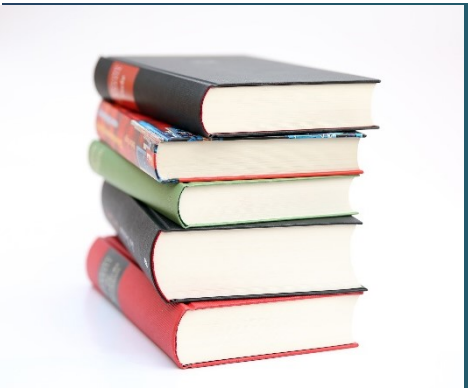
UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

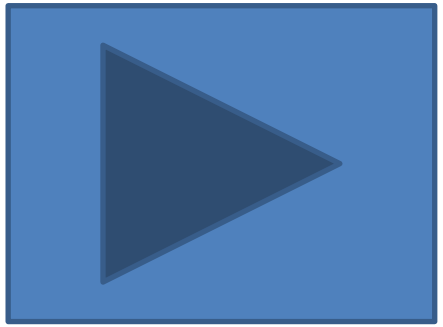
Chapter 6:
Securing the Local Area Network

CCNA Security v2.0 / Network Security
Ch.6 / Modules 13 - 14



Chapter Outline

- 6.1 Endpoint Security
  - Cisco Solutions
- 6.2 Layer 2 Security Threats
  - CCNA + CCNP SWITCH concepts



Layer 2 security

Section 6.1: Endpoint Security – Cisco view

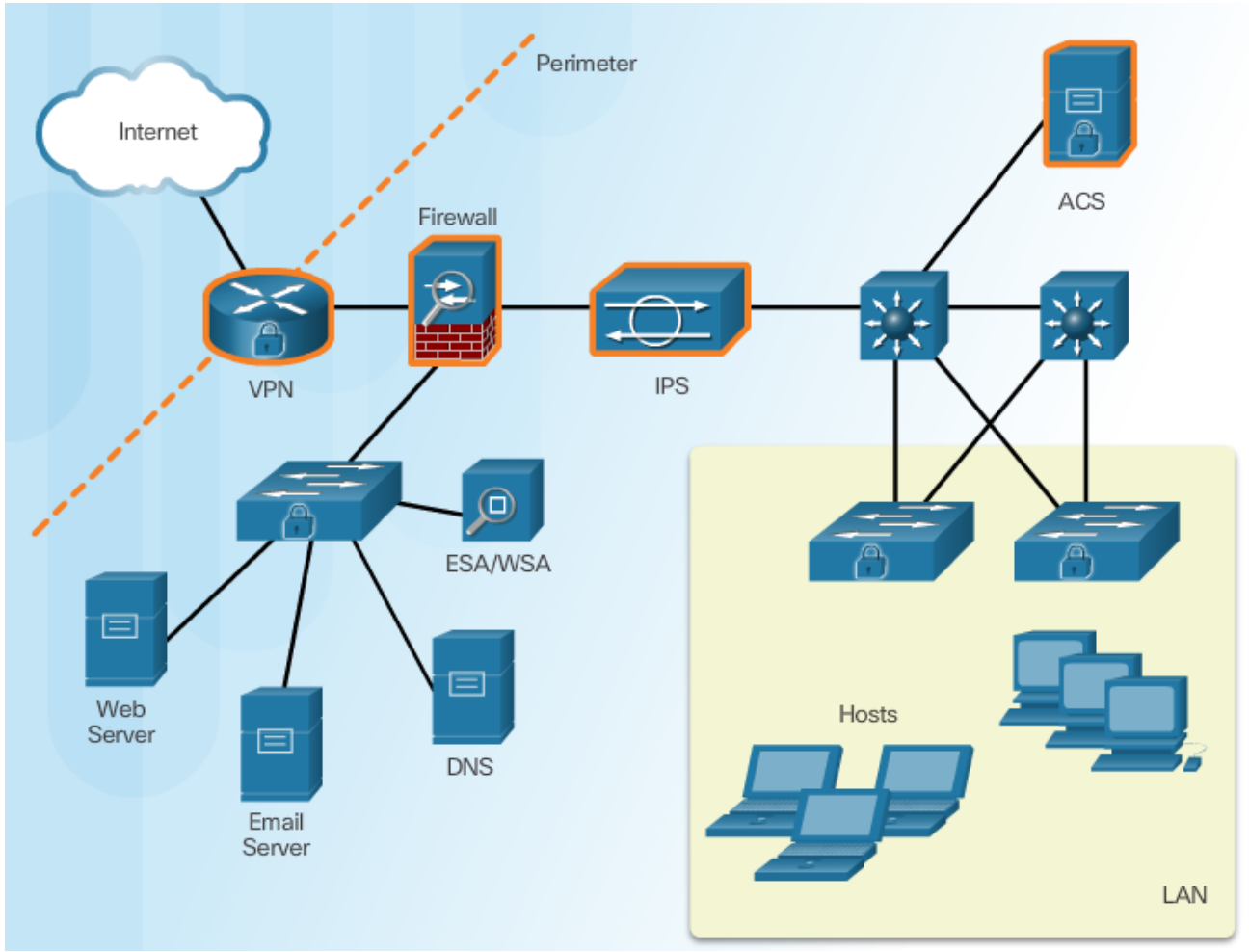
Upon completion of this section, you should be able to:

- Describe endpoint security and the enabling technologies.
- Explain how Cisco AMP is used to ensure endpoint security.
- Explain how Cisco NAC authenticates and enforces the network security policy.

Topic 6.1.1:
Introducing Endpoint Security

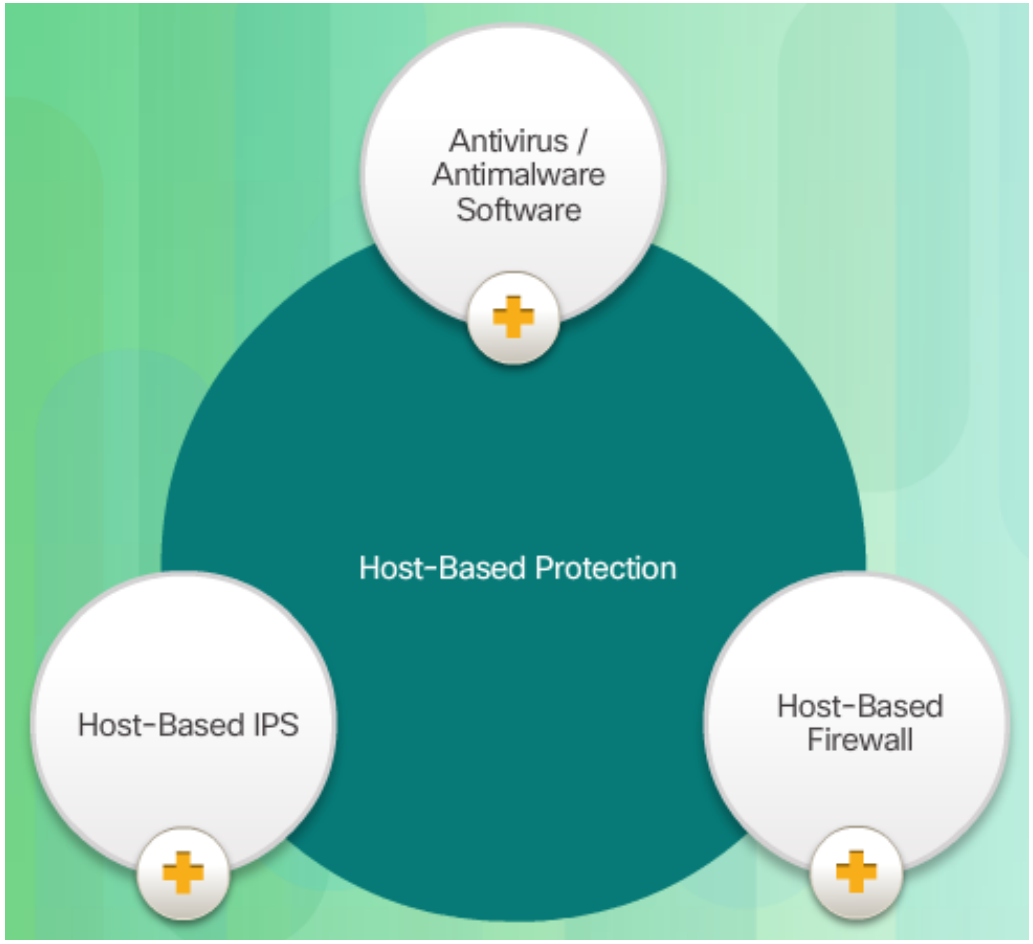
Securing LAN Elements

- People under a network attack usually imagine attacks from outside external networks
  - DoS/DDoS
  - Breach of organization's servers
    - Web, data, mail …
- Focus of perimeter security
  - Hardened ISR, ASA, IPS, AAA
- However, there is a need to protect against attacks from **the inside too**
  - Securing the LAN
- Two internal LAN elements need to be secured
  - **Endpoints**
  - **Network infrastructure**



Traditional Endpoint Security (before...)

- Endpoints
  - (Before) usually employee company-issued computers
    - With nicely defined security border – LAN access perimeter
  - (Before) protected a traditional way
    - Host based firewall
      - Software based solution
      - Restricts incoming and outgoing connections
      - ZoneAlarm, Tiny Personal Firewall, MS firewall, etc
    - Host based IPS
      - Monitor, control and report system activities; provides log analysis,
    - Antivirus / antimalware
      - MS Defender, Eset, McAffee, Norton Security …



The Borderless Network (now)

- Endpoints evolutions
  - New, lightweight, portable, consumerized endpoints appeared
    - Tablets, smartphones …
  - The network border becomes blurred
    - Access to info resources anytime, from anywhere using anything - mobility
- Traditional endpoint security methods does not work so well now
  - Network-based security devices do not share information among themselves
  - Host-based endpoint security does not perform well
    - Many different devise, OSs, performance and so on

Securing Endpoints in the Borderless Network

- Now the protection before, during, and after an attack is required
- Post malware attack questions:
  - Where did it come from?
  - What was the threat method and point of entry?
  - What systems were affected?
  - What did the threat do?
  - Can I stop the threat and root cause?
  - How do we recover from it?
  - How do we prevent it from happening again?

- Endpoint host-based protection
  - Antivirus/Antimalware
    - Protection from viruses and malware
  - SPAM Filtering
    - SPAM filtering before they reach the endpoint
  - URL Filtering
    - Filtering of websites before they reach the endpoint
  - Blacklisting
    - Block websites with bad reputation
  - Data Loss Prevention (DLP)
    - Prevents from lost or stolen of sensitive information

Modern Endpoint Security Solutions

- Protection includes more layers of scanning and sharing capabilities
- Elements included
  - Antimalware Protection (AMP)
    - Protection from viruses and malware
  - Email Security Appliance (ESA)
    - SPAM mails filtering before they reach the endpoint
  - Web Security Appliances (WSA)
    - Website filtering and blacklisting
  - Network Admission Control (NAC)
    - Perform network access decisions
    - Only authorized and compliant systems may connect

Hardware and Software Encryption of Local Data

- Securing Endpoints
  - Think on data theft if a corporate laptop is lost or stolen
    - HDD may contain sensitive information, contact information, personal information, and more
- Solution
  - Locally encrypt the disk drive with a strong encryption (AES-256)
  - Tools - Windows
    - BitLocker, TrueCrypt, Credant, VeraCrypt, and more…

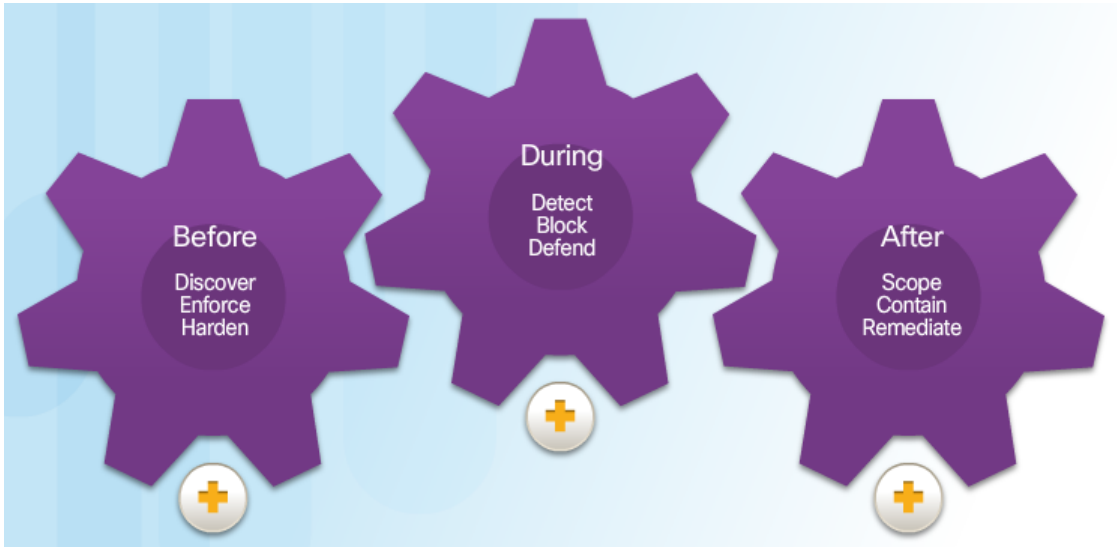
Topic 6.1.2:
Antimalware Protection

Cisco products and solutions

Layer 2 security

Advanced Malware Protection (AMP)

- Cisco AMP is based on Sourcefire (acquired in 2013)
- AMP solution includes
  - **File Reputation** – Analyze files inline and block or apply policies
  - **File Sandboxing** – Analyze unknown files to understand true file behavior
  - **File Retrospection** – Continue to analyze files for changing threat levels



AMP and Managed Threat Defense

- AMP access and uses collective security intelligence of the Cisco Talos Security Intelligence and Research Group (Talos)
- Talos
  - https://www.talosintelligence.com/
  - 600 engineers, technicians, and researchers that work around the clock, 365 days a year, in more than 40 languages
  - Detects and correlates threats in real time using the largest threat-detection network in the world.
- Talos teams gather real-time threat intelligence from a variety of sources:
  - 1.6 million deployed security devices, including firewall, IPS, web, and email appliances
  - 150 million endpoints
  - They then analyze this data:
  - 100 TB of security intelligence daily
  - 13 billion web requests per day
  - 35% of the world's enterprise email traffic

AMP for Endpoints

- **AMP protection solutions**
  - **AMP for Endpoints**
    - Runs a FireAMP agent and becomes a FireAMP connector
    - AMP for Endpoints integrates with Cisco AMP for Networks to deliver comprehensive protection across extended networks and endpoints.
  - **AMP for Networks**
    - Provides a network-based solution and is integrated into dedicated Cisco ASA Firewall and Cisco FirePOWER network security appliances.
  - **AMP for Content Security**
    - This is an integrated feature in Cisco Cloud Web Security or Cisco Web and Email Security Appliances to protect against email and web-based advanced malware attacks.

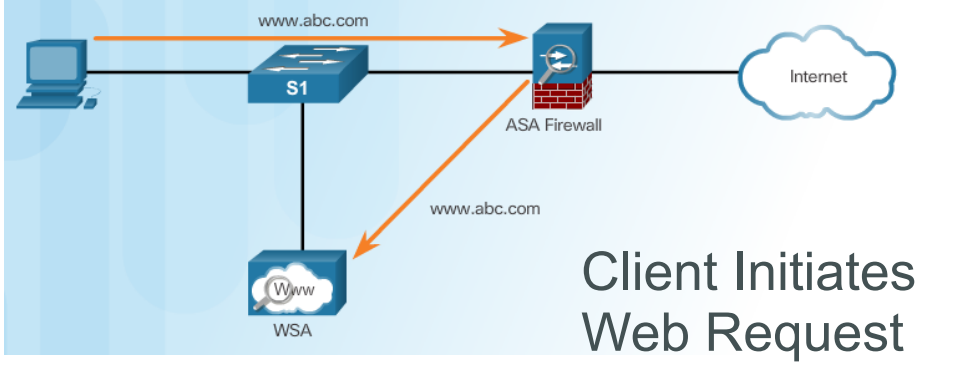
Topic 6.1.3:
Email and Web Security

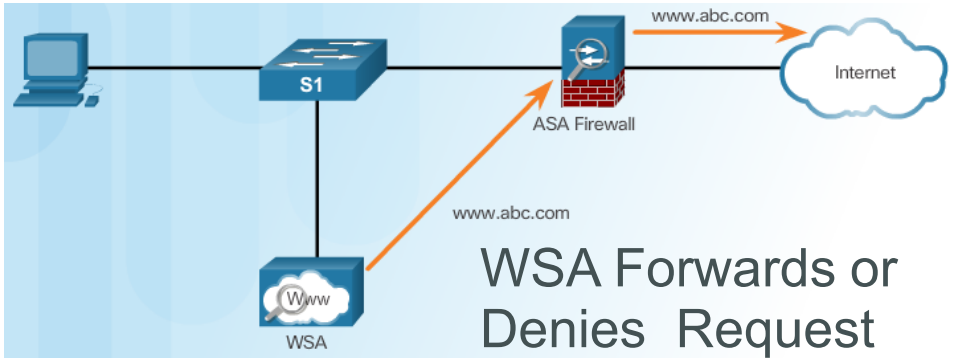
Email Security - Cisco Email Security Appliance (ESA)

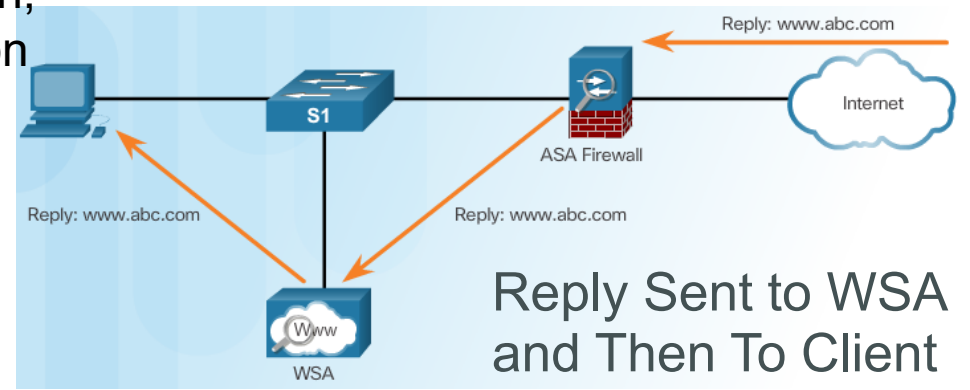
- Email has evolved to become the backbone of corporate communications
  - Recommendation: never click on attached or included files and web links (at least unknown or unusual)
- Cisco solution - Cisco Email Security Appliance (ESA)
  - Based on IronPort Systems
  - Acquired in 2007
- Features and benefits of Cisco Email Security solutions:
  - Uses global threat intelligence from Talos
  - Spam blocking
    - Multilayered defense of filtering and reputation
  - Advanced malware protection
  - Outbound message control
    - DLP control

Cisco Web Security Appliance

- De facto proxy web server
- Based on IronPort System solution
  - Complete control over how users access the Internet
- Combines
  - malware protection, application visibility and control, use policy controls, reporting, and secure mobility
- Can perform
  - blacklisting, URL-filtering, malware scanning, URL categorization, Web application filtering, and TLS/SSL encryption and decryption
- Features
  - Talos Security Intelligence
  - Cisco Web Usage Controls
  - Advanced Malware Protection (AMP), Data Loss Prevention (DLP)
- Think on opposite direction
  - Outiside to inside => Web application firewall

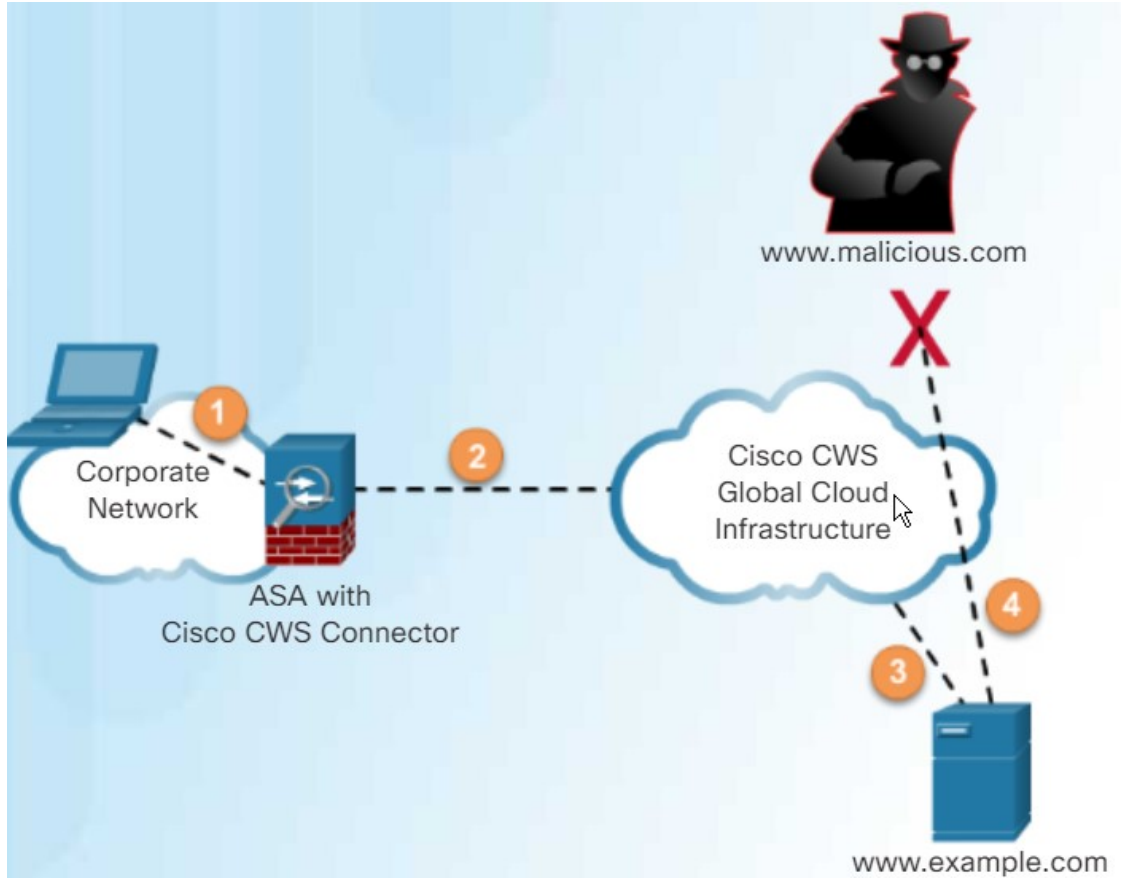






Cisco Cloud Web Security (CWS)

