KOMPIUTERIŲ TINKLAI

10 paskaita

Taikomojo lygmens protokolai

Globalūs tinklai (kartojimas)

- Kas yra globalūs tinklai?
- Kuo skiriasi kanalų komutacija nuo paketų komutacijos?
- Kuo pasižymi skirtinės linijos?
- Kam naudojamos DSL linijos?
- Kuo pasižymi ATM technologija?

OSI taikomasis lygmuo

OSI taikomasis lygmuo atsakingas už komunikacijas tarp programų (procesų).

Šiam lygiui taip pat priklauso elektroninis paštas, naršymas web tinkle, užduočių įvedimas į nutolusius kompiuterius, failų siuntimas, tinklo valdymas, laiko sinchronizavimas ir t.t.

Taikomajame lygmenyje veikia daug protokolų: HTTP, Telnet, FTP, ICMP, SMTP, POP3, DNS, SNMP, NTP ir t.t.

Elektroninis paštas

Elektroninis paštas egzistuoja jau virš 30 metų. Jis pradėjo veikti ARPANET tinkle ir laiškas buvo siunčiamas kaip tekstinis failas.

Elektroninio pašto veikimas paremtas RFC 822 specifikacija.

Paprastai e-pašto sistemos sudarytos iš dviejų posistemių:

1. Vartotojo agentai (programos), kurie leidžia skaityti ir siųsti paštą
2. Pranešimų perdavimo agentai, perduodantys pranešimus adresatui.

Elektroninis paštas

RFC 822 antraštės laukai, susiję su pranešimo perdavimu

Antraštė	Reikšmė
To:	Pirminių gavėjų adresai
Cc:	Antrinių gavėjų adresai
From:	Asmuo ar asmenys, kurie sukūrė pranešimą
Bcc:	Adresai paslėptųjų, “kalkinių” kopijų
Sender:	Tikrojo siuntėjo el. pašto adresas
Received:	Šia eilutę prideda kiekvienas perdavimo agentas visame maršrute
Return-Path:	Gali būti panaudotas kelio atgal pas siuntėją nuorodai

MIME

MIME (Multipurpose Internet Mail Extensions).

RFC 822 sukūrimo metu tiko tik tekstiniams pranešimams, naudojantiems ASCII kodavimą. Dėl to atsirado problemų siunčiant pranešimus kalbomis, naudojančiomis ne lotynišką abėcėlę, ar iš viso ne raides. Taip pat buvo problemų, siunčiant audio ir video failus.

Sprendimas pasiūlytas RFC 1341 ir RFC 1521 ir pavadintas MIME.

Pagrindinė idėja - lieka galioti RFC 822, tačiau yra pranešimo kūnas struktūrizuojamas ir apibrėžiamos netekstinių pranešimų kodavimo taisyklės. Visi MIME pranešimai gali būti perduodami, naudojant egzistuojančias pašto programas ir protokolus.

MIME

MIME apibrėžia penkias naujas pranešimo antraštes.

Antraštė	Reikšmė
MIME-Version:	Identifikuoja MIME versiją
Content-Description:	Eilutė, nusakanti pranešimo turinį
Content-Id:	Unikalus identifikatorius
Content-Transfer-Encoding:	Pranešimo kodavimo būdas
Content-Type:	Pranešimo tipas

Content-Type: *Text/richtext, Image, Audio, Video, Application, Postscript, Message, Multipart*

SMTP

SMTP (Simple Mail Transfer Protocol). 25 prievadas.

Skirtas nusiųsti e-laišką iš kliento programos į pašto serverį.

SMTP protokolas yra apibrėžtas RFC 821 …RFC 5321.

Algoritmas

Jeigu serveris pasiruošęs priimti paštą, klientas praneša, kas ir kam siunčia paštą. Jeigu toks gavėjas egzistuoja, serveris leidžia klientui siųsti pranešimą. Pranešimas išsiunčiamas, serveris patvirtina, kad pranešimas gautas. Kai įvyksta pilnas pasikeitimas paštu iš abiejų pusių, susijungimas atlaisvinamas.

