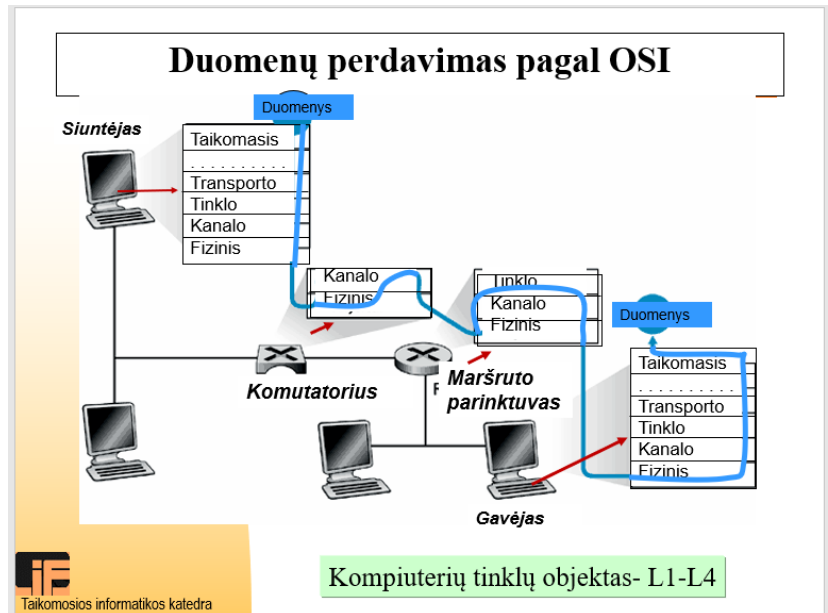


## 1. OSI modelio sluoksniai. Sluoksnių apibūdinimas. Komunikavimo procesas

- Atvirųjų sistemų jungimo (Open Systems Interconnection ) protokolų modelis
- Autorius: International Organization for Standardization (ISO)
- Teorinė sistema, bet plačiai naudojama praktiškai
- 7 sluoksniai
  - Taikymo – skirtas **vartotojui**, pvz. HTTP aprašo sąveiką “naršyklė - WEB serveris”
  - Pateikimo - duomenų **formatai**, šifravimas
  - Sesijos - autentifikacija, **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 naudoja naršyklę ir per ją kreipiasi į tinklo 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 (portą 80) ir atidaro savo portą 1212 duomenų priėmimui
5. Perduoda paketą tinklo sluoksniui – IP
6. Tinklo sluoksnis: Prieš formuojant antraštę reikia gauti IP adresą.
7. Į IP antraštę įrašo gavėjo ir siuntėjo IP adresus ir perduoda į Ethernet sąsają
8. Kanalo sluoksnis: Jis perduos paketą tik lokalaus tinklo ribose, Taigi ne galiniam gavėjui 94.16.59.10 o tarpiniam mazgui 193.12.0.254. Reikia sužinoti šio mazgo MAC adresą



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

### Lokalus tinklas

- **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 nebūtinai reikalingas konfigūravimas ir įrenginių valdymas
- Mes LAN'u laikysime tokį tinklą (tinklo dalį), kuriame duomenų perdavimas vyksta L2 sluoksnyje

### Kanalo sluoksnis (L2)

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

## Perdavimo metodai lokaliame tinkle

**Transliacijų metodas** kai visi įrenginiai sujungti taip, kad bet kuris signalas pasiekia visus. Laidinėse terpėse istoriškai tai vadinama magistrale. Kad nekiltų sumaištis, magistralės ilgis arba tinklo diametras ribotas: minimalaus ilgio (64 baitai) paketas turi pasiekti visus mazgus kol dar nebaigtas siuntimas.

- Bet kurio mazgo perduodamus duomenis 'girdi' (priima) visi kiti -> bendrai visų mazgų naudojama ta pati tyšio terpė
- Kai [beveik] vienu metu pradeda siuntimą keli mazgai, neišvengiamos kolizijos. Paketai sugadinami. Reikalingi mechanizmai susidūrimų skaičiui minimizuoti:
  - laidinėse terpėse IEEE 802.3 – Ethernet CSMA/CD
  - belaidėse IEEE 802.11 – CSMA/CA

Tinklas negali būti didelis, nei atstumais, nei vienu metu dirbančių mazgų skaičiumi.

Laidinėse terpėse nebenaudojamas dėl žemo efektyvumo esant didelėms (1-10 Gbps) spartoms.

Nėra kuo pakeisti belaidžio ryšio Wi-Fi zonose, kur tenka dalintis ta pačia dažnių juosta

**Paketų komutavimo metodas** kai 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 apsimokyti, t.y. įsiminti į kokias jungtis ateina paketai iš tam tikrų adresų.
- Adresacijos sistema lokali
- Siuntimo sparta gali būti labai didelė  
10/100/1000/10000 Mbps
- Tuo pačiu metu galima ir siųsti ir priimti paketus (duplexinis perdavimas)

1 Gbps ir ypač 10 Gbps paketų komutavimo technologijos konkuruoja su tradicinėmis telekomunikacijų technologijomis WAN (globalių tinklų) srityje, nes galimi dideli atstumai tarp įrenginių.

## Komutavimo algoritmas

Pagrindinis principas: nukreipti į komutatorių ateinantį paketą į VIENĄ iš jungčių pagal paketo antraštėje esantį gavėjo adresą

**Priimti į jungtį X ateinantį paketą. Žiūrėti siuntėjo ir gavėjo adresus.**

1. Apsimokymas pagal **siuntėjo** adresą:

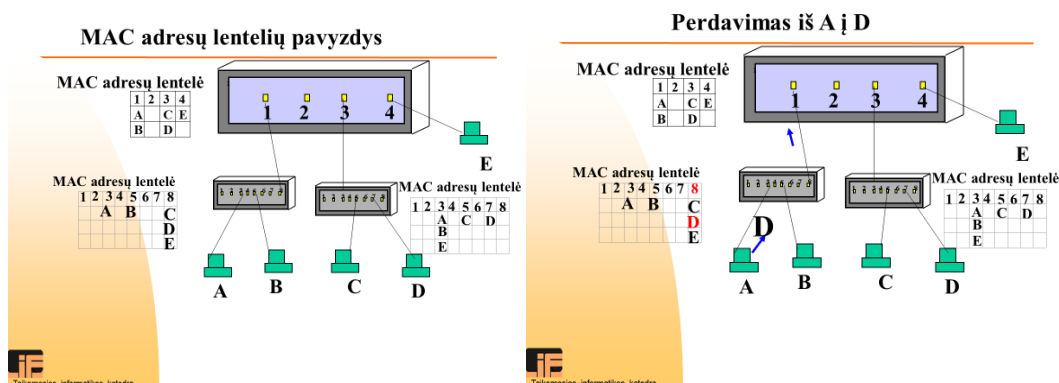
- Jei **siuntėjo** **adreso** dar nėra MAC adresų lentelėje, įrašyti į MAC adresų lentelę (X, naujas\_siuntėjo adresas)
- Jei **siuntėjo** **adresas** yra MAC adresų lentelėje, tačiau ten nurodyta kita jungtis, pakeisti įrašą MAC adresų lentelėje (su išlygom)

2. Persiuntimas pagal gavėjo adresą:

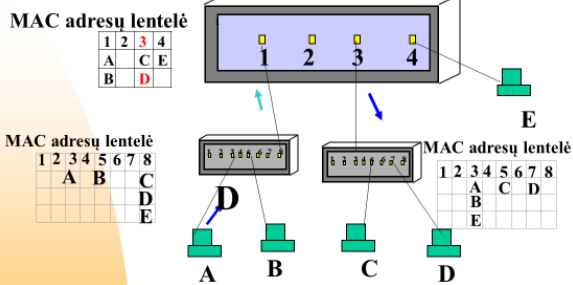
- Nustatyti išėjimo jungtį Y iš MAC adresų lentelės pagal **gavėjo adresą**.
- Jei  $X=Y$  paketą sunaikinti (**filter**) (atgal perduoti netikslinga)
- Jei  $X \neq Y$  paketą perduoti (**forward**) į Y
- Jei **gavėjo** **adreso** nėra lentelėje, paketą paskleisti (**flood**) per visas jungtis, išskyrus X

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

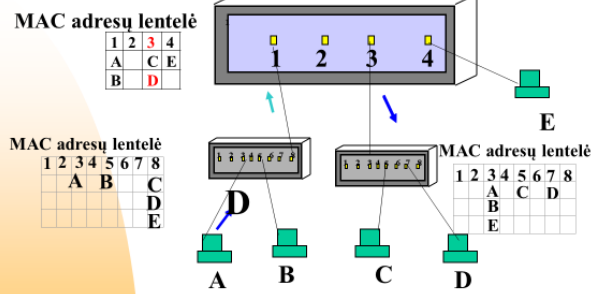
## MAC lentelės ir ARP.



