# KOMPIUTERIŲ TINKLAI

**12 paskaita**

Tinklo valdymas ir monitoringas

# Tinklo valdymas

Tinklo administravimas ir valdymo pagrindiniai uždaviniai:

- Užtikrinti tinklo aukštą patikimumą ir našumą
- Išvengti tinklo topologijos ir konfigūravimo klaidų
- Esant poreikiui plėsti tinklą
- Stebėti tinklą ir vesti tinklo išteklių naudojimo apskaitą
- Užtikrinti tinklo saugą

# Tinklo valdymas

**Apibrėžimas** (*Journal of Networks and System Management*)

**Network management** includes the *deployment, integration and coordination* of the hardware, software, and human elements to *monitor, test, poll, configure, analyze, evaluate, and control* the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost.

# Tinklo valdymo komponentai

ISO **Network Management Forum** išskiria penkias tinklo valdymo funkcines sritis:

- Gedimų valdymas (Fault Management)
- Konfigūracijos valdymas (Configuration Management)
- Saugos valdymas (Security Management)
- Našumo valdymas (Performance Management)
- Apskaitos valdymas (Accounting Management)

# Tinklo valdymas

**Gedimų valdymas** – tai procesas, skirtas tinklo problemų ar gedimų indentifikavimui ir šalinimui.

Gedimų valdymas apima:

- Problemos ar gedimo suradimas ir identifikavimas
- Problemų izoliavimas
- Problemų sprendimas

**Konfigūracijų valdymas** – tai procesas, apimantis tinklo įrenginių konfigūracijų nustatymą ir keitimą.

**Apskaitos valdymas** apima atitinkamų rolių ir teisių priskyrimą, tinklo resursų priskyrimą vartotojams.

# Tinklo valdymas

**Saugos valdymas** – tai procesas, kontroliuojantis prieigą prie informacijos duomenų perdavimo tinkle. Jis apima tinklo monitoringą, auditavimą, tinklo perimetro aktyvią ir pasyvią apsaugą.

**Tinklo našumo valdymas** apima tinklo įrenginių aparatūrinės ir programinės dalies greitaveikos matavimus.

Paprastai matuojami:

- Bendras tinklo pralaidumas
- Apkrovimas
- Klaidų procentas
- Uždelsimas

# Tinklo valdymo įrankiai

Efektyviam tinklo valdymui reikalingi įrankiai. Tam, kad įrankiai veiktų visuose tinkluose, reikia turėti tinklo valdymo ir monitoringo protokolus.

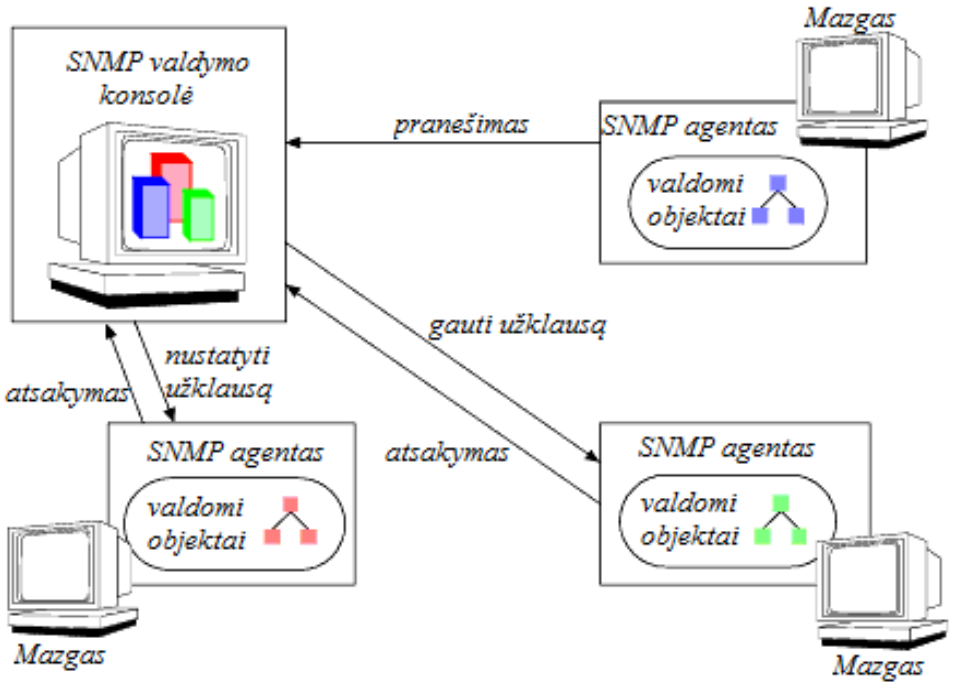
Tinklo valdymui naudojami:

