KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sieťová a komunikačná bezpečnosť

02 Bezpečnosť prenosu údajov na spojovej úrovni komunikačného modelu

KCKB UPJS CSIRT UPJS

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

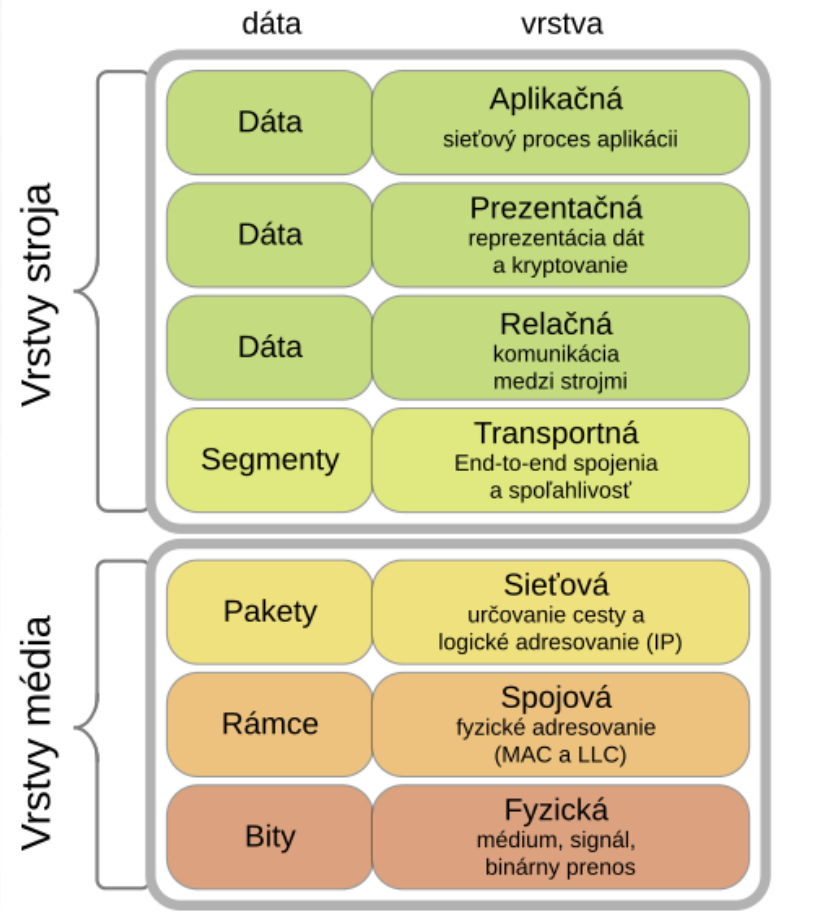
Bezpečnosť prenosu údajov na spojovej úrovni komunikačného modelu

- 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

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

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

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

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

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

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

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

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

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

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

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

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

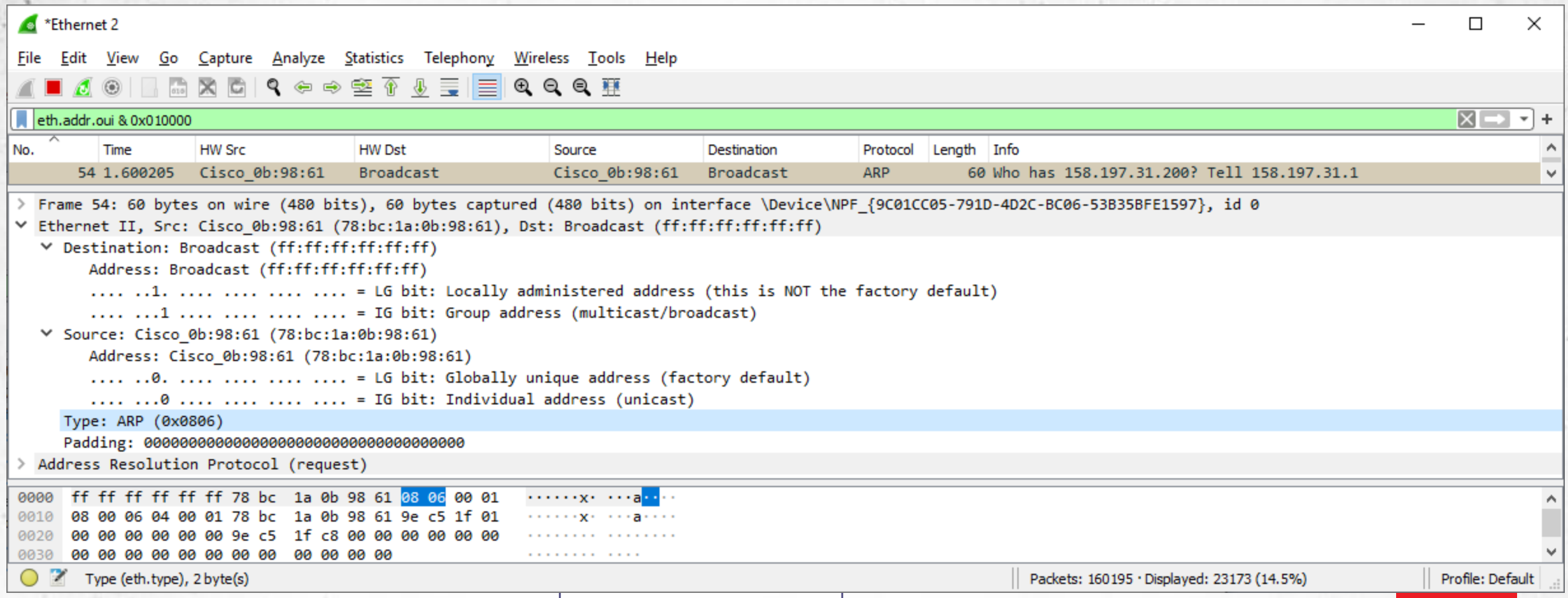
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

