UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

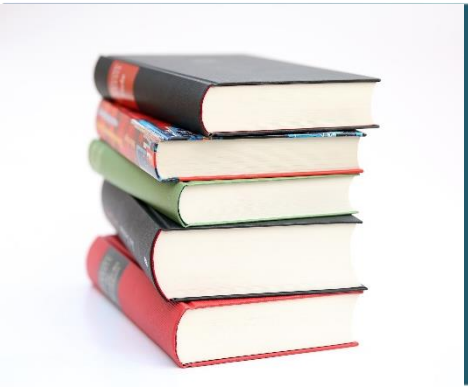
Koncepia bezpečnosti na prepínaných sieťach LAN

CCNA2 (v7)

SRWE_10: LAN Security Concepts

SRWE_11 Switch Security Configuration

Vytvorené v rámci projektu KEGA 026TUKE-4/2021.



Obsah prednášky

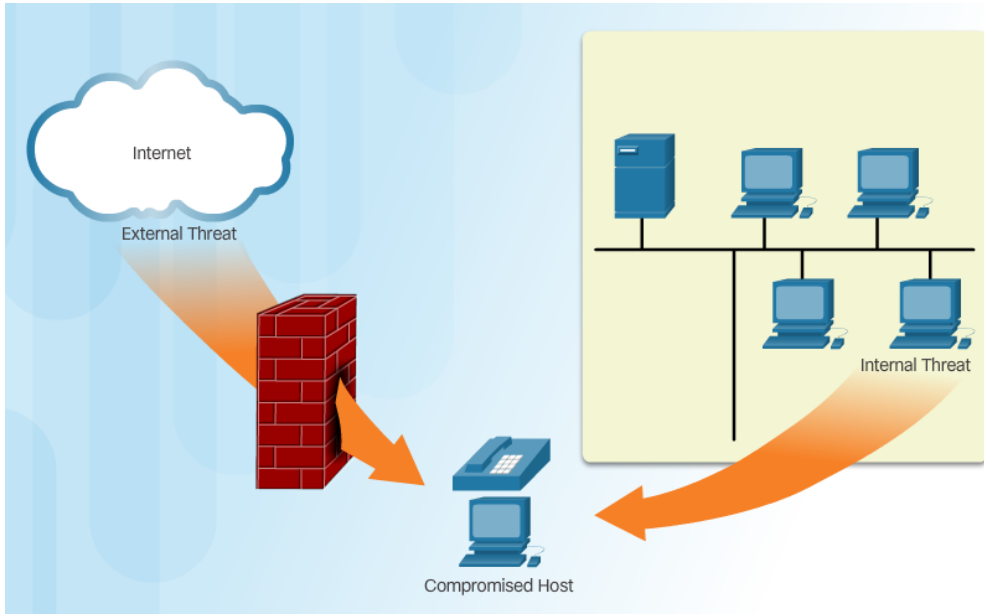
- **LAN Security Concepts**
  - Endpoint Security
  - Riadenie prístupu (Access Control)
  - Bezpečnostné hrozby na Layer 2 / Útoky a ochrana na LAN
    - Útoky na MAC Address Table, DHCP , ARP, STP,
- **Viac v CCNA Security / CCNP Switch**
- **Switch Security Configuration**
  - Ako to spraviť :-) pre
    - Port Security
    - VLAN Attacks
    - DHCP Attacks
    - ARP Attacks
    - STP Attacks

Bezpečnosť sietí

Termíny a pojmy

- Zraniteľnosť (Vulnerability)
  - Slabina v sieti
    - Nezabezpečený protokol, program. chyby, slabé zásady atď.
  - Môže byť objavená a zneužitá útočníkom
- Ohrozenie/hrozba (Threat)
  - Potenciál zraniteľnosti
    - Malvér, zneužitie, ...
- Riziko (Risk)
  - Potenciál hrozby ako výsledku zneužitia zraniteľnosti
  - Pravdepodobnosť výskytu
- Potláčanie/zmierňovanie (Mitigation)
  - Opatrenia zamerané na zníženie závažnosti zraniteľnosti

- Vektor sieťového útoku
  - Cesta alebo iný spôsob, ako sa útočník snaží získať prístup
- Hrozby
  - Vonkajšie hrozby
  - Vnútorné hrozby
    - Naberá na obrátkach



Sieťová bezpečnosť

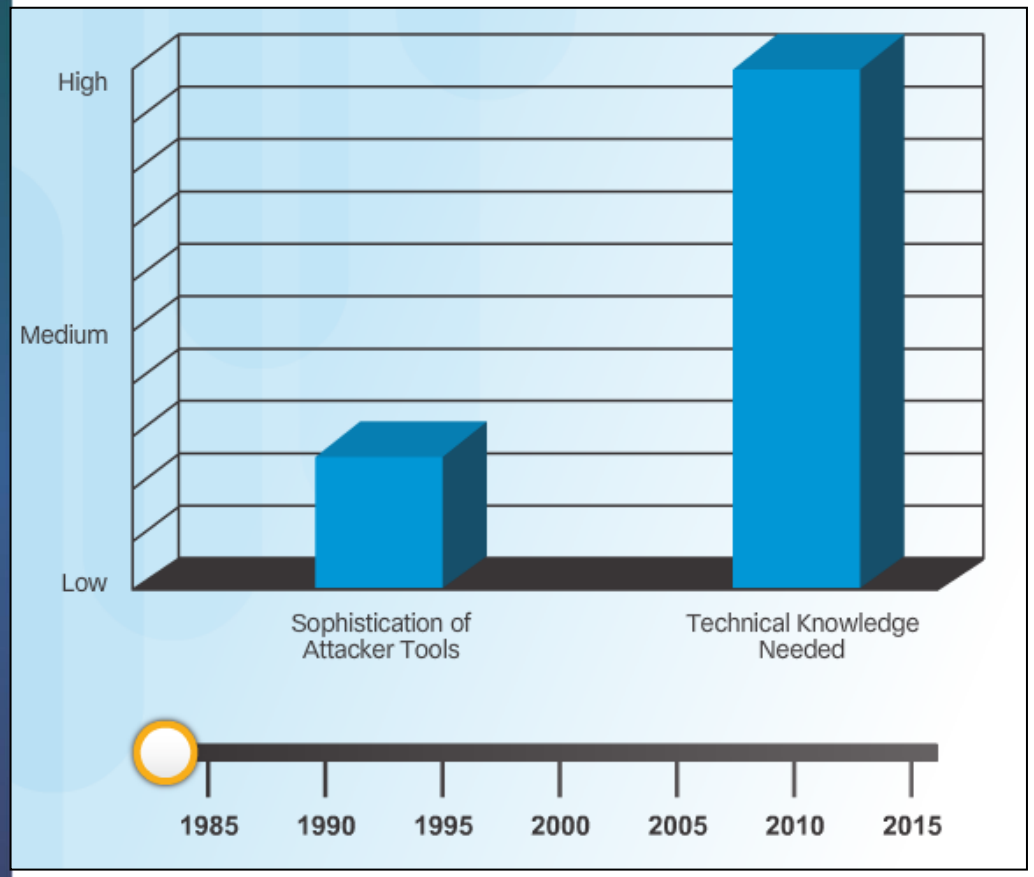
- **Zabezpečenie siete**
  - Protokoly
  - Technológie
  - Zariadenia
  - Nástroje
  - a techniky
- Sieťové útoky
  - Vírusy, červy a trójske kone, DoS / DDoS
- Zabezpečenie siete => je neoddeliteľnou súčasťou počítačových sietí
- Teraz sa rýchlo vyvíja
- => Siete sú cieľom útokov
  - „Buď o krok vpred pred hackermi“

- **Zabezpečenie sieťovej komunikácie**
  - CIA triáda
    - **Confidentiality** (dôvernosť)
      - Šifrovanie
    - **Integrity** (Integrita)
      - Hashovanie
    - **Authenticity** (Autenticita)
      - Zdieľané kľuče (PreShareKey - PSK)
        - Vrátane hashing s kľúčom
      - PKI a certifikáty

Hacker & evolúcia hacker-ov

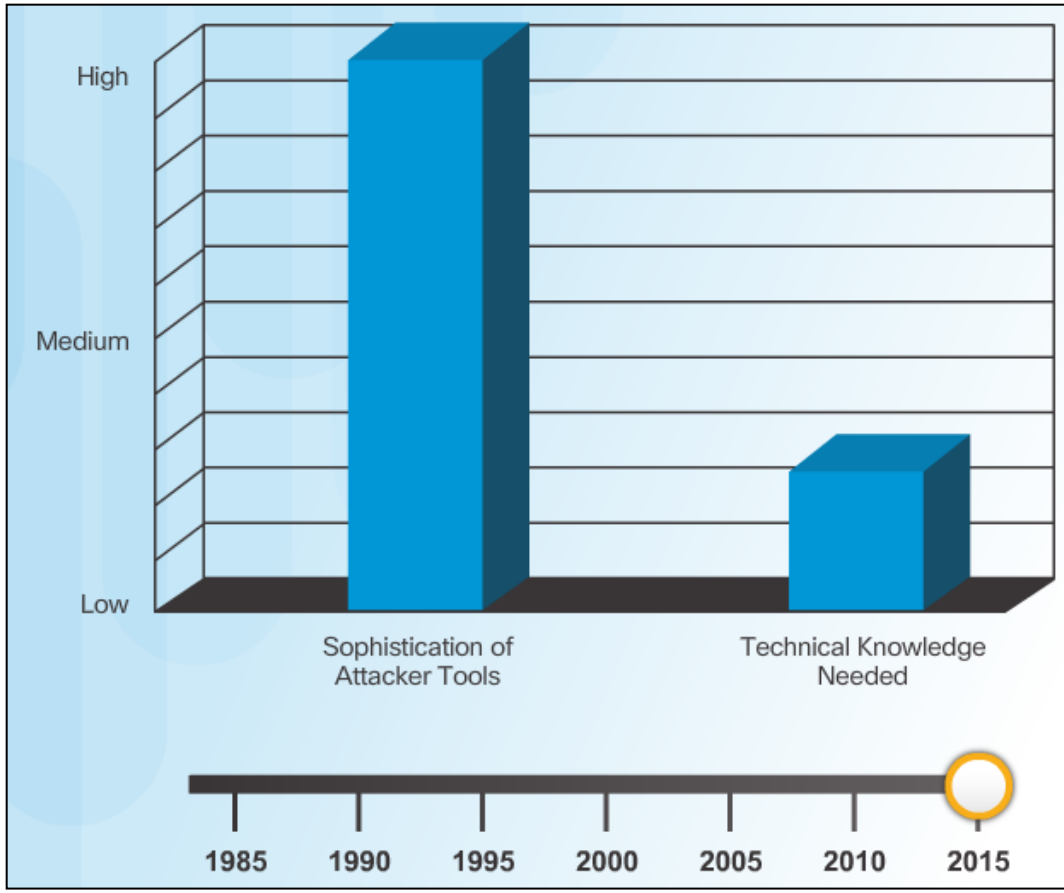
- **Hacker**
  - Teraz (žijeme v zjednodušenom svete)
    - Spravidla ide o kybernetického útočníka cez sieť
      - Využíva zraniteľné miesta
  - Predtým alebo lepšia definícia
    - Kvalifikovaný počítačový expert, ktorý využíva svoje technické znalosti na prekonanie problému
- Typy hackerov
  - **White** Hat (the good one)
    - Zručnosti v mene dobra
    - Ethical hackers, pentesters, skill testers, vulnerability researchers ☺, admins
  - **Black** Hat (the bad one)
    - Neeticky hacking
    - Hackuje pre osobný zisk alebo iných zlých dôvodov
    - Slovensky: Lotor, oplan, niktoš, galgan, paskuda., pľuha, gauner....viac slov. Ľ. Štúra)
  - **Gray** Hat (the … last one)
    - Robte neetické veci, ale nie pre zisk
  - Green, Red, Blue Hat
- Ďalšie moderné pomenovanie :
  - Script Kiddies (blue one)
    - Tínedžery or používatelia s menšími vedomosťami
    - Používajú predripravené skripy či nástroje (Kali?)
  - Vulnerability Brokers (grey)
    - Objav a nahlás
  - Hacktivists (grey)
    - Vyjadrenie prostestu(anonymous)
  - Cyber Criminals (black)
    - Operate in underground economy (Lone volwes)
      - buy, sell, and trade attack toolkits, zero day exploit code, botnet services, banking Trojans, keyloggers, private information, intellectual property, and much more.
  - Štátom sponzorovaný hacker (? ? ??)
    - Najnovší typ, veľmi pokročilý
      - Útočníci financovaní vládou (stuxnet)
    - Nie sú oficiálne priznaný

Hacker Tools



- Simpler, self made

Evolution



- Quantum of prepared tools
- Some of them very sophisticated and highly automated

Hacking operating systems /

Kali, BlackBox, Parrot Security, BlackArch, Fedora security, Network security toolkit …

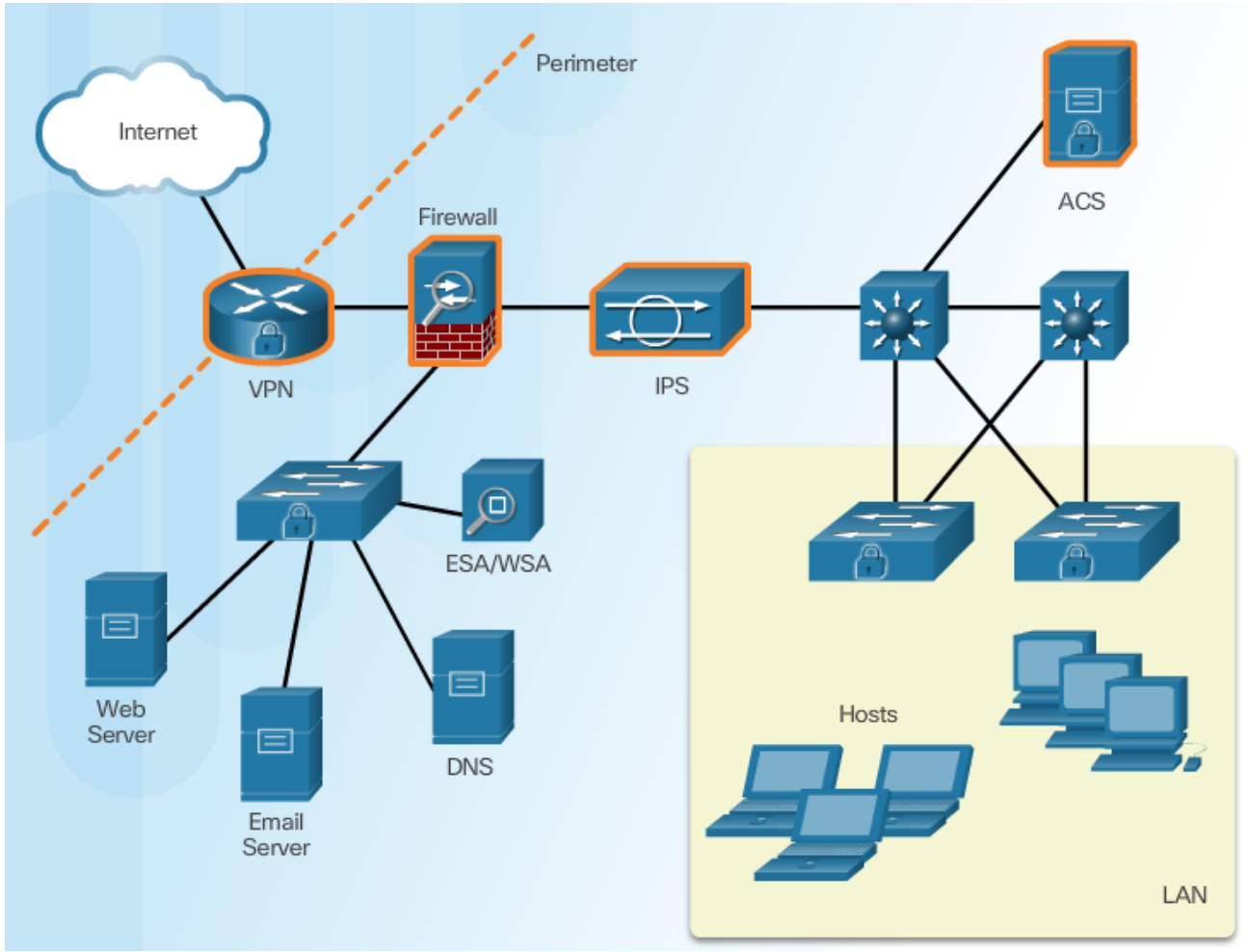
Kategórie útokov či nástrojov

- Penetration testing tools and toolkits:
  - Password crackers
    - Also called password recovery tool ☺
    - Ripper, Ophcrack, L0phtCrack, THC Hydra, Rainbow Crack, Meduse
  - Wireless hacking
    - Kismet, Aircrack-ng, KisMAC, Firesheep
  - Network scanning and hacking
    - Network probing
    - Nmap, SuperScan, Angry IP Scanner, hping3
  - Packet crafting
    - Firewall test tools, packet generators
    - Hping, scapy, Socat, Netcat, Nemesis …
  - Packet sniffers
    - Capture and analyze
    - Wireshark, tcpdump, Ettercap, Paros, Dsniff, Fiddler, EtherApe. SSLstrip …
  - Rootkit detectors
    - Directory and file integrity checkers
    - AIDE, NetFilter …
- Fuzzers to search vulnerabilities
  - Fuzzing = assurance technique used to discover coding errors and security loopholes in software, operating systems or networks
  - Fuzzer, Social Engineering Toolkit (SET), Skipfish, Wapitti, W3af, wfuzz …
- Forensic
  - computer investigation and analysis techniques in the interests of determining potential legal evidence.
  - Kit, Helix, Maltego, Encase
- Debuggers
  - Reverse engineering
  - GDB, WinDog, IDA, Imunity Debugger
- Encryption
- Vulnerability exploitation
  - Metasploit, Netsparker, Sqlmap, Core Impact
- Vulnerability Scanners
  - Network and system identity scans
  - OpenVAS, Nessus, Nipper, Secuma PSI
- … many of them *nix based

Hrozby a zabezpečenie pre koncové zariadenia

Securing LAN Elements

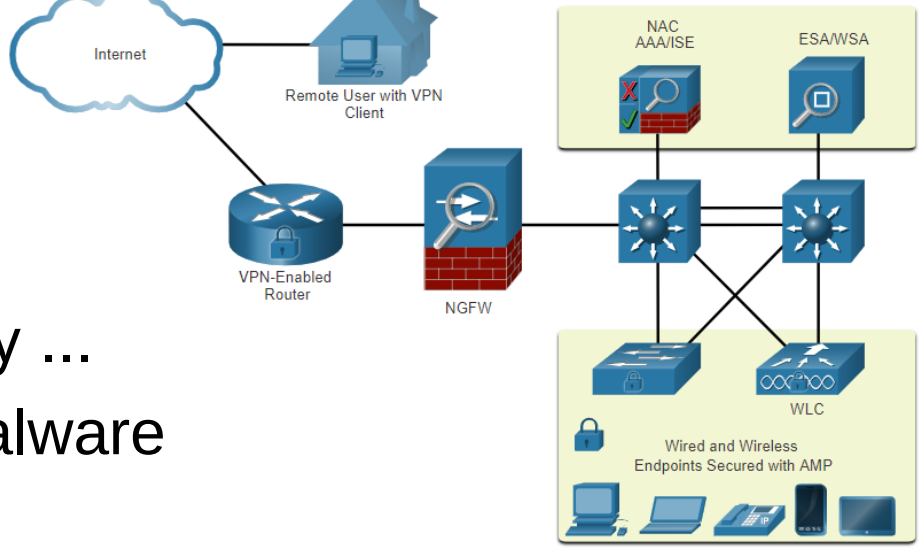
- People under a network attack usually imagine attacks from outside external networks
  - DoS/DDoS
  - Breach of organization's servers
    - Web, data, mail …
- Focus of perimeter security
  - Hardened ISR, ASA, IPS, AAA
- However, there is a need to protect against attacks from **the inside too**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



Hrozby pre koncové zariadenia (system attacks)

- Malware
  - Wiki: "*Malware or Malicious software* is *any software intentionally designed to cause damage to a computer, server, client, or computer network*"
  - Nejaké kategorizovanie
    - Virusy, Trojské kone, Červy, Rootkity, Backdoory, Ransomware, Spyware, Adware ...
- Denial of Service / Distribuovaný DoS
  - Odopretie služby, napr. DDoS
    - koordinovaný útok z viacerých zariadení nazývaných zombie s úmyslom degradovať alebo zastaviť prístup na sieť či k zdrojom
  - Ping of death, Smurf attack (zosilňovanie), TCP SYN Flood ...
- Odpočúvanie
- Získanie prístupu
- ...

