



Financované  
Európskou úniou  
NextGenerationEU

**PLÁN [OBNOVY]**



MINISTERSTVO  
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA  
A INFORMATIZÁCIE  
SLOVENSKEJ REPUBLIKY



KOMPETENČNÉ CENTRUM  
KYBERNETICKEJ BEZPEČNOSTI  
ŽILINSKEJ UNIVERZITY V ŽILINE

# Úvod k prevádzke elektronických komunikačných systémov

Technické opatrenia (BLOK IV)

**Kurz: Manažér kybernetickej bezpečnosti**

Ing. Matúš Madleňák

**KC KYB UNIZA, <https://kc.uniza.sk/>**

[kcskolenia@uniza.sk](mailto:kcskolenia@uniza.sk)

# Obsah

## 1. Základné koncepty a terminológia

- Čo sú elektronické komunikačné systémy

## 2. Počítačové siete

- Základné princípy
- Princípy sieťových zariadení

## 3. Referenčné modely

- OSI a TCP/IP
- Enkapsulácia/De-enkapsulácia

## 4. Protokoly

- Úloha protokolov
- Hlavné sieťové protokoly

## 5. Mapovanie siete

- Význam
- Nástroje

# Elektrické komunikačné systémy

## Pevné telefónne siete

- Telekomunikačná infraštruktúra založená na metalických alebo optických vedeniach, ktorá umožňuje prenos hlasu a dát medzi pevne pripojenými účastníkmi.



## Mobilné telefónne siete

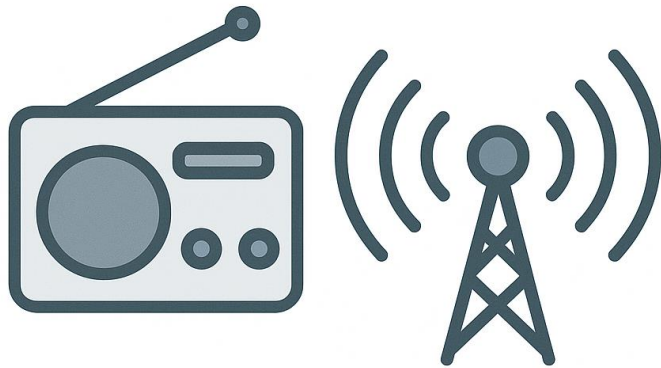
- Bezdrôtové telekomunikačné siete využívajúce rádiové frekvencie (GSM, UMTS, LTE, 5G), ktoré umožňujú hlasovú komunikáciu, SMS a prenos dát prostredníctvom mobilných zariadení.



# Elektrické komunikačné systémy

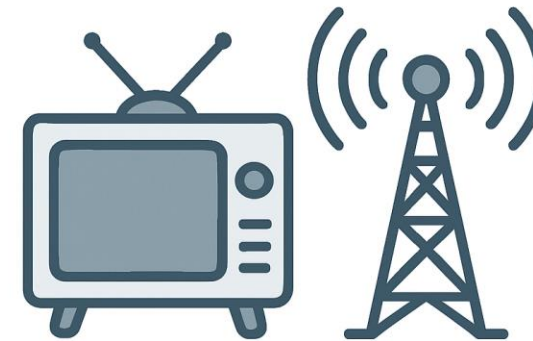
## Rozhlasové vysielanie

- Jednosmerná forma komunikácie, pri ktorej je zvukový signál prenášaný prostredníctvom rádiových frekvencií alebo internetu k širokému publiku.



## Televízne vysielanie

- Masová komunikácia, ktorá sprostredkúva obraz a zvuk prostredníctvom rádiových vln, satelitov, káblových alebo internetových sietí k divákovi.



# Elektrické komunikačné systémy

## Satelitná komunikácia

- Prenos hlasu, dát alebo multimédií cez komunikačné satelity na obežnej dráhe Zeme.
- Používa sa na televízne vysielanie, navigáciu, internetové pripojenie a spojenie vo vzdialených oblastiach.



## Internetové pripojenie

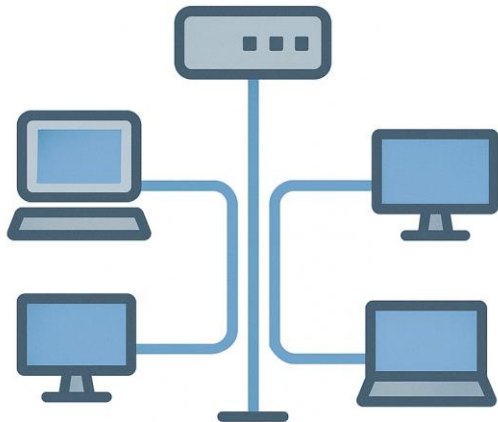
- Služba, ktorá umožňuje používateľovi alebo celej lokálnej sieti prístup do celosvetovej siete Internet prostredníctvom technológií ako DSL, optika, mobilné siete alebo satelit.



# Elektrické komunikačné systémy

## Počítačové siete

- Prepojenie viacerých počítačov/koncových zariadení a zariadení, ktoré si navzájom vymieňajú údaje a zdieľajú zdroje.





# ÚVOD DO POČÍTAČOVÝCH SIETÍ

# Počítačové siete ovplyvňujú naše životy

- V dnešnom svete zohrávajú počítačové siete kľúčovú úlohu v našom **každodennom živote**
- Moderný spôsobu **komunikácie, práce, vzdelávania aj zábavy**
- Sieťové technológie nám umožňujú zostať v **kontakte** s priateľmi a rodinou, **spolupracovať** so vzdialenými kolegami a rýchlo **prístupovať k informáciám** kdekoľvek na svete

# Počítačové siete nás spájajú

- Počítačové siete sú základom digitálnej komunikácie – od **e-mailov** a **sociálnych sietí** až po **videohovory** a **online kurzy**
- Umožňujú ľuďom **pracovať** na diaľku, **študovať** cez internet a okamžite **komunikovať** s kýmkoľvek na svete
- Vďaka sieťam sa môžeme pripojiť k rôznym **službám** – internetovému bankovníctvu, e-shopom či streamovacím platformám.



# Hranice sietí – existujú?

- Počítačové siete majú svoje **logické a fyzické hranice** – tieto hranice určujú, ako sa zariadenia v rámci siete navzájom prepájajú a komunikujú.
- Napríklad **domáca sieť** môže byť oddelená od verejného internetu pomocou smerovača a firewallu, čím sa zabezpečuje ochrana pred hrozbami zvonka.
- Vo všeobecnosti však môžeme povedať, že počítačové siete nemajú takmer žiadne hranice a **môžeme ich nájsť kdekoľvek na svete.**



# Siet'ové komponenty

## Koncové zariadenia

- Sú to zariadenia, ktoré používateľ priamo využíva na komunikáciu v sieti.
  - počítače,
  - smartfóny,
  - tablety,
  - tlačiarne,
  - servery
- Koncové zariadenia majú IP adresy, ktoré im umožňujú adresovať a prijímať dáta.

## Siet'ové zariadenia

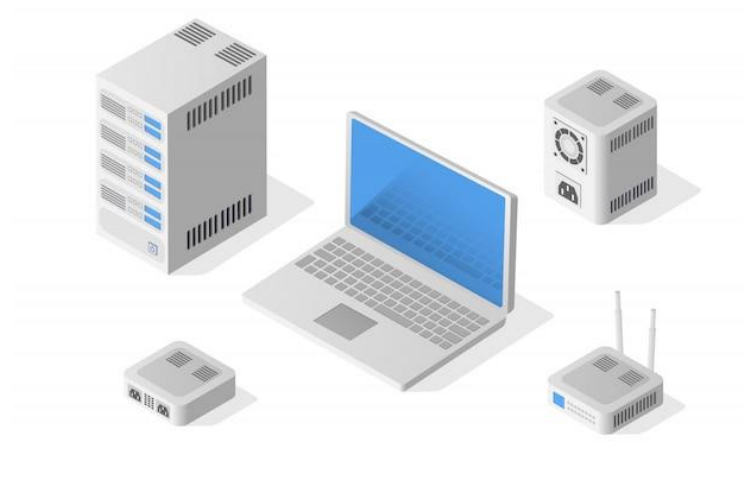
- Sú to zariadenia, ktoré sprostredkujú komunikáciu medzi koncovými zariadeniami.
  - **Smerovač** (router),
  - **prepínač** (switch),
  - **prístupový bod** (access point),
  - **Firewall**,
  - **Multilayer Switch**



# HARDVÉR V POČÍTAČOVÝCH SIĚTÁCH

# Základný hardvér v oblasti počítačových sietí

- Sieťová karta (NIC)
- Prepínač (Switch)
- Smerovač (Router)
- Prístupový bod (Access Point)
- Opakovač (Repeater)
- Firewall (Sieťový bezpečnostný systém)
- Server (webserver, DHCP, DNS, ...)



# Sieťová karta (NIC - Network Interface Card)

- Sieťová karta umožňuje zariadeniam **pripojiť sa k sieti**, pričom konvertuje dáta do formátu, ktorý je vhodný na prenos cez sieťové médium (kábel alebo bezdrôtovo).
- Môžu byť **Ethernetové** (káblové pripojenie) alebo **Wi-Fi** (bezdrôtové pripojenie).
- Každá sieťová karta má jedinečnú **MAC adresu**, ktorá slúži na identifikáciu zariadenia v rámci siete.



# Rozbočovač (hub)

- Rozbočovač (hub) je sieťové zariadenie prvej vrstvy OSI modelu (fyzická vrstva), ktoré slúži na prepojenie viacerých zariadení v lokálnej sieti.
- Keď hub prijme signál (bitový tok) na jednom porte, **bez akejkoľvek inteligencie ho skopíruje na všetky ostatné porty.**
- Všetky pripojené zariadenia tak dostanú rovnaký signál, aj keď je určený iba jednému z nich.



# Prepínač (switch)

- Prepínač slúži na pripojenie viacerých zariadení v **lokálnej sieti (LAN)** a umožňuje im komunikovať.
- Na rozdiel od rozbočovača (hub), prepínač **inteligentne riadi tok dát**, aby zabránil kolíziám a optimalizoval prenos.
- Prepínače operujú na **linkovej vrstve** a smerujú dáta pomocou **MAC adries** zariadení.



# Smerovač (router)

- Smerovač **prepája rôzne siete** a zabezpečuje **smerovanie dát** medzi nimi. Najčastejšie smeruje dáta medzi domácou alebo firemnou sieťou a internetom.
- Zariadenie **analyzuje IP adresy** v rámci prichádzajúcich paketov a rozhoduje, ktorým smerom sa majú dáta odoslať.
- V domácnostiach často kombinuje funkcie smerovača, prepínača a prístupového bodu (Wi-Fi).



# Prístupový bod (Access Point)

- Prístupový bod umožňuje **bezdrôtovým zariadeniam** (smartfóny, laptopy) pripojiť sa k sieti.
- Je to nevyhnutný komponent pre vytváranie **Wi-Fi sietí**.
- Bežne sa používa v domácnostiach, kanceláriách alebo verejných priestoroch na vytváranie Wi-Fi sietí.



# Opakovač (repeater)

- Opakovač **zosilňuje signál** na fyzickej vrstve siete.
- Používa sa na **predĺženie dosahu siete** na väčšiu vzdialenosť.
- Používa sa v miestach, kde káblové alebo bezdrôtové signály nepostačujú na pokrytie požadovanej oblasti, môže opakovač zvýšiť ich dosah.



# Modem

- Modem umožňuje pripojenie k internetu prostredníctvom rôznych technológií (DSL, káblové pripojenie, optické vlákno).
- Modem "**moduluje**" a "**demoduluje**" signály medzi domácou sieťou a poskytovateľom internetového pripojenia.
- **Konvertuje** digitálne signály na analógové signály.
- Typy modemov: **DSL modem, káblový modem, optický modem**
- Často je integrovaný v „domácom smerovači“, ktorý kombinuje Switch, router a modem.



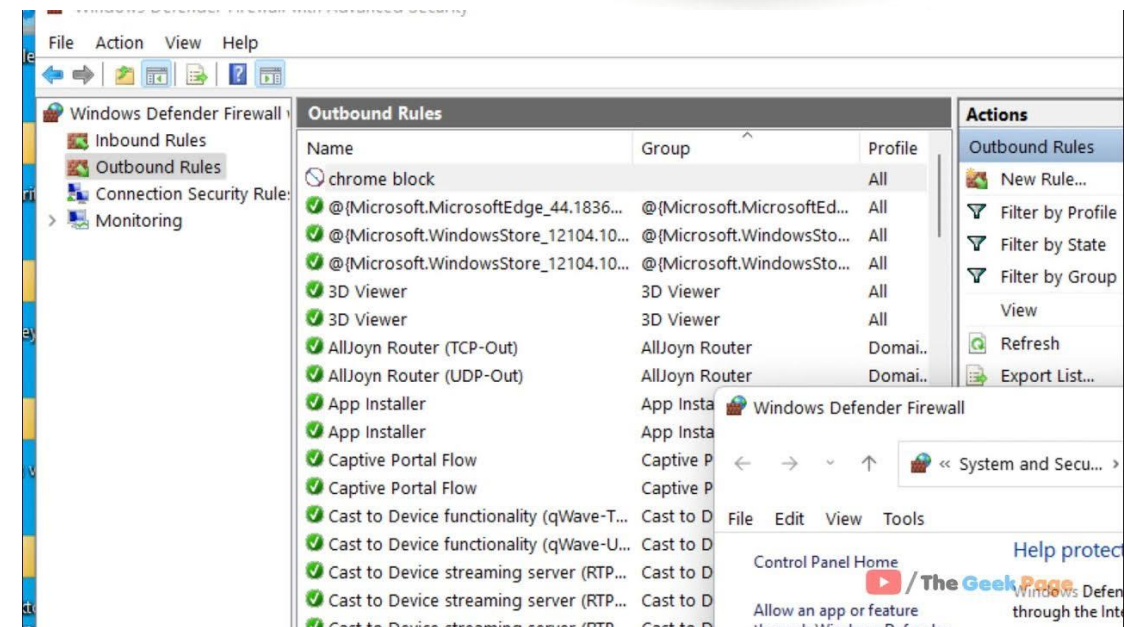
# Firewall

- Slúži na **kontrolu a riadenie** sieťovej premávky na základe definovaných **bezpečnostných pravidiel**.
- Chráni zariadenia a siete pred **neoprávneným prístupom a kybernetickými útokmi**.