SMTP

SMTP yra į sujungimą orientuotas tekstinis (text-based) protokolas. Komunikacija tarp kliento ir serverio atliekama siunčiant komandas ir duomenis (klientas siunčia, serveris atsako) naudojant TCP.

SMTP transakciją sudaro 3 užklausimų/atsakymų seka.

- **MAIL** komanda nurodomas siuntėjo adresas, t.y. kam grąžinti laišką, jei jo nepavyktų išsiųsti.
- **RCPT** komanda nurodomas gavėjo adresas. Komanda gali būti naudojama daug kartų, jei yra daug gavėjų.
- **DATA** komanda, siunčianti laiško tekstą/turinį (content). Ją sudaro laiško teksto antraštė ir tekstas (body), atskirtas tuščia eilute. Serveris atsako du kartus t.y. patvirtinimas, kad gali priimti tekstą ir patvirtinimas, kad tekstas priimtas/atmestas.

POP3

POP3 (Post Office Protocol v.3, 110 prievadas) protokolas naudojamas naudojamas elektroninių laiškų gavimui iš serverio ir jo išsaugojimui vartotojo kompiuteryje.

Paprastai yra naudojamas kartu su SMTP.

POP3 aprašytas RFC 1225, 1939.

POP3 turi specialias komandas prisijungti prie pašto serverio (login), atsijungti (logoff), paimti pranešimus, ištrinti pranešimus.

POP3 palaiko šifravimą naudojant:

- **TLS** (transport layer security)
- **SSL** (secure socket layer), 995 prievadas

POP3 seansas

POP3 protokole numatytos 3 seanso būsenos:

1. **Autorizacija**
   Klientas atlieka autorizacijos procedūrą.

2. **Transakcija**
   Klientas gauna informacija apie elektroninės pašto dėžutės būseną, priima ir pašalina paštą.

3. **Atnaujinimas**
   Serveris ištrina pasirinktus laiškus ir nutraukia susijungimą.

IMAP

Žymiai sudėtingesnis e-laiškų pristatymo protokolas yra IMAP (Interactive Mail Access Protocol), aprašytas RFC 1064, 3501. Prievado numeris 143.

IMAP leidžia ne tik pasiekti laiškus pašto serveryje, bet ir juos tvarkyti.

Visi laiškai saugomi pašto serveryje kaip reliacinė duomenų bazė, prie kurios įrašų galima prieiti, naudojant įvairius požymius.

IMAP ypatingai patogus vartotojams, kurie dirba su keletu kompiuterių (pvz. namuose ir darbe), nes nereikia e-pašto laiškų kopijuoti į kiekvieną iš jų.

IMAP

Naudojant POP protokolą, klientas trumpam prisijungia prie pašto serverio ir parsisiunčia laiškus. IMAP klientas lieka prisijungęs prie pašto serverio tol, kol aktyvi klientinė programa.

IMAP protokolas leidžia prie tos pačios pašto dėžės vienu metu jungtis keletui klientų ir detektuoja pakeitimus, kuriuos atlieka kiekvienas iš klientų.

HTTP

HTTP (Hypertext Transfer Protocol) – tai protokolas, skirtas sujungti paskirstytas informacines sistemas hypertekstininių nuorodų pagalba.

HTTP kūrimą koordinavo WWW (*World Wide Web)* konsorciumas ir IETF (*Internet Engineering Task Force)* darbo grupė, vėliau pateikusios RFC 2616, kuris apibrėžė HTTP/1.1 (plačiausiai naudojamą HTTP versiją).

HTTP yra **užklausimo - atsakymo** protokolas, jungiantis klientą ir serverį. HTTP klientas, pvz. naršyklė inicijuoja užklausimą prisijungdamas prie nutolusio kompiuterio prievado (pagal nutylėjimą naudojamas 80).

