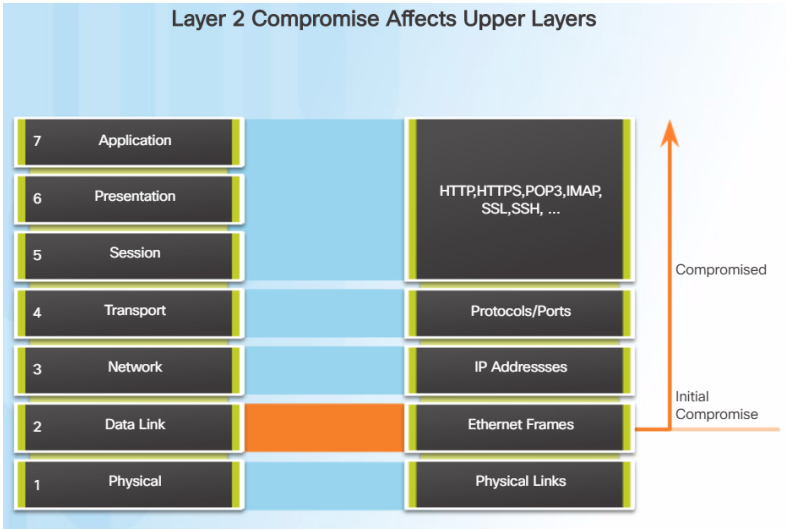
APS
Sieťová bezpečnosť a monitoring

Vytvorené v rámci projektu KEGA 026TUKE-4/2021

Katedra počítačov a informatiky
Fakulta elektrotechniky a informatiky
Technická univerzita v Košiciach

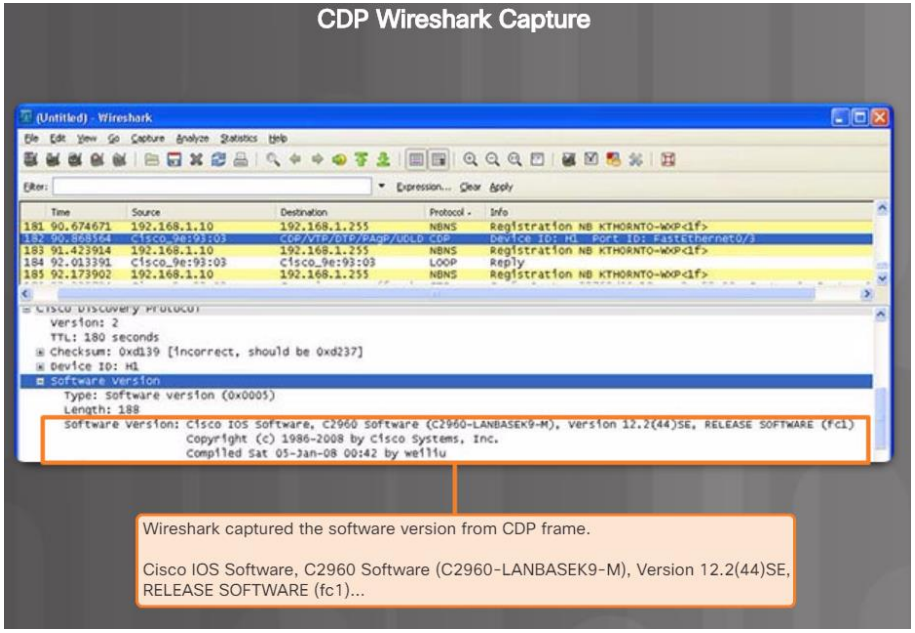
Bezpečnosť LAN

- Vrstva L1/L2
- Typické útoky L2:
  - CDP Reconnaissance Attacks
  - Telnet Attacks
  - MAC Address Table Flooding Attacks
  - VLAN Attacks
  - DHCP Attacks



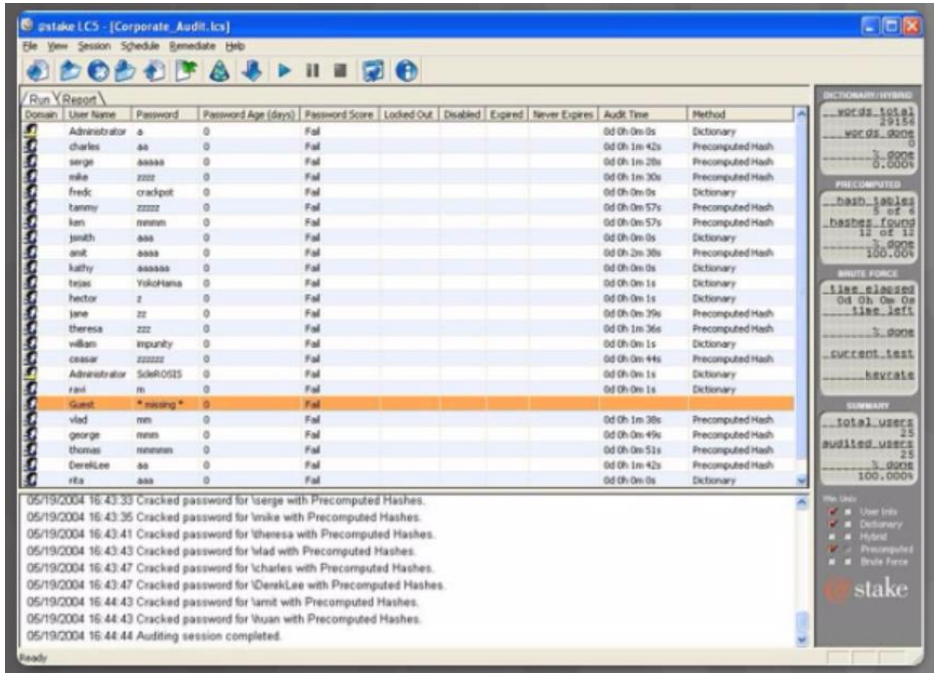
CDP Reconnaissance

- Cisco Discovery Protocol (CDP) – štandardne zapnutý
  - verzia OS
  - IP adresy všetkých portov
  - identifikácia portov
  - duplex
  - VTP doména
  - Natívna VLAN
  - spotreba PoE zariadení
- vypnutie:
  - `no cdp run` (globálne)
  - `no cdp enable` (rozhranie)



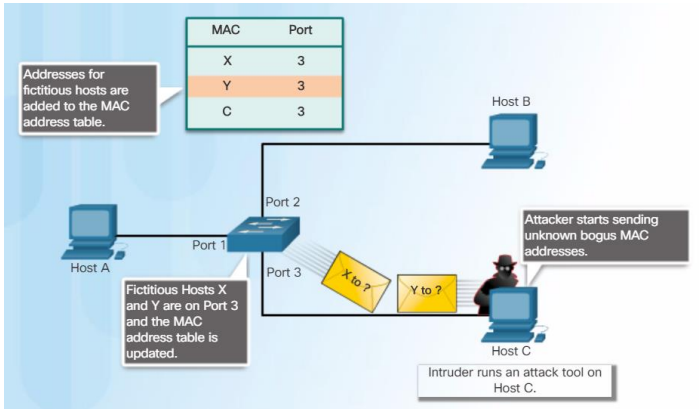
Telnet útoky

- Brute Force Password Attack
  - slovníkový útok
  - uhádnutie hesla
- Telnet DoS Attack
  - znefunkčnenie služby zahltením
- Odporúčania:
  - používať SSH
  - silné heslá
  - ACL na prístup
  - využitie AAA



MAC Address Table Flooding

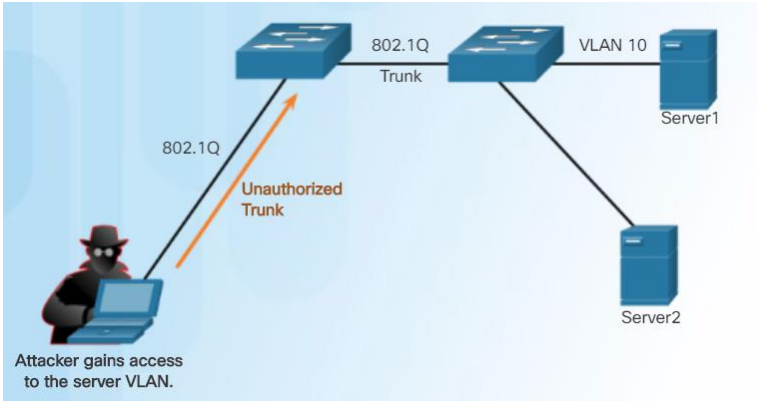
- zahĺtenie (pretečenie MAC tabuľky)
- prechod do fail-open módu -> broadcast-ovanie celej komunikácie
- využiť port-security
- Cisco 2960




```
switch1#show mac-address-table count
Mac Entries for Vlan 10:
---------------------------
Dynamic Address Count   : 5
Static  Address Count   : 0
Total Mac Addresses     : 5
Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count   : 1
Static  Address Count   : 0
Total Mac Addresses     : 1
Total Mac Address Space Available: 8024
```

VLAN útoky

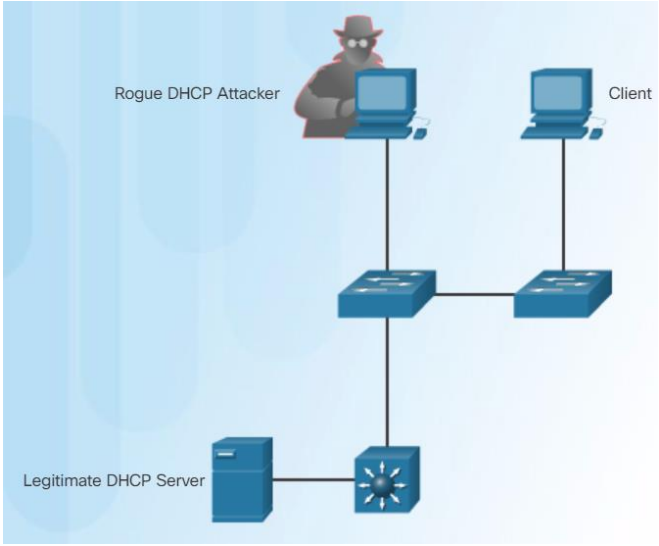
- zneužitie 802.1Q trunking protokolu
- zneužitie DTP (Dynamic Trunking Protokolu)
- získanie prístupu do všetkých VLAN



- Odporúčanie:
  - natvrdo prideliť porty do VLAN
  - vypnúť trunk mód AUTO
  - manuálne nastaviť trunk porty
  - vypnúť nepoužívané porty, samostatná VLAN
  - zmeniť natívnu VLAN
  - nahodiť port-security

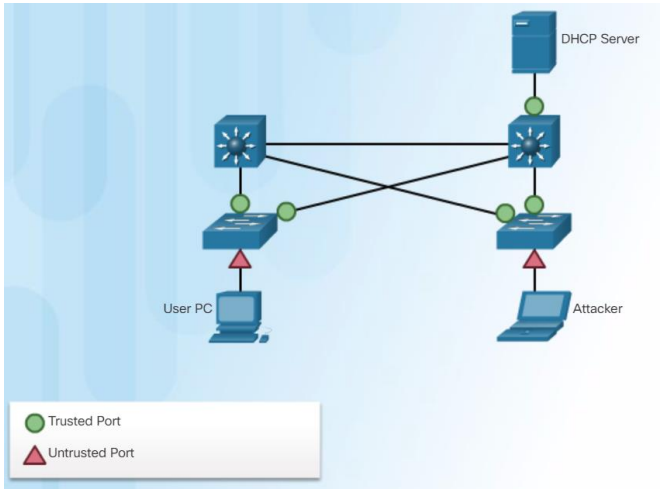
DHCP útoky

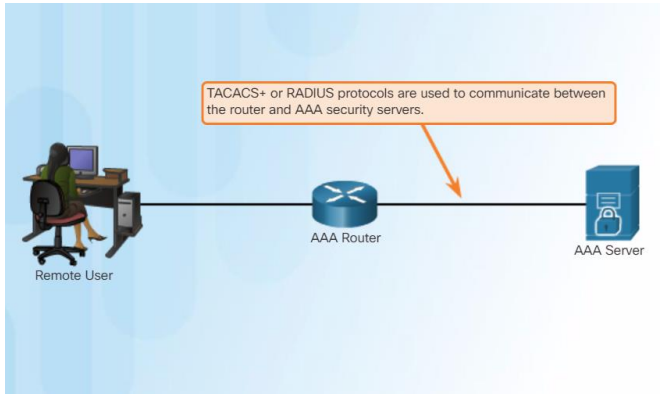
- DHCP spoofing attack
  - falošný DHCP server v sieti (IP, GW, DNS)
- DHCP starvation attack
  - vezmem si všetky dostupné IP adresy z poolu



Pár odporúčaní

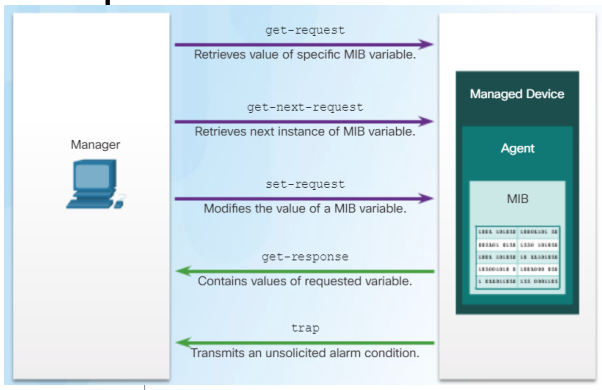
- využívať port-security // MAC address flooding
- vypnúť DTP
  - `switchport nonegotiate` (na porte)
- zapnúť DHCP snooping pre boj s DHCP spoofing
  - Trusted DHCP ports
  - Untrusted ports
- využiť AAA
  - Authentification, Authorization, Accounting
  - TACACS+ / Radius / 802.1X

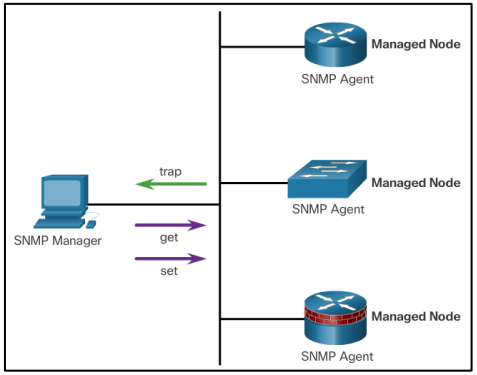




SNMP

- umožňuje administrátorom spravovať a monitorovať zariadenia v sieti
- SNMP emelenty:
  - Manager
  - Agent
  - MIB (Management Information Base)
- SNMP akcie:
  - Trap
  - Get
  - Set





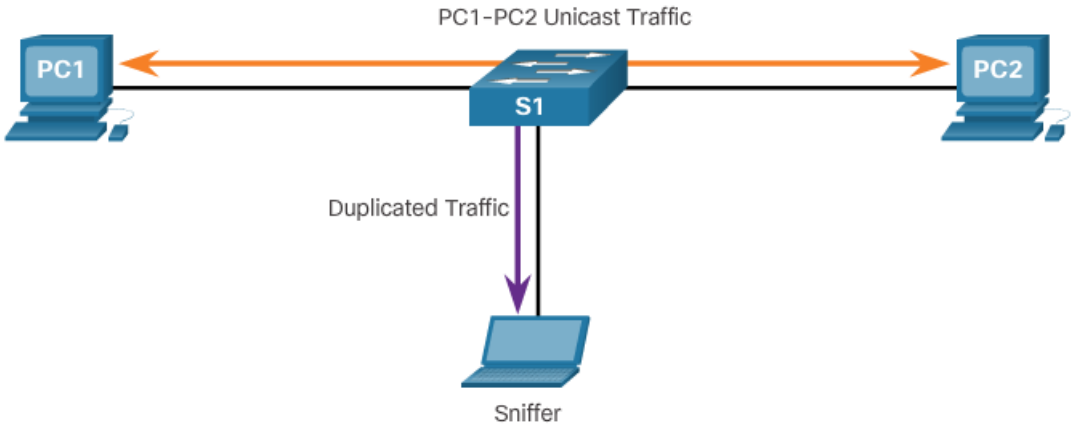
Operation	Description
`get-request`	Retrieves a value from a specific variable.
`get-next-request`	Retrieves a value from a variable within a table; the SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
`get-bulk-request`	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. (Only works with SNMPv2 or later.)
`get-response`	Replies to a `get-request`, `get-next-request`, and `set-request` sent by an NMS.
`set-request`	Stores a value in a specific variable.

