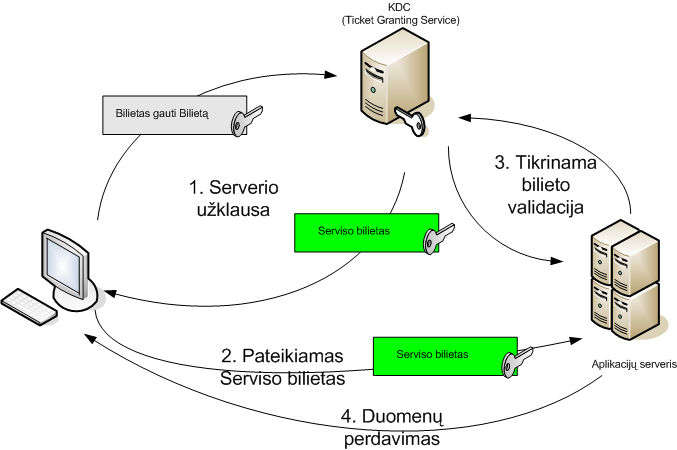
1. **Autorizacija, prieigų nustatymo mechanizmai** **:**

DAC - Kiekvienas objektas turi sąrašą, aprašantį, kokie subjektai turi konkrečias teises (skaityti, rašyti, vykdyti). RBAC - Prieigos kontrolė priklauso nuo rolės. Subjektai priklauso konkrečiai rolei. Subjektas gali priklausyti tik vienai rolei. Prieigos teisės aprašomos rolėmis. MAC - Privaloma teisių valdymo strategija. Failo savininkas neturi galimybės suteikti sukurtam failui teisių. Objektas – failas. Subjektas – vartotojas.

**Autentifikacijos metodai :** Kerberos - 2005 m. RFC 1510 -> RFC 4120. Single sign-on Mac OS, Win Server2000 . Win Server2012, ubuntu ir kt.



CHAP - 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 - 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).

1. **Viešųjų raktų infrastruktūra:** taikymas: Elektroniniams parašams; El. paštui šifruoti;Dokumentams šifruoti ir (ar) autentifikuoti; Vartotojams autentifikuoti informacinėse sistemose; GRID/Cloud tinkluose.

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

**Sertifikatai** Šifravimo būdai:

*Simetrinis –* užšifruojama tuo pačiu raktu, tačiau iškyla problema raktą perduoti gavėjui.



*Asimetrinis –* užšifruojama viešuoju, atšifruojama privačiuoju raktu. Raktai kuriami taip, kad žinant vieną iš jų, negalima sužinoti kito.



*Hibridinis* – stengiamasi sumažinti simetrinių ir asimetrinių sistemų atskiro naudojimo trūkumus (simetrinio – saugus rakto perdavimas, asimetrinis – laiko sąnaudos generuojant raktus).



1. **WWW –** pasaulinis žiniatinklis.

**WEB1**



**WEB2 -** 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), kurioje kuriami ir vykdomi įvairūs uždaviniai.

**WEB3** - *Mobilumas*–sprendimai, pritaikyti mobiliems prietaisams; *Statistika* –~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; *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-** 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*). Skirtingos HTML kalbos versijos dar vadinamos HTML specifikacijomis.

1. **CSS –**

CSS dėka galime nurodyti visiškai visą puslapio dizainą, teksto šriftus, išdėliojimą, spalvas ir atstumus tarp įvairių elementų.CSS leidžia apibrėžti stilių, bet kokiam konkrečiam HTML elementui ir priskirti jį keliems puslapiams

**XML** - XML - EXtensible Markup Language - gairių kalba, sukurta duomenų aprašymui; XML gairės nėra fiksuotos. Gaires reikia pačiam susikurti; XML su DTD (Document Type Definition) ar su XML schema yra “save aprašanti” kalba; XML yra W3C standartas nuo 1998 m. Naudojant XML duomenys saugomi atskirai nuo HTML; Naudojant XML galima keistis duomenimis tarp nesuderinamų sistemų; Naudojant XML tekstinius failus galima paprastai saugoti ir dalintis duomenimis; XML galima naudoti naujų kalbų kūrimui (pav. WML);

XML ir HTML skirtumai: XML sukurta duomenų aprašymui, HTML – duomenų vaizdavimui; XML nieko neatlieka; XML skirta sudaryti duomenų struktūras, saugoti ir siųsti duomenis; XML yra išplečiama kalba; XML yra HTML papildymas; XML Web kūrime taip pat svarbi kaip HTML;

**XSD -** XML schema yra XML pagrindu sudaryta DTD (dokumentų tipo aprašymas) alternatyva; XML schema aprašo XML dokumento struktūrą; XML schemos kalba yra XSD (XML Schema Definition);

**XSL** - Nustato dokumento gaires; Nustato dokumento atributus; Nustato kuri gairė yra dukterinė gairė; Nustato dukterinių gairių tvarką; Nustato dukterinių gairių kiekį; Nustato ar gairės yra tuščios ar gali turėti tekstą; Nustato gairių ir atributų duomenų tipus; Nustato gairių ir atributų numatytąsias reikšmes ir fiksuotas reikšmes; kalba, aprašanti XML dokumento transformaciją į HTML dokumentą arba į kitokios struktūros XML dokumentą; Visos dabartinės Interneto naršymo programos supranta XML ir XSLT;

1. **OSI modelio sluoksniai:**

Atvirųjų sistemų jungimo **(**Open Systems Interconnection **)** protokolų modelis;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 naudojasi naršykle 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. Transporto sluoksnis: TCP formuoja sujungimo su paslauga prašymo paketą (SYN), Antraštėje nurodo paslaugos rūšį (portą 80) ir atidaro savo portą 1212 duomenų priėmimui. 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