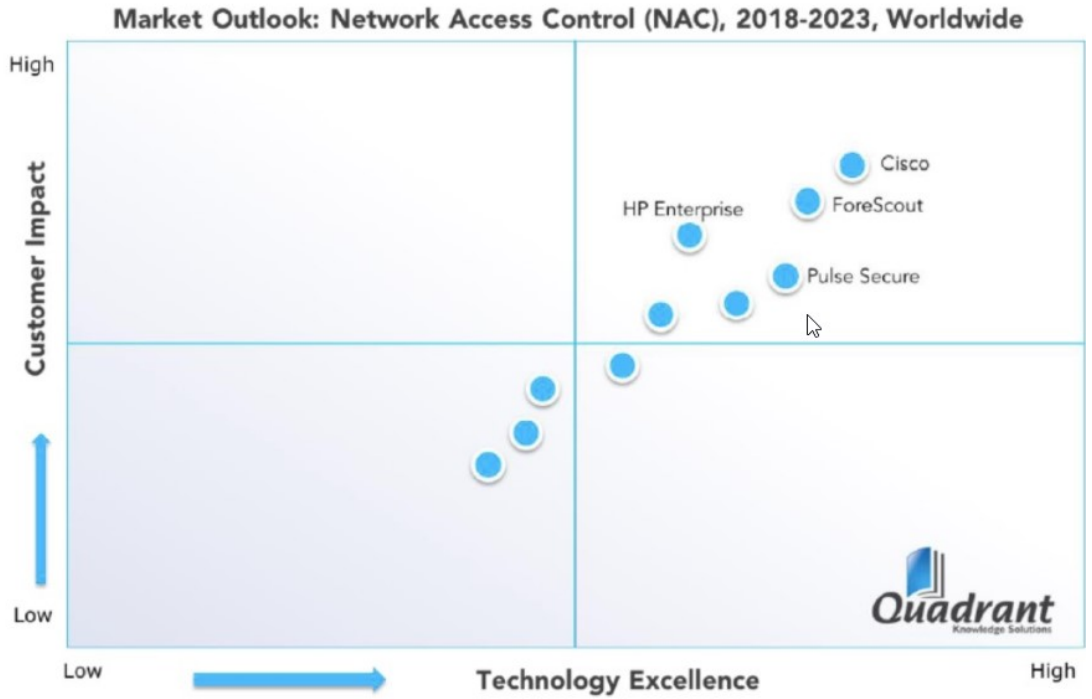
- A cloud-based security service
- Integration
  - Host:
    - proxy autoconfiguration (PAC)
  - Net: CWS connector
    - Cisco ISR G2 routers
    - Cisco ASA
    - Cisco WSA
    - Cisco AnyConnect Secure Mobility Client

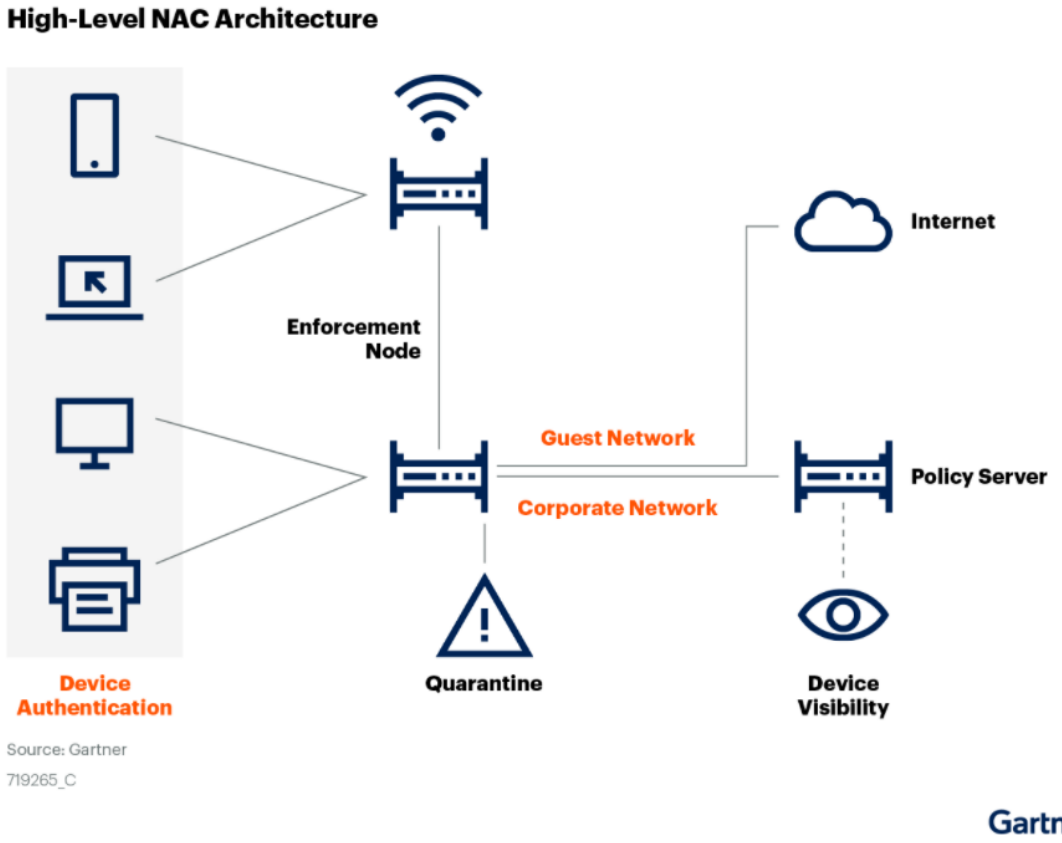


Topic 6.1.4:
Controlling Network Access

Layer 2 security

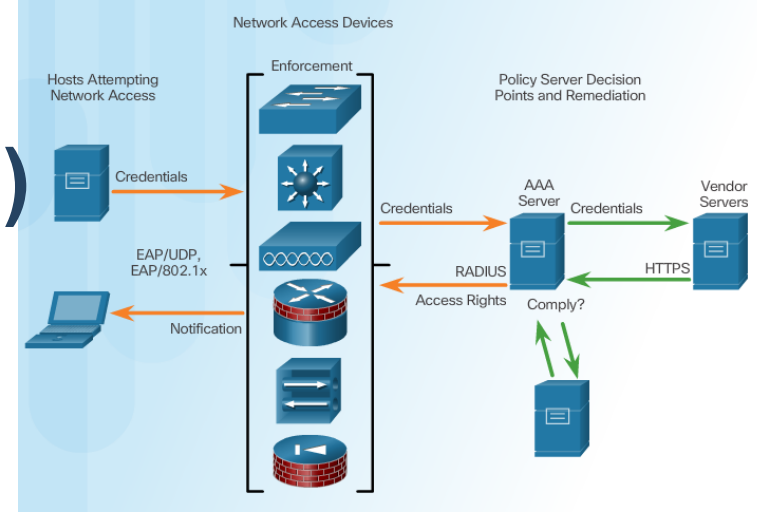
NAC Magic Quadrant





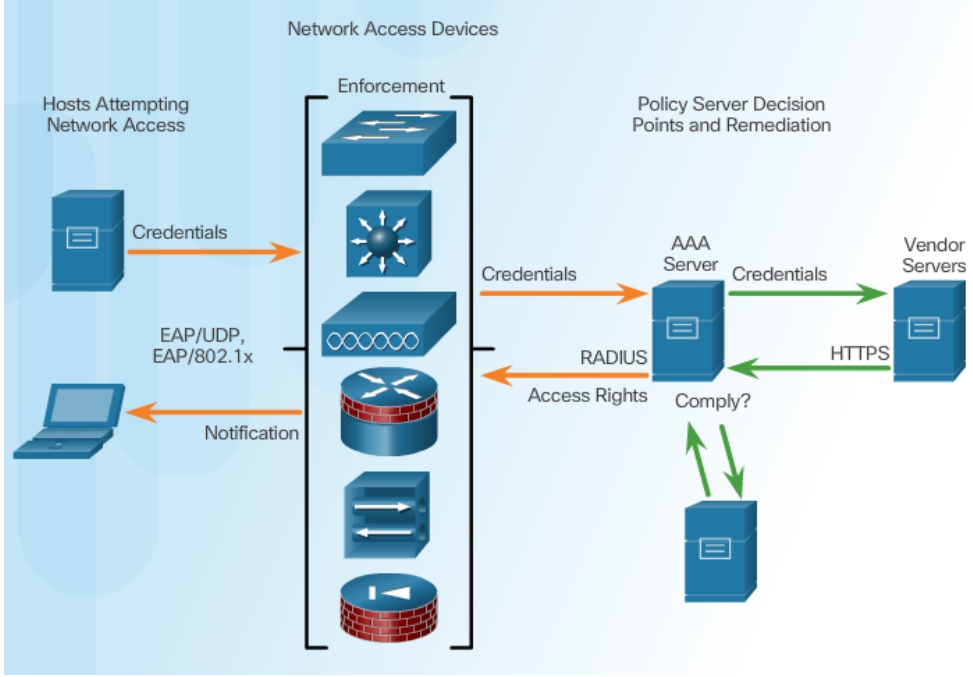
https://www.cisco.com/c/n/us/products/collateral/security/nac-appliance-clean-access/product_data_sheet0900aecd802da1b5.html

Cisco Network Admission Control (NAC)



- Policy lifecycle management:
  - Enforces policies (allow, block, isolate) for all operating scenarios without requiring separate products or additional modules.
- Profiling and visibility:
  - Recognizes and profiles users and their devices before malicious code can cause damage.
- Guest networking access:
  - Manage guests through a customizable, self-service portal that includes guest registration, guest authentication, guest sponsoring, and a guest management portal.
- Security posture check:
  - Evaluates security-policy compliance by user type, device type, and operating system.
- Incidence response:
  - Mitigates network threats by enforcing security policies that block, isolate, and repair noncompliant machines without administrator attention.
- Bidirectional integration:
  - Integrate with other security and network solutions through the open/RESTful API.

NAC Features and Benefits



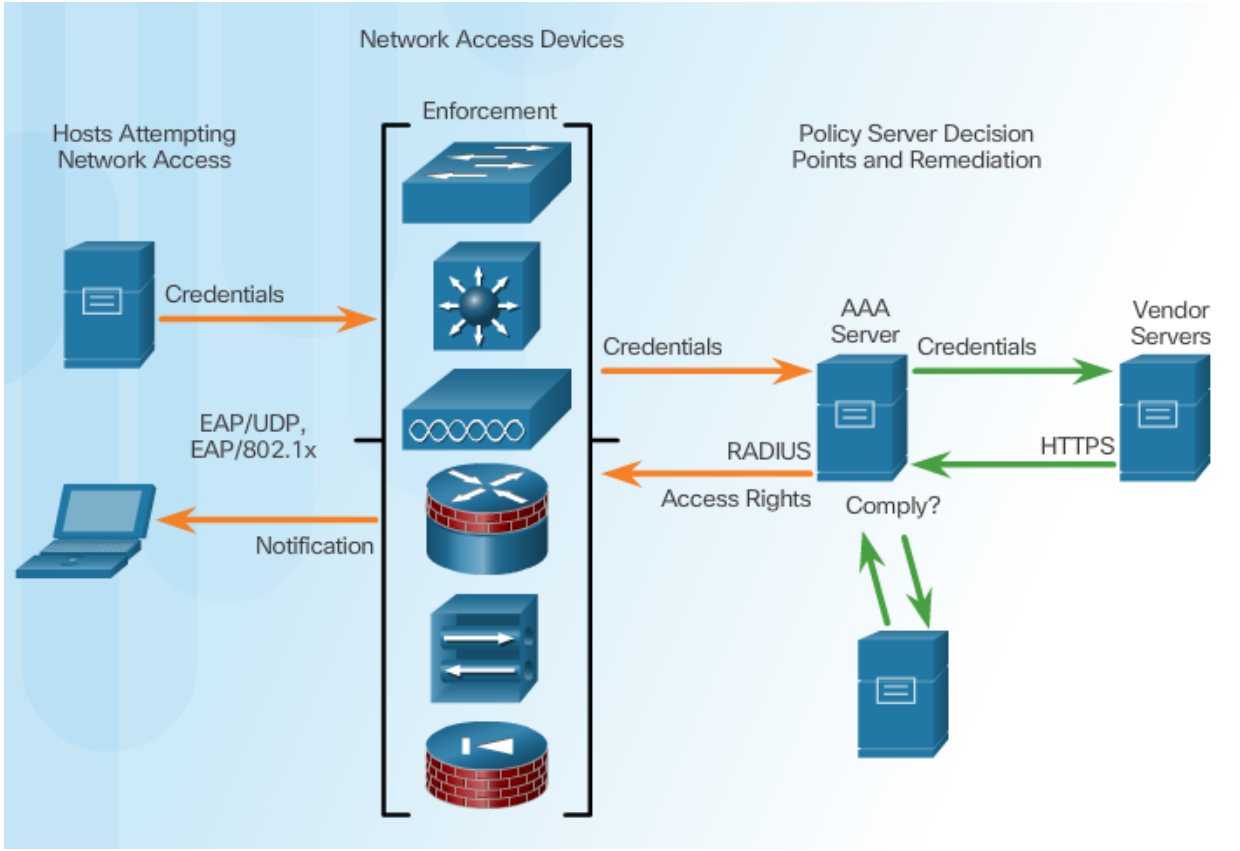
- Authentication Integration with Single Sign-On
  - natively integrating with Active Directory, Lightweight Directory Access Protocol (LDAP), RADIUS, Kerberos, S/Ident, and others.
- Device Quarantine
  - Places noncompliant machines into quarantine, preventing the spread of infection while giving the machines access to remediation resources
- Automatic Security Policy Updates
  - Updating and maintenance
  - include policies that check for critical operating system updates, virus definition updates for antivirus software, and antispyware definition updates
- Centralized Management
  - Over web-based management console
- Remediation and Repair
  - Quarantining allows remediation servers to provide operating system patches and updates, virus definition files, or endpoint security solutions to compromised or vulnerable devices.
- Flexible Deployment Modes

https://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean-access/product_data_sheet0900aecd802da1b5.html

Cisco Network Admission Control (NAC) - simply

- **NAC main function**
  - Ensure that only hosts that are authenticated and have had their security posture examined and approved are permitted onto the network
  - Controls the net access only for authorized, policy conformed and compliant systems only
    - And apply quarantine for noncompliant devices
      - For example those without sec updates
  - Control the access to the network and resources
    - based on user credentials
    - user roles in the organization
    - policy compliance of endpoint devices

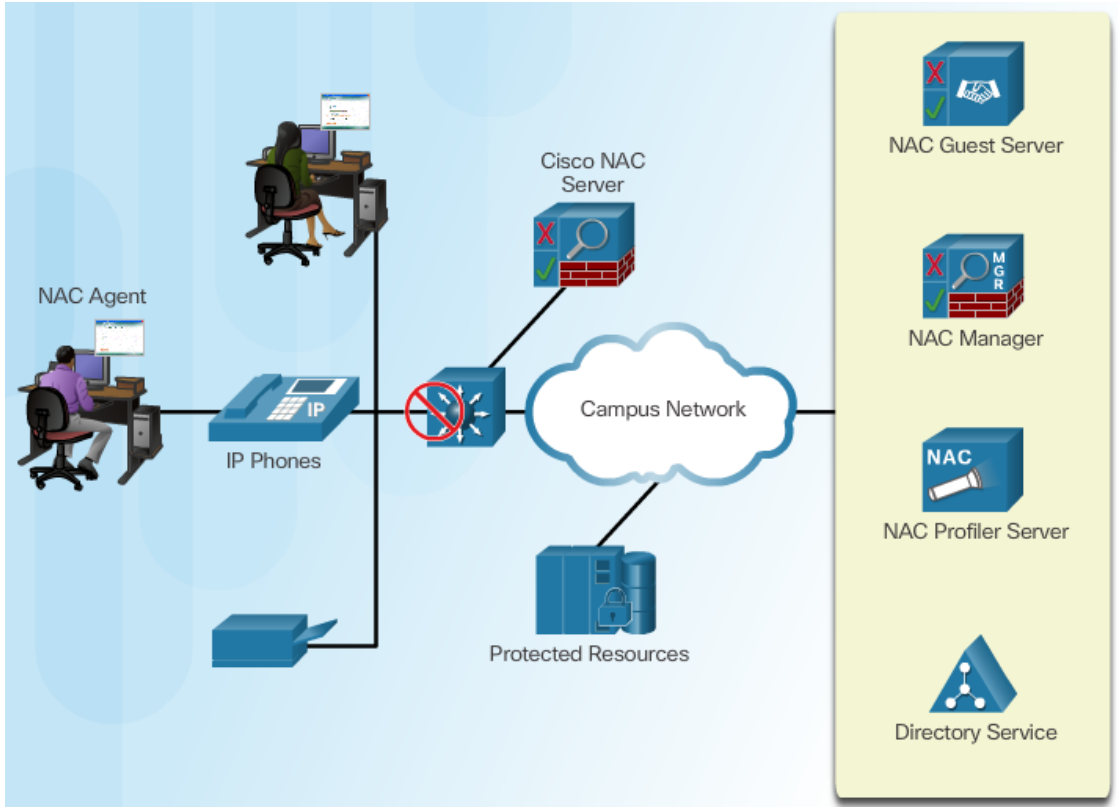
- Two solutions
  - NAC Framework
    - Integrates cisco and third party solutions
  - NAC Appliance
    - Part of Cisco TrustSec solution



NAC Framework	Cisco NAC Appliance
• Software module embedded within NAC-enabled products.	• Can be used with any Cisco or non-Cisco switch or router platforms.
• Integrated framework leveraging multiple Cisco and NAC-aware vendor products.	• Natural fit for medium-sized networks requiring a self-contained, turnkey solution.
• Best suited for high-performance network environments with diverse endpoints requiring a consistent LAN, WAN, wireless, extranet, and remote access solution that integrates into the existing security and patch software, tools, and processes.	• Ideal for organizations that need simplified and integrated tracking of operating system and antivirus patches and vulnerability updates.

Cisco NAC Components (Part of Cisco TrustSec solution)

- **Components**
  - **Cisco NAC Server (NAS)**
    - **A**ssesses and enforces security policy compliance and user authentication
    - A user cannot gain access to the network until they authenticate and the device meets defined posture requirements
  - **Cisco NAC Manager (NAM)**
    - The policy and management center (server) – web based
    - Defines role-based user access, endpoint security policies, checks. rules
  - **Cisco NAC Agent (NAA)**
    - An optional entity
    - Lightweight agent running on an endpoint device
    - Performs deep inspection of the device's security profile by analyzing registry settings, services, and files.



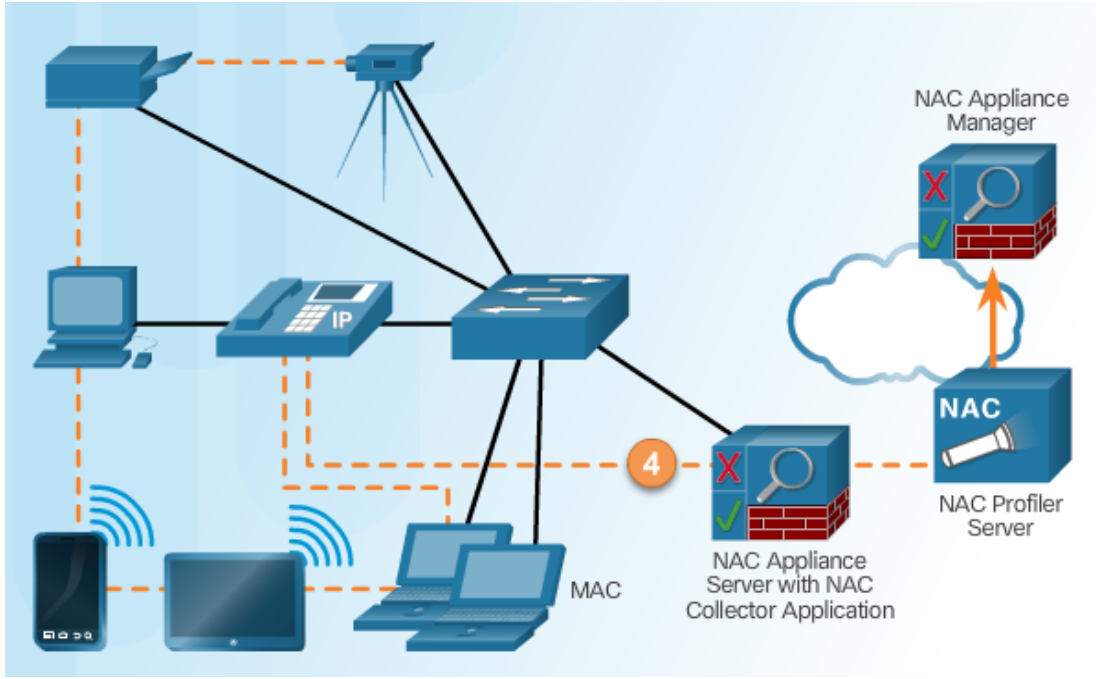
- Two additional TrustSec Policy enforcement tools:
  - **Cisco NAC guest server**
    - Manages guest network access
    - Including provisioning, notification, management, and reporting of all guest user accounts and network activities.
  - **Cisco NAC profiler => Cisco Identity Services Engine (ISE)**
    - Helps to deploy policy-based access control by providing discovery, profiling, policy-based placement, and post-connection monitoring of all endpoint devices.

Network Access for Guests

- Applied by Cisco NAC Guest Server
  - Cooperate with the Cisco NAC Appliance or the Cisco Wireless LAN Controller
  - Solution that allows guests (Visitors) to access network
    - Wifi/wired
  - Sponsors (dedicated employees of the company) are allowed to manage guest accounts
    - Create, edit, delete, suspend
- Three ways to grant sponsor permissions:
  - to only those accounts created by the sponsor
  - to all accounts
  - to no accounts (i.e., they cannot change any permissions)

Cisco NAC Profiler

- NAC Profiler, using user-defined security policies, allows:
  - dynamic discovery
  - identification,
  - inventory
  - monitoring and management of device behavior of all network-attached endpoints
    - Port swapping, profile changes, address spoofing
  - deploy NAC with 802.1X support
  - secure all endpoints



- Has two components:
  - NAC Profiler Collector
    - Continuously collects, aggregates, filters, and updates device data
    - Sends it to profiler server
  - NAC Profiler Server application
    - Aggregates info from collectors
    - Maintains DB of all net-attached endpoints
      - Phones, printers, badge readers, …

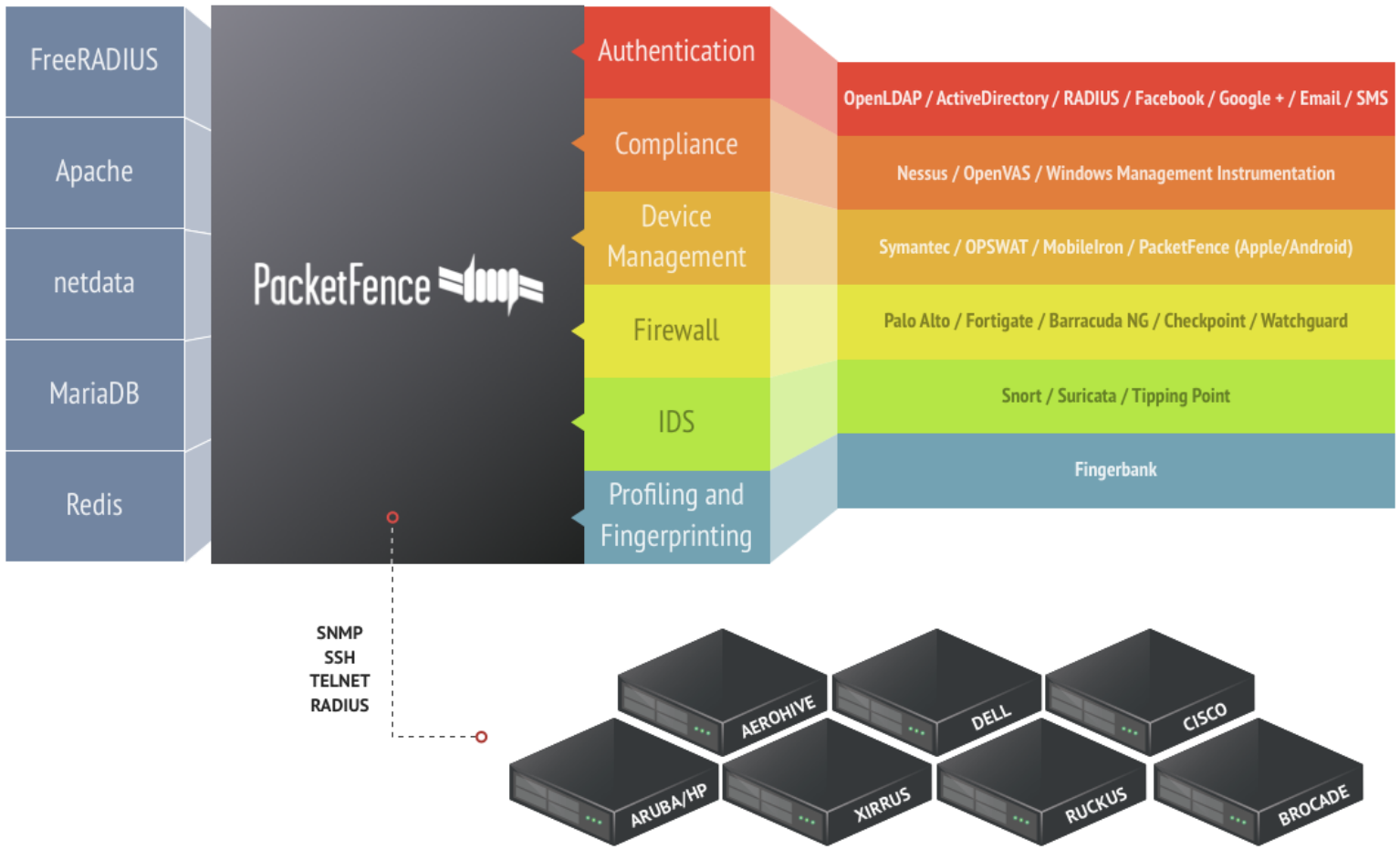
2021 state (note)

- ISE – Actual NAC solution
- Cisco Identity Services Engine (ISE)
  - Identity-based access and control policy platforms allow IT admins to take control of who can access their network by relating identities to access switches, WLCs, VPN gateways, and data center switches.
  - ISE is Cisco's latest access control technology and focus for innovation
  - NAC replacement
- ISE consolidates hardware in most cases.
  - The average NAC deployment uses a CAM, CAS, Profiler and Guest server plus double everything for high availability.
- ISE can be virtualized while NAC is appliance only.
- ISE can scale better than NAC.
- ISE has better reporting and troubleshooting capabilities than NAC

Open Source alternative

PacketFence

- … is a fully supported, trusted, Free and Open Source network access control (NAC) solution. Boasting an impressive feature set including a captive-portal for registration and remediation, centralized wired, wireless and VPN management, industry-leading BYOD capabilities, 802.1X and RBAC support, integrated network anomaly detection with layer-2 isolation of problematic devices; PacketFence can be used to effectively secure small to very large heterogeneous networks.



