Základy sieťových technológií

Predstavenie

Andrej Hyben

- Člen oddelenia oSBATA na SITVS
- Pracujem so sieťovými technológiami od roku 2012 :
  - 1 Rok v Orange-i na L1
  - 5 rokov v Deutsche Telekome na L2 a L3
  - 5 rokov vo firme ngena, ktorá sa zaoberá automatizáciou sieťových technológií, no hlavne SDWAN, kde som pôsobil ako Platform Architekt
  - Od 01.07.2023 pracujem na MIRRI full-time
- V ngene sme mali projekt, kde sme pomáhali lokálnej komunite v Košiciach. V rámci tohto projektu som 2 roky učil základy sieťových technológií na Gymnáziu Katkin Park 2.

Agenda na dnes

1. Úvod do sieťových technológií
    1. Kedy a ako bola technológia objavená
    2. Ako to vyzerá v produkcií
    3. Ako vyzerá kabeláž
    4. Aká je rôznorodosť prác v sieťových technológiách

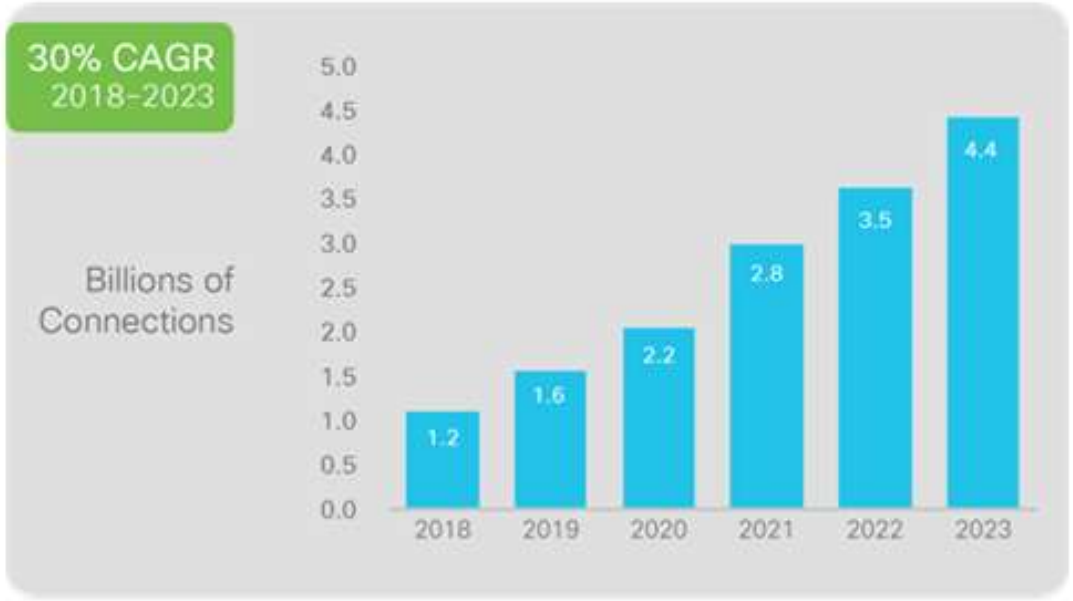
2. Základy
    1. TCP/IP a ISO/OSI modely
    2. Fyzická vrstva
    3. Predstavenie 2 a 3 vrstva

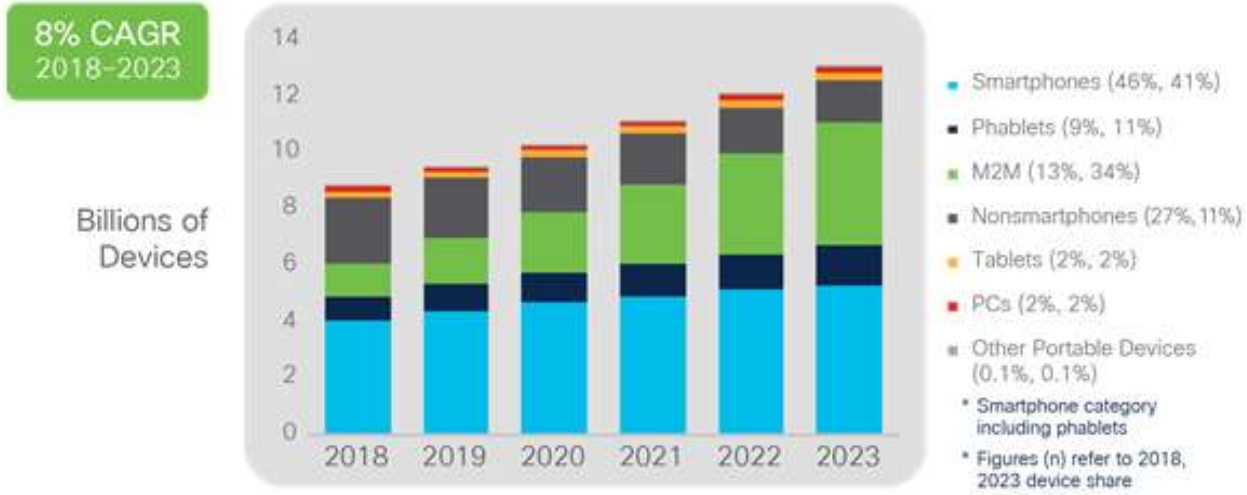
3. Data-Linková vrstva
    1. MAC adresa
    2. Frame
    3. Switch
    4. VLAN a Trunk
    5. Prenos dát cez switch

4. Sieťová vrstva
    1. IP adresa
    2. ARP
    3. Prenos dát cez router
    4. Protokoly : DHCP, ARP
5. IP subnetting

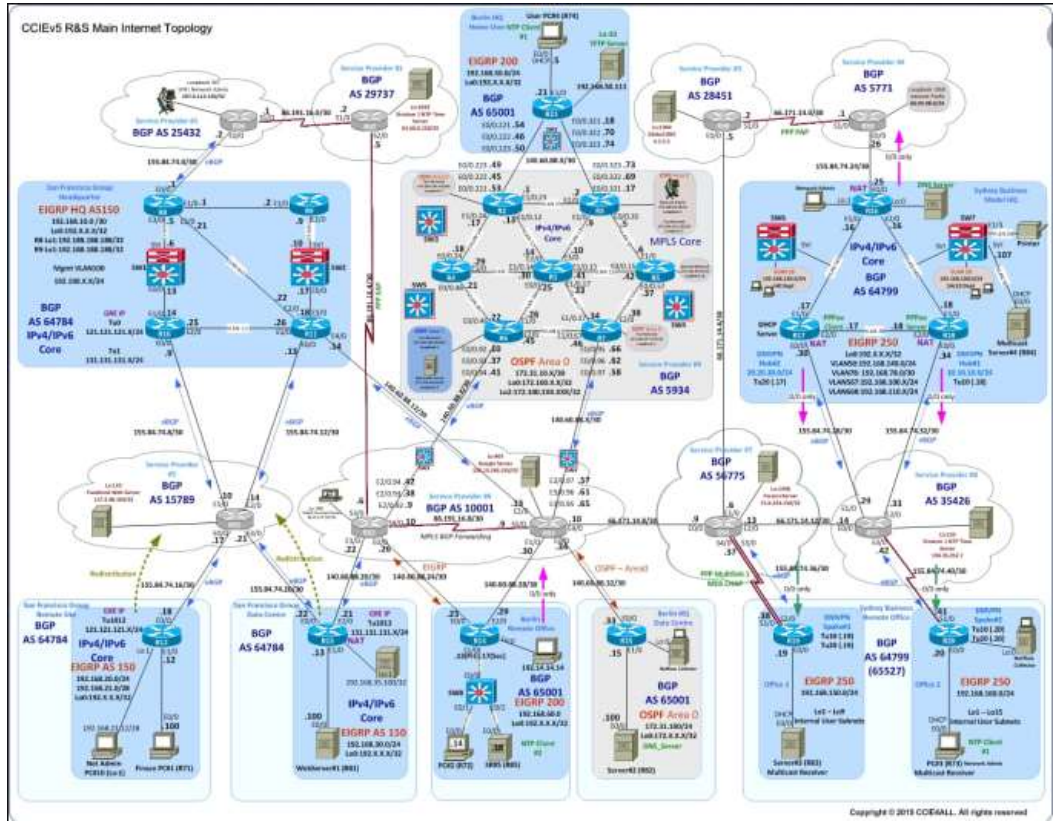
História sieťových technológií

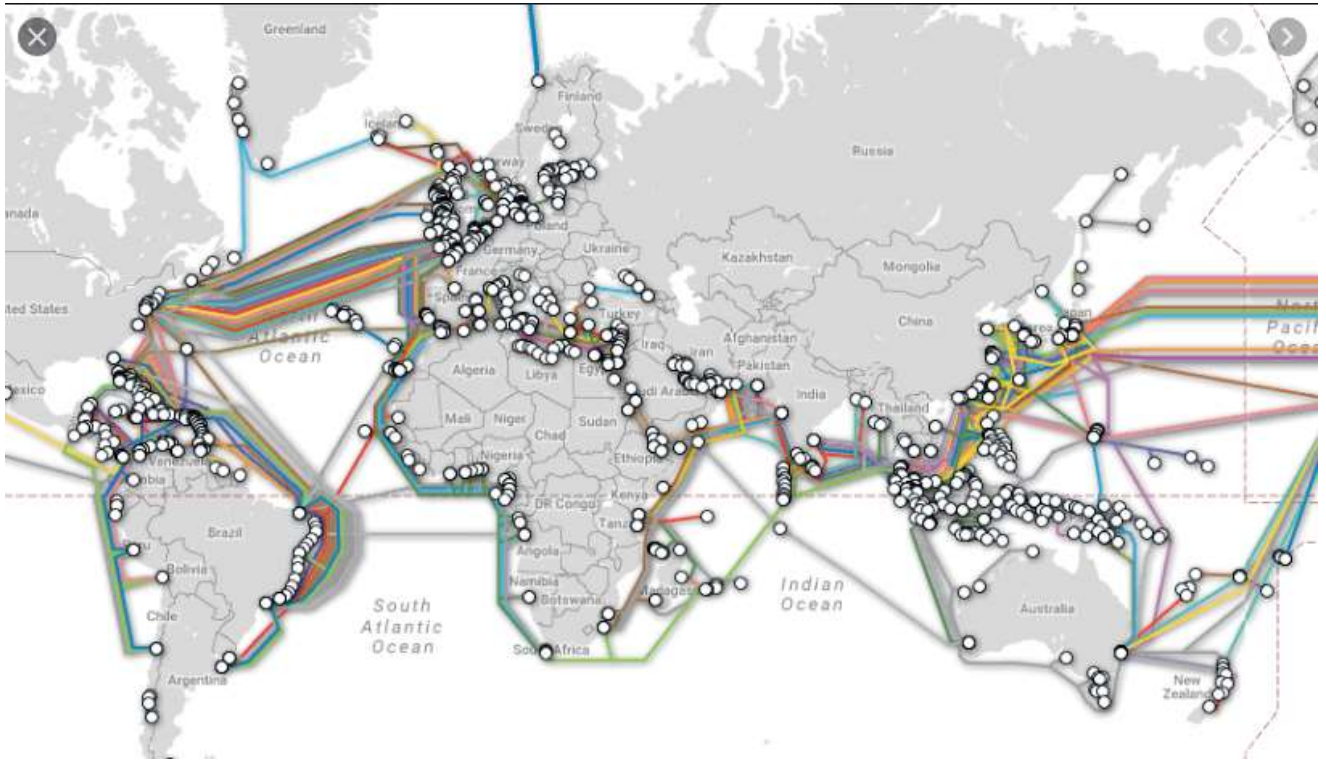
- Prečo potrebujeme internet ?
  - Rýchle zdieľanie informácií skrz planétu
- Kedy bol internet spustený ?
  - ARPANET 1969
    - Advanced Research Project Agency at MIT
  - Prvý packet switching network
- Ako sa to v čase vyvíjalo ?
- Ako rastie dnes ?





Ako to vyzerá #01

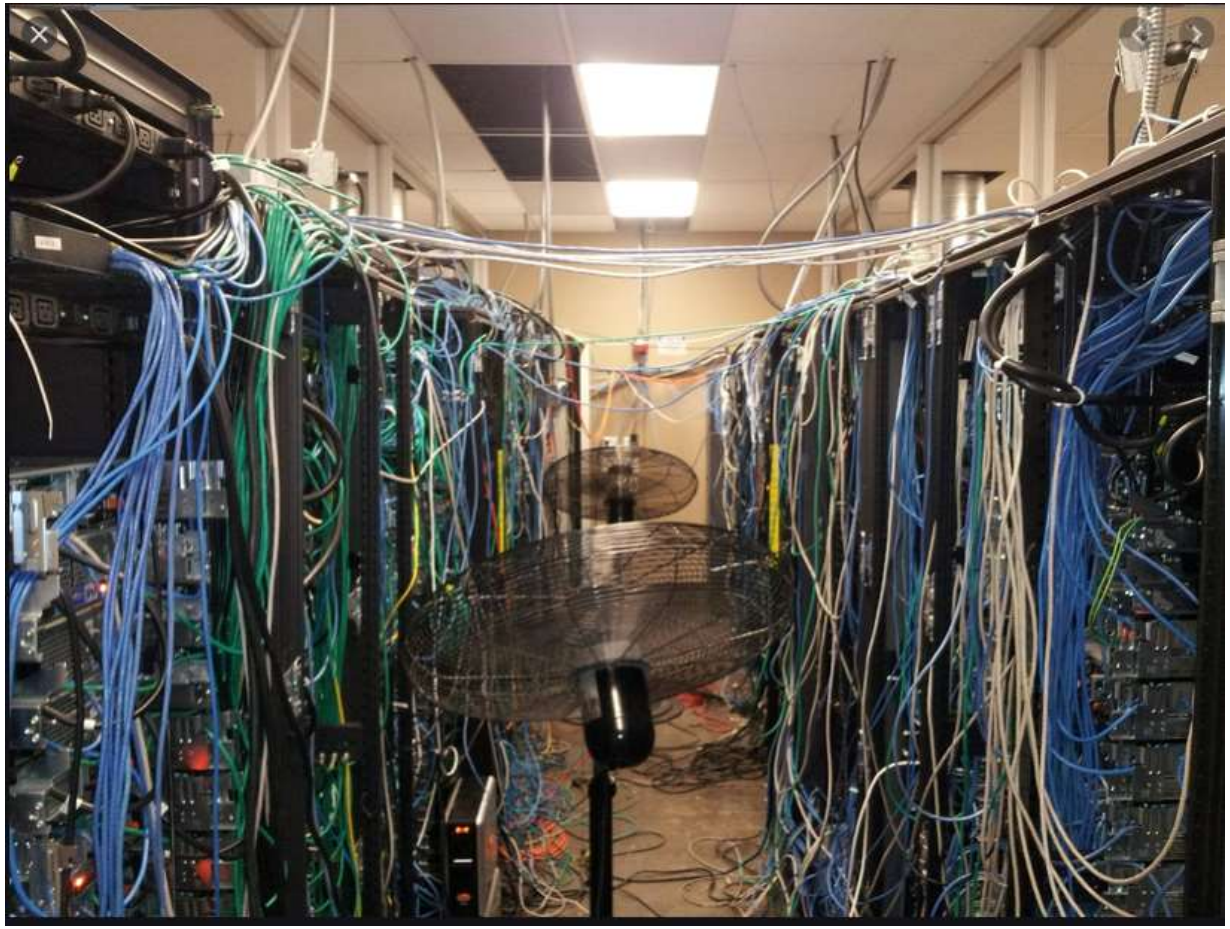


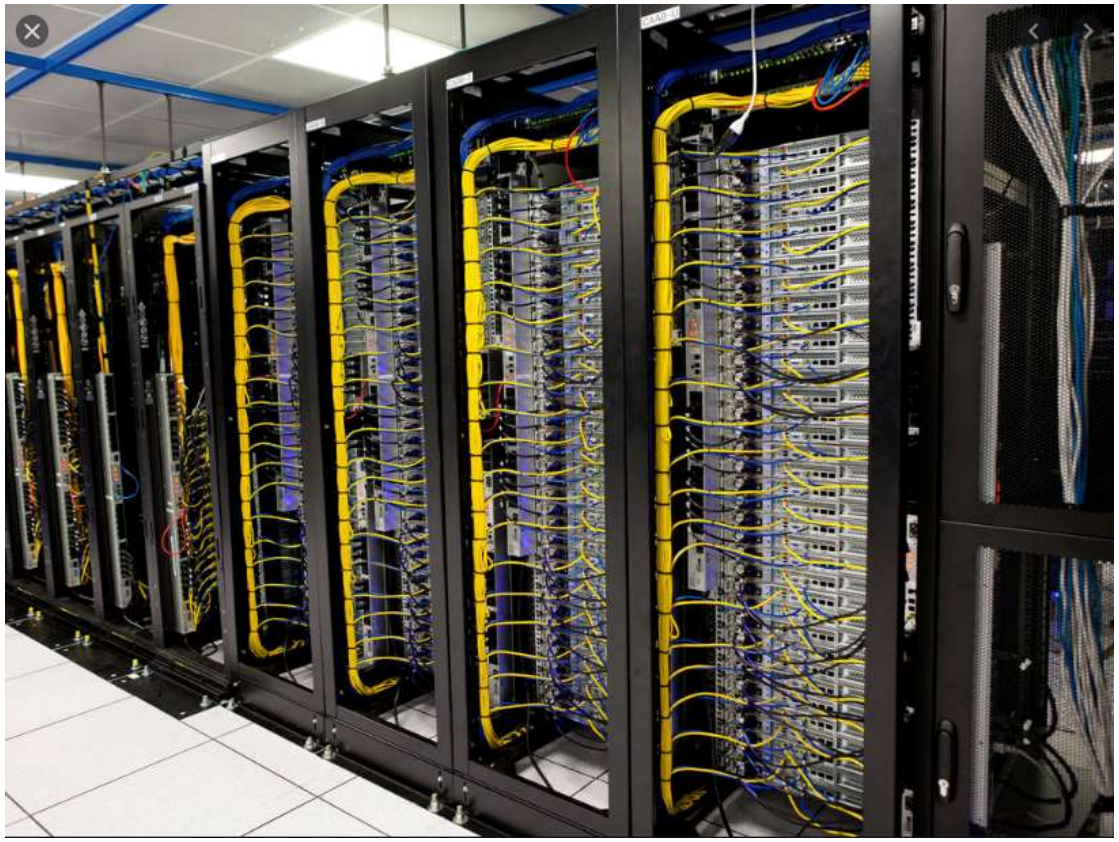


Ako to vyzerá #02

- Zariadenia môžu byť malé (pre domácnosti), väčšie pre kancelárie a najväčšie pre internetových poskytovateľov.