- Simple Network Management Protocol (SNMP)
- Common Management Information Protocol (CMIP)
- Netfow (Cisco)
- Management Information Base (MIB)
- Network Management System (NMS)
- Windows Management Interface

Tinklo monitoringo:

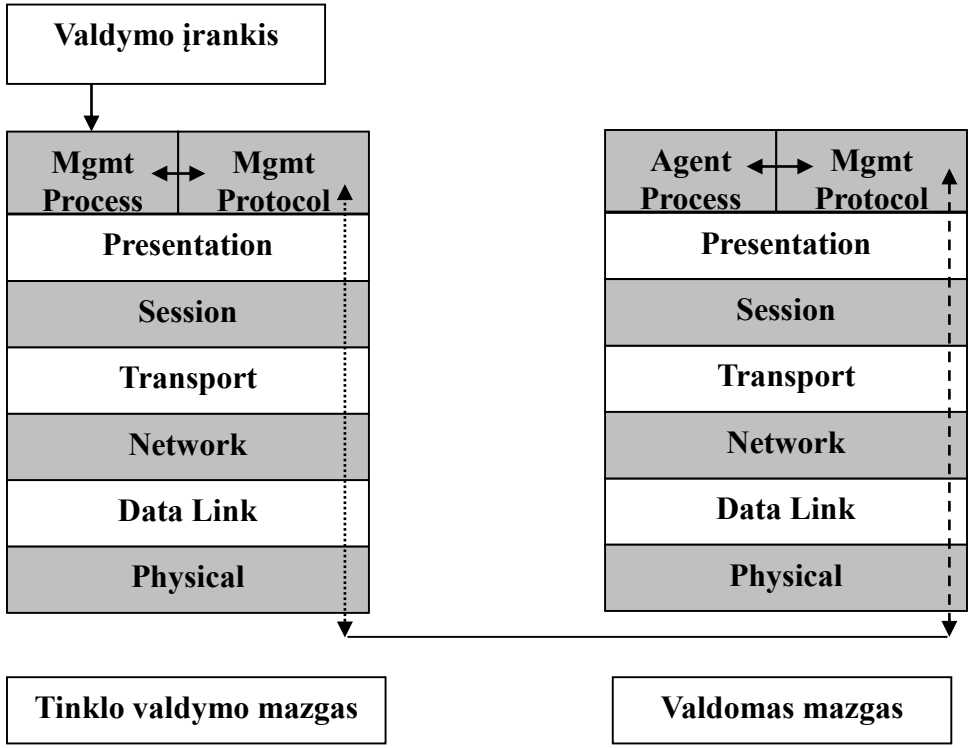
- Remote Monitoring (RMON)