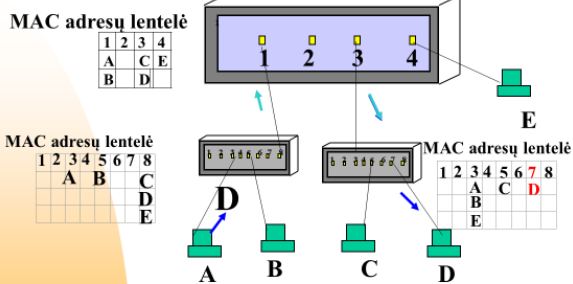
### Perdavimas iš A į D



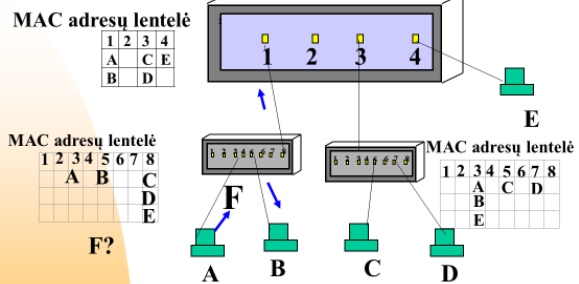
### Perdavimas iš A į D



### Perdavimas iš A į D

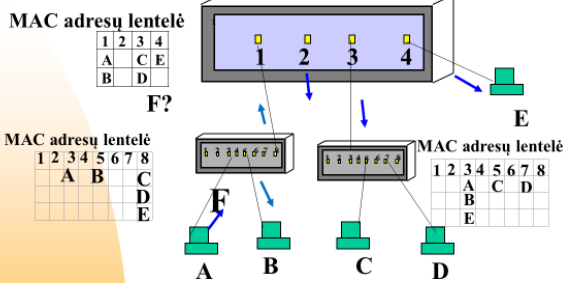


### Užtvindymas

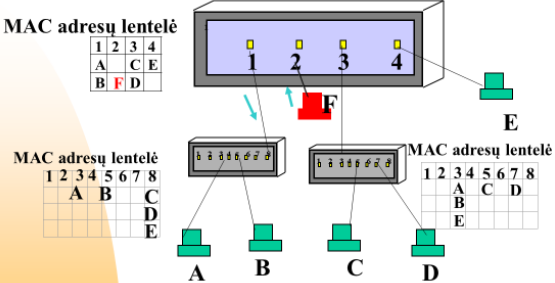


Siunčiamas paketas dar negirdėtam mazgui F.  
Jo nėra MAC lentelėse

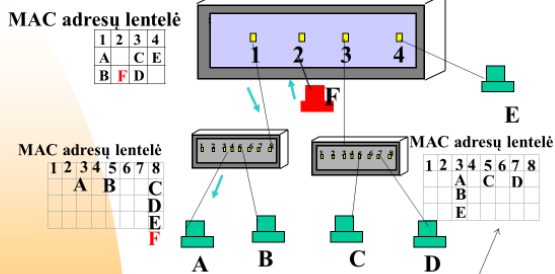
### Užtvindymas



### F atsako į A



### F atsako į A



Šioje lentelėje F adresas neatsirado

Naudojamas 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 [laikiniai] nebereiks.

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

#### IEEE 802.3 standartai

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

Pavadinimas	IEEE	Terpė	Atstumas
10BaseT	802.3	Vyta pora CAT3	100 m
10BaseFL	802.3j	MM (850 nm)	2 km
100BaseTX	802.3u	Vyta pora CAT5	100 m
100BaseFX		MM (850 nm)	2 km
		SM (1310 nm)	10 (20) km
1000BaseTX	802.3z	Vyta pora CAT5/6 (4 poros)	100 m
1000BaseSX		MM (850 nm)	550 m
1000BaseLX		SM (1310 nm)	5 (10) km
		550 m	
10GBaseSR	802.3ae	MM (850 nm)	65 m
10GBaseLR		SM (1310 nm)	10 km
10GBaseER		SM (1550nm)	40 km

**MAC adresai** (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:FF16 Skirtingai nuo IP, MAC adresai niekaip negrupuojami: nesvarbu koks jis yra, svarbu tik kad tame pačiame LAN jis būtų unikalus.

#### Komutatoriai

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

#### Nevaldomi LAN komutatoriai

Paprastai jungtys gali dirbti skirtinguose režimuose:

- Viena iš kelių spartų: 10/100/1000
- Pilnas duplexas/pusiau duplexas
- Automatinis režimo nustatymas: sparta/duplexas (autosensing/autonegotiation)

#### 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 reikalingas
- 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 konsolėi

- 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

### ***Būtina žinoti ir suprasti:***

- Komutatoriais kompiuteriai jungiami į vieną tinklą, tinklai tarpusavyje jungiami maršrutizatoriais
- Visi tarpusavyje sujungti komutatoriai ~ vienas didelis
- Komutatoriai jungiami be kilpų
- Komutatorius iš esmės yra nematomas tinkle automatiškai veikiantis įrenginys, neturi jokių adresų
- L2 perdavimas (Ethernet paketais) vyksta tik vieno LAN ribose.
- Kaimynų MAC adresai sužinomi klausiant broadcast užklausomis (ARP metodas)

## **4.Virtualūs lokalūs tinklai. Kadru žymėjimas IEEE802.1q**

Įprastinėmis lokalių tinklų technologijomis sunku realizuoti šiuolaikinius tinklus. Naudojant VLAN technologiją skirtingos paskirties įrenginius (t.y. keletą LAN'ų) galima jungti prie to paties komutatoriaus. Iš kitos pusės, 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.

### ***Kadru 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

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 gali būti taikomas arba **įeinantiems** į maršrutizorių 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** (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
<b>Vienas adresas</b>	1.1.1.1 255.255.255.255	1.1.1.1 0.0.0.0 host 1.1.1.1
<b>Segmentas /24</b>	1.1.1.0 255.255.255.0	1.1.1.0 0.0.0.255
<b>Segmentas /28</b>	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

## ACL naudojimas

1. Blokuoti (deny) komunikavimui pakanka blokuoti paketus bent viena kryptimi.
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*

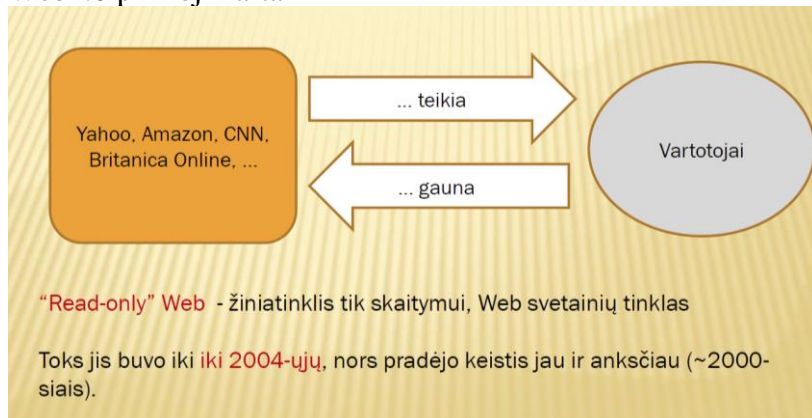
Blokuoti 3.3.3.20. Galimi trys variantai:

- 1) deny ip 1.1.1.0 0.0.0.255 host 3.3.3.20 - ant 1.1.1.254 jungties
- 2) deny ip host 3.3.3.20 1.1.1.0 0.0.0.255 - ant 192.168.0.1 jungties
- 3) abu filtrai

Vieno filtro pakanka duomenų apsikeitimui nutraukti, bet lieka vienkrypčio siuntimo galimybė

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

Web1.0 pirmoji karta



Web 2.0. Kas pasikeitė?