Ochrana koncových systémov



- Notebooky, stolové počítače, servery a IP telefóny ...
- Útoky cez sieť a jej služby => najčastejšie cez Malware
- Ochrana => nie je jednoduchý proces
- **Ochana na KS**
  - Antivírus/antimalware
    - MS Defender, Eset, McAffee, Norton Security ...
  - Personálny firewall
    - Win, Tiny personal FW, Kerio....
  - Host-based intrusion prevention systems (HIPSs)
  - Používanie šifrovania
    - Prístup => VPN
    - Komunikácia (L3/L4 VPN, šifrované verzie proto)
    - Data => šifrovanie HDD (BitLocker ..)
- **Ochrana na sieti**
  - **Perimeter**
    - NextGen Firewall
      - Intrusion Prevention System + URL filtering + AM + AV + ďalšie techniky
    - Ochana služieb
      - Mail: email security appliance (ESA)
      - Web: web security appliance (WSA)
  - Riadenie prístupu do siete
    - Network Admission Control (NAC
      - Cisco Identity Services Engine
    - **Na prepínačoch**

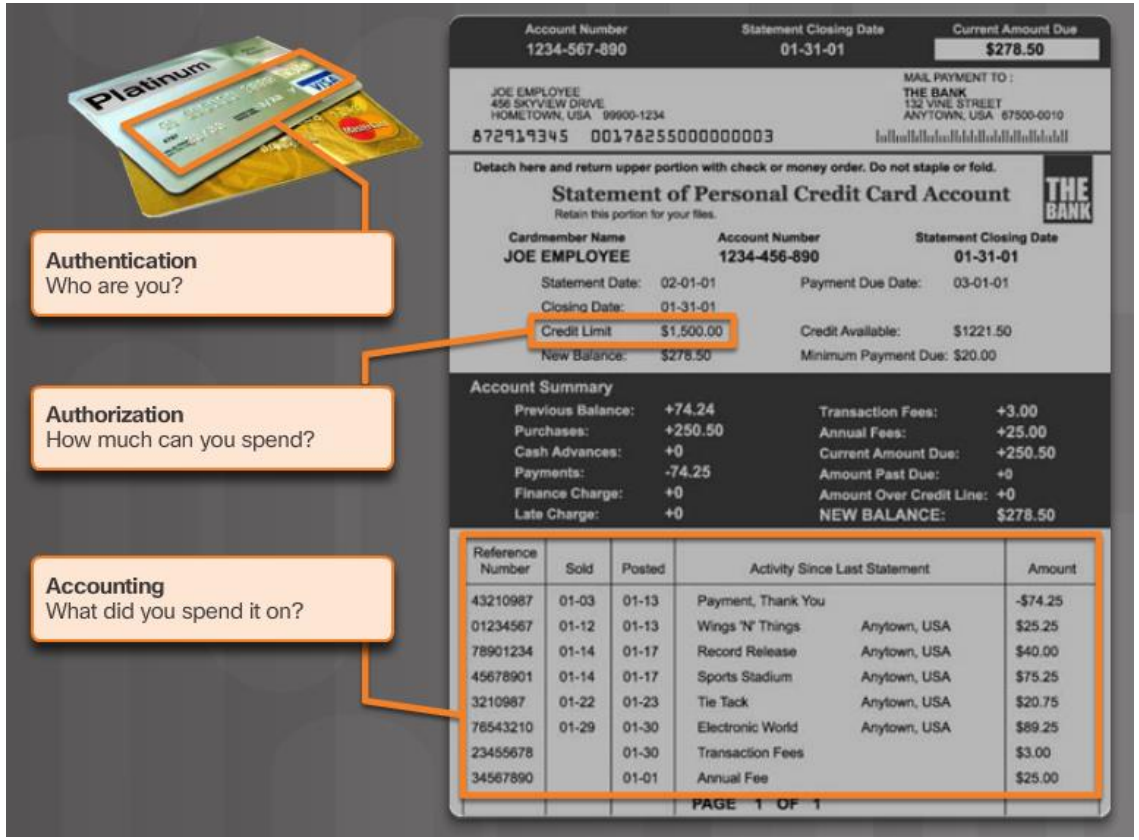
Hrozby a zabezpečenie sieťových zariadení

Sieťové zariadenia

- Smerovače, prepínače, AP, servery, ...
- Zabezpečenie
  - **Fyzická bezpečnosť**
    - Fyzické zabezpečenie zariadenia
      - Zahŕňa veci ako zabezpečená miestnosť:
        - Autorizovaný prístup, ochrana pred elektrostatickým alebo magnetickým rušením, ...
      - Hlásenie a potlačenie požiaru, teplota, vlhkosť, prašnosť...
    - Ochrana pred výpadkom
      - UPS, záložný generátor nafty
  - **Zabezpečenie operačného systému**
    - Patchovanie
      - Používaj najnovšie OS
    - Zálohovanie
      - Uschovanie kópie IOS a konfigurácií
  - **Device hardening**
    - Riadenie prístupu cez AAA
    - Použitie zabezpečených sieťových procesov
    - Vypnutie všetkých nepoužívaných služieb
    - ...

AAA overview

- Účel AAA
  - Určiť **kto** má povolené pristupovať
    - Správcovia, firemní používatelia, vzdialení používatelia, návštevníci, skupiny, obchodní partneri ..
  - **Kedy** majú dovolené pristupovať
  - A **čo môžu** robiť
- AAA je súbor mechanizmov (rámec) na autentifikáciu, autorizáciu a fakturáciu/účtovanie
  - Autentifikácia:
    - Overiť (Kto je to?)
  - Autorizácia:
    - Prideliť práva (Čo môžem urobiť?)
  - Účtovanie (výkazníctvo a audit):
    - Záznamy o používaní služieb (koľko zaplatíte, koľko použijete a čo?)
- Na zariadeniach Cisco sa AAA používa na rôzne účely
  - Administratívna kontrola prístupu (EXEC)
  - 802.1X na prepínačoch
  - WPA alebo WPA2 Enterprise na prístupových bodoch WiFi
  - PPP, IPSec…



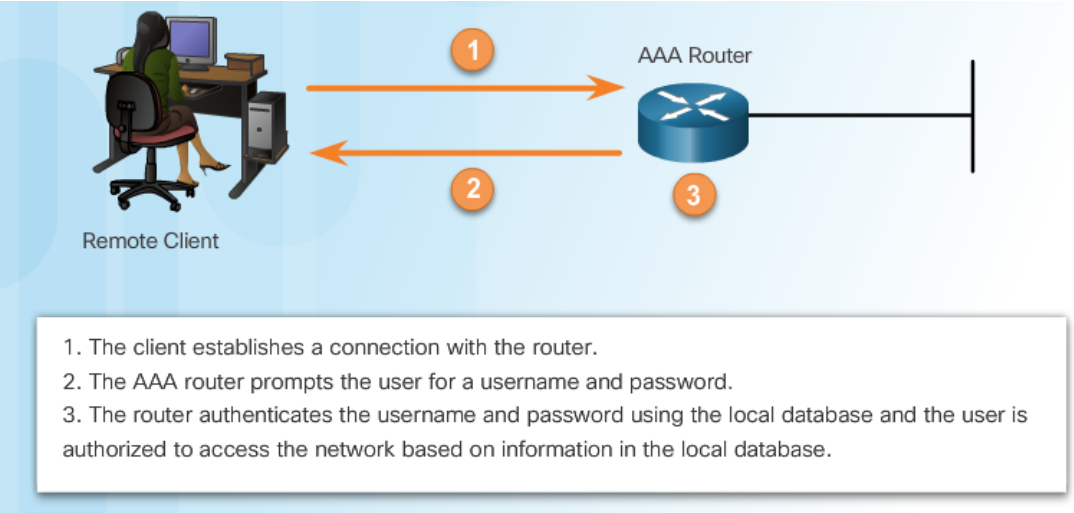
Autenitifikácia vs. Autorizácia vs Accouting

- **Autentifikácia** zaisťuje, že zariadenie alebo koncový používateľ je legitímny
  - Vieme kto to je
- **Autorizácia** umožňuje alebo zakazuje prístup autentifikovaných používateľov do určitých oblastí / programov / služieb / príkazov v sieti
  - Ak viem kto to je, určím čo a kde môže robiť
- **Accouting**
  - Vieme čo sa dialo a kto čo robil,
    - Napr. aké príkazy konfiguroval
    - Logy, záznamy

Cisco AAA modes

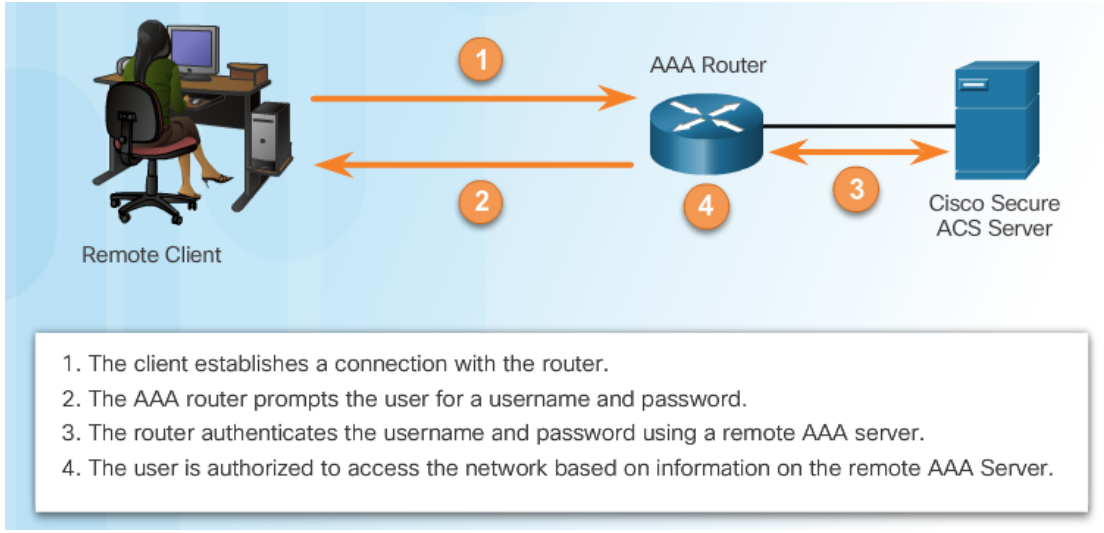
Local AAA

- Older method
- Uses a local database
  - database is the same one as required for establishing role-based CLI.
  - Stores names and passwords
- Supports authentication and authorization
- Accounting is very limited

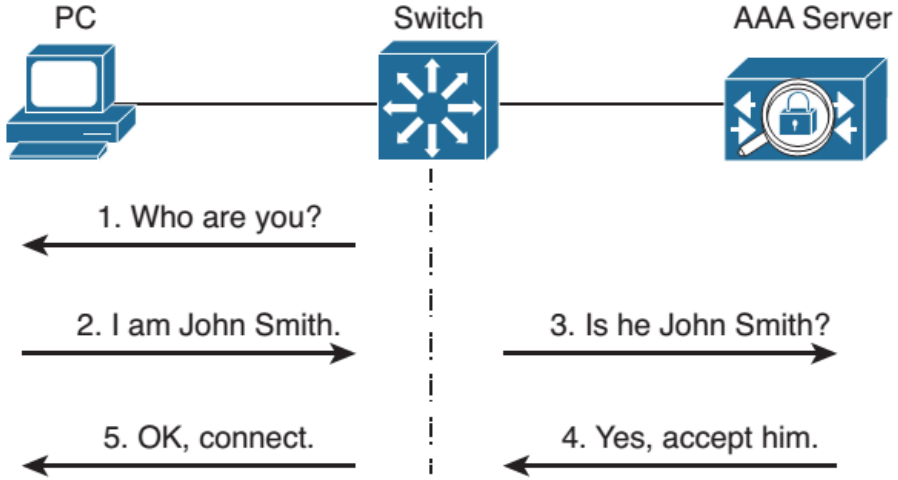


Server-Based AAA

- Newer method
- Uses a central AAA server
  - Username and passwords for authentication
  - Rights and cmds for authorization
  - Activity logging for accounting
  - For example Cisco Secure Access Control System (TACACS) or radius
- Better flexibility
  - allows different services to target AAAs to different databases



Možnosti serverovej autentifikácie a autorizácie



- **Radius (Remote Authentication Dial-In User Service)**
  - Otvorené riešenie, viaceré RFC
  - Používa UDP porty
    - IANA 1812 (auth) / 1813 (account)
    - cisco def. 1645 (auth) / 1646 (account)
  - Šifrovaná je len časť správy s heslom
  - Kombinuje autentifikáciu a autorizáciu
  - Ponúka robustné account fcie
  - Podporuje remote-access riešenia (dot1x)

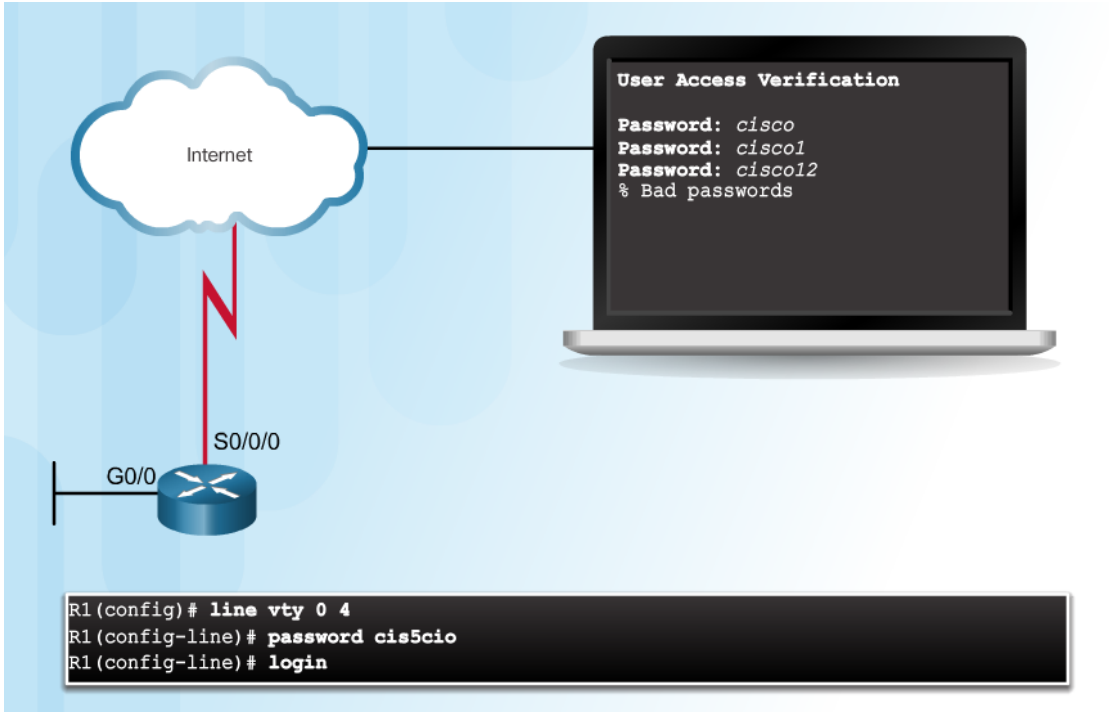
- Používané skôr v enterprise
  - Viac zariadení a adminov, či admin rolí
- Možnosti serverovej AAA - sieťové servery
  - Tacacs+ a Radius
    - Cisco Secure ACS vs. FreeRadius (MS NPS – Network Policy Server)