Section 6.2: Layer 2 Security Considerations

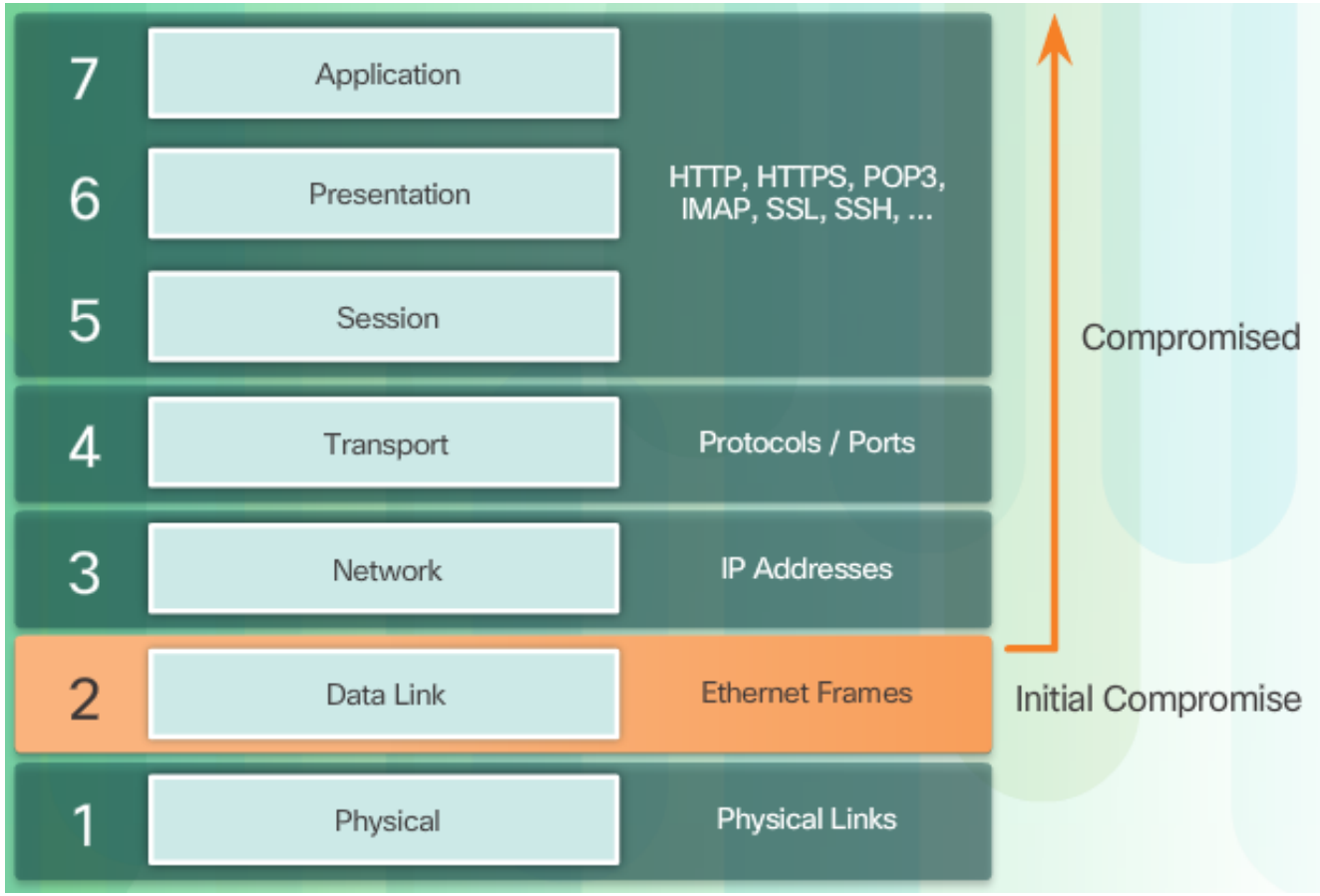
Upon completion of the section, you should be able to:

- Describe Layer 2 vulnerabilities.
- Describe CAM table overflow attacks.
- Configure port security to mitigate CAM table overflow attacks.
- Configure VLAN Truck security to mitigate VLAN hopping attacks.
- Implement DHCP Snooping to mitigate DHCP attacks.
- Implement Dynamic Arp Inspection to mitigate ARP attacks.
- Implement IP Source Guard to mitigate address spoofing attacks.

Topic 6.2.1:
Layer 2 Security Threats

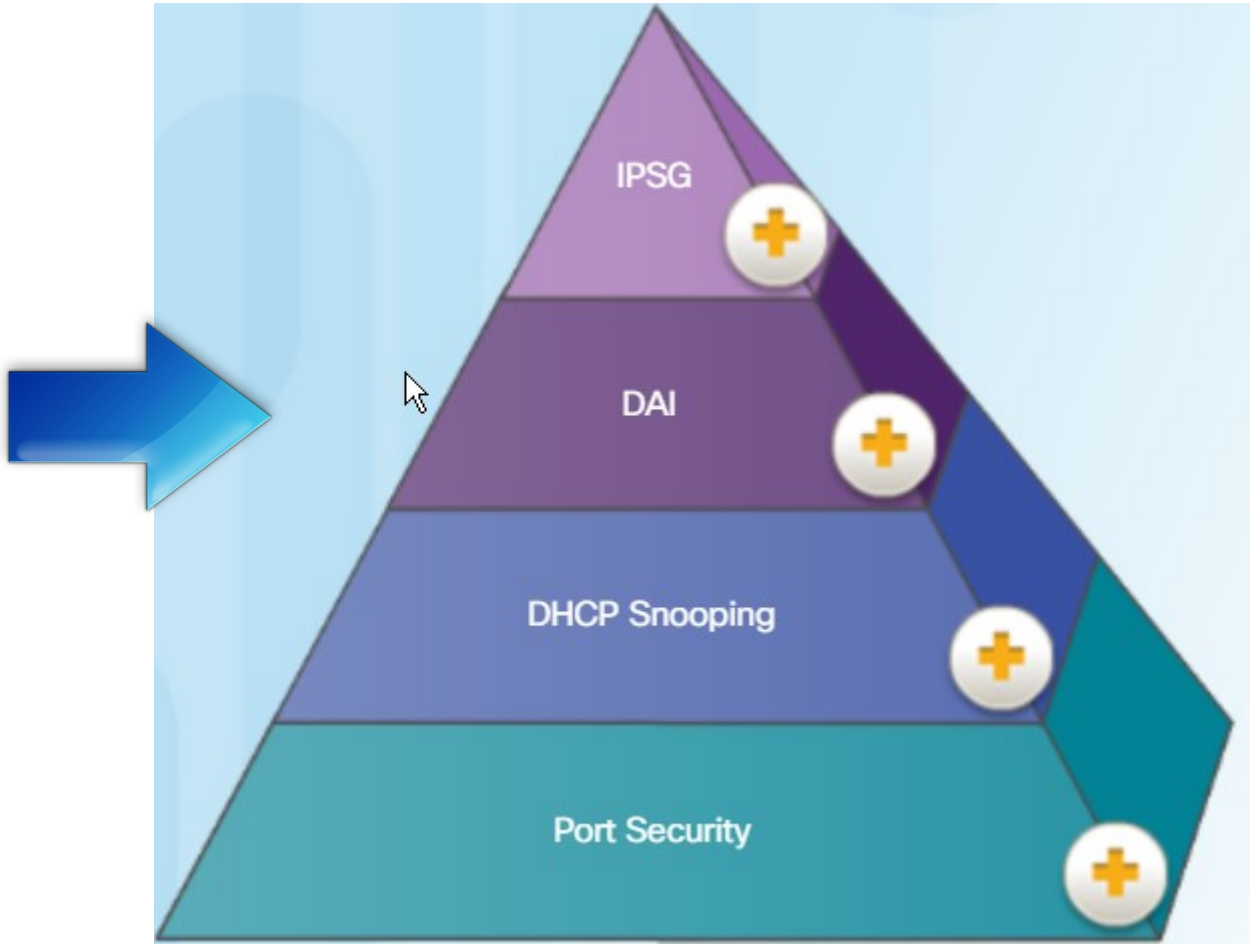
Describe Layer 2 Vulnerabilities

- Network security effort
  - Focuses on perimeter
  - Usually protects the elements in Layer 3 up through Layer 7
- L2 is also important
  - Compromising L2 affects all layers above
  - Layer 2 is considered to be that weakest link



Switch Attack Categories

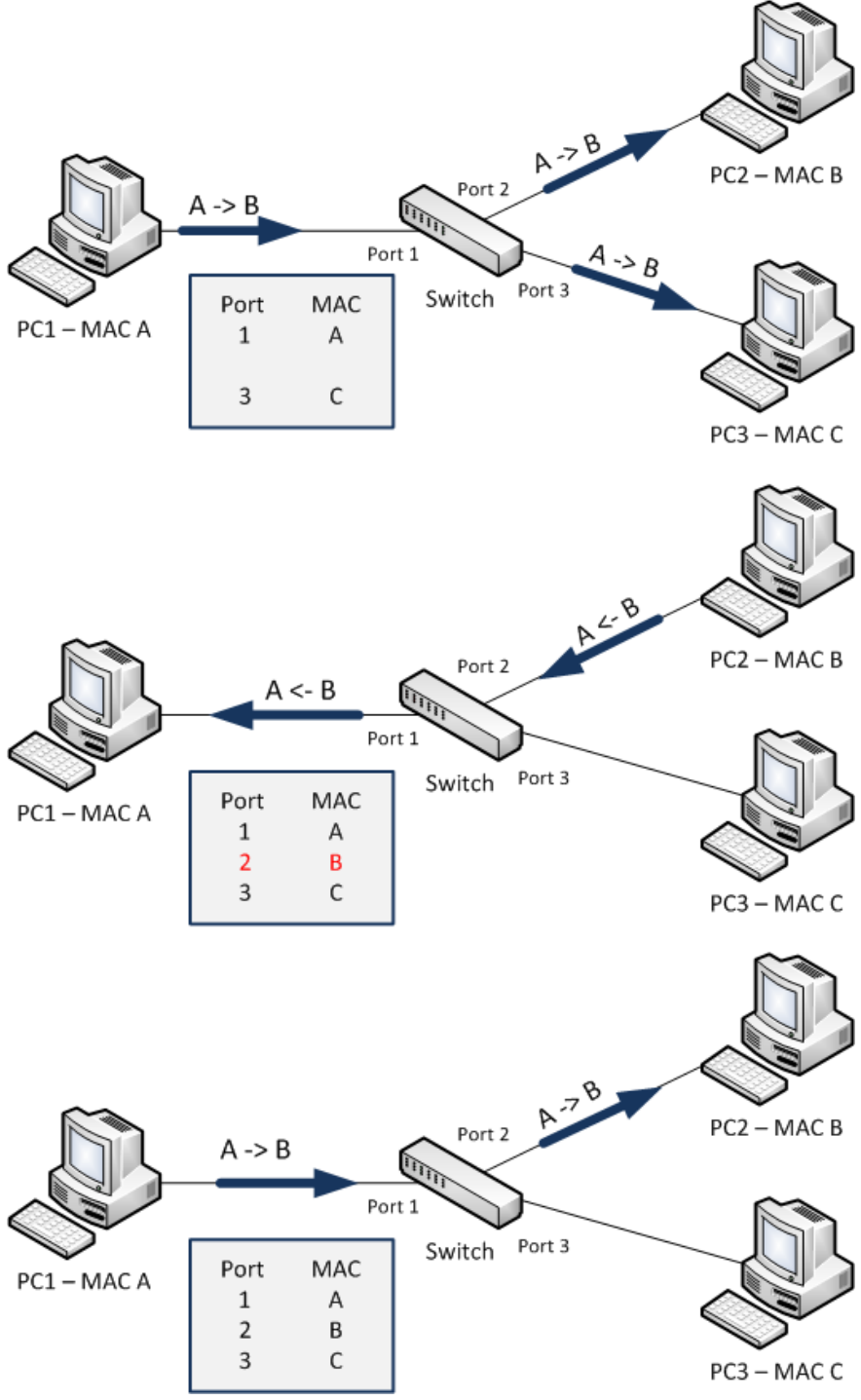
- CAM Table attacks
  - Usually CAM overflow (*macoff*)
- VLAN attacks
  - Vlan hopping, VLAN double tagging (*yersinia*)
- DHCP attacks
  - DHCP starvation, DHCP spoofing
- ARP attacks
  - ARP spoofing, ARP poisoning
- Address spoofing attacks
  - MAC/IP address spoofing
- STP attacks
  - STP manipulation
- Switch device attack
  - CDP manipulation, SSH/Telnet pass attack



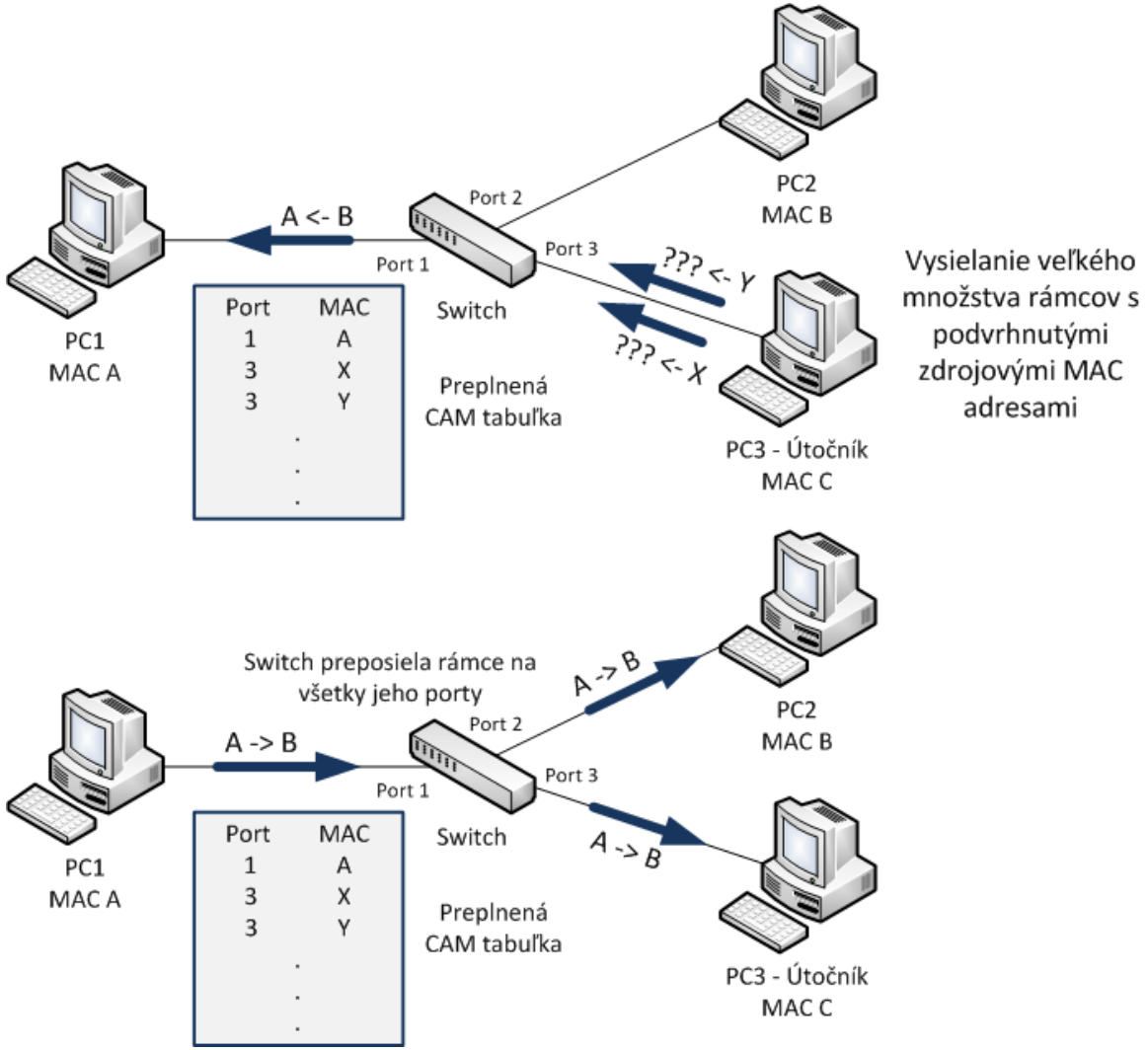
Topic 6.2.2:
CAM Table Attacks

CAM operation - Threat

- Building CAM
  - Learning Process of L2 Switch
    - show mac-address-table
- Threat
  - The CAM table size and the number of items in the table are **limited**
  - Depends on the switch platform



CAM attack – CAM overflow



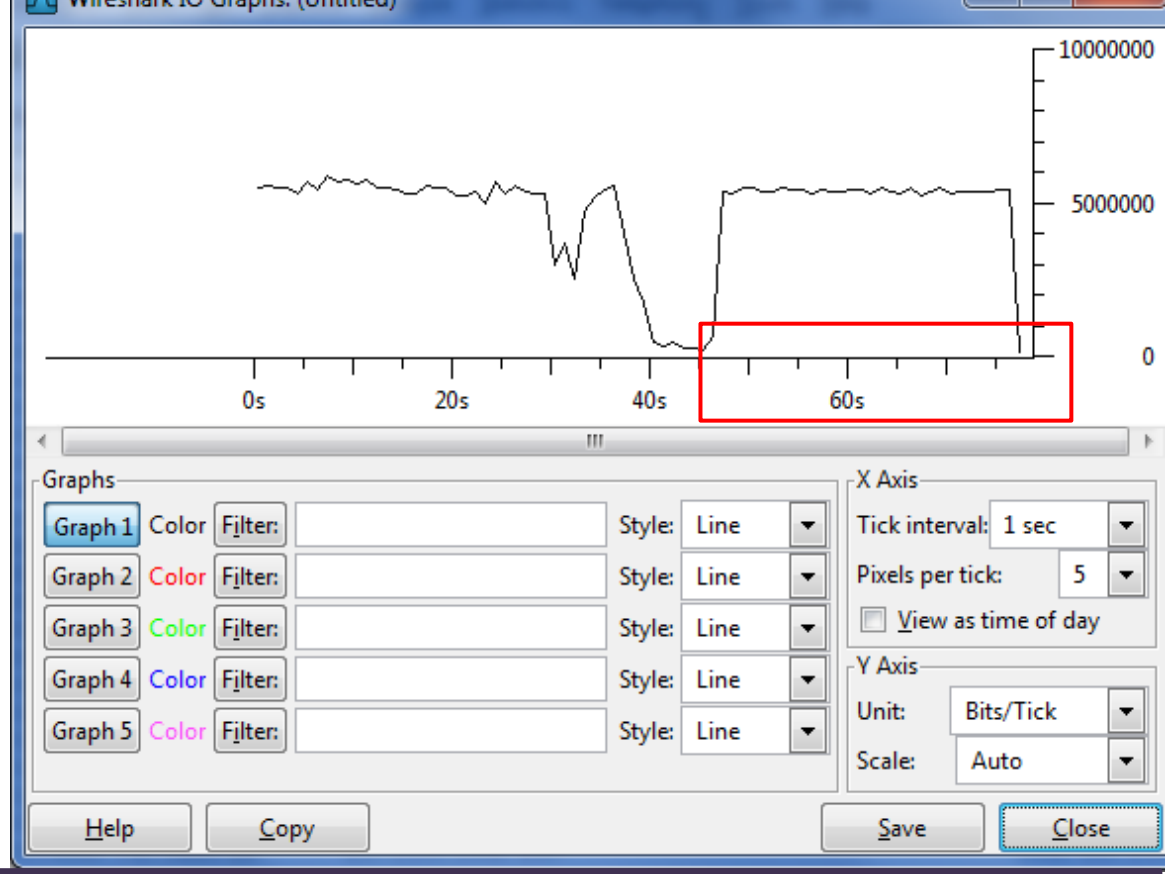
- An attacker sends a large number of frames with different false MAC addresses causes to fill the CAM table
  - Macof, Yersinia
- Switch can not add any new switching info
  - Attack usually starts before employee start to work
- The switch starts to propagate these frames

Realization - macof

- Command (linux)

  macof –i eth0

- Aggressive mode (listing to dev/null)
  - macof –i eth1 2>/dev/null
  - Thousands of messages in a while even on Virtual machine




```
macof -i eth0
9:9e:3b:44:5:20 bd:35:99:23:1d:80 0.0.0.0.41911 > 0.0.0.0.3042: S 535014429:535014429(0) win 512
77:3e:75:40:79:fd 83:78:23:47:5e:6d 0.0.0.0.37577 > 0.0.0.0.16073: S 1654749076:1654749076(0) win 512
1d:2b:8c:65:14:ed 2:ce:2e:1a:8e:3e 0.0.0.0.39944 > 0.0.0.0.65129: S 902864306:902864306(0) win 512
9e:91:d4:77:97:b6 c3:41:e8:33:c9:e2 0.0.0.0.17930 > 0.0.0.0.23148: S 73203385:73203385(0) win 512
f0:78:1f:59:2:82 86:4e:ff:40:b6:11 0.0.0.0.17666 > 0.0.0.0.555: S 1988508690:1988508690(0) win 512
b9:8a:3e:6d:41:c3 6f:40:de:4b:28:60 0.0.0.0.61444 > 0.0.0.0.40408: S 370775209:370775209(0) win 512
d7:ea:a7:8:35:34 66:b0:b8:49:2a:69 0.0.0.0.24670 > 0.0.0.0.56585: S 115082340:115082340(0) win 512
ee:73:27:7b:4f:dd 23:83:53:62:9a:fe 0.0.0.0.29291 > 0.0.0.0.46088: S 1238142262:1238142262(0) win 512
df:56:62:7c:fa:4e e0:a2:65:45:8f:df 0.0.0.0.35816 > 0.0.0.0.40744: S 224492172:224492172(0) win 512
af:ba:0:28:6c:7b cb:34:15:36:ce:dc 0.0.0.0.36257 > 0.0.0.0.17653: S 1640037673:1640037673(0) win 512
2a:1f:3f:9:ff:cd 85:a:ad:6b:e1:d 0.0.0.0.58040 > 0.0.0.0.16133: S 2028675158:2028675158(0) win 512
```

