1.OSI modelio sluoksniai. Sluoksnių apibūdinimas. Komunikavimo procesas

OSI modelio sluoksniai ir jų apibūdinimai:

- Taikymo – skirtas vartotojui, pvz. HTTP aprašo sąveiką „naršyklė – WEB serveris".
- Pateikimo – duomenų formatai, šifravimas
- Sesijos – authentifikacija, ryšio paruošimas, eiga ir nutraukimas
- Transporto – apsikeitimas tarp taikomųjų procesų
- Tinklo – transportavimas tinklu, adresacija, maršrutų parinkimas
- Kanalo – kadrai, antraštės, perdavimas tarp gretimų mazgų
- fizinis – signalai, jungtys, dažniai ir pan.

Komunikavimo procesas:

1. Taikymo sluoksnis – vartotojas naudojasi naršykle ir per ją kreipiasi į inklo paslaugą
2. Taikymo sluoksnis – naršyklė prie vartotojo duomenų prideda antraštę
3. Taikymo sluoksnis – naršyklė prie vartotojo duomenų prideda antraštę ir perduoda paketą transporto sluoksniui TCP
4. Transporto sluoksnis – TCP formuoja sujungimo su paslauga prašymo paketą (SYN), antraštėje nurodo paslaugos rūšį (pvz. portą 80) ir atidaro savo portą (pvz. 1212) duomenų priėmimui
5. Transporto sluoksnis – perduoda paketą tinklo sluoksniui – IP
6. Tinklo sluoksnis – iš DNS serverio gauna paslaugos IP ir įrašo į antraštę kartu su siuntėjo IP adresu, perduoda į Ethernet sąsają
7. Kanalo sluoksnis – perduoda paketus tik lokaliame tinkle, taigi perduos ne galutiniam gavėjui, o esančiam tarpiniam lokalaus tinklo mazgui (pvz. Maršrutizatoriui). Į antraštę prideda siuntėjo ir savo MAC adresus, išsiunčia paketą.

2.Lokalūs tinklai. Kanalo sluoksnis.Perdavimo metodai lokaliame tinkle.Komutavimo algoritmas. MAC lentelės ir ARP

Lokalūs tinklai:

- Lokalus tinklas – (LAN – Local Area Network) yra kompiuterių ar kitų įrenginiš tinklas mažoje teritorijoje. Didžioji dalis lokalių tinklų apsiriboja viename pastate.
- LAN'e naudojamos paprastos ir pigios guomenų perdavimo technologijos.
- Kiekvienas LAN įrenginys veikia autonomiškai ir automatiškai.

Kanalo sluoksnis:

- Kanalo sluoksnis užtikrina duomenų paketų formavimą ier perdavimą tarp gretimų tinklo mazgų.
- Formuojant paketą į antraštę įrašomi gavėjo ir siuntėjo MAC adresai.
- Kanalo sluoksnyje įrenginys turi turėti atmintinę priimtam duomenų paketui įsiminti.

Perdavimo metodai lokaliame tinkle:

- Transliacijų metodas – visi įrenginiai sujungti taip, kad bet kuris signalas pasiekia visus.
- Paketų komutavimo metodas – centrinis tinklo įrenginys su galiniais mazgais sujungtas atskirais ryšio kanalais. Tinklo įrenginis turi teisingai paskirstyti atėjusius paketus prijungtiems prietaisams.

Komutavimo algoritmas:
Priimti į jungtį X ateinantį paketą. Žiūrėti siuntėjo ir gavėjo adresus.

1. Apsimokymas pagal siuntėjo adresą:

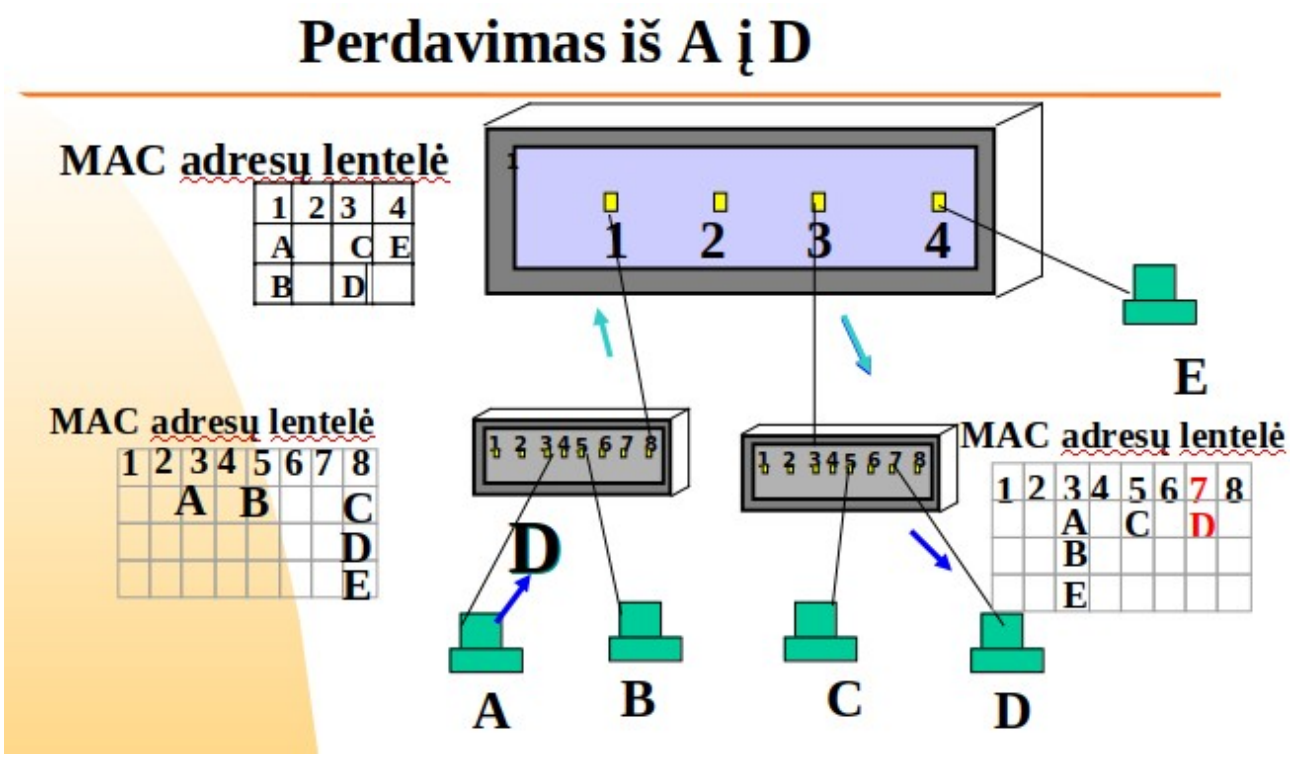
- Jei siuntejo adreso dar nėra MAC lentelėje, įrašyti į MAC adresų lentelę (X, naujas_siuntėjo adresas)
- Jei siuntėjo adresas yra MAC lentelėje, tačiau ten nurodyta kita jungtis, pakeisti įrašą MAC adresų lentelėje

2. Persiuntimas pagal gavėjo adresą:
Nustatyti išėjimo jungtį Y iš MAC adresų lentelės pagal gavėjo adresą.

- Jei X=Y paketą sunaikinti
- Jei X!=Y paketą perduoti į Y
- Jei gavėjo adreso nėra lentelėje, paketą paskleisti per visas jungtis išskyrus X

3. Išmesti įrašus, kuriems baigėsi galiojimo laikas iš MAC adresų lentelės

MAC lentelė:



ARP:
ARP (Address Resolution Protocol) – tai broadcast užklausa, siunčiama visiems lokalaus tinklo kompiuteriams. Tas kompiuteris, kuris turi nurodytą IP adresą atsako pranešdamas savo MAC adresą. Gautas adresas įrašomas į laikiną lentelę, daugiau klausti [laikinai] nebereiks.

3. IEEE 802 standartai. MAC adresai. Ethernet paketo struktūra. Komutatoriai, jų rūšys ir savybės

IEEE 802 standartai – aprašo duomenų perdavimo spartą, ryšio terpes ir atstumus. Visi naudoja tą patį Ethernet paketo formatą, todėl tarpusavyje suderinami.

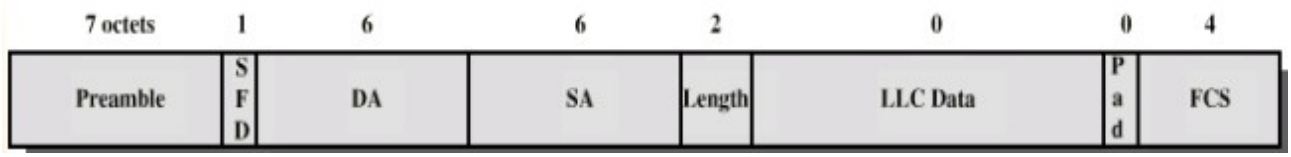
Standartai:

- 10 Mbps IEEE802.3
- 100 Mbps IEEE802.3u
- 1000 Mbps IEEE802.3z
- 10 Gbps IEEE802.3ae
- 40 ir 100 Gbps IEEE802.3bm

MAC adresai:
MAC adresas (Ethernet adresas) susideja iš dviejų dalių po 3 baitus:
gamyklai suteiktas + mazgo eilės numeris

Visuotinis (broadcast) adresas yra FF:FF:FF:FF:FF:FF
Svarbu, kad lokaliame tinkle MAC adresas butų unikalus

Ethernet paketo struktūra:



- Preamble – imtumo sincronizacijai
- SDF – kadro pradžios žymė
- DA – gavėjo adresas

- SA – siuntėjo adresas
- Length – paketo ilgis
- LLC Data – duomenys + kamšalas
- FCS – paketo kontrolinė suma (pvz. 5827: 5+8=1**3**+**2**=5+7=1**2**=2)

Komutatoriai, jų rūšys ir savybės:
Komutatorius:

- Komutuoja gautą paketą į tam tikrą jungtį pagal gavėjo MAC adresą
- Automatiškai susiformuoja MAC adresų lentelę
- Nekeičia paketo
- Nereikalauja konfigurafimo
- Neturi jokių adresų

Rušys:

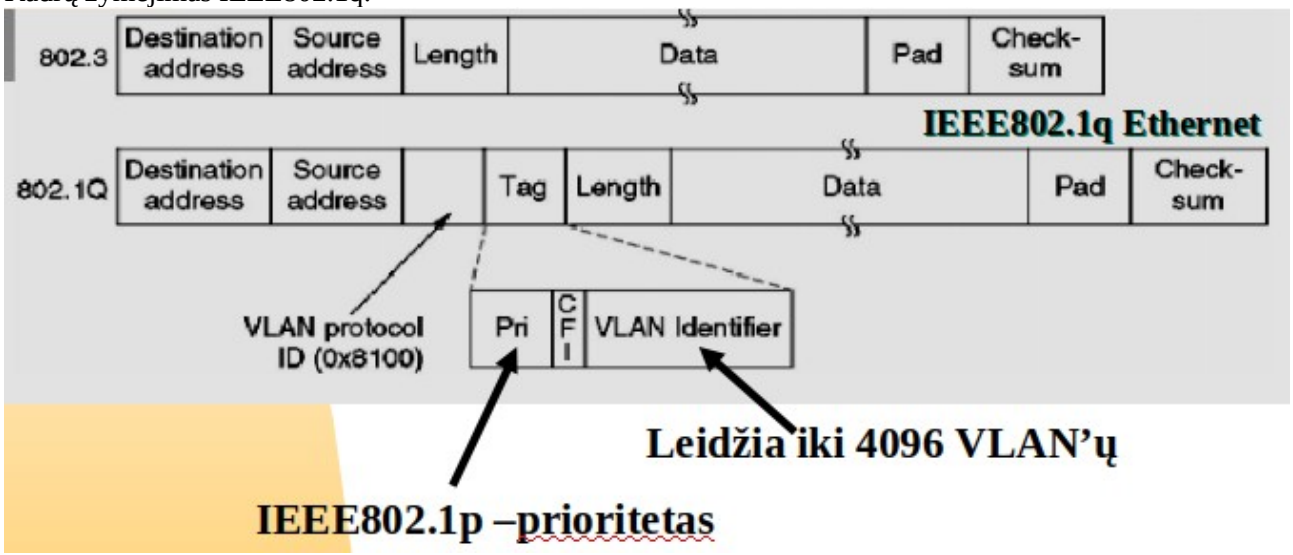
- Nevaldomi LAN komutatoriai – jungtys gali dirbti skirtinguose režimuose. Turi automatinį režimo nustatymą: sparta/dupleksas
- Valdomi ir konfiguruojami komutatoriai, savybės:
  - MAC adress filtering
  - Spanning tree
  - Port mirroring
  - VLAN

4. Virtualūs lokalūs tinklai, Kadrų žymėjimas IEEE802.1q

Virtualūs tinklai:
Skirtingos paskirties įrenginius galima jungti prie to paties komutatoriaus. Tam pačiam LAN priklausantys įrenginiai gali būti prijungti prie skirtingų komumtatorių.

1. Komutatorius sadalinamas į keletą virtualių komutatorių suteikiant skirtingas VLAN žymes(numerius) jungtims
2. Kiekvienas VLAN turi nuosavą MAC adresų lentelę ir neturi jokio ryšio su kitais.
3. Komutatoriai tarpusavyje sujungiami bendromis jungtimis
4. Kad perduodant bendru kanalu paketai nesusimaišytų, komutatorius jų antraštes papildone VLAN žyme.

Kadrų žymėjimas IEEE802.1q:



Atrodo kaip įprastas Ethernet paketas, tik papildytas VLAN žyme

5. Pasiekiamumo kontrolės sąrašai. ACL savybės. Adresų segmento aprašas. ACL naudojimas

Pasiekiamumo kontrolės sąrašai – skirti apsauginėms užkardoms be vidinės būsenos (stateless firewall) realizuoti. Jie diegiami maršrutizatoriuose arba specialiuose srautų filtravimo stotyse (pvz. Linux iptables pagrindu)

ACL savybės:

- Paketų tikrinimas pagal nurodytą filtrą vykdomas nustatytoje maršrutizatoriaus sąsajoje.
- Filtras gali būti taikomas arba įeinantiems į maršrutizatorių per šią sąsają paketams (in) arba išeinantiems iš jo (out).
- Kiekvienas persiunčiamas ta kryptimi paketas tikrinamas ar atitinka kurios nors taisyklės aprašą.
- ACL rezultatas gali būti permit (leisti) arba deny (drasti) paketus.
- Kai tik randama tinkama taisyklė, vykdomas joje nurodytas permit/deny veiksmas, tolesnės taisyklės nebetikrinamos.
- Sąrašo pabaigoje visada taikoma taisyklė deny ip any any

Adresų segmento aprašas:
Adresų segmentas, kuriam taikoma taisyklė aprašomas nurodant segmento pradini adresą ir šabloną (wildcard).

	Užrašas su kauke	Užrašas su šablonu
Vienas adresas	1.1.1.1 255.255.255.255	1.1.1.1 0.0.0.0 host 1.1.1.1
Segmentas /24	1.1.1.0 255.255.255.0	1.1.1.0 0.0.0.255
Segmentas /28	2.2.2.0 255.255.255.240	2.2.2.0 0.0.0.15

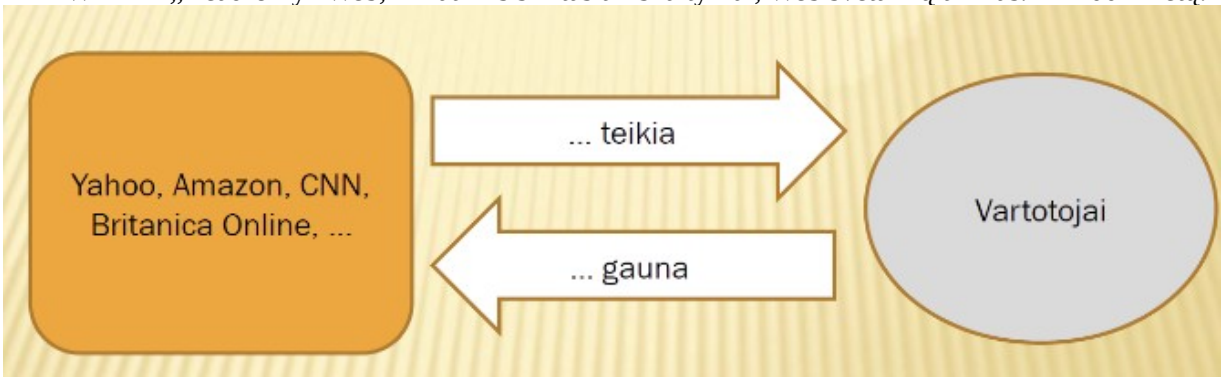
ACL naudojimas:

1. Blokuoti (deny) komunikavimui pakanka blokuoti paketus bent viena kryptimi.
2. Leisti išimtinį duomenų apsikeitimą (permit) būtina iš abiejų pusių.
3. Jeigu jungtyje nėra jokio ACL, joje visi paketai leidžiami.
4. Sąrašo pabaigoje automatiškai taikoma taisyklė „blokuoti viską”. Norint blokuoti tik atskirą atvejį, būtina gale pridėti permit (pvz. deny ip 1.1.1.0 0.0.0.255 host 3.3.3.20, permit ip any any)

6. WEB kartos: WEB1, WEB2, WEB3. HTML5 principai, skirtumai nuo ankstesnių versijų.

WEB kartos: WEB1, WEB2, WEB3.

- WEB1 - „Read-only” Web, žiniatiklis skirtas tik skaitymui, Web svetainių tinklas. Iki 2004 metų.



- WEB2 - „Read-Write” Web, žiniatiklis ir skaitymui ir rašymui. Tai tarsi didelė kompiuterinė sistema (platforma), kuriai kurioje kuriami ir vykdomi įvairūs uždaviniai. Interneto turinį bendradarbiaudami gali kurti visi

- WEB3 – pritaikytas mobiliems prietaisams. Apie 50% vartotojų naršo per mobilųjų telefoną. Galimybes išnaudoti vartotojo kontekstą (pvz. Vietą). Atviri standartai. Suderintos sistemos.

HTML5 principai, skirtumai nuo ankstesnių versijų:
HTML - tai kompiuterinė žymėjimo kalba, naudojama pateikti turinį internete.

HTML elementas turi vardą ir gali turėti bet kokį skaičių atributų. Elemento viduje gali būti tekstas bei kiti elementai. Tiek tekstas, tiek ir dukteriniai elementai paprastai gali kartotis ir sekti bet kuria tvarka.

HTML4+CSS3+JS=HTML5

2009m buvo patvirtitas HTML5. HTML5 keičia ir HTML4, ir XHTML1, bet išlieka suderinamas su jais. Naujas standartas smulkiai ir iki galo tiksliai aprašo kaip naršyklės turi vienodai atvaizduoti tinklapius.

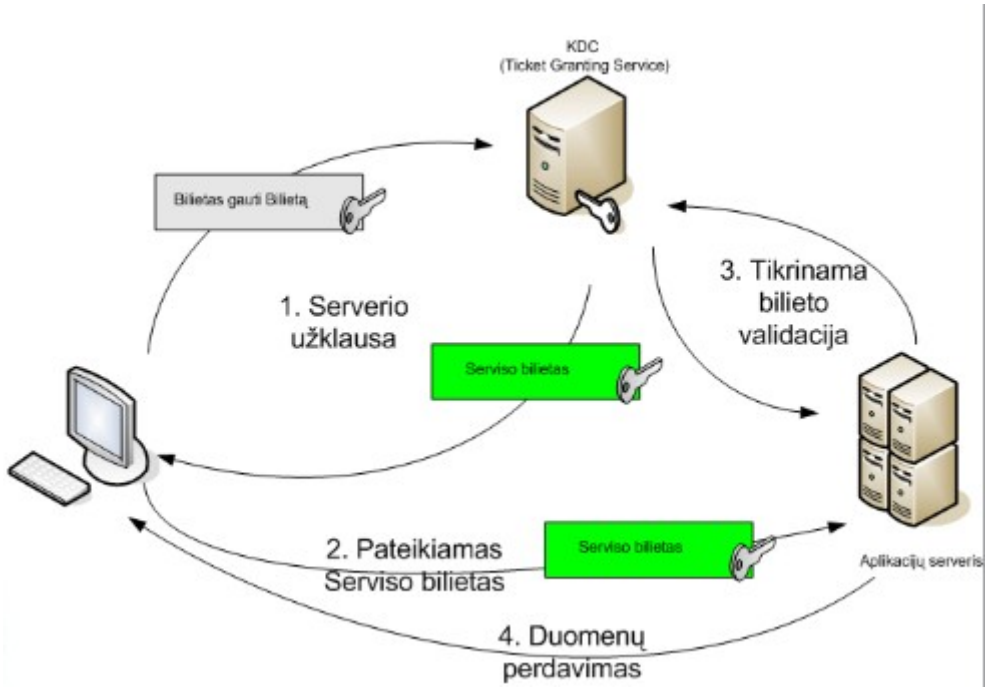
7. Autorizacija, prieigų nustatymo mechanizmai. Autentifikacijos metodai Kerberos, CHAP, EAP

Objektas – failas
Subjektas - vartotojas

Autorizacija – tam tikrų teisių suteikimas subjektui, kad jis galėtų pasiekti objektą.

Prieigų nustatymo mechanizmai:
- DAC (Discretionary Access Control)– kiekvienas objektas turi sąrašą, aprašantį, kokie subjektai turi konkrečias teises (skaityti, rašyti, vykdyti)
- RBAC (Role-based Access Control)– prieigos kontrolė priklauso nuo rolės. Subjektai priklauso konkrečiai rolei. Subjektas gali priklausyti tik vienai rolei. Prieigos teisės aprašomos rolėmis.
- MAC (Mandatory Access Control) – privaloma teisių valdymo strategija. Failo savininkas neturi galimybės sutekti sukurtam failui teisių.

Kerberos:



CHAP (Challenge Handsake Authentication Protocol) – buvo plėtojamas kaip dalis TCP/IP point-to-point protokolo (PPP), naudojamo perduoti TCP/IP duomenis per dial-up sujungimus. Jis buvo apibūdintas RFC dokumente 1994 metais.

EAP (Extensible Authentication Protocol) – suteikia struktūrą skirtingoms autentifikacijos technologijoms. Jis plačiai taikomas nuotoliniams ryšiams ir wireless autentifikacijai. EAP naudojamas kartu su smard card'ais ir biometrika ar paprastesniais duomenimis (vartotojo vardai ir slaptažodžiai).

8. Viešųjų raktų infrastruktūra. Sertifikatai. Sertifikato pasirašymas su CA

Viešųjų raktų infrastruktūra – yra technikinės, programinės įrangos, žmonių ir procedurų visuma, kuri naudojama saugoti, kurti, valdyti, suteikti, atnaujinti sertifikatus viešojo rakto kriptografijos metodais.

Taikoma:
- Elektroniniams parašams
- El. paštui šifruoti
- Dokumentams šifruoti ir autentifikuoti

Sertifikatai – generuojamos Viešo ir Privataus rakto poros
Sertifikatuose gali būti naudojami šifravimo būdai:
- Simetrinis
- Asimetrinis
- Hibridinis

Sertifikato pasisrašymas su CA:
1. Sukuriamas vartotojo privatus raktas
2. Sukuriamas sertifikato pasirašymo prašymas
3. Sertifikato pasirašymas su CA

9. Transporto sluoksnis. Prievadai (portai). Klaidų taisymas ir spartos reguliavimas. Siuntimo lango metodas

Transporto sluoksnis:
- Aprašo duomenų mainus tarp tinklinių taikomųjų procesų
- Tinklo sluoksnis pristato duomenis į nurodytą tinklo mazgą. Išpakuotų duomenų srautą konkrečiam taikomajam procesui atiduoda transporto sluoksnis.
- Tai paskutinis OSI modelio sluoksnis, kuriame numatytas duomenų perdavimo klaidų taisymas

Funkcijos:
- Keistis duomenimis tarp taikomųjų procesų → prievadai (port)
- Taisyti perdavimo klaidas → patvirtinimai (ACK)
- Valdyti duomenų siuntimo spartą → siuntimo langas

Prievadai (portai):
- Į transporto sluoksnį ateinantys paketai rikiuojami į atskiras eiles kiekvienam taikomąjam procesui, veikiančiam tame kompiuteryje
- Duomenų paketų eilė prie taikomojo proceso vadinamas prievadu
- Prievadų numeriai tai yra transporto sluoksnio paketų adresai
- Standartiniams taikomiesiems procesams skirti fiksuoti prievadų numeriai. Juos nustato IANA – Internet Assigned Numbers Authority

Klaidų taisymas ir spartos reguliavimas:
- Siuntėjas numeruoja siunčiamų duomenų porcijas ir kiekvienai iš jų per nustatytą laiką Δt turi gauti patvirtinimą ACK (Acknowlegment) iš gavėjo.
- Nesulaukus ACK per nustatytą laiką Δt, duomenų porcijos siuntimas kartojamas
- Kada **siuntėjas** siunčia paketą pakartotinai?
  - Jei per užduotą laiko intervalą negaunamas ACK, laikoma, kad paketas nepasiekė gavėjo arba paketas pasiekė gavėją susgadintas. Reikia kartoti siuntimą.

Siuntimo langas:
- Išsiunčiamos n porcijų paeiliui.
- Kol tebevyksta siuntimas, turėtų ateiti pirmųjų porcijų gavimo patvirtinimas. Taigi, tolesnio siuntimo galima nestabdyti tol, kol kelyje esančių porcijų skaičius neviršys n (n-siuntimo langas)
- Esant idealioms siuntimo sąlygoms n porcijų dydžio langas „slysta“ išsiunčiamų duomenų eile maksimaliai galimu siuntimo greičiu.

10. TCP ir UDP protokolai. TCP savybės. Siuntimo spartos valdymas. Siuntimo klaidų taisymas.

TCP ir UDP protokolai – transporto sluoksnio protokolai:
- UDP – duomenų perdavimas tarp taikomųjų procesų be pristatymo garantijų. UDP paprastas, spartus, nereikia didelių resursų. Gali būti naudojamas multicast režime. Taikomas kai:
  - taikomasis procesas negali laukti, kol kelyje prarasti duomenys bus perduoti pakartotinai, o nedidelė prarastų duomenų neturi didelės įtakos (vaizdas, garsas)
  - arba taikomasis procesas pats rūpinasi duomenų siuntimo pakartojimu
  - arba duomenų perdavimas vyksta rezervuotu kanalu, kuriame paketų praradimo praktiškai nėra
- TCP – duomenų perdavimas tarp taikomųjų procesų su klaidų taisymu.
  - Gali aptarnauti kelis sujungimus tuo pačiu portu
  - Potencialiai skirtingi RTT (reikia adaptyvaus laukimo laiko nustatymo mechnaizmo)
  - Potencialiai didelis vėlinimas ir didelė vėlinimo sklaida (reikia sugebėti atpažinti vėluojančius paketus)
  - Potencialiai skirtingi gavėjo talpumai (reikia reguliuoti siuntimą pagal gavėjo galimybes priimti duomenis)
  - Potencialiai skirtingi tinklo pralaidumai pagal gavėjus/pagal laiką (reikia reaguoti į perkrovas tinkle)

Siuntimo spartos valdymas:
1. TCP bando tinklo pralaidumo galimybes
2. TCP reaguoja į perkrovas sulėtindamas duomenų siuntimą

Siuntimo klaidų taisymas:
- Siuntėjas pats nežino, kokie paketai nepasiekė gavėjo
- Gavėjas turi pranešti siuntėjui apie gautus paketus siusdamas patvirtinimus
- Siuntimo langas mažinamas pusiau, jei per timeout laiką negaunamas patvirtinimas

11. E-pašto protokolai ir struktūra. Protokolai SMTP, MIME, IMAP ir POP

E-pašto protokolai ir struktūra:
- Laiškų persiuntimui naudojamas SMTP protokolas
- Atėjusio laiško paėmimui naudojami POP, IMAP protokolai
- lokali_dalis@pašto_serveris

SMTP:
- Naudoja nuolatinį sujungimą laiško perdavimui
- SMTP yra „push“ protokolas (stumiantis)
- SMTP naudoja kai kuriuos simbolius valdymui, jų negali būti pranešime
- Serveris, priimdamas laišką, įsipareigoja pristatyti jį adresatui arba gražinti klaidos pranešimą
- Laiškas gali pereiti keletą serverių, kol pateks galutiniam adresatui
- Laiškų adresacija vykdoma pagal DNS MX įrašus
- Nėra autentifikacijos – leidimai išsiųsti laiškus apibrėžiami pagal IP adresus

MIME – Mail extensions standartas, leidžiantis prie laiško prikabinti failus. Taip pat leidžia persiųsti turtingesniu turinio ir kelių dalių laiškus

Pašto pasiekimo protokolai:
- POP - Autorizacija ir nuskaitymas. Skirtas gautiems laiškas perkelti iš serverio pašto dėžutės į vartotojo kompiuterį. Veikia TCP pagrindu, 110 portas. Palaiko kelias operacijas:

    - autentifikaciją
    - laiškų parsiuntimą
    - antraščių parsiuntimą
    - laiško pašalinimą
    - paprastai toks serveris nesaugo išsiųstų laiškų kopijų
- IMAP – sudėtingesnis, manipuliacijos pačiame serveryje
    - laiškai tvarkomi tiesiogiai pašto serveryje
    - vartotojas laisva gali su laiškas dirbti iš kelių kompiuterių
    - laisvai konstruojami laiškų katalogai
    - naudojamas TCP 143 portas
    - IMAP saugo vartotojų būklę tarp seansų
    - saugomi guati ir išsiūsti laiškai

12. Optinė gija ir signalo sklidimo ypatybės. Šviesolaidžio savybės ir tipai. Optinis biudžetas

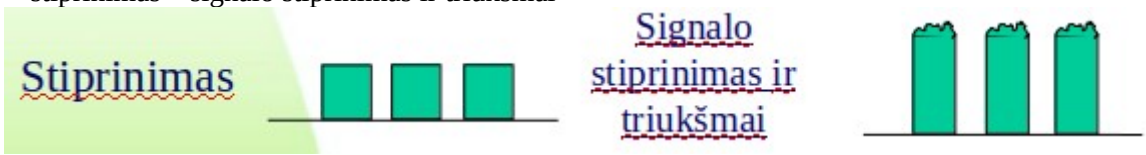
Optinė gija ir signalo sklidimo ypatybės:

- Optinė gija susideda iš:
    - šerdies
    - apvalkalo
    - apsauginio sluoksnio
- Šviesos sklidimas – šviesa atsispindti nuo šerdies ir apvalkalo ribos. Spindulys kuris atsispindės daugiausią kartų, optinės gijos gale pasirodys vėliausiai

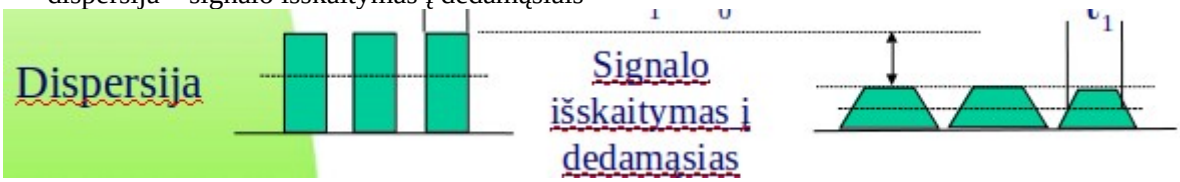
Šviesolaidžio savybės ir tipai – didėjant atstumui tarp transmiterio ir receiverio gali atsirasti įvairių pokyčių:

- nuostoliai – signalo išsibarstymas

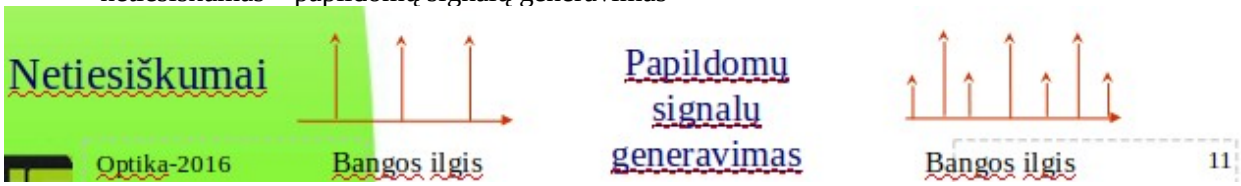
- stiprinimas – signalo stiprinimas ir triukšmai



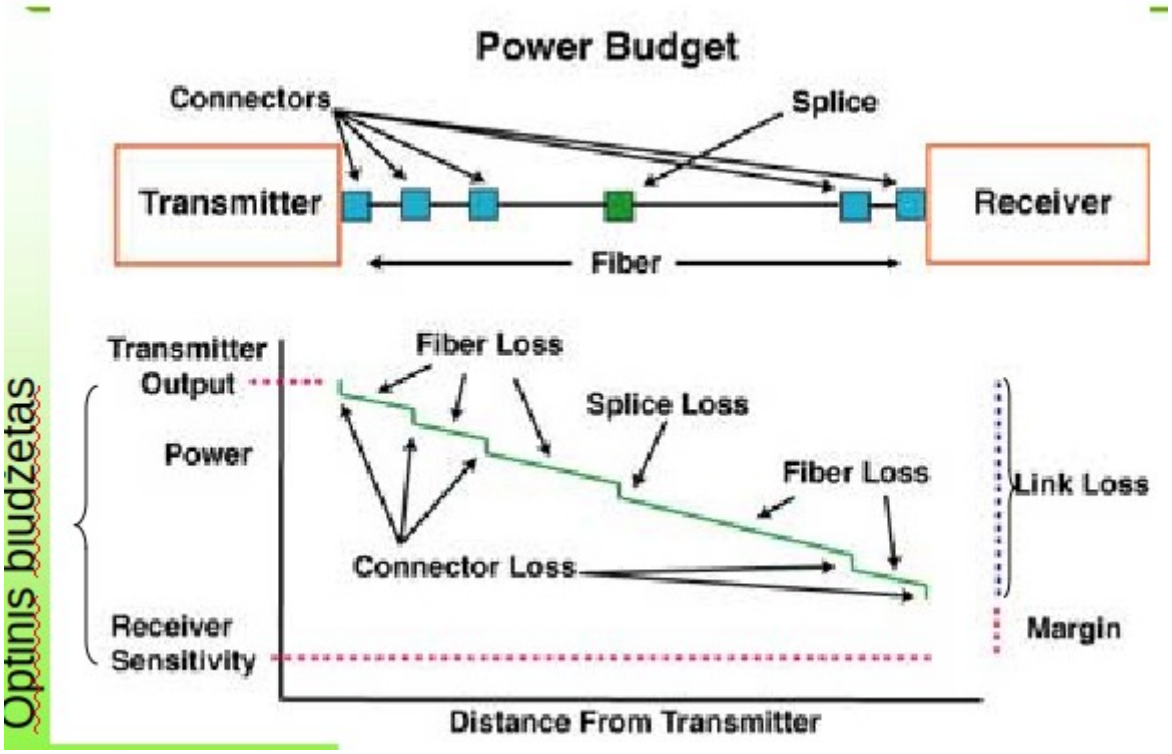
- dispersija – signalo išskaitymas į dedamąsiais



- netiesiškumas – papildomų signalų generavimas



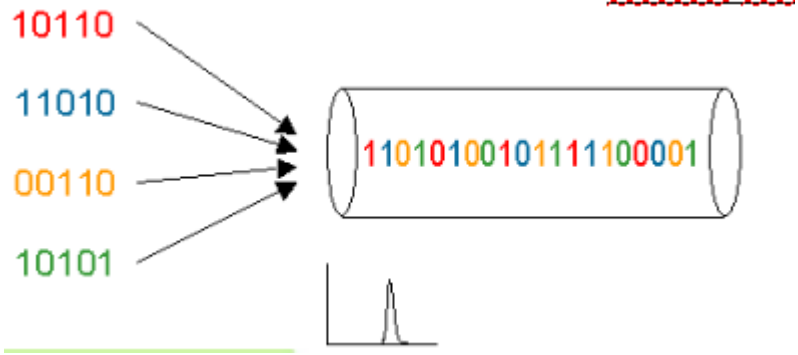
Optinis biudžetas – didėjant atstumui didėja signalo slopinimas:



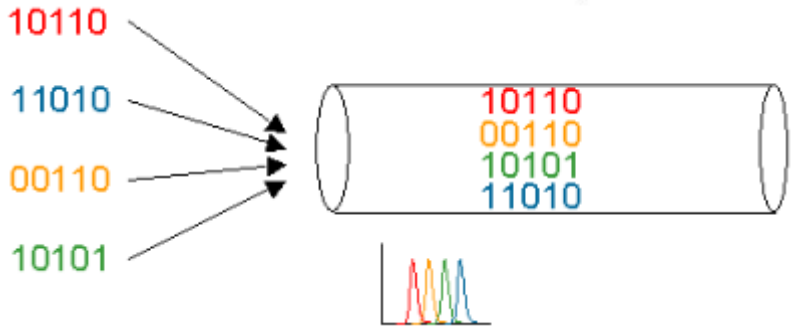
13. Multipleksavimo rūšys. Bangų multipleksavimo variantai. CWDM ir DWDM skirtumai

Multipleksavimo rūšys:

- TDM - duomenys siunčiami skirtingais laikas tuo pačiu bangos ilgiu



- WDM – duomenys siunčiami tuo pačiu laiku skirtingais bangų ilgiais



Bangų multipleksavimo variantai:

- Viena gija – abiem kryptimis, kliento pajungimui vietoj paprastai naudojamų dviejų gijų (po vieną į priekį ir atgal) pakanka vienos
- CWDM
- DWDM

CWDM ir DWDM skirtumai:
- CWDM gali turėti 18 skirtingų bangų, DWDM paprastai nuo 20 iki 160
- CWDM atstumas tarp bangų didelis: 20 nm, o DWDM bangų atstumas gali būti nuo 0.2 nm iki 1.6 nm

14. Wi-Fi tinklai. Dažnių juostos, standartų palyginimas

Wi-Fi tinklai – lokalios aprėpties radijo prieiga, naudojami bevielio ryšio zonos nešiojamiems kompiuteriams viešbučiuose, salėse, auditorijose

Dažnių juosta:
- 2.4 GHz:
  - IEEE 802.11b (iki 11Mbps)
  - IEEE 802.11g (iki 54Mbps)
  - Bluetooth
  - IEEE 802.11n (iki 300Mbps)
  - IEEE 802.11ac (iki 3x433Mbps)
- 5 GHz:
  - IEEE 802.11a (iki 54Mbps)
  - IEEE 802.11n (iki 300Mbps)
  - IEEE 802.11ac (iki 3x433Mbps)

Palyginimas:
- Didėjant dažniui didėja perduodamų duomenų pralaidumas
- Didėjant dažniui mažėja signalo stiprumas
- Didėjant dažniui mažėja signalo trukdžiai

15. Wi-Fi duomenų perdavimas, tinklų architektūros palyginimas

Wi-fi duomenų perdavimas:
Naudojamas CSMA protokolas su kolizijų išvengimo (CA) mechanizmu, kuris leidžia išvengti laike sutampančio duomenų perdavimo tarp daugelio įrenginių

Principai:
- Stebėk kanalą
- Kai jis atsilaisvina – nepulk iš karto siųsti

Bazinis įrenginys – prieigos taškas (access point, AP)
Kiekvienas jų turi savo SSID – WLAN identifikatorius

Tinklų architektūros palyginimas (tarp BSS ir ESS):

Pavadinimas	BSS	ESS
Apibūdinimas	Kiekvienas AP turi atskirą SSID ir savo zoną	Visi AP sudaro vieną zoną su tuo pačiu SSID
Įranga	belaidis	Prieeigos taškų sistema
Taikymas	Individualiam naudojimui	Didelėms zonoms sukurti
Autentifikacija	Nustatytas slaptažodis (WEB, WPA2)	Individualizuota (802.1x)
Problemos	Galimi trukdžiai esant daugeliui AP netoli vienas kito (pvz maršrutizatoriai butuose)	Vartotojas yra kelių AP zonose Vartotojas juda iš vieno AP zonos į kitą Dėl to reikalingas zonos kontroleris (pvz eduroam)

16. Debesų infrastruktūra. IaaS, PaaS, SaaS. Talpyklų rūšys block, blob, shared, ephemeral ir jų skirtumai

Debesų infrastruktūra:

- compute – virtual or bare metal machines
- network – isolated cloud networks, routing, peering
- storage – block, blob, shared, ephemeral
- PaaS – abstracts infrastucture
- SaaS – abstracts PaaS, adds software on top

IaaS, PaaS, Saas:

Name	IaaS	PaaS	Saas
Applicatios	+	+	-
Data	+	+	-
Runtime	+	-	-
Middleware	+	-	-
O/S	+	-	-
Virtualization	-	-	-
Servers	-	-	-
Storage	-	-	-
Networking	-	-	-

- Software as a service (SaaS) – vartotojas interneto pagalba gali naudotis konkrečiomis programomis (pvz. Elektroniniu paštu, CRM ir t.t.)
- Platform as a service (PaaS) – vartotojui suteikia ne tik infrastruktūrinius išteklius, bet ir operacinę sistemą kartu su programomis, programavimo kalbomis, bibliotekomis ir kitais įrankiais bei paslaugomis
- Infrastructure as a service (IaaS) – leidžia vartotojams naudotis serverių, duomenų saugyklų ištekliais bei tinklo įranga pagal poreikį

Talpyklų rūšys block, blob, shared, ephermal:

- block – managed virtual block devices:
  - supports file systems
  - attached to instances vie networks
  - persists data after instance dies
  - supports block level replication
  - supports provisioned IOPS
- block – managed object storage:
  - operates vie an API
  - scales to petabytes automatically
  - one of the core cloud services
- ephermal:
  - best performance
  - directly attached to the host machines should only ever be used for temporary data
  - sually comes with more expensive instances

17. Konteineriai: Architektūra; Konteinerio atvaizdas (image); Docker failas; Repositorijos; Kubernetes: paskirtis ir pagrindiniai elementai

Architektūra:

- suteikia izoliuotą aplinką
- veikia paprastai kaip foregound procesai
- gali būti lyginami su micro VM

- host resursai yra padalinti
- viską supakuoja geriau nei virtualios mašinos

Konteinerio atvaizdas (image):
- supakuoja taikomąją programą ir jos dependencies
- sukonstruojama iš nepajudinamų (nekeičiamų) sluoksnių
- lengvai perkeliama ir cross-platform
- viena image gali buti naudajama kaip kitos image bazė
- kuo sluoksnių skaičius didesnis, tuo image didesnė

Docker failas – tekstinis dokumentas, kuriame yra surašytos visos komandos, kurių pagalba sukuriamas image failas

Repositorijos – tai saugykla kuri gali saugi programos kodo versijas, duomenų bazės backupus, image failų versijas. Užtikrina, kad atsitikus nelaimei viską būtų galima nesunkiai atstatyti.

Kubernetes: paskirtis ir pagrindiniai elementai:
- nepakeičiama infrastruktūra
- deklaratyvi insfraktūra
- self healing
- Suteikia galymybę naudojant:
  - pods – gali laikyti vieną arba kelis konteinerius
  - services – suteikia interneto prieeigą viduryje cluster
  - deployments – scales and monitors containers (valdo ir prižiūri kontainerius)
  - configmaps – suteikia konfiguravimo galimybę konteineriams
  - secrets – suteikia apsaugą sfor sensitive informatiom / configuration
  - ingress – paskirsto tiklo apkrovas for services

Susidaro iš:
- cluster – savyje turi node, programos konteinerį, deployment
- node – savyje turi pods

18. Statinio maršrutizavimo trūkumai. Maršrutizavimo protokolų skirtumai. RIP ir OSPF veikimo principai.

Statinio maršrutizavimo (kai kiekvienas pasiekiamas tinklas ir sekančio šiolio adresas įvedamas rankomis, administratoriaus) trūkumai:
- netinka dideliam tinklui
- nėra automatinio maršrutų parinkimo
- nuktrūkus ryšiui kurioje nors sąsajoje, dalis tinklų gali tapti nepasiekiami

Maršrutizavimo protokolas nusako:
- kaip pasiųsti maršrutų pasikeitimus
- maršrutų pasikeitimus apibūdinančią informaciją ir jos formatus
- kada siųsti maršrutų pasikeitimus
- kaip surasti, kam turi būti siunčiami maršrutų pasikeitimai

Tipai:
- atstumų vektoriaus:
  - maršrutizatorius transliuoja savo maršrutų lenteles kaimynams kas tam tikrą laiko intervalą.
  - Pasikeitimai maršrutų lentelėse sklinda bangos principu
- ryšių būsenos:
  - kiekvienas maršrutizatorius žino visą tinklo topologiją ir ryšių būsenas.
  - Savo ryšių pasikeitimus siunčia multicast būdu
  - kiekvienas maršrutizatorius maršrutus skaičiuoja pats pagal trumpiausio kelio grafe radimo algoritmą

RIP veikimo principas:

1. Maršrutizatoriai žino tiesiai prijungtus tinklus
2. Žinomi kaimyninių maršrutizatorių adresai
3. Maršrutizaroiai periodiškai perduoda savo lenteles kaimynams
4. Lentelės perskaičiuojamos

OSP veikimo principas:

- tinklas sudalinamas į nepriklausomas maršrutų skaičiavimo sritis, kurios apjungiamos per kamieninę sritį
- kraštiniai maršrutizatoriai jungiami į dvi sritis: vidinę ir kamieninę
- kiekvienas maršrutizatorius suranda kaimyninius OSPF maršrutizatorius. Jiems siunčia Hello žinutes, kad galėtų stebėti ryšio pasikeitimą
- Jei ryšio būsena pasikeičia, pranešama visiems srityje esantiems maršrutizatoriams. Jie persiskaičiuoja savo maršrutų lenteles

19. Tinklo sluoksnis. Interneto principai. IP paketo formatas

Tinklo sluoksnis – atlieką duomenų perdavimą tarp bet kurių dviejų mazgų, tačiau dažniausiai negarantuoja duomenų perdavimo teisingumo. Taip pat atliekam maršruto tinkle paiešką

Interneto principai:

- IP paketo antraštė turi visą informaciją, kuri reikalinga pristatyti paketą į gavėjo kompiuterį.
- Maršrutizatorius analizuoja kiekvieno paketo IP antraštę ir jį nukreipia gavėjo kryptimi

IP paketo formatas:

- TTL – time to live – paketo gyvavimo laikas
- TOS – Type Of Service – požymiai naudojami perdavimo kokybės valdymui
- Fragmentai – kai IP paketas tampa per didelis ir yra išskaidomas I kelis

20. Autonominės sistemos: paskirtis, savybės, rūšys. Maršrutizavimas tarp AS

AS – centralizuotai ir nepriklausomai nuo kitų administruojama interneto tinklų dalis, turinti bendras maršrutizavimo taisykles:

- IP numerių skirstymo sistema
- Maršrutizavimo taisyklės viduje AS
- Duomenų srautų valdymas
- Tinklų skelbimas į kaimynines AS
- Maršrutų į kitas AS (ir globalų internetą) parinkimas
- paslaugų teikėjas paprastai turi vieną AS visiems savo ir savo klientų tinklams

Maršrutizavimas tarp AS:

- kiekvienas AS turi unikalų numerį
- kiekvienas AS turi IP adresų aibė
- reikalingas bendras protokolas maršrutams iš vienos AS tinklų į kitos AS tinklus skelbti
- du maršrutizatorių tipai:
  - vidiniai – dalinasi informacija ape maršrutus vienos AS viduje
  - kraštiniai – keičiasi informacija apie maršrutus tarp AS ir reikalingą dalį perduoda vidiniams
  - kraštiniai bendrauja tarpusavyje Border Gateway protokolu (BGP)

21. DNS sistemos funkcijos, herarchijai, replikavimas. Vardų serverių rūšys, rekursyvios ir iteratyvios užklausos, DNS įrašai

DNS sistemos funkcijos, herarchija, replikavimas:

- DNS – interneto vardų sistema („verčia“ interneto vardą į IP adresą). Gali paversti vardą į IP ir atvirkščiai
- DNS herarchija:
  - 13 šakninių serverių [a-m].root-servers.net
  - 1 lygio sritis - .com, .net, .lt, ir t.t.
  - 2 lygio sritis google.com, litnet.lt
  - 3 lygio sritis – if.ktu.lt
  - <...>

Vardų serverių rūšys – autoritatyvūs ir neautoritatyvūs:

- kiekviena interneto zona turi pirminį (master), vardų serverį kuriame įrašus apie zonos vardus daro zonos administratorius
- kiekvienos zonos įrašai turėtų bent vieną kopiją kitame (antriniame, slave) serveryje
- pirminiai ir antriniai vardų serveriai vadinami autoritatyviais
- kiekviena zona turi sesijos numerį, kuris didinamas, jei padaromi pakeitimai
- pakeitimai į antrinius serverius replikuojami pagal administratoriaus užduotus laiko intervalus
- neautoritatyviuose vardų serveriuose duomenys apie svetimų zonų vardus atsiranda DNS proceso metu

Rekursyvios ir iteratyvios užklausos:

- rekursyvios – užklausą gavęs ir nežinantis atsakymo serveris perduoda originalią užklausą kitam (savo vardu)
- iteratyvios – užklausą gavęs ir nežinantis atsakymo serveris gražina tik tinkamesnio serverio adresą ,,klausk pats“

DNS įrašai – kiekvienas serveris įsimena gauto vardo sprendimą kešo lentelėje.