## Typy firewallov:

- **Hardvérový firewall:** Zariadenie
- **Softvérový firewall:** Program



# Server (DNS, DHCP, Web)

## DNS server

- DNS server je špecializovaný server, ktorý slúži na **preklad doménových mien na IP adresy** a naopak.
- Keď používateľ zadá URL (napríklad `www.example.com`), DNS server prehľadá svoju databázu a nájde príslušnú IP adresu (napríklad `192.0.2.1`), aby mohol prehliadač nadviazať spojenie so správnym serverom.

## DHCP server

- DHCP server automaticky prideluje **IP adresy a ďalšie sieťové konfiguračné informácie** (ako subnet mask, bránu a DNS servery) zariadeniam pripojeným do siete.
- To umožňuje jednoduchšie a rýchlejšie nastavenie zariadení bez nutnosti manuálneho zasahovania.
- DHCPv4 (IPv4) a DHCPv6 (IPv6)

# Server (DNS, DHCP, Web)

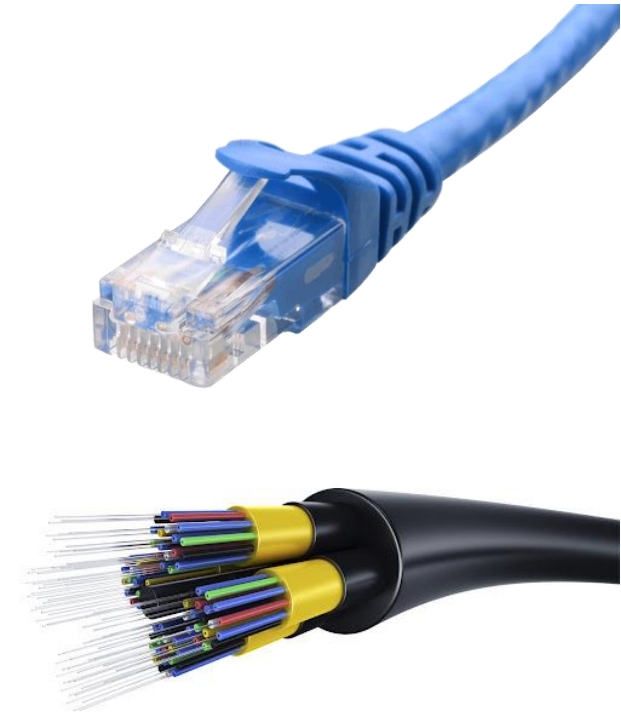
### Webserver:

- Webserver „prevádzkuje“ webové stránky a poskytuje obsah používateľom prostredníctvom **HTTP** (Hypertext Transfer Protocol) alebo **HTTPS** (HTTP Secure).
- Keď používateľ zadá adresu URL do prehliadača, webserver spracuje požiadavku a zasiela požadované webové stránky alebo súbory.



# Sieťové médiá

- Sieťové a koncové zariadenia sú v rámci siete navzájom prepojené pomocou sieťových médií.
- **Metalické káble (Ethernet)** – lacné, ale náchylné na rušenie.
- **Optické vlákna** – vysoká rýchlosť a spoľahlivosť, drahšie riešenie.
- **Bezdrôtové technológie (Wi-Fi, Bluetooth)** – flexibilita, ale nižšia bezpečnosť.