1. **Kanalo sluoksnis L2 :**

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 (Media Access Control - MAC adresus); Tarpinis kanalo sluoksnio įrenginys nekeičia perduodamo paketo; Kanalo sluoksnio įrenginys turi turėti atmintinę priimtam duomenų paketui įsiminti;

**Komutavimo algoritmas:**

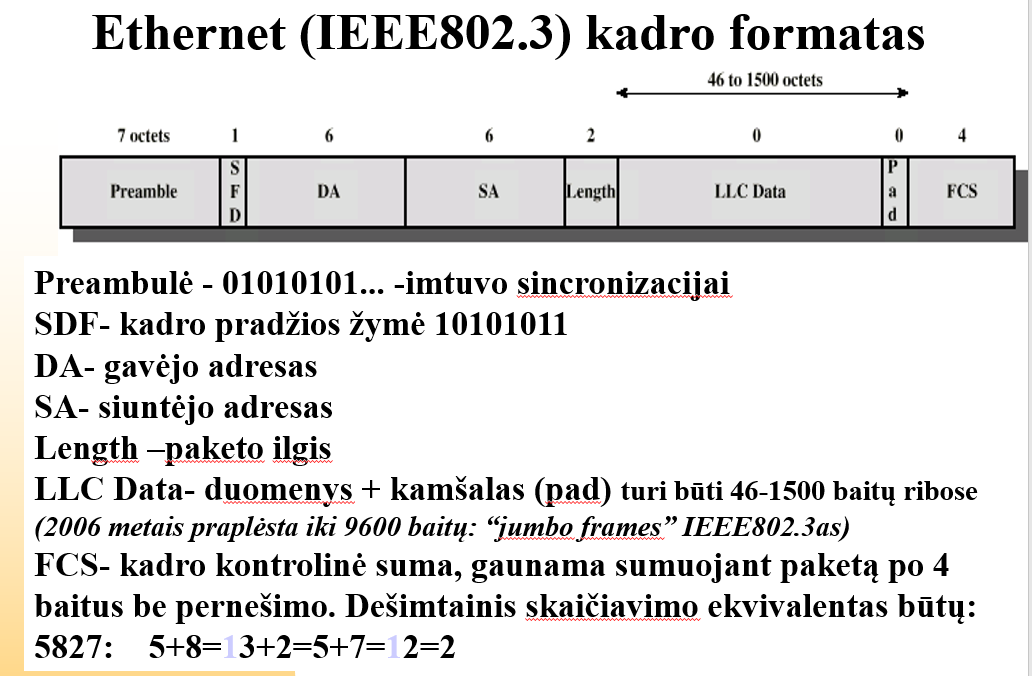
Priimti į Port1 ateinantį paketą. Žiūrėti jo antraštę: siuntėjo ir gavėjo adresus.

1. Apsimokymas:Jei siuntėjo adreso dar nėra MAC adresų lentelėje, įrašyti į MAC adresų lentelę (naujas\_siuntėjo adresas, Port1) ;Jei siuntėjo adresas yra MAC adresų lentelėje, tačiau ten nurodyta kita jungtis, pakeisti įrašą MAC adresų lentelėje (su išlygom)

2. Persiuntimas:Nustatyti išėjimo jungtį (Port2) iš MAC adresų lentelės pagal gavėjo adresą. Jei Port2=Port1 > paketą sunaikinti (filter); Jei Port2≠Port1 > paketą perduoti (forward) į Port2; Jei gavėjo adreso nėra lentelėje > paketą paskleisti (flood) per visas jungtis, išskyrus Port1; Išmesti įrašus, kuriems baigėsi galiojimo laikas iš MAC adresų lentelės; Flood – viso tinklo užtvindymas tuo pačiu paketu. Panašus “broadcast” efektas, tačiau prigimtis kita: broadcast paketas specialiai skiriamas visiems tinklo mazgams

1. **IEEE 802 standartai:**

10 Mbps - IEEE802.3; 100 Mbps - IEEE802.3u; 1000 Mbps - IEEE802.3z; 10 Gbps- IEEE802.3ae; 40 ir 100 Gbps IEEE802.3bm-2015;



**Komutatoriai**: Nekeičia persiunčiamo paketo turinio, nei formato; Niekaip papildomai neįpakuoja: perduodama tiksli kopija; Yra skaidrus (nematomas) stotims: visos jos lieka viename LAN’e; Neturi jokių adresų; Tik medžio topologija – kilpos negalimos

Našumo charakteristikos: Filtravimo (filtering)/ Perdavimo (forwarding) sparta. Maksimalus pralaidumas (throughput) –visomis kryptimis vienu metu; Pilnas pralaidumas (Switching Capacity - iki Full wire speed).

Komutatoriais kompiuteriai jungiami į vieną tinklą, tinklai tarpusavyje jungiami maršrutizatoriais; Visi tarpusavyje sujungti komutatoriai ~ vienas didelis; Komutatorius iš esmės yra nematomas tinkle automatiškai veikiantis įrenginys, neturi jokių adresų

1. **Virtualūs lokalūs tinklai:**

“Tvarkinga” įmonė : Kompiuteriai sugrupuoti į potinklius pagal administracinį požymį. Kiekvienam padaliniui- atskiras komutatorius, kompiuteriai ;išdėstyti kompaktiškai kiekvieno komutatoriaus atžvilgiu. Maršrutizatoriuje nustatyti bendrų resursų pasiekimo apribojimai;

Sudaryti loginius tinklus:LAN grupuoja stotis geografiniu principu. Tikslas: grupuoti administraciniu principu; Trys problemos: 1. Atskirti į atskirus tinklus prie vieno komutatoriaus prijungtus skirtingus vartotojus; 2. Sujungti į tą patį tinklą prie skirtingų komutatorių prijungtus tuos pačius vartotojus; 3. Padaryti visiems pasiekiamus serverį ir maršrutizatorių;

