Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Mechanizmy riadenia prístupu

Sieťová bezpečnostná architektúra (Blok II.)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Pavel Segeč

KC KYB UNIZA https://kc.uniza.sk

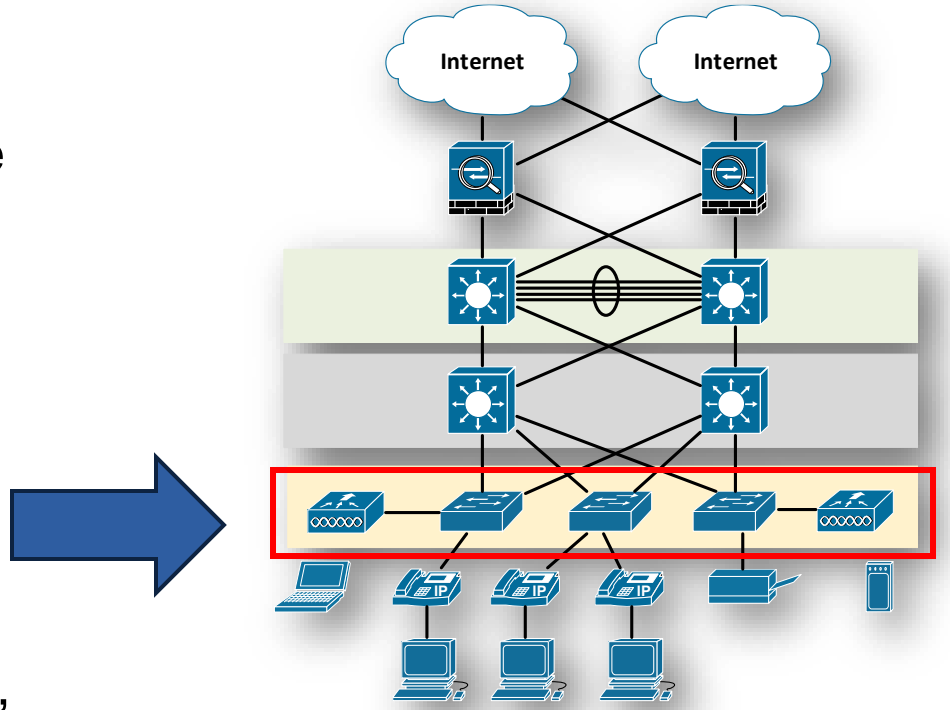
Pavel.Segec@fri.uniza.sk

Čo nás čaká ...

- Riadenie prístupu v sieti
  - Dot1x
  - NAC (Network Access Control) systémy
- Zabezpečenie LAN infraštruktúry
  - First Hop Security

HMS vrstvy a ich bezpečnostná rola - access

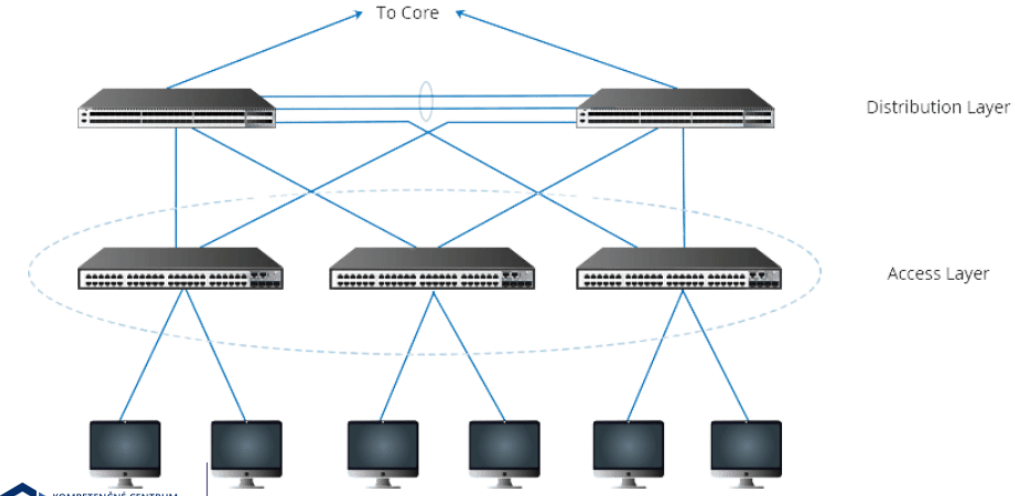
- Hierarchický model = pevný základ bezpečnostnej architektúry
  - Jasné body pre riadenie prístupu, kontrolu a vynucovanie politík
- **Access Layer → detailná granularita**
  - Pripájanie autorizovaných koncových zariadení (PC, IoT, tlačiarne) + WiFi
  - **Bezpečnostný cieľ:** prvá línia obrany → First Hop Security
  - **Princípy**: Zero Trust/Never Trust, Least Privilege, Segmentation, NAC (802.1X), Accountability (telemetria/flow)...
  - **Opatrenia:** VLAN segmentácia, Guest/Quarantine VLAN, Private VLANs, Port Security, DHCP Snooping, ARP Inspection, IP soruce guard, BPDU Guard, MAC ACL...
  - **Hrozby & mitigácie (L2)**
    - MAC flooding → Port security; Rogue DHCP → DHCP Snooping/NAC; ARP spoofing → DAII; IP Spoofing → Source Guard; BYOD/IoT → segmentácia



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Riadenie prístupu k LAN – prečo?

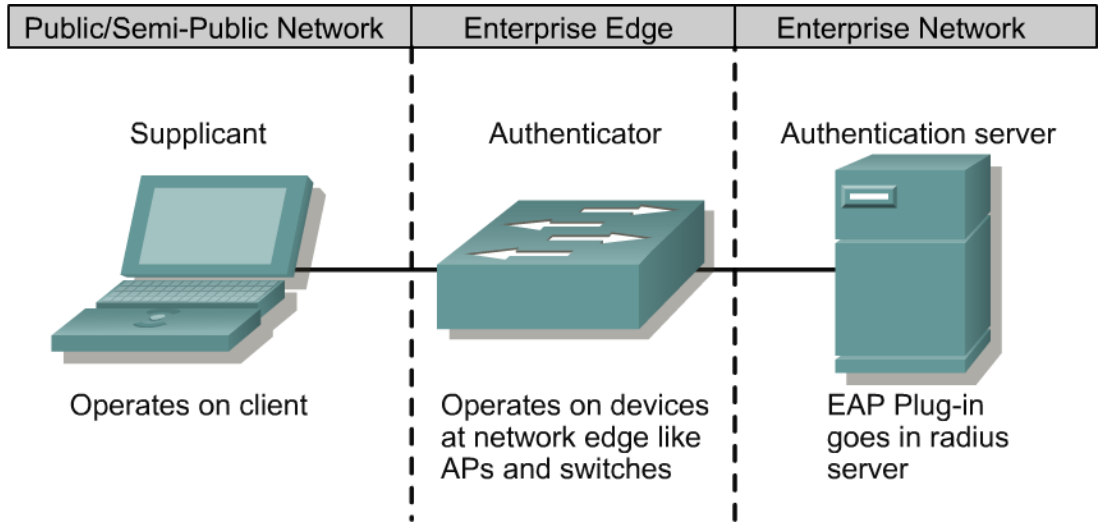
- Access Layer = miesto pripojenia používateľov a zariadení
  - rozhoduje, kto môže vstúpiť do siete
  - kontrolný bod bezpečnosti (policy enforcement point - PEP)
- **Cieľ: zabrániť pripojeniu neautorizovaných alebo kompromitovaných hostov**
  - len dôveryhodné zariadenia majú prístup k podnikovej infraštruktúre
  - vyžaduje sa autentifikácia pred prístupom
- Základný mechanizmus
  - IEEE 802.1X – port-based authentication
    - AAA (RADIUS/TACACS+) – identity verification, authorization, accounting
  - integrácia do Network Access Control (NAC) rámca
    - Rozširuje 802.1X o **politiky, kontrolu stavu zariadenia (posture)** a **centralizované rozhodovanie**
- Prepojenie na modernú bezpečnosť
  - Identity & Posture Validation
  - Dynamické priradenie VLAN / ACL / SGT
  - Zero Trust / Least Privilege
- Nadväzuje na ďalšie časti
  - ➜ 802.1X princíp a komponenty
  - ➜ NAC architektúra a funkcie
  - ➜ First Hop Security – doplnkové L2 ochrany



802.1x (dot1x) – port-based access control

802.1x (dot1x) v skratke

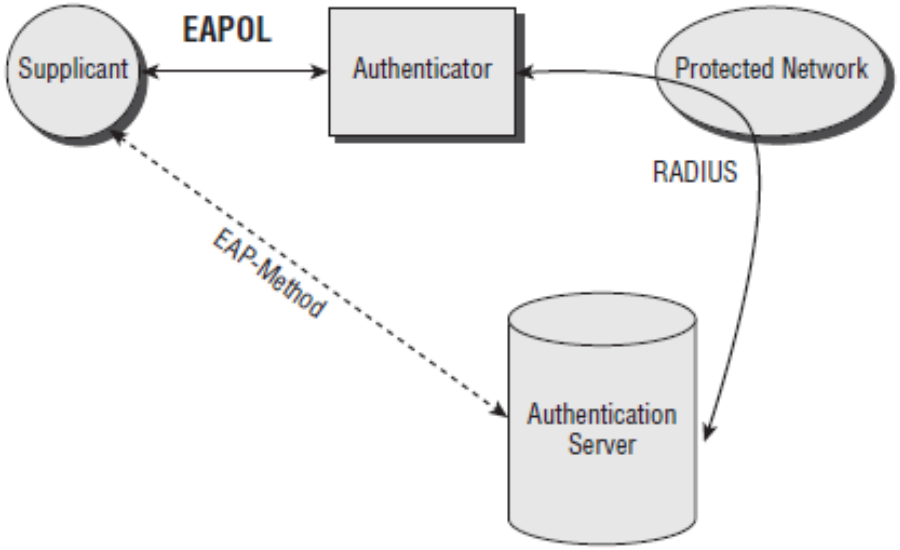
- Robustný štandardizovaný rámec pre „port-based network access control“ na L2
  - LAN port
  - aj WiFi (WPA2/3-Enterprise)
  - Pred prístupom do siete musí koncové zariadenie preukázať identitu
- Účel
  - Zabránenie neautorizovanému prístupu
  - Centrálna politika
  - Podpora rôznych metód (heslo, certifikát, token)
- Základ pre NAC systémy



- Štandardy a špecifikácie, ktoré tvoria kompletný systém portovej autentifikácie 802.1X
  - **Institute of Electrical and Electronics Engineers (IEEE)**
    - 802.1X – Port-based Network Access Control
    - EAPOL (EAP over LAN) protokol
  - **Internet Engineering Task Force (IETF)**
    - EAP (Extensible Authentication Protocol)
    - EAP metódy
    - RADIUS protokol

802.1x - Komponenty

- **Supplicant (klient)**
  - Zariadenie, ktoré sa pokúša získať prístup do siete
  - Softvérový klient v OS (napr. Windows supplicant, wpa_supplicant), ktorý odosiela autentifikačné údaje
- **Authenticator (sprostredkovateľ)**
  - Sieťové zariadenie, ktoré sprostredkuje proces autentifikácie
  - Zariadenie, na ktoré sa klient fyzicky pripája a ktoré od klienta vyžaduje overenie (switch alebo access point)
- **Authentication Server (AAA server)**
  - Obsahuje databázu informácií o používateľoch/identitách
  - Overuje identitu klienta a vracia rozhodnutie (Accept/Reject) + autorizačné atribúty
  - Typicky **RADIUS** server (napr. Cisco ISE, FreeRADIUS, Microsoft NPS)
- EAP + EAPOL
  - Autentifikačné informácie (username, password) sa postupne zapuzdrujú od klienta k autentifikujúcemu zariadeniu v rámci protokolov 802.1X:
  - **EAP methods**
    Špecifické protokoly alebo mechanizmy, ktoré definujú, ako sa autentifikácia vykonáva v rámci rámca EAP
  - **EAP protocol**
    Komunikačný prostriedok
  - **EAPOL** L2 protokol

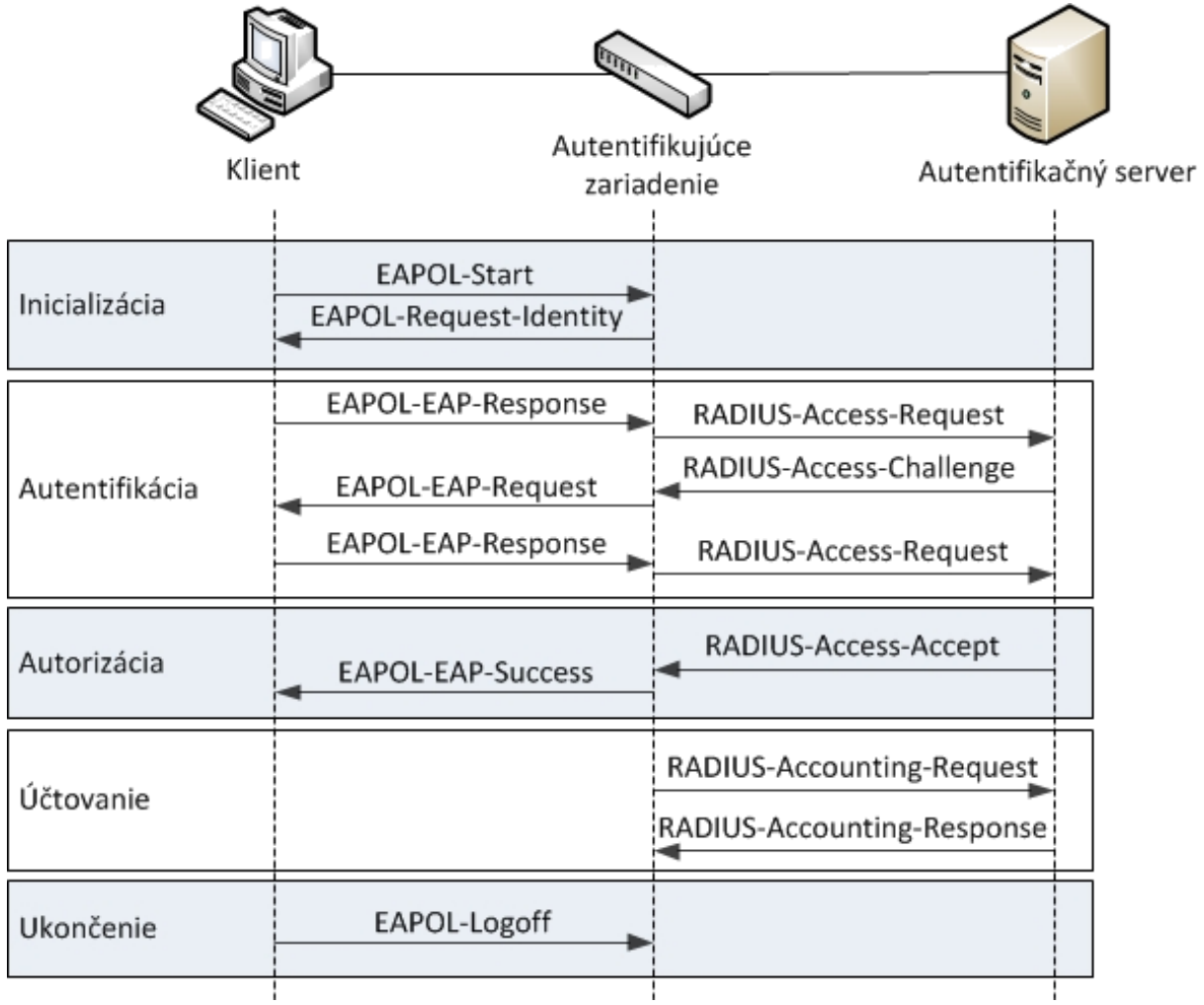


EAPOL (EAP over LAN) – správy

Typ EAPOL správy	Popis
1. EAPOL-Start	**Inicializuje proces autentifikácie.** **Odosielateľ:** Supplicant (klientské zariadenie). **Funkcia:** Signalizuje autentifikátoru, že klient sa chce začať autentifikovať.
2. EAPOL-Logoff	**Ukončuje autentifikačnú reláciu.** **Odosielateľ:** Supplicant. **Funkcia:** Informuje autentifikátor, že klient sa odpája zo siete, čo umožní autentifikátoru vyčistiť údaje o relácii.
3. EAPOL-Key	**Riadi výmenu kľúčov pre šifrovanie.** **Odosielateľ:** Autentifikátor a Supplicant. **Funkcia:** Umožňuje generovanie a distribúciu kryptografických kľúčov používaných na zabezpečenie komunikačného kanála (napr. počas EAPOL handshake).
4. EAPOL-EAP (Encapsulated EAP)	**Prenáša EAP správy.** **Odosielateľ:** Autentifikátor aj Supplicant. **Funkcia:** Zapuzdruje správy EAP-Request a EAP-Response, aby sa mohli vymieňať autentifikačné informácie medzi klientom a autentifikačným serverom prostredníctvom autentifikátora.
5. EAPOL-Success	**Indikuje úspešnú autentifikáciu.** **Odosielateľ:** Autentifikátor. **Funkcia:** Oznámi klientovi, že autentifikácia bola úspešne dokončená a prístup do siete je povolený.
6. EAPOL-Failure	**Indikuje neúspešnú autentifikáciu.** **Odosielateľ:** Autentifikátor. **Funkcia:** Oznámi klientovi, že autentifikácia zlyhala, a prístup do siete je zamietnutý.

