Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Základy počítačových sietí a komunikácie

Ochrana koncových zariadení v LAN a online bezpečnosť (Blok V.)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti vo verejnej správe

doc. Ing. Jozef Papán, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

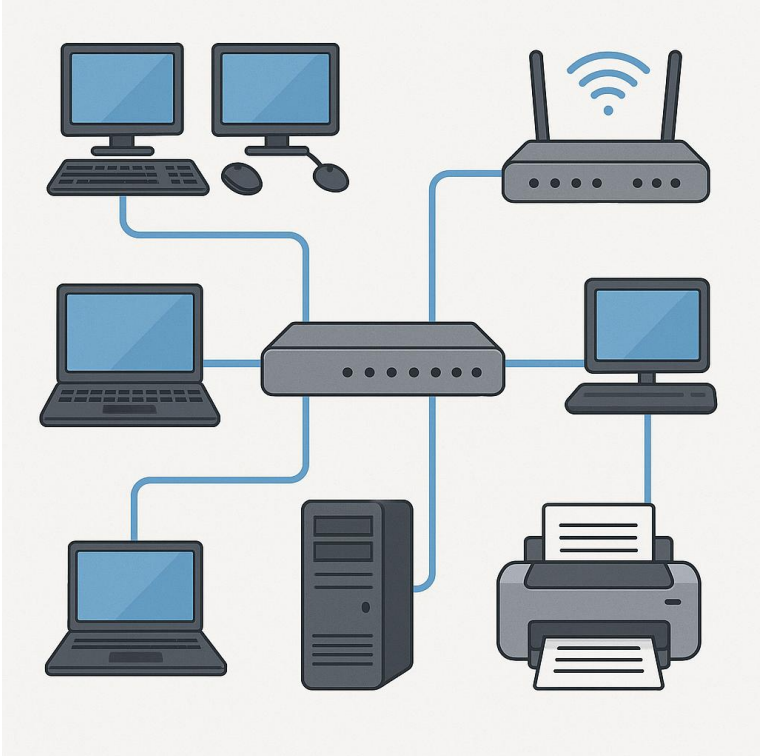
jozef.papan@uniza.sk

Obsah

Počítačové siete
Typy sieti a topológie
Komponenty sietí, typy a prepojenia
Princípy komunikácie v prepojenom svete
Zabezpečenie LAN sieti
....a iné ☺

Čo je to počítačová sieť?

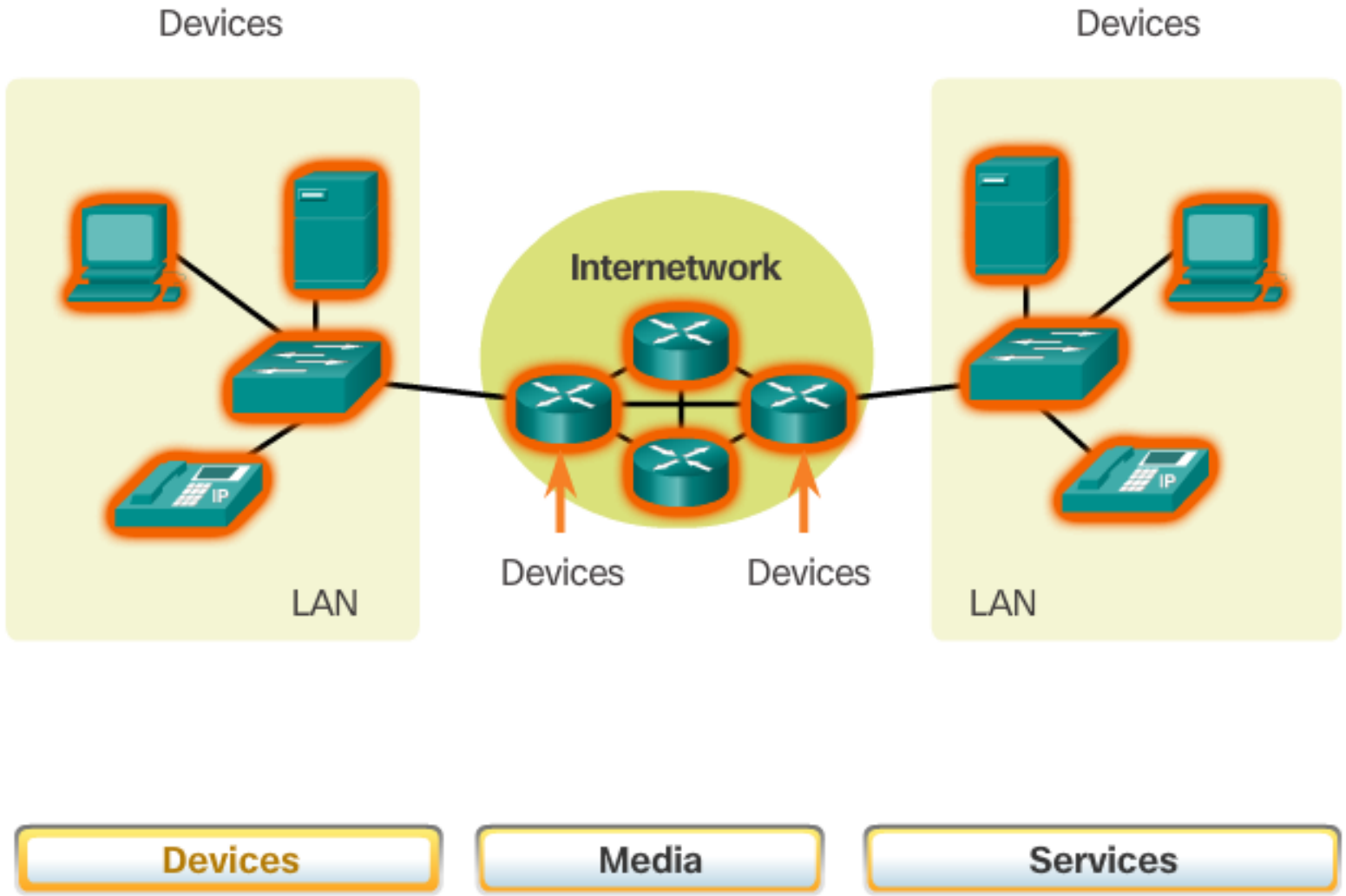
- Počítačová sieť je prepojenie dvoch alebo viacerých zariadení (napr. počítače, servery, tlačiarne), ktoré medzi sebou komunikujú za účelom výmeny dát a zdrojov.
- Sieť môže byť malá – napríklad domáca sieť medzi dvoma počítačmi, alebo extrémne rozsiahla ako internet, ktorý prepája miliardy zariadení na celom svete.
- Cieľom siete je umožniť zdieľanie informácií, prístup k vzdialeným službám a centralizáciu správy.
- Počítačové siete sú základom moderného digitálneho sveta a umožňujú komunikáciu v reálnom čase, elektronický obchod, prácu na diaľku a mnoho ďalšieho.



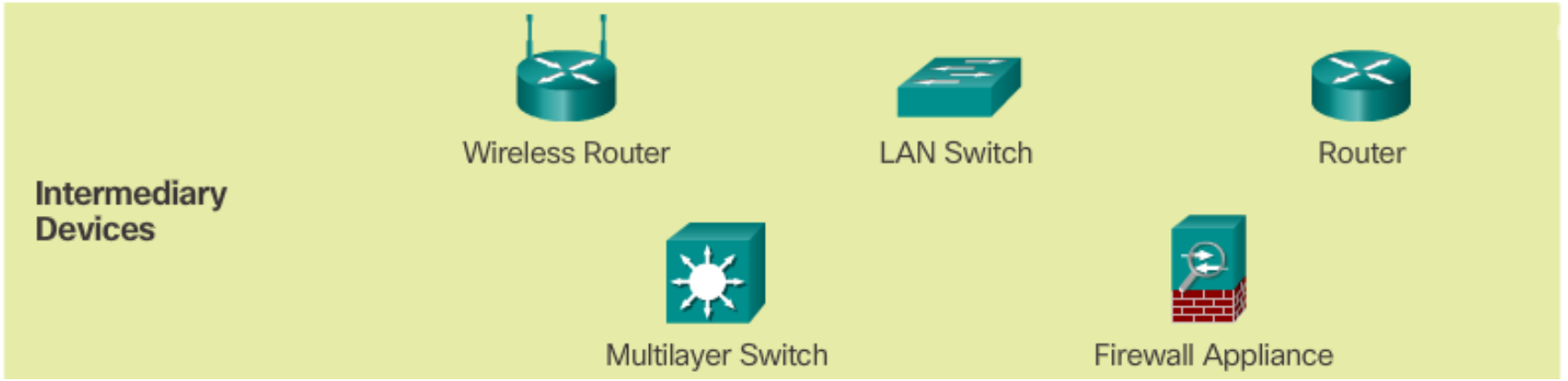
Celkový pohľad na sieťové komponenty I.

- Cesta ktorou prechádza správa môže byť rôzne dlhá
  - od 1 kábla, po x10-x100 sietí po celom svete
- Hoci sú komunikačné siete mimoriadne rozmanité, predsa majú isté rysy spoločné:

1. **Zariadenia**, ktoré komunikujú alebo komunikáciu sprostredkujú

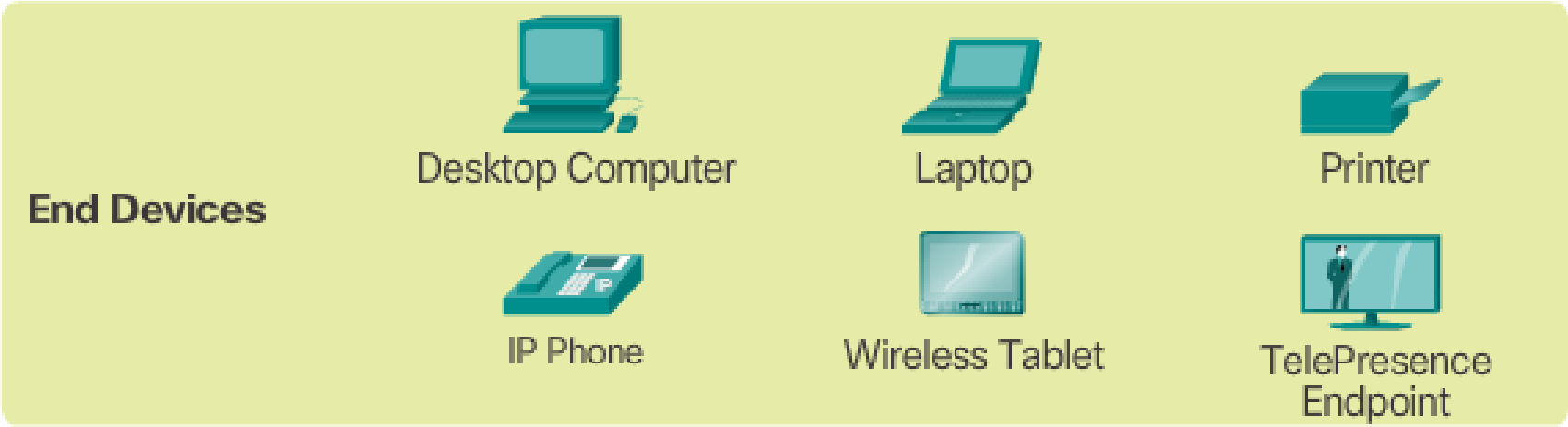


1.A. Medziľahlé zariadenia



- Regenerujú a preposielajú prenášaný signál
- Udržiavajú informácie o cestách do cieľových sietí
- Informujú ďalšie zariadenia o chybách a zlyhaniach v komunikácii
- Pri výpadku primárnej cesty presmerujú dáta záložnými trasami
- Obsluhujú tok dát na základe požiadaviek na kvalitu služby
- Povoľujú alebo zakazujú tok dát na základe bezpečnostných pravidiel
- Typické zariadenia: rozbočovače (hub), prepínače (switch), smerovače (router), firewally, prístupové body (access point), opakovače (repeaters), ...

1.B. Koncové zariadenia

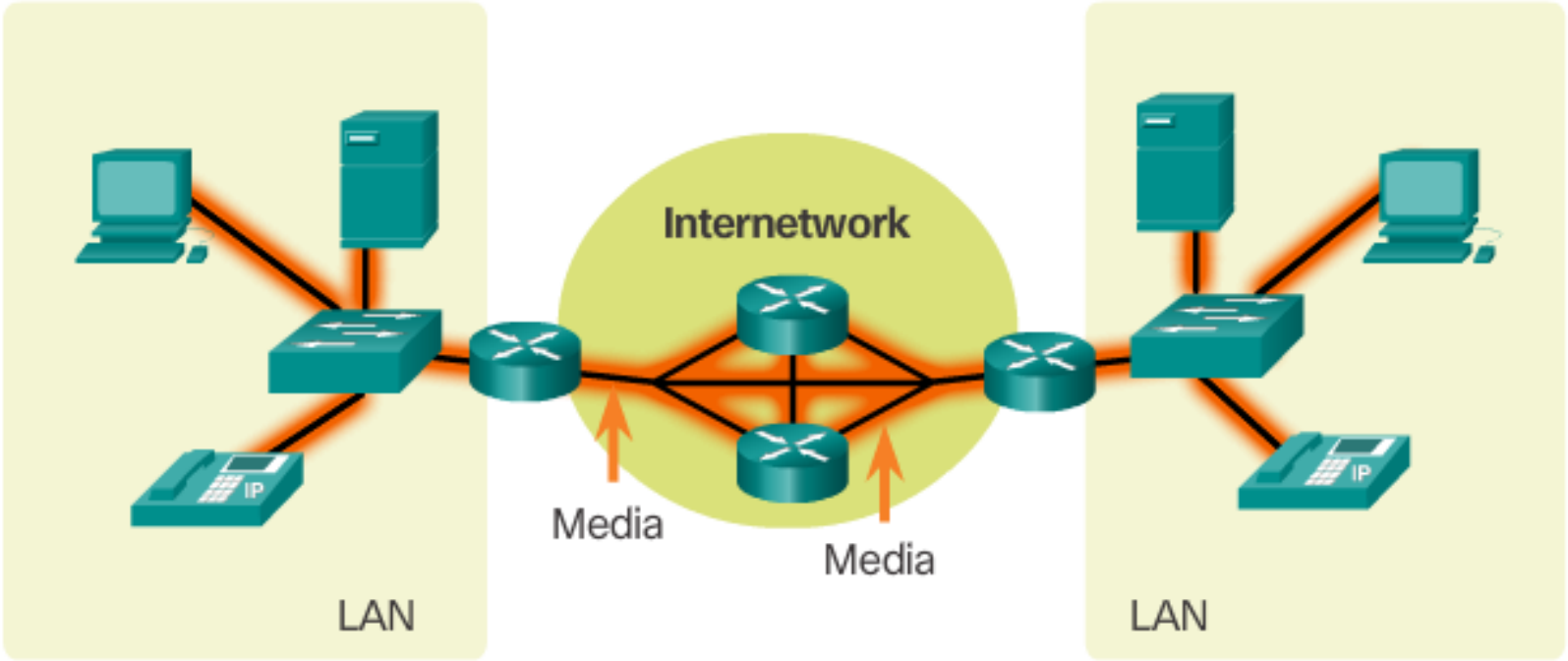


- Koncové zariadenia (end devices) predstavujú koncový bod komunikácie
  - Typicky ich ovláda používateľ – človek
  - Dáta v koncových zariadeniach vznikajú a spracúvajú sa, obvykle však cez ne neprechádzajú
  - Typické úlohy koncových zariadení: klient, server, klient i server

Celkový pohľad na sieťové komponenty II.

2. Médiá, ktorými sú zariadenia prepojené

- O mediach, typoch, ich parametroch, charakteristikách, využití - na 3. prednáške



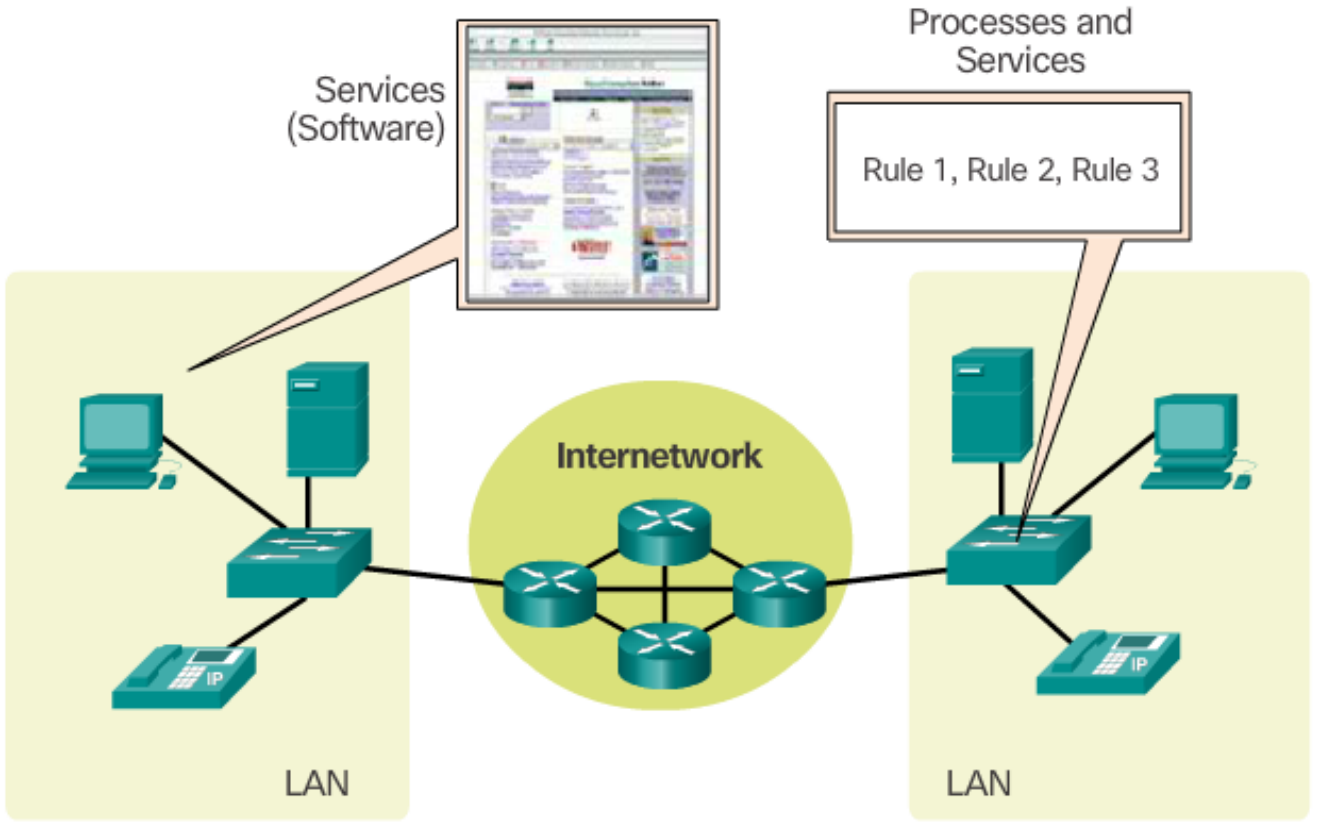
Devices | Media | Services

2. Médiá v sieťach

Celkový pohľad na sieťové komponenty III.

3. Služby, ktoré sieť ponúka pomocou **správ** a **pravidiel** (protokolov)

- v sieťach nazývame protokoly

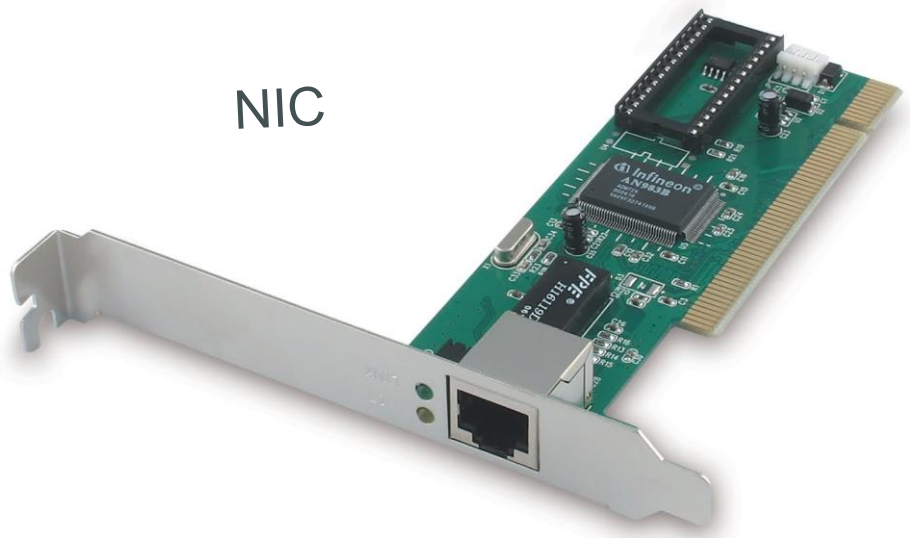


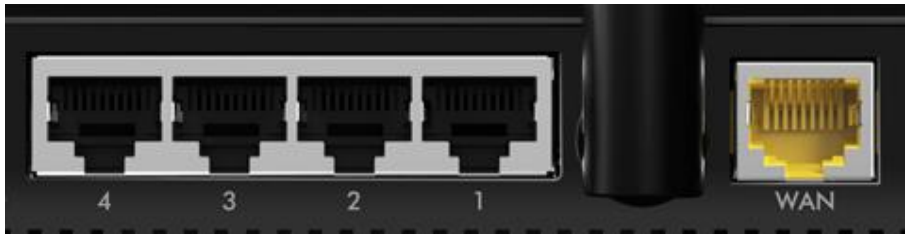
Devices | Media | Services

NIC, fyzický port / sieťové rozhranie

- NIC = sieťový adaptér
  - na fyzické pripojenie do siete pre PC alebo iné zariadenie, kábel/médium sa zasúva priamo do NIC
- Fyzický port
  - Konektor, alebo zásuvka sieťového zariadenia, kde sa zasúva médium
- Rozhranie
  - špecializovaný port na zariadení, na prepojenie k iným sieťam – preto sieťové rozhranie
- Posledné dva sú synonymá.

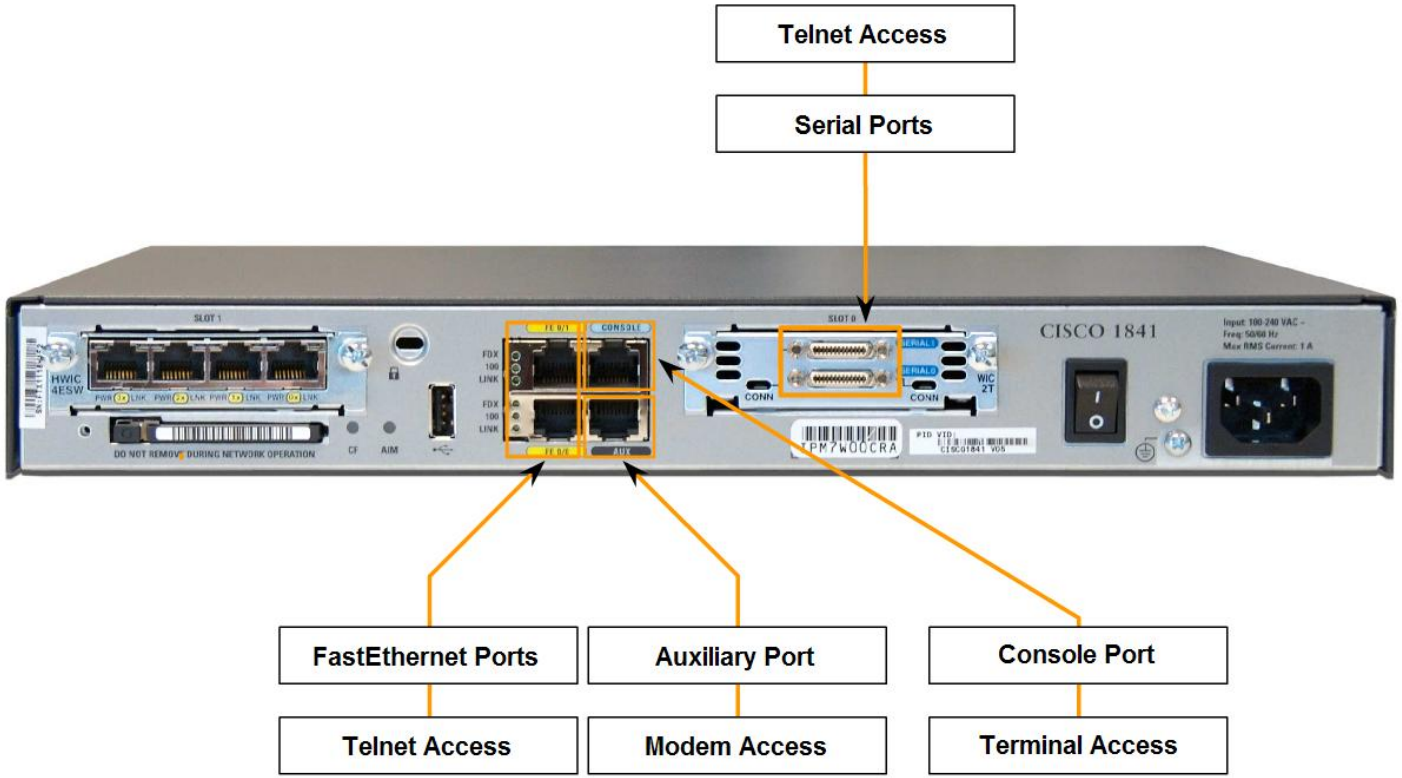
NIC





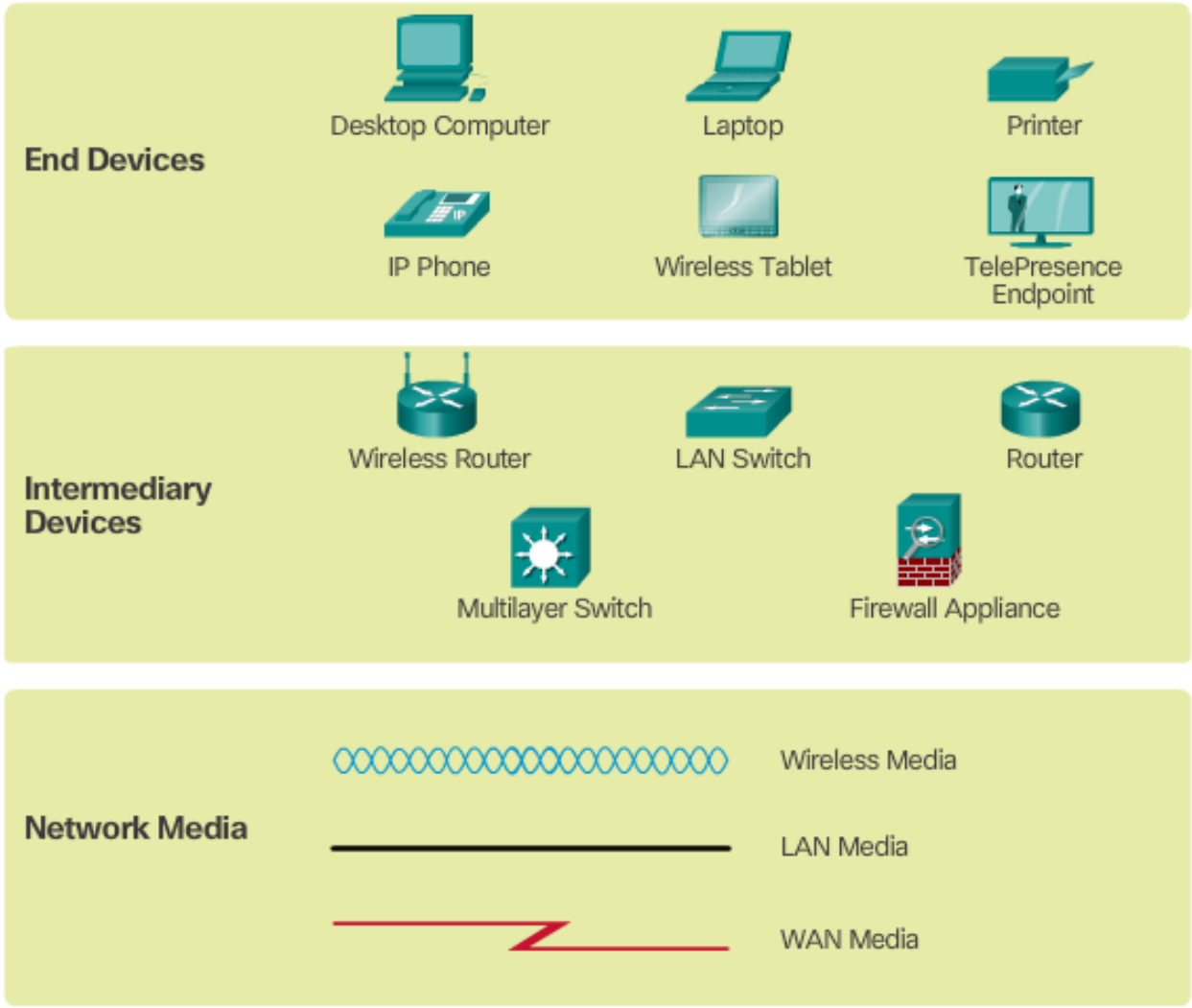
Konektory Cisco zariadení

- Konektory typického Cisco smerovača
  - Console: Manažmentový port, pripája sa ku COM portu počítača, slúži na konfiguráciu
  - AUX: Manažmentový port, pripája sa spravidla k modemu, slúži na konfiguráciu
  - FastEthernet, Serial: Sieťové rozhrania rôznych typov, slúžia na dátovú komunikáciu
- Na rozhraniach používaných v laboratóriách KIS je možné pripájať i odpájať kábel počas behu, bez vypínania zariadenia



Typy sietí a topológie

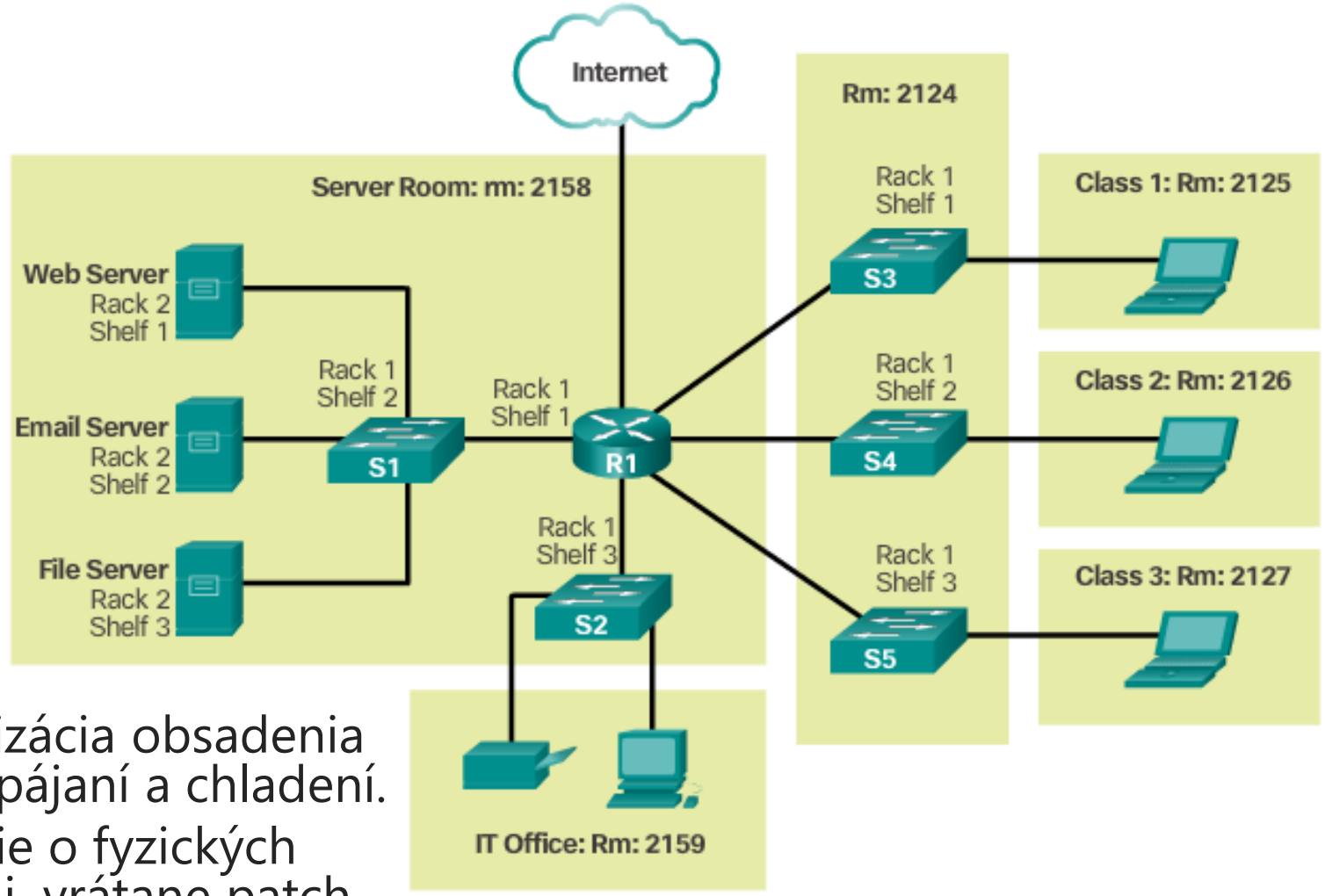
Symboly sieťových prvkov



Diagramy sieťových topológií

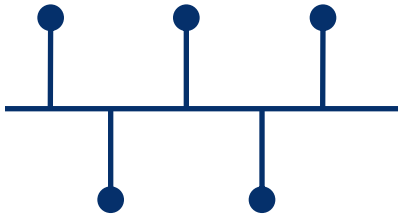
Fyzická topológia

1. **Umiestnenie zariadení**: Detailné schémy a diagramy zobrazujúce fyzické umiestnenie všetkých sieťových zariadení v rámci rackov a miestností.
2. **Káblovanie**: Presné trasy káblov, typy použitých káblov (napr. optické vlákna, medené káble), prepojenia medzi zariadeniami.
3. **Rackové usporiadanie**: Vizualizácia obsadenia rackov, vrátane informácií o napájaní a chladení.
4. **Fyzické prepojenia**: Informácie o fyzických spojeniach medzi zariadeniami, vrátane patch (prepojovacích) panelov a konektorov.
5. **Bezpečnostné prvky**: Umiestnenie fyzických bezpečnostných prvkov, ako sú zámky, kamery a prístupové systémy

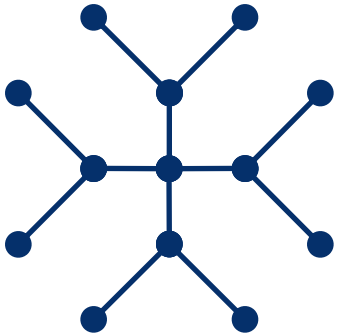


Fyzické topológie

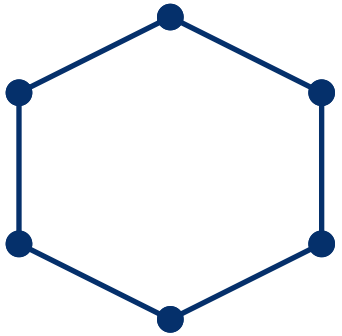
bod-bod (WAN)