VLAN pagal komutatoriaus jungtis: Paprasčiausias būdas sukurti virtualius tinklus, užtikrina didžiausią saugumą ; Įrenginiai priskiriami vienam ar kitam VLAN pagal tai, prie kurios jungties jie prijungti; Komutatorius virtualiai padalintas į kelis komutatorius, kurie tarpusavyje paketų neperduoda;

VLAN per kelis komutatorius: Jungiant VLANus per kelis komutatorius, reiktų atskirų sujungimų kiekvienam VLANui. 1. Neekonomiška, daug laidų ir papildomų jungčių sunaudojama; 2. Padidėja rizika sukurti kilpas; To reikia išvengti

1. **Optinių kabelių parametrai:**

Optinio signalo stiprumo pakitimo parametrai: Signalo silpimas, dB/km; Netiesiniai iškraipymai (harmonikos- λ1, λ2,...) ;Triukšmų įtaka (Signalas-trukšmas santykis –SNR)

Optinio signalo trukmės parametrai: Dispersija (impulso trukmės pakitimas ). Priežastis - signalo dedamųjų skirtingas vėlinimas: a) modinė dispersija (modų skirtingas vėlinimas), MHz∙km; b) chromatinė dispersija (Spektro dedamųjų skirtingas vėlinimas), ps/nm/km; c) modų poliarizacijos dispersija (Optinių gijų nesimetriškumo sąlygotas dedamųjų skirtingas vėlinimas ), ps/√km;

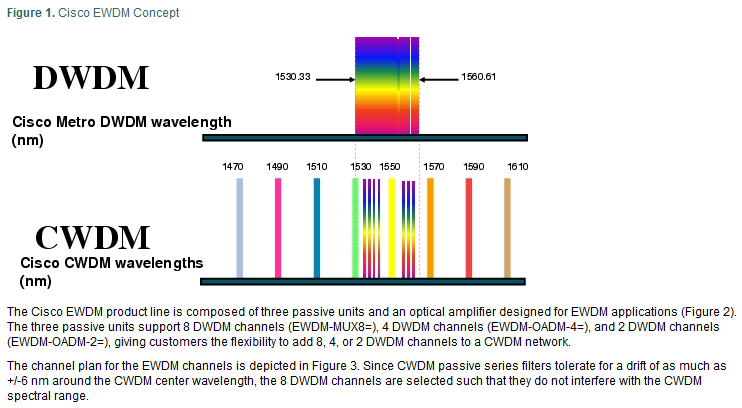
1. **CWDM sistema, DWDM sistema**

CWDM (angl. – Coarse Wavelenght Division multiplexing) – stambus bangų ilgių sutankinimas, yra būdas, kuris leidžia sudėti lazerio spindulių sudėtinius signalus į vieną skaidulą ir taip perduoti informaciją. CWDM technologijoje kanalų skaičius yra mažesnis nei DWDM, tačiau didesnis nei standartinėje WDM. CWDM sistemose atstumai tarp kanalų yra 20nm, kai tuo tarpu DWDM sistemose 0.4 nm. Tai sąlygoja žemesnę technologijos kainą. Tipinėje CWDM sistemoje lazeris spinduliuoja 8 nustatytus bangų ilgius: 1610 nm, 1590 nm, 1570 nm, 1550 nm, 1530 nm, 1510 nm, 1490 nm, and 1470 nm.

Kai naudojama CWDM sistemoje 18 kanalų, tuomet bangų ilgiai nusileidžia iki 1270 nm. CWDM sistemose leistinas lazerio nuokrypis yra ± 3 nm, kai tuo tarpu nuokrypis DWDM sistemose yra žymiai mažesnis. Dėl šios priežasties CWDM sistemos yra pigesnės nei DWDM ir išeikvoja mažiau energijos. Be to didžiausias įgyvendinamas atstumas tarp taškų, taikant CWDM technologiją yra mažesnis. CWDM sistema veikia analogiškai kaip DWDM, tik skirtumas tame, kad CWDM yra ne tokia galinga ir naudoja mažiau kanalų informacijos perdavimui.

Skaidulinėse – optinėse komunikacijose DWDM (angl. – Dense Wavelengh Division Multiplexing) – didelis bangos ilgių sutankinimas, yra technologija, kuri sutankina sudėtinius optinius nešlio signalus į vieną optinę skaidulą, panaudojant skirtingus lazerio šviesos bangos ilgius, tam kad perneštų skirtingus signalus. Tiesą sakant, viena skaidula yra paverčiama į sudėtines virtualias skaidulas. DWDM sistemos siūlo patrauklų, rentabilų būdą telekomunikacijų pramonei išplėsti tinklo juostos plotį. Ši nauja technologija leidžia operatoriams susidoroti su visada naujoms paslaugoms augančiais reikalavimais ir turi didesnį lankstumą šių paslaugų tiekime.

DWDM technologija yra naudojama trečiame optiniame lange, kuriame bangų ilgiai yra 1520 – 1620 nm, informacijos perdavimui dideliais atstumais. Šis bangų ilgių diapazonas buvo pasirinktas dėl mažo slopinimo ir galimybės stiprinti signalus optiniame lygyje be regeneratorių, kurie sąlygoja brangesnę eksploataciją. Šiandien naudojamos svarbesnės stiprinimo technologijos yra erbiu dengti stiprintuvai EDFA‘s (erbium droped fiber amplifiers) ir Ramano stiprintuvai. EDFA‘s stiprintuvai yra veiksmingi bangos ilgiams tarp 1525 – 1565 nm (C juosta) arba 1570 – 1610 nm (L juosta) (žiūr. 2 pav.). C ir L bangos ilgių juostų panaudojimas buvo standartizuotas ir patvirtintas Tarptautinės telekomunikacijų sąjungos telekomunikacijų standartizacijos sektoriaus (ITU – T). EDFA‘s stiprintuvai iš tikrųjų buvo sukurti pakeisti SONET/SDH optinis – elektrinis – optinis (OEO) regeneratorius, kuriuos EDFA‘s padarė praktiškai nebevartojamus. EDFA‘s gali sustiprinti bet kokius optinius signalus jų darbiniame diapazone.