HTTP

HTTP serveris klausosi 80 prievado, laukdamas kliento užklausos, pavyzdžiui, „GET / HTTP/1.1“ (užklausiančios pradinio serverio puslapio), bei susijusio MIME informacinio pranešimo, nusakančio užklausos prigimtį.

Gavęs užklausą, serveris atgal siunčia atsakymo eilutę („200 OK“ sėkmės atveju), ir susijusį pranešimą, kuris dažniausiai yra HTML puslapis.

HTTPS yra saugi HTTP versija, naudojanti SSL/TLS saugos metodus. Šis protokolas įprastai naudoja 443 TCP prievadą.

HTTP užklausos

GET – dažniausia užklausa, reikalaujanti tam tikro resurso duotu URL adresu.

POST – panašu į *GET*, bet siunčiama papildoma informacija, paprastai raktų ir reikšmių poros, nusakančios HTML formos laukų reikšmes.

PUT – naudojama failų įkėlimui į serverį.

DELETE – naudojama trynimui.

HEAD – panaši į *GET*, tačiau reikalaujama tik atsakymo antraštės, o pats atsakymo dokumentas nelaukiamas.

TRACE – grąžina gautą užklausą, gali būti naudojama tikrinimui, kokių papildomų meta - duomenų prideda tarpiniai serveriai.

CONNECT – retai palaikoma.

HTTP užklausos

HTTP kliento užklausos pavyzdys:

```
GET / HTTP/1.1
Host: www.google.com
```

Serverio atsakymas

```
HTTP/1.1 200 OK
Content-Length: 3059
Server: GWS/2.0 Date: Sat, 12 Jan 2013 14:49:31 GMT
Content-Type: text/html
Cache-control: private
Set-Cookie:
PREF=ID=73d4aef52e57bae9:TM=1042253044:LM=1042253044
:S=SMCc_HRPCQiqy X9j; expires=Sun, 17-Jan-2038
19:14:07 GMT; path=/; domain=.google.com
Connection: keep-alive
```

FTP protokolas

FTP (File Transfer Protocol) apibrėžia failų perdavimo procedūras tarp dviejų kompiuterių. (21 prievadas).

FTP išsiskiria tuo, kad naudoja du loginius sujungimus tarp kompiuterių. Vienas sujungimas yra reikalingas sujungimui su kitu kompiuteriu ir naudoja Telnet protokolą. Kitas sujungimas yra naudojamas duomenų perdavimui.

FTP perdavimas gali vykti **tekstiniu** arba **binariniu** pavidalu.

FTP naudoja daug vidinių komandų: vartotojo identifikacijai, vykstančio duomenų perdavimo valdymui. Taip pat yra visa serija atsakymų (reakcijų) į komandas.

FTP sesija

FTP sesiją suformuojama tokiais etapais:

Prisijungimas prie nutolusio kompiuterio. Ši operacija turi būti įvykdyta prieš pradedant duomenų perdavimą. Turi būti įvestas teisingas vardas ir slaptažodis. Jei FTP serveris leidžia naudotis tam tikrais resursais visiems vartotojams, tuomet pakanka vietoj vardo įvesti “anonymous”, o vietoj slaptažodžio savo el. pašto adresą.

Katalogo pasirinkimas.

Failo pasirinkimas. Nurodoma, kokį failą reikia perduoti. Dažniausiai yra naudojamos GET ir PUT komandos.

FTP sesija

Perdavimo režimo nustatymas. Nurodoma, kaip turi būti perduodami failai. Tam skirta keletas komandų.

- **Block**. Šis parametras reiškia, kad failas bus perduodamas blokais.
- **Stream**. Duomenys siunčiami kaip bitų srautas.
- **TYPE**. Ši moda naudojama su IMAGE ir ASCII parametrais.
- **ASCII**. Šis parametras naudojamas pagal nutylėjimą. Naudojama, siunčiant tekstinius failus.
- **IMAGE**. Perduodamas bitų, supakuotų į 8 bitų baitus, srautas. Dažniausiai naudojamas perduodant dvejetainius failus.