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 deliminiter)
  - 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)

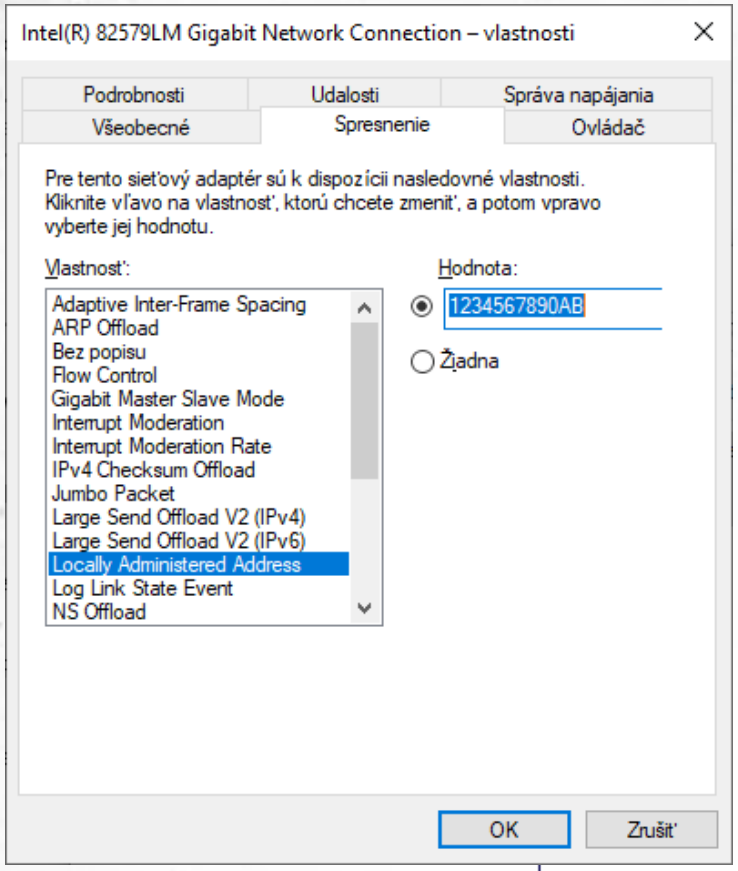
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ethernetový rámec



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ethernetový rámec – zmena MAC

