Tutorial worksheet 10

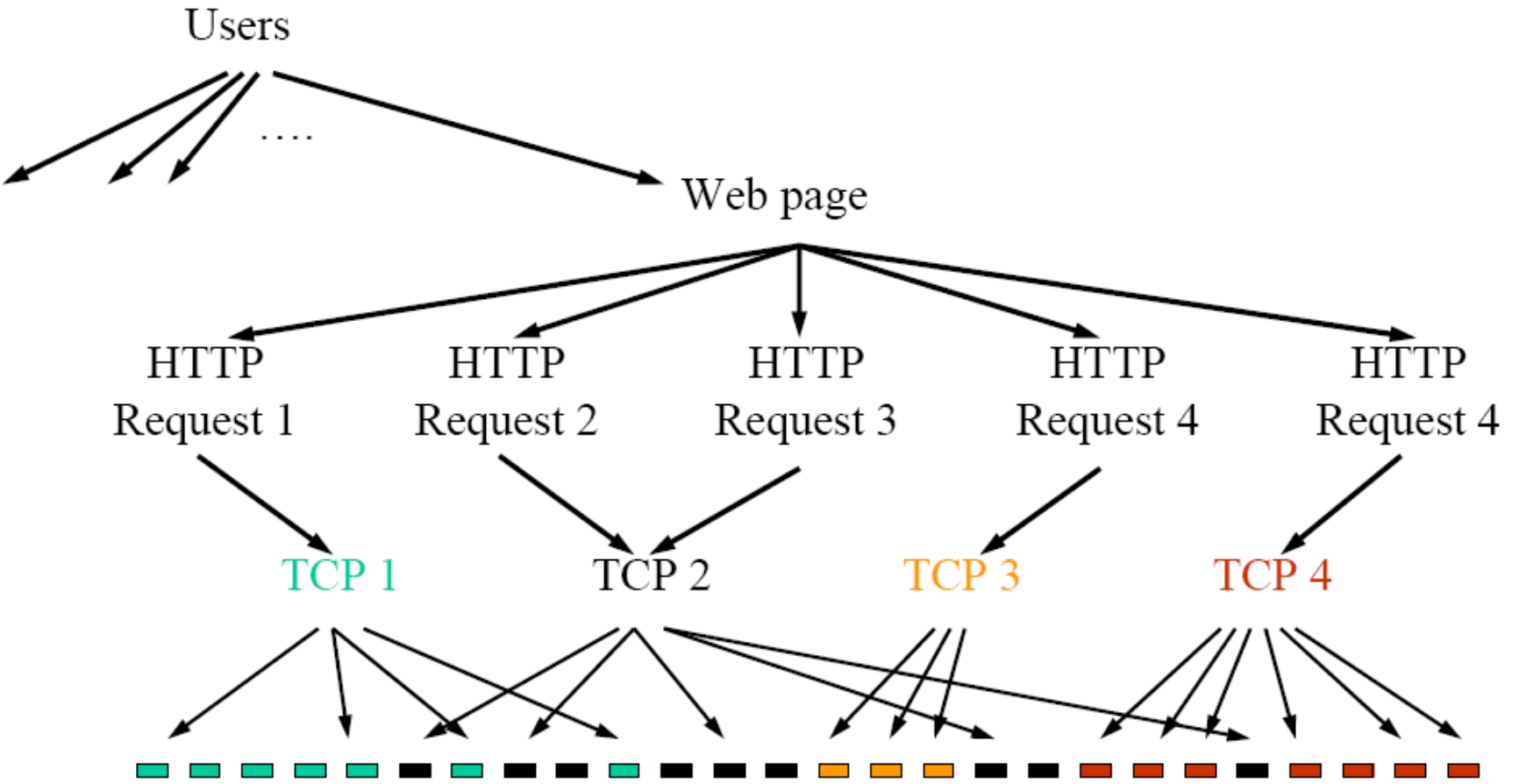
What you have done so far.

- You have so far configured
  - VLANs
  - Routing protocols with in the backbone network (RIP, OSPF, BGP).
  - Wireless mesh networking.
  - IPv6
  - Firewall policies on linux.
  - And now ‘Core Network Operations, monitoring and management.’

Work Load Generation and Monitoring.

