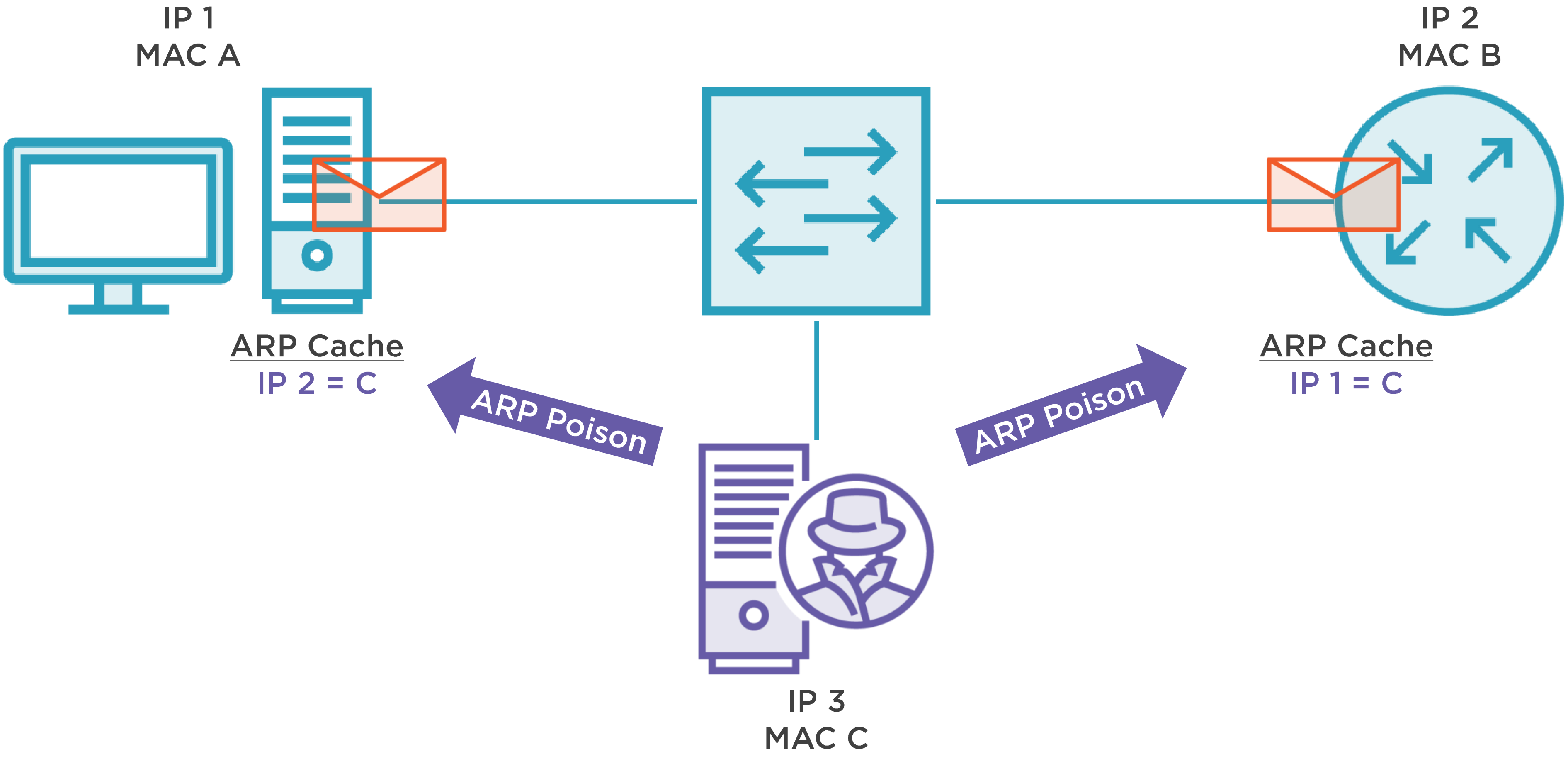
Normal Traffic



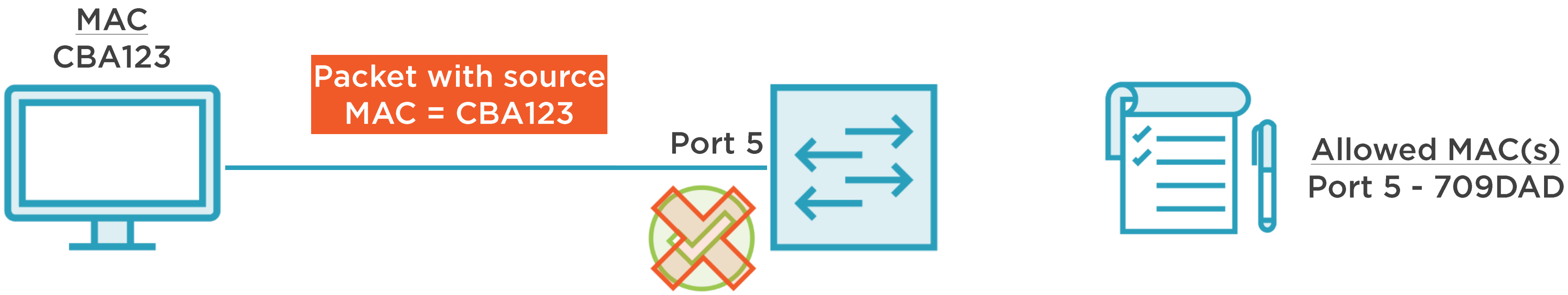
ARP Poisoning



ARP Poisoning Blackhole



Mitigating ARP Spoofing – Port Security



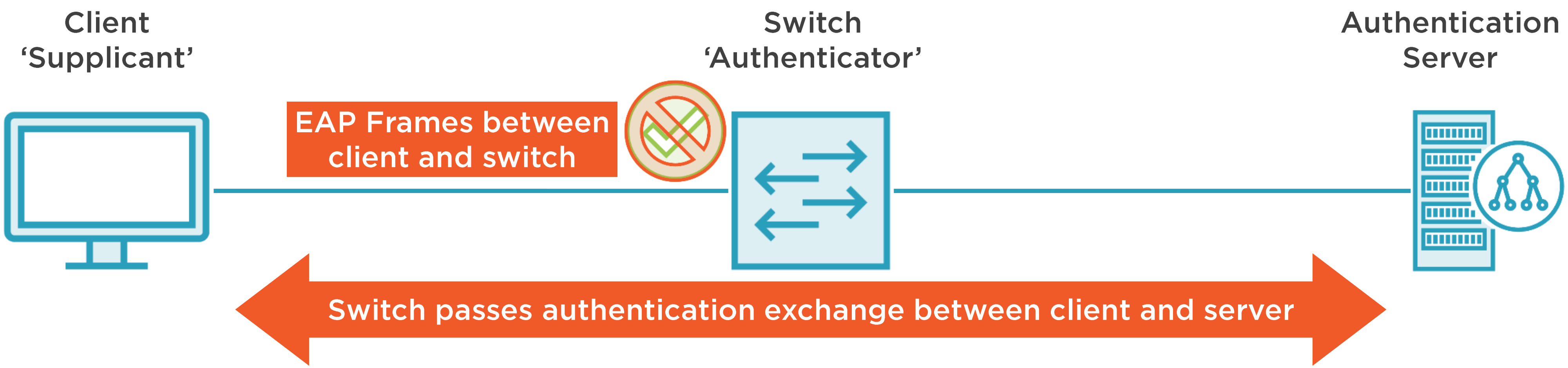
How it works

- Port-based MAC address authentication
- MAC addresses learned statically or dynamically
- Limits total MAC addresses per port
- Valid source MAC addresses can pass traffic
- Violation restricts traffic or disables port
- SNMP traps and violation counters can be logged
- Manual or auto-recovery after violation corrected

Implementation considerations

- Best for stable environments at access layer
- Plan processes for new equipment integration and equipment decomission
- Plan for port recovery process
- Challenges include:
    - Administrative overhead
    - User awareness vs. frustration
    - Spoofed MAC addresses