FTP sesija

Duomenų perdavimo pradžia. Šis žingsnis gali prasidėti su daugeliu FTP komandų (GET, PUT ir t.t.).

Duomenų perdavimo pabaiga. Tai galima padaryti, įvedus QUIT arba BYE komandą, kuri panaikina sujungimą su nutolusiu kompiuteriu.

Galima pasinaudoti komanda CLOSE, kuri nutraukia duomenų perdavimą, tačiau nepanaikina sujungimo. FTP lieka aktyvus ir kitas vartotojas gali pradėti naują FTP sesiją, pasinaudodamas OPEN komanda.

ICMP

ICMP (Internet Control Message Protocol) – tai protokolas, skirtas informuoti siuntėją apie „nelaimingą atsitikimą“ įvykusį su siunčiamu paketu.

ICMP apibrėžtas RFC 792.

IP protokolas nesirūpina paketų pristatymu ir klaidų taisymu, todėl ICMP seka paketo kelią ir jei paketą maršrutizatorius atmeta, apie tai informuojamas siuntėjas naudojant ICMP protokolą.

ICMP

IP paketo atmetimo priežastys:

- Baigėsi paketo gyvavimo laikas.
- Maršrutizatoriaus maršrutizavimo lentelėje nėra įrašo apie kelią iki gavėjo.
- IP paketo antraštės lauko „kontrolinė suma“ reikšmė nesutampa su apskaičiuota.
- Perpildytas maršrutizatoriaus buferis.

ICMP

ICMP protokolas yra naudojamas ir tinklo monitoringui.

Ping, tracert, traceroute komandos naudoja ICMP pranešimus.

ICMP pranešimų pagalba galima:

- Sužinoti IP paketų maršrutą
- Įvertinti tinklo pralaidumą ir stabilumą
- Nustatyti paketų keliavimo laiką iki gavėjo
- Nustatyti gavėjo IP adresą

ICMP

ICMP pranešimai būna dviejų tipų:

- Diagnostiniai pranešimai apie klaidas
- Informaciniai pranešimai (užklausa/atsakymas)

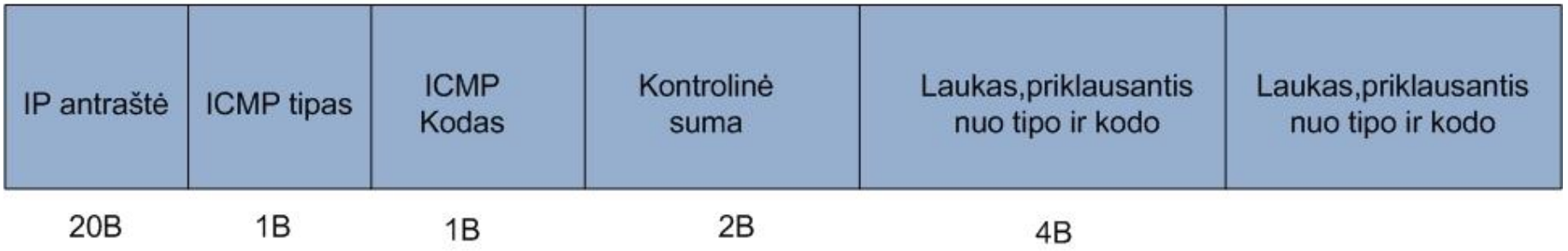
ICMP pranešimas inkapsuliuojamas IP paketo duomenų lauke. ICMP pranešimo antraštės ilgis sudaro 8 baitus.

Iš antraštėje pateiktos informacijos galima nustatyti problemą dėl kurios IP paketas nepasiekė gavėjo.