# Typy počítačových sietí

# Typy počítačových sietí

## Malé domáce siete

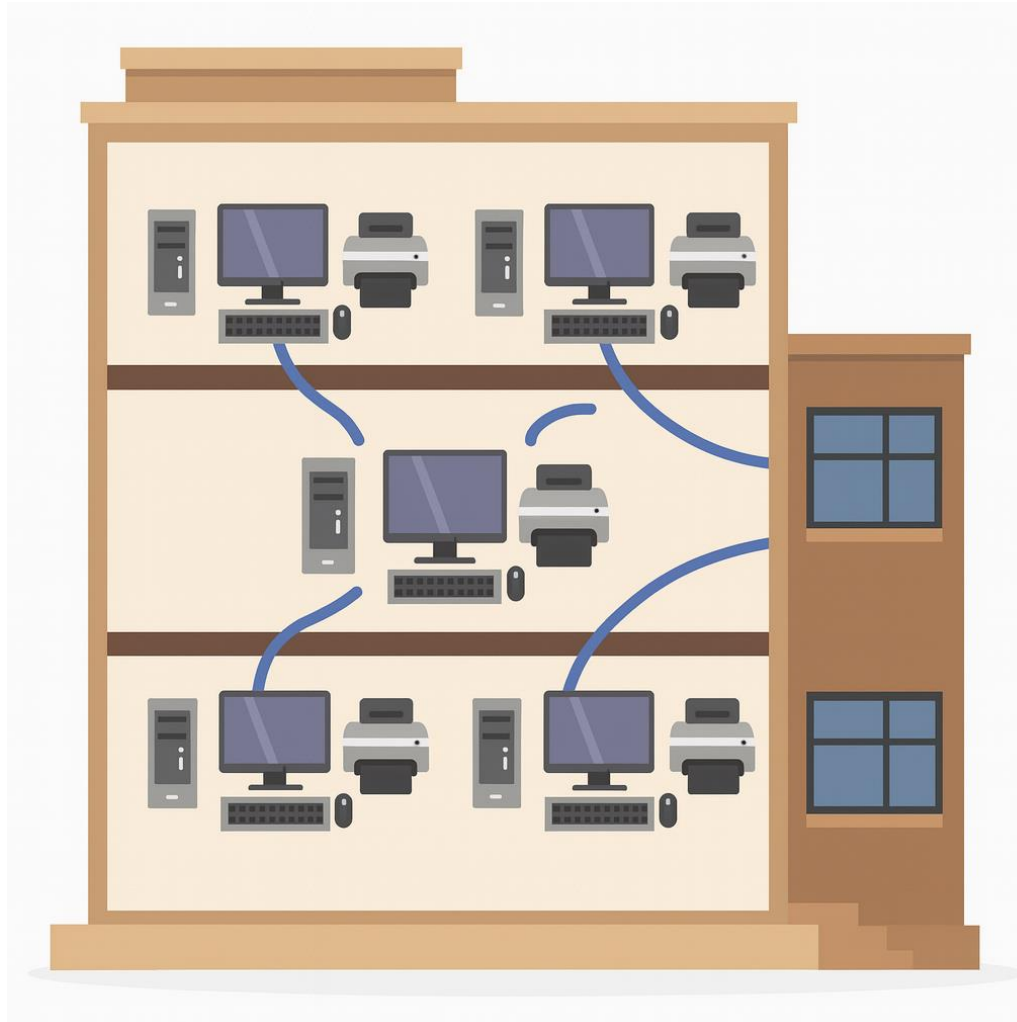


## Malé kancelárske a home office siete (SOHO)



# Typy počítačových sietí

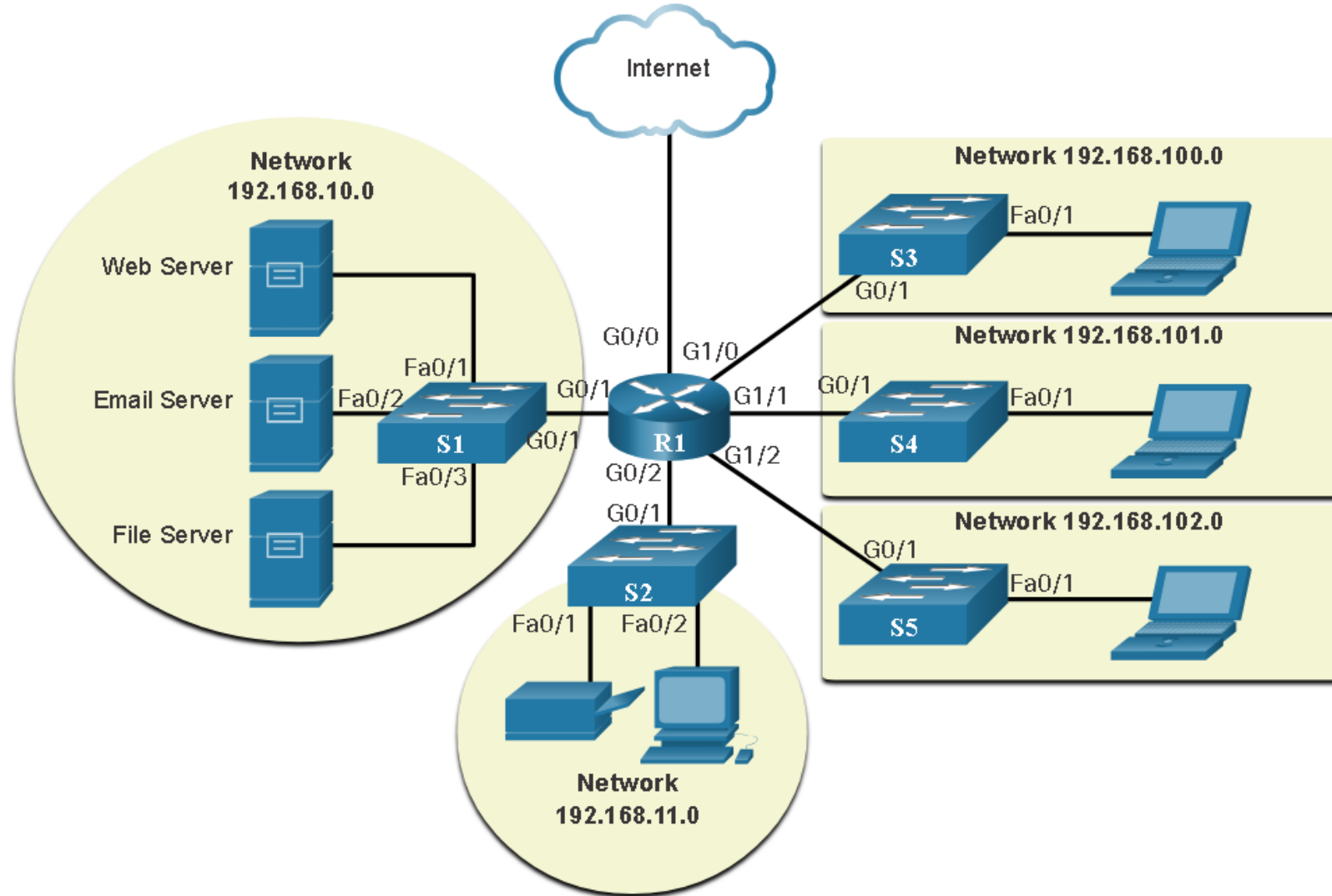
## Stredné až veľké siete



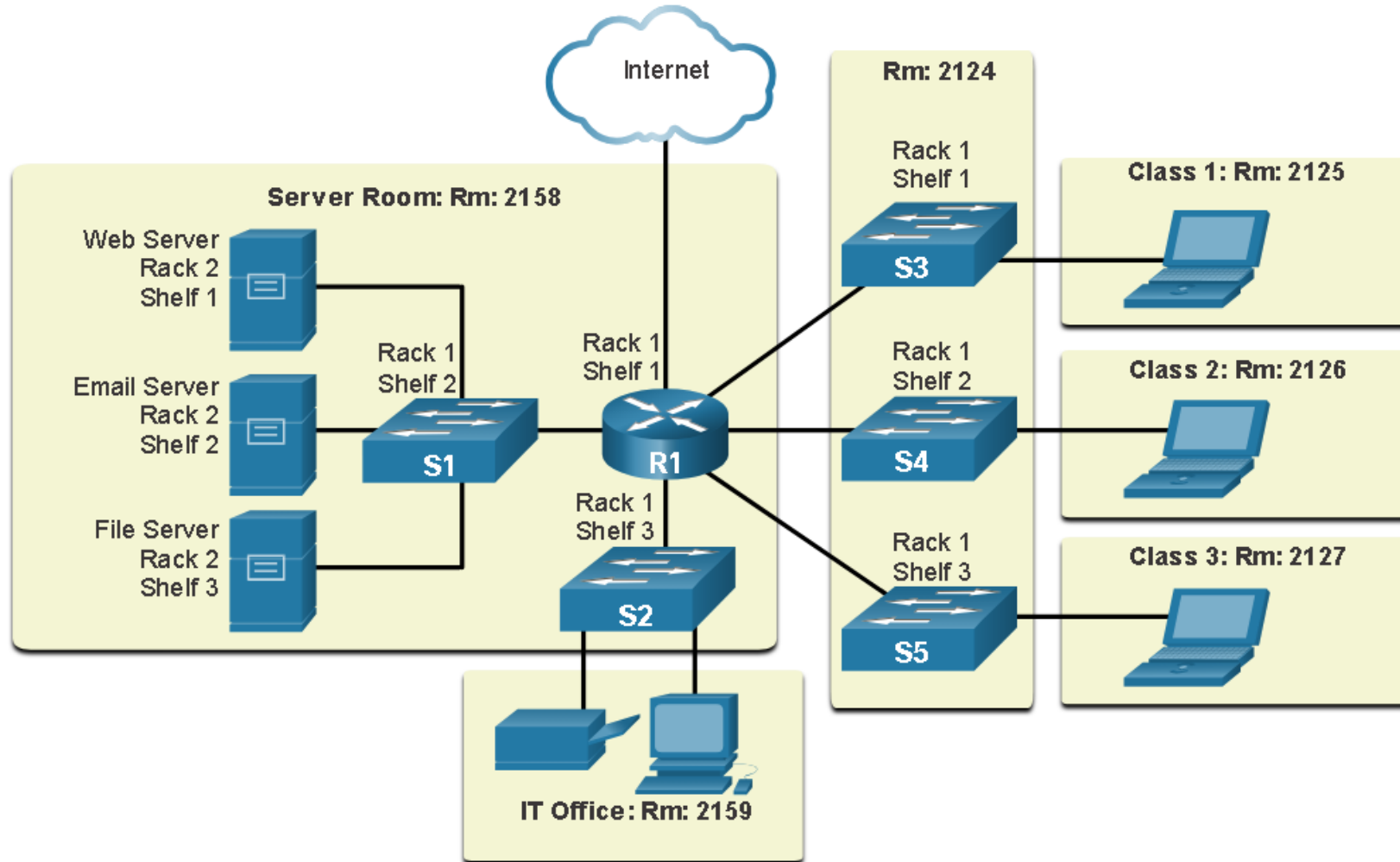
## Celosvetové siete



# Reprezentácia siete – Fyzická topológia



# Reprezentácia siete – Logická topológia



# LAN a WAN

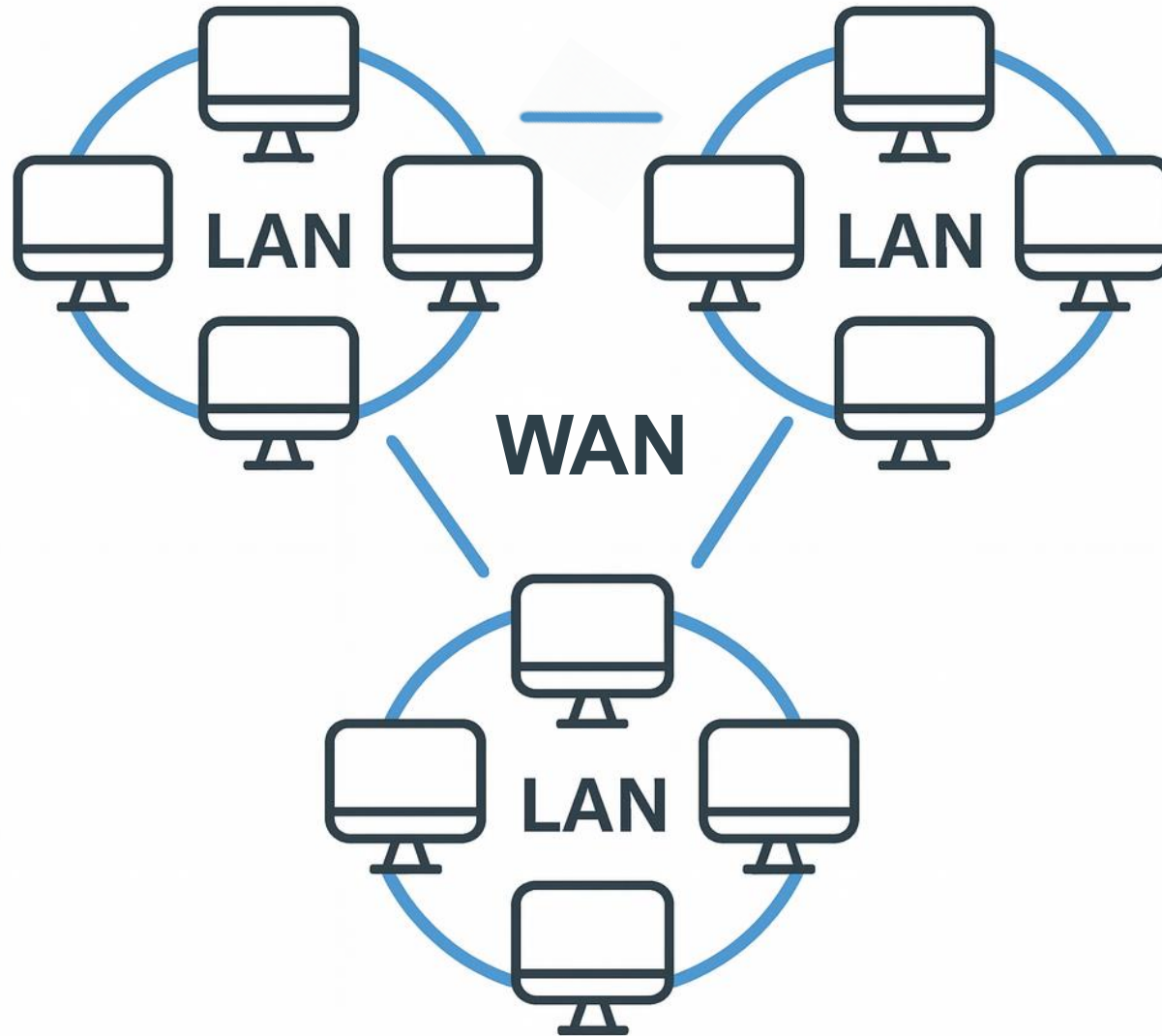
### LAN – Local Area Network:

- Sieť, ktorá poskytuje prístup používateľov a koncových zariadení v malom geografickom priestore
- Domáca sieť,
- Pracovná sieť,
- Jednotlivé oddelenia v rámci budovy,

### WAN – Wide Area Network:

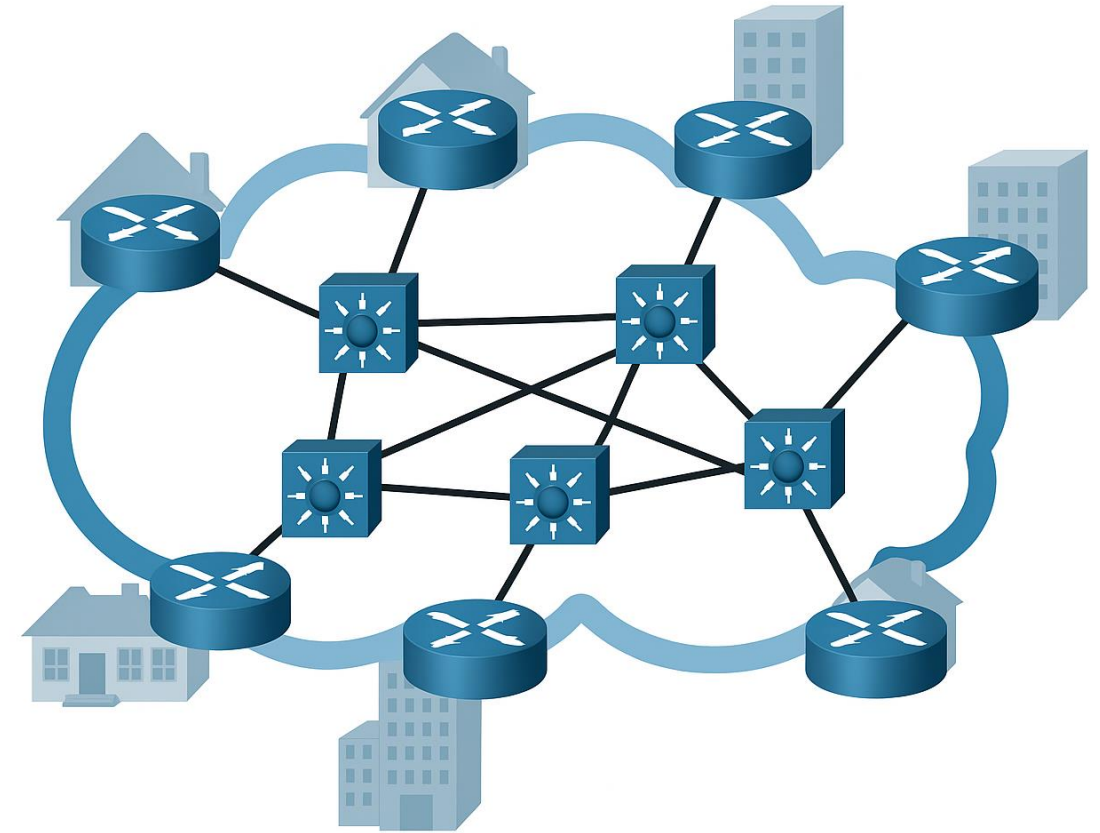
- Sieť, ktorá poskytuje prístup do ďalších sietí, ktoré sa nachádzajú v inom geografickom priestore.
- Zvyčajne sú riadené a vlastnené väčšími spoločnosťami alebo poskytovateľmi internetových služieb.

# LAN a WAN

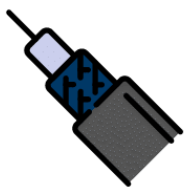


# Internet (internetwork)

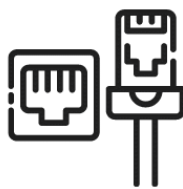
- Internet môžeme definovať ako vzájomné prepojenie:
  - LAN/LAN,
  - WAN/WAN,
  - LAN/WAN.
- Siete môžu byť prepojené metalický, opticky a bezdrôtovo.



Fiber Optic Internet



Cable Broadband



DSL Internet



Satellite Internet



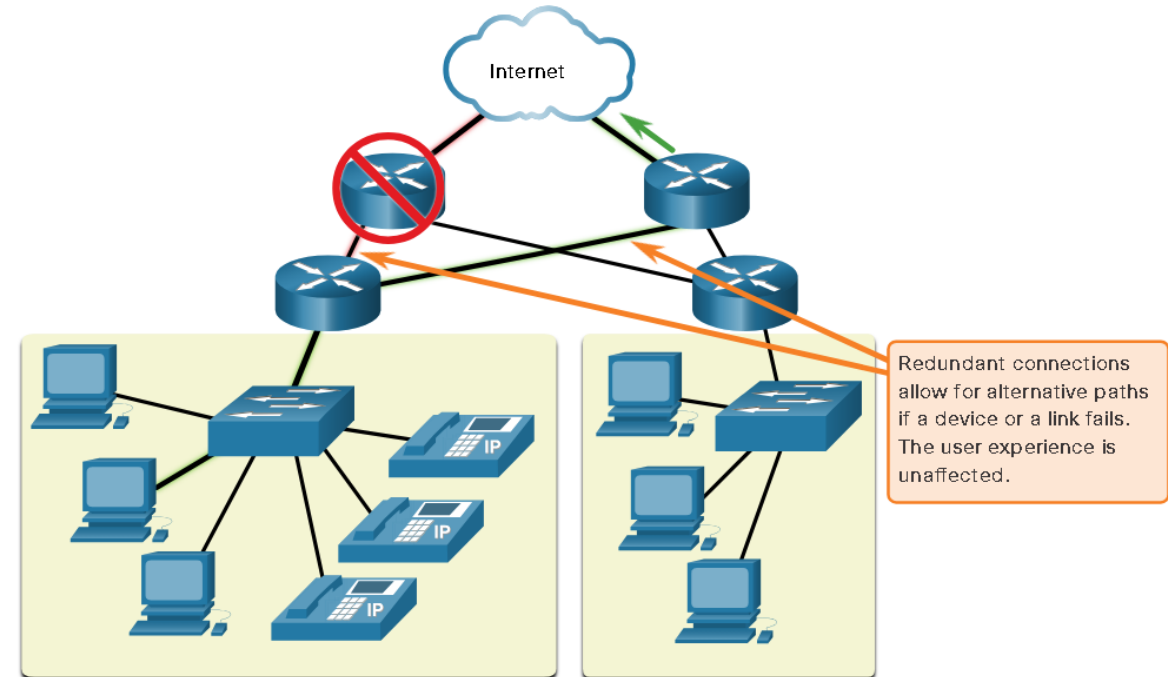
Fixed Wireless Access

# Ideálne vlastnosti počítačovej siete

- Každá dobre navrhnutá sieť by mala mať tieto 4 vlastnosti
  - **Odolnosť voči chybám** - Fault tolerance
  - **Škálovateľnosť** - Scalability
  - **Ohľad na kvalitu služby** - Quality of service
  - **Bezpečnosť** - Security
- Vedieť dobre navrhnúť sieť je otázka veľkých vedomostí a dlhoročných skúseností