Mitigating ARP Spoofing – 802.1x Authentication


Client
'Supplicant'
Switch
'Authenticator'
Authentication
Server
EAP Frames between client and switch
Switch passes authentication exchange between client and server

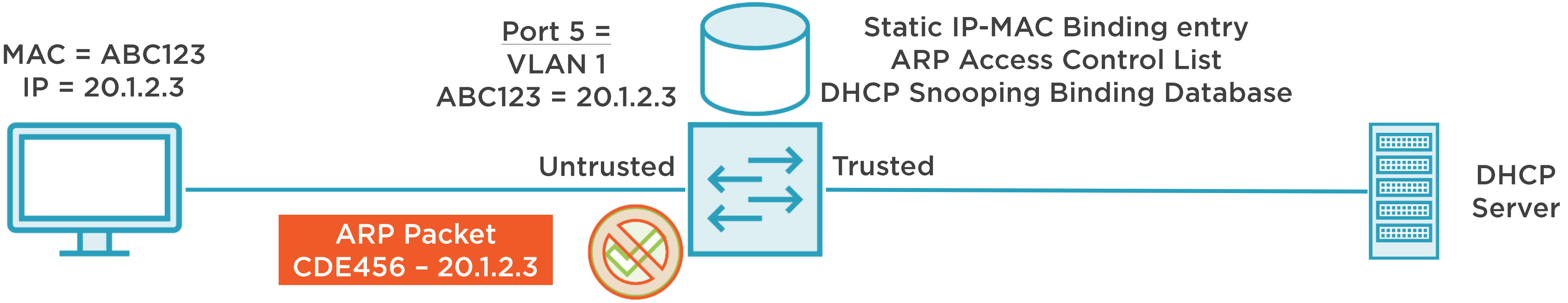
How it works

- Only EAP frames are allowed on connection
- Clients and switch exchange 802.1x EAP frames
- Switch translates authentication requests and responses between client and authentication server
- Authentication success ends with switchport authorized and traffic passes
- Switchport remains unauthorized if access is not granted by server.

Implementation considerations

- Centralizes security & removes switch from authentication
- Supports various authentication models
- Works for wired and wireless
- Can be bidirectional and combines with other security methods
- can include other features like VLAN assignment
- Some systems are not 802.1x compliant

Dynamic ARP Inspection (DAI)



MAC = ABC123
IP = 20.1.2.3

Port 5 =
VLAN 1
ABC123 = 20.1.2.3

Static IP-MAC Binding entry
ARP Access Control List
DHCP Snooping Binding Database