1. **Debesų kompiuterijos ir paslaugų tipai –**

**Debesų kompiuterija** ([angl.](https://lt.wikipedia.org/wiki/Angl%C5%B3_kalba) *Cloud computing*) – paslaugos, kurioms pateikti reikalingas tik interneto ryšys. Debesį sudaro programos, kurių nereikia įdiegti į kompiuterį, [Web 2.0](https://lt.wikipedia.org/wiki/Web_2.0), asmeninių bylų (pvz., nuotraukų) bei katalogų talpinimas ir kitos technologinės tendencijos.

Debesys – tai serveriai (kompiuteriai) pastoviai prijungti prie interneto į kuriuos vartotojai už tam tikrą mokestį (o kartais ir nemokamai) gali įsikelti savo norimus failus ir vėliau juos atsidaryti ar parsisiųsti iš serverio naudodami bet kurį įrenginį prijungtą prie interneto (kompiuterį, telefoną, planšetę) suvedę savo prisijungimo duomenis.

Paslaugos užsakymo procesas automatizuotas; Platus paslaugų pasiekiamumas įprastais tinklais; Abstraktūs resursų telkiniai, palaikantys daugelį įzoliuotų klientų; Resursai pagal poreikį nesudėtingai plečiami ar sumažinami; Panaudotų paslaugų ir resursų apskaitomumas;

**Serviso(Paslaugų) modeliai**

Software as a service (SaaS) - Vartotojas interneto pagalba gali naudotis konkrečiomis programomis (pvz., elektroniniu paštu, CRM, ERP ir kitomis).

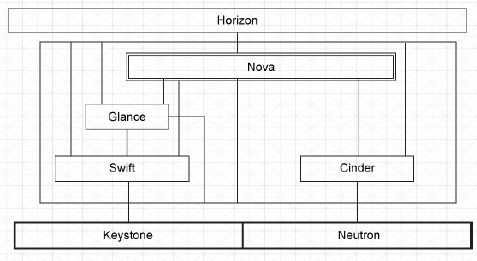
Platform as a service (PaaS) - vartotojui suteikia ne tik infrastruktūrinius išteklius, bet ir operacinę sistemą kartu su programomis, programavimo kalbomis, bibliotekomis ir kitais įrankiais bei paslaugomis.

Infrastructure as a service (IaaS) - leidžia vartotojams naudotis serverių, duomenų saugyklų ištekliais bei tinklo; įranga pagal poreikį.

**Virtualizacijos būdai:** Skaičiavimo resursų virtualizacija; Duomenų saugyklos virtualizacija; Tinklo lygio virtualizacija

1. **Openstack architektūra:**

Atvirojo kodo debesų kompiuterijos paslaugų valdymo sistema. Openstack – tai labiau platforma, o ne naudojimui paruoštas produktas. Visiškai modulinė, nestipriai susietų (loose coupled) elementų sistema, kurios pagalba įmonės gali sukonstruoti savo debesų kompiuterijos valdymo sistemas.



Keystone: Autentikacijos ir teisių valdymo servisas. Visos API užklausos tarp komponentų yra vykdomo per Keystone, taip užtikrinant prieigos teisių valdymą

Swift(objektų saugykla):Decentralizuota; Automatiškai atsistatanti trikio atveju; Plečiama horizontaliai iki daugelio petabaitų; Aukšto našumo, gaunamo iš paskirstytos architektūros; Gali būti sukurta naudojant nebrangią aparatūrinę įrangą;

Glance: Virtualių mašinų atvaizdų saugykla. Atvaizdai gali būti saugomi tiesiogiai jame, tačiau dažniau būna realizuota kaip nuorodos į objektinę saugyklą.

Cinder: Blokinė saugykla. Teikia tokias paslaugas: 1.Virtualių diskų valdymas; 2. Momentinių atvaizdų (snapshot) valdymas; 3.Virtualių diskų prijungimas ar atjungimas nuo virtualių serverių; 4.Virtualių diskų klonavimas; 5.Virtualių diskų sukūrimas iš momentinių atvaizdų; 6.Virtualių diskų kopijavimas į atvaizdus (images) ir atvaizdų kopijavimas į virtualius diskus; 7.Gali būti realizuota kaip interfeisas į blokinę saugyklą

Nova: Nova-api: skaičiavimo resursų api interfeisas; Nova-compute: valdo atskirą hipervizorių; Nova-scheduler: skirsto užduotis tarp skirtingų hipervisorių

Neutron: Tinklo servisas, palaikantis daugelį įskiepių, galinčių dirbti su skirtinga tinklo įranga;

Kiti komponentai: Horizon - valdymo aplinka realizuota web technologijomis,Užduočių eilė; Duomenų bazė