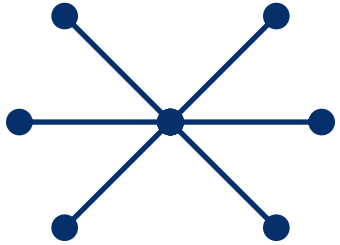
Zbernica (LAN)



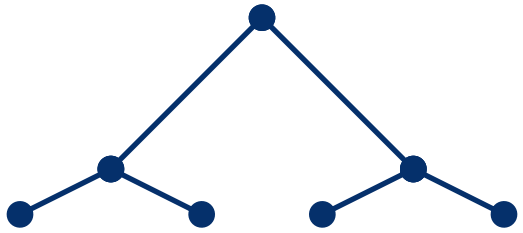
rozšírená hviezda (LAN)



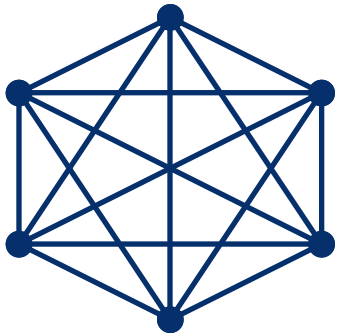
Kruh (LAN)



Hviezda (pre LAN)
Hub&Spoke (pre WAN)

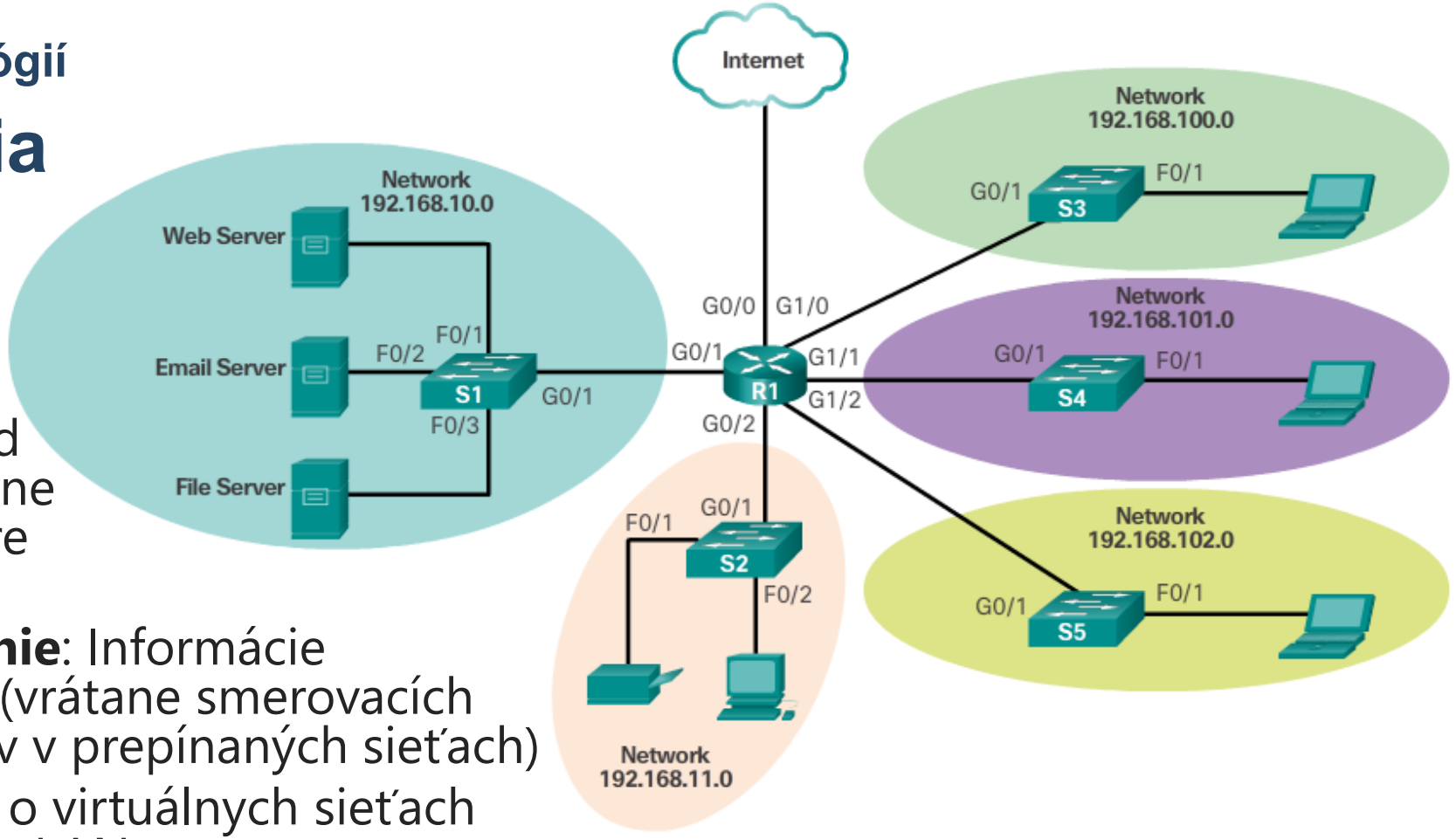


Stromová/Hierarchická (LAN)



full mesh (WAN)

Logická topológia



1. **Členenie siete na logické celky**
2. **Logické adresy**: prehľad logickej adresácie, vrátane IP adries, IP rozsahov pre LAN a virtuálne LAN
3. **Smerovanie a prepínanie**: Informácie o logických trasách dát (vrátane smerovacích protokolov, a protokolov v prepínaných sieťach)
4. **Virtuálne siete**: Detaily o virtuálnych sieťach (ako sú VLAN – virtuálne LAN,
   VPN - Virtual Private Network, virtuálna privátna sieť, technológia, ktorá umožňuje bezpečné pripojenie k inej sieti cez internet.
5. **Bezpečnostné politiky**: logické bezpečnostné opatrenia, ako sú firewall pravidlá, segmentácia siete.
6. **Kvalita služby:** QoS, Quality of Service, nastavenia pre riadenie kvality služieb, vrátane priorít pre rôzne typy dátového prenosu

Siete rôznych veľkostí

- Malé siete inštalované doma – umožňujú zdieľanie zdrojov, tlačiarní, dokumentov, obrázkov, hudby medzi domácimi PC
- Vo väčších firemných sieťach alebo väčších organizáciách ako napr. ŽU – sa siete využívajú vo väčšom rozsahu – sú potrebné sieťové úložiská, sieťové servery s rôznymi službami, nástroje kolab., 100-1000 zariadení

Small Home Networks

Small Office/Home Office Networks

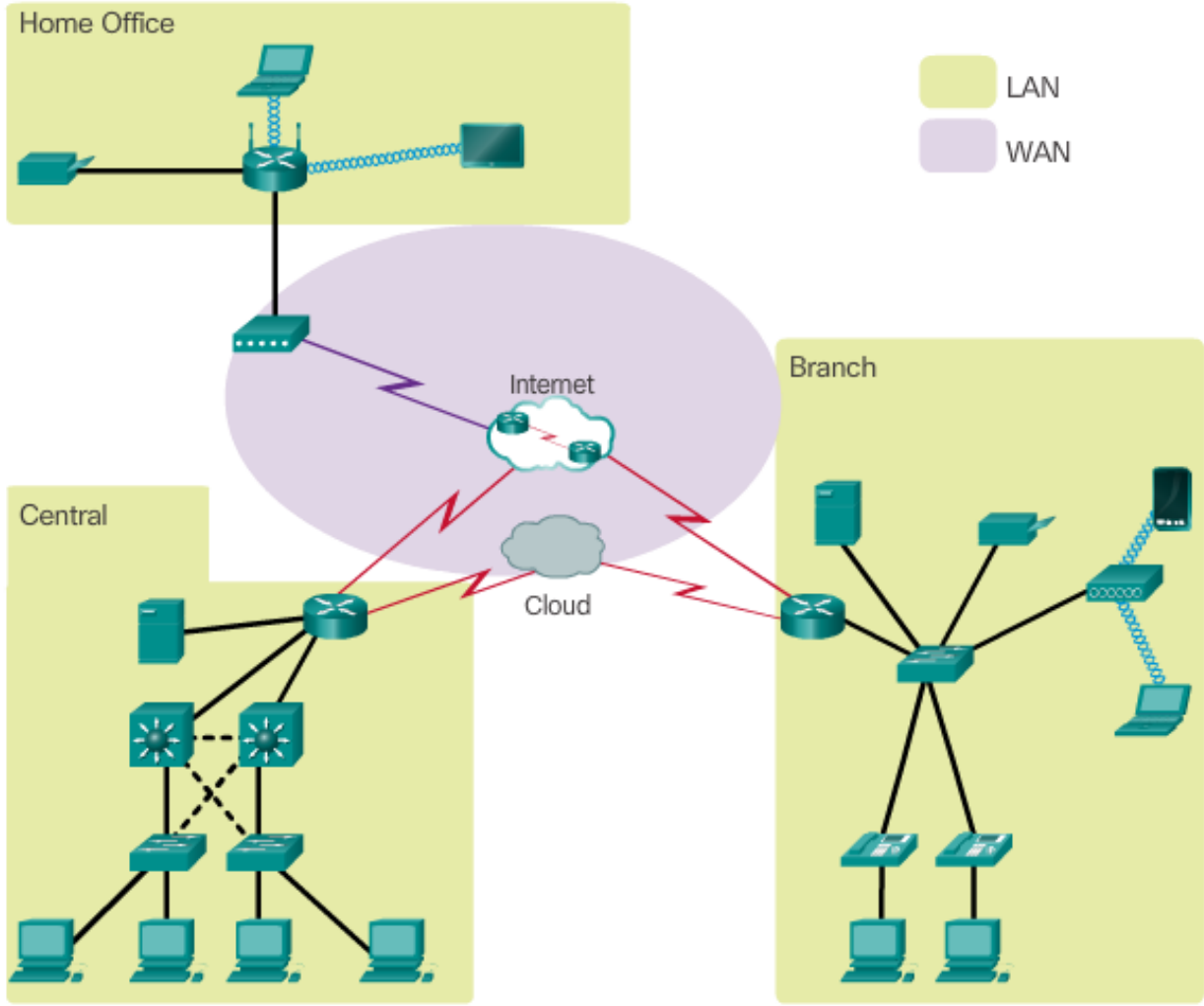
Medium to Large Networks

World Wide Networks

- Keď niekto pracuje z domu a pripája sa do firemnej siete, alebo má niekto menšiu firmu doma, kde poskytuje služby alebo predáva produkty cez internet
- Internet je najväčšou existujúcou sieťou dneška, sieť sietí, je to prepojenie privátnych a verejných sietí rôznych veľkostí, milióny zariadení

Typy sietí

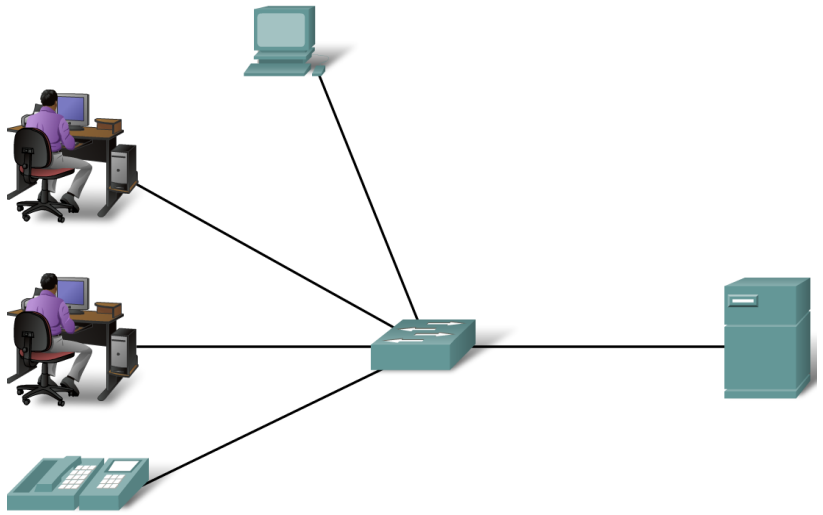
- Najznámejšie typy sieťovej infraštruktúry:
  - Lokálna sieť(Local Area Network, LAN)
  - Sieť veľkého rozsahu(Wide Area Network, WAN)
- Iné typy sietí:
  - Metropolitan Area Network (MAN)
  - Wireless LAN (WLAN)
  - Storage Area Network (SAN)



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

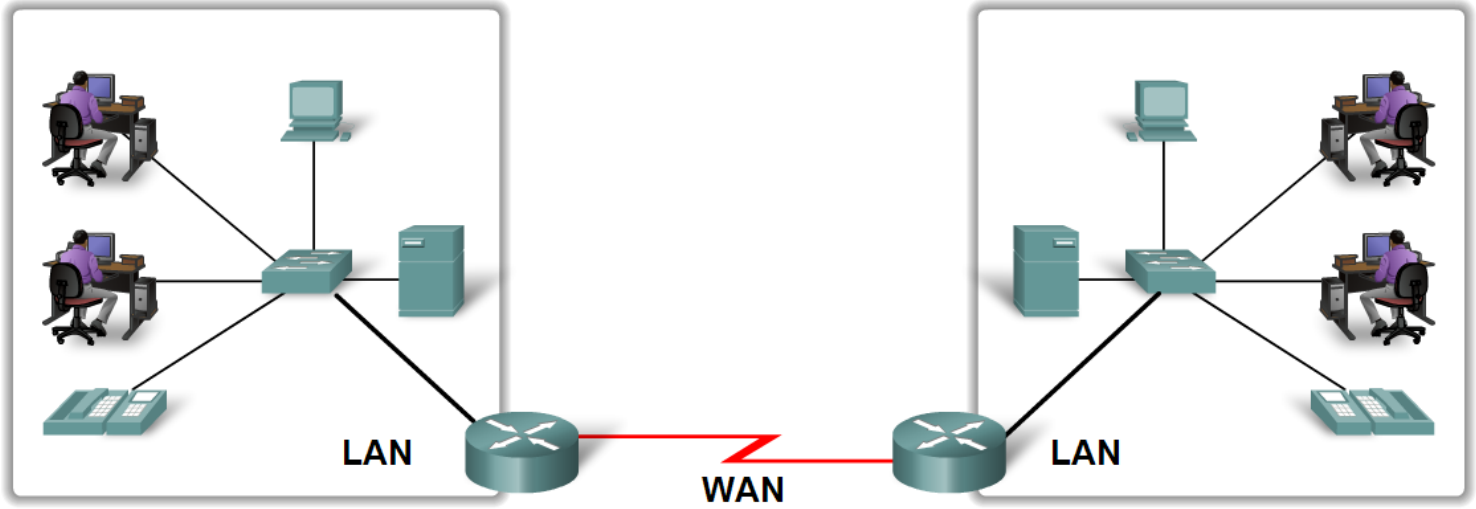
Lokálna sieť (Local Area Network, LAN)

- Sieť spravidla menšieho rozsahu, pomerne vysoké rýchlosti
- Vlastníkom a používateľom je obvykle jedna organizácia
- Typickými LAN sieťami sú domáce či vnútrofiremné siete
- Technológie: Ethernet, WiFi



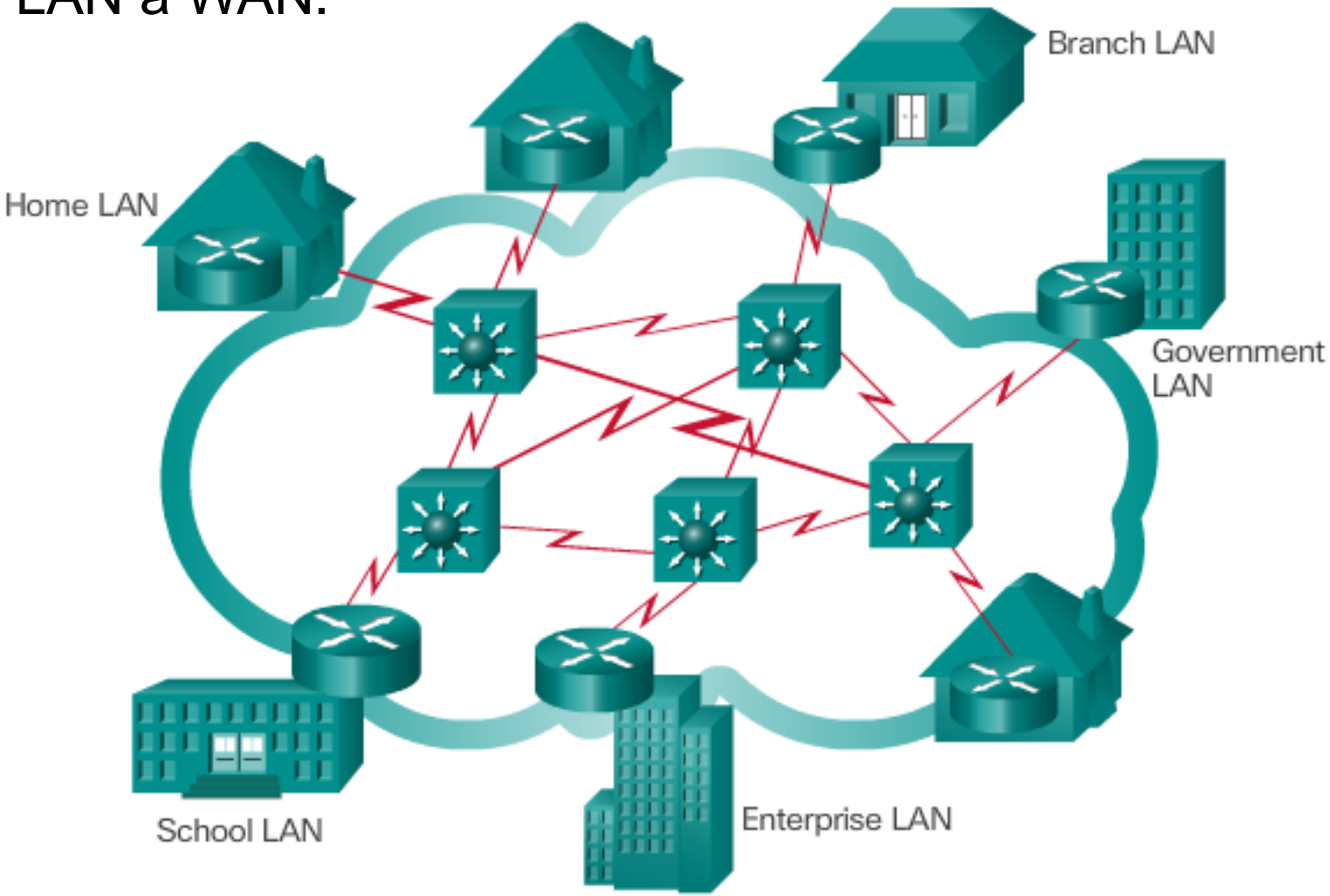
Sieť veľkého rozsahu (Wide Area Network)

- Sieť veľkého geografického rozsahu, prepájajúca vzdialené lokality
- Používateľ tejto siete je spravidla iný ako jej vlastník – WAN sieť alebo komunikáciu po nej si používateľ od jej vlastníka prenajíma
- Vlastník WAN sa nazýva „poskytovateľ služby“ (service provider)
- Technológie: dial-up, HDLC, PPP, ISDN, Frame Relay, DSL, FTTx, GPON, MPLS, ATM, Carrier Ethernet, X.25, SONET/SDH, ...
- Pomerne široký diapazón rýchlostí



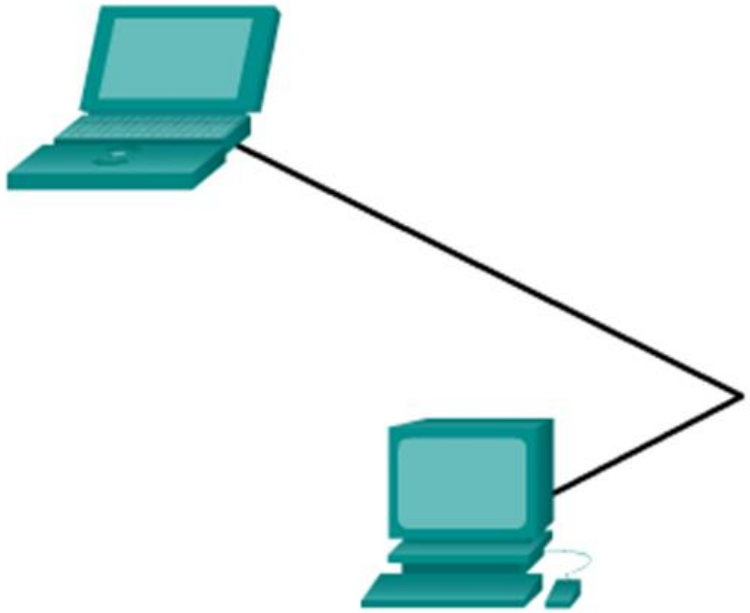
Internet

- Prepojené LAN a WAN.

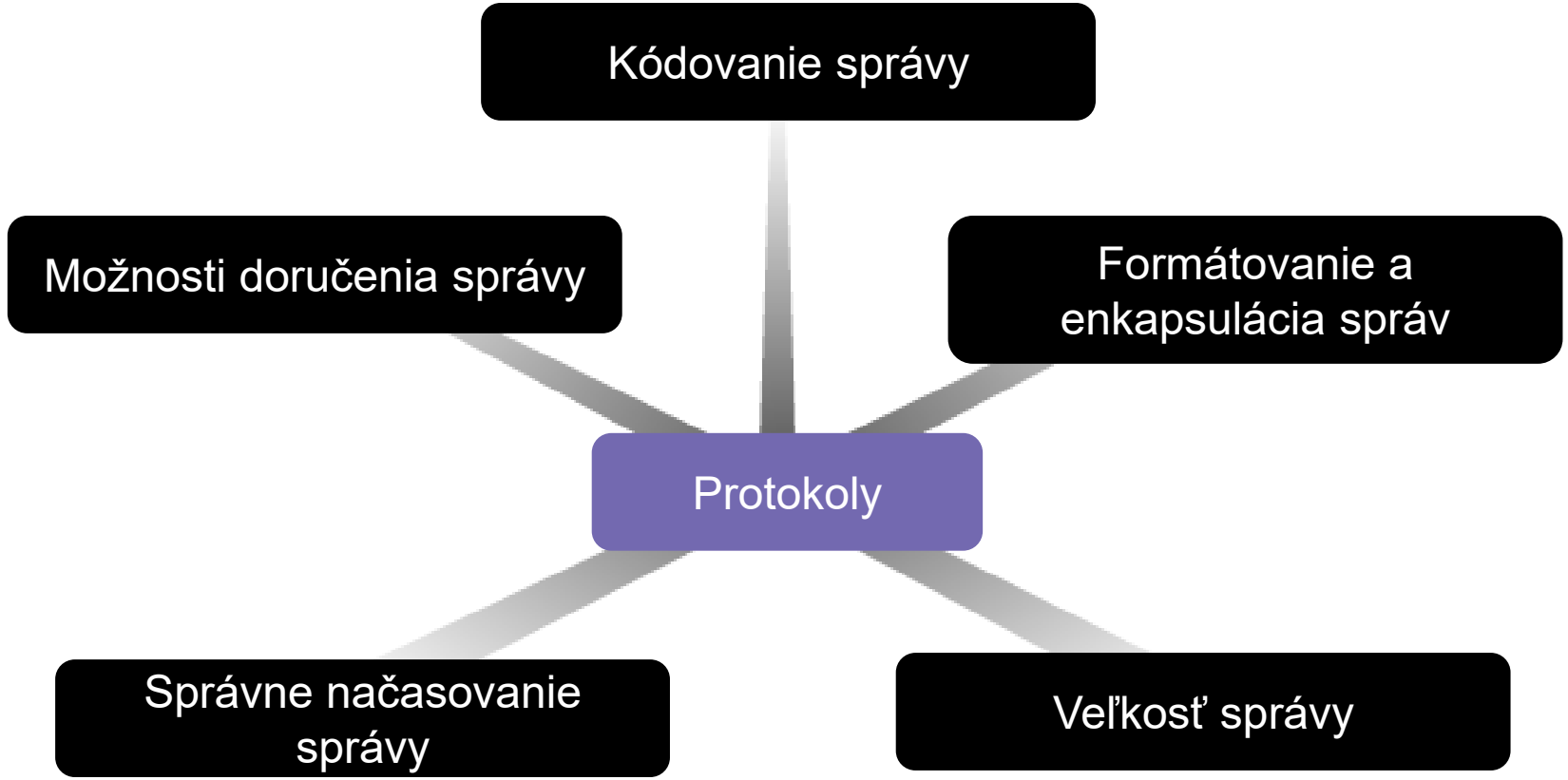


Pravidlá komunikácie

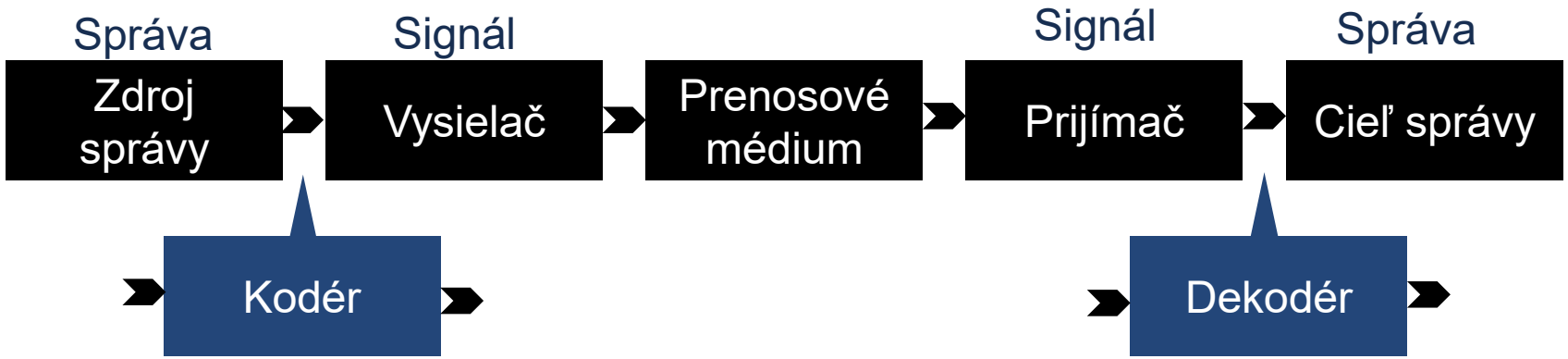
Základy komunikácie

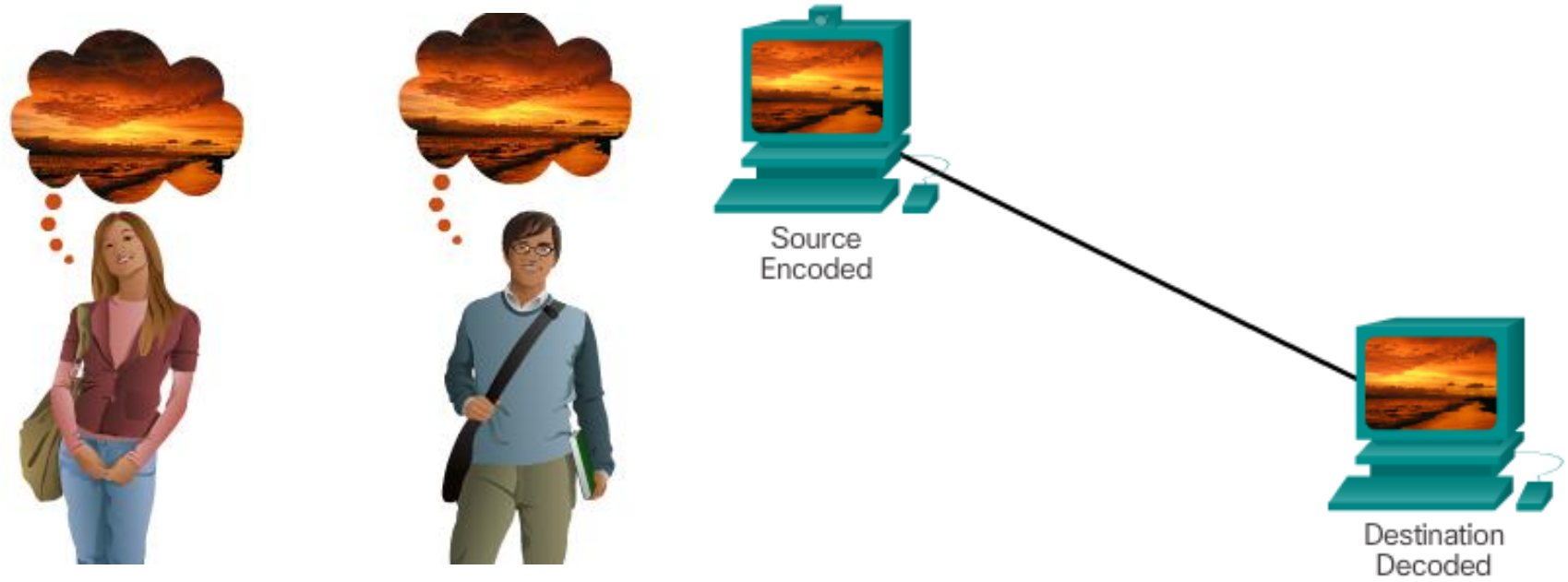


Vytvorenie pravidiel

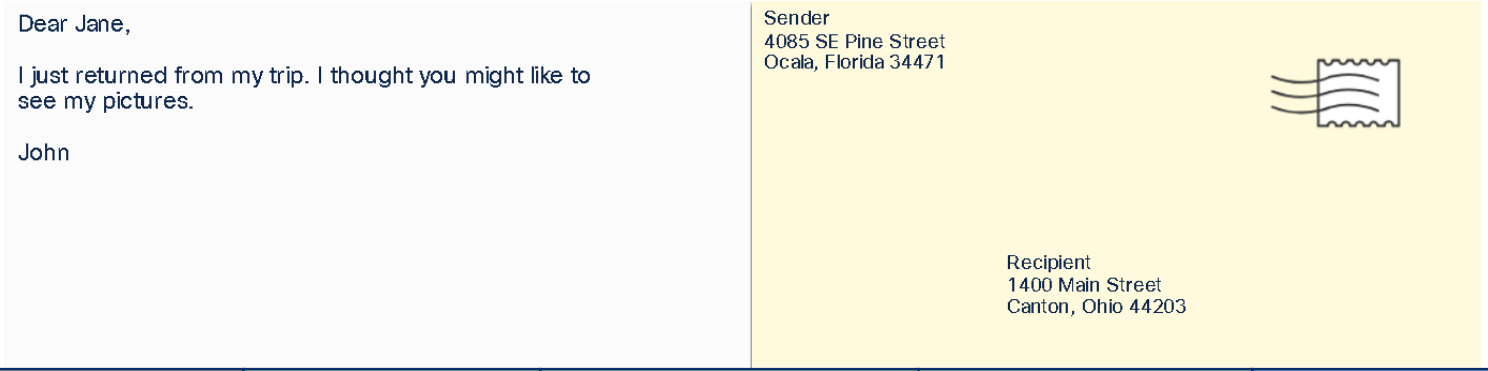


Kódovanie správy





Formátovanie správ a zapúzdrenie



Cieľ (fyzická/HW adresa)	**Zdroj** (fyzická/HW adresa)	**Začiatočná značka** (indikátor začiatku správy)	**Príjemca** (identifikátor cieľa)	**Odosieľateľ** (identifikátor zdroja)	**Zapúzdrené dáta**	**Koncová značka** (indikátor konca správy)
Adresovanie rámca		**Zapúzdrená správa**				
1400 Main Street Canton, Ohio 44203	4085 SE Pine Street Ocala, Florida 34471	Dear	Jane	John	I just returned from my trip. I thought you might like to see my pictures.	