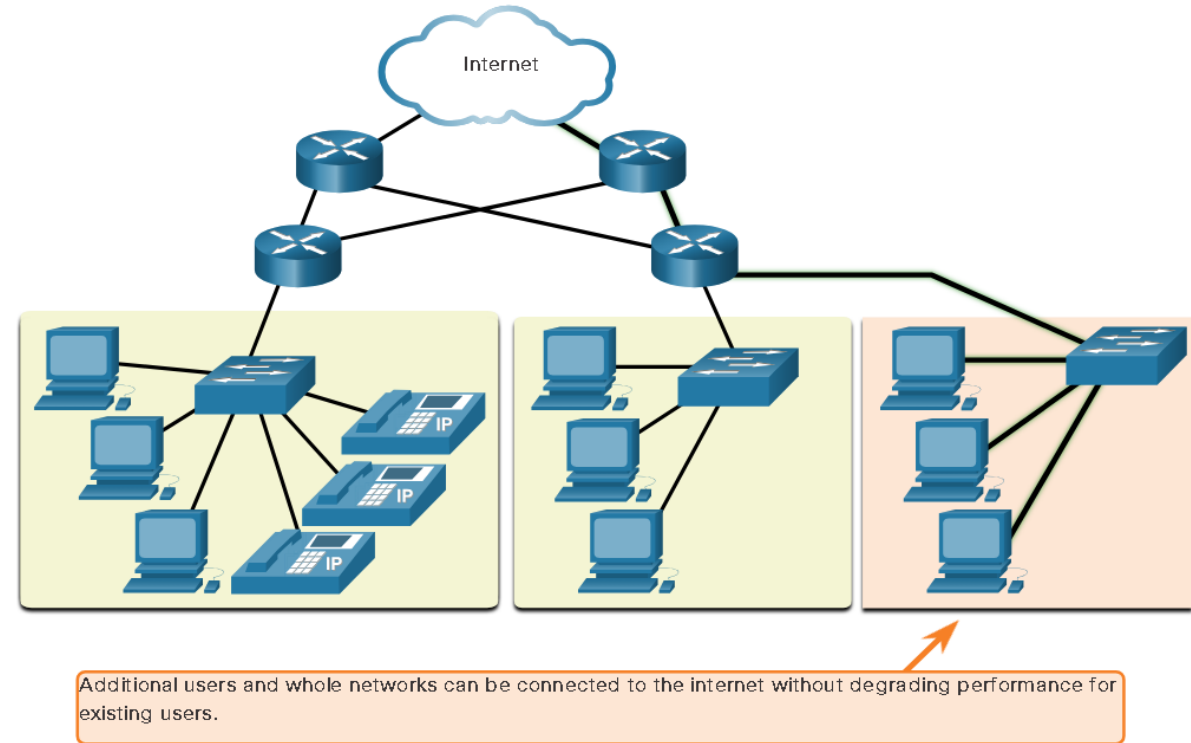
# Odolnosť voči chybám (Fault Tolerance)

- Odolnosť voči chybám je schopnosť siete **efektívne fungovať aj v prípade chýb alebo výpadkov** v komponentoch siete.
- To zahŕňa schopnosť automatického obnovovania po výpadku a minimalizovanie vplyvu chýb na celkový chod siete.
- Tieto siete závisia od viacerých ciest medzi zdrojom a cieľom správy. Ak jedna cesta zlyhá, správy sa okamžite odošlú prostredníctvom inej cesty.
- Mať viac ciest k cieľu je známe ako **redundancia**.



# Škálovateľnosť (Scalability)

- Škálovateľná sieť je taká, ktorá sa dokáže **prispôbiť narastajúcemu počtu používateľov v sieti**
- Robí to hlavne bez zníženia výkonu služieb, ku ktorým majú prístup existujúci používatelia.



## Ohľad na kvalitu služby (Quality of Service - QoS)

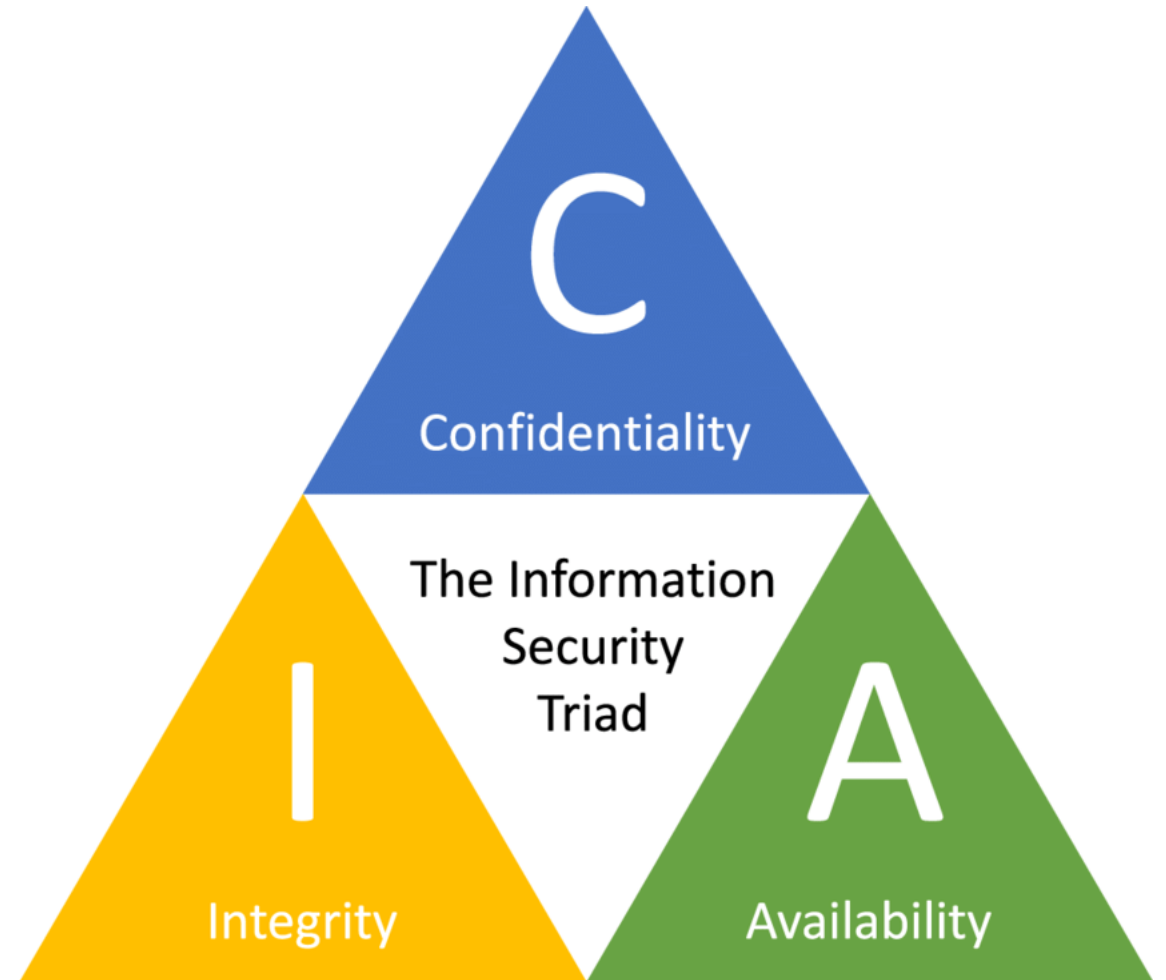
- QoS je súbor techník a mechanizmov v počítačových sieťach, ktoré zabezpečujú, že určité typy dátovej prevádzky majú prednosť a sú prenášané s požadovanou kvalitou.
- Nie všetky dáta majú rovnaké nároky – e-mail znesie oneskorenie, ale videohovor alebo online hra potrebuje nízku latenciu, minimálny jitter a žiadne výpadky.

### Ako to funguje:

- Označovanie prevádzky (napr. VoIP pakety s vyššou prioritou).
- Riadenie frontov a plánovanie (Priority Queuing, Weighted Fair Queuing).
- Vyhradenie šírky pásma pre kritické aplikácie.

## Bezpečnosť (Security)

- **Dôvernosť** – K údajom môžu pristupovať a čítať ich len oprávnení príjemcovia.
- **Integrita** – Zaisťuje používateľom, že informácie neboli zmenené pri prenose zo zdroja do cieľa.
- **Dostupnosť** – Zaisťuje používateľom včasný a spoľahlivý prístup k dátovým službám pre oprávnených používateľov.