# Tinklo valdymo schema




Tinklo valdymo schema, naudojant SNMP protokolą

# Tinklo valdymo pavyzdys



# SNMP

**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.

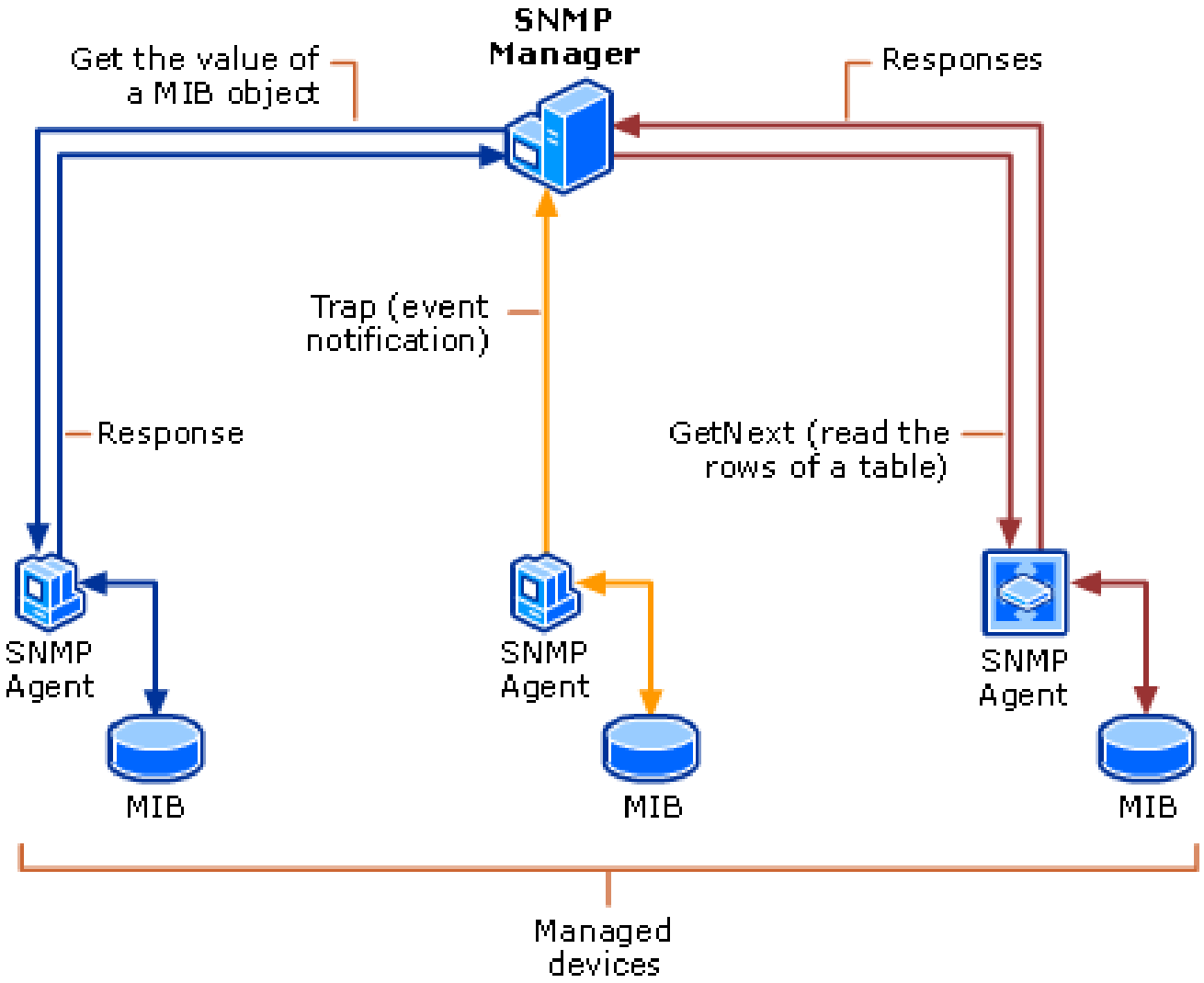
SNMP protokolas turi 3 versijas.
Pirmoji versija išleista 1988 m., o trečioji versija 2004 m.

# 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

SNMP protokolo branduolį sudaro nesudėtingų operacijų rinkinys ir taisyklės aprašančios, kaip šios operacijos turi būti vykdomos.

SNMP naudoja tris pagrindines komandas:

- Get
- Set
- Get Next

# SNMP

SNMP architektūroje išskiriami du pagrindiniai objektai:

- agentas
- tinklo valdymo mazgas, kuris yra ne kas kita, kaip serveris su programine įranga, gebančia atlikti tinklo valdymo užduotis.

Agentas ir tinklo valdymo mazgas siunčia informaciją naudodami tokius principus:

- Sinchroninis (polling)
- Asinchroninis (trap)

# SNMP trap

Jei tinklo įrenginyje įvyksta tam tikras įvykis, tinklo valdymo mazgui siunčiamas pranešimas.

Pranešimą sudaro:

- Tinklo įrenginio vardas
- Įvykio data ir laikas
- Įvykio tipas

Jei tinklo įrenginyje generuojami dideli įvykiai, gali būti toks įvykis, kad tinklo apkrovimas stipriai išauga, todėl turi būti nustatomi slenksčiai.

# SNMP polling

Tinklo valdymo mazgas periodiškai siunčia užklausas stebimiems įrenginiams. Toks informacijos gavimo metodas vadinamas sinchroniniu (polling).