- **TACACS/TACACS+ (Terminal Access Controller Access Control System+)**
  - Cisco proprietárny
  - Robustné (heavy) riešenie
  - Zabezpečuje celé spojenie šifrovaním
  - Používa TCP port 49
  - Separuje autentifikáciu a autorizáciu
    - Umožňuje kombinovať rôzne metódy

Lokálna autentifikácia (už poznáme)

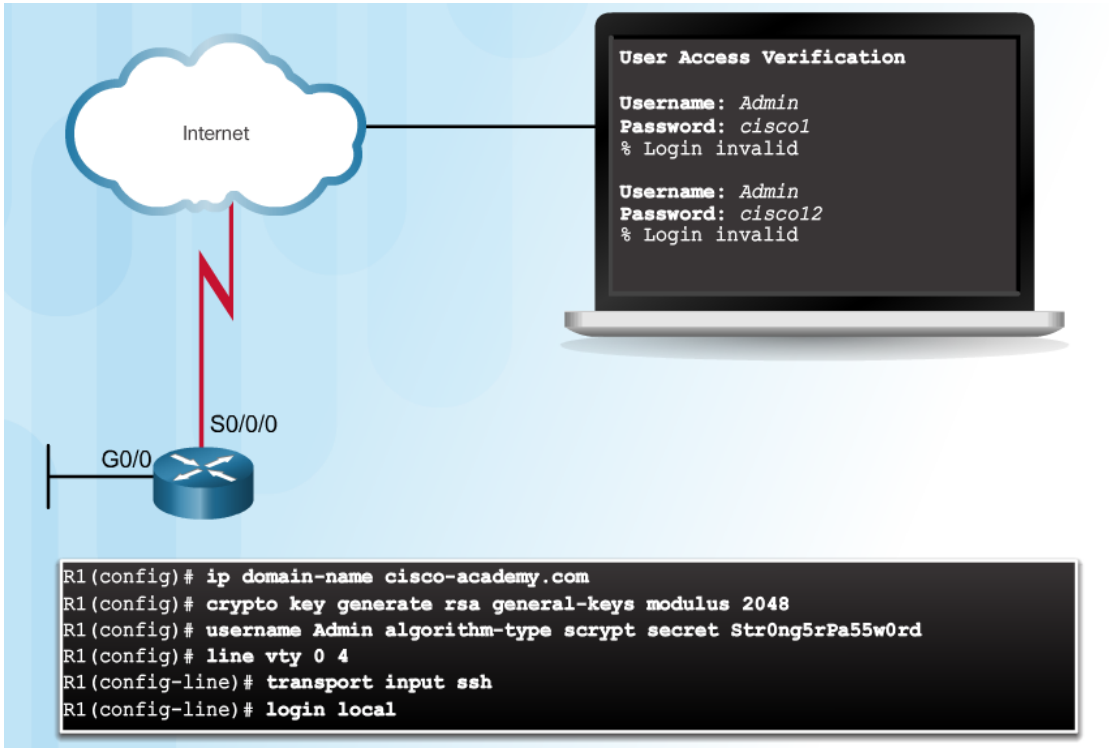
Telnet with shared pass

- Simplest method
- Must be configured on each device
- Telnet is Vulnerable to Brute-Force Attacks
- Weakest
  - No encryption,
  - No accounting
  - Shared pass



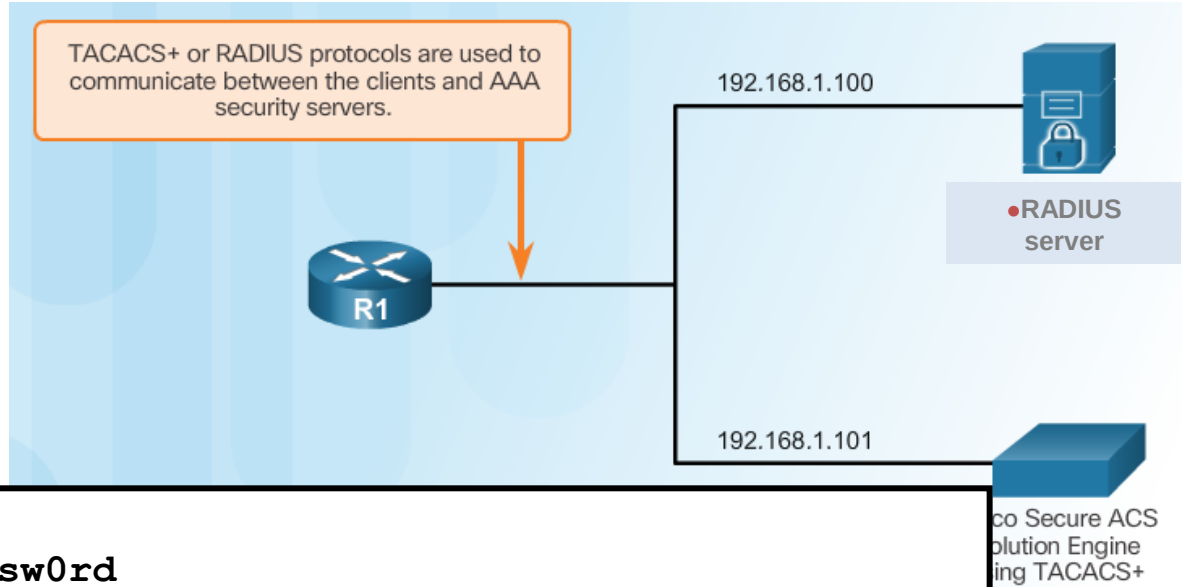
SSH using Local DB

- More secure
  - Encryption, user passwords
  - Login recording
- Must be configured on each device



Serverová autentifikácia voči TACACS+/RADIUS Serverom

Server-Based AAA Reference Topology – out of CCNA RS scope




```
Router(config)# aaa new-model
Router(config)# username lastresort password MySecretP@ssw0rd
Router(config)# radius server SERVER-R
Router(config-radius-server)# address ipv4 192.168.1.100 auth-port 1812 acct-port 1813
Router(config-radius-server)# key RADIUS-pa55w0rd
Router(config-radius-server)# exit
Router(config)# tacacs server SERVER-T
Router(config-radius-server)# address ipv4 192.168.1.101
Router(config-radius-server)# single-connection
Router(config-radius-server)# key TACACS-pa55w0rd
Router(config-radius-server)# exit
Router(config)# aaa authentication login MY_AUTH_RAD+TAC group radius group tacacs+ local-case
Router(config)# line vty 0 15
Router(config-line)# login authentication MY_AUTH_RAD+TAC
```

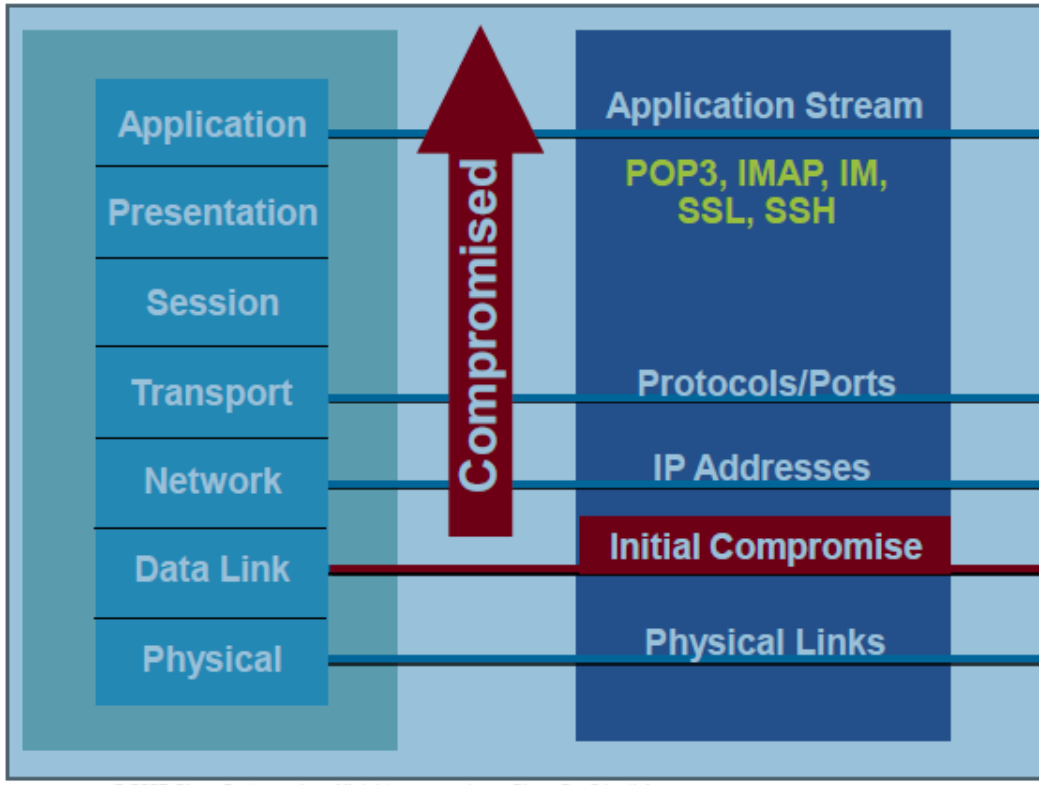
UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

Bezpečnostné útoky na L2

Vytvorené v rámci projektu KEGA 026TUKE-4/2021.

Zabezpečenie LAN infraštruktúry

- Bezpečnosť je pri klasickom 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 campuse (1)

Attack Method	Description	Steps to Mitigation
MAC Layer Attacks		
MAC Address Flooding	Frames with unique, invalid source MAC addresses flood the switch, exhausting content addressable memory (CAM) table space, disallowing new entries from valid hosts. Traffic to valid hosts is subsequently flooded out all ports.	Port security. MAC address VLAN access maps.
VLAN Attacks		
VLAN Hopping	By altering the VLAN ID on packets encapsulated for trunking, an attacking device can send or receive packets on various VLANs, bypassing Layer 3 security measures.	Tighten up trunk configurations and the negotiation state of unused ports. Place unused ports in a common VLAN.
Attacks between Devices on a Common VLAN	Devices might need protection from one another, even though they are on a common VLAN. This is especially true on service-provider segments that support devices from multiple customers.	Implement private VLANs (PVLAN).

Kategórie L2 útokov v campuse (2)

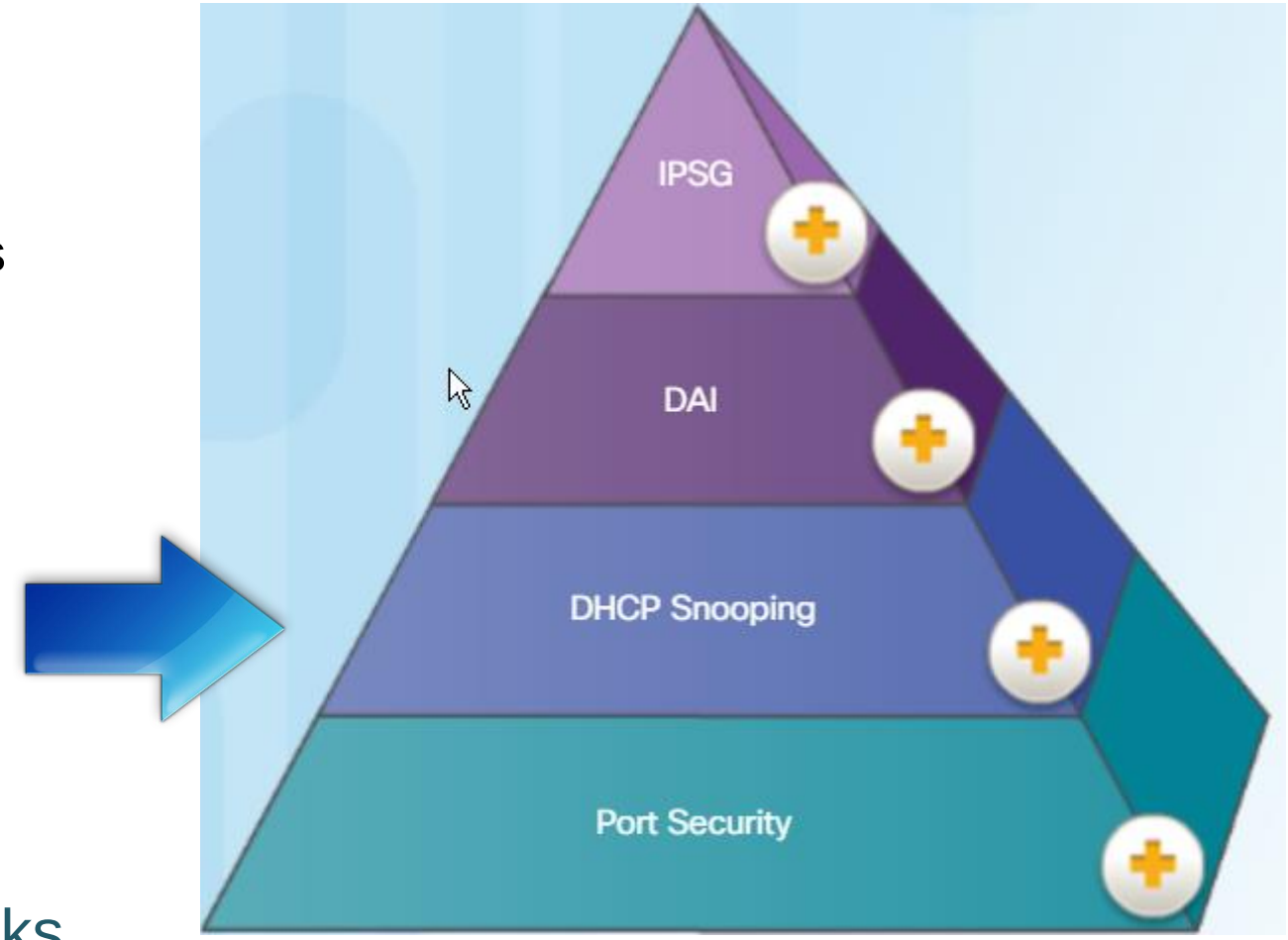
Attack Method	Description	Steps to Mitigation
Spoofing Attacks		
DHCP Starvation and DHCP Spoofing	An attacking device can exhaust the address space available to the DHCP servers for a period of time or establish itself as a DHCP server in man-in-the-middle attacks.	Use DHCP snooping.
MAC Spoofing	Attacking device spoofs the MAC address of a valid host currently in the CAM table. The switch then forwards frames destined for the valid host to the attacking device.	Use DHCP snooping, port security.
Address Resolution Protocol (ARP) Spoofing	Attacking device crafts ARP replies intended for valid hosts. The attacking device's MAC address then becomes the destination address found in the Layer 2 frames sent by the valid network device.	Use Dynamic ARP Inspection (DAI), DHCP snooping, port security.

Kategórie L2 útokov v campuse (3)

Attack Method	Description	Steps to Mitigation
STP Attacks		
Spanning-tree Compromises	Attacking device spoofs the root bridge in the STP topology. If successful, the network attacker can see a variety of frames.	Proactively configure the primary and backup root devices. Enable root, bpdu guard or filter
Switch Device Attacks		
Cisco Discovery Protocol (CDP) Manipulation	Information sent through CDP is transmitted in clear text and unauthenticated, allowing it to be captured and divulge network topology information.	Disable CDP on all ports where it is not intentionally used.
Secure Shell Protocol (SSH) and Telnet Attacks	Telnet packets can be read in clear text. SSH is an option but has security issues in version 1.	Use SSH version 2. Use Telnet with vty ACLs.

Potláčanie L2 útokov

- 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*)

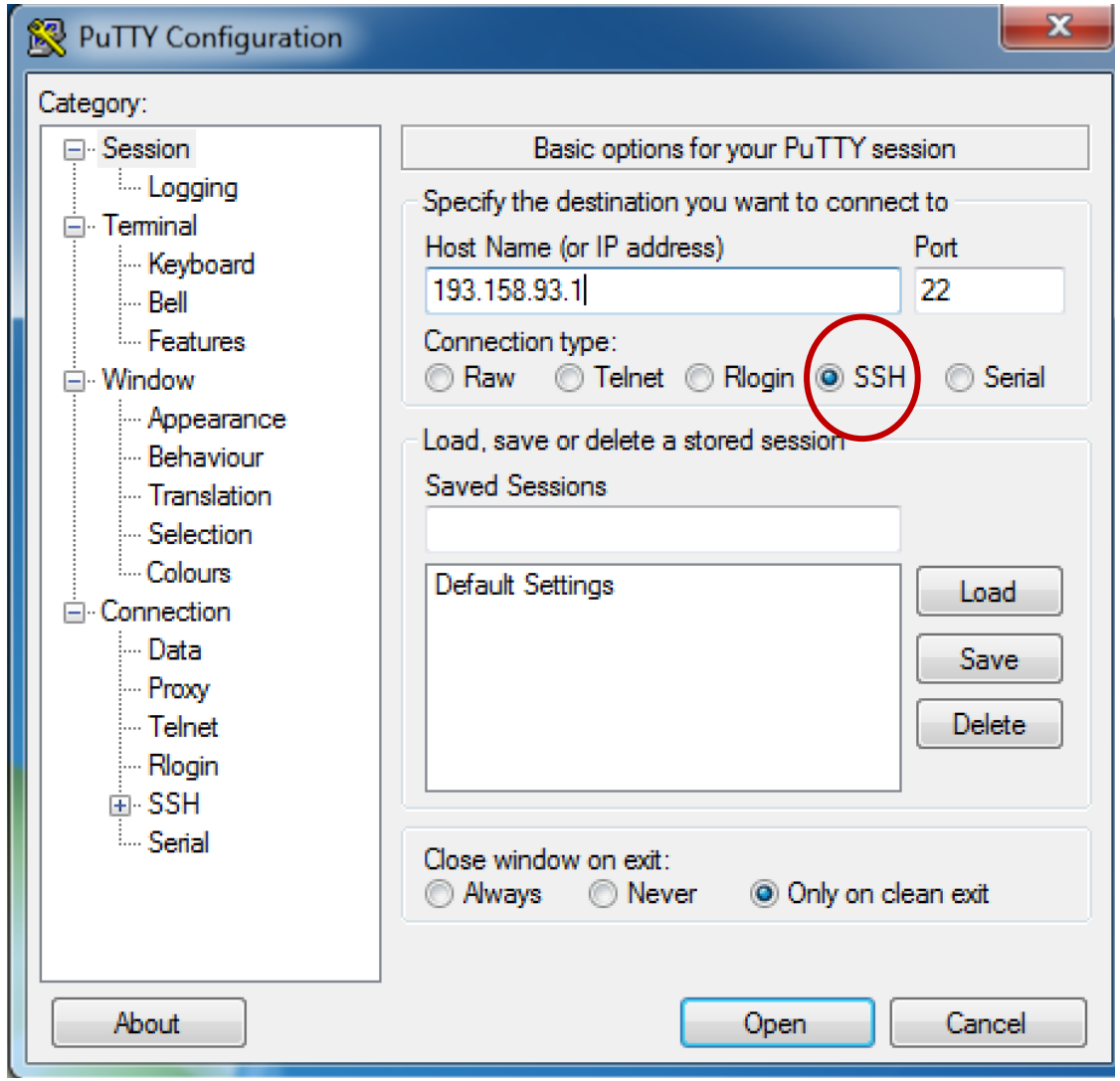


Potláčanie L2 útokov – zabezpečenie manažmentu

- **Zabezpeč heslá**
  - Nepoužívaj `enable password`
  - Použi kde sa dá `enable secret`
  - Použi šifrovanie hesiel v konfiguráku `service password-encryption`.
  - Použi externé AAA
- **Používaj system bannery**
  - Informuj a varuj neautorizovaných používateľov o následkoch
  - `banner login`
- **Zabezpeč prístup na konzolu a AUX**
  - Bez ohľadu na umiestnenie v serverovni/rack-och
- **Zabezpeč prístup na vty**
  - Vždy zabezpeč všetky vty lines daného zariadenia.
  - Filtruj prístup z IP cez ACL
- Ak sa dá zaveď out-of-band (OOB) VLAN pre manažment
- Používaj **šifrované** verzie protokolov
  - HTTPS, SSH, SSL, SCP ...
  - Použiť neštadardnú manažment VLAN ako vlan 1
  - Nastaviť ACL prep prístup

