



Siet'ová a komunikačná bezpečnosť

02 Bezpečnosť prenosu údajov na spojovej úrovni komunikačného modelu



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

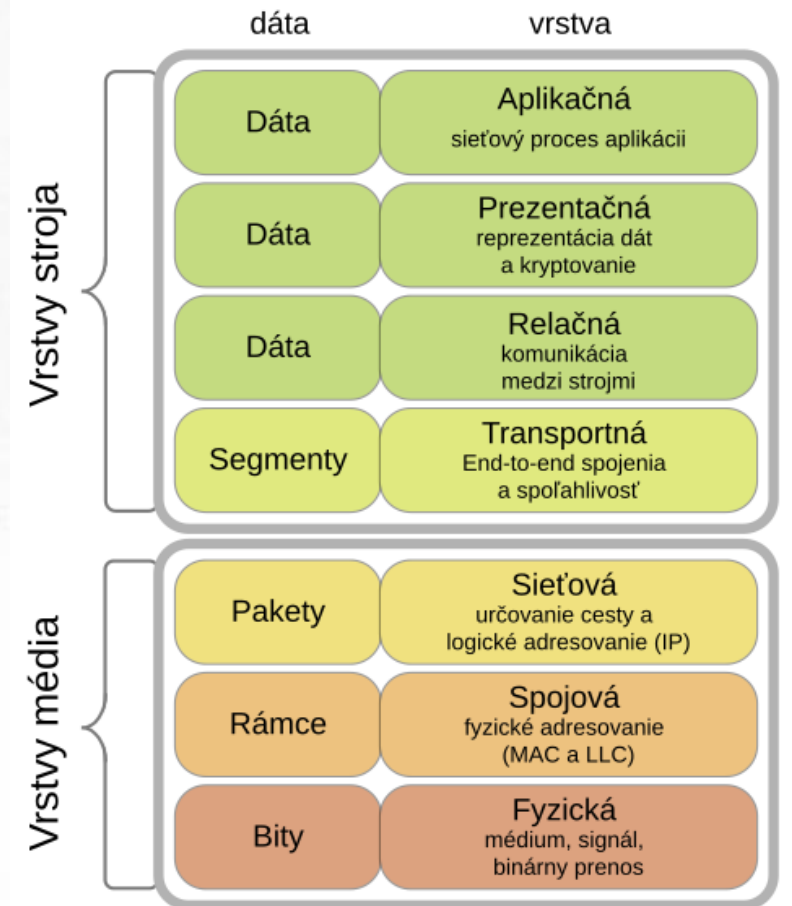
Bezpečnosť prenosu údajov na spojovej úrovni komunikačného modelu

- riadenie údajových tokov v lokálnych sieťach
- prepínanie
- STP
- virtualizácia
- MACsec
- multiprotokolové prepínanie
- VLAN

OSI Model

- Open Systems Interconnection
- abstraktný komunikačný model
- funkčne rozdeľuje sieťové protokoly do 7 vrstiev

- fyzická vrstva
 - kábel/optické vlákno
 - prenos bitov, modulácia
 - opakovač (repeater)
 - prepojenie segmentov



https://upload.wikimedia.org/wikipedia/commons/8/8d/OSI_Model_v1.svg





Spojová úroveň

- zabezpečuje spoľahlivosť prenosu údajov medzi susednými uzlami siete
- postupnosť bitov (bajtov) s definovaným začiatkom a koncom **rámec** (frame)
- kontrola chýb, možnosti potvrdzovania, riadenie prístupu pre viacero používateľov spoja, riadenie toku dát (flow controll) – proti zahlteniu
- jednoznačná identifikácia – **fyzické adresy** (MAC medium access control), identifikácia virtuálneho okruhu





Spojová úroveň

- znakové (bajtové) prenosy
 - DLE STX data DLE ETX (byte stuffing, escape char DLE)
- bitovo orientované prenosy
 - FLAG data FLAG (bit stuffing)
- **detekcia chýb** – kontrola parity resp. zvyšky po delení cyklických polynómov (CRC – cyclic redundancy check)
- v rámci bezdrôtových sietí LLC poskytuje aj **riadenie toku**
 - potvrdzovanie, opakované vysielanie





Spojová úroveň

- High-Level Data Link Control (HDLC)
 - bitovo orientovaný protokol, 2 aj viac bodové spojenie
- Point to Point Protocol (dial-up, dsl)
 - bajtové (oktetové) prenosy – ESC oktet 01111101
 - možnosť autentifikácie
 - Password Authentication Protocol (PAP)
 - Challenge Handshake Authentication Protocol (CHAP)
- Layer 2 Tunneling Protocol (L2TP)
 - pre virtuálne siete





Spojová úroveň

- štandard IEEE 802 (Institute of Electrical and Electronics Engineers)
- 802.2 **LLC** Logical link control
- 802.3 **Ethernet**
- 802.5 **Token Ring**
- 802.11 **Wi-Fi**
- 802.15 **Wireless PAN**