1. **IP paketų perdavimas:**

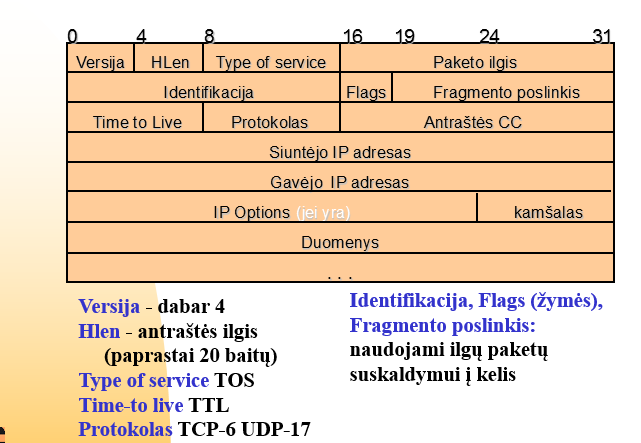
Komutatoriai sujungia kompiuterius į vieną LAN. Maršrutizatoriai sujungia tinklus ir turi po atskirą jungtį kiekvienam LAN

apibūdinamas tokiomis charakteristikomis: 1. nesusijęs perdavimas – kiekvienas paketas perduodamas tinklu nepriklausomai nuo kitų;2. negarantuotas perdavimas – paketas gali būti naikinamas nesiunčiant jokio pranešimo siuntėjo įrenginiui; 3. nepatikimas perdavimas – paketai gali dingti, būti sugadinti, pakartoti ar sumaišyti.

IP paketas perduodant gali būti suskaidytas į dalis (fragmentus). Fragmentai atsiranda, kai IP paketas netelpa į vieną kanalo sluoksnio kadrą. Vieną kartą suskaidyti paketai toliau keliauja kaip atskiri IP paketai. Fragmentus į pradinį paketą surenka gavėjo įranga. Tam reikalingi antroje antraštės eilutėje parodyti laukai.

Kaip surasti kuris kompiuteris turi reikiamą IP adresą? 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 [laikinai] nebereiks,

**IP paketo formatas:** IP paketo antraštė turi visą informaciją, kuri reikalinga pristatyti paketą į gavėjo kompiuterį: 1. Gavėjo IP adresą, 2. TTL, 3. TOS, 4. Siuntėjo adresą, 5. Fragmento identifikaciją; Maršrutizatorius analizuoja kiekvieno paketo IP antraštę ir jį nukreipia gavėjo kryptimi.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.



1. **Maršrutų lentelės:**

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

* **Pagrindiniai stulpeliai:**
  + 1. **Paskirties tinklas**
    2. **Sekantis maršutizatorius**
    3. **Kelio vertė (atstumas)**

Informacija apie siuntimo kryptį saugoma maršrutų lentelėje: Išvardinami žinomų tinklų adresai; Kiekvienam paskirties tinklui nurodomas sekančio pakeliui maršrutizatoriaus IP adresas (Next Hop); Turi būti keičiama keičiantis tinklo topologijai; Sudarymas: Statinis, kai kiekvienas pasiekiamas tinklas ir sekančio šuolio adresas įvedamas rankomis, administratoriaus; (**netinka dideliam tinklui,**

* **nėra automatinio maršrutų parinkimo**

**Nutrūkus ryšiui nuo sąsajos 10.0.13.2, dalis tinklų taps nepasiekiami**)

Dinaminis, kai maršrutizatoriai patys keičiasi informacija apie pasiekiamus tinklus ir ryšio linijų būsenas.

**Maršrutizavimo protokolai aprašo:** 1.Kaip pasiųsti maršrutų pasikeitimus, 2. marštutų pasikeitimus apibūdinačią informaciją ir jos formatus, 3. kada siųsti maršrutų pasikeitimus, 4. kaip surasti, kam turi būti siunčiami maršrutų pasikeitimai.

**Atstumų vektoriaus tipo maršrutizavimo protokolai:** Atstumų vektoriaus tipo maršrutizavimo protokolai remiasi tokiais principais: 1. maršrutizatoriai transliuoja savo maršrutų lenteles kaimynams kas tam tikrą laiko intervalą, 2. maršruto ilgis skaičiuojamas iteratyviai: kai X praneša maršrutą α kaimynui Y, Y maršruto α ilgį padidina atstumu (x,Y), 3. Jei gautas maršruto α ilgis geresnis už kitą žinomą, tai įsimenamas naujas maršrutas; 4. sekančio šuolio maršrutizatoriumi maršrutui tampa jo pranešėjas (X), 5. pasikeitimai maršrutų lentelėse sklinda bangos principu.

**Ryšių būsenų tipo marštutizavimo protokolai:** Ryšių būsenų tipo marštutizavimo protokolai remiasi tokiais principais: 1. kiekvienas marštutizatorius žino visą tinklo topologiją ir ryšių būsenas, 2. maršrutizatorius savo ryšių pasikeitimus siunčia multicast būdu, 3. kiekvienas maršrutizatorius maršrutus skaičiuoja pats pagal trumpiausio kelio grafe radimo algoritmą.

1. **Interneto struktūra: autonominės sistemos:**

tai centralizuotai ir nepriklausomai nuo kitų administruojama interneto tinklų dalis, turinti bendras maršrutizavimo taisykles: 1. IP numerių skirstymo Sistema; 2. Maršrutizavimo taisyklės viduje AS; 3. Duomenų srautų valdymas; 4. Tinklų skelbimas į kaimynines AS; 5. 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. Kiekvienos AS valdymo savarankiškumas.