Bezpečný vzdialený prístup k prepínaču Secure Shell (SSH)

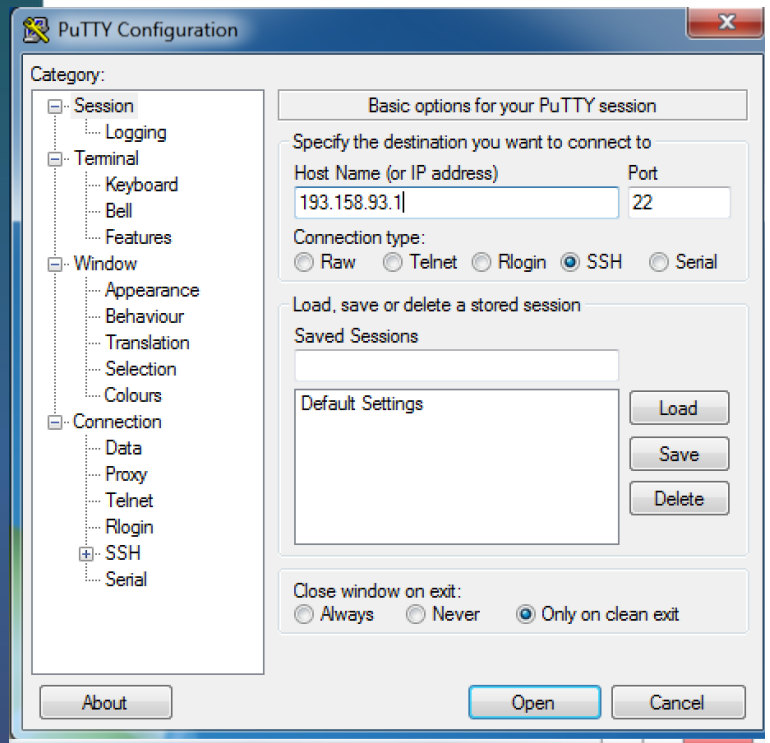
- Umožňuje šifrovaný prístup k príkazovému riadku na vzdialenom zariadení
- Bežne sa používa v UNIX systémoch
- Podporuje ho aj Cisco IOS
- Kvôli bezpečnosti ho treba vždy uprednostniť pred Telnetom
- SSH používa TCP port 22, Telnet používa TCP port 23

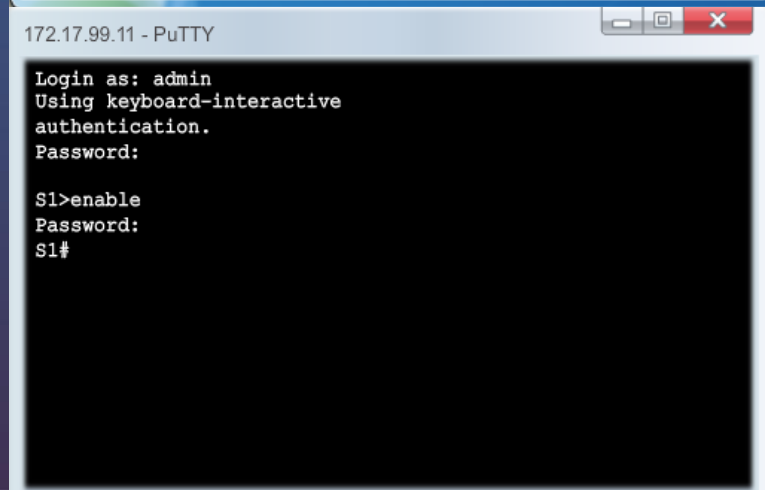


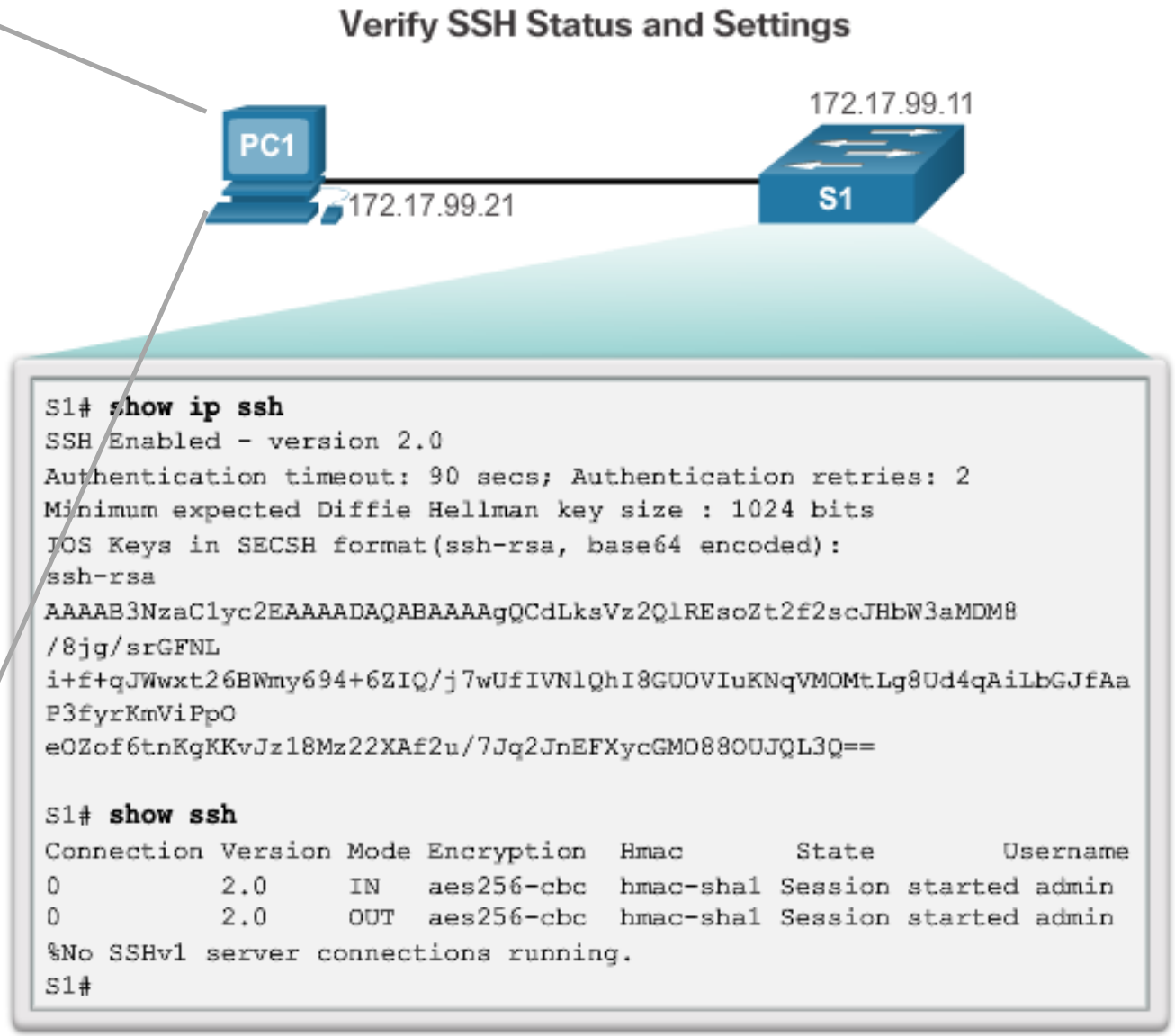
Konfigurácia IP SSH prístupu

```
Switch(config)#username Meno password Heslo
! Domena musi byt zadefinovana
Switch(config)#ip domain-name pepe.sk
Switch(config)#ip ssh version 2
*III 1 0:1:9.780:  %SSH-5-ENABLED: SSH 2 has been enabled
Switch(config)#crypto key generate rsa
The name for the keys will be: Switch.pepe.sk
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Switch(config)#line vty 0 15
Switch(config-line)#transport input ssh
Switch(config-line)#login local
! Ssh timeout v sec (doba neaktivity)
Switch(config)#ip ssh time-out 15
! Ssh login auth retries
Switch(config)#ip ssh authentication-retries 2
```

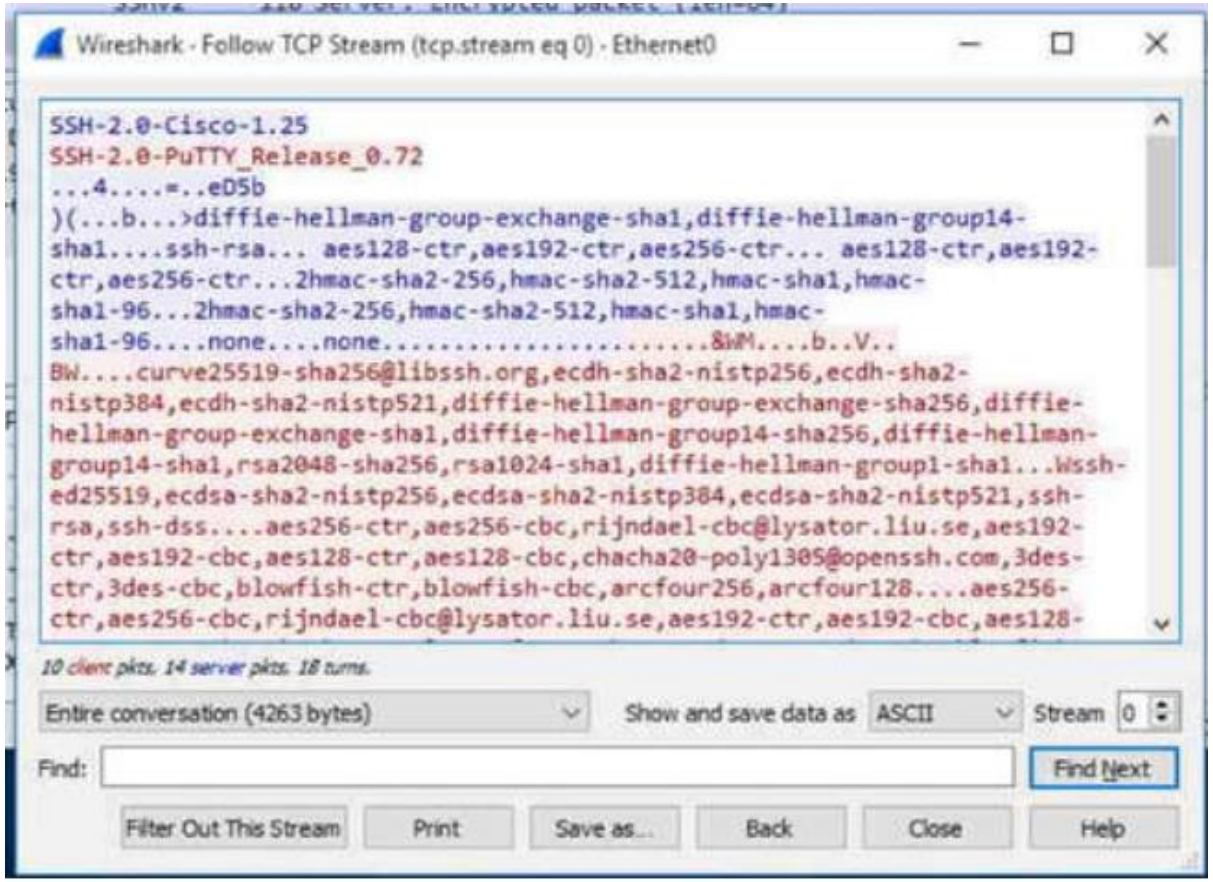
Overenie SSH





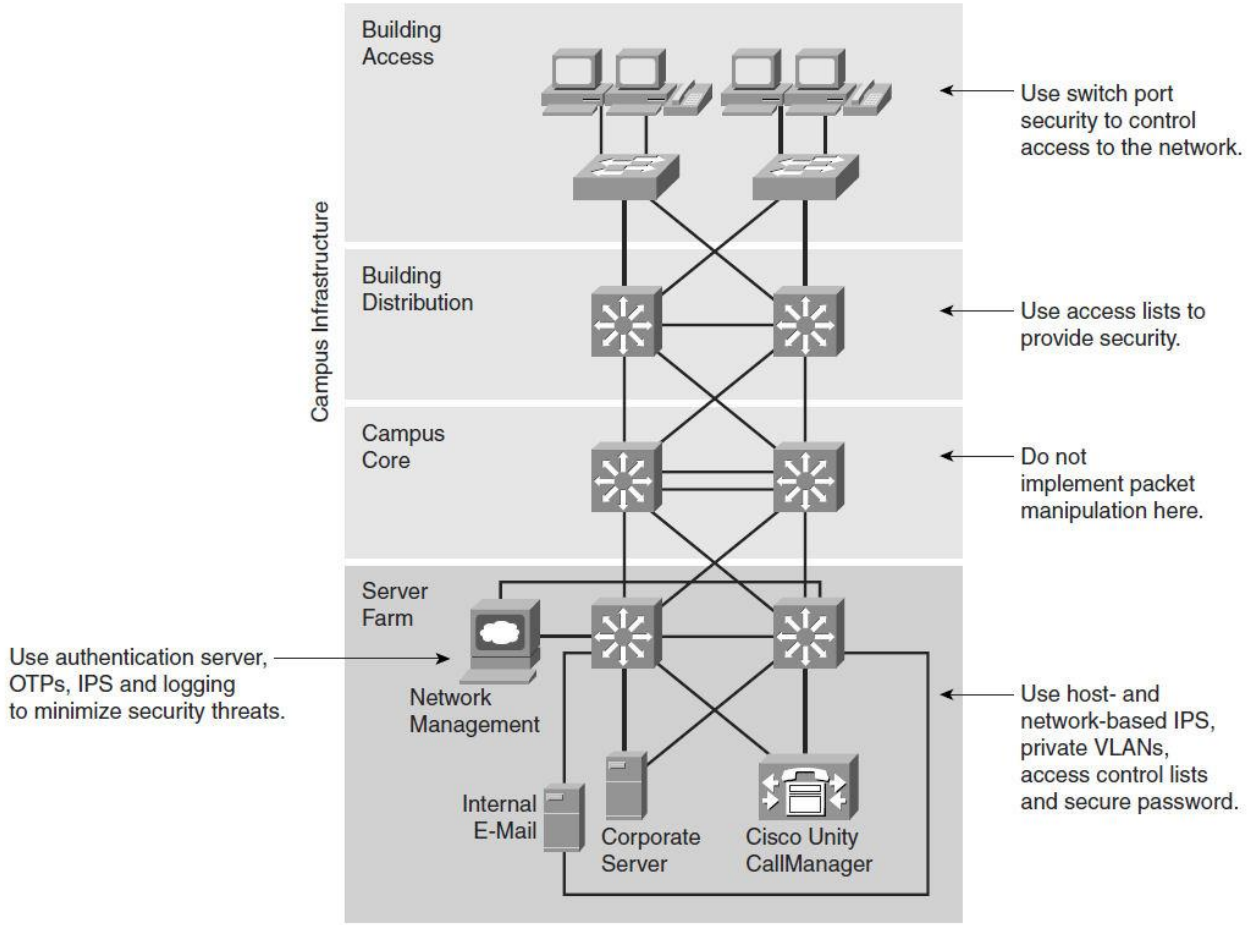


Telnet vs SSH



Zabezpečenie L2 infraštruktúry

- Core
  - Nie je vhodné implementovať bezpečnostné mechanizmy
  - Musí rýchlo spracovávať pakety/rámce
- Distribution
  - Vykonáva inter VLAN routing
  - Vhodné aplikovať packet filtering.
- **Access**
  - **Riadenie prístupu do siete na úrovni portu**
- Server farm
  - Poskytuje aplikačné služby
  - Vhodné aplikovať sieťový manažment