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

WEB3.0 –KAS TOLIAU?

- Mobilumas–sprendimai, pritaikyti mobiliems prietaisams
- Statistika —~50% vartotojų internetu naudojasi per mobiliųjį 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 sukurama ir įkeliama norimoje vietoje ir norimu laiku
- *Taisyklė*–vartotojas turi patogiai pasiekti paslaugą iš bet kokio terminalo
- 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)

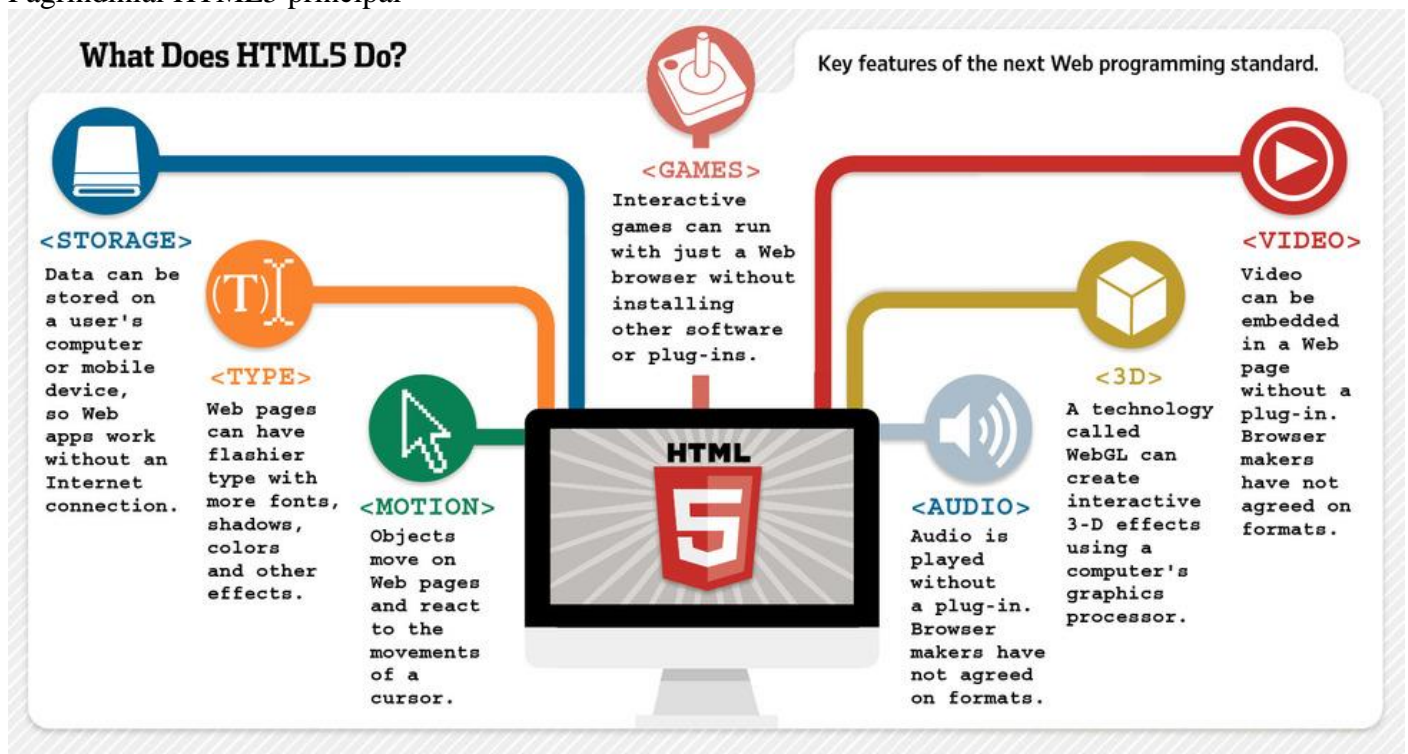
#### HTML standartas

- HTML kalbos standartą kuria **W3C** (*World Wide Web Consortium*) - tarptautinis įvairių internetą bei WWW tobulinančių kompanijų konsorciumas.
- HTML standartas buvo sukurtas naudojantis ISO (*International Organisation for Standards*) sukurta dokumento elementų bei jų žymėjimų sistema \* **SGML** \* (*Standard Generalized Markup Language*).

#### Kas pakeitė HTML4?

- Ilgai buvo neaišku, kokia kryptimi tobulės HTML standartas: yra du skirtingi ir labai stipriai konkuruojantys pasiūlymai, kiekvienas su savo privalumais ir trūkumais:
- XHTML2 (*eXtensible HyperText Markup Language*)
- HTML5
- XHTML 2 siekė sukurti naują, logiškai tvarkingą kodo sistemą pagal klasikinius SGML kanonus taip, kad joje nebeliktų atgyvenų ir erdvės klaidingai interpretacijai;
- X/HTML 5 tęsė senąją HTML tobulinimo tradiciją tobulėti palaipsniui, pridėdant naujų kodo elementų ir palaipsniui atsisakant „atgyvenusių“.

#### Pagrindiniai HTML5 principai



#### Nauji formų tipai HTML5:

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

#### Nauji elementai –

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

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

Autorizacija - Kam priklauso kas?

*Autorizacija DAC (Discretionary Access Control)* - Kiekvienas objektas turi sąrašą, aprašantį, kokie subjektai turi konkrečias teises (skaityti, rašyti, vykdyti).

*Autorizacija RBAC (Role-based Access Control)* - Prieigos kontrolė priklauso nuo rolės. Subjektai priklauso konkrečiai rolei. Subjektas gali priklausyti tik vienai rolei. Prieigos teisės aprašomos rolėmis.

*Autorizacija MAC (Mandatory Access Control)* - Privaloma teisių valdymo strategija. Failo savininkas neturi galimybės suteikti sukurtam failui teisių.

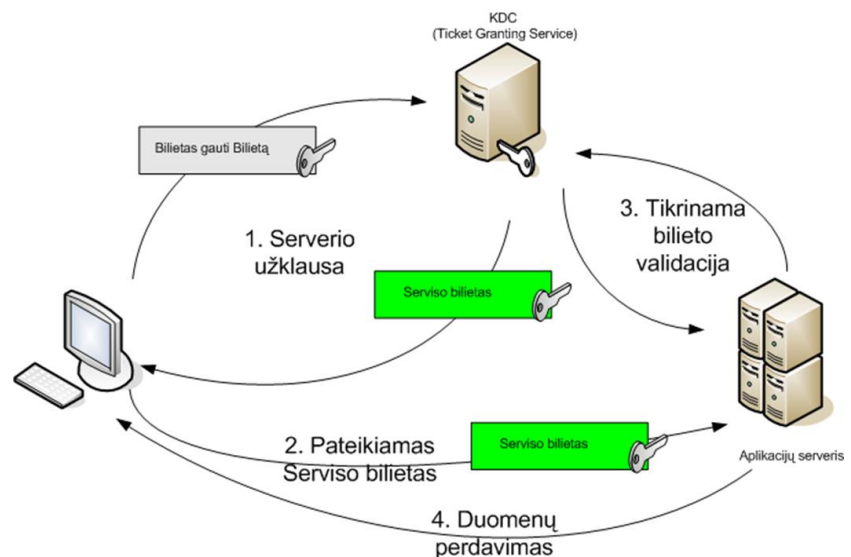
### Kerberos:

2005 m. RFC 1510 -> RFC 4120

Single sign-on

Mac OS, Win Server2000

.... Win Server2012, 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).