AS1 tinklai galės naudotis keliais per AS2 tik tokiu atveju jei: - AS2 kraštinis maršrutizatizatorius skelbs kelius per AS2 į AS1; - AS1 kraštinis maršrutizatorius tuos skelbimus priims

Taip sumažinama apsikeitimų maršrutų lentelėmis apimtis: tik kraštinis vienos AS marštutizatorius keičiasi sutartais duomenimis su kraštiniu kitos AS marštutizatoriumi. Vidiniams maršrutizatoriams perduodama minimali reikalinga gautos informacijos dalis

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)

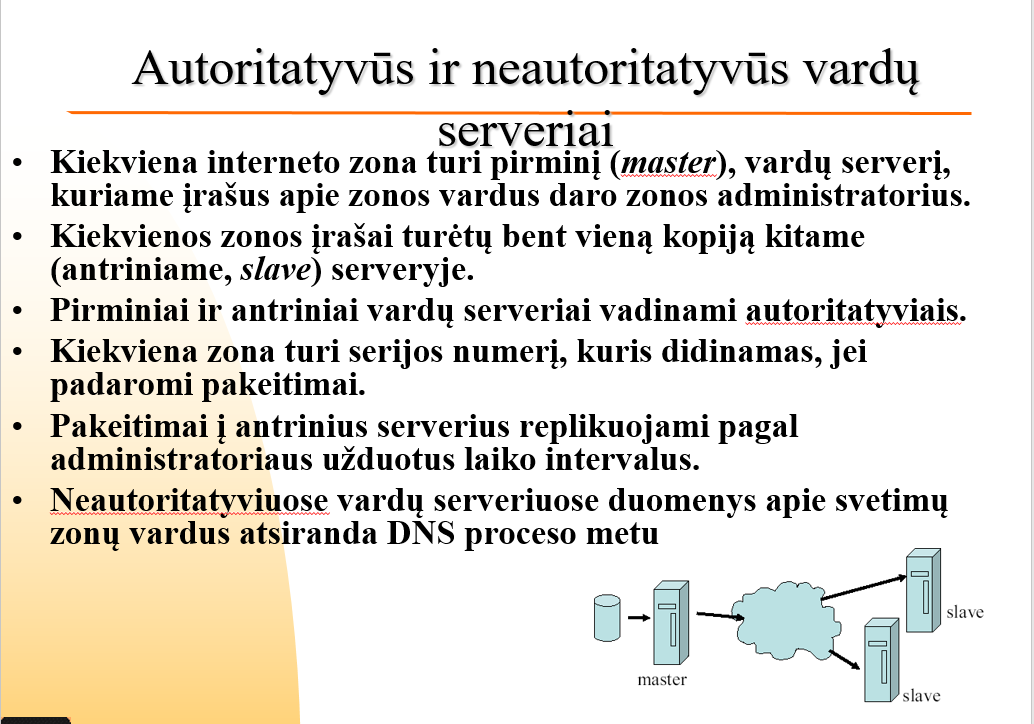
1. **DHCP funkcijos:**

Dynamic Host Configuration Protocol (DHCP), RFC 2131,Paskiria laisvą IP adresą iš turimo segmento [laikinam naudojimui]; DHCP klientas gali gauti visus konfigūravimo parametrus ir užkrauti OS iš tinklo;

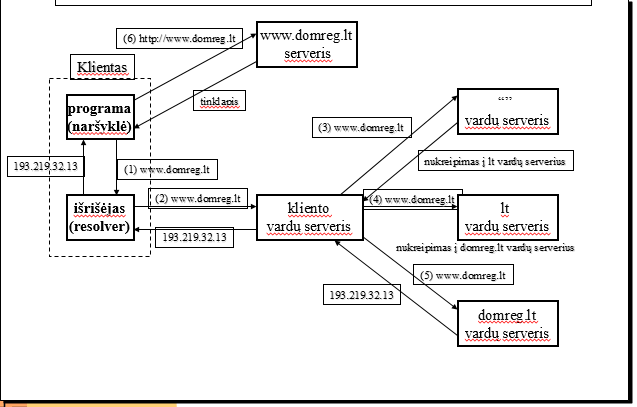
**veikimo principai**: 1. surasti DHCP serverį [-ius], gauti pasiūlymus. 2.-pasirinkti, pranešti kas pasirinkta, gauti papildomus konfigūravimo parametrus, jei reikia

**DNS funkcijos :** 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 “interneto vardas “ -> “IP adresas” nebūtinai turi būti vienareikšmė. Pasinaudojant tuo DNS gali atlikti papildomas funkcijas.

DNS palaiko dvi užklausų rūšis: 1. rekursyvias: užklausą gavęs ir nežinantis atsakymo serveris perduoda originalią užklausą kitam (savo vardu); 2.iteratyvias: užklausą gavęs ir nežinantis atsakymo serveris gražina tik tinkamesnio serverio adresą “klausk pats”



**ir veikimo principai:**



1. **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;

**Transporto sluoksnio funkcijos-> priemonės:** 1.Keistis duomenimis tarp taikomųjų procesų -> prievadai (port); 2.Taisyti perdavimo klaidas -> patvirtinimai (ACK); 3. Valdyti duomenų siuntimo spartą -> siuntimo langas

**Klaidų 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. 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 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.

**spartos reguliavimas :** 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. Tas padeda tinkle išvengti lavininio perkrovų didėjimo, kuris būtų, jei siuntėjai pradėjus jų paketus naikinti ir toliau nemažintų siuntimo spartos. Jei nesulaukiama išsiustų duomenų gavimo patvirtinimo, pakartotinai siunčiama mažiau duomenų -sparta mažėja, perkrova ar grūstis kažkuriame tinklo mazge išnyksta. Jei kelias iš eilės porcijas pasiuntėme sėkmingai, galime didinti siuntimo langą.