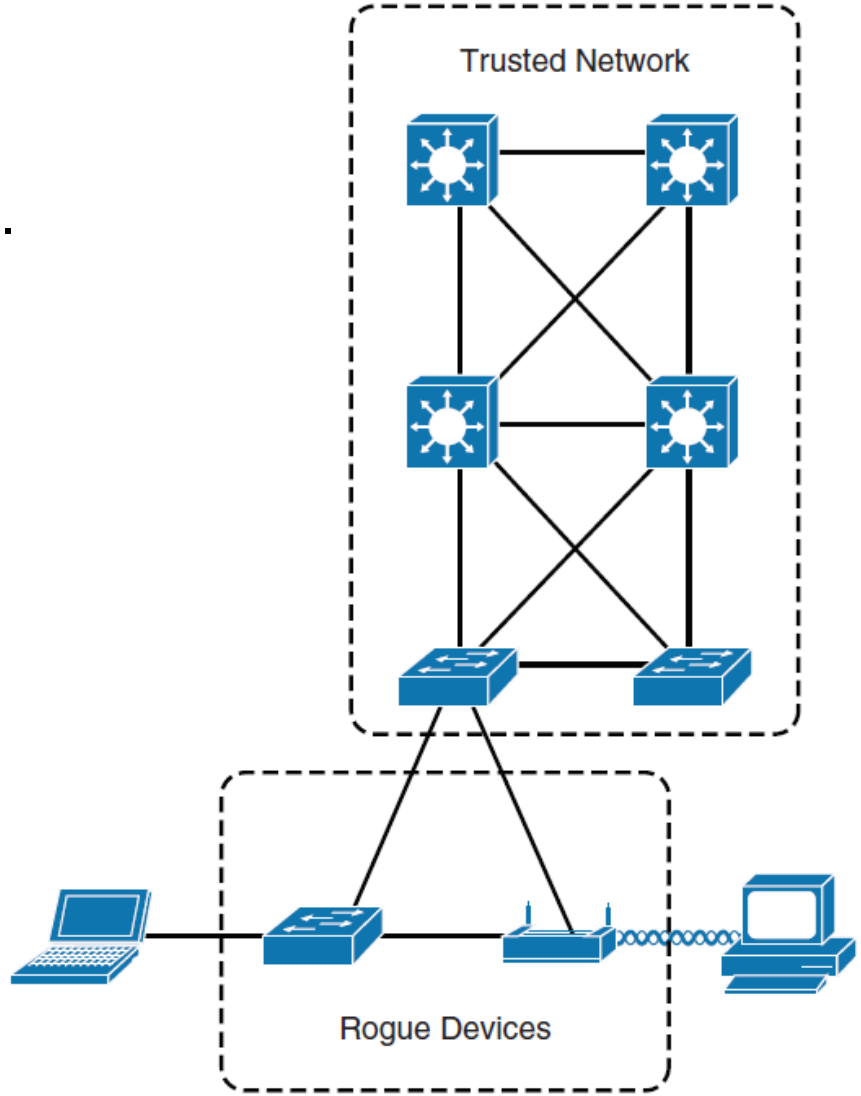


Kontrola prístupu do prepínanej siete

Port Security

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 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
    - Network Admission Control (posledný nie je predmetom tohto kurzu)
    - Port Security

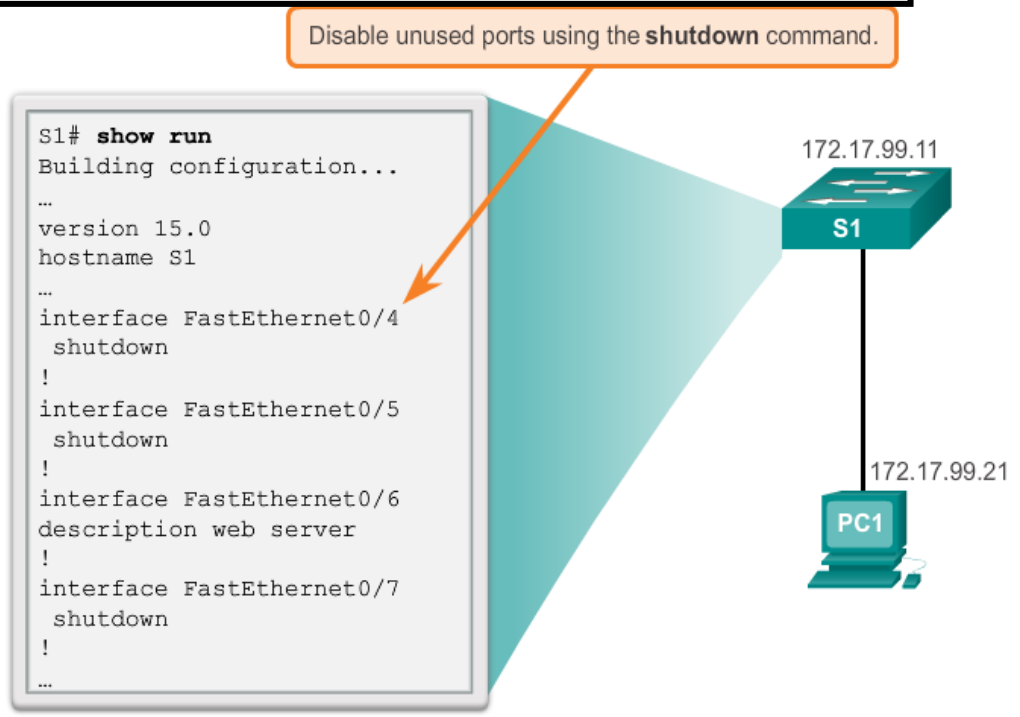


Zabezpečenie nepoužívaných portov

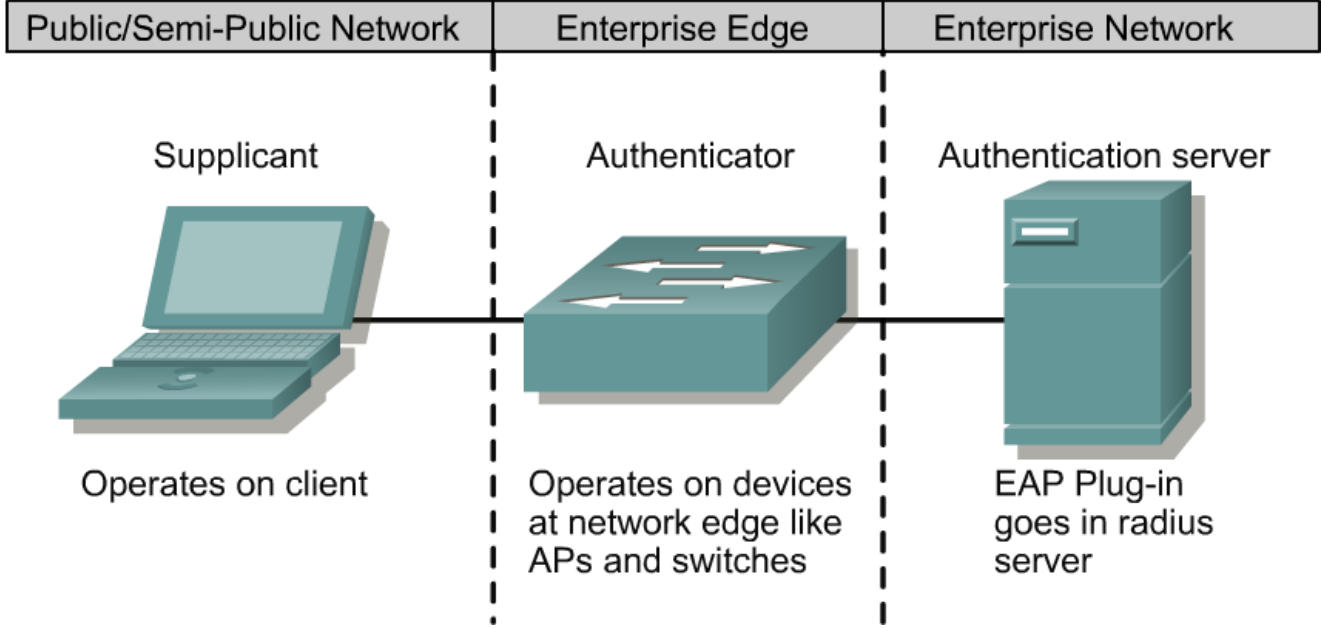
- Nepoužívané porty
  - Vypnúť => jednoduché a efektívne
    - Oplatí sa CMD

```
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

802.1X authentication components

- 802.1X Authentication uses several supporting components and protocols:
  - **Supplicant (Client):** Software client on PC, responsible for uploading client' authentication data
  - **Authenticator**: The device, to which PC connects and which requires the client to authenticate correctly (switch, AP)
  - **Authentication Server:** Contains user information database. Confirms client identity (TACACS / Radius server)
  - **Extensible Authentication Protocol (EAP**): A generic protocol for transmitting authentication information, specified in RFC 3748
  - **RADIUS**: authentication communication protocol used between a Network Access Server (or authenticator) and an authentication server
    - specified in RFC 2865. RADIUS and EAP cooperation in RFC 3579
  - **802.1X**: IEEE standard for Port-Based Authentication using EAP messages over Ethernet frameworks (EAP over LAN = EAPOL) and RADIUS protocol

Útoky na CAM/MAC tabuľku a ochrana

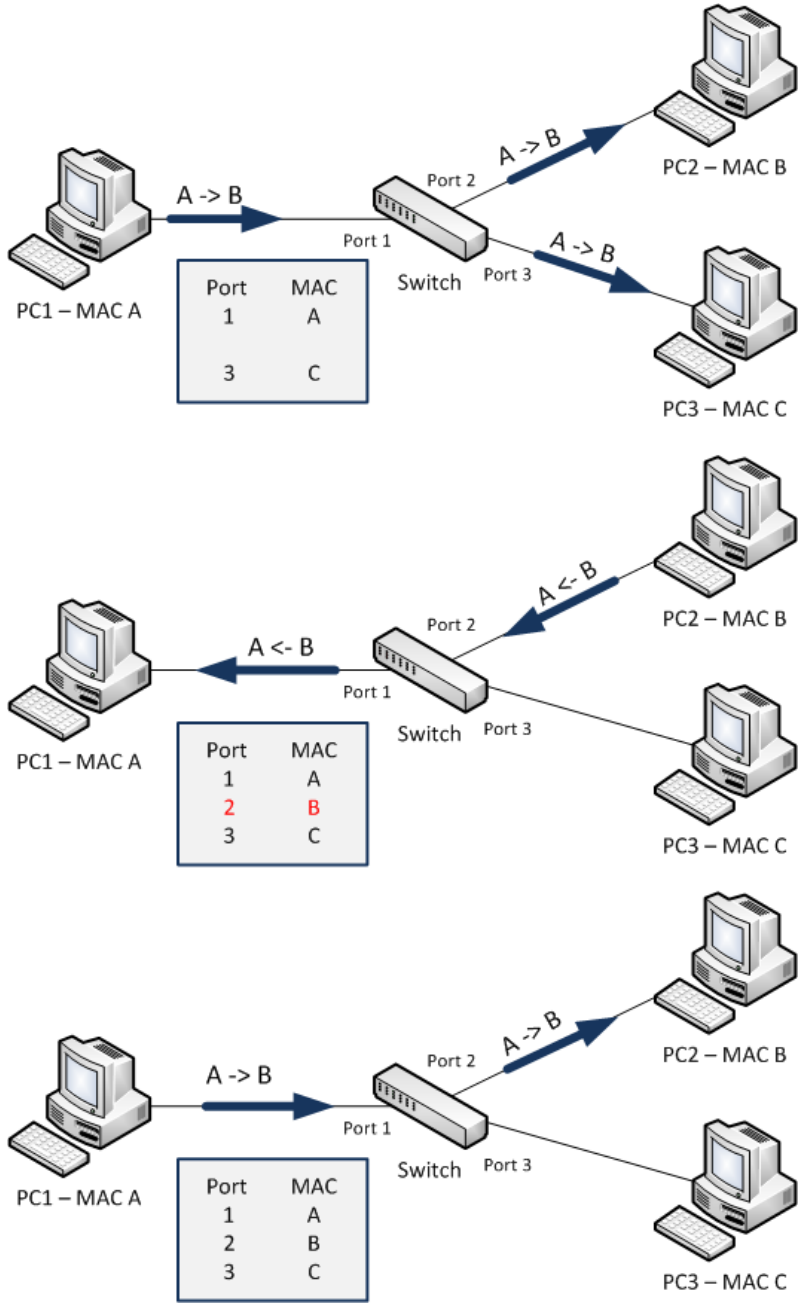
Budovanie a zobrazenie MAC tabuľky

- Prepínače sa dynamicky učia o výskyte MAC adries na svojich rozhraniach
  - Položky sa automaticky nulujú po 300 sekundách
- Zobrazenie MAC (CAM) tabuľky

```
S1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
S1#
```

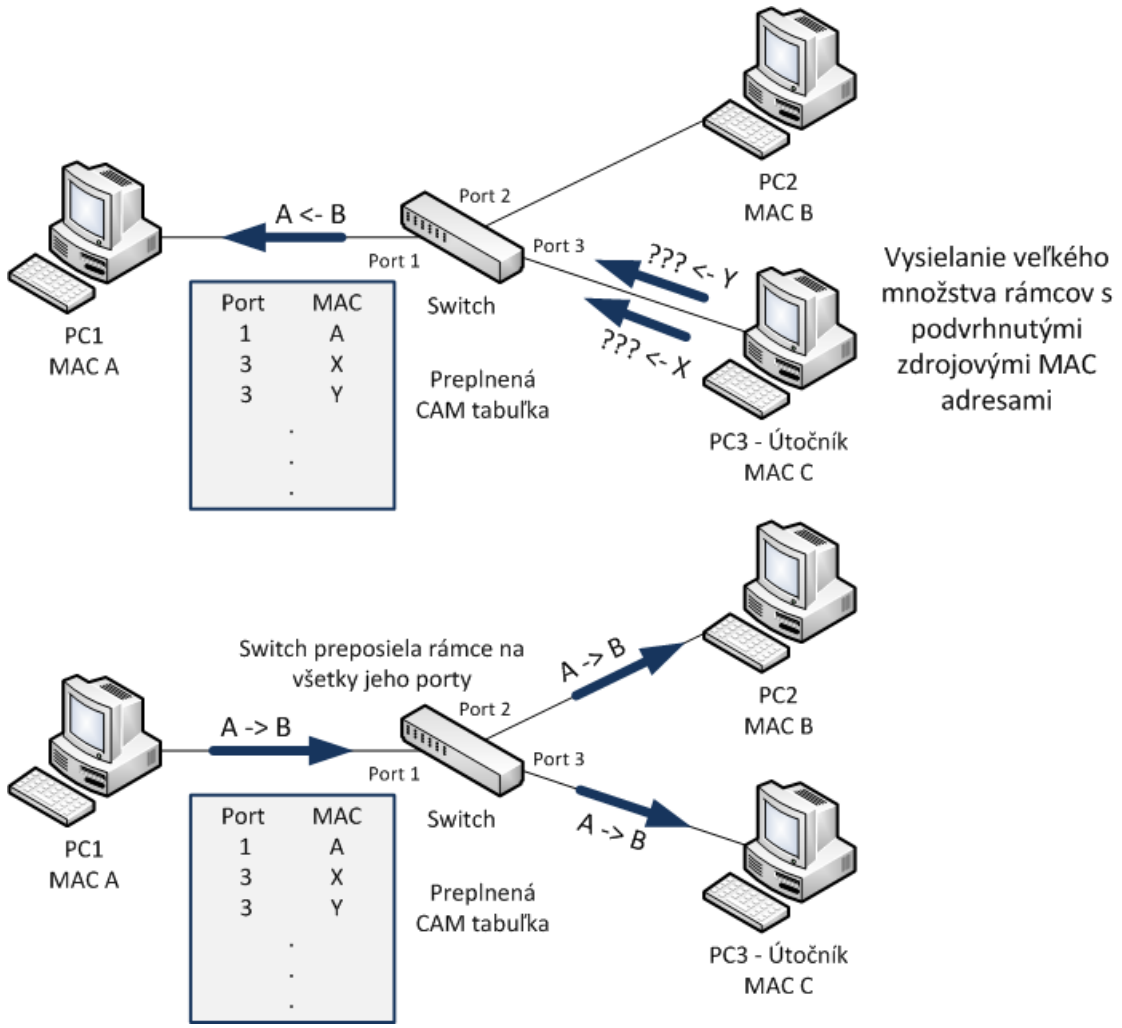
CAM činnosť - Hrozba

- Bežný postup učenia sa L2 prepínača – Budovanie CAM
- Hrozba
  - Veľkosť CAM tabuľky a početnosť položiek v nej je obmedzená



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



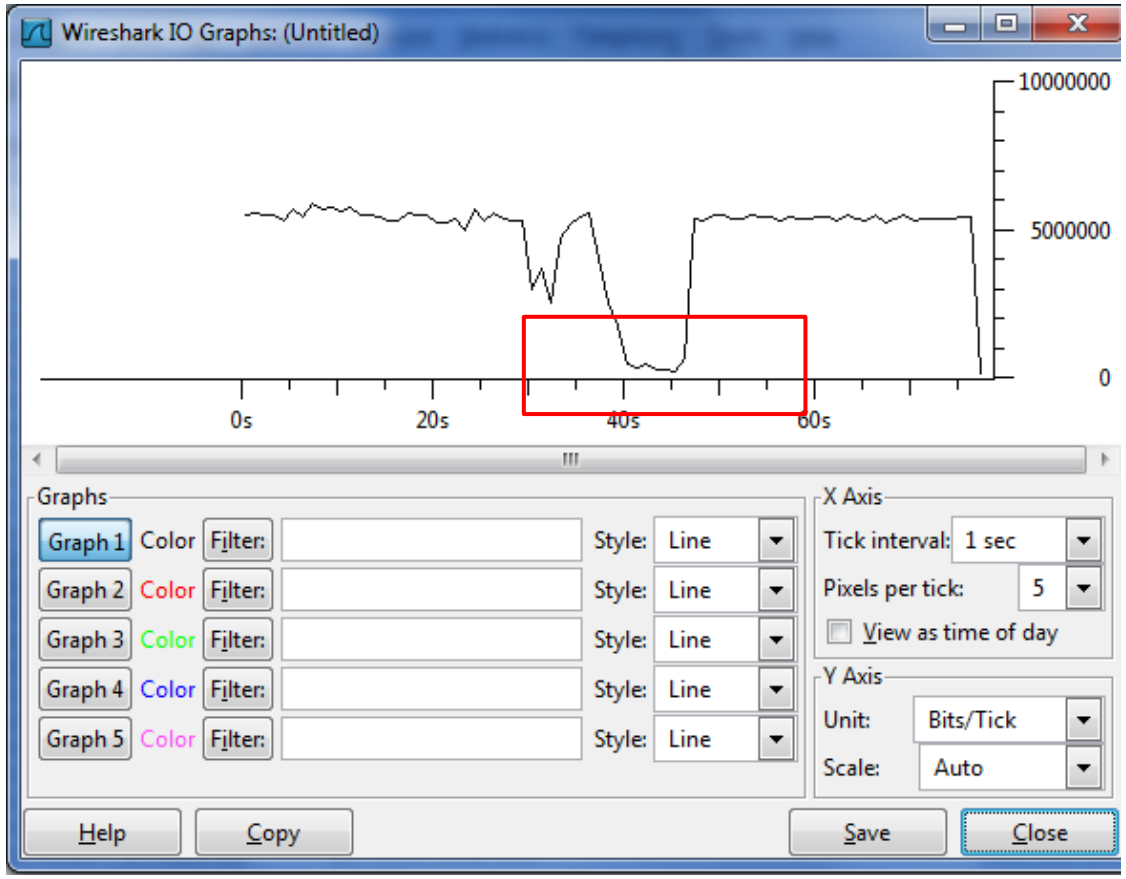
Realizácia - macof

- Príkaz

  macof –i eth0

- Agresívnejší režim (výpis do dev/null)

  macof –i eth0 2>/dev/null