Ako to vyzerá #03





Pracovné pozície v sieťových technológiách

- Sú rôzne typy prác, ktoré sú delené na horizontálnej úrovni :
  - Service Provider (IPS)
  - Data Center
  - Local Administrators (Internal IT)
  - Collaboration (Voice & Video technológie)
  - Cloud Networking
    - Google (GCP), Amazon (AWS), Microsoft (Azure), e.t.c.
  - Security
    - Každá IT security pozícia vyžaduje aspoň nejaký level porozumenia so sieťovými technológiami
      - F.e. : Penetration Tester
  - Atď.

- Každá práca na horizontálnej úrovni má rozdelenie na vertikálnej úrovni :
  - Lead Architect
  - Architect
  - Solution Designer
  - Engineering
  - Operation
  - Support

Pravdaže názvy sa môžu meniť podľa implementácie.


MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY
Tak začnime !

Cisco & ich certifikačné skúšky

Čo je firma Cisco ?

- Firma, ktorá v podstate vymyslela sieťové technológie ako ich poznáme dnes
- Vytvorili väčšinu RFC (niečo ako vyhlášok) a sedia v komisií na schvaľovanie nových.

Čo je Cisco certifikácia ?

- Cisco má veľmi dobrý certifikačný program pre svojich zákazníkov a ich sieťových expertov.

Prečo by ste mali chcieť Cisco certifikáciu ?

1. Tieto certifikačné cesty sú pripravené pre záujemcov, ktorý sa chcú učiť o najnovších technológiách a pravidelne sa to aktualizuje.
2. Firmy, ktoré deklarujú isté počty zamestnancov s platným certifikátom, dostávajú veľké zľavy na zariadenia a podporu. (až ku 80 percentám)

Cisco certifications

Cisco has redesigned our training and certification programs to address today's dynamic technologies and prepare students, engineers, and software developers for success in the industry's most critical jobs.

Technology	Entry Use this as a starting point if you're interested in a career as a networking professional.	Associate Master the essentials needed to launch a rewarding career as a networking professional and realize your potential with the latest technologies.	Professional Select a core technology track and a focused concentration exam to customize your professional-level certification.	Expert Become an expert in your field by earning the most prestigious certification in the technology industry.
Collaboration	CCT Collaboration		CCNP Collaboration	CCIE Collaboration
CyberOps		CyberOps Associate	CyberOps Professional	
Data Center	CCT Data Center		CCNP Data Center	CCIE Data Center
DevNet (Dev and Automation)		DevNet Associate	DevNet Professional	DevNet Expert
Design				CCDE
Enterprise	CCT Routing & Switching	CCNA	CCNP Enterprise	CCIE Enterprise Infrastructure CCIE Enterprise Wireless
Security			CCNP Security	CCIE Security
Service Provider			CCNP Service Provider	CCIE Service Provider

Where can I learn for those certifications?

Čo bude na našom školení ?

- Prejdeme si len základy, ktoré sú súčasťou CCNA
- Ak sa chcete doučiť zvyšné veci z CCNA, tak podľa dostupných zdrojov to trvá približne 2 mesiace ak sa budete učiť aspoň pár hodín denne, 5 dní v týždni.

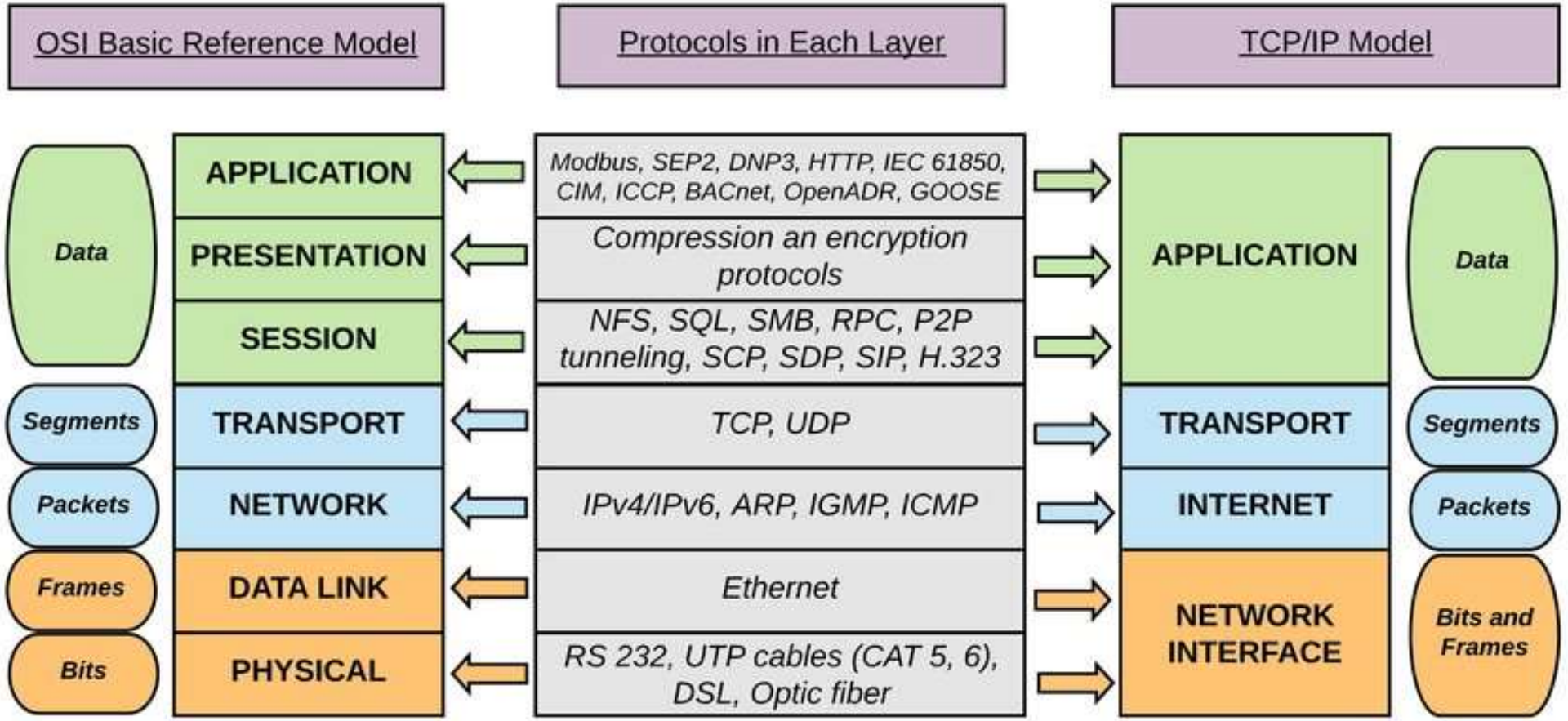
Kde sa to viete učiť zadarmo :

- Network Chuck : https://www.youtube.com/c/NetworkChuck
- Keith Barker : https://www.youtube.com/c/KeithBarker
- Jeremy Ciara : https://www.youtube.com/c/KeepingITSimple
- Jeff Kish : https://www.youtube.com/user/KishSquared

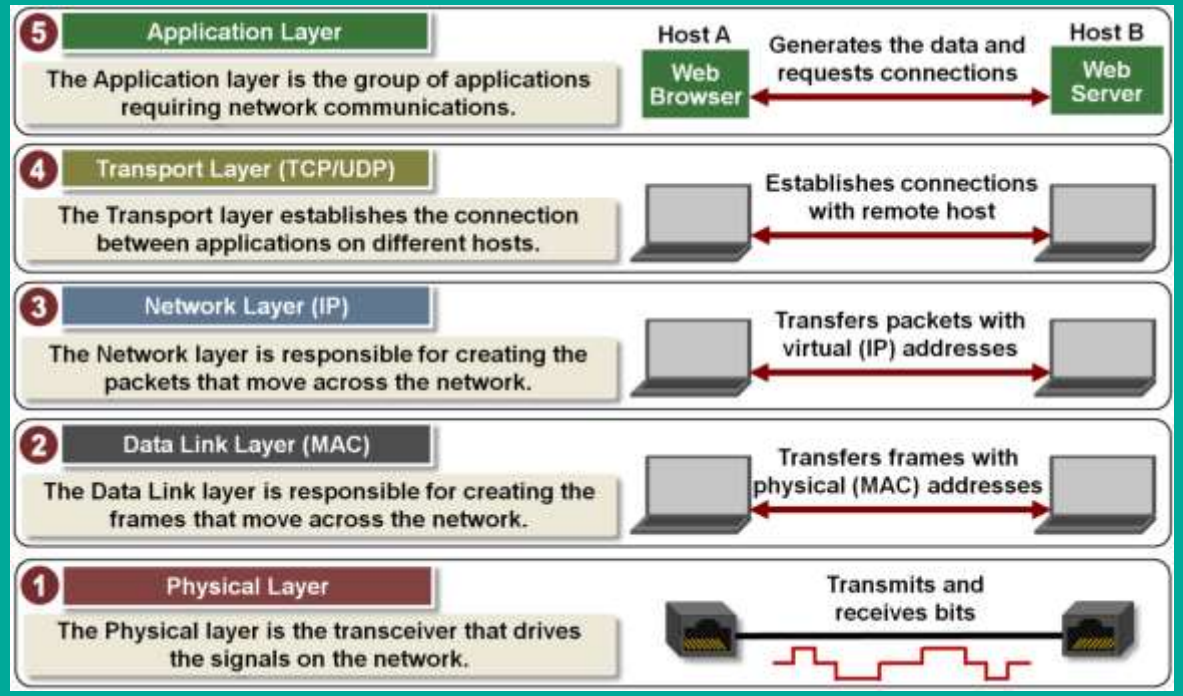
Kde sa dajú učiť komplexnejšie veci (platené služby):

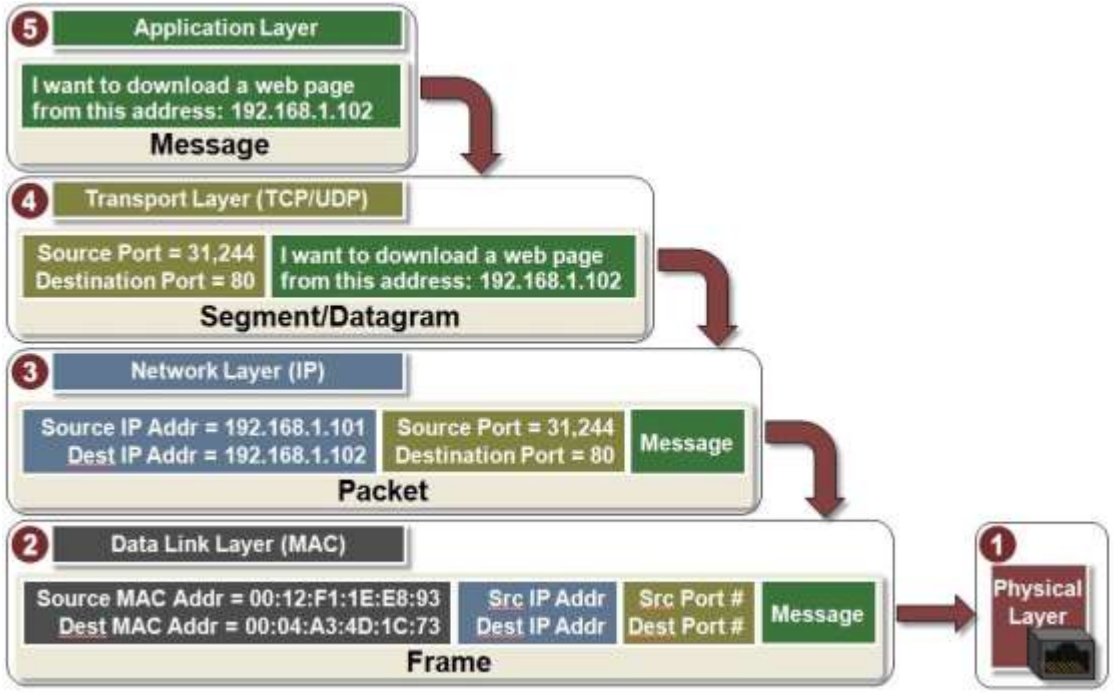
- Väčšina trénerov sú tí z youtube, ale na týchto stránkach je bonusový kontent.
- https://www.cbtnuggets.com/
- https://ine.com/
- https://www.udemy.com/

ISO OSI vs TCP / IP model



TCP IP model


5
Application Layer
The Application layer is the group of applications requiring network communications.
Host A
Web Browser
Generates the data and requests connections
Host B
Web Server
4
Transport Layer (TCP/UDP)
The Transport layer establishes the connection between applications on different hosts.
Establishes connections with remote host
3
Network Layer (IP)
The Network layer is responsible for creating the packets that move across the network.
Transfers packets with virtual (IP) addresses
2
Data Link Layer (MAC)
The Data Link layer is responsible for creating the frames that move across the network.
Transfers frames with physical (MAC) addresses
1
Physical Layer
The Physical layer is the transceiver that drives the signals on the network.
Transmits and receives bits


5
Application Layer
I want to download a web page from this address: 192.168.1.102
Message
4
Transport Layer (TCP/UDP)
Source Port = 31,244
Destination Port = 80
I want to download a web page from this address: 192.168.1.102
Segment/Datagram
3
Network Layer (IP)
Source IP Addr = 192.168.1.101
Dest IP Addr = 192.168.1.102
Source Port = 31,244
Destination Port = 80
Message
Packet
2
Data Link Layer (MAC)
Source MAC Addr = 00:12:F1:1E:E8:93
Dest MAC Addr = 00:04:A3:4D:1C:73
Src IP Addr
Dest IP Addr
Src Port #
Dest Port #
Message
Frame
1
Physical Layer

OSI model

- **Open Systems Interconnection (OSI) model** bol vytvorený **International Organization for Standardization (ISO)** a sformulovaný v roku 1984. Poskytoval prvý pohľad na to, ako by mal vyzerať prenos dát cez sieť.

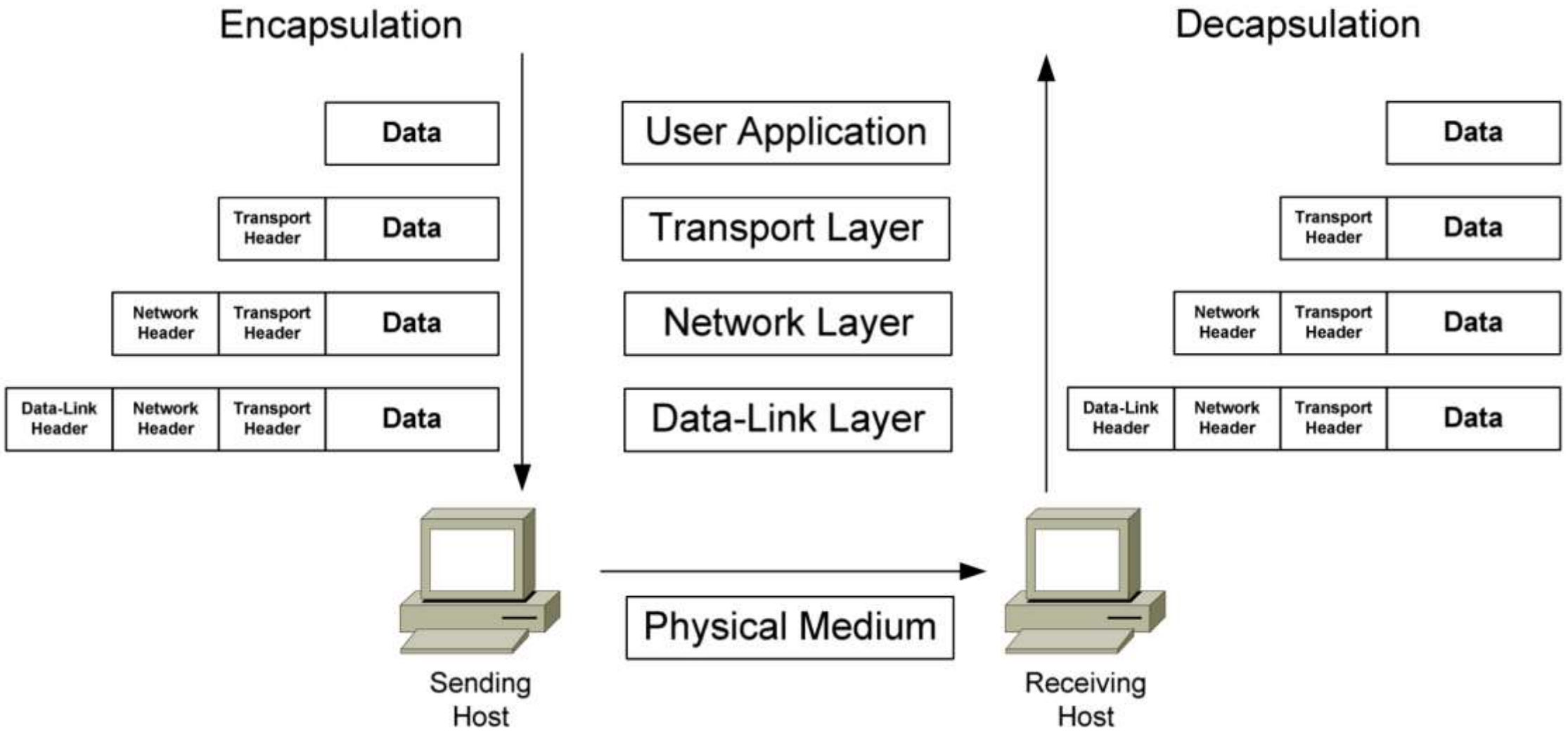
7	Application	**A**ll	**A**way
6	Presentation	**P**eople	**P**izza
5	Session	**S**eem	**S**ausage
4	Transport	**T**o	**T**hrow
3	Network	**N**eed	**N**ot
2	Data-link	**D**ata	**D**o
1	Physical	**P**rocessing	**P**lease

Protocol Datagram Units - PDUs

- Ako sa dáta posúvajú vo vrstvách z aplikačnej po fyzickú, každá vrstva si pridá vlastnú hlavičku, ktorá obsahuje informácie o použitom protokole v tejto vrstve. Výsledný objekt po pridaní hlavičky sa nazýva PDU, a tento proces sa volá **enkapsulácia**.
- Každá vrstva komunikuje so svojou korešpondujúcou vrstvou na strane prijímateľa. Príkladom je data-linková vrstva, pri ktorej je v hlavičke uvedená zdrojová a cieľová MAC adresa. Na strane prijímateľa sa rozozná, že ide o jeho MAC a preto ďalej **dekapsujuje** správu.