Formátovanie správ a zapúzdrenie

Cieľ (fyzická/HW adresa)	**Zdroj** (fyzická/HW adresa)	**Začiatočná značka** (indikátor začiatku správy)	**Príjemca** (identifikátor cieľa)	**Odosieľateľ** (identifikátor zdroja)	**Zapúzdrené dáta**	**Koncová značka** (indikátor konca správy)
Adresovanie rámca		**Zapúzdrená správa**				

Veľkosť správy

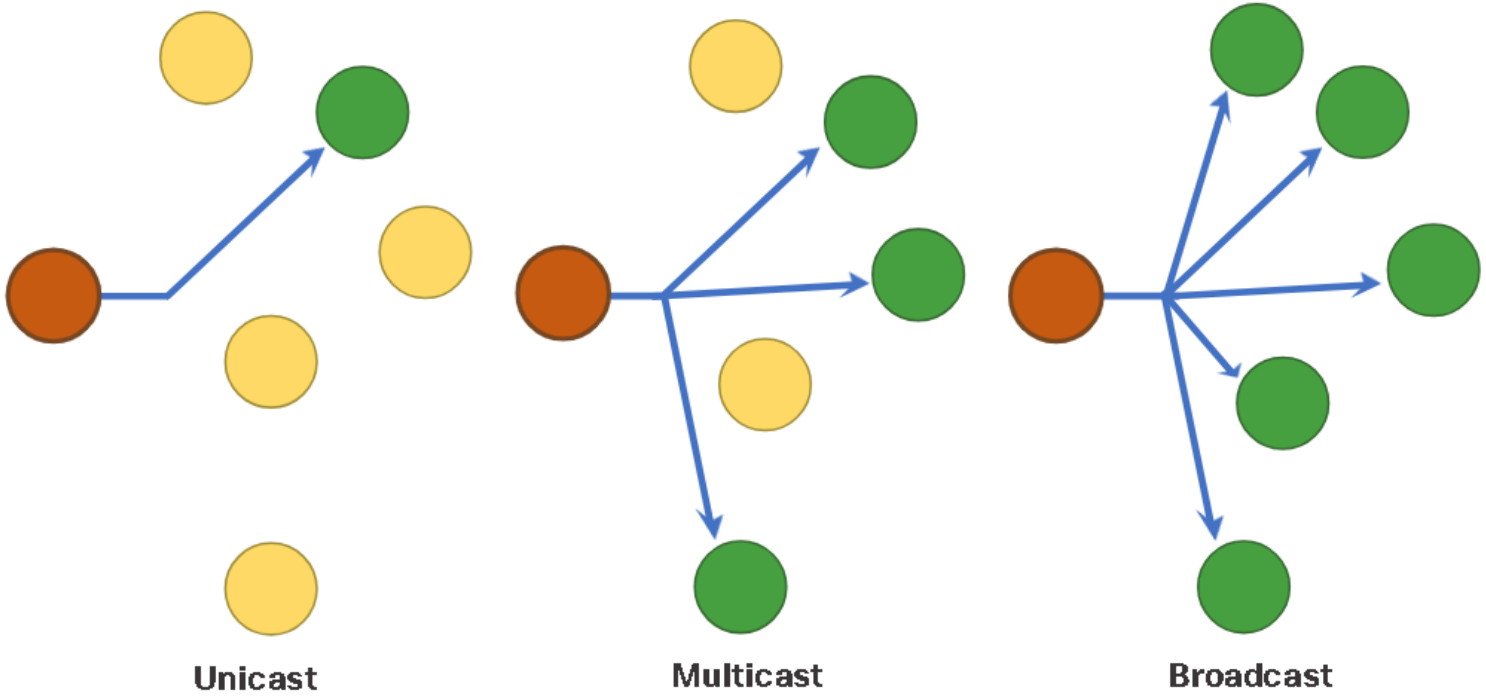
- Počítačová komunikácia
- Zdroj **rozdelí** dlhú správu na menšie bloky alebo rámce, ktoré spĺňajú minimálne a maximálne požiadavky na ich dĺžku
- Každý rámec bude mať svoje **adresné informácie**
- Príjemca prijaté rámce **rekonštruuje** aby ich mohol spracovať a interpretovať

Správne načasovanie správy

Pravidlá na ktorých sa treba dohodnúť:

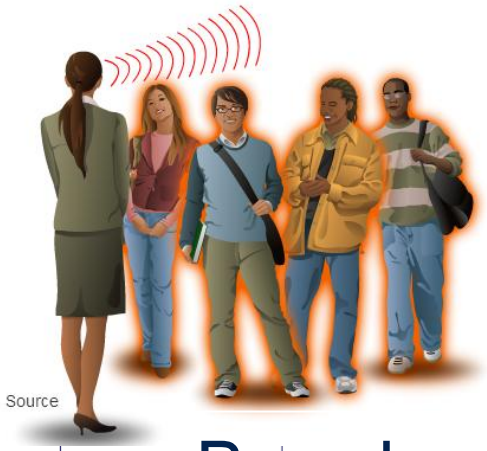
- **Prístupová metóda** (Access Method)
- **Kontrola toku dát** (Flow Control)
- **Vypršanie času čakania na odpoveď** (Response Timeout)

Možnosti doručovania správ



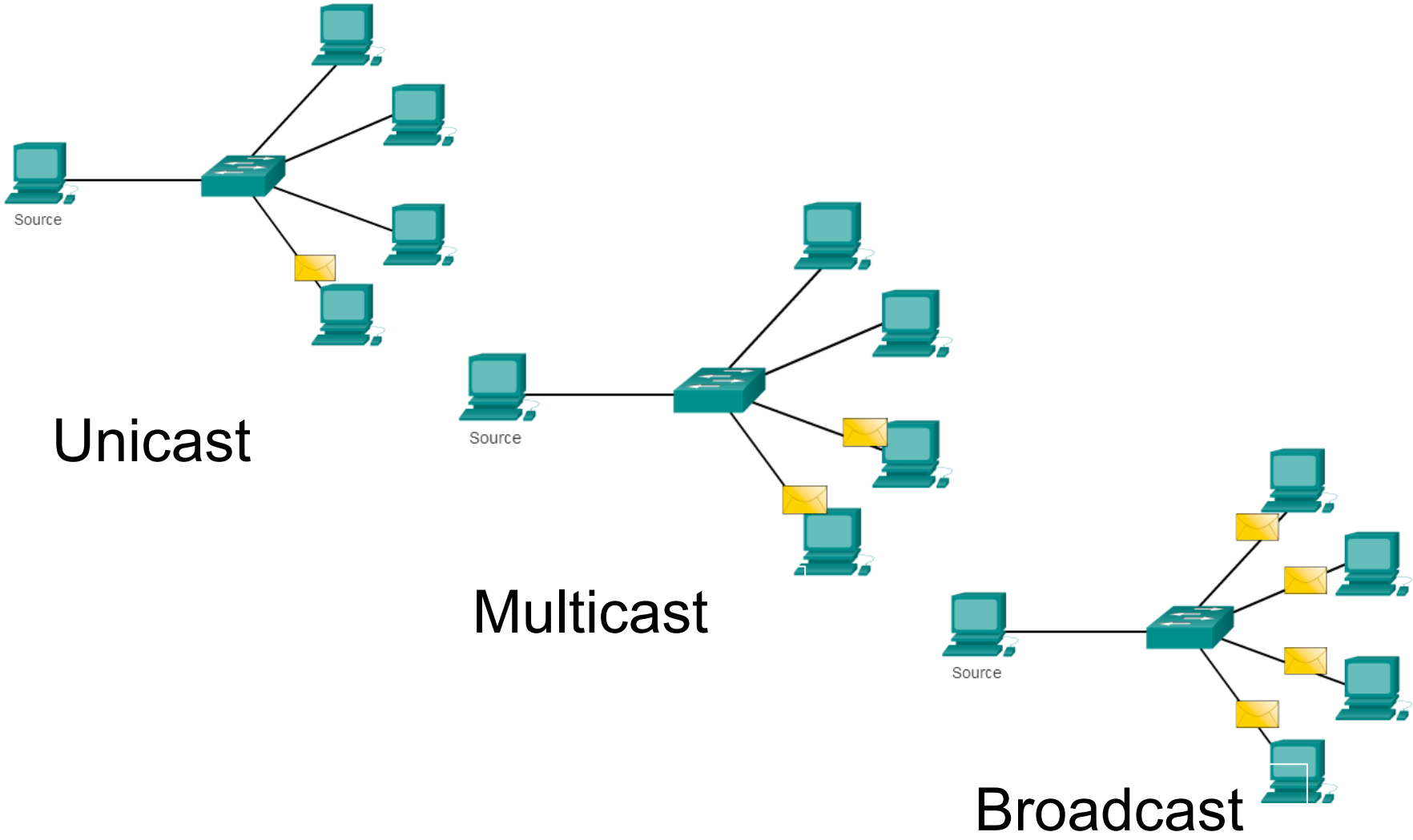
Unicast

Multicast



Broadcast

Možnosti doručovania správ



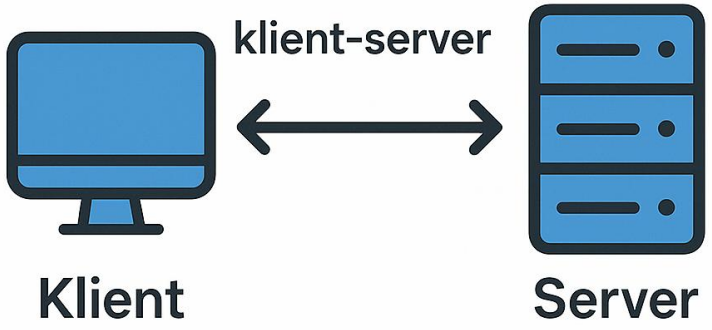
Spôsoby komunikácie s ohľadom na počet príjemcov

- S ohľadom na počet príjemcov existujú tri možnosti, ako sa každý datagram doručuje
- **Unicast**
  - Príjemcom je práve jeden adresát
  - Odosiela sa jeden datagram, môže byť prijatý mnohými uzlami, no spracovaný bude iba svojím zamýšľaným príjemcom
- **Multicast**
  - Príjemcom je presne vyhranená skupina adresátov, tzv. multicastová skupina
  - Odosiela sa jeden datagram, môže byť prijatý mnohými uzlami, no spracovaný bude len členmi multicastovej skupiny, ktorej je určený
- **Broadcast**
  - Príjemcami sú všetky uzly v dosahu
  - Odosiela sa jeden datagram, bude prijatý a spracovaný všetkými uzlami, ku ktorým sa doručí
  - Priestor šírenia broadcast datagramu sa nazýva **broadcastová doména**

Komponenty sietí, typy a prepojenia

Klienti a servery v sieti

- Klient – zariadenie alebo softvér, ktorý požaduje služby alebo zdroje zo servera (napr. počítač, ktorý si sťahuje e-maily).
- Server – zariadenie alebo softvér, ktorý poskytuje služby klientom (napr. webový server, ktorý hostuje webové stránky).



Komponenty sieťovej infraštruktúry

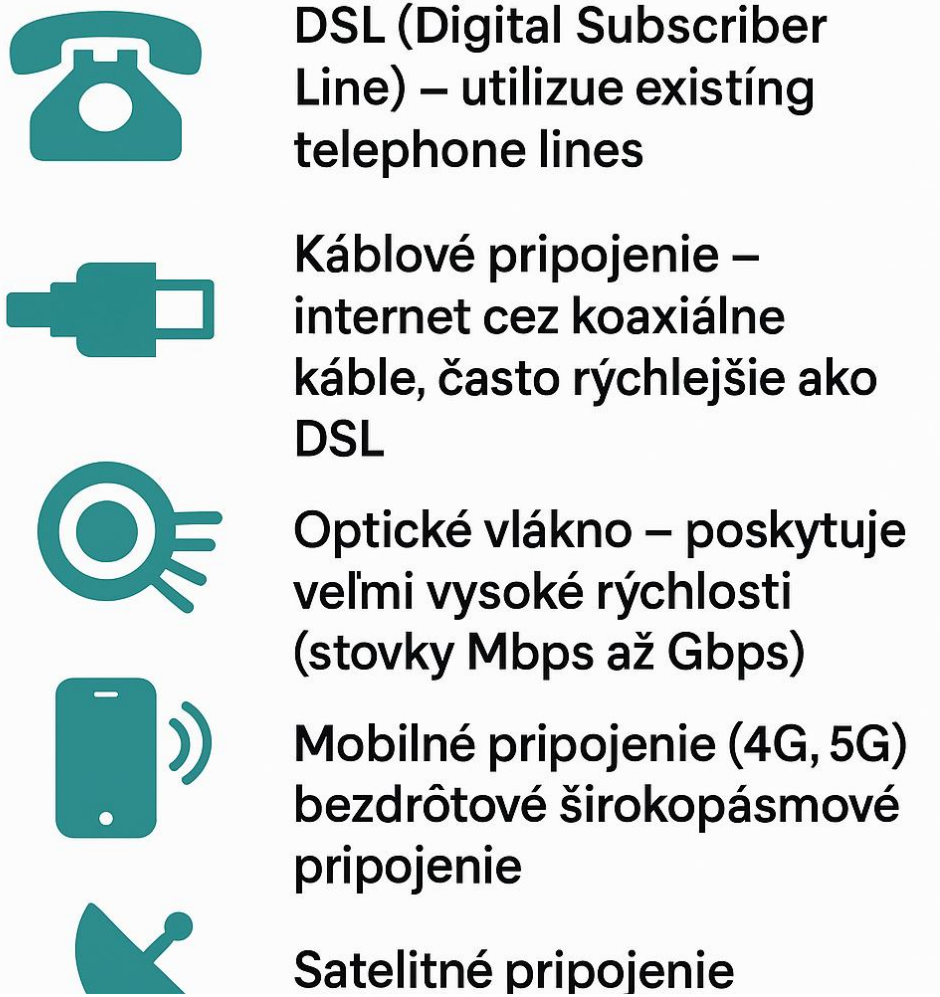
- Smerovače (routery) – prepájajú siete dohromady, smerujú dáta na správne miesto.
- Prepínače (switches) – prepojujú zariadenia v LAN sieti, inteligentne smerujú komunikáciu iba medzi správne zariadenia.
- Prístupové body (Access Points, AP) – umožňujú bezdrôtové pripojenie zariadení k LAN sieti.

Rozhrania a porty

- Komunikácia v sieti závisí od rozhraní koncových zariadení, rozhraní medziľahlých sieťových zariadení, a od káblov, ktoré ich prepíjajú
- Najpoužívanejšie typy médií sú krútená dvojlinka, optický kábel, koaxiálny kábel a wifi.
- Rôzne médiá majú rôzne parametre a výhody/nevýhody pri nasadení v konkrétnom prostredí.
- Ethernet je najpoužívanejšou LAN technológiou.
- Ethernetové porty nájdeme na koncových zariadeniach, prepínačoch, smerovačoch a iných sieťových zariadeniach.
- Prepínače s Cisco IOS majú tiež fyzické ethernetové porty pre pripojenie koncových staníc. Ale majú tiež 1 alebo viac virtuálnych rozhraní (switch virtual interfaces, SVI), ktoré neprislúchajú žiadnemu fyzickému hardvéru (ani portu), ale sú vytvorené v softvéry zariadenia.
- Virtuálne rozhrania na prepínači sa používajú na jeho vzdialené menežovanie/konfiguráciu.

Možnosti pripojenia k poskytovateľovi internetu (ISP)

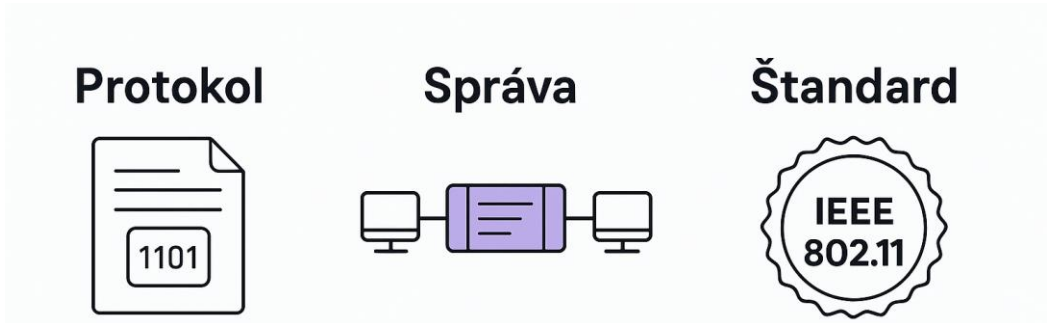
- **DSL** (Digital Subscriber Line) – využíva existujúce telefónne linky.
- **Káblové pripojenie** – internet cez koaxiálne káble, často rýchlejšie ako DSL.
- **Optické vlákno** – poskytuje veľmi vysoké rýchlosti (stovky Mbps až Gbps).
- **Mobilné pripojenie** (4G, 5G) – bezdrôtové širokopásmové pripojenie.
- **Satelitné pripojenie** – vhodné pre vzdialené oblasti, ale s vyššou latenciou.



Princípy komunikácie v prepojenom svete

Protokol, správa, štandard

- **Protokol** – je definovaný súbor pravidiel a postupov, ktoré určujú, ako majú zariadenia medzi sebou komunikovať v sieti. Zabezpečuje, že údaje budú správne odoslané, prenesené a prijaté. Príkladom je TCP/IP protokol, ktorý určuje, ako sa dáta rozdeľujú na pakety a ako sa znovu skladajú. Správa – jednotka dát, ktorá sa prenáša cez sieť.
- **Štandard** – zabezpečujú kompatibilitu medzi rôznymi výrobcami zariadení a systémov. Ide o dohodnuté pravidlá, špecifikácie a normy. Napríklad štandard IEEE 802.11 definuje technické požiadavky pre bezdrôtové siete Wi-Fi.
- **Správa** – Správa predstavuje logickú jednotku dát, ktorá sa odosiela medzi zariadeniami v sieti. Môže to byť napríklad požiadavka na zobrazenie webovej stránky, e-mail alebo iná forma dát. Každá správa je zabalená do formátu, ktorý vyhovuje konkrétnemu protokolu.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Otvorené a proprietárne protokoly

- Protokoly sa zvyknú podľa svojho pôvodu a dostupnosti rozlišovať na **proprietárne** a **otvorené**
- **Proprietárny protokol**

  Protokol, ktorý si jeho výrobca chráni ako intelektuálne vlastníctvo

  Nezverejnil jeho popis, prípadne

  Jeho časti alebo celý protokol si patentoval, prípadne

  Požaduje za jeho používanie či implementáciu poplatky

  Typické firemné protokoly konkrétnych výrobcov

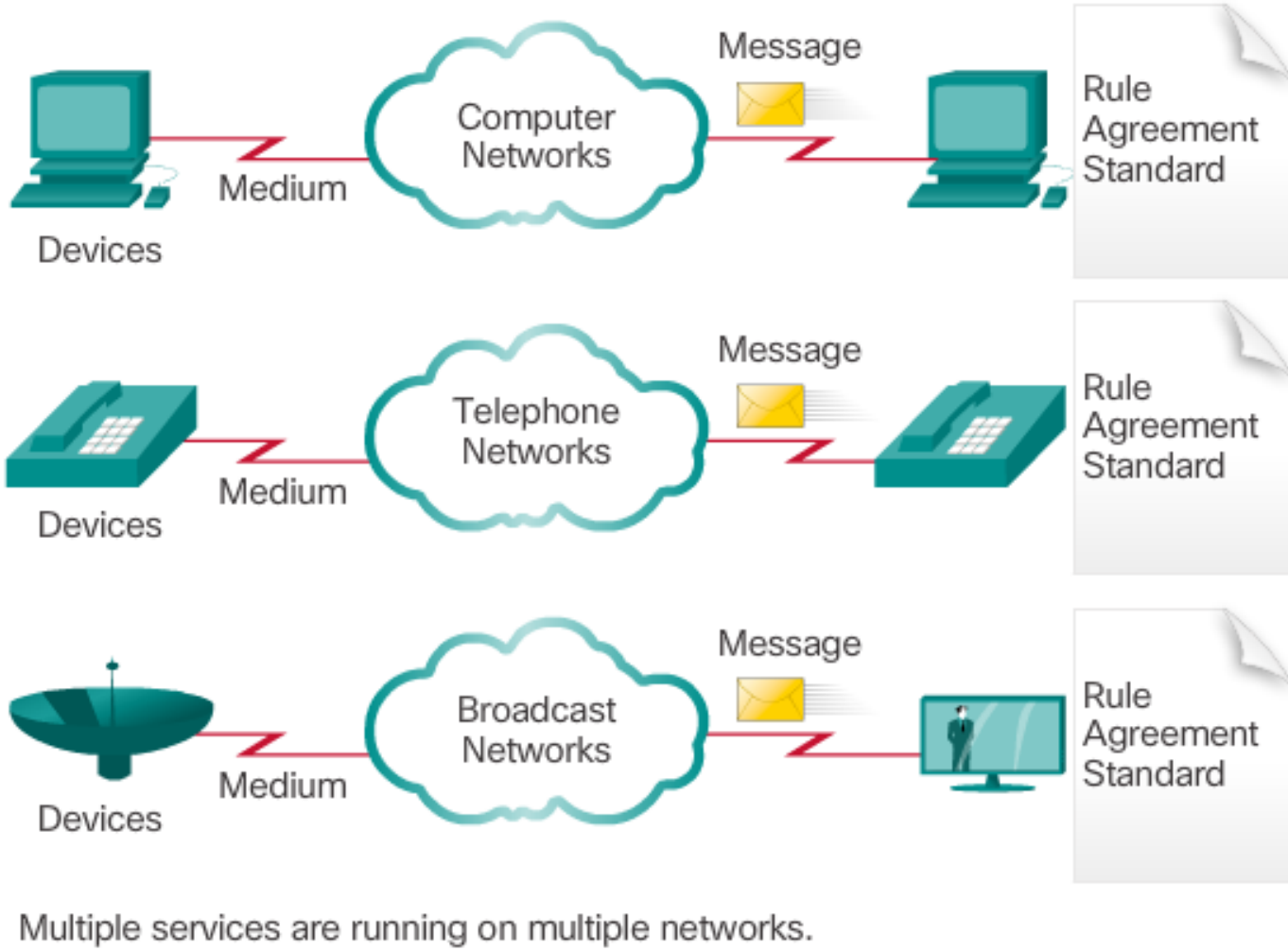
- **Otvorený protokol**

  Protokol, popis ktorého je voľne k dispozícii (nie nevyhnutne zadarmo) a ktorý môže slobodne implementovať akýkoľvek výrobca

  Otvorené protokoly sú najčastejšie dielom tzv. štandardizačných alebo normalizačných organizácií (IEEE, ISO, ITU-T, ETSI, IETF, ...)

  Používanie otvorených protokolov by malo byť preferované, pretože umožňuje kompatibilitu zariadení rôznych výrobcov

Tradičné oddelené siete

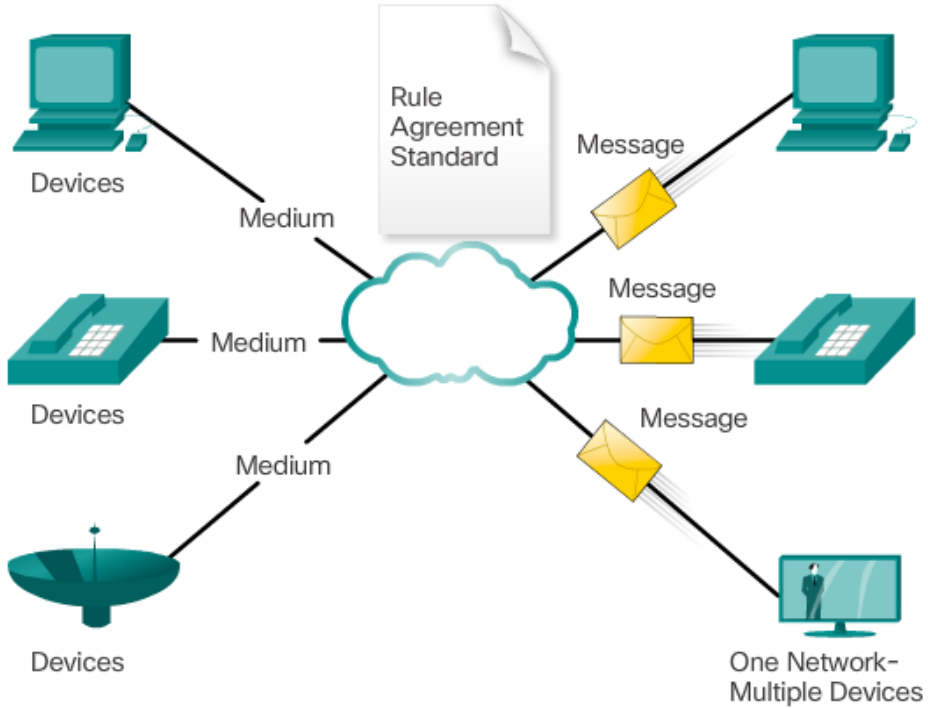


Multiple services are running on multiple networks.

- Aké to má výhody a aké nevýhody?

Konvergencia sietí

- Nahrádzanie jednoúčelových sietí univerzálnou sieťou



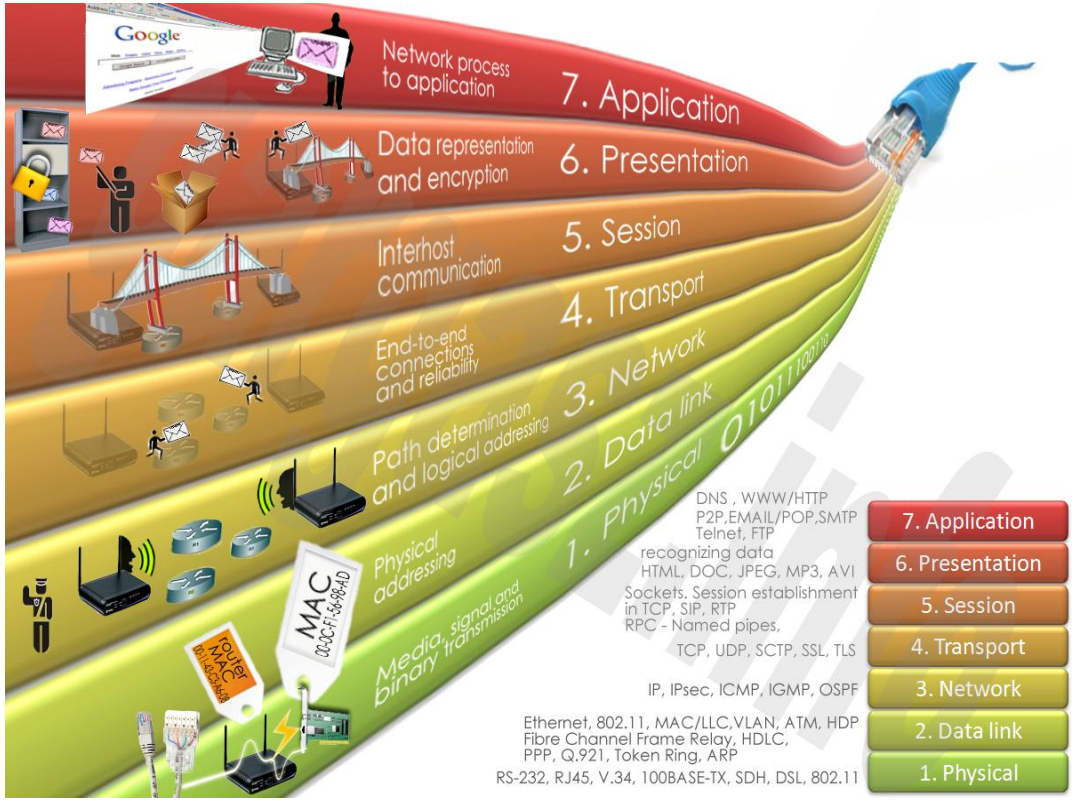
Converged data networks carry multiple services on one network.

- Aké to má výhody a aké nevýhody?

Referenčné sieťové modely

Referenčné sieťové modely

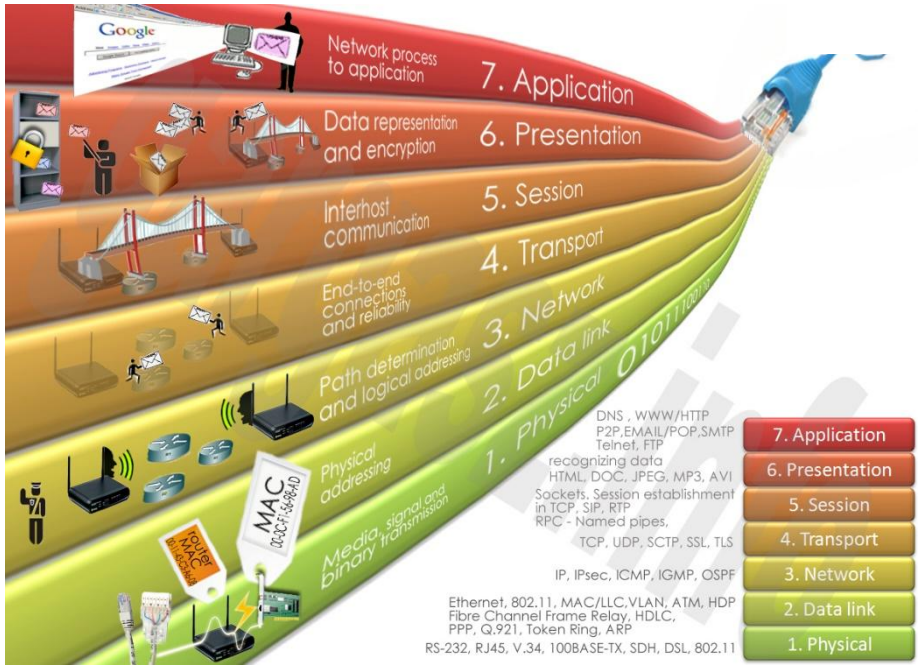
- **Vrstvové modely** sú v problematike komunikačných sietí veľmi obľúbenými pomôckami



- Modelovanie a návrh sietí podľa vrstvových modelov má podstatné výhody
  - **Zjednodušuje pohľad** na sieť a pochopenie jednotlivých dejov v nej
  - **Uľahčuje návrh** protokolov – protokoly sa totiž vytvárajú pre činnosť na konkrétnej vrstve, a teda majú jasne vymedzené kompetencie
  - Umožňuje **modulárny prístup** – zmena v jednej vrstve sa nedotýka iných vrstiev, kým zostanú dodržané rozhrania medzi nimi
  - Poskytuje **spoločný pojmový aparát** na popis sietí
- Ak sa istý vrstvový model stane istým vzorovým prototypom, nazývame ho **referenčný model**
- V našich sieťach je najobľúbenejším referenčným modelom **Open Systems Interconnection** (ISO **OSI model**)

Referenčný sieťový model OSI

- Pochádza od organizácie ISO
  - International Standards Organization
  - Správne: International Organization for Standardization
  - V preklade: Medzinárodná organizácia pre normalizáciu

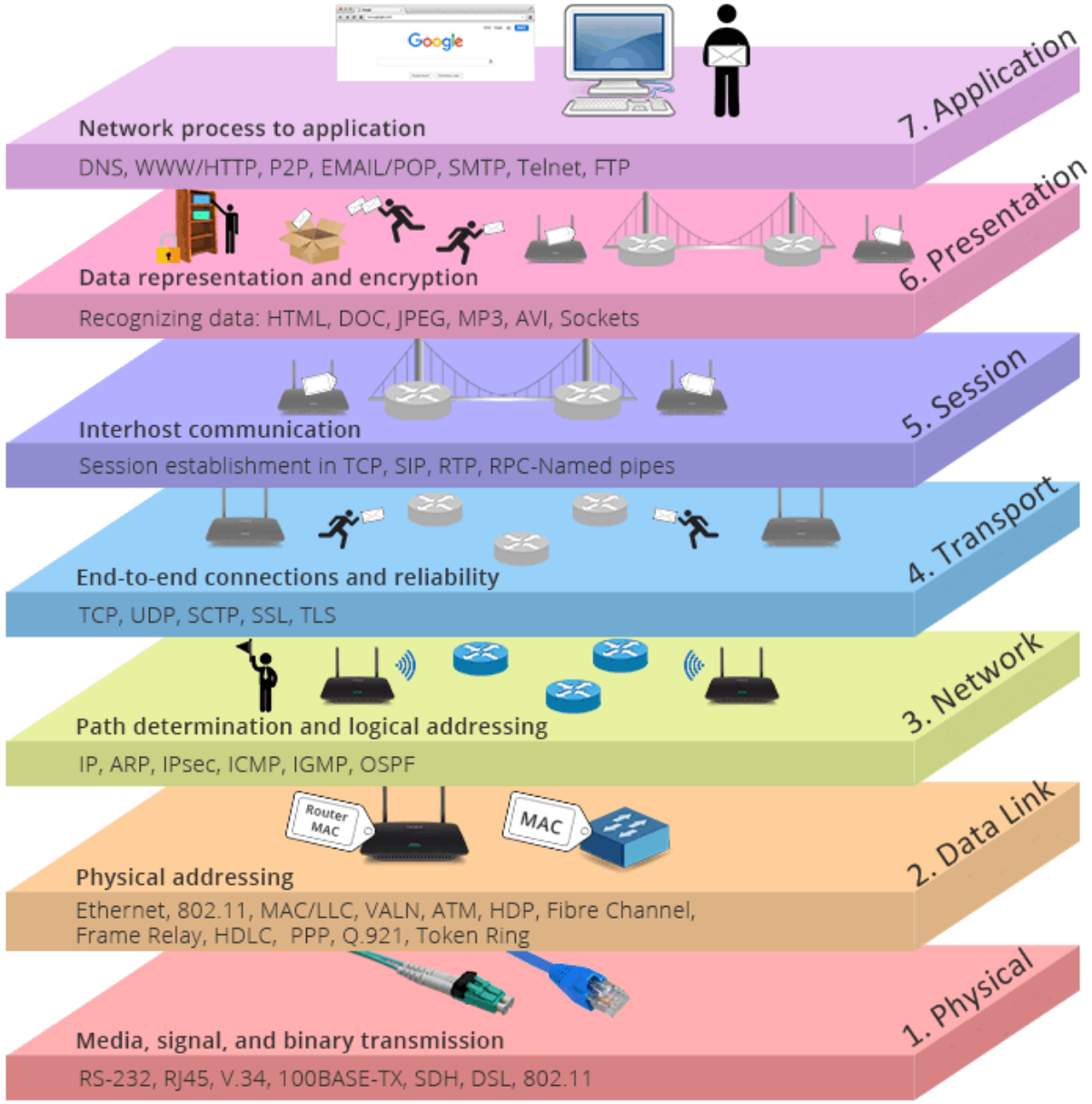


- Členovia ISO sú národné normalizačné inštitúcie
  - Za SR: UNMS = Úrad pre normalizáciu, metrológiu a skúšobníctvo
- RM ISO/OSI reagoval na vznik proprietárnych sieťových architektúr
  - Ako je SNA (Systems Networs Architecture od IMB)
  - Alebo DECNET (od firmy DEC/Digital)
- RM ISO/OSI mal byť oficiálnym riešením
  - Riešením, ktoré presadzovali „orgány štátu“ a chceli ho nasadiť do praxe
    - keď budovali siete pre potreby verejnej správy
  - Bol „megalománskym“ riešením, vznikajúcim od zeleného stola
    - chcel byť maximalistický, vedieť všetko, ale nakoniec sa v praxi nedal použiť
  - Dnes je RM ISO/OSI pre prax odpísaný, prehral v súboji s TCP/IP
    - dostupné sieťové technológie sú založené predovšetkým na TCP/IP

Referenčný sieťový model OSI

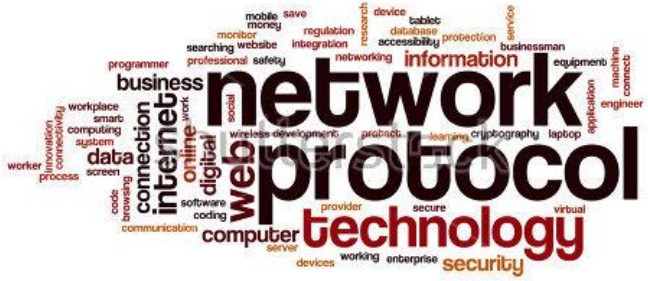
RM OSI pozostáva zo 7 vrstiev

- **Aplikačná vrstva**:
  - poskytuje nástroje pre tvorbu sieťových aplikácií a služieb
- **Prezentačná vrstva**:
  - zabezpečuje spoločný formát prenášaných aplikačných dát
- **Relačná vrstva**:
  - zabezpečí odovzdanie prenášaných dát konkrétnemu procesu (bežiacemu programu) na cieľovom počítači, riadi dialóg medzi procesmi
- **Transportná vrstva**:
  - prenáša dáta rozdelené na segmenty, u príjemcu ich usporadúva do pôvodného poradia, rieši opravu chýbajúcich segmentov
- **Sieťová vrstva**:
  - prenáša pakety (t.j. segment+hlavička sieťovej vrstvy) medzi **koncovými** uzlami
- **Linková vrstva**:
  - prenáša rámec (t.j. paket+hlavička a pätička linkovej vrstvy) medzi **susednými** uzlami, v pätičke sa nachádza kontrolný súčet pre detekciu prípadnej chyby pri prenose
- **Fyzická vrstva**:
  - prenáša informáciu vo forme bitov po danom médiu



Protokolový a referenčný model

- Pojmom **protokolový model** sa označuje model konkrétnej sady protokolov
  - Protokolový model nie je celkom to isté ako referenčný model
    - Protokolový model popisuje delenie protokolov vo vnútri istej protokolovej sady, ich funkcie, služby a kompetencie, nepopisuje však všetky deje v sieti. Je modelom protokolov, nie celej siete
    - Referenčný model popisuje deje v sieti, nepredpisuje však konkrétne protokoly ani služby. Je modelom všetkých procesov v sieti, nie však špecifických protokolov
- Najpoužívanejším protokolovým modelom je **TCP/IP**
  - TCP/IP vzniklo historicky skôr než ISO OSI
  - Predpokladalo sa, že TCP/IP je dočasné riešenie a keď ISO dokončí svoj OSI model a súvisiace protokoly, TCP/IP zanikne
  - Stal sa však pravý opak



Protokolové modely a priemyselné štandardy

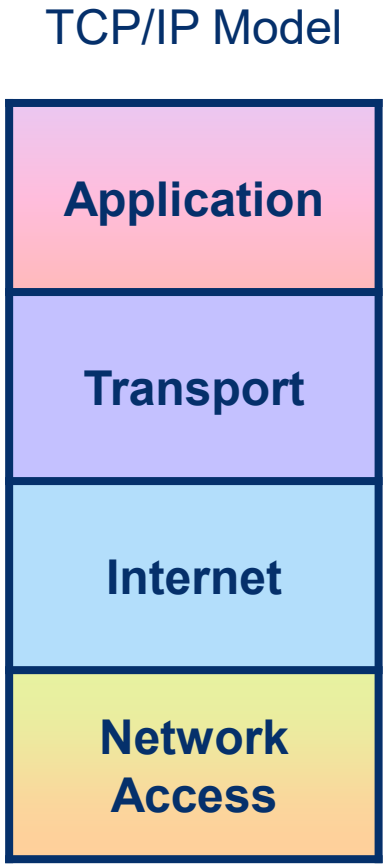
Proprietárne

Layer name	TCP/IP	ISO	Apple Talk	Novell Netware
Application	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
Transport	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
Internet	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Network Access	Ethernet PPP Frame Relay ATM WLAN			

- V tomto predmete iba TCP/IP
- Bežne sa stáva: proprietárny => otvorený
- Použitie štandardov pri vývoji a implementácii protokolov zabezpečí, aby produkty od rôznych výrobcov spolupracovali.