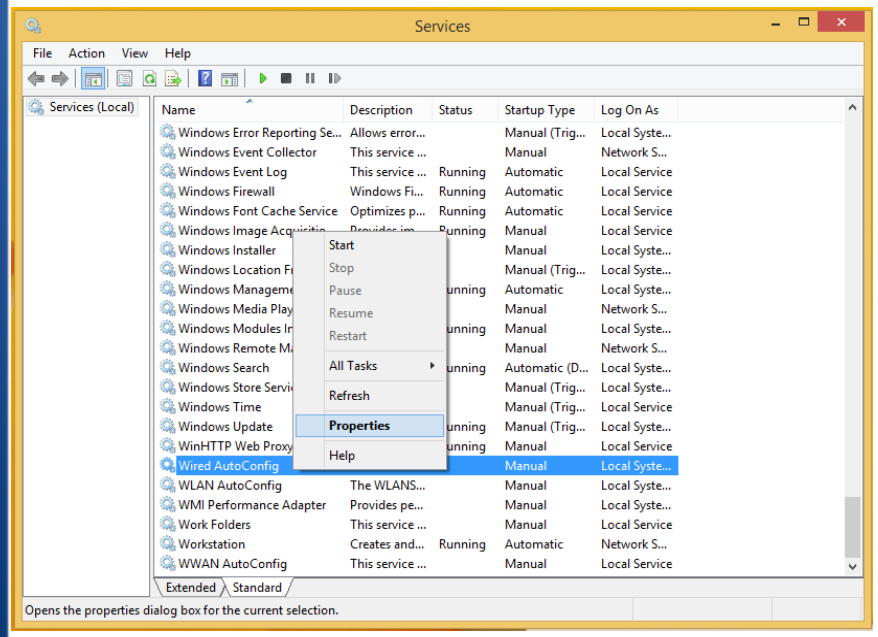
802.1x Port-Based Authentication

- **Klient odošle EAPOL-Start**
  - Alebo najprv **odpovie na EAP-Request/Identity** z authenticatora
- **Switch/AP vyžiada identitu**
  - Kým nie je overený, cez port prejdú len riadené rámce: **EAPOL** (a L2 kontrolné BPDU/CDP/LLDP podľa politiky)
- **Switch zabalí EAP do RADIUS** a pošle **Access-Request** na AAA server
- **RADIUS server** môže overiť hneď **alebo** prebehne výmena **Challenge/Response** (viac krokov podľa EAP metódy)
- Po úspechu server pošle **Access-Accept** (+ autorizačné atribúty: **VLAN/voice-VLAN, dACL/SGT, session-timeout**)
- **Switch otvorí port** (stav *authorized*), priradí politiku a informuje klienta
- Voliteľne sa odošlú **RADIUS Accounting** správy (**Start/Stop**, prípadne **Interim-Update**)
- Ukončenie relácie: **EAPOL-Logoff** (alebo timeout/reauth)

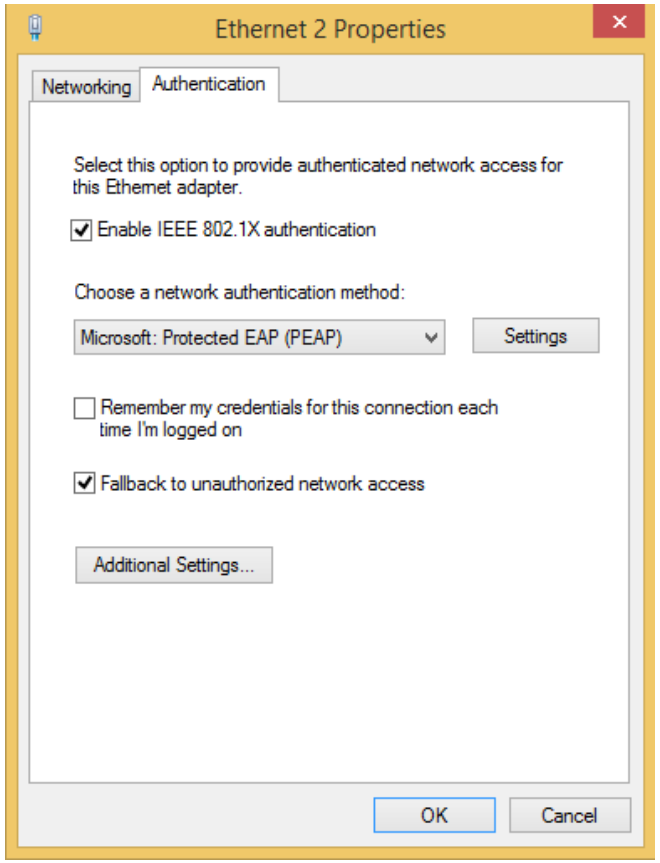


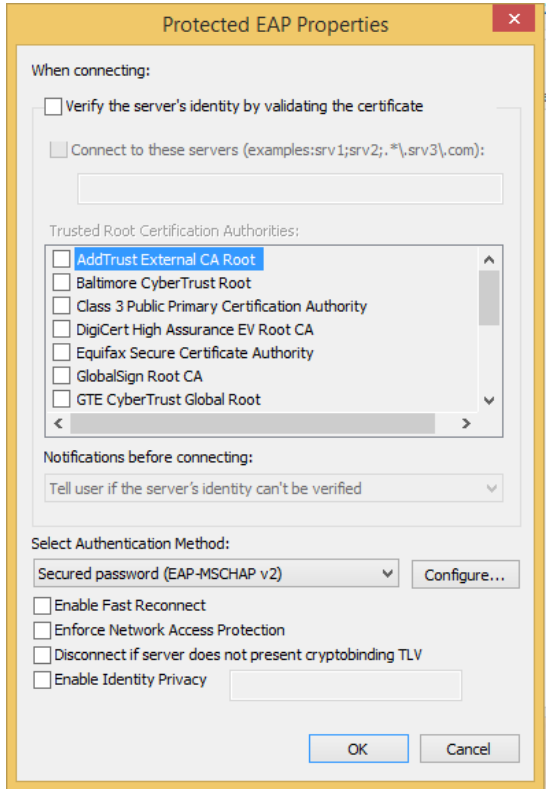
Konfigurácia – klient

- Hľadať „services.msc“
- Zapnúť službu „Wired AutoConfig“

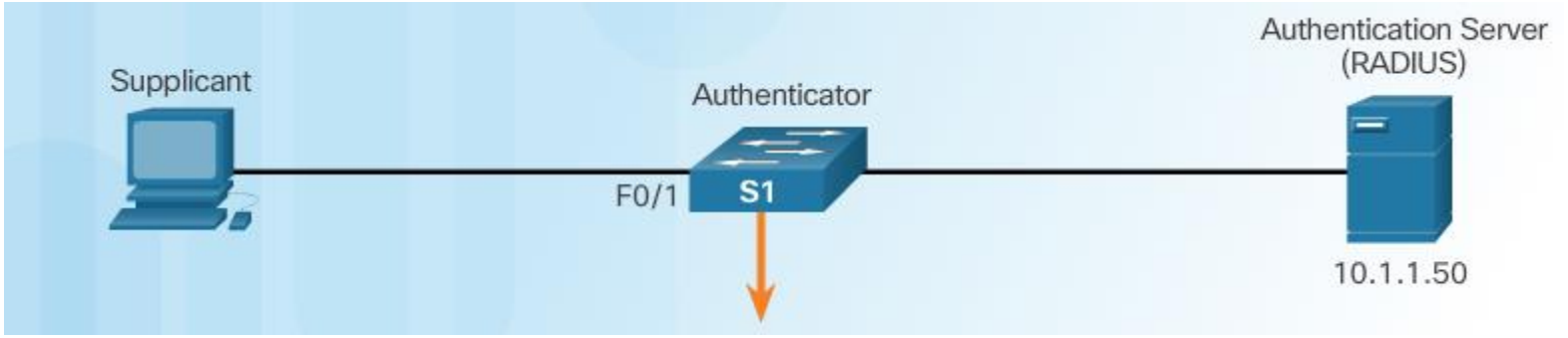


- V nastaveniach pripojenia zapnúť autentifikáciu 802.1X a vybrať EAP metódu





Configuring 802.1X – an example




```
aaa new-model
!
radius-server SERVER-R
   address ipv4 10.1.1.50 auth-port 1812 acct-port 1813
   key HESLO
!
aaa authentication dot1x default group radius
! Nasledujúci riadok netreba, ak nechceme dynamicky prideľovať VLAN
aaa authorization network default group radius
!
dot1x system-auth-control
!
interface FastEthernet 0/1
 switchport mode access
! Zapni dot1x na porte
 authentication port-control auto
 dot1x pae authenticator
```

Minimalistická konfigurácia – freeRADIUS server

```
apt-get install freeradius

/etc/freeradius/clients.conf
            client 192.168.99.253 {
            secret = kluc123
            shortname = klient2
      }
/etc/freeradius/users
            meno        Cleartext-Password := „heslo"
                        Tunnel-Type = VLAN,
                        Tunnel-Medium-Type = IEEE-802,
                        Tunnel-Private-Group-Id = číslo_vlan

; V prípade použitia tunelovanej metódy:
/etc/freeradius/eap.conf
            use_tunneled_reply = yes

/etc/init.d/freeradius restart
```

Network Access Control (NAC) systémy

Systémy riadenia prístupu k sieti - NAC v moderných sieťach

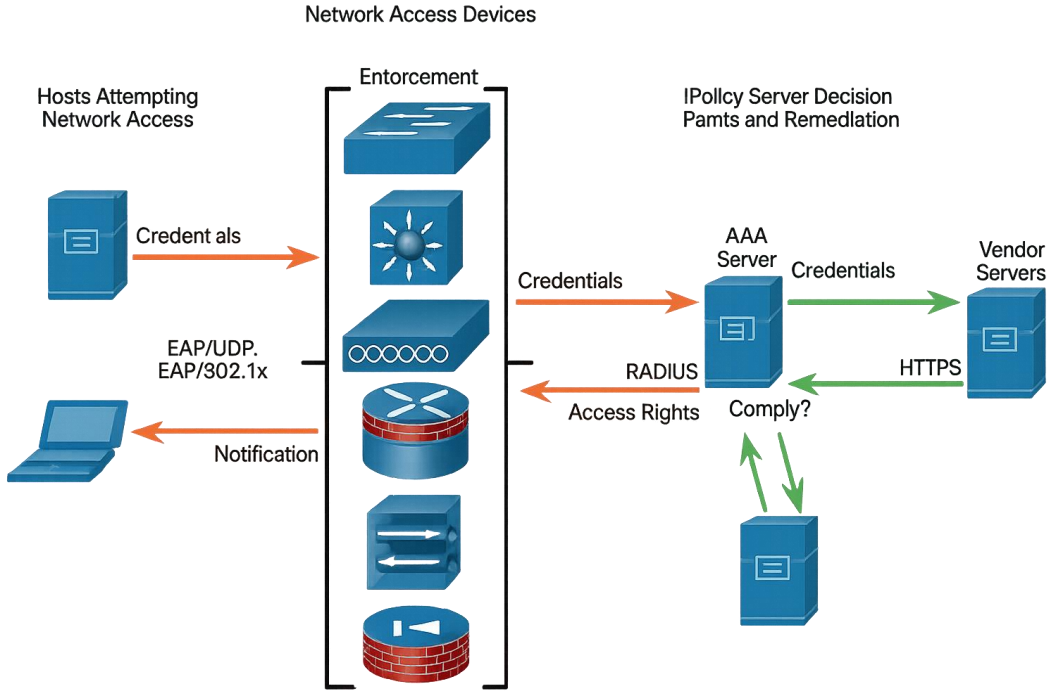
- **Cieľ NAC**
  - Riadiť prístup k podnikových sieťovým zdrojom
  - Zabrániť pripojeniu neautorizovaných alebo infikovaných zariadení
  - Autentifikovať používateľov a zariadenia pred udelením prístupu
  - Overiť zhodu s bezpečnostnou politikou organizácie
  - Vynucovať prístupové práva a aplikovať karanténu, ak nie sú splnené požiadavky

- **Prečo kontrolovať prístup do siete**
  - Nekontrolovaný prístup = bezpečnostné riziko
  - Neznáme alebo nespravované zariadenia a používatelia môžu:
    - Šíriť malware alebo ransomware
    - Exfiltrovať citlivé údaje
    - Obísť vnútorné bezpečnostné mechanizmy
    - BYOD a IoT výrazne zvyšujú riziko expozície
  - NAC zabezpečí, že sa pripoja len dôveryhodné a vyhovujúce zariadenia
  - Podporuje viditeľnosť, segmentáciu a vynucovanie politík
  - Kľúčový prvok Zero Trust architektúry

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Network Admission Control (NAC) - Koncept

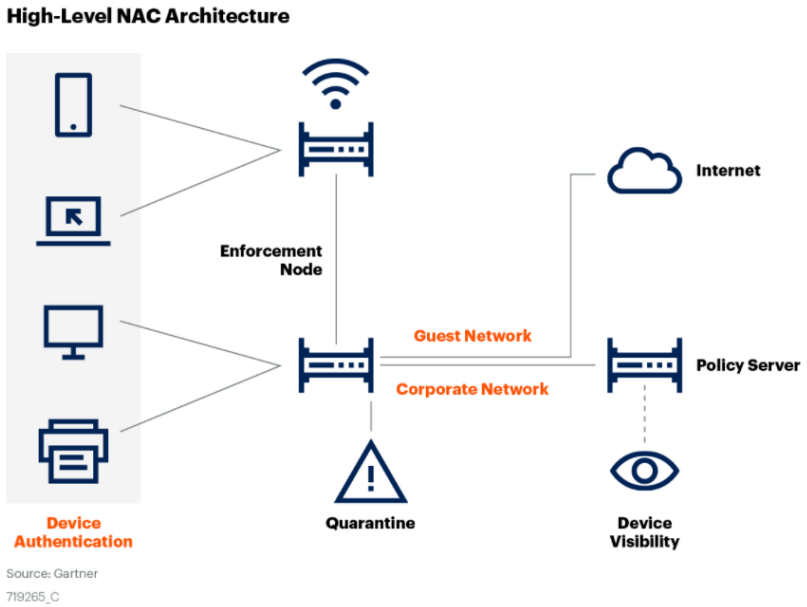
- NAC - hlavná funkcia
  - Zabezpečiť, aby do siete boli pripojené iba autentifikované a s politikou vyhovujúce zariadenia a používatelia
- Overenie bezpečnostného stavu koncových zariadení pred prístupom
  - Úroveň aktualizácií OS, antivírus, firewall, konfigurácia
- Povoliť prístup iba
  - Autorizovaným, s politikou zladeným a vyhovujúcim systémom
- Karanténa pre nevyhovujúce zariadenia
  - napr. chýbajúce bezpečnostné aktualizácie alebo zastaraný antivírus
- Rozhodnutia o prístupe založené na:
  - Prihlasovacích údajoch používateľa
  - Role používateľa v organizácii
  - Stave zhody zariadenia (compliance state)
  - ...
- Dynamické riadenie prístupu k sieti a zdrojom
  - Vynútenie rôznych úrovní prístupu (úplný / obmedzený / zamietnutý)



- Aplikovanie politiky
  - *Allow* → plný prístup
  - *Quarantine* → obmedzený prístup
  - *Deny* → žiadny prístup
- Integrácia s AAA (RADIUS, LDAP, AD)
- Funguje v káblových, bezdrôtových aj VPN sieťach

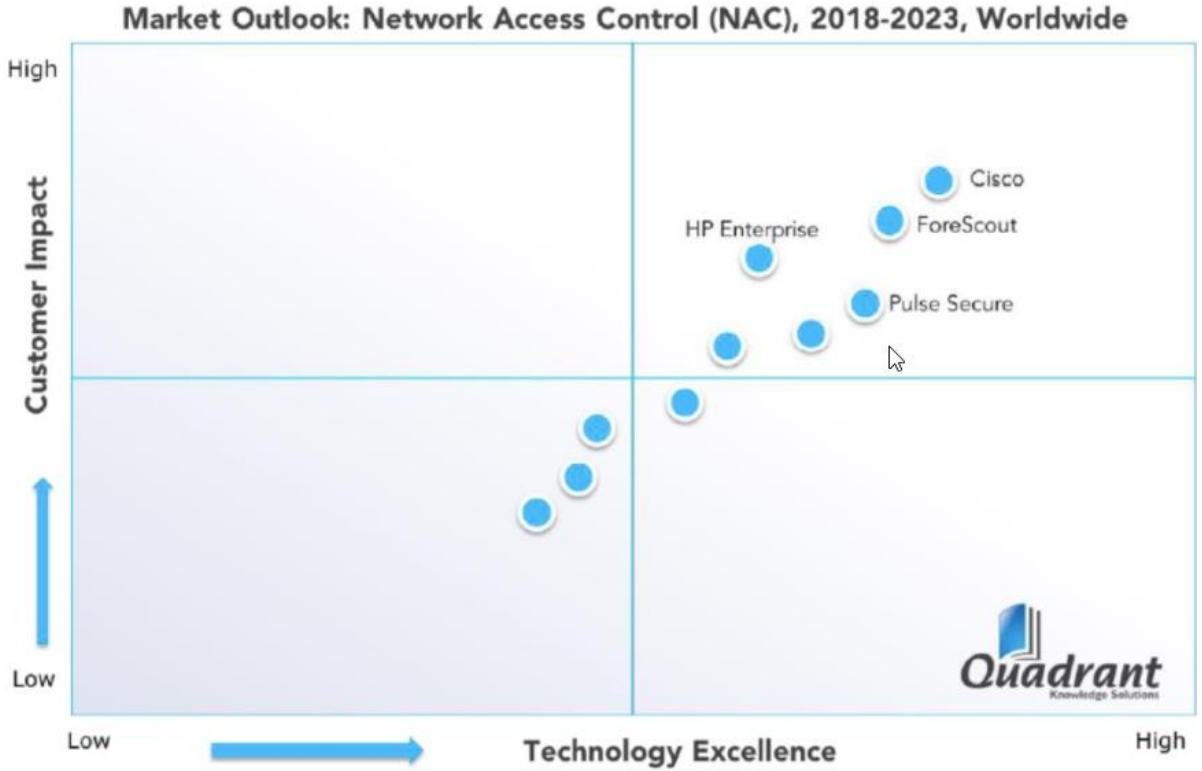
Architektúra NAC – vyšší pohľad

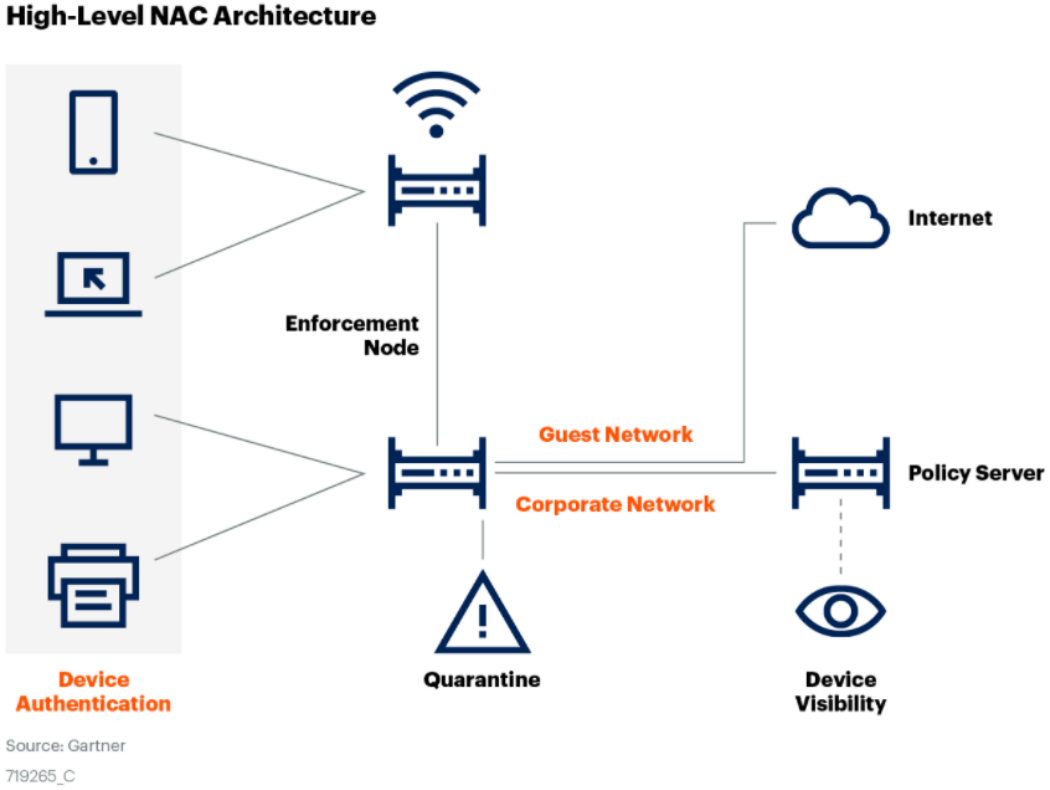
- **Koncové zariadenie (Supplicant)**
  - Zariadenie, ktoré žiada o prístup do siete
  - Poskytuje prihlasovacie údaje používateľa a informácie o stave zariadenia
  - Môže využívať agentový alebo bezagentový mechanizmus kontroly stavu
  - **Autentifikácia zariadenia**
    - Koncové zariadenia (káblové / bezdrôtové / VPN) sa autentifikujú cez 802.1X, MAB alebo webový portál
    - Prihlasovacie údaje overuje **Policy Server** (napr. RADIUS)
- **Policy Server (server politík)**
  - Centrálne rozhodovacie miesto (ISE, ClearPass, Forescout)
  - Hodnotí identitu používateľa, stav zariadenia a súlad s politikou
  - Odosiela autorizačný profil uzlu, ktorý vynucuje rozhodnutie
- **Enforcement Node (vynucovací uzol)**
  - Sieťový prepínač, WLC alebo brána, ktorá aplikuje rozhodnutie NAC
  - Priraďuje prístup do podnikovej, hosťovskej alebo karanténnej siete
  - Vynucuje priradenie VLAN, ACL alebo SGT (TrustSec)



- **Sieť pre nápravu / karanténu (Remediation / Quarantine Network)**
  - Izolovaná oblasť pre nevyhovujúce zariadenia
  - Poskytuje prostriedky na nápravu (aktualizácie, antivírus)
  - Izolovaná VLAN alebo segment určený pre nevyhovujúce zariadenia
- **Viditeľnosť zariadení (Device Visibility)**
  - Neustále profilovanie koncových zariadení (MAC, OS, typ, úroveň rizika)
  - Umožňuje monitorovanie a dynamické prispôsobovanie politík
- **Integrácia**
  - Úzka integrácia s AAA, AD/LDAP, EDR, MDM a SIEM
  - Poskytuje kontextovo riadený prístup

NAC Magic Quadrant

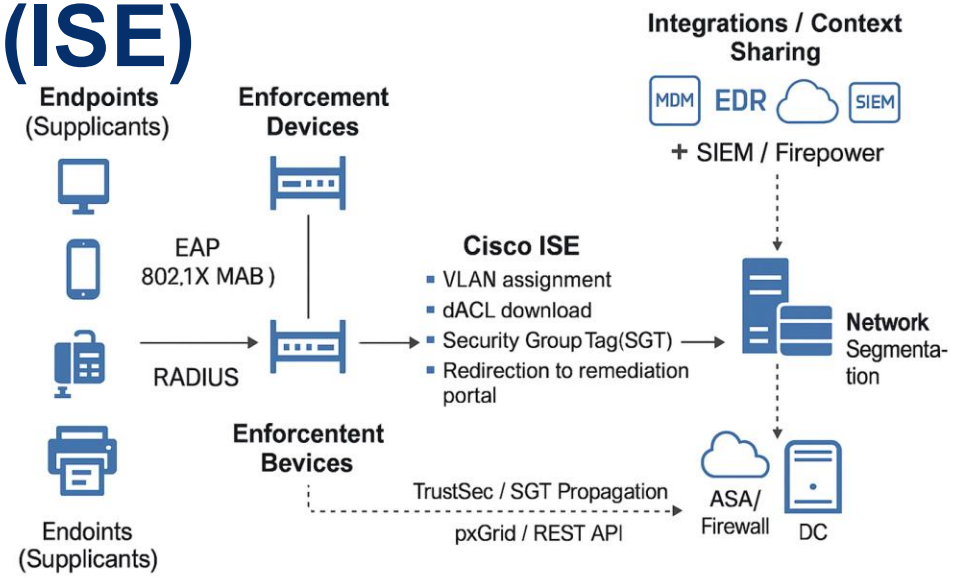




https://www.cisco.com/c/n/us/products/collateral/security/nac-appliance-clean-access/product_data_sheet0900aecd802da1b5.html

Cisco Identity Services Engine (ISE)

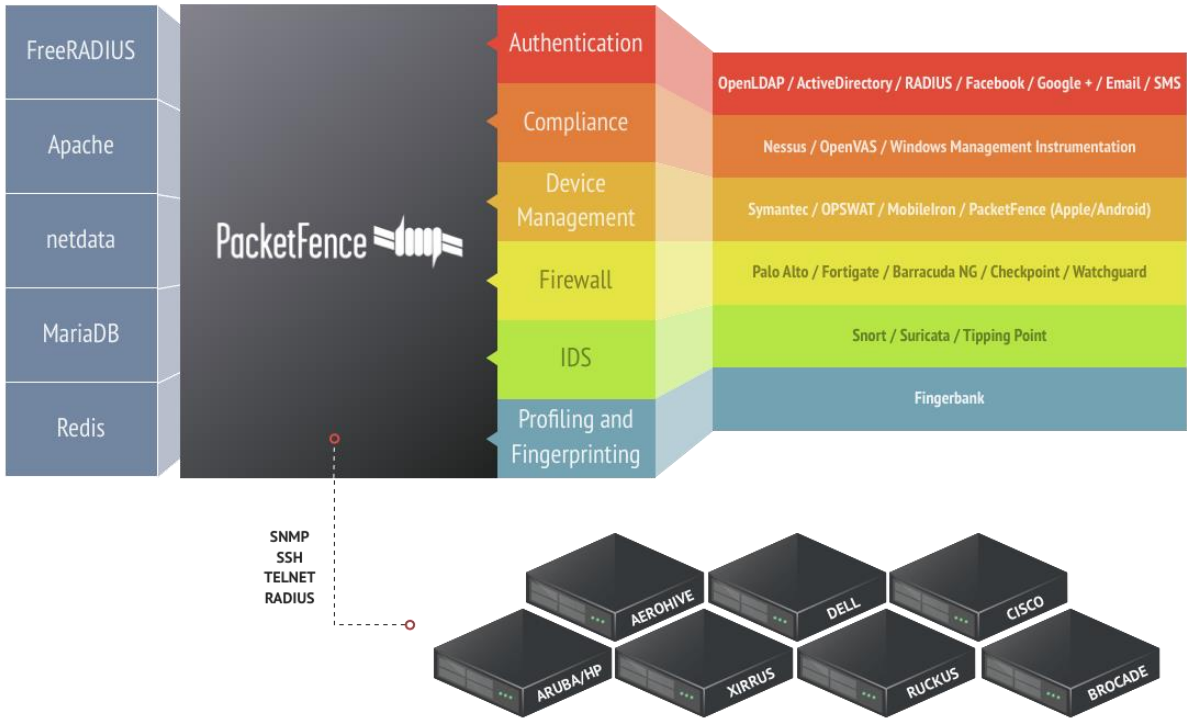
- **ISE – Cisco NAC riešenie**
  - Nástupca pôvodného systému Cisco NAC
  - Účel:
    - Riadiť prístup do siete na základe identity používateľa a zariadenia
    - Vynucovať politiku ešte pred povolením pripojenia
- Centralizovaná NAC platforma
  - Jadro riešenia Cisco TrustSec a Zero Trust
  - Spája autentifikáciu, autorizáciu a kontrolu stavu zariadenia (posture assessment)
- Hlavné funkcie
  - Autentifikácia používateľov a zariadení (802.1X, web)
  - Riadenie prístupu na základe politiky (rola, typ zariadenia, stav)
  - Správa hostí a onboarding BYOD zariadení
  - Overenie stavu zariadenia a profilovanie koncových bodov
- Vynucovanie na základe identity
  - Rozhodnutia o prístupe závisia od:
    - Prihlasovacích údajov a organizačnej roly používateľa
    - Typu zariadenia a jeho súladu s politikou
  - Dynamicky priraďuje VLAN, dACLs alebo SGTs (Security Group Tags)



- Integrácia
  - Spolupracuje so switchmi Catalyst, WLC, ASA/Firepower, VPN bránami
  - Integruje sa s AD/LDAP, MDM, EDR a SIEM systémami
  - Podpora pre Splunk
- Metódy vynucovania
  - Dynamické priraďovanie VLAN
  - Downloadable ACLs (dACLs)
  - SGTs pre segmentáciu založenú na TrustSec
- Režimy nasadenia
  - Samostatný (Standalone) alebo Distribuovaný (Distributed)
  - Roly uzlov:
    - Policy Service Node (PSN) / Administration Node (PAN) / Monitoring Node (MnT)

PacketFence – Open-Source NAC riešenie

- Charakteristika
  - Plnohodnotné a dôveryhodné open-source riešenie Network Access Control (NAC)
  - Určené pre heterogénne siete (malé aj veľké podniky, školy, univerzity)
  - Podporuje káblové, bezdrôtové aj VPN pripojenia
- Hlavné funkcie
  - Captive portal pre registráciu, autentifikáciu a nápravu zariadení
  - Podpora 802.1X, WebAuth a RBAC
  - BYOD onboarding – správa vlastných zariadení používateľov
  - Posture assessment – kontrola antivírusu, patchov, konfigurácie
  - Automatická karanténa infikovaných alebo nevyhovujúcich zariadení
  - Integrácia s IDS/IPS – izolácia kompromitovaných hostov
  - Centralizovaná správa politík a audit
- Integrácie
  - FreeRADIUS – autentifikácia a accounting
  - LDAP / Active Directory / RADIUS / Google / Facebook / Email / SMS
  - OpenVAS / Nessus / Snort / Suricata / Palo Alto / Fortigate / Watchguard
  - MDM / MobileIron / OPSWAT / Checkpoint



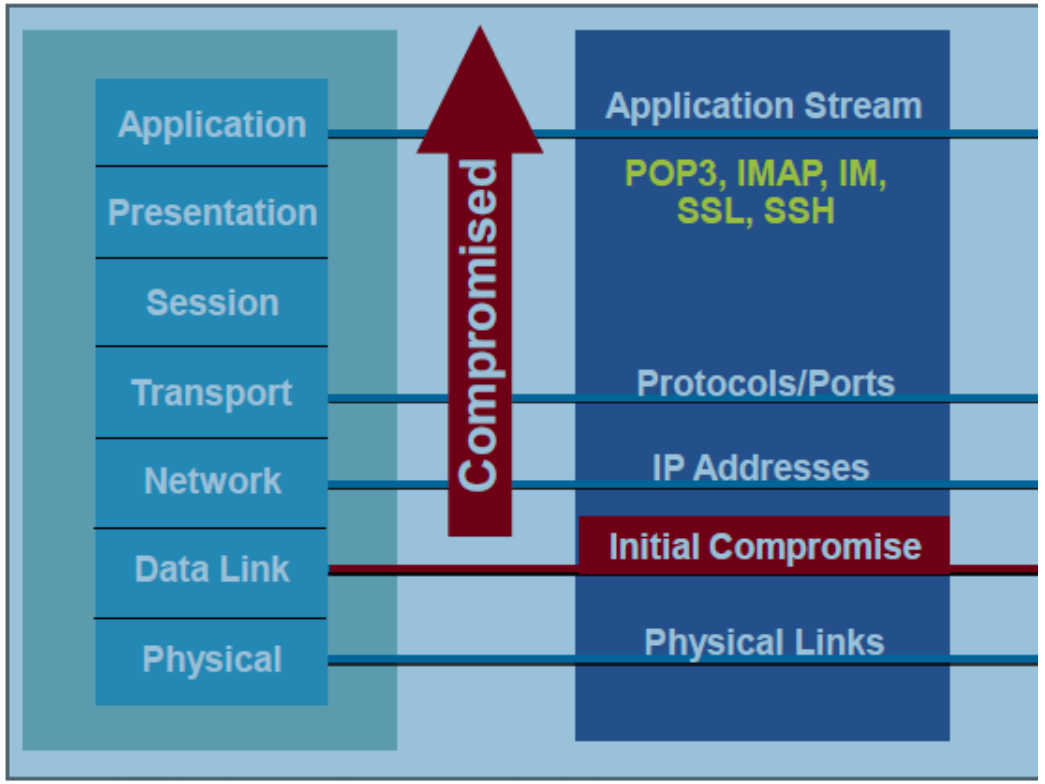
- Kľúčové vlastnosti
  - Bezplatné, otvorené a rozšíriteľné riešenie
  - Plná podpora Layer-2 izolácie pre problémové zariadenia
  - Vhodné pre kampusové, univerzitné a enterprise prostredia

Bezpečnosť na prístupe do LAN (Layer 2 Security / Access hardening / First hop security)

Data plane security

Zabezpečenie LAN infraštruktúry – prečo?

- Bezpečnosť
  - Pri klasickom (legacy) prístupe tlačená na perimeter siete
  - Firewall, edge smerovač
    - Defaultne nastavené na zakázanie komunikácie, ktorú treba povoľovať
- Prepínače
  - Nastavané def. na povolenie komunikácie
  - Veľmi vhodné na útok zvnútra
    - Ak kompromitujem vnútro, zvyšok pôjde rýchlo
- => Implementácia L2 security

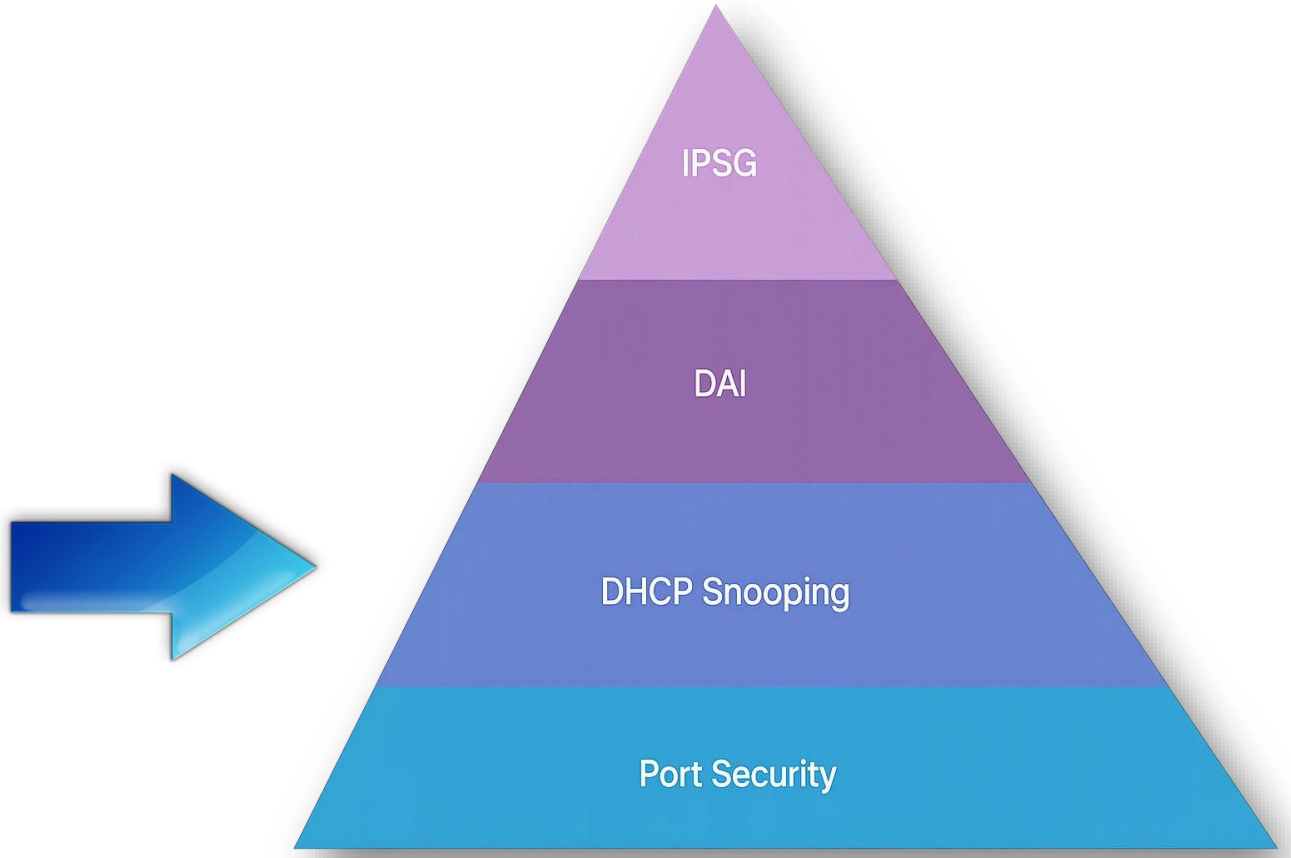


Kategórie L2 útokov v enterprise sieťach

Attack Method	Description	Steps to Mitigation
MAC Layer Attacks – MAC Address Flooding	Útočník zaplaví switch falošnými MAC → CAM tabuľka sa zaplní, switch začne floodovať všetky porty	Port Security, obmedziť počet MAC na port, VLAN access mapy
VLAN Attacks – VLAN Hopping (DTP spoofing, double-tagging)	Manipulácia s VLAN ID umožní prístup do inej VLAN	Zakázať DTP (nonegotiate), natívnu VLAN tagovať, nepoužívať VLAN 1, parking VLAN
Common VLAN Attacks	Zariadenia v jednej VLAN sa môžu navzájom útočiť, najmä v multi-tenant prostredí	Implementovať PVLAN (Private VLANs) alebo ACL medzi portmi
Spoofing Attacks – DHCP Starvation / DHCP Spoofing	Útočník vyčerpá pool DHCP alebo sa vydáva za server	DHCP Snooping, definovanie trusted portov
Spoofing Attacks – MAC Spoofing	Útočník si nastaví MAC iného hosta → obíde ACL alebo získava prevádzku	Port Security (limit MAC), DHCP Snooping
ARP Spoofing / ARP Poisoning	Podvrhnuté ARP odpovede → MITM alebo DoS	Dynamic ARP Inspection (DAI), DHCP Snooping, Port Security
STP Attacks – Root Spoofing	Útočník posiela falošné BPDU, stane sa root switchem	BPDU Guard, Root Guard, Loop Guard, správna STP konfigurácia
CDP/LLDP Manipulation	CDP/LLDP leakujú infra info alebo sa dajú zneužiť na flooding	Vypnúť CDP/LLDP na access portoch, povoliť len tam, kde treba
Telnet/SSH Misuse	Clear-text Telnet odposluch, brute-force na SSH	Zakázať Telnet, používať SSH v2, ACL na management prístup

Útoky na L2 a ich potláčanie

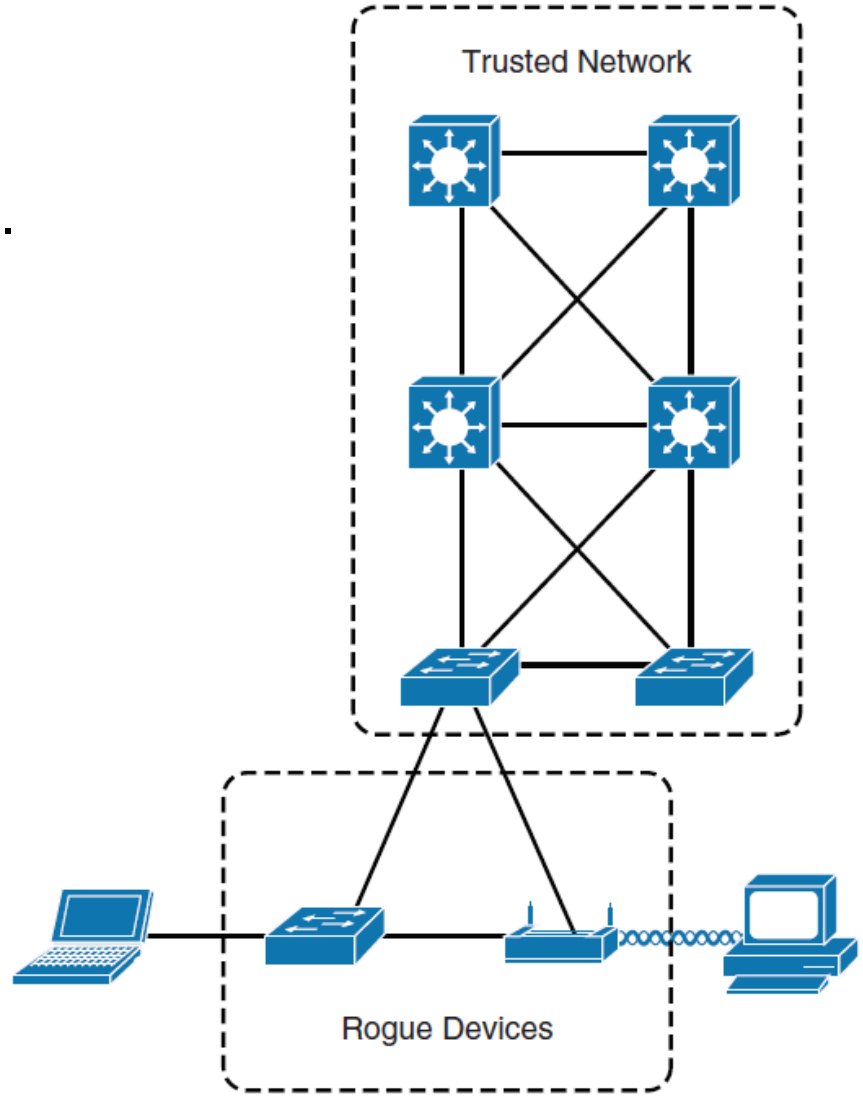
- VLAN attacks
  - Vlan hopping, VLAN double tagging (*yersinia*)
- Switch device attack
  - CDP manipulation, SSH/Telnet pass attack
- STP attacks
  - STP manipulation
- Address spoofing attacks
  - MAC/IP address spoofing
- ARP attacks
  - ARP spoofing, ARP poisoning
- DHCP attacks
  - DHCP starvation,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



Kontrola prístupu do prepínanej siete - Baseline Portov a VLAN

Riadenie prístupu k prepínanej sieti

- Častým (a neželaným) javom je nekontrolované pripájanie zariadení k prepínanej sieti
  - Nové notebooky, PC, prístupové body, routery, PDA, ...
- Úlohou prepínačov v prístupovej vrstve je aj **ochrana prístupu do siete**
- Prepínače (Cisco a iný) ponúkajú niekoľko mechanizmov na riadenie prístupu k prepínanému portu
  - **Procesná**:
    - Nepoužívané porty
      - by mali byt shutdown
      - or v parking VLAN
  - **Riadenie prístupu do siete**
    - Autentifikácia 802.1X
    - Port Security
    - Network Admission Control

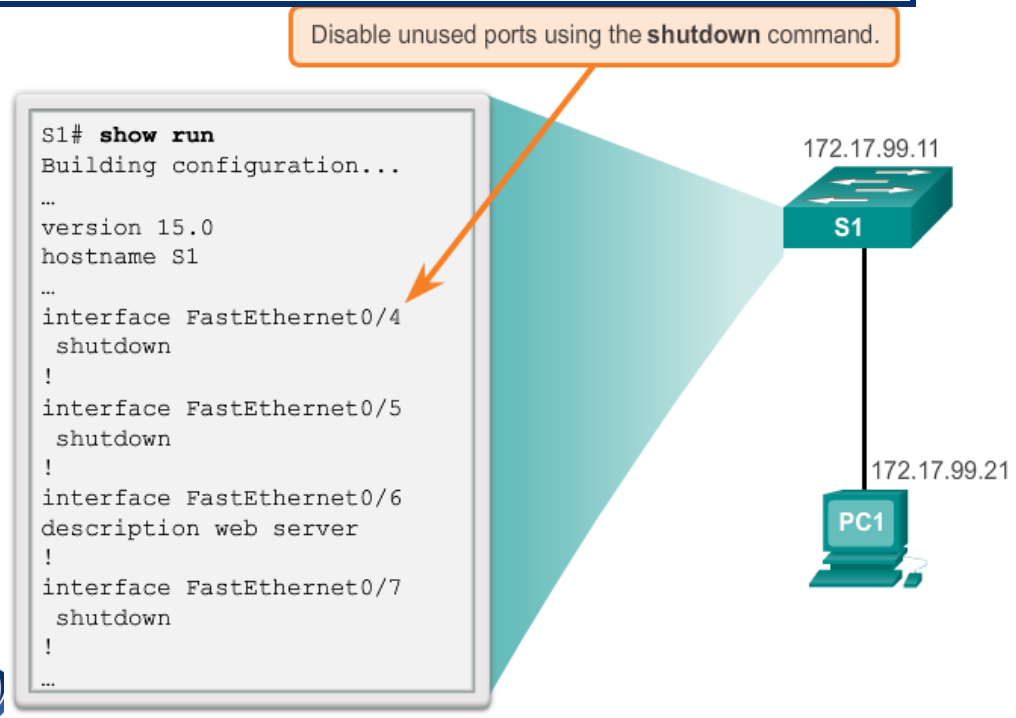


Zabezpečenie nepoužívaných portov

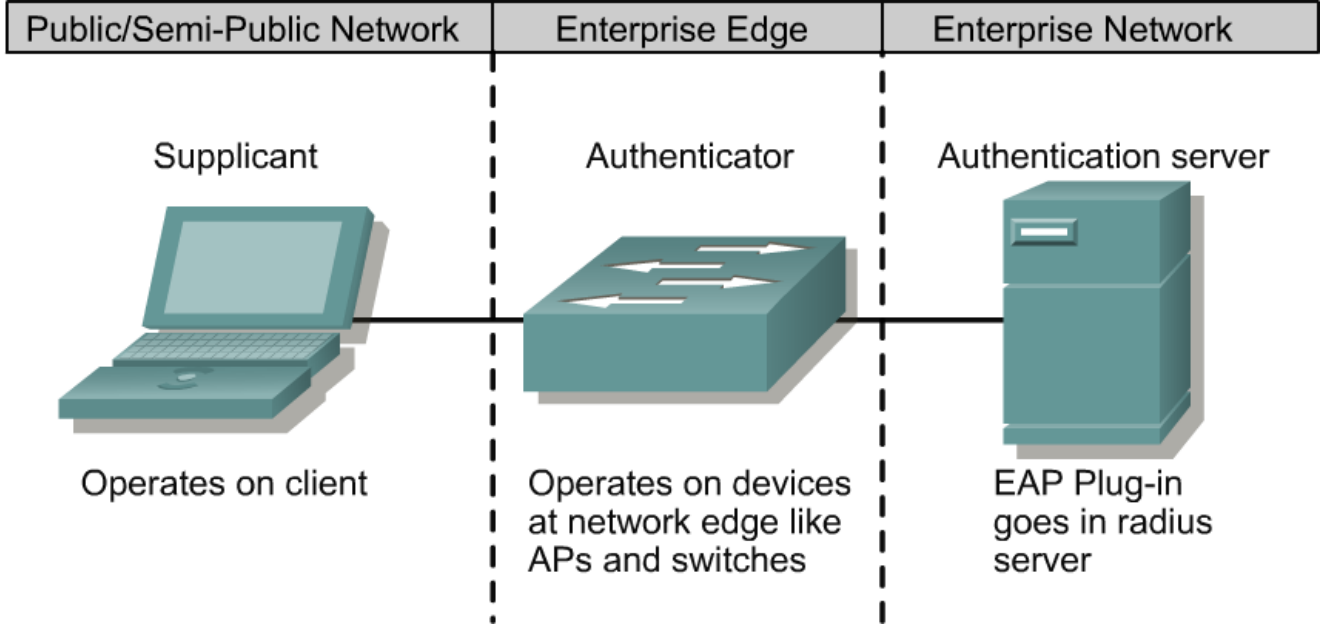
- Nepoužívané porty
  - Vypnúť => jednoduché a efektívne
    - Oplatí sa CMD

```
Switch(config)# interface range type module/first-number - last-number
Switch(config-if-range)# shutdown
```

  - Umiestni port do black hole or suspend/parking vlan



Riadenie prístupu do prepínanej siete – 802.1x

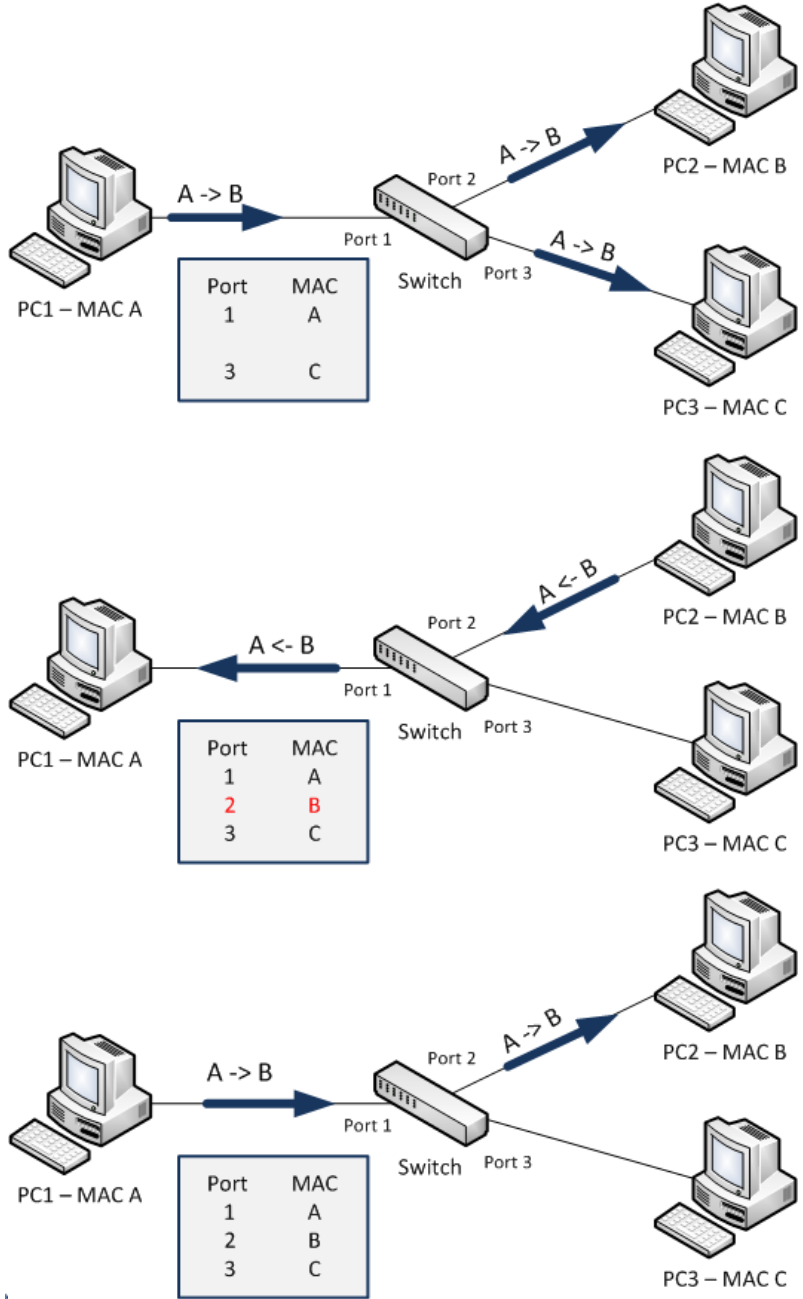


- Definuje port-based mechanizmus riadenia prístupu a autentifikácie
- Ten obmedzuje pripojenie neoprávnených pracovných staníc k sieti LAN
  - Autentifikačný server pred sprístupnením akýchkoľvek služieb autentifikuje každú pracovnú stanicu, ktorá sa pripojila k portu prepínača
  - Port prepínača sa odomkne až po úspešnom prihlásení (predvolený stav je neoprávnený).
    - Medzitým sú povolené iba STP, CDP a EAPOL
  - Ak sa používateľ neoverí
    - Port zostáva neoprávnený alebo sa môže pohybovať v karanténe alebo hosťovskej sieti VLAN alebo znova vykonať autorizáciu

Útoky na CAM/MAC tabuľku a ochrana

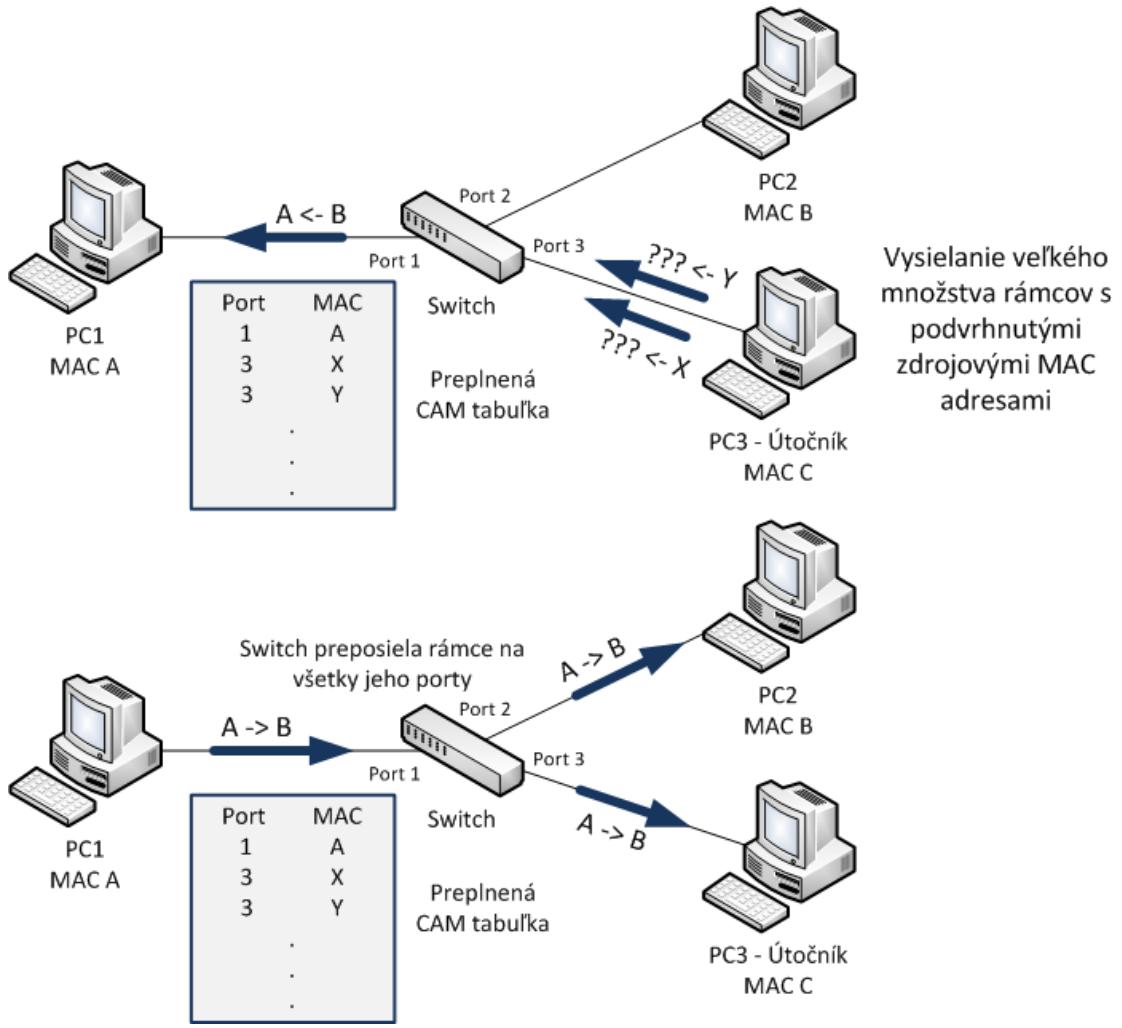
CAM činnosť

- **Budovanie CAM**
  - Proces učenia sa L2 prepínača show mac-address-table – príkaz na zobrazenie MAC tabuľky
- **Hrozba**
  - Veľkosť CAM tabuľky a počet položiek v tabuľke sú obmedzené Závisí od platformy prepínača



Útok na CAM – CAM overflow

- Útočník zasielaním veľkého počtu rámcov s rôznymi falošnými zdrojovými MAC adresami spôsobí zaplnenie CAM
  - Macof, yersinia
- Nové položky nie je kam písať
  - Útok často realizovaný pred začatím práce väčšiny
- Prepínač začne tieto rámce záplavovo šíriť



Realizácia – macof (dsniff package)

- Príkaz: **macof** / macof –i eth0
- Agresívnejší režim
  - spusť na danom rozhraní a výpis pošli do dev/null

macof –i eth0 2>/dev/null

```
└──╼ $apt-cache show  dsniff
Package: dsniff
Version: 2.4b1+debian-30
Installed-Size: 430
Maintainer: Debian Security Tools <team+pkg-
security@tracker.debian.org>
Architecture: amd64
Depends: libc6 (>= 2.15), libdb5.3, libnet1 (>= 1.1.2.1), libnids1.21
(>= 1.23), libpcap0.8 (>= 0.9.8), libssl1.1 (>= 1.1.0), libtirpc3 (>=
1.0.2), libx11-6, libxmu6, openssl
Size: 104628
SHA256:
ead32e2029593afccc9282f1a5690eab2b346754f68df039ab36fef85dc3efb2
SHA1: 6eb09c4d6ee08b86e135e3e3e1262917ad926ab9
MD5sum: 798e63016163b956ae482f6162fa3d6d
Description: Various tools to sniff network traffic for cleartext
insecurities
 This package contains several tools to listen to and create network
traffic:
…

sudo apt install dsniff
```

```
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 – plnenie tabuľky položkami

- Ak nastane preplnenie CAM tabuľky
  - Prevádzka bez položky v CAM je floodovaná na všetky porty danej VLAN
- Tento útok preplní CAM tabuľky aj ostatných prepínačov

Before Macof

```
Access01#show mac-address-table count

NM Slot: 1
--------------

Dynamic Address Count:                  2
Secure Address (User-defined) Count:    0
Static Address (User-defined) Count:    0
System Self Address Count:              3
Total MAC addresses:                    5
Maximum MAC addresses:                  8192
```

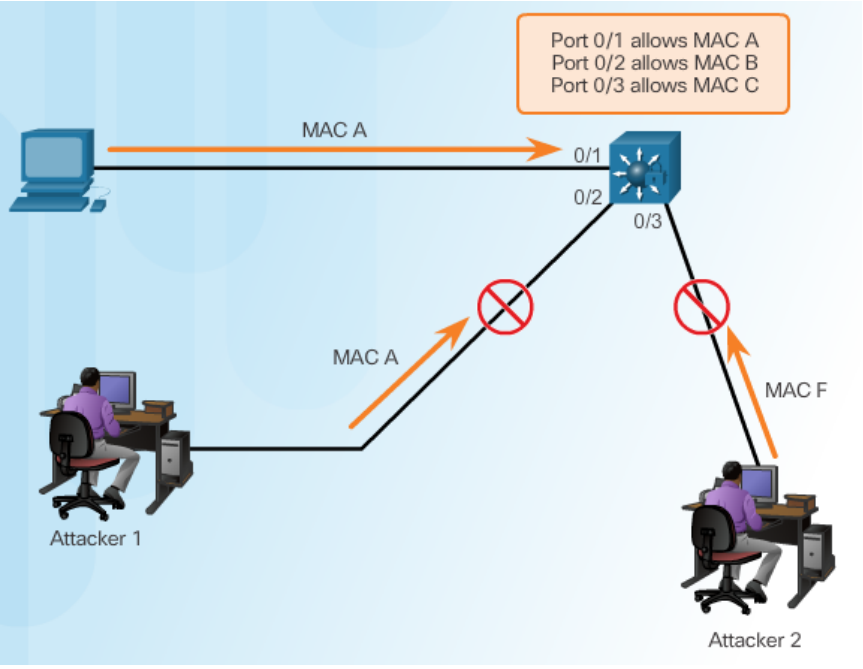
After Macof

```
Access01#show mac-address-table count

NM Slot: 1
--------------

Dynamic Address Count:                  8187
Secure Address (User-defined) Count:    0
Static Address (User-defined) Count:    0
System Self Address Count:              2
Total MAC addresses:                    8189
Maximum MAC addresses:                  8192
```

```
switch1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0011.5ccc.5c00    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0009.5b44.9d2c    DYNAMIC     Fa0/1
   1    000f.66e3.352b    DYNAMIC     Fa0/1
   1    0012.8015.c940    DYNAMIC     Fa0/24
   1    0012.8015.c941    DYNAMIC     Fa0/24
   1    001a.adb3.bef7    DYNAMIC     Fa0/1
   1    0025.2266.d104    DYNAMIC     Fa0/1
   1    0026.b865.313e    DYNAMIC     Fa0/1
   1    64a7.6973.8e4d    DYNAMIC     Fa0/1
   1    6c71.d976.fce7    DYNAMIC     Fa0/1
   1    74f6.12d4.1e1c    DYNAMIC     Fa0/1
   1    a477.3344.98b6    DYNAMIC     Fa0/1
```

Ochrana voči MAC flooding => Port security

- **Zmiernenie útokov** → **Port Security** (Cisco, Juniper, Huawei, Extreme...)
  - Umožňuje definovať maximálnu veľkosť zoznamu bezpečných/povolených MAC adries na porte
    - Komunikovať môžu iba koncové stanice s bezpečnými MAC adresami
    - Stanice s nebezpečnými (nezabezpečenými) MAC adresami porušujú port security – vykoná sa akcia
- **Tri typy bezpečných MAC adries**
  - Statická bezpečná MAC adresa
  - Dynamická bezpečná MAC adresa
  - Sticky bezpečná MAC adresa
- **Akcie pri porušení (Violation actions)**
  - **Protect**
  - **Restrict**
  - **Shutdown** *(predvolená akcia, port sa stane err-disabled)*
    - Port je možné obnoviť:
    - **manuálne** alebo
    - pomocou **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

Konfigurácia a overenie

```
! Konfiguracia
Sw(config)# interface fa0/2
! Port nesmie byt DTP dynamic, musi byt access alebo trunk
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 type absolute
Sw(config-if)# switchport port-security
```

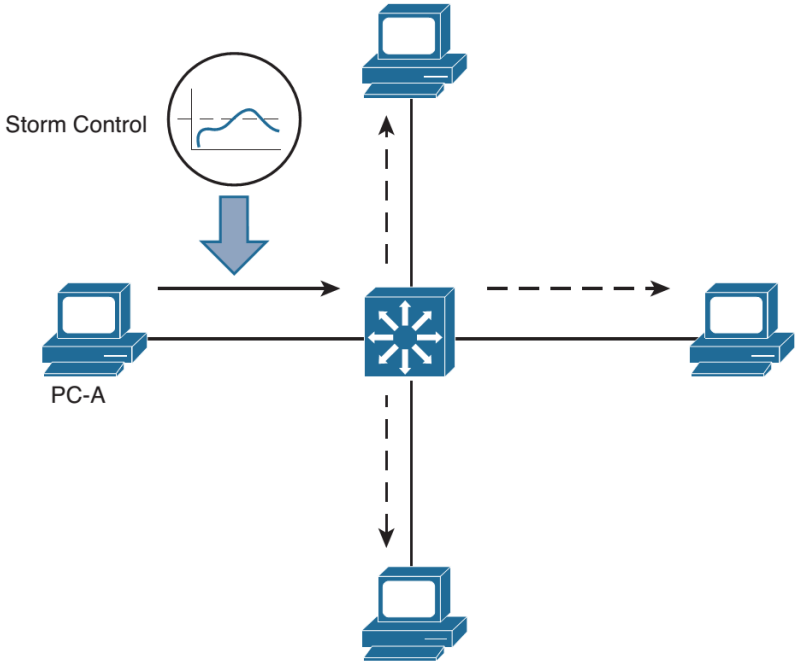
```
! Verify
Sw# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)          (Count)
-----------------------------------------------------------------------
      Fa0/2                5            3                  0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

Blocking Uni/Multicast Flooding – Blocking port

- Prepínače rady Cisco Catalyst môžu obmedziť flooding tokov neznámych multicast MAC alebo unicast MAC adries z daného portu na iné
- Vhodné ak viem, že na danom porte nie je nik neznámy
  - máme v CAM staticky definované dané MAC/PORT/VLAN
  - máme staticky alebo sticky definované bezpečné MAC adresy

```
4503# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
4503(config)# interface FastEthernet 3/22

! Block unknown unicast forwarding out of the port.
4503(config-if)# switchport block unicast

! Block unknown multicast forwarding out of the port.
4503(config-if)# switchport block multicast
```

Storm control (traffic supression)



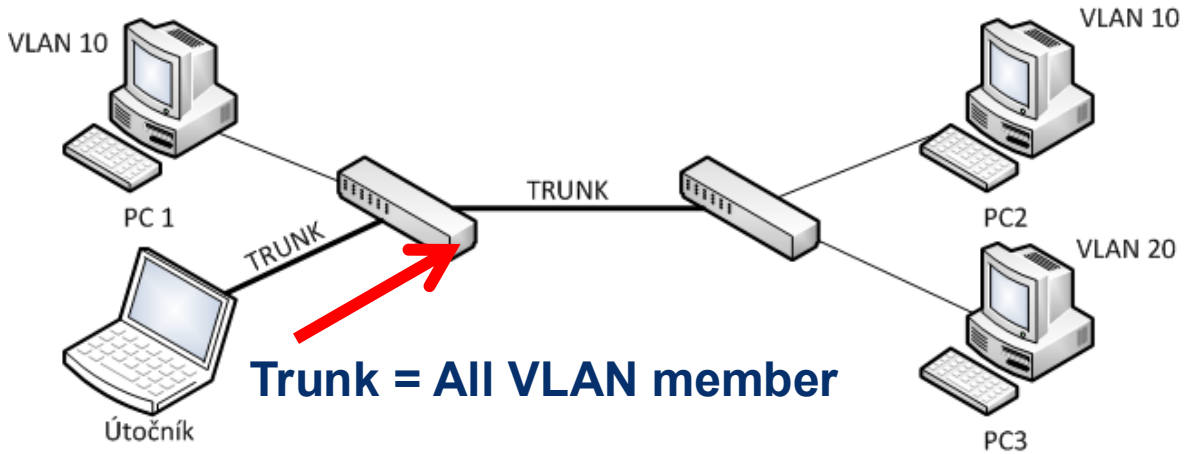
- Idea Storm control (SC)
  - Zabrániť zahlteniu prepínača a siete ešte pred vstupom toku rámcov do portu
  - SC je aktivovateľný pre broadcast, multicast, aj unicast
  - Zahltenie sa meria pre incoming rámce v 1s. intervaloch hardvérom prepínača
  - Level zahltenia môže byť definovaný
    - **Absolútne**: bps or pps
    - **Percentuálne**: úroveň zahltenia voči celkovej kapacite daného portu
  - Sú podporované dva treshold-y:
    - Level-low: ak padne pod, port je odblokovaný
    - Level: ak je prekročený vykoná sa akcia (shutdown or trap)

```
! Prístupový port s potláčaním bcast/mcast/ucast
! búrok
interface GigabitEthernet1/0/1
 switchport mode access
! Level 10, low 5
 storm-control broadcast level 10 4
 storm-control multicast level  10 4
 storm-control unicast  level   10 4
! po prekročení sa port errdisable-uje
 storm-control action shutdown
!
! auto-recovery po intervale nižšie
errdisable recovery cause storm-control
! (sekundy)
errdisable recovery interval 60
```

Útoky na VLAN / Ochrana a potláčanie

VLAN Hopping

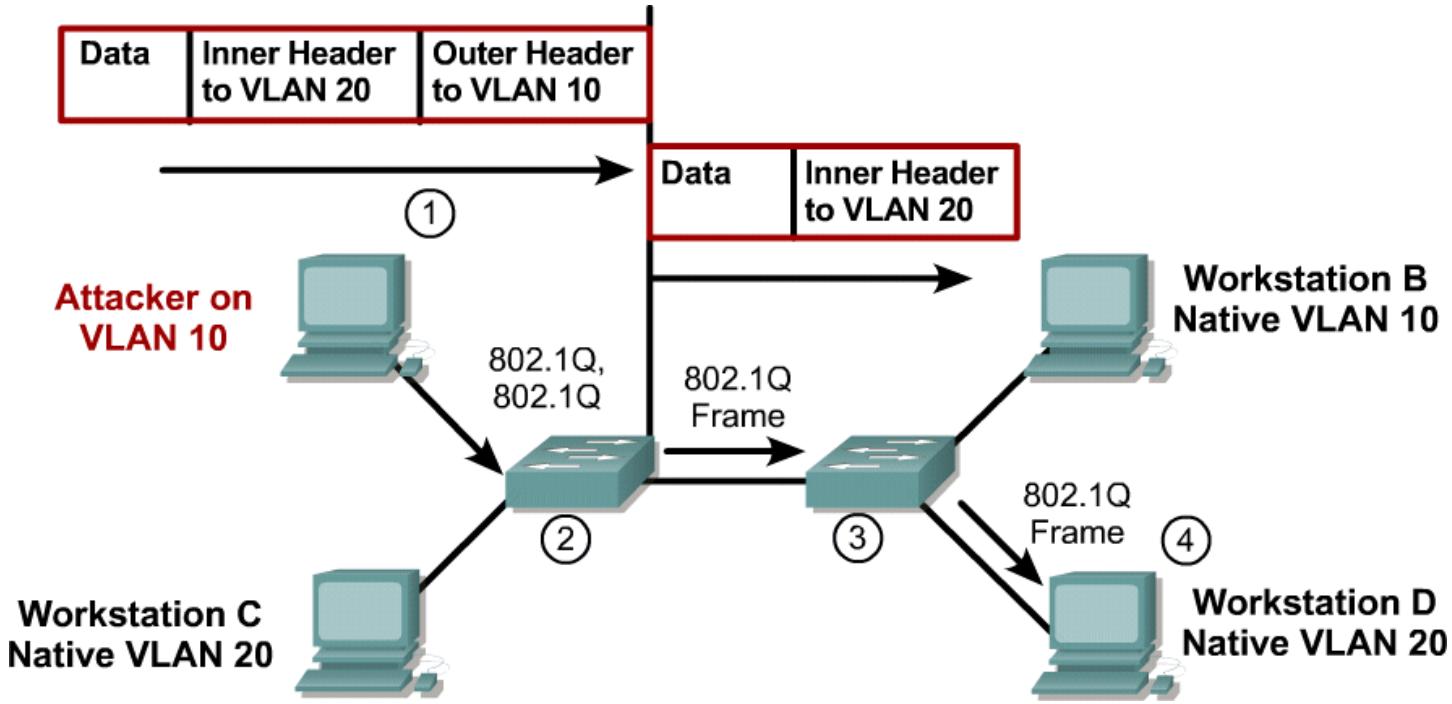
- Existuje niekoľko druhov útokov, ktoré sa snažia spôsobiť, aby rámec zo stanice v istej VLAN „pretiekol“ do inej VLAN
  - Nie vždy sa očakáva návrat (t.j. musí existovať cesta nazad)
  - To však nie je nutne problém – napr. pri TCP SYN Flood Attack
- Dva najbežnejšie vektory útoku:
  - **Útok na DTP** (Switch Trunk Spoofing)
    - Falošný prepínač alebo zariadenie s vhodným sw.
      - Snaha vytvoriť trunk cez DTP
      - tool yersinia
        - yersinia dtp –attack 1



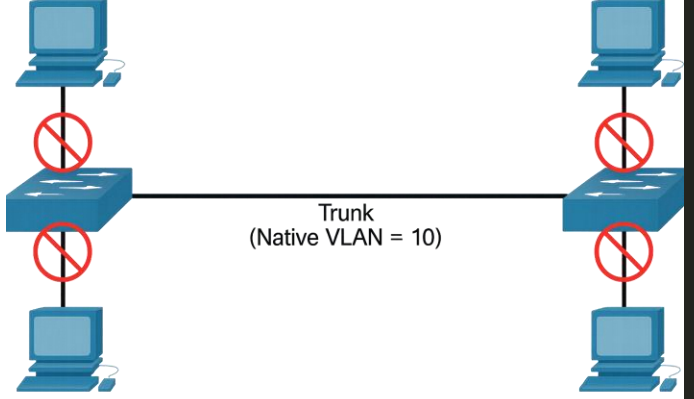
  - **Dvojité značkovanie pri 802.1Q** (Double tagging)
    - Yersinia 802.1q –attack 1

Útok dvojitým značkovaním

- Trunk medzi switchmi má natívnu VLAN 10
- Útočník vo VLAN 10 odošle rámec, ktorý má dva tagy
  - Vrchný má VID 10
  - Spodný má VID 20
- Switch akceptuje tento rámec
- Pretože rámec patrí do VLAN 10, ale tá je na trunku natívna, switch odstráni vrchný tag
- Na ďalší switch dorazí rámec s tagom 20
- Nič netušiaci switch ho spracováva vo VLAN 20



Ochrana

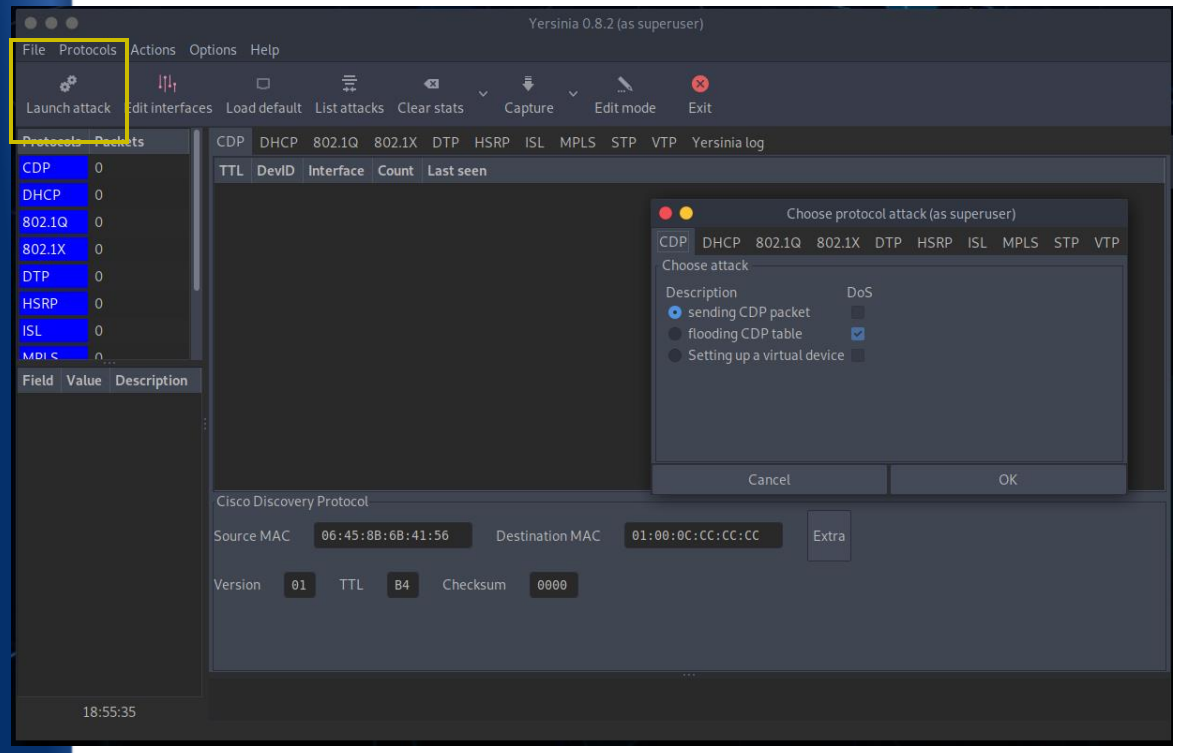



```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# end
S1#
```

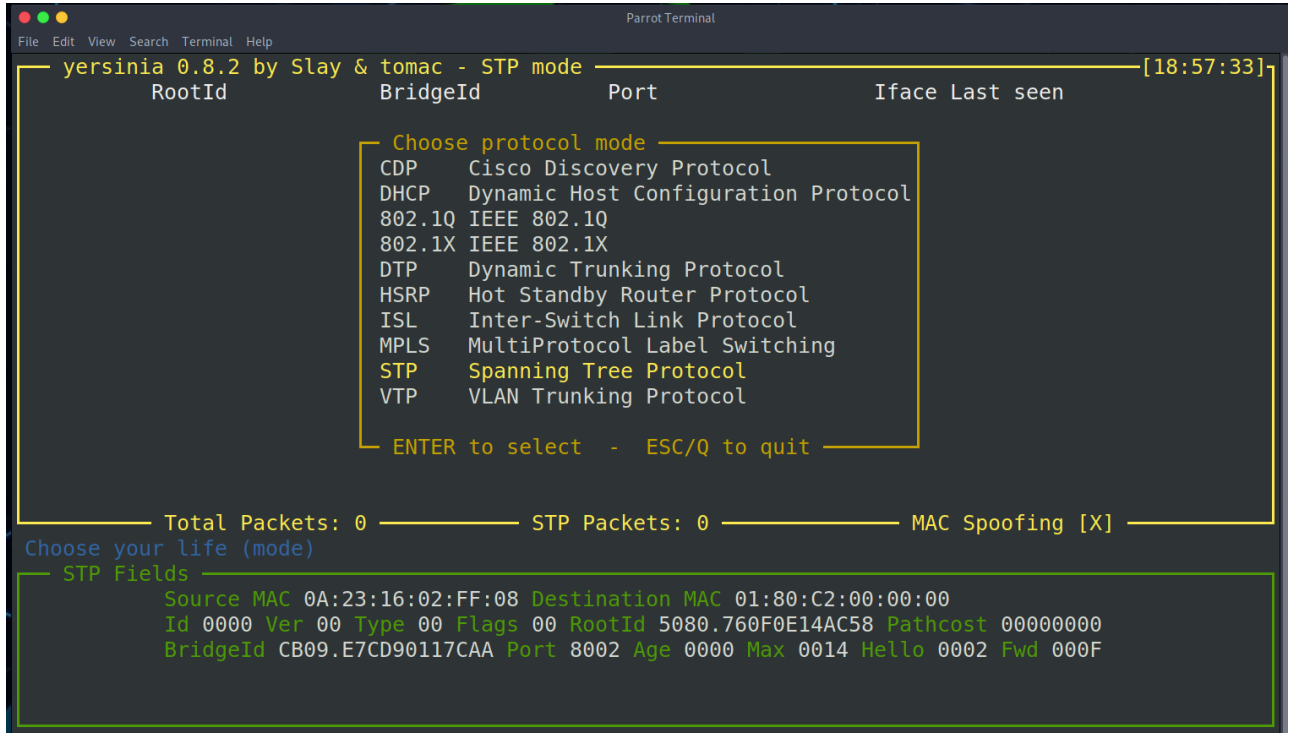
- **Útok na DTP**
  - Ochrana je jednoduchá
    - Zakáž auto trunking, explicitne nakonfiguruj trunk kde má byť
      - Nepoužívať dynamický režim na portoch a deaktivovať DTP
      - DTP je deaktivovaný na portoch, ktoré sú
        - Staticky nastavené ako prístupové `switchport mode access`
        - Staticky nastavené ako trunkové a DTP je deaktivované príkazom `switchport nonegotiate`
        - Nastavené ako smerované L3 porty príkazom `no switchport`
- **Dvojité značkovanie pri 802.1Q** (Double tagging)
  - Tento problém vzniká vtedy, ak je útočník v tej istej VLAN, ktorá je zároveň na nejakom trunku natívna
  - Spôsoby ochrany sú viaceré
    - Na trunkoch používať rovnakú natívnu VLAN, ktorá nikdy nebude nikde použitá ako data access alebo voice VLAN
      - `switchport trunk native vlan` *vlan_number*
    - Na switchoch vyšších radov existuje v globálnom konfiguračnom režime príkaz `vlan dot1q tag native` aktivujúci tagovanie všetkých VLAN na trunku vrátane natívnej
    - Nepoužité porty umiestniť do parkovacej VLAN

Yersinia - sudo apt install yersinia

yersinia -G



yersinia -I

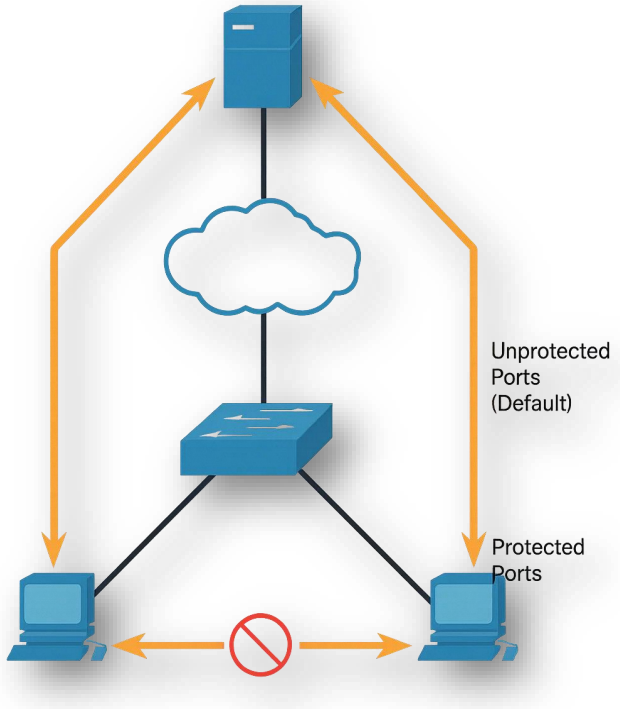


- CLI

```
[palo@palo-papagaj]-[~]
  $sudo yersinia dhcp -attack 1
Warning: interface eth0 selected as the default one
<*> Starting DOS attack sending DISCOVER packet...
<*> Press any key to stop the attack <*>


MOTD: The nightly bird catches the worm ;)
```

Potláčanie útokov v rámci VLAN – Private VLAN Edge

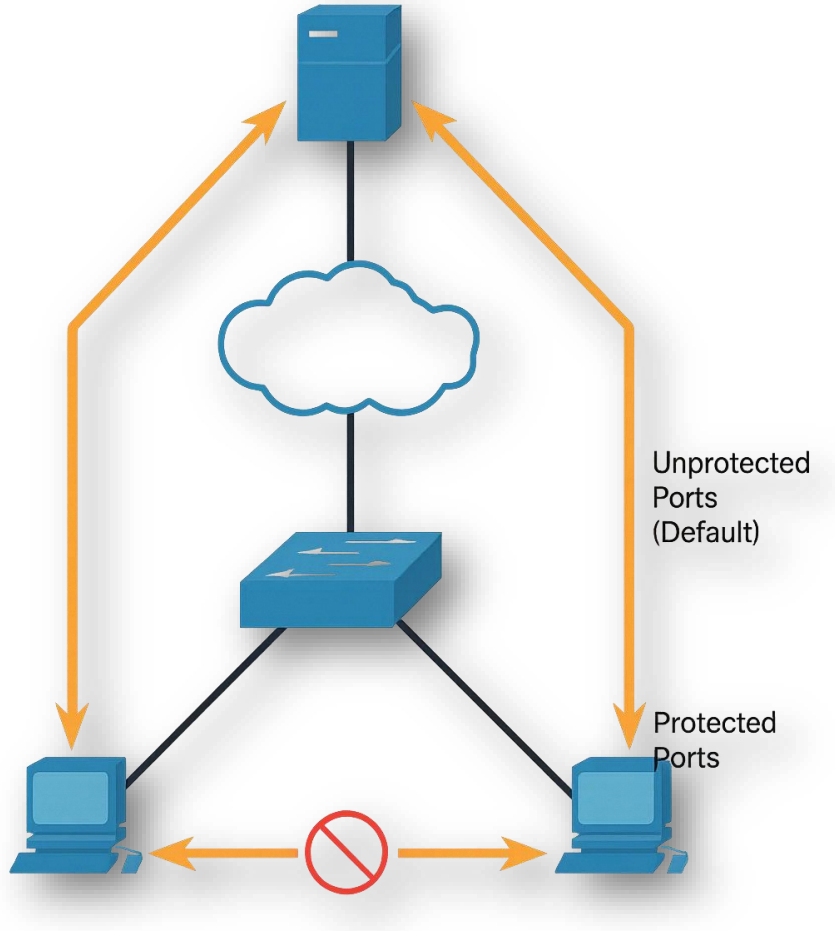
- **Private VLAN Edge / Port Isolation**
  - Jednoduchší koncept, používaný v lacnejších prepínačoch
  - Zakazuje prepínanie medzi portami v rámci rovnakej VLAN na tom istom prepínači
    - Izolácia portov
    - Má iba lokálny význam
  - Chránený port nepreposiela žiadnu prevádzku (unicast, multicast ani broadcast) na iný port, ktorý je tiež chránený
    - Na komunikáciu je potrebné prejsť cez zariadenie 3. vrstvy (L3)
    - Riadiaca prevádzka (control traffic) sa preposiela
  - Komunikácia medzi chráneným a nechráneným portom je povolená



- Cisco, Juniper, HP Aruba, Extreme, Huawei

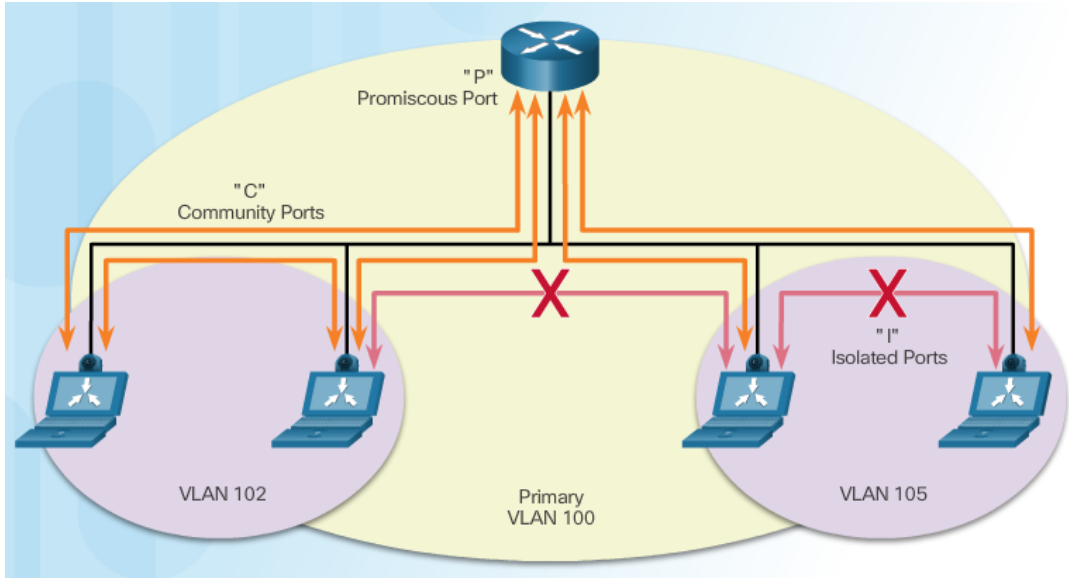
Príklad - Port Isolation (switchport protected)

```
! VLAN
vlan 10
 name USERS

! Uplink
interface GigabitEthernet1/0/1
 switchport
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast

! Chránené host porty
interface GigabitEthernet1/0/2
 switchport
 switchport mode access
 switchport access vlan 10
 switchport protected
 spanning-tree portfast
!
interface GigabitEthernet1/0/3
 switchport
 switchport mode access
 switchport access vlan 10
 switchport protected
 spanning-tree portfast
```



Privátne VLANs

- **Zložitejšie ako PVLAN Edge**
  - Zvyčajne doména multilayer prepínačov
  - Umožňuje riadiť L2 prepínanie medzi portami v rámci rovnakej VLAN
  - Povoliť alebo zakázať komunikáciu medzi portami
  - Používa koncept **primárnej VLAN**
    - Interné rozdelenie na **sekundárne VLANy**
- **Sekundárne VLANy – dva typy**
  - **Community**
    - Porty môžu komunikovať s inými community portami a promiscuous portami
  - **Isolated**
    - Úplná L2 izolácia od ostatných portov v rámci tej istej PVLAN
    - Môžu komunikovať iba s promiscuous portami
    - Môže existovať iba jedna
- **Promiscuous port**
  - Vstupný bod do všetkých VLAN
  - Port môže komunikovať so všetkými



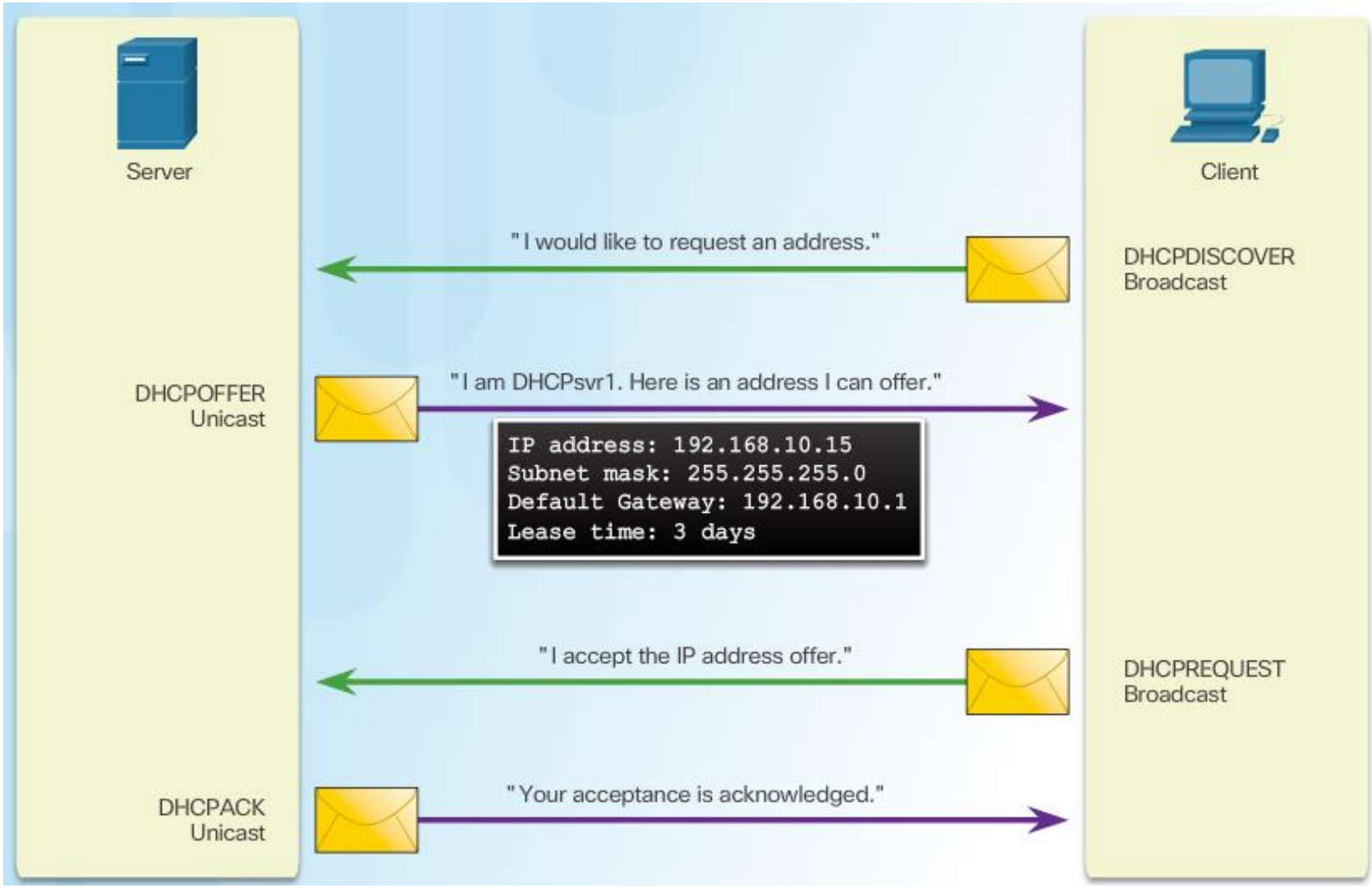
- Cisco, Juniper, HP Aruba, Extreme, Huawei

Príklad - PVLAN

```
! Definícia PVLAN
vlan 100
 private-vlan primary
 private-vlan association 101,102

vlan 101
 private-vlan isolated

vlan 102
 private-vlan community

! Trunk, ktorý prenáša PVLAN (na uplink do distribúcie/ASA/NGFW)
interface GigabitEthernet1/0/1
 switchport mode trunk
 switchport trunk allowed vlan add 100,101,102
 switchport trunk private-vlan mapping 100 add 101,102

! Promiscuous port (gateway/server, ktorý má vidieť všetkých)
interface GigabitEthernet1/0/10
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 100 add 101,102

! Host port – izolovaný (nevidí iných hostov)
interface GigabitEthernet1/0/2
 switchport mode private-vlan host
 switchport private-vlan host-association 100 101
 spanning-tree portfast

! Host port – community (vidí členov rovnakého komunitného segmentu)
interface GigabitEthernet1/0/3
 switchport mode private-vlan host
 switchport private-vlan host-association 100 102
 spanning-tree portfast
```

Útoky na DHCP a ich potláčanie

DHCP princíp činnosti (DORA mnemo)

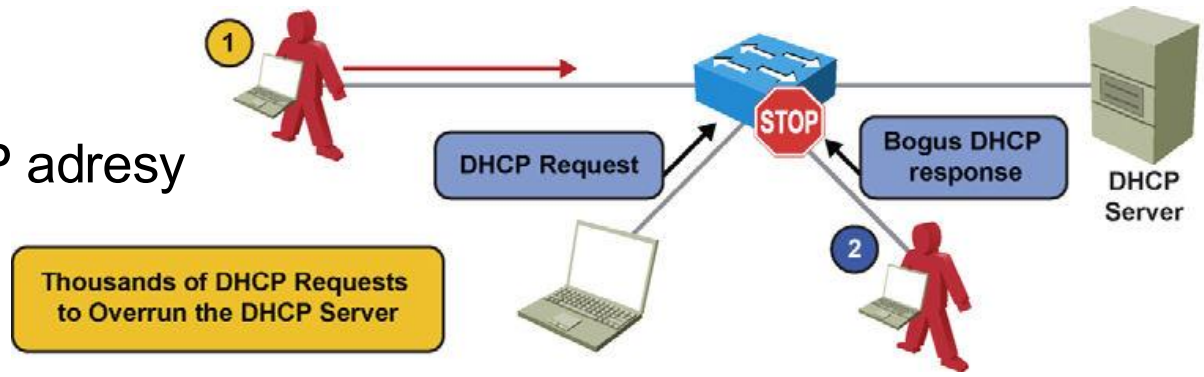


Správy servera

Správy killenta

DHCP Spoofing a DHCP starvation

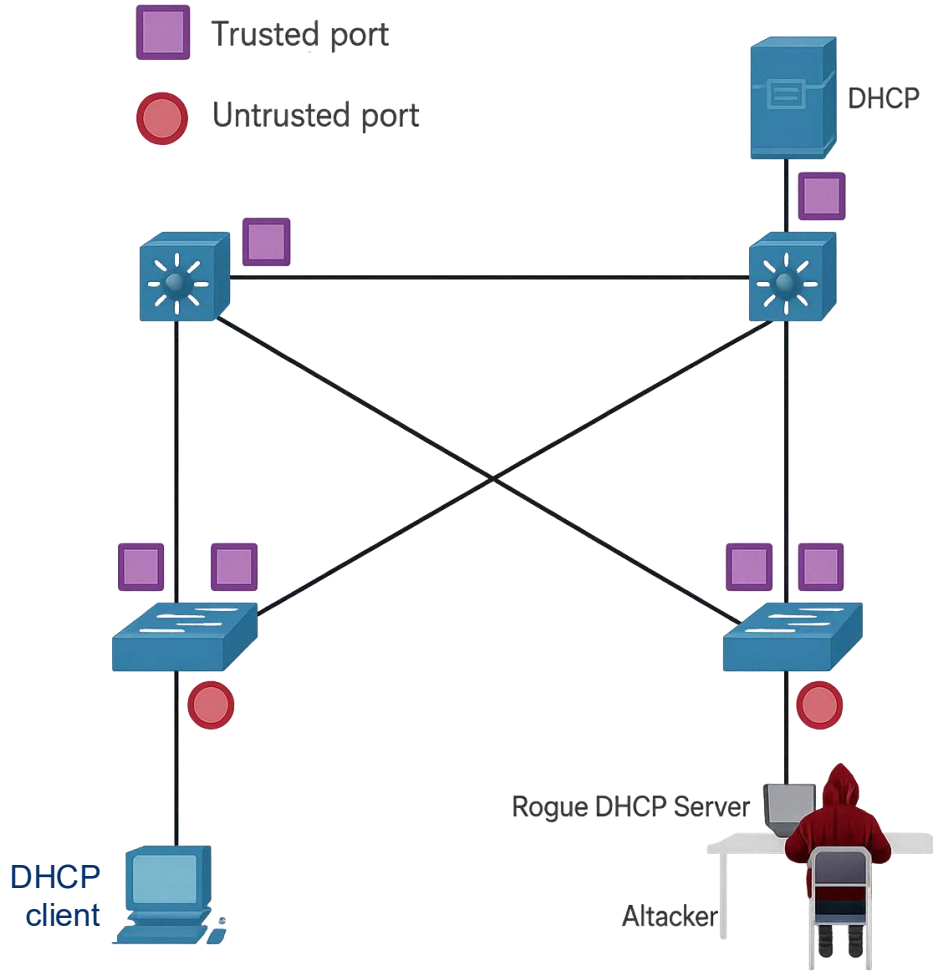
- Môže vykonať útočník fyzicky prítomný v danej LAN, alebo získal prístup z Internetu na niektorý PC v danej LAN
- **DHCP starvation (vyhladovanie)**
  - Generuje sa veľké množstvo žiadostí o IP adresy (posiela sa broadcastom),
  - DHCP serveru neostanú voľné IP adresy
    - Gobbler, yersinia



- **DHCP spoofing (podvrhnutie)**
  - Zapojenie neautorizovaného DHCP servera (rogue DHCP server) do siete
  - Útočník môže podvrhnúť:
    - **Nesprávny default gateway**: Útočník je Gateway (M-i-M)
    - **Nesprávny DNS server**: Útočník je DNS
    - **Nesprávnu IP adresu:** Útočník urobí s danou IP DoS

Potláčanie DHCP útokov

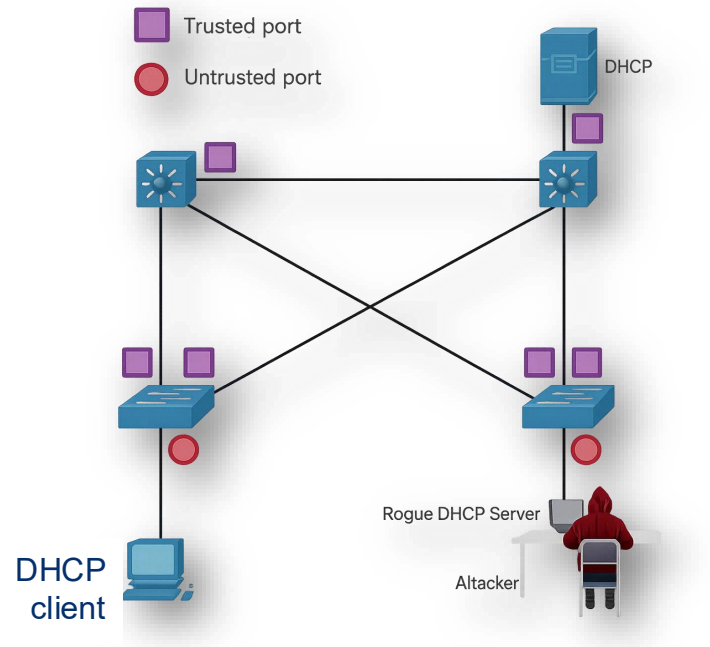
- **DHCP Starvation attack** =>
  - Port security
  - Dhcp snooping limit rate
    - Obmedzím počet DHCP requestov za sekundu
  - *yersinia dhcp -attack 1*
- **DHCP spoofing attack** => DHCP Snooping
  - **Trusted porty:** port kde môžu prísť odpovede na DHCP žiadosti
  - **Untrusted porty:** ostatné
    - čítam DHCP DORA proces => budujem **DHCP Snooping DB**
      - IPčka + MAC + port + doba zápožičky
    - Povoľujem len klient správy
    - Server správy dropujem




```
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
```