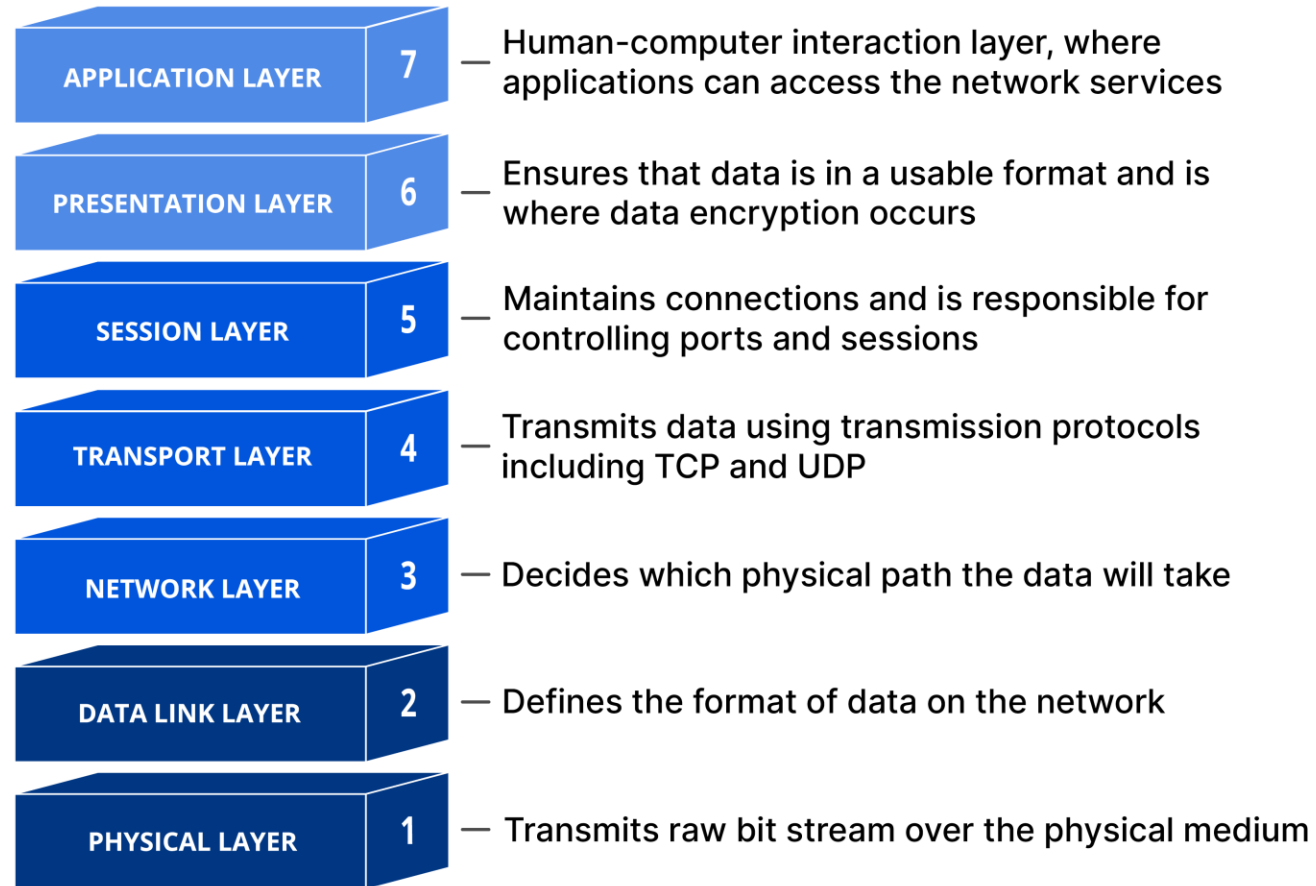
# Kybernetické bezpečnostné hrozby

**AKÁ JE NAJČASTEJŠIA KYBERNETICKÁ  
BEZPEČNOSTNÁ HROZBA?**

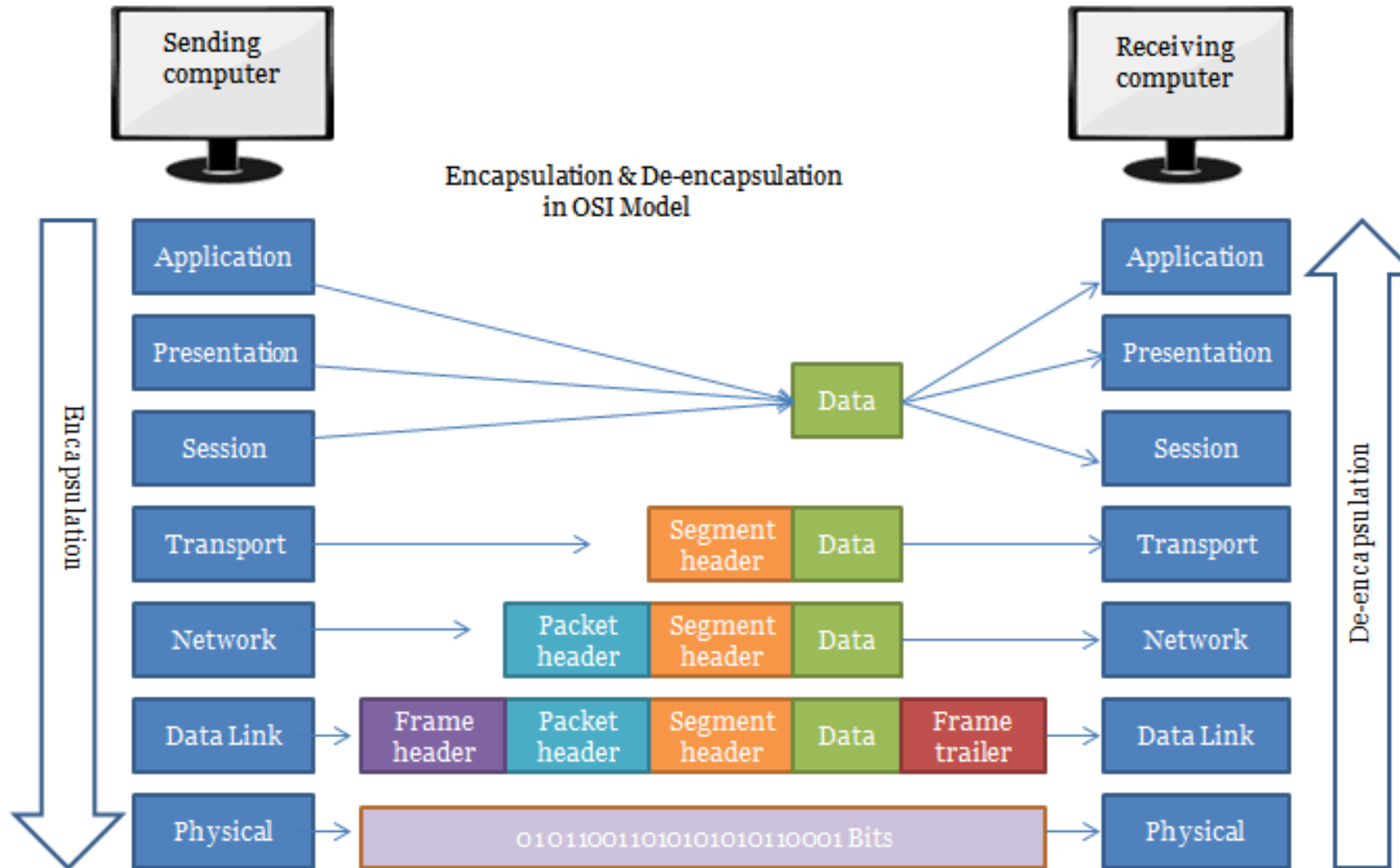


# REFERENČNÉ MODELY

## Referenčné modely



# Referenčné modely



# Protokolové dátové jednotky - Protocol Data Units (PDU)

- PDU (Protocol Data Unit) je jednotka dát, ktorú používa konkrétna vrstva sieťového modelu.
- Každá vrstva používa iný názov pre svoju PDU

Aplikačná

**Dáta**

Prezentačná

**Dáta**

Relačná

**Dáta**

Transportná

**Segment (TCP), Datagram (UDP)**

Sieťová

**Packet**

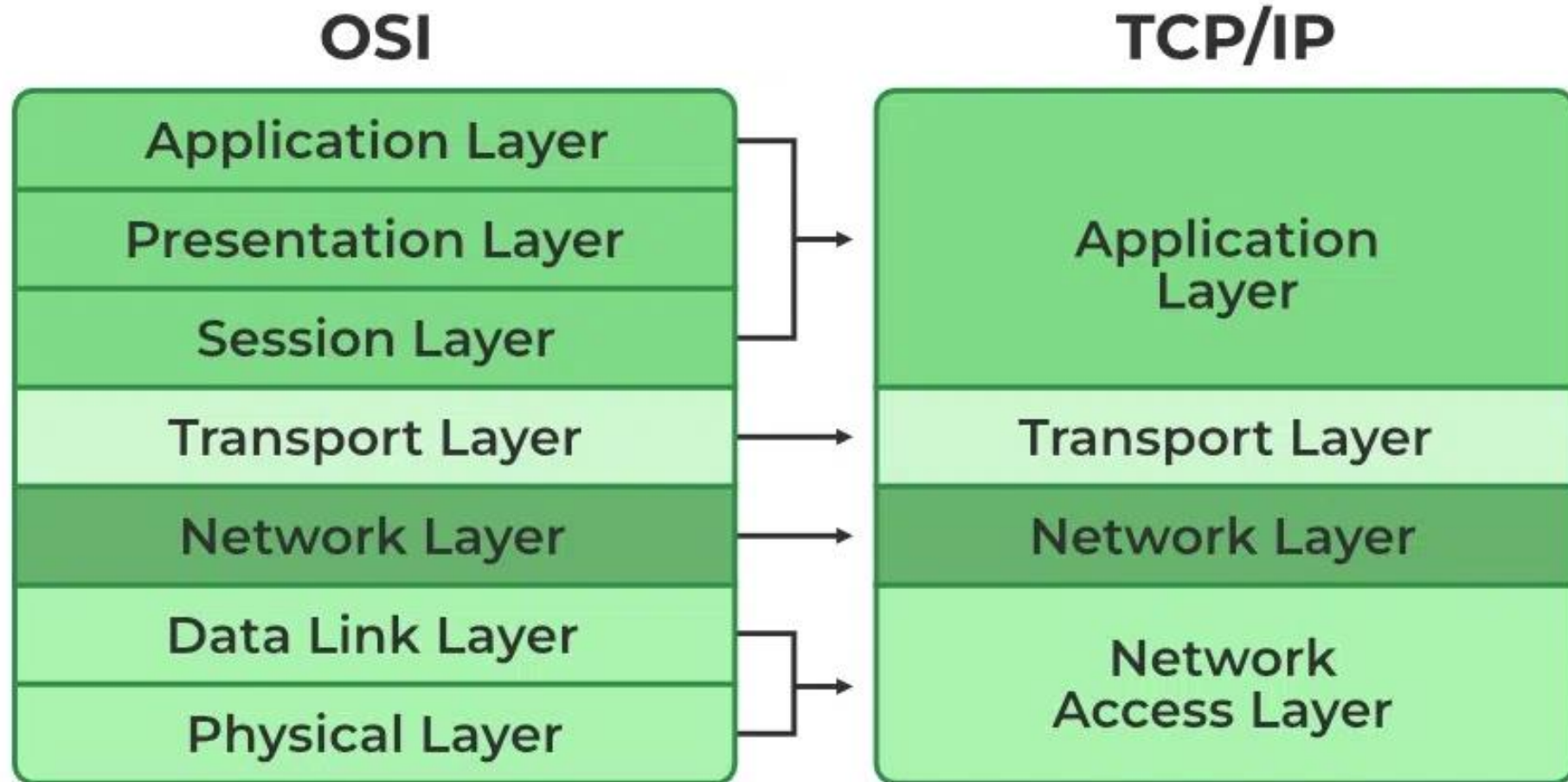
Linková

**Rámec**

Fyzická

**Bity**

# ISO/OSI vs. TCP/IP



# Zapuzdrenie dát - Data Encapsulation

- Dátové zapuzdrenie je proces, pri ktorom sa dáta postupne obalujú vrstvami protokolových informácií, keď sa pohybujú cez sieťový model (OSI model alebo TCP/IP model).
- Tento proces zabezpečuje, že dáta sú správne adresované, prenášané a spracované na prijímacej strane.
- Opakom zapuzdrenia je **rozbalenie dát – De-encapsulation**

# Príklad

### ▪ Aplikačná vrstva

- Používateľ napíše e-mail v e-mailovom klientovi (napr. Outlook, Gmail).
- E-mail je len obyčajný text, ktorý aplikácia spracuje a pripraví na odoslanie.

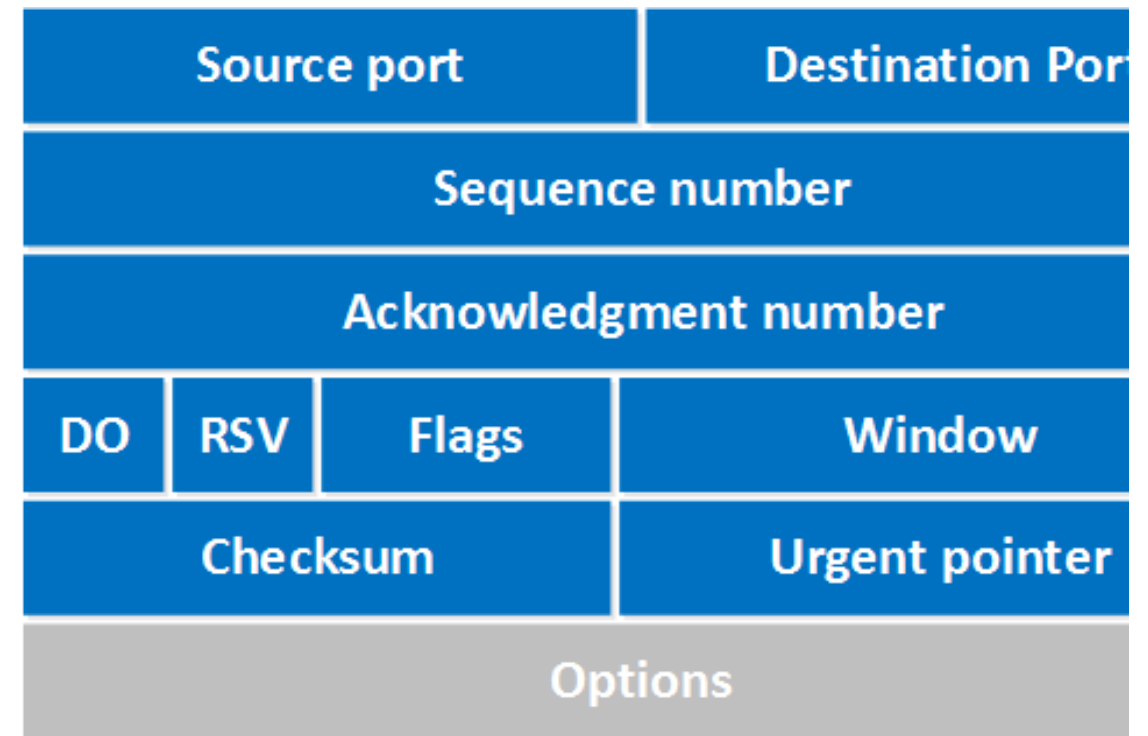
### • Príklad dát:

- **Od:** user1@example.com
- **Komu:** user2@example.com
- **Predmet:** Stretnutie  
**Obsah:** Ahoj, zajtra o 10:00 máme schôdzku.

## Príklad

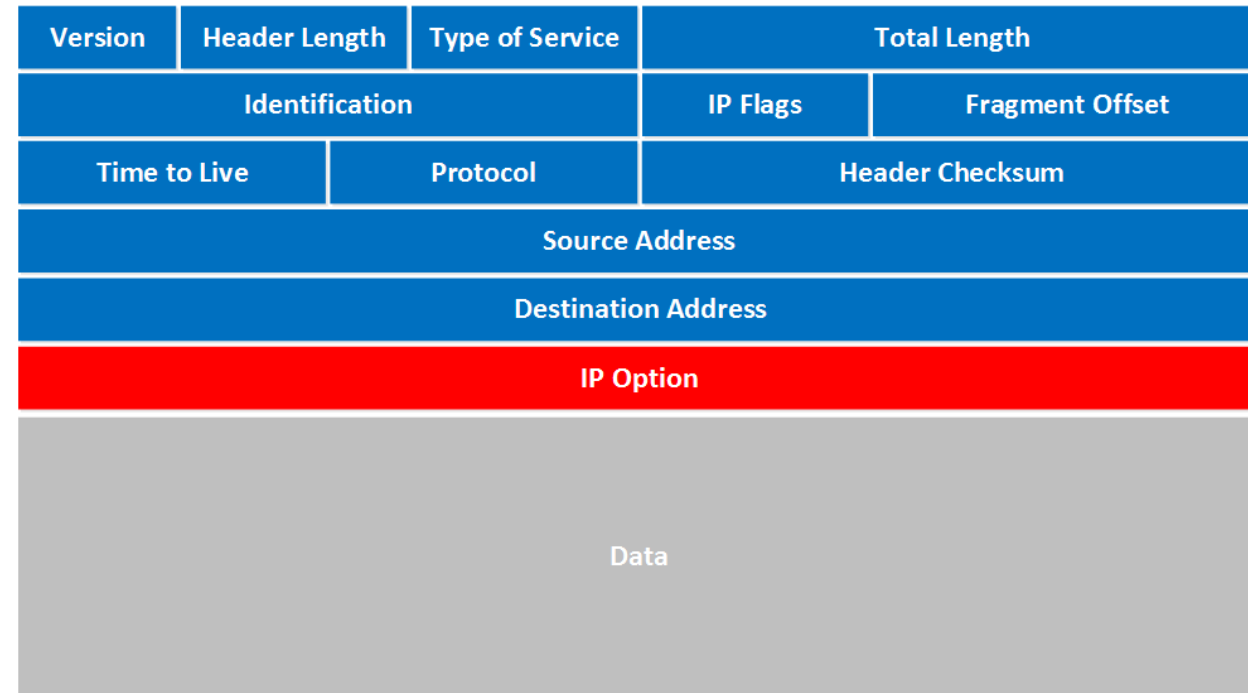
### ▪ Transportná vrstva

- Dáta sú rozdelené na segmenty (ak sú príliš veľké).
- Ak sa používa TCP, na transportnej vrstve sa pridá TCP hlavička