Protokolový model TCP/IP

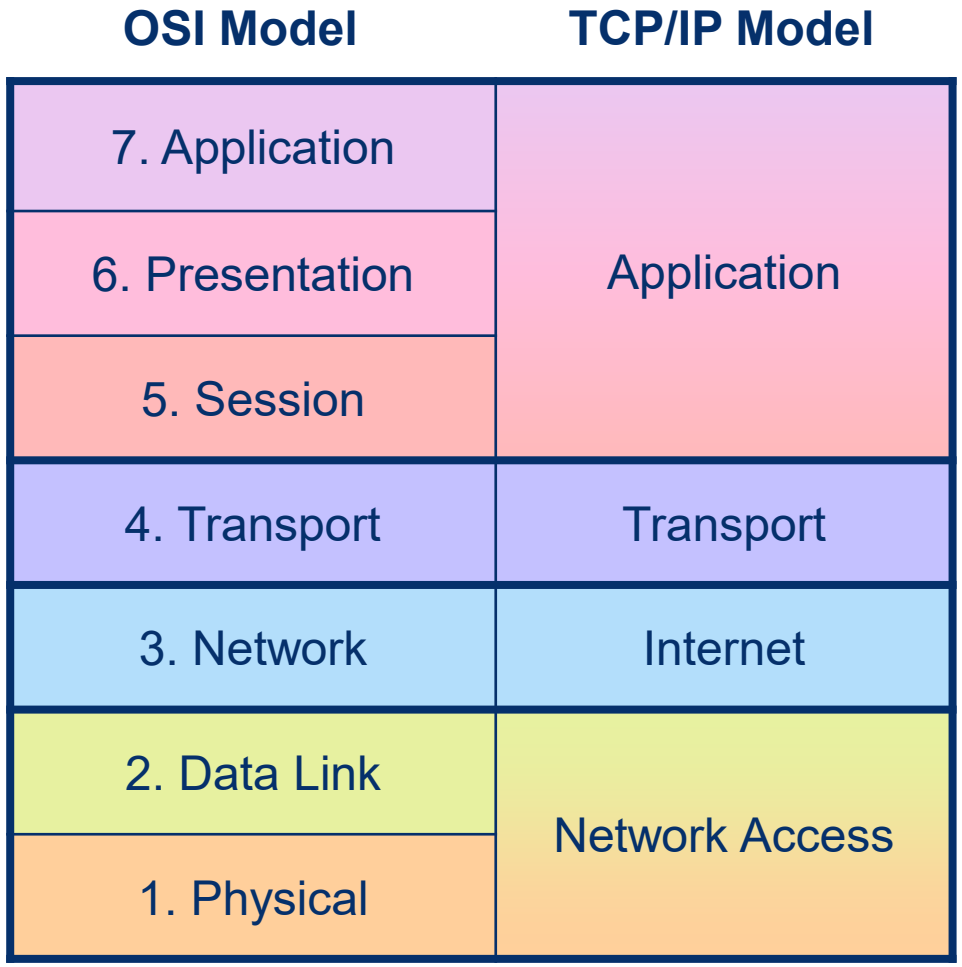
- TCP/IP model pozostáva zo 4 vrstiev
  - **Aplikačná vrstva**: poskytuje nástroje na tvorbu sieťových aplikácií a služieb vrátane identifikácie spoločného formátu prenášaných dát, kódovania a riadenie dialógov medzi komunikujúcimi procesmi
  - **Transportná vrstva**: prenáša dáta rozdelené na segmenty vrátane adresovania vhodnému procesu na cieľovom počítači, rieši otázky spoľahlivosti, spojovanosti a riadenia toku dát
  - **Internetová vrstva**: prenáša pakety medzi koncovými uzlami, určuje vhodnú cestu pre paket idúci sieťou
  - **Vrstva prístupu k sieti**: zabezpečuje funkcie spojené s prenosom rámcov k susedným staniciam po danom médiu, kontroluje hardvérové zariadenia a prenosové médium



TCP/IP protokolová sada

Application Layer	**Name System** DNS	**Host Config** BOOTP DHCP	**Email** SMTP POP IMAP	**File Transfer** FTP TFTP	**Web** HTTP
Transport Layer	UDP		TCP		
Internet Layer	IP NAT	**IP Support** ICMP	**Routing Protocols** OSPF	EIGRP	
Network Access Layer	ARP	PPP	Ethernet	Interface	Drivers

Vzťah ISO OSI a TCP/IP

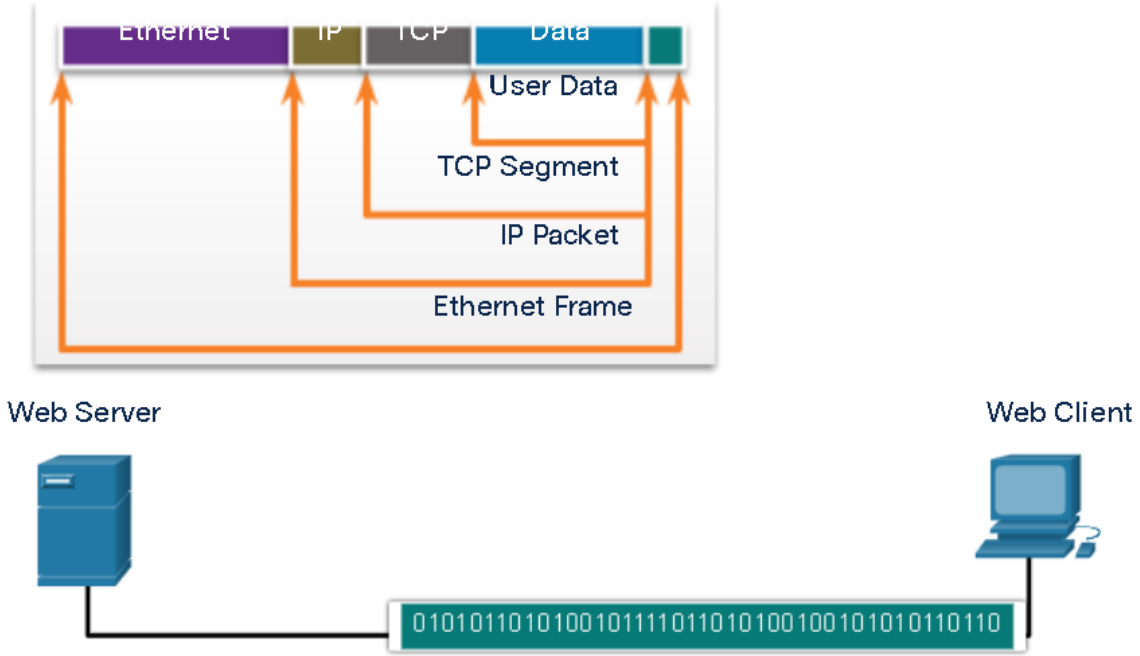


The key parallels are in the Transport and Network layers.

- Hoci OSI a TCP/IP nie je možné priamo porovnať, predsa je medzi nimi možné znázorniť aspoň kľúčové paralely

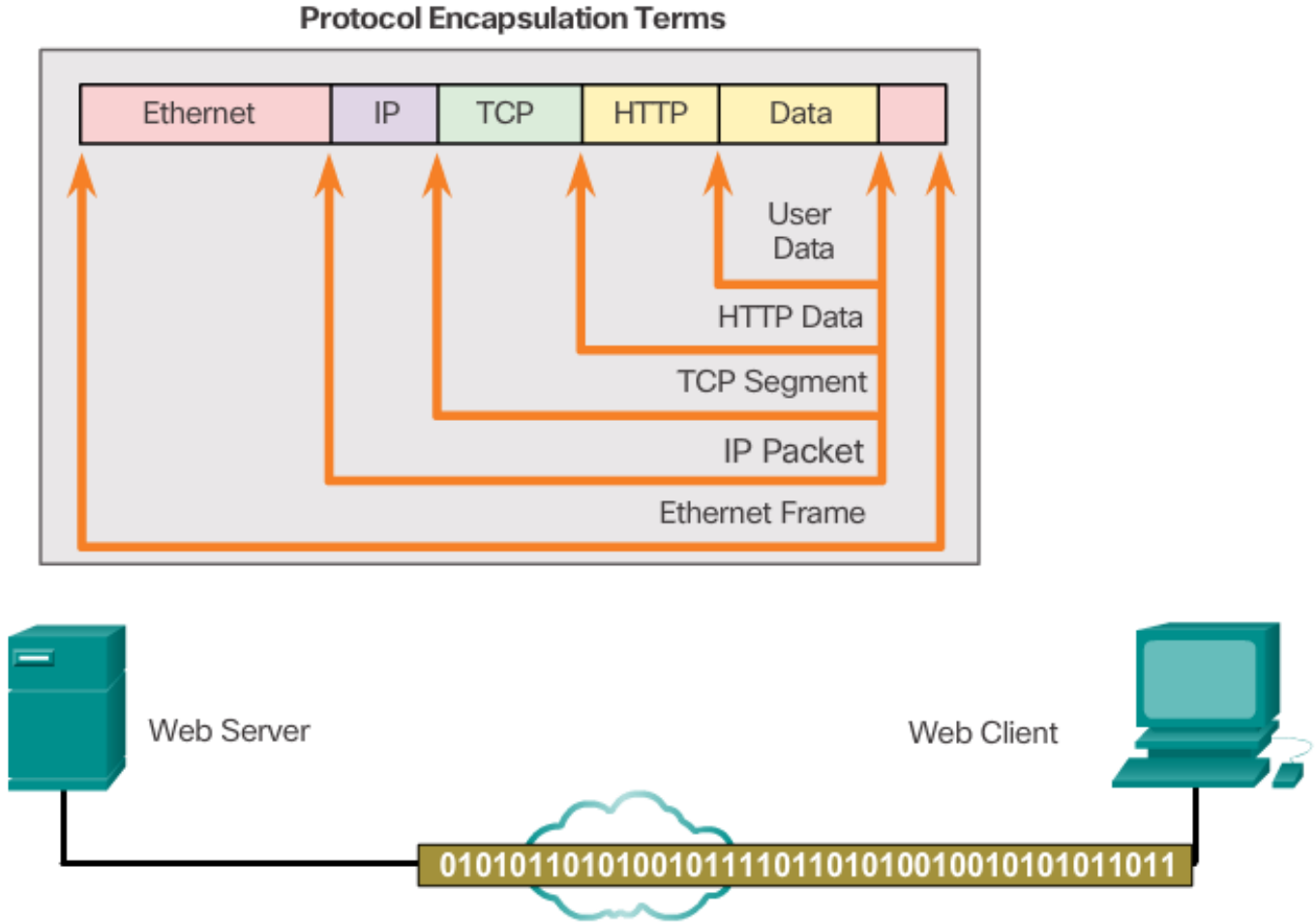
Enkapsulácia a dekapsulácia vo vrstvách

- Proces pridávania riadiacich hlavičiek na jednotlivých vrstvách sa nazýva **enkapsulácia**
  - Protocol Data Unit – PDU – je datagram danej vrstvy, ktorý vznikne enkapsuláciou správy prijatej z vyššej vrstvy
- Spätný proces analyzovania a odstraňovania hlavičiek na jednotlivých vrstvách sa nazýva **dekapsulácia** (**de-enkapsulácia**)
- Enkapsuláciu vykonáva odosielateľ
- Dekapsuláciu vykonáva príjemca
- Čiastočnú enkapsuláciu a dekapsuláciu môžu vykonávať všetky medziľahlé zariadenia



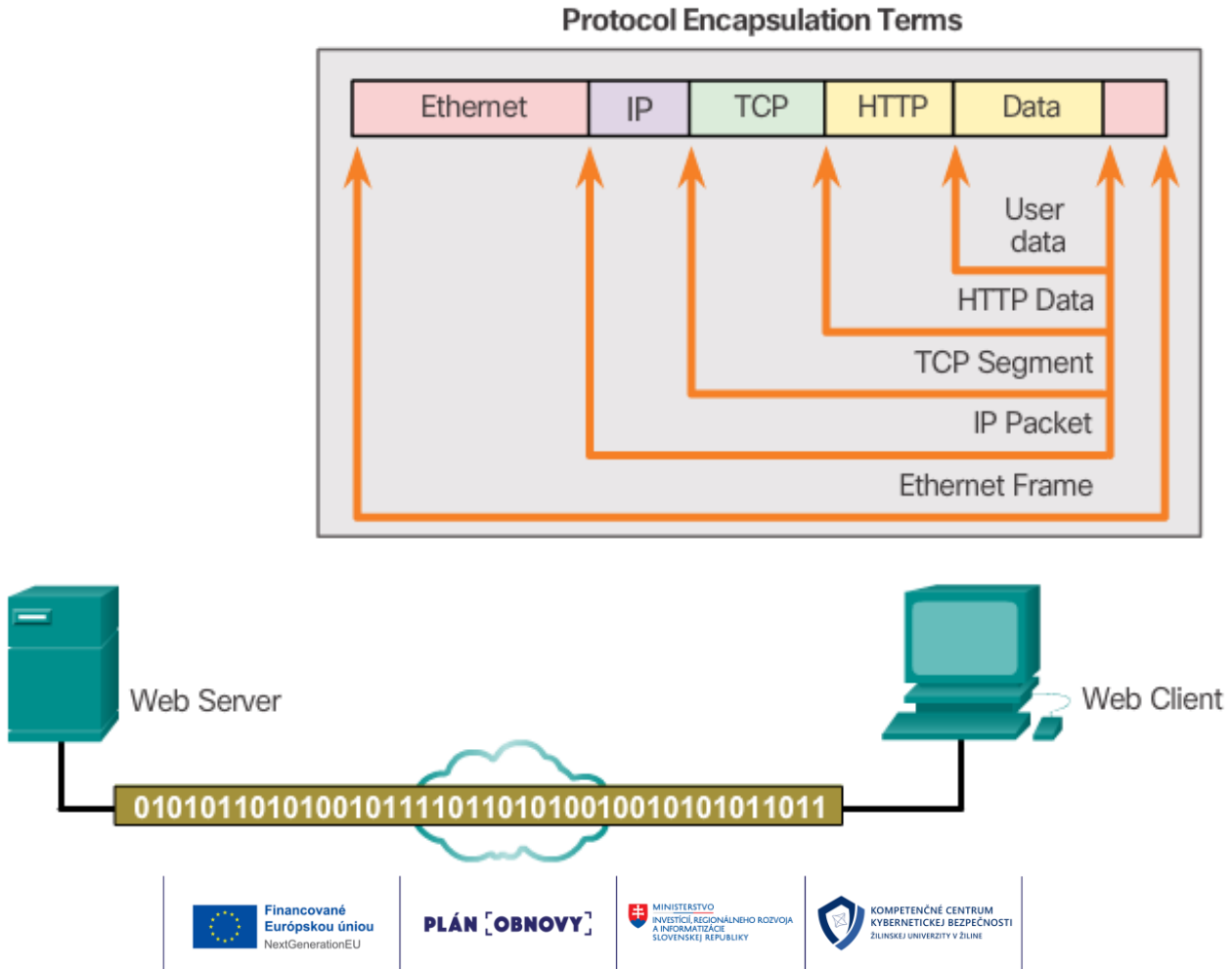
Enkapsulácia a dekapsulácia vo vrstvách

TCP/IP komunikačný proces: **odoslanie** správy



Enkapsulácia a dekapsulácia vo vrstvách

TCP/IP komunikačný proces: **prijatie** správy



Vzťah ISO OSI a TCP/IP

OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application	HTTP, DNS, DHCP, FTP	Application
Presentation		
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	PPP, Frame Relay, Ethernet	Network Access
Physical		

Everything over IP
IP over everything

Prístupy autorov ISO OSI a TCP/IP

RM ISO/OSI

- Prístup autorov odtrhnutý od reality
  - **Nechceli preberať iné riešenia**

    Napr. Ethernet
  - **Chceli vymyslieť všetko sami**

    A to nestíhali, preto ich predbehol TCP/IP
- „Od zložitejšieho k jednoduchšiemu
  - Autori najprv vymysleli čo najkomplexnejšie riešenie a až potom premýšľali, či je to realizovateľné
  - Následne museli sledovať a hľadať implementovateľnú podmnožinu
  - „Od zložitejšieho k jednoduchšiemu
- Vychádzali z predstavy, že „potrebujú niekomu niečo predať“
  - preto: preferencia „bohatých“ služieb

    Spojované, spoľahlivé

    Podpora QoS

TCP/IP

- Prístup autorov veľmi realistický
  - **Ochota preberať „cudzie“ riešenia**

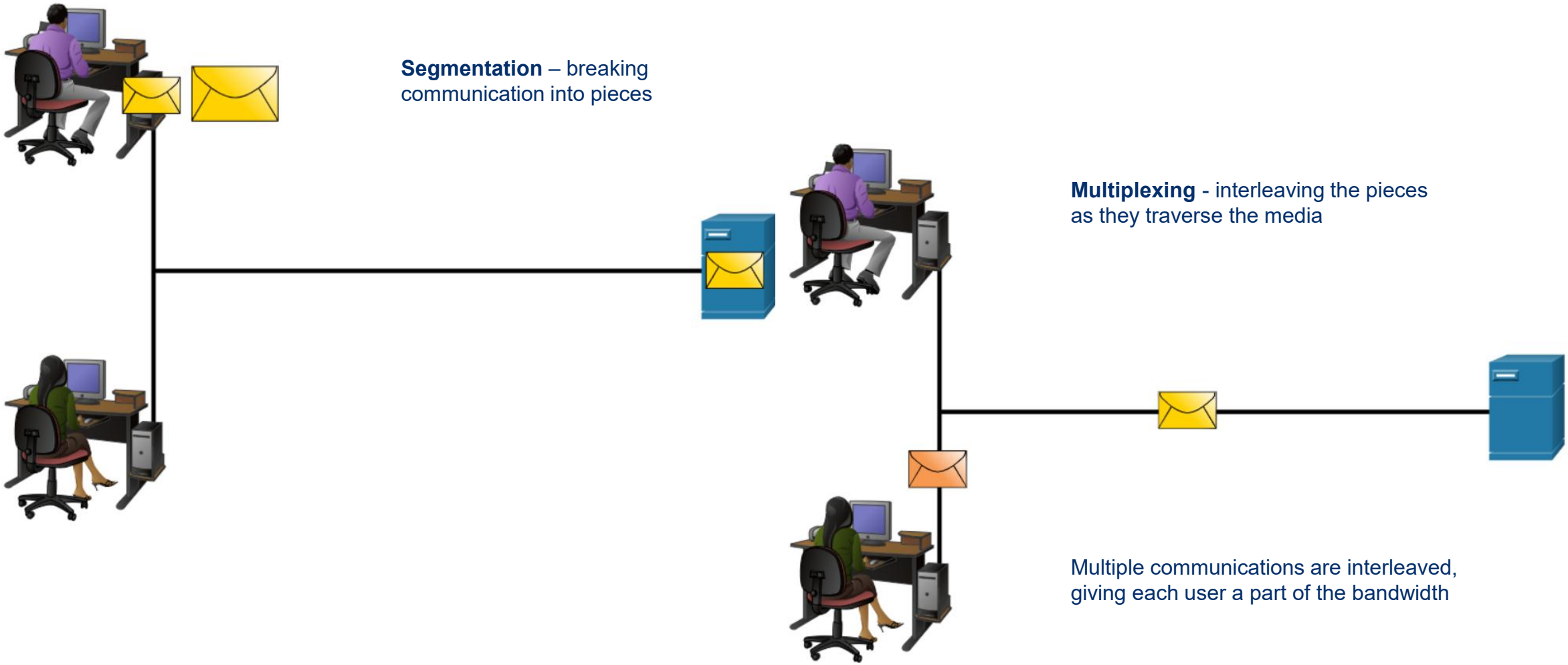
    Napr. Ethernet od IEEE
  - **Sústredili sa na to, ako „cudzie“ riešenie využiť čo najlepšie**

    napr. ako vkladať IP pakety do Ethernet rámcov
- „Od jednoduchšieho k zložitejšiemu
  - Najrpv sa navrhne jednoduché riešenie
    - Realizovateľnosť je podmienkou štandardizácie
  - Postupne sa rozširuje a zdokonaľuje
    - Ak je o to záujem
    - Ak je to reálne, použiteľné

V TCP/IP všetko opačne

Adresovanie na jednotlivých vrstvách

Segmentácia a multiplexovanie správ

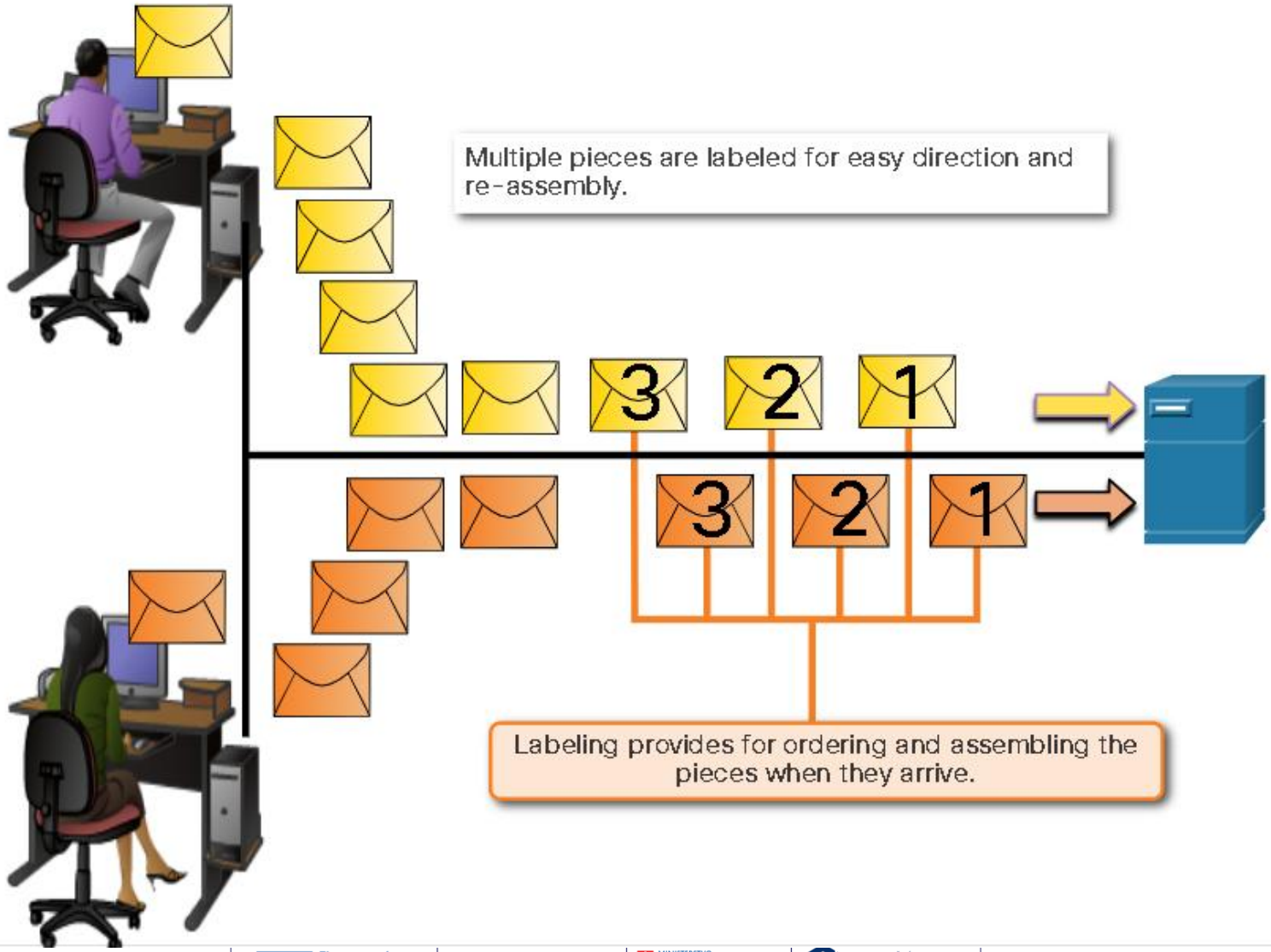


Segmentation – breaking communication into pieces

Multiplexing - interleaving the pieces as they traverse the media

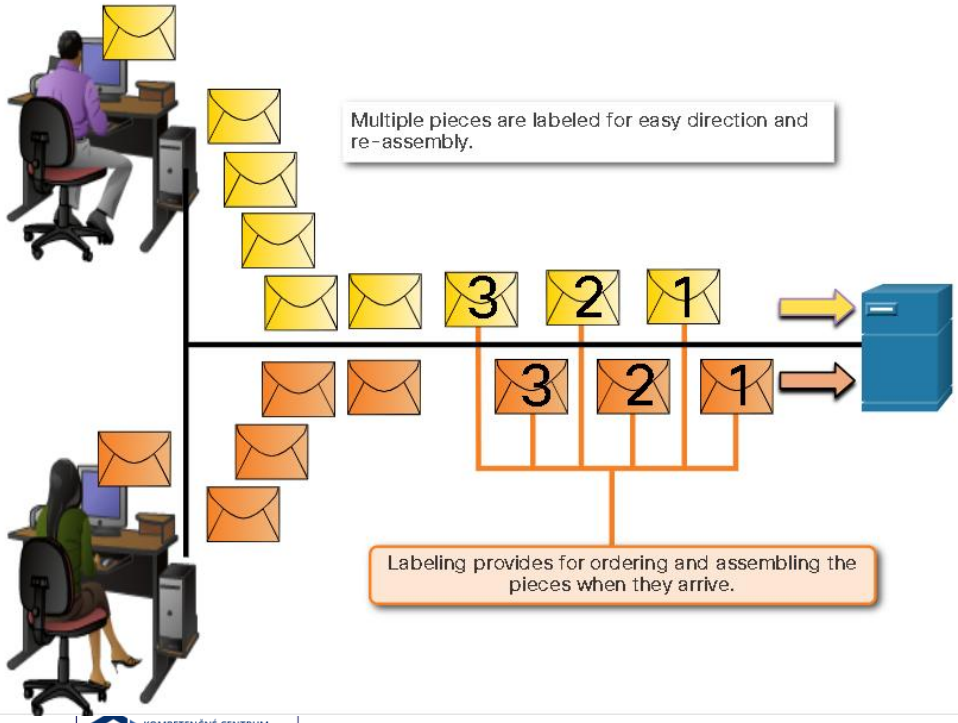
Multiple communications are interleaved, giving each user a part of the bandwidth

Multiplexovanie správ

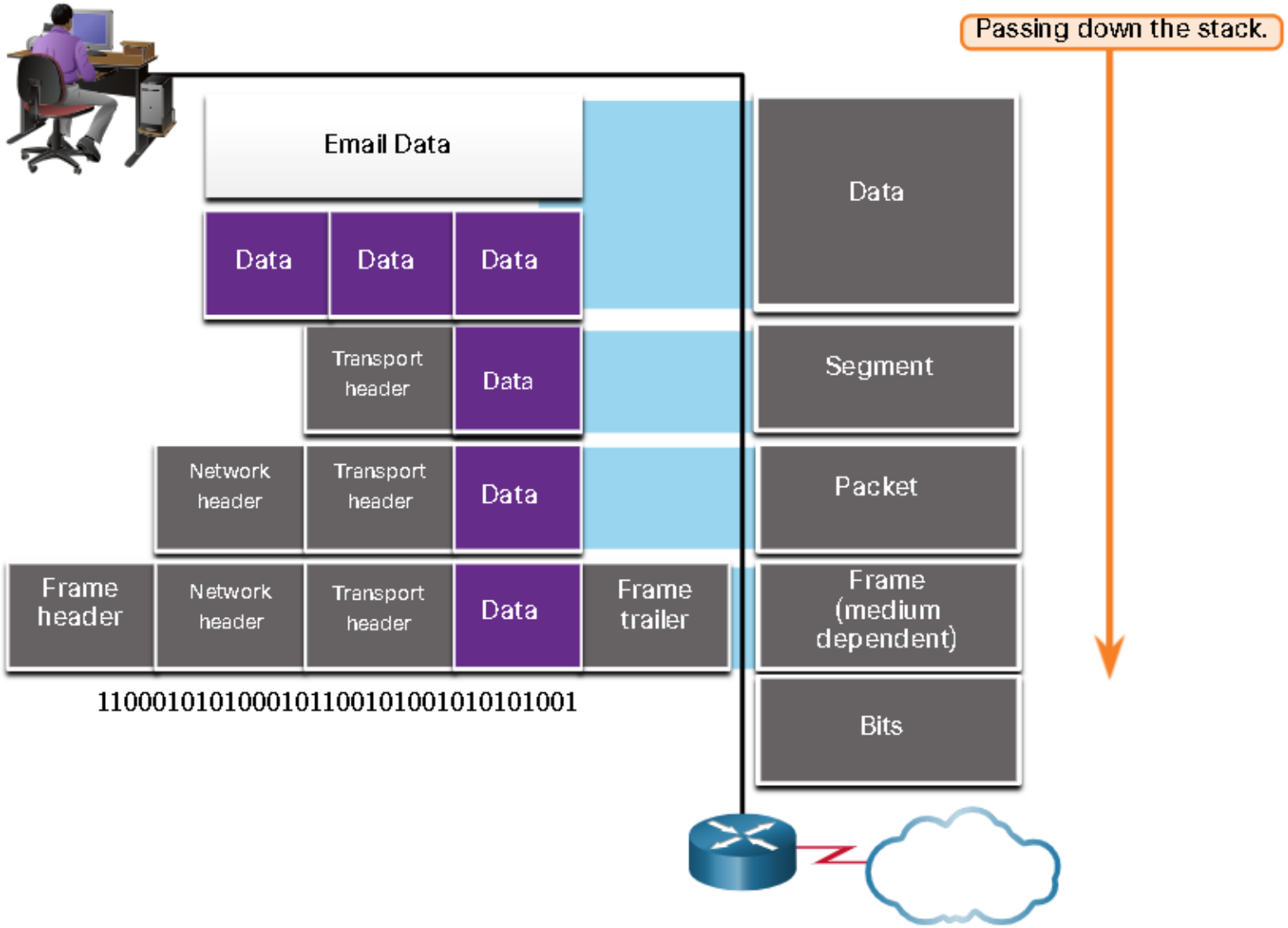


Prenos správ cez komunikačné siete

- V tzv. paketových sieťach, ktorými sa budeme zaoberať, sa prenášané dáta prenášajú po diskrétnych úsekoch
  - Tieto úseky sa všeobecne nazývajú datagramy a podľa ich typu ich neskôr budeme deliť na rámce, pakety a segmenty
  - Rozdelenie dát do datagramov nazývame **segmentácia**
- Tento princíp má svoje výhody
  - Datagramy sú doručované nezávisle na sebe
  - Na prenosovom médiu sa môžu rýchlo striedať mnohí odosielatelia a využívať ho spoločne – tzv. **multiplexovanie**
  - Ak sa datagram poškodí, stačí zopakovať jeho odoslanie, netreba opakovať odoslanie celej správy
- Aj nevýhody
  - Každý datagram musí niesť samostatnú informáciu o tom, kto ho odoslal, komu je adresovaný a ako má byť použitý. Túto informáciu treba pre každý datagram vytvoriť, spolu s ním preniesť a použiť ju

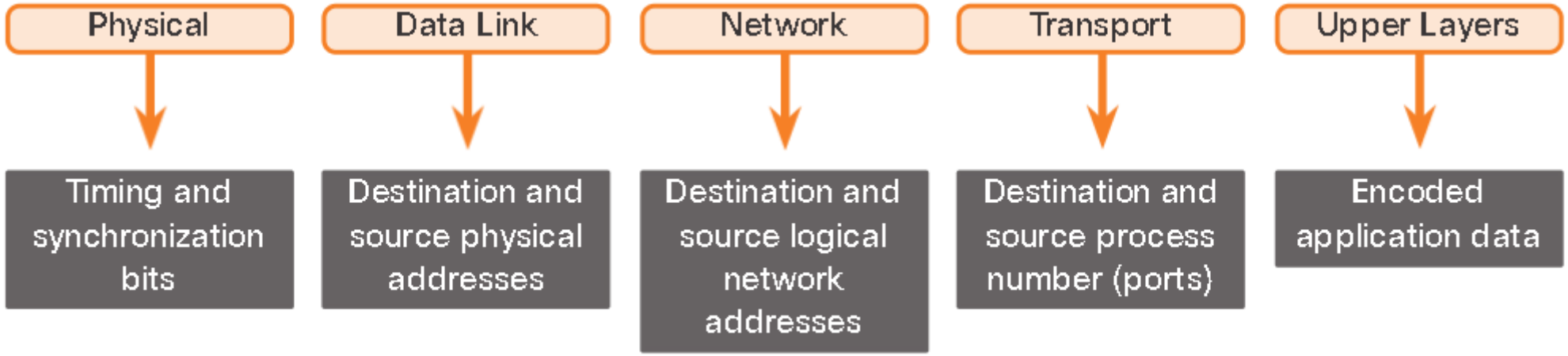


Prechod dát vrstvami TCP/IP



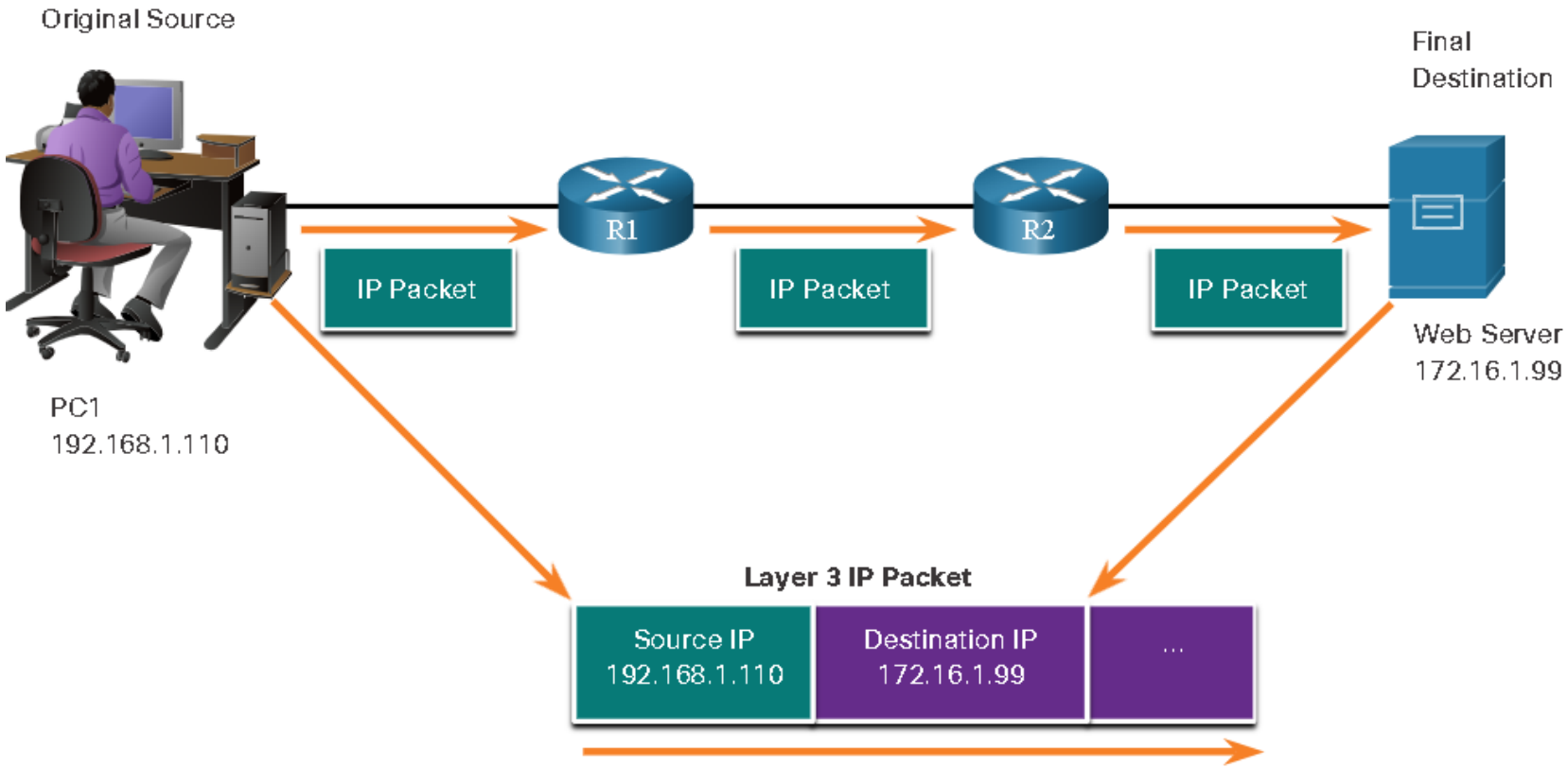
Adresovanie na vrstvách

- Jednotlivé vrstvy vo svojich hlavičkách uvádzajú aj adresové informácie
  - Jedná sa vždy o adresy podľa schopností konkrétnej vrstvy
  - Linková vrstva používa fyzické adresy susedných zariadení (napr. MAC adresy)
  - Sieťová vrstva používa logické adresy koncových alebo medziľahlých zariadení (napr. IP adresy)
  - Transportná vrstva používa adresy komunikujúcich procesov (napr. TCP alebo UDP porty)
- V jednom datagrame sa teda nachádza množstvo adries