1. **TCP ir UDP protokolai, savybės ir elementai**

Transporto sluoksnio protokolai:

|  |  |  |  |
| --- | --- | --- | --- |
| **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** | |
| **Didelių duomenų kiekių ir dokumentų patikimam perdavimui** | **Kritiniams laiko atžvilgiu taikymams,**  **užklausoms, kurios gali būti kartojamos** | |

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 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

**UDP Paketo antraštė (8 baitai):**

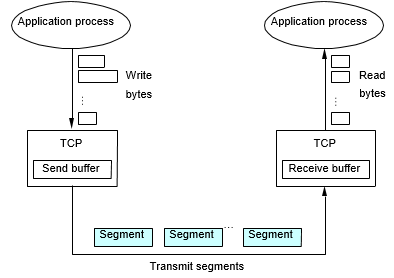


Jei nurodytam paskirties portui nėra aktyvaus proceso, paketas naikinamas; Jei taikomasis procesas nespėja apdoroti į portą ateinančių paketų, netelpantys į buferį paketai naikinami; UDP siuntėjas pats parenka spartą ir jos nekaitalioja nei pagal tinklo sąlygas, nei pagal gavėją. Siunčiama netgi ir tada, jei gavėjas iš viso nepriima (pvz ta programa ar portas gavėjo kompiuteryje neaktyvus)

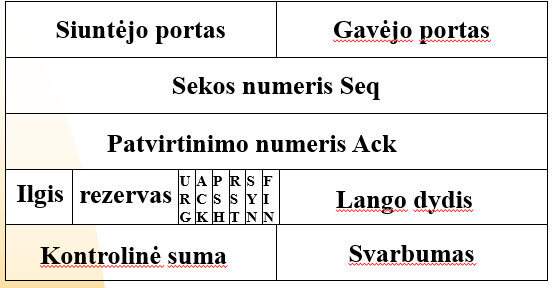
**TCP savybės:**

Gali aptarnauti kelis sujungimus tuo pačiu portu, tam reikia aiškių sujungimo įkūrimo ir užbaigimo procedūrų; Potencialiai skirtingi RTT, tam reikia adaptyvaus laukimo laiko nustatymo mechanizmo; Potencialiai didelis vėlinimas ir didelė vėlinimo sklaida, tam reikia sugebėti atpažinti vėluojančius paketus; Potencialiai skirtingi gavėjo talpumai, tam reikia reguliuoti siuntimą pagal gavėjo galimybes priimti duomenis; Potencialiai skirtingi tinklo pralaidumai pagal gavėjus/pagal laiką, tam reikia reaguoti į perkrovas tinkle;

Sujungimas įkuriamas tarp siuntėjo ir gavėjo visam numatytų duomenų perdavimo laikui; Patikimas perdavimas: gavėjas galų gale gauna tikslią išsiustų duomenų kopiją; Srauto valdymas: kad neperpildyti gavėjo buferių, gavėjas gali pranešti siuntėjui apie likusios vietos apimtį



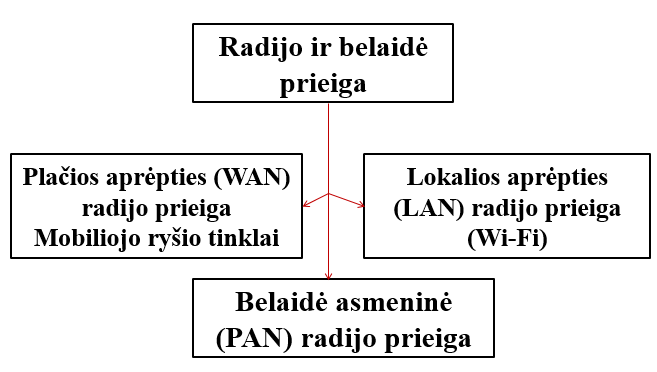
**TCP antraštės formatas (20 baitų)**



**Tinklapio užklausa per TCP**

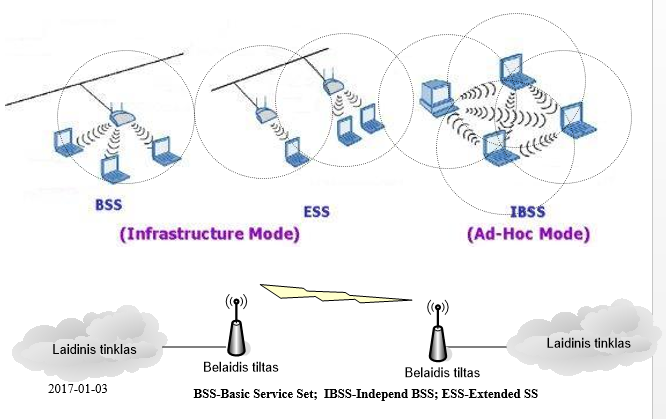
Užmezgant ryšį siuntėjas kreipiasi į gavėją, nurodydamas į kokį portą kreipiasi, kokį portą skiria atsakymams priimti, kokį siūlo lango dydį. Gavėjas atidaro prašomą portą priėmimui ir patvirtina, kad pasiruošęs. Gali sumažinti langą, jei trūksta buferio. Tada galima pradėti keistis duomenimis.

1. **Belaidės prieigos tinklai (WLAN):**



**Prieigos taškas (access point)** - Belaidei prieigai sudaryti būtinas prieigos taškas; Dažnai zonos persidengia; Zonai atskirti būtinas zonos SSID (Service Set Identifier) - unikalus 32 simbolių identifikatorius siunčiamas kiekvieno paketo antraštėje Dvi antenos sumažina atspindžių įtaką priėmimo metu.

**Belaidžių tinklų architektūros**:



Infrastructure būdas– su fiksuotais prieigos punktais **:** Stotis ieško AP visuose kanaluose. Persijungimas galimas pagal signalo lygį ir pagal apkrovas. Dažniausiai naudojama autentifikacija

Ad Hoc tinklo ypatybė – nėra prieigos punktų : Mobilūs Ad Hoc tinklai (*angl. Mobile Ad Hoc networks*) yra judančių įrenginių rinkinys, sujungtų tarpusavyje belaidžio ryšio jungtimis.