Tokio metodo privalumas tame, kad tinklo valdymo mazgas mato bendrą vaizdą apie įrenginių darbą.

Trūkumas – gali atsirasti informacijos trūkumai, jei intervalai bus dideli.

Problema:

- Trumpi intervalai – didėja tinklo apkrova
- Ilgi intervalai - trūksta informacijos apie stebimus įrenginius.

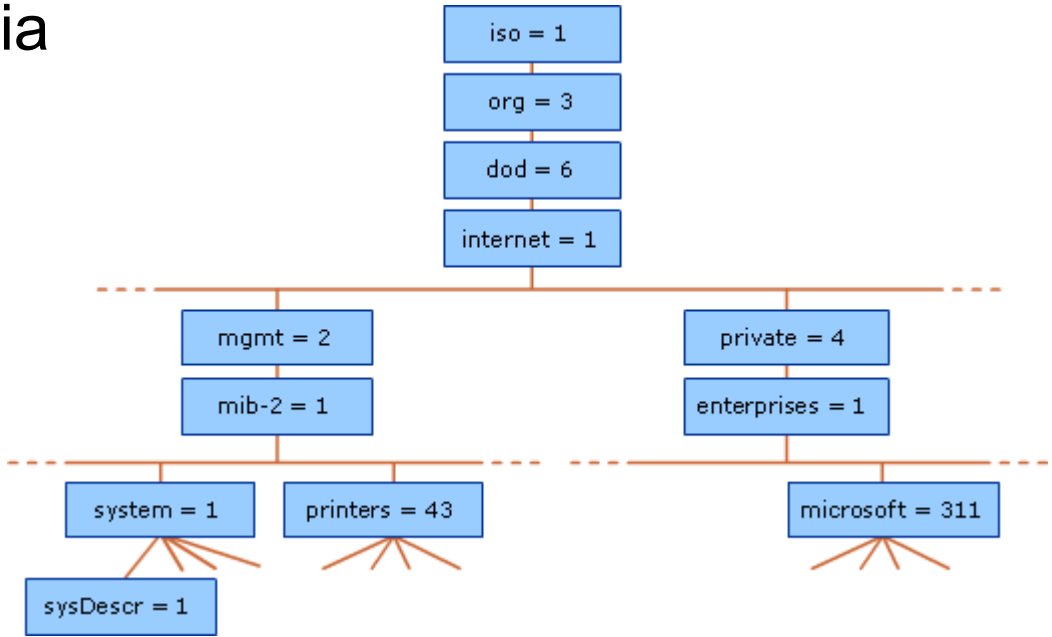
# SNMP MIB

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.



# SNMP MIB

**Valdymo duomenų bazė** (*angl. Management Information Base*), tai hierarchinė informacijos saugykla, kurią sudaro objektai virtualioje duomenų bazėje.

Ji skirta informacijos, kurią agentas protokolo pagalba siunčia iš valdomo įrenginio į NMS, saugojimui.

Valdymo duomenų bazė yra neatsiejama SNMP protokolo dalis, o **kiekvienas objektas joje turi savo unikalų identifikatorių** (*angl. OID*), pagal kurį atliekamos užklausos.

Paprastai valdymo  duomenų bazės atvaizduojamos **medžio tipo struktūra**, kur kiekvienam objektui medyje yra priskiriamas tekstinis pavadinimas, tam, kad būtų suprantama žmogui.

Objekto pavadinimas atitinka objekto identifiaktorių, pvz.: *1.3.6.1.2.1.2 – iso.org.dod.internet.mgmt.mib.interfaces.*

# SNM MIB

**Valdymo duomenų bazė** palaiko 171 kintamąjį, todėl ją galima išskirstyti į tokias pagrindines grupes:

- sistemos,
- sąsajos (*if*),
- adresų transliavimo (*at*),
- interneto protokolo (*ip*),
- interneto kontrolės žinučių protokolas (*icmp*),
- perdavimo kontrolės protokolas (*tcp*),
- vartotojo datagramų protokolas (*udp*),
- išorinių šliuzų protokolas (*egp*),
- transmisijos,
- paprastasis tinklo valdymo protokolas (*snmp*).