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

PIK (Viešųjų raktų infrastruktūros) sertifikatai – Generuojamos viešo ir privataus rakto poros.,

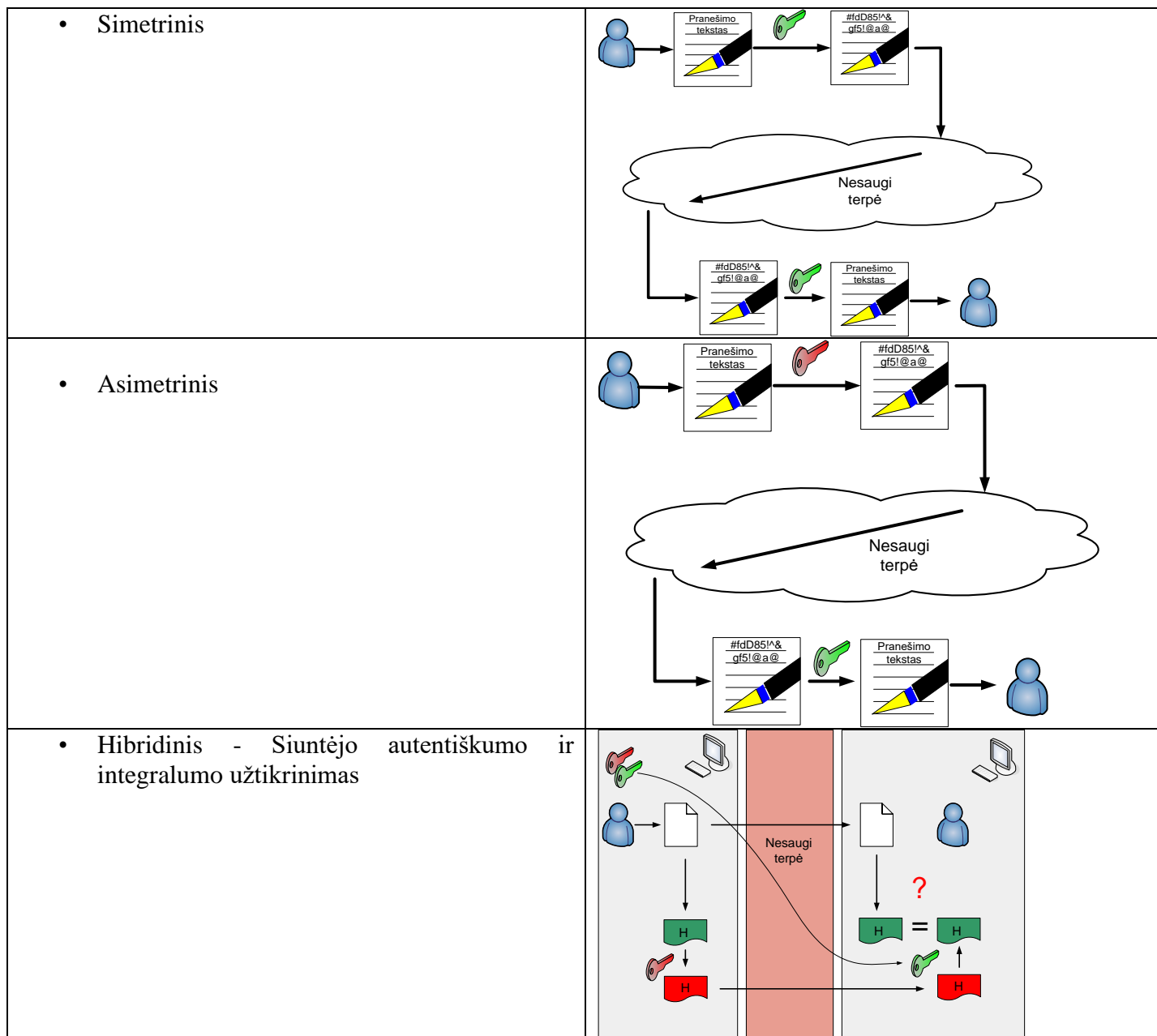
Viešųjų raktų infrastruktūros (PKI) taikymas:

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

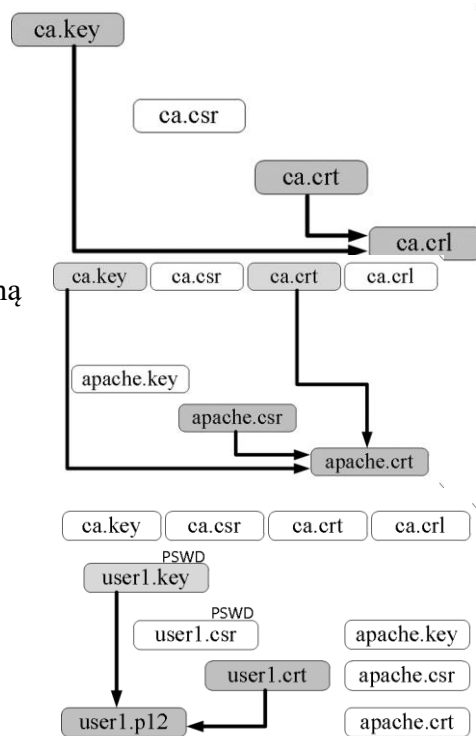
PIK sertifikatai

Šifravimo būdai:





1. CA privatus raktas
2. Sertifikato pasirašymo prašymas
3. Pasirašytas sertifikatas su CA
4. Sertifikatų paskelbimo negaliojančiais sąrašas
5. Sukuriamas WWW serverio privatus raktas
6. Sukuriame WWW serverio sertifikato pasirašymo prašymą
7. Prašymas pasirašomas su CA raktu
8. Sukuriamas vartotojo privatus raktas
9. Sukuriamas sertifikato pasirašymo prašymas
10. Prašymo pasirašymas su CA raktu
11. Sertifikato konvertavimas į PKCK12 formatą



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

### Transporto sluoksnis (L4):

- 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 -> priemonės

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

### Prievadai:

- Į transporto sluoksnį ateinantys paketai rikiuojami į atskiras eiles kiekvienam taikomajam procesui, veikiančiam tame kompiuteryje
- Duomenų paketų eilė prie taikomojo proceso vadinama prievadu
- Prievadų numeriai tai yra transporto sluoksnio paketų adresai
- Standartiniais taikomiesiems procesams skirti fiksuoti prievadų numeriai. Juos nustato IANA - Internet Assigned Numbers Authority

### Klaidų valdymas:

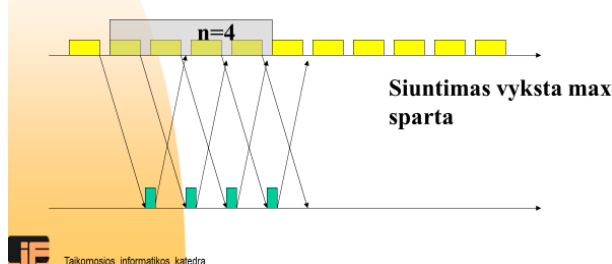
- Siuntėjas numeruoja siunčiamų duomenų porcijas ir kiekvienai iš jų per nustatytą laiką  $\Delta t$  turi gauti patvirtinimą ACK (Acknowledgegment) iš gavėjo.
- Nesulaukus ACK per nustatytą laiką  $\Delta t$ , duomenų porcijos siuntimas kartojamas
- Kada siuntėjas siunčia paketą pakartotinai?
  - Jei per užduotą laiko intervalą negaunamas ACK, laikoma, kad paketas nepasiekė gavėjo arba paketas pasiekė gavėją sugadintas. Reikia kartoti siuntimą

### Siuntimo langas:

Metodo esmė: išsiunčiamos  $n$  porcijų pailei. 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.

Siuntimo langas -1

Pirmosios porcijos gavimo patvirtinimas gautas dar prieš išsiunčiant  $n$ -tąją. Jei patvirtinimai suspėja ateiti n dydžio lango rėmuose, pasiekiamas maksimalus duomenų perdavimo greitis



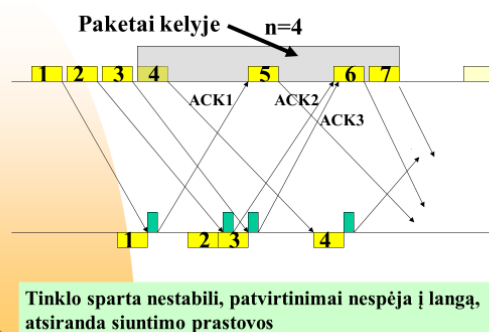
Perdavimo efektyvumas

$$N\text{-lango dydis, } a = \frac{t_{\text{kel}}}{t_{\text{siunt}}}$$

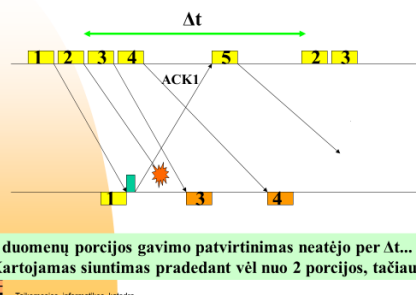
1) $N=1$	$U = \frac{1}{1+2a}$
2) $N \geq 2a+1$	$U=1$
3) $N < 2a+1$	$U = \frac{N}{2a+1}$

Galioja, kai nėra paketų nuostolių

Siuntimo langas -2



Siuntimo langas -3



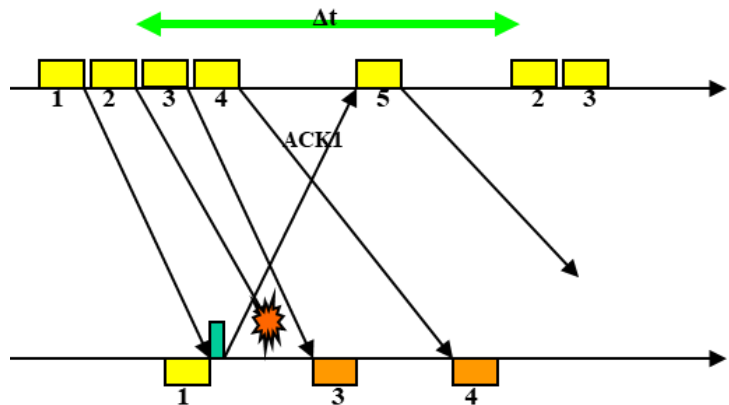
## Spartos reguliavimo principas

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

Kaitaliojant lango dydį priklausomai nuo tinklo būklės, tiksliau nuo prarandamų paketų kiekio, siuntimo sparta adaptuojama prie esamų sąlygų. Jei nesulaukiama išsiustų duomenų gavimo patvirtinimo, pakartotinai siunčiama mažiau duomenų -sparta mažėja, perkrova ar grūstis kažkuriame tinklo mazge išnyksta. Tas padeda tinkle išvengti lavininio perkrovų didėjimo, kuris būtų, jei siuntėjai pradėjus jų paketus naikinti ir toliau nemažintų siuntimo spartos.

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



**Prarasta 2 duomenų porcija**

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

### UDP - User Datagram Protocol

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)
- arba taikomasis procesas pats rūpinasi duomenų siuntimo pakartojimu
- arba duomenų perdavimas vyksta rezervuotu kanalu, kuriame paketų praradimo praktiškai nėra

UDP paprastas, spartus, nereikia didelių resursų

Gali būti naudojamas multicast režime

### Paketo antraštė (8 baitai)

<b>Siuntėjo portas</b>	<b>Gavėjo portas</b>
<b>UDP duomenų ilgis</b>	<b>Paketo kontrolinė suma</b>
<b>Duomenys</b>	

- Jei nurodytam paskirties portui nėra aktyvausproceso, paketas naikinamas
- Jei taikomasis procesas nespėja apdoroti į portą ateinančių paketų, netelpantys į buferį paketinaikinami
- 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 ta programa ar portas gavėjo kompiuteryje neaktyvus)

### TCP savybės - TCP antraštės formatas (20 baitų)

- Gali aptarnauti kelis sujungimus tuo pačiu portu
  - Reikia aiškių sujungimo įkūrimo ir užbaigimo procedūrų
- Potencialiai skirtingi RTT
  - Reikia adaptyvaus laukimo laiko nustatymo mechanizmo
- 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

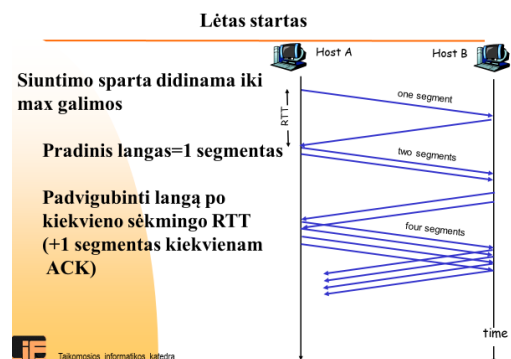
Siuntėjo portas				Gavėjo portas				
Sekos numeris Seq								
Patvirtinimo numeris Ack								
Ilgis	rezervas	U	A	P	R	S	F	Lango dydis
		R	C	S	S	V	I	
		G	K	H	T	N	N	
Kontrolinė suma				Svarbumas				

TCP	UDP
Įkuria loginį sujungimą	Be sujungimo
Patikimas, taiso paketų praradimus, sugadinimus ir neteisingą tvarką	Be garantijų
Dvipusis ryšis	vienpusis ryšis
Dvitaškis ryšis	Dvitaškis arba daugiataškis ryšis
Srauto perdavimas	Paketų perdavimas
Automatinis spartos valdymas	Spartą nustato siuntėjas

TCP taikymai	UDP taikymai
HTTP - WEB protokolas	Srautinės audio/video transliacijos, IP telefonija
FTP - failų siuntimo protokolas	DNS užklausos
Dokumentų ir kitų duomenų patikimam perdavimui	Kritiniams laiko atžvilgiu taikymams; Užklausoms, kurios gali būti kartojamos

### TCP siuntimo spartos valdymas:

- Jacobson (1988) įvedė į TCP perkrovų valdymo mechanizmą. Jo idėjos:
  - TCP bando tinklo pralaidumo galimybes
  - TCP reaguoja į perkrovas sulėtindamas duomenų siuntimą
    - AIMD- “Additive Increase (+1 segmentas) ;
    - Multiplicative Decrease” (du kartus).



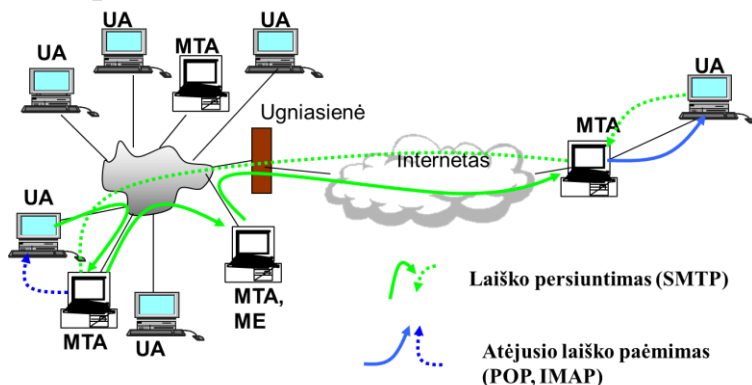
### Siuntimo klaidų taisymas:

Pakartojam principus:

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

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 bendrąja taisykle.

## 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, išsipareigoja 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.

## MIME:

- 1992 metų birželį paskelbtas Multipurpose Internet Mail Extensions (MIME) standartas, leidžiantis prie laiško prikabinti failus
- MIME suderintas su pagrindiniais e-pašto protokolais SMTP, POP and IMAP.
- MIME paskirtis - leisti persiųsti turtingesnio turinio ir kelių dalių laiškus
- MIME nėra apribotas tik naudojimu e-paštui: jį naudoja ir HTTP

## POP3:

- Skirtas gautiems laiškam perkelti iš serverio pašto dėžutės į vartotojo kompiuterį
- POP3 - dabartinė versija
- Veikia TCP protokolo pagrindu, naudojamas 110 portas
- Palaikomos tik kelios operacijos – autentifikacija, laiškų parsisiuntimas, antraščių parsisiuntimas, laiško pašalinimas
- Komandos ir atsakymai tekstiniai
- Paprastai toks serveris nesaugo ir išsiųstų laiškų kopijų

## 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.

### POP3

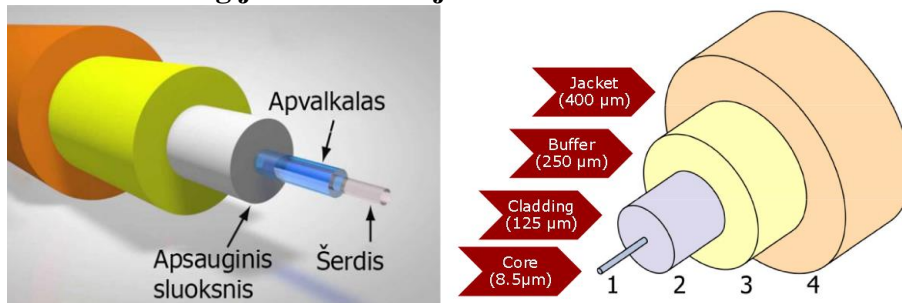
- **“Download and delete”** režimas - negalima paimti laiškų iš kitos vietos
- **“Download-and-keep”**: galima turėti kopijas keliose vietose, bet imlus serverio resursams
- POP3 – be būklės saugojimo tarp seansų

### IMAP

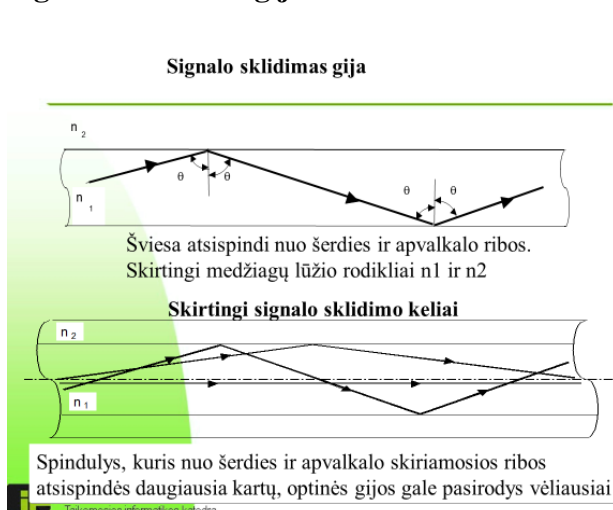
- Visi laiškai serveryje: vietos problema
- Laisvai konstruojami laiškų katalogai
- IMAP saugo vartotojų būklę tarp seansų
  - Katalogų vardus ir laiškų ID susiejimą su katalogų vardais
- Geresnė autentifikacija

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

### Vienos kabelio gijos konstrukcija

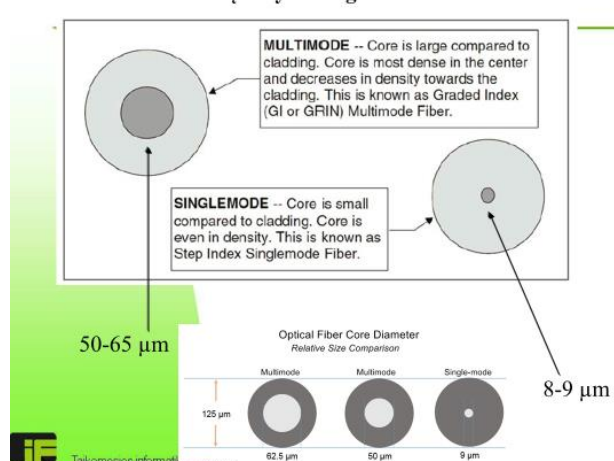


### Signalų sklaidimas gija

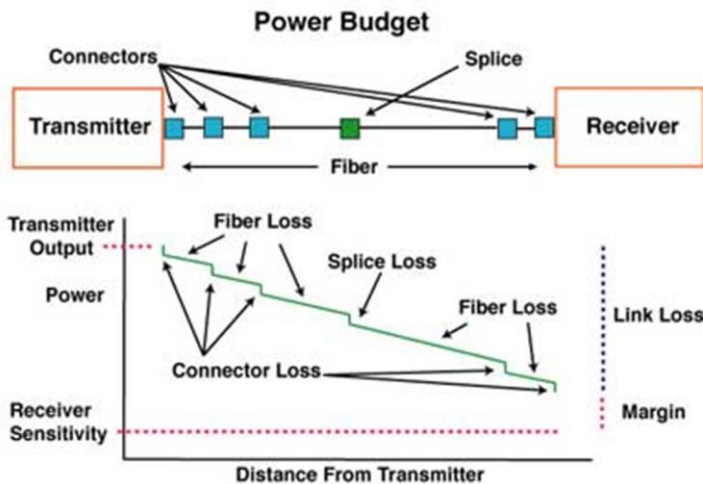


### Optinis biudžetas

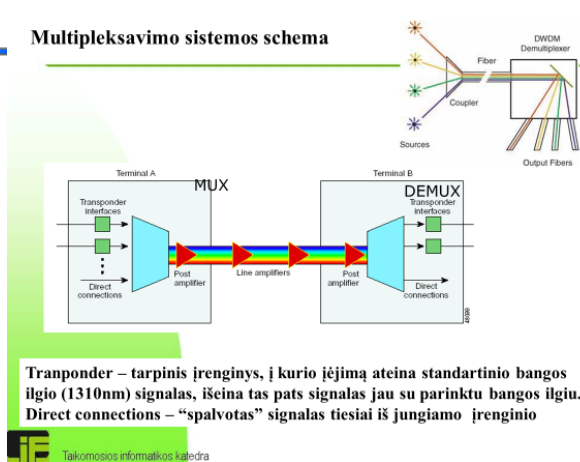
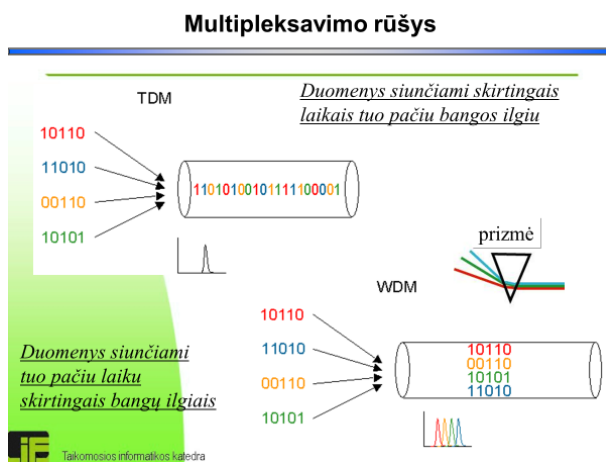
### Kabelių rūšys: daugiamodis ir vienmodis



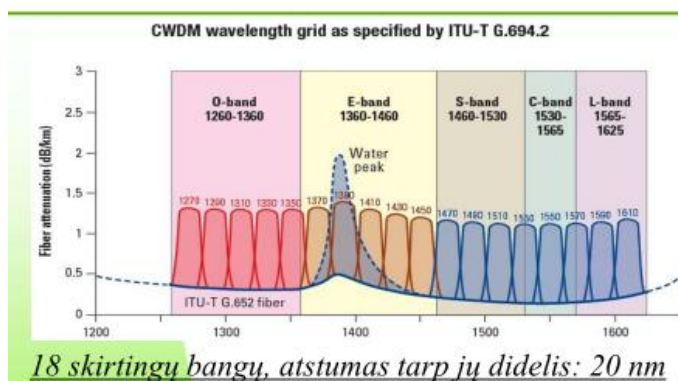




### 13. Multipleksavimo rūšys. Bangų multipleksavimo variantai. CWDM ir DWDM skirtumai.



### CWDM – “retas” multipleksavimas



### DWDM – “tankus” multipleksavimas

What exactly is Dense WDM (DWDM)?

- A much more tightly packed WDM system.
- Typically used for commercial long-haul systems.
- And typically based in the C-band.
- Specific channel sizes are standardized in an “ITU Grid”.
- Within C-band, these channel spacings are common:
  - 200GHz – 1.6nm spacing, 20 channels possible
  - 100GHz – 0.8nm spacing, 40 channels possible
  - 50GHz – 0.4nm spacing, 80 channels possible
  - 25GHz – 0.2nm spacing, 160 channels possible



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

#### Wi-Fi

Kilmė:

- ALOHAnet sukurta University of Hawaii (1971) – visų lokalių tinklų pirmtakas

Pagrindinė paskirtis:

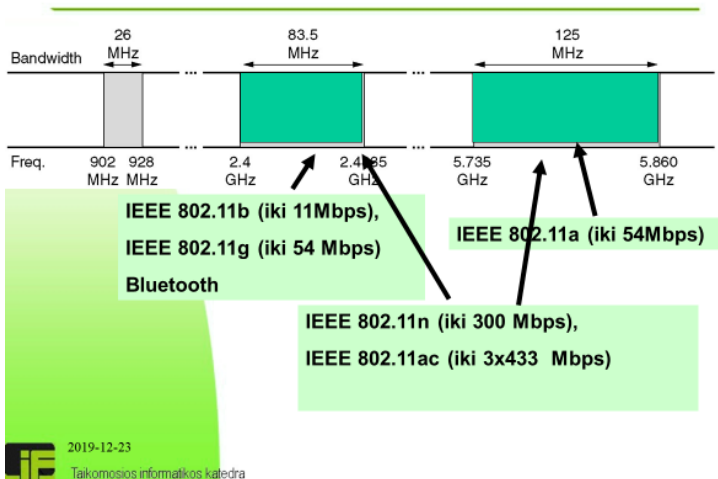
- bevielio ryšio zonos nešiojamiems kompiuteriams viešbučiuose, salėse, auditorijose, įmonių teritorijose.

Pagrindinės ypatybės:



- tie patys dažniai siuntimui ir priėmimui
- persidengiantys kanalai

### Wi-Fi dažnių juostos



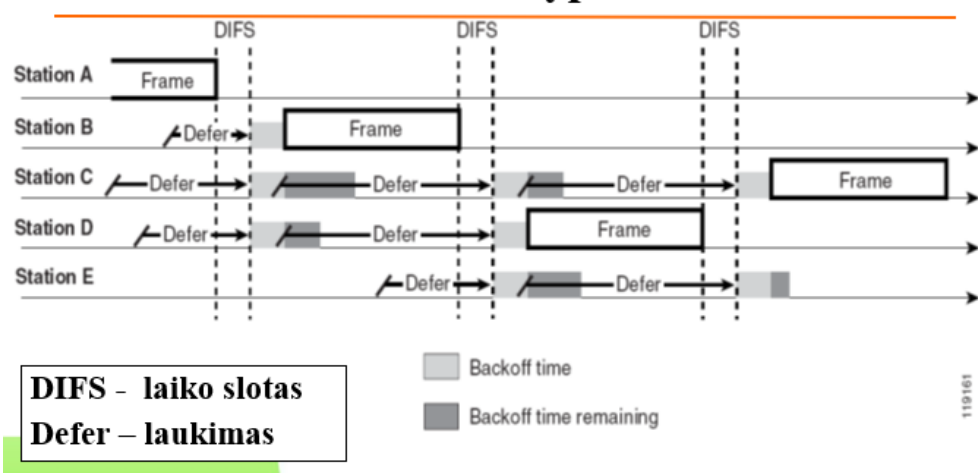
### Wi-Fi prieigos standartai IEEE 802.11

	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



### Palyginimas:

BSS	ESS
Kiekvienas AP turi atskirą SSID ir savo zoną <u>Iranga</u> : Belaidis maršrutizatorius <u>Taikymas</u> : individualiam naudojimui <u>Autentifikacija</u> : nustatytas slaptažodis (WEP, WPA2)	Visi AP sudaro vieną zoną su tuo pačiu SSID <u>Iranga</u> : Prieigos taškų sistema <u>Taikymas</u> : didelėms zonoms sukurti <u>Autentifikacija</u> : individualizuota (802.1x)
	<u>Problemos</u> :

Vartotojas yra kelių AP zonose  
Vartotojas juda iš vieno AP  
zonos į kitą  
-> reikalingas zonos kontrolieris

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

- Compute – virtual or bare metal machines
- Network – isolated cloud networks, routing, peering
- Storage – block, blob, shared, ephemeral
- PaaS – abstracts infrastructure, provides added service
- SaaS – abstracts PaaS, adds software on top, No infrastructure or software to maintain, Lower cost of ownership, Highly scalable

### Blob:

- Managed object storage
- Operates via an API
- Scales to petabytes automatically
- One of the core cloud services

### Block:

- **Managed virtual block devices**
- Supports file systems
- Attached to instances via network
- Persists data after instance dies
- Supports block level replication
- Supports provisioned IOPS

### Ephemeral:

- Best performance
- Directly attached to the host machine
- Should only ever be used for temporary data
- Usually comes with more expensive instances



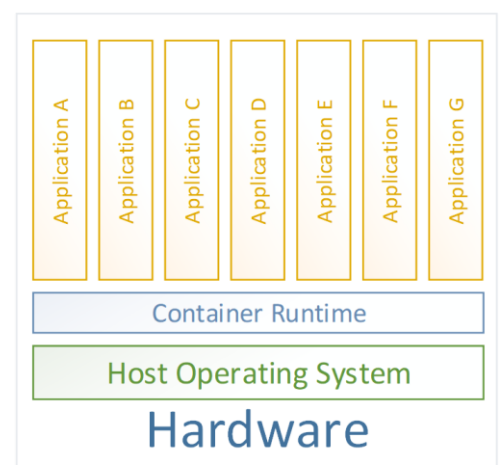
## 17. Konteineriai: Architektūra; Konteinerio atvaizdas (image); Docker failas; Repositorijos. Kubernetes: paskirtis ir pagrindiniai elementai

### Konteineriai:

- Provides isolated environment
- Runs one foreground process by default
- Can be compared to Micro VM
- Host resources are shared
- Packs better than virtual machines

### Konteinerio atvaizdas (image)

- Packages application and its dependencies
- Constructed from immutable layers
- Portable and cross-platform by nature
- One image can be a base for another
- More layers result in bigger image



Docker failas

## DOCKERFILE

```
FROM golang:1.12-alpine3.9

COPY . /k8s
WORKDIR /k8s
RUN go build -mod=vendor -o k8s101

FROM alpine:3.9
LABEL maintainer="tomas.adomavicius@centric.eu"

RUN apk --no-cache add ca-certificates
WORKDIR /k8s
COPY --from=0 /k8s/k8s101 k8s101
COPY static /k8s/static
ENV PATH="/k8s/:${PATH}"

EXPOSE 8080
CMD ["k8s101", "server"]
```

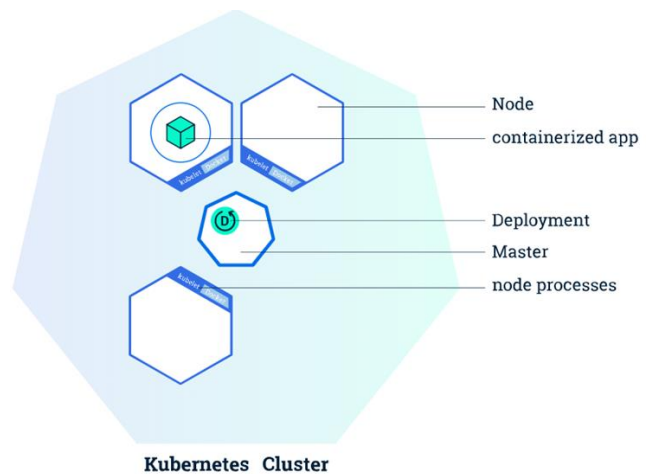
36ffb2d9b78	CMD ["k8s101" "server"]
b8a56d588a10	EXPOSE 8080
2d4999eb3219	ENV PATH=/k8s/:/usr/local/sbin:/usr/local...
81f3ec764f3c	COPY dir:3d02cf37eb2a1b176...
f5047510c77e	COPY file:b4d3308fb5795d32...
366fe75fed2c	WORKDIR /k8s
f50dffc28fa	apk --no-cache add ca-certificates
101d66874300	LABEL maintainer=tomas.adomavicius@centric.eu
055936d39205	CMD ["/bin/sh"]
<missing>	ADD file:a86aeaf3a7d68f6a...

Resulting Container Image Layers



### Kubernetes:

- Provides additional concepts
  - Pods - holds one or more containers
  - Services – provides network connectivity inside the cluster
  - Deployments – scales and monitors containers
  - ConfigMaps – provides manageable configuration for containers
  - Secrets – for sensitive information / configuration
  - Ingress – routes network for Services (and thus, to pods)
- Self healing
- Immutable infrastructure
- Declarative infrastructure



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

### Trūkumai:

- netinka dideliame tinklui,
- nėra automatinio maršrutų parinkimo

Nutrukus ryšiui nuo sąsajos 10.0.13.2, dalis tinklų taps nepasiekiami

### Maršrutizavimo protokolai

Maršrutizavimo protokolas aprašo:

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

Atstumų vektoriaus tipo

Ryšių būsenų tipo

### Atstumų vektoriaus tipo maršrutizavimo protokolai

Atstumų vektoriaus tipo maršrutizavimo protokolai remiasi tokiais principais:

- maršrutizatoriai transliuoja savo maršrutų lenteles kaimynams kas tam tikrą laiko intervalą,
- maršruto ilgis skaičiuojamas iteratyviai: kai X praneša maršrutą  $\alpha$  kaimynui Y, Y maršruto  $\alpha$  ilgį padidina atstumu (x,Y),
- Jei gautas maršruto  $\alpha$  ilgis geresnis už kitą žinomą, tai įsimenamas naujas maršrutas
- sekančio šuolio maršrutizatoriumi maršrutui tampa jo pranešėjas (X),

- pasikeitimai maršrutų lentelėse sklinda bangos principu.

### **Ryšių būsenų tipo maršrutizavimo protokolai:**

Ryšių būsenų tipo maršrutizavimo protokolai remiasi tokiais principais:

- kiekvienas maršrutizatorius 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(1)**

1. Maršrutizatoriai žino tiesiai prijungtus tinklus
2. Žinomi (Router Discovery arba administratorius nurodo) kaimyninių maršrutizatorių adresai
3. Maršrutizatoriai periodiškai perduoda savo lenteles kaimynams.
4. 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 protokolas**

- OSPF (Open Shortest Path First) ryšių būsenos tipo protokolas, naudojamas maršrutizavimui AS viduje
- 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 būseną pasikeičia (prarandamas ar vėl atsiranda), pranešama visiems srityje esantiems maršrutizatoriams. Jie perskaičiuoja savo maršrutų lenteles

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

### **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 (routing)

Paketo perdavimas sekančiam mazgui (forwarding)

### **Pagrindiniai interneto principai:**

- Paketų komutavimas= kiekvienas paketas keliauja tinklu savarankiškai -> paketo formatas
- Klaidų taisymas ->prarastų paketų pakartotinis siuntimas iš pradinio mazgo
- Nėra dedikuotos tinklo infrastruktūros -> visi mazgai lygiateisiai ir vieninga globali adresacija
- Tinklų tinklas -> perdavimas iš vieno tinklo į kitą per maršrutizatorius
- Autonominės sistemos = savarankiški paslaugų teikėjai -> kaip keičiamasi maršrutais = BGP
- Duomenų perdavimo kokybė, apskaita ir saugumas neužtikrinami -> „best effort“

- TTL- Time To Live - paketo gyvavimo laikas. Kiekvienas maršrutizatorius jį mažina vienetu, o kai jis baigiasi paketas naikinamas.
- Dabartiniame internete pakanka suformuoti pradinį TTL 64.
- TOS -Type Of Service - požymiai gali būti naudojami perdavimo kokybės valdymui. Tačiau vien požymių nepakanka: siuntėjas gali piktnaudžiauti ir nurodyti neteisingą. Reikalingas specialus protokolas.
- Fragmentai atsiranda kai IP paketas netelpa į vieną kanalinio sluosnio kadrą. (Pvz. Klasikinis Ethernet kadras talpina 1500 baitų). Tada tenka jį suskaldyti į kelis. Viena kartą suskaldyti paketai toliau keliauja atskirai. Fragmentus atgal į paketą surenka gavėjas.

## IP paketo formatas

0	4	8	16	19	24	31							
Versija	HLen	Type of service	Paketo ilgis										
Identifikacija			Flags	Fragmento poslinkis									
Time to Live		Protokolas	Antraštės CC										
Siuntėjo IP adresas													
Gavėjo IP adresas													
IP Options (jei yra)					kamšalas								
Duomenys													

Versija - dabar 4

Hlen - antraštės ilgis

(paprastai 20 baitų)

Type of service TOS

Time-to live TTL

Protokolas TCP-6 UDP-17

Identifikacija, Flags (žymės),

Fragmento poslinkis:

naudojami ilgų paketų suskaldymui į kelis



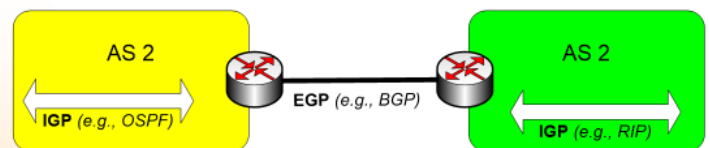
Taikomosios informatikos katedra

## 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 (ir globalų internetą) parinkimas
- Tai stambiausias registruojamas Interneto darinys.
- Paslaugų teikėjas paprastai turi vieną AS visiems savo ir savo klientų tinklams
- Autonominė sistema aprašoma parodant jos vietą kaimyninių AS aplinkoje:
  - iš kokių AS ir kokius skelbimus priima (from xxx accept)
  - kokioms AS perduoda savo skelbimus (to xxx announce)

## Interdomain vs Intradomain



### • Intradomain routing

- Routing is done based on metrics
- Routing domain is one autonomous system

### • Interdomain routing

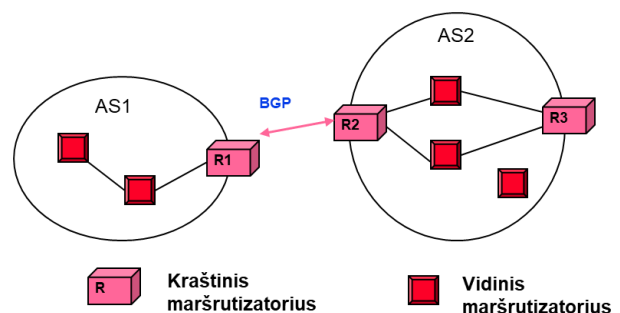
- Routing is done based on policies
- Routing domain is the entire Internet



Taikomosios informatikos katedra

## Maršrutizavimas tarp AS:

- Kiekviena AS turi unikalų numerį
- Kiekviena AS turi IP adresų aibę
- Reikalingas bendras protokolas maršrutams iš vienos AS tinklų į kitos AS tinklus skelbti
- 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 (BGP)



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

DNS “verčia” interneto vardą į IP adresą

DNS - Interneto vardų sistema. Duomenų perdavime tinklu interneto vardai nenaudojami: jie skirti žmonėms, kad būtų lengviau įsiminti.

Transliacija “internetu vardas “ -> “IP adresas” nebūtinai turi būti vienareikšmė. Pasinaudojant tuo DNS gali atlikti papildomas funkcijas

### Interneto vardų sistemos funkcijos:

- interneto vardas → IP numeris (ADDRESS),
  - sirius.cs.pdx.edu → 131.1.2.3,
- IP numeris → interneto vardas (PTR),
  - 131.1.2.3 → sirius.cs.pdx.edu,
- elektroninio pašto adresas → zonos pašto serveris (MX),
  - mail cat@cs.pdx.edu → sirius.cs.pdx.edu,
- antrinis vardas (aliasas) → pirminis vardas (CNAME),
  - www.cs.pdx.edu → sirius.cs.pdx.edu.

### DNS hierarchija

- 13 šakninių serverių – [a-m].root-servers.net
- 1 lygio sritys - .com, .net, .lt, .co.uk ir t.t.
- 2 lygio sritys – google.com, litnet.lt
- 3 lygio sritys – if.ktu.lt

Replikavimas



### Autoritatyvūs ir neautoritatyvūs vardų serveriai:

- 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 serijos 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:

DNS palaiko dvi užklausų rūšis:

- rekursyvias: užklausą gavęs ir nežinantis atsakymo serveris perduoda originalią užklausą kitam (savo vardu)
- iteratyvias: užklausą gavęs ir nežinantis atsakymo serveris gražina tik tinkamesnio serverio adresą “klausk pats”



**DNS įrašų tipai:**

Type=A

name=vardas, value= IPv4 adresas

Type=NS

name=srities\_vardas, value= šios srities autoritatyvus vardų serveris

Type = MX

value= Šios srities pašto serverio vardas

Type = CNAME

name=aliasas, value= pirminis vardas