SNMP verzie

Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication (an improvement over SNMPv2c).
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	authPriv (requires the cryptographic software image)	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms: • DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. • 3DES 168-bit encryption. • AES 128-bit, 192-bit, or 256-bit encryption.

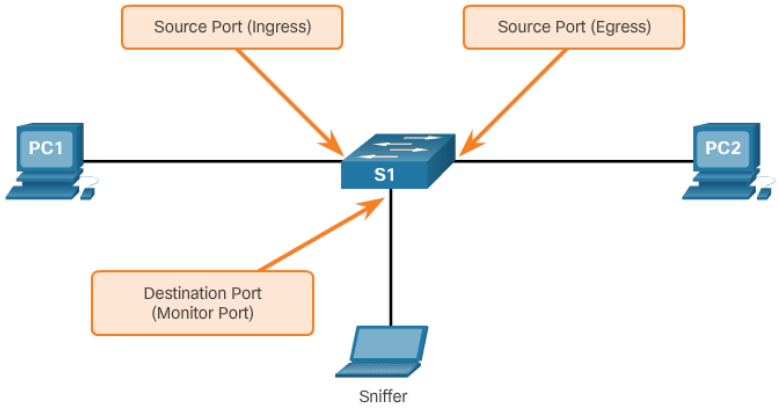
SPAN

- Cisco Switch Port Analyzer
- umožňuje prepínaču **kopírovať** Ethernet rámce zo špecifického portu na zvolený port kde je pripojený analyzátor rámcov



SPAN terminológia

Term	Definition
Ingress traffic	This is traffic that enters the switch.
Egress traffic	This is traffic that leaves the switch.
Source (SPAN) port	This is a port that is monitored with use of the SPAN feature.
Destination (SPAN) port	This is a port that monitors source ports, usually where a packet analyzer, IDS or IPS is connected. This port is also called the monitor port.
SPAN session	This is an association of a destination port with one or more source ports.
Source VLAN	This is the VLAN monitored for traffic analysis.



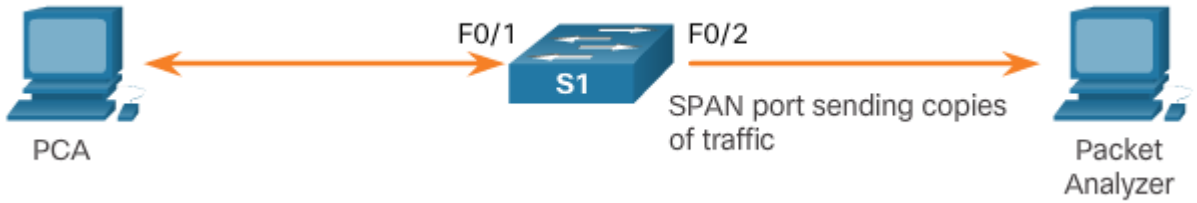
Konfigurácia SPAN

Associate a SPAN session with a source port

```
Switch(config)# monitor session number source [ interface interface | vlan vlan ]
```

Associate a SPAN session with a destination port

```
Switch(config)# monitor session number destination [ interface interface | vlan vlan ]
```




```
S1(config)# monitor session 1 source interface fastethernet 0/1
S1(config)# monitor session 1 destination interface fastethernet 0/2
```

Ďakujem za pozornosť