# MIB objektų grupės

| Pavadinimas | OID | Aprašymas |
|---|---|---|
| sistemos | 1.3.6.1.2.1.1 | Charakterizuoja objektų sąrašą, kurie susiję su sistemos veikimu: sistemos veiksnumas laiko atžvilgiu, sistemos pavadinimas ir kt. |
| if | 1.3.6.1.2.1.2 | Stebimas kiekvienos valdomo objekto fizinės sąsajos statusas, taip pat priimti ir išsiųsti oktetai (baitai), klaidos, atmesti paketai ir kt. |
| at | 1.3.6.1.2.1.3 | Adresų transliacijos lentelė. |
| ip | 1.3.6.1.2.1.4 | Stebimas interneto protokolas daugelyje aspektų, įskaitant ir IP maršruto parinkimą. |
| icmp | 1.3.6.1.2.1.5 | Stebimos ICMP protokolo klaidos, atmesti paketai ir kt. |
| tcp | 1.3.6.1.2.1.6 | Stebimos TCP protokolo ryšio būsenos: uždaryta, klausomasi, sinchronizuojama ir kt. |
| udp | 1.3.6.1.2.1.7 | Stebima UDP protokolo statistika, įeinačios ir išeinančios datagramos. |
| egp | 1.3.6.1.2.1.8 | Stebima EGP protokolo statistika. Retai naudojamas, nes pastarąjį protokolą pakeitė BGP. |
| transmisijos | 1.3.6.1.2.1.10 | Skirta D1, E1, T1, ISDN terminalo valdymui. |
| snmp | 1.3.6.1.2.1.11 | Stebima SNMP protokolo (užklausų) statistika. |

# SNMP sauga

SNMP protokole autorizacija ir autentifikacija nustatoma pagal bendruomenės žodį (*community string*).

Bendruomenės žodis gali suteikti *read-only* arba *read-write* teises.

Pagal nutylėjimą naudojami tokie žodžiai (mažosios raidės):

- public (read-only)
- private (read-write)

# SNMP konfigūravimas

**Linux**

Konfigūruojamas failas:

/etc/snmp/snmp.conf (skirtingai serveriui ir klientui)

- `sudo service snmpd start`

**Microsoft Windows Server**

Control Panel -> Administrative Tools -> Computer Management -> Services and Applications -> SNMP Service

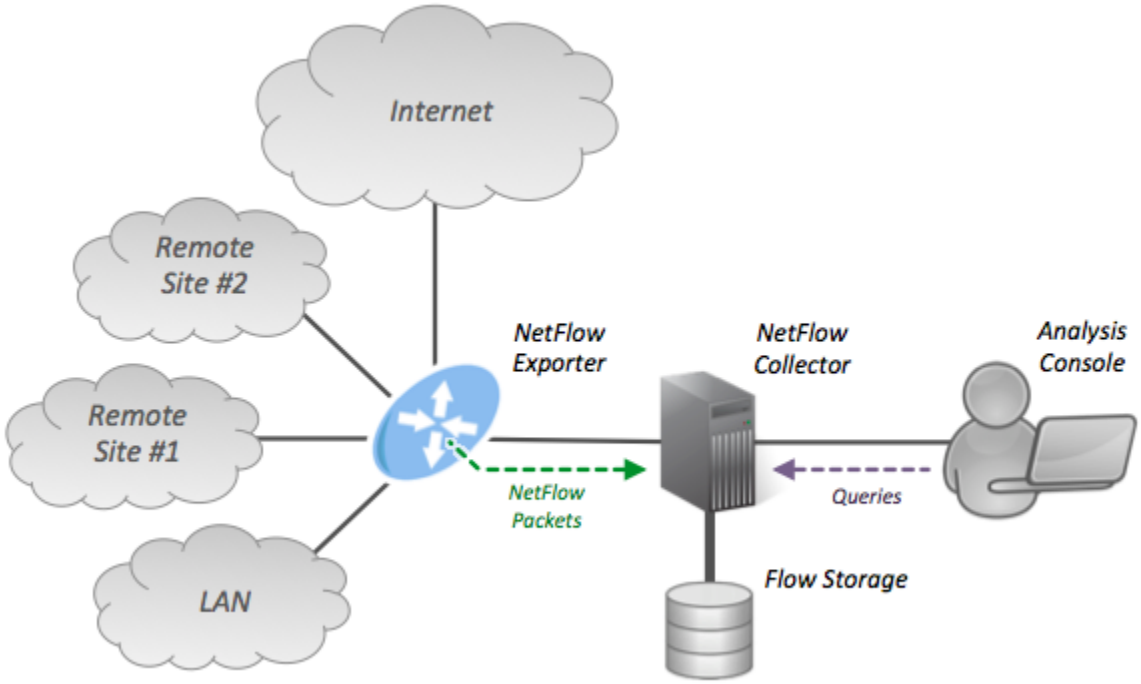
# Netflow

NetFlow srautas – tai vienkrypčių iš siuntėjo gavėjui siunčiamų paketų aibė.