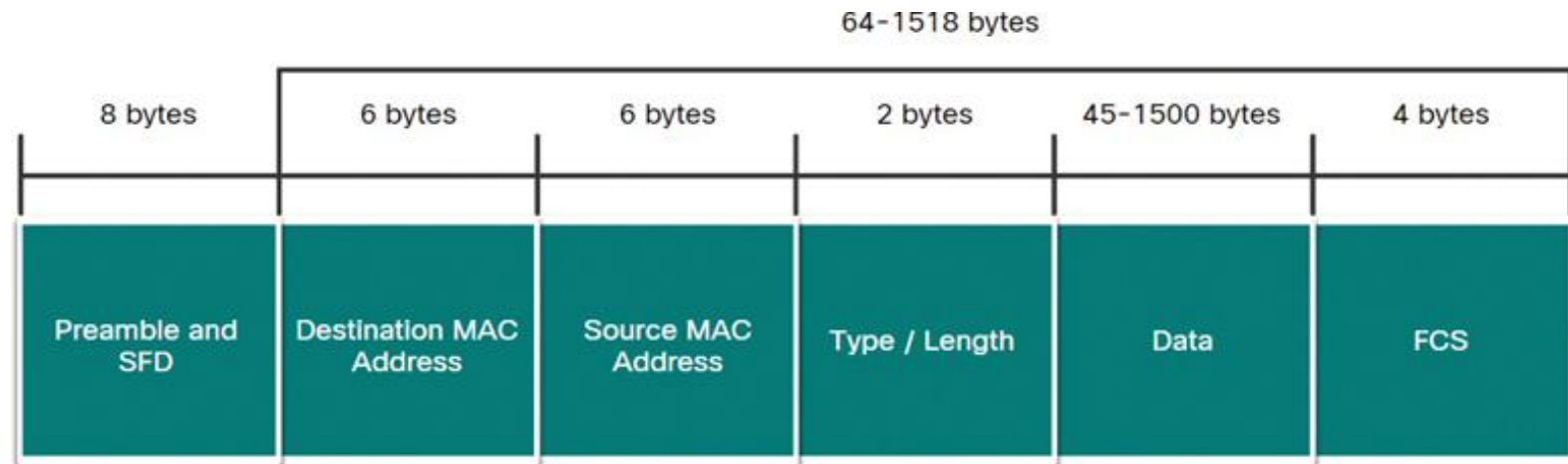
## Príklad

- **Sieťová vrstva**
- TCP segment sa vloží do IP paketu.
- Pridáva sa IP hlavička



## Príklad

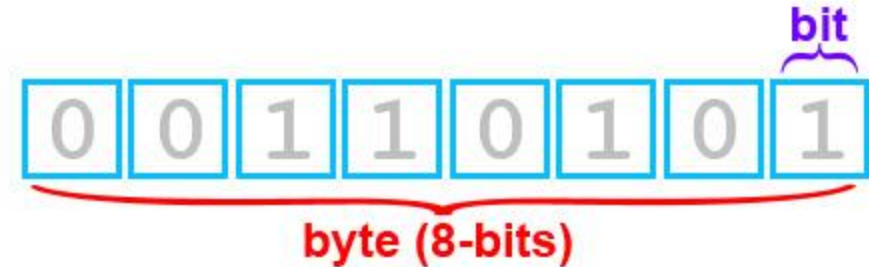
- **Dátová linková vrstva**
  - IP paket je vložený do rámca (Frame), ktorý sa používa na fyzickú komunikáciu.
  - Pridáva sa Ethernet hlavička



## Príklad

### ▪ Fyzická vrstva

- Ethernet rámec je premenený na elektrické signály, rádiové vlny alebo svetelné impulzy a poslaný cez sieť.
- Pridáva sa Ethernet hlavička



## Zhrnutie

Vrstva (TCP/IP)	Názov dát (PDU)	Pridaná hlavička
Aplikačná	Dáta	Žiadna
Transportná	Segment (TCP/UDP)	TCP alebo UDP hlavička
Sieťová	Paket (IP Packet)	IP hlavička
Linková	Rámec (Ethernet Frame)	Ethernet hlavička
Fyzická	Bity (Bits)	Dáta v podobe signálov

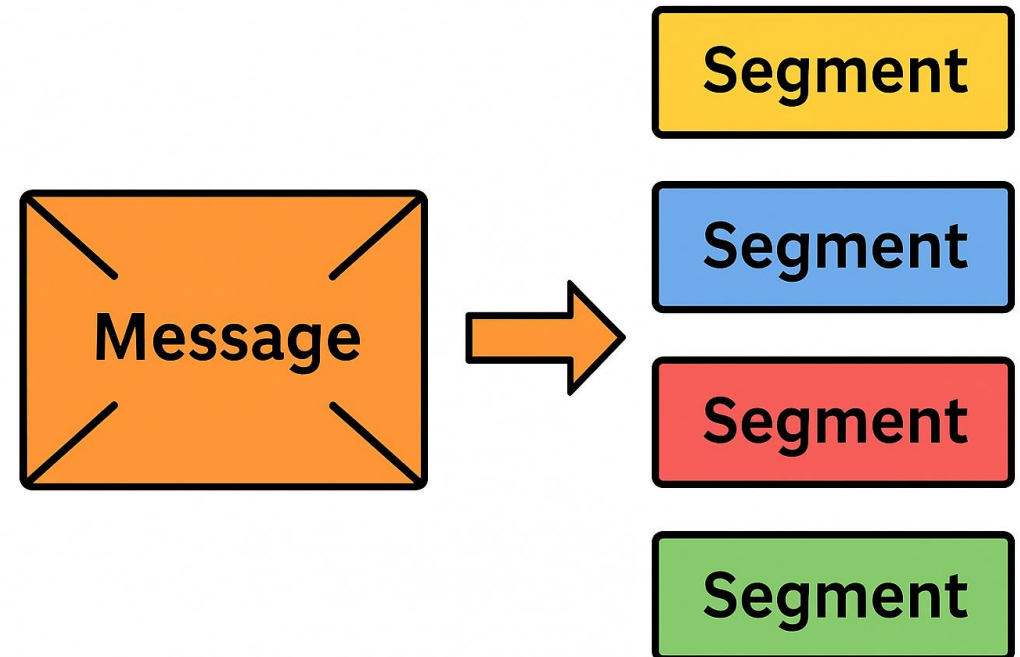
# UKÁŽKA - WIRESHARK

# Ukážka – Wireshark

- Otvorte Wireshark
- Otvorte stránku: <http://testphp.vulnweb.com/login.php>
- Zadajte fiktívne prihlasovacie meno a heslo
- Analyzujte HTTP (TCP port 80) pomocou Wireshark

# Segmentácia správ - Segmentation

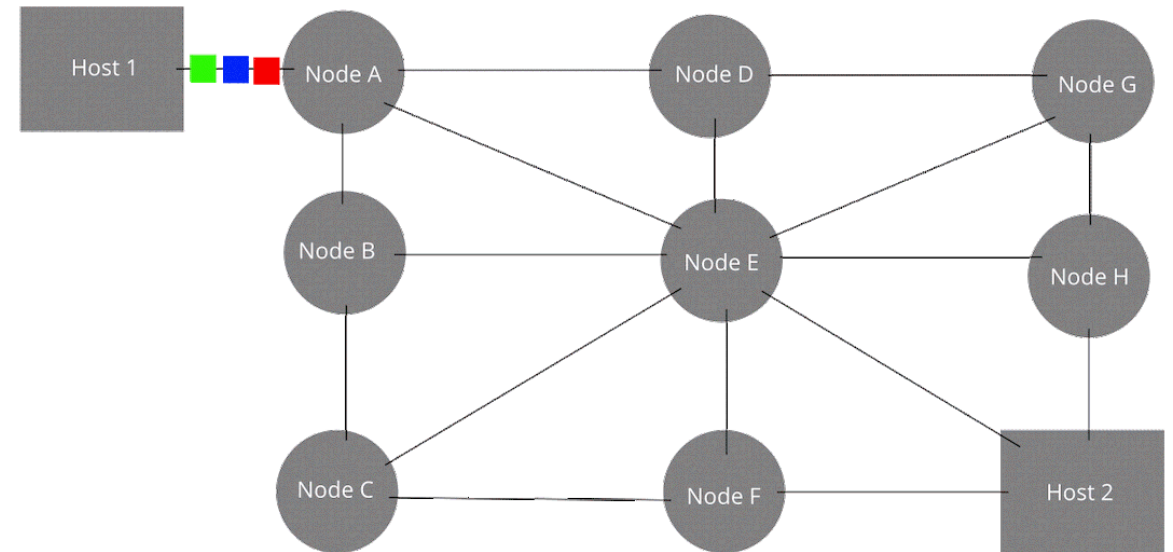
- Keď sa veľké súbory alebo správy prenášajú cez sieť, sú rozdelené na **menšie časti - segmenty**, aby mohli byť efektívne spracované.
- Každá sieťová technológia má **maximálnu veľkosť rámca** (MTU - Maximum Transmission Unit), ktorú môže preniesť naraz.
- Ak sú dáta väčšie, musia byť rozdelené.



# Sekvencovanie - Sequencing

- Každému segmentu je priradené **číslo sekvencie**, aby mohol byť na prijímacej strane správne poskladaný.
- Ak sa niektorý segment **stratí alebo príde v nesprávnom poradí**, prijímateľ môže požiadať o jeho **opätovné odoslanie**.
- TCP je zodpovedné za **sekvencovanie** jednotlivých segmentov

The original message is **Green, Blue, Red**.





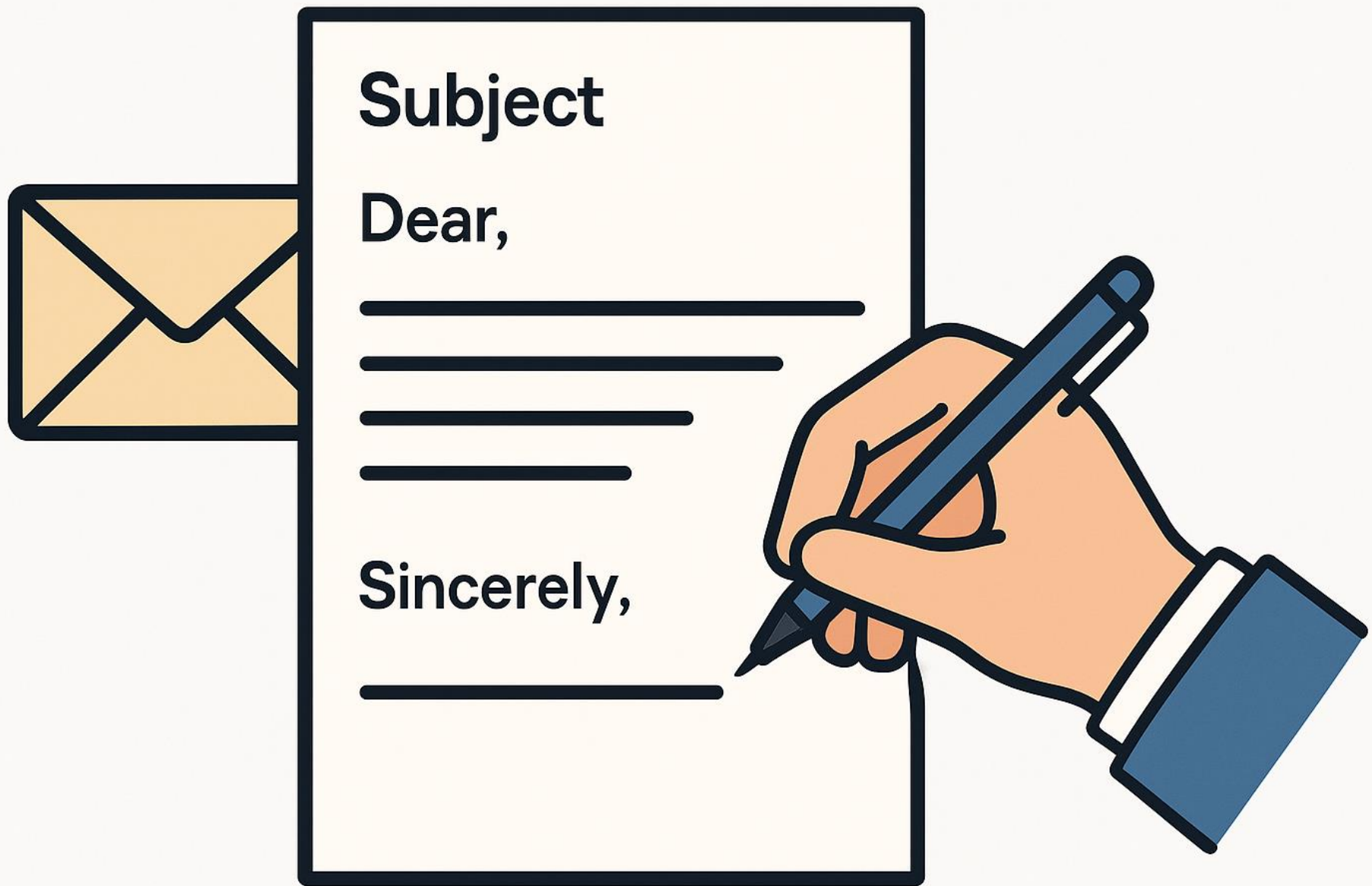
# PROTOKOLY

# Komunikácia

- Aby elektronické komunikačné systémy fungovali efektívne a spoľahlivo, musia sa riadiť presne definovanými pravidlami.
- Tieto pravidlá sa nazývajú komunikačné protokoly a predstavujú štandardizované postupy, ktoré určujú, ako budú zariadenia medzi sebou komunikovať.
- Bez protokolov by bol prenos dát chaotický – každé zariadenie by používalo iný formát, iný spôsob adresovania a kontrolovania správnosti.
- V takom prostredí by spolupráca medzi rôznymi výrobcami, sieťami a aplikáciami nebola možná.