Layer	*PDU Name*
Application	-
Presentation	-
Session	-
Transport	**Segments**
Network	**Packets**
Data-Link	**Frames**
Physical	**Bits**

Encapsulation / Decapsulation



Fyzická vrstva

- Posiela a príma signály vo forme jednotiek a núl a to tak, aby rozoznával medzery medzi signálmi.
- Každé zariadenie pripojené k sieti má sieťovú kartu, ktorá funguje na fyzickej vrstve

- Existujú rôzne typy médií a rýchlosti :
  - Metalické káble :
    - Coaxial
    - Serial
    - Ethernet
      - 10Mbit/s - 10Gbit/s
  - Optické káble - 1Gbit/s – 400 Gbit/s
  - Wireless connectivity – Wi-Fi, WiMAX, GSM, Edge, HSDPA/HSUPA, LTE (4G), 5G, 6G

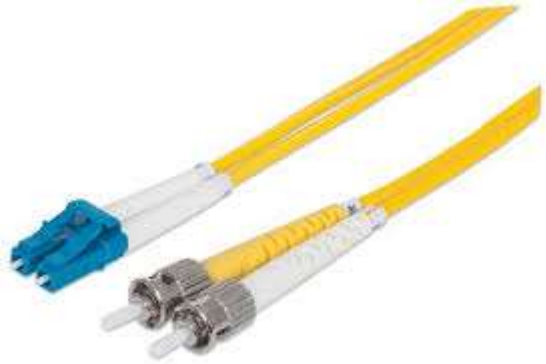
Physical Layer – Media types Quiz

Choose the right cable type :

- Coaxial
- Fiber
- DSL
- Ethernet
- Serial

A

B



C

D

E

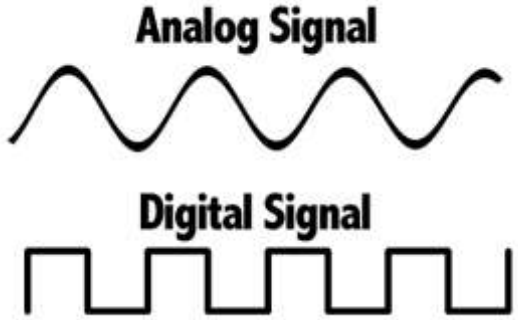
Fyzická vrstva– Typy vysielačov

Fyzická vrstva– Signály

- Posiela a prijíma signály na fyzickom kábli alebo anténe, aby prenieslo jednotky a nuly.
- Sú 2 typy signálov – Analógové (už nepoužívané) a Digitálne (reprezentované jednotkami a nulami)

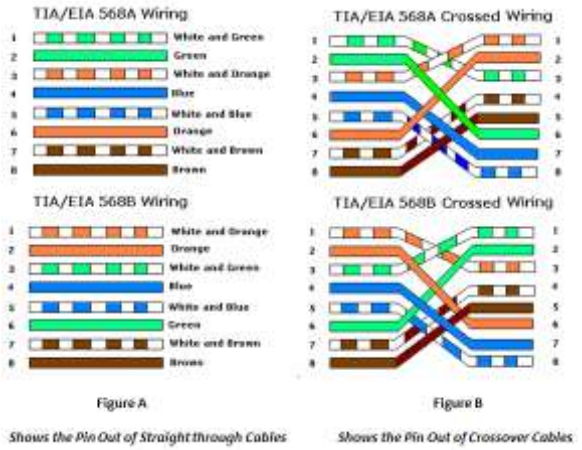
- Spôsoby prenosu dát:

1. Simplex
2. half-duplex
3. full duplex



Fyzická vrstva – Aké káble použiť?

- Existujú 3 základné typy káblov:
  - Priamy (Straight)
  - Krížený (Crossover)
  - Pretočený? (Rollover)



1. Pravidlo – zariadenia pracujúce na rovnakej vrstve sa prepájajú kríženým káblom1st rule
2. Pravidlo – zariadenia pracujúce na iných vrstvách sa prepájajú priamym káblom

Príklady – router <--> router – krížený, switch <--> switch – krížený; PC <--> PC router – krížený;
Router <-->switch – priamy; PC <--> switch – priamy; **PC <--> router - krížený**

Dôležitá informácia: dnes už nie je dôležité, či dáte medzi 2 zariadenia priamy alebo krížený kábel, pretože výrobcovia sieťových kariet vymysleli mechanizmus na úrovni čipov. V Datacentrách ale stále treba dávať pozor, lebo zámena priameho a kríženého kábla môže spôsobovať výkonnostné problémy.

Základné sieťové kontroly na počítačoch

Windows 10 :

- Ako otvoriť CLI ?
  - Kliknúť na štart a hľadať cmd
- Ako skontrolovať status interface-u?
  - netsh int show int
- Ako skontrolovať nastavenie interface-u?
  - ipconfig
  - ipconfig /all
- Ako skontrolovať nastavenie routing-u?
  - netstat –rn
- Ako skontrolovať otvorené porty?
  - netstat –an
  - netstat –an | findstr *
- Ako vykonať základné sieťové kontroly?
  - ping www.google.com
  - tracert www.google.com

macOS :

- Ako otvoriť CLI?
  - Otvoriť aplikáciu “Terminal”
- Ako skontrolovať status interface-u & zároveň nastavenie interface-u ?
  - ifconfig
- Ako skontrolovať routing (smerovanie) ?
  - netstat -rn
- Ako skontrolovať otvorené porty ?
  - netstat –an
  - netstat –an | grep *
- Ako vykonať základné sieťové kontroly ?
  - ping www.google.com
  - traceroute www.google.com

Ukážky výstupov z OS Windows

```
C:\Users\ahyben>netsh int show int

Admin State    State          Type             Interface Name
-------------------------------------------------------------------------
Enabled        Connected      Dedicated        Ethernet


C:\Users\ahyben>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : localdomain
   IPv6 Address. . . . . . . . . . . : fdb2:2c26:f4e4:0:dce4:3b7a:da4c:ccb5
   Temporary IPv6 Address. . . . . . : fdb2:2c26:f4e4:0:299d:dfbe:2ab:84a0
   Link-local IPv6 Address . . . . . : fe80::dce4:3b7a:da4c:ccb5%8
   IPv4 Address. . . . . . . . . . . : 10.211.55.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::21c:42ff:fe00:18%8
                                       10.211.55.1
```

```
C:\Users\ahyben>netstat -rn
===========================================================================
Interface List
  8...00 1c 42 ef 4e ae ......Intel(R) 82574L Gigabit Network Connection
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      10.211.55.1      10.211.55.3     25
      10.211.55.0    255.255.255.0         On-link       10.211.55.3    281
      10.211.55.3  255.255.255.255         On-link       10.211.55.3    281
    10.211.55.255  255.255.255.255         On-link       10.211.55.3    281
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link       10.211.55.3    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link       10.211.55.3    281
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  8    281 ::/0                     fe80::21c:42ff:fe00:18
  1    331 ::1/128                  On-link
  8    281 fdb2:2c26:f4e4::/64      On-link
  8    281 fdb2:2c26:f4e4:0:299d:dfbe:2ab:84a0/128
                                    On-link
  8    281 fdb2:2c26:f4e4:0:dce4:3b7a:da4c:ccb5/128
                                    On-link
  8    281 fe80::/64                On-link
  8    281 fe80::dce4:3b7a:da4c:ccb5/128
                                    On-link
  1    331 ff00::/8                 On-link
  8    281 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

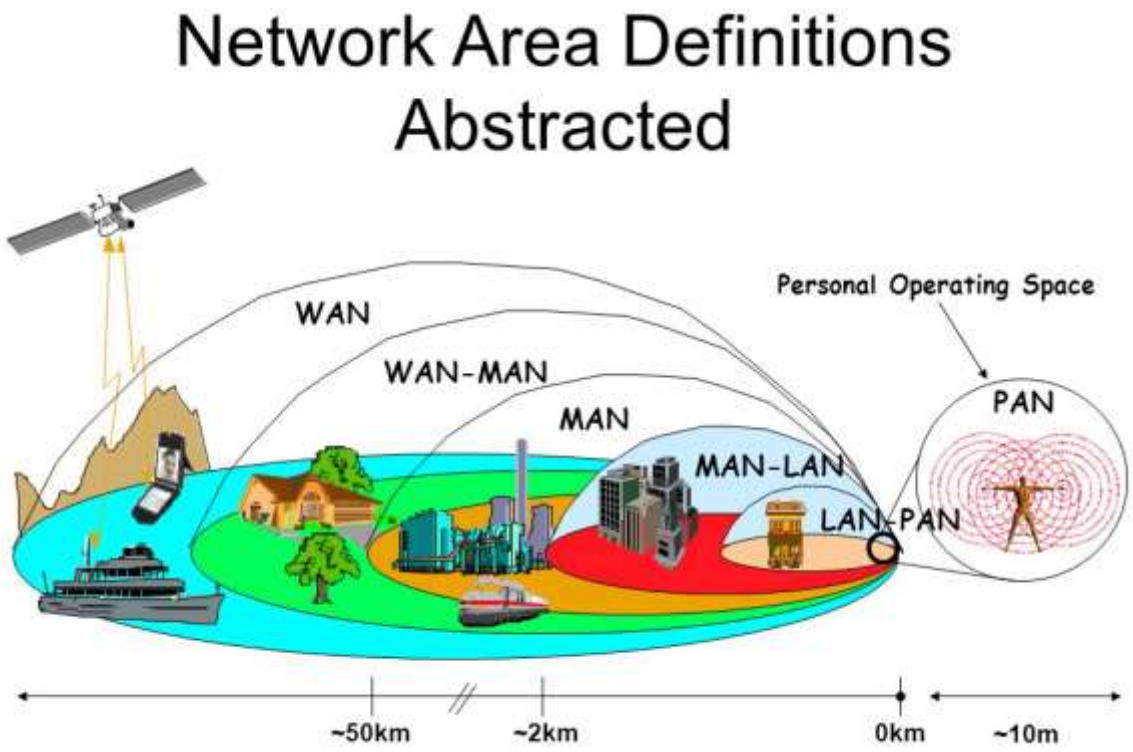
Prestávka

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Data-Linková vrstva

PAN / LAN / MAN / WAN

- **PAN** : Personal Area Network – niečo veľmi blízke ku mne, napr. bluetooth
- **LAN** : Local Area Network - napr. všetko v našej domácnosti pripojené v jednej wifi sieti.
- **MAN** : Metropolitan Area Network – Budovy v jednom meste prepojené do jednej siete (napr. Antik Košice)
- **WAN** : Wide Area Network – Siete, ktoré sú od seba geograficky vzdialene, ale sú navzájom prepojené
  - Internet ako ho poznáme je tiež WAN



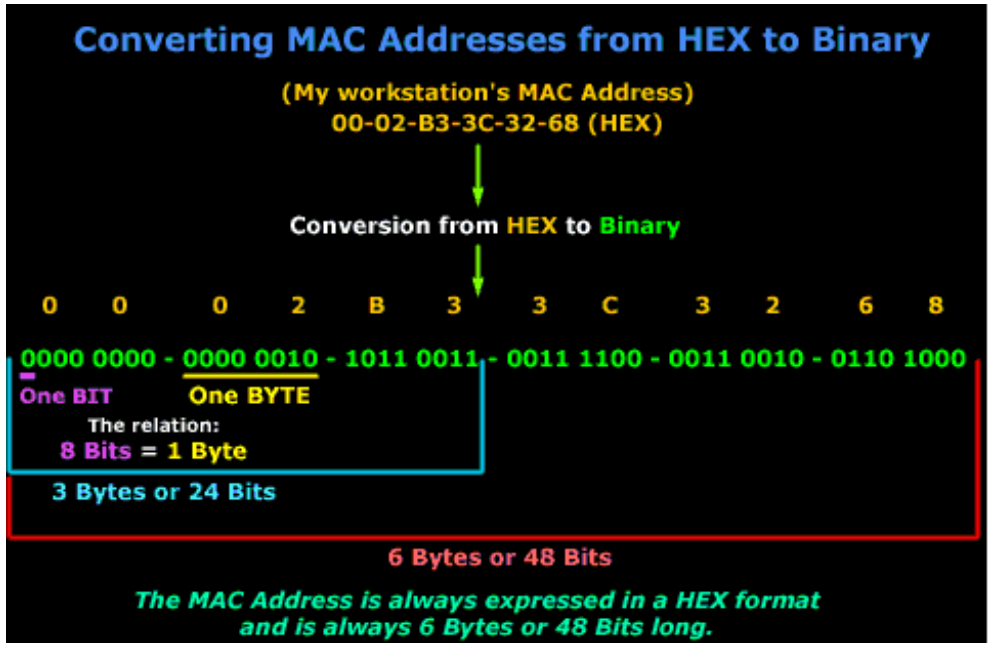
Data-Linková vrstva

- Je zodpovedná za prenos dát v rámci jednej siete (**LAN**)
- Zabaľuje packety z tretej vrstvy do **frames**, aby mohli byť na fyzickej vrstve rozbite na jednotky na nuly. Ako sme si už spomínali, tento proces sa nazýva **enkapsulácia**.
- Typ **enkapsulácie** závisí od technológie použitej na fyzickej vrstve. Medzi najčastejšie používané patrí :
  - **Ethernet**
  - **802.11 Wireless**
  - **802.15.1 Bluetooth**

- Data-linkový **frame** obsahuje zdrojovú a cieľovú HW (alebo fyzickú) adresu. Tá jednoznačne a unikátne identifikuje host v sieti, pretože je často vpísaná do sieťovej karty pri výrobe. Táto vrstva ale neobsahuje mechanizmus, ktorý by zabezpečil komunikáciu mimo siete.
  - Najčastejšie sa používa Ethernet **MAC adresa**.

MAC Adresa

- Media control address (MAC adresa) je unikátny identifikátor pridelený sieťovej karte (NIC), ktorá sa používa na komunikáciu v jednej sieti. Toto je bežne využívané v IEEE 802 sieťových štandardoch, ktoré zahŕňajú Ethernet, Wi-Fi a Bluetooth.
- Je to 48 bitov / 6 bajtov dlhý identifikátor, ktorý je obvykle označovaný ako 12 hexa-decimálnych znakov, ktoré sú zvyčajne delené po dvoch buď pomlčkou alebo iným znakom.
- Možných je 2^{48} (over 281 trillion) kombinácií
- Možnosti zápisu tej istej MAC adresy:
  - f0:18:98:64:6d:75
  - F018.9864.6d75
  - F0-18-98-64-6d-75
  - f01898646d75

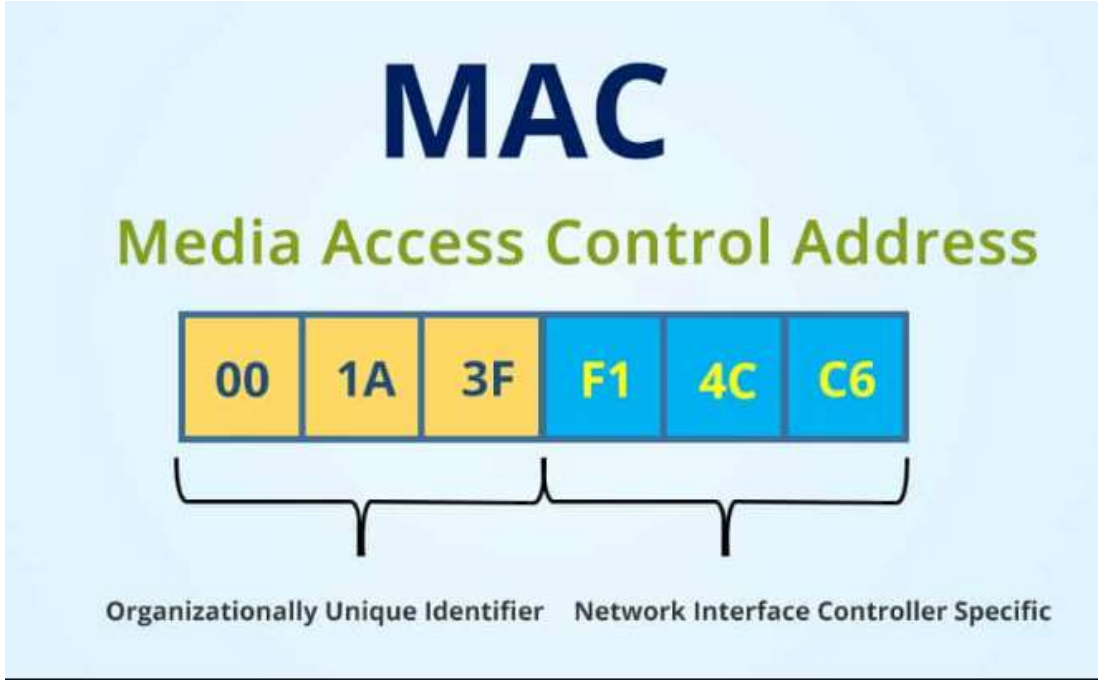


MAC Adresa

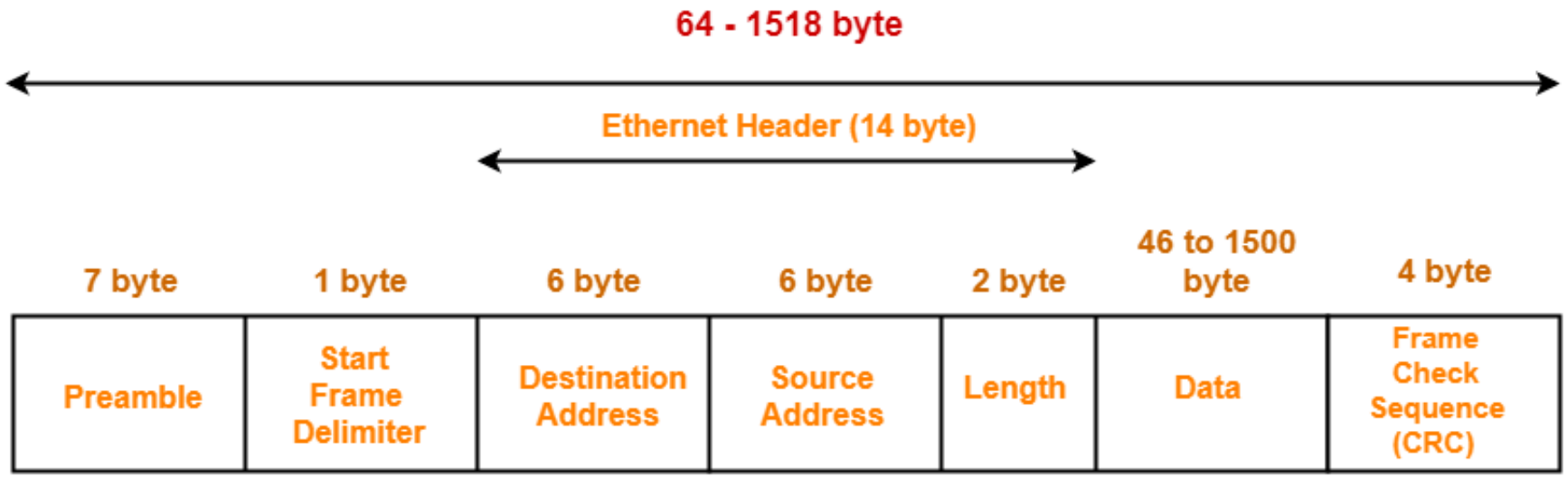
- MAC adresa pozostáva z:
  - OUI – prvých 24bits / 3 bytes
    - Tie reprezentujú výrobcu sieťovej karty (napr. Apple, Asus, atď.)
  - NIC špecifická – druhých 24 bits / 3 bytes
    - Čo je unikátny identifikátor tejto NIC

- Ako si vyhľadať výrobcu NIC?
  - Zadajte “OUI lookup” do google
  - Najčastejší & najdôveryhodnejší link:

https://ouilookup.com/



Frame



IEEE 802.3 Ethernet Frame Format

- **Preamble and SFD** : Synchronizuje a oznamuje, že prichádza nový frame
- **Destination MAC & Source MAC & Length** : Hlavička frame-u, ktorá hovorí presne v poradí : kam má ísť, kto to poslal a aká je správa dlhá
- **Data** : V tomto prípade sú dáta packet (niekedy to tiež voláme payload)
- **CRC** : Check sequence – kontrolná sekvencia, podľa ktorej vieme povedať, či frame dorazil v poriadku.

Switch

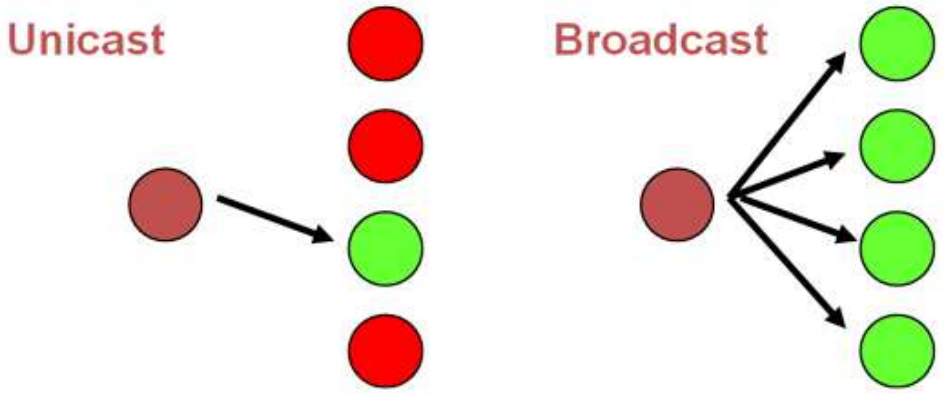
- Je zariadenie operujúce výlučne na Data-linkovej vrstve podľa zdrojovej a cieľovej MAC adresy z hlavičky frame-u.
- Ako to funguje ?
  - Switch má CAM (Content-addressable memory), kde ukladá informácie o tom, ktorá MAC adresa je dostupná cez ktorý port.
  - Keď príde frame na switch, ten si uloží zdrojovú MAC a port z ktorého to prišlo. Väčšinou si túto informáciu uchováva na 5min. Časomiera sa s každým prichádzajúcim frame-om môže resetovať. Tiež sa resetuje ak ide interface dole a späť hore.
  - Ak cieľová MAC nie je v tabuľke, switch pošle frame na všetky porty okrem toho odkiaľ to prišlo.
  - Keď príde odpoveď, tak sa switch naučí odkiaľ a uloží si to do CAM tabuľky
  - Následná komunikácia je potom už preposielaná len medzi zdrojom a cieľom.

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

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000a.000b.2222    DYNAMIC     Fa0/2
   1    000a.abcd.3333    DYNAMIC     Fa0/3
   1    940a.ca0b.1111    DYNAMIC     Fa0/1
```