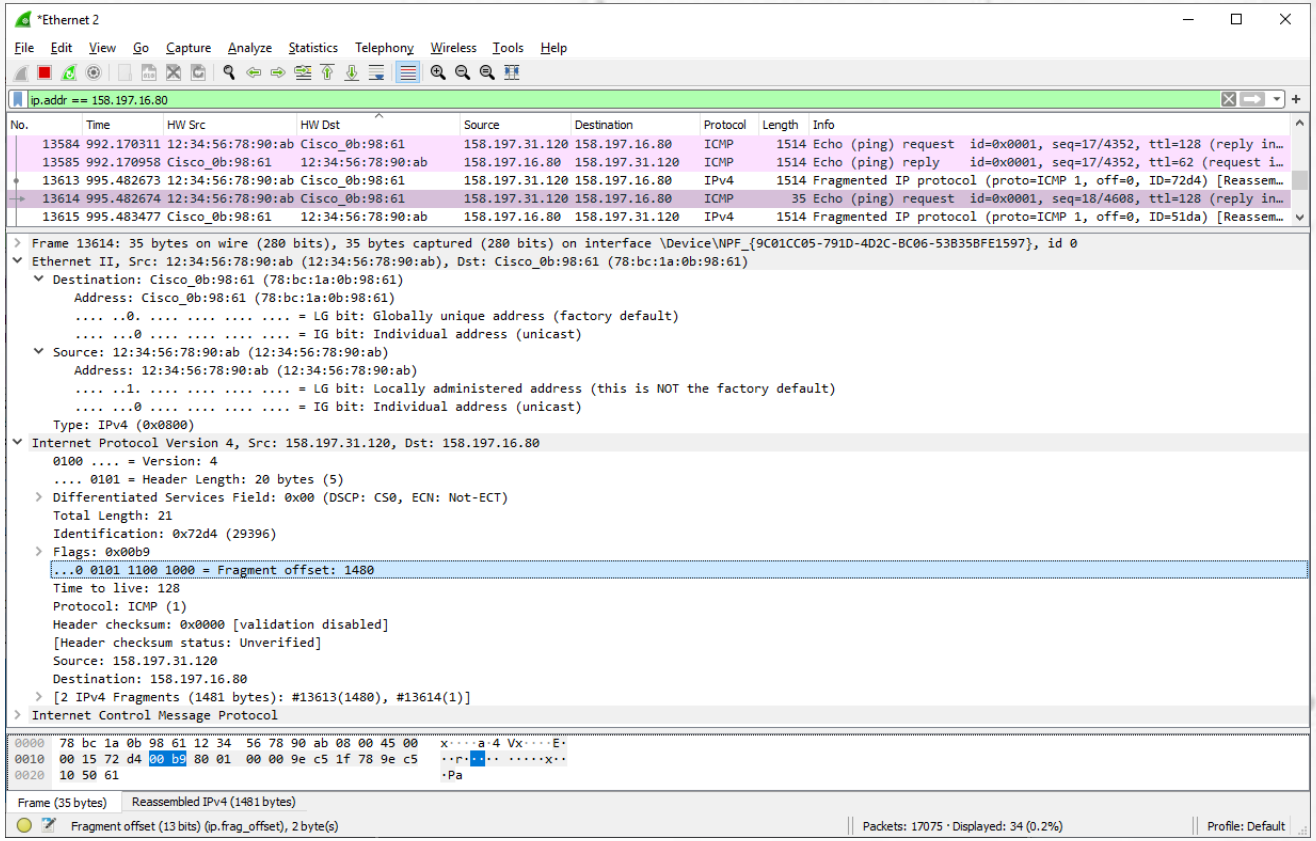



```
ip link set dev address
02:01:02:03:04:08
```