Untrusted

Trusted

DHCP
Server

ARP Packet
CDE456 – 20.1.2.3

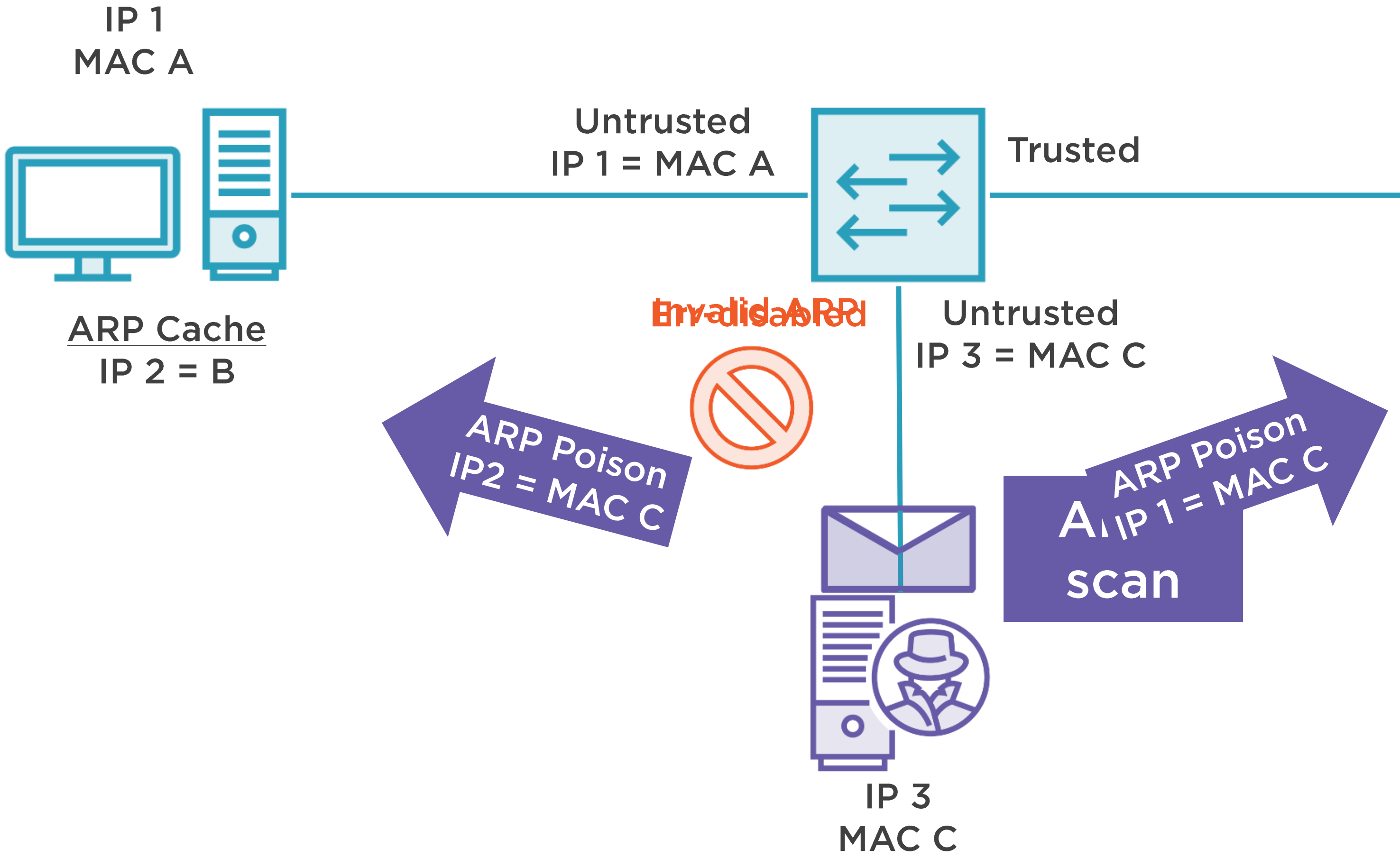
How it works

- Inspects ingress ARP requests and responses
- Intercepts only on untrusted interfaces
- Validates IP-to-MAC address bindings against
  - Static IP-to-MAC bindings
  - ARP Access Control Lists (ACLs)
  - DHCP snooping binding database
- Drops any ARP traffic with invalid bindings
- Rate limits ARP packets at each untrusted interface

Implementation considerations

- DAI drops ARP traffic without trusted source
- Trusted interfaces are not tested
- Static ARP bindings and ACLs not scalable
- DHCP snooping used for DHCP environments
- DHCP snooping and DAI configured per VLAN
- Be careful on default configurations. E.g. Rate limit violation disables port

DAI vs. ARP Scanning & Poisoning



Overview

ARP is insecure

ARP DoS, poisoning, spoofing & MITM

Mitigations include authenticating users, devices, and traffic

- Port-Security
- 802.1x Authentication
- Dynamic ARP Inspection (DAI)