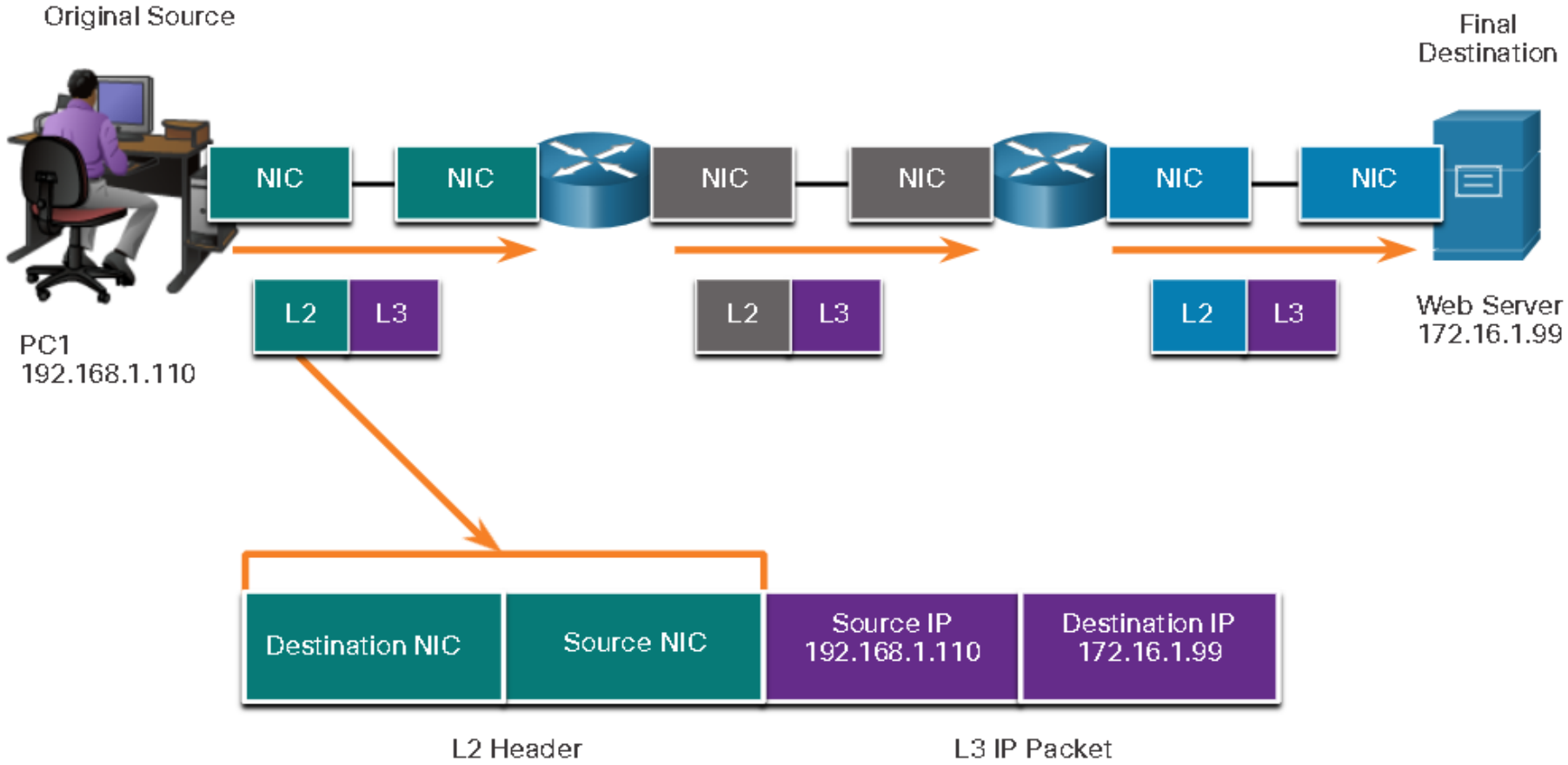
Logické adresy

- Layer 3 network addresses
- Adresy 192.168.1.110 a 192.16.1.99 v tomto obrázku nazývame IP adresy (sú nastavené správcom siete, nachádzajú sa v záhlaviach IP paketov)
- Zodpovedajú za doručenie IP paketu od zdroja k cieľu

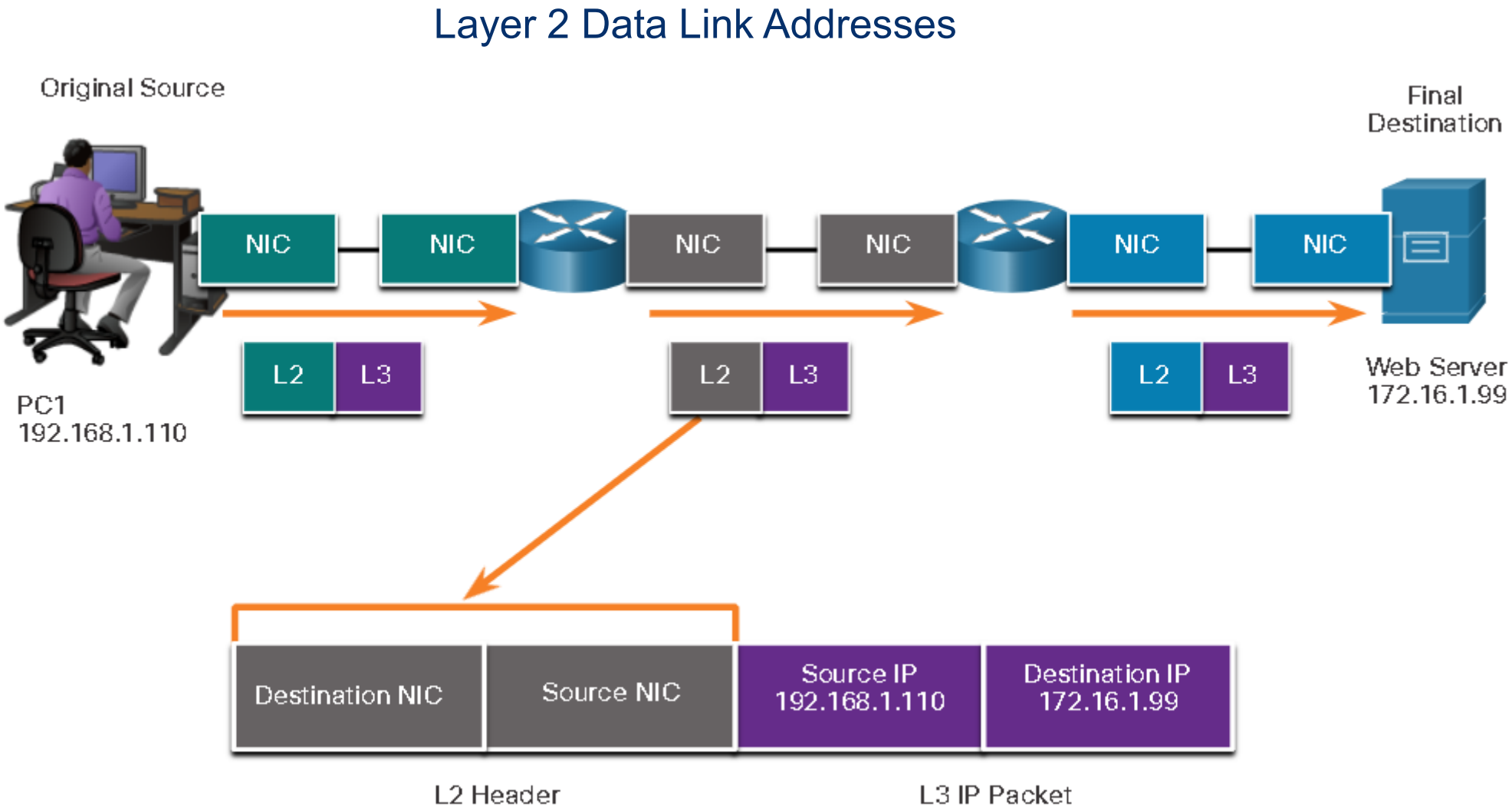


Fyzické adresy

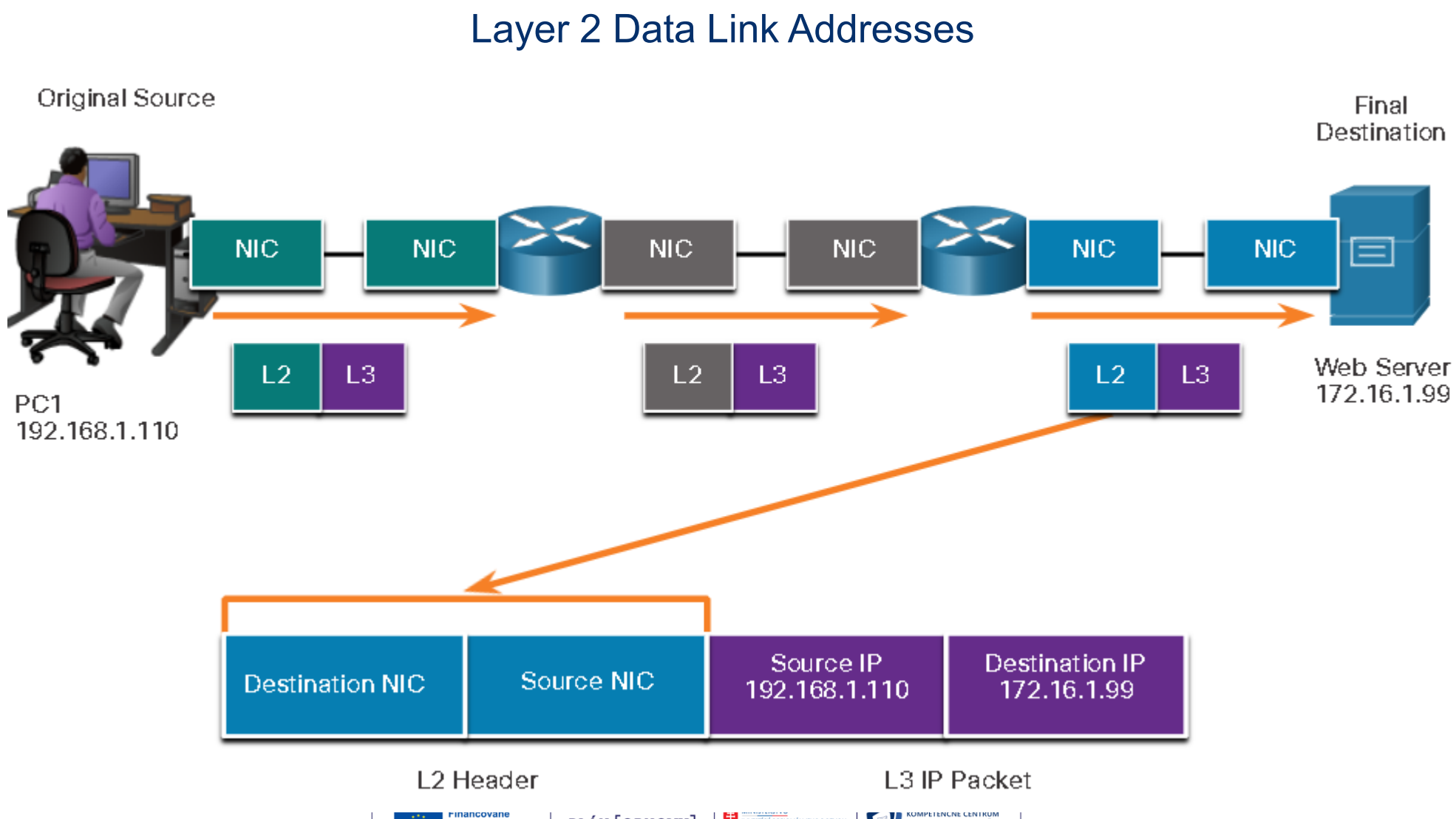
- Layer 2 Data Link Addresses
- Zodpovedné za doručenie linkových rámcov z jednej sieťovej karty k druhej sieťovej karte v spoločnej sieti



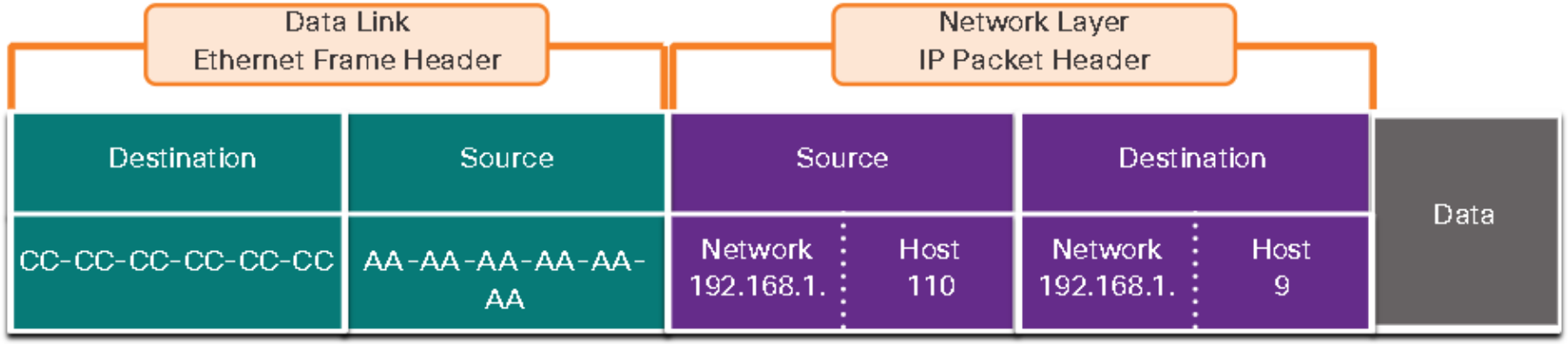
Fyzické adresy

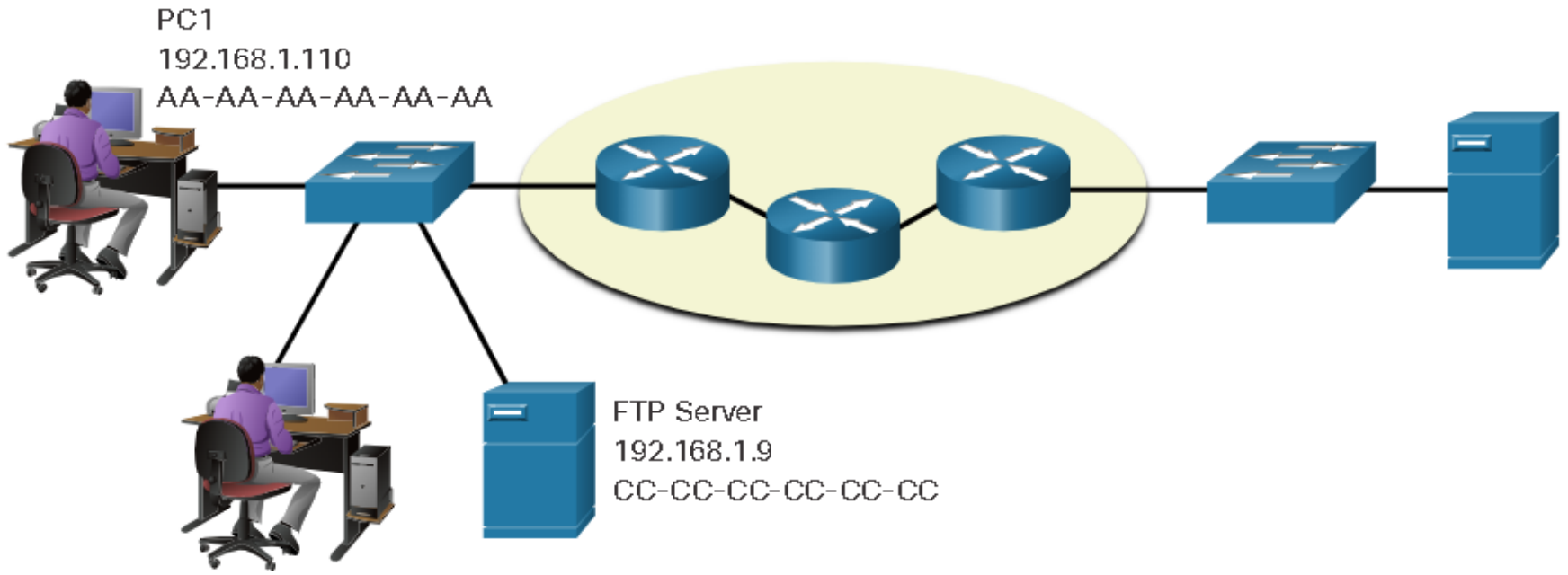


Fyzické adresy

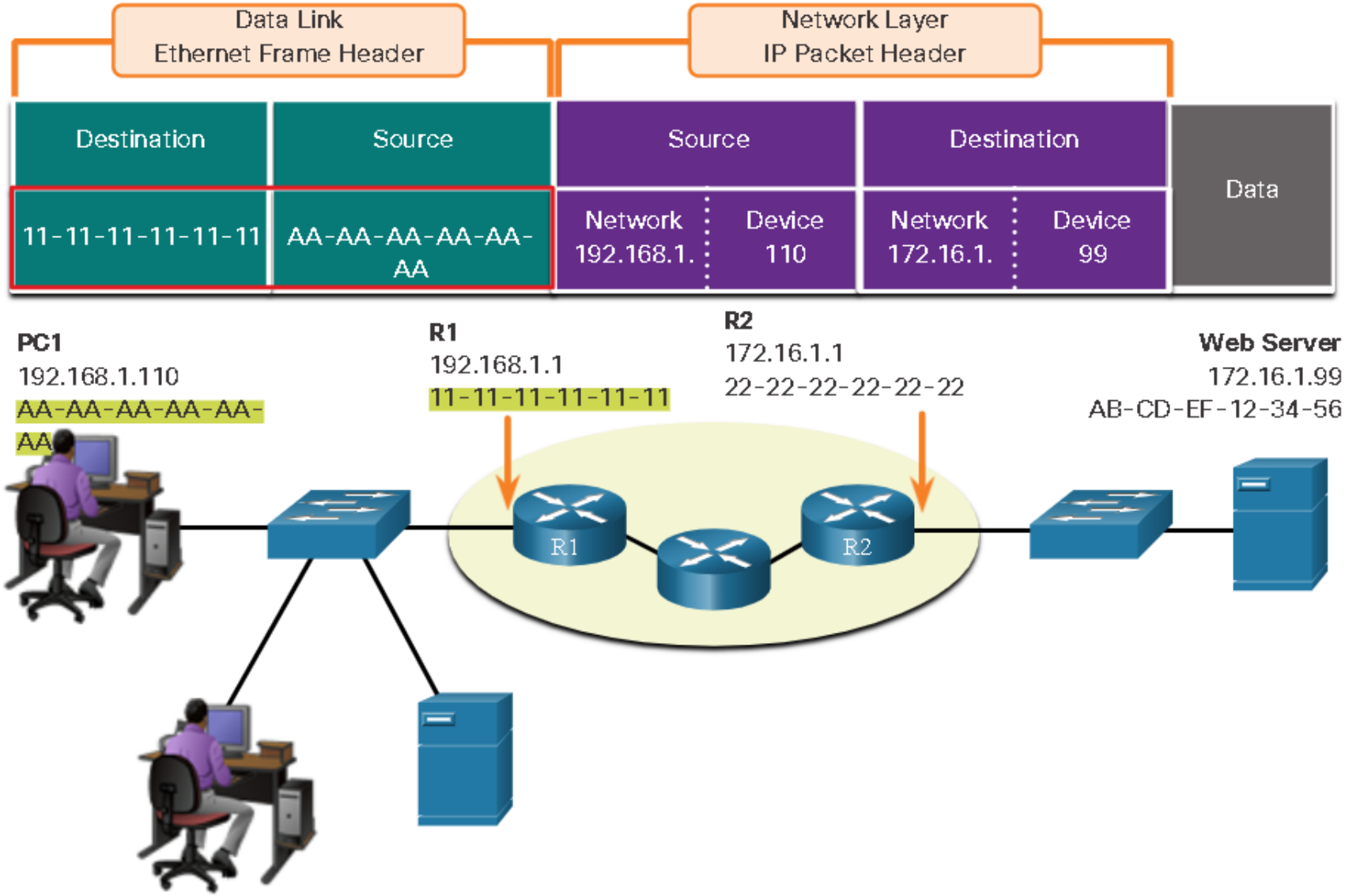


Priama komunikácia v spoločnej sieti

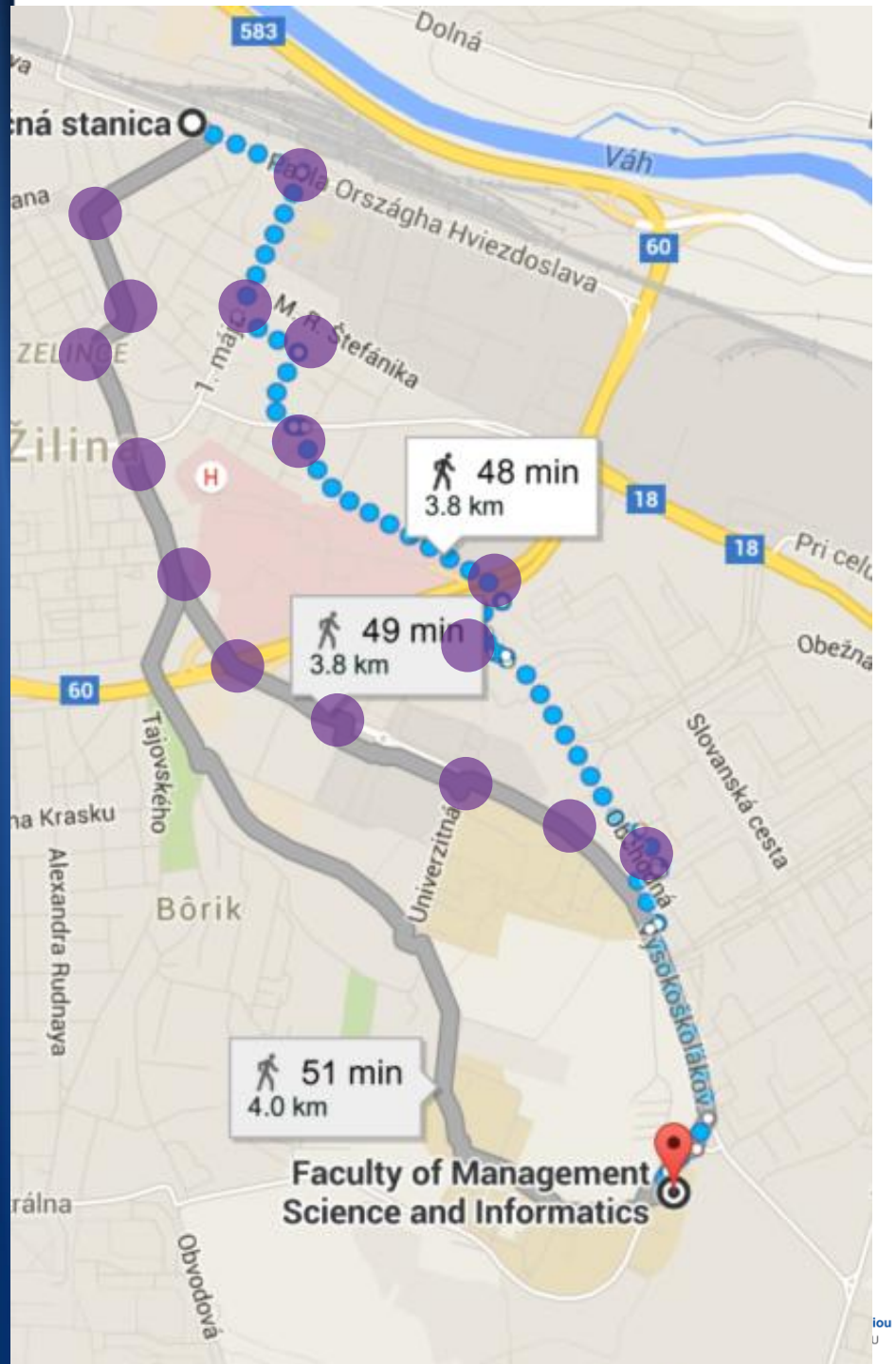




Vzdialená komunikácia prostredníctvom brány



Sieťová vrstva - Protokol IP



Smerovanie (je navigácia.. tadiaľto)

Cudzinec (španiel) z MT ide na deň otvorených dverí na FRI, príde vlakom a štartuje pešo zo ŽSR, nemá GPS, ani mapu:

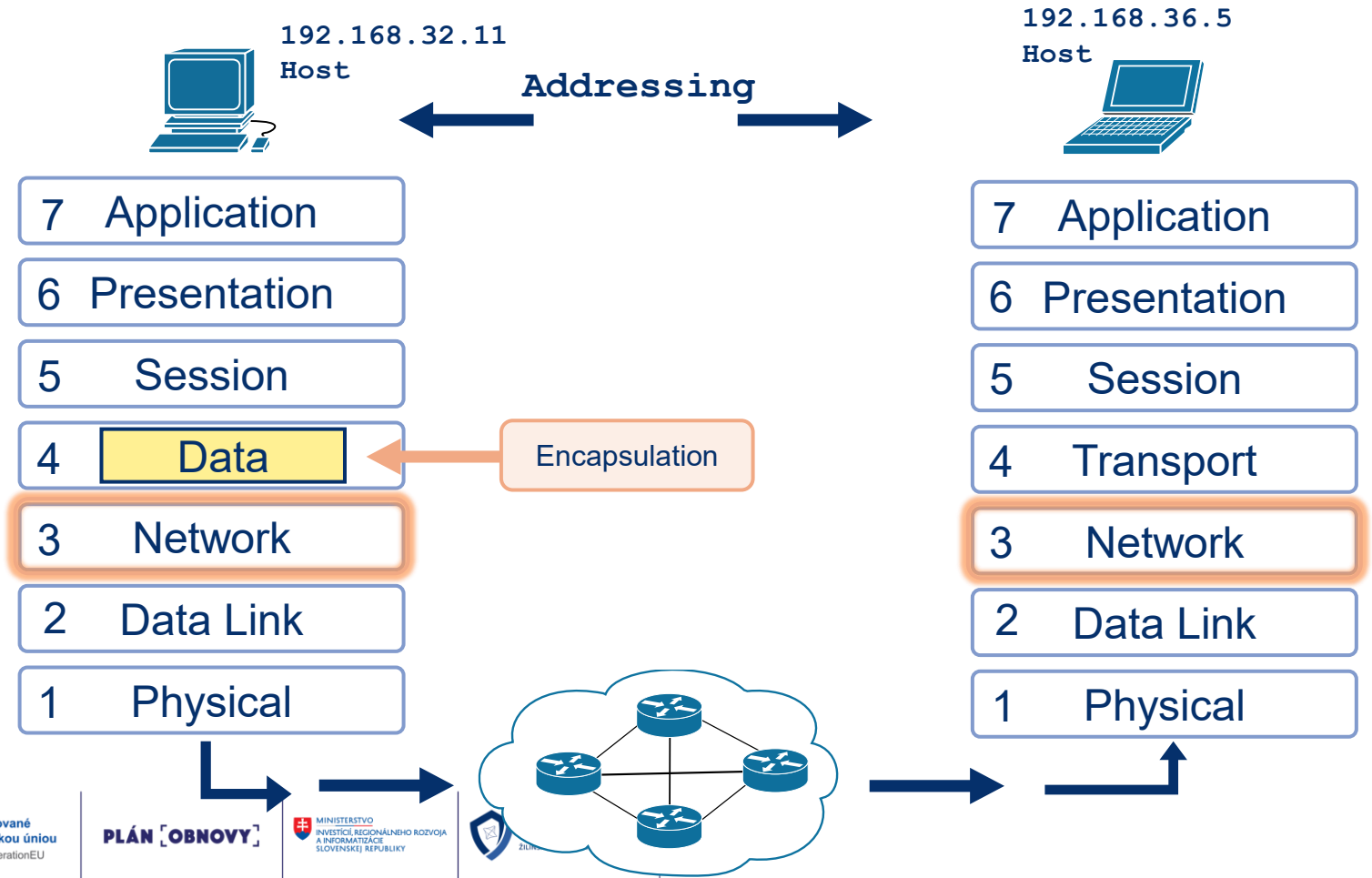
Domorodci, ktorých osloví, ho smerujú spôsobom:

„Choď rovno po tejto ulici (Masarička), a keď prídeš na križovatku (Hlinkovo námestie), zase sa niekoho opýtaj kadiaľ ísť.“

- zmenilo by sa niečo tým, keby mu niekto povedal na začiatku celú trasu?
- čo by sa stalo, keby na nejakej križovatke ten, ktorého žiada o ďalšie nasmerovanie, nevedel kde je FRI?
- čo by sa stalo, keby ho na nejakej križovatke niekto nasmeroval zle?
- je pri tomto spôsobe cestovania dôležité pri pýtaní sa na križovatkách uviesť danému domorodcovi, že odkiaľ vyštartoval? (že začal na ŽSR?) Prečo?
- naspäť sa rovnako pýta okoloidúcich na cestu. Má zaručené, že pôjde po tej istej trase z FRI na ŽSR, ako išiel ráno zo ŽSR na FRI? Prečo?