Broadcast vs Unicast

Broadcast

- Keď koncové zariadenie (napr. počítač, laptop, mobil) pošle dáta na MAC adresu ff:ff:ff:ff:ff:ff (kde všetkých 48 bitov sú “1”), vtedy switch pošle tento frame na všetky porty.
  - Tento typ komunikácie sa volá „broadcast“ a je to veľmi používaná feature.
  - Každé zariadenie, ktoré takýto frame dostane, ho musí dekapsulovať a zhodnotiť na tretej vrstve, či mu náhodou nepatrí. Presne pre toto je dobre, keď nie je všetko v jednej sieti – aby tento „ruch“ nepohltil väčšinu liniek.
  - Tiež je to dôvod, prečo sa LAN tiež volá “broadcast domain”.

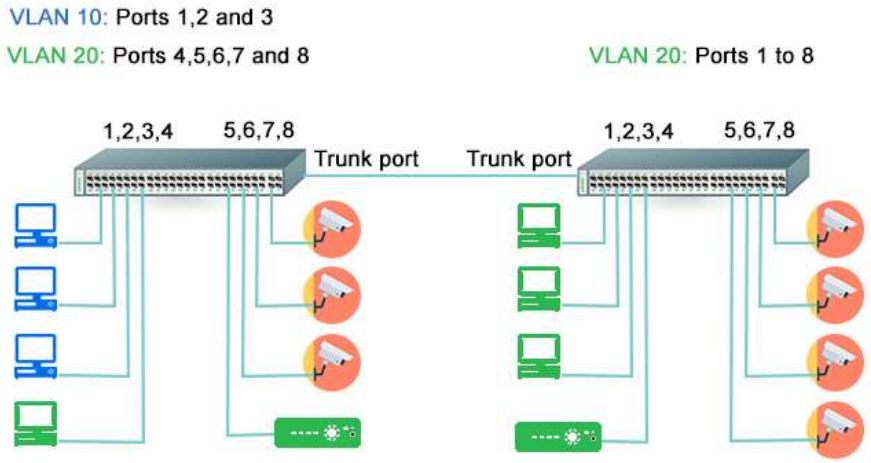


Unicast

- Je komunikácia, v ktorej je presne špecifikovaná cieľová MAC adresa, ktorá patrí konkrétnemu komponentu.

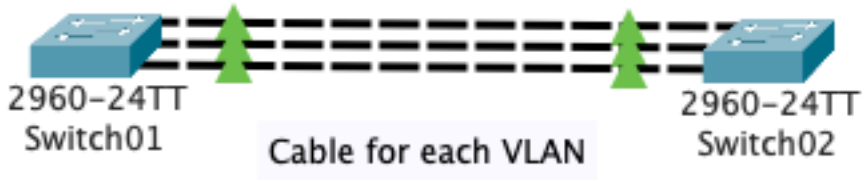
VLAN-ky

- VLAN-ky (Virtual LAN) sú logické rozdelenia zariadení pripojených do toho istého switch-a. Ten sa nakonfiguruje tak, aby bol logicky rozdelený na viacero virtuálnych switchov, kde každý má unikátne číselné označenie.
- Na jednom switch-i môžeme mať VLAN-ky od 1-4096
- Takže teoreticky vieme vytvoriť 4096 virtuálnych switch-ov na jednom switch-i a každý z nich bude mať :
  - ID : číslo medzi 1 – 4096
  - Meno (nepovinný údaj) : môže byť akékoľvek slovo (napr. “Students”)

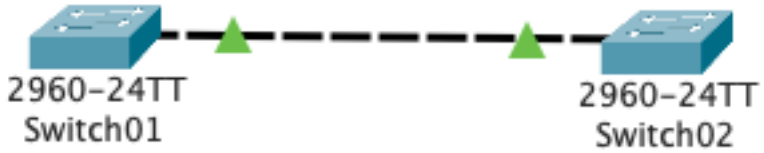


Trunk

- Z predchádzajúceho slide vieme, že jeden switchport vie byť priradený práve jednej VLAN-ke
  - V takýchto prípadoch hovoríme o „access“ portoch
  - Najčastejšie sa to používa na porty smerujúce ku koncovým zariadeniam (počítače, laptopy)



- Nie je veľmi praktické mať medzi dvomi switch-ami dedikovaný kábel pre každú VLAN
- Preto inžinieri vymysleli možnosť zdieľania jedného fyzického portu viacerými VLAN-kami, ktoré nazvali „Trunk“ port.
- Ako to funguje ?
  - Na oboch switchoch musí byť prepájajúci port nastavený v „trunk“ móde
  - Na oboch switch-och musíme nastaviť na trunk porte rovnaké povolené VLAN-ky
  - Na oboch switchoch musia byť tieto VLAN-ky vytvorené.