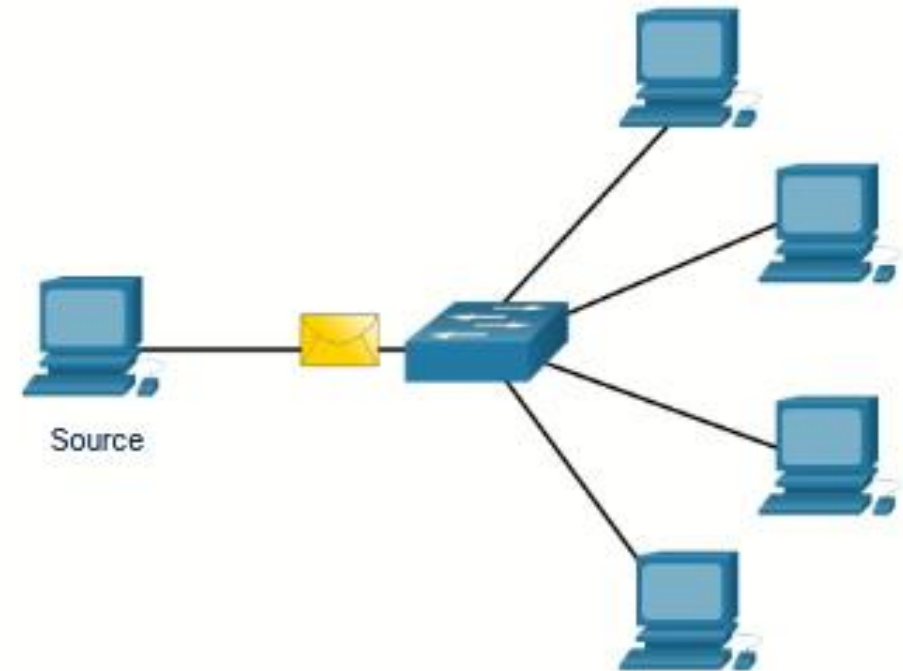
# Úloha protokolov v komunikácii

- **Formát dát** – určuje štruktúru správy a poradie polí (napr. rámec Ethernet, hlavička IP).
- **Časovanie** – definuje pravidlá odosielania, prijímania a časové limity (napr. TCP time-out, Wi-Fi intervaly).
- **Rozdelenie dát na menšie časti** – veľké správy sa fragmentujú na pakety alebo rámce (napr. TCP segmentácia, IP fragmentácia).
- **Adresovanie** – zabezpečuje identifikáciu odosielateľa a prijímateľa (napr. MAC adresa, IP adresa).
- **Riadenie toku dát** – chráni prijímača a sieť pred zahltením (napr. TCP window, congestion control).
- **Kontrola chýb** – zisťuje alebo opravuje chyby prenosu (napr. CRC, kontrolný súčet).
- **Opätovné zostavenie dát** – skladá prijaté časti do pôvodnej správy (napr. sekvenčné čísla v TCP).
- **Spôsob potvrdenia prijatia dát** – určuje mechanizmus potvrdení a opakovaných prenosov (napr. ACK/NACK, TCP ACK).



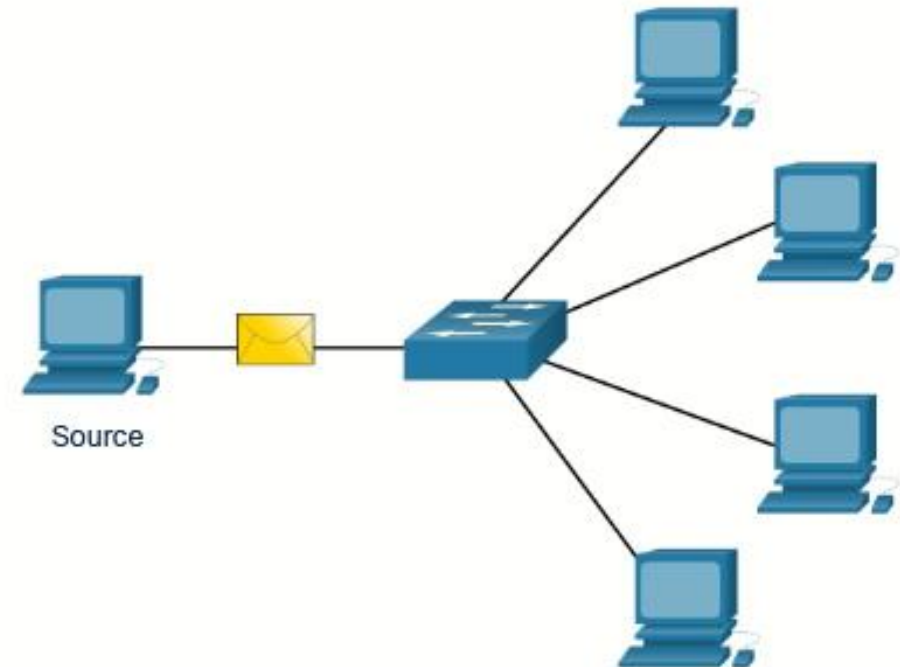
# Možnosti doručovania správ

- **Unicast** – správa sa posiela jednému konkrétnemu zariadeniu.
- **Multicast** – správa sa posiela skupine zariadení.
- **Broadcast** – správa sa posiela všetkým zariadeniam v sieti.



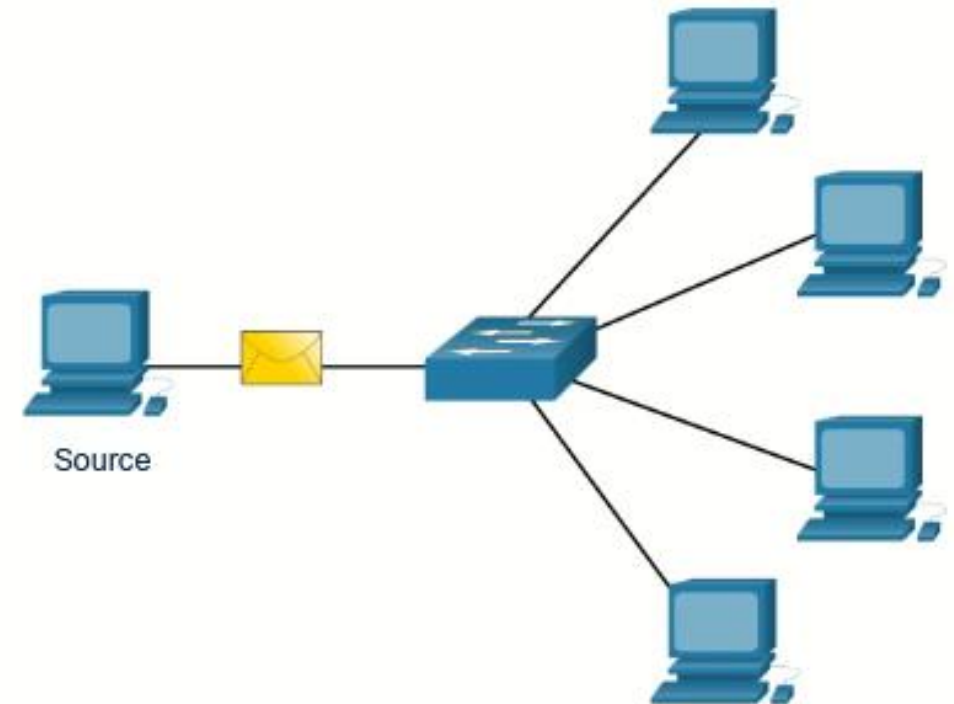
# Možnosti doručovania správ

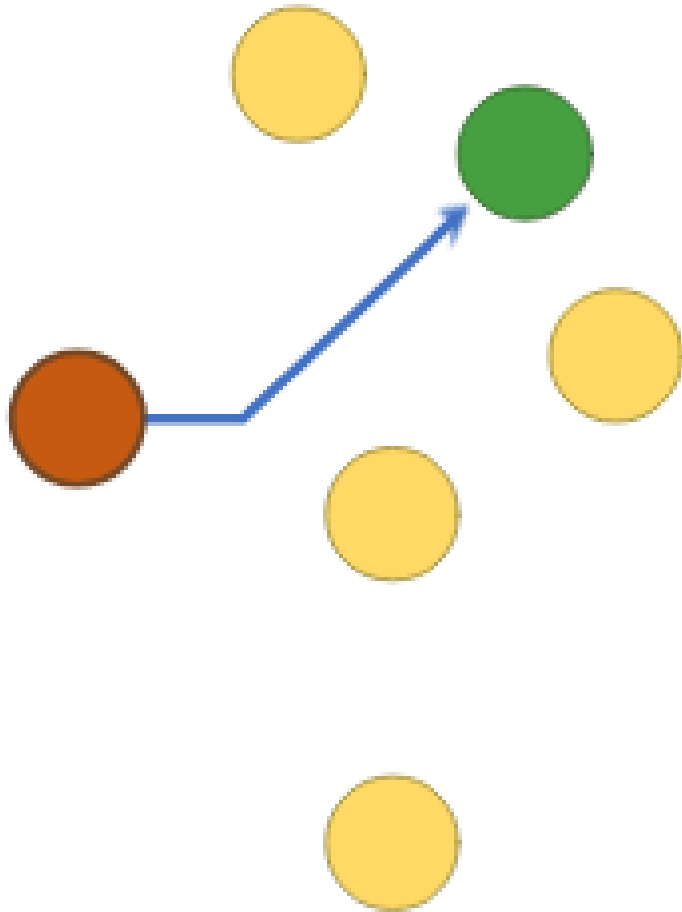
- **Unicast** – správa sa posiela jednému konkrétnemu zariadeniu.
- **Multicast** – správa sa posiela skupine zariadení.
- **Broadcast** – správa sa posiela všetkým zariadeniam v sieti.



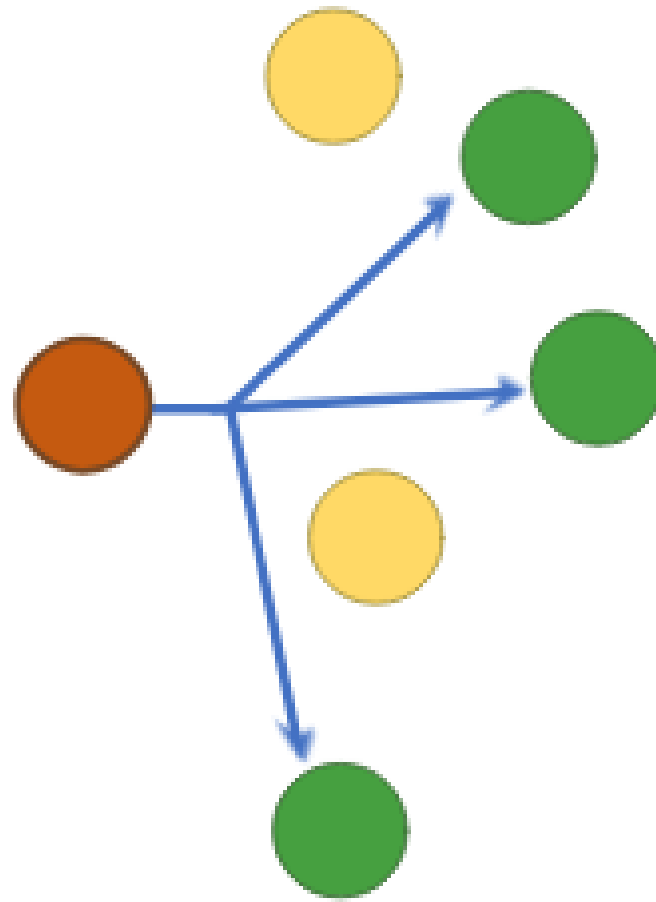
# Možnosti doručovania správ

- **Unicast** – správa sa posiela jednému konkrétnemu zariadeniu.
- **Multicast** – správa sa posiela skupine zariadení.
- **Broadcast** – správa sa posiela všetkým zariadeniam v sieti.