ICMP

ICMP pranešimo struktūra

ICMP pranešimas



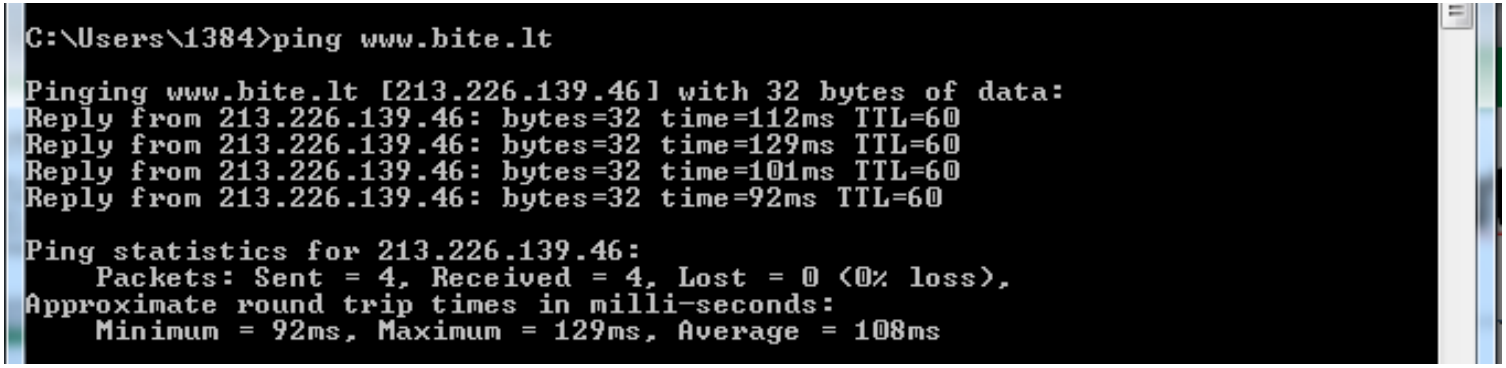
Tipas – pranešimo tipo kodas (0 – echo atsakymas, 3 – mazgas nepasiekiamas, 8 – echo užklausa, 11-baigėsi gyvavimo laikas, 12 – paketo parametrų problema ir t.t.)
Kodas – smulkesnis pranešimo tipo apibūdinimas – kodas. (0 – tinklas nepasiekiamas, 1 – mazgas nepasiekiamas, 2 – protokolas nepasiekiamas, 3 – prievadas nepasiekamas ir t.t.)
Kontrolinė suma – ICMP pranešimo kontrolinė suma

ping

ping – tai progama, veikianti ICMP protokolo pagrindu, kuri siunčia ICMP pranešimus, kuriuose antraštės lauko TIPAS reikšmė lygi 0 arba 8.

Tinklo mazgas, gavęs echo tipo pranešimą (tipas = 0), formuoja atsakomąjį echo pranešimą (tipas = 8).

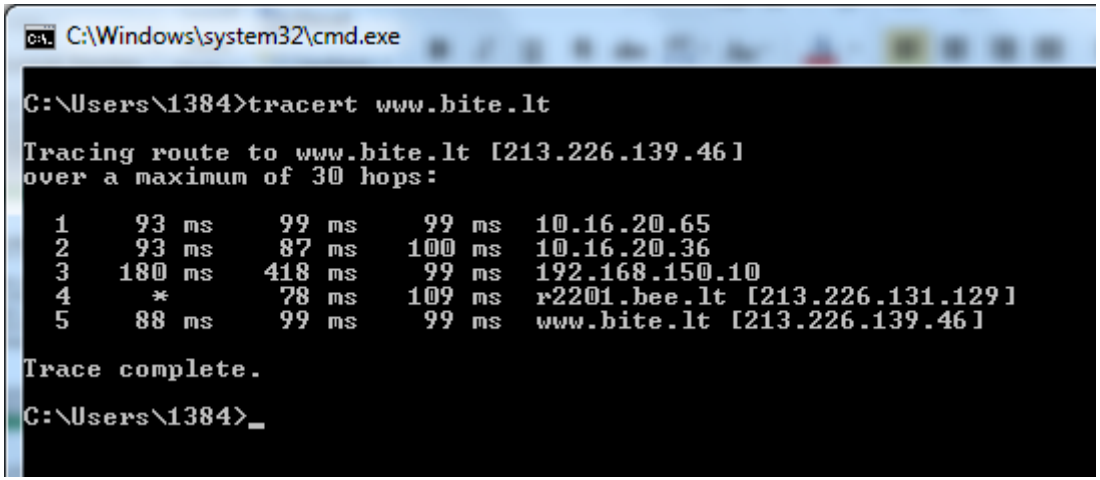
ping programa naudojama testuoti ar mazgas yra pasiekiamas. Šia pragrama taip pat galima išmatuoti apytikslį linijos pralaidumą.