Demo

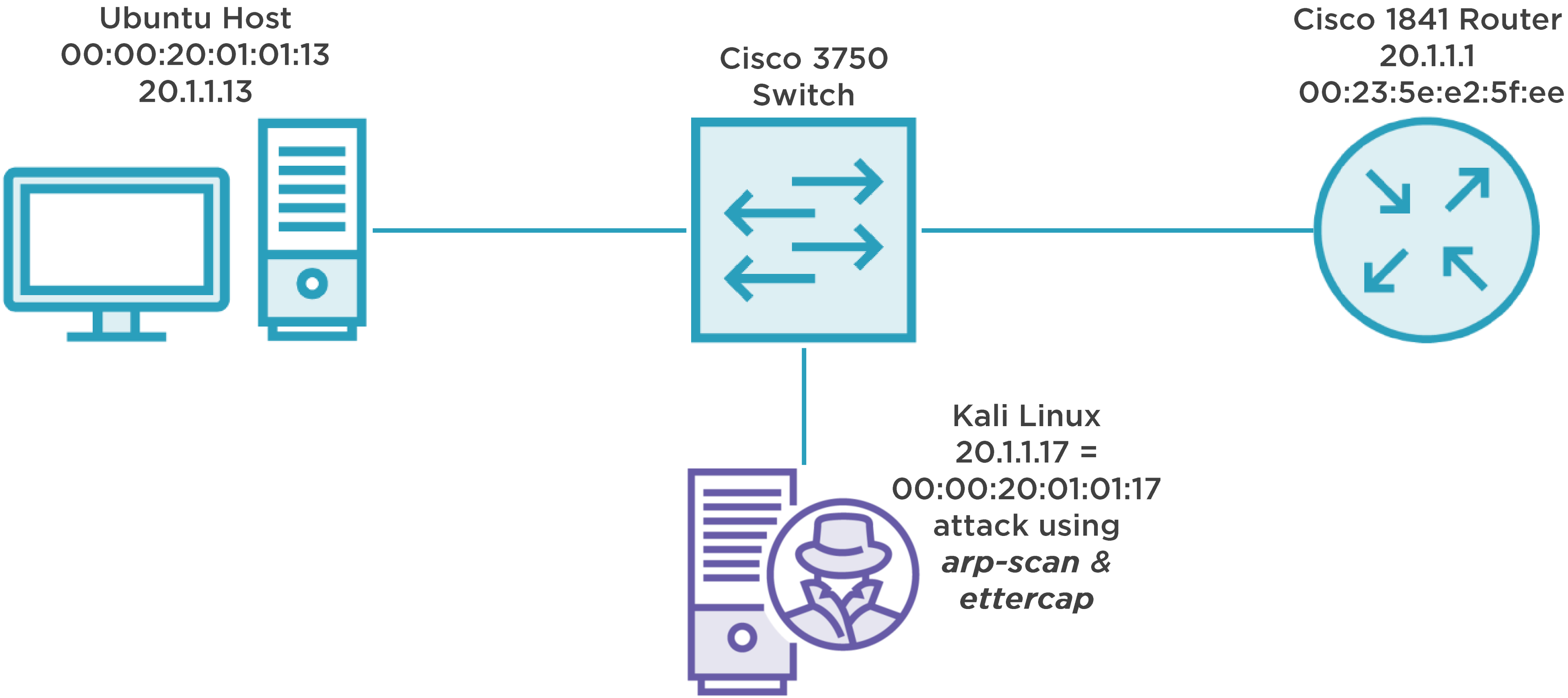
ARP poisoning/spoofing

- Man in the Middle (MITM)

Dynamic ARP inspection (DAI)

- Trusted vs. untrusted interfaces
- Static IP-to-MAC bindings
- ARP Access Control List (ACL)
- DAI static configuration
- ARP rate limiting

Prevent ARP Scanning & Spoofing with DAI



Ubuntu Host
00:00:20:01:01:13
20.1.1.13

Cisco 3750
Switch

Cisco 1841 Router
20.1.1.1
00:23:5e:e2:5f:ee

Kali Linux
20.1.1.17 =
00:00:20:01:01:17
attack using
arp-scan **&**
ettercap

Overview

ARP Scanning, poisoning & MITM

Dynamic ARP Inspection

- Requires DB source of IP-MAC bindings
- DHCP Snooping and Static bindings
- Trusted vs. untrusted interfaces
- Rate limiting on untrusted interfaces