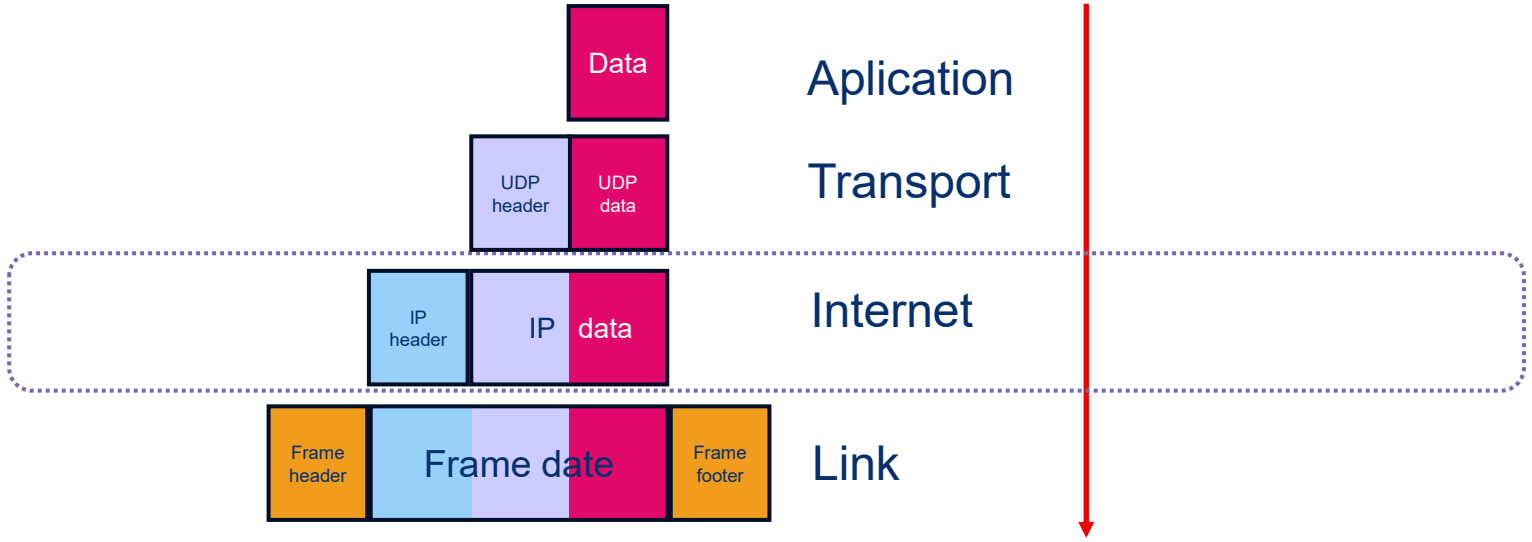
Úlohy sieťovej vrstvy

- Sieťová vrstva je zodpovedná za doručovanie dát medzi komunikujúcimi uzlami
  - End-to-end komunikácia – uzly sa môžu nachádzať kdekoľvek
- Úlohy, ktoré sieťová vrstva rieši:
  - Enkapsulácia (segmentu prilepí IP hlavičku)
  - Logické adresovanie sietí a staníc v nich
  - Hľadanie cesty do každej existujúcej cieľovej siete
  - Doručovanie dát vo forme paketov po najlepších cestách cieľovému uzlu (smerovanie)
  - De-enkapsulácia (spracuje sa info z IP hlavičky)



Zapúzdrenie na L3 = tvorba IP paketu

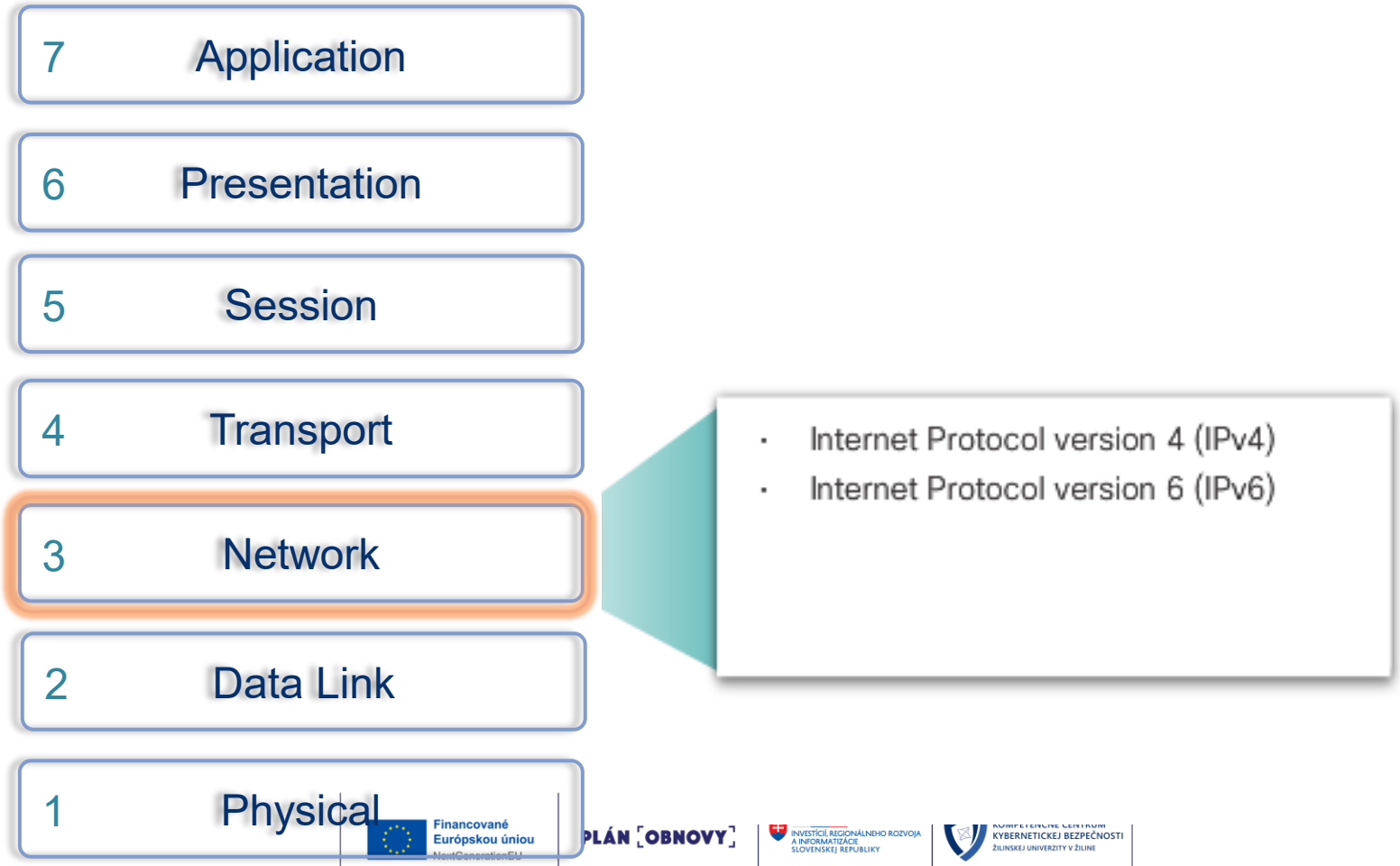
- Transportná vrstva (L4) **odosielajúcej** stanice segmentuje dáta aplikačnej vrstvy (L7) a pridáva každému segmentu hlavičku, aby prijímajúca stanica vedela znovu poskladať segmenty do správneho poradia a predať aplikačnej vrstve kompletné prenesené dáta



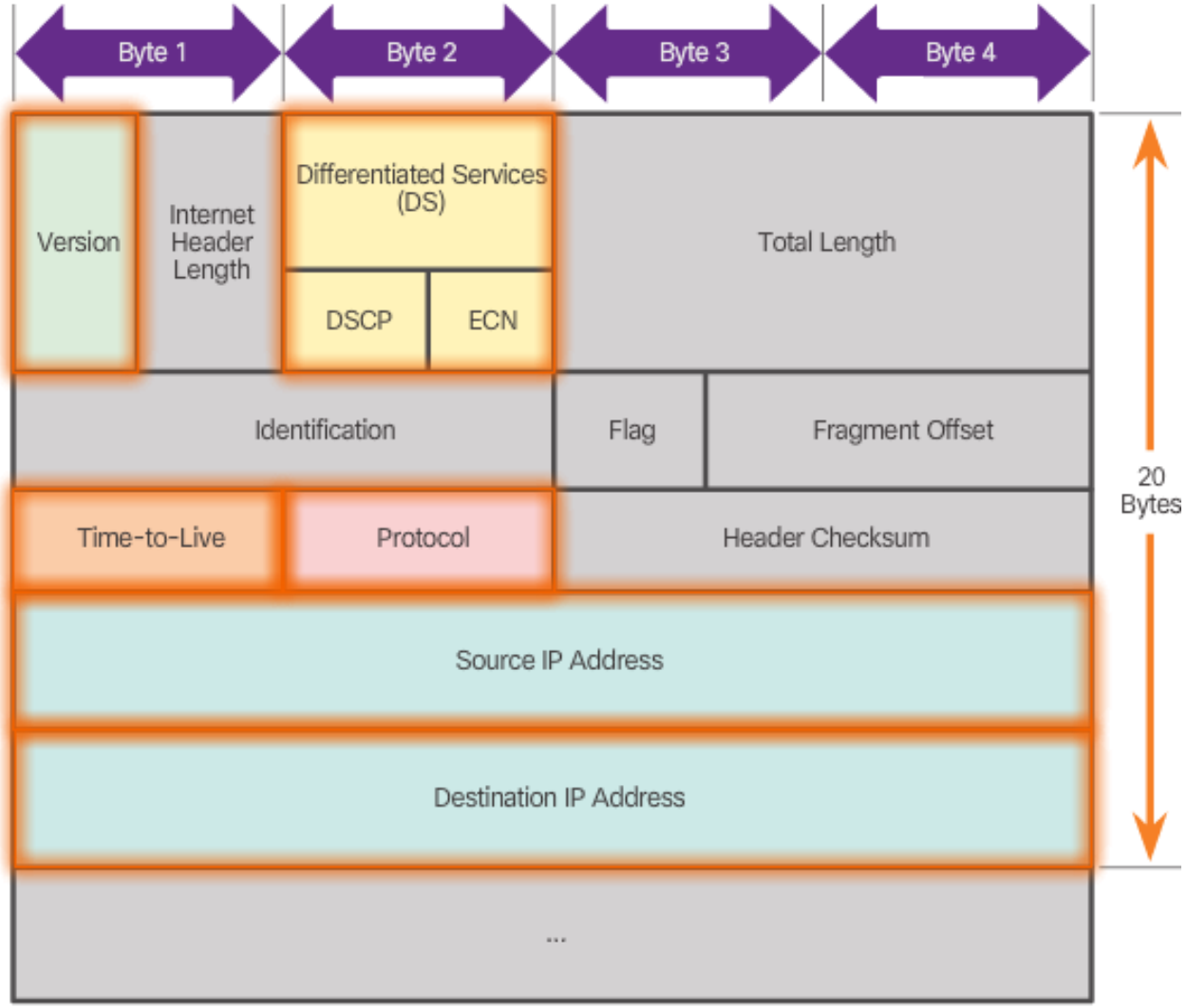
- Sieťová vrstva (L3) **odosielajúcej** stanice si prevezme segment pripravený vyššou vrstvou - transportnou (L4) a zapúzdri ho = pridá k nemu IP hlavičku (v tej musí dôkladne vyplniť potrebné polia, aby takýto paket mohol byt neskôr prenesený cez celú IP sieť až k príjemcovi), čím vznikne IP paket, ktorý ďalej predá protokolu linkovej vrstvy na spracovanie.

Úlohy sieťovej vrstvy

- Ktorý protokol je v súčasnosti v TCP/IP protokolom sieťovej vrstvy?
- V akých verziách sa dnes vyskytuje?

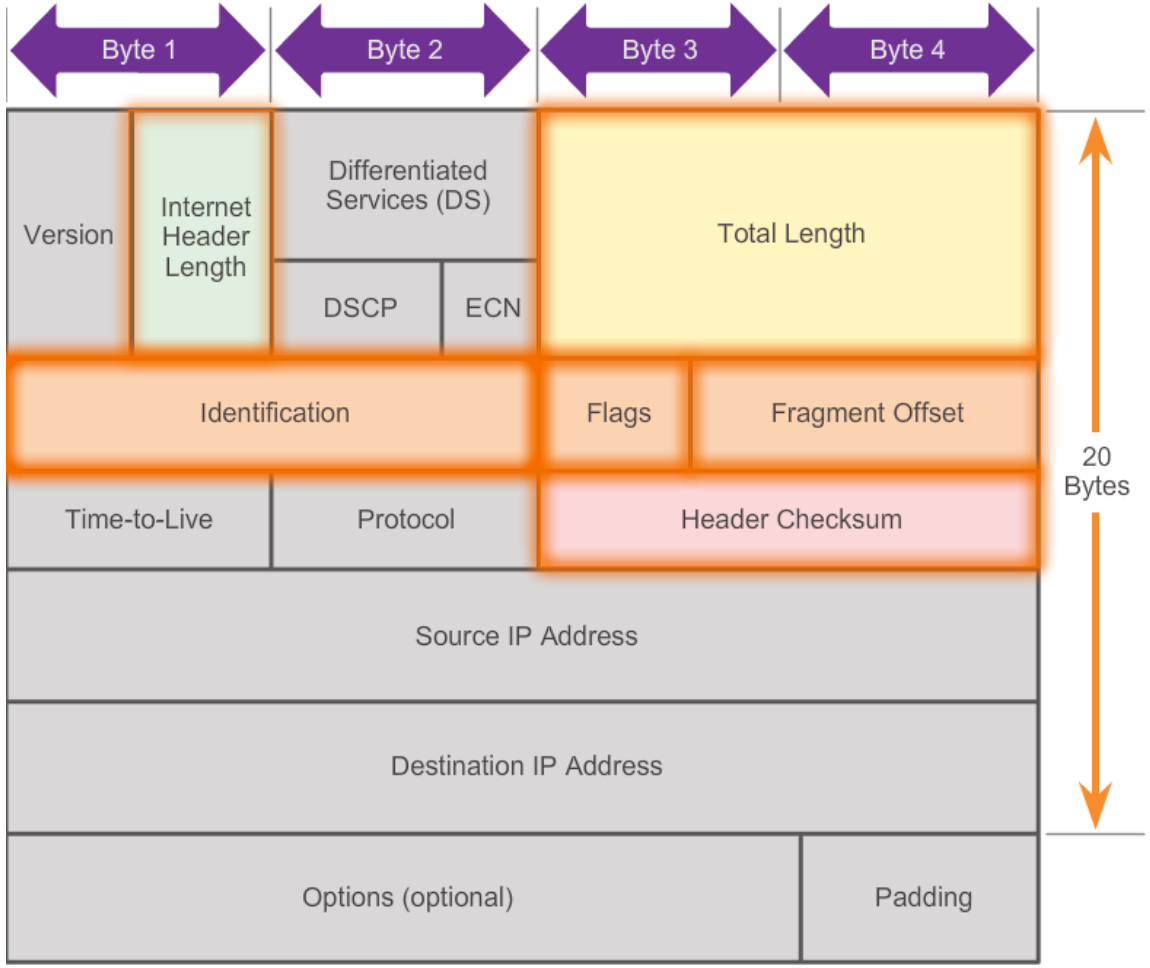


Formát hlavičky IPv4 paketu



- **Version** = 0100 (IPv4)
- **DS** = priorita paketu
- **TTL** = Životnosť paketu [počet preskokov], znižuje sa vždy o 1 pri prechode každým smerovačom
- **Protocol** = kód pre identifikáciu protokolu vyššej vrstvy, ktorý je zabalený v IP pakete (napr. TCP=6, UDP=17, ICMP=1)
- **Source IP Address** = kto je zdroj paketu
- **Destination IP Address** = kto je cieľ paketu

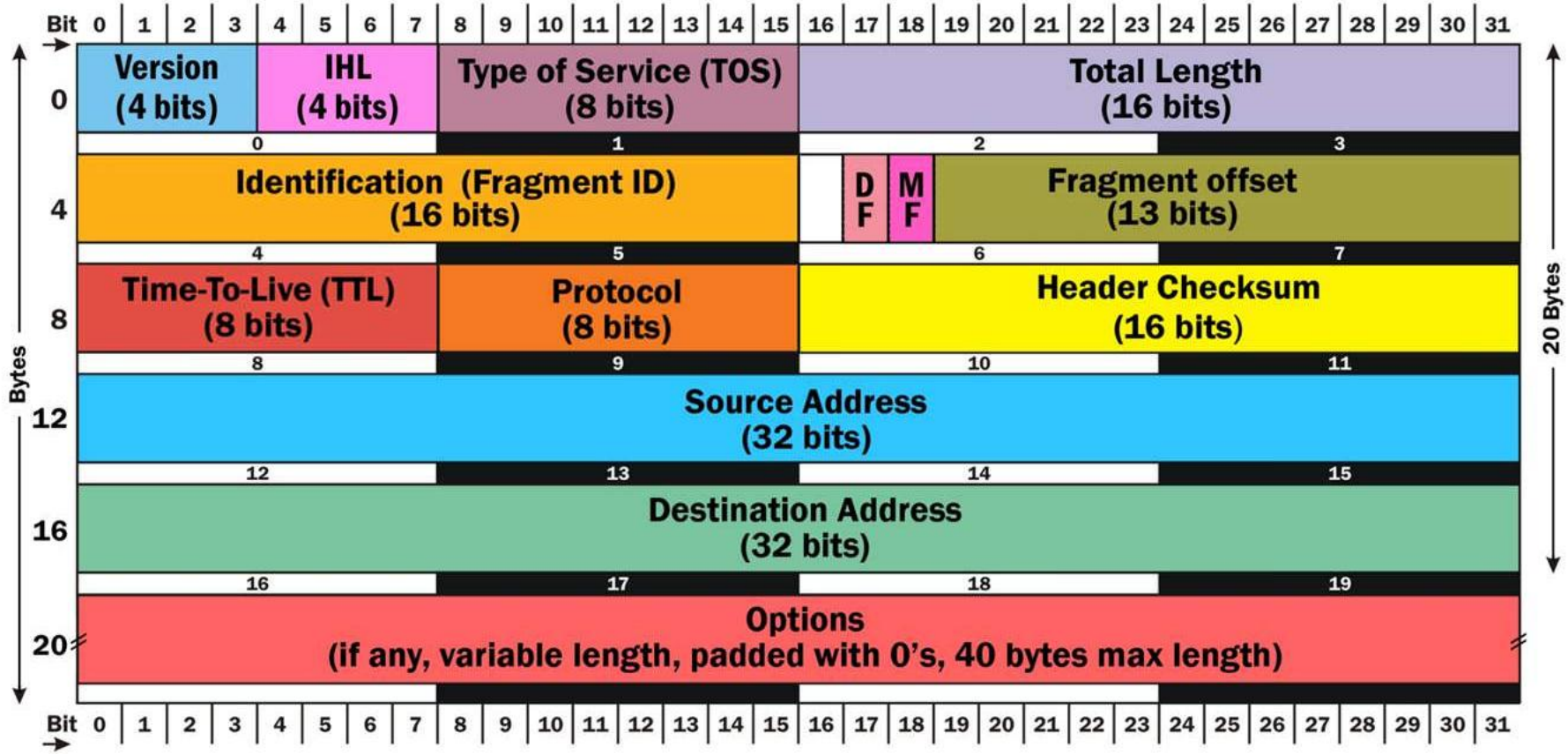
Formát hlavičky IPv4 paketu



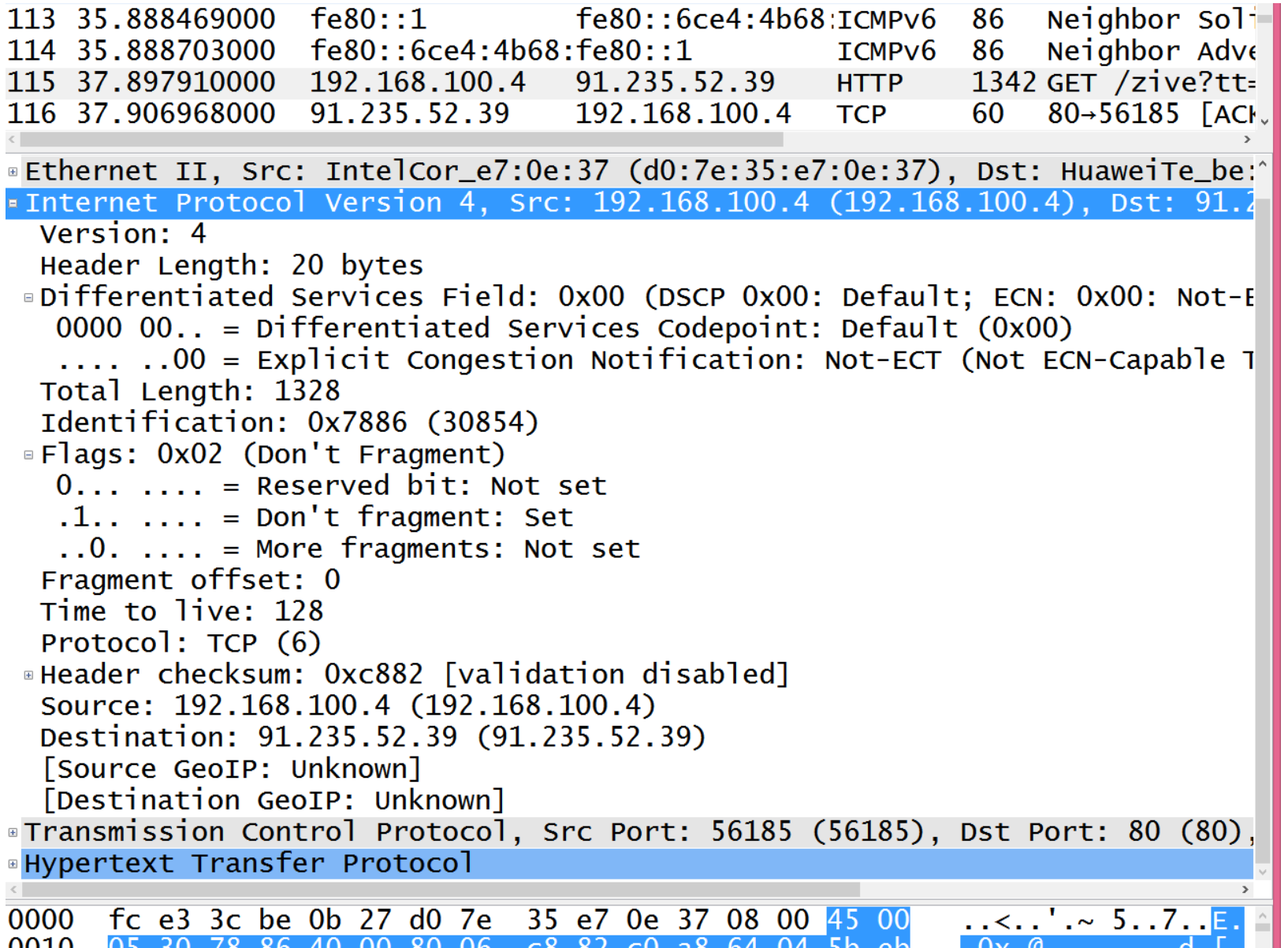
- **IHL** – nemusí mať vždy 20 B, máme totiž k dispozícii pole „Options“ = voliteľné položky
- **Total Length** – celková veľkoť IP paketu (hlavička/header + telo/payload)
- **Header Checksum** = detekcia chýb pri prenose
- **Identification** (identifikácia fragmentu, ak bol paket fragmentovaný (rozdelený na menšie kusy)
- **Flags**: **DF (dont fragment)** = 1, ak nechcem paket nechať fragmentovať , DF=0 ak mi je to jedno, **MF (more fragments)** = 1 ak tento fragment nie je posledný v rade, MF=0 ak je posledný
- **Fragment Offset** = pozícia na ktorú patrí daný fragment v pôvodnom pakete, FO=0 ak je to prvý fragment, udáva sa v násobkoch 8 bitov

Formát hlavičky IPv4 paketu
(aj s veľkosťami jednotlivých polí)

- Minimálna (štandardná) veľkosť IP hlavičky je 20 B (poradie bajtov 0 až 19):



IPv4 hlavička – Wireshark



Vyčerpanie IPv4 a nástup IPv6

Predikcia o počte potrebných IP adries do r. 2020:

- Cisco predikuje: 50 biliónov
- Intel predikuje: 200 biliónov

IPv4 (32 bitové pole)

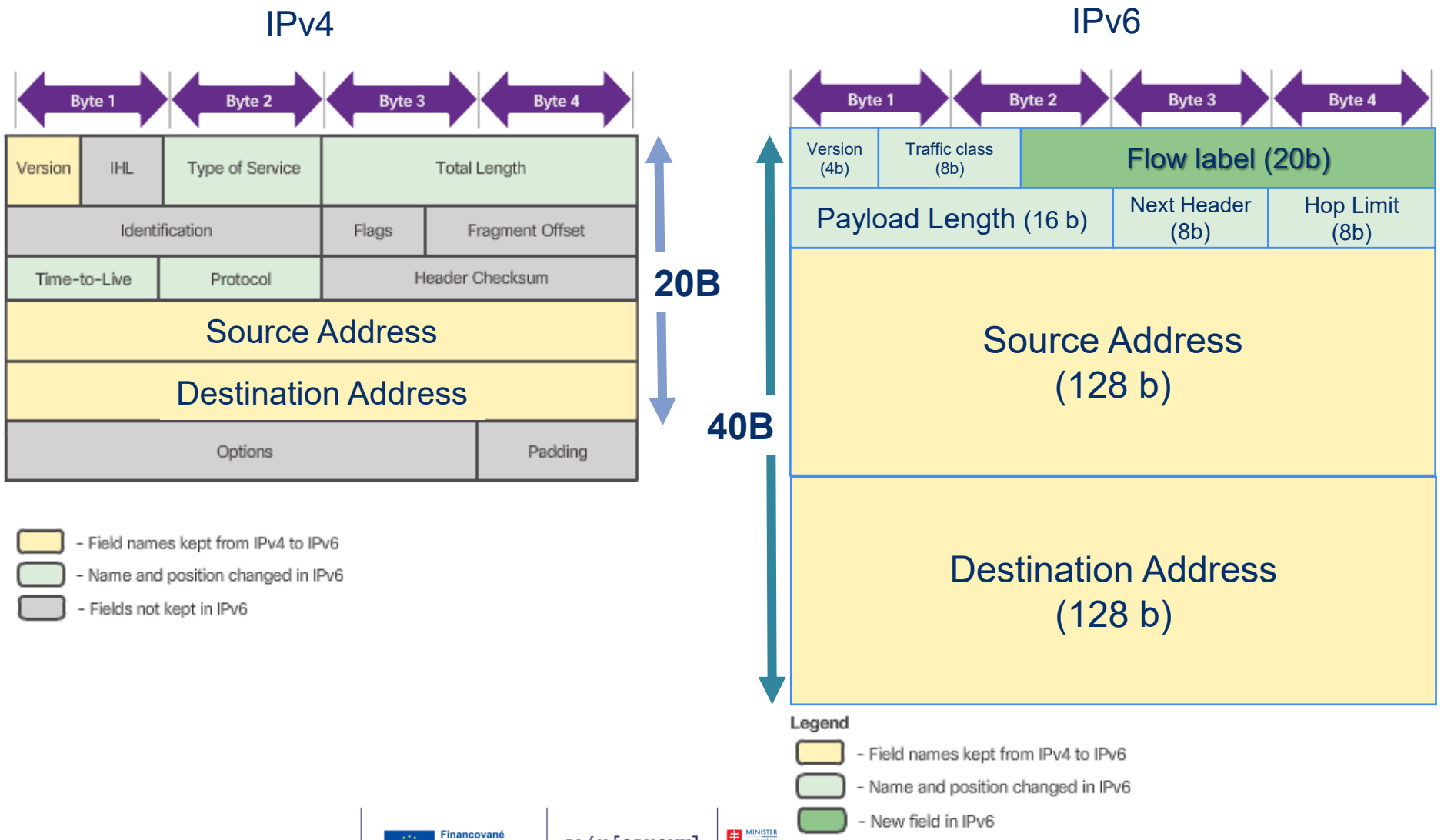
- 4 bilióny IPv4 adries 4,000,000,000
- Adresný priestor sa vyčerpal
- Narastanie smerovacej tabuľky
- Záchranou bolo NAT
  - Nie je použiteľné pre služby ktoré potrebujú end-to-end konektivitu s verejnými IP adresami

vs.

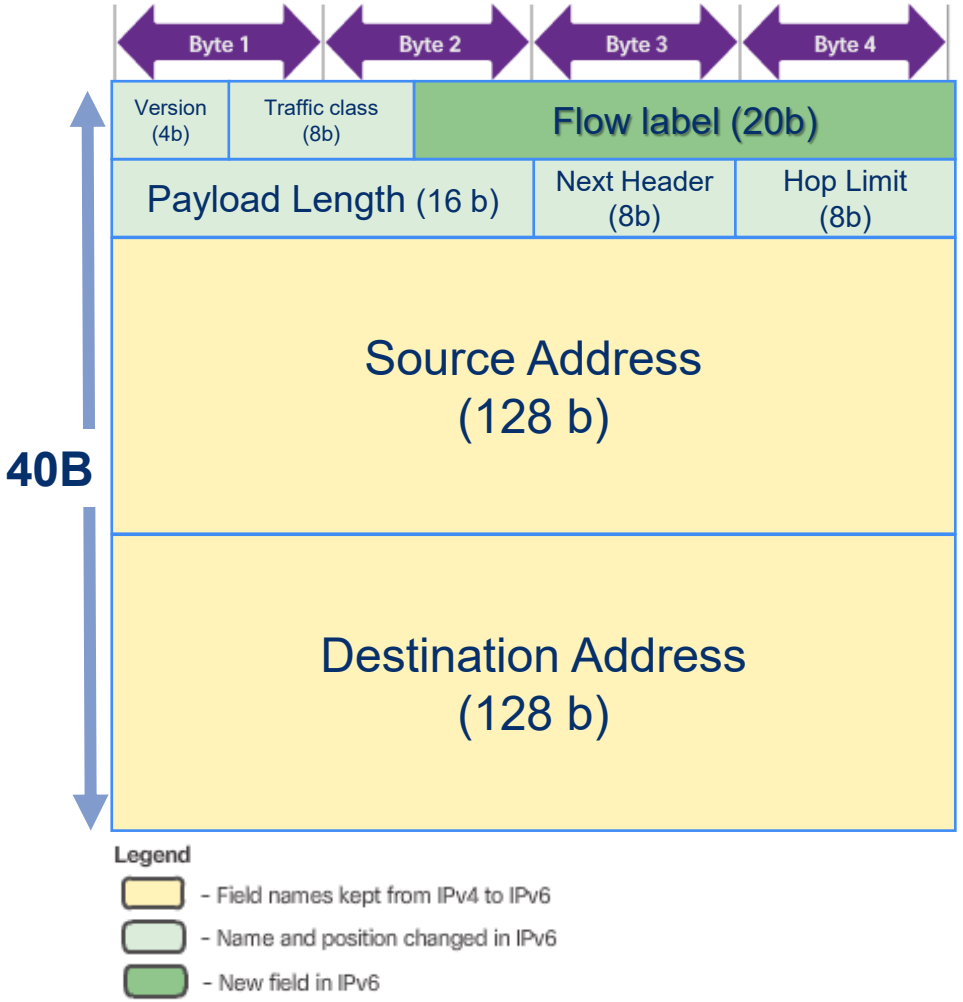
IPv 6 (128 bitové pole)

- 340 undeciliónov 340,000,000,000,000,000,000,000,000,000,000,000,000
- Adresný priestor s veľkou rezervou
- Zjednodušená štruktúra hlavičky
- Nepotrebuje NAT

Porovnanie IPv4 a IPv6 hlavičiek

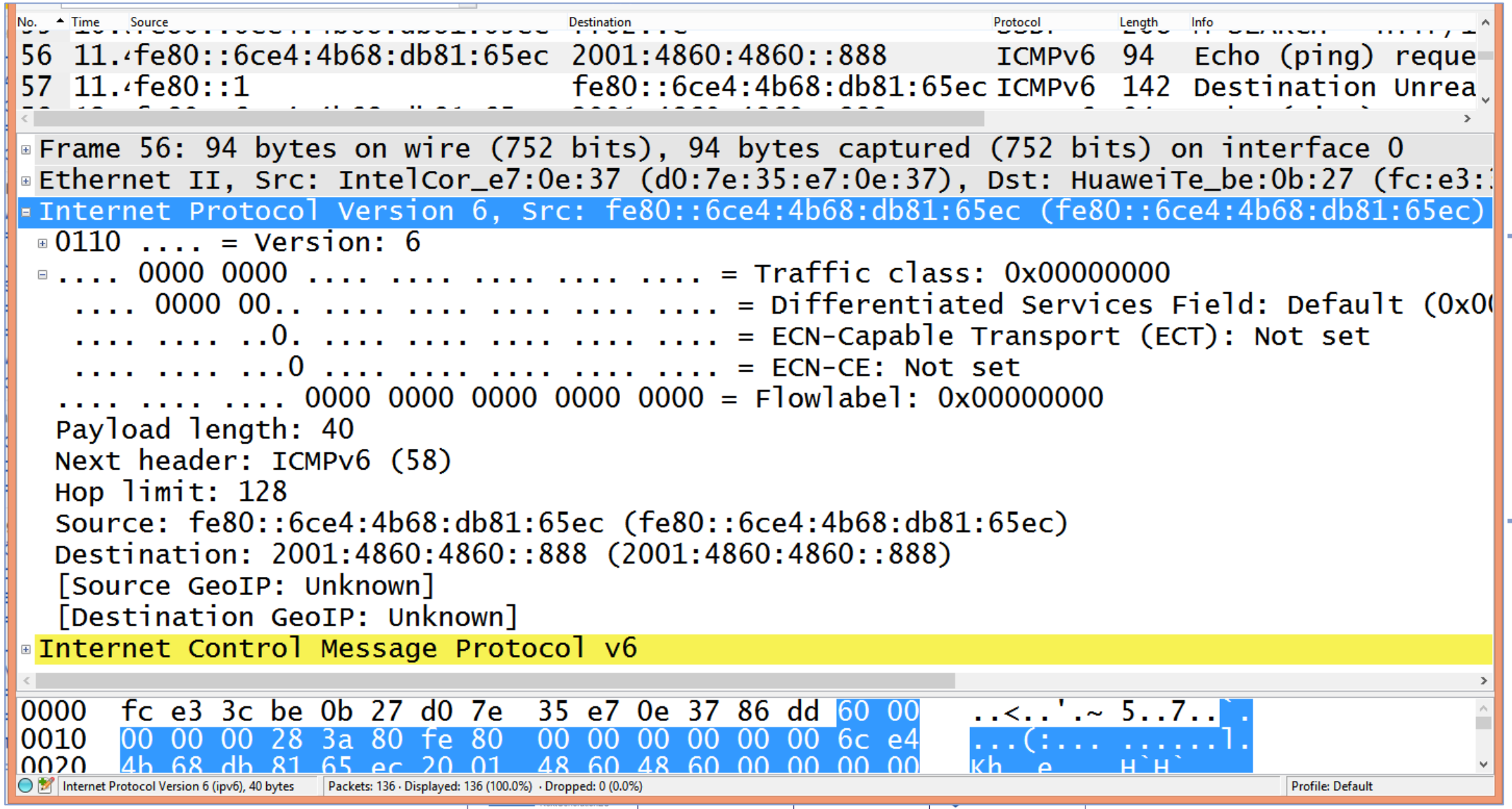


IPv6 hlavička

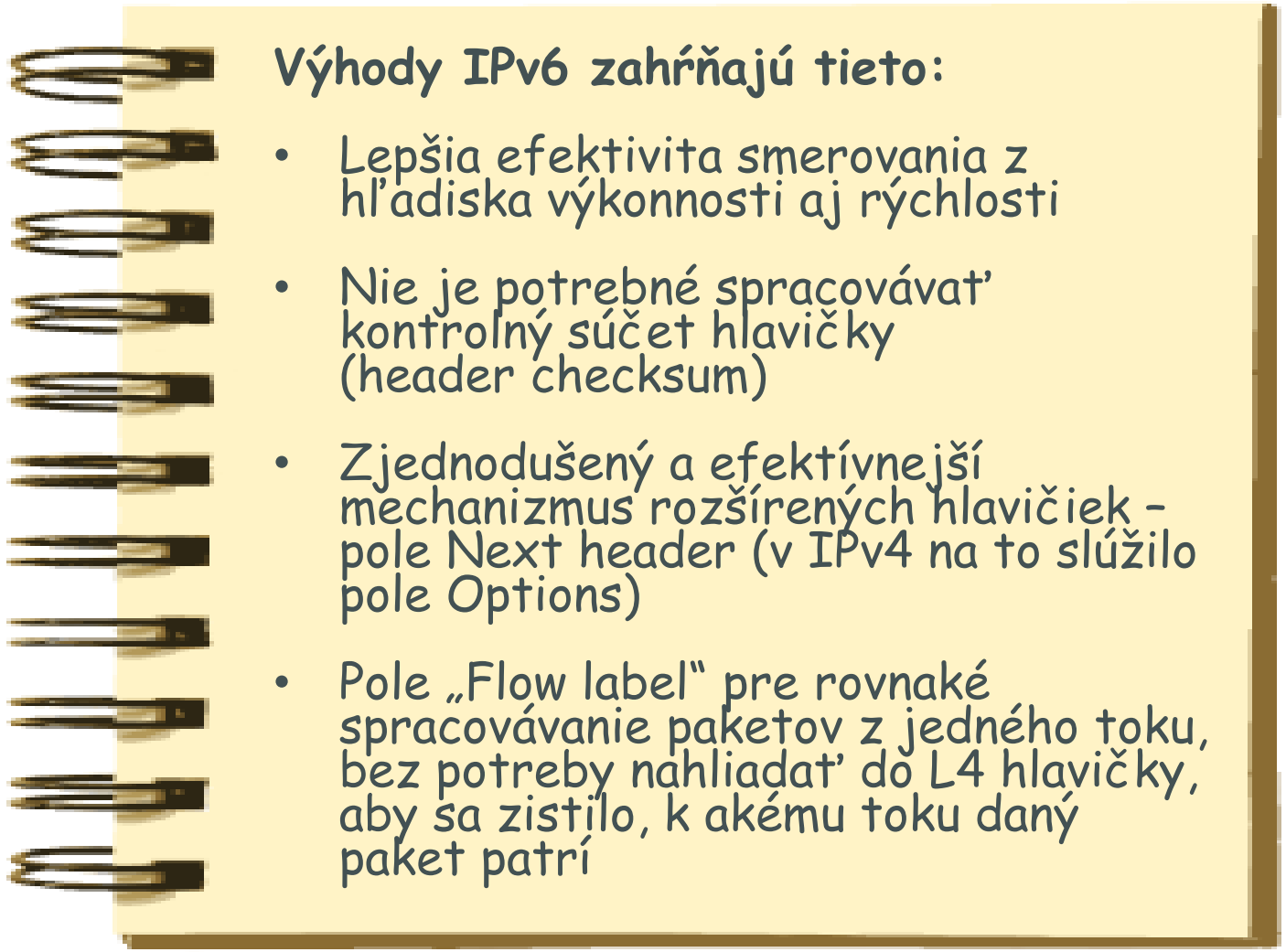


- **Version** = 0110 (IPv6)
- **Traffic Class** = Priorita paketu
  - keď nastane zahltenie, menej prioritné pakety môže smerovač začať zahadzovať
- **Flow Label** = označenie toku – všetky pakety z jedného toku budú smerovačmi spracované rovnako
- **Payload Length** = Total length v IPv4
- **Hop Limit** = ako TTL v IPv4
- **Source Address** = 128 bitová IPv6 adresa odosieľateľa paketu
- **Destination Address** = 128 bitová IPv6 adresa príjemcu paketu
- **Next Header** = ako pole Protocol v IPv4, typ L4 protokolu, alebo odkaz na rozšírenú hlavičku:
  - Medzi IPv6 hlavičku a telo sa môžu vkladať ešte prídavné-rozširujúce hlavičky, tzv. **extensions headers**
    - Kvôli fragmentácií paketu
    - Zabezpečeniu podpore mobility, ...