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

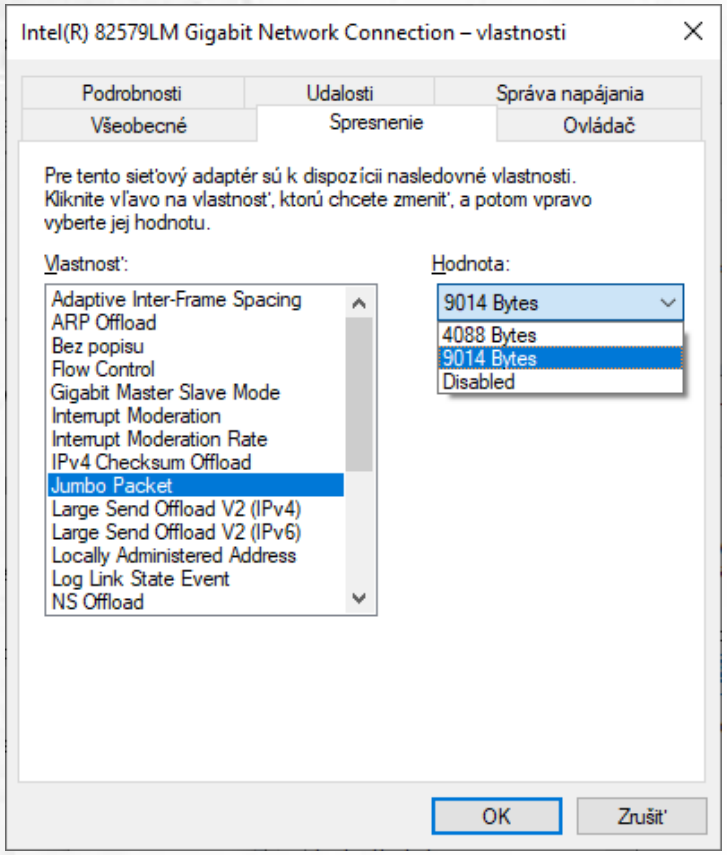
Jumbo rámce

- pakety vyšších vrstiev musia byť rozdelené do viacerých rámcov



Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

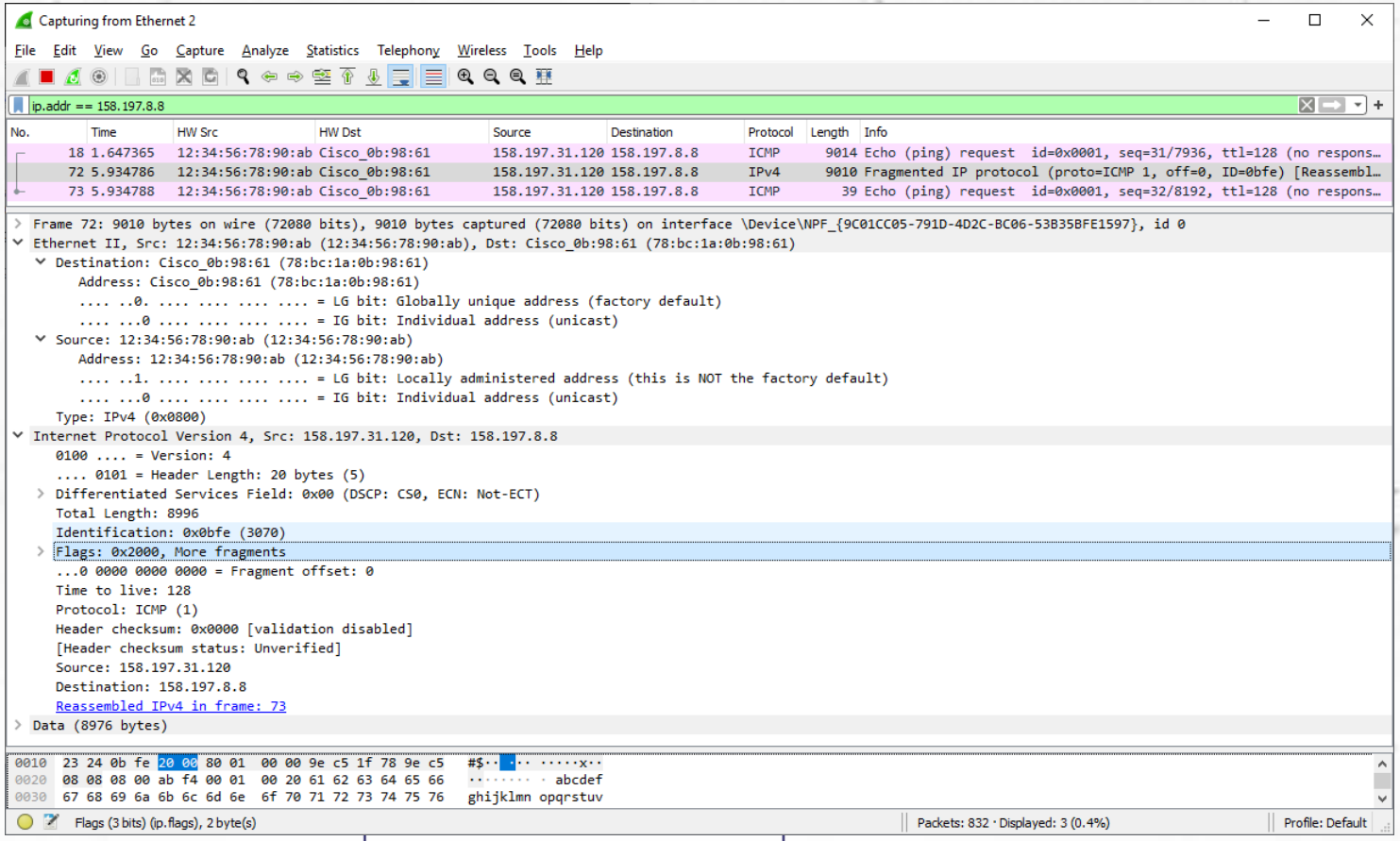
Jumbo rámce




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