Tinklo srauto monitoringo schemą sudaro:

- **Flow exporter**: agreguoja paketus į srautą ir eksportuoja srauto surinkimo įrenginiui (flow collector).
- **Flow collector**: surenka srauto paketus iš eksportuojojų.
- **Analyzer**: analizuoja srauto duomenis (pvz. IDS/IPS)

# Netflow schema




Naudojant Netflow galima stebėti tinklo aprovą, vykdyti tinklo panaudojimo apskaitą, panaudoti IDS, stebėti vartotojus, analizuoti jų veiklą ir t.t.

# Netflow

NetFlow srautą identifikuoja septyni raktiniai paketo laukai:

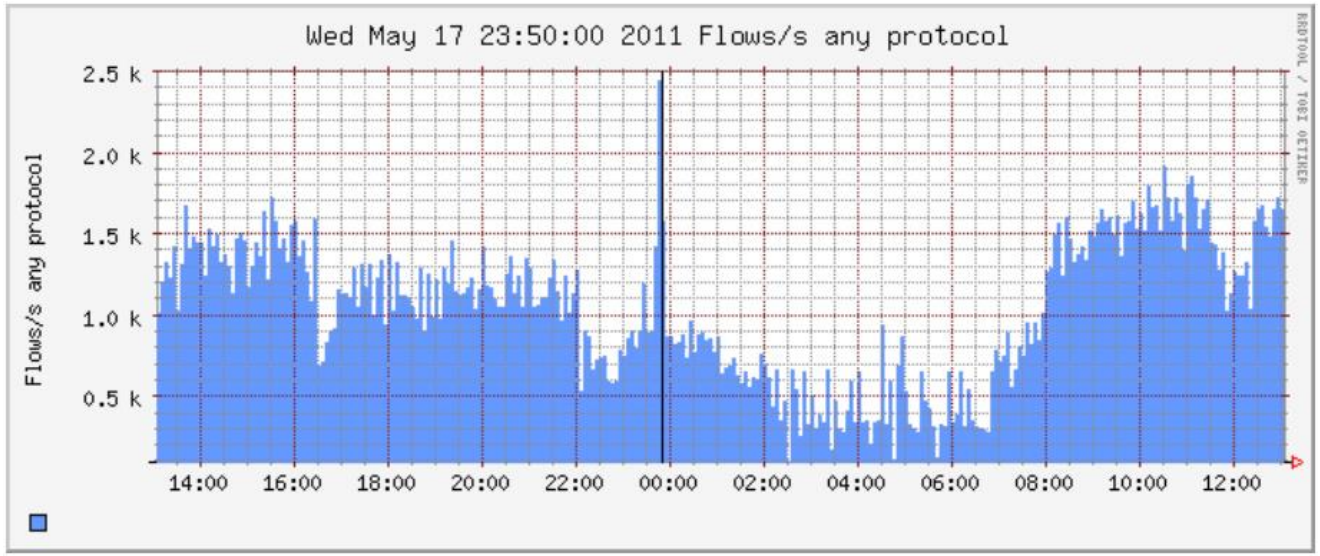
- siuntėjo IP adresas,
- gavėjo IP adresas,
- siuntėjo prievado numeris,
- gavėjo prievado numeris,
- protokolo numeris,
- TOS (type of service) reikšmė,
- priimančios sąsajos SNMP indeksas.

| Date | flow start | Duration | Proto | Src IP Addr:Port | | Dst IP Addr:Port | Packets | Bytes | Flows |
|---|---|---|---|---|---|---|---|---|---|
| 2015-09-01 | 00:00:00.459 | 0.000 | UDP | 127.0.0.1:24920 | -> | 192.168.0.1:22126 | 1 | 46 | 1 |
| 2015-09-01 | 00:00:00.363 | 0.000 | UDP | 192.168.0.1:22126 | -> | 127.0.0.1:24920 | 1 | 80 | 1 |

# Netflow įrankiai

Netflow technologiją palaiko Cisco, Juniper, Alcatel, Nortel gamintojų maršrutizatoriai.