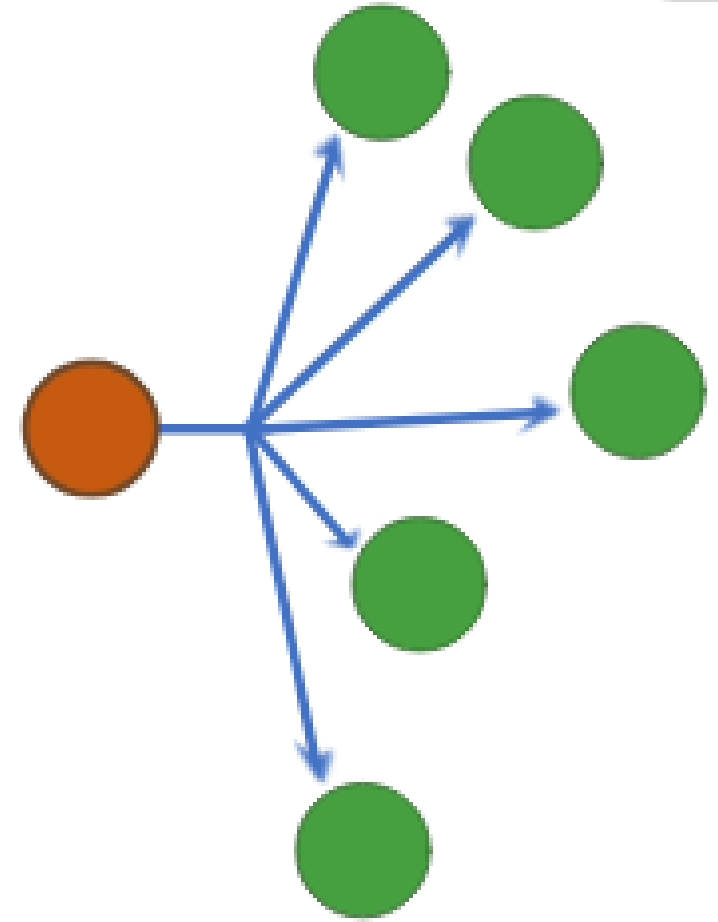




**Unicast**



**Multicast**



**Broadcast**

# Prehľad sieťových protokolov

## LINKOVÁ VRSTVA (LAYER 2)

- **Ethernet (IEEE 802.3):** základná technológia drôtových LAN; definuje rámce a spôsob komunikácie cez kábel.
- **Wi-Fi (IEEE 802.11):** bezdrôtový prenos v lokálnych sieťach, zabezpečený (WPA2/WPA3).
- **PPP (Point-to-Point Protocol):** prenos dát cez sériové linky, často pri pripojení k poskytovateľovi.

## Sieťová vrstva (Layer 3)

- **IP (Internet Protocol, IPv4/IPv6):** poskytuje adresovanie a smerovanie paketov naprieč sieťami.
- **ICMP (Internet Control Message Protocol):** diagnostické správy a testy (napr. ping).
- **ARP (Address Resolution Protocol):** prevádza IP adresu na MAC adresu v lokálnej sieti.
- **NDP (Neighbor Discovery Protocol):** IPv6 ekvivalent ARP, rieši aj autokonfiguráciu.

# Prehľad sieťových protokolov

## TRANSPORTNÁ VRSTVA (LAYER 4)

- **TCP (Transmission Control Protocol):** spoľahlivý prenos dát s potvrdeniami, používaný pri webe, e-maile, súboroch, FTP, SSH.
- **UDP (User Datagram Protocol):** rýchly, nespoľahlivý prenos, vhodný na streaming, hovory, online hry, VoIP, DNS, DHCP.

## RELAČNÁ VRSTVA (LAYER 5)

- **SIP** - Protokol na nadväzovanie, správu a ukončenie multimedialných relácií – VoIP.
- **NetBIOS** - Umožňuje aplikáciám na rôznych počítačoch komunikovať v lokálnej sieti bez ohľadu na to, aký hardvér alebo OS používajú.

# Prehľad sieťových protokolov

## Prezentačná vrstva (Layer 6)

- **TLS/SSL** – šifrovanie komunikácie (HTTPS, VPN).
- **JPEG, MP3, GIF, MPEG** – kódovanie multimédií (nie sú sieťové protokoly, ale fungujú na prezentačnej úrovni).

# Prehľad sieťových protokolov

## APLIKAČNÁ VRSTVA (LAYER 7)

- **HTTP/HTTPS (Hypertext Transfer Protocol):** komunikácia webových stránok; HTTPS je verzia so šifrovaním (TLS).
- **DNS (Domain Name System):** prevádza názvy domén (napr. [www.uniza.sk](http://www.uniza.sk))
- **DHCP (Dynamic Host Configuration Protocol):** automatické pridelovanie IP adries a nastavení zariadeniam.
- **SMTP (Simple Mail Transfer Protocol):** odosielanie e-mailov.
- **IMAP/POP3:** prijímanie e-mailov (IMAP ponecháva správy na serveri, POP3 sťahuje lokálne).
- **FTP (File Transfer Protocol):** prenos súborov medzi klientom a serverom (dnes často nahradený SFTP/FTPS).
- **SSH (Secure Shell):** bezpečný prístup na diaľku k zariadeniam a serverom.
- **LDAP (Lightweight Directory Access Protocol):** prístup k adresárovým službám (správa používateľov, oprávnení).

# Prehľad sieťových protokolov

## SMEROVACIE PROTOKOLY (ROUTING PROTOCOLS)

- **RIP (Routing Information Protocol)**
- **IGRP (Interior Gateway Routing Protocol)**
- **EIGRP (Enhanced Interior Gateway Routing Protocol)**
- **OSPF (Open Shortest Path First)**
- **BGP (Border Gateway Protocol)**

# Funkcie sieťových protokolov

## Addressing (Adresovanie)

- Určuje jedinečné identifikátory zariadení v sieti, aby bolo možné správne smerovať a doručovať dáta medzi odosielateľom a príjemcom.
- Príkladom sú IP adresy.

## Reliability (Spoľahlivosť)

- Zabezpečuje, že dáta sú doručené úplne a bez chýb. Používa mechanizmy, ako napríklad potvrdenie prijatia (ACK) a opätovné odoslanie stratených paketov (retransmisia).
- Príkladom je TCP.

# Funkcie sieťových protokolov

## Flow Control (Riadenie toku)

- Reguluje rýchlosť odosielania dát tak, aby odosielateľ nepreťažil príjemcu.
- Príkladom je TCP – Window size

## Sequencing (Sekvenčná kontrola)

- Zabezpečuje správne usporiadanie paketov v správach, aby ich príjemca mohol rekonštruovať v správnom poradí.
- Používa sa v protokoloch ako TCP, ktoré priradujú číslovanie paketom.

# Funkcie sieťových protokolov

## Error Detection (Detekcia chýb)

- Mechanizmus, ktorý umožňuje odhaliť chyby v prenose dát spôsobené šumom, rušením alebo stratou paketov.
- Zvyčajne pomocou Checksum – kontrolný súčet

## Application Interface (Aplikačné rozhranie)

- Klient server komunikácia
- Napríklad na Web stránke a používa HTTP alebo HTTPS na komunikáciu medzi klientom a serverom



# Mapovanie siete

# Mapovanie siete (Network Mapping)

- Mapovanie siete je proces **získavania prehľadu o štruktúre, zariadeniach a spojeniach v počítačovej sieti.**
- Výsledkom je vizuálna alebo textová mapa, ktorá ukazuje, aké zariadenia sú v sieti, ako sú prepojené a aké služby alebo protokoly používajú.

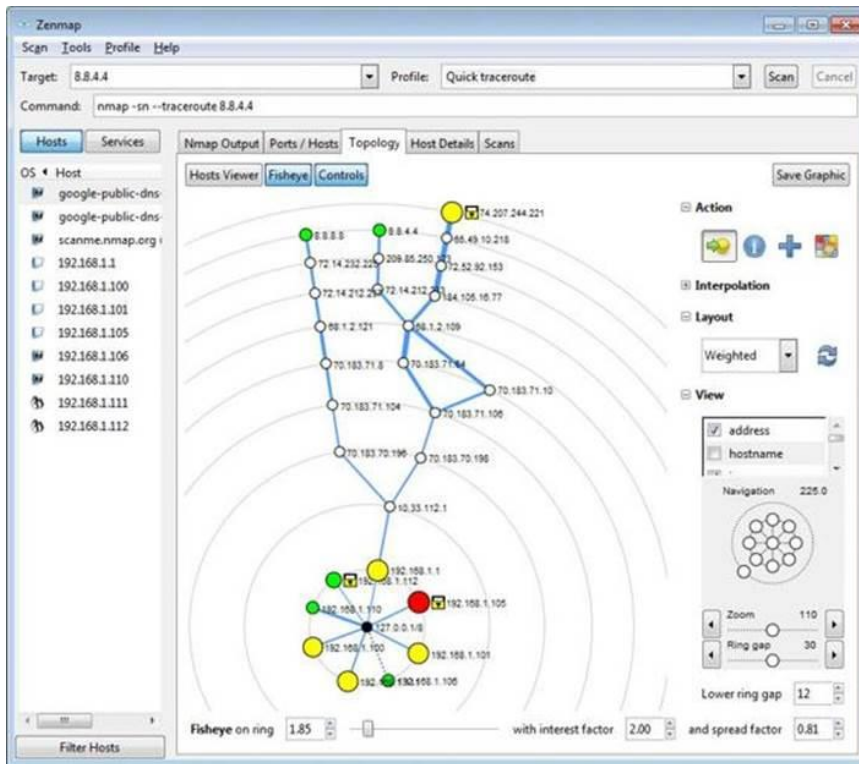
## Ciel':

- **Inventarizácia zariadení:** zistenie, aké počítače, servery, smerovače, prepínače a ďalšie uzly sú v sieti.
- **Topologický prehľad:** identifikácia, ako sú jednotlivé zariadenia navzájom prepojené (hviezda, strom, sieťová topológia).
- **Zabezpečenie:** odhalenie neautorizovaných zariadení alebo otvorených portov, ktoré by mohli byť zneužitú.
- **Správa siete:** podklad pre plánovanie rozšírenia, odstraňovanie chýb alebo optimalizáciu výkonu.

## Typy mapovania

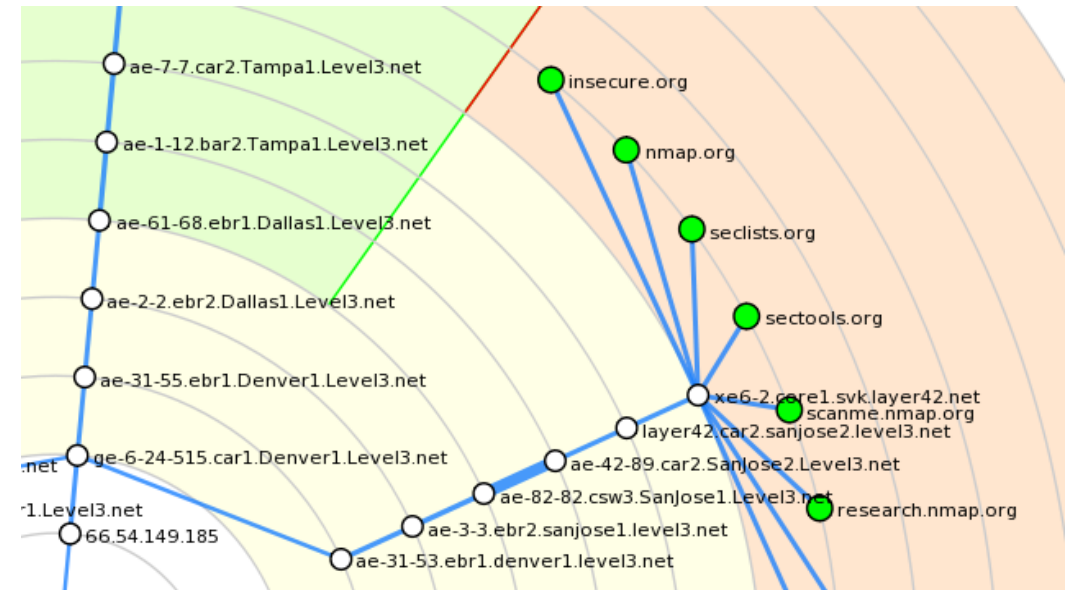
### Fyzické mapovanie:

- ukazuje fyzické prepojenia (káble, switche, routery).



### Logické mapovanie:

- zobrazuje logické vzťahy (IP adresy, VLAN, podsiete, smerovanie).



# Nástroje a metódy

- **Ping a traceroute:** základné príkazy na zisťovanie cesty a dostupnosti.
- **Nmap (Network Mapper):** nástroj na skenovanie hostov, portov a služieb.
- **SNMP (Simple Network Management Protocol):** protokol umožňujúci zisťovať informácie o zariadeniach.
- **Ďalšie nástroje:** SolarWinds, PRTG, Nagios – dokážu automaticky generovať mapy a sledovať výkon siete.

## Príklad využitia:

- V univerzitnej sieti správca spustí mapovanie a zistí, že do siete je pripojený neautorizovaný Wi-Fi router študenta → potenciálne bezpečnostné riziko.



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

## Úvod k prevádzke elektronických komunikačných systémov

Technické opatrenia (BLOK IV)

**Kurz: Manažér kybernetickej bezpečnosti**

Ing. Matúš Madleňák

**KC KYB UNIZA, <https://kc.uniza.sk/>**

matus.madlenak@uniza.sk