CAM table - Full

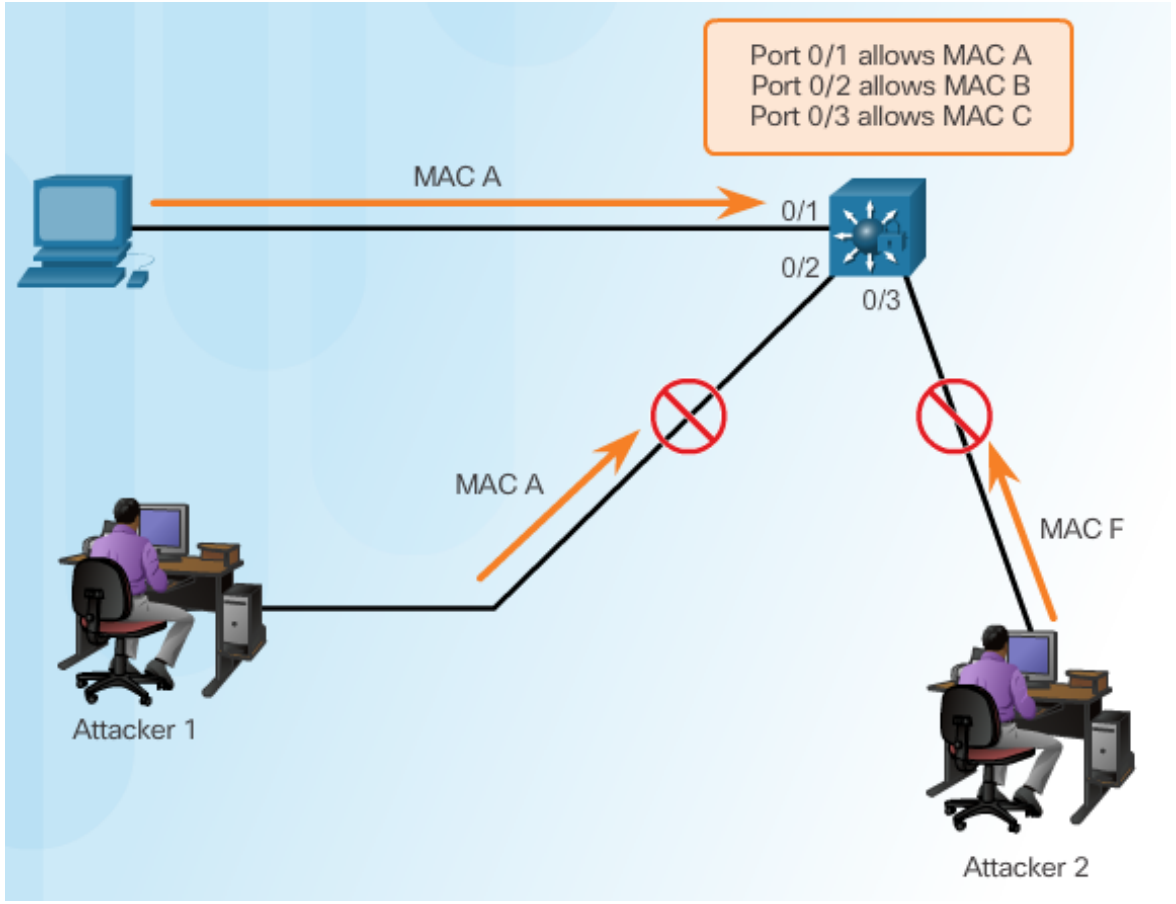
- Once the CAM table is overloaded
  - All frames with unknown destination AMC addresses are flooded to all ports of the VLAN
- This attack affect the CAM tables on other switches too

```
10.1.1.22 -> (broadcast)  ARP C Who is 10.1.1.1, 10.1.1.1 ?
10.1.1.22 -> (broadcast)  ARP C Who is 10.1.1.19, 10.1.1.19 ?
10.1.1.26 -> 10.1.1.25    ICMP Echo request (ID: 256 Sequence number: 7424) ← OOPS
10.1.1.25 -> 10.1.1.26    ICMP Echo reply (ID: 256 Sequence number: 7424) ← OOPS
```

Topic 6.2.3:
Mitigating CAM Table Attacks

Port security - Countermeasure for CAM Table Attacks

- Attack mitigation => **Port security**
  - Allows define the max size list of secure/permitted MAC addresses per port
    - Only end stations with secured mac addresses are **allowed to** communicate
    - Stations with unsecured addresses violates port security – an action is performed
- Three types of secured MAC addresses
  - Static Secure MAC
  - Dynamic Secure MAC
  - Sticky Secure MAC
- Violations action
  - Protect
  - Restrict
  - Shutdown
    - Default action, port becomes err-disabled
    - Up manually or
      - **errdisable recovery cause psecure-violation**



Security Violation Modes

Violation Mode	Forwards Traffic	Sends Syslog Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No
Restrict	No	Yes	Yes	No
Shutdown	No	Yes	Yes	Yes

Configure Port Security

- Port Security is configured individually on switched ports
- Recommended procedure:
  - Set the port to "access" or "trunk"
    - **Necessary** - Port Security is not supported on dynamic ports
  - Set maximum allowed number of MAC addresses
    - Optional, default is 1
    - Max is the number of available addresses defined by SDM template
      - Show sdm prefer
  - Define static secure addresses or sticky learning
    - optional
  - Identify a security breach response (violation action)
    - Optional, the default response is shutdown
  - Specify the way expired safe addresses
    - Optional. Without additional settings, static and sticky addresses do not expire at all, dynamic expires only when the port is disconnected
  - Enable port security
    - **Necessary,** and often overlooked!

Configure and verify

```
! Configure
Sw(config)# interface fa0/2
Sw(config-if)# switchport mode access
Sw(config-if)# switchport port-security maximum 5
Sw(config-if)# switchport port-security mac-address 001c.2320.3a28
Sw(config-if)# switchport port-security violation restrict
Sw(config-if)# switchport port-security aging time 10
Sw(config-if)# switchport port-security
```

```
! Verify
Sw# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/2                5            3                  0          Restrict
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 2
Max Addresses limit in System (excluding one mac per port) : 8192
```

Port Security Aging

- Sets the aging time for static and dynamic secure addresses on a port
  - Absolute
    - Secure address is deleted after elapsing aging timer
  - Inactivity
    - Secure address is deleted after time of inactivity

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

Parameter	Description
static	• Enable aging for statically configured secure addresses on this port.
time time	• Specify the aging time for this port. • The range is 0 to 1440 minutes. • If the time is 0, aging is disabled for this port.
type absolute	• Set the absolute aging time. All the secure addresses on this port age out exactly after the time (in minutes) specified and are removed from the secure address list.
type inactivity	• Set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

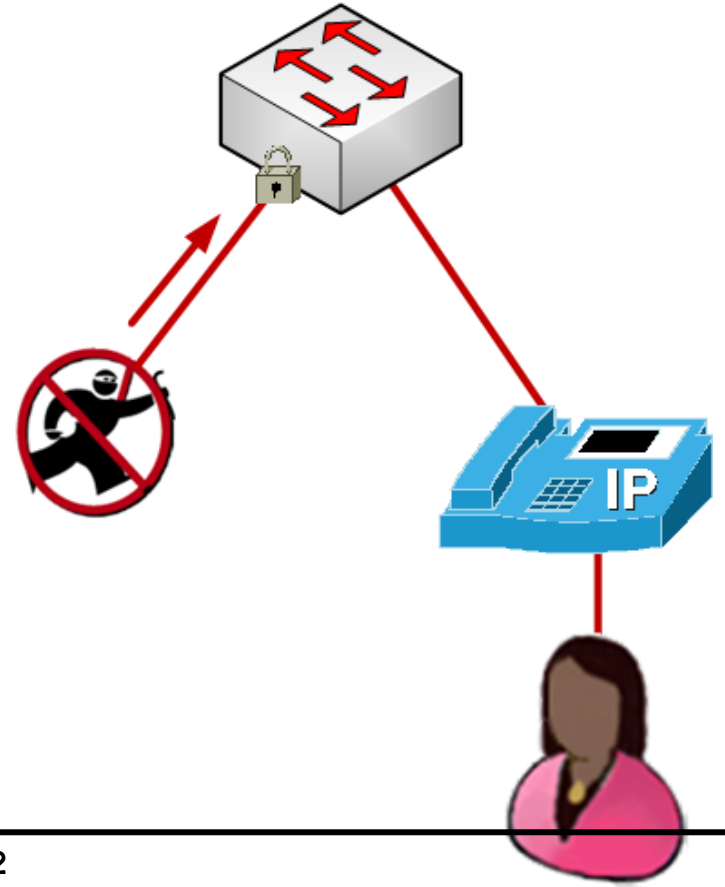
Verify

```
Sw# show port-security interface fa0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 10 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 3
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00e0.4c3b.b787:1
Security Violation Count   : 0
```

```
Sw# show port-security address
          Secure Mac Address Table
-----------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    0011.2233.4455    SecureConfigured              Fa0/2         -
   1    00e0.4c3b.b787    SecureDynamic                 Fa0/2         8
   1    0200.0000.0001    SecureDynamic                 Fa0/2         8
-----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 2
Max Addresses limit in System (excluding one mac per port) : 8192
```

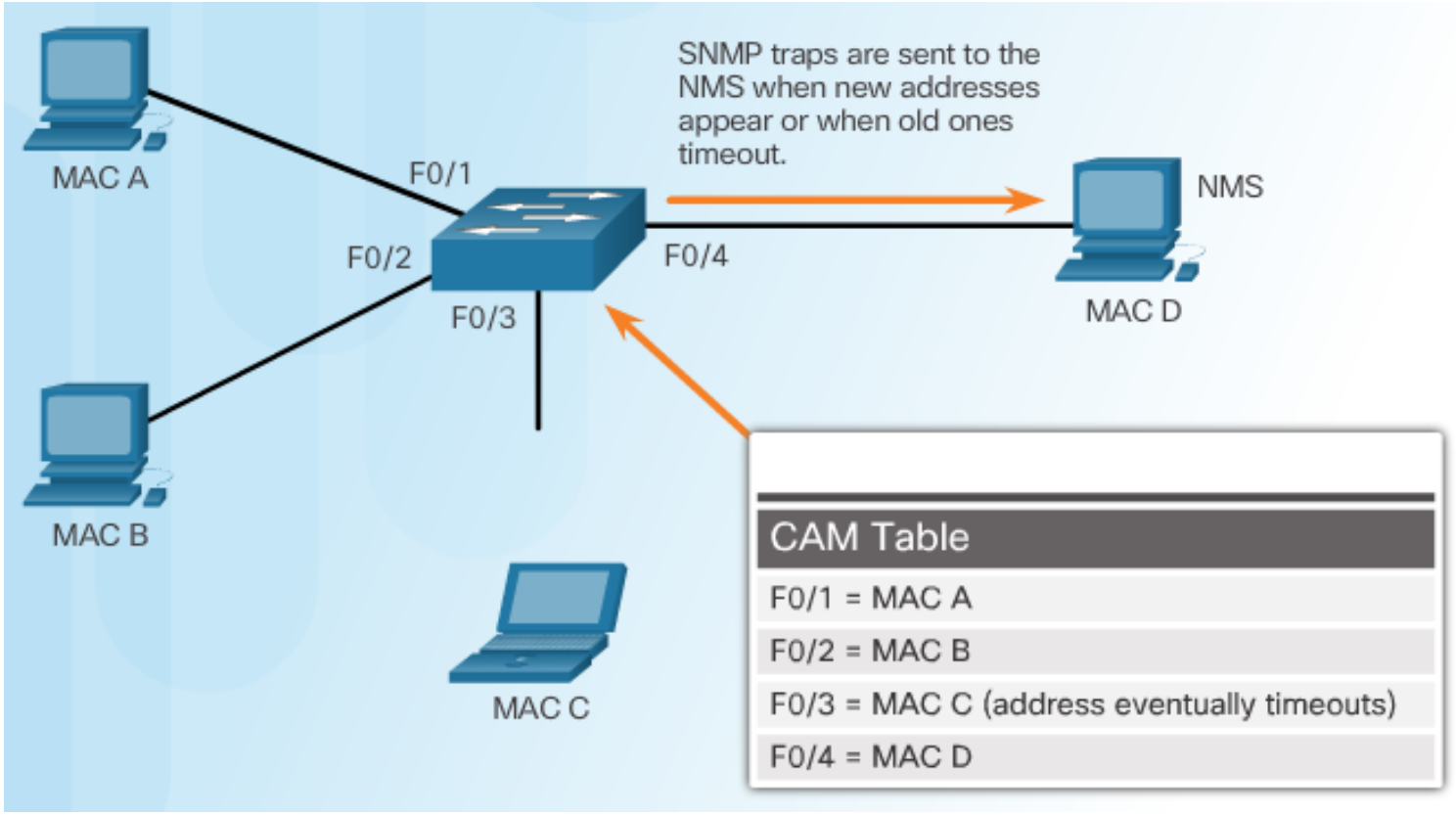
Port security on ports with VoIP phone

- VoIP phones may use two or three MAC addresses
  - According to HW
    - If they use CDPs they requires three
    - If they do not use CDPs two
- Consider action on violation
  - Recommended is Restrict
  - Acceptable shutdown (by policies)
- The goal is to protect the service and the switch not control the access




```
Sw(config)# interface fa0/2
Sw(config-if)# switchport port-security
Sw(config-if)# switchport port-security maximum 3
Sw(config-if)#

! Umozni VoIP aj v podmienkach utoku
Sw(config-if)# switchport port-security violation restrict

!nastav aging poloziek na 2 minuty neaktivity
Sw(config-if)# switchport port-security aging time 2
Sw(config-if)# switchport port-security aging type
inactivity
```

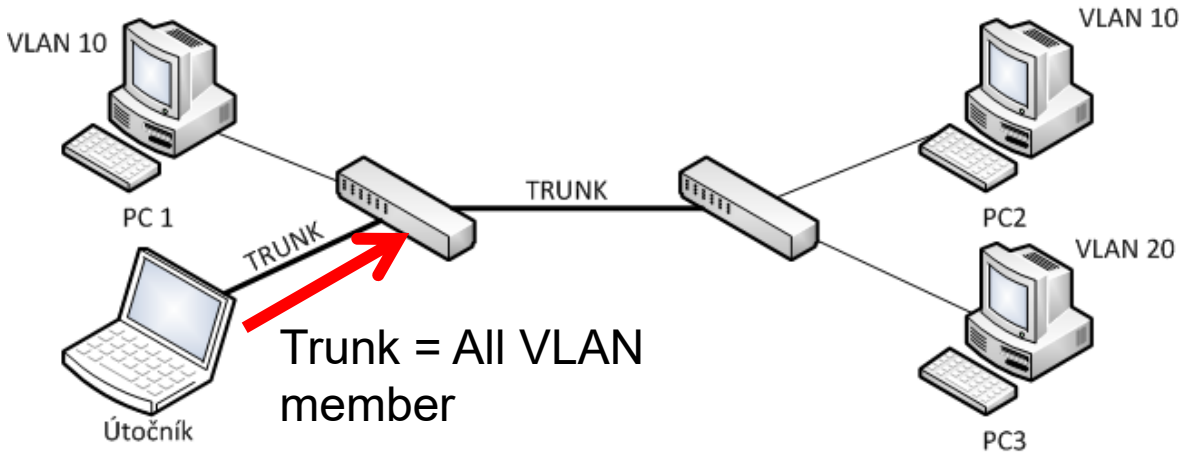
SNMP MAC Address Notification



Topic 6.2.4:
Mitigating VLAN Attacks

VLAN hopping attacks

- There are several types of attacks that try to cause that the frame from a station in a VLAN X try to "flee" to another VLAN Y
  - No way back is required
  - This is not a problem, for example, with TCP SYN Flood Attack
- The two most common attack vectors:
  - DTP Attack (Switch Spoofing)
    - Attach attacker host or rogue switch and perform DTP signaling attack (yersinia)

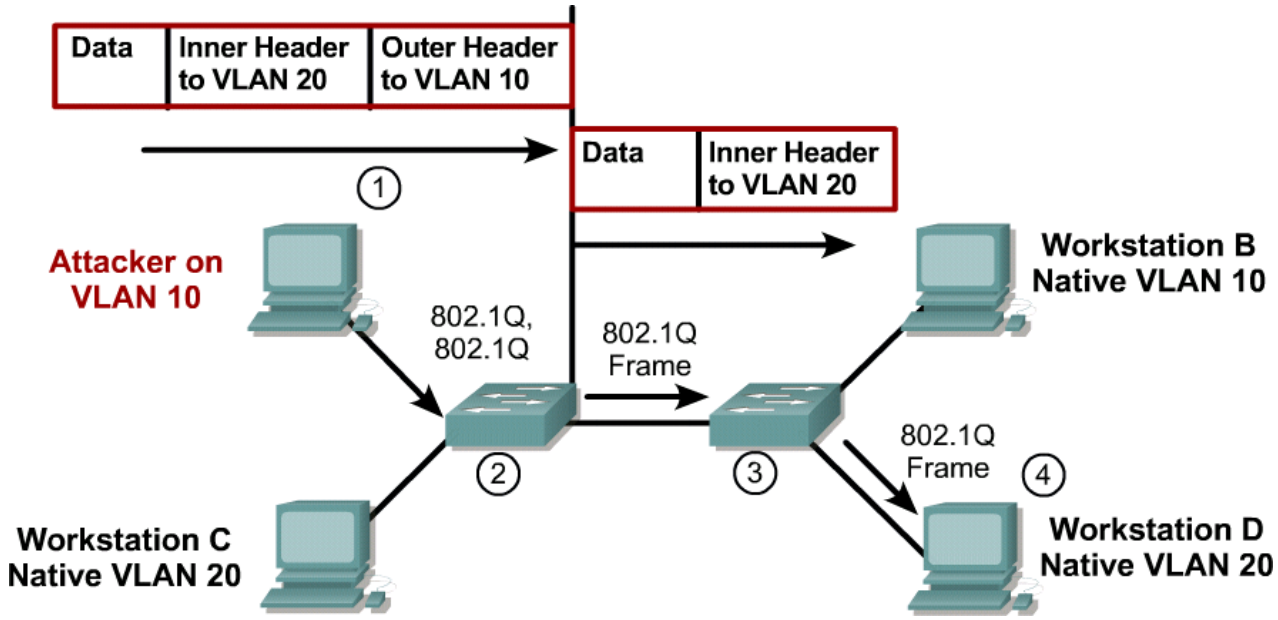


  - Double tagging at 802.1Q (Double tagging)
  - + attack between hosts of the same vlan

VLAN Double-Tagging Attack

- The trunk port between switches has native VLAN 10
- An attacker in VLAN 10 sends a frame that has two tags
  - The top has VID 10
  - The bottom has a VID 20
- Switch accepts the frame
- As the frame belongs to VLAN 10, the native vlan on the trunk, the switch removes the top tag
- The frame will arrive on the next switch with the tag 20
- Receiving switch processes it in VLAN 20

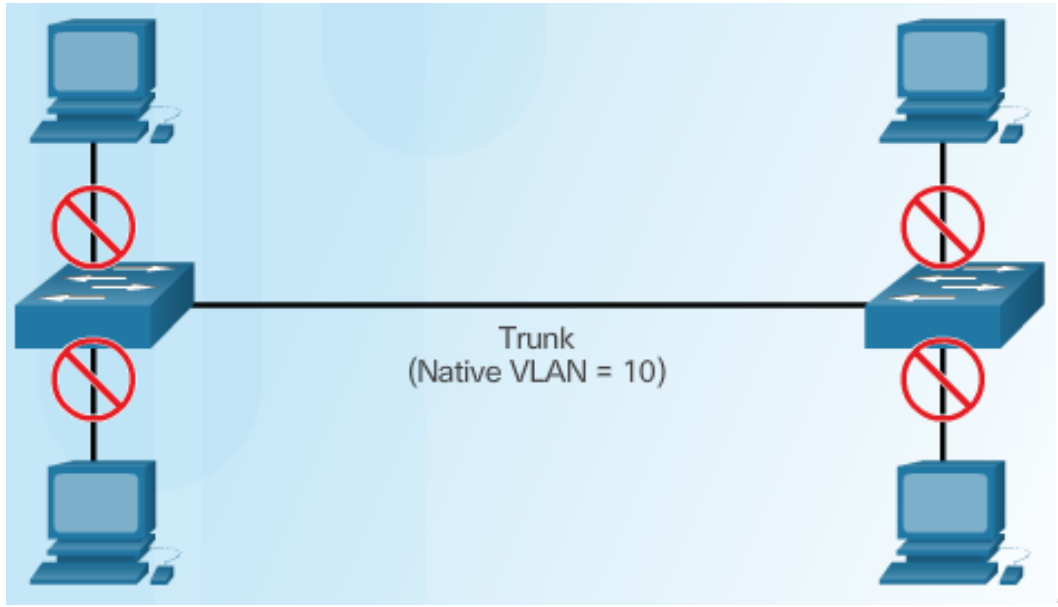
- Works only if an attacker has access to the port residing on the same vlan as native vlan



Mitigating VLAN DTP/Hopping Attacks

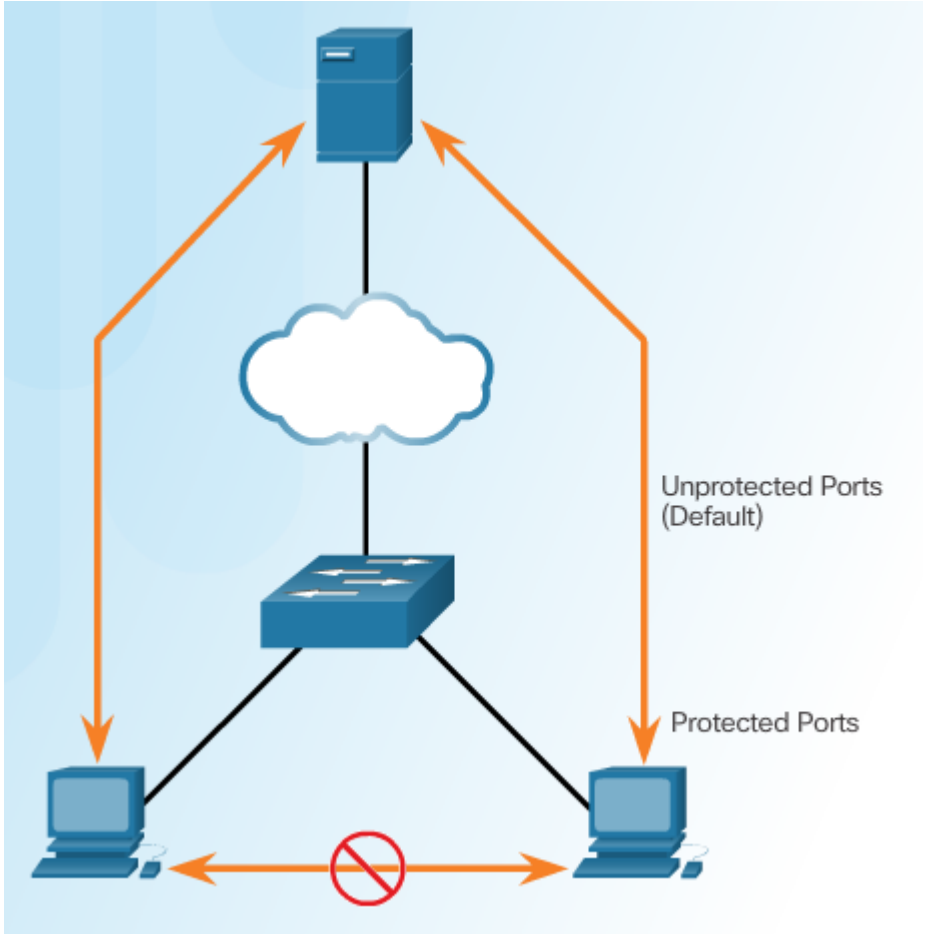
- VLAN Hopping mitigation
  - Use a native vlan which is never assigned as a data vlan (access vlan)
  - Turn on tagging of all vlans
    - `Vlan dot1q tag native`
  - Disable dynamic trunk negotiation
  - Disable unused ports and put them in an unused VLAN
  - Do not use VLAN 1 for anything