PLÁN [OBNOVY]

https://upload.wikimedia.org/wikipedia/commons/8/8d/OSI_Model_v1.svg





Ethernetový rámec 802.3

- štandardne 64-1518 bajtov, z toho 18 bajtová hlavička
 - 7 bajtov **preambula** (striedavo 0 a 1)
 - 1 bajt **začiatok rámca** (start frame delimititer)
 - 6 bajtov **cieľová adresa**
 - 6 bajtová **zdrojová adresa** (špec. bity – unicast/multicast, global unique/local)
 - 2 bajty **dĺžka**
 - X bajtov **údaje** (+ prípadny padding)
 - 4 bajty **kontrolný súčet** (crc)





Ethernetový rámec

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr.oui & 0x010000

No.	Time	HW Src	HW Dst	Source	Destination	Protocol	Length	Info
54	1.600205	Cisco_0b:98:61	Broadcast	Cisco_0b:98:61	Broadcast	ARP	60	Who has 158.197.31.200? Tell 158.197.31.1

> Frame 54: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{9C01CC05-791D-4D2C-BC06-53B35BFE1597}, id 0

▼ Ethernet II, Src: Cisco_0b:98:61 (78:bc:1a:0b:98:61), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Address: Broadcast (ff:ff:ff:ff:ff:ff)
 -1. = LG bit: Locally administered address (this is NOT the factory default)
 -1. = IG bit: Group address (multicast/broadcast)
- ▼ Source: Cisco_0b:98:61 (78:bc:1a:0b:98:61)
 - Address: Cisco_0b:98:61 (78:bc:1a:0b:98:61)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)

Type: ARP (0x0806)
 Padding: 00000000000000000000000000000000

> Address Resolution Protocol (request)

0000	ff ff ff ff ff ff 78 bc 1a 0b 98 61 08 06 00 01x.a...
0010	08 00 06 04 00 01 78 bc 1a 0b 98 61 9e c5 1f 01x.a....
0020	00 00 00 00 00 00 9e c5 1f c8 00 00 00 00 00 00
0030	00 00 00 00 00 00 00 00 00 00 00 00

Type (eth.type), 2 byte(s) | Packets: 160195 · Displayed: 23173 (14.5%) | Profile: Default



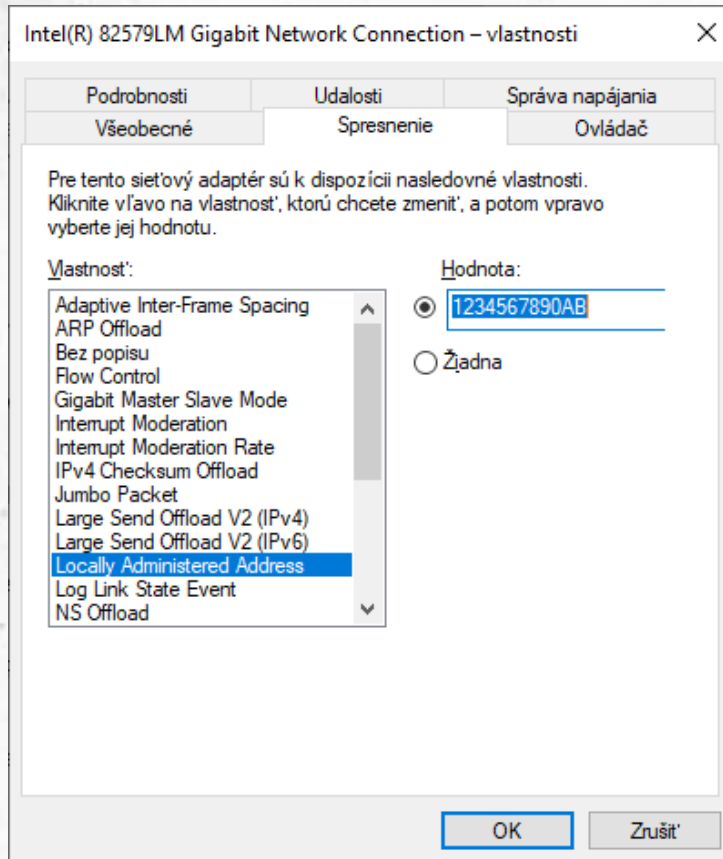
Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ethernetový rámec – zmena MAC



```
ip link set dev address  
02:01:02:03:04:08
```



Jumbo rámce

- pakety vyšších vrstiev musia byť rozdelené do viacerých rámcov

```
*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 158.197.16.80
No. Time HW Src HW Dst Source Destination Protocol Length Info
13584 992.170311 12:34:56:78:90:ab Cisco_0b:98:61 158.197.31.120 158.197.16.80 ICMP 1514 Echo (ping) request id=0x0001, seq=17/4352, ttl=128 (reply in...
13585 992.170958 Cisco_0b:98:61 12:34:56:78:90:ab 158.197.16.80 158.197.31.120 ICMP 1514 Echo (ping) reply id=0x0001, seq=17/4352, ttl=62 (request in...
13613 995.482673 12:34:56:78:90:ab Cisco_0b:98:61 158.197.31.120 158.197.16.80 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=72d4) [Reassem...
13614 995.482674 12:34:56:78:90:ab Cisco_0b:98:61 158.197.31.120 158.197.16.80 ICMP 35 Echo (ping) request id=0x0001, seq=18/4608, ttl=128 (reply in...
13615 995.483477 Cisco_0b:98:61 12:34:56:78:90:ab 158.197.16.80 158.197.31.120 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=51da) [Reassem...

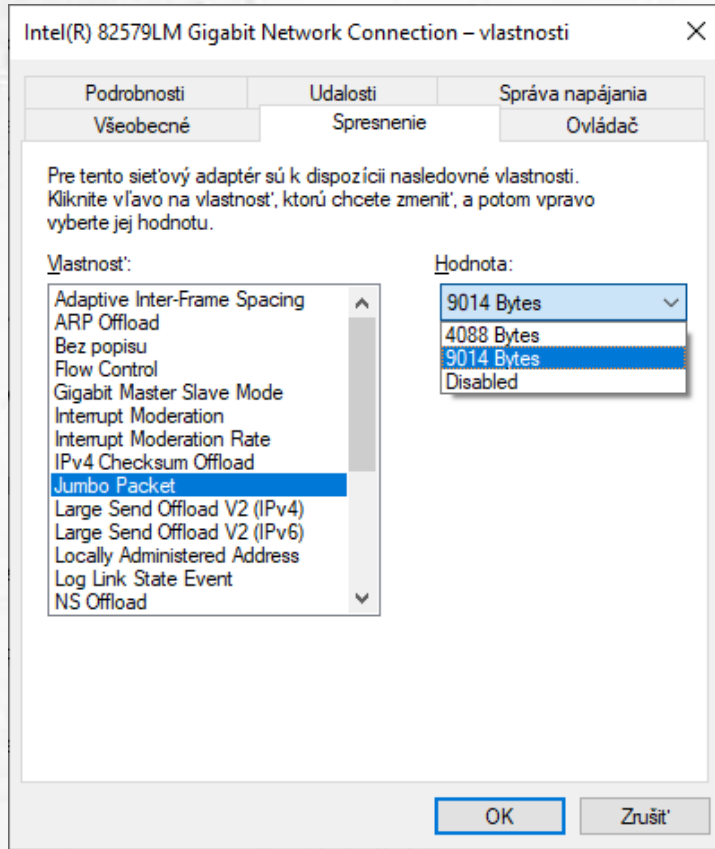
> Frame 13614: 35 bytes on wire (280 bits), 35 bytes captured (280 bits) on interface \Device\NPF_{9C01CC05-791D-4D2C-BC06-53B358FE1597}, id 0
Ethernet II, Src: 12:34:56:78:90:ab (12:34:56:78:90:ab), Dst: Cisco_0b:98:61 (78:bc:1a:0b:98:61)
  Destination: Cisco_0b:98:61 (78:bc:1a:0b:98:61)
    Address: Cisco_0b:98:61 (78:bc:1a:0b:98:61)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: 12:34:56:78:90:ab (12:34:56:78:90:ab)
    Address: 12:34:56:78:90:ab (12:34:56:78:90:ab)
      ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 158.197.31.120, Dst: 158.197.16.80
    0100 .... = Version: 4
    ....0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 21
      Identification: 0x72d4 (29396)
      Flags: 0x00b9
      [...] 0101 1100 1000 = Fragment offset: 1480
      Time to live: 128
      Protocol: ICMP (1)
      Header checksum: 0x0000 [validation disabled]
      [Header checksum status: Unverified]
      Source: 158.197.31.120
      Destination: 158.197.16.80
    > [2 IPv4 Fragments (1481 bytes): #13613(1480), #13614(1)]
  > Internet Control Message Protocol

0000 78 bc 1a 0b 98 61 12 34 56 78 90 ab 08 00 45 00 x.....4 Vx....E.
0010 00 15 72 d4 00 b9 80 01 00 00 9e c5 1f 78 9e c5 ..r.....x...
0020 10 50 61 .Pa

Frame (35 bytes) Reassembled IPv4 (1481 bytes)
Fragment offset (13 bits) (ip.frag_offset), 2 byte(s) || Packets: 17075 · Displayed: 34 (0.2%) || Profile: Default
```



Jumbo rámce



```
ip link set dev mtu 9000
```





Jumbo rámce

Capturing from Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 158.197.8.8

No.	Time	HW Src	HW Dst	Source	Destination	Protocol	Length	Info
18	1.647365	12:34:56:78:90:ab	Cisco_0b:98:61	158.197.31.120	158.197.8.8	ICMP	9014	Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (no respons...
72	5.934786	12:34:56:78:90:ab	Cisco_0b:98:61	158.197.31.120	158.197.8.8	IPv4	9010	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0bfe) [Reassembl...
73	5.934788	12:34:56:78:90:ab	Cisco_0b:98:61	158.197.31.120	158.197.8.8	ICMP	39	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (no respons...

> Frame 72: 9010 bytes on wire (72080 bits), 9010 bytes captured (72080 bits) on interface \Device\NPF_{9C01CC05-791D-4D2C-BC06-53B358FE1597}, id 0

Ethernet II, Src: 12:34:56:78:90:ab (12:34:56:78:90:ab), Dst: Cisco_0b:98:61 (78:bc:1a:0b:98:61)

- Destination: Cisco_0b:98:61 (78:bc:1a:0b:98:61)
Address: Cisco_0b:98:61 (78:bc:1a:0b:98:61)
... ..0 = LG bit: Globally unique address (factory default)
... ..0 = IG bit: Individual address (unicast)
- Source: 12:34:56:78:90:ab (12:34:56:78:90:ab)
Address: 12:34:56:78:90:ab (12:34:56:78:90:ab)
... ..1 = LG bit: Locally administered address (this is NOT the factory default)
... ..0 = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 158.197.31.120, Dst: 158.197.8.8

- 0100 ... = Version: 4
- ... 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 8996
- Identification: 0x0bfe (3070)
- > **Flags: 0x2000, More fragments**
...0 0000 0000 0000 = Fragment offset: 0
- Time to live: 128
- Protocol: ICMP (1)
- Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
- Source: 158.197.31.120
- Destination: 158.197.8.8
- [Reassembled IPv4 in frame: 73](#)

> Data (8976 bytes)

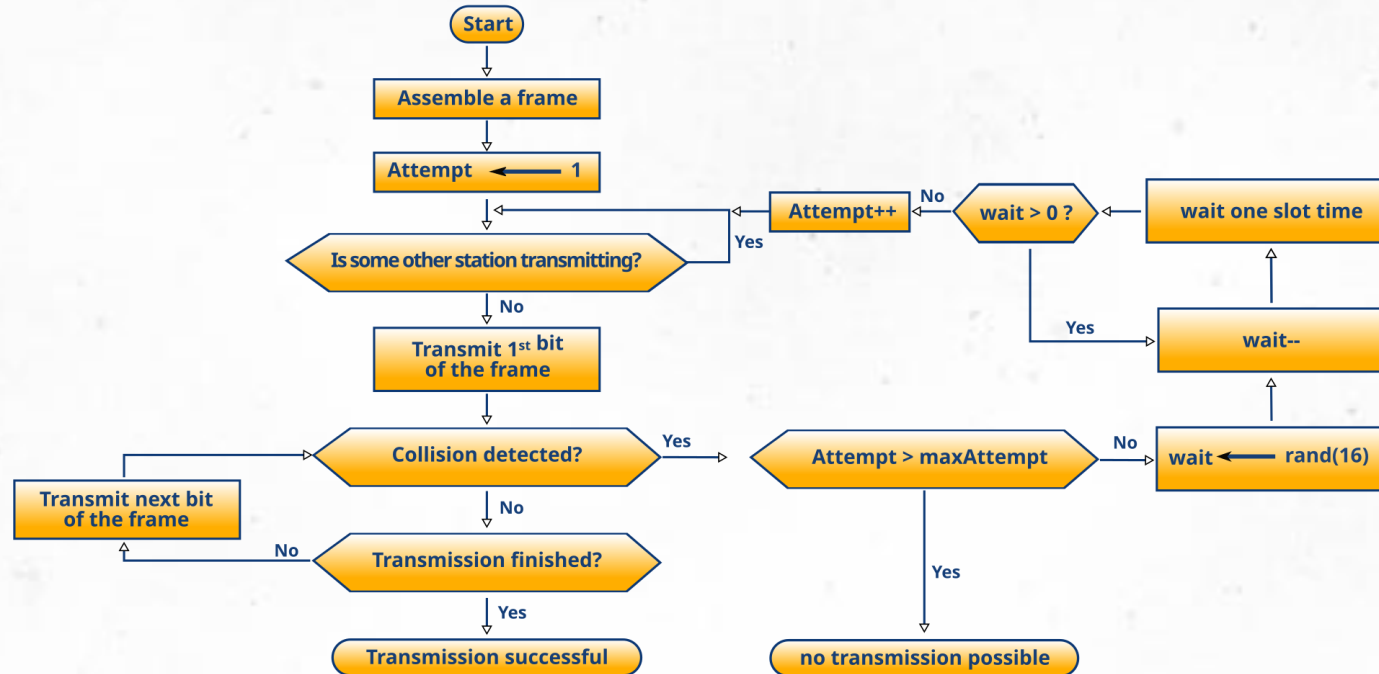
```
0010 23 24 0b fe 20 00 80 01 00 00 9e c5 1f 78 9e c5  #$. . . . .x..
0020 08 08 08 00 ab f4 00 01 00 20 61 62 63 64 65 66  . . . . . abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
```

Flags (3 bits) (ip.flags), 2 byte(s) | Packets: 832 · Displayed: 3 (0.4%) | Profile: Default



Kolízne domény

- Carrier-sense multiple access with collision detection (CSMA/CD)

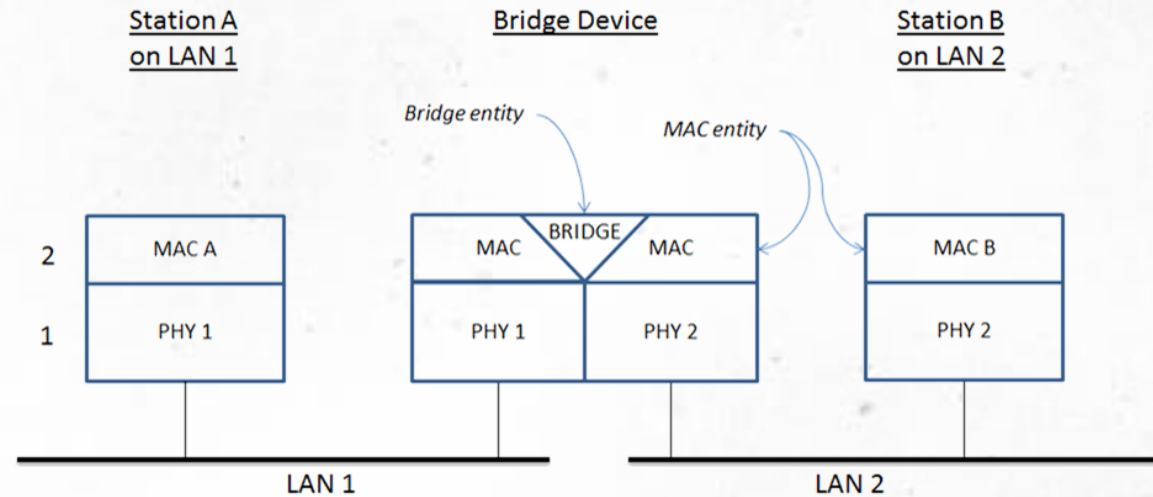


<https://upload.wikimedia.org/wikipedia/commons/thumb/3/37/CSMACD-Algorithm.svg/1920px-CSMACD-Algorithm.svg.png>



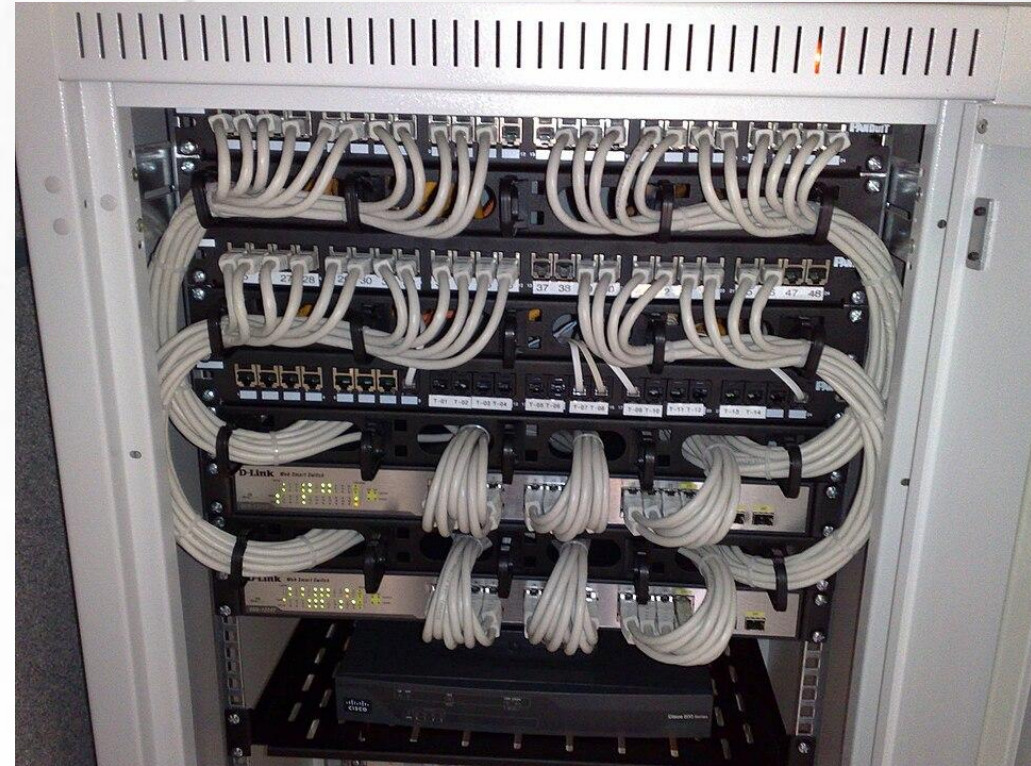
Rozbočovač, Most, Prepínač

- rozbočovač (hub) – viacportový opakovač na spojovej úrovni
- most (bridge) - odddeľuje kolízne domény
- počúva a presmeruje, ak je určené druhej sieti - smerovacia tabuľka
- metódy:
 - store and forward
 - cut through
 - fragment free
 - adaptive switching



Prepínač

- **prepínač** (switch)
 - full-duplex komunikácia
 - viacportový most
 - prepínacia tabuľka (MAC-port)
 - problém zacyklenia rieši STP
- V prípade zaplenia tabuľa sa prepne na rozbočovač

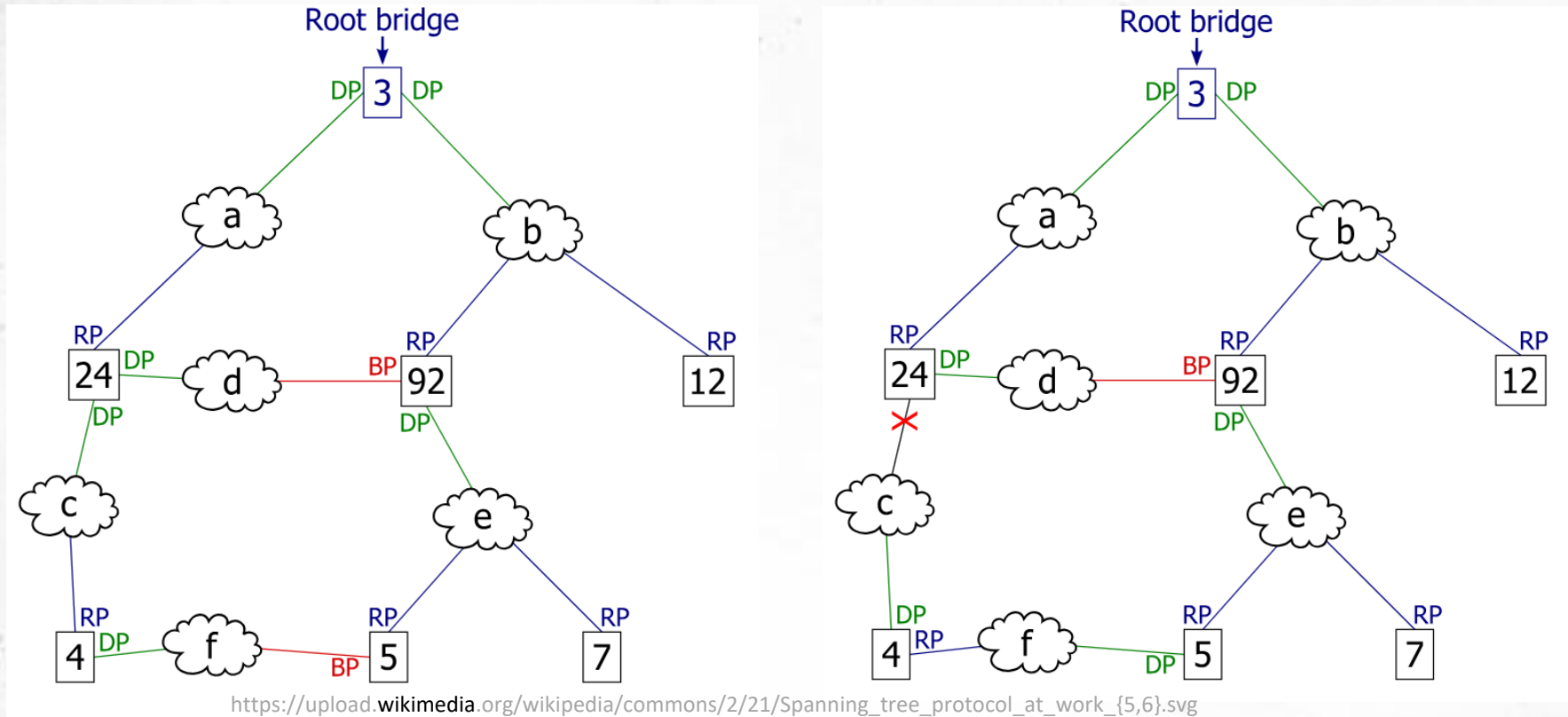


https://upload.wikimedia.org/wikipedia/commons/b/bc/19-inch_rackmount_Ethernet_switches_and_patch_panels.jpg



STP protokol (I.)

Spanning Tree Protocol – hľadanie kostsry



STP protokol (II.)

- BPDU (Bridge Protocol Data Unit) multicastové rámce (MAC 01:80:C2:00:00:00) pre komunikáciu medzi prepínačmi na nájdenie kostry siete
- každé 2 sekundy sa posiela:
 - ID koreňového prepínača (8 B)
 - cena cesty ku koreňu (4 B)
 - ID prepínača (8 B)
 - ID portu (2 B)

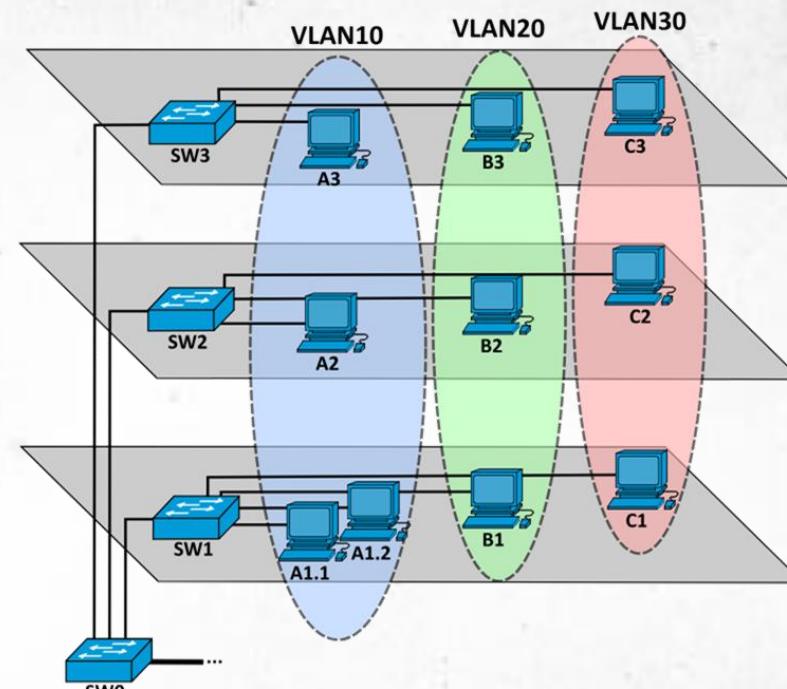
Stav portu	Popis
Disabled	Konfiguruje rámce; neučí sa nové adresy; neprijíma a nespracováva BPDU.
Blocking	Konfiguruje rámce; neučí sa nové adresy; prijíma a spracováva BPDU
Listening	Konfiguruje rámce; neučí sa nové adresy; prijíma, spracováva a prenáša BPDU.
Learning	Konfiguruje rámce; učí sa nové adresy; prijíma, spracováva a prenáša BPDU.
Forwarding	Vedie rámce ďalej, učí sa nové adresy; prijíma, spracováva a prenáša BPDU.

https://sk.wikipedia.org/wiki/Spanning_Tree_Protocol



VLAN

- vytváranie virtuálnych LAN (broadcastové domény)
 - statické vytvorenie VLAN broadcastových domén
 - dynamické vytváranie na základe prijatých značiek
 - podľa portov prepínača
 - podľa MAC adres
 - podľa protokolov
- IEEE 802.1Q – tagované VLAN
 - VLAN hopping



https://upload.wikimedia.org/wikipedia/commons/a/a3/VLAN_Concept.svg





MacSEC

- IEEE 802.1AE MACsec
 - MAC Security Entities
 - MACsec Key Agreement
- šifrovanie a integrita
- autentifikácia

```
ip link add link dev macsec0 type macsec
ip macsec add macsec0 tx sa 0 pn 1 on key 01
12345678901234567890123456789012
ip macsec add macsec0 rx address AA:BB:CC:DD:EE:FF port 1
ip link set dev macsec0 up
```





multiprotokolové prepínanie

Multi Protocol Label Switching

- k paketu sa pridá (label)
- dokáže prenášať rôzne typy sieťových protokolov (IP, Ethernet, ATM, Frame Relay) v rámci jednej MPLS infraštruktúry, čo zjednodušuje sieťové operácie
- 2,5-ta vrstva OSI modelu



LLDP

Link Layer Discovery Protocol (LLDP)

- IEEE 802.1AB
- umožňuje sieťovým zariadeniam oznamovať svoje schopnosti, identitu a konfiguráciu priamo pripojeným susedom v sieti LAN

```
▼ Ethernet II, Src: 12:34:56:78:90:ab (12:34:56:78:90:ab), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
  ▼ Destination: LLDP_Multicast (01:80:c2:00:00:0e)
    Address: LLDP_Multicast (01:80:c2:00:00:0e)
    .... ..0. .... .. = LG bit: Globally unique address (factory default)
    .... ..1. .... .. = IG bit: Group address (multicast/broadcast)
  ▼ Source: 12:34:56:78:90:ab (12:34:56:78:90:ab)
    Address: 12:34:56:78:90:ab (12:34:56:78:90:ab)
    .... ..1. .... .. = LG bit: Locally administered address (this is NOT the factory default)
    .... ..0. .... .. = IG bit: Individual address (unicast)
  Type: 802.1 Link Layer Discovery Protocol (LLDP) (0x88cc)
> Link Layer Discovery Protocol
0000  01 80 c2 00 00 0e 12 34 56 78 90 ab 88 cc 02 07  ....4 Vx..
0010  04 12 34 56 78 90 ab 04 07 03 12 34 56 78 90 ab  ..4Vx... 4Vx..
0020  06 02 0e 11 fe 09 00 12 0f 01 03 00 01 00 00 fe  ....

Type (eth.type), 2 byte(s) | Packets: 20768 · Displayed: 1 (0.0%) | Profile: Default
```





VLAN (I.)

- Virtual Local Area Network
- Oddelenie sietí bez potreby použitia L3 zariadenia (Smerovač, MLS)
- Oddelenie dátových tokov do konkrétnych rozhraní (dáta, hlas, IPTV)
- Identifikovaná číslom (VLAN ID) z rozsahu 1 - 4096





Typy VLAN

- Dátová
- Natívna
- Predvolená (defaultná)
- Hlasová (voice)
- Menežment
- Parkovacia (blackhole)





Dátová VLAN

- Prenos dát (internetový prístup)



PLÁN [OBNOVY]





Natívna VLAN

- Prenáša neznačkované dáta
- Predvolené VLAN ID = 1



PLÁN [OBNOVY]





Predvolená VLAN

- Nakonfigurovaná v každom prepínači od výroby
- Zabezpečuje základnú činnosť prepínača, ak ho nevieme/nemôžeme konfigurovať
- Predvolené VLAN ID = 1



PLÁN [OBNOVY]





Hlasová VLAN

- Použitie pri nasadení VoIP
 - Potrebné dodržať isté parametre siete (priepustnosť, oneskorenie)
 - Nutné oddeliť od ostatných (bezpečnosť)



PLÁN [OBNOVY]





Menežment VLAN

- Slúži na správu (lokálnu alebo vzdialenú) prepínačov pri realizácii VLAN
- Nutné oddeliť (bezpečnosť)





Parkovacia VLAN

- Slúži na umiestnenie nepoužitých rozhraní prepínača



PLÁN [OBNOVY]





Rozsahy VLAN

- Štandardný
 - VLAN 1 – 1005
 - VLAN 1 a VLAN 1001 – 1005 majú špeciálny účel
- Rozšírený
 - VLAN 1006 – VLAN 4096





Typy rozhraní vo VLAN

- **Access**

- pripojenie koncových zariadení
- pripojenie smerovača (dnes sa nepoužíva)
- prenáša informácie len z 1 konkrétnej VLAN

- **Trunk**

- pripojenie viacerých vlanov





Typy rozhraní vo VLAN

- Access
- Trunk
- Hybrid





Access rozhrania

- Pripojenie koncových zariadení
- Pripojenie smerovača
 - Legacy inter-vlan Routing (dnes sa nepoužíva)
- Prenáša informácie len z 1 konkrétnej VLAN





Trunk rozhrania

- Pripojenie ďalšieho prepínača
- Pripojenie ďalšieho smerovača
 - Router on a Stick
- Prenáša informácie z viacerých príp. všetkých VLAN



PLÁN [OBNOVY]





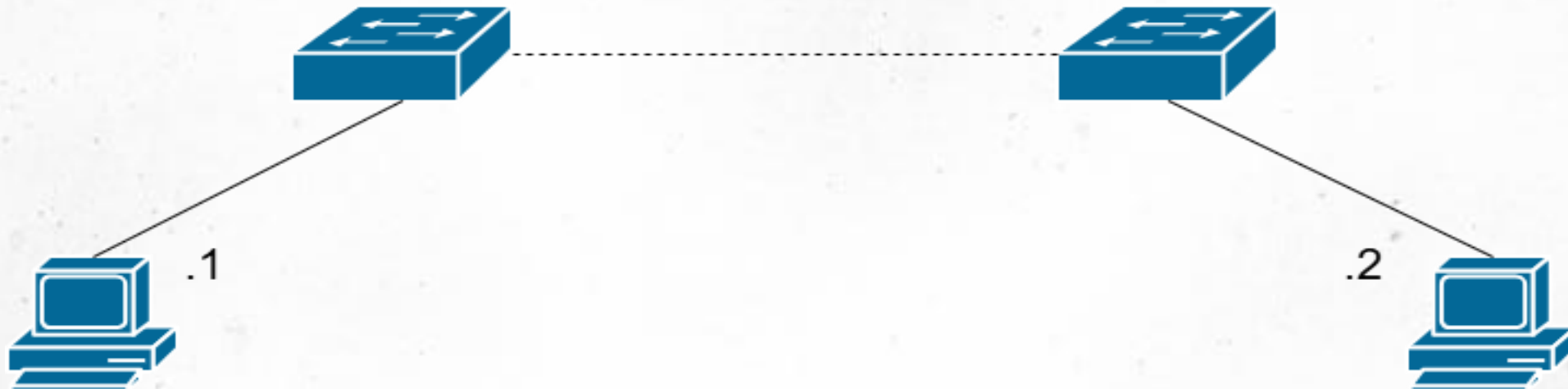
Aktivita – MikroTik a VLAN

- Pracovní list číslo 3
 - v tomto pracovnom liste využijete vedomosti z konfigurácie VPN protokolu PPTP (klient-server) a L2TP (klient-server) z predošlých aktivít.
 - taktiež využijete teoretické vedomosti z témy VPN.
 - pracovný list sa skladá z miesta pre zakreslenie sieťovej topológie, postupu pre generovanie a export certifikátov, postupu pre konfiguráciu VPN servera, postupu pre inštaláciu OpenVPN klienta, editáciu a načítanie konfiguračného súboru a postupu pre overenie fungovania konfigurácie.



Topológia

172.24.12.0/26



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY





UNIVERZITA
PAVLA JOZEFA ŠAFÁRIKA
V KOŠICIACH



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ďakujeme za pozornosť