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

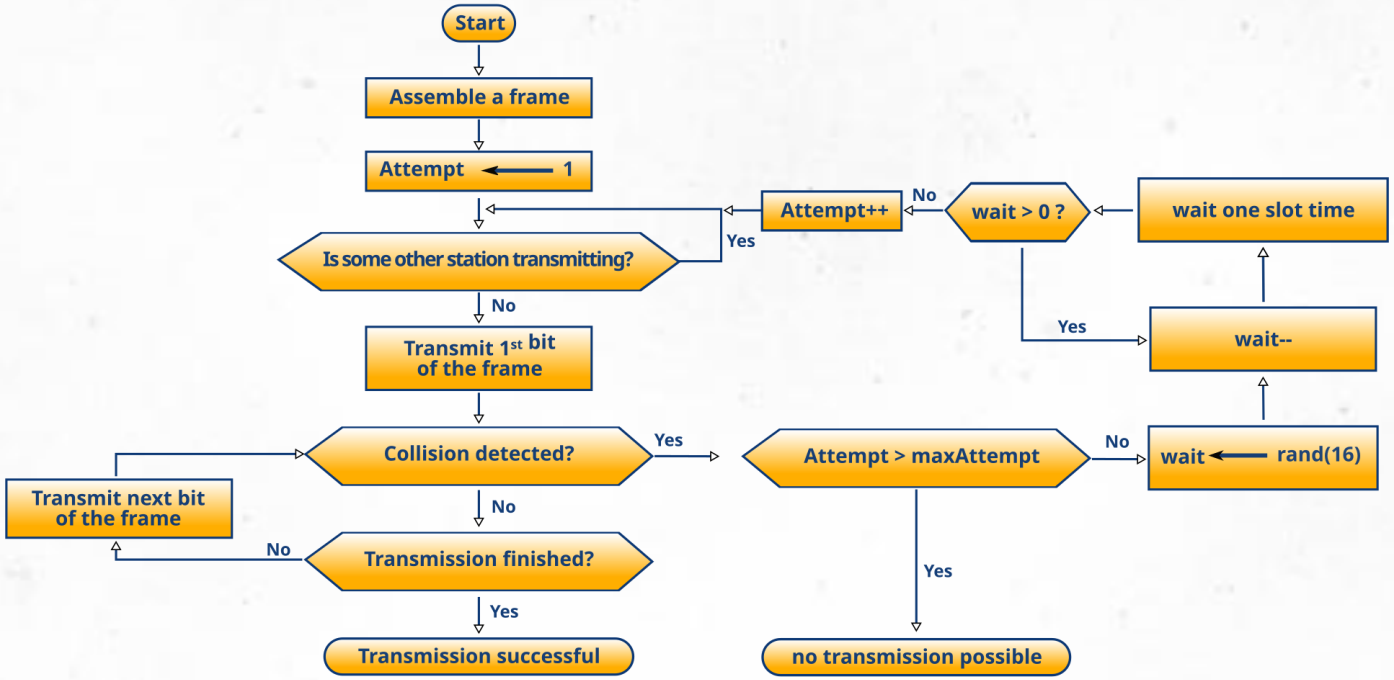
Jumbo rámce



Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kolízne domény

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

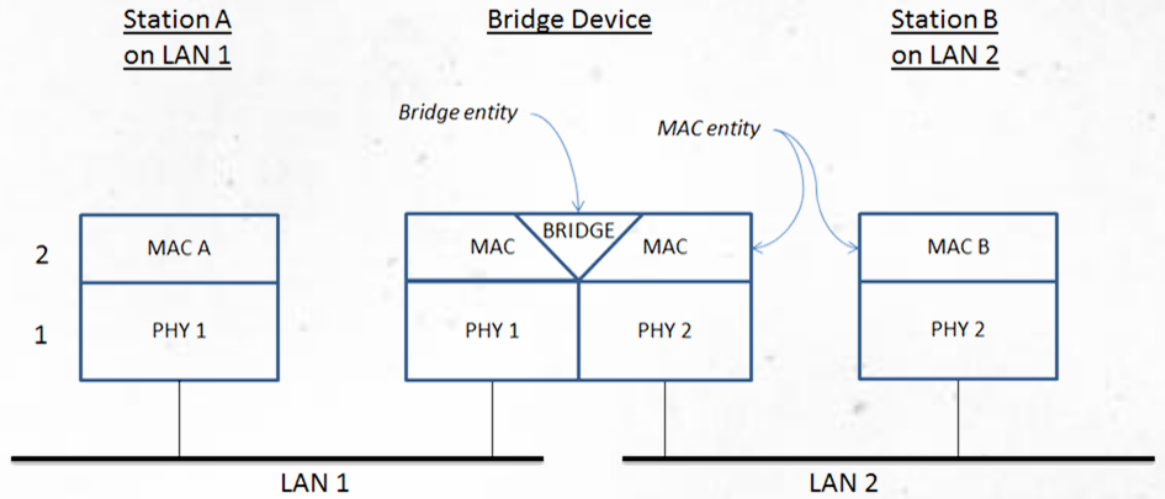


https://upload.wikimedia.org/wikipedia/commons/thumb/3/37/CSMACD-Algorithm.svg/1920px-CSMACD-Algorithm.svg.png