**Galima išskirti dvi Ad Hoc tinklų veikimo rūšis:**

* Taškas-taškas (*angl.* ***Point-to-point***) Ad Hoc – kai tinklo įrenginiai komunikuoja su gretimais įrenginiais, t.y. kurie yra jų belaidžio ryšio aprėpties zonoje.
* Daugelio žingsnių (*angl.* ***Multi-hop***) Ad Hoc – kai tinklo įrenginiai gali komunikuoti kitų tarpinių mazgų pagalba, pvz. kai jie yra toli vienas nuo kito ir negali bendrauti tiesiogiai. Taigi įrenginiai Ad Hoc tinkle vienu metu turi būti ir **informacijos siuntėjai/gavėjai** (tinklo resursų vartotojai), ir **maršrutizatoriai**, persiunčiantys kitų įrenginių paketų srautus. Tokiu atveju reikalingi maršrutų parinkimo protokolai optimalių maršrutų paieškai. Įrenginiai gali būti statiški arba dinamiški – laisvai, atsitiktinai arba apibrėžtai judėti skirtingais greičiais ir kryptimis.

Pavyzdžiai:

* Įmonės, namų ir asmeniniai tinklai
* Karo lauko komunikacijoms – kariniai daliniai suformuoja judantį tinklą
* Prieiga prie Interneto nuošaliose vietovėse
* Intelektualios transporto sistemos
* Viešasis saugumas (policija, gaisrinė, greitoji pagalba)
* Kritiškoms situacijoms – kai jokia komunikacinė infrastruktūra neegzistuoja
* Sensoriniai tinklai

ir visa eilė kitų...

1. **Belaidžių tinklų sauga:**

Atvira autentifikacija: 1. Klientas siunčia paketą su įrenginio (AP) SSID; 2.AP išsiunčia autentifikavimo atsakymo (patvirtinimo) paketą, jei gautasis SSID atitinka AP SSID.

Bendrojo rakto autentifikacija: Tiek AP, tiek klientas turi naudoti tą patį iš anksto nustatytą (bendrąjį) raktą . 1. Klientas siunčia autentifikavimo užklausą. 2. Iš AP gauna nešifruoto teksto užklausą. 3. Klientas siunčia šifruoto teksto atsakymą. 4. AP išsiunčia autentifikacijos patvirtinimą.

WEP protokolas: Pagrindiniai principai: 1. Konfidencialumas; 2. Prieinamumas; 3. Vientisumas; Naudojami saugumo mechanizmai: 1. RC4 šifravimo algoritmas ir XOR operacija; 2. Prieigos taškas gali turėti 4 bendro naudojimo raktus (40 arba 104 bitų ilgio); 3. Naudojamas iniciacijos vektorius (IV): a) Prie rakto pridedamas 24 bitų iniciacijos vektorius; b) Iniciacijos vektoriaus pagalba sukuriamas kintantis šifravimo raktas;

WEP (*Wired Equivalent Privacy*) standartas buvo sukurtas norint belaidžius tinklus padaryti patikimesnius ir saugesnius – tokius kaip laidiniai tinklai. Pagrindiniai WEP principai: apsaugoti tinklą nuo slapto duomenų nuskaitymo (konfidencialumas), leisti autorizuotą prisijungimą prie tinklo (prieinamumas) ir apsaugoti belaides komunikacijas nuo suklastojimo (vientisumas). Netrukus po to, kai buvo išleistas WEP standartas, pastebėta saugumo spragų ir šis protokolas imtas laikyti nesaugiu.

WPA protokolas: Du autentifikavimo metodai:1. EAP (Extensible Authentication Protocol) – autentifikavimas 802.1x standartu (dažniausiai naudojamas įmonėse); 2. PSK (Pre-Shared Key) – iš anksto numatytas raktas: 256 bitų ilgio skaičius arba slaptažodis nuo 8 iki 63 simbolių (dažniausiai naudojamas namuose ir mažose įmonėse); TKIP (Temporal Key Integrity Protocol) realizacija ir buvo pavadinta WPA.

802.1x standartas: IEEE 802.1x sukurtas autentifikavimui pagal prievadus visiems IEEE 802 tinklams. Siūlo ne šifravimą, o skirtingus metodus: EAP naudojamas autentifikavimui ir šifravimui belaidžiuose tinkluose; Autentifikavime dalyvauja trys objektai: 1. autentifikavimo serveris (RADIUS serveris); 2. autentifikatorius (AP ar maršrutizatorius); 3. prašytojas (klientas);

Belaidžių tinklų atakos ir pavojai: Slaptas klausymasis; SSID nustatymas; Neautorizuotas prisijungimas; MAC adresų filtravimas; WEP duomenų šifravimas; Paslaugų blokavimo atakos (DoS – Denial-of-Service); Suklastotas prieigos taškas; “Įsiterpusio žmogaus” (Man-in-the-Middle) ataka

1. **Judriojo ryšio technologijos:**

NULINĖS KARTOS TECHNOLOGIJOS (0G–0.5G): 0G kartos mobilus ryšys buto taikomas automobiliams.

PIRMOS KARTOS TECHNOLOGIJOS(1G): 1G wireless networks used analog radio signals. Through 1G, a voice call gets modulated to a higher frequency of about 150MHz and up as it is transmitted between radio towers.

ANTROS KARTOS TECHNOLOGIJOS(2G - 2.75G): 2.5G – GPRS (General Packet Radio Service)-Duomemims perduoti naudoja skaitmeninio balso kanalus; 2.75 – EDGE (Enhanced Data rates for GSM Evolution)- Balsui ir duomenims perduoti (IMT-2000, UMTS-2000)

TREČIOS KARTOS TECHNOLOGIJOS (3G – 3.75G)- Balsui ir duomenims perduoti (IMT-2000, UMTS-2000)

KETVIRTOS KARTOS TECHNOLOGIJOS–4G -Taikomas pirmiausiai duomenims perduoti

PENKTOS KARTOS TECHNOLOGIJOS– 5G **–** pasižymi didele sparta.