IPv6 hlavička - Wireshark



Formát hlavičky IPv6 paketu

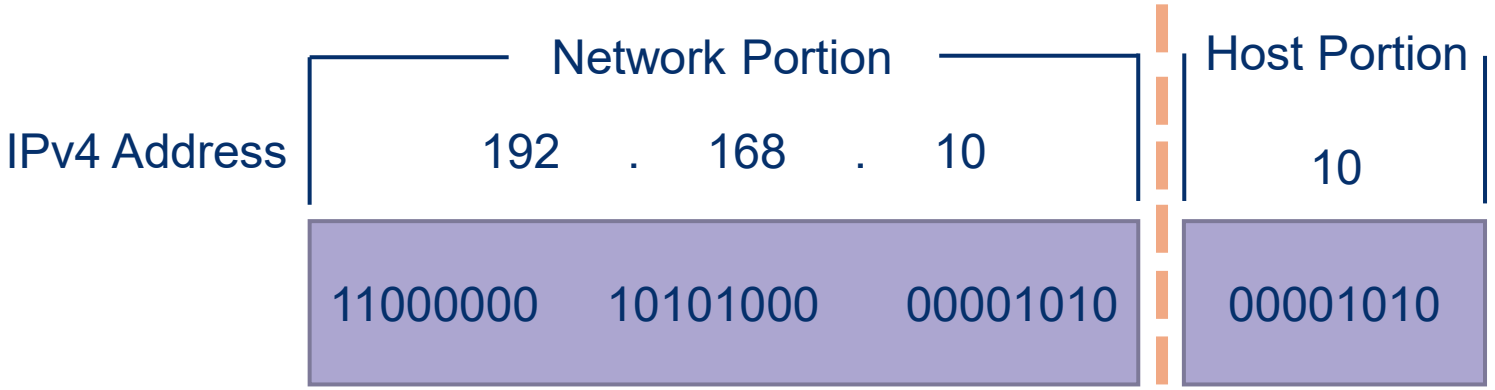


Výhody IPv6 zahŕňajú tieto:

- Lepšia efektivita smerovania z hľadiska výkonnosti aj rýchlosti
- Nie je potrebné spracovávať kontrolný súčet hlavičky (header checksum)
- Zjednodušený a efektívnejší mechanizmus rozšírených hlavičiek – pole Next header (v IPv4 na to slúžilo pole Options)
- Pole „Flow label" pre rovnaké spracovávanie paketov z jedného toku, bez potreby nahliadať do L4 hlavičky, aby sa zistilo, k akému toku daný paket patrí

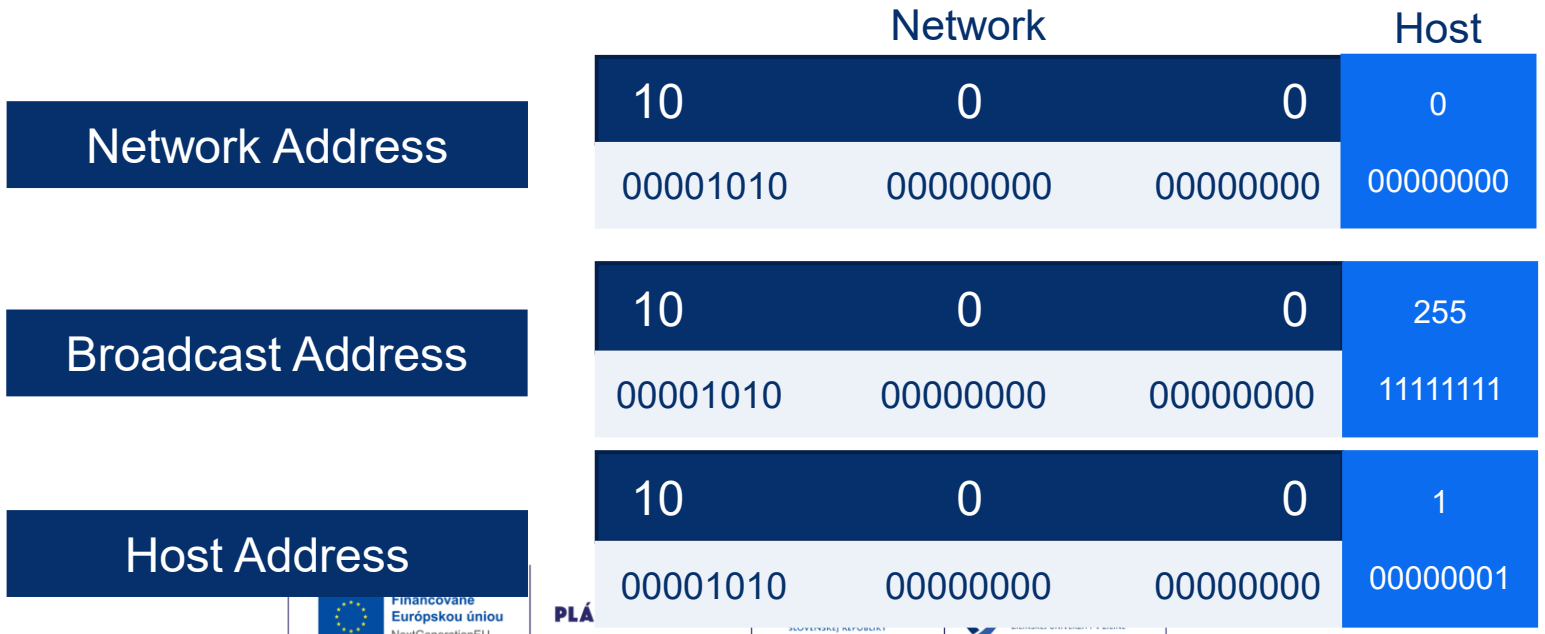
Predčíslie siete a číslo uzla

- IPv4 adresa je 4-bajtové číslo
- Toto číslo je rozdelené na dve časti
  - **Predčíslie siete** (Network Portion)
    - PSČ alebo telefónne čísla (predvoľba) sú pekným príkladom adries, ktoré vyjadrujú príslušnosť objektu do istej spoločnej skupiny príjemcov. Podobne je to s predčíslým siete.
  - **Číslo uzla** (Host Portion)
- Bajt IPv4 adresy sa zvykne nazývať aj oktet
- Hranica medzi predčíslím siete a číslom uzla je v IP adrese pohyblivá
- **Dva uzly sú v tej istej IP sieti práve vtedy, ak majú rovnaké predčíslie siete**

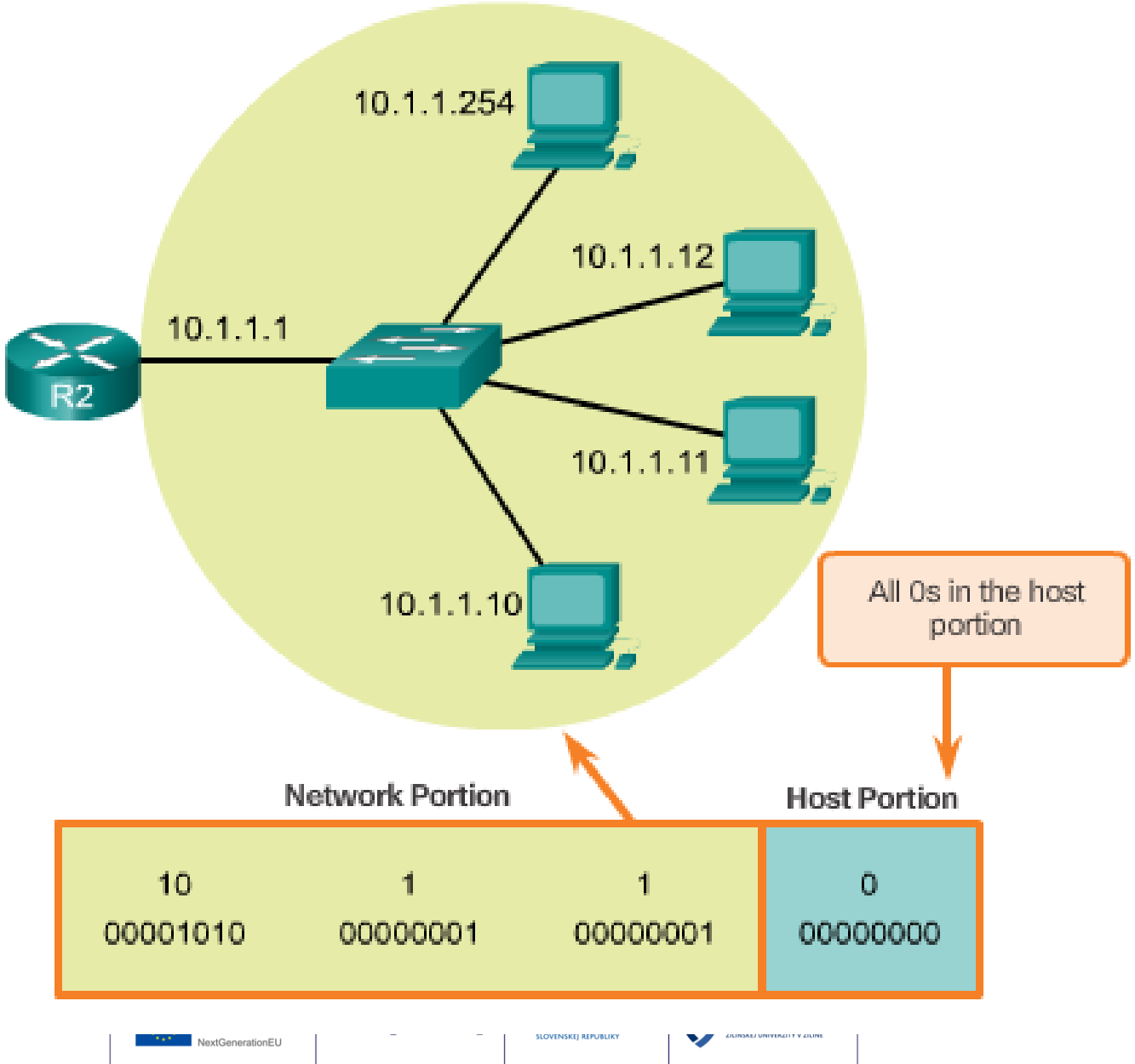


Adresa siete, broadcast, adresa uzla

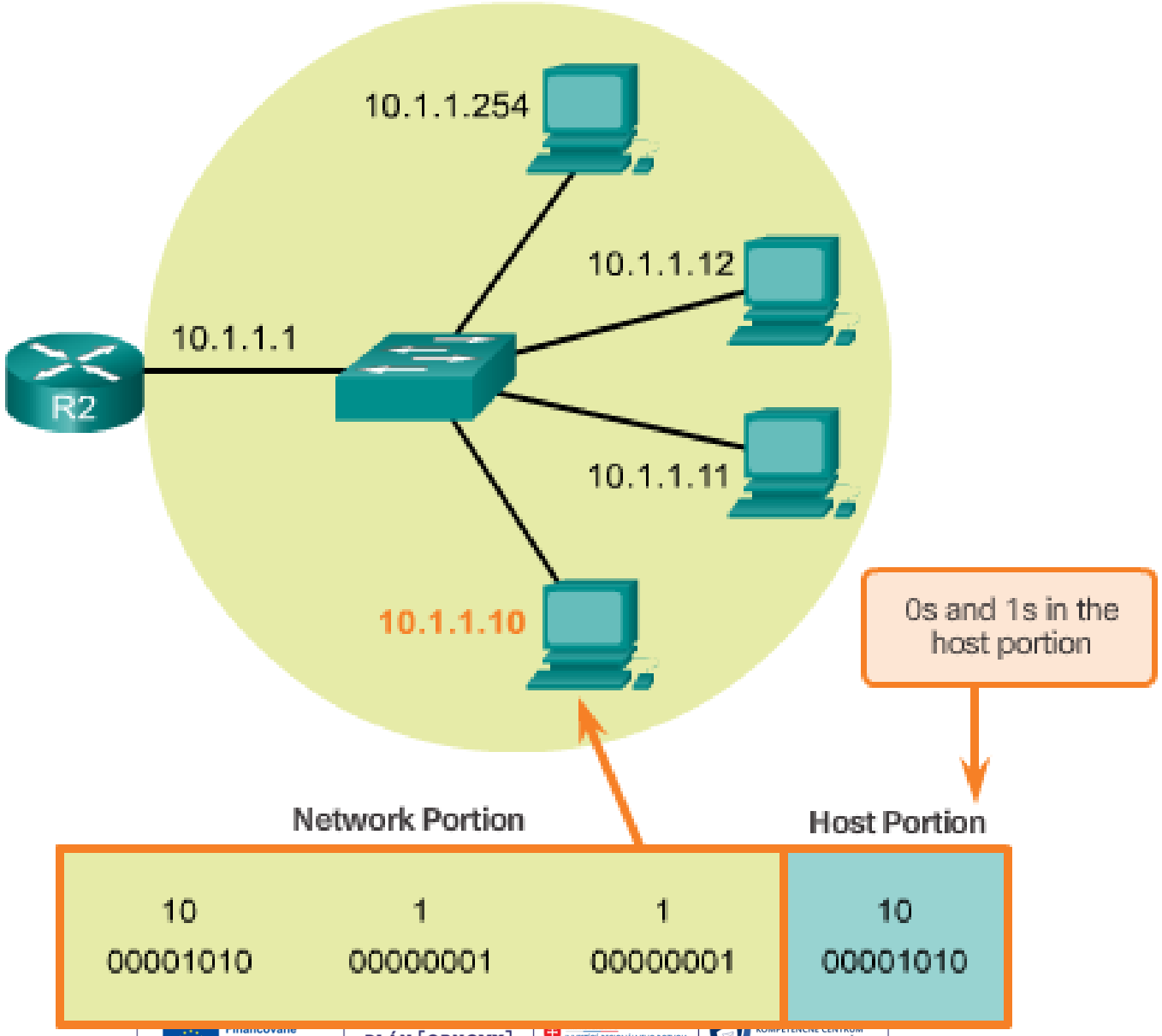
- Podľa toho, čo IP adresa označuje, rozoznávame
  - **Adresu siete**: **Najnižšia** adresa s daným predčíslím, označuje sieť ako celok (predčíslie sa doplní **nulami** do 32 bitov)
  - **Broadcastovú adresu**: **Najvyššia** adresa s daným predčíslím, počúva na nej každá stanica v danej sieti (predčíslie sa doplní **jednotkami** do 32 bitov)
  - **Adresu uzla**: **Každá iná** adresa s daným predčíslím, označuje konkrétny uzol



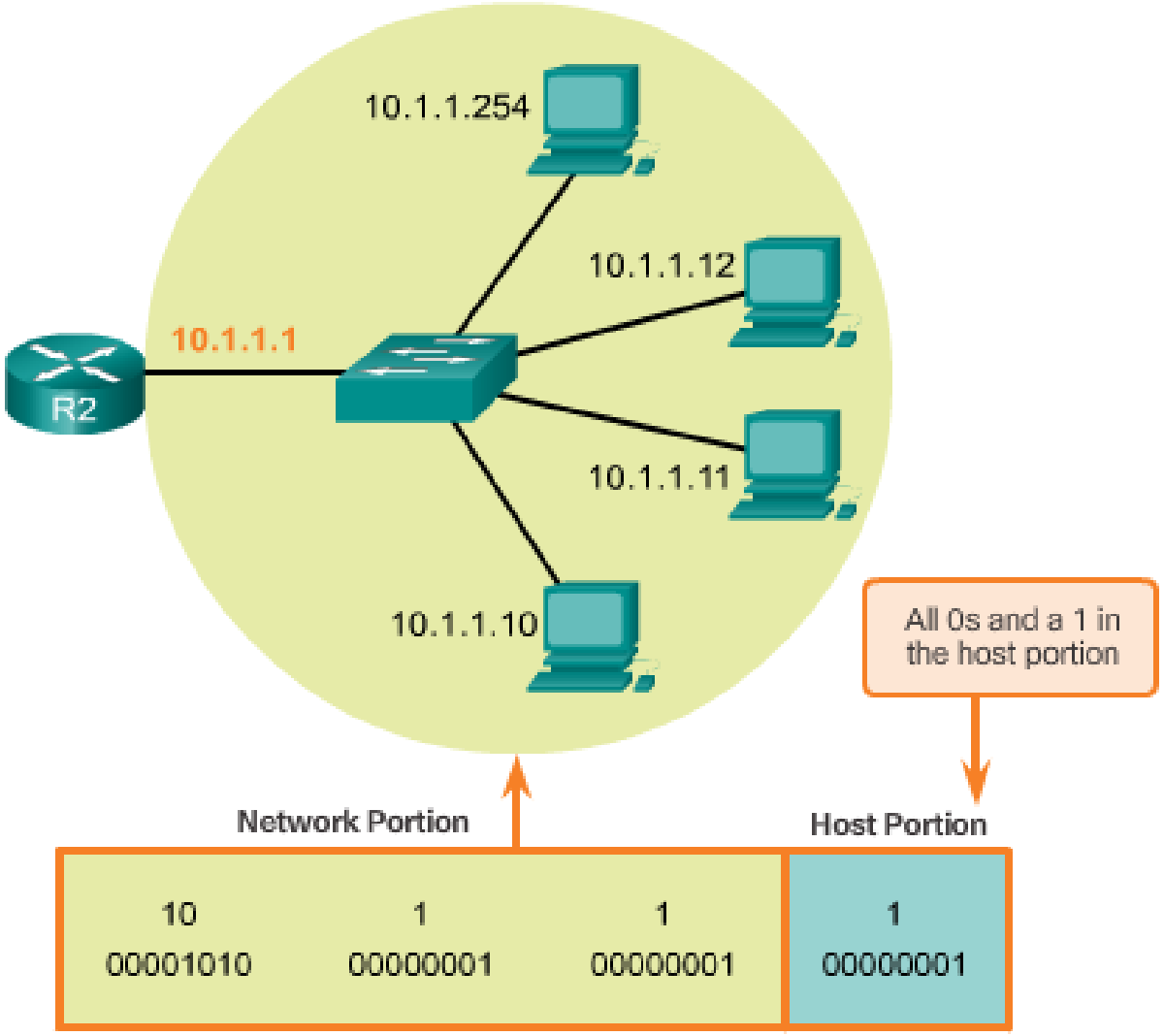
Adresa siete

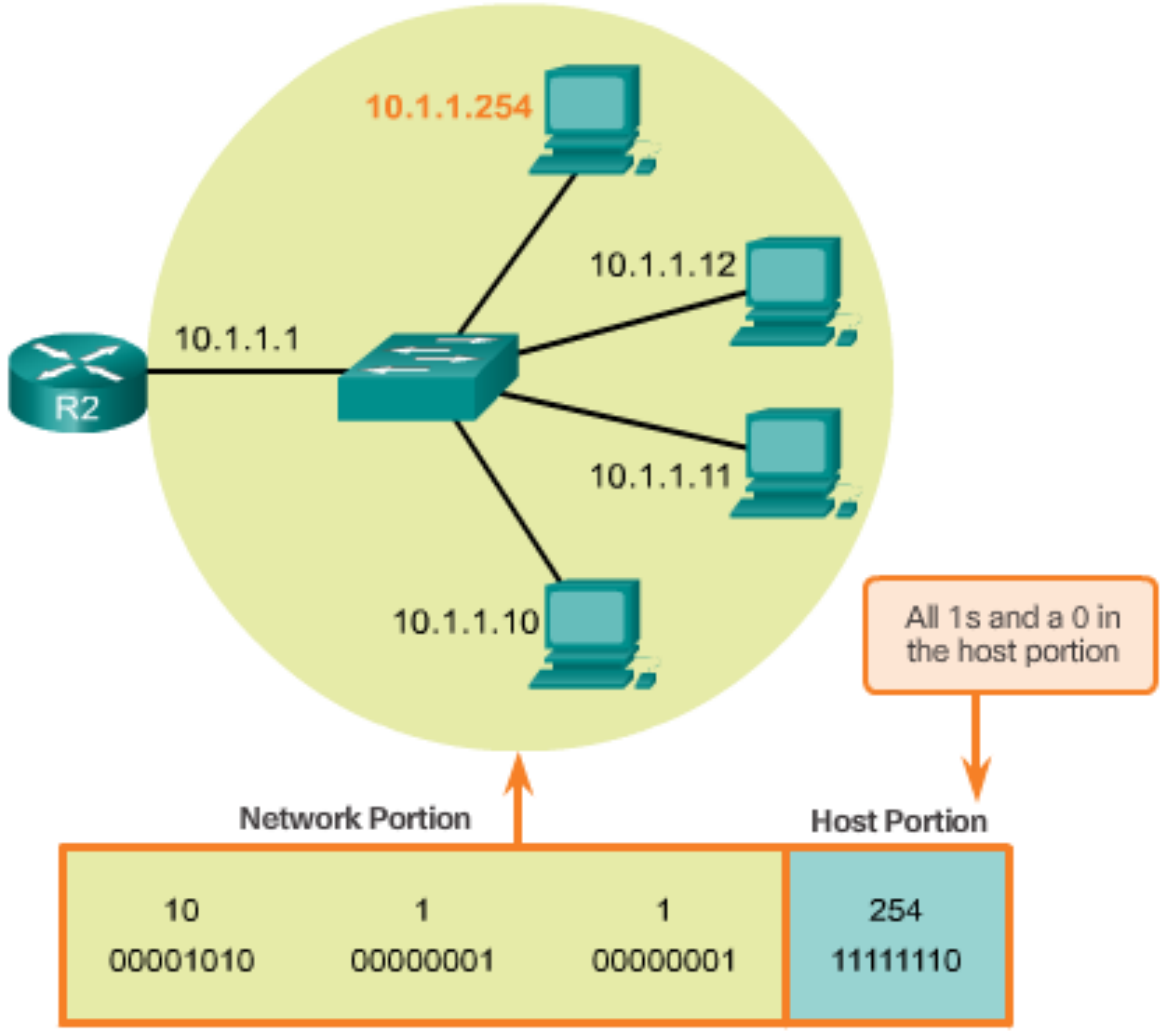


Adresa uzla

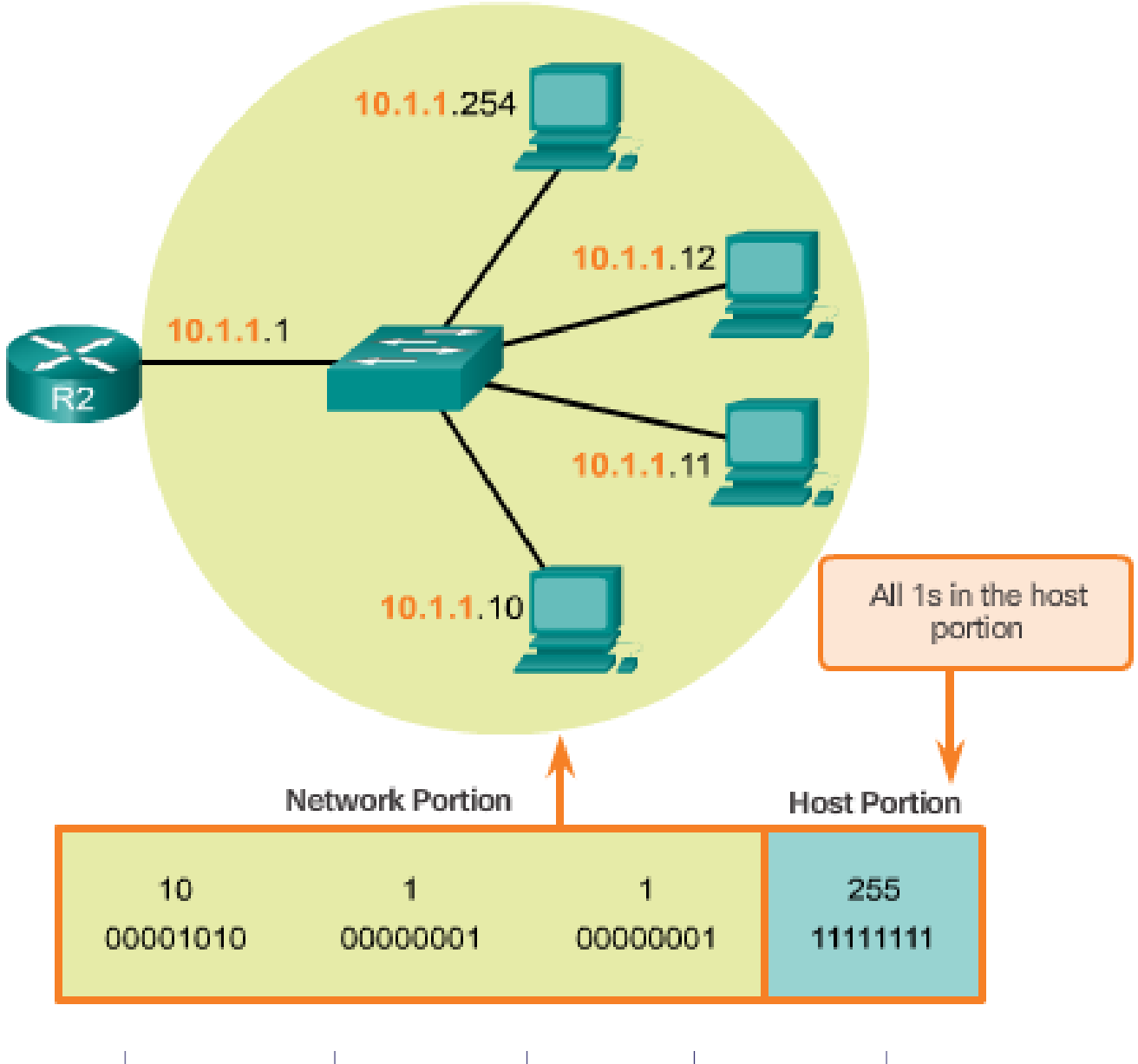

10.1.1.254
10.1.1.12
10.1.1.1
R2
10.1.1.11
10.1.1.10
0s and 1s in the host portion
Network Portion
Host Portion
10
00001010
1
00000001
1
00000001
10
00001010

Adresa uzla - prvá a posledná použiteľná IP

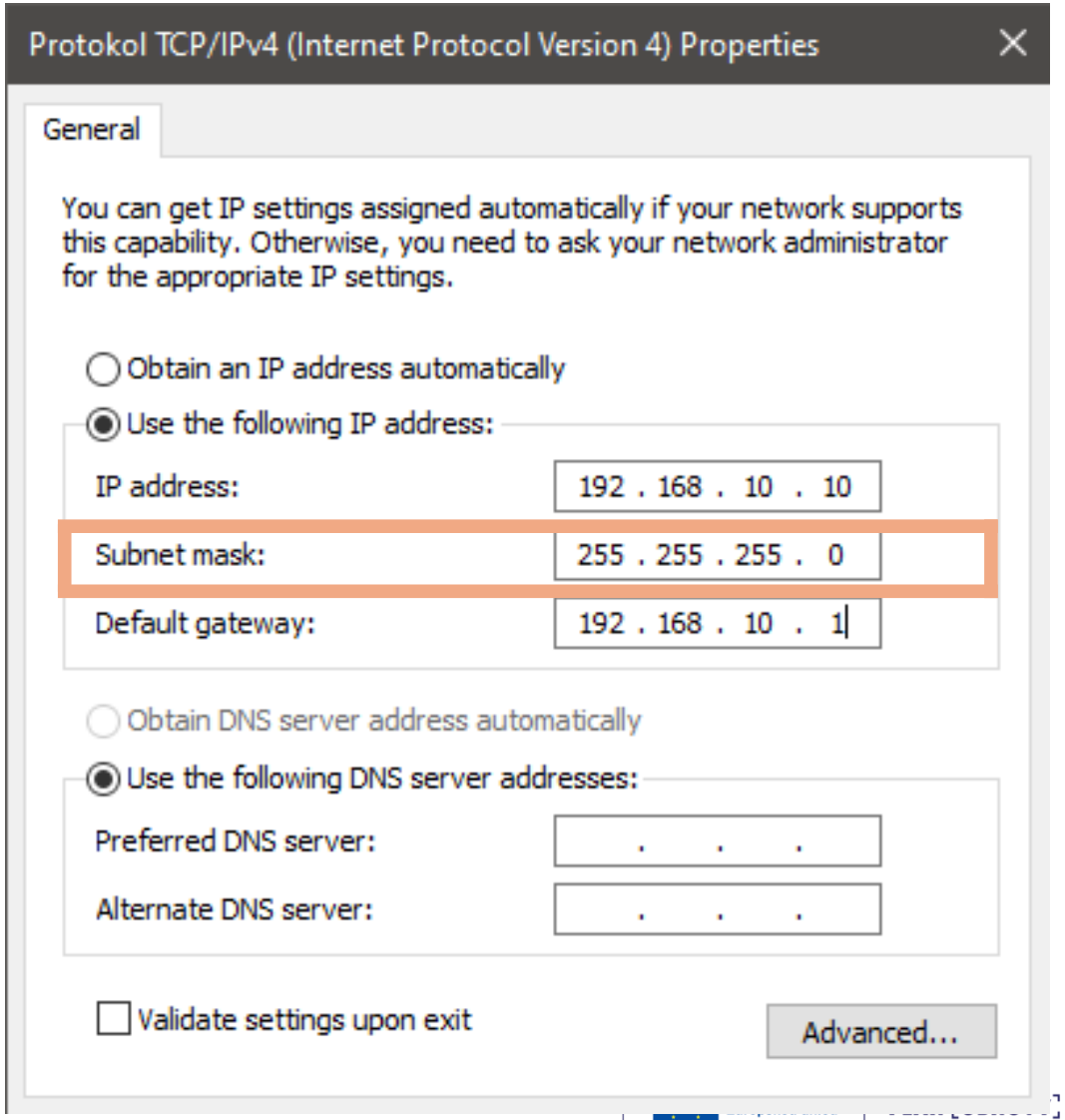




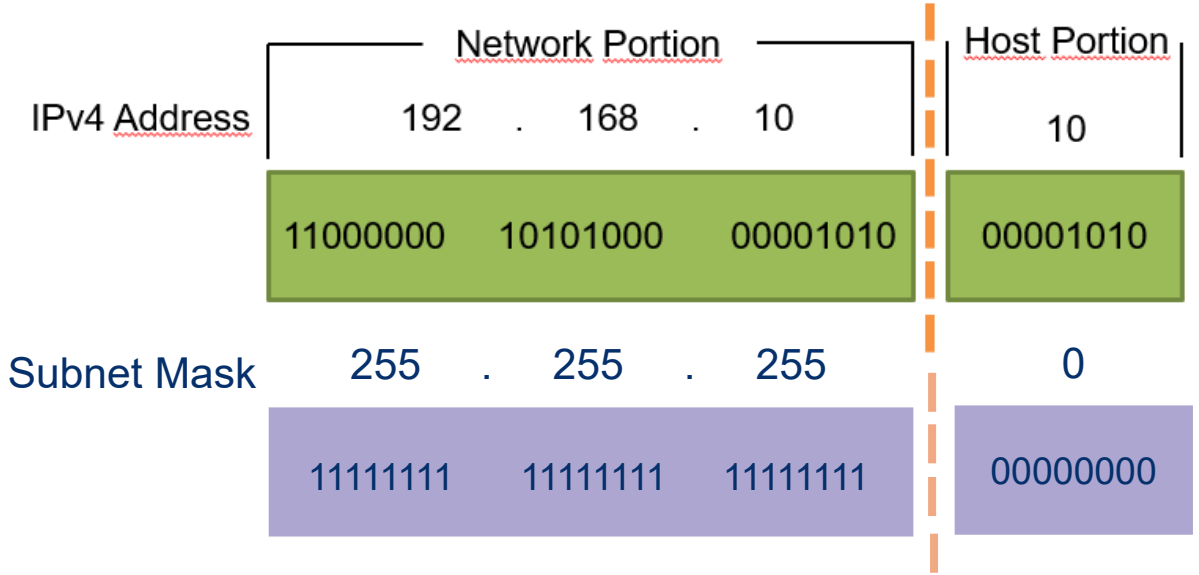
Broadcastová adresa



Sieťová maska (Subnet Mask)



Význam bitov sieťovej masky



- Maska je postupnosť 32 bitov v tvare 1...10....0, t.j. súvislý blok bitov nastavených na 1 nasledovaný súvislým blokom bitov nastavených na 0
- Ak je n-ty bit v maske nastavený na
  - 1: príslušný n-ty bit v IP adrese patrí do predčíslia siete
  - 0: príslušný n-ty bit v IP adrese patrí do čísla stanice
- IP adresu rozdeľuje na predčíslie siete a číslo počítača hranica medzi blokom bitov nastavených na 1 a blokom bitov nastavených 0 v maske

Test konektivity koniec-koniec

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\jozef>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=15ms TTL=55
Reply from 8.8.8.8: bytes=32 time=15ms TTL=55
Reply from 8.8.8.8: bytes=32 time=15ms TTL=55
Reply from 8.8.8.8: bytes=32 time=15ms TTL=55