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

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



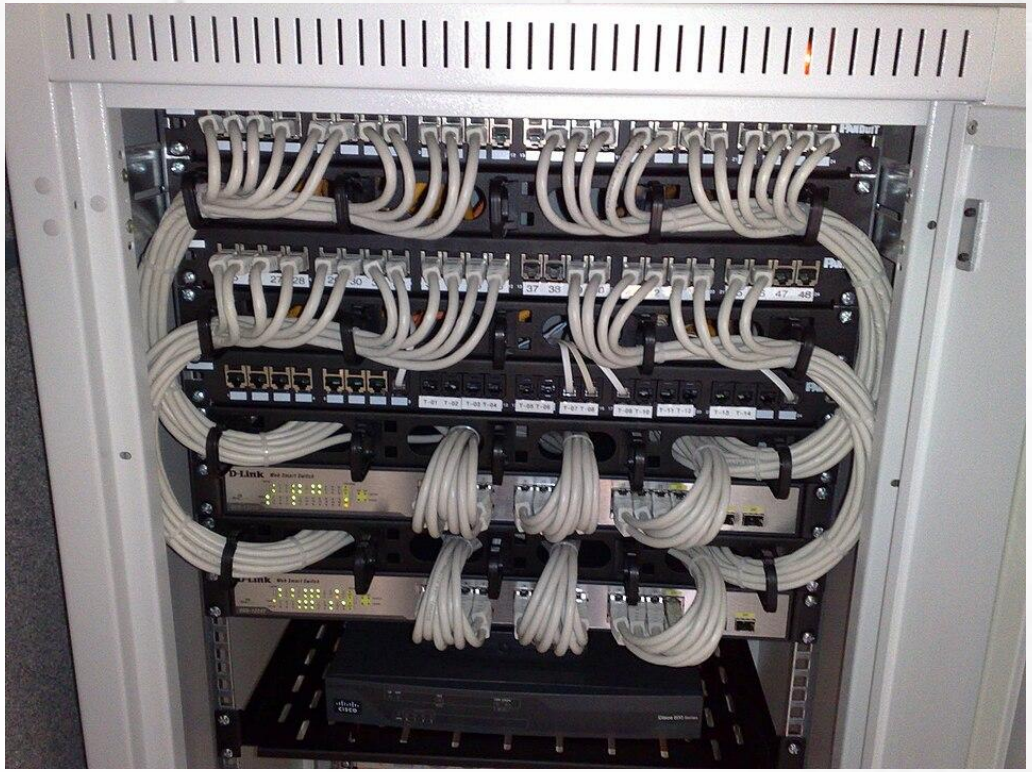
- metódy:
- store and forward
- cut through
- fragment free
- adaptive switching

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Prepínač

- prepínač (switch)
  - full-duplex komunikácia
  - viacportový most
  - prepínacia tabuľka (MAC-port)
  - problém zacyklenia rieši STP