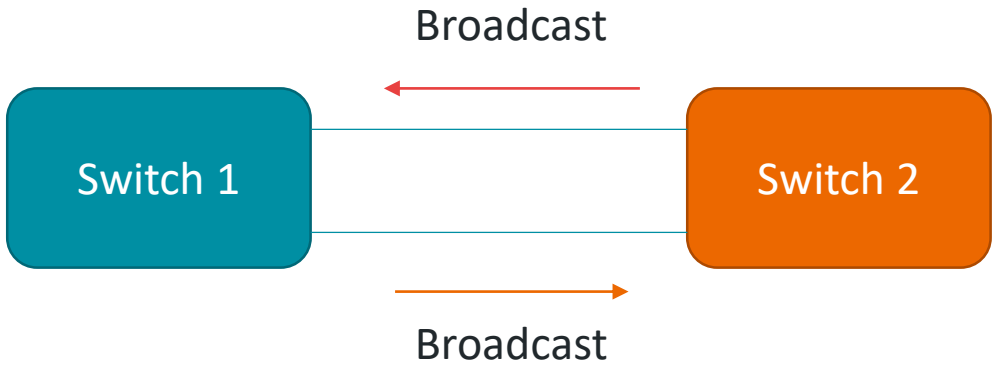


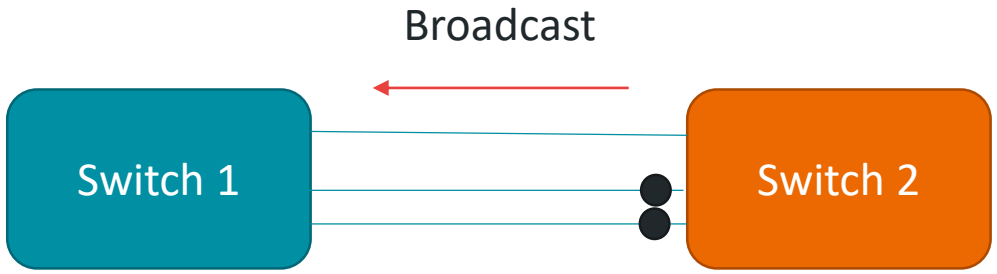

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1,10,20

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20

Switch#
```

Spanning Tree Protokol / STP

- Ako jeden z mála protokolov, bol tento protokol vymyslený ženou. Legenda hovorí, že hneď potom ako bol protokol schválený, požiadala komisiu IEEE o zmenu znenia. (Keď si pozriete históriu zmien štandardu – sedí to)

- O čo teda ide ?
  - Keď switch posiela broadcast na všetky porty, okrem toho na ktorý mu informácia prišla – tak ak má na nejaký port pripojený ďalší switch
  - Ak by bolo takýchto portov medzi dvoma switch-ami viac, tak môže nastať „**broadcast storm**“, čo je v podstate pád siete kvôli preťaženiu.
  - Riešením je matematický výpočet, ktorý jeden z tých portov vyradí z prevádzky. Tento výpočet zabezpečuje **STP** protokol.
  - V aktualizáciách protokolu hovoríme aj o :
    - RSTP (Rapid STP)
    - PVSTP (Per-VLAN STP)



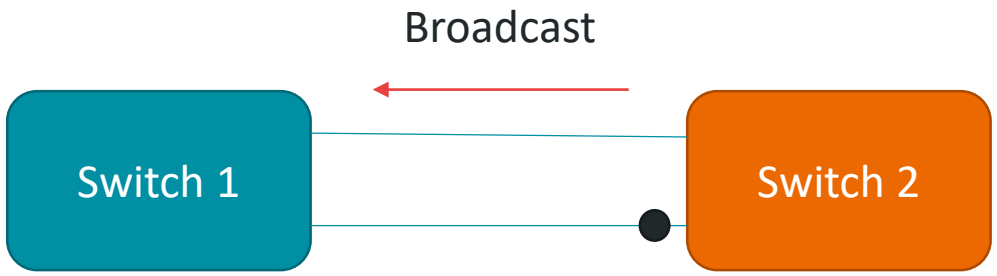


Cesta je zablokovaná
Ak je takýchto pripojení medzi switchami viac, počet vypnutých je (n-1)

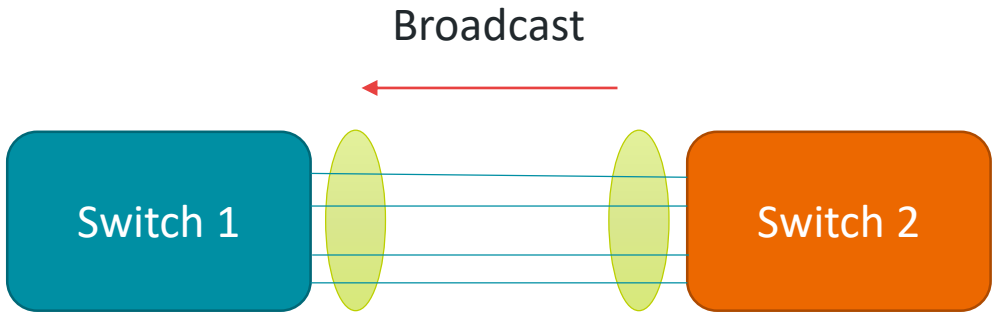
Port-Channel / LACP

- Keďže z predchádzajúceho slide-u vieme, že STP nám zablokuje akúkoľvek snahu o zvýšenie priepustnosti pridaním viacerých pripojení medzi switch-ami.

- Presne kvôli potrebe mať vyššiu priepustnosť medzi switch-ami, vznikol protokol LACP.
  - Link Aggregation Control Protocol
  - Umožňuje kombinovať viacero (podľa typu a výrobcu 2-8) portov do jedného logického portu, ktorý má výslednú priepustnosť rovnú (takmer) súčtu ich priepustnosti.
  - Podmienky sú :
    - Na oboch switchoch musia byť nastavené rovnaké porty
    - Musí byť použité rovnaké nastavenie protokolu (check timers, atď.)
- Výsledkom je port-channel, čiže virtuálny port, ktorý sa dá nastaviť napr. ako trunk.



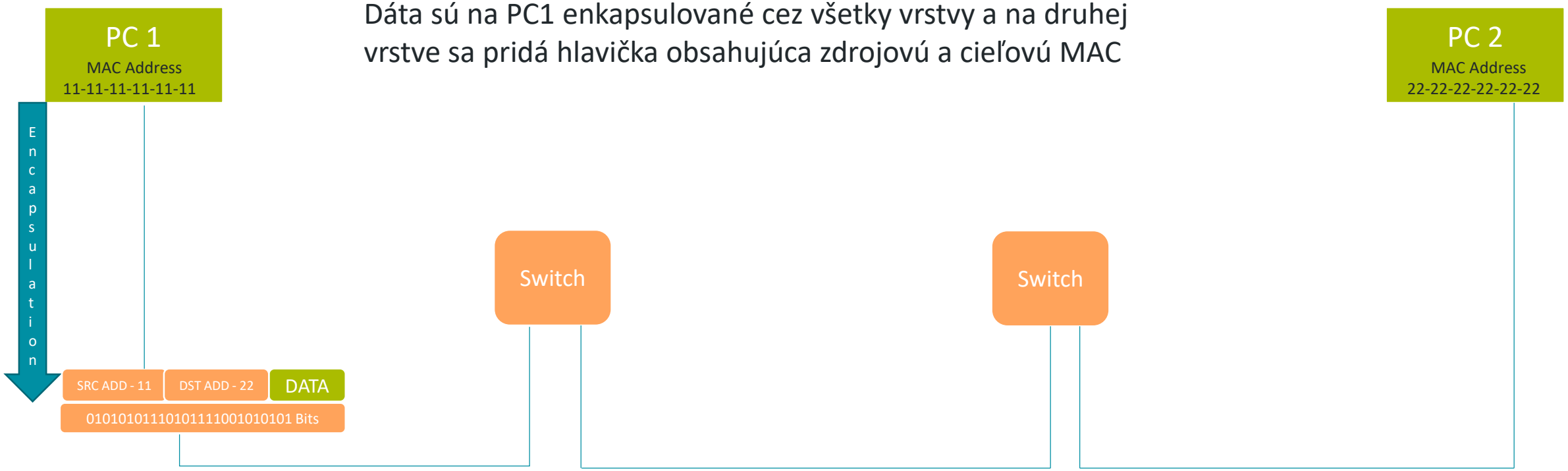
Cesta je zablokovaná
Aj keď by bolo 10 * 1Gbps prepojení
Stále by sa používala len 1



Viaceré porty sa správajú ako jeden
V nastaveniach nájdeme port s názvom po1
Výsledná priepustnosť je (takmer) súčet
Priepustností portov v jednom port-channeli.

Komunikácia na druhej vrstve #1

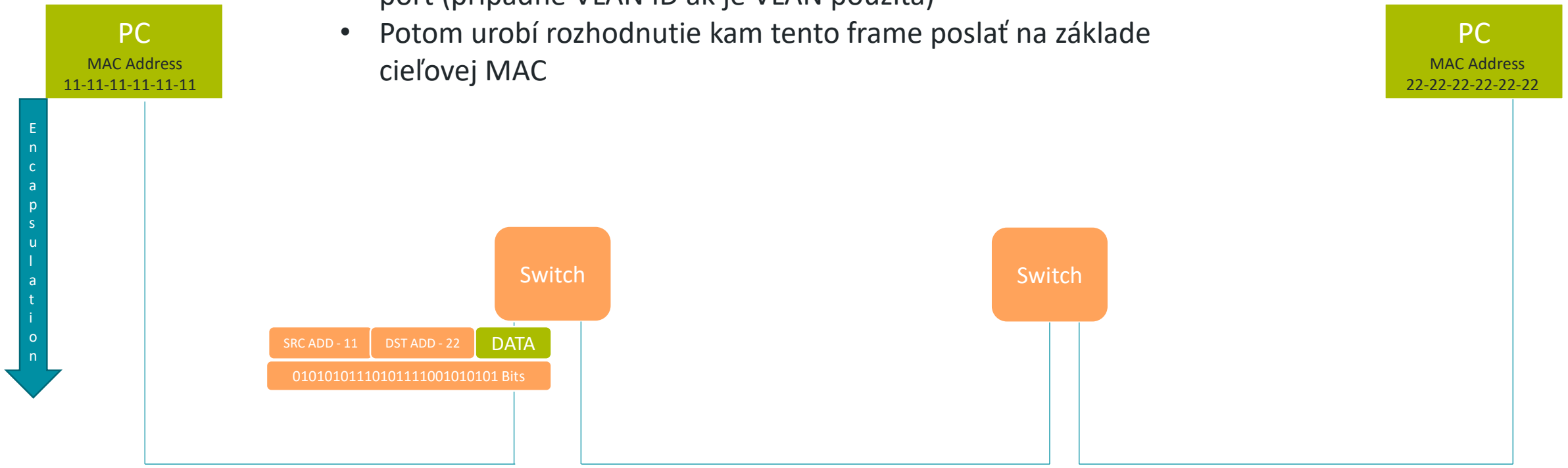
PC 1 – posiela dáta smerom na PC 2, ktorý je v tej istej LAN
Dáta sú na PC1 enkapsulované cez všetky vrstvy a na druhej vrstve sa pridá hlavička obsahujúca zdrojovú a cieľovú MAC



Komunikácia na druhej vrstve #2

Ako sa bude chovať switch:

- Skontroluje hlavičku frame-u, kontrolný súčet no hlavne zdrojovú a cieľovú MAC
- Do CAM tabuľky si poznačí zdrojovú MAC a prichádzajúci port (prípadne VLAN ID ak je VLAN použitá)
- Potom urobí rozhodnutie kam tento frame poslať na základe cieľovej MAC

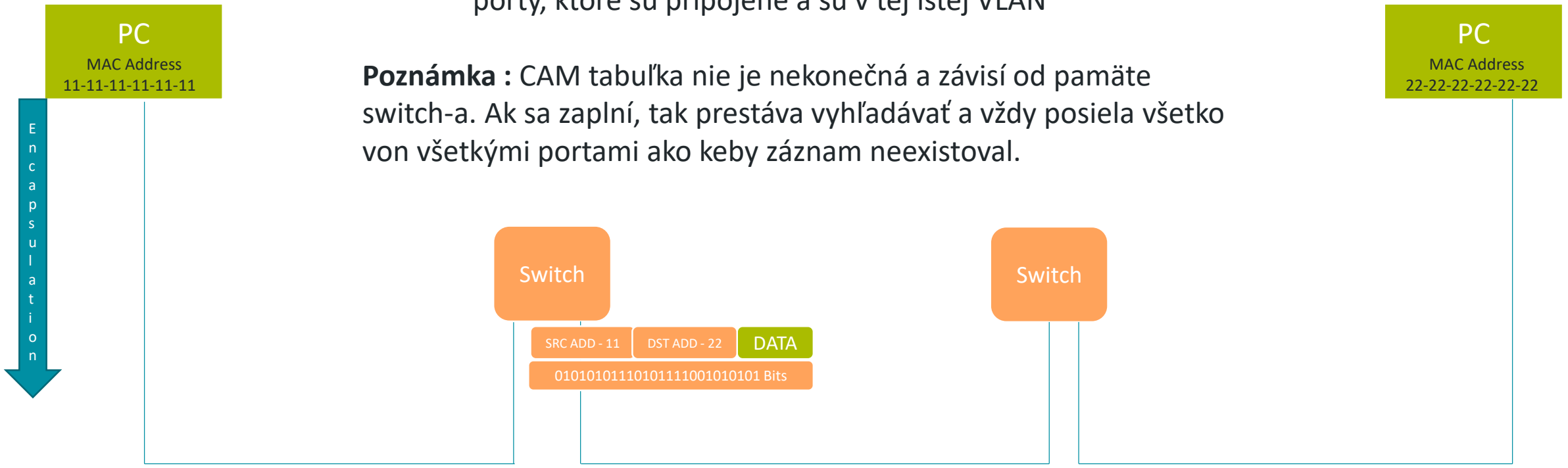


Komunikácia na druhej vrstve #3

Rozhodovanie switch-a kam poslať frame:

1. Prehľadá CAM tabuľku, či tam nenájde cieľovú MAC
    1. Ak tam je (a je v tej istej VLAN-ke) tak odošle frame na odchádzajúci port podľa tejto tabuľky
    2. Ak záznam neexistuje, switch pošle tento frame cez všetky porty, ktoré sú pripojené a sú v tej istej VLAN

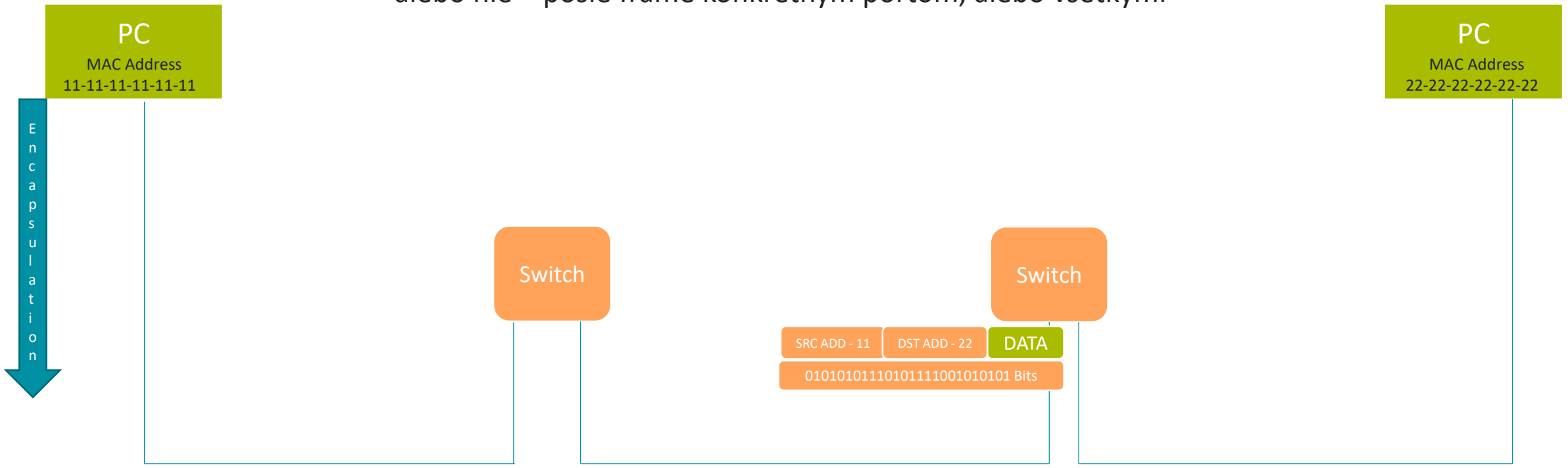
Poznámka : CAM tabuľka nie je nekonečná a závisí od pamäte switch-a. Ak sa zaplní, tak prestáva vyhľadávať a vždy posiela všetko von všetkými portami ako keby záznam neexistoval.



Komunikácia na druhej vrstve #4

Tento proces sa zopakuje aj na ďalšom switch-i

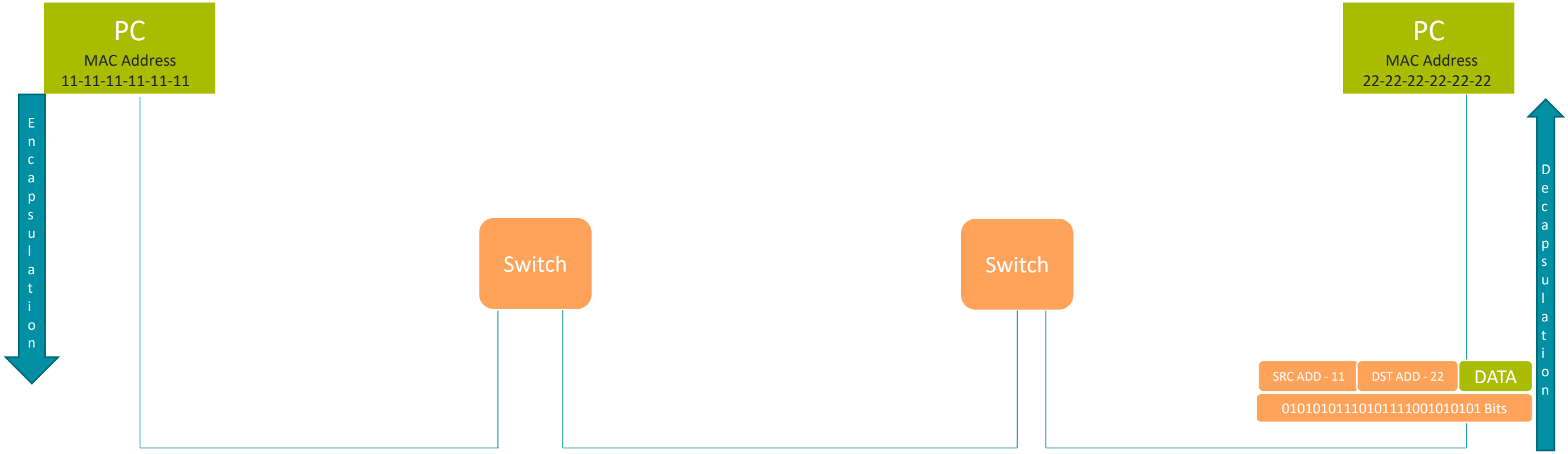
- Kontrola hlavičky frame-u
- Uloženie zdrojovej MAC to CAM tabuľky
- Vyhľadanie cieľovej MAC v CAM a podľa toho či tam záznam je, alebo nie – pošle frame konkrétnym portom, alebo všetkými



Komunikácia na druhej vrstve #5

PC 2 konečne prijíma dáta z PC 1, pripojeného v tej istej LAN

- aj na cieľovom PC 2 sa znova skontroluje kontrolný súčet CRC
- PC 2 skontroluje, či cieľová MAC patrí jemu
- Ak áno – dekapsujuje frame ďalej cez všetky vrstvy



Quick quiz

- Ktorá v poradí je Data-linková vrstva v ISO/OSI modeli ?
  - Druhá vrstva
- Ako sa volá adresa, ktorá sa používa v Data-Linková vrstva ?
  - MAC address
- Ako sa volá PDU(Protocol Datagram Unit) na Data-Linkovej vrstve ?
  - Frame
- Ako sa volá zariadenie, ktoré funguje na Data-Linkovej vrstve ?
  - Switch

Prestávka

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Sieťová vrstva

Sieťová vrstva / 3. vrstva

- PDU (Protocol Data Unit) – Packet
- Zariadenie pracujúce na tretej vrstve – router
  - Protokoly:
    - IPv4 (Internet Protocol version 4)
    - IPv6 (Internet Protocol version 6)
    - ARP (Address Resolution Protocol) – používa sa na mapovanie MAC adries ku IP adresám