tracert (traceroute)

tracert – tai programa, veikianti ICMP protokolo pagrindu ir skirta nustatyti maršrutą iki gavėjo, nustatyti RTT (round-trip time), tarpinių maršrutizatorių IP adresą ir domeno vardą.

tracert programa siunčia ICMP echo paketus su skirtingomis TTL reikšmėmis. Maršrutizatorius, gavęs paketą su TTL reikšme 1, atsako į jį su klaidos pranešimu 11 ir grąžina siuntėjui.



SNMP

Bet kuri didesnė tinklo infrastruktūra turi būti valdoma ir dažniausiai centralizuotai. Valdymui atlikti būtina surinkti informaciją iš tinklo įrenginių ir priklausomai nuo jų būsenos atlikti atitinkamus sprendimus.

SNMP (Simple Network Management Protocol) skirtas tinkle veikiantiems įrenginiams stebėti ir valdyti. SNMP protokolas veikia TCP/IP ir IPX/SPX tinkluose. (161,162 pr.)

Specifikacijos pateiktos RFC 3411 – 3418.

Informacija apie irenginius saugoma **MIB** (Management Information Base).

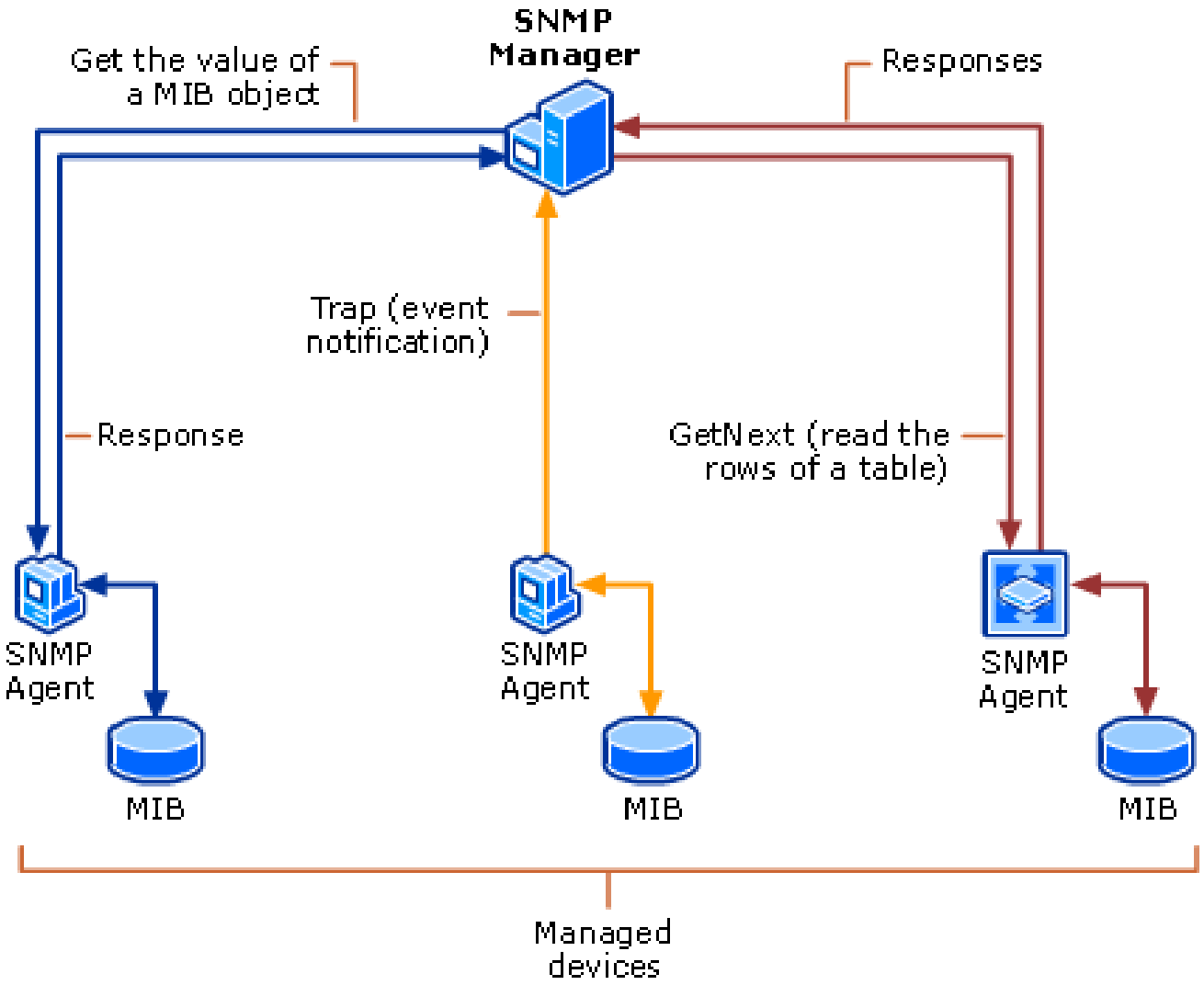
MIB modeliai ir SNMP naudoja ASN.1 notacijų kalbą.