- DTP attacks mitigation
  - On ports turn off dynamic negotiations and DTP
  - DTP is deactivated if
    - If port is set as static access
      - `Switchport mode access`
    - Port is set as a static trunk
      - `Switchport mode trunk`
    - Manually deactivate DTP
      - `Switchport nonegotiate`
    - Port is set as routed (L3)
      - `No switchport`



Mitigating intra VLAN attacks - PVLAN Edge Feature

- Private VLAN Edge
  - Or Protected Ports
  - Simpler concept, domain of lower cost switches
  - Disable switching between ports of the same vlan *on the same switch*
    - Something as port isolation
    - Only local significance
  - Protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port
    - to pass the communication through L3 device is required
    - Control traffic is forwarded
  - Communication between protected and un-protected is allowed



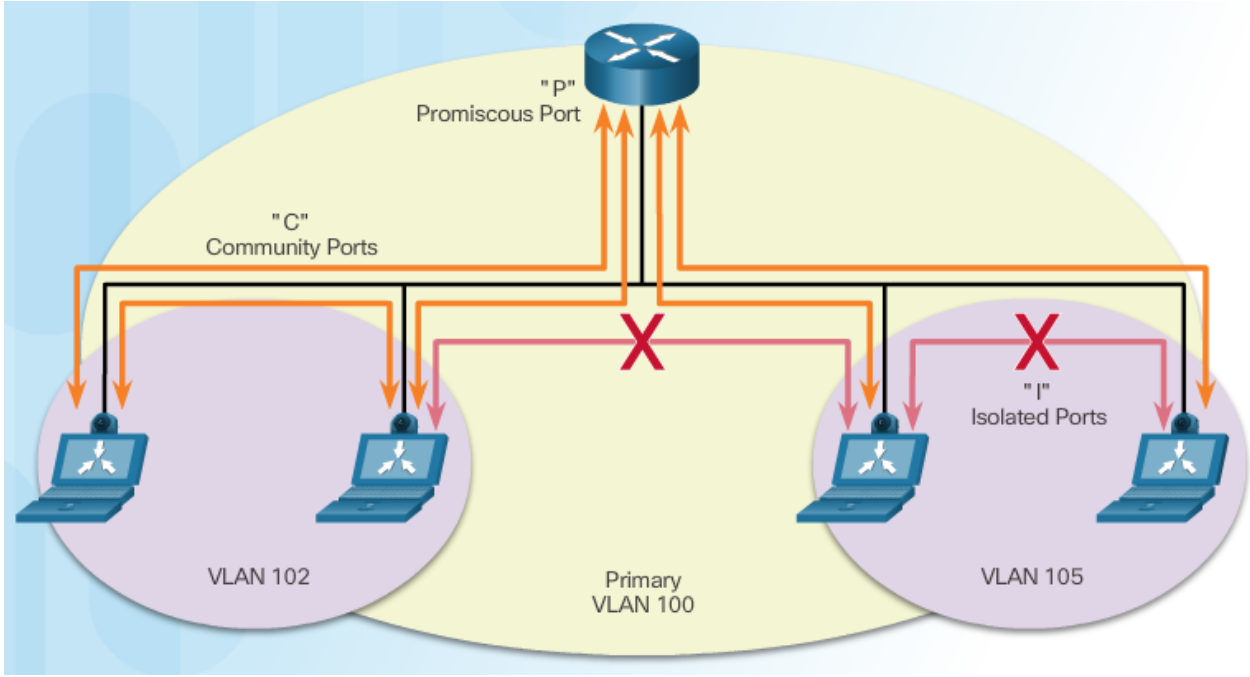
Configuring and verifying Protected Ports

```
Switch(config-if)# switchport protected
```

```
Switch# show interfaces gigabitethernet1/0/1 switchport
Name: G1/0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
<output omitted >
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

Voice VLAN: none (Inactive)
Appliance trust: none
```

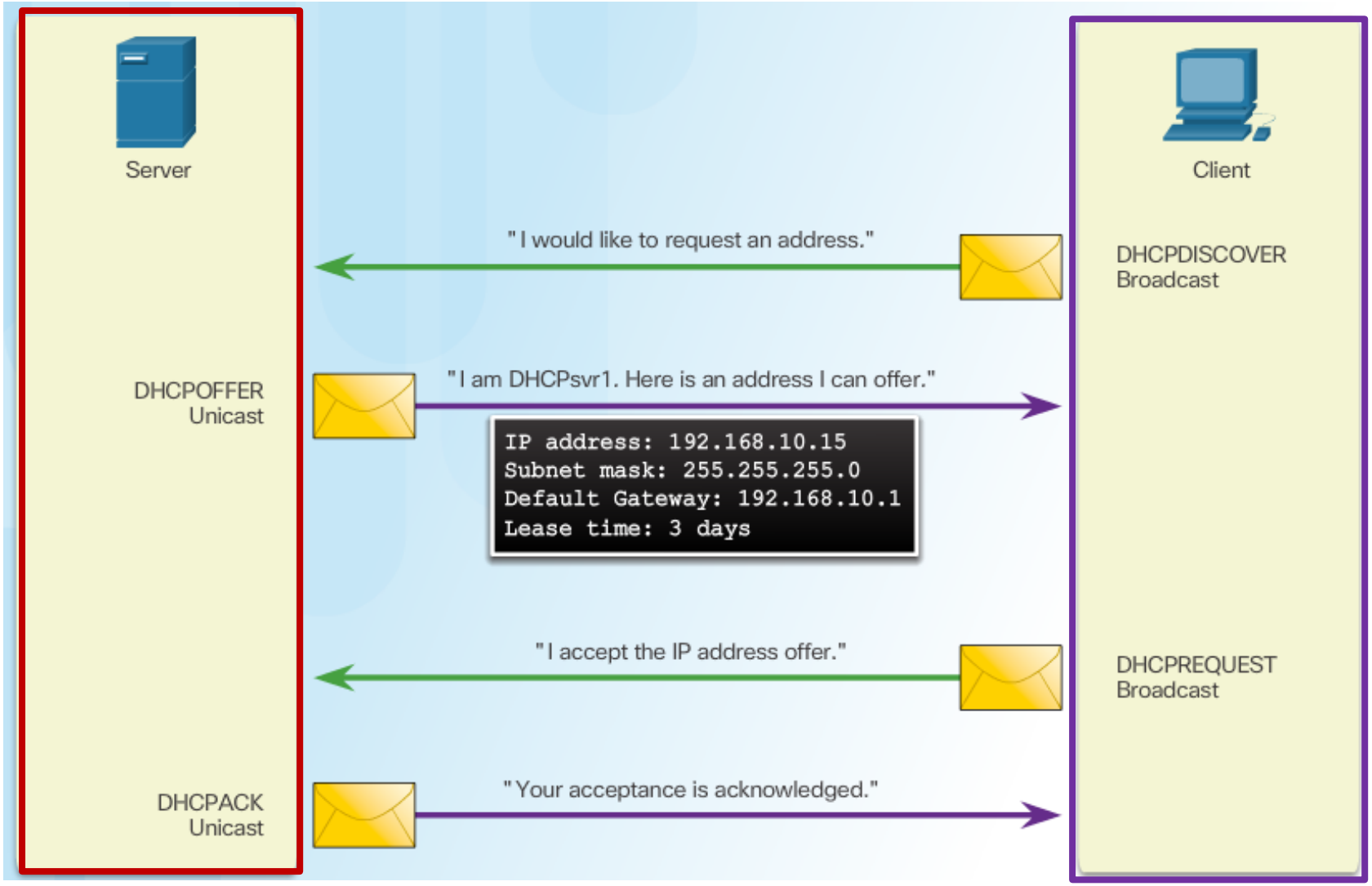
Private VLANs

- More complex as PVLAN Edge
- Usually domain of Multilayer switches
- Allows to control L2 switching between ports of the same VLAN
  - Permit or disable inter port communication
- Use concept of primary vlan
  - Internally separated into secondary VLANs
- Secondary VLANs – two types
  - Community
    - Ports can talk to other community and promiscuous ports
  - Isolated
    - Complete Layer 2 separation from the other ports within the same PVLAN
    - Only able to talk to promiscuous ports
    - Can be only the one
- Promiscuous port
  - An entry point to all vlans
  - port can talk to everyone



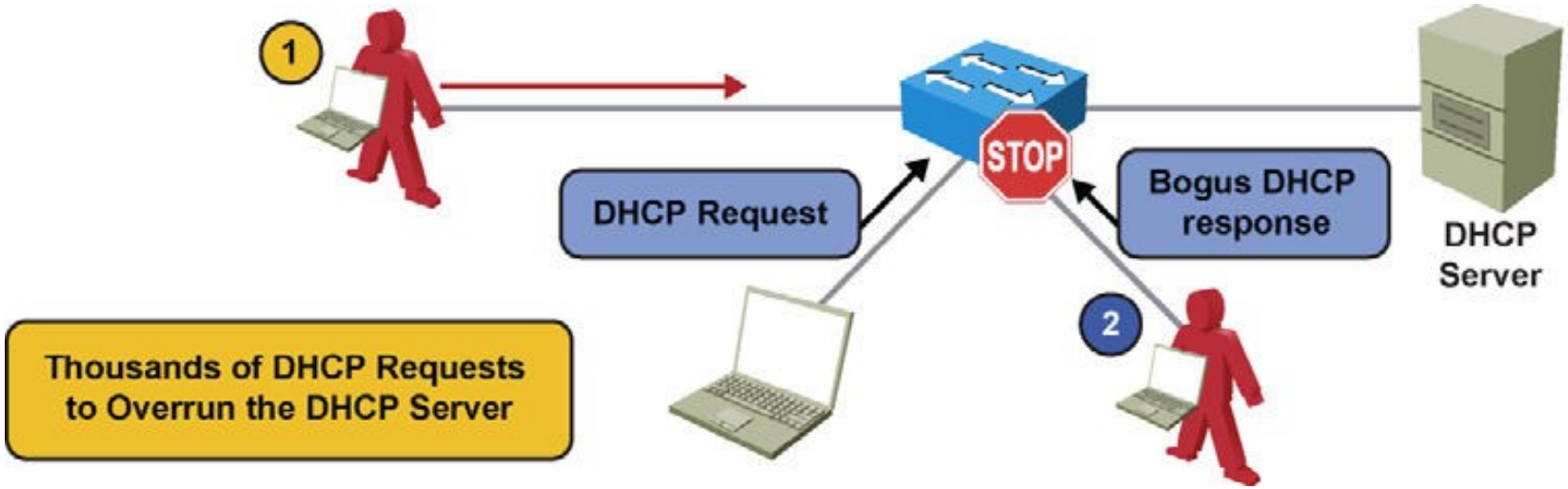
Topic 6.2.5:
Mitigating DHCP Attacks

DHCP – principle of operation (*DORA mnemo*)



DHCP spoofing

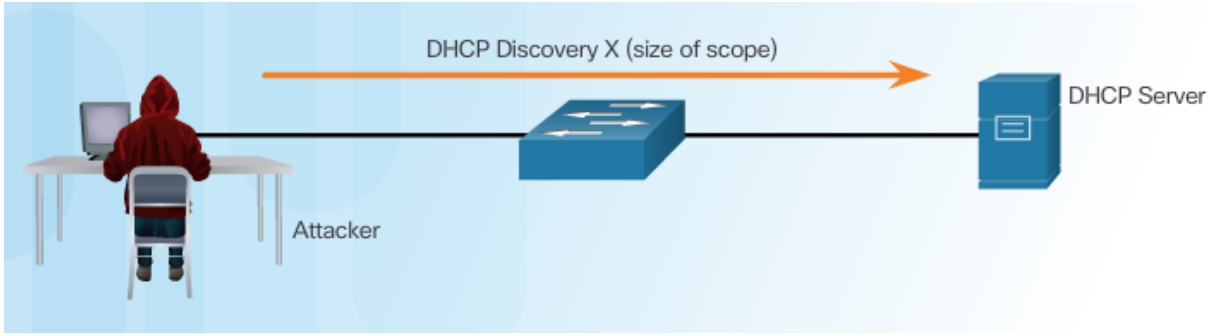
- Attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients
  - This could be a malicious activity
  - Many times, however, it is rather negligent
    - a custom access point, a notebook with network software, and so on
- A rogue server can provide a variety of misleading information
  - **Wrong default gateway**
    - An attacker may becomes a gateway (M-i-M)
    - Or DoS attack
  - **Wrong DNS server**
    - An attacker is DNS
    - Or DoS attack
  - **Wrong IP address**
    - DoS



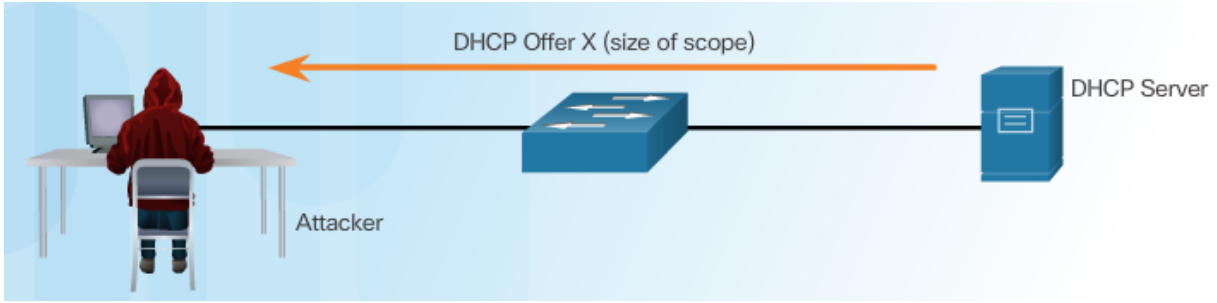
DHCP Starvation Attack

- DoS attack
- An attacker tries to exhaust the whole DHCP pool/range
  - Generates a lot of DHCP Discovery requests, that seems as legal
    - yersinia dhcp -attack 1

Attacker Initiates a Starvation Attack

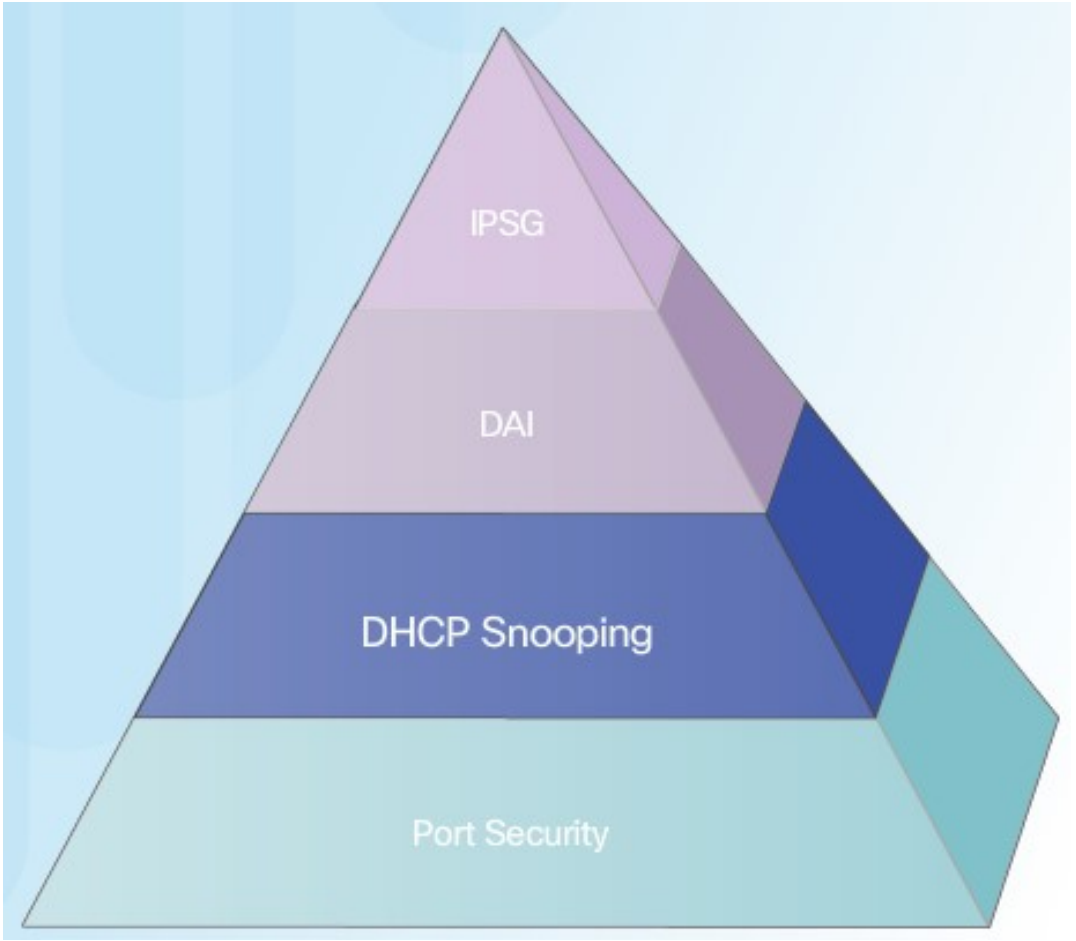


DHCP Server Offers Parameters



Mitigating DHCP Attacks

- DHCP Starvation attack
  - Port security
  - Dhcp snooping limit rate
- DHCP spoofing attack
  - DHCP Snooping (solution)
    - The switch will deny packets containing specific information:
      - Unauthorized DHCP server messages from an untrusted port
      - Unauthorized DHCP client messages not adhering to the snooping binding table or rate limits
      - DHCP relay-agent packets that include option-82 information on an untrusted port

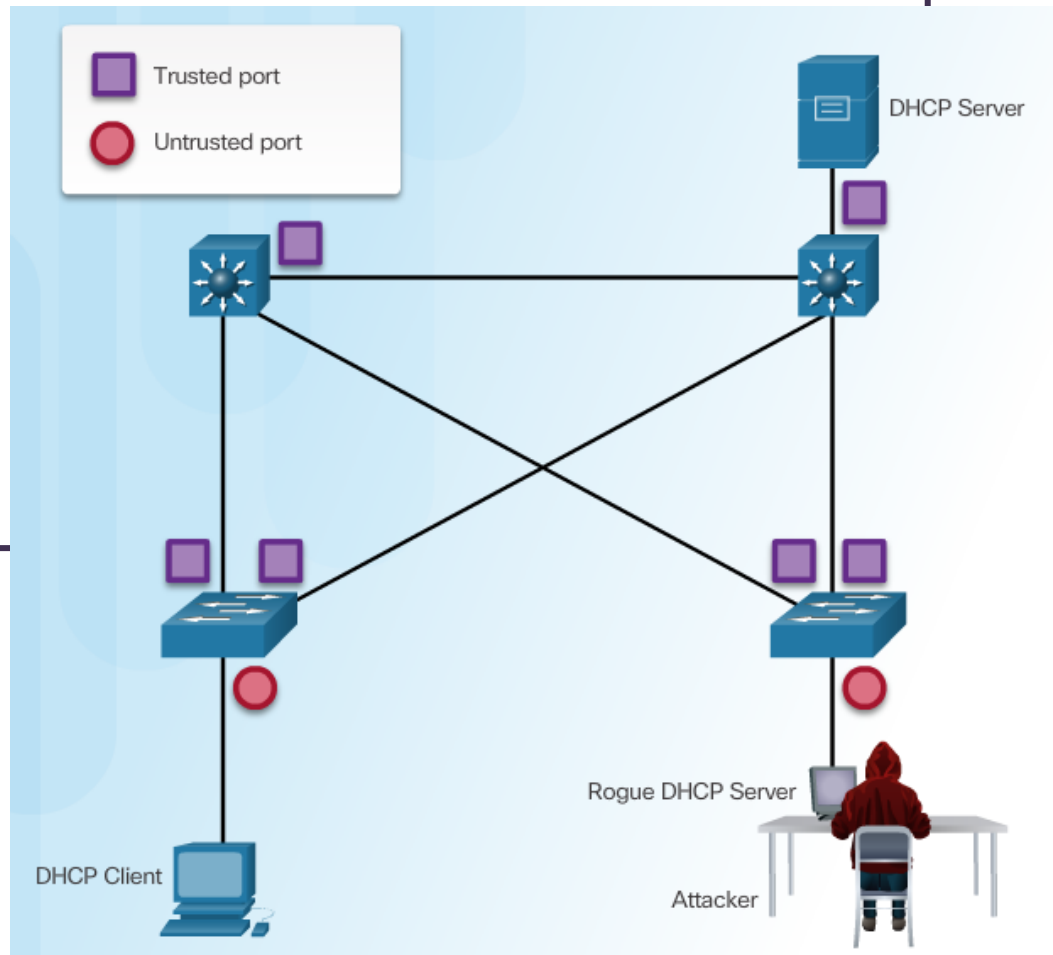


DHCP Snooping

- DHCP Snooping recognizes trusted and untrusted ports
  - Untrusted ports:
    - There are stations
    - The default port type
  - Trusted ports (or behind them)
    - There are DHCP servers or a network core
- DHCP Snooping sniff DHCP communication on untrusted ports and creates a DHCP binding database
  - Database contains records as the client MAC address, assigned IP, lease time, VLAN, and port
    - Note: in a large network, the DHCP binding table may take time to build
  - This database later uses DHCP Snooping as well as other security mechanisms
- If DHCP Snooping passes a DHCP message from a client, DHCP Option-82 is inserted into it
  - An information field that identifies which switcher and which port the client is connected to

Configuring DHCP Snooping

```
! Zapni globalne
Sw(config)# ip dhcp snooping
! Zapni pre vlan 1, 10 a 20, 100 az 110
Sw(config)# ip dhcp snooping vlan 1,10,20,100-110
! Definuj ktore porty su trust
Sw(config)# interface fa0/24
Sw(config-if)# ip dhcp snooping trust
Sw(config-if)# int fa0/1
! Na untrusted zapnit limit rate
Sw(config-if)# ip dhcp snooping limit rate 10

! Zapni options 82, volitelne
Sw(config)# ip dhcp snooping information option
```



Verifying DHCP Snooping

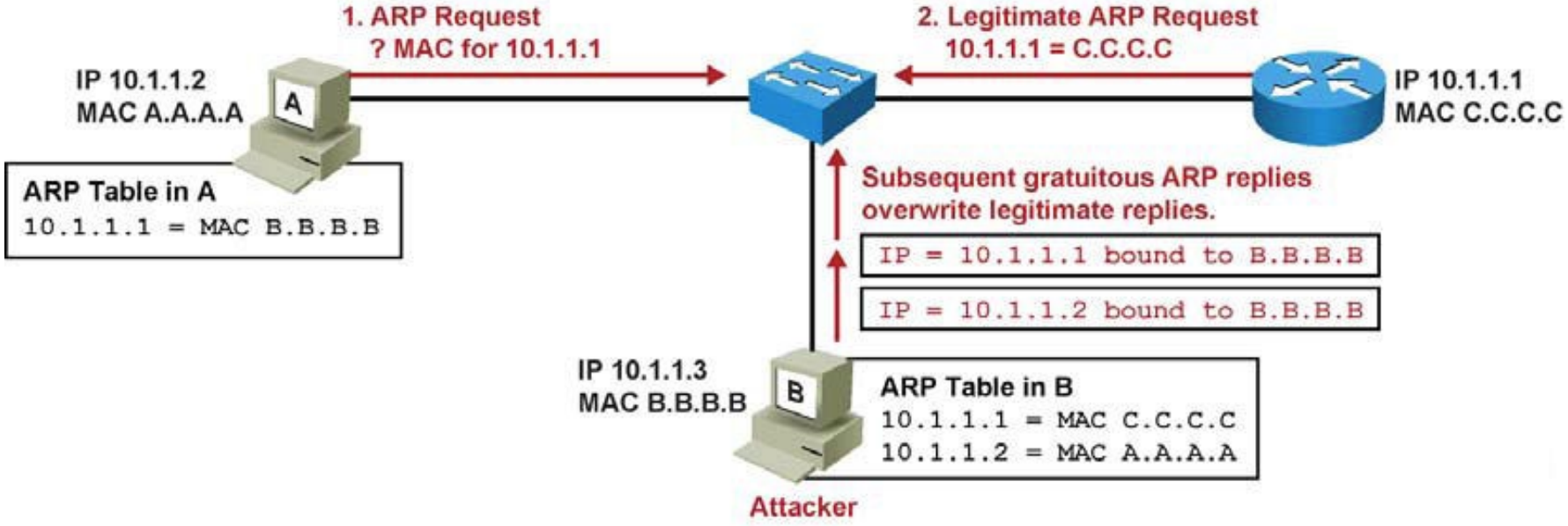
```
Sw# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1,10,20,100-110
DHCP snooping is operational on following VLANs:
1,10,20,100-110
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 001d.e5be.e380 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet0/24           yes        yes             unlimited
  Custom circuit-ids:
```

```
Sw# show ip dhcp snooping binding
MacAddress          IpAddress    Lease(sec)  Type            VLAN  Interface
------------------  ----------   ----------  -------------   ----  ---------
00:E0:4C:41:3C:E9   10.0.0.4     84960       dhcp-snooping    1     Fa0/11
00:E0:4C:3B:B7:87   10.0.0.6     85042       dhcp-snooping    1     Fa0/1
Total number of bindings: 2
```

