Obsah

[1. Poznám jednotlivé sieťové zariadenia, viem ich rozdeliť na aktívne, pasívne 2](#_Toc90577136)

[2. Poznám jednotlivé typy sietí - LAN, WAN, MAN, WLAN, SAN 2](#_Toc90577137)

[3. Viem si zabezpečiť prístup na Cisco Router a Switch. 4](#_Toc90577138)

[4. Viem opísať, aké sú funkcie každej vrstvy ISO/OSI modelu. 5](#_Toc90577139)

[5. Poznám vrstvy TCP/IP modelu a viem opísať, z čoho sa skladajú jednotlivé PDU. 7](#_Toc90577140)

[6. Poznám protokol Ethernet II, viem nakresliť jeho hlavičku a viem, aká je funkcia jednotlivých políčok. 8](#_Toc90577141)

[7. Viem detailne vysvetliť a opísať ARP proces. 8](#_Toc90577142)

[8. Dokážem podrobne vysvetliť CSMA/CD prístupovú metódu. Objasniť, kde sa (ne)používa a prečo. 8](#_Toc90577143)

[9. Dokážem vysvetliť CSMA/CA proces. Objasniť, kde sa používa a prečo. 8](#_Toc90577144)

[10. Poznám aké rôzne Switch Forwarding Methods používajú Cisco switche a viem ich navzájom porovnať. 9](#_Toc90577145)

[11. Viem opísať proces prepínania aj určenie portu podľa prepínacej tabuľky. 9](#_Toc90577146)

[12. Viem povedať, z čoho sa skladá router, ako sa nazývajú jednotlivé konektory. 10](#_Toc90577147)

[13. Poznám hlavičku protokolu IPv4 a IPv6. Viem ich navzájom porovnať. 10](#_Toc90577148)

[14. Poznám rôzne spôsoby koexistencie IPv6 a IPv4 svetov. 10](#_Toc90577149)

[15. Dokážem určiť, do ktorej siete IP adresa patrí, aký je jej rozsah. Daný rozsah adries viem podsieťovať. 11](#_Toc90577150)

[16. Viem porovnať protokoly UDP a TCP. 11](#_Toc90577151)

[17. Dokážem podrobne vysvetliť TCP three-way handshake. 11](#_Toc90577152)

[18. Poznať čísla portov spomínaných protokolov aplikačnej vrstvy. 12](#_Toc90577153)

[19. Viem opísať proces stiahnutia súboru z FTP serveru. 12](#_Toc90577154)

[20. Vysvetliť HTTP Request a Response. Opísať, čo sa deje na každej vrstve TCP/IP modelu. 12](#_Toc90577155)

[21. Viem opísať celý proces DNS požiadavky na server. Kedy sa používa UDP a kedy TCP port na komunikáciu. 12](#_Toc90577156)

[22. Dokážem vysvetliť pojem kolízna doména, broadcastová doména a aké zariadenia ich oddeľujú. 13](#_Toc90577157)

[23. Viem, aký port má SSH, Telnet, aký je medzi týmito protokolmi rozdiel, načo slúžia a čo je to SVI. 13](#_Toc90577158)

[24. Viem opísať ukončenie spojenia TCP. 13](#_Toc90577159)

[25. Viem opísať DHCP proces. 13](#_Toc90577160)

[26. Viem opísať prenos dát pri TCP komunikácií a vysvetliť ako TCP poskytuje flow control a na čo vlastne potrebujeme flow control. 13](#_Toc90577161)

[27. Viem vysvetliť rozdiel medzi simplex, half-duplex a full-duplex komunikáciou a aké komplikácie vznikajú pri half-duplex komunikácií. 14](#_Toc90577162)

[28. Viem vysvetliť enkapsuláciu a deenkapsuláciu. 14](#_Toc90577163)

[29. Viem vysvetliť multiplexing a demultiplexing na transportnej vrstve. 14](#_Toc90577164)

[30. Poznám terminológiu a viem vysvetliť čo je to protokol, balík protokolov, technológia, socket, médium a opísať základné typy médií 14](#_Toc90577165)

[31. Opísať proces smerovania a vyhľadania cesty v smerovacej tabuľke 15](#_Toc90577166)

# 1. Poznám jednotlivé sieťové zariadenia, viem ich rozdeliť na aktívne, pasívne

**Passive Networking Hardware** are those parts of [computer network](https://managementmania.com/en/computer-network" \o "Computer Network) that are involved in [data](https://managementmania.com/en/data" \o "Data) transmission in the network, but they don’t change or affect the data.

The passive network hardware includes:

* Cables (fiber optic cable, coaxial cables)
* Connectors
* Switchboards
* Clutches
* Plugs

**Active Networking Hardware** comprises all parts of a [computer network](https://managementmania.com/en/computer-network" \o "Computer Network) which in some way actively work with the signals in the network (amplify them, modify them, evaluate them, etc.). Active Networking Hardware are usually specific devices located in the hubs of the network.

Active networking hardware includes:

* [Switch](https://managementmania.com/en/switch)
* Repeater
* Hub
* Bridge
* [Router](https://managementmania.com/en/router)
* [Print Server](https://managementmania.com/en/print-server)
* Access point (AP)
* Power E-Net

# 2. Poznám jednotlivé typy sietí - LAN, WAN, MAN, WLAN, SAN

LAN – Local Area Network

A LAN is a network infrastructure that spans a small geographical area. LANs have specific characteristics:

* LANs interconnect end devices in a limited area such as a home, school, office building, or campus.
* A LAN is usually administered by a single organization or individual. Administrative control is enforced at the network level and governs the security and access control policies.
* LANs provide high-speed bandwidth to internal end devices and intermediary devices, as shown in the figure.

WAN – Wide Area Network

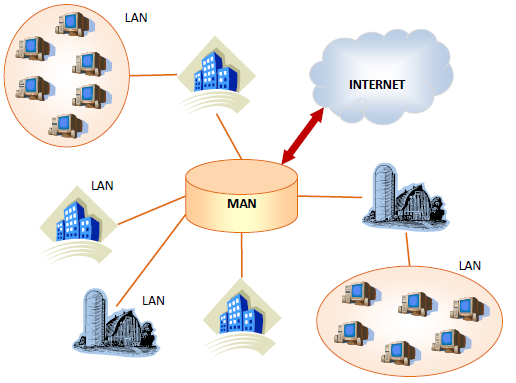
The figure shows a WAN which interconnects two LANs. A WAN is a network infrastructure that spans a wide geographical area. WANs are typically managed by service providers (SPs) or Internet Service Providers (ISPs).

WANs have specific characteristics:

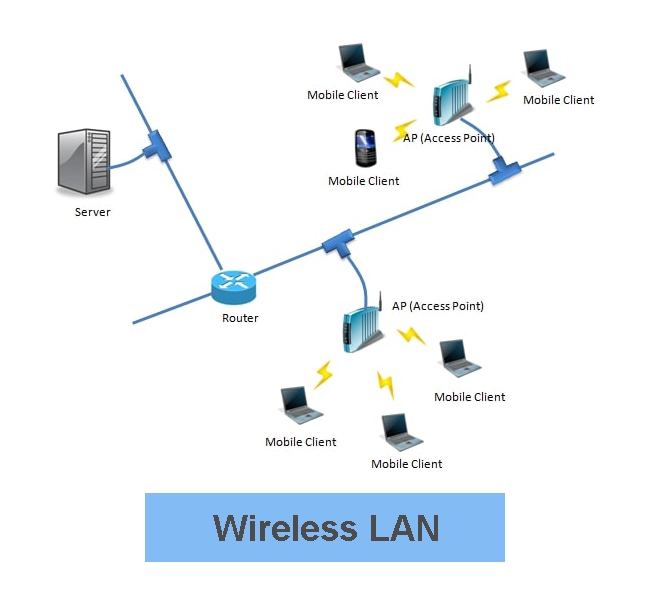
* WANs interconnect LANs over wide geographical areas such as between cities, states, provinces, countries, or continents.
* WANs are usually administered by multiple service providers.
* WANs typically provide slower speed links between LANs.

MAN – Metropolitan Area Network

MAN sieť je väčšia ako LAN, ale menšia ako WAN – prepája zariadenia vo väčšej oblasti ako napríklad mesto, alebo hocijaká oblasť s viacerými budovami

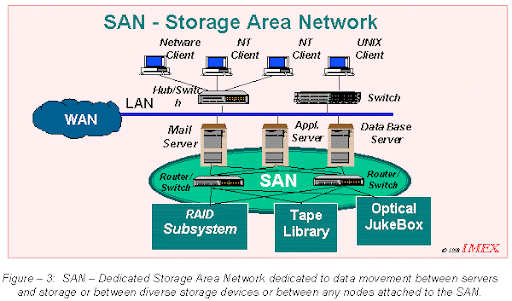


WLAN – Wireless LAN

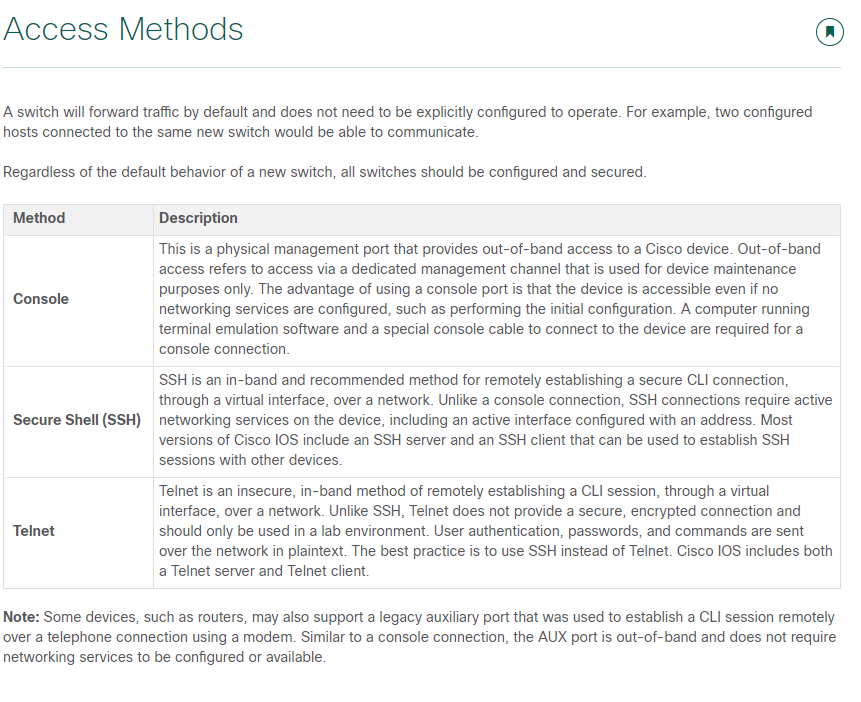


SAN – Storage Area NetworkTCP

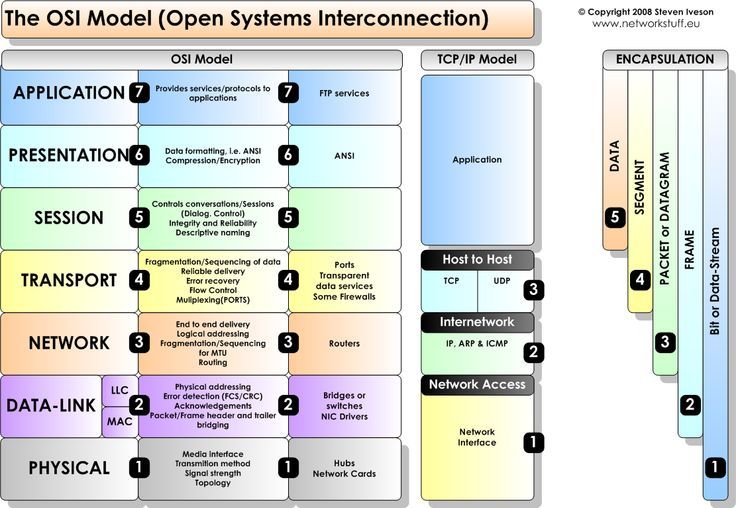
Používa sa hlavne na prístup z zariadeniam ktoré uchovávajú dáta

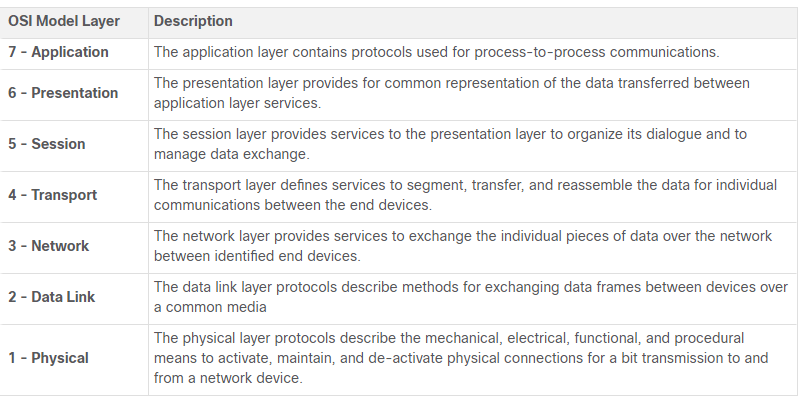


# 3. Viem si zabezpečiť prístup na Cisco Router a Switch.



# 4. Viem opísať, aké sú funkcie každej vrstvy ISO/OSI modelu.





**Fyzická vrstva:**

Pred každou sieťovou komunikáciou musí byť nastavené sieťové spojenie – káblové pripojenie alebo bezdrôtové pripojenie ktoré využíva rádiové vlny. Typ pripojenia závisí od typu a požiadaviek siete. NIC pripája zariadenie do siete. Ethernet NIC sa používa na káblové pripojenie, zatiaľ čo WLAN NIC na bezdrátové pripojenie. Veľa zariadení obsahuje oba typy NIC (network interface card).

Táto vrstva prijíma úplný rámec z data link vrstvy a a kóduje ho ako sériu signálov, ktoré sa prenášajú na lokálne médium. Kódované bity, ktoré obsahujú rámec, prijíma buď koncové zariadenie alebo sprostredkujúce zariadenie.

Fyzická vrstva riadi:

* Fyzické komponenty (Káble, NIC...)
* Kódovanie (prevod do bin)
* Signalizáciu

**Data link vrstva:**

Pripravuje dáta pre fyzickú vrstvu. Táto vrstva je zodpovedná za NIC, umožňuje vyšším vrstvám dostať sa k prenášaným dátam, vyššie vrstvy nemusia vedieť aké médium sa používa a podobne. Príjme packety z 3 vrstvy, zabalí ich do rámca pre fyzickú vrstvu, alebo príjme encapsulovaný rámec, odbalí ho a pošle packet na vyššiu vrstvu. Riadi prístup k médiu – vyberie sa vhodný protokol, a topológia siete je vybratá podľa veľkosti siete, počtu hostiteľov, službami. Vymieňa packety medzi endpointmi. Kontroluje packety, ak sú nesprávne zahodí ich.

Táto vrstva je rozdelená na 2 podvrstvy:

LOGICAL LINK CONTROL (LLC) – komunikuje medzi softvérom a vyššími vrstvami, a hardvérom a nižšími vrstvami. Pridáva do hlavičky info aký protokol je vybratý pre daný packet

MEDIA ACCESS CONTROL (MAC) – implementuje vrstvu do HW, je zodpovedný za:

* enkapsuláciu (balí do frame, pridáva MAC adresu na presun medzi eth NIC a eth NIC na rovnakej LAN, pridáva frame check sequence)
* media access control (MAC), napr kontroluje NIC
* Obsahuje špecifikácie pre rôzne typy médií
* Obsahuje CSMA/CA alebo /CD

**Sieťová vrstva**

Vďaka nej si môžu koncové zariadenia vymieňať dáta. Základné funkcie 3 vrstvy:

* Adresácia (jedinečnou) IP adresou
* Zabalenie packetu – PDU z transportnej vrstvy na packet, pridá IP adresu dest a sourc
* Routing – sieťová vrstva poskytuje služby na presun packetu na host do inej siete cez routery (každý router je jeden hop)
* Odbalenie packetu (keď packet dorazí na sieťovú vrstvu cieľového zariadenia, skontroluje sa dest IP adresa

Protokoly 3 vrstvy (IPv4 a IPv6) špecifikujú štruktúru packetu a použité spracovanie na prenos dát medzi hostami.

**Transportná vrstva**

Je zodpovedná za komunikáciu medzi aplikáciami ktoré bežia na odlišných hostoch. Je to link medzi aplikačnou vrstvou a nižšími vrstvami zabezpečujúcimi presun dát po sieti. Transportná vrstva teda presúva dáta medzi aplikáciami v sieti. Nemá info o použitom médiu, type zariadenia ktoré príjma dáta.

Transportná vrstva obsahuje TCP a UDP protokoly.

Transportná vrstva má na starosti:

* Udržiavanie a tracking konverzácie medzi 2 aplikáciami (host môže mať otvorených viacero aplikácií ktorých dáta a správy sa nemôžu miešať
* Segmentovanie dát – dáta sa rozdelia na segment (TCP) alebo datagramy (UDP)
* Pridáva header info (ktoré obsahujú informácie potrebné pre korektné presunutie packetov po sieti)
* Identifikovať jednotlivé aplikácie a osobitne každú spravovať (čo obnáša použitie správnych portov)
* Multiplexing – aplikačné dáta z rôznych aplikácií sú posielané na striedačku

**Aplikačná vrstva**

Aplikačná vrstva je najbližšie ku používateľovi, poskytuje interface medzi aplikáciami ktoré spolu komunikujú, a nižšími vrstvami ktoré zabezpečujú prenos po sieti. Aplikačné protokoly majú teda za úlohu vymieňať dáta medzi programami ktoré bežia na komunikujúcich hostoch. Na TCP/IP modeli je to aplikačná vrstva, v ISO/OSI je táto vrstva rozdelená na session, presentation a aplication vrstvu.

Protokoly: DNS, DHCP, FTP, STP, POP, STMP

Prrezentačná vrstva

* **Formátovanie** dát na vhodnú formu v akej ju dest zariadenie prijme
* **Kompresia** dát
* **Šifrovanie** dát, dešifrovanie pri prijatí

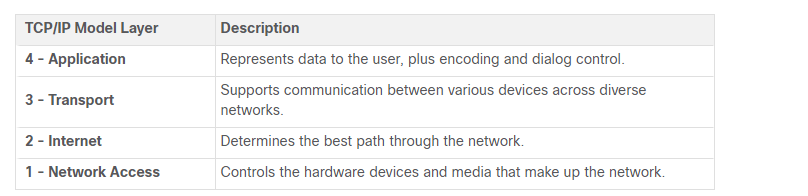
Session vrstva

* Vytvorenie a udržiavanie komunikácie medzi aplikáciami
* Vytvorenie session

Aplikačná vrstva

* Špecifikuje formát a kontrolné info
* Obsahuje protokoly (čísla sú porty):
* Name system (DNS -53)
* device config (DHCP, BOOTP—68,67)
* email (POP-110, SMTP-25, IMAP-143)
* file transfer (FTP – 20/21 , TFTP-69)
* web (http-80/8080, https-443)

# 5. Poznám vrstvy TCP/IP modelu a viem opísať, z čoho sa skladajú jednotlivé PDU.



Aplikačná – Dáta

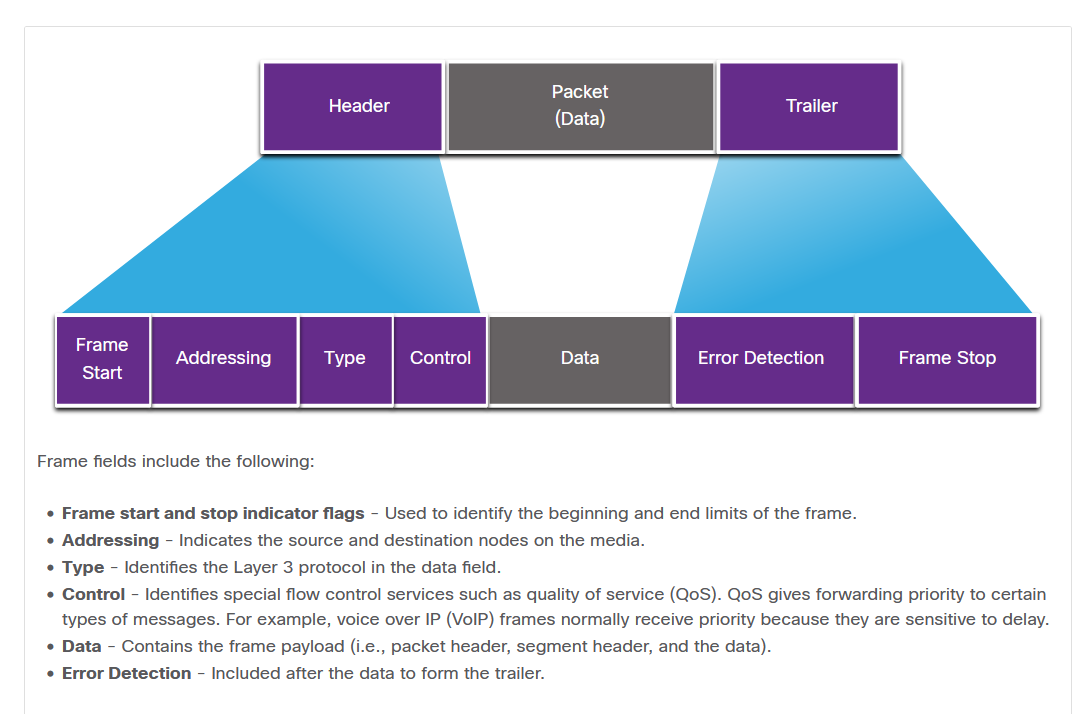
Transportná – Segmenty

Internet – packet (IP adresa)

Network Access – bits & rámce (MAC adresa)

# 6. Poznám protokol Ethernet II, viem nakresliť jeho hlavičku a viem, aká je funkcia jednotlivých políčok.

MAC adresy + ethertype (ďalší protokol 2 vrstvy – ARP, STP...)



# 7. Viem detailne vysvetliť a opísať ARP proces.

ARP protokol – IP na MAC, udržiava tabuľku IP adries na MAC adresy

* Záznamy sú uložené v ARP cache, pričom sa vymazávajú pokiaľ nie sú používané

V prípade zapnutia množstva zariadení naraz ktoré si potrebujú vytvoriť ARP tabuľky, sieť sa dočasne spomalí a nastane pokles výkonu, pretože všetky ARP requesty sú broadcast

ARP spoofing – zariadenie príjme ARP request, a aj keď nepatrilo priamo jemu, pošle reply so svojou MAC adresou, pričom vo výsledku príjma dáta ktoré neboli určené jemu

Ak pri posielaní packetu zdrojové zariadenie zistí že v ARP tabuľke nemá záznam cieľovej IP na MAC, odošle ARP request, ktorý sa odošle všetkým zariadeniam v sieti. Packet na odoslanie zatiaľ odloží. Zariadenie pre ktoré bola správa určená (vie podľa IP) odošle v ARP reply svoju MAC adresu. Akonáhle príjde na zdrojové zariadenie požadovaná MAC adresa, odložený packet môže byť odoslaný, a do ARP tabuľky sa pridá nový záznam.

# 8. Dokážem podrobne vysvetliť CSMA/CD prístupovú metódu. Objasniť, kde sa (ne)používa a prečo.

Používa sa pri ethernetovom spojení ktoré komunikuje pomocou half duplex, cez káble sa dá detekovať kolízia.

Media access control protokol v ktorom noda skontroluje či žiadny iný uzol neposiela po médiu, kým začne komunikáciu. Zatiaľ čo konkrétne zariadenie odosiela packety, všetky ostatné zariadenia zdieľajúce médium musia počkať kým bude médium znovu voľné.

CD je pre collision detection, ak nastane, všetky dáta budú corrupnuté, tým pádom bude musieť prebehnúť posielanie znova, alebo NIC rozozná že amplitúda signálu je vyššia ako obvykle.

# 9. Dokážem vysvetliť CSMA/CA proces. Objasniť, kde sa používa a prečo.

Používa sa pri bezdrôtovom wifi pripojení.

Kontroluje či je médium voľné tiež ako CSMA/CD, ale používa aj pridané techniky – nie je možné detekovať kolíziu preto sa jej snaží čo najlepšie vyhnúť tým, že ak je médium voľné, odošle prvý packet s info ako dlho bude odosielať dáta access pointu (routeru) – ready to send správa. Acccess point odošle naspäť clear to send. Takto môže AP-u posielať správy veľa zariadení. Pri následnom posielaní packetov AP tieto packety potvrdí. Access point môže byť router.

10. Poznám aké rôzne Switch Forwarding Methods používajú Cisco switche a viem ich navzájom porovnať.

SWITCH

* Rozhoduje sa čisto podľa MAC adresy ako bude packet preposielať ďalej
* Postupne si vytvorí MAC adress tabuľku, väčšina switchov si po čase tabuľku premazávajú
* Unknown unicast – ak switch nemá záznam pre MAC adresu a teda nevie kam má packet poslať, pošle ho všade okrem source portu
* Switch môže mať na jednom porte aj viac zariadení (ak je napr na tom porte ďalší switch)

Metódy :

* store and forward (prijme packet a vypočíta crc, ak je správne, pozrie sa na destination adresu, a packet je poslaný správnym portom), je nutná pri QoS
* cut-through (rovno začne presmerovať packet ešte pred tým ako mu celý prišiel – keďže dest adresa ide prvá, nemusí čakať na celý packet, nekontroluje ho)
  + fast-forward switching (hneď ako dostane destination MAC, prepošle packet ďalej, môžu ale nastať chyby, dest zariadenie potom packet zahodí. Ponúka ale nízku latenciu (oneskorenie)
  + fragment-free switching (uloží si prvých 64B kde zvyčajne dochádza k chybám, okontroluje ich a až potom pošle ďalej)--- kompromis medzi store-and-forward a fast-forward

Niektoré switche prepínajú medzi týmito dvoma metódami podľa error rate.

Buffering je buď zdieľaná pamäť, alebo podľa portov (sú v queue podľa toho ako prišli, ak je jeden port vyťažený spomaľuje ostatné)

Na switchi sú najdôležitejšie šírka pásma, a duplex možnosti

# 

# 11. Viem opísať proces prepínania aj určenie portu podľa prepínacej tabuľky.

SWITCH

* Rozhoduje sa čisto podľa MAC adresy ako bude packet preposielať ďalej
* Postupne si vytvorí MAC adress tabuľku, väčšina switchov si po čase tabuľku premazávajú
* Unknown unicast – ak switch nemá záznam pre MAC adresu a teda nevie kam má packet poslať, pošle ho všade okrem source portu
* Switch môže mať na jednom porte aj viac zariadení (ak je napr na tom porte ďalší switch)

Keď switch obdrží packet, pozrie sa odkiaľ prišiel. Ak na ten port ešte nemá namapovanú MAC adresu, pridá ju do MAC adresnej tabuľky.

# 12. Viem povedať, z čoho sa skladá router, ako sa nazývajú jednotlivé konektory.

Router obsahuje viacero portov:

- LAN porty: FastEthernet + GigabitEthernet

- internet port

- power socket

- AUX port (pripojenie ku routeru cez modem na diaľku)

- console port (na pripojenie konzoly ku routeru)

- Sériové porty

# 13. Poznám hlavičku protokolu IPv4 a IPv6. Viem ich navzájom porovnať.

Negatíva IPv4:

* Nedostatok adries
* Nedostatok end to end spojenia (používa NAT - preklad z privátnej na verejnú IP)
* NAT zvyšuje komplexnosť sietí, zťažuje hľadanie chýb v sieti

IPv6 :

* Viac adries
* Jednoduchšie IP hlavičky
* Netreba NAT
* Flow control zaručí že packety prichádzajú postupne

Traffic class v IPv6 nahradilo Differentiated services v IPv4

Hop limit v IPv6 nahradilo TTL z IPv4

V IPv6 niesú flagy

IPv6 používa viac miesta na adresy (miesto 4B na adresu sa používa 16B)

Dĺžka IPv4 packetu je 20B, IPv6 má 40B

IPv6 nemá checksum field

https://afteracademy.com/blog/difference-between-ipv4-and-ipv6

# 14. Poznám rôzne spôsoby koexistencie IPv6 a IPv4 svetov.

Vylepšenia IPv6 oproti IPv4:

ICMPv6 obsahuje address resolution (ARP v IPv4), narozdiel od IPv4

Nieje potrebný NAT protokol (máme dostatok adries)

Koexistencia IPv6 a IPv4:

* Dual stack (sieť funguje ako IPv4 aj IPv6, má IPv6 pripojenie na ISP)
* Tunneling (posielanie IPv6 packetu po IPv4 sieti – IPv6 packet je obalený do IPv4 hlavičky)
* Translation (router obsahuje protokol NAT64 ktorý prekladá adresy pri preposielaní packetov – IPv6 a IPv4 siete tak môžu cez takýto router spolu komunikovať)

Tunneling a translation treba používať iba v nevyhnutných situáciách, cieľom je postupne prejsť na IPv6 adresáciu.

# 15. Dokážem určiť, do ktorej siete IP adresa patrí, aký je jej rozsah. Daný rozsah adries viem podsieťovať.

# 16. Viem porovnať protokoly UDP a TCP.

TCP Overview

TCP establishes sessions, ensures reliability, provides same-order delivery, and supports flow control. A TCP segment adds 20 bytes of overhead as header information when encapsulating the application layer data. TCP header fields are the Source and Destination Ports, Sequence Number, Acknowledgment Number, Header Length, Reserved, Control Bits, Window Size, Checksum, and Urgent. Applications that use TCP are HTTP, FTP, SMTP, and Telnet.

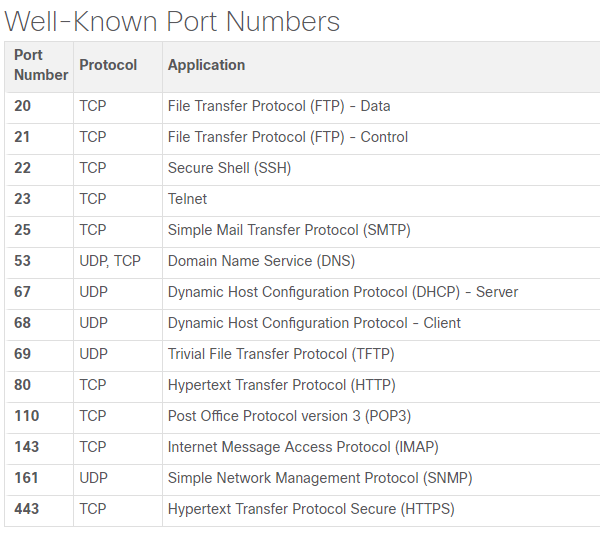
UPD Overview

UDP reconstructs data in the order it is received, lost segments are not resent, no session establishment, and UPD does not inform the sender of resource availability. UDP header fields are Source and Destination Ports, Length, and Checksum. Applications that use UDP are DHCP, DNS, SNMP, TFTP, VoIP, and video conferencing.

# 17. Dokážem podrobne vysvetliť TCP three-way handshake.

Prenos dát pomocou TCP protokolu si vyžaduje nadviazanie spojenia s dest zariadením. Odosielajúci uzol odošle TCP packet s nastavenou SYN flagou,a vygenerovaným sequence number ktorý sa bude pri komunikácii používať na overenie správnosti komunikácie. Dest zariadenie odpovie TCP packetom s nastavenými flagmi SYN, ACK, pričom si vygeneruje vlastné sequence number. ACK number ktoré bude odoslané je prijaté sequence number +1. Odosielajúce zariadenie potvrdí obdržanie SYN,ACK packetu, získa sequence number prijímajúceho zariadenia, a odpovie svojim novým SYN number ktorý sa rovná obdržanému ACK number, a ako ACK number odošle prijaté SEQ number +1. PO úspešnom three way handshake môže začať prenos dát. Pri three way handhake sa nastaví počiatočná hodnota window na riadenie toku dát, a zvykne sa odoslať MSS (maximum size of segment), teda maximálny počet B ktoré dokáže dest uzol prijať vrámci jedného segmentu.

# 18. Poznať čísla portov spomínaných protokolov aplikačnej vrstvy.



# 19. Viem opísať proces stiahnutia súboru z FTP serveru.

FTP protokol sa používa na prenos dát medzi klientom a serverom. FTP client je aplikácia ktorá je spustená na klientovi ktorý posiela a sťahuje dáta z FTP servera. Najskôr klient otvorí komunikáciu pre kontrolné údaje na porte 21 - táto komunikácia obsahuje commandy klienta a server replies. Potom otvorí komunikáciu pre presun dát na porte 20. Podľa príkazov v kontrolných údajoch sa dáta buď posielajú klientovi (pull) alebo klient odosiela dáta(push).

Obrázok, na ktorom je text

Automaticky generovaný popis

# 20. Vysvetliť HTTP Request a Response. Opísať, čo sa deje na každej vrstve TCP/IP modelu.

Prehliadač získa 3 informácie: protokol (http/https), doménu, a konkrétny súbor ktorý chceme získať zo servera. Cez DNS protokol na aplikačnej vrstve zistíme IP adresu z domény. Formátujeme dáta podľa protokolu ktorý je použitý, prebehne kompresia a šifrovanie dát (ak protokol šifruje dáta)(preseniation layer). Vytvorí sa session, ak je už vytvorená udržiava sa (session layer). Pridá sa GET request do hlavičky. Na transportnej vrstve sa vytvorí socket s IP adresou zariadenia a vygenerovaného portu, ak je už vygenerovaný použije sa, a socket s IP adresou domény a portu protokolu (https 443, http – 80). Na tejto vrstve sa segmentujú dáta podľa veľkosti MSS, a vytvorí sa segment, alebo datagram, v závislosti od použitého protokolu transportnej vrstvy. Z transportnej vrstvy sa PDU presunie na sieťovú vrstvu kde sa PDU obalí do hlavičky 3 vrstvy – pridajú sa IP adresy, protokol použitý na vyššej vrstve, pridá sa checksum. Zo segmentu sa stáva zabalením v 3 vrstve packet. Na data link vrstve sa pridajú MAC adresy, zdrojová a cieľová podľa ARP záznamu v tabuľke. Ak záznam neexistuje, použije sa ARP protokol na zistenie MAC adresy, alebo ICMPv6 NA pre IPv6. Zabalením na datalink vrstve je PDU rámec. Na fyzickej vrstve sa rámec kóduje a prebieha signalizácia, čím sa PDU vyšle do siete. Na cieľovej IP adrese sa nachádza server ktorý počúva na porte. Príjme PDU, postupne ho rozbalí, podľa použitého TCP alebo UDP protokolu odošle potvrdenie, na aplikačnej vrstve spracuje požiadavku, a odošle ako odpoveď požadovaný súbor.

# 21. Viem opísať celý proces DNS požiadavky na server. Kedy sa používa UDP a kedy TCP port na komunikáciu.

DNS protokol je dôležitý na preklad domien na IP adresy. Vďaka nemu si nemusíme pamätať IP adresy, ale iba jednoducho zapamätateľné doménové mená. DNS protokol využíva jediný formát na všetky typy správ – message.

Užívateľ zadá doménové meno do prehliadača. DNS query je odoslaná na DNS server ktorý má zariadenie vopred nakonfigurované. Bez IP adresy DNS servera nieje možné používať prehliadač s doménami, museli by sme zadávať priamo IP adresy. Po prijatí packetu na DNS server vyberie záznam pre FQDN a jeho IP adresu. Pokiaľ server neobsahuje danú doménu, kontaktuje iné servery, a dočasne si záznam uloží pokiaľ by bol potrebný znova. DNS query response je odoslaná klientovi s IP adresou domény. Klient túto doménu použije na get request zo servera ktorého IP adresu sa pomocou DNS dozvedel. Ďalšie typy response môže byť IPv6, IP email servera, IP autoritativneho servera.

DNS bežne používa UDP, pretože je rýchlejšie a pokiaľ klient nedostane odpoveď, môže sa nastaviť timeout na aplikačnej vrstve a odoslať požiadavku znova. Ak je odpoveď dlhšia ako 512B a obe strany podporujú EDNS, použije sa väčší packet, inak sa použije TCP protokol. TCP protokol sa taktiež používa pri zone transfers.

# 22. Dokážem vysvetliť pojem kolízna doména, broadcastová doména a aké zariadenia ich oddeľujú.

1. Kolízna doména je priestor v sieti ovplyvnený kolíziou, túto časť siete zdieľajú viaceré zariadenia. Problém nastane, keď začnú naraz vysielať. Všetky port na hube, pretože hub pracuje na fyzickej vrstve. Na switchi len jeden port, delí kolíznu doménu.

2. Broadcastová doména je priestor v sieti, kam sa šíri broadcast. V zásade (okrem výnimočných prípadov ako DHCP helper address a pod.) sa šíri len po najbližší router.

23. Viem, aký port má SSH, Telnet, aký je medzi týmito protokolmi rozdiel, načo slúžia a čo je to SVI.

22 – ssh (šifrovaná zabezpečená komunikácia)

23 – telnet (nešifrovaná komunikácia)

SVI – switch virtual interface slúži na vzdialený prístup ku switchu – na switchi treba nastaviť vlan 1 – IP adresa + maska, a zapnúť ho. Nieje to fyzický port ale virtuálny.

# 24. Viem opísať ukončenie spojenia TCP.

Na ukončenie TCP spojenia sa používajú flagy FIN, ACK. Pri komunikácii hociktorý z dvoch uzlov môže odoslať FIN packet. Následne príjmajúci uzol odošle potvrdenie prijatia FIN packetu, s ACK flagou, a odošle vlastný FIN packet. Môže sa stať že tieto flagy sú odoslané vrámci jedného packetu, nie dvoch. Odosielajúca strana nakoniec potvrdí prijatie packetu ďalším ACK. Po ukončení spojenia sa uvoľnia všetky zdroje použité na komunikáciu (porty). V prípade nedostatku zdrojov na komunikáciu na jednej alebo druhej strane, zlyhalnia spracovania dát alebo obdržania packetu ktorý nemá nastavenú SYN flagu aj keď nieje nastavený žiadny prenos sa posiela packet s RST flagou, ktorý okamžite ukončí akékoľvek spojenie.

# 25. Viem opísať DHCP proces.

Obrázok, na ktorom je text

Automaticky generovaný popis

Obrázok, na ktorom je text

Automaticky generovaný popis

# 26. Viem opísať prenos dát pri TCP komunikácií a vysvetliť ako TCP poskytuje flow control a na čo vlastne potrebujeme flow control.

TCP protokol poskytuje error správy a informačné správy keď komunikujú s iným IP zariadením. Tieto správy sú poslané pomocou ICMP. Tieto správy poskytujú feedback o chybách ktoré nastali, nie aby spravili IP spoľahlivým.

Window field v hlavičke – definuje koľko bytov dát môže byť naraz spoľahlivo presunutých a spracovaných kým sa odošle ACK potvrdenie ( bežne sa ale ACK odošle skôr, aby odosielajúci uzol vedel že môže ďalej posielať dáta. Ak neprichádza, odošlú sa dáta podľa window size, a čaká sa na potvrdenie – ktoré spracujúci uzol odošle hneď ako spracuje prijaté dáta. Ak sa odošle ACK pred prijatím všetkých dát podľa window size, na odosielajúcom uzle sa inkrementuje window size o počet B ktorý bol v danom okne presunutý. Tento process sa nazýva sliding window

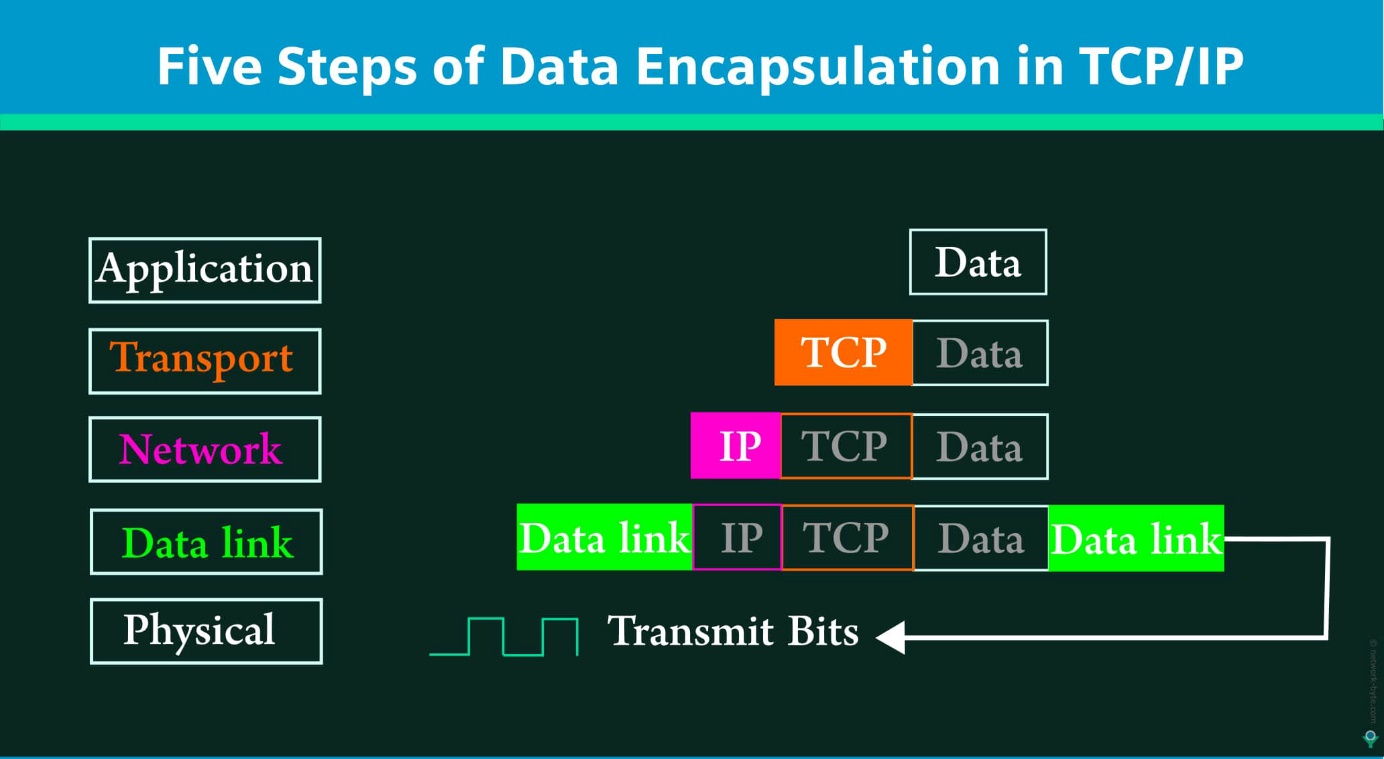
Ak nastane zahltenie siete, router zahodí packety a TCP protocol nedostane potvrdenia. Tým pádom sa môže stat že klient začne odosielať všetky packet znova, čím situáciu ešte zhorší. TCP protocol má teda algoritmy a časovače aby takýmto situáciám predchádzal. Napríklad zníži počet odoslaných B pred potvrdením (aj bez toho že mu pride menší window size od prijímateľa), obmedzí svoju premávku.

# 27. Viem vysvetliť rozdiel medzi simplex, half-duplex a full-duplex komunikáciou a aké komplikácie vznikajú pri half-duplex komunikácií.

<https://www.geeksforgeeks.org/transmission-modes-computer-networks/>

Pri half duplex je problém ak je jedna strana vo full-duplex a druhá strana v half-duplex móde. Nastávajú kolízie, dáta sú poškodené. Toto sa môže stať zlou konfiguráciou, alebo zlyhaním autokonfigurácie v zariadeniach.

# 28. Viem vysvetliť enkapsuláciu a deenkapsuláciu.



# 29. Viem vysvetliť multiplexing a demultiplexing na transportnej vrstve.

Multiplexing and Demultiplexing services are provided in almost every protocol architecture ever designed. UDP and TCP perform the demultiplexing and multiplexing jobs by including two special fields in the segment headers: the source port number field and the destination port number field.

Multiplexing –   
Gathering data from multiple application processes of the sender, enveloping that data with a header, and sending them as a whole to the intended receiver is called multiplexing.

Demultiplexing –   
Delivering received segments at the receiver side to the correct app layer processes is called demultiplexing. 

# 30. Poznám terminológiu a viem vysvetliť čo je to protokol, balík protokolov, technológia, socket, médium a opísať základné typy médií

The combination of the source IP address and source port number, or the destination IP address and destination port number is known as a socket. The socket is used to identify the server and service being requested by the client

Protokol je súhrn pravidiel na komunikáciu.

The protocols that are used in network communications share many of these fundamental traits. In addition to identifying the source and destination, computer and network protocols define the details of how a message is transmitted across a network. Common computer protocols include the following requirements:

* Message encoding
* Message formatting and encapsulation
* Message size
* Message timing
* Message delivery options

There are three main types of network protocols. These include [network management](https://www.cdw.com/content/cdw/en/solutions/data-center-and-network-infrastructure/network-management.html" \o "Discover network management solutions) protocols, network communication protocols and [network security](https://www.cdw.com/content/cdw/en/products/networking-products/network-security.html" \o "Learn about network security) protocols:

Communication protocols include basic data communication tools like TCP/IP and HTTP.

Security protocols include HTTPS, SFTP, and SSL.

Management protocols maintain and govern the network through protocols such as ICMP and SNMP.

Soket sa používa na identifikáciu servera a služby, ktoré klient požaduje. Klientsky soket môže vyzerať takto, pričom 1099 predstavuje číslo zdrojového portu: 192.168.1.5:1099

Socket pár – client + server socket.

Sockety umožňujú viacerým procesom, ktoré bežia na klientovi, aby sa navzájom odlíšili a aby sa odlíšili viaceré pripojenia k procesu servera.

Modern networks primarily use three types of media to interconnect devices:

Medené káble

Existujú 3 typy káblov, káble sú limitované vzdialenosťou a rušením z vonkajšieho prostredia. Dáta sú prenášané ako elektrické impulzy. Útlm signálu – čím ďalej majú byť dáta prenášané, tým viac sa kazia.

EMI (electromagnetic) a RFI ( radio frequency) singnály rušia dáta prenášané káblami. Crosstalk nastáva keď sú dáta vyrušené elektrickými alebo magnetickými poľami signálu v jednom kábli, ktorý ovplyvňuje signál v druhom kábli. Na vyrušenie EMI alebo RMI sa niektoré káble balia do kovového chrániča a musia byť uzemnené, alebo majú opačné páry káblov zmotané dokopy. Pri voľbe typu káblov sa má brať ohľad na prostredie v ktorom sa bude využívať, vyhnúť sa rušivým miestam, a využívať techniky ktoré správne používajú káble aj s ich ukončením.

Crosstalk - skreslenie prenášaných správ zo signálov prenášaných v susedných vodičoch

Optické vlákno

Je drahšie, preto sa toľko nepoužíva. Presúvajú dáta na dlhšie vzdialenosti s vyššou šírkou pásma, bez útlmu, a nerušia ju EMI a RFI. Bity sú encodované na fyzickej vrstve na svetelné pulzy.

Sú rozdelené na 2 typy – single mode fiber (SMF) – jedna cesta svetla, drahšie, na dlhšiu vzdialenosť, používa laser

-multi mode fiber (MMF) – viacero možných ciest svetla – pod rôznym uhlom, lacnejšie, na kratšie vzdialenosti, má väčšiu disperziu (strata sily signálu), používa LEDky

Bezdrôtové pripojenie

Prenášané elektromagnetickými signálmi na rádiových alebo microwave frequencies.

Pri tomto type pripojenia musíme dávať pozor na oblasť kde ju zapájame – niektoré materiály limitujú dosah siete. Signál môže byť vyrušený mikrovlnkou, inými bezdrôtovými sieťami ... treba dávať pozor aj na bezpečnosť, taktiež treba brať do úvahy že čím viac používateľov sa pripojí tým bude pre každého používateľa nižšia šírka pásma.

# 31. Opísať proces smerovania a vyhľadania cesty v smerovacej tabuľke

Smerovacia tabuľka sa nachádza na smerovači (routeri). Obsahuje IP adresu siete, a port na ktorej sa sieť nachádza, alebo záznam o next hope. Posupne prechádzame tabuľkou a vyberieme záznam ktorý má zhodu so sieťovou adresou s najväčšou maskou, do ktorej patrí. Ak nájdeme v tabuľke záznam o next hope, uložíme si adresu a vykonávame rekurzívne prehľadnávanie v tabuľke, pričom hľadáme novo uloženú IP adresu. Po nájdení portu sa ním daný packet odošle.