- V prípade zaplenia tabuľa sa prepne na rozbočovač

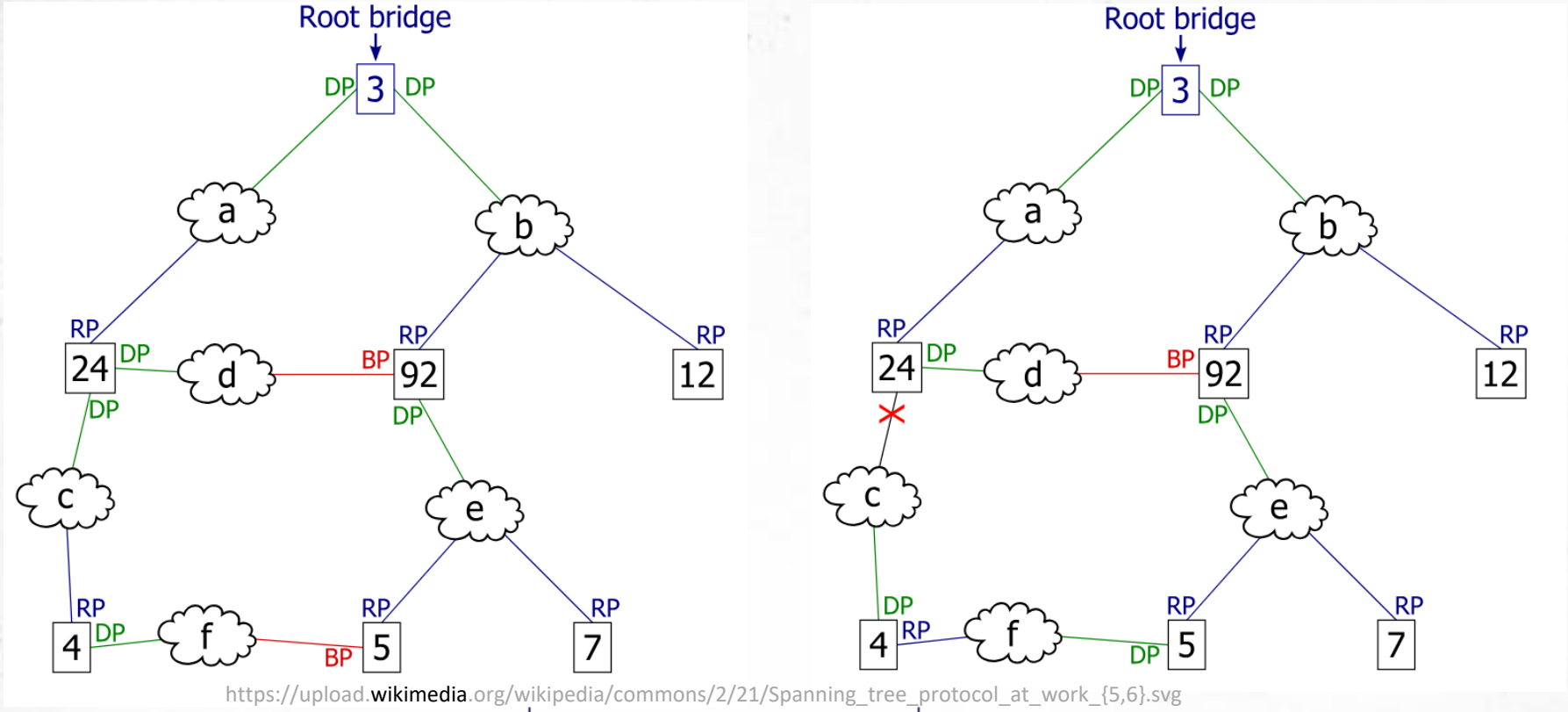


https://upload.wikimedia.org/wikipedia/commons/b/bc/19-inch_rackmount_Ethernet_switches_and_patch_panels.jpg

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

STP protokol (I.)

Spanning Tree Protocol – hľadanie kostsry



https://upload.wikimedia.org/wikipedia/commons/2/21/Spanning_tree_protocol_at_work_{5,6}.svg

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

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; nepríjma 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.

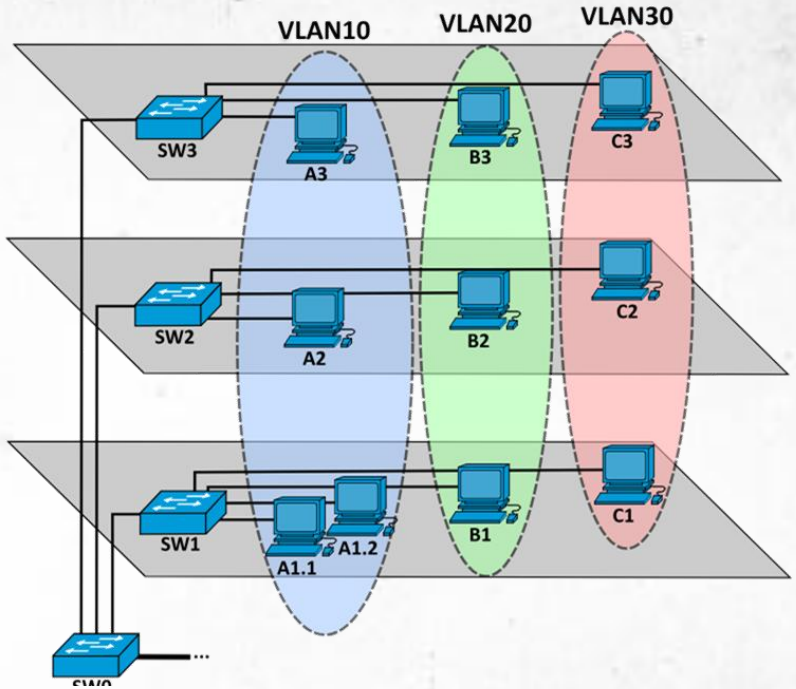
https://sk.wikipedia.org/wiki/Spanning_Tree_Protocol

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

VLAN

- vytváranie virtuálnych LAN (broadcastové domény)
  - statické vytvorenie VLAN broadcastových domén
  - dynamické vytváranie na základe prijatých značiek
    - podľa portov prepínača
    - podľa MAC adries
    - podľa protokolov