```
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
```

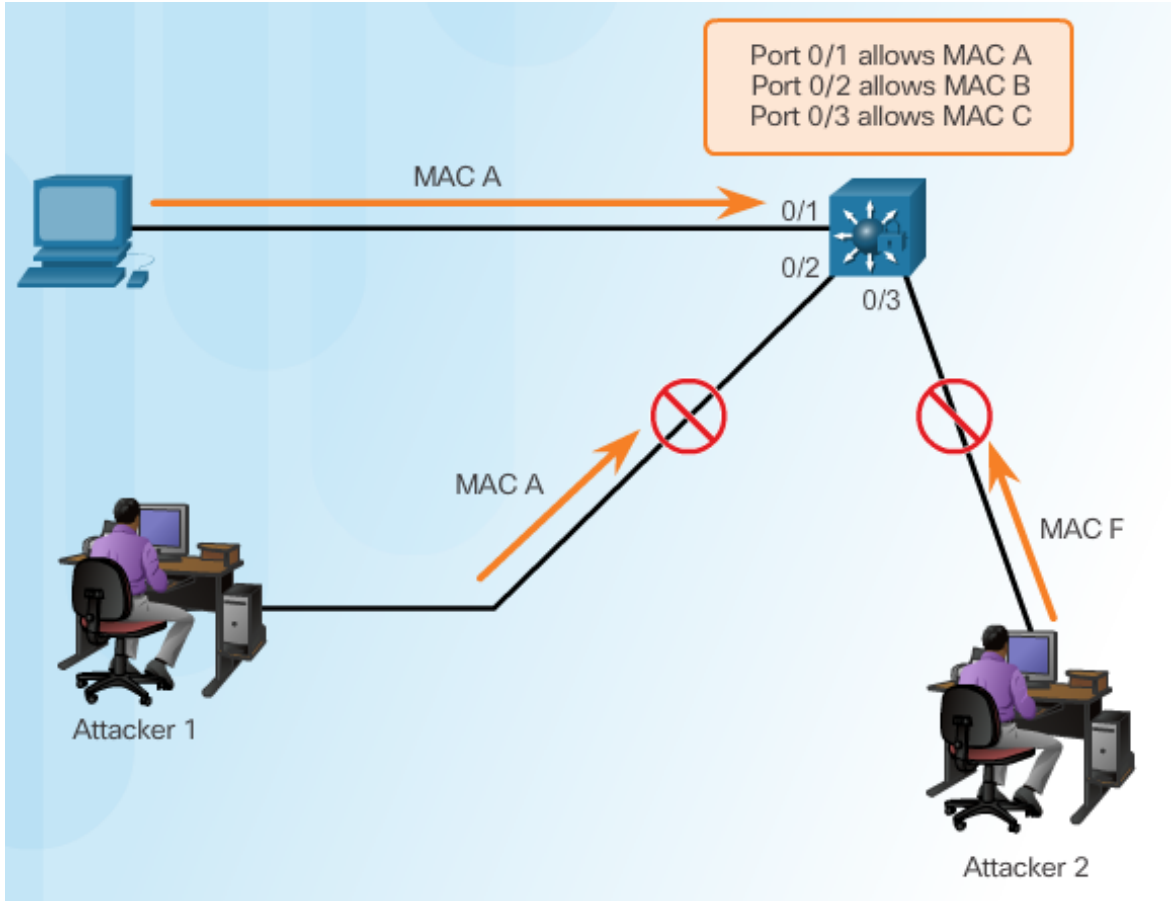
After Macof

```
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

- Funkcia Port Security umožňuje na porte
  - Obmedziť počet zariadení, ktoré môžu byť pripojené k jednému rozhraniu prepínača
    - Definovaním maxima MAC adries vyskytujúcich sa na porte
  - Definovať zoznam bezpečných MAC adries staníc, ktoré smú byť pripojené k danému rozhraniu prepínača
    - Uviesť kto je bezpečný
    - Alebo nechať rozhodnúť prepínač
  - Definovať, čo sa stane, ak dôjde k porušeniu niektorého z týchto bezpečnostných pravidiel
    - Tzv. violation
    - Stanica, ktorej MAC nie je v zozname bude „nejako“ obmedzená



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

Ktoré MAC adresy sú bezpečné?

- Bezpečné adresy môžu byť troch druhov:
  - Static secure MAC:
    - manuálne nakonfigurovaná adresa
    - Nachádza sa v konfigurácii aj v CAM tabuľke
    - Po reštarte prepínača sa opätovne načíta z uloženej konfigurácie
  - Dynamic secure MAC (dynamic learning):
    - dynamicky získaná adresa z CAM
    - Nachádza sa len v CAM tabuľke
    - Po odpojení portu alebo reštarte prepínača sa stráca
  - Sticky secure MAC (sticky learning):
    - hybrid medzi statickou a dynamickou adresou
    - Získava sa dynamicky, no prepínač automaticky vygeneruje záznam do bežiacej konfigurácie
    - Nachádza sa v konfigurácii aj v CAM tabuľke
    - Po reštarte prepínača sa opätovne načíta z uloženej konfigurácie
- Default je Dynamic

Koľko MAC adries môže byť bezpečných?

- Na porte možné definovať maximálny počet bezpečných adries
  - Statické adresy sa započítavajú do počtu bezpečných adries
  - Prepínač automaticky pridá každú novú neznámu MAC adresu do zoznamu bezpečných adries ako dynamickú, resp. sticky
  - Ak by sa však pridaním novej adresy prekročil maximálny počet bezpečných adries, nastáva tzv. porušenie bezpečnosti (security violation)
- Default je JEDNA

Čo robiť pri prekročení počtu?

- Reakcia na porušenie => **Violation Modes**
- Na bezpečnostné porušenie možno zareagovať trojakým spôsobom
  - Protect: rámec s nepovolenou MAC adresou sa zahodí
  - Restrict: rámec s nepovolenou MAC adresou sa zahodí a zároveň sa incident zaznamená (hláška na konzolu, syslog, SNMP trap...)
  - Shutdown: port sa pri prijatí rámca s nepovolenou MAC adresou automaticky uvedie do stavu err-disabled
- Default je SHUTDOWN

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

- Port Security sa konfiguruje individuálne na prepínaných portoch
- Odporúčaný postup:
  - Port nastaviť do režimu „access“ alebo „trunk“
    - Nevyhnutné – Port Security nie je podporovaná na dynamických portoch
  - Nastaviť maximálny povolený počet MAC adries
    - Nepovinné, predvolený počet je 1
  - Definovať statické bezpečné adresy, prípadne sticky learning
    - Nepovinné, default je dynamic learning
  - Určiť reakciu pri porušení bezpečnosti
    - Nepovinné, predvolená reakcia je shutdown
  - Určiť spôsob expirácie bezpečných adries
    - Nepovinné. Bez dodatočného nastavenia statické a sticky adresy neexpirujú vôbec, dynamické expirujú až pri odpojení portu
  - Aktivovať port security
    - Nevyhnutné a často prehliadnuté!

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
```

.... overenie ....

```
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 Aging

- Nastavuje čas trvania záznamu pre statické a dynamické zabezpečené adresy na porte
  - **Absolute**
    - Zabezpečená adresa sa odstráni po uplynutí časovača starnutia
  - **Inactivity**
    - Zabezpečená adresa sa odstráni po čase nečinnosti

```
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.

Porty v stave „Error Disabled“

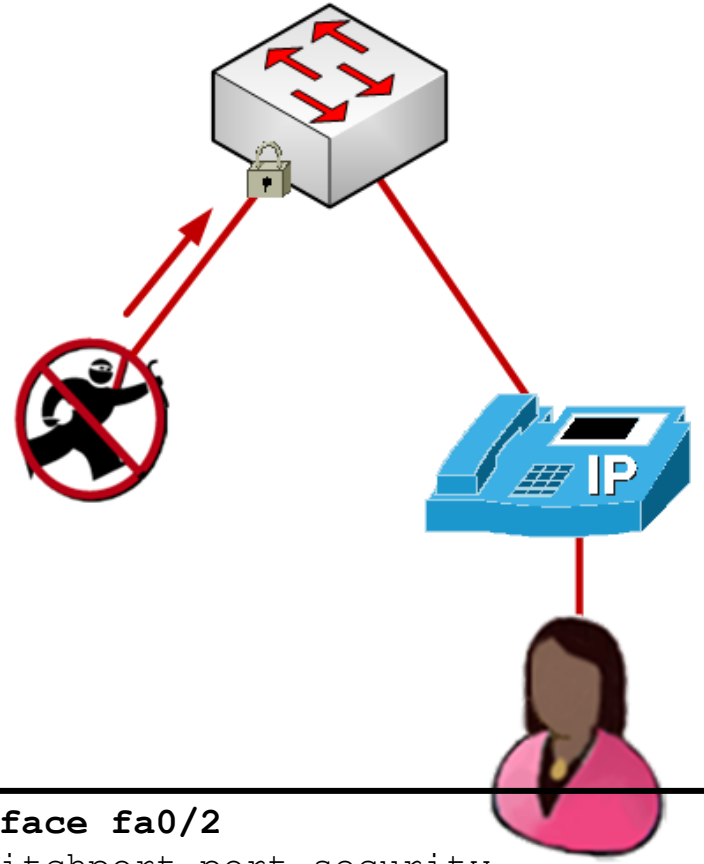
- Error Disabled => keď je na porte nastavená akcia pri narušení na shutdown a narušenie nastane
  - Port je vtedy v skutočnosti shutdown-utý
  - Prepínač túto zmenu oznámi cez konzolové správy
- Aktivácia portu
  - `shutdown + no shutdown`

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to down
```

```
S1# show interface fa0/18 status
Port Name   Status         Vlan   Duplex   Speed    Type
Fa0/18      err-disabled   1      auto     auto     10/100BaseTX

S1# show port-security interface fastethernet 0/18
Port Security                 : Enabled
Port Status                   : Secure-shutdown
Violation Mode                : Shutdown
Aging Time                    : 0 mins
Aging Type                    : Absolute
SecureStatic Address Aging    : Disabled
Maximum MAC Addresses         : 1
Total MAC Addresses           : 0
Configured MAC Addresses      : 0
Sticky MAC Addresses          : 0
Last Source Address:Vlan      : 000c.292b.4c75:1
Security Violation Count      : 1
```

Port security s VoIP

- VoIP telefóny môžu používať 2 až 3 MAC adresy
  - Podľa HW
  - Ak používajú CDP tak tri
  - Ak nepoužívajú CDP tak dve
- Zváž akciu pri porušení na
  - Vhodné Restrict
  - Akceptovateľné shutdown (podľa politík)
- Cieľom nie je riadiť prístup ale ochrániť službu a prepínač

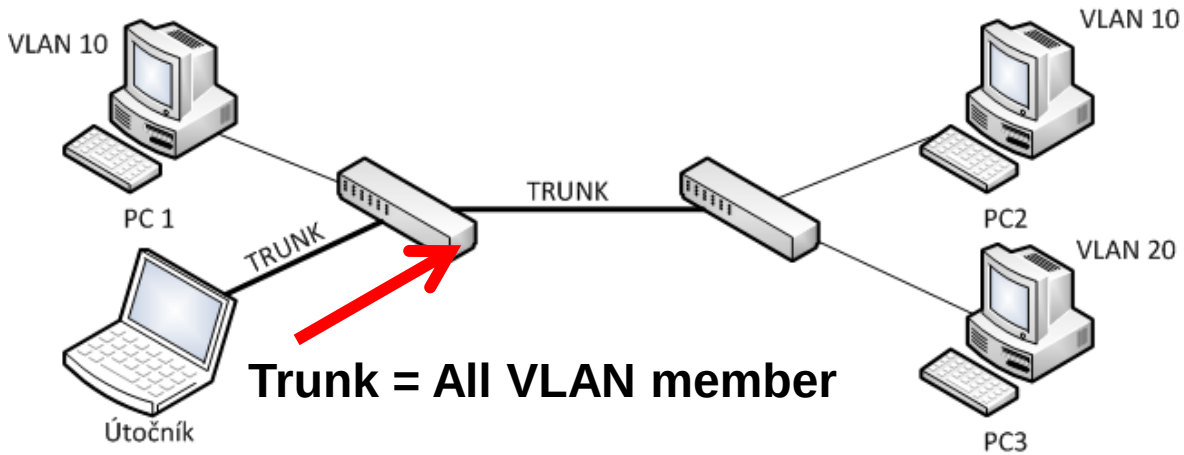



```
Sw(config)# interface fa0/2
Sw(config-if)# switchport port-security
Sw(config-if)# switchport port-security maximum 3
Sw(config-if)#

! 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
```

Útoky na VLAN / Ochrana a potláčanie

VLAN Hopping

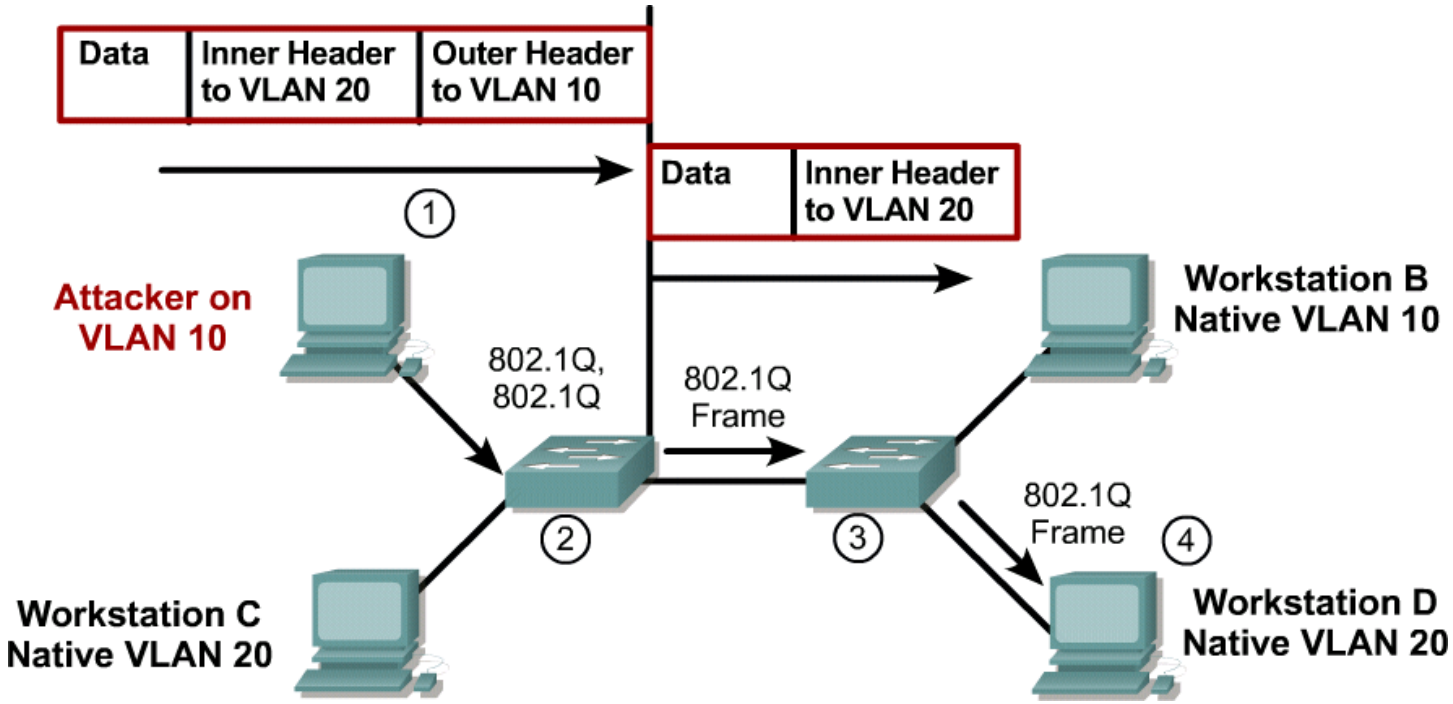
- Existuje niekoľko druhov útokov, ktoré sa snažia spôsobiť, aby rámec zo stanice v istej VLAN „pretiekol“ do inej VLAN
  - Nie vždy sa očakáva návrat (t.j. musí existovať cesta nazad)
  - To však nie je nutne problém – napr. pri TCP SYN Flood Attack
- Dva najbežnejšie vektory útoku:
  - **Útok na DTP**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



  - **Dvojité značkovanie pri 802.1Q** (Double tagging)