DHCP Snooping

- DHCP Snooping rozpoznáva **dôveryhodné** a nedôveryhodné porty
  - Nedôveryhodné porty:
    - Nachádzajú sa na nich stanice
    - Predvolený typ portu
  - Dôveryhodné porty (alebo za nimi):
    - Nachádzajú sa na nich DHCP servery alebo sieťové jadro
- DHCP Snooping odpočúva DHCP komunikáciu na nedôveryhodných portoch a vytvára databázu DHCP väzieb (binding database)
  - Databáza obsahuje záznamy ako:
    - MAC adresa klienta
    - Pridelená IP adresa
    - Čas prenájmu (lease time)
    - VLAN
    - Port




```
! 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
```

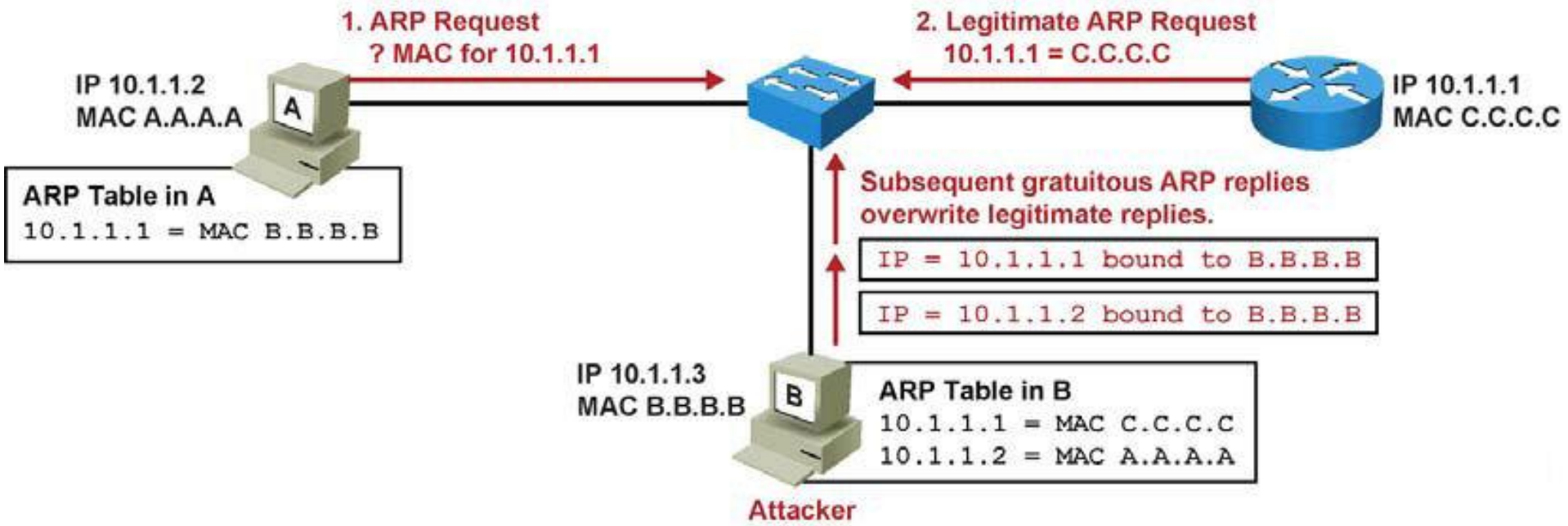
Útoky na ARP + address spoofing a ich potláčanie

Útoky typu „Address Spoofing“

- **Address spoofing**
  - Akýkoľvek útok, pri ktorom sa niekto snaží predstaviť ako iná entita
    - Spoofing je snaha o to, aby si niekto myslel, že som kto nie som
- Všeobecne známe (*well-known*) kategórie útokov
  - MAC/ARP spoofing
  - IP spoofing
  - DHCP spoofing

ARP Spoofing

- ARP Spoofing je odosielanie nevyžiadaných (gratuitous) ARP správ, v ktorých mapujeme zvolenú IP na inú než skutočnú MAC adresu
  - Denial of Service: mapovaním IP na neexistujúcu MAC
  - Man-In-The-Middle: mapovaním cudzej IP na moju MAC
- Nástroje: Cain&Abel (win), ettercap -G



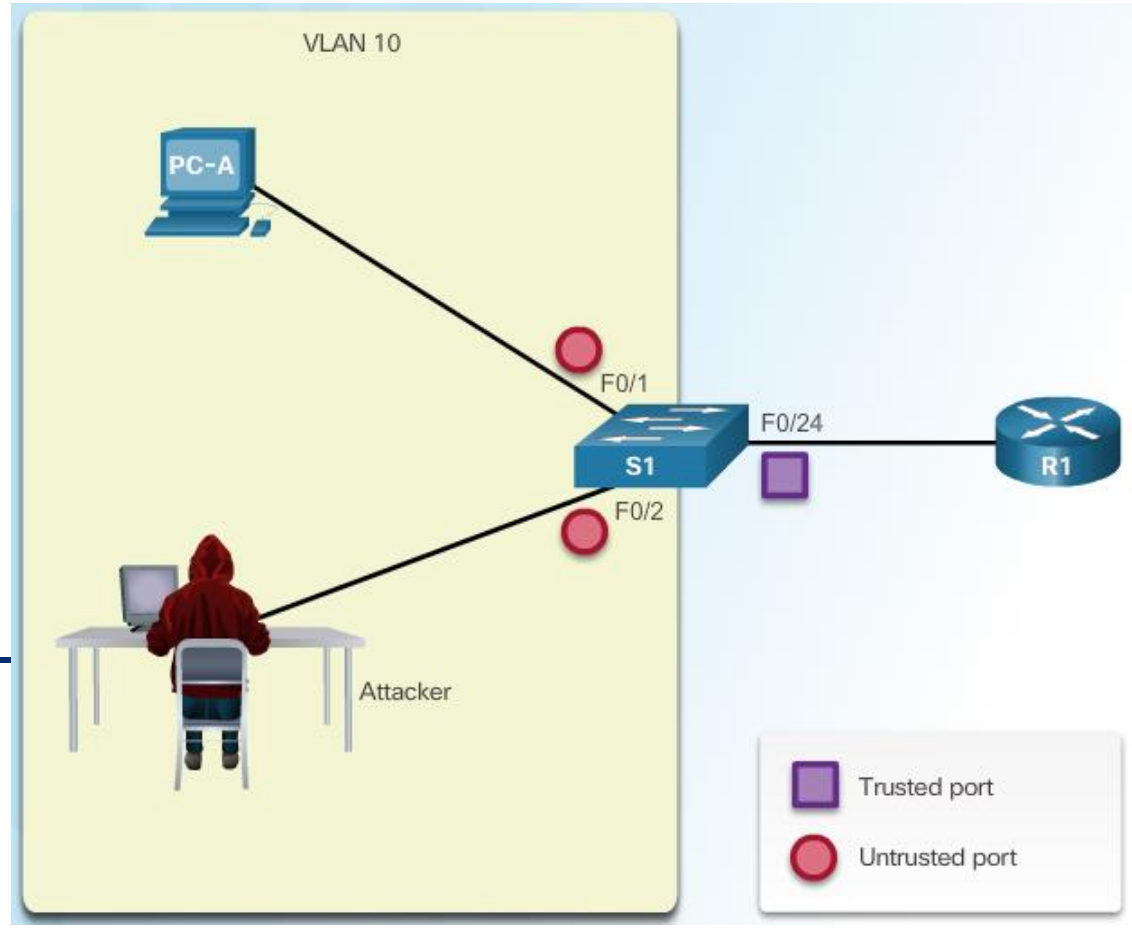
Ochrana proti ARP Spoofing => Dynamic ARP Inspection

- Dynamic ARP Inspection (DAI)
  - Používa databázu z DHCP Snoopingu
  - Každá ARP správa obsahuje o. i. polia
    - Sender MAC a Sender IP
    - Target MAC a Target IP
  - DAI
    - Kontroluje, či si tieto údaje v ARP správach podľa databázy z DHCP Snoopingu navzájom zodpovedajú
      - MAC adresa v ARP request a ARP reply sa musia zhodovať s DHCP Snooping položkou
    - Dropne invalid a gratuitous ARP odpovede na untrusted portoch
    - Zhodí port pri prekročení limitu
  - DAI môže dodatočne kontrolovať aj správnosť ďalších údajov
    - Napr. zdrojovú MAC adresa rámca

```
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)
```

Konfigurácia Dynamic ARP Inspection

- DAI tiež klasifikuje porty ako
  - Trusted
  - Untrusted (default typ)
    - prepínač kontroluje obsah prichádzajúcich správ ARP voči databáze DHCP Snooping
  - Ak sú ARP správy nevhodné => Dropne
- DAI musí mať funkčný 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
! Ak je utok
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])
```

IP Spoofing => IP Source Guard (IPSG)

- Ukradnutie a používanie platnej IP adresy inej stanice
  - Používa sa napr. na Ping smrti, nedosiahnuteľná búrka ICMP, povodeň SYN
- Zdroj mnohých existujúcich útokov DoS a DDoS
  - Podvrhnem zdrojovú adresu obete, kde sa budú vracať odpovede
- Ochranou proti IP Spoofingu na prístupovej vrstve
  - => **IP Source Guard (IPSG)**
    - IP adresu stanici pridelí DHCP server
    - DHCP Snooping zaznačí MAC adresu stanice a pridelenú IP do snoop databázy
      - DHCP Snooping môže opäť výrazne pomôcť
    - IP Source Guard skontroluje, či IP adresa odosielateľa na porte (prípadne dokonca MAC adresa odosielateľa) zodpovedá záznamu v databáze
      - Podobne ako DAI, ale kontroluje každý paket a nielen ARP
      - Prepusti len pakety s validnou IP zdrojovou adresou
- Na L3
  - Extended ACL
    - Ktoré v podmienke na pozícii zdroja nepoužívajú ***Any***
    - Filtrujú invalid zdroj: Bcast nad multicast, privátne adresy
  - Unicast Reverse Path Forwarding

Konfigurácia IP Source Guard – over len IP

- Prepusti len pakety s validnou IP zdrojovou adresou (voliteľne MAC)
- Konfigurácia
  - Predpokladom pre konfiguráciu IP Source Guard je funkčný DHCP Snooping
  - IPSG sa konfiguruje na untrusted portoch
  - Samotný IP Source Guard s kontrolou zdrojovej IP adresy odosielateľa sa konfiguruje jednoducho:

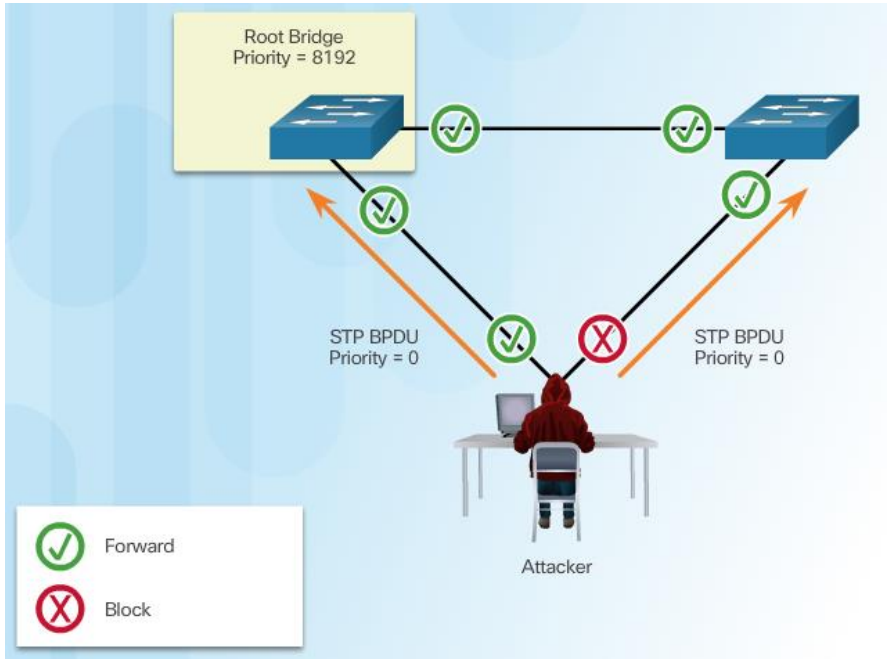
```
Sw(config)# ip dhcp snooping
Sw(config)# ip dhcp snooping vlan 1, 10
Sw(config)# int fa0/1
Sw(config-if)# ip verify source vlan dhcp-snooping

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

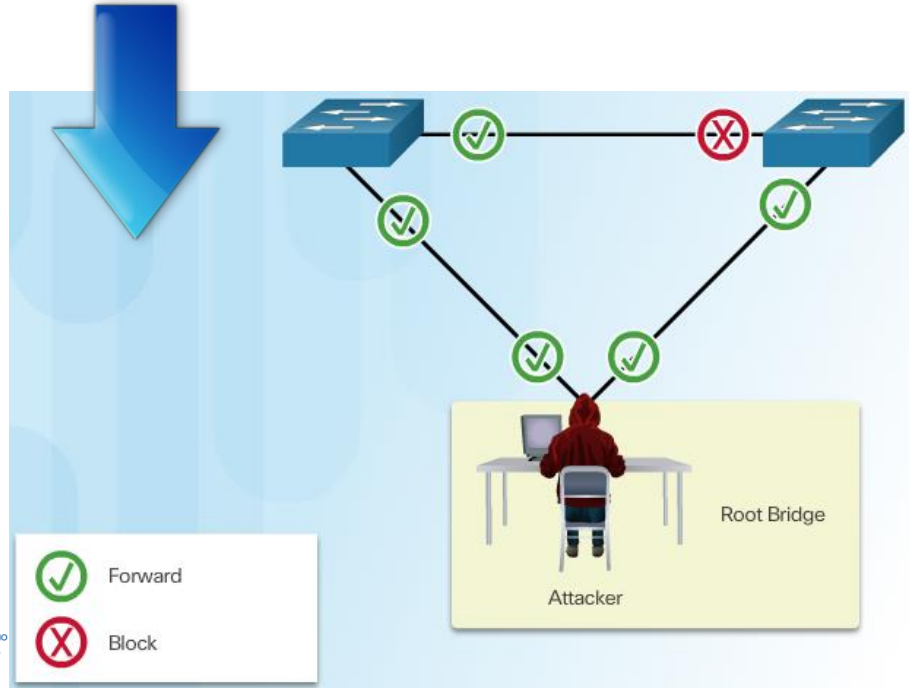
Útoky na STP a ich potláčanie

Útoky na STP

- Snaha modifikovať STP strom
  - => ovplyvnenie priepustnosti
  - => získanie prístupu k dátam
- Spoofing Root bridge-a
  - MiTM, DoS, ...
- Snaha generovať zmeny
  - => flush MAC tabuliek a nárast komunikácie-zahltenie

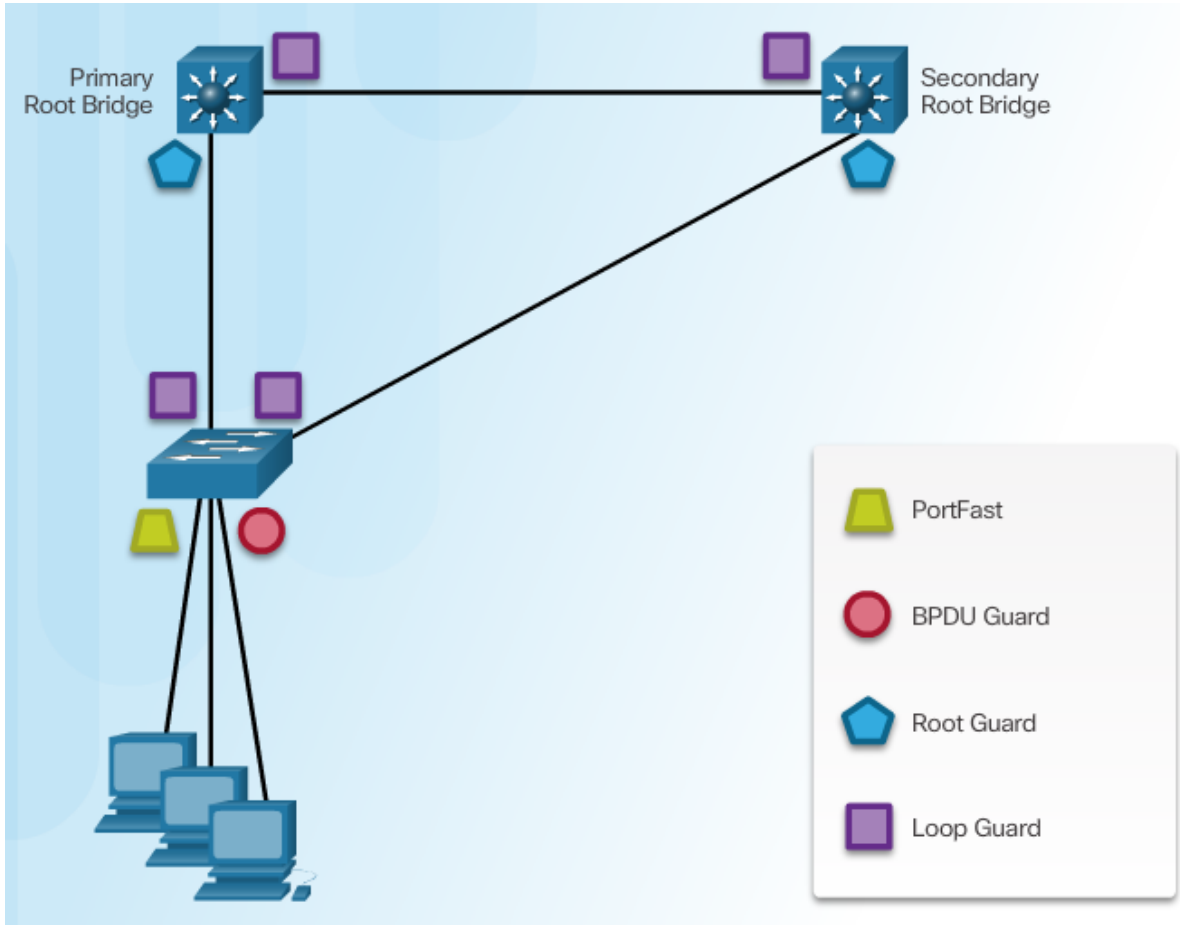
- *Nástroj: yersinia stp -attack .....*





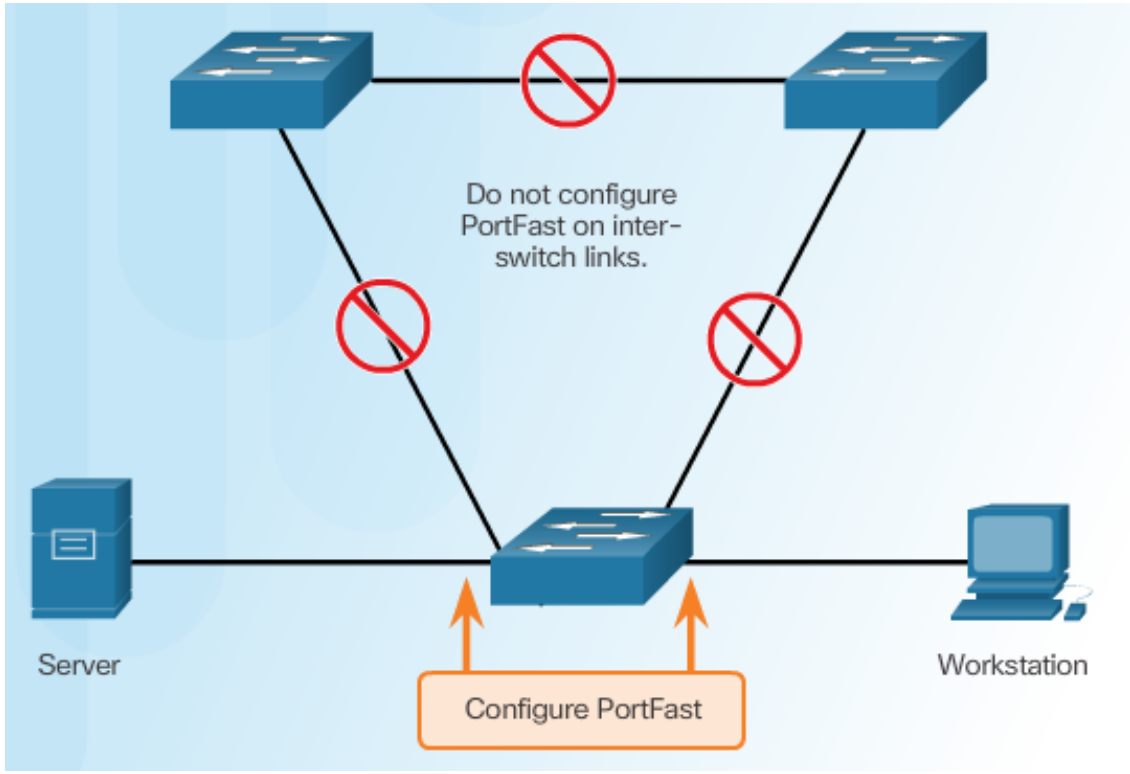
Potláčanie STP útokov

- Viac mechanizmov
  - **PortFast**
    - „obživne“ rozhranie okamžite zo stavu blokocking do forwarding
    - Odporúča sa používať na portoch k PC
  - **BPDU Guard**
    - Ochrana pred prijatím akýchkoľvek BPDU rámcov
    - Ak porušenie => zhodí rozhranie do err-disabled
  - **Root Guard**
    - Zabraňuje aby sa z nevhodného prepínača stal nový root bridge
      - i.e. ochraňuje umiestnenie súčasného RB
    - Port umiestni do root-inconsistent state
  - **BPDU Filter**
    - Zabraňuje odosielanie BPDU správ von cez daný port