- IEEE 802.1Q – tagované VLAN
  - VLAN hopping



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

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

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
```

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

multiprotokolové prepínanie

Multi Protocol Label Switching

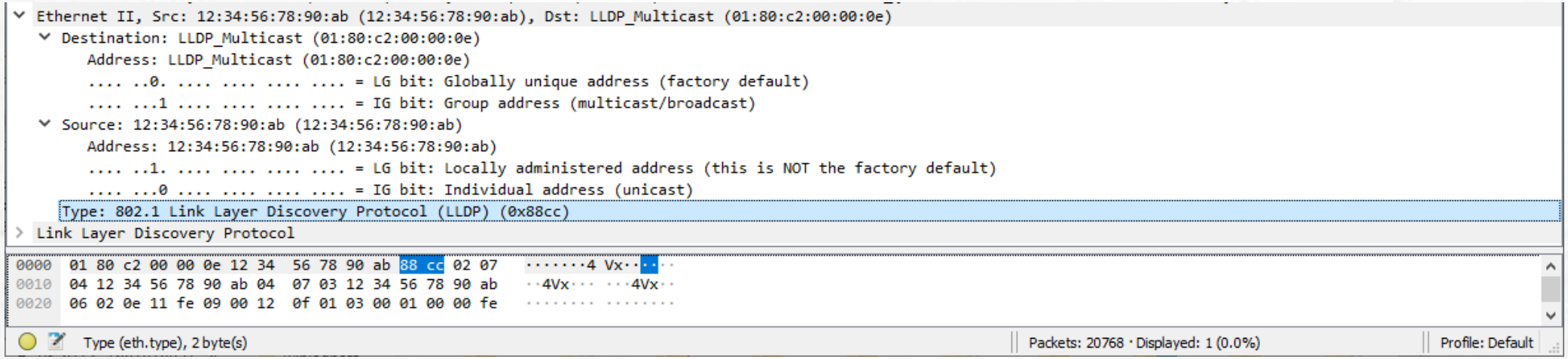
- k paketu sa pridá (label)
- dokáže prenášať rôzne typy sieťových protokolov (IP, Ethernet, ATM, Frame Relay) v rámci jednej MPLS infraštruktúry, čo zjednodušuje sieťové operácie
- 2,5-ta vrstva OSI modelu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

LLDP

Link Layer Discovery Protocol (LLDP)

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



Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

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

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Typy VLAN

- Dátová
- Natívna
- Predvolená (defaultná)

- Hlasová (voice)
- Menežment
- Parkovacia (blackhole)

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Dátová VLAN

- Prenos dát (internetový prístup)

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Natívna VLAN

- Prenáša neznačkované dáta
- Predvolené VLAN ID = 1

Predvolená VLAN

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

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Hlasová VLAN

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

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Menežment VLAN

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

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Parkovacia VLAN

- Slúži na umiestnenie nepoužitých rozhraní prepínača

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Rozsahy VLAN

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

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Typy rozhraní vo VLAN

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

- **Trunk**
  - pripojenie viacerých vlanov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Typy rozhraní vo VLAN

- Access
- Trunk
- Hybrid

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Access rozhrania

- Pripojenie koncových zariadení
- Pripojenie smerovača
  - Legacy inter-vlan Routing (dnes sa nepoužíva)

- Prenáša informácie len z 1 konkrétnej VLAN

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Trunk rozhrania

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

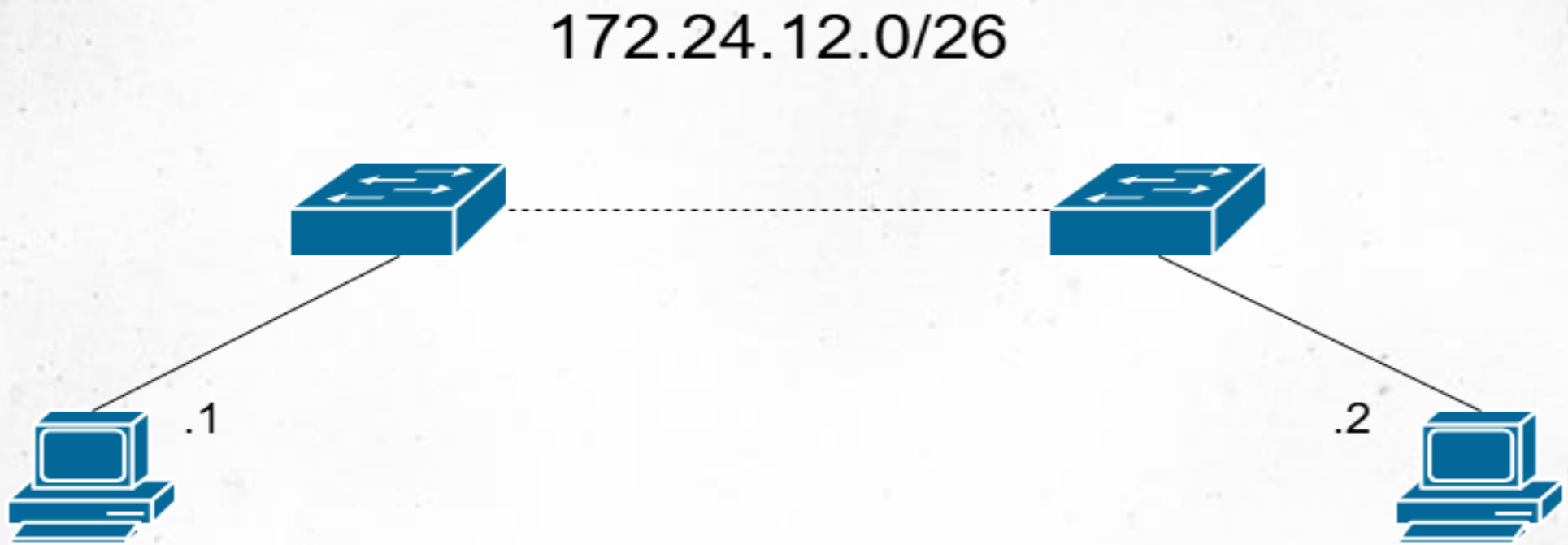
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Aktivita – MikroTik a VLAN

- Pracovný 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.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Topológia



Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujeme za pozornosť