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



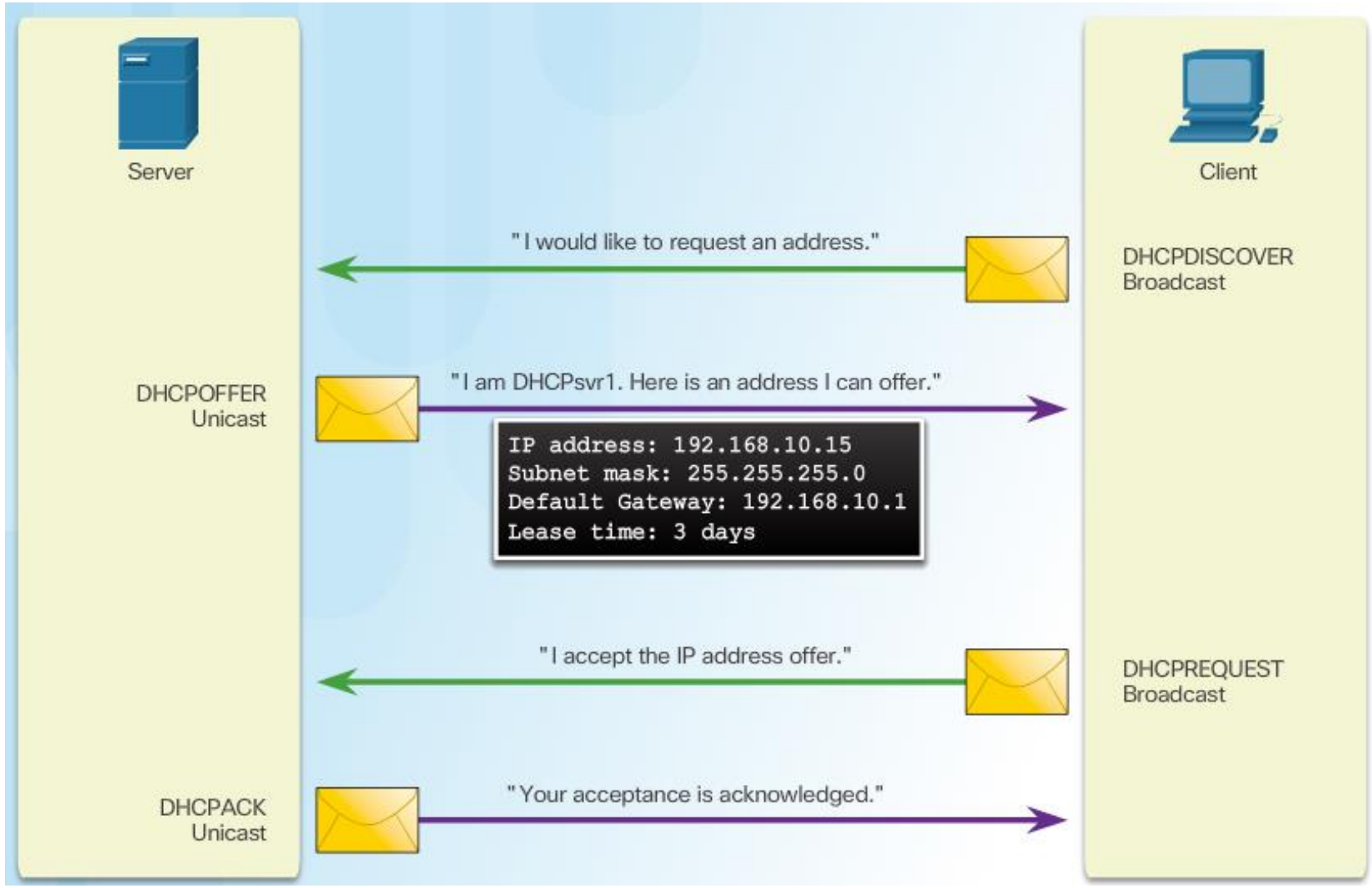
Ochrana

- **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

```
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#
```

Útoky na DHCP a ich potláčanie

DHCP princíp činnosti (DORA mnemo)

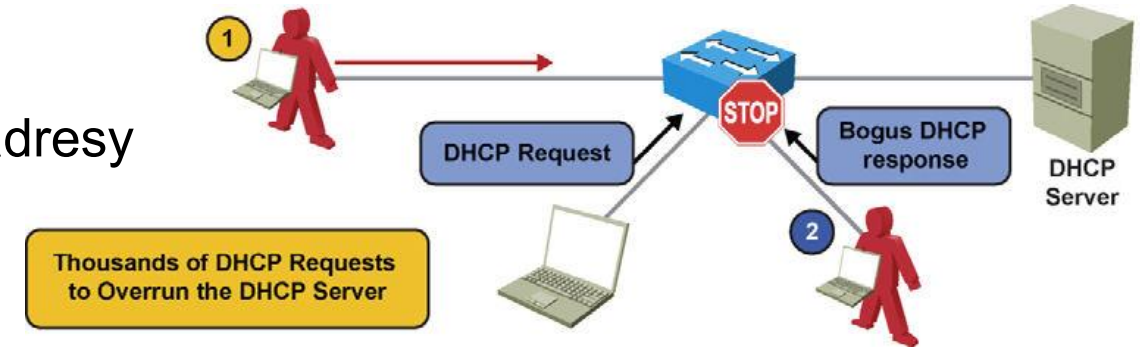


Server správy

Správy kienta

DHCP Spoofing a DHCP starvation

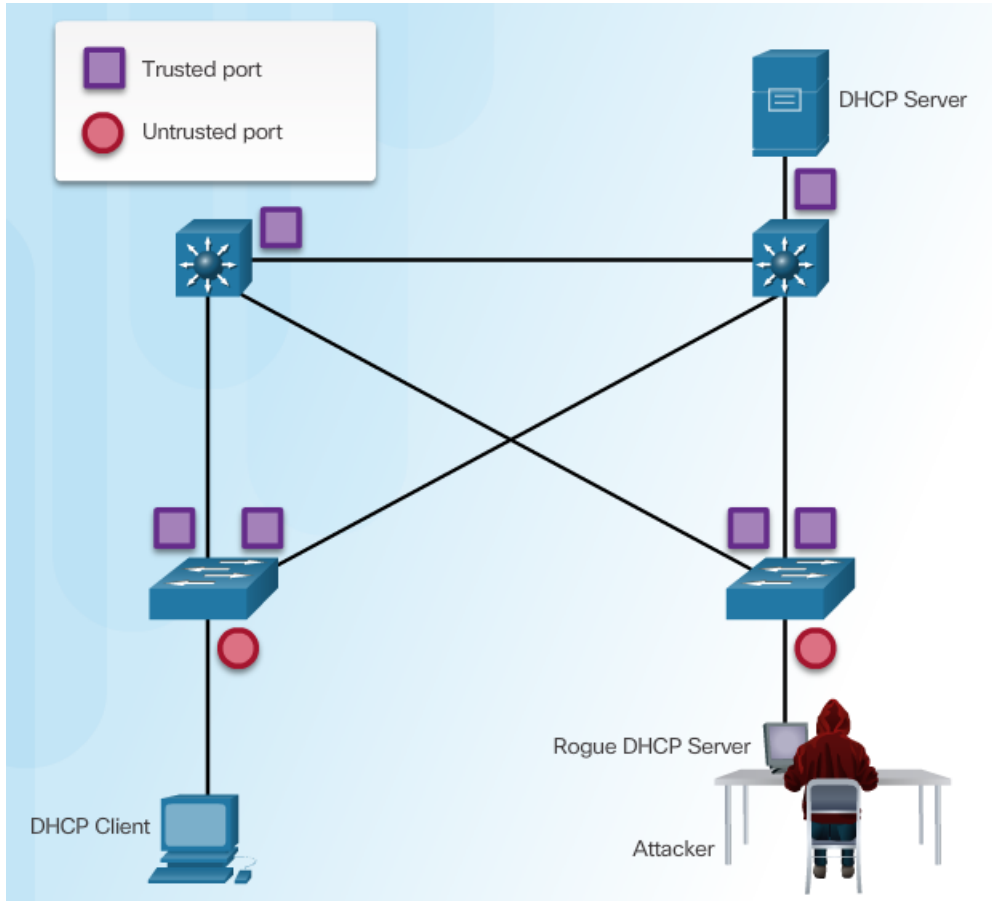
- Môže vykonať útočník fyzicky prítomný v danej LAN, alebo získal prístup z Internetu na niektorý PC v danej LAN
- **DHCP starvation (vyhladovanie)**
  - Generuje sa veľké množstvo žiadostí o IP adresy (posiela sa broadcastom),
  - DHCP serveru neostanú voľné IP adresy
    - Gobbler, yersinia



- **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
- 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



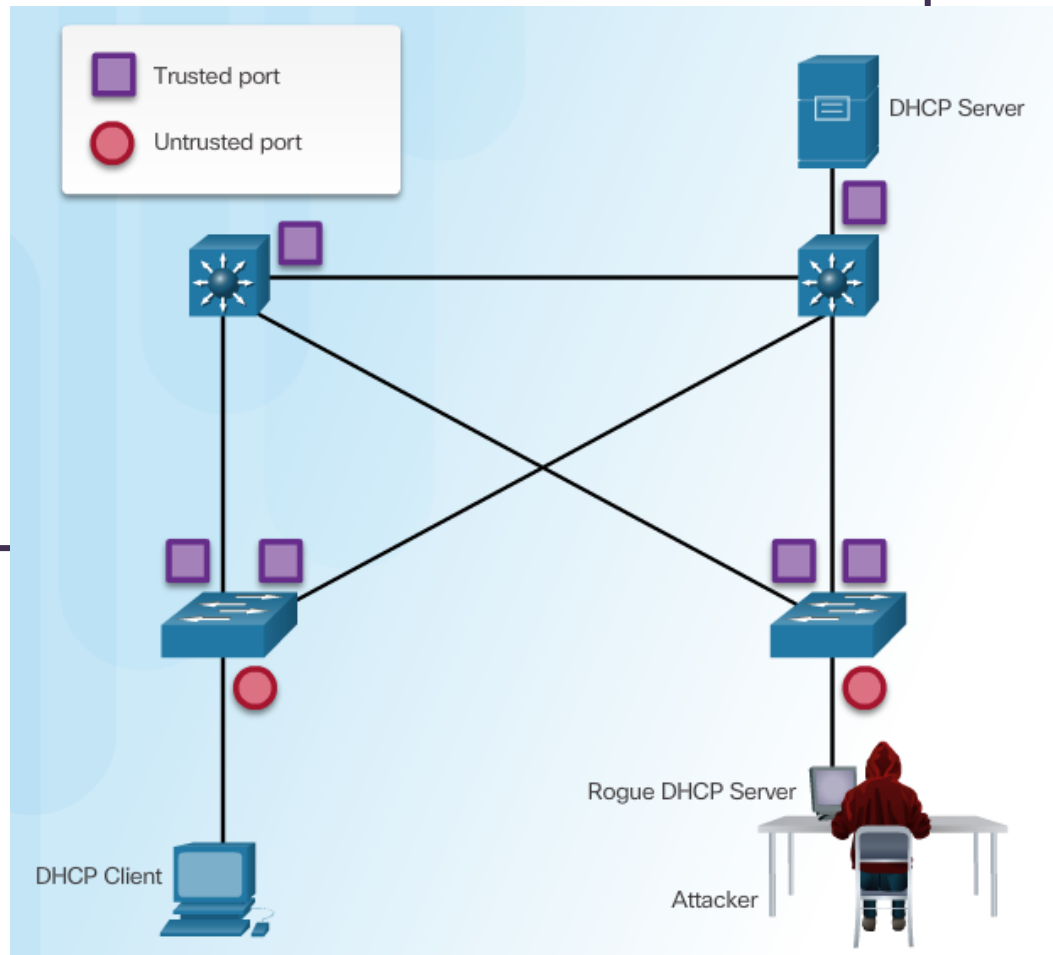

```
Sw# show ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type            VLAN  Interface
------------------  ----------  ----------  -------------  ----  ---------
00:E0:4C:41:3C:E9 10.0.0.4    84960       dhcp-snooping   1      Fa0/11
00:E0:4C:3B:B7:87 10.0.0.6    85042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

DHCP Snooping

- DHCP Snooping je podpora na prepínačoch Catalyst, ktorá sleduje a riadi tok DHCP správ
- DHCP Snooping rozoznáva dôveryhodné a nedôveryhodné porty
  - Na nedôveryhodných portoch sa nachádzajú stanice, buduje sa DHCP snooping DB
  - Na dôveryhodných portoch (alebo za nimi) sa nachádzajú DHCP servery
  - Predvolený typ portu je nedôveryhodný
- DHCP Snooping si podľa DHCP komunikácie na nedôveryhodných portoch vytvára databázu
  - V databáze si switch zaznamenáva MAC adresu stanice, pridelenú IP, čas výpožičky, VLAN a port
  - Túto databázu neskôr využíva DHCP Snooping ako i ďalšie ochranné mechanizmy
- Ak DHCP Snooping-om prejde DHCP správa od klienta, vloží sa do nej DHCP Option-82
  - Informačné pole, ktoré identifikuje, na ktorom prepínači, a ktorom jeho porte je tento klient pripojený

Konfigurácia 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
```



Overenie 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
```

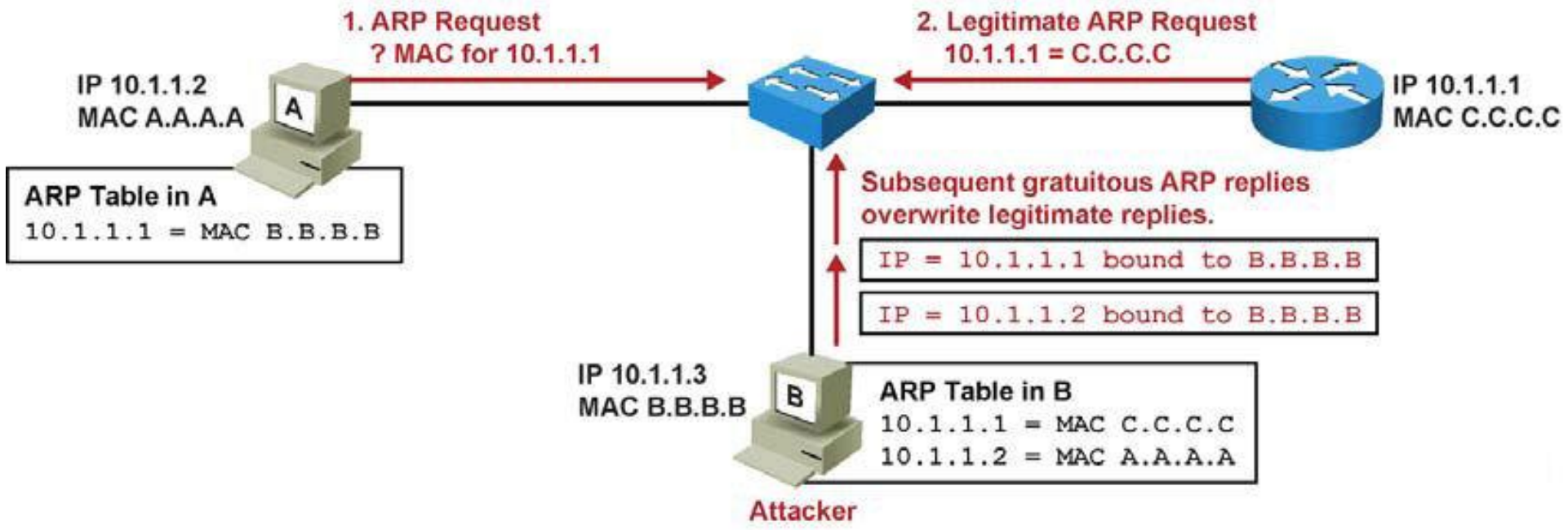
Útoky na ARP + address spoofing a ich potláčanie

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



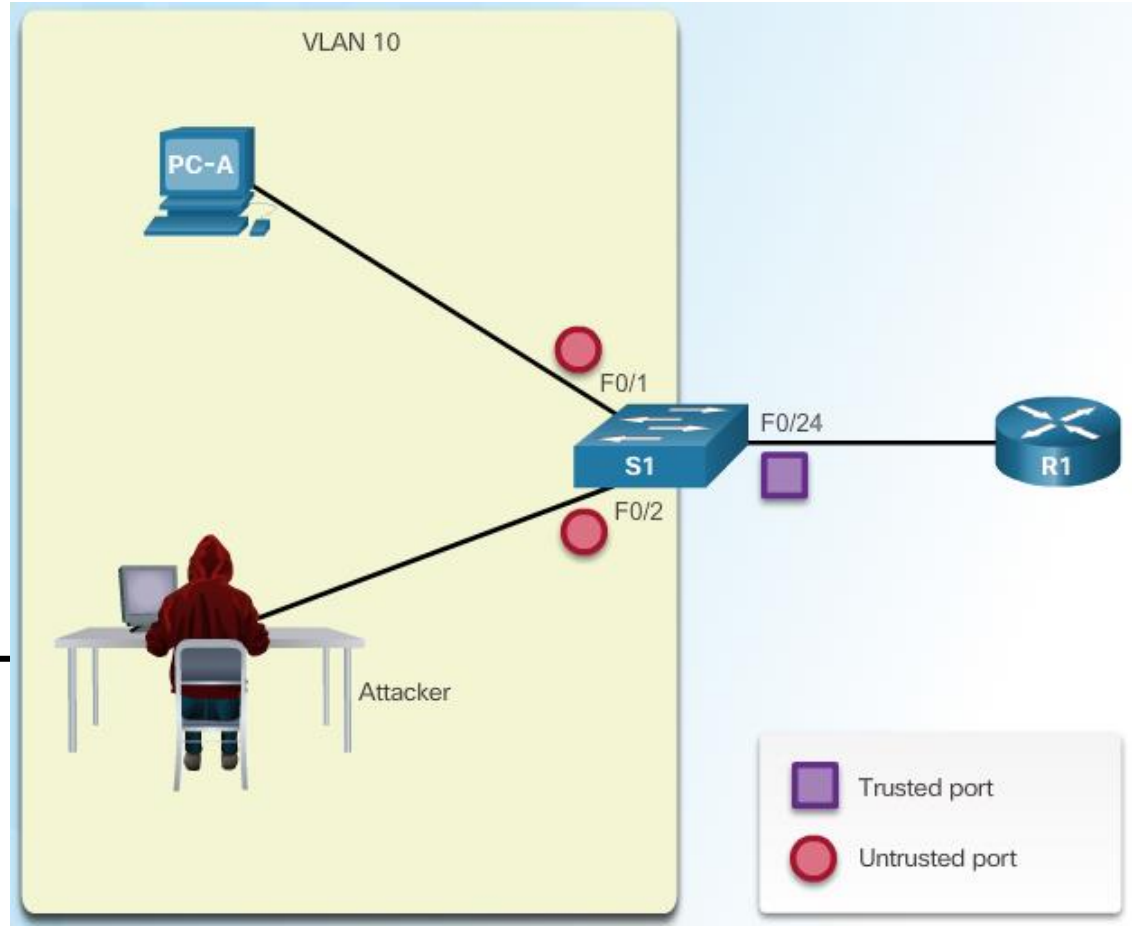
Ochrana proti ARP Spoofing => Dynamic ARP Inspection

- 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])
```