    - ICMP (Internet Control Message Protocol) – ping, ktorý možno poznáte
- Čo robí router ?
  - Routuje (smeruje) trafiku na základe cieľovej IPv4 alebo IPv6 adresy v hlavičke packetu.
  - Prepája 2 a viac sietí medzi sebou a to tak, že slúžia ako default gateway pre všetky koncové zariadenia v sieti a zároveň sú pripojené do inej siete, kde sú aj ďalšie routre

Čo je IP adresa ?

IPv4 adresa :

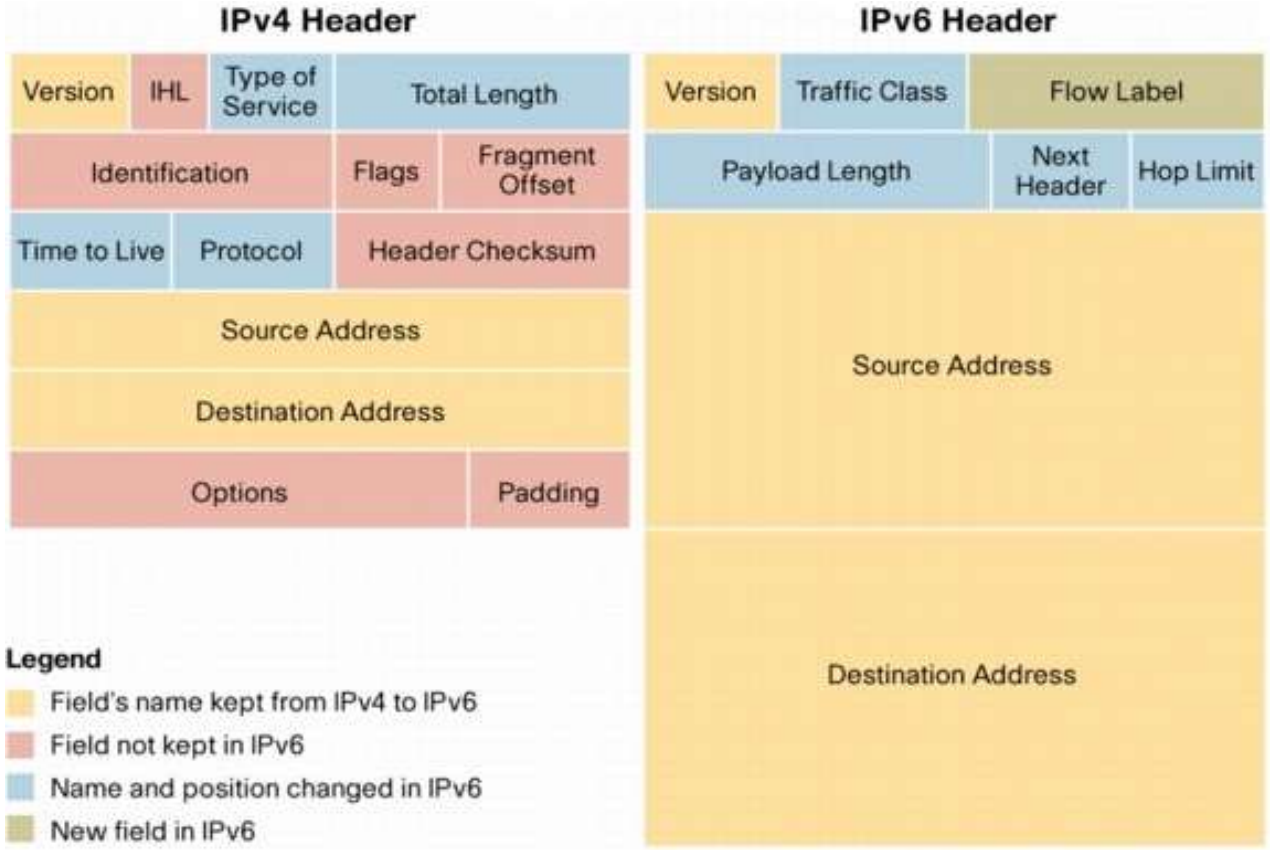
- Je 32 bitová logická adresa sieťovej karty zariadenia, ktorá nie je pridaná z výroby ale nastavená manuálne, či automaticky podľa siete v ktorej sa nachádza.
  - 4x8 bitové polia oddelené bodkou
- To znamená že dostupných je 2^{32} IPv4 adries
  - 2^32 = 2x2x2x2x2x2….x2= 4,294,967,296
  - 4.3 miliardy adries
  - Možno ste sa dočítali, že verejné IPv4 adresy už došli
  - Len ukážka IPv4 = 192.168.0.5

IPv6 adresa :

- Je 128 bitová logická adresa sieťovej karty zariadenia, ktorá nie je pridaná z výroby ale nastavená manuálne, či automaticky podľa siete v ktorej sa nachádza.
- To znamená, že máme dostupných 2^{128} IPv6 adries
- 2^128 = 2x2x2x2x2x2….x2…x2x2x2x2 = $3.4x10^{38}$
- huge vychádza to približne na 1*IPv6 na cm2 pre celú planétu
- Aj keď bola vytvorená v 90 rokoch, stále ju nepoužívajú všetci
- Ukážka : 2a0b:2900:115e:ba3::f:1

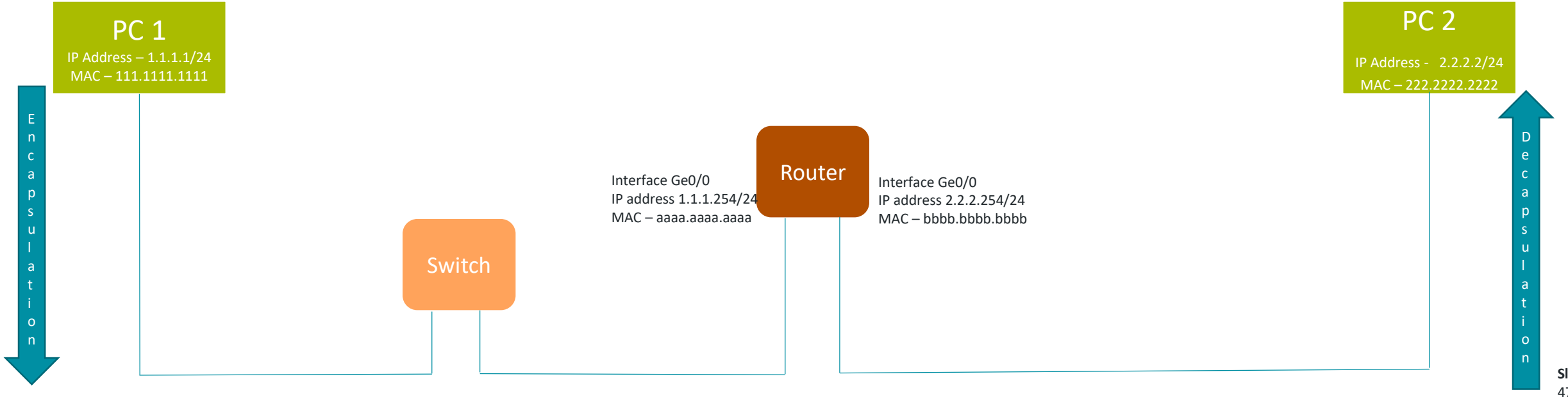
IP konfigurácia :

- statická – manuálna konfigurácia
- dynamická – DHCP protokol (Dynamic Host Configuration Protocol)



Komunikácia na tretej vrstve #1

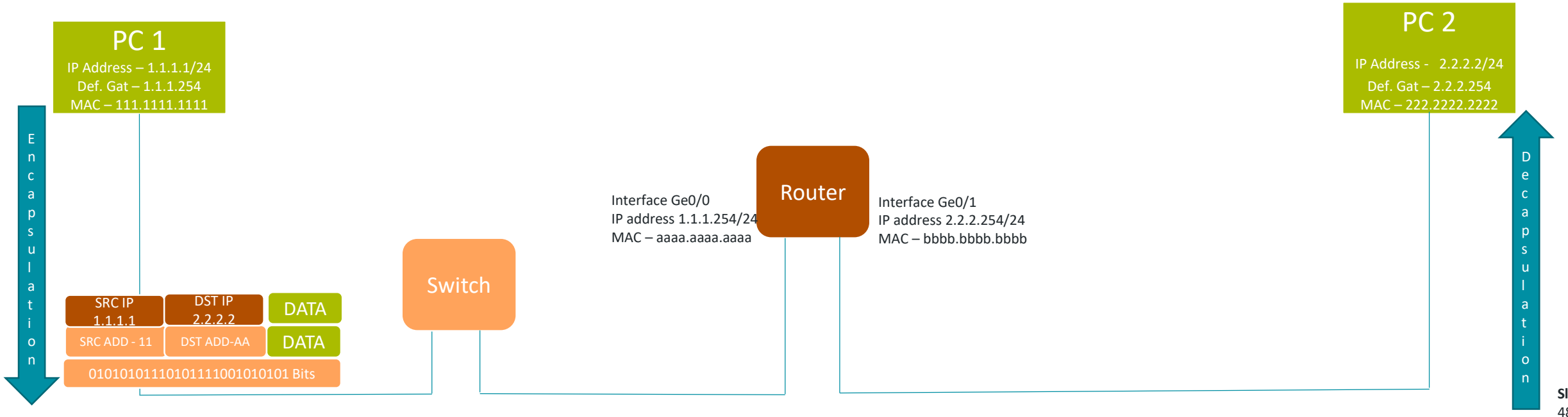
- Pri odosielaní dát a enkapsulácií tretia vrstva pridá hlavičku, ktorá obsahuje zdrojovú a cieľovú IP adresu ku dátam, ktoré prišli z transportnej vrstvy. Takto sa vytvorí packet, ktorý je ďalej spracovávaný na data-linkovej vrstve.
- Keď dáta prichádzajú na túto vrstvu, kontroluje sa (rovnako ako pri druhej vrstve), či cieľová IP adresa patrí prijímateľovi. Jedine vtedy je packet ďalej dekapsulovaný.



Komunikácia na tretej vrstve #2

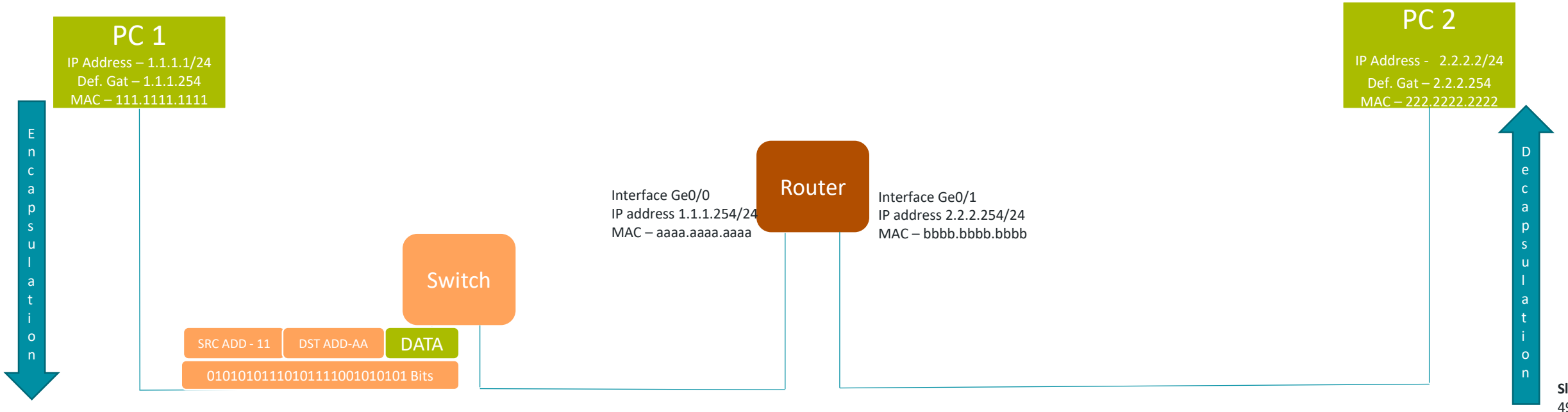
PC 1 posiela dáta na PC 2, ktorý je pripojený v inej sieti. Medzi nimi je router, ktorý siete prepája.

- PC 1 najprv interným prepočtom svojej IP a masky zistí, že cieľová adresa je v inej sieti
- Enkapsuluje dáta cez všetky vrstvy až po sieťovú vrstvu, kde do hlavičky pridá zdrojovú a cieľovú IP adresu
  - Cieľová IP adresa je v tomto prípade PC 2
- Packet sa ďalej enkapsujuje na data-linkovú vrstvu, kde sa pridá zdrojová a cieľová MAC adresa – no pozor !
  - Zdrojová MAC bude PC 1
  - **Cieľová MAC adresa nebude PC 2**, ale MAC adresa interface-u routra pripojeného do siete, kde je PC 1



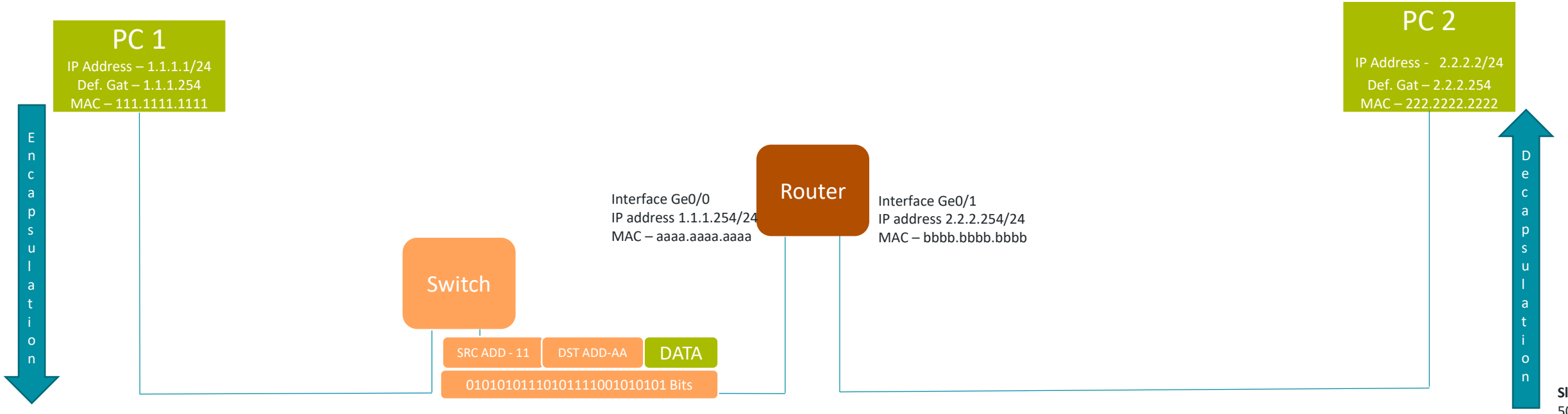
Komunikácia na tretej vrstve #3

Switch funguje presne ako sme si vysvetlili, čiže skontroluje prichádzajúci frame a z hlavičky si uloží zdrojovú MAC a port z ktorého frame prišiel (ak je tam VLAN, tak aj tú).



Komunikácia na tretej vrstve #4

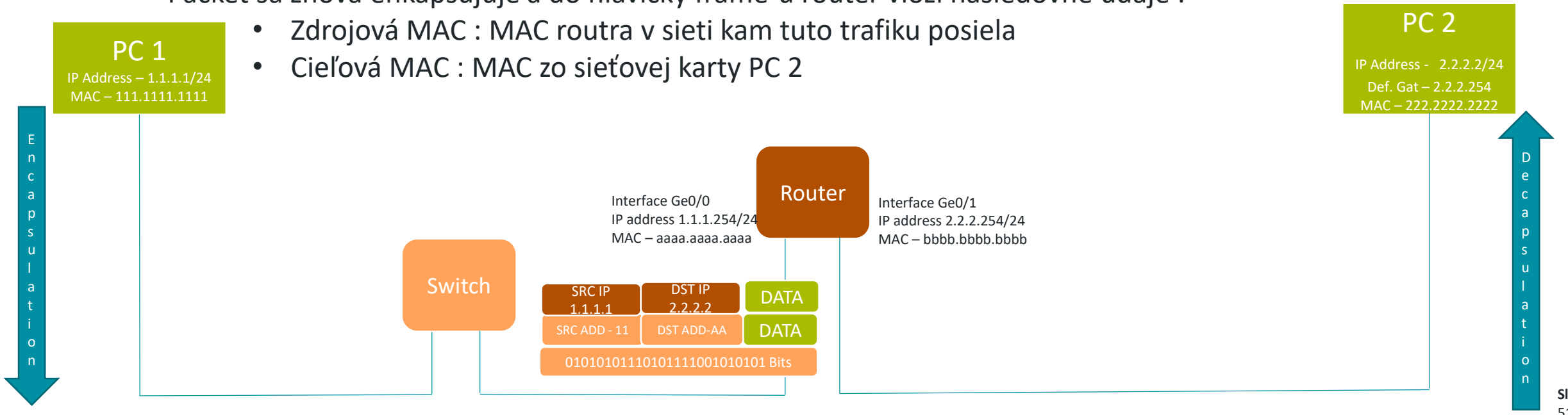
Cieľová MAC je buď už známa v CAM tabuľke, alebo frame pošle cez všetky zapojené interface.
Switch každopádne pošle frame smerom na router, ktorého MAC adresa je v hlavičke frame-u.



Komunikácia na tretej vrstve #5

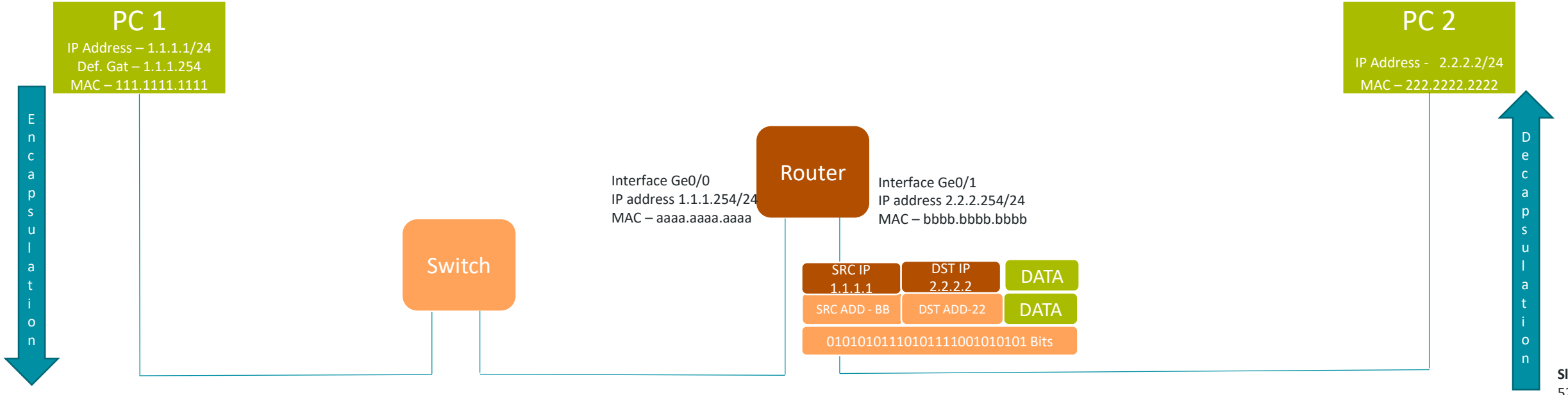
Čo urobí router potom ako príde frame ?

- Prvá je klasická kontrola integrity, potom kontroluje či je cieľová MAC jeho a má sa s ním ďalej zaoberať.
- Ak je cieľová MAC jeho, tak dekapsujuje frame a pozerá sa na hlavičku packetu
- Skontroluje 2 hlavné údaje v hlavičke
  - TTL (Time to Live) – ak je toto číslo rovné 1, zahadzuje trafiku a zdrojovej IP pošle správu o nedoručení
  - Cieľová IP adresa – skontroluje svoju routovaciu tabuľku, podľa ktorej vie kde sa ktorá sieť nachádza
- Ak packet posiela ďalej :
  - V hlavičke packetu zníži TTL o 1
  - Packet sa znova enkapsujuje a do hlavičky frame-u router vloží nasledovné údaje :
    - Zdrojová MAC : MAC routra v sieti kam tuto trafiku posiela
    - Cieľová MAC : MAC zo sieťovej karty PC 2



Komunikácia na tretej vrstve #6

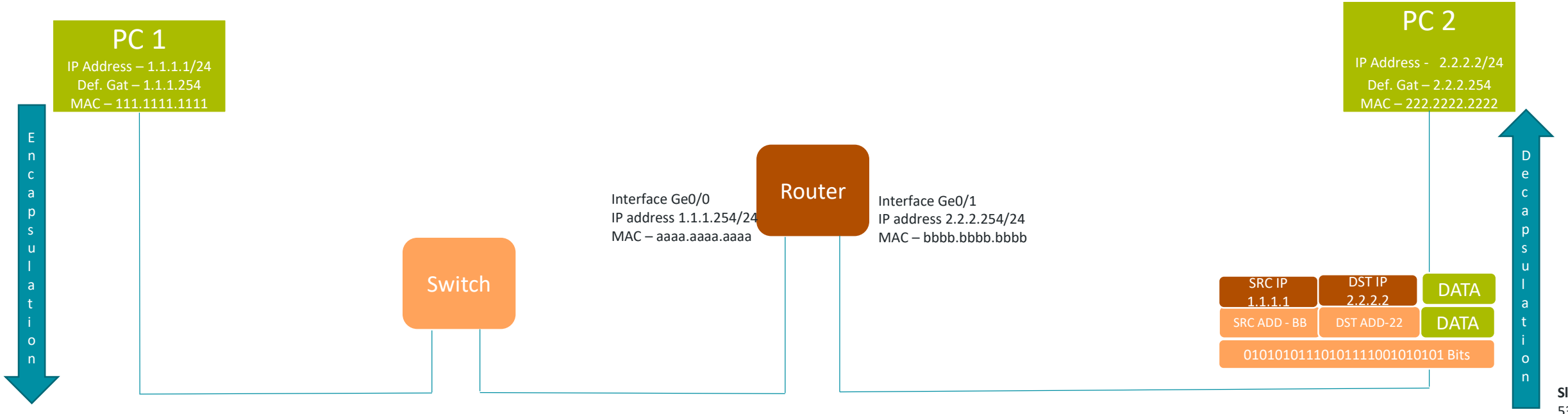
```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/0
L        1.1.1.254/32 is directly connected, GigabitEthernet0/0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/1
L        2.2.2.254/32 is directly connected, GigabitEthernet0/1
```



Komunikácia na tretej vrstve #7

PC 2 príjme dáta od PC 1, ktorý je pripojený v inej sieti

- Znova skontroluje hlavičku frame-u
- Enkapsujuje z frame-u packet a skontroluje jeho hlavičky
- Ak MAC aj IP patria jemu, tak ďalej enkapsujuje cez všetky vrstvy až ku aplikácií.



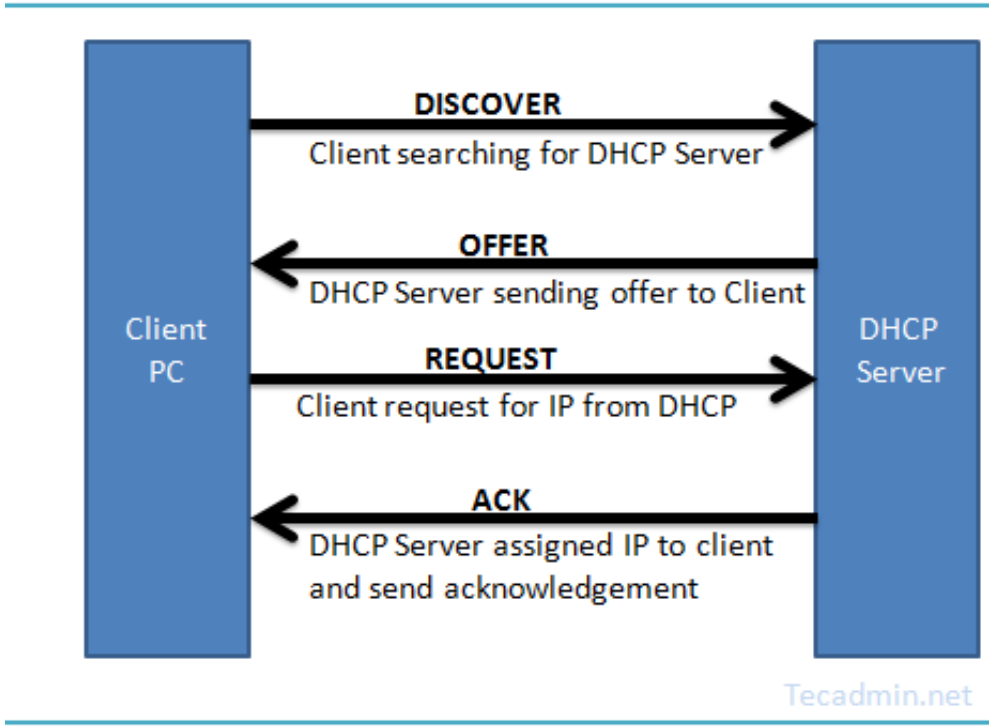