Topic 6.2.6:
Mitigating ARP Attacks

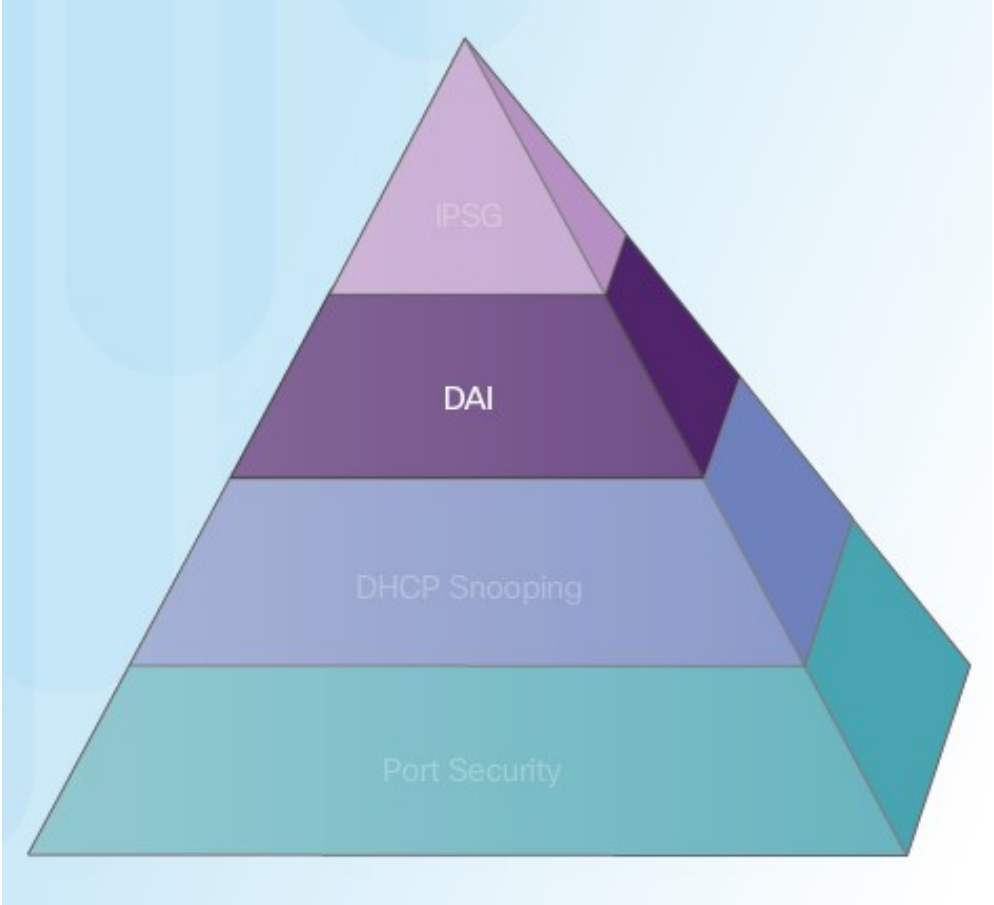
ARP Spoofing

- ARP Spoofing
  - is the sending of gratuitous ARP (unsolicited) messages in which selected IP is mapped to a non-real MAC address
    - Denial of Service attack: IP mapping to nonexistent MAC
    - Man-In-The-Middle attack, ARP poisoning attack: mapping of victim IP to an attacker MAC
  - Tools: Cain & Abel (win), ettercap -G, yersinia



Mitigating ARP Attacks - *Dynamic ARP Inspection (DAI)*

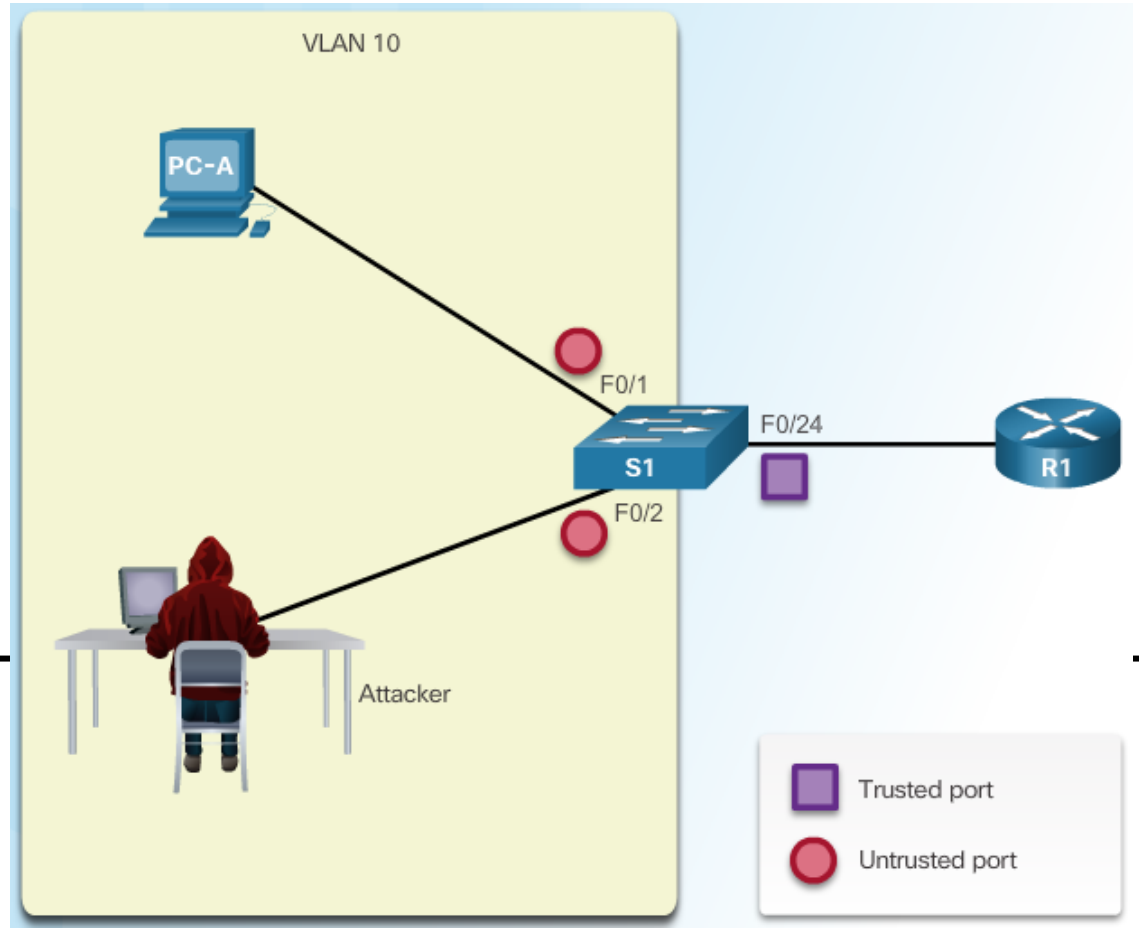
- Dynamic ARP Inspection (DAI)
  - Uses ARP validation against DHCP snooping database
  - Each ARP message contains among others
    - Sender MAC and Sender IP
    - Target MAC and Target IP
  - DAI checks whether these data in ARP messages conform against DHCP Snooping database
    - If the source MAC or ARP reply match DHCP leased IP address




```
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: IntelCor_b0:06:bc (9c:4e:36:b0:06:bc)
  Sender IP address: 192.168.1.102 (192.168.1.102)
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.1.101 (192.168.1.101)
```

Configuring Dynamic ARP Inspection

- DAI again classify ports as
  - Trusted
  - Untrusted
    - The default type
    - the switch checks the content of incoming ARP messages against the DHCP Snooping database
  - If ARP messages are inappropriate
    - discard
- DAI configuration assumes functional DHCP Snooping




```
Sw(config)# ip dhcp snooping
Sw(config)# ip dhcp snooping vlan 10
Sw(config)# ip arp inspection vlan 10
Sw(config)# int gigabitEthernt 1/1
Sw(config-if)# ip dhcp snooping trust
Sw(config-if)# ip arp inspection trust
! Messages under attack
Mar  1 01:06:49.880: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/23, vlan
10.([0800.27e2.2182/172.16.10.1/0000.0000.0000/172.16.10.2/01:06:49 UTC Mon Mar 1 1993])
*Mar  1 01:06:51.893: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/23, vlan
10.([0800.27e2.2182/172.16.10.1/0000.0000.0000/172.16.10.2/01:06:51 UTC Mon Mar 1 1993])
```

Dynamic ARP Inspection

- Additional functionality – ARP message validation

```
Sw(config)# ip arp inspection validate { [src-mac] [dst-mac] [ip [allow-zeros] ] }
```

- Možnosti:
  - **src-mac**: Zdrojová MAC rámca sa musí zhodovať so zdrojovou MAC v tele ARP správy. Kontrolujú sa queries aj replies
  - **dst-mac**: Cieľová MAC rámca sa musí zhodovať s cieľovou MAC v tele ARP správy. Kontrolujú sa iba replies
  - **ip**: IP adresy v tele ARP správy musia byť iné ako 0.0.0.0, 255.255.255.255 a nesmú byť multicastové. Kontrolujú sa queries aj replies, cieľová IP adresa sa kontroluje iba v replies
  - **allow-zeros**: Pri kontrole „ip“ sa povoľuje, aby zdrojová IP mohla byť 0.0.0.0

Topic 6.2.7:
Mitigating Address Spoofing Attacks

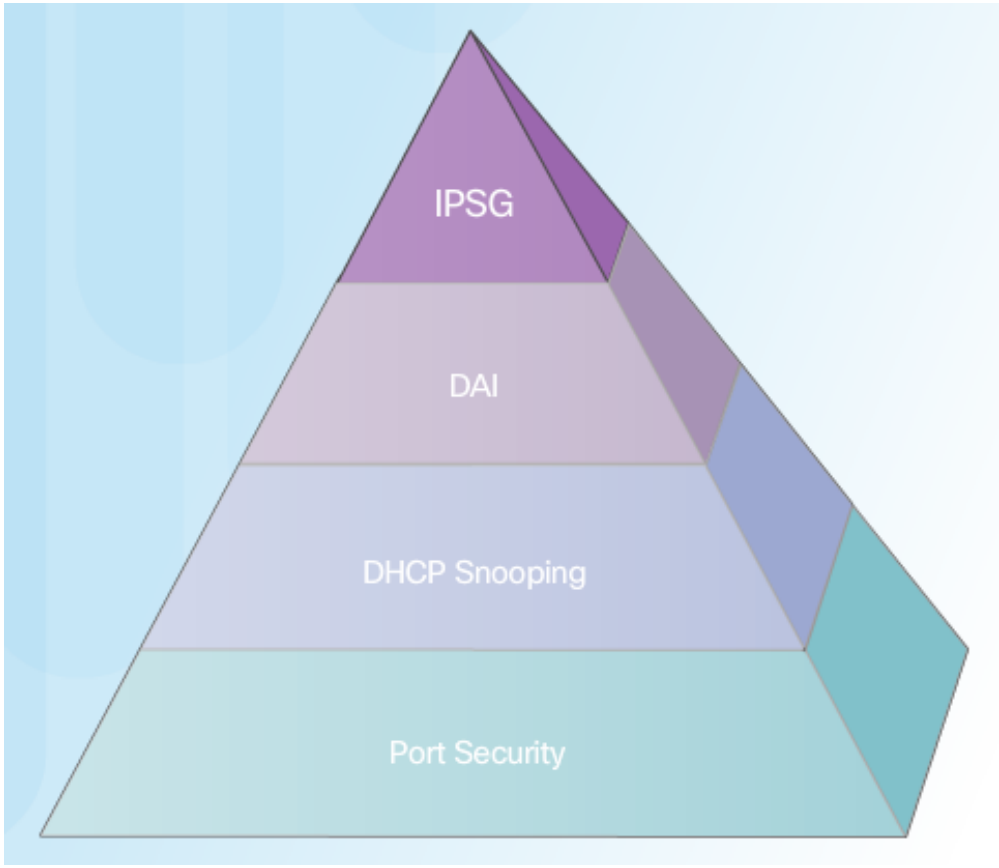
Address Spoofing Attack

- Address spoofing
  - Any attack where someone is trying to introduce as the other entity
    - Spoofing is an effort to make think someone as who is not
- Well known spoof categories
  - MAC spoofing
  - IP spoofing
  - DHCP spoofing

- IP Spoofing
  - The steal of an valid IP address from another station
    - Used, e.g. at Ping of death, ICMP unreachable storm, SYN flood
  - The source of many existing DoS and DDoS attacks
- Mitigation = IP Source Guard (IPSG)

Mitigating Address Spoofing Attacks - IPSG

- IPSG
  - Requires DHCP snooping
  - Once a client has obtained dynamic IP address
    - IPSG Install per-port VLAN ACLs (PVACL) based on IP-to-MAC-to-switch-port bindings
  - Then checks each IP packet source address on a port
    - As DAI does for ARP
  - Permits traffic for packets with valid source IP address
    - Deny all others
- For each untrusted port, there are two possible levels of IP traffic security filtering:
  - Source IP address filter
    - Permit only traffic with a source IP address that matches the IP source binding entry
  - Source IP and MAC address filter
    - Permit only traffic with a valid source IP address and MAC address



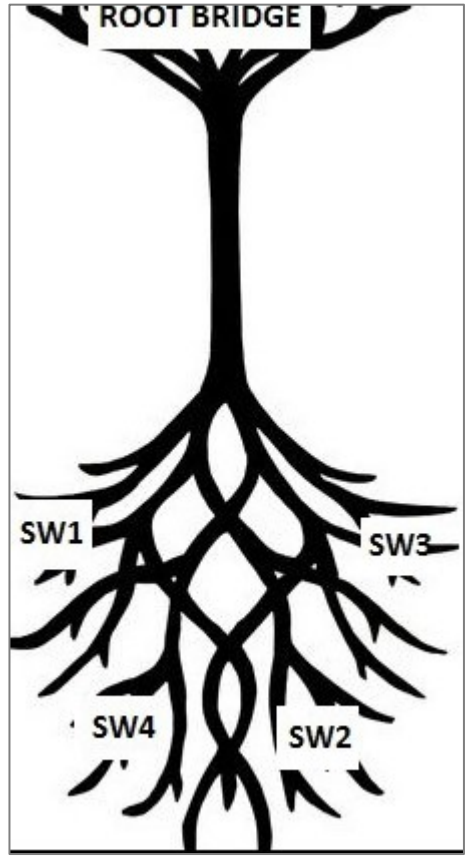
Configuring and verifying IP Source Guard

```
! Dhcp snooping is required
Sw(config)# ip dhcp snooping
Sw(config)# ip dhcp snooping vlan 1, 10
Sw(config)# int fa0/1
Sw(config-if)# ip verify source vlan dhcp-snooping

! Or
Sw(config-if)# ip verify source
```

```
! Zobraz IP SG
Switch# show ip verify source
Interface Filter-type Filter-mode  IP-address       Mac-address        Vlan
--------- ----------- -----------  ---------------  -----------------  ----------
Fa2/1     ip-mac      active       10.1.1.11        00:02:B3:3F:3B:99  1
Fa2/18    ip-mac      active       10.1.10.11       00:00:00:0a:00:0b  10
```

Topic 6.2.8:
Spanning Tree Protocol

Introduction to the Spanning Tree Protocol



- Standardized as IEEE 802.1d
- Works on the L2 layer
- Prevents looping in switched networks
  - Detects redundant links and blocks them
  - Permits only one route to each destination
  - Protects against brodcast storms and connectivity problems
- Allows switches to communicate with one another
  - By sending BPDU frames (every 2 seconds)
- Uses Spanning Tree Algorithm (STA)
  - This selects the reference point within of a network, the ROOT switch (RBridge)
  - Other switches determine the best path to RB
    - Based on the price (speed) of the line forming the path
  - If there are two ways, the better is ACTIVE, worse BLOCKED
  - STP forms so-called "a tree"

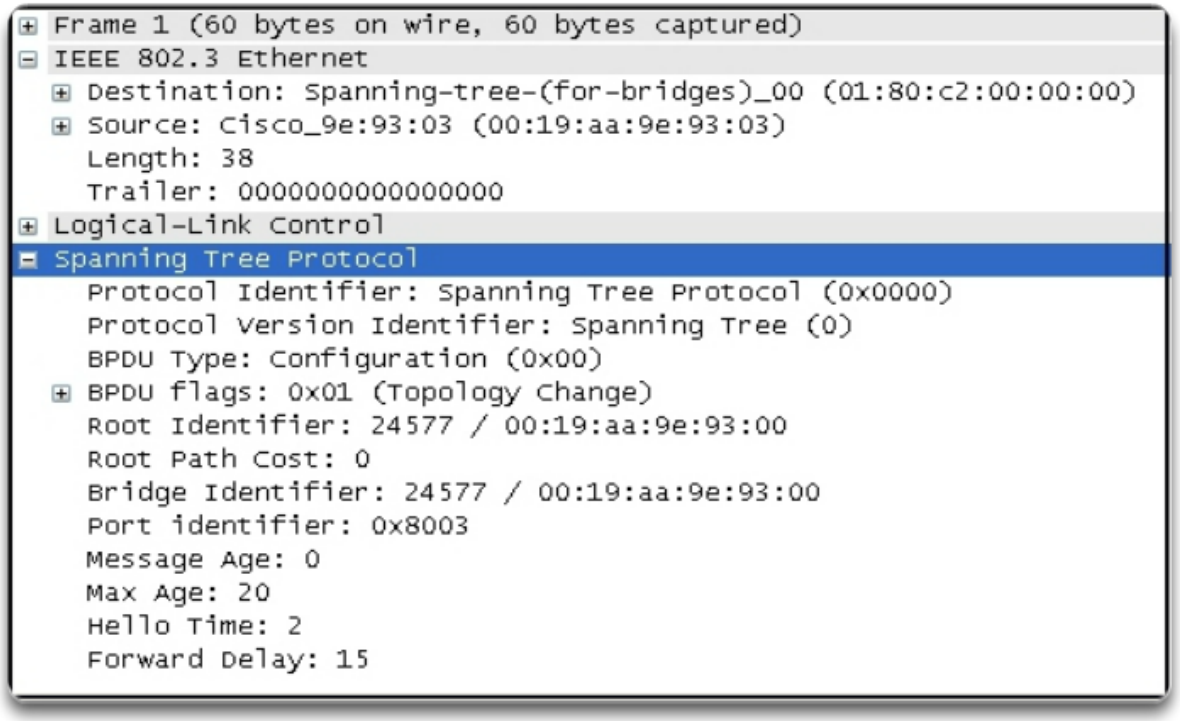
STP check

STP …

- Switches communicate using STP frames (BPDU - Bridged Protocol Data Unit) to:
  - Step 1: Select Root Bridge (RB)
    - The point of the tree is only one
  - Step 2: Selects ROOT ports
    - Ports on non-RB switch closest to Root
  - Step 3: Specifies Designated ports and non-Designated for each segment
- The result is a LOOP FREE topology
  - It can be actively reviewed and respond to network changes
  - One topology for the entire switched network, or for all VLANs in it
- Each switch remembers the last best BPDU (superior)

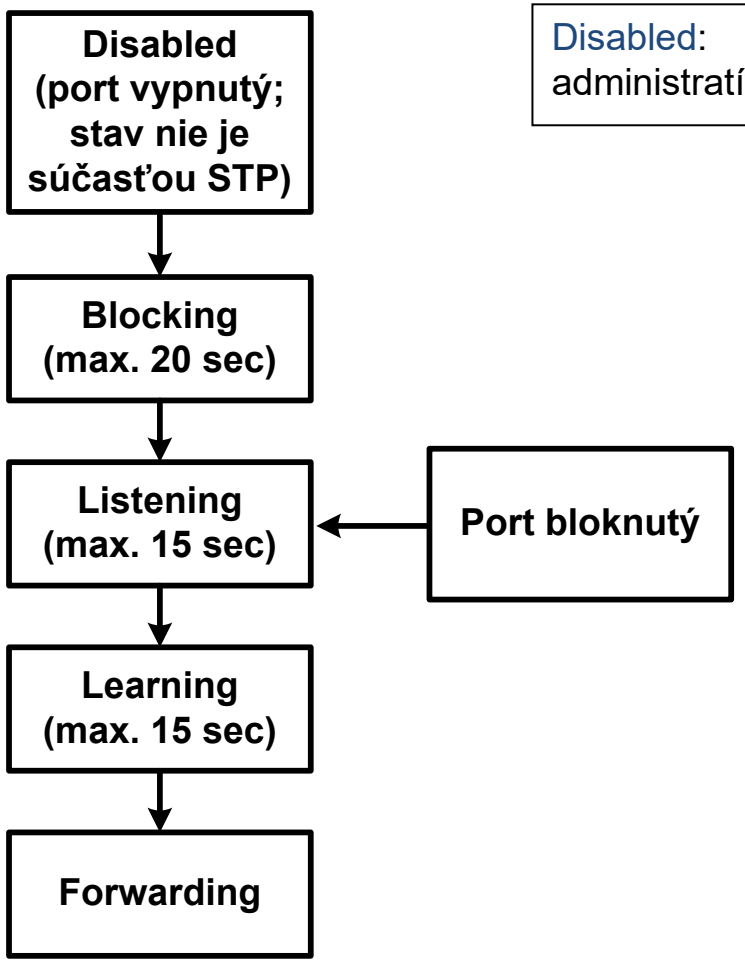
802.1D BPDU Frame Format

- Two BPDU types
  - Configuration BPDU
  - Topology Change Notification (TCN) BPDU
  - Sent by RB each 2 sec to 01:80:C2:00:00:00 STP MAC address



Bytes	Field
2	Protocol ID
1	Version
1	Message type
1	Flags
8	Root ID
4	Cost of path
8	Bridge ID
2	Port ID
2	Message age
2	Max age
2	Hello time
2	Forward delay

Port states



Disabled: administratívne down

Blocking: Prijíma BPDU, neprijíma dátové rámce. Neposiela BPDU.

Ostáva v ňom Max Age timer (20sec.). Zistenie Root BID a úloh portov.

Listening: Prijíma, spracováva a preposiela BPDU (info. že port je pripravený pracovať v aktivnej topo), neprijíma dátové rámce, neučí sa MAC adresy

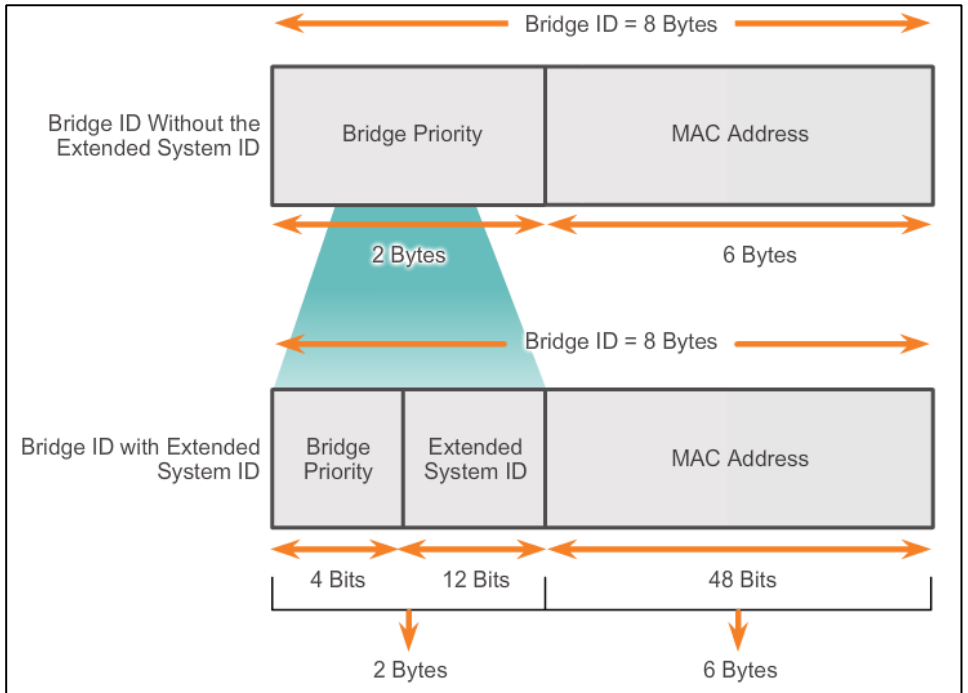
Learning: Spracováva BPDU, neposiela dátové rámce, učí sa však MAC adresy (buduje Bridging table)

Forwarding: Spracováva BPDU, posiela, prijíma dátové rámce, učí sa MAC adresy

Pozn. Def. stav po oživnutí portu je listening

STP Bridge ID and Port Cost

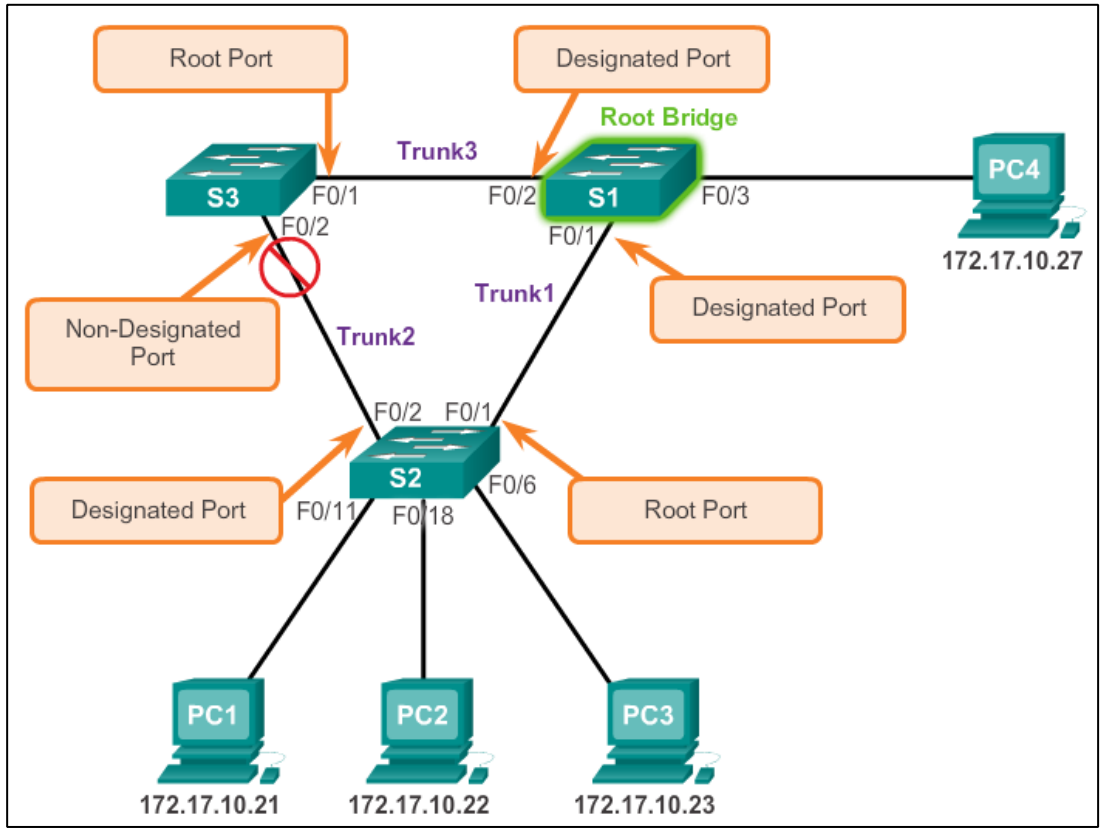
- Each switch/bridge
  - Identified by Bridge ID (8B)
    - 2B Priority
      - Configurable, def. 32768
    - 6B MAC address
      - Switch mac address



Link Speed and Name	Cost (Revised IEEE Specification)	Cost (Previous IEEE Specification)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

- Each Port
  - **Port Identifier**
    - Unique locally per switch
  - **Port Cost**
    - Configurable, def. reflects port speed
  - **Port priority**
    - Configurable, def. 128

STP Port Roles



Rola	Popis
Root Port	Port na non-root prepínačoch. Je to port na najkratšej ceste k Root Bridge. Existuje len jeden Root Port pre prepínač.
Designated Port	Existuje aj na RB aj na non-RB. Je to port, ktorý forwarduje data smerom k RB. Na RB všetky porty sú Designated. Na non-RB len jeden per segment, ak viac prepínačov musí byť voľba.
Non Designated Port	Port v stave BLOCKING, neforwarduje žiadne uživ. dáta.
Disabled Port	Port ktorý je SHUT DOWN.

Rozhodovací proces používaný pri porovnávaní BPDU

- STP stavia svoju činnosť na schopnosti porovnať dvojicu BPDU a vyhlásiť, ktoré je lepšie (superior) a ktoré je horšie (inferior)
- BPDU sa porovnávajú v tomto poradí parametrov:
  - 1 – Root Bridge ID (má dve časti!)
  - 2 – Root Path Cost
  - 3 – Sender Bridge ID (má dve časti!)
  - 4 – Sender Port ID (má dve časti!)
  - 5 – Receiver Port ID (má dve časti; porovnáva sa len výnimočne)
- Parameter N sa porovnáva len vtedy, ak sú všetky predošlé parametre zhodné
- Lepšie je to BPDU, v ktorom sa pri danom poradí porovnávania parametrov nájde prvýkrát nižšia hodnota

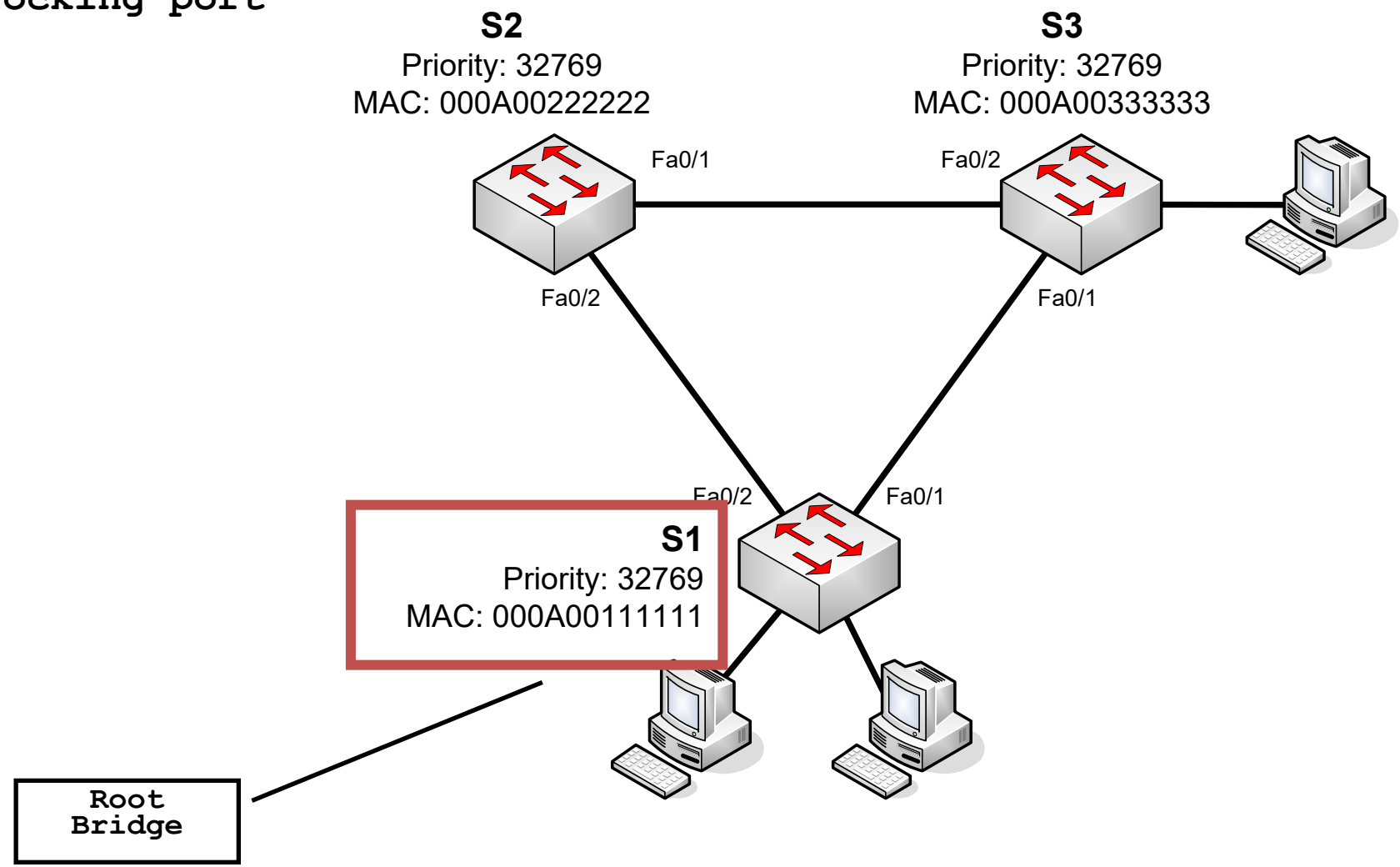
Prvý krok - voľba Root bridge (RB)

- Výber RB ovplyvní dátový tok v prepínanej sieti
- Každý prepínač po zapnutí začne posielať STP rámce (BPDU) so svojim BID
  - Defaultne predpokladá, že RB je on sám
  - Rozposlané všetkým prepínačom
- Ak nejaký iný prepínač:
  - Má nižšie BID ako je uvedené v prijatom BPDU rámci, rámec prepínač zahodí
  - Má vyššie BID, poznačí si lepšie BID a rámec pošle ďalej
- RB sa stane prepínač s najnižšou BID
  - Stane sa Root-om siete (začiatkom STP stromu)
    - Ovplyvňuje dátové toky v LAN
  - Defaultne je nastavená rovnaká priorita, rozhoduje sa na základe MAC adresy
    - Prioritu môže zmeniť admin a ovplyvniť tak voľbu RB

STP – prvý krok - voľba Root bridge (RB)

Forwarding port

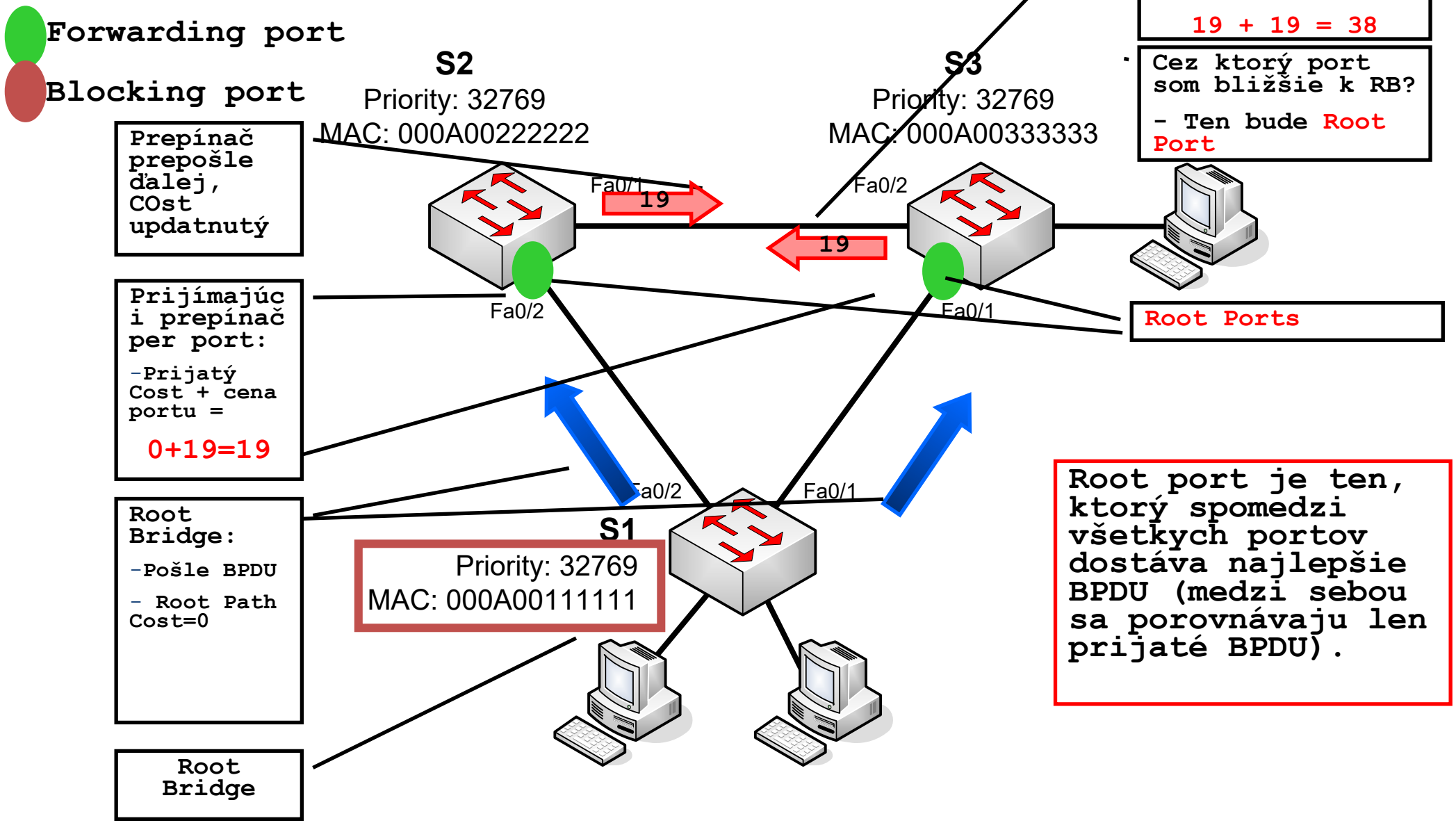
Blocking port



STP činnosť – ďalej ...

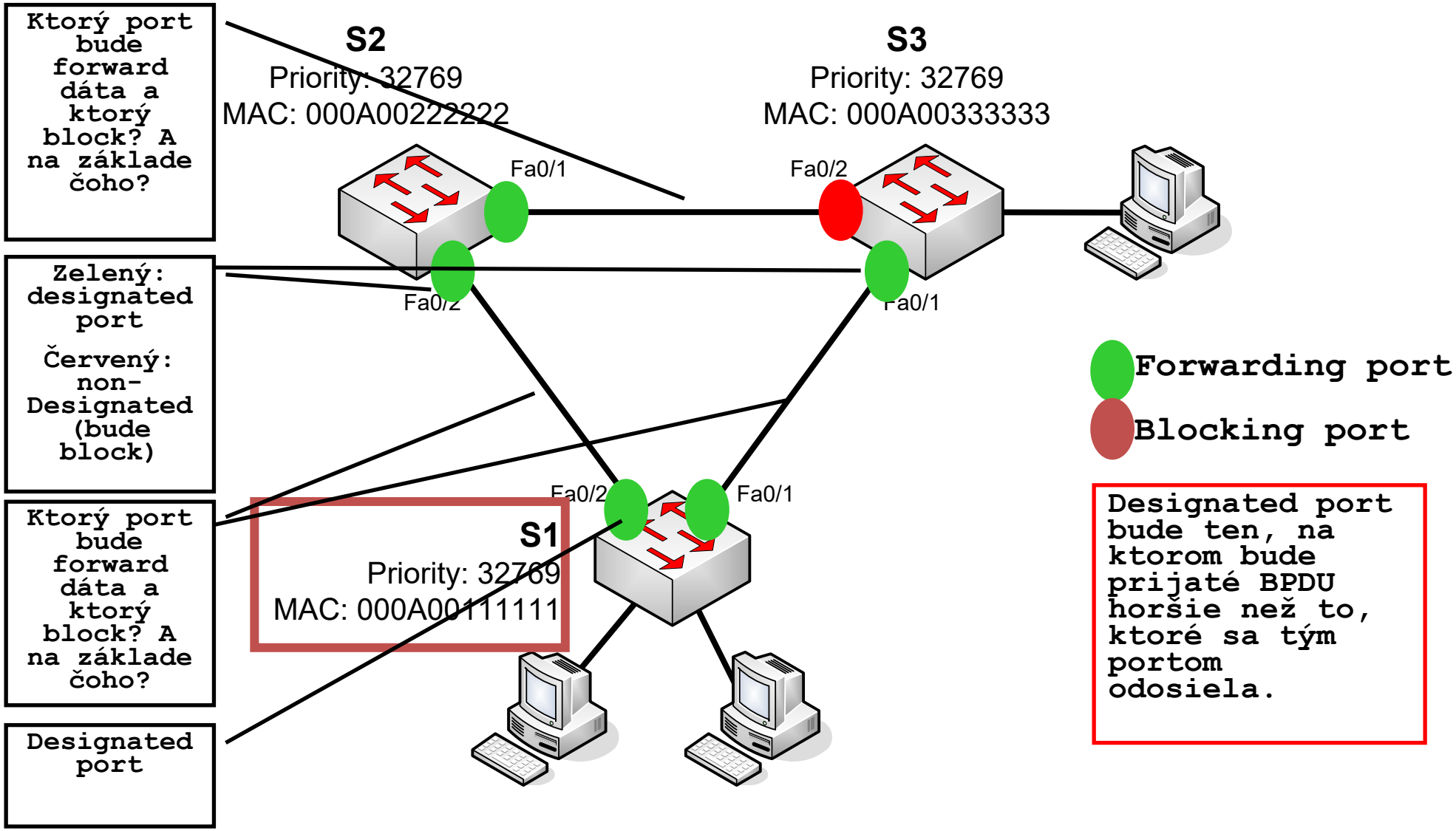
- **Root bridge** (RB)
  - Po voľbe je v sieti len jeden RB
  - Je počiatkom počítaného STP stromu
    - Od RB do každého segmentu siete je len jedna cesta
    - Všetky redundantné cesty, ktoré nebudú súčasťou STP stromu sú blokované
  - Všetky porty RB sú zvyčajne designated portami
    - Špeciálny prípad je slučka sám na seba
      - Tam sú niektoré blokované
  - Začne vysielať BPDU s cost = 0
- **Ďalšie kroky**
  - Určenie najkratšej cesty k RB (Root Path Cost), „root“ portov, určenie „designated“ prepínačov a „designated portov“

STP činnosť – voľba Root Portov



STP činnosť – voľba Designated portov

1 – Root Bridge ID (má dve časti!)
2 – Root Path Cost
3 – Sender Bridge ID (má dve časti!)
4 – Sender Port ID (má dve časti!)
5 – Receiver Port ID (má dve časti)



Show spanning-tree na S1

```
S1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000A.0011.1111
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769
              Address     000A.0011.1111
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

Configuring BID – select the RB

```
! 1) METODA: Nastavenie priority prepinaca per VLAN
Switch(config)#spanning-tree vlan vlan-id priority PRIORITY
! PRIORITY = priradena priorita v ramci STP per vlan s ID
% Allowed values are:
   0 4096 8192 12288 16384 20480 24576 28672
   32768 36864 40960 45056 49152 53248 57344 61440
```

```
! 2) METODA: MAKRO: Nastavenie root bridge
! Ak aktual root ma hodnotu > 24576, nastavi local switch prioritu na 24576
! Ak priorita root je < 24576, nastavi local switch priorotu o 4000 nizsiu

Switch(config)#spanning-tree vlan vlan-id root primary
```

```
! MAKRO: Nastavenie zalohy root bridge
! Nastavi na predefinovanu hodnotu 28,672, nakolko nie je moznost zistit
! Druhu najnizsiu prioritu z BPDU