Netflow srauto analizatoriai: Ntop, NetraMet, FlowViewer, ...

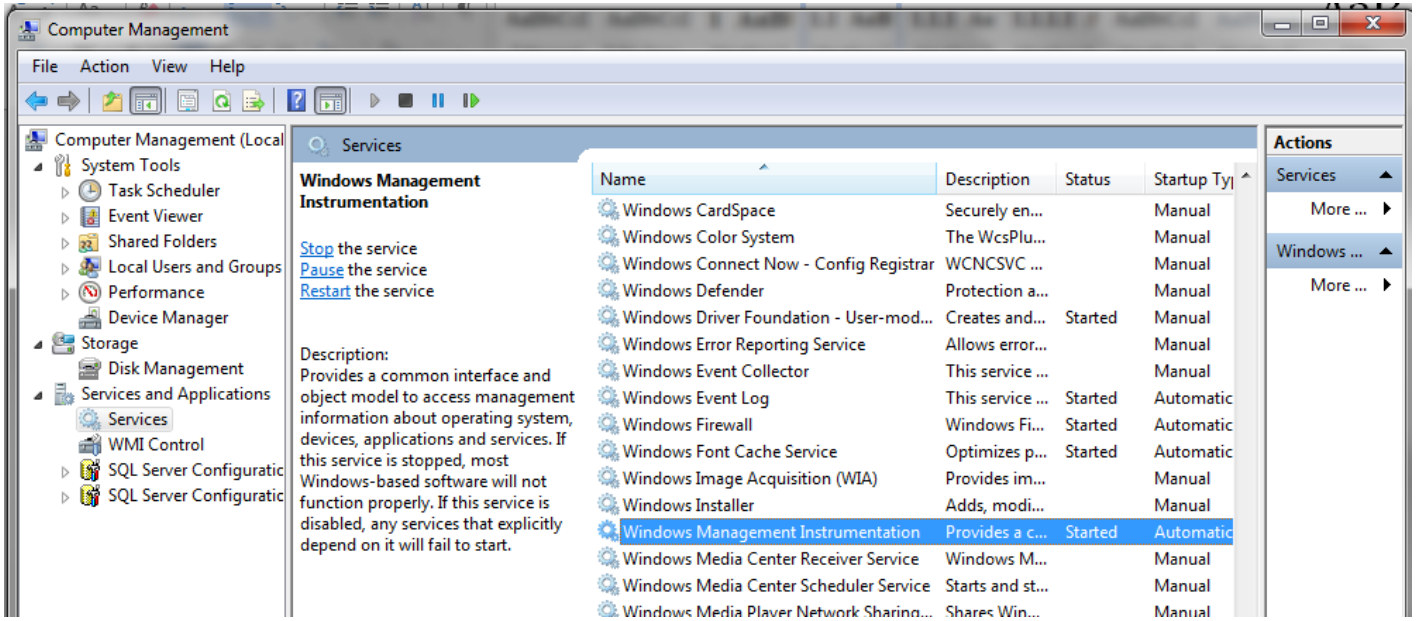


# WMI

- **Windows Management Instrumentation  arba WMI –** tai Windows Driver Model išplėtimas, teikiantis interfeisą prie operacinės sistemos, per kurį pasiekiama informacija ir atliekami nuotoliniai operacinės sistemos konfigūravimo darbai.
- **WMI** - tai Microsoft sukurtas Web-Based Enterprise Management and Common Information Model arba CIM, atitinkantis Distributed Management Task Force (DMTF) standartą.

- WMI naudoja VBScript arba Windows PowerShell Windows operacinės sistemos valdymui lokaliai ir nuotoliniu būdu. WMI naudoja Remote Procedure Call, veikiantį per TCP prievadą 135 ir atsitiktinį UDP prievadą, aukštesnį nei 1024.

# WMI




```
wmic /node:SERVER1 printer list status

wmic /node:SERVER1, cpu get name, caption,
maxclockspeed, systemname
/format:textvaluelist.xsl
```