Prestávka

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Dynamic Host Configuration Protocol (DHCP)

- IP adresa môže byť nastavená staticky alebo dynamicky
  - DHCP sa používa na dynamickú konfiguráciu IP adries
- Je to protokol, ktorý funguje na aplikačnej úrovni a vie poskytnúť :
  - IP adresu (Príklad 1 – napr. 192.168.1.100)
  - Masku podsiete (Príklad 2 – napr. 255.255.255.0)
  - Default Gateway (Príklad 3 – napr. 192.168.1.1)
  - DNS Adresy (Príklad 4 – napr. 8.8.8.8, 1.1.1.1)
  - ... Ale aj mnoho iného, príklady sú najčastejšie používané, no dá sa poskytnúť aj proxy IP, atď. ...
- DHCP je postavený na klient – server komunikácií, pomocou 4 typov hlášok : DORA
- DHCP používa protokol UDP (povieme si viac zajtra) a na komunikáciu so serverom port 67 a klient ma zdrojový port 68(tiež si povieme viac pri transportnej vrstve).

Dynamic Host Configuration Protocol (DHCP)



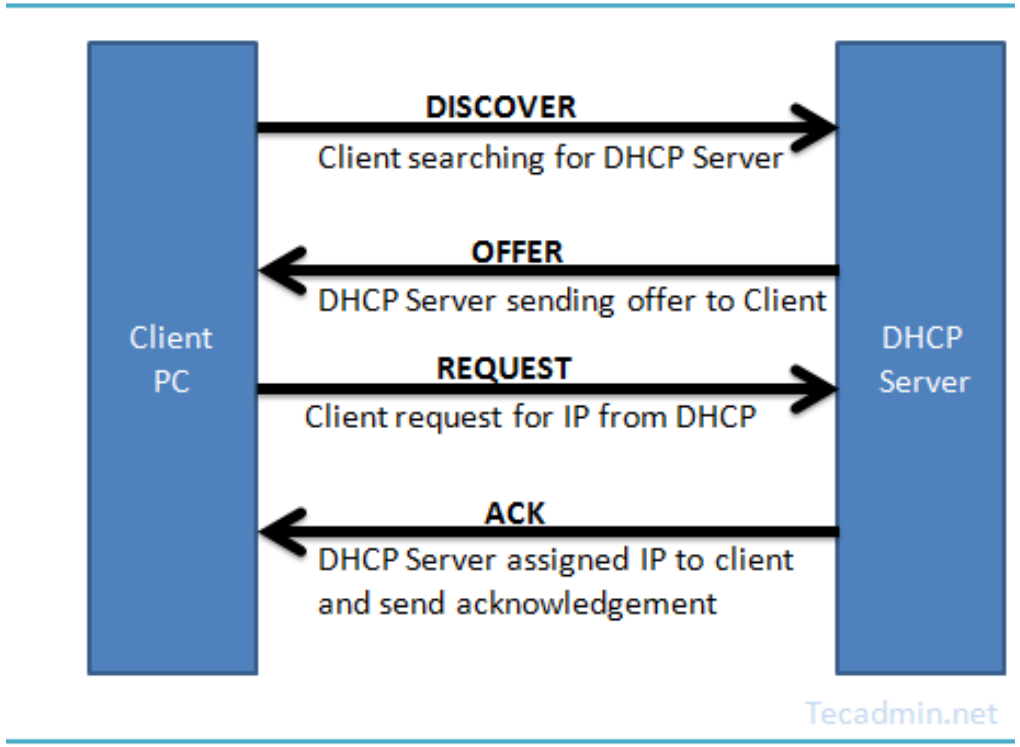
DORA proces a DHCP správy:

- **Discover** – keďže nemáme IP, posielame broadcast do našej siete s našou MAC a cieľovou broadcast IP aj MAC adresou (ľudovo – kričíme o pomoc)
- **Offer** – DHCP server zachytí volanie a použije cieľovú broadcast IP no pravú MAC adresu žiadateľa. V dátach mu navrhne jednu z voľných IP.

Dynamic Host Configuration Protocol (DHCP)

DORA proces a DHCP správy:

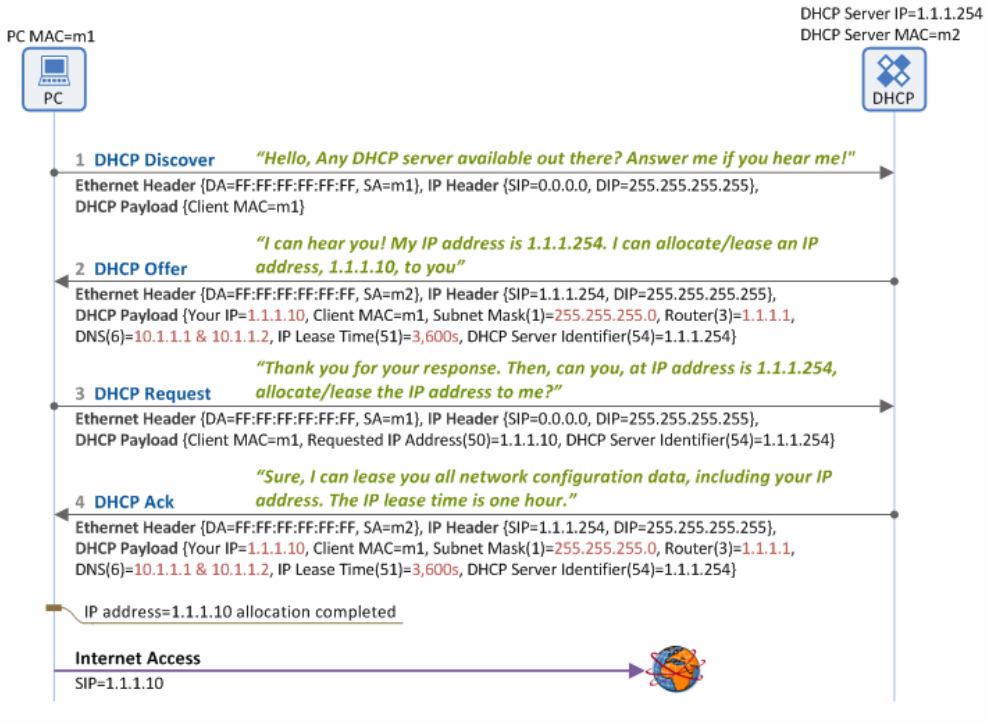
- **Request** – klient súhlasí s návrhom IP a žiada server o registráciu na najbližších xx hodín.
- **ACK** – DHCP server dostane žiadosť, zaregistruje si IP ku MAC adrese do svojej DHCP lease tabuľky a potvrdí klientovi, že ju môže používať.

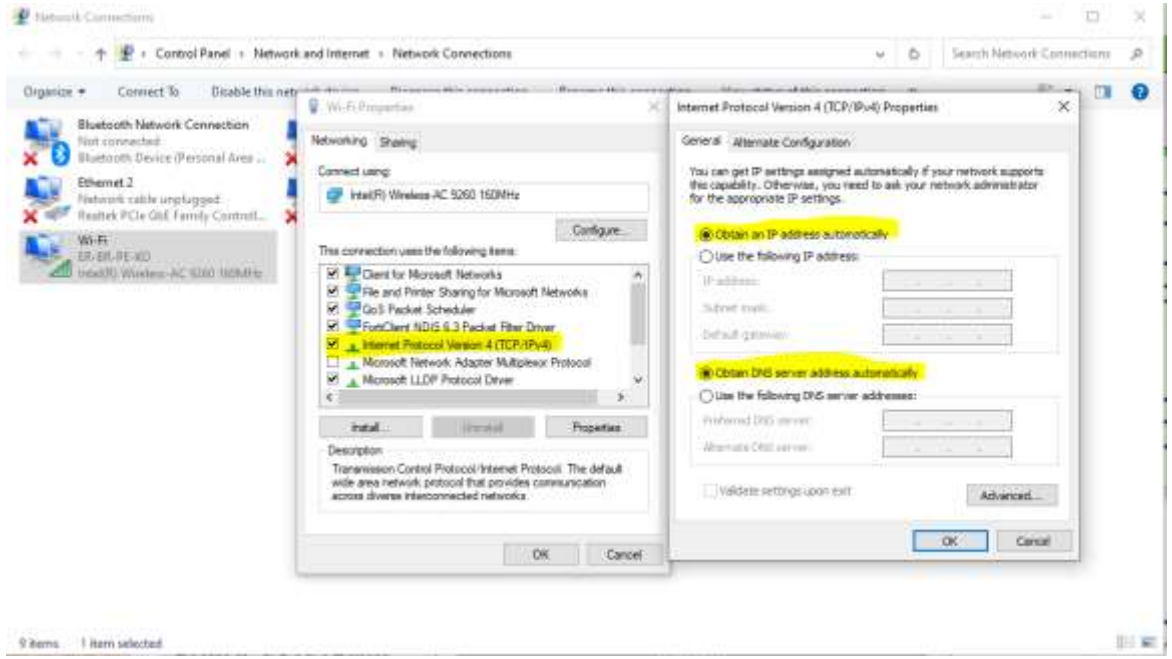


Dynamic Host Configuration Protocol (DHCP)

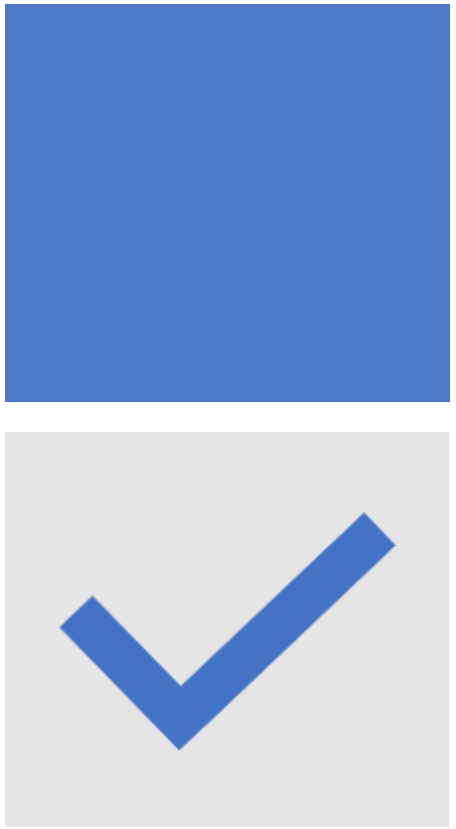
Príklad : Ako na Windows PC nastavíme statickú alebo dynamickú IP adresu.

- Všetky vaše laptopy to majú nastavené takto aby ste vedeli pracovať z domu aj z práce.





Address Resolution Protocol (ARP)



Mapovanie IP adresy & MAC adresy

Address Resolution Protocol (ARP)

- Zariadenia používajú Address Resolution Protocol (ARP) na objavovanie zariadení v ich sieti a to tak, že mapujú hardvérovú (MAC) adresu ku IP adrese zariadenia, ktoré chce kontaktovať.
- Inými slovami, ARP pomáha zistiť cieľovú MAC adresu zariadenia predtým ako ju použije v hlavičke frame-u. **Na komunikáciu** totiž používame **IP** adresy (napr. facebook.com je DNS záznam s cieľovou IP, nie MAC).
- Predtým ako pošle zariadenie packet, skontroluje svoju ARP tabuľku, v ktorej si ukladá všetky doposiaľ namapované IP a MAC adresy. Pravdaže každý záznam má „idle timeout“, čiže ak sa znova neoverí jeho pravosť, tak po čase vyprší. Ten je väčšinou okolo 5 minút.
- ARP je jednoduchý **request-response** protokol, ktorého správy sú enkapsulované až na druhú vrstvu. Komunikuje len v rámci jednej siete – router nikdy ARP request-y nepreposiela !

- **Poznámka:** Pri **IPv6** sieťach, funkciu ARP preberá **NDP** (Neighbor Discovery Protocol)

Address Resolution Protocol (ARP) Messages

2 typy správ

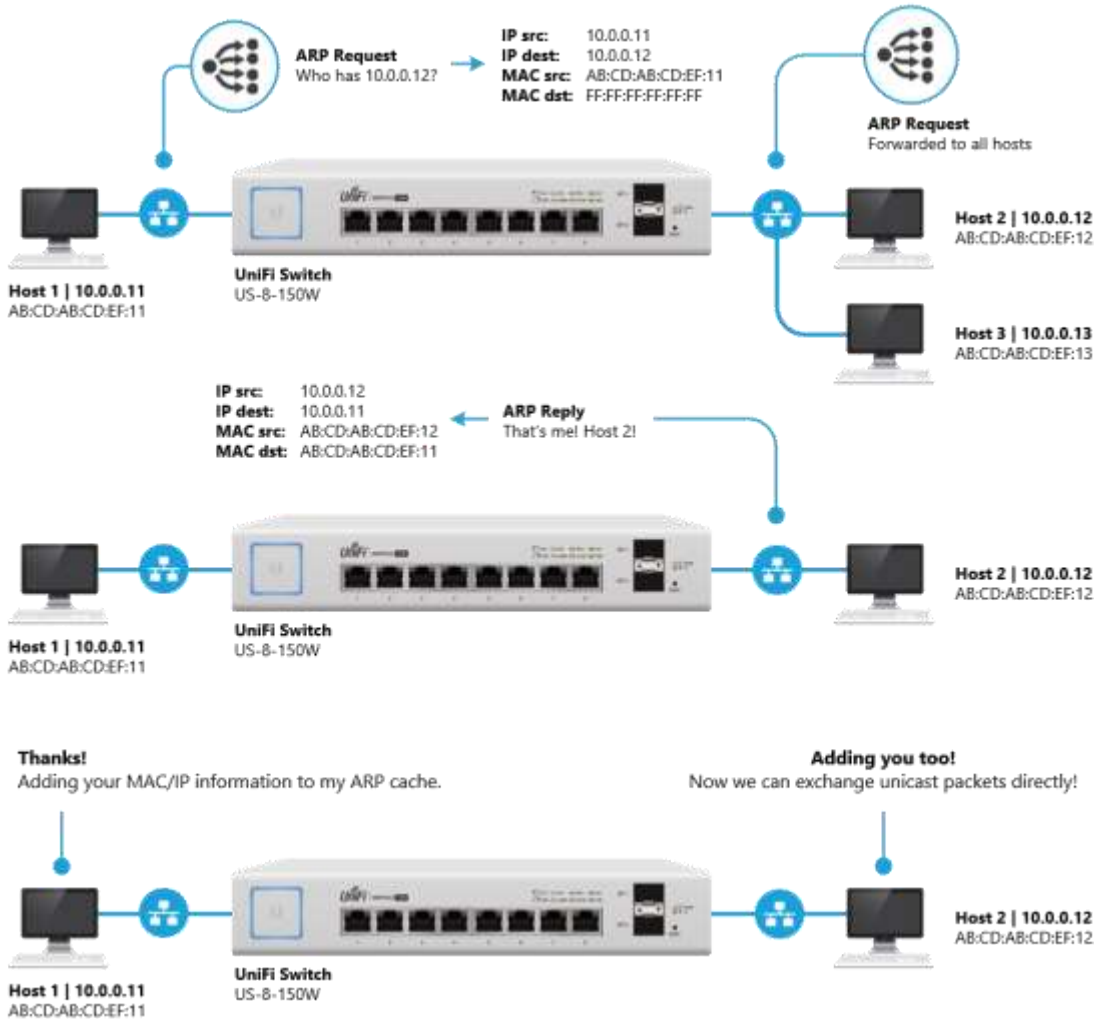
ARP Request

ARP Response

Address Resolution Protocol (ARP)

ARP v rámci jednej LAN :

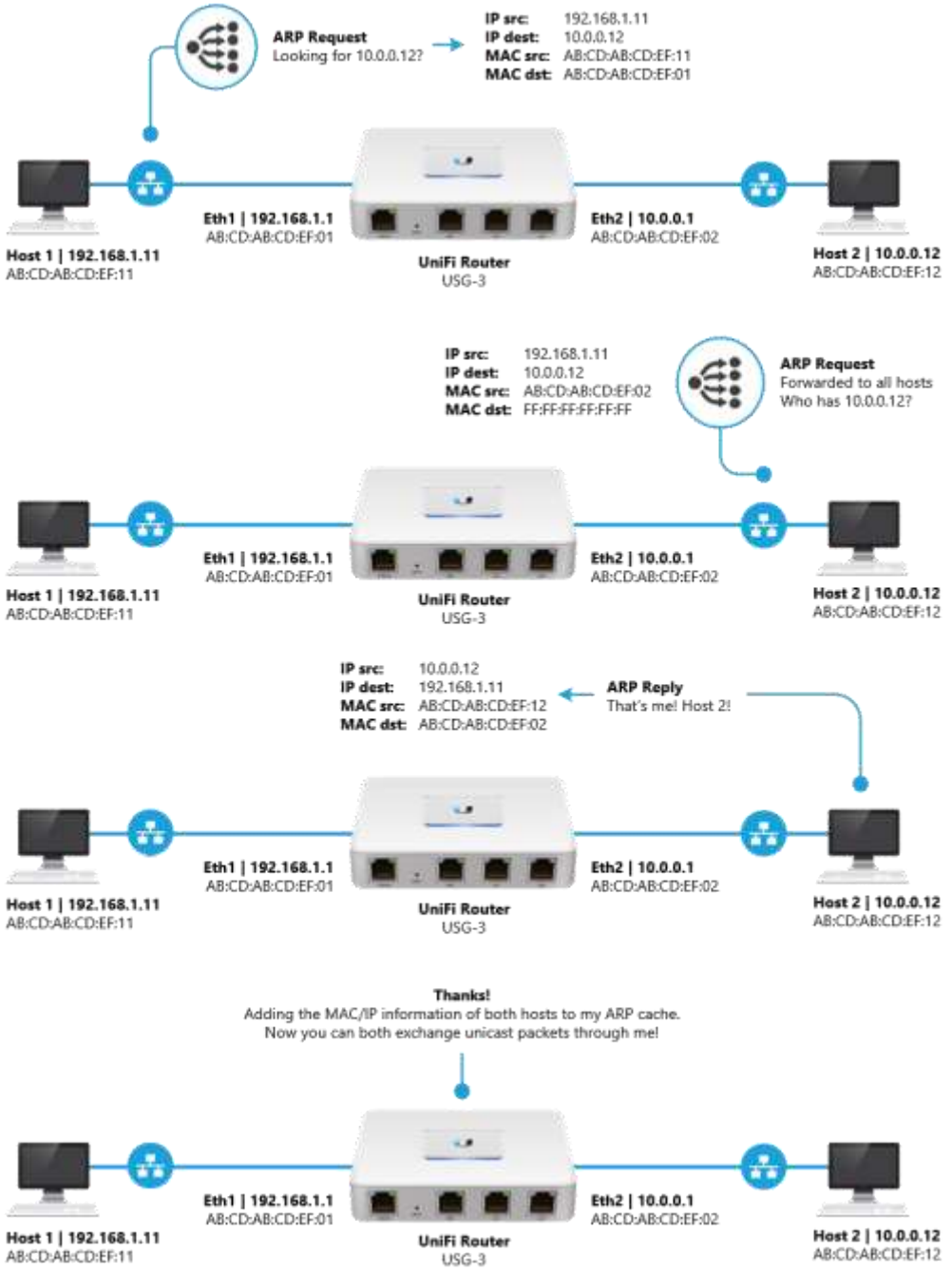
- Ak cieľová IP adresa patrí zariadeniu v tej istej LAN kde sa nachádza zdrojová IP, potom zdroj posiela ARP request na broadcast MAC (FF:FF:FF:FF:FF:FF)
- Na príklade vidíte ako switch posiela ARP request cez všetky porty na switch-i.
- Host 2 a Host 3 dostanú ARP request. IP adresa v hlavičke requestu patrí Hostu 2, preto odpovie iba on a Host 3 tento request zahodí.
- Host 2 už ale odpovedá ARP reply na presný zdroj – teda použije unicast.
- V hlavičkách ARP reply už sú jednoznačne uvedené :
  - Zdrojová a cieľová MAC
  - Zdrojová a cieľová IP



Address Resolution Protocol (ARP)

ARP medzi LAN sieťami

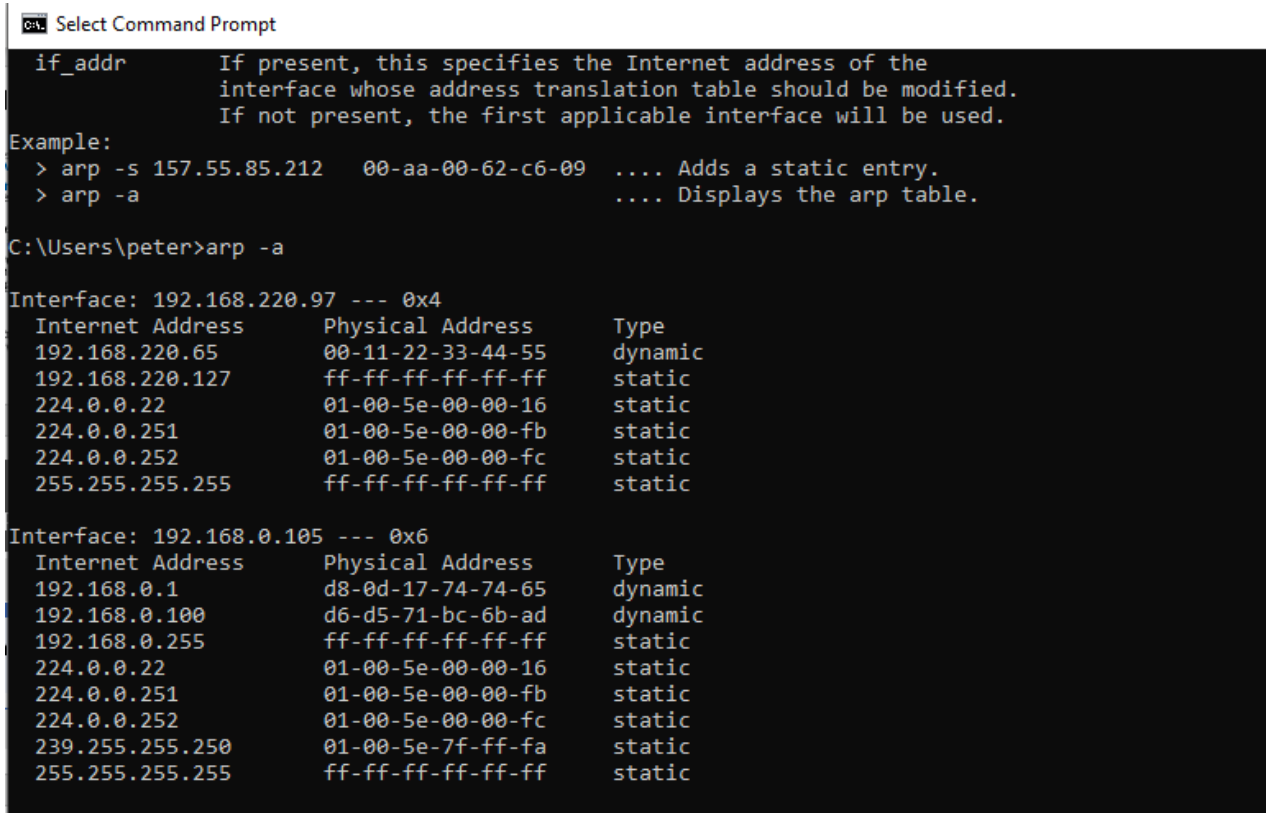
- Ak je cieľová IP adresa v inej sieti ako zdrojová, tak sú packety posielané najprv na gateway v sieti, kde sa nachádza zdroj.
- Ak Host 1 nemá ARP záznam z ARP cache pre Gateway IP, tak najprv urobí ARP request aby zistil jeho MAC adresu
- Gateway odpovie Host 1 ARP reply a potom už Host 1 bude poznať MAC a zaznamená si to v ARP cache aby tam vedel posielať frame.
- Gateway znova skontroluje, či má ARP záznam pre Host 2, ak nemá – urobí ARP request a počká na odpoveď z Hostu 2. Odpoveď si poznačí v ARP cache a potom bude vedieť posielať frames.
- Výsledkom je, že Host 1 vie cez Gateway komunikovať s Hostom 2, pretože všetky potreby na túto komunikáciu boli naplnené.



ARP Cache / Tabuľka

Windows – otvorte príkazový riadok a zadajte :

`arp –a`