Switch(config)#spanning-tree vlan vlan-id root secondary
```

Cisco STP implementations

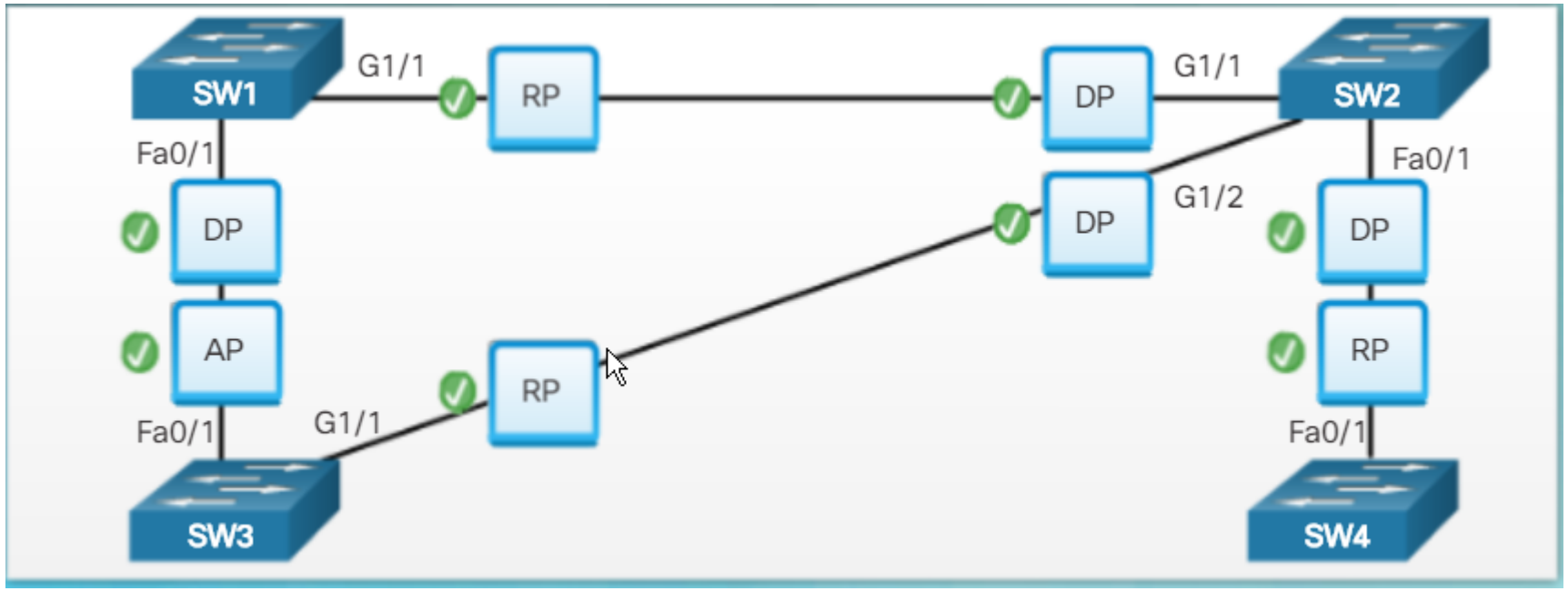
- IEEE standards
  - Spanning Tree Protocol: IEEE802.1D-1998
  - Rapid Spanning Tree: IEEE 802.1w (IEEE 802.1D-2004)
    - Latest, superseds STP
  - Multiple STP (MSTP): IEEE 802.1s
- Cisco terminology and solutions
  - IEEE802.1D = Common STP (CST)
    - One STP tree for all VLAN
  - PVST (Per Vlan Spanning Tree)
    - One STP tree per each VLAN
    - Supports ISL trunking, + Cisco improvements BackboneFast, UplinkFast, PortFast
  - PVST+ (Per Vlan Spanning Tree)
    - One STP tree per each VLAN
    - Compatibility with 802.1D, + Cisco improvements BackboneFast, UplinkFast, PortFast
  - Rapid PVST+
  - MSTP

Protocol	Standard	Resources Needed	Convergence	Tree Calculation
STP	802.1D	Low	Slow	All VLANs
PVST+	Cisco	High	Slow	Per VLAN
RSTP	802.1w	Medium	Fast	All VLANs
Rapid PVST+	Cisco	Very high	Fast	Per VLAN
MSTP	802.1s Cisco	Medium or high	Fast	Per Instance

Check

1 – Root Bridge ID (má dve časti!)
2 – Root Path Cost
3 – Sender Bridge ID (má dve časti!)
4 – Sender Port ID (má dve časti!)
5 – Receiver Port ID (má dve časti)

Back to STP intro

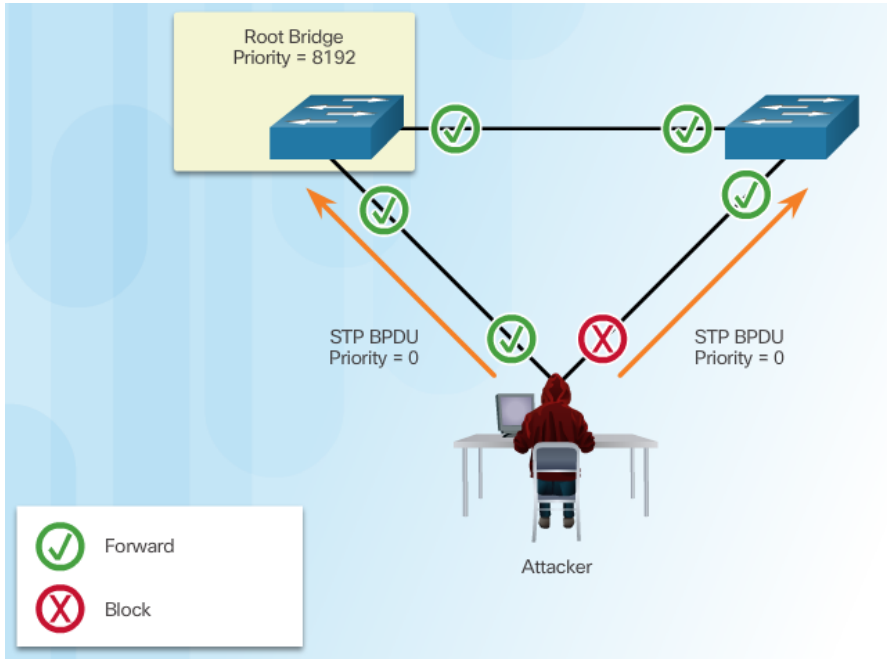


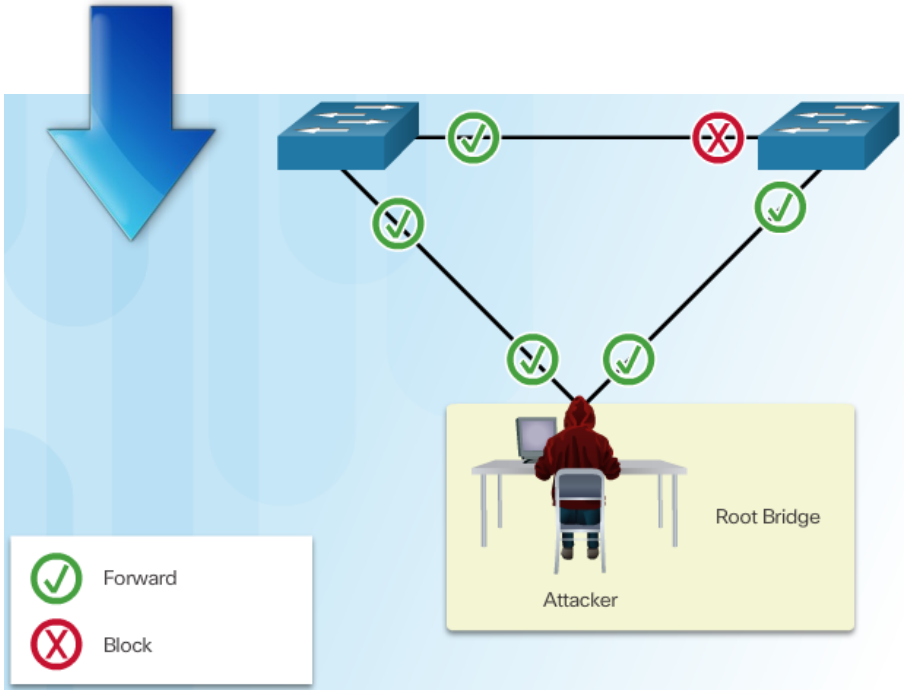
	Priority	Address
SW1	32769	000A00111111
SW2	24577	000A00222222
SW3	32769	000A00333333
SW4	32769	000A00444444

Topic 6.2.9:
Mitigating STP Attacks

STP Manipulation Attacks

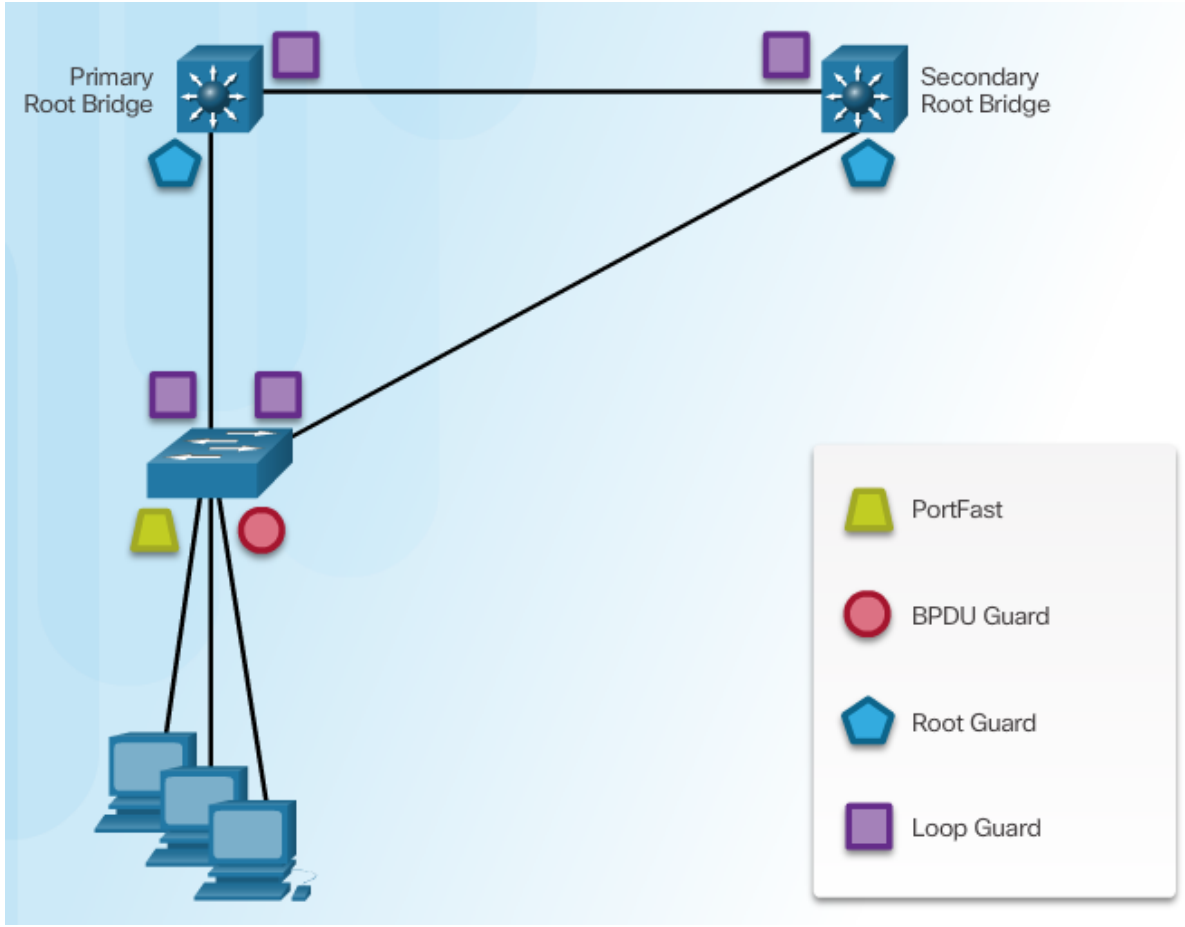
- Attacker may manipulate STP
  - Changing the topology
  - Flushing CAM
    - flooding
  - Spoofing the Root Bridge
    - MiTM, DoS, LAN performance reduction (low power switch)
  - Tool: *yersinia*





Mitigating STP Attacks

- Several mechanisms
  - **PortFast**
    - Brings interface immediately up from blocking state
      - Receiving BPDU force port to go through all states
    - Recommended to use on host ports
  - **BPDU Guard**
    - Protection against receiving any BPDU frames
  - **Root Guard**
    - prevents an inappropriate switch from becoming the root bridge
      - i.e. protect the placement of present RB
    - Port placed in root-inconsistent state
  - **Loop Guard**
    - Protects against unidirectional link failure
  - **BPDU Filter**
    - Prevents to send BPDU messages out of specific port



Mitigating STP Attacks

BPDU Guard

- Protection against security violation
  - Receiving any BPDU frames put ports immediately to the error disabled state
  - Port have to be manually activated by def.
  - Alternatively timer for auto activation may be specified
- Useful
  - Protection of access PortFast ports
  - Protection against connecting rogue switch/AP
  - Any STP manipulation

Root Guard

- Prevents an inappropriate switch from becoming the root bridge
  - i.e. protect the placement of present RB
- Port receiving superior BPDU place the RG to root-inconsistent blocking state
  - The state is automatically removed within 20sec. after port stops receiving superior BPDU

Mitigating STP Attacks

Loop Guard

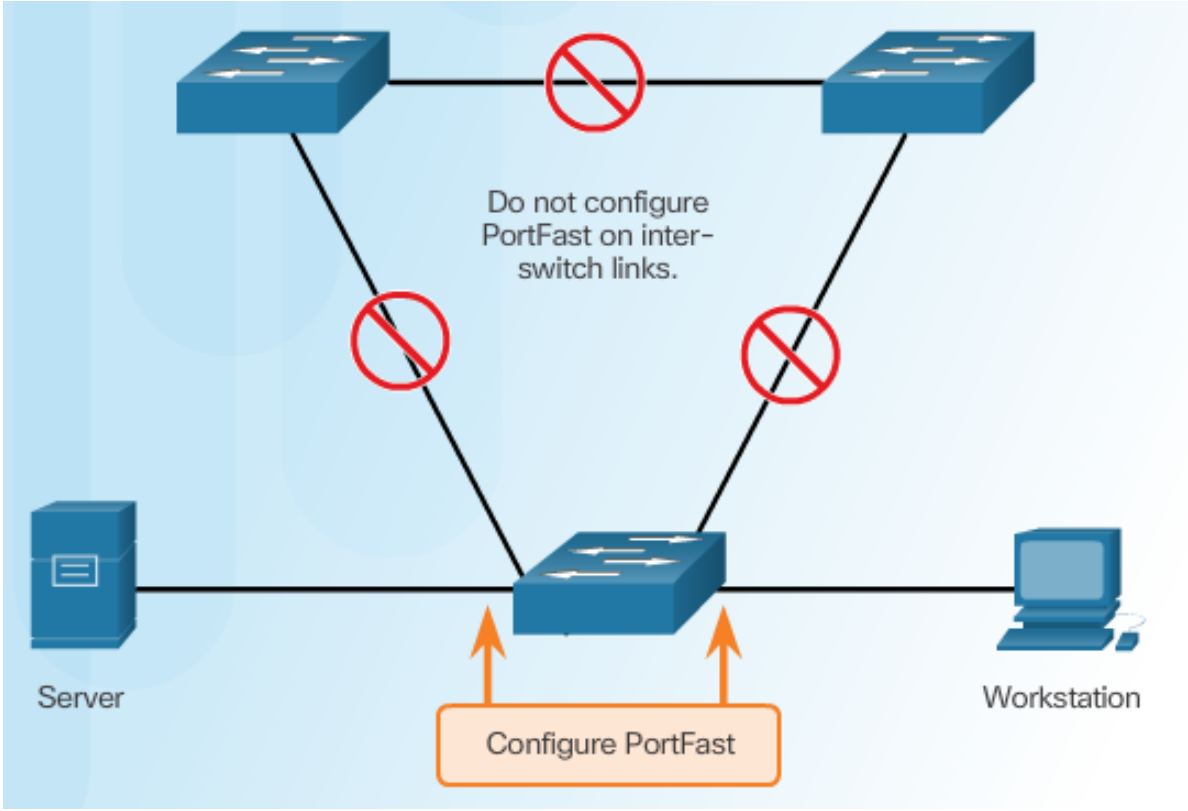
- L2 loop protection mechanism
  - Protects Alternate and Backup ports from immediately becoming Designated ports
  - If blocked non-designated port stops receiving BPDU, port is placed in *loop-inconsistent blocking state*

BPDU Filter

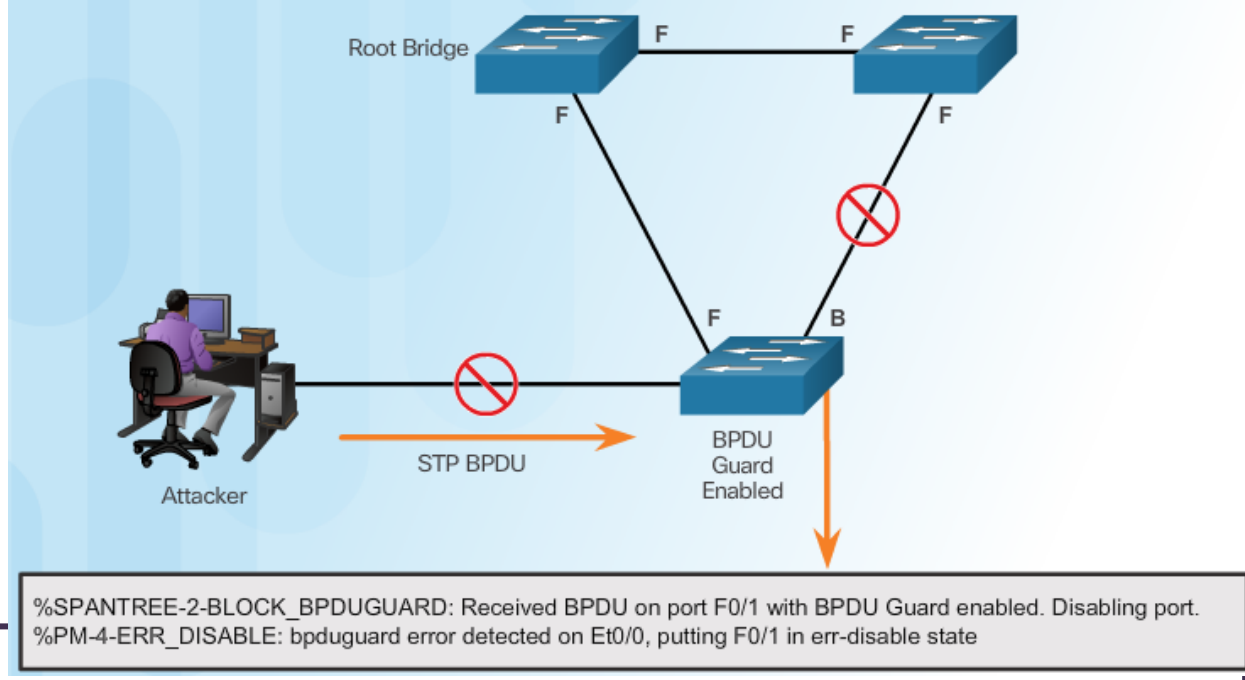
- Prevents to send BPDU messages out of specific port
- Configuration
  - Globally
  - Per port

Configuring PortFast

```
! Spustí PortFast automaticky na všetkých
! access portoch
Pravy(config)# spanning-tree portfast default

! Konfigurácia Cisco PortFast na portoch fa 0/1 - 10
! príkazmi priamo na access rozhraniach (neplatí pre
! trunky)
Pravy(config)# int range fa 0/1 - 10
Pravy(config-if)# spanning-tree portfast

! Zrušenie Cisco PortFast na portoch fa 0/1 - 10, ak
! Je aktivované na globálnej úrovni
Pravy(config)# int range fa 0/1 - 10
Pravy(config-if)# spanning-tree portfast disable

! Overenie stavu portu z pohľadu PortFast
ALS1# sh spanning-tree interface fa 0/1 portfast
VLAN0100            enabled
```

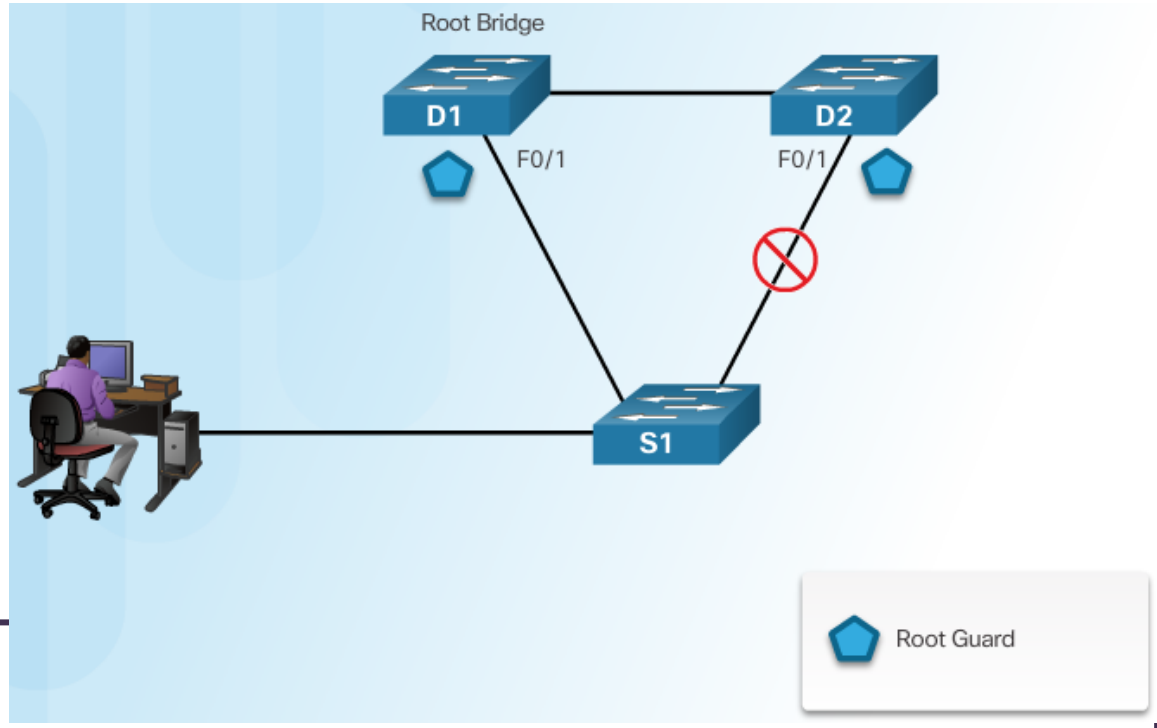


Configuring BDPU Guard



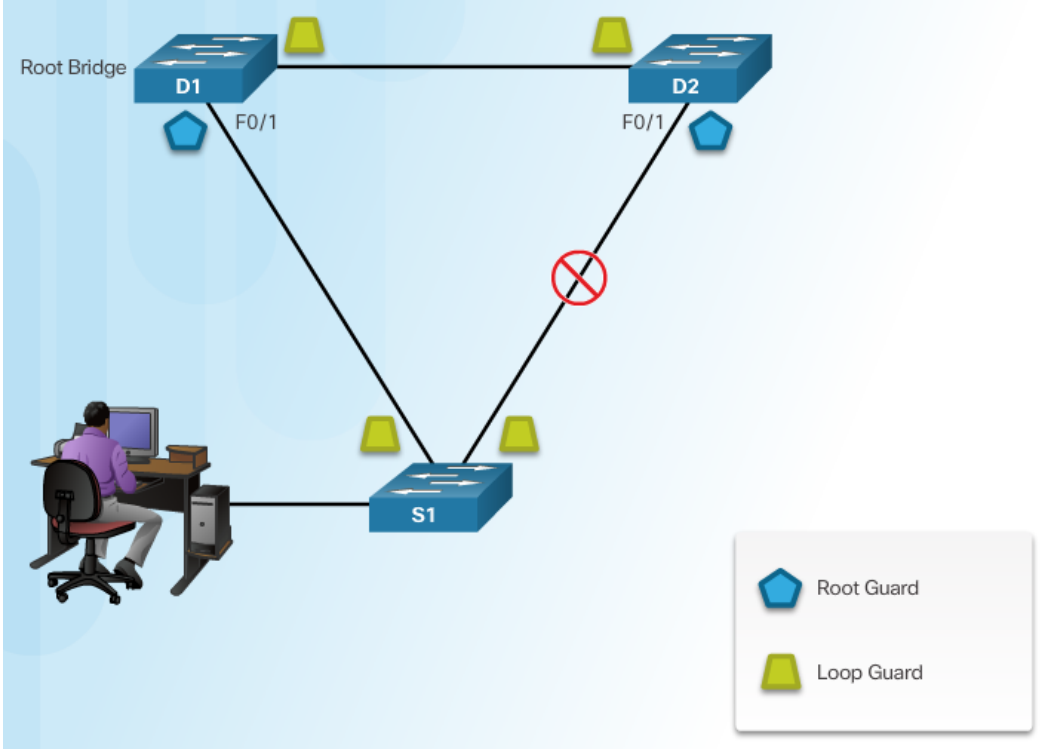

```
! Globálne
Switch(config)# spanning-tree portfast bpduguard default

! Per port
Switch(config)# int fa0/23
Switch(config-if)# spanning-tree bpduguard enable
! Po prijme BPDU
*Mar  1 00:19:00.213: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa0/23 with BPDU Guard enabled.
Disabling port.
*Mar  1 00:19:00.213: %PM-4-ERR_DISABLE: bpduguard error detected on Fa0/23, putting Fa0/23 in err-disable
state
*Mar  1 00:19:01.219: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to
down

Switch# sh int status err-disabled

Port      Name               Status       Reason               Err-disabled Vlans
Fa0/23                       err-disabled bpduguard
```

Configuring Root Guard




```
Switch(config)# int fa0/1
Switch(config-if)# spanning-tree guard root

%SPANTREE-2-ROOTGUARDBLOCK: Port 0/1 tried to become non-designated in VLAN 1. Moved to root-inconsistent
state


! Zobrazi porty v nekonzistentom stave
Switch# show spanning-tree inconsistentports
Name              Interface                Inconsistency
----------------- ------------------------ ------------------
VLAN0001          FastEthernet0/1   Port Type Inconsistent
VLAN0001          FastEthernet0/2   Port Type Inconsistent
VLAN1002          FastEthernet0/3   Port Type Inconsistent
VLAN1002          FastEthernet0/4   Port Type Inconsistent
Number of inconsistent ports (segments) in the system :4
```

Configuring Loop Guard




```
Switch(config)# spanning-tree loopguard default ! Globálne
Switch(config)# int fa0/1
Switch(config-if)# spanning-tree guard loop ! Na porte
```

Verify

```
Router# show spanning-tree summary
Root bridge for:VLAN0001
EtherChannel misconfiguration guard is enabled
Extended system ID   is disabled
Portfast             is enabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is enabled by default
Loopguard            is disabled by default
UplinkFast           is disabled
BackboneFast         is disabled
Pathcost method used is long
```

UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

--