SNMP

Tinklo valdymo struktūra, sudaryta SNMP pagrindu, susideda iš:

- **SNMP agento**. SNMP agentas atsako į valdytojo SNMP užklausas. SNMP agentas tvarko ir prižiūri kompiuterio MIB
- **SNMP valdytojo** (manager). SNMP valdytojas surenka valdymo informacija iš SNMP agentų ir ją apdoroja.
- **MIB** (*Management Information Base*). Egzistuoja keletas MIB modelių: MIB-I, MIB-II, RMON, RMON2) Per MIB pateikiami agentų prižiūrimi duomenų objektai. MIB naudoja ASN.1 notacijas.

SNMP


SNMP
Manager
Get the value of
a MIB object
Responses
Trap (event
notification)
Response
GetNext (read the
rows of a table)
SNMP
Agent
SNMP
Agent
SNMP
Agent
MIB
MIB
MIB
Managed
devices

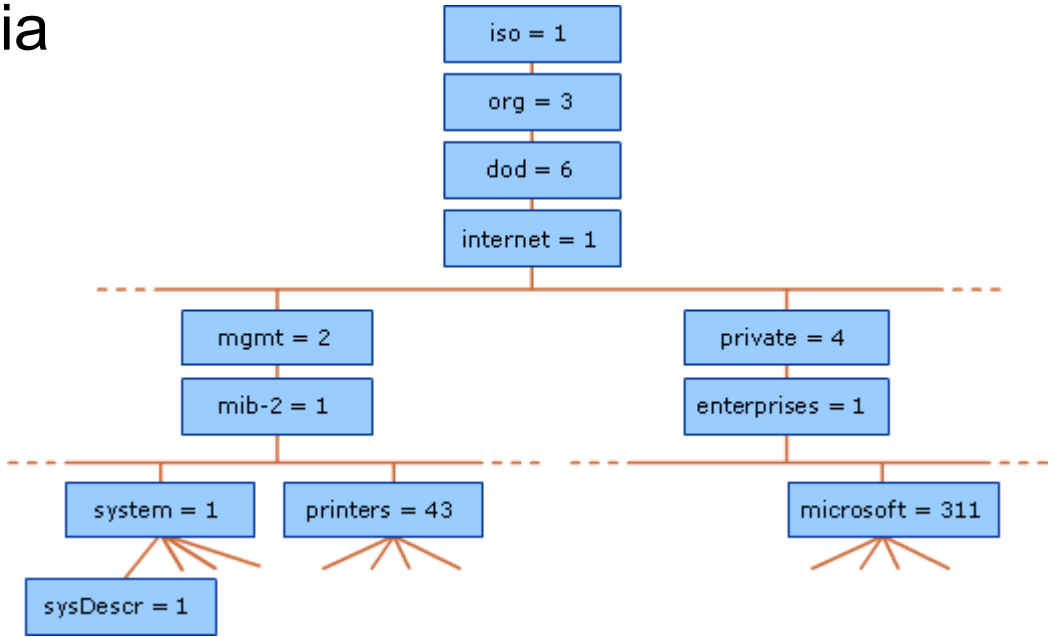
SNMP MIB

MIB apibrėžia stebimo mazgo valdomų duomenų struktūrą.

Duomenys saugomi medžio tipo duomenų bazėje, kurioje apibrėžti tam tikri **objektų identifikatoriai** (OID).

Stebimo objektai: OS versija, IP adresas, sąsaja, HDD laisvos vietos dydis, atidarytų failų skaičius.

Kiekvienas OID apibrėžia kintamąjį, kurio reikšmė gali būti nuskaityta per SNMP.



Telnet

Telnet – tai protokolas, kurio paskirtis suteikti dvikryptį interaktyvų tekstinį terminalą į nutolusį tinklo įrenginį. (23 port)

Sujungimas vykdomas per TCP protokolą, duomenys perduodami 8 bitų srautu.

Telnet protokolas buvo sukurtas 1969 m. (RFC 15, 854), ir tai buvo vienas pirmųjų IETF interneto standartų.