Dynamic ARP Inspection

- Dodatočnou možnosťou DAI je validácia ARP správ

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

- Možnosti:
  - **src-mac**: Zdrojová MAC rámca sa musí zhodovať so Sender 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

```
S1(config)# ip arp inspection validate ?
  dst-mac  Validate destination MAC address
  ip       Validate IP addresses
  src-mac  Validate source MAC address
S1(config)# ip arp inspection validate src-mac
S1(config)# ip arp inspection validate dst-mac
S1(config)# ip arp inspection validate ip
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```

IP Spoofing => IP Source Guard (IPSG)

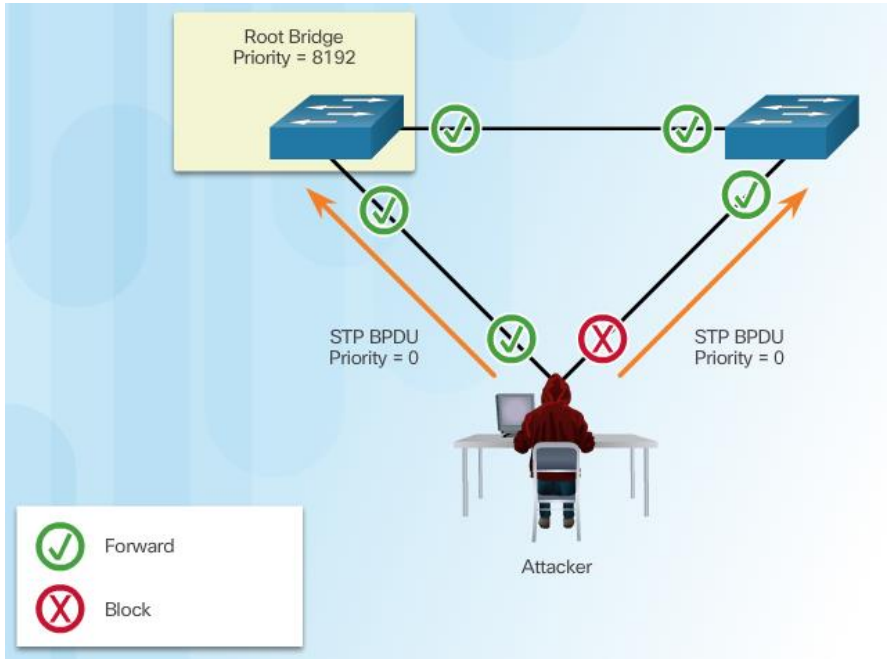
- Ukradnutie a používanie platnej IP adresy inej stanice
  - Používa sa napr. na Ping smrti, nedosiahnuteľná búrka ICMP, povodeň SYN
- Zdroj mnohých existujúcich útokov DoS a DDoS
  - Podvrhnem zdrojovú adresu obete, kde sa budú vracať odpovede
- Ochranou proti IP Spoofingu na prístupovej vrstve
  - => **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

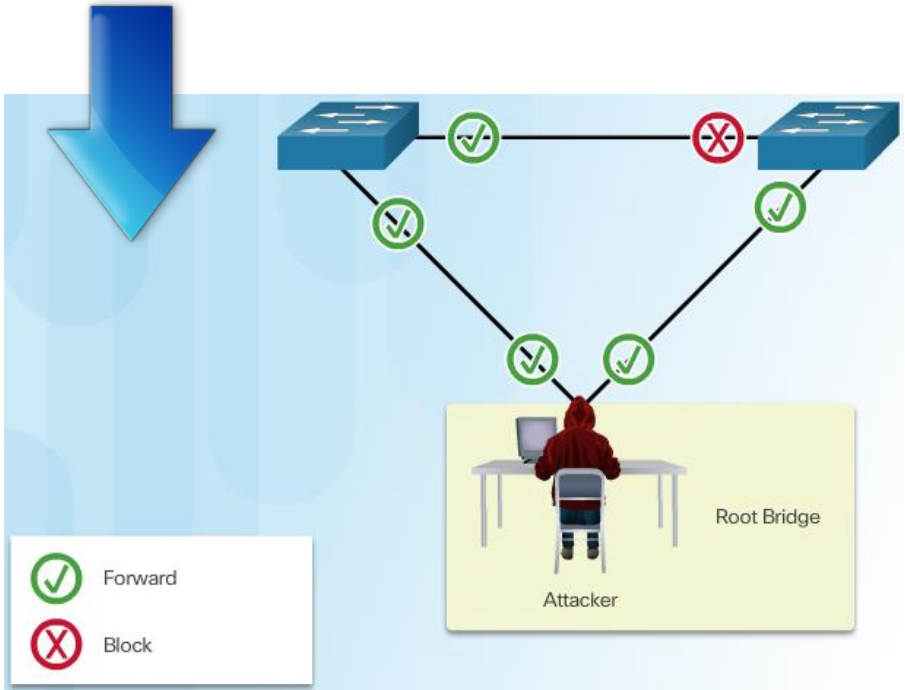
Útoky na STP a ich potláčania

Útoky na STP

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

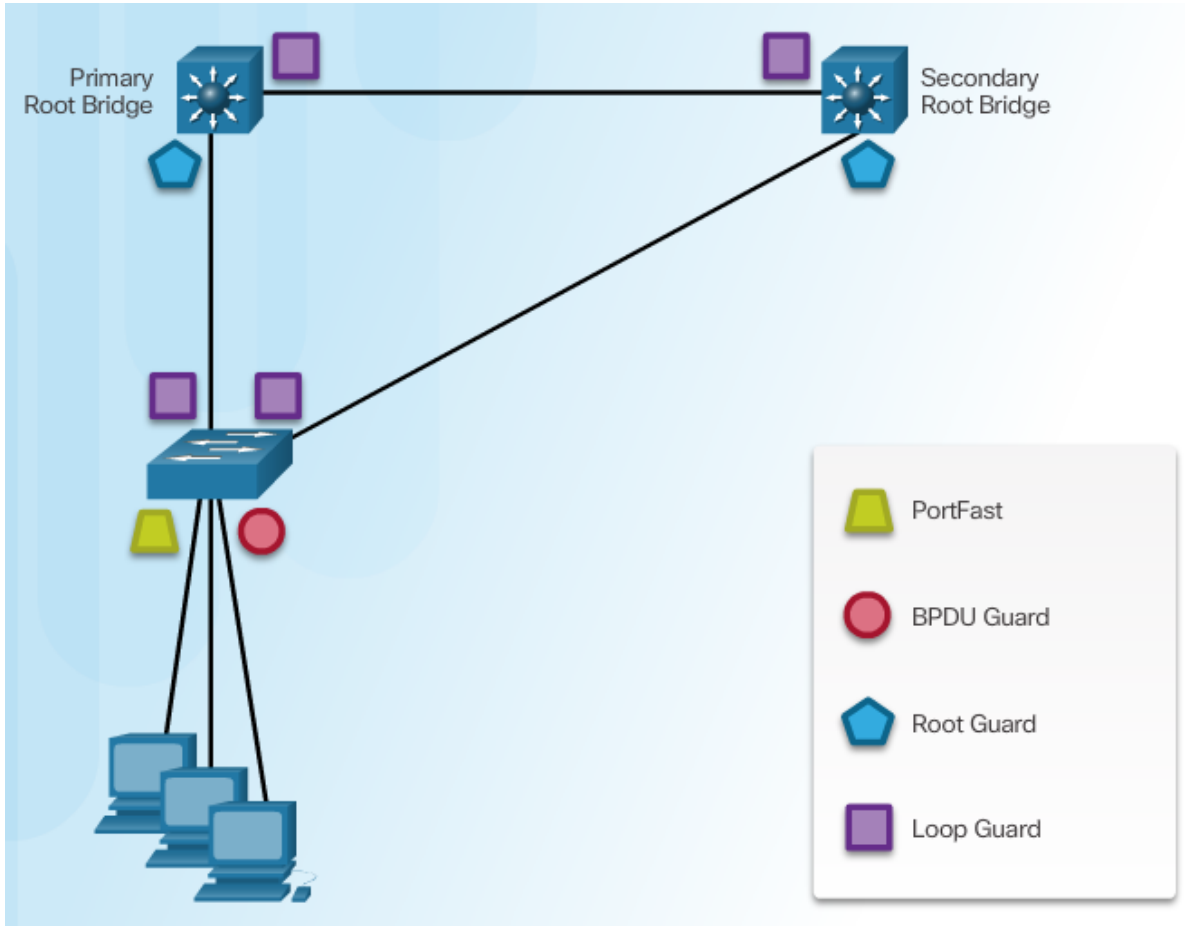
- Nástroj: *yersinia*





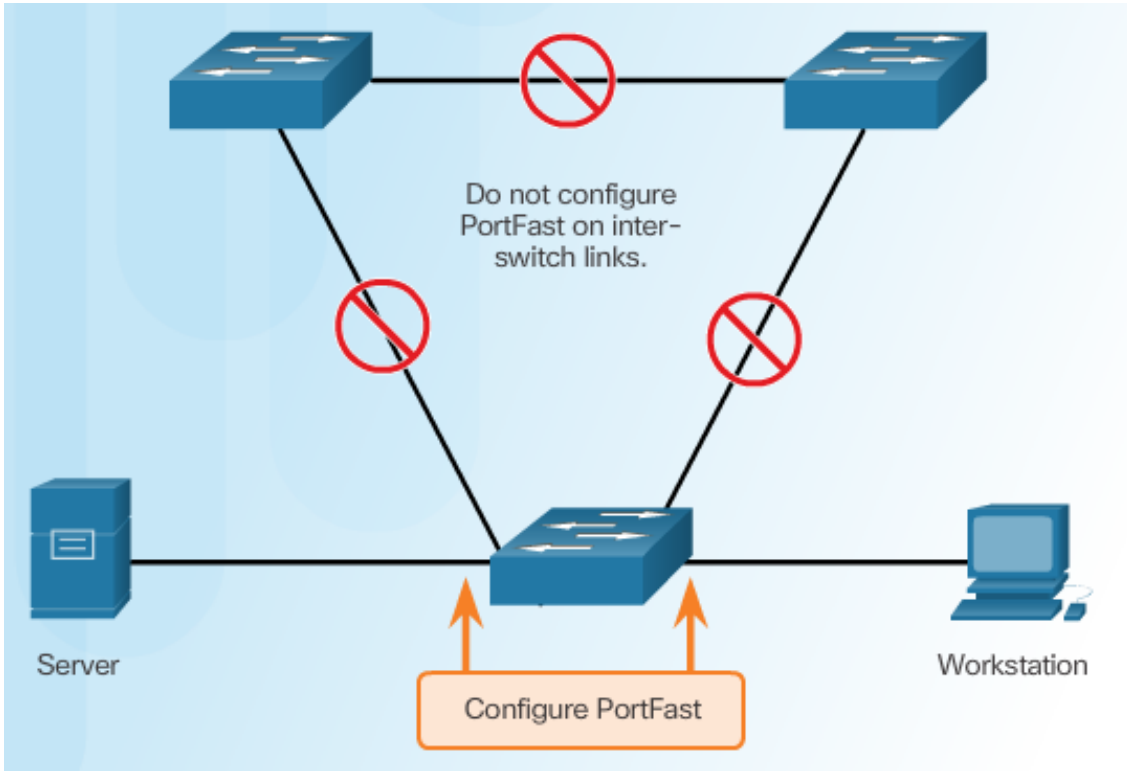
Potláčanie STP útokov

- 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



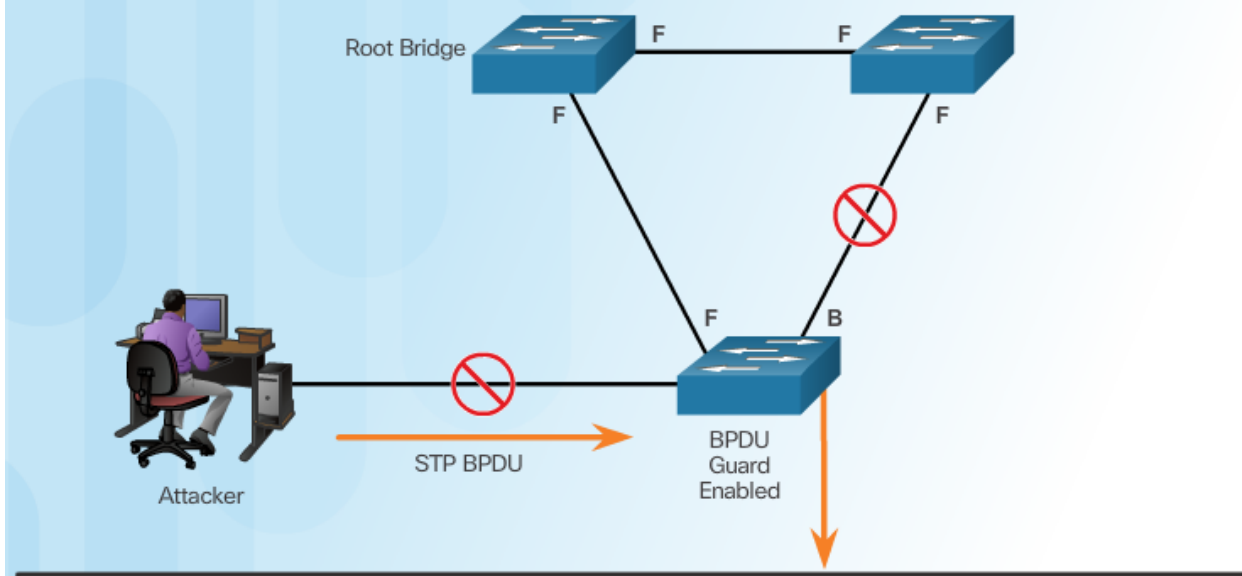
Konfigurácia a overenie Port Fast

```
! 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

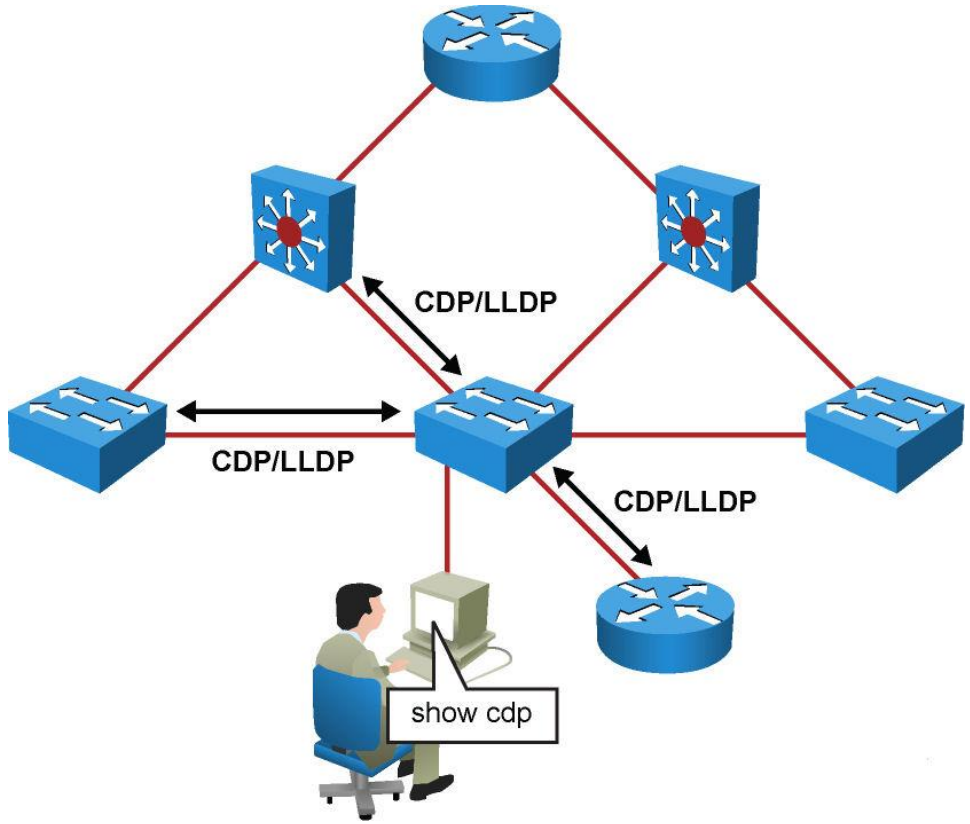



```
! Globálne
Switch(config)# spanning-tree portfast bpduguard default

! 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)

- Cisco Discovery Protocol (CDP)
  - Cisco proprietárny
- Link Layer Discovery Protocol (LLDP)
  - IEEE štandard
- Protokoly komunikujú
  - Nešifrovane, bez autentifikácie
- Útoky
  - Sniffing
    - Získam info počúvaním
  - Zahltenie
    - Typicky flooding hlúposťami
      - => zahltenie pamäte
- Ochrana: vypni
  - Celkovo (neodporúča sa – VoIp): no cdp run / **no lldp run**
  - na portoch kde je bežný používateľ: no cdp enable / **no lldp transmit || receive**



UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

KATEDRA INFORMAČNÝCH SIETÍ * FAKULTA RIADENIA A INFORMATIKY ŽU *

Cisco | Networking Academy®
Mind Wide Open™

Ohodnoť našu CNA na google:

- https://goo.gl/maps/BAnFvQKYCBpffcEX7

Vytvorené v rámci projektu KEGA 026TUKE-4/2021

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY