1. OSI, TCP/IP modeļi

OSI (*Open System Interconnection)* ir modelis, kas kategorizē visus datortīklu savienojumus 7 līmeņos. Šis standarta modelis ļauj datortīklu kompānijām ražot savienojumus tehnoloģiskos savienojumus. Septiņi OSI līmeņi, sākot no zemākā:

1. **Fiziskais** – apraksta mehāniskās, elektroniskās un funkcionālās metodes, kā tiek aktivizēti, uzturēti un deaktivizēti fiziskie savienojumi bitu pārsūtīšanai. Šis līmenis pieņem datu kadrus no kanāla līmeņa un iekodē tos kā signālus.

Tie var būt kabeļi (optiskie, varu, koaksiālie) vai bezvadu metodes (Wi-Fi un citi).

Šajā slānī darbojas NIC, Ethernet, signālu atkārtotāji un citas ierīces.

1. **Kanāla** – kanāla līmeņa protokoli apraksta metodes datu kadru apmaiņai kopīgā medijā. Kanāla līmenis atbild par saziņu starp tīkla kartēm (NIC to NIC)

Ir 2 apakšslāņi - MAC (atbildīgs par to, ka datu paketi ir novietoti medijā) un LLC (identificē lietoto tīkla slāņu protokolu).

Šajā slānī darbojas komutatori (switch).

1. **Tīkla** – tīkla līmeņa protokoli apraksta metodes loģiskai adresācijai lai apmainītu individuālas paketes. Šis līmenis ļauj sazināties starp tīkliem.

IP protokoli (IPv4, IPv6), šajā slāni tipiski strādā maršrutētāji.

1. **Transporta** – transporta līmeņa protokoli ļauj sadalīt, pārsūtīt un salikt kopā datus individuāliem savienojumiem starp iekārtām.

(Pārraides Vadības Protokols (TCP), kuri dati ir sadalīti **segmentos**)

(Lietotāja Datogrammu Protokols (UDP), kuri dati ir sadalīti **datagrammās**)

1. **Sesijas** – sesijas līmeņa protokoli palīdz prezentācijas un lietojumu slāņiem organizēt datu plūsmas, atbild par sesiju pārvaldību.

(Paroles Autentificēšanas Protokols (PAP), Attāls Procedūras Izsaukums (RPC), Real-Time Transport Control Protocol (RTCP) un citi.)

1. **Prezentācijas** – prezentācijas līmeņa protokoli definē kopīgu veidu kā reprezentēt datus, kas tiek sūtīti starp lietojumu līmeņa servisiem.

(JPEG, MKV, GIF un citi.)

1. **Lietojumu** – lietojumu līmenis nodrošina tīkla pakalpojumus programmatūrai.

(HTTPS, FTP, POP3, SMTP)

Sarežģītus konceptus par tīkla darbību un iekšējām norisēm var būt grūti saprast, tādēļ nepieciešams slāņos sadalīts modelis. Ieguvumi no slāņota modeļa, lai aprakstītu tīkla operācijas:

* Kļūst vienkāršāk veidot jaunus tīkla protokolus, jo protokoliem, kas strādā ar konkrētu OSI modeļa līmeni ir labi definēti dati, kurus tie apstrādā, kā arī labi definēts interfeiss uz augšu un apakšu esošajiem līmeņiem.
* Palīdz konkurētspējai, jo produkti no dažādiem ražotājiem var strādāt kopā
* Novērš situācijas, kur izmaiņas vienā tehnoloģiju slāni rada neparedzētas izmaiņas citos slāņos
* Rada kopīgu valodu, lai aprakstītu tīkla funkcijas un spējas

Analogi OSI modelim, vel viens tīkla modelis ir TCP/IP modelis, ko dažkārt sauc par interneta modeli. TCP/IP modelis ir gan protokolu modelis, kas nozīmē ka tas satur reālu protokolu saimi, gan references modelis, līdzīgi kā OSI modelis. TCP/IP modelim ir tikai 4 slāņi:

1. **Tīkla pieejas (network access)** – kontrolē fiziskās iekārtas, kas veido tīklu
2. **Interneta ( Internet)** – Nosaka labāko maršrutu pa tīklu.
3. **Transporta(Transport)** – atbalsta komunikācijas starp dažādām ierīcēm un dažādiem tīkliem.
4. **Lietojumu ( Application) ­­**– reprezentē datus lietotājam.

A screenshot of a computer program

Description automatically generated

Protokoli, kas veido TCP/IP protokolu saimi, var tikt raksturoti izmantojot OSI references modeli. OSI modeļa sesijas, prezentācijas un lietojumu slāņi TCP/IP modelī tiek apvienoti vienā lietojumu slāni, kā arī OSI kanāla un fiziskie slāņi apvienoti tīkla pieejas slānī.

OSI 3. slānis jeb tīkla slānis ir tieši analogs TCP/IP interneta slānim. Šis slānis tiek lietots lai aprakstītu protokolus, kas adresē un sūta starptīklu ziņas.

Osi 4. slānis jeb transporta slānis ir tieši analogs TCP/IP transporta slānim. Šis slānis apraksta vispārīgus servisus un funkcijas, kas ļauj uzticami un secīgi nosūtīt datus starp sūtītāju un saņēmēju.

Pašreizējas TCP/IP modelis tika standartizēts jau 1980. gadu sākumā, tomēr TCP/IP protokolu saime nepārtraukti mainās. Piemēram, tās izveidošanās laikā nebija IPv6 protokola.

TCP/IP interneta līmeņa galvenā funkcija ir maršrutēšana – labākā paketes ceļa izvēle. Galvenais šī līmeņa protokols ir IP, tas nepārbauda, vai pakete sasniedz galamērķi, tikai pārsūta pareizajā virzienā. Šo sauc par “labākā mēģinājuma” (“best effort”) sūtīšanu. Šī iemesla dēļ IP ir neuzticams protokols. IP protokola galvenie uzdevumi ir definēt paketes kā informācijas vienības, pārsūtīt paketes starp citiem TCP/IP līmeņiem, maršrutēt paketes. Citi interneta līmeņi ir ICMP, kas sūta kontrolētas ziņas, ARP, kas atrod MAC adresi no zināmas IP adreses, RARP, kas atrod IP adresi no zināmas MAC adreses. Arī ipv4 un ipv6 ir interneta līmeņa protokoli.

TCP/IP transporta līmenī parādās sūtīšanas integritāte, garantijas, ka sūtītā informācija tiks piegādāta. TCP/IP modelī transporta slāni ir divi protokoli – TCP un UDP.

1. Vītā pāra kabeļu datu pārraides vide.

Lai pārraidītu datus, atkarībā no apstākļiem, var lietot varu vītā pāra kabeļus.

Ir 3 galveni tipi:

* UTP (Unshielded Twisted-Pair) – Neekranēts vītā pāra kabelis.

UTP ir visizplatītākais vadu veids. Tās ir lēts un ar to ir viegli darboties, bet nav visātrākais un drošākais kabeļu veids.

* FTP(foil shield twisted pair) – daļēji ekranēts vītā pāra kabelis, kurš tiek ekranēts ar apkārtējo folija kārtu starp vītā pāra kabeļiem un izolācijas slāni
* STP (Shielded Twisted-Pair) - ekranēts vītā pāra kabelis. Uz galos arī ir RJ45 savienotāji, bet iekšā tās atšķiras. Ir ārējais apvalks, pēc tām folijas ekrāns, katrā kabeļu pāra ir sava atsevišķā apvalkā, un katrs vads ir savā atsevišķā apvalkā.

STP ir labāk aizsargāts no trokšņiem, lietojot savu ekrānizāciju, lai pasargātu informāciju no EMI un RFI. Kā UTP, vadi ir savīti, lai cīnītos ar šķērsrunu. Lai iegūtu maksimālu aizsardzību, galos tiek lietoti speciāli STP savienotāji.

Vara kabeļos pārraidīto elektrisko impulsu nobīdes laikā un sprieguma vērtības ir jūtīgas pret interferenci no diviem galvenajiem avotiem:

* Elektromagnētiskā interference (EMI) – EMI signāli var traucēt datu signāliem kas tiek pārraidīti vara mēdijā. Potenciālie trokšņu veidotāji ir fluorescētas lampas vai elektriskie motori.
* Crosstalk, jeb šķērsruna – elektromagnētiskie trokšņi, kurus izraisa blakus esošie kabeļu signāli. Kad elektriskais signāls plūst cauri kabelim, ap viņu veidojas neliels elektriskais lauks, kas var traucēt citiem vara kabeļu signāliem.

Šajā brīdī ir astoņas vītā pāra kabeļa paaudzes, taču mūsdienu pielietojumā tiek plaši izmantoti Cat 5, 5e un 6 revīzijas.

1. Optisko kabeļu datu pārraides vide.

Optiskie kabeļi pārraida datus ātrāk un tālāk nekā citi kabeļu tipi.

Atšķirība no vara kabeļiem, optiskie kabeļi ir izturīgi pret elektromagnētiskiem traucējumiem un radiofrekvences traucējumiem.

Optiskais kabelis ir elastīgs, bet ārkārtīgi plāns (thin), caurspīdīgs un tā vidū ir tīra stikla dzīsla, ne biezāka par cilvēka matu. Biti ir kodēti kā gaismas impulsi.

Ir divi optisko kabeļu veidi:

* Single-Mode Fiber (SMF) - ļoti maza serde un dārgs lazērs, lai sūtītu vienu gaismas staru (ray). Populārs lielu distanču aplikācijās (telefonija, kabeļu televīzija). Vienmodas šķiedras kodols ir šaurāks nekā daudzmodas, gaisma izplatās tikai pa vienu trajektoriju, mazās impulsa izkliedes dēļ, to var izmantot datu sūtīšanai lielos attālumos kas sasniedz 1000km. Gaismas avots, lāzeri, priekš koncentrētas gaismas nodošanas.
* Multimode Fiber (MMF) - lielākā serde, vairāki LED lāzeri. Populārs veids lokālajos tīklos, jo ātrums sasniedz līdz pat 10 Gbps maksimāli 550 metru distancē. Daudzmodu šķiedru kodoli ir lielāki 50 vai 62,5 mikroni. Gaismas stari tiek padoti vairākās trajektorijās, vairāki stari var nonākt līdz galamērķim ar dažādu laika intervālu. Daudzmodu maksimālais garums ir 2km, lai neveidotos izsmērētie gaismas stari, kas rada negatīvas sekas. Gaismas avoti – LED diodes.

MMF, atšķirībā no SMF, ir vairāk dispersijas. Tas nozīme, ka jau pēc 500 metriem, MMF var zaudēt signālu.

Optiskas kabeļus lieto 4 industrijās:

* Uzņēmumu tīklos (Enterprise Networks) - lai savienot infrastruktūras ierīces
* Fibre-līdz-mājam (FTTH, Fiber-to-the-Home) - lai piedavāt vienmēr aktīvus platjosla (broadband) servises mājam un maziem uzņemumiem
* Ilgu vilkšanas tīkli (Long-Haul Networks) - to lieto pakalpojumu sniedzēji lai savienot valstus un pilsētus
* Zemūdens kabeļu tīkli (Submarine Cable Networks) - lai piedavāt uzticamus risinājumus ar lielo ātrumu un ietilpību bargos (harsh) apstakļos.

Salīdzinājumā ar vītā pāra kabeļiem, optiskiem kabeļiem joslas platums ir lielāks (10Mbps-100Gbps), tie var ceļot tālāk (1-100,000m), un optiskais kabelis ir “imunizēts” pret EMI un RFI, kā arī pret elektriskiem draudiem.

Taču viņi ir dārgāki, pieprasa vairāk prasmes instalācijā un pieprasa visaugstākās drošības piesardzības.

Ir 4 tipu savienotāju:

* Straight-Tip (ST) - pirmie no savienotājiem. Apaļa forma. Savienotājs ir aizsargāts ar “twist-on/twist-off” tipa durkli.
* Subscriber-Connectors (SC) - dažreiz to nosauc par “square” vai “standard” savienotājiem. Plaši lietots LAN un WAN savienotājs, kurš lieto “push-pull” mehanismu savienošanai. Lietots ar SMF un MMF.
* Lucent Connector (LC) - SC savienotāja mazāka versija.
* Duplex Multimode LC - savienotājs, kurš ir tuvs LC “simplekss” (simplex) savienotājam, bet lieto dubultu (duplex) savienotāju.

1. Bezvadu lokālie tīkli

Bezvadu lokālie tīkli pārnēsā informāciju izmantojot elektromagnētisko viļņu palīdzību. Tie izmanto radio viļņus un microviļņu frekvences. Galvenie iemesli bezvadu tīkla izmantošanai ir tās ērtības, jo tīklam var piekļūt neizmantojot fiziskus savienojums, kā arī nav nepieciešama sarežģīts instalācijas process. Tas ir vismobīlākais no visiem tīklu mēdijiem.

Galvenie ierobežojumi bezvadu mēdijam ir:

* Pārklājuma diapazons – bezvadu tīklu tehnoloģijas labi funkcionē atvērtā vidē bez šķēršļiem, un konkrēti lietoti ēkas materiāli var ietekmēt signāla pārklājumu un kvalitāti.
* Interference – bezvadu tīklus var traucēt citas bezvadu iekārtas, piem., bezvadu telefoni, fluorescējošas gaismas, mikroviļņu krāsnis un citas bezvadu iekārtas.
* Drošība – atšķirībā no tikla kabeļiem, bezvadu tīklos garnadzim nevajag fizisku savienojumu, lai piekļūtu un noklausītos pārraidītos datus.
* Dalīts medijs – WLAN tipa tīkli operē pusdupleksa režīmā, kas nozīmē, ka tikai viena tīkla iekārta var sūtīt un saņemt datus vienlaikus. Ja pie iekārtas ir liels ierīču skaits, tīkla joslas platums tiek samazināts .

Lai gan bezvadu tīkli tiek arvien vairāk izmantoti, vara un optiskie kabeļi ir joprojām vispopulārākā izvēle savienojumus starp iekārtām. Bezvadu medijiem ir izveidoti standarti, kas attiecas gan uz fizisko slāni, gan kanāla slāni. Šie standarti attiecas uz:

* Datu kodēšanu radio signālos(data-to-radio encoding)
* Signālu frekvenci un transmisijas jaudu
* Signāla uztveršanas un atkodēšanas procesu
* Antenas dizainu

Daži no bezvadu standartiem:

* WIFI bezvadu lokālā tīklu tehnoloģija (Wireless LAN), neformāli sauc par Wi-Fi. Wlan izmanto nesējkontroles daudzpiekļuves sadursmju novēršanas protokolu ( carier sensemultiple access/collision avoidance jeb CSMA/CA). Bezvadu tīkla daskarnes kartei sākumā jāklausās , lai noteiktu vai radio signāls ir brīvs tikai tad tā var sūtīt datus. Ja cita iekārta tajā brīdī sūta datus, tīkla kartei ir jāgaida, kamēr kanāls ir brīvs. Wi-Fi ir reģistrēta preču zīme, kas pieder *wifi alliance*. Tas var tikt lietots tikai sertificētiem wlan iekārtām, kas saderīgas ar IEEE 802.11 standartu.

WLAN iekārta ar 2,4 GHz antenu var izmantot frekvenci 2,40 GHz līdz 2,48 GHz. Frekvenču joslas sadalītas frekvenču kanālos. Kanāli 2,4ghz frekvencē pārklājas, par 5ghz tā nevar teikt.

* Bluetooth ( IEEE 802.15) – bezvadu personālo tīklu (wpan) standarts, ko bieži sauc par “Bluetooth”. Izmanto iekārtu sapārošanas procesu, lai sūtītu datus līdz pat 100 metru attālumam
* WiMAX (IEEE 802.16) – worldwide interoperability for microwawe access
* Zigbee(IEEE 802.15.4) – specifiska zema datu pārraides ātruma un zemas jaudas komunikācijām. Piemērots tuvas darbības iekārtām, kurām nepieciešams ilgs akumulatora darbības laiks
* Satelītu komunikācija, utt.

Lai wlan tīkls strādātu ir vajadzīgs:

* Bezvadu piekļuves punkts(WAP) – bezvadu piekļuves punkti koncentrē bezvadu signālus no lietotājiem, un savienojas ar vara vai optiskajiem kabeļiem.
* Bezvadu tīkla kartes adapteri(*wireless nic adapters*) – ļauj sazināties ar tīkla iekārtām.

Galvenie mūsdienās izmantotie bezvadu autentifikācijas standarti ir WPA(*wifi protected access*), kas aizstāj nedrošo WEP standartu. Ir nākušas klāt WPA2, kas tiek plaši izmantots un WPA3, kurš vel netiek izmantots un atbalstīts visās ierīcēs.

Galvenās šifrēšanas metodes, kas izmantotas bezvadu autentifikācijas protokolos ir TKIP( novecojis, izmanto WPA), AES(droša metode, izmanto WPA2), galuā šifrs(izmanto WPA3)

1. Decimālā, binārā un heksadecimālā skaitīšanas sistēmas.

Nu bļe, ko tur var stāstīt

1. Ethernet protokols.

**Ethernet** ir **fizikāla LAN** tehnoloģija, kurā iekļauj vītā pāra, koaksiālus un optiskus kabeļus. Protokols operē gan **fizikālajā**, gan **kanāla** slānī (**Tīkla pieejas** slānis TCP/IP modelī). Tā ir **noteikto tīklu tehnoloģija ģimene**, kurā ir aprakstīta **IEEE 802.2** un **802.3**.

IEEE 802 LAN/MAN protokoli, tai skaitā Ethernet, izmanto divus atsevišķus kanāla līmeņa apakšslāņus. Šie apakšslāņi ir loģiskā posma vadības (LLC jeb Logical Link Control) slānis un medijpiekļuves vadības (Media Access Control jeb MAC) slānis.

LLC apakšslānis. Šie IEEE 802.2 definētais apakšslānis komunicē starp tīkla programmatūru augšējos slāņos un aparatūru(hardware) zemākajos slāņos. Tā datu kadros ievieto informāciju, kas indentificē, kurš tīkla sļāņa protokols tiek lietots šim kadram. Šī informācija atļauj vairākiem 3. slāņa protokoliem, piemēram ipv4 un ipv6, izmantot to pašu tīkla interfeisu un mediju. LLC galvene dod kanāla slānim informāciju par to, ko darīt ar paketi. Piemēram, ja iekārta saņem datu kadru, tā var apskatīt LLC galveni un noskaidrot, ka tā ir domāta IP protokolam tīkla slānī.

MAC apakšslānis. MAC(Media Access Control) apakšslānis ir definēts IEEE 802.3 un atbild par datu iekapsulēšanu un piekļuvi medijam. Tas ietver Ethernet kadru adresēšanu un Ethernet kļūdu noteikšanu

Mazākasi pieļaujamais Ethernet kadra izmērs ir 64 baiti un lielākāis pieļaujamais ir 1518 baiti. Tas iekļauj visus baitus sākot no galamērķa MAC adreses līdz pat kadra kontolsummai (Frame Check Sequence jeb FCS)

Kadri, kuru izmērs ir zem 64 baitiem, tiek uzskatiīt par nederīgiem (“collision fragment” jeb “runt frame”) un tiek automātiski ignorēti. Kadri ar vairāk nekā 1518 baitiem arī tiek izmesti (tos sauc par “baby giant frames”)

Ethernet kadru sastāvs:

* Preambula – izmanto sinhronizācijai starp sūtītāju un saņēmēju
* Galamērķa MAC adrese
* Sūtītāja MAC adrese
* Tips - identificē augstāko līmeņu protokolu, kurš iekapsulēts Ethernet kadrā, piemēram, 0x86DD apzīmē IPv6
* Dati
* Kontrolsumma (FCS)

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) jeb nesēja jušanas un sadursmju atklāšanas daudzpiekļuve ir tehnoloģija, kas ļauj vairākām iekārtam izmantot to pašu mediju pus-dupleksajā režīmā, nosakot sadursmes un definējot algoritmu retranslācijai. Mūsdienu Ethernet LAN tīkli izmanto komutatorus, kas atbalsta pilnu duplekso režīmu, tādēļ CSMA/CD nav nepieciešams.

Kad tikla iekārta veic transmisiju, tas signālu mēdz dēvēt par nesēju . Tīkla karte nosaka nesēja esamību un konsekventi nesūta signālu. Ja nesējs nav noteicams, iekārta zina, ka medijs ir brīvs translācijai. Šis ir iemesls tam, kādēļ CSMA/CD nosaukuma ir “nesēja jušana” .

Tīkla segmenta daļu, kurā notiek sadursme (collision), sauc par sadursmes domēnu (collision domain). Jo lielāks sadursmes domēns, jo lielāka ietekme sadursmēm ir uz datu apgrozījumu.

Sākotnēji Ethernet tīkli izmantoja vienu kabeli (parasti koaksiālo), kas kalpoja kā tīkla mugurkauls, tam fiziski pieslēdzās pārējie kabeļi. Šis risinājums pieprasīja CSMA/CD. Pēc tam notika migrēšana uz tīkla centmezgliem (hubs), kurus vēlāk aizstāja komutatori (switches), kas arī ir mūsdienās pieņemtais risinājums.

Ehternet ir ļoti svarīgi datus sūtīt pareizajos brīžos:

* Slota laiks (slot time) – minimālais transmisijas laiks
* Starpkadru atstarpe (Interframe Spacing) – laiks starp kadru transmisiju
* Atkāpes laiks (backoff) – laiks, kas tīkla iekārtām ir jāgaida pirms retransmisijas, kad notikusi sadursme

Trīs galvenie tīklu komunikācijas veidi ir:

* Uniraide (unicast, one to one) – tīkla iekārta nosūta datu kadru, kas adresēta kādai citai specifiskai tīkla iekārtai. Viens sūtītājs, viens saņēmējs.
* Apraide (broadcast, one to all) – tīkla iekārta nosūta datu kadru visām citām adresēm. Viens sūtītājs, vairāki saņēmēji
* Multiraide (multicast, one to many) – tīkla iekārta nosūta datus specifiskai grupai ar vairākām citām iekārtām. Atšķirībā no apraides, iekārtām jābūt specifiskā multiraides grupā, lai saņemtu šos datus. Viens sūtītājs, vairāki saņēmēji.

MAC adresi izmanto lai Ethernet LAN tīklos nosūtītu datus uz pareizo galamērķi. MAC adrese ir 48 bitus jeb 6 baitus liela, tā sastāv no divām daļām

* Organizatoriskais unikālais identifikators (Organizational Unique Indentifier jeb OUI)(24 biti) – identificē tīkla kartes ražotāju. Šo identifikatoru piešķiršanu regulē IEEE. Iekš OUI ir divi nozīmīgi biti – apraides/multiraides bits un lokāli administrētas adreses bits. Kas jāiestata, ja adrese tiek mainīta.
* Ražotāja piešķirtā adrese ( vendor-assigned end station address)(24 biti) – unikāli identificē Ethernet iekārtu

1. Ethernet komutēšana (switching).

Jo lielāks ir Ethernet tīkla segments, jo lielāks ir sadursmju domēns, kas palielina sadursmju biežumu, kas, savukārt, samazina tīkla datu apmaiņas efektivitāti.

Tādēļ Ethernet tīklus ir labi sadalīt vairākos segmentos, lai samazinātu kolīziju domēnus. To var darīt ar divām galvenajām tīkla iekārtām:

* **Tilts (bridge) -**  tilts ir tīkla iekārta, kas sadala vienu sadursmju domēnu divos. Kad tilts saņem datu kadru, tas pārbauda, vai galamērķa MAC adrese ir tā MAC adrešu tabulā. Tas attiecīgi nosūta kadru pa vienu no tā diviem portiem.
* **Komutators (switch) –** komutators ir tilts ar vairākiem portiem. Tam var būt pat desmitiem portu. Pie katra porta pieslēgtās iekārtas ir nodalītas atsevišķā sadursmju domēnā. Ja pie porta ir pieslēgta tikai viena ierīce, tās sadursmju domēnā ir tikai divas iekārtas – šī pieslēgtā iekārta un komutators. Šādus sadursmju domēnus mēdz saukt par mikrosegmentiem ( *microsegments* ).

Jāpiebilst ka centrālmezgli (*hubs*) nesadala sadursmju domēnus.

**MAC adrešu tabula.** Tīkla komutators izmanto MACadreses, lai veiktu lēmumus par to, kurus kadrus kur pārsūtīt. Komutators nosaka, vai galamērķa adrese ir uniraides adrese, komutators meklēs šo adresi savā MAC tabulā. Ja tā ir šajā tabulā, komutators to pārsūtīs pa pareizo portu. Ja adrese nav šajā tabulā ( šādu situāciju sauc par unknown unicast), tas pārsūtīs adresi pa visiem portiem izņemot to, pa kuru tā ienāca.

Komutators analizē visus kadrus, kas tiek sūtīti tam cauri. Tas izpēta sūtītāja MAC adresi un nosaka porta skaitli tam portam, pa kuru kadrs ienāca. Ja sūtītāja MAC adrese nav tabulā, komutators to pievieno tabulai kopā ar ienākošā porta skaitli. Ja sūtītāja MAC adrese jau ir tabulā, komutators atjaunina šī ieraksta taimeri. Noklusēti Ethernet komutatori patur ierakstus MAC adrešu tabulā 5 minūtes. Dažkārt MAC tabulu sauc par CAM (*content addressable memory*) tabulu.

Cisco komutatoriem ir divas pāradresēšanas (*forwarding*) metodes:

* Uzkrājnosūtes komutēšana (*Store-and-forward swithing*) – komutators sagaida visu kadru, izrēķina CRC (cyclic redundancy check jeb cikliskā redundances pārbaude), kas ir matemātisks tests, kas nosaka, vai kadrā ir kļūda, balstoties uz bināro vieninieku skaitu tajā. Ja CRC ir derīgs, komutators meklē galamērķa adresi MAC tabulā un atbilstoši izvēlās portu kadra pārsūtīšanai
* Caurtekas nosūtīšana (cut-through switching) – komutators pārsūta (forwards) datu kadru pirms tas ir pilnībā saņemts (tam ir jāsagaida vismaz galamērķa adrese)

Priekšrocība uzkrājnosūtes komutēšanai ir, ka tā nosaka vai kadrā ir kļūdas pirms tā pārsūtīšanas. Kad kļūda ir noteikta, komutators izmet kļūdaino kadru. Tas nozīmē, ka mazāka daļa joslas platuma tiek aizņemta ar kļūdainiem kadriem. Uzkrājnosūtes komutēšana ir nepieciešama tīklos, kur servisa kvalitātes (QoS) nolūkos jāveic satiksmes klasifikācija un prioritātes noteikšana ( piemēram, situācijas, kad VoIP datiem jābūt ar lielāku prioritāti par tīkla pārlūkošanas datiem).

Komutatori, kas veic caurtekas komutēšanu, analizē saņemtos kadru fragmentus pirms transmisija ir pabeigta. Komutators sagaida tieši tik datu, lai nolasītu galamērķa MAC adresi, lai tas varētu noteikti, pa kuru portu kadrs jāpārsūta. Komutators neveic kļūdu pārbaudi šiem kadriem.

Caurtekas komutēšanai ir divi apakštipi:

* **“Fast-forward switching” –** šim komutēšanas veidam ir vismazākā aizture. Aizture ir laiks no brīža, kad kadru sāk izsūtīt pirmā ierīce, līdz brīdim, kad kadra sākums ir sasniedzis galamērķa ierīci. Tā kā fast-forwarding komutatori sāk pārsūtīt kadru pirms tas ir ticis pilnībā saņemts, var rasties gadījumi, kad tiek pārsūtīti kļūdaini kadri. Tas nenotiek bieži un galamērķa NIC ignorē šādus nederīgus kadrus
* **Bezfragmentu komutēšana (Fragment-free switching)** – bezfragmentu komutēšanā komutators saglabā kadra pirmos 64 baitus pirms tā pārsūtīšanas. Bezfragmentu komutēšana ir kompromiss starp uzkrājnosūtes komutēšanu un fast-forward komutēšanu. Iemesls, kādēļ bezfragmentu komutēšana uzglabā tikai pirmos 64 kadra baitus, ir, ka lielākā daļa tīkla kļūdu un sadursmju notiek pirmajos 64 baitos. Bezfragmentu komutēšana cenšas uzlabot fast-forward komutēšanu, veicot kļūdu pārbaudes kadra pirmajiem 64 baitiem. Tādēļ šī metode ir kompromiss starp uzkrājnosūtes komutēšanu, kurai ir liela aizkave, un fast-forward komutēšanu, kurai ir mazāka uzticamība.

Ir iespējams komutatoru konfigurēt tā, ka tas izmanto caurtekas komutēšanu līdz ir sasniegts lietotāju skaita slieksnis, kad tas tiek sasniegts, komutators pārslēdzas uz uzkrājnosūtes komutēšanu, lai samazinātu kļūdu skaitu.

**Komutatoru atmiņas buferizācija**. Ethernet komutatori mēdz izmantot buferizācijas tehniku, lai uzglabātu datu kadrus pirms to pārsūtīšanas. Buferizācija var tikt lietota arī gadījumos, kur galamērķa ports ir nepieejams pārslodzes dēļ. Komutators uzglabā kadru līdz brīdim, kurā tas var tikt retransmitēts. Ir divas galvenās buferizācijas metodes:

* **Uz portiem balstīta atmiņa ( port-based memory) –** kadri tiek glabāti rindās (queues), kas ir piesaistītas specifiskie ieejošajiem un izejošajiem portiem. Kadrs tiek transmitēts uz izejošo portu tikai tad, kad visi tam rindā priekšā esošie kadri ir tikuši veiksmīgi transmitēti. Ir iespējams, kas viens kadrs novēlo visu atmiņā esošo kadru transmisiju.
* **Dalītā atmiņa (shared memory) –** visi kadri tiek ievietoti kopīgā atmiņas buferī.

**Auto-MDIX** (automatic medium-dependent interface crossover) ir tehnoloģija, kas ļauj komutatoriem automātiski noteikt portam pievienoto kabeļa tipu – caurplūdes(straight-through) vai pārejas(crossover), lai atbilstoši konfigurētu tīkla interfeisu.

1. IPv4 protokols.

IPv4 ir viens no galvenajiem tīkla līmeņa protokoliem. IP jeb interneta protokols tiek lietots, lai iekārtas, kas piesaistītas internetam, varētu sazināties ar jebkurām citām internetam piesaistītām publiski pieejamām iekārtām. IP nodrošina globālu adresācijas sistēmu (IP adreses), īpašu datu struktūru (IP paketi), kas nodrošina standartizētu datu apmaiņu.

IPv4 paketēm ir galvene, kas tiek lietota, lai nodrošinātu, ka konkrētā pakete tiek piegādāta uz tās nākamo “pieturvietu” ceļā uz tās galamērķa iekārtu. IPv4 pakete satur:

* Versija – izmantotā IP versija
* Interneta galvenes garums (Internet Header Lenght) – visas IP galvenes kopīgais garums
* DSCP (Differenciated Services Code Point) – agrāk zināms kā ToS ( Type of service). Izmanto, lai noteiktu paketes prioritāti
* Dzīvlaiks (time to live jeb TTL) – vērtība, kas ierobežo paketes dzīves laiku. Katru reizi, kad paketi apstrādā maršrutētājs, šī vērtība tiek samazināta par 1. ja tā sasniedz nulli, maršrutētājs to izmet un oriģinālajam sūtītājam sūta ICMP ziņu par šo kļūdu
* Protokols – izmanto, lai noteiktu nākamā līmeņa protokolu. Bieži izmantotas vērtības ir ICMP(1), TCP(6) un UDP(17)
* Sūtītāja IPv4 adrese – 32 bitu vērtība. Vienmēr uniraides tipa adrese
* Galamērķa IPv4 adrese – 32 bitu vērtība. Var būt gan uniraides, gan multiraides, gan apraides adrese
* Galvenes kontrolsumma ( Header Checksum) – izmanto, lai notektu kļūdas IPv4 galvenē

*Šie ir galvenie paketes lauki, taču ir vel citi.*

**IPv4 adreses.** Ipv4 adreses decimālais pieraksts ietver 4 ar punktu atdalītus skaitļus no 0 līdz 255 ieskaitot. Adrese satur 32 bitus, kas dod aptuveni 4 miljardus adrešu. 90-to gadu beigās jau tika skatīta adrešu nepietiekamības iespēja.

Noklusējuma vārteja (Default Gateway). Noklusējuma vārteja ir tīkla iekārta (parasti maršrutētājs), kas var pārsūtīt paketes uz citoem tīkliem. Noklusējuma vārtejas raksturiezīmes:

* Tai ir lokālā IP adrese tajā pašā adrešu diapazonā kā citām tīkla iekārtām
* Tā var pieņemt datus no ārējiem tīkliem un nosūtīt tos lokālajām iekārtām (un vice versa)

Noklusējuma vārteja ir nepieciešama, lai nosūtītu paketes ārpus lokālā tīkla. Paketes nav iespējams izsūtīt ārpus lokālā tīkla, ja noklusējuma vārtajas nav, ja tā ir nepareizi konfigurēta vai ja tās savienojums ar ārējiem tīkliem nestrādā.

Tīkla adrešu translēšana (Network Address Translation jeb NAT) ir tehnika IP adrešu saglabāšanai. Tā ļauj privātiem IP tīkliem, kas lieto nereģistrētas IP adreses, pieslēgties internetam. NAT tehnoloģiju izmanto maršrutētājos, parasti, lai savienoto kopā divus tīklus. Tas ļauj translēt privātās (tādas, kas nav globāli unikālas) adrese par legālām tīkla adresēm pirms tās tiek sūtītas arējos tīklos. NAT atļauj vienai iekārtai, piemēram, maršrutētājam, būt kā aģentam starp internetu un lokālo tīklu. Tas nozīmē, ka grupu ar datoriem var reprezentēt ar tikai vienu unikālu IP adresi.

Mūsdienās NAT tiek izmantots, lai saglabātu ipv4 Ieejamās adreses, kuras pakāpeniski izbeidzas.

Publiskajā internetā lietotas IP adreses piešķir IANA(internet assigned numbers authority), kas pieder ICANN(internet corporation for assigned names and numbers). Ip adrešu piešķiršanu interneta pakalpojumu sniedzējiem konkrētos reģionos veic reģionālie interneta reģistri (regional internet registry jeb RIR). Tādi kopā ir 5. Eiropas, Tuvo Austrumu un Centrālāzijas reģionos adrešu piešķiršanu veic RIR “RIPE NCC”.

Ipv4 adrese sastāv no tīkla daļas (network potion) un saimniekdatora adreses (host address).

Internetam pievienotie saimniekdatori var sūtīt informāciju citiem trīs dažādos veidos:

* Uniraide (unicast, one-to-one)
* Apraide (broadcast, one-to-all) adrese – 255.255.255.255
* Multiraide (multicast, one-to-many)

Eksistē arī kādamraide (anycast, one-to-one-of-may), kur dati tiek nosūtīti vienam no grupas ar potenciāliem saņēmējiem, balstoties uz to, kurš no saņēmējiem ir vistuvākais(neobligāti ģeogrāfiski, bet gan saziņas ziņā)(least-expensive routing metric). Šo tehniku bieži izmanto satura piegādes tīklos(CDN), lai panāktu mazākas aizkaves pakalpojuma sniegšanai.

1. IPv6 protokols.

Ipv6 ir jaunākā IP versija, kas nākotnē pilnībā aizvietos ipv4, kas mūsdienās vel ir bieži izmantots.

Ipv4 galvenie trūkumi:

* Adrešu trūkums – ipv4 adrešu diapazonā ir tikai 4 miljardi unikālu adrešu. Arvien populārākas kļūst tīklam pieslēgtās lietu interneta(IoT) iekārtas, arvien vairāk tehnoloģiju pieprasa vienmēr pieslēgtos savienojumus(always-on connectivity) un 3. pasaules valstis kļūst arvien attīstītākas, veidojot lielāku pieprasījumu pēc tīkla iekārtām
* “end-to-end” savienojumu trūkums – tīkla adrešu translācija (NAT), kas ir bieži izmantotoa tehnoloģija ipv4 tīklos, piešķir vesalai grupai ar iekārtām vienu publisku ipv4 adresi. Šī dalītā IP adrese paslēpj gala iekārtas iekšējo adresi. Tas var radīt problēmas iekārtām, kam nepieciešami “end-to-end” savienojumi
* Palielināta tīkla sarežģītība – lai gan NAT ir paildzinājis ipv4 lietojamības mūžu, tas bija domāts tikai kā pārejas mehānisms uz ipv6. NAT padara tīklu sarežģītāku, izveido papildus aiztures, kā arī padara traucējummeklēšanu (troubleshooting) grūtāku

90-to gadu sākumā IETF sāka veidot IP nākamo paaudzi, kas atrisina dažādas ipv4 problēmas, uzlabojumi iekļauj:

* Palielināts pieejamo adrešu skaits – ipv6 adreses izmanto 128 bitu hierarhisko adresāciju
* Uzlabota pakešu struktūra – ipv6 paketes galvenē ir mazāk lauku
* Nav nepieciešamības pēc NAT – lielais skaits iespējamo ipv6 adrešu likvidē NAT vajadzību. Tas arī novērš lieku NAT veidoto aizkavi.

Nav konkrēta datuma, līdz kuram ir plānots veikt pilnīgu pāreju uz IPv6, tādēļ ipv4 un ipv6 tiek lietoti kopā. Ir trīs galvenās metodes ipv4 un ipv6 kopīgai izmantošanai

* Duālais steks (dual-stack) – duālā steka iekārtas darbina gan ipv4,gan ipv6 protokola stekus vienlaikus
* Tunelēšana (tunneling) – metode, kas ļauj transportēt ipv6 paketes pa ipv4 tīklu, ipv4 paketes iekapsulē sevī ipv6 paketes
* Translēšana ( translation) – NAT64 ļauj ipv6 iekārtām komunicēt ar ipv4 iekārtām, izmantojot tehniku, kas ir līdzīga ipv4 NAT. Translēšaā paketestiek dinamiski pārveidotas par tā protokola paketēm, kuras tīkls atbalsta. Šī metode, atšķirībā no tunelēšanas, ļauj tīkliem, kuri atbalsta tikai ipv4, sazināties ar tīkliem, kas atbalsta tikai ipv6

Ipv6 adrešu formāts. Ipv6 sastāv no astoņiem hekstetiem je 16 bitu fragmentiem, ko parasti apzīmē kā četrus bāzes 16 simbolus. Vadošās nulles katrā hekstetā tiek atmestas. Dubultais kols apzīmē virkni ar hekstetiem, kuri sastāv tikai no nullēm. Dubulto kolu drīkst izmantot tikai vienu reizi ipv6 adresē.

Ipv6 ir trīs galvenie kategoriju tipi:

Uniraides adr. (unicast) – ipv6 uniraides adrese identificē interfeisu ipv6 iekārtai

Multiraides adr. (multicast) – ipv6 multiraides adreses tiek izmantotas, lai sūtītu paketi vairākiem galamērķiem

Kādamraides adr. (anycast) – vairākām iekārtām piederošan iena ipv6 adrese. Paketes tiek sūtītas uz vispieejamāko galamērķi

Ipv6 tīkla prefiksi var būt diapazonā no 0 līdz 128 bitiem, tos raksta ar slīpsvītru aiz adreses. Prefiksa garums nosaka to, kura adreses daļa identificē tīklu, kura interfeisu. Ipv6 uniraides adreses var iedalīt 6 kategorijās:

* Globālās uniraides (GUA) – analoga publiskaijai ipv4 adresei. Globāli unikālas, interneā maršrutējamas adreses
* Lokālā kanāla (LLA) (Link-local Addr.) – nepieciešama katrai ipv6 iekārtai. Šī adrese tiek izmantota, lai komunicētu ar citām iekārtām tajā pašā apakštīklā. Maršrutētāji nepārsūta paketes ar LLA galamērķa vai sūtītāja adresi
* Atgriezeniskā (Loopback) – viena adrese, kas ir analoga ipv4 atgriezenisko adrešu diapazonam 127.0.0.0/8 – tā ir ::1/128
* Nonoteiktā (unspecified) – adrese ::/128
* Unikālās lokālās (unique local) – adreses diapazonā fc00::/7. maršrutējamas tikai iekš privātā tīkla, taču ne internetā. Var tikt brīvi (bez reģistrēšanas) lietotas vienas organizācijas vai organizāciju grupas ietvaros
* Iegultās ipv4 (embedded IPv4) – sauktas arī par ipv4 derīgajām ipv6 adresēm (“IPv4-compatible IPv6 address”). Izmanto tunelēšanas nolūkiem

GUA adreses. GUA adrese sastāv no globālā maršrutēšanas prefiksa(Global Routing Prefix jeb GRP), ko piešķir interneta pakalpojumu sniedzējs. Maršrutēšanas prefiksa izmērs parasti ir 48 biti. Tālāk ir apakštīkla identifikators (Subnet IP), kura izmērs ir parasti 16 biti. Tā ir viena no nozīmīgākajām atšķirībām IPv6 – tam pēc dizaina ir atvēlēti biti apakštīklu izveidei. Visbeidzot ir interfeisa identifikators(Interface ID), kas ir ekvivalents ipv4 adreses “host” daļai. Termins “interfeisa identifikators” tiek lietots, jo vienai tīkla iekārtai var būt vairāki tīkla interfeisi, katrs ar savu IPv6 adresi

LLA adreses. Atļauj tīkla iekārtām sazināties ar citām IPv6 iekārtām, taču tikai tā apakštīka ietvaros. Paketes ar LLA adresi netiek maršrutētas. Lai gan GUA adrese nav obligāta, katram IPv6 tīkla interfeisam nepieciešams LLA. Noklusējuma vartejai parasti izmanto maršrutētāja LLA adresi. Ir divas metodes LLA piešķiršanai:

* Statiskā, kur iekārta ir tikusi manuāli konfigurēta
* Dinamiskā, kur iekārta izveido pati savu interfeisa ID, izmantojot gadījumskaitļu ģeneratoru

1. IP virzīšana (routing).

Maršrutēšana ir maršruta noteikšanas metode datu pārraides laikā, ko bieži realizē, izmantojot maršrutēšanas tabulas, kad tīkla iekārta vēlas nosūtīt datus citai tīkla iekārtai, tā izmanto savu maršrutēšanas tabulu, lai veiktu lēmumu, kā to nosūtīt. Ja galamērķa iekārta ir citā tīklā, pakete tiek pārsūtīta noklusējuma vārtejai kas parasti ir maršrutētājs.

Maršrutētājs parasti apskata paketes galamērķa IP adresi, meklē to savā maršrutēšanas tabulā, lai noteiktu, kur to tālāk pārsūtīt. Maršrutēšanas tabula satur sarakstu ar visām zināmajām tīkla adresēm un to, kur nepieciešams pārsūtīt paketi, lai tā nonāktu uz šo adresi. Šos ierakstus sauc par maršrutiem. Maršrutētājs pārsūta paketi, izmantojot vislabāko (tādu, kurš visvairāk sakrīt, “best-matching”) maršrutu.

Maršrutēšanas tabulā glabā 3 dažādu veidu ierakstus:

* Tieši savienoti tīkli ( directly-connected networks) – maršruti, kas ved uz maršrutētājam tieši pieslēgtām iekārtām.
* Tālie tīkli (remote networks) – maršruti, kas ved uz iekārtā, kas ir citos tīklos
* Noklusētais maršruts (default route) – arī maršrutētājiem ir noklusētā vārteja, ko tie izmanto gadījumos, kur to tabulā nav labākā maršruta

Maršrutētāji var uzzināt vairāk par tīkliem vienā no diviem veidiem:

* Manuāli – tālie tīkli tiek manuāli ievadīti maršrutu tabulā, izmantojot statisku maršrutus
* Dinamiski – tālie tīkli tiek automātiski atklāti, izmantojot dinamisko maršrutēšanas protokolu

**Statiskā maršrutēšana.** Statiskie maršruti ir tādi, kas tiek manuāli konfigurēti. Statiskie maršruti iekļauj tālā tīkla adresi, kā arī adresi nākamā lēciena(“next-hop”) maršrutētājam. Ja notiek izmaiņas tīkla topoloģijā, statiskie maršruti netiek automātiski atjaunināti, tādēļ tos nepieciešams manuāli rekonfigurēt. Statiskie maršruti piemēroti maziem tīkliem, kuros nav redundantu posmu

**Dinamiskā maršrutēšana.** Dinamiskie maršrutēšanas protokoli ļauj maršrutētājiem automātiski uzzināt informāciju par tālajiem tīkliem. Maršrutētāji, kas izmanto dinamisko maršrutēšanu, automātiski dalās ar maršrutēšanas informāciju ar citiem maršrutētājiem, automātiski nosaka topoloģijas izmaņas bez tīkla administratora iesaistes. Ja ir izmaiņas tīkla topoloģijā, maršrutētāji dalās ar šo informāciju un automātiski atjaunina savu maršrutēšanas tabulu. Dinamiskie maršrutētāji:

* Atklāj tālos tīklus
* Uztur aktuālu maršrutēšanas informāciju
* Izvēlas labāko maršrutu uz galamērķa tīkliem
* Atrod jaunu maršrutu, ja iepriekšējais maršruts vairs nav pieejams

**Maršrutēšanas informācijas protokols.** Viens no maršrutēšanas protokoliem, ko izmanto IP tīklu iekārtas ir maršrutēšanas informācijas protokols(Routing Information Protocol jeb RIP).

RIP izmanto lēcienu (hops) skaitu, lai noteiktu dažādu maršrutu vērtības. Lēcienu skaits nosaka to, cik iekārtām maršruts “ved cauri”. Liekākā RIP pieļautā lēcienu vērtība ir 15(nesasniedzamiem tīkliem šī metrika ir 16), kas nozīmē, ka RIP nav piemērots lieliem tīkliem.

RIP regulāros intervālos izsūta maršrutēšanas atjauninājumu ziņas (Routing-update messages), kuru sniegtā informācija ļauj tīkla iekārtām uzlabot to maršrutēšanas tabulas. RIP mūsdienās vairs netiek plaši izmantots mazā pieļautā lēcienu skaita, taču Cisco tīkla iekārtas to joprojām atbalsta.

**Pirmā Atvērtā Īsākā Ceļa Protokols** (Open Shortest Path First). Mūsdienās plašāk izmantots protokols par RIP. Sākotnējā versija (OSPF v2) atbalstīja tikai ipv4, taču nākamā versija atbalstīja arī ipv6. OSPF dizainēja IETF un tas mūsdienās ir plaši izmantots korporatīvajos tīklos

1. TCP protokols.

TCP jeb pārraides vadības kontroles protokols (Transmission Control Protocol) ir tīklu protokols, kas strādā OSI līmeņa 4. slānī (transporta) un nodrošina šādas funkcijas

* **Uzticama piegāde** (Reliability, guaranteed delivery) – nodrošina uzticamu datu piegādi, ieviešot mehānismus gadījumiem, kur dati tiek bojāti vai pazaudēti
* **Plūsmas vadība** (Flow control) – nodrošina efektīvāku datu plūsmu starp iekārtām
* **Sekvencēšana** (Sequencing) – nodrošina unikālu marķējumu (labeling) katram datu segmentam, ko saņēmējiekārta izmanto, lai datus saliktu sākotnējā formā. Noderīgi, ja datu segmenti tiek piegādāti nepareizā secībā

Tas nodrošina šīs funkcijas , izmantojot šādas operācijas:

* Saņemto datu apstiprināšana (acknowledgement)
* Neapstiprināto datu retransmisija pēc konkrēta laika
* Datu sūtīšana saņēmēja pieņemamā ātrumā

TCP segmentē augstāku līmeņu protokolu dotos datus jeb sadala tos sīkākās daļās, kas nozīmē ka augstāku līmeņu protokoli var domāt par pārraidītajiem datiem kā vienu kopumu un ļaut TCP organizēt to sadalīšanu.

Lai uzturētu sarunas stāvokli un izsekotu informāciju, TCP izveido savienojumu starp sūtītāju un saņēmēju. Šī iemesla dēļ TCP sauc par savienojumu orientētu protokolu (connection-oriented protocol). Šo savienojumu sauc par sesiju un to ir nepieciešams izveidot pirms datu transmisijas. Sesijas izveides laikā iekārtas sarunā satiksmes daudzumu, kas var tikt pārsūtīts konkrētā laika posmā.

TCP uzticamības dēļ ir pieņemtais transporta līmeņa protokols, piemēram, e-pastu un mājaslapu datu plūsmām, kur datiem ir jāierodas tā, kā tie oriģināli sūtīti.

TCP galvenes lauki kuri aizņem 160 bitus un tie ir:

* **Sūtītāja ports (Source port) –** nosaka sūtītāja lietojumprogrammu
* **Galamērķa ports (Destination port) –** nosaka galamērķa lietojumprogrammu
* **Sekvences skaitlis (Sequence number) –** sekvencēšanas nolūkiem
* **Apstiprinājuma skaitlis (Acknowledgement number) –** izmanto, lai norādītu, ka dati tikuši saņemti un tiek sagaidīts nākamais sūtījums
* **Galvenes garums (Header lenght) –** nosaka TCP segmenta galvenes garumu
* **Rezervētais lauks (Reserved) –** rezervēts nākotnes izmantošanai
* **Kontroles biti(control bits) –** nosaka TCP segmenta mērķi
* **Loga izmērs (Window size) –** nosaka baitu skaitu kas var tikt pieņemts vienlaikus
* **Kontrolsumma (checksum) –** izmanto kļūdu noteikšanai
* **Steidzamības lauks (urgent) –** izmanto lai noteiktu, vai sūtītie dati ir steidzami

**Trīs virzienu rokasspiediens (Three-way handshake)** TCP sesijas izveidei izmanto 3 speciālas kontroles ziņas, lai izveidotu savienojumu IP tīklā. Šīs trīs ziņas ir:

* SYN (*synchronize*) – savienojuma uzsākšanas pakete, kas satur nejauši ģenerētu sekvence skaitli (piemēram, 5432). šis sekvences skaitlis apzīmē sākumu sekvences skaitļiem iekārtas A sūtītajiem datiem.
* SYN-ACK (*synchronize-acknowledgement*) iekārta B atbild pati ar savu sekvences skaitli (piemēram,6501), kā arī iekārtas A sūtīto sekvences skaitli, palielinātu par 1 (5433)
* ACK (Acknowledgement) – iekārta A apstiprina iekārta b sūtīto, atbildot ar iekārtas B sūtīto sekvences skaitli, palielinot par 1 (6502)

Neviens no trīs virzienu rokasspiediena paketēm nenes derīgus datus.

Lai terminētu TCP savienojumu, izmanto FIN (Finish) TCP ziņu, kuru otra iekārta apstiprina ar ACK ziņu.

Gan TCP, gan UDP protokoli izmanto portus(identificējošs skaitlis, kas nosaka, kuram operētājsistēmas procesam jāpiegādā ziņa). Daži bieži sastopami porti ir 443, ko izmanto HTTPS, 25 – ko izmanto e-pastu protokols SMTP.

TCP var būt nepiemērots gadījumos kad svarīga ir maza aizkave, piemēram, VoIP vai interneta video zvanos. Ir gadījumi kur tīkla ugunsmūri bloķē UDP, tādēļ IP telefonijas programmām nācās pāriet uz TCP.

Aplikācijas kas straumē uzglabātus (t.i. ne reāllaika) audio un vide ierakstus, izmanto TCP. Ja tīkls pēkšņi vairs nevar atbalstīt joslas platumu, kas nepieciešams, piemēram, pēc pieprasījuma (“on-demand”) straumētai filmai, programma iepauzē atskaņošanu. Pauzes laikā iespējams redzēt ielādes ekrānu, kura laikā TCP cenšas atjaunot savienojumu.

TCP protokolu izmanto tādi augstāku līmeņu protokoli ka FTP, SMTP, SSH un HTTP. TCP protokols ir augstāka līmeņa protokols pār IP.

TCP atļauj tīkla iekārtām uzturēt vairākus savienojumus vienlaikus.

TCP savienojumu neatļauj veidot multiraides ziņas ( tam ir strikta “viens sūtītājs – viens saņēmējs” politika). Tas nozīmē, ka protokoli, kam jāsasniedz vairāki galamērķi, izmanto UDP transporta līmenī. Piemērs šādam protokolam ir DHCP (*Dynamic Host Configuration Protocol*) jeb dinamiskais saimniek datora konfigurācijas protokols, kas dinamiski piešķir IP adreses un citus tīkla konfigurācijas parametrus tīkla iekārtām.

TCP “pārnēsā” aptuveni 80% interneta satiksmes, pārējo pārnēsā UDP.

**TCP plūsmas kontrole.** Plūsmas kontrole sastāv no diviem galvenajiem kontroles mehānismiem – loga izmērs un maksimālais segmenta izmērs. Loga izmērs nosaka to, cik baiti var tikt pārsūtīti līdz sūtītājs sagaida apstiprinājumu(ACK). Piemēram, ja loga izmērs ir 10,000 baiti, iekārta var sūtīt 10,000 baitu, nesaņemot apstiprinājumu. Loga izmērs tiek iekļauts katrā pieprasījumā, lai to varētu vienkārši dinamiski mainīt, atbildot uz izmaiņām savienojumā, piemēram, pārslodzi tīkla iekārtās. Maksimālais segmenta izmērs (MSS), kura vērtība parasti ir 1,460 baitu, nosaka lielāko segmentu, ko galamērķa iekārta var saņemt vienlaikus. MSS neietver sevī galvenes izmēru

1. UDP protokols.

UDP (User Datagram Protocol) ir labākā mēģinājuma transporta līmeņa protokols, tas ir vienkāršs, salīdzinot ar TCP. UDP atšķirības no TCP:

* UDP nenodrošina sekvencēšanu, dati tiek salikti kopā tādā secībā, kā tiek saņemti
* Nepiegādātie segmenti netiek pārsūtīti
* Nenotiek sesijas izveide

UDP neglabā sarunas stāvokli. Ja nepieciešama uzticama piegāde, izmantojot UDP, tā jāīsteno lietojumprogrammai.

UDP sauc par bezsavienojumu (connectionless) protokolu, tas neveido sesijas un tam nav rokasspiedienu mehānismu. UDP ir ļoti piemērots gadījumiem, kur nepieciešama maza aizture, piemēram tiešsaistes video saziņā un VoIP zvanos. Dzīvā video un audio plūsmas var tolerēt nelielus pakešu zudumus bez pamanāma efekta, kas to padara piemērotus UDP

UDP komunikācijas blokus sauc par datagrammām(datagrams) jeb segmentiem(segments)

UDP galvenie ir tikai 4 lauki un tā aizņem tikai 8 baitus. Katrs lauks aizņem 2 baitus un tie ir:

* Sūtītāja ports (Source port) – identificē sūtītāja aplikāciju
* Galamērķa ports (Destination port) – identificē saņēmēja aplikāciju
* Garums (length) – nosaka UDP datagrammas galvenes garumu
* Kontrolsumma (Checksum) – izmanto kļūdu noteikšanai. UDP kontrolsummu aprēķina no UDP galvenes informācijas, UDP datagrammas datiem, kā arī informācijas no IP paketes (galamērķa IP adreses un sūtītāja IP adreses). Datagrammas ar nederīgu kontrolsummu tiek “izmestas” un par šo kļūdu netiek informēta programmatūra

Ir trīs dažādi aplikāciju veidi, kuriem piemērots UDP:”

* Tiešsaistes video un multimediju lietojumprogrammas – nepieciešama maza aizkave
* Vienkāršas pieprasījuma-atbildes programmas (Request and reply applications) – Programmas ar vienkāršām transakcijām, piemēram, DNS (taču tas var lietot arī TCP)
* Programmas, kas uzticamu piegādi nodrošina pašas – vienvirziena komunikācija, kur plūsmas vadība, kļūdu noteikšana, sūtījumu apstiprināšana nav nepieciešamas vai tiek ieviesta lietojumu slānī

UDP datagrammas var ceļot pa dažādiem maršrutiem, kas var rezulteties ar to, ka tās tiek saņemtas nepareizā secībā. Ja datu secība programmai ir svarīga, tai pašai ir jānodrošina pareiza sekvencēšana.

Tā pat kā ar TCP, UDP ir vairāki labi zināmi jeb reģistrēti porti, piemēram, ports 53 apzīmē DNS. Kad iekārta saņem datagrammas, tā apskata galamērķa portu, lai noteiktu, kurai aplikācijai šie dati ir paredzēti.

Uzsākot komunikāciju, UDP klients pieprasa datus no servera. UDP klienta process dinamiski izvēlas porta skaitli no porta skaitļu diapazona. Šis skaitlis ir sarunas sūtītāja ports (Source port). Galamērķa ports parasti ir kāds no labi zināmajiem jeb reģistrētajiem portu skaitļiem. Pēc tam, kad klients ir izvēlējies sūtītāja un galamērķa portus, šis portu skaitļu pāris tiek iekļauts visu datagrammu galvenēs šīs transakcijas ietvaros. Servera sūtītajās datagrammās šie portu skaitļi ir apmainītie vietām.

UDP var tikt izmantot DDoS uzbrukumos, kur uzbrucēji, neveicot sesijas izveidi, uz servera nosūta lielu skaitu UDP datagrammu uz nejaušiem portiem. Serveris ir spiests atbildēt ar ICMP ziņu, kura paziņo, ka konkrētais ports nav pieejams. Šādu ICMP atbildes ziņu ģenerēšana var aizņemt pietiekami daudz datora resursu, neatļaujot tam atbildēt uz reāliem pieprasījumiem.

TCP un UDP portus var iedalīt vairākās kategorijās:

* Labi zināmie porti (well-known ports) – porti diapazonā no 0 līdz 1023. Unix bāzētās sistēmās nepieciešamas superlietotāja tiesības, lai izmantotu šos portus. Definēti bieži izmantotiem servisiem, piemēram, tīmekļa pārlūkprogrammām
* Reģistrētie porti (Registered ports) – porti diapazonā 1024 – 49151. tos specifiskiem servisiem atvēl IANA
* Dinamiskie poerti ( Dynamic ports, Ephemeral ports) – porti diapazonā 49152 – 655353. Šos portus nav iespējams reģistrēt ar IANA. Lieto privātiem servisiem vai gadījumus, kur ports ir nepieciešams īslaicīgi

UDP lietojošo protokolu piemēri:

* DNS – DNS nepieciešams iegūt atbildes ar īsu aizkavi (jāpebilst, ka “DNS-over-HTTPS” izmanto TCP; komunikācijas starp diviem DNS serveriem izmanto TCP)
* RIP (Routing Information Protocol) – RIP ir uz apraides bāzēts protokols, taču TCP atļauj tikai uniraides ziņu apmaiņu

1. Populārākie lietojumu slāņa protokoli un pielietojumi.

DNS (Domēnu Vārdu sistēma) – ports 53 – glabā domēnu vārdiem atbilstošās IP adreses. Šis serviss ļauj gala lietotājiem izmantot domēnu vārdus, ko ir vienkāršāk atcerēties cilvēkam, IP adrešu vietā. Šis serviss ļauj domēnu īpašniekiem mainīt savu domēnu IP adreses, nemainot pašu domēnu. Tas nozīmē, ka gala lietotājiem domēna IP adreses maiņa ir neredzama un neizraisa apgrūtinājumus. DNS standarti nosaka pieprasījumu un atbilžu formātu. DNS komunikāciju vienību sauc par ziņu (mesaage). Ziņas tiek izmantotas, lai veiktu pieprasījumus, sūtītu kļūdas un domēnu ierakstus. DNS ieraksts ietver domēna nosaukumu, adresi un tipu. 4 galvenie DNS ierakstu tipi:

* A – gala iekārta ar ipv4 adresi
* NS – autoratīvs vārdu serveris
* AAAA – gala iekārta ar ipv6 adresi
* MX - Pasta serveris

Telnet – ports 23 – telnet ir divvirzienu teksta orientēts protokols, kas nodrošina virtuālu piekļuvi datoram. telnet nav drošs, tā saziņu ietvaros nenotiek šifrēšana, las nozīmē, ka paroles un citi dati tiek sūtīti tīklam un ir pieejami uzbrucējam.

SSH – ports 22 – Nodrošina virtuālu piekļuvi datoram. Salīdzinot ar Telnet, SSH ir drošs, jo komunikācija starp ierīcēm caur tīklu tiek šifrēta un tiek nodrošināta droša piekļuve. SSH autentifikācija parasti notiek ar publisko-privāto atslēgu pāri.

DHCP – ports 67;68 – Automātiksi iedala IP adreses un tīkla uzstādījumus. Kad tīkla iekārta, kas ir konfigurēta izmantot DHCP, pieslēdzas tīklam, šis klients apraida DHCP “discover” ziņu, lai identificētu pieejamos DHCP serverus. DHCP serveris atbild ar ipv4 adresi, apakštīkla masku, ipv4 DNS servera adresi un ipv4 noklusējuma vārtajas adresi.

HTTP – ports 80 – paredzēts datu apmaiņai starp tīmekļa serveriem un pārlūkprogrammām. HTTP definē ziņas tipu jeb modeli. 3 populārās HTTP metodes:

* GET – klients pieprasa datus serverim
* POST – klients sūta datus serverim
* PUT – augšuplādē resursu, piemēram, attēlu, uz serveri

SMTP – ports 25; 465 – paredzēts saziņai starp epastu serveriem. Definē pieprasījumu galvenes un datu formātu. Kad klients suta epastu, kllienta SMTP process savienojas ar SMTP serveri un cenšas nosūtīt ziņu. Serveris nosaka, vai ziņa ir lokāla, atbilstoši izvēloties, vai to pārsūtīt uz citu serveri vai nē.

1. Enkapsulācijas/dekapsulācijas procesi.

Datu enkapsulācija ir process kurā dati nonāk no augstākie sļāņiem OSI modelī uz zemākiem, katrā slānī tiek pievienota protokolu informācija. Kad ta ir nonākusi līdz zemākajam slānim, tad tā ir beidzot gatava sūtīšanai. Kad tā sasniedz Tīkla piekļuves slāni pēc TCP/IP modeļa headeris jeb galvene tiek izveidota un mac adrese tiek pievienota. Tad tā ir saucama par frame jeb rāmi. Tieši tāpat katrā slānī tiek pievienoti protokolu dati. Dekapsulācija ir pretējais process ir datu izņemšana no rāmja

Datu enkapsulācija nodrošina trīs primāras funkcijas:

* kadra noteikšana/atpazīšana;
* Adresēšanu;
* Kļūdu noteikšanu.

Datu enkapsulācijas process iekļauj kadrs salikšanu pirms pārsūtīšanas kā arī tā pārsēšanu, kad tas tiek saņemts. kadrs veidošanas procesā MAC slānis pievieno headeri un traileri 3. līmeņa PDU. kadra lietošana palīdz bitu pārsūtīšanas procesā, kad tie tiek ievietoti pārsūtīšanas vidē, kā arī bitu grupēšanā tur, kur biti tiek saņemti.

“kadrēšanas process” nodrošina svarīgus atdalītājus, kas tiek izmantoti, lai identificētu bitu grupu, kas veido “kadru”;. Šis process nodrošina sinhronizāciju starp sūtītāj un saņēmēj ierīcēm.

Vēl enkapsulācija nodrošina Data Link (Datu posma) slāņa adresēšanu. Katrs Ethernet “headeris”, kas pievienots “kadram” satur fizisko adresi(MAC adresi), kas ļauj “kadru” nogādāt gala ierīcei.

Papildus funkcija datu enkapsulācijai ir kļūdu noteikšana. Katrs Ethernet “kadrs” satur “asti” (trailer - asti) ar cyclic redundancy check (CRC) ar rāmja saturu. Kad “kadrs ir saņemts”, saņēmējierīce uzģenerē savu CRC un salīdzina ar to, kas ir saņemts. Ja šīs vērtības sakrīt, tad var uzskatīt, ka “kadrs” ir saņemts bez kļūdām.

Kad signālu plūsma ir nonākusi līdz saņēmēja datoram, to virza pa līmeņiem uz augšu, līdz kamēr sasniedz lietojumu līmeni, kurā attiecīgā programma saņem sākotnējo pieprasījumu. Šo procesu, savukārt, sauc par dekapsulēšanu. Iekapsulēšanas procesā informācija tiek dalīta aizvien sīkākās daļās un apaudzēta ar papildus dienesta informāciju. Dekapsulēšanas gaitā, savukārt informācijas fragmentiem ņem nost papildus informāciju un savieno tos kopā, lai iegūtu katram nākamajam līmenim paredzētu atjaunotu informāciju līdz pašās beigās nonāk līdz derīgajai informācijai.

1. DNS sistēma.

Tā kā atcerēties konkrētas iekārtu adreses, lai piekļūtu tīkla resursiem ir ļoti nepraktiski, tiek izmantoti domēnu nosaukumi. DNS protokols definē automatizētu servisu, kas ļauj atrast domēnu vārdiem atbilstošās IP adreses. DNS specifikācijas nosaka pieprasījumu (queries) un atbilžu formātu. DNS protokola komunikācijas izmanto ziņas (messages). Ziņas var pārnēsāt gan pieprasījumu informāciju, gan atbilžu informāciju, gan kļūdas.

DNS apmaiņas struktūra ir aptuveni šāda:

* Saimniekdators vēlas veikt pieprasījumu uz domēnu, kuram tas nezina IP adresi, piemēram <https://google.com>
* DNS pieprasījums tiek nosūtīts uz klienta konfigurēto DNS serveri
* DNS serveris atrod FQDN (*fully qualified domain name*) atbilstošo ierakstu
* DNS serveris atbild klientam ar pieprasītā FQDN IP adresi
* Klients veic pieprasījumu uz FQDN adresi

DNS serveri uzglabā dažādu tipu ierakstus. Ieraksti satur vārdu, adresi un ieraksta tipu. Daži no ierakstu tipiem ir:

* A – gala iekārta ar ipv4 adresi
* NS – autoratīvs vārdu serveris
* AAAA – gala iekārta ar ipv6 adresi
* MX - Pasta serveris

Kad klients veic pieprasījumu, DNS serveris vispirms apskata savus ierakstus. Ja pieprasītais domēns nav pieejams tā ierakstos, tas sazinās ar citiem DNS serveriem. Pēc tam, kad ir atrasts atbilstošais ieraksts, DNS serveris īslaicīgi uzglabā šo ierakstu, lai gadījumā, kur domēns tiek pieprasīts velreiz, DNS serverim tas jau būtu pieejams. DNS ziņa satur 4 galvenos laukus:

* Jautājums (*Question*) – jautājums vārdu serverim
* Atbilde (*Answer*) – ieraksts, kas atbild jautājumu
* Autoritāte (*Authority*) – ieraksts, kas norāda uz autoritāti atbilstošajam domēnam
* Citi (*Additional*) – ieraksts, kas norāda papildu informāciju

DNS parasti izmanto UDP segmentus to mazās aizkaves dēļ, taču ar dažiem izņēmumiem, piemēram:

* Ja DNS pieprasījums ir pārāk liels
* Saziņais starp DNS serveriem
* “DNS-over-HTTPS”

Šajos izņēmuma gadījumos tiek lietots TCP. DNS protokols izmanto hierarhisku sistēmu, kuras hierarhiju nosaka domēna vārds.

Domēna vārdu struktūra ir sadalīta mazākās zonās. Katrs DNS serveris uztur konkrētu datubāzes failu un ir atbildīgs tikai par konkrētiem vārda-uz-IP ( “name-to-IP”) pieprasījumiem. Kad DNS serveris saņem pieprasījumu, kas ir ārpus tā zonas, tas pārsūta šo pieprasījumu citam DNS serverim. Šī tehnika padara DNS sistēmu efektīvāku, jo katram serverim nav jāuztur pilnā DNS datubāze.

Domēniem ir vairākas daļas, piemēram augšējā līmeņa domēns (top-level domains), kas parasti nosaka vai nu organizācijas, kurai pieder domēns, tipu, vai valsti. Piemēri augšējā līmeņa domēniem:

* .com – biznesiem
* .org – bezpeļņas organizācijām
* .au – Austrālijai
* .lv – Latvijai

Augšējā līmeņa domēnus iedala vairākās kategorijās, piemēram:

* ccTLD (coutry code top-level domain) – vienmēr 2 simbolus garš augšējā līmeņa domēna vārds, ko lieto valstīm, kuras identificētas ar valsts kodu
* gTDL (generic top-level domains) – vienmēr garāks par 2 simboliem, lieto vispārīgiem nolūkiem

ir divi DNS servisu tipi:

* **Autoratīvie DNS (Authorative DNS) –** autoratīvajiem DNS serveriem ir autoritāte pār kādu reģionu. Tie glabā savas zonas DNS ierakstu tabulu un atbild uz rekursīvo DNS serveru pieprasījumiem.
* **Rekursīvie DNS (recursive DNS) –** rekursīvie DNS serveri neglabā ierakstus ( izņemot īslaicīgi), taču tie zina, kur atrast atbildes.

Lai rekursīvais DNS serveris nonāktu līdz atbilstošajam autoratīvajam DNS serverim, tas veic šādu pieprasījumu virkni:

* Rekursīvais DNS serveris veic pieprasījumu *root* vārdu serverim
* *Root* serveris atgriež adresi augšējā līmeņa domēnu (TDL) DNS serverim, piemēram, . com vai .net serverim
* Rekursīvais DNS serveris veic pieprasījumuTLD DNS serverim, kurš atgriež konkrētā domēna vārdu servera adresi
* Rekursīvais DNS serveris veic pieprasījumu uz DNS vārdu serveri, lai iegūtu domēna adresi

Katru domēna “daļu”, kas atdalīta ar punktiem, sauc par iezīmi (label). Katrs iezīmes maksimālais garums ir 63 simboli, bet visa domēna maksimālais garums ir 253 simboli. Lielie un mazie burti tiek uzskatīti par ekvivalentiem. Domēni var izmantot alfanumeriskos simbolus un defises, tomēr tie nevar sākties vai beigties ar defisi

1. Kādas datortīkla plūsmas notiek, atverot Tīmekļa vietni.
2. Cisco IOS lietošana un iekārtas konfigurēšana..

Cisco IOS ir operētājsistēma, ko izmanto Cisco tīkla iekārtas – maršrutētāji un komutatori

Cisco IOS ir divi dažādi komandu izpildes režīmi

* Lietotāja režīms jeb “EXEC”, ļauj veikt dažas apsekošanas komandas, neļauj veikt izmaiņas konfigurācijā
* Priviliģētais režīms jeb “Privileged EXEC”, ļauj veikt sistēmas izmaiņas

Priviliģētajam režīmam ir vairāki apakšrežīmi. Lai konfigurētu iekārtu, lietotājam ir jāieiet globālās konfigurācijas režīmā, no kura iespējams veikt vispārīgas izmaiņas iekārtai. Globālajam konfigurācijas režīmam nepieciešams piekļūt pirms lietotājs var ieiet kādā no specifiskajiem konfigurācijas režīmiem, piemēram:

* Līnijas konfigurācijas režīms (Line Configuration Mode) – izmanto, lai konfigurētu konsoles, SSH un Telnet piekļuvi
* Interfeisa konfigurācijas režīms (Interface configuration mode) – izmanto, lai konfigurētu komutatora portus un maršrutētāja interfeisus

Lai nokļūt dažādam režīmam, ir jālieto komandas (neņemot vērā paroles):

* User EXEC - nekas nav jāraksta
* Privileged EXEC - “enable” lai piekļūtu pie tā, “disable” lai atslēgtos no priviliģētā režīma
* Global Configuration - “configure terminal” lai piekļūtu globālai konfigurācijas režīmam, “exit” lai izietu no režīma. “exit” komanda ir lietota visiem konfigurācijas režīmiem, to vietā var arī lietot kombināciju Ctrl+Z.
* Line Configuration - ir jāraksta šādi (viss kopā vienā līnijā):
  + “line” - sākums
  + “console” - vadīšanas līnījas tips (console kā piem.)
  + “0” - numuris, kuram gribam piekļut (0 kā piem.)
* Interface configuration - ir jāraksta šādi (viss kopā vienā līnijā):
  + “Interface” - sākums
  + “FastEthernet 0/1” - interfeisa identifikācija (FastEthernet 0/1 kā piemērs).

Iekārtu konfigurācijas pamati

Iekārtu pārsaukšana. Iekārtas iespējams pārsaukt, lai tās var vieglāk identificēt. Pēc noklusējuma Cisco komutatoriem ir vārds “Switch”, taču tos vēlams mainīt tā, ka to vārdiem ir cilvēka saprotama nozīme, piemēram, “Switch-F2” varētu apzīmēt komutatoru otrajā stāvā. Iekārtu nosaukumos nedrīkst būt atstarpes un jāsākas ar burtu, drīkst lietot tikai burtus, ciparus un domuzīmes.

Paroļu iestatīšana. Lai nodrošinātu labāku tīkla drošību, nepieciešams iestatīt iekārtām paroli. To var izdarīt līnijas konfigurācijas režīmā, izmantojot “password” komandu. Parole ir atsevišķi jāiestata konsoles piekļuvei, virtuālā terminālā jeb VTY piekļuvei kā arī priviliģētā režīma piekļuvei.

Paroļu šifrēšana. Pēc noklusējuma paroles konfigurācijas failos var redzēt nešifrētas, tas ir drauds tīkla drošībai. Lai liktu komutatoram šifrēt visas paroles, globālās konfigurācijas režīmā nepieciešams lietot komandu “service password-encryption”. Komandas nolūks ir neatļaut neautorizētiem lietotājiem apskatīt paroles konfigurācijas failā.

Cisco iekārtām ir divu veidu konfigurācijas:

* Startup-config – saglabātais konfigurācijas fails, kas tiek glabāts NVRAM. Šī konfigurācija tiek glabāta arī pēc iekārtas izslēgšanas.
* Running-config – tiek glabāts RAM, izmanto pašreizējai konfigurācijai. Šī faila izmainīšana rezultējas tūlītējas izmaiņās iekārtas konfigurācijā.

Ja ir nepieciešamība pašreizējo konfigurāciju saglabāt arī pēc iekārtas izslēgšanas , nepieciešams to pārkopēt startup-config vietā, izmantojot “copy” komandu

1. Datoru tīklu drošība

4 galvenie uzbrukuma mērķi:

* Informācijas zādzība – ielaušanās datorsistēmā, lai iegūt konfidenciālu informāciju kas var tikt pārdota vai izmatota citiem nolūkiem
* Datu zaudēšana/iznīcināšana un manipulācija -ielaušanās datorsistēmā lai iznīcinātu vai mainītu ierakstus/datus
* identitātes zādzība – personīgās informācijas zādzība ar nolūku pārņemt cilvēka identitāti. Izmantojot šādu personīgo informāciju iespējams ,piem., pieteikties aizdevumiem, veikt neautorizētus pirkumu un citas darbības.
* Pakalpojumu/servisa traucējumi -traucējumu izraisīšana, kas liedz sistēmas lietotājiem tai piekļūt pilnvērtīgi.

Ievainojamība ir tīkla vai ierīces vājuma pakāpe. Noteikta ievainojamības pakāpe ir raksturīga maršrutētājiem, komutatoriem, galddatoriem, serveriem un pat drošības ierīcēm. Parasti uzbruktās tīkla ierīces ir galapunkti, piemēram, serveri un galddatori.

Pastāv trīs galvenās ievainojamības jeb vājās vietas:

* Tehnoloģiskās ievainojamības var ietvert TCP/IP protokola vājās vietas, operētājsistēmas vājās vietas un tīkla aprīkojuma vājās vietas.
* Konfigurācijas vājās vietas var ietvert nenodrošinātus lietotāju kontus, sistēmas kontus ar viegli uzminamām parolēm, nepareizi konfigurētus interneta pakalpojumus, nedrošus noklusējuma iestatījumus un nepareizi konfigurētas tīkla iekārtas.
* Drošības politikas vājās vietas var būt rakstiskas drošības politikas trūkums, politika, autentifikācijas nepārtrauktības trūkums, nepiemērotas loģiskās piekļuves kontroles, programmatūras un aparatūras instalēšana un izmaiņas, kas neatbilst politikai, un neesošs avārijas seku novēršanas plāns.

4 galvenie fiziskās drošības draudi:

* Bojājumi aparatūrai
* Nepiemērota vide – pārāk augsta vai zema temperatūra, neatbilstošs gaisa mitrums.
* Elektriskie bojājumi – sprieguma pīķis, nepietiekams spriegums, elektrības padeves zudums.
* Uzturēšanas saistīt draudi – nepietiekams rezerves daļu trūkums, nepareiza kabeļu instalācija

Ir 3 galvenie ļaunprogrammatūras tipi:

* Vīrusi – vīrusi izplatās, pievienojot savu kodu citām programmām. Gandrīz visi vīrusi ir saistīti at kādu izpildāmu failu, kas nozīmē, ka tie nevar strādāt līdz lietotājs nam palaidis saistīto failu.
* Tārpi – līdzīgi vīrusiem, jo cenšas izplatīties uz vairākām iekārtām, taču tārpi neprasa cilvēka darbību, lai izplatītos
* Trojas zirgi – līdzīgi vīrusiem, taču Trojas zirgi neinficē citus failus, tie replicē savu kodu.

Tīkla draudu mazināšana:

* Datu un konfigurācijas failu kopiju veidošana – viena no svarīgākajām tehnikām aizsardzībā prewt datu iznīcināšanas uzbrukumiem, kā arī iekārtu bojājumiem. Pareiza kopiju politika:
  + Kopijas jāveido bieži
  + Jāpārbauda, vai kopijās esošie faili ir pareizi
  + Kopijām jābūt labi aizsargātām ar stiprām parolēm
* Programmatūras atjauninājumu politika – svarīgi lai lietotā programmatūra, tostarp anti-ļaunatūras programmatūra, vienmēr tiktu lietota jaunākajā versijā, viens risinājums šim ir iestatīt programmatūras automātisko atjaunināšanu.
* Autentifikācija, autorizācija, un ierakstu veidošana – autentifikācija nosaka, kurš drīkst piekļūt tīklam, autorizācija nosaka, ko šis lietotājs var darīt un ierakstu veidošana saglabā vēsturi ar lietotāja darbībām.
* Ugunsmūris – aizsargā datorus un tīklus, novēršot nevēlamas datu plūsmas. Tīkla ugunsmūri atrodas starp vairākiem tīkliem, kontrolējot satiksmi starp tiem. Ugunsmūri var būt konfigurēti atļaut pikļuvi ārējiem lietotājiem konkrētam tīkla daļām – t;ados gadījumos šīs iekārtas mēdz tikt novietotas speciālā apakštīklā, ko sauc par demilitarizēto zonu(DMZ). Ugunsmūriem ir četri galvenie tipi:
  + Pakešu filtrēšana – nosaka piekļuvi, balstoties uz ip un mac adresēm
  + Lietojumprogrammu filtrēšana – nosaka piekļuvi, balstoties uz izmantotajiem portiem
  + url filtrēšana – atļauj vai aizliedz piekļuvi konkrētiem URL vai atslēgas vārdiem
  + “Stateful packet inspection” – ienākošajā paketēm jābūt uz iekšējo iekārtu pieprasījumiem