Ping statistics for 8.8.8.8:
      Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
      Minimum = 15ms, Maximum = 15ms, Average = 15ms
```

Network Address Translation NAT

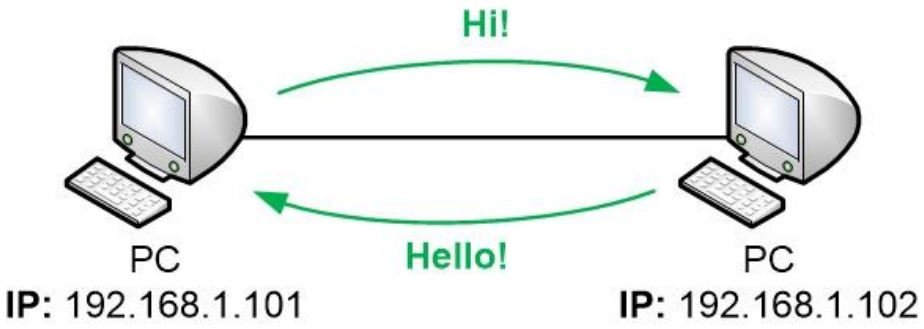
- je mechanizmus, ktorý mení IP adresy v hlavičkách paketov pri ich prechode cez router alebo firewall.
- Používa sa hlavne preto, lebo verejné IPv4 adresy sú obmedzený zdroj, zatiaľ čo súkromných adries je veľa.
- Prečo NAT?
  - Umožňuje viacerým zariadeniam v súkromnej sieti používať jednu verejnú IPv4 adresu na prístup k internetu.
  - Zvyšuje bezpečnosť – vnútorné IP adresy nie sú priamo viditeľné z internetu. – **už to nie je taká pravda.**
  - Predlžuje životnosť IPv4.

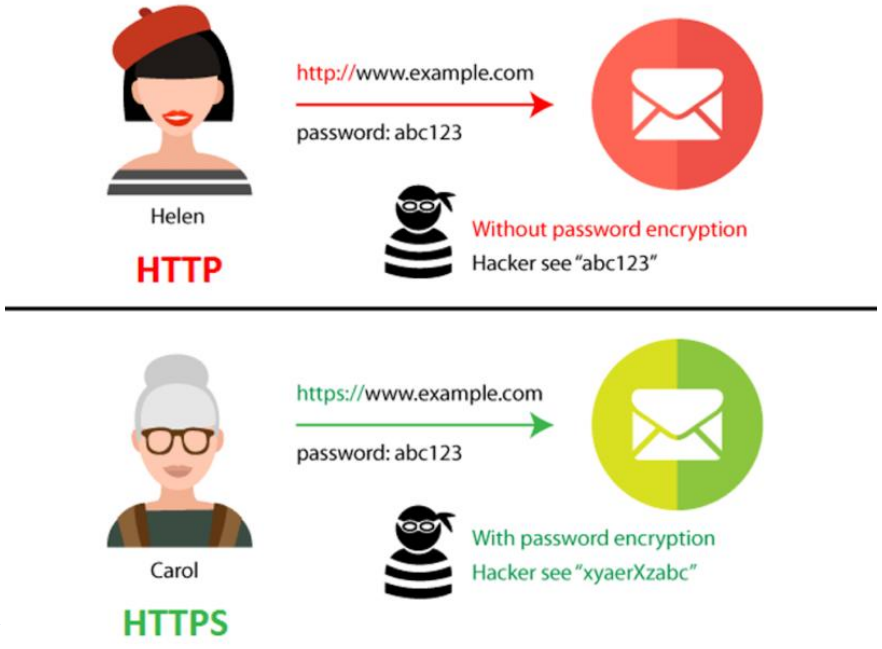
Komunikačné protokoly

Komunikačné protokoly

Komunikačné protokoly sú pravidlá určujúce formát a prenos dát medzi zariadeniami. Medzi kľúčové protokoly patria:

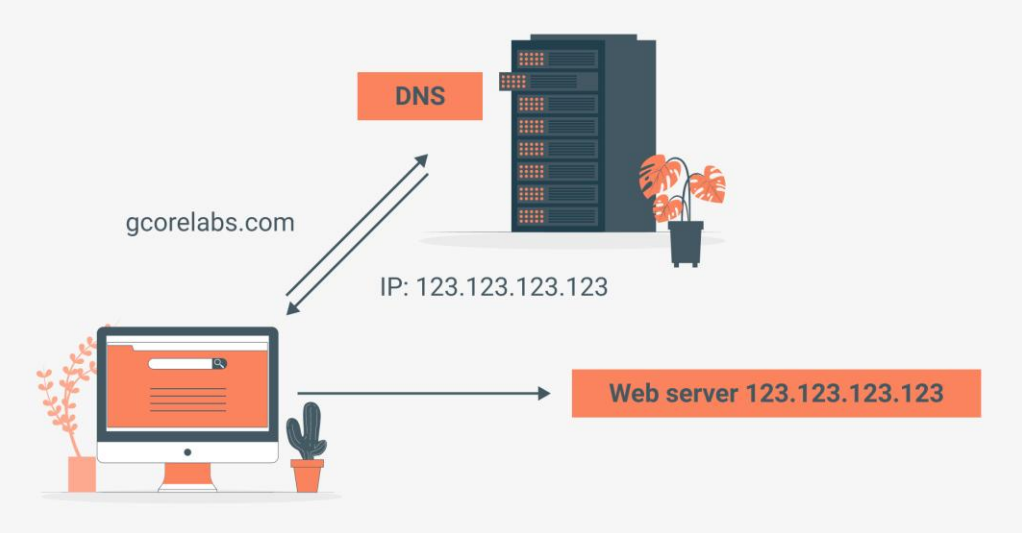
- **TCP/IP (Transmission Control Protocol/Internet Protocol)**: Základný protokol internetu zabezpečujúci spoľahlivý prenos dát.
- **HTTP/HTTPS (HyperText Transfer Protocol/Secure)**: Protokoly pre prenos webových stránok; HTTPS pridáva šifrovanie pre bezpečnosť.

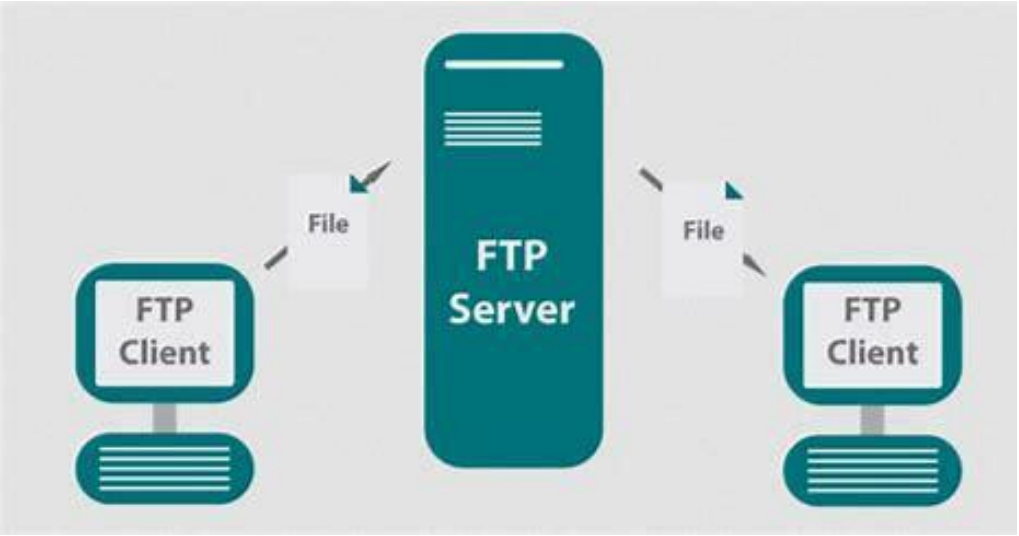




Komunikačné protokoly

- **FTP (File Transfer Protocol)**: Umožňuje prenos súborov medzi klientom a serverom.
- **DNS (Domain Name System)**: Prekladá doménové mená na IP adresy, umožňujúc ľahší prístup k webovým stránkam.
- **DHCP (Dynamic Host Configuration Protocol)**: Automaticky prideľuje IP adresy zariadeniam v sieti.



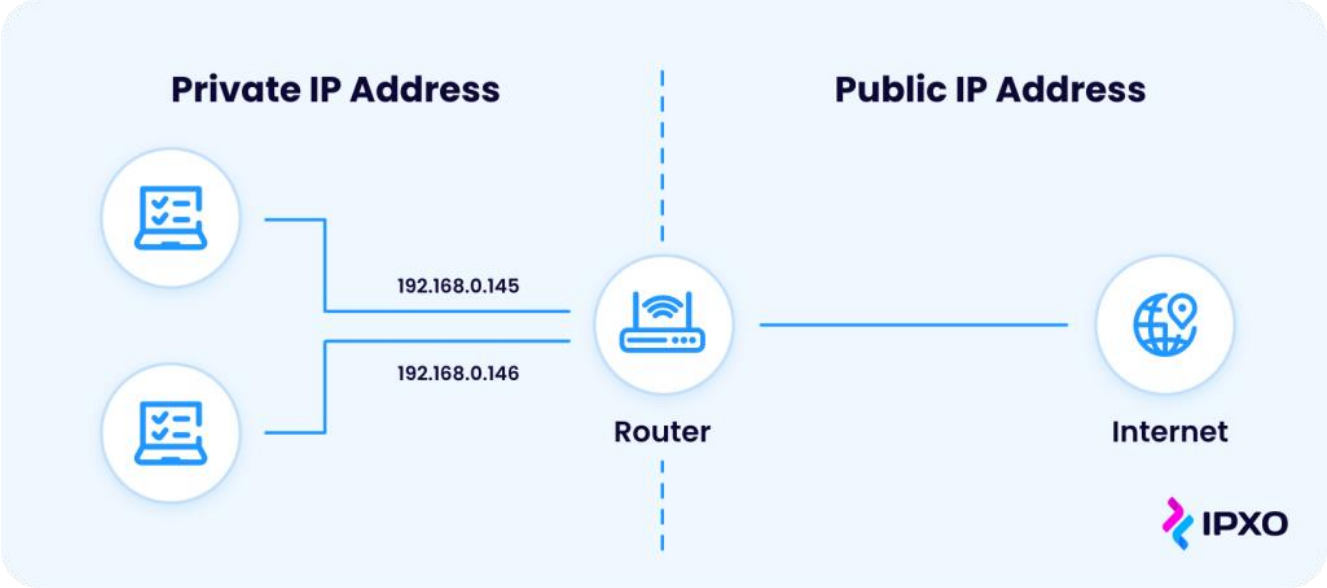


Ako prebieha prenos dát

- Prenos dát v sieti prebieha v niekoľkých krokoch:
  - Dáta sú najprv rozdelené na menšie časti nazývané pakety.
  - Každý paket obsahuje informácie o odosielateľovi, príjemcovi, poradí v rámci celej správy a kontrolné údaje.
  - Pakety sú posielané sieťou nezávisle, často rôznymi trasami.
  - Po doručení ich cieľové zariadenie opätovne poskladá do pôvodnej správy.

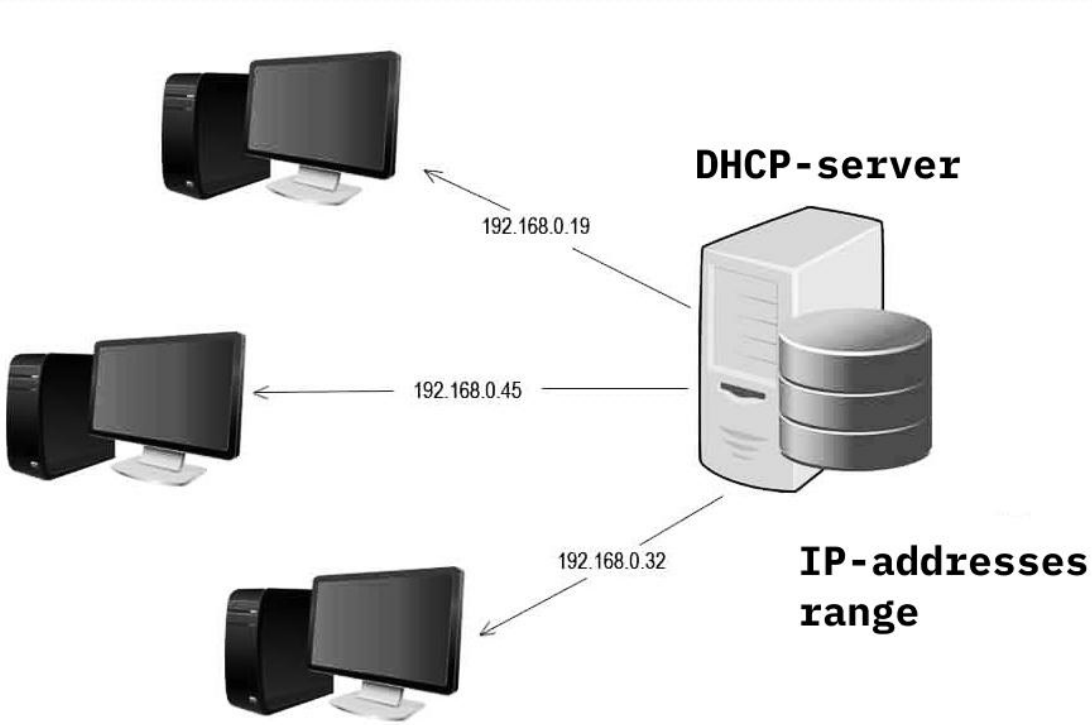
IP adresy: verejné vs. súkromné

- **Verejná IP adresa**
  - Je jedinečná adresa priradená zariadeniu, ktoré komunikuje s internetom. Tieto adresy sú prideľované poskytovateľmi internetu a sú viditeľné z vonkajšej siete.
- **Súkromná IP adresa**
  - Používa sa vo vnútorných sieťach, ako napr. v domácnostiach alebo firmách. Príklady: 192.168.0.1 alebo 10.0.0.1. Tieto adresy nie sú priamo dostupné z internetu.



Dynamic Host Configuration Protocol (DHCP)

- Tento protokol slúži na automatické priraďovanie IP adries zariadeniam v sieti. DHCP server zabezpečí, že každé zariadenie dostane jedinečnú IP adresu, čím sa zjednodušuje správa siete.



Operačné systémy

- **Shell**
  - používateľské rozhranie, ktoré umožňuje používateľom zadávať konkrétne úlohy počítaču
  - požiadavky môžu byť vykonané buď prostredníctvom
    - CLI (Command Line Interface)
      - používateľ priamo interaguje so systémom v textovom prostredí zadávaním príkazov na klávesnici v príkazovom riadku
      - systém vykoná príkaz a často poskytne textový výstup
      - CLI vyžaduje veľmi málo prostriedkov na prevádzku
      - Treba však znalosti o základnej štruktúre príkazov
    - alebo GUI (Graphical User Interface) rozhraní
      - Windows, macOS, Linux KDE, Apple iOS, Android
- **Kernel**
  - komunikuje medzi hardvérom a softvérom počítača
  - riadi, ako sú hardvérové zdroje využívané na splnenie požiadaviek softvéru
- **Hardware**
  - fyzická časť počítača vrátane základnej elektroniky

Zabezpečenie LAN sietí

Riziká v LAN sieťach

- Neoprávnený prístup k dátam – hrozí, že útočník sa dostane k citlivým informáciám bez povolenia.
- Malware a vírusy – škodlivý softvér môže infikovať zariadenia, spôsobiť výpadky alebo úniky dát.
- Útoky typu Man-in-the-Middle – útočník zachytáva alebo mení komunikáciu medzi dvoma zariadeniami.
- Nezabezpečené bezdrôtové siete – Wi-Fi siete bez hesla alebo so slabým zabezpečením sú ľahko zneužiteľné.

Metódy zabezpečenia

- Firewall
  - Hardvérové alebo softvérové riešenie, ktoré monitoruje a kontroluje sieťovú prevádzku. Pomáha zabrániť neoprávnenému prístupu.
- Antivírusový softvér
  - Slúži na detekciu, blokovanie a odstraňovanie škodlivého softvéru. Je dôležité ho pravidelne aktualizovať.
- Šifrovanie
  - Zabezpečuje, že dáta počas prenosu nie sú čitateľné pre tretie strany. Príkladom je WPA3 pre šifrovanie Wi-Fi komunikácie.
- Autentifikácia
  - Overuje identitu používateľov alebo zariadení predtým, ako im umožní prístup do siete. Bežná forma je zadanie mena a hesla.
- Segmentácia siete
  - Znamená rozdelenie siete na menšie časti (subnety), čo obmedzuje šírenie hrozieb a zvyšuje kontrolu nad prístupom.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Bezpečnosť bezdrôtových sietí

- Používanie silných hesiel
  - Zložité a dlhé heslá výrazne sťažujú neoprávnený prístup do Wi-Fi siete.
- Aktualizácia firmvéru prístupového bodu (AP)
  - Výrobcovia pravidelne opravujú zraniteľnosti, preto je dôležité aktualizovať softvér zariadenia.
- Vypnutie vysielania SSID
  - Skrytie názvu siete sťažuje jej objavenie náhodnými útočníkmi.
- Použitie VPN (Virtual Private Network)
  - Zabezpečuje šifrované spojenie medzi používateľom a cieľovou službou, čo chráni pred odpočúvaním aj v nezabezpečených sieťach.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

IP zranitel’nosti

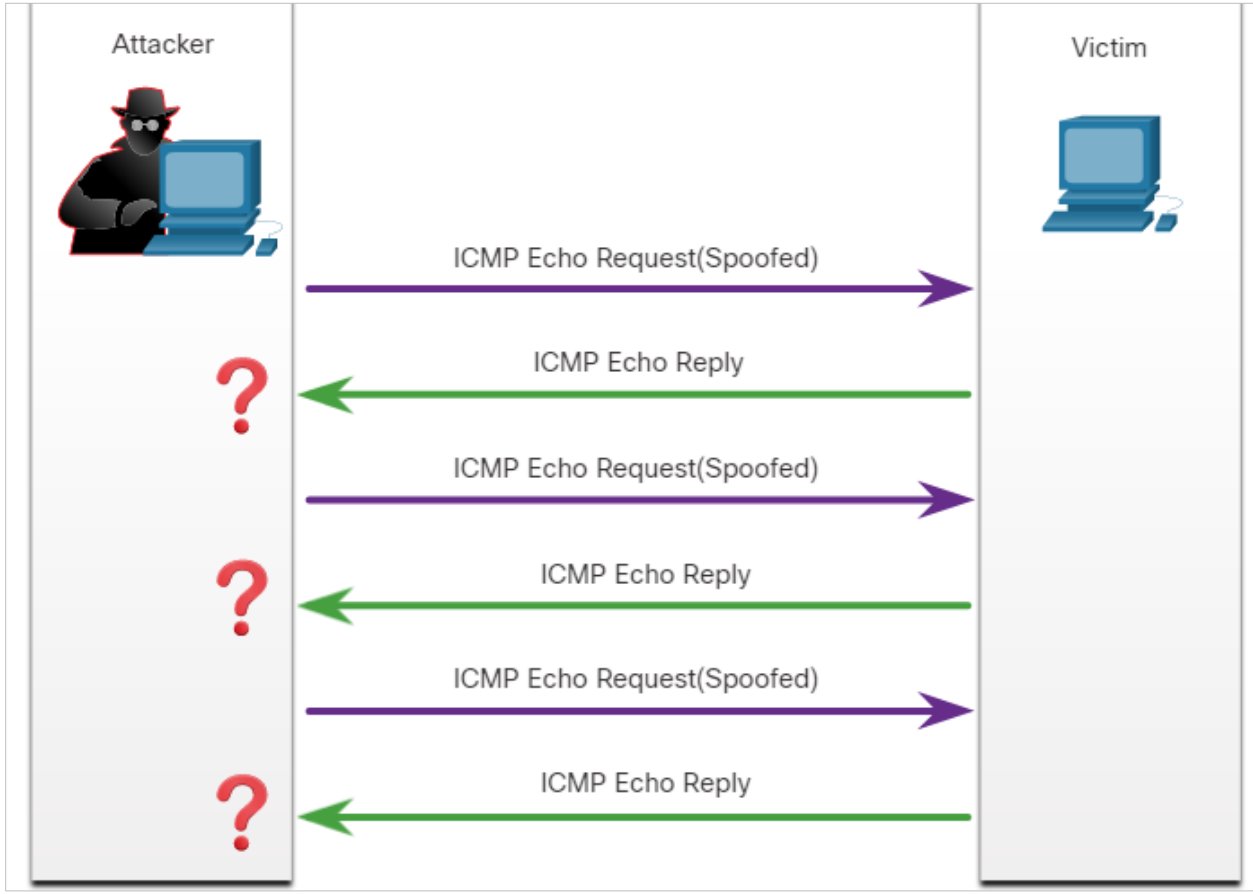
IP Vulnerabilities

V nasledujúcej tabuľke sú uvedené niektoré z bežných útokov súvisiacich s IP:

IP útoky	Popis
ICMP attacks	Útočníci používajú **ICMP echo** pakety na **zisťovanie podsietí a zariadení** v chránenej sieti, na vytváranie útokov DoS a na zmenu smerovacích tabuliek.
DoS attacks	Útočníci sa pokúšajú **zabrániť** legitímnym používateľom **v prístupe** k informáciám alebo službám.
DDoS attacks	Podobný útok ako útok DoS, ale predstavuje simultánny, koordinovaný útok z viacerých **zdrojových** zariadení.
Address spoofing attacks	Útočníci podvrhnú zdrojovú IP adresu v snahe vykonať blind spoofing alebo non-blind spoofing.
Man-in-the-middle attack (MiTM)	Útočníci sa umiestnia medzi zdroj a cieľ, aby mohli transparentne monitorovať, zachytávať a riadiť komunikáciu. Môžu odpočúvať komunikáciu prezeraním paketov alebo meniť pakety a preposielať ich do pôvodného cieľa.
Session hijacking	Útočníci získajú prístup do fyzickej siete a potom pomocou útoku MiTM ovládnu reláciu.

ICMP útoky

- ICMP bol vyvinutý na prenos diagnostických správ a hlásenie chybových stavov
  - keď sú cesty, zariadenia a porty nedostupné
  - správy ICMP generujú zariadenia, keď dôjde k chybe alebo výpadku siete
- Príkaz ping je používateľom generovaná správa ICMP, nazývaná echo request, ktorá sa používa na overenie konektivity k cieľu.
- Útočníci používajú ICMP na:
  - prieskumné a skenovacie útoky.
  - útoky DoS a DDoS, ako je znázornené na obrázku v prípade útoku ICMP flood.
- Poznámka: ICMP pre IPv4 (ICMPv4) a ICMP pre IPv6 (ICMPv6) sú náchylné na podobné typy útokov.



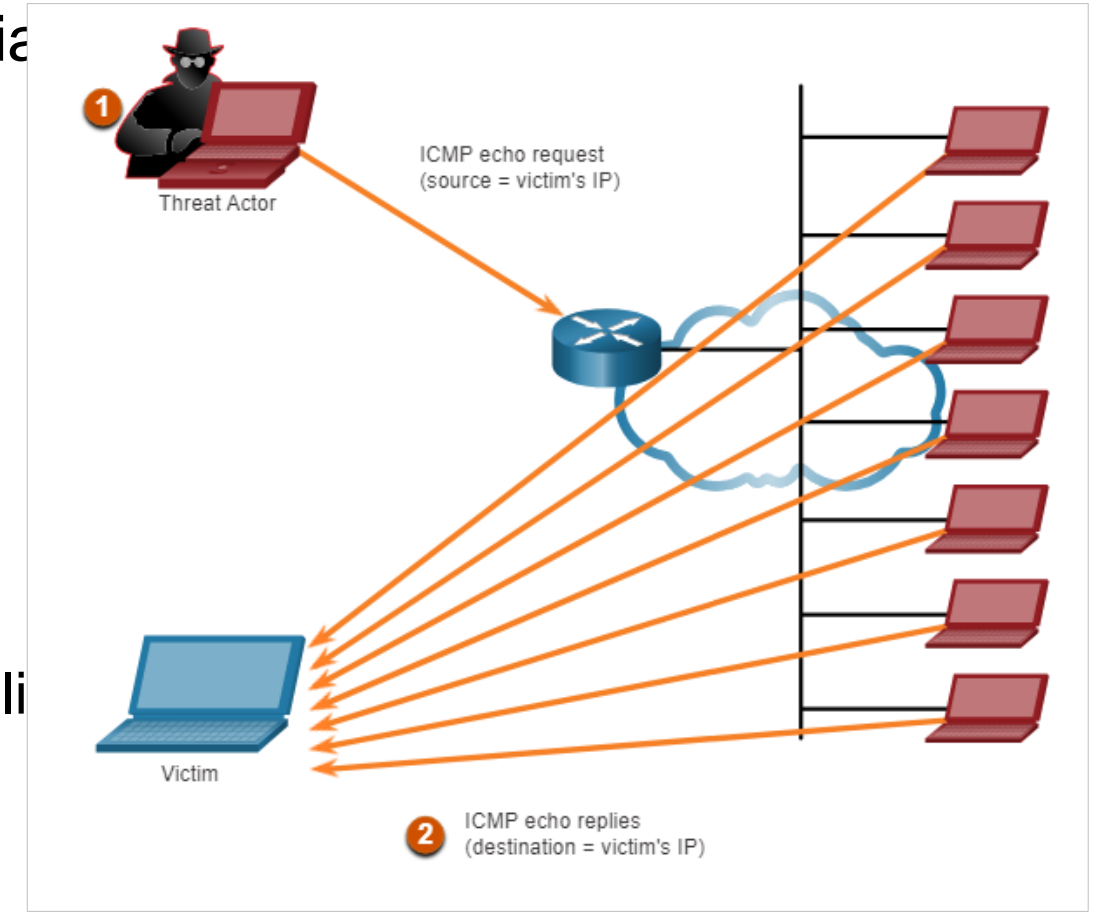
ICMP útoky (Pokr.)

- Siete by mali mať zavedené prísne filtrovanie ICMP prostredníctvom ACL
  - a to práve na okraji siete, aby sa zabránilo ICMP sondovaniu z internetu
- V nasledujúcej tabuľke sú uvedené bežné ICMP správy, ktoré sú užitočné pre útočníkov:

ICMP správa	Popis
ICMP echo request and echo reply	Používa sa na overovanie zariadenia a útoky DoS.
ICMP unreachable	Používa sa na vykonávanie prieskumu siete a skenovacích útokov
ICMP mask reply	Používa sa na mapovanie vnútornej siete (ICMP Address Mask Request)
ICMP redirects	Používa sa na nalákanie cieľového zariadenia na odosielanie všetkej prevádzky cez podvrhnuté zariadenie a na vytvorenie útoku MITM.
ICMP router discovery	Útočník pošle správu ICMP Router Solicitation do siete, aby zistil, ktoré smerovače sú dostupné, odpoveď ide cez ICMP Router Advertisment. Identifikácia smerovačov, získanie metriky smerovania, zraniteľnosti smerovačov, vloženie falošných záznamov o smerovaní do smerovacej tabuľky cieľového zariadenia – ako?

Amplification and Reflection Attacks

- Útočníci často používajú techniky zosilnenia a odrazu na vytváranie DoS útokov.
- Obrázok ukazuje, ako sa na zahltenie cieľového zariadenia používa technika zosilnenia a odrazu nazývaná útok **Smurf**.
  - **Amplification** - Útočník preposiela správy ICMP echo request mnohým zariadeniam. Tieto správy obsahujú zdrojovú IP adresu obete
  - **Reflection** - Všetky zariadenia odpovedajú na podvrhnutú IP adresu obete, aby ju zahltili
- Útočníci používajú aj útoky na vyčerpanie zdrojov.
- V súčasnosti sa používajú novšie formy útokov typu zosilnenie a odraz, napríklad útoky založené na DNS alebo NTP.



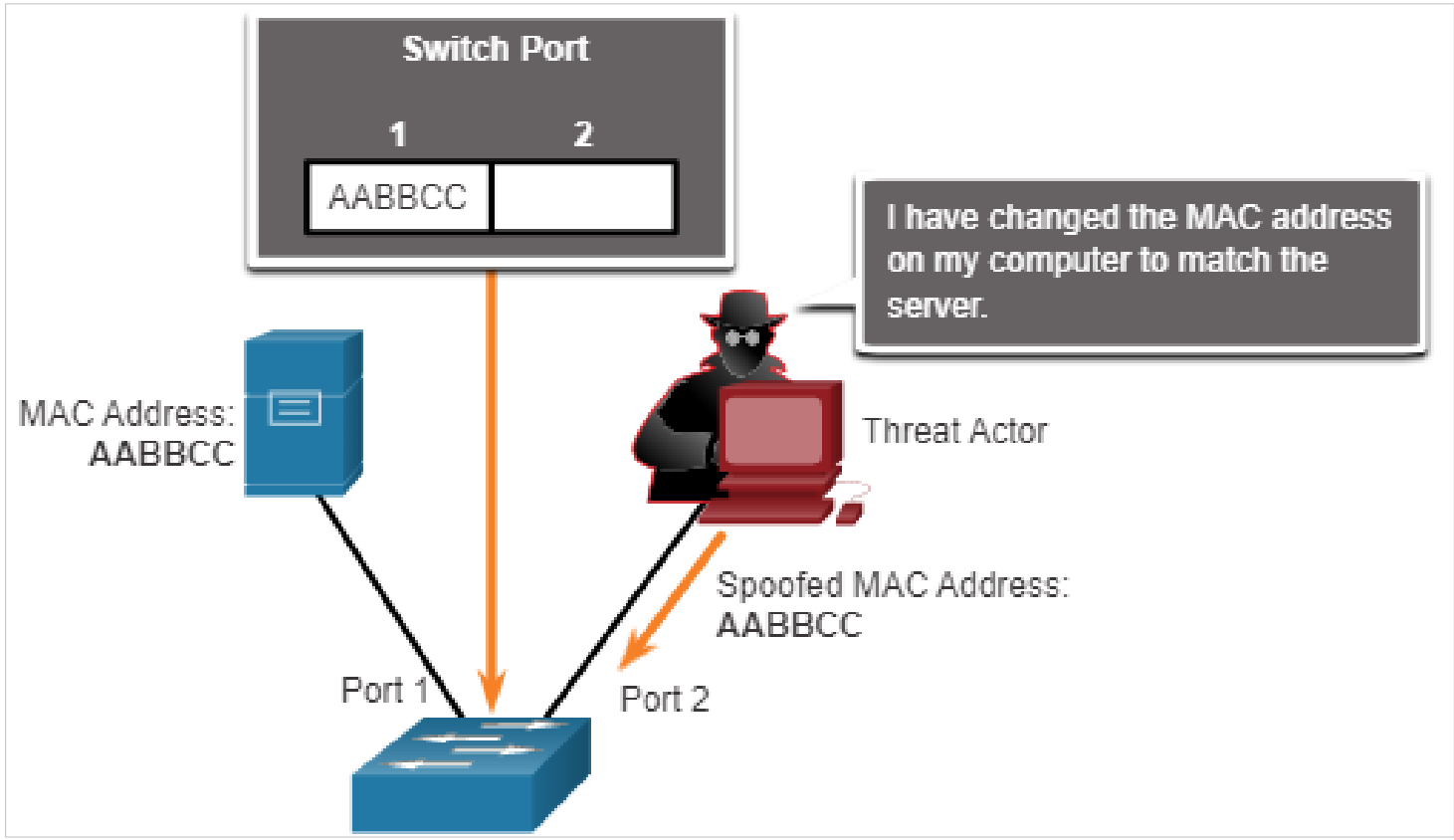
Address Spoofing Attacks

- Útoky na báze falšovania IP adries sa vyskytujú vtedy, keď útočník vytvára pakety s falošnými informáciami o zdrojovej IP adrese, aby skryl identitu odosielateľa alebo sa vydával za iného legitímneho používateľa.
- Útočník tak môže získať prístup k inak nedostupným údajom alebo obísť bezpečnostné konfigurácie.
- Spoofing je zvyčajne súčasťou iného útoku, napríklad útoku Smurf.
- Tento typ útokov môže byť non-blind alebo blind:
  - **Non-blind spoofing**
    - Útočník má prístup k informáciám o komunikácii, napríklad cez sniffing (odpočúvanie) siete.
    - Útočník používa tento typ útoku na kontrolu paketu odpovede od cieľovej obete.
    - Pomocou toho určuje stav firewallu a vykonáva predikciu sekvenčných čísiel. Môže tiež zneužiť autorizovanú reláciu.
  - **Blind spoofing**
    - Útočník nevidí prevádzku, ktorá sa odosiela medzi zdrojom a cieľom.
    - Používa sa pri útokoch DoS.

Address Spoofing Attacks (Pokr.)

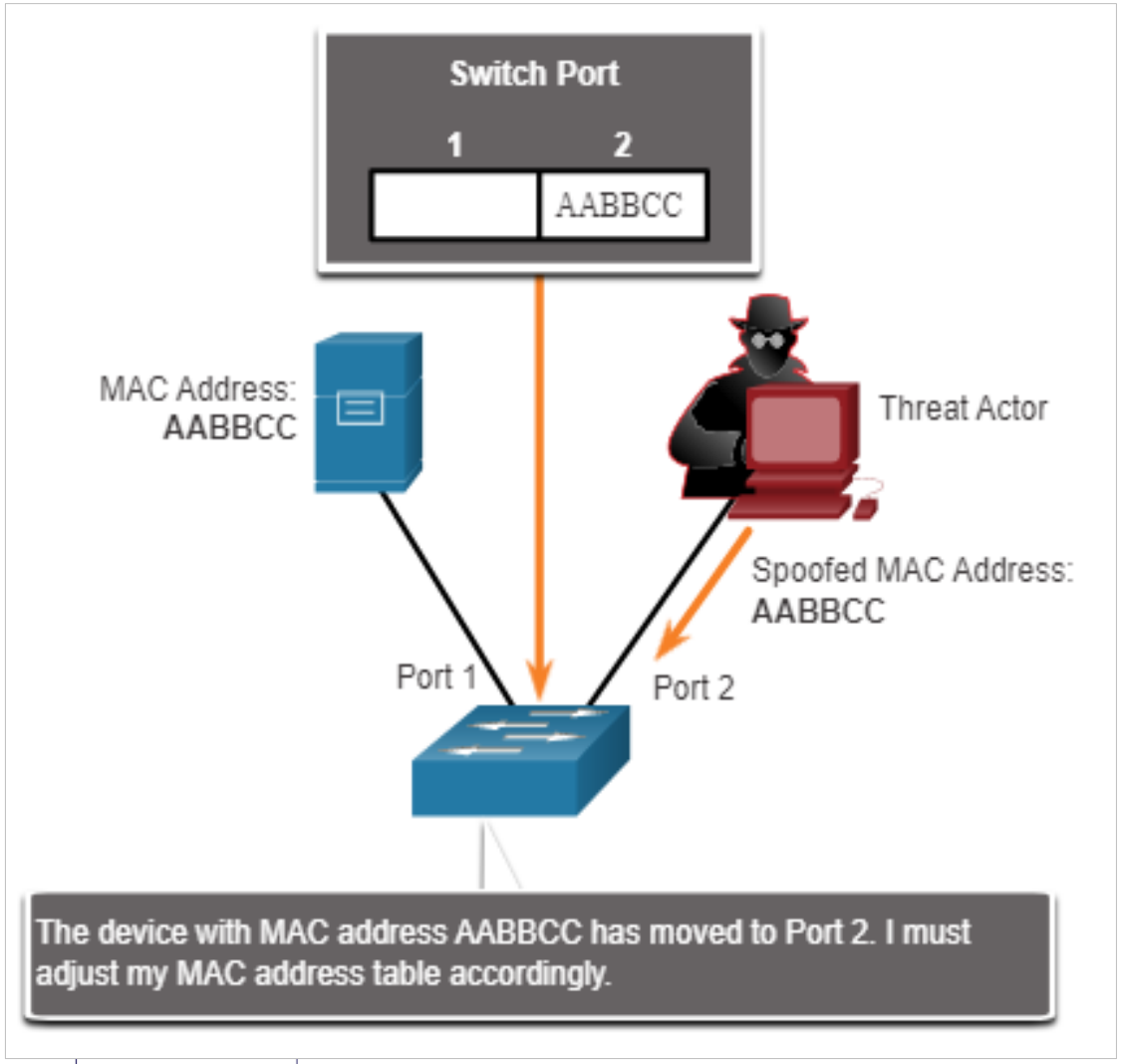
- Útoky falšovania MAC adries (MAC address spoofing) sa používajú vtedy, keď má útočník prístup do vnútornej siete.

- Útočníci zmenia MAC adresu svojho systému tak, aby zodpovedala inej známej MAC adrese, ako je znázornené na obrázku.
- Útočník potom odošle do celej siete rámec s novou MAC adresou.
- Keď prepínač príjme rámec, preskúma zdrojovú MAC adresu.



Address Spoofing Attacks (Pokr.)

- Ako funguje učenie prepínača?
  - prepínač prepíše aktuálnu položku CAM tabuľky
  - a priradí MAC adresu novému portu, ako je znázornené na obrázku.
- Potom prepošle rámce určené pre pôvodný cieľ útočníkovi.
- Ďalším príkladom spoofingu je
  - spoofing aplikácie alebo služby
  - útočník môže do siete pripojiť podvrhnutý DHCP server a vytvoriť tak útok MiTM.



Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Základy počítačových sietí

Ochrana koncových zariadení v LAN a online bezpečnosť (Blok V.)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti vo verejnej správe

doc. Ing. Jozef Papán, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Jozef.Papan@fri.uniza.sk