Telnet protokolas nešifruoja duomenų, todėl jo naudojimas šiuo metu yra labai ribotas dėl saugumo sumetimų.

Nuotoliniam prisijungimui prie tinklo mazgo yra naudojama **Telnet programa**, kuri veikia kliento-serverio principu.

SSH

SSH (Secure Shell, 22 port) – tai kriptografinis tinklo protokolas, skirtas saugiam susijungimui tarp dviejų tinklo mazgų. Paprastai SSH naudojamas norint gauti nuotolinę konsolę (tekstinį terminalą) per saugų kanalą.

Yra naudojamos dvi SSH versijos SSH-1 ir SSH-2.

SSH buvo sukurtas kaip alternatyva Telnet ir kitiems nesaugiems protokolams (rsh, rexec), kuriais siunčiami duomenys atviru tekstu.

SSH pavadinimu yra programa, naudojama saugiam nuotoliniam prisijungimui, veikianti kliento-serverio principu.

SSH

SSH naudoja **viešo rakto principą X.509** nuotolinio vartotojo autentifikavimui.

SSH galima naudoti dviem būdais:

- Automatiškai susigeneruoti viešą ir privatų raktą tam, kad šifruoti sujungimą, o autentifikacijai naudoti prisijungimo vardą ir slaptažodį.
- Rankiškai susigeneruoti viešą ir privatų raktą ir naudoti jį autentifikavimui, taip leidžiant vartotojams saugiai prisijungti nenaudojant slaptažodžių. Tam tikslui viešas raktas patalpinamas visuose kompiuteriuose iš kurių norima prisijungti, o kompiuteris į kurį norima prisijungti turi turėti privatų raktą. Svarbu, kad viešas raktas būtų siejamas su atitinkamu vartotoju, nes priešingu atveju galima įvykti įsilaužimas į kompiuterį.

KLAUSIMAI?