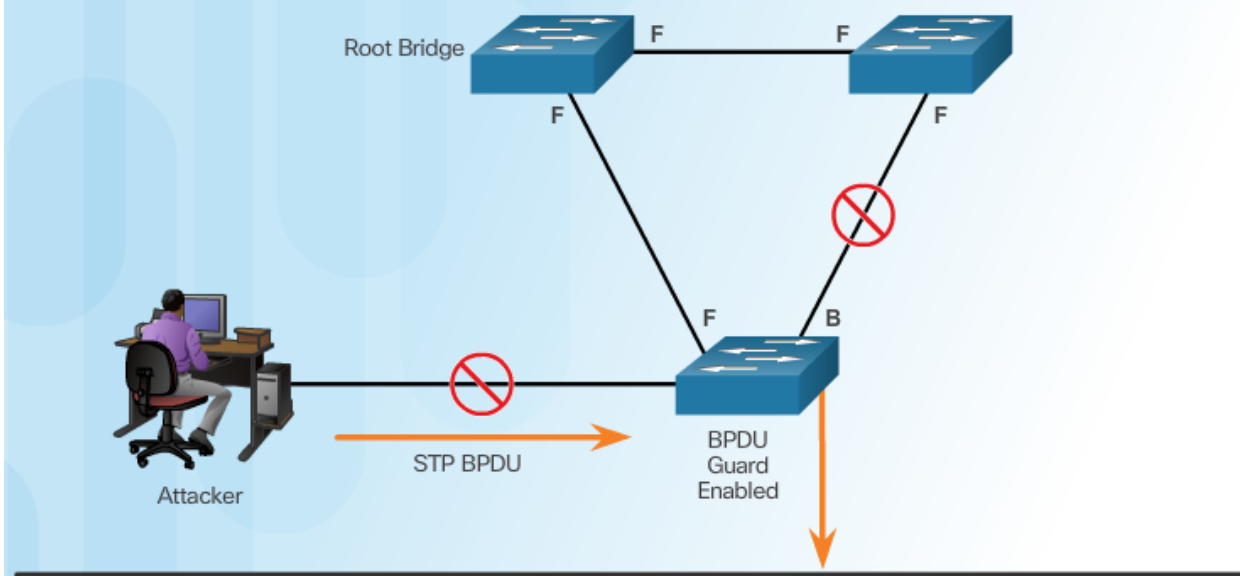
Konfigurácia a overenie Port Fast

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

! Na porte
! 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
```



- Overenie
  - show **running-config | begin span**
  - show **spanning-tree summary**
  - show **running-config interface *TYPE/NUMBER***
  - show **spanning-tree interface *TYPE/NUMBER* detail**

Konfigurácia 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
```

Iné útoky

Útoky na Neighbor Discovery Protocols (NDP)

- NDP
  - Cisco Discovery Protocol (CDP): Cisco proprietárny
  - Link Layer Discovery Protocol (LLDP): IEEE štandard
  - Protokoly sú nešifrované, bez autentifikácie
- Útoky
  - Sniffing: Získam info počúvaním (IOS verzia, manažment IP...)
  - Zahltenie: Typicky flooding hlúposťami
    - => zahltenie pamäte
  - Spoofing a manipulácia: podvrh falzov
- Ochrana: vypni
  - Celkovo: no cdp run / **no lldp run**
  - Na portoch kde je bežný používateľ: no cdp enable / **no lldp transmit || receive**
  - Neodporúča sa na VoIP portoch

```
Device ID: MENO_ZARIADENIA.kis.fri.uniza.sk
Entry address(es):
  IP address: 10.255.255.14
Platform: cisco WS-C3850-12XS,  Capabilities:
Switch IGMP
Interface: TenGigabitEthernet1/1,  Port ID
(outgoing port): TenGigabitEthernet1/0/9
Holdtime : 148 sec

Version :
Cisco IOS Software [Gibraltar], Catalyst L3 Switch
Software (CAT3K_CAA-UNIVERSALK9-M), Version
16.12.7, RELEASE SOFTWARE (fc2)
Technical Support:
http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Wed 02-Feb-22 07:28 by mcpre

advertisement version: 2
VTP Management Domain: 'kis'
Native VLAN: 1000
Duplex: full
Management address(es):
  IP address: 10,255.255.14
Unidirectional Mode: off
```

VoIP porty – CDP a LLDP MED

- Baseline => povoľ kde je telefón
  - LLDP-MED (**Link Layer Discovery Protocol – Media Endpoint Discovery**)
    - Rozšírenie štandardného LLDP (IEEE 802.1AB)
    - špecificky pre **VoIP/Unified Communications zariadenia**
    - Telefón vie získať info => jednoduchšie nasadenie
      - VLAN, QoS, sieťové politiky, lokalizáciu
      - Telefón sa pripojí do správnej Voice VLAN
      - Nastaví DCSP QoS hodnotu
  - Platí aj pre CDP

Baseline

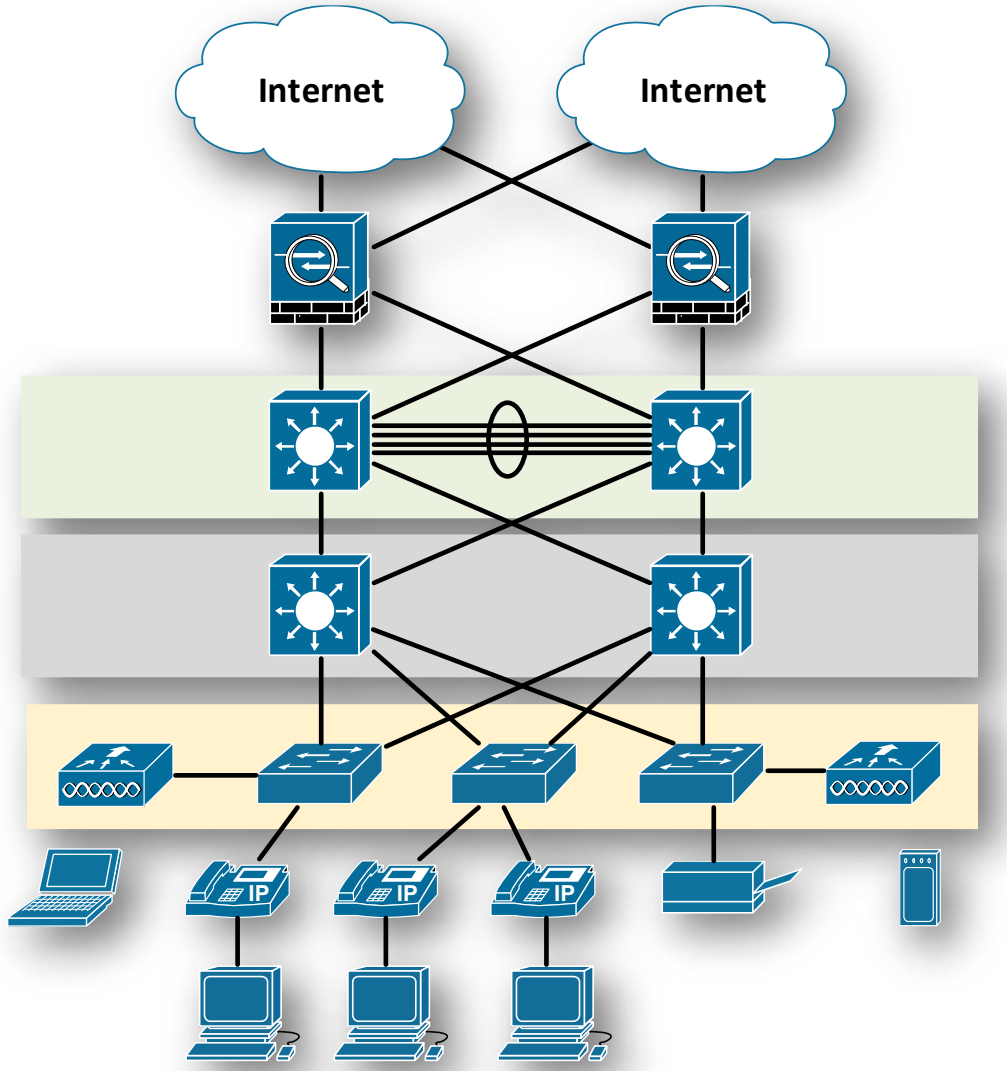
Štandardizované odporúčania pre bezpečnosť na prístupe

- **Baseline =** súbor minimálnych bezpečnostných opatrení a konfigurácií pre prístup do LAN siete
- **Cisco Secure Access Design**
  - **Port hardening -** Zakázať DTP, použiť voliteľne NAC
  - **VLAN hardening** - tagovať native VLAN, nepoužívať VLAN 1, režim činnosti (sw mode access), whitelist VLAN na trunku
  - **DHCP Snooping** + DAI + IPSG ako trio
  - **Port Security** – limit MAC adries 1 až 2 (VoIP), režimy *protect/restrict/shutdown* podľa politiky
  - **Prevídateľné STP -** STP guardy na prístupe (BPDU Guard, Root Guard, Loop Guard)
  - **CDP/LLDP** – Vypnúť na user portoch, povoľ do vnútra
  - **Storm-Control** – limitovať broadcast, multicast a unknown unicast traffic
  - **Management plane hardening**
    - ACL na VTY prístupy, používať SSH v2, Logging/NTP synchronizácia pre auditovanie
  - **Consistency/Audit**
    - Zlaté šablóny (gold config) pre access port, trunk port, voice port
    - Pravidelná kontrola compliance
- **NIST SP 800-41 Rev.1**
  - NAC ako doplnok k baseline
  - Definícia trusted/untrusted portov
  - Pravidelný audit konfigurácie access vrstvy
- **Best practice:** baseline + NAC + monitoring (Syslog, SIEM)
- **Výsledok:** konzistentný hardening + kontrola identity = robustná obrana L2

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Access vs. Distribution vs. Core – kde čo riešiť

- **Access layer (prístupová vrstva):**
  - Najzraniteľnejšia časť – používateľské porty
  - Baseline hardening: Port Security, DHCP Snooping, DAI, IPSG
  - VLAN hardening: zákaz DTP, VLAN1 nepoužívať, tag native VLAN
  - STP Guardy na prístupových portoch
- **Distribution layer (distribučná vrstva):**
  - Enforcement politiky a segmentácia (ACL, VACL)
  - Agregácia VLAN → inter-VLAN routing
  - Redundancia a kontrola STP/HSRP
  - Filtrácia broadcastov/multicastov
  - Zabezpečenie routing
- **Core layer (jadro):**
  - Maximálna rýchlosť, minimálna komplexnosť
  - Žiadne ACL ani security feature, ktoré spomaľujú forwarding
  - Zameranie na dostupnosť, spoľahlivosť a rýchly transit
  - Bezpečnosť riešená na prístupovej a distribučnej vrstve



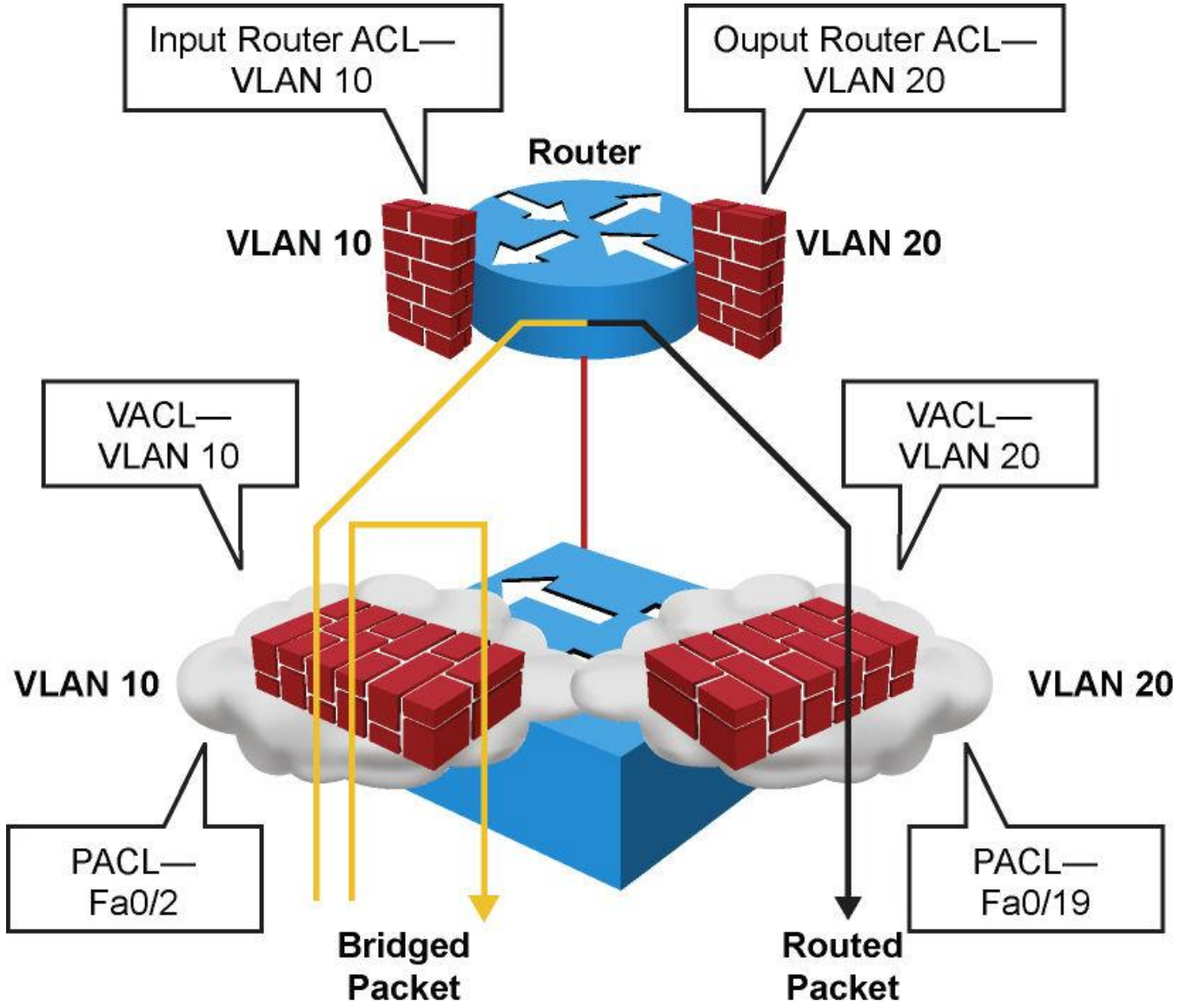
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Riadenie prístupu na prepínačoch pomocou ACL

ACL na prepínačoch

- Prepínače podporujú viaceré druhy ACL
  - **Router ACL (RACL)**
    - klasické IP ACL, ktoré môžu byť umiestnené na smerovaných (routed or SVI) portoch
    - Na MLS prepínačoch hardvérová podpora v TCAM
  - **VLAN ACL** (Cisco volá VLAN map)
    - aplikované na VLAN a všetky jej porty ako celok (nemajú smer, interne využívajú IP alebo MAC ACL)
- **Port ACL (PACL)**
  - môžu byť umiestnené na prepínaných portoch (MAC ACL iba inbound smer), trunk portoch, EtherChannel
  - Pracuje na L2 port úrovni, ale triediace informácie môžu byť založené na L2/L3/L4 informáciach
    - Je vhodná HW podpora
    - Nemá vplyv na control plane rámce a pakety
    - Nutné konzultovať dokumentáciu!
- Dva typy
  - MAC access list
    - Filtruje rámce na základe polí hlavičky Ethernet rámca
  - IP access list
    - Na danom porte filtruje IPv4 a IPv6 pakety

ACL na prepínačoch



Zhrnutie - Riadenie prístupu v LAN

- **Access Layer = prvá línia obrany**
  - Miesto, kde sa sieť „dotýka“ používateľa alebo zariadenia
  - Riadi, *kto a čo sa pripája* k infraštruktúre
- **802.1X – základná technológia port-based autentifikácie**
  - Overenie identity používateľa a zariadenia ešte pred prístupom
  - Komponenty: *Supplicant – Authenticator – Authentication Server (RADIUS)*
  - Prenáša sa cez EAP/EAPOL
  - Základ pre moderné NAC riešenia
- **NAC – Network Access Control**
  - Centrálne riadenie prístupu na základe identity a stavu zariadenia
  - Politiky: *Allow / Quarantine / Deny*
  - Integrácia s IAM, SIEM, EDR, MDM → kontextové rozhodovanie
  - Príklady: *Cisco ISE, Aruba ClearPass, PacketFence*
- **First Hop Security (FHS)**
  - Dopĺňa NAC o ochranu vrstvy 2 po autentifikácii
  - Mechanizmy: *DHCP Snooping, DAI, IP Source Guard, Port Security, PVLAN Edge*
  - Zabraňuje spoofingu, floodingom a lokálnym útokom
- **Kľúčový princíp – Zero Trust / Least Privilege**
  - *Never trust, always verify*
  - Každý prístup je overený, každý port kontrolovaný, každé zariadenie overené

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Mechanizmy riadenia prístupu

Sieťová bezpečnostná architektúra (Blok II.)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Pavel Segeč

KC KYB UNIZA, https://kc.uniza.sk

Pavel.Segec@fri.uniza.sk