```
Select Command Prompt
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.

C:\Users\peter>arp -a

Interface: 192.168.220.97 --- 0x4
  Internet Address      Physical Address      Type
  192.168.220.65        00-11-22-33-44-55     dynamic
  192.168.220.127       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.0.105 --- 0x6
  Internet Address      Physical Address      Type
  192.168.0.1           d8-0d-17-74-74-65     dynamic
  192.168.0.100         d6-d5-71-bc-6b-ad     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Cisco Router – príkaz

`show ip arp`

```
FRA-A-ROOB001#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  89.202.101.249         0   cce1.7fc1.adc1  ARPA   Gig8
Internet  89.202.101.250         -   2c33.1126.05c8  ARPA   Gig8
Internet  192.168.212.66         -   2c33.1126.05b6  ARPA   Vlan13
Internet  192.168.212.69       164   286f.7f01.455e  ARPA   Vlan13
Internet  192.168.212.70        19   00f6.63c5.d27e  ARPA   Vlan13
Internet  192.168.214.1          0   286f.7f55.4fec  ARPA   Vlan11
Internet  192.168.214.2          0   286f.7f55.2378  ARPA   Vlan11
Internet  192.168.214.3          0   843d.c66f.8d1e  ARPA   Vlan11
Internet  192.168.214.4          0   286f.7ff0.0b3e  ARPA   Vlan11
Internet  192.168.214.8          0   843d.c6ec.609c  ARPA   Vlan11
Internet  192.168.214.9          0   843d.c6ec.4cfe  ARPA   Vlan11
Internet  192.168.214.10       252   843d.c6ec.42cc  ARPA   Vlan11
```

Prestávka

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Čo je IP adresa ?

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e421:3b02:b3c8:c4e6%5
   IPv4 Address. . . . . . . . . . . : 192.168.0.107
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

Existujú 2 verzie protokolu:

- **IPv4** a IPv6 (nebude súčasťou školenia)
- IPv4 adresa, je adresa, ktorá sa používa na jednoznačne identifikovanie zariadenia **v IP sieti**.
- Pozostáva z **32-och bitov**, ktoré sa delia na sieťovú a hosťovu časť.
- To, koľko bitov je v sieťovej a koľko v hosťovej časti, nám určuje **maska podsiete**.
- Ak chce zariadenie komunikovať so zariadením mimo jeho siete, pošle komunikáciu na jeho default gateway. To je zariadenie zodpovedné za routing trafiky mimo lokálnej siete (napr. u Vás doma Váš domáci router).
- Z toho vyplýva, že default gateway sa vždy musí nachádzať v rovnakej sieti ako zariadenia, ktoré sa na neho odkazujú.

Prečo treba vedieť IP kalkulácie

- Architekti sú zodpovední za definovanie drobných sieti, preto musia vedieť ako sa to počíta a zároveň musia poznať ak všeobecne používané pravidlá.
- Čo teda nevyhnutne musíme vedieť po tejto kapitole ?
  - subnetting – rozdeľovanie sietí na menšie tak, aby bol efektívne využití priestor
  - sumarizácia – spájanie menších sietí do väčších za účelom zjednodušeného routingu

Existujú 2 typy IPv4 adries :

1. **Verejné IP adresy** – sú byť routované v internete
2. **Privátne IP adresy** – nie je routované v internete
   - Ak packet, ktorý príde na internetový router má privátnu zdrojovú IP adresu, internetový router ju zahodí. Na komunikáciu v internete sú potrebné výlučne verejné IP adresy.
   - Privátne sa používajú v uzatvorených systémoch (domácnosť, kancelária, cloud, atď.), a ak majú komunikovať s niečím v internete, musí sa použiť NAT (Network Address Translation – viac sa dozvieme zajtra).

Privátne a Verejné IP adresy

Privátne IP rozsahy sú definované v RFC 1918 vyhláške takto :

- 10.0.0.0/8 – 10.0.0.0 – 10.255.255.255
- 172.16.0.0/12 – 172.16.0.0 – 172.31.255.255
- 192.168.0.0/16 – 192.168.0.0 – 192.168.255.255

Iné privátne rozsahy, ktoré nie sú definované v tomto RFC, ale v internete nemôžu byť routované :

- 100.64.0.0/10 – 100.64.0.0 – 100.127.255.255
- 224.0.0.0/4 – 224.0.0.0 - 224.239.255.255

Verejné IP adresy sú všetky ostatné, ktoré neboli definované v tomto texte.

Príklady Verejných IP adries

- Verejné IPv4 rozsahy sú už všetky vypredané
- V dnešnej dobe je veľmi ťažké dostať verejnú IPv4 adresu
- Jediná možnosť ako ju dostať, je zakúpiť si ju od RIR (Regional Internet Registries) alebo od nejakého operátora, čo sa zásoboval dopredu.
- Kým cena za jednu IP bolo 13 rokov dozadu približne 8 Eur – dnes sa to pohybuje na úrovni 40-50 Eur.
  - Chceš investovať ? Toto tak skoro dole nepôjde ☺

```
C:\Users\peter>nslookup google.sk
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    google.sk
Addresses:  2a00:1450:4014:801::2003  -> IPv6 address
          216.58.201.67 -> IPv4 address

C:\Users\peter>nslookup facebook.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    facebook.com
Addresses:  2a03:2880:f107:83:face:b00c:0:25de -> IPv6 address
          31.13.84.36 -> IPv4 address

C:\Users\peter>nslookup sgcr.sk
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    sgcr.sk
Address:  92.240.253.3 -> IPv4 address
```

IPv4 adresa – ako sa vypočíta ?

Je 32-bitová sieťová adresa nastavená na sieťovej karte zariadenia (nie natvrdo ako MAC adresa)

- 4x8 bitových dielov oddelených bodkou, ako napríklad:

- **Decimálna reprezentácia:**
  192.168.0.15

- **Binárna reprezentácia:**
  11000000. 10101000.00000000.00001111

Nebojte sa – na počítanie nebude treba vedieť dvojkovú (binárnu) sústavu, toto je len ukážka aby ste rozumeli ako to vypočítali prvý krát a ako to odvodili.

	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal Value	128	64	32	16	8	4	2	1
192. [192=128+64]	1	1	0	0	0	0	0	0
168. [168=128+32+8]	1	0	1	0	1	0	0	0
0.	0	0	0	0	0	0	0	0
15 [15=8+4+2+1]	0	0	0	0	1	1	1	1

Subnet / Sieťová maska

Definuje koľko bitov je súčasťou sieťovej a koľko hostovej časti IP adresy

Môže byť reprezentovaný v troch formátoch :

- /24
- 11111111. 11111111. 11111111.00000000
- 255.255.255.0

Príklad :

192.168.0.15/24

- Binárna reprezentácia :
- 11000000. 10101000.00000000.00001111
- 11111111. 11111111. 11111111.00000000

- /24 definuje:
- že prvých 24 bitov je sieťová časť
- Zvyšných 8 bitov je hostová časť

	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal Value	128	64	32	16	8	4	2	1
255.	1	1	1	1	1	1	1	1
255.	1	1	1	1	1	1	1	1
255.	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0

Počítanie IP sietí

Jednoduché pravidlá :

- Ak je maska /32 – ide o jednu IP
- Každým znížením masky o 1, sa počet IP v sieti násobí dvomi, presne ako v tabuľke.
- 2 IP v každej sieti sú vždy obsadené a preto hovoríme o „počte IP“ a „počte použiteľných IP“ (vždy o 2 menej).
  - Prvá – tzv. IP siete
  - Posledná – tzv. Broadcast IP
  - Logicky neplatí pre /32 a /31

Zadania :

- Úrad Vás požiada o vytvorenie siete, v ktorej potrebujú umiestniť presne 31 VM-iek. Akú veľkú sieť by ste im odporučili ?
- Vypočítajte IP siete a broadcast IP pre sieť v ktorej je 10.15.15.171/26.
- Koľko použiteľných IP je v sieti 192.168.33.100/27?
- Koľko bude použiteľných IP v sieti 10.1.1.0/22 ?
- Ako bude vyzerať IP siete pre tieto IP :
  - 10.10.10.10/24
  - 10.10.10.200/24

Maska	24	25	26	27	28	29	30	31	32
Počet IP	256	128	64	32	16	8	4	2	1

Priradzovanie IP sietí

Jednoduché pravidlá :

- IP plán musí byť vytvorený na začiatku, pretože je veľmi ťažké meniť ich „za behu“ a vyžaduje si to výpadok.
- Vytvárajte logické rezervy a to tak, aby sa siete s konkrétnym určením dali sumarizovať (napr. jedno mesto, región)
- Keď si koncový používateľ vyžiada určitý počet IP, vždy počítajte s rezervou (užívateľ väčšinou nepočíta s rastom) – ak je IP dostatok, pripočítajte približne dvojnásobok ak je maska väčšia ako 23
- Vždy prideľujte IP od začiatku a neskáčte na koniec.

Príklad z eSKa Cloudu :

- Vybrali sme privátny rozsah 10.0.0.0/8
- Vedeli sme o 3och poskytovateľoch a pri každom o jednom regióne. No pre istotu sme vytvorili rezervy.
- To čo v tabuľke nevidno, je ďalšie delenie vo vnútri každého poskytovateľa. Pripravili sme /12 na 2 regióny. Tam sme to znova rozdelili na menšie rozsahy pre jednotlivé využitia a všade sme nechali rezervy.
- Prečo ? – keď napr. príde nový poskytovateľ, alebo región u poskytovateľa – sme pripravení a tak to má byť.

Hlavný subnet 10.0.0.0/8			
Cloud provider	IP range	Prvá IP	Posledná IP
OCI	10.0.0.0/11	10.0.0.0	10.31.255.255
Rezervované	10.32.0.0/11	10.32.0.0	10.63.255.255
Azure	10.64.0.0/11	10.64.0.0	10.91.255.255
Rezervované	10.92.0.0/11	10.92.0.0	10.127.255.255
Privátna časť VC	10.128.0.0/11	10.128.0.0	10.159.255.255
Rezervované	10.160.0.0/11	10.160.0.0	10.191.255.255
Rezervované	10.192.0.0/11	10.192.0.0	10.223.255.255
Rezervované	10.224.0.0/11	10.224.0.0	10.255.255.255

Počítanie IP sietí / násobky pre výpočet v rôznych oktetoch

Maska	24	25	26	27	28	29	30	31	32
4. Oktet	256	128	64	32	16	8	4	2	1
Maska	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**
3. Oktet	256	128	64	32	16	8	4	2	1
Maska	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
2. Oktet	256	128	64	32	16	8	4	2	1
Maska	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1. Oktet	256	128	64	32	16	8	4	2	1

Koniec

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY