Teoriniai klausimai:

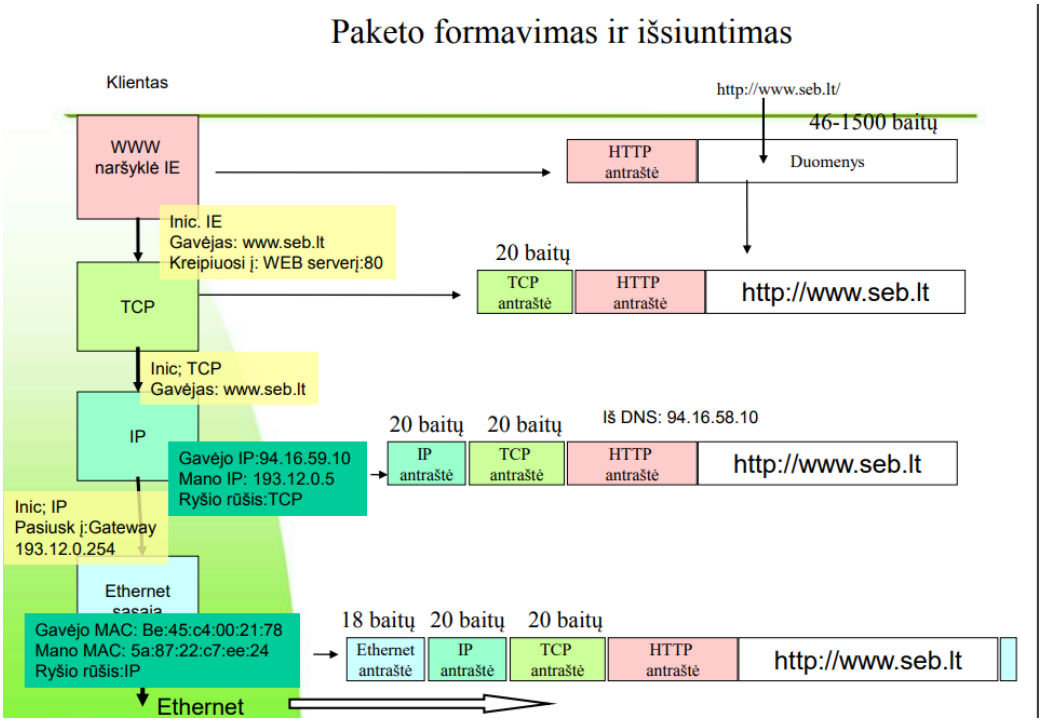
ANTRA PASKAITA

1.OSI modelio sluoksniai. Sluoksnių apibūdinimas. Komunikavimo procesas.

Komunikavimo proceso sudėtingumui sumažinti, jis suskirstomas į keletą sluoksnių.
Sluoksnių funkcionalumas gali būti keičiamas ribose, kuriose jo teikiama paslauga aukštesniam sluoksniui išlieka nepakitusi.
Kiekvienas sluoksnis turi savo funkcijas ir protokolus.

Atvirųjų sistemų jungimo (**Open Systems Interconnection**) protokolų modelis. Autorius: ISO. 7 sluoksniai.
Teorinė sistema, bet naudojama ir praktiškai.

Sluoksniai:
L7-Taikymo – skirtas vartotojui, pvz. HTTP aprašo sąveiką “naršyklė - WEB serveris”.
L6-Pateikimo - duomenų formatai, šifravimas
L5-Sesijos - autentifikacija, ryšio paruošimas, eiga ir nutraukimas
L4-Transporto - apsikeitimas tarp taikomųjų procesų
L3-Tinklo - transportavimas tinklu, adresacija, maršrutų parinkimas
L2-Kanalo – kadrai (duomenų paketai), antraštės, perdavimas tarp gretimų mazgų
L1-Fizinis - signalai, jungtys, dažniai ir pan.



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

Lokalus tinklas (LAN - **Local Area Network**) yra kompiuterių ar kitų įrenginių tinklas mažoje teritorijoje.
Didžioji dalis lokalių tinklų apsiriboja viename pastate.
LAN'e naudojamos paprastos ir pigios duomenų perdavimo technologijos.
Kiekvienas LAN įrenginys veikia autonomiškai ir automatiškai.
LAN'o veikimui nebūtinas konfigūravimas ir įrenginių valdymas.
Mes LAN'u laikysime tokį tinklą (tinklo dalį), kuriame duomenų perdavimas vyksta **L2** sluoksnyje.

OSI kanalo sluoksnis užtikrina duomenų paketų (kadrų) formavimą ir perdavimą tarp **gretimų** tinklo mazgų.
Kanalo sluoksnyje siuntėjas suformuoja duomenų paketą (kadrą), kurio **antraštė** turi gavėjo ir siuntėjo fizinių sąsajų adresus (t.y. Media Access Control - **MAC adresus**).
Tarpinis kanalo sluoksnio įrenginys (komutatorius/maršrutizatorius) **nekeičia** perduodamo paketo.
Kanalo sluoksnio įrenginys turi turėti **atmintinę** priimtam duomenų paketui įsiminti.

Transliacijų metodas: visi įrenginiai sujungti taip, kad bet kuris signalas pasiekia visus. Laidinėse terpėse tai vadinama magistrale. Kad nekiltų sumaišties, magistralės ilgis arba tinklo diametras ribotas:

- minimalaus ilgio (64 baitai) paketas turi pasiekti visus mazgus kol dar nebaigtas siuntimas.

Bendrai visų mazgų naudojama ta pati tyšio terpė.
Neišvengiamos kolizijos, kai keli mazgai pradeda siųsti vienu metu. Paketai sugadinami. Reikalingi mechanizmai tam minimizuoti:

- laidinėse terpėse IEEE 802.3 – Ethernet CSMA/CD
- belaidėse IEEE 802.11 – CSMA/CA

Tinklas negali būti didelis.
Laidinėse terpėse nebenaudojamas dėl prasto efektyvumo.

Paketų komutavimo metodas: centrinis tinklo įrenginys su galiniais mazgais sujungtas atskirais ryšio kanalais. Tinklo įrenginio paskirtis teisingai paskirstyti atėjusius paketus į išėjimo jungtis. Atstumą iki mazgo riboja tik signalo silpimas.

Centrinis įrenginys kiekvienam atėjusiam paketui „komutuoja" reikalingą išėjimo jungtį.
Komutavimo tikslumui reikia įsiminti į kokias jungtis ateina paketai iš tam tikrų adresų.

Adresacijos sistema lokali.
Siuntimo sparta gali būti labai didelė.
Tuo pačiu metu galima ir siųsti ir priimti paketus (dupleksinis perdavimas).

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

1. *Apsimokymas pagal siuntėjo adresą:*
   Jei siuntėjo adreso nėra MAC lentelėje, INSERT į MAC lentelę
   Jei siuntėjo adresas yra MAC lentelėje, bet ten nurodyta kita jungtis, UPDATE data MAC lentelėje.
2. *Persiuntimas pagal gavėjo adresą:*
   Nustatyti išėjimo jungtį Y iš MAC adresų lentelės pagal gavėjo adresą.
   Jei X = Y, DELETE data (filter)
   Jei X != Y, SEND to Y
   Jei gavėjo adreso nėra lentelėje, paketą paskleisti (flood) per visas jungtis, išskyrus X.
3. *Išmesti įrašus, kuriems baigėsi galiojimo laikas iš MAC adresų lentelės.*

ARP (Address Resolution Protocol, RFC 826) - 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

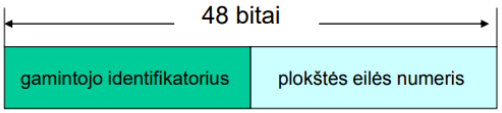
Ethernet
Pagrindinė duomenų perdavimo lokaliais tinklais technologija. Duomenys siunčiami 64-1500 baitų paketais naudojant fizinius (MAC) įrenginių adresus.

IEEE 802.3 standartai
Aprašo duomenų perdavimo spartą, ryšio terpes ir atstumus. Visi naudoja tą patį Ethernet paketo formatą, todėl tarpusavyje suderinami.

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

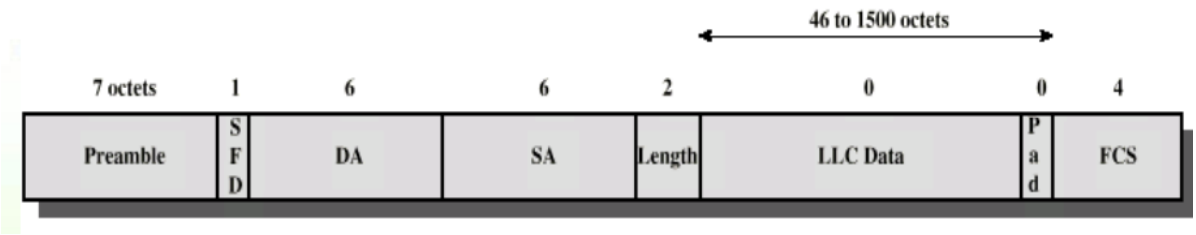
MAC adresas (dar vadinamas fiziniu ar Ethernet adresu) susideda iš dviejų dalių po 3 baitus:
gamyklai suteiktas kodas + mazgo eilės numeris

Visuotinis (broadcast) adresas yra $FF{:}FF{:}FF{:}FF{:}FF{:}FF_{16}$
Skirtingai nuo IP, MAC adresai niekaip negrupuojami: nesvarbu koks jis yra, svarbu tik kad tame pačiame LAN jis būtų unikalus.



00:A0:C9:43:65:80

Ethernet paketo struktūra



Preambulė - 01010101... - imtuvo sincronizacijai
SDF - kadro pradžios žymė 10101011
DA - gavėjo adresas
SA - siuntėjo adresas
Length – paketo ilgis
LLC Data - duomenys + kamšalas (pad) turi būti 46-1500 baitų ribose
FCS - kadro kontrolinė suma, gaunama sumuojant paketą po 4 baitus be pernešimo
Pvz: 5827
5 + 8 = 13 + 2 = 5 + 7 = 12 = 2

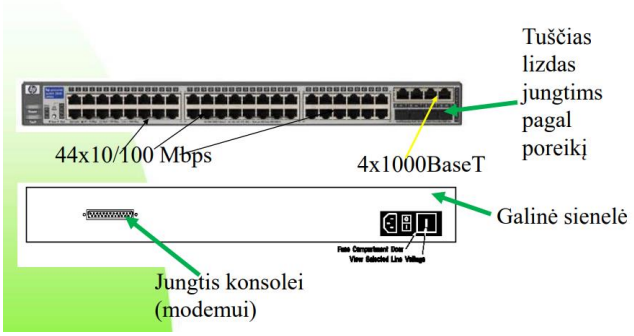
Ethernet komutatoriai
Savybės:

- Komutuoja gautą paketą į tam tikrą jungtį pagal gavėjo MAC adresą
- Automatiškai susiformuoja MAC adresų lentelę
- Nekeičia nei persiunčiamo paketo turinio, nei formato
- Yra skaidrus (nematomas) stotims: visos jos lieka viename LAN'e
- Nereikalauja konfigūravimo
- Neturi jokių adresų

Komutatorių rūšys
Nevaldomi LAN komutatoriai:
Paprastai jungtys gali dirbti skirtinguose režimuose viena iš kelių spartų: 10/100/1000
Pilnas dupleksas/pusinis dupleksas

Automatinis režimo nustatymas: sparta/dupleksas
Visos jungtys vienodos
4-16 jungčių

Valdomi ir konfigūruojami komutatoriai:



MAC address filtering/ACL – fizinių adresų filtrai, MAC adresų “pririšimas”
Spanning tree (IEEE 802.1D)– kilpų išvengimo protokolas
VLAN (IEEE 802.1Q/P) – virtualių tinklų ir prioritetų palaikymas
Port mirroring- jungties dubliavimas stebėjimo reikalams
Port trunking/aggregation – jungčių ryšulių sudarymo galimybė
Multicast (IGMP snooping) – grupinio perdavimo režimo palaikymas
SNMP, RMON -veikimo parametrų stebėjimas ir valdymas per tinklą
Broadcast and multicast storm control – užtvindančių srautų valdymas
Rate limiting/ port bandwidth control – jungties spartos ribojimas žemiau fizinių galimybių
NTP – laiko sinchronizavimas
Syslog - įvykių žurnalas, galimybė jį eksportuoti
RS232 – jungtis konsolei
Telnet, ssh- prisijungimas valdymui per tinklą
tftp- konfigūracijos ir OS užkrovimo galimybė
802.1x (port Based Access Control) – prisijungimo autentifikacija
Jumbo frames – ilgesnių už 1500 baitų Ethernet paketų perdavimas
PoE (Power over Ethernet) –maitinimas per tą patį varinį Ethernet kabelį

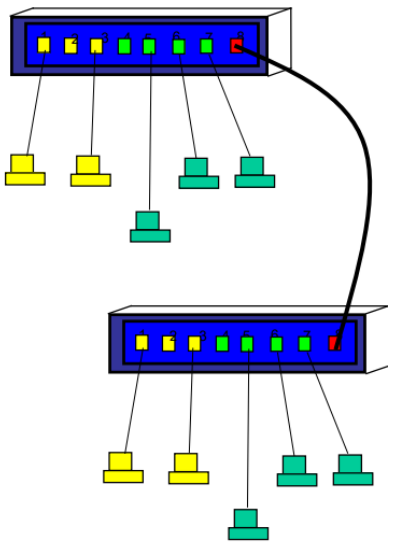
4.Virtualūs lokalūs tinklai. Kadrų žymėjimas IEEE802.1q

Virtualūs lokalūs tinklai
Įprastinėmis lokalių tinklų techologijomis sunku realizuoti šiuolaikinius tinklus.

Prie VLAN galima jungti kelis LAN tinklus viename komutatoriuje. Tam pačiam LAN priklausantys įrenginiai gali būti prie skirtingų komutatorių.

1. Komutatorius sudalinamas 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 (trunk) jungtimis.
4. Kad perduodant bendru kanalu paketai nesusimaišytų, komutatorius jų antraštes papildo VLAN žyme.

Įrenginiai priskiriami vienam ar kitam VLAN pagal tai, prie kurios jungties jie prijungti.
Skirtingos MAC adresų lentelės: komutatorius virtualiai padalintas į kelis komutatorius, kurie tarpusavyje paketų neperduoda.
Toks padalinimas atliekamas sužymint jungtims VLAN numerius.

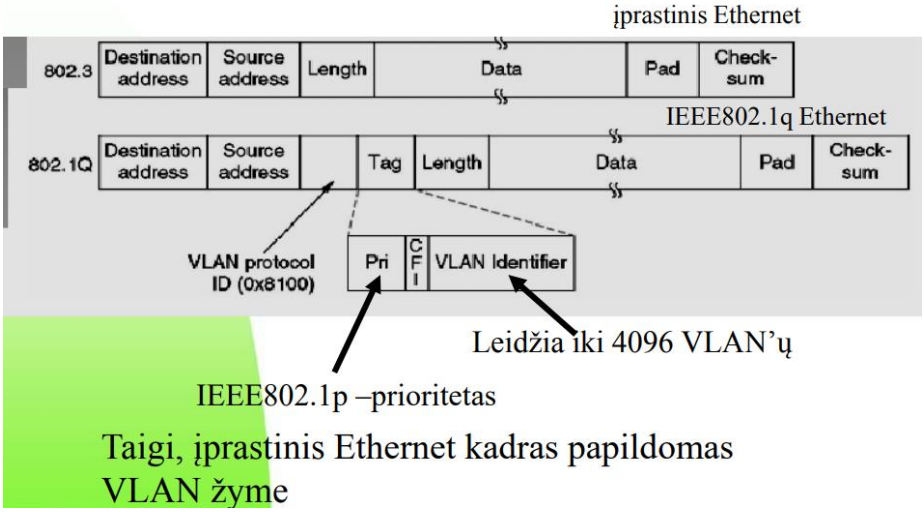


VLAN per kelis komutatorius
Jungtys prie kurių jungiami galiniai mazgai tai prieigos (access) jungtys.
Jungtys, kurios sujungia komutatorius tarpusavyje ar į maršrutizatorių tai bendros (trunk) jungtys visiems VLAN’ams.
Kad skirtingų VLAN paketai perėję trunk ryšį būtų atiduoti teisingam VLAN, jie turi būti sužymėti, t.y. į perduodamą paketą turi būti įrašytas VLAN numeris.

Kadrų žymėjimas IEEE802.1q

1. Komutatorių jungtys padalinamos į VLAN'us
2. Perduodant Ethernet paketą iš komutatoriaus 1 į 2, į paketą įrašomas papildomas laukas (tag): VLAN žymė.
3. Jungiančioje linijoje (trunk-magistralė) yra visų VLAN'ų siunčiami sužymėti paketai.
4. Priėmęs pažymėtą paketą, komutatorius 2 perduoda į atitinkamą VLAN paprastą Ethernet paketą, numetęs VLAN žymę.

Skirtumas tarp įprastinio Ethernet protokolo 802.3:



Sudėtingame tinkle rankiniu būdų konfigūruoti VLAN'ų sistemą sunku. VTP (Virtual Trunking Protocol) protokolas tam padeda.

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

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

ACL savybės
Paketų tikrinimas pagal nurodytą filtrą vykdomas nustatytoje maršrutizatoriaus sąsajoje.
Filtras taikomas arba įeinantiems (in) arba išeinantiems paketams (out).
Kiekvienas persiunčiamas ta kryptimi paketas tikrinamas ar atitinka kurios nors taisyklės aprašą.
ACL rezultatas gali būti **permit** (leisti) arba **deny** (drausti) 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 pradinį adresą ir šabloną (wildcard).
Šablonas yra adreso kaukės inversija:

	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

Patogiau nustatyti taip: (segmento dydis-1)
Pvz /27 tai 32 numeriai, šablonas bus 0.0.0.31

Standartiniai ir išplėstiniai ACL
Standartiniai ACL taikomi **tik filtravimui** pagal paketų **siuntėjų** IP adresus, su jais galima aprašyti tik labai paprastus reikalavimus.
Standartinių ACL sąrašai numeruojami 1-99 numeriais.

Išplėstiniai ACL leidžia tikrinti tiek **siuntėjų**, tiek **gavėjų** IP adresus (ip-based formatas), o taip pat transporto sluoksnio (TCP,UDP) **antraštes** (application-based formatas).
Jie numeruojami 100-199 numeriais.
Išplėstiniai ACL taikomi galimai arčiau jų taisyklėse apibrėžtų **siuntėjų**.

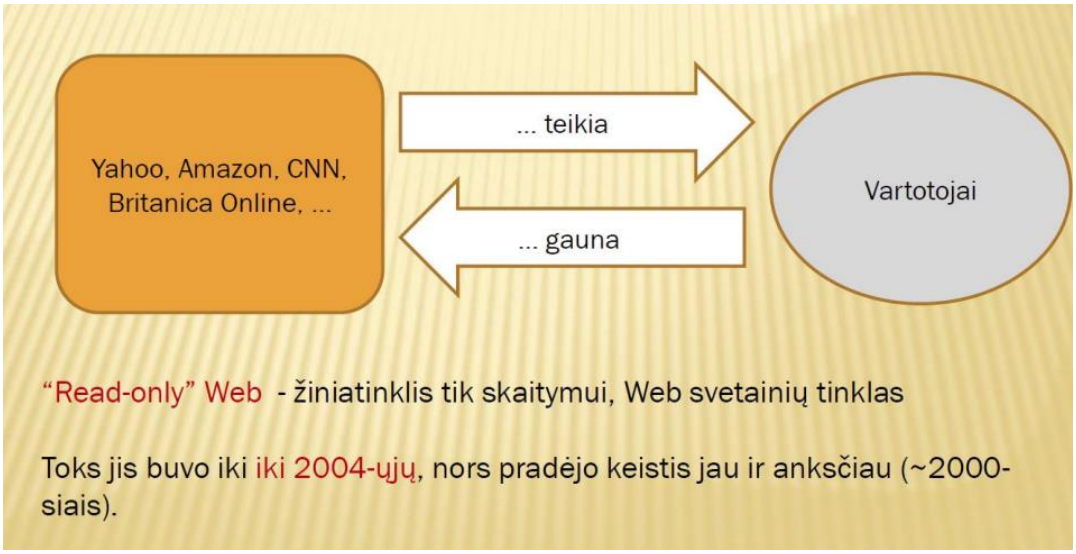
ACL naudojimas

1. Blokuoti (deny) komunikavimui pakanka blokuoti paketus bent viena krypimi.
2. Leisti išimtinį duomenų apsikeitimą (permit) būtina iš abiejų pusių.
3. Jei 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:

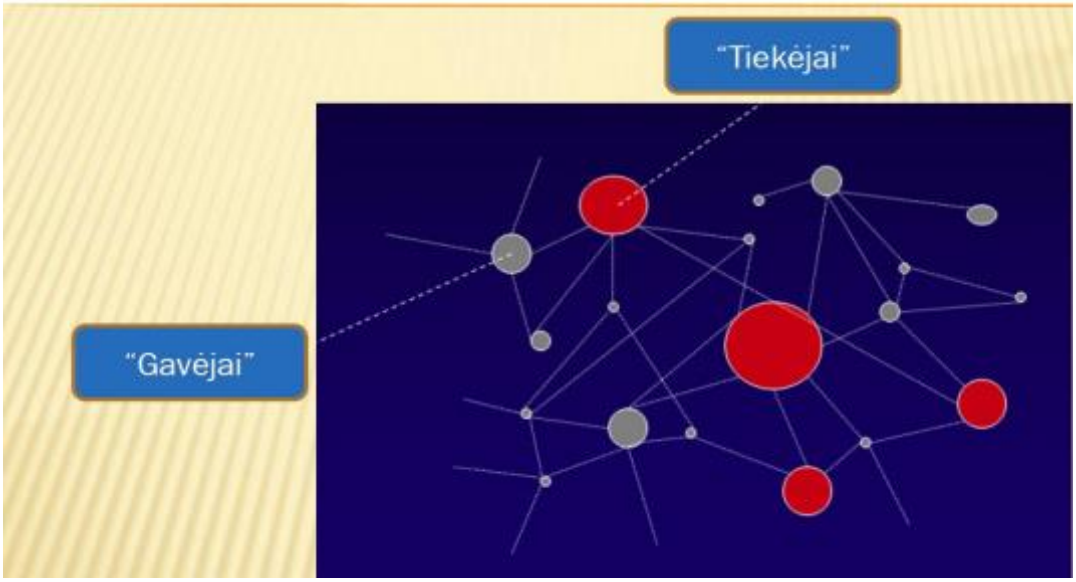
   deny ip 1.1.1.0 0.0.0.255 host 3.3.3.20 3.3.3.20
   permit ip any any

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

WEB1



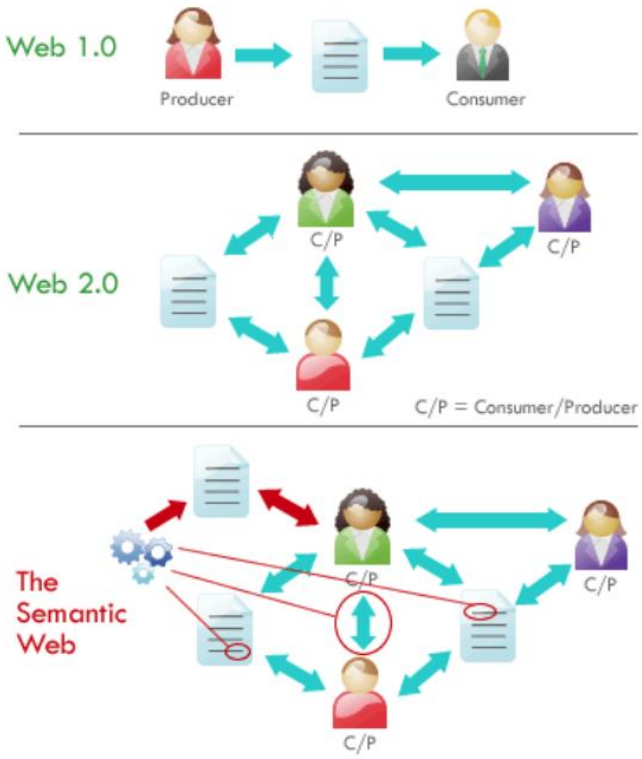
WEB2



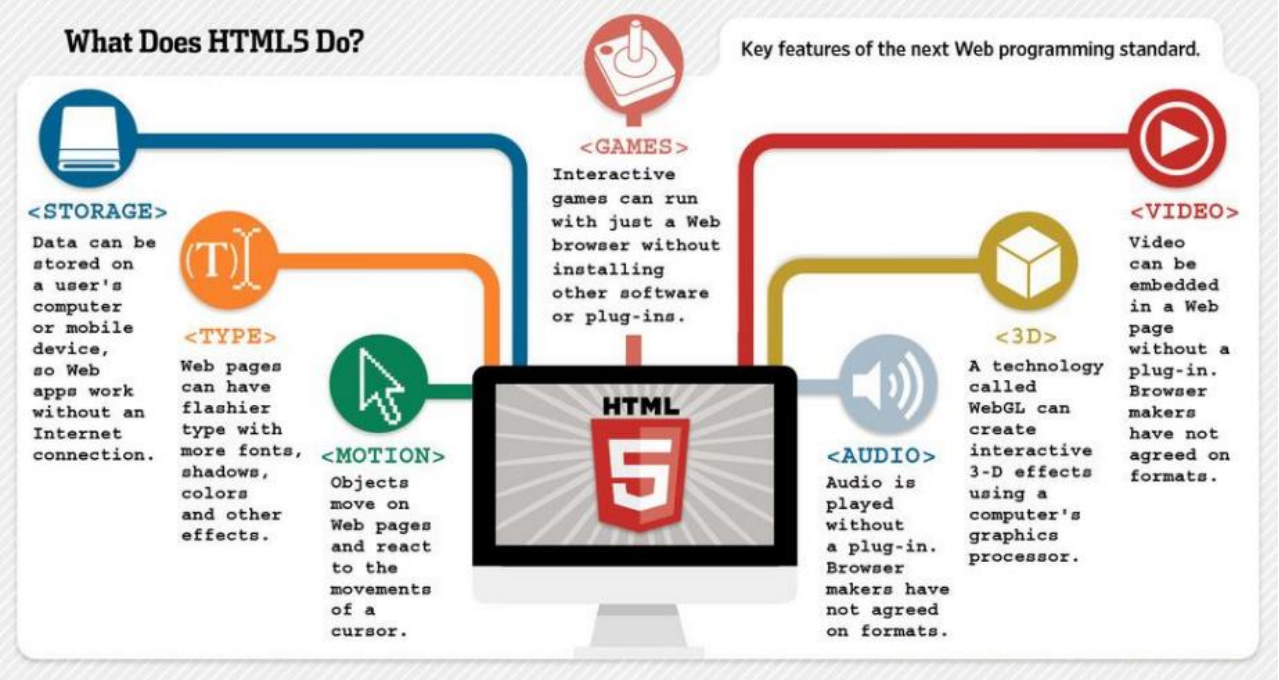
Esmė –interneto turinį bendradarbiaudami gali kurti visi (Wisdom of Crowds).
"Read-Write" Web – žiniatinklis ir skaitymui, ir rašymui.
Žiniatinklis –tai tarsi didelė kompiuterinė sistema (platforma), kuriai kurioje kuriami ir vykdomi įvairūs uždaviniai.

WEB3 (dabar)

- Sprendimai, pritaikyti mobiliems prietaisams.
- ~50% vartotojų internetu naudojasi per mobilųjį telefoną.
- Internetas reikiamoje vietoje ir reikiamu laiku
- Galimybės išnaudoti vartotojo kontekstą (pvz. nuo buvimo vietos priklausomos paslaugos)
- Vartotojas gali dar patogiau kurti įvairialypį interneto turinį
- Tobulėjančios multimedia valdymo galimybės telefone
- Informacija sukuriama ir įkeliama norimoje vietoje ir norimu laiku
- Atvirumas – vystoma tai, kas jau pradėta
- Atviri standartai
- Mashups - galimybės panaudoti esamas paslaugas kaip statybinius blokelius naujoms paslaugoms
- Suderintos sistemos (pvz. galimybė apjungti įvairių socialinių tinklų informaciją)



Pagrindiniai HTML5 principai



HTML4 + CSS3 + JS = *HTML5*

Su HTML5 buvo pridėta:

- datetime
- datetime-local
- date
- month
- week
- time
- number
- range
- email
- url

Tačiau palaikomi ir seni atributai.

Nauji elementai:

- <canvas> - grafinių elementų braižymas
- <video> - pridėti video
- <audio> - pridėti audio.

Pašalinti elementai:

- acronym
- applet
- basefont
- big
- center
- dir
- font
- frame
- frameset
- isindex
- noframes
- noscript
- s
- strike
- tt
- u

Panagrinėjus naująjį standartą, atrodo, kad HTML5 yra gera naujiena, pažangos nemažai.
O nuostolio jokio, senų tinklapių WWW paveldas nepaliktas už borto.

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

AAA – autentifikacija, autorizacija, apskaita.

Autorizacija
Prieigų nustatymo mechanizmai:

- DAC
- RBAC
- MAC

DAC
Disrectionary 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.

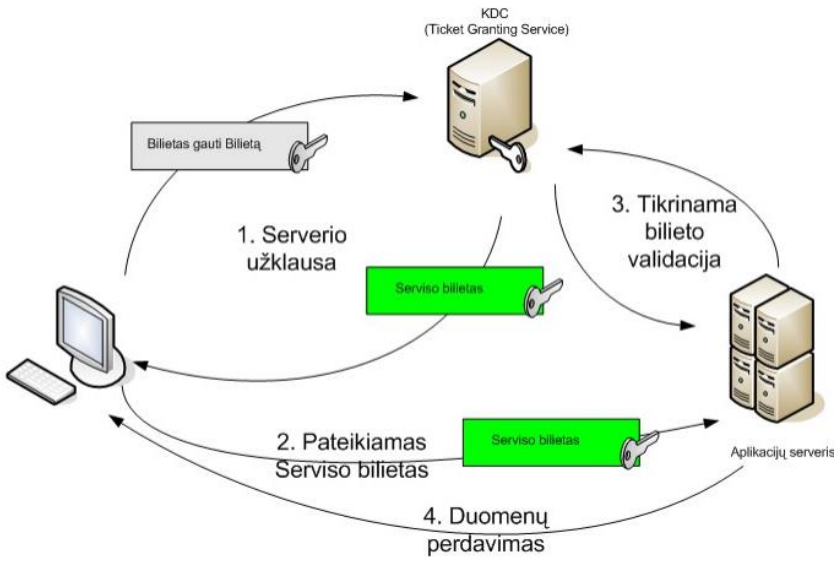
MAC
Mandatory Access Control

Privaloma teisių valdymo strategija. Failo savininkas neturi galimybės suteikti sukurtam failui teisių.

Autentifikacija
Autentifikacijos metodai:

- Kerberos
- CHAP
- EAP

Kerberos
2005m. RFC 1510 -> RFC 4120
Single sign-on
Veikia ant Mac OS, Win Server 2000, Win Server 2012, Ubuntu ir kt.



CHAP
Challenge Handshake Authentication Protocol

CHAP 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

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

Apskaita

- „Logai“
- Vartotojų veiklos stebėjimas
- Tinkle persiunčiamų paketų stebėjimas
- Pranešimai apie įvykius

SSH (Secure shell) – tai tinklo protokolas, aprašantis apsaugotą kliento prisijungimą prie serverio aplinkos (shell) ir komandų vykdymą. Standartinis ssh prievadas (portas) yra 22 (TCP). Naudojamas beveik visose šiuolaikinėse IS.

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

PIK (viešųjų raktų infrastruktūros) sertifikatai
Generuojamos PRIVATAUS rakto poros.

Viešųjų raktų infrastruktūros taikymas:

- Elektroniniams parašams
- El. paštui šifruoti
- Dokumentams šifruoti ir (ar) autentifikuoti
- Vartotojams autentifikuoti informacinėse sistemose
- Cloud tinkluose / GRID

PIK sertifikatų šifravimo būdai:

- Simetrinis – raktas yra persiunčiamas tiesiai skaitytojui
- Asimetrinis – sugeneruojami du raktai
- Hibridinis – vienas raktas užšifravimui, kitas atšifravimui. Užtikrina siuntėjo autentiškumą ir integralumą

Elektroninis parašas – tai duomenys, kurie įterpiami, prijungiami ar logiškai susiejami su kitais duomenimis pastarųjų autentiškumui patvirtinti ir (ar) pasirašančiam asmeniui identifikuoti.

Elektroninio pasirašymo priemonės:

- Asmens tapatybės kortelės
- Lustinės kortelės
- USB laikmenos
- M. Parašas
- „Smart-ID“

Sukuriamas CA privatus raktas **->** sukuriamas sertifikato pasiraš ymo prašymas **->** pasirašymas su CA **-> ->** sukuriamas sertifikatų paskelbimo negaliojančiais sąrašas

Tuomet:

1. Sukuriamas WWW serverio privatus raktas
2. Sukuriamas WWW serverio sertifikato pasirašymo prašymas
3. Prašymas pasirašomas su CA raktu

Serveryje veikia HTTPS protokolas

Tada:

1. Sukuriamas vartotojo privatus raktas
2. Sukuriamas sertifikato pasirašymo prašymas
3. Prašymo pasirašymas su CA raktu
4. Sertifikato konvertavimas į PKCK12 formatą

Slaptažodžio pilno perrinkimo laikas

$$T_S = \frac{A^S}{V \cdot N}$$

A – simbolių, iš kurių sudarytas slaptažodis, skaičius
S – slaptažodžio ilgis
V – perrankamų slaptažodžių
N – lygiagrečiai dirbančių perrinkimo mašinų skaičius

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

- 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

Transporto sluoksnio funkcijos

- Keistis duomenimis tarp taikomųjų procesų
  - Prievadai (port)
- Taisyti perdavimo klaidas
  - Patvirtinimai (ACK)
- Valdyti duomenų siuntimo spartą
  - Siuntimo langas

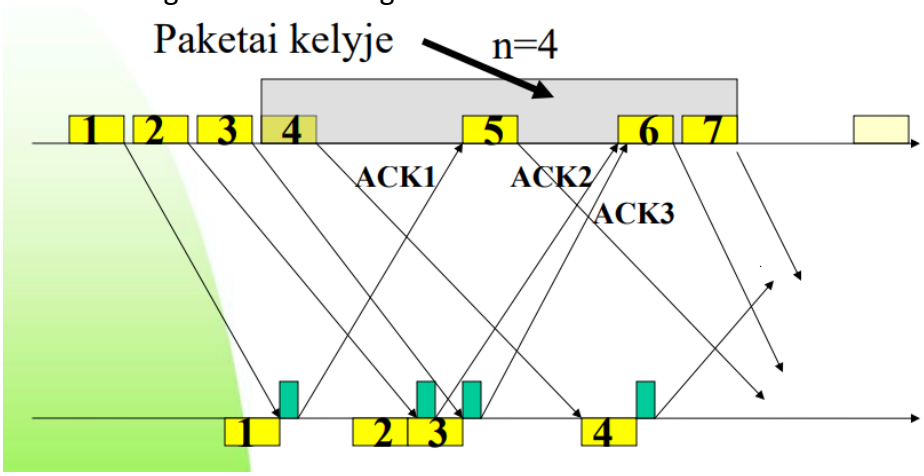
Prievadai (ports)

- Į transporto sluoksnį ateinantys paketai rikiuojami į atskiras eiles kiekvienam taikomąjam procesui, veikiančiam tame kompiuteryje
- Duomenų paketų eilė prie taikomojo proceso vadinama 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/valdymas
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, nes paketas buvo sugadintas arba nepasiekė gavėjo.

Siuntimo lango metodas

Metodo esmė: 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.



Kadangi pirmasis paketas grįžta vėliau negu n=4, tai atsiranda siuntimo prastovos.

N – lango dydis,

$$a = \frac{t_{keliamų}}{t_{siunčiamų}}$$

1. Kai $N = 1$ $U = \frac{1}{1+2a}$
2. Kai $N \geq 2a + 1$ $U = 1$
3. Kai $N < 2a + 1$ $U = \frac{N}{2a+1}$

Galioja, kai nėra paketų nuostolių

Nesulaukus per nustatytą laiką patvirtinimo apie 2 porcijos gavimą, siuntėjas kartoja siuntimą iš naujo nuo 2 porcijos, nors kelyje jau buvo 3,4 ir 5.

Bet dabar lango dydį sumažina per pusę

Jeigu negaunami išsiųsti duomenys, reikia siųsti jų mažiau ir didinti langą, tuo atveju sparta sumažės, jeigu sparta yra nemažinama, tai susidarys lavininės perkrovos.

Jei kelias iš eilės porcijas pasiuntėme sėkmingai, galime didinti siuntimo langą.

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

UDP – User Datagram Protocol
TCP – Transmission Control Protocol

UDP
Tai yra duomenų perdavimas tarp taikomųjų procesų be pristatymo garantijų.
Taikomas, kai:

- taikomasis procesas negali laukti, kol kelyje prarasti duomenys bus perduoti pakartotinai o nedidelė dalis prarastų duomenų neturi didelės įtakos (vaizdas, garsas)
- taikomasis procesas pats rūpinasi duomenų siuntimo pakartojimu
- duomenų perdavimas vyksta rezervuotu kanalu, kuriame paketų praradimo praktiškai nėra

UDP yra paprastas, spartus, nereikia didelių resursų.
Gali būti naudojamas multicast režime.

Jei nurodytam paskirties portui nėra aktyvaus proceso, paketas naikinamas.
Jei taikomasis procesas nespėja apdoroti į portą ateinančių paketų, netelpantys į buferį paketai naikinami.

UDP siuntėjas pats parenka spartą ir jos nekaitalioja nei pagal tinklo sąlygas, nei pagal gavėją.
Siunčiama netgi ir tada, jei gavėjas iš viso nepriima (pvz. Pati programa ar portas gavėjo kompiuteryje neaktyvus).

TCP

- Gali aptarnauti kelis sujungimus tuo pačiu portu
- Potencialiai skirtingi RTT
- Potencialiai didelis vėlinimas ir didelė vėlinimo sklaida
- Potencialiai skirtingi gavėjo talpumai
- Potencialiai skirtingi tinklo pralaidumai pagal gavėjus/laiką

TCP siuntimo spartos valdymas
Jacobson (1988) įvedė į TCP perkrovų valdymo mechanizmą. Jo idėjos:

1. TCP bando tinklo pralaidumo galimybes
2. TCP reaguoja į perkrovas sulėtindamas duomenų siuntimą

Siuntimo klaidų taisymas
Bendroji taisyklė:
kartoti siuntimą iš naujo nuo paskutinio patvirtinto segmento. Tačiau ji neekonomiška. Gal būt prapuolė tik vienas paketas, o paskesni priimti. Bet modernizacija turi būti suderinama su bendraja taisykle.

Perkrovų išvengimas:
Didinant siuntimo langą pradeda ilgėti laikai iki patvirtinimų atėjimo. Lango didinimas nebepadidina srauto: padidėja paketų buvimo eilėse laikas, todėl laikas mažinti langą, nelaukiant kol paketai pradės prapuldinėti.
---Šis būdas neprigijo, nes TCP yra geresnis.

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

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 grąžinti 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.

Failų prikabinimas

Elektroninis paštas naudojamas internete nuo 1971 metų. Iki 1990 buvo galimybė tik tekstinių laiškų siuntimui. Failus siusdavo tik FTP protokolu: kodavimo ir dydžio problemos.

MIME – Multipurpose Internet Mail Extensions (leidžia prie laiško prikabinti failus).
MIME suderintas su pagrindiniais e-pašto protokolais SMTP, POP and IMAP.

Pašto pasiekimo protokolai

POP – Post Office Protocol (autorizacija ir nuskaitymas)
IMAP – Internet Mail Access Protocol (Sudėtingesnis ir manipuliuoja pačiame serveryje)

Palaikoma:

- Autentifikacija
- Laiškų parsiuntimas
- Antraščių parsiuntimas
- Laiško pašalinimas

IMAP

Laiškai tvarkomi tiesiogiai pašto serveryje.
Vartotojas gali su jais dirbti iš kelių kompiuterių.
Laisvai konstruojami laiškų katalogai.
Naudoja TCP, 143 portas.
IMAP saugo vartotojų būklę tarp seansų.
Saugomi gauti ir išsiųsti laiškai
Dabar naudojama IMAP4 versija.

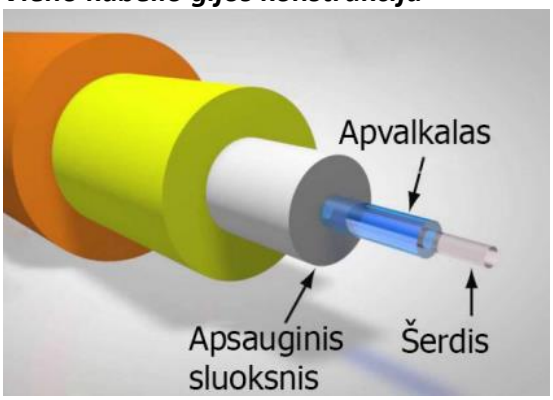
IMAP yra bendrai geresnis už POP3, tik turi problemą su vieta.

POP3

Skirtas gautiems laiškams perkelti iš serverio pašto dėžutės į vartotojo kompiuterį.
Veikia TCP protokolo pagrindu, naudojamas 110 portas.

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

Vieno kabelio gijos konstrukcija



Kabelių rūšys:

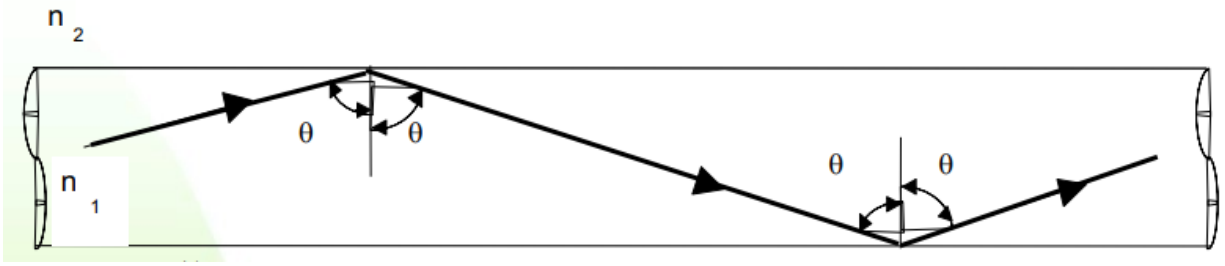
- Daugiamodis
- Vienmodis

MULTIMODE -- Core is large compared to cladding. Core is most dense in the center and decreases in density towards the cladding. This is known as Graded Index (GI or GRIN) Multimode Fiber.

SINGLEMODE -- Core is small compared to cladding. Core is even in density. This is known as Step Index Singlemode Fiber.

Signalo sklidimas gija

Šviesa atsispindi nuo šerdies ir apvalkalo ribos. Skirtingi medžiagų lūžio rodikliai n1 ir n2.



Spindulys, kuris nuo šerdies ir apvalkalo skiriamosios ribos atsispindės daugiausia kartų, optinės gijos gale pasirodys vėliausiai.

Sklidimo greitis

Jis priklauso nuo lūžio rodiklio

$$n = \frac{c_0}{v}$$

n – lūžio rodiklis
c0 – šviesos greitis vakuume
v – šviesos greitis stikle

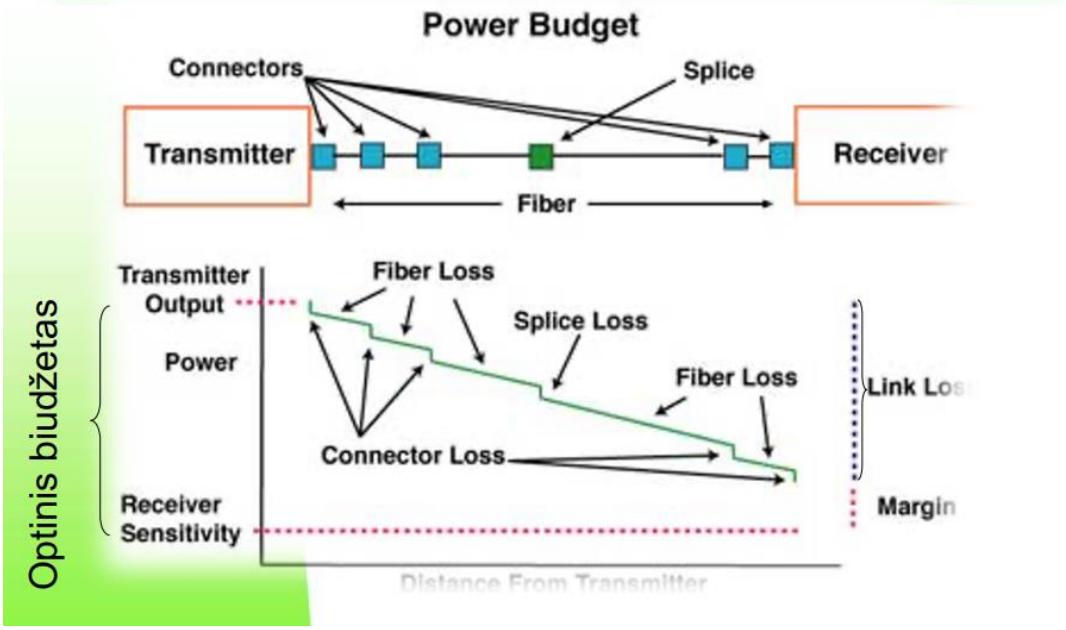
Stiklo lūžio rodiklis artimas 1.5, taigi šviesos sklidimo greitis stikle 1.5 karto mažesnis negu vakuume: $2 \cdot 10^8 m/s$

Optinių signalų pakitimai optinėje gijoje

Siunčiamo signalo pokyčiai	**Pokyčių priežastis**
Nuostoliai	Signalo išbarstymas
Stiprinimas	Signalo stiprinimas ir triukšmai
Dispersija	Signalo išskaudymas į dedamąsias
Netiesiškumai	Papildomų signalų generavimas

Skirtingo ilgio bangoms stiklo skaidrumas nevienodas.
Mažiausias slopinimas apie 1500 nm = 1.5 mikrometrų

Optinis biudžetas



Nuostoliai
Slopimas dB/km
vienmodė gija ~0,25dB/km, daugiamodė skaidula ~1dB/km

Sujungimo nuostoliai (jungiamos dvi gijos) ~0,3dB/sujungimui

Jungčių nuostoliai ~0.5dB/jungčiai

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

Multipleksavimo rūšys

- TDM – duomenys siunčiami skirtingais laikais tuo pačiu bangos ilgiu
- WDM – duomenys siunčiami tuo pačiu laiku skirtingais bangų ilgiais

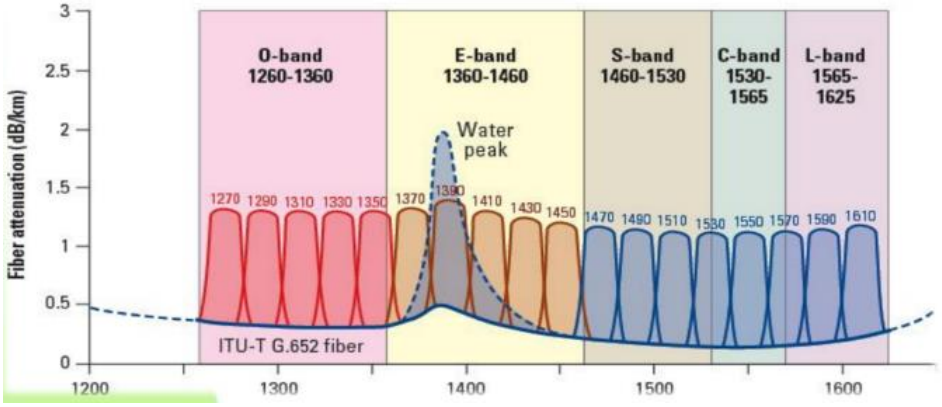
Viena gija – abiem kryptimis
Kliento pajungimui vietoj paprastai naudojamų dviejų gijų (po vieną į priekį ir atgal) pakanka vienos.

Transponder – tarpinis įrenginys, į kurio įėjimą ateina standartinio bangos ilgio (1310nm) signalas, išeina tas pats signalas jau su parinktu bangos ilgiu.
Direct connections – “spalvotas” signalas tiesiai iš jungiamo įrenginio

Erdvinis multipleksavimas
Multiple-Input-Multiple-Output (MIMO)
Daugelis nepriklausomų duomenų srautų yra persiunčiami tarp transmit ir receive antenų, kad persiųsti daugiau bitų nurodytame pralaidume.

Bangos išėmimas/įterpimas (add/drop)
Dalis bangų tranzitinės.
Kitos išimamos ir įdedamos

CWDM – „retas“ multipleksavimas



18 skirtingų bangų, atstumas tarp jų didelis: 20 nm

DWDM – „tankus“ multipleksavimas

- Žymiai tankiau supakuota WDM sistema
- Dažniausiai naudojama komercinėms ilgo kelio sistemoms
- Dažniausiai naudojamas C-band (1530-1565 bangos ilgio)
- Specifiniai kanalų dydžiai yra standartizuoti „ITU tinklelyje“
- C-band‘e šie kanalų dydžiai yra dažniausiai naudojami:
    - 200GHz – 1.6nm tarpai, 20 įmanomų kanalų
    - 100GHz – 0.8nm tarpai, 40 įmanomų kanalų
    - 50GHz – 0.4nm tarpai, 80 įmanomų kanalų
    - 25GHz – 0.2nm tarpai, 160 įmanomų kanalų

Skirtumas tarp DWDM ir CWDM

DWDM naudojami bangų ilgiai yra tik tarp 1530 ir 1565 ilgio, o CWDM gali būti naudojama visa gama bangų ilgių nuo 1470 iki 1610, bet tik tam tikrų ilgių.

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

Belaidžių ryšių rūšys

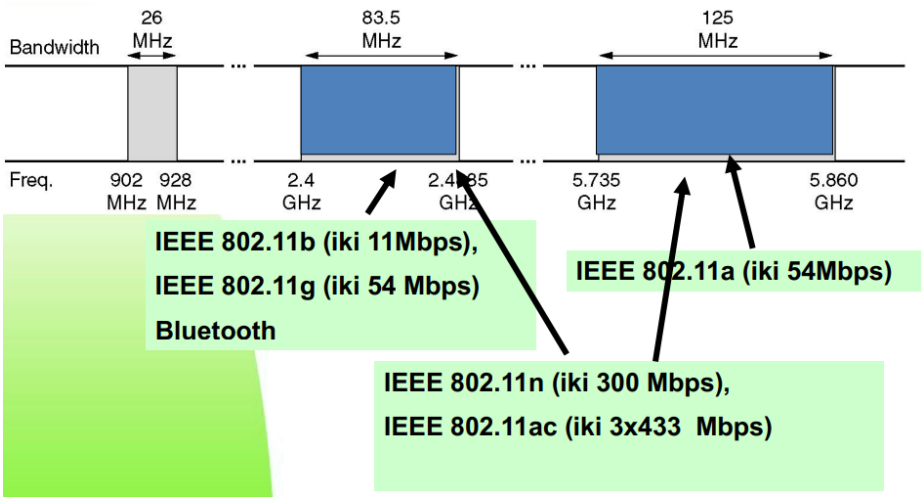
Plačios aprėpties radijo prieiga	Mobiliojo ryšio tinklai
Lokalios aprėpties radijo prieiga	Wi-Fi
Belaidė asmeninė radijo prieiga	PAN

Pagrindinė paskirtis

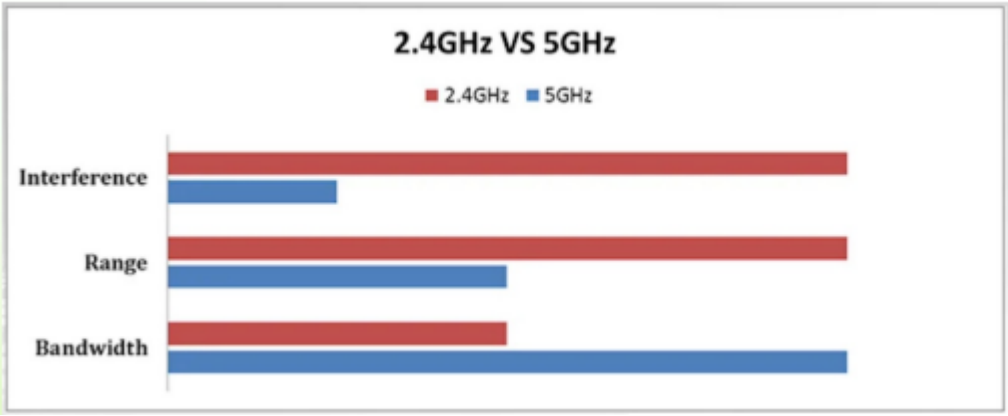
Bevielio ryšio zonos nešiojamiems kompiuteriams viešbučiuose, salėse, auditorijose, įmonių teritorijose.

Pagrindinės ypatybės

- Tie patys dažniai siuntimui ir priėmimui
- Persidengiantys kanalai



Skirtumas tarp 2.4GHz ir 5GHz dažnių



Standartų palyginimas

	IEEE 802.11	IEEE 802.11b	IEEE 802.11g	IEEE 802.11a	IEEE 802.11n	IEEE 802.11ac
Dažniai, GHz	2,4	2,4	2,4	5	2,4 / 5	2,4 / 5
Max sparta, Mbps	2	11	54	54	300	1300
Atstumas patalpose, m	20	35	38	35	70	70
Atstumas lauke, m	100	140	140	120	250	250
Suderinamumas	-	-	b	-	g, a	n
Antenos	1	1	1	1	2	≥3

15.Wi-Fi duomenų perdavimas, tinklų architektūrų palyginimas.

Naudojamas CSMA (Carrier Sense Multiple Access) protokolas su kolizijų išvengimo (CA – collision avoidance) mechanizmu, kuris leidžia išvengti laike sutampančio duomenų perdavimo tarp daugelio įrenginių.

Principai:

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

Wi-Fi tinklų architektūros

- BSS – Basic Service Set
- IBSS – Independant Basic Service Set
- ESS – Extended Service Set

Bazinis įrenginys – prieigos taškas (Access point, AP)
Kiekvienas jų turi SSID – WLAN identifikatorių

BSS
Kiekvienas access point turi atskirą SSID ir savo zoną

Įranga:
Belaidis maršrutizatorius

Taikymas:
Individualiam naudojimui

Autentifikacija:
Nustatytas slaptažodis (WEP, WPA2)

ESS
Visi access points sudaro vieną zoną su tuo pačiu SSID

Įranga:
Prieigos taškų sistema

Taikymas:
Didelėms zonoms sukurti

Autentifikacija:
Individualizuota (802.1x)

Problemos:
Vartotojas yra kelių access points zonose
Vartotojas juda iš vieno access point zonos į kitą
Reikalingas zonos kontroleris

Tinklų architektūrų palyginimas

802.11b
Teorinis: 11Mbps
Praktinis: <5Mbps

802,11a/g
Teorinis: 54Mbps
Praktinis: <25Mbps

802.11n
Teorinis: 300Mbps
Praktinis: <100Mbps

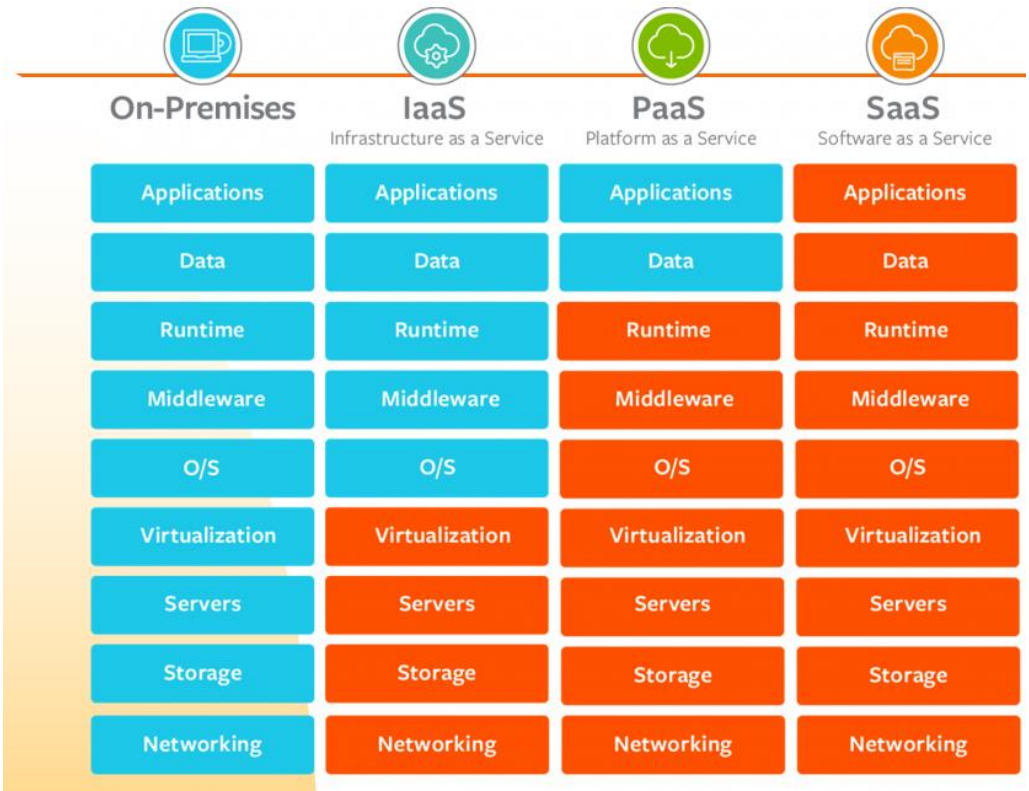
16.Debesų infrastruktūra. IaaS, PaaS, SaaS. Talpyklų rušys block, blob, shared, ephemeral ir jų skirtumai.

Software as a Service (SaaS)
Tai programinės įrangos (aplikacijų) pateikimo modelis
Aplikacija veikia debesyje
Klientas ja naudojasi per naršyklę
Nieko nereikia instaliuoti
Skirta galutiniam vartotojui

Google Docs
Dropbox
Failų konverteriai online

Platform as a Service (PaaS)
Paruošta aplinka tam tikro tipo aplikacijoms
Aplinka visam gyvavimo ciklui: paruošimas, paleidimas, palaikymas
Pateikiamos reikalingos priemonės: redagavimas, konfigūravimas, logai, VPN prieiga, IP ir DNS, apkrovų balansuotojas, firewall ir t.t.
Pateikiamos automatizavimo priemonės

Infrastructure as a Service (IaaS)
Infrastruktūros pagal pareikalavimą paslauga
Pateikiama plati gama pasirinkimų: procesoriai, vidinės ir išorinės atmintys, operacinės sistemos, tinklas



Talpyklų rūšys
Block – virtuali failų sistema
Primontuojama/pasiekiama per naršyklę
Duomenų saugojimas kontroliuojamas
Failų ar blokų lygio replikavimas

Blob – objektų saugykla
Nestruktūrizuota – video, nuotraukos ir panašiam turiniui

Ephemeral – trumpalaikė
Dingsta sustabdžius procesą
Viduje resurso
Ne vartotojų duomenims, o vidinei aplikacijai

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

Docker konteineris
Tai atskiras, vykdomas programinės įrangos paketas su jame paleistu vienu servisu

Jame yra viskas, ko reikia servisui paleisti: kodas, vykdymo aplinka, sistemos bibliotekos ir parametrai
Minimalus apvalkalas
Nėra nieko nebūtino serviso veikimui

Konteinerio atvaizdas
Atvaizdas (image) tai servisas ar programa supakuota su visa jos vykdymui reikalinga aplinka.
Konteineris tai vykdomas atvaizdo egzempliorius.

Sudaryti iš nedalomų sluoksnių
Portabilus ir gali būti naudojamas tarp skirtingų platformų
Vienas atvaizdas gali būti kito atvaizdo pagrindu
Daug sluoksnių sudaro didelį atvaizdą

Konteinerių vykdymo aplinka
Suteikia izoliuotą aplinką
Paleidžia vieną pradinį procesą (by default)
Gali būti lyginamas su Micro VM
Savininko resursai yra vieši
Pakuoja geriau negu virtualios mašinos

Kubernetes

Tai didelės apimties konteinerių technologijos pagrindu sukurtoms programoms valdyti skirta infrastruktūra.

Kubernetes leidžia efektyviau išnaudoti reikalingus resursus ir užtikrinti, kad nei padidėjus naudotojų skaičiui, nei sutrikus dalies serverių veiklai, sistema „neužlūš“.
Taip pat leidžia atnaujinti sistemą „nepastebimai“, neišjungiant jos ilgesniam laikui ir leidžia lengviau perkelti sistemas ar jų dalis iš vienos infrastruktūros į kitą.

Programuotojams integravus kodą į bendrą repositoriją, turima sistema automatiškai kodą kompiliuoja, testuoja ir įdiegia į reikiamą aplinką

Infrastruktūros valdymo įrankiai
Didelėms sistemoms: valdyti sąsajas tarp susietų resursų.

Naudoja programinį kodą, o ne interaktyvius įrankius.

Orkestravimo įrankiai yra naudojami infrastruktūros kūrimui.

Konfigūravimo – programinės įrangos konfigūravimui.

Terraform – įrankis skirtas sukurti infrastruktūrą (CD) naudojant kodą, kiti daugiau konfigūracijos valdymui

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

Maršrutizatorius

- Tai tinklo mazgas, jungiantis du ar daugiau lokalių tinklų.
- Tinklo sluoksnio (L3) paketų perdavimas tarp mazgų, priklausančių skirtingiems LAN, galimas tik per maršrutizatorių.
- Maršrutizatorius parenka kelią pagal maršrutų lentelę
- Tiesiogiai prijungti tinklai nusirodo konfigūruojant jungtis (sąsajas) ir į maršrutų lentelę patenka automatiškai

Statinių maršrutizavimo lentelių trūkumai

- Netinka dideliam tinklui
- Nėra automatinio maršrutų parinkimo

Maršrutizavimo protokolai

Aprašo:

- kaip pasiųsti maršrutų pasikeitimus
- marštutų pasikeitimus apibūdinačią informaciją ir jos formatus
- kada siųsti maršrutų pasikeitimus
- kaip surasti, kam turi būti siunčiami maršrutų pasikeitimai

Egzistuoja du tipai:

- Atstumų vektoriaus (*probably RIP*)
    - maršrutizatoriai transliuoja savo maršrutų lenteles kaimynams kas tam tikrą laiko intervalą
    - maršruto ilgis skaičiuojamas iteratyviai
    - Jei gautas maršruto α ilgis geresnis už kitą žinomą, tai įsimenamas naujas maršrutas
    - sekančio šuolio maršrutizatoriumi maršrutui tampa jo pranešėjas
    - pasikeitimai maršrutų lentelėse sklinda bangos principu
- Ryšių busenų (*probably OSPF*)
    - kiekvienas marštutizatorius žino visą tinklo topologiją ir ryšių būsenas
    - maršrutizatorius savo ryšių pasikeitimus siunčia multicast būdu
    - kiekvienas maršrutizatorius maršrutus skaičiuoja pats pagal trumpiausio kelio grafe radimo algoritmą

RIP – Routing Information Protocol

- Maršrutizatoriai žino tiesiai prijungtus tinklus
- Žinomi kaimyninių maršrutizatorių adresai
- Maršrutizatoriai periodiškai perduoda savo lenteles kaimynams
- Lentelės perskaičiuojamos

Keičiasi maršrutų informacija su kaimynais kas 1-3 minutės
Pasikeitimai sklinda banga
Dideliame tinkle lėtai konverguoja
Maksimalus tinklo skersmuo 16 šuolių
Sudėtingos konfigūracijos tinkle galimos pranešimų lenktynės ir dėl to atsirandančios klaidos lentelėse

OSPF – Open Shortest Path First

Standartizuotas IETF (RFC 2328)
Hierarchinis: 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. Tam jis siunčia Hello žinutes lokaliame tinkle. Hello siunčiami dažnai, kad greitai pastebėti ryšio pasikeitimą.
- Jei ryšio būsena pasikeičia (prarandamas ar vėl atsiranda), pranešama visiems srityje esantiems maršrutizatoriams. Jie perskaičiuoja savo maršrutų lenteles.

19.Tinklo sluoksnis. Interneto principai. IP paketo formatas.

Interneto principai

- Paketų komutavimas
- Klaidų taisymas
- Nėra dedikuotos tinklo infrastruktūros
- Tinklų tinklas (perdavimas iš vieno tinklo į kitą per maršrutizatorius)
- Autonominės sistemos. Savarankiški paslaugų tiekėjai
- Duomenų perdavimo kokybė, apskaita ir saugumas neužtikrinami

OSI modelio tinklo sluoksnis (L3)

Atlieka duomenų perdavimą tarp bet kurių dviejų mazgų bet kokio dydžio ir bet kokio sudėtingumo tinkle, tačiau dažniausiai negarantuoja duomenų perdavimo teisingumo.

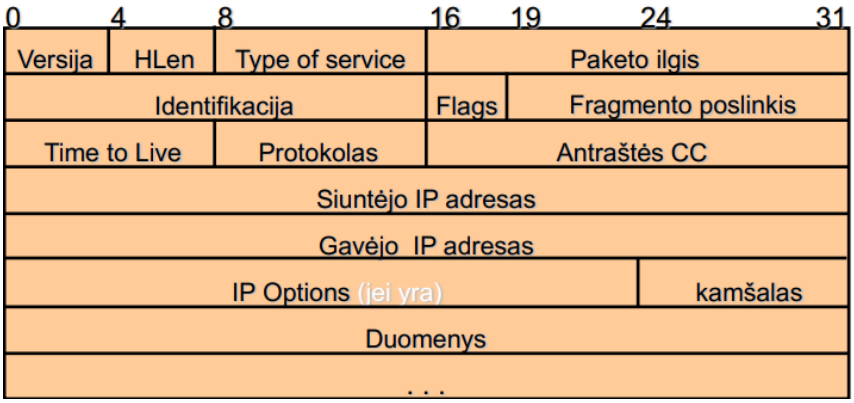
Funkcijos:

- Maršruto tinkle paieška
- Paketo perdavimas sekančiam mazgui

Perdavimo tarp tinklų principai

IP paketo antraštė turi visą informaciją, kuri reikalinga pristatyti paketą į gavėjo kompiuterį:

- Gavėjo IP adresą
- TTL
- TOS
- Siuntėjo adresą
- Fragmento identifikaciją



TTL (Time To Live) - paketo gyvavimo laikas. Kiekvienas maršrutizatorius jį mažina vienetu, o kai jis baigiasi paketas naikinamas.
TOS (Type Of Service) - požymiai gali būti naudojami perdavimo kokybės valdymui. Tačiau vien požymių nepakanka, reikalingas specialus protokolas.
Fragmentai atsiranda kai IP paketas netelpa į vieną kanalinio sluoksnio kadrą. Reikia suskaldyti į kelis. Fragmentai surenkami atgal gavėjo.

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

Autonominė sistema (AS) tai 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

Tai stambiausias registruojamas interneto darinys
Paslaugų teikėjas turi vieną AS.

Autonominė sistema aprašoma parodant jos vietą kaimyninių AS aplinkoje:

- iš kokių AS ir kokius skelbimus priima
- kokioms AS perduoda savo skelbimus

Autonominių sistemų rūšys

- Vienaryšė AS – single homed
    - Mažos lentelės
    - Užtenka žinoti kelius tik savoje AS
    - **Nėra** tiesioginio kelio tarp kaimyninių AS
- Vienaryšė AS – single homed + peering
    - Užtenka žinoti kelius tik savoje AS
    - Kraštiniai maršrutizatoriai turi ***du*** kelius – nėra tranzito.
    - Peering – nemokamas
- Daugiaryšė AS – multihomed
    - kiekvienu ryšiu naudojasi tik viena dalis tinklų
    - Nustatomi skirtingi *default* keliai, skelbiama tik dalis tinklų
    - Nutrūkus vienam – reikia perkonfigūruoti
- Tranzitinė AS – transit
    - Yra pagrindinė AS naudojama savo vartotojų
    - Naudojamos papildomos AS duomenų perdavimui, tačiau atsiranda tranzito kaina

Maršrutizavimas tarp AS

- Kiekviena AS turi unikalų numerį
- Kiekviena AS turi IP adresų aibę
- Reikalingas bendras protokolas skelbti maršrutams iš vienos AS tinklų į kitos AS tinklus
- Du maršrutizatorių tipai:
    - vidiniai – dalinasi informacija apie maršrutus vienos AS viduje
    - kraštiniai– keičiasi informacija apie maršrutus tarp AS ir reikalingą dalį perduoda vidiniams
- Kraštiniai bendrauja tarpusavyje Border Gateway protokolu

21.DNS sistemos funkcijos, hierarchija, replikavimas. Vardų serverių rušys, rekursyvios ir iteratyvios užklausos, DNS įrašai.

Interneto vardai
DNS "verčia" interneto vardą į IP adresą

DNS – interneto vardų sistema. Duomenų perdavime tinklu interneto vardai nenaudojami. Jie skirti žmonėms dėl paprastumo.

Transliacija iš interneto vardo į IP nebūtinai vienareikšmė. Dėl to DNS gali atlikti papildomas funkcijas.

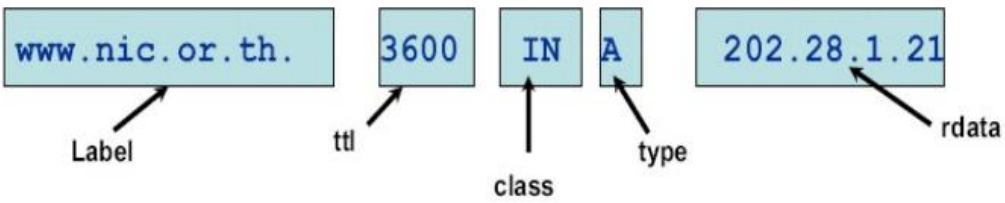
DNS hierarchija
- 13 root serverių – [a-m].root-servers.net
- 1 lygio sritis - .com, .net, .lt ir t.t.
- 2 lygio sritis – google.com, litnet.lt
- 3 lygio sritis – if.ktu.lt

Vardų serverių rūšys
Autoritatyvūs – pirminiai ir antriniai vardų serveriai
Neautoritatyvūs – duomenys juose 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
- Resursų įrašai susidaro iš savo vardo, TTL, klasės, tipo ir RDATA
- TTL yra laiko nustatymo parametras
- IN klasė plačiausiai naudojama
- Yra daug RR įrašų tipų
- Viskas už tipo identifikatoriaus yra vadinama RDATA



DNS įrašų tipai
Type=A
Type=NS
Type=MX
Type=CNAME