- .
- To test network we need to generate traffic with similar characteristics that we see in the real internet. This is called representative web workload.

But how does Web traffic look like



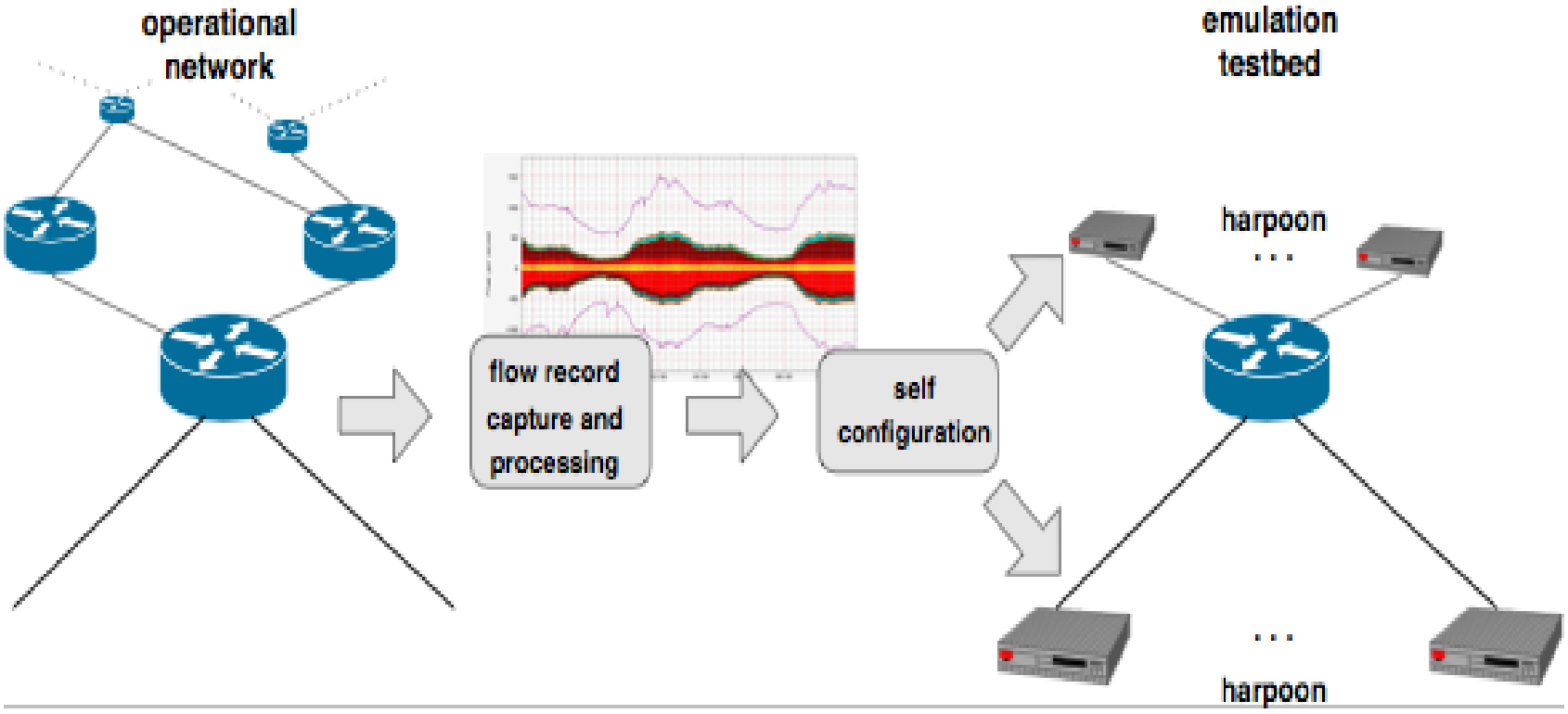
Web traffic generation-Tools

- Iperf
- SURGE
- Harpoon:
  - A Flow-level Traffic Generator by ‘Joel Sommers’

Harpoon Traffic Generator

- The design objectives of Harpoon are
  - to scalably generate application-independent network traffic at the IP flow level
  - to be easily parameterized to create traffic that is statistically identical to traffic measured at a given vantage point in the Internet.

Harpoon usage



Parameters

- File size distributions at server side
- Inter-connection time distributions at client side.
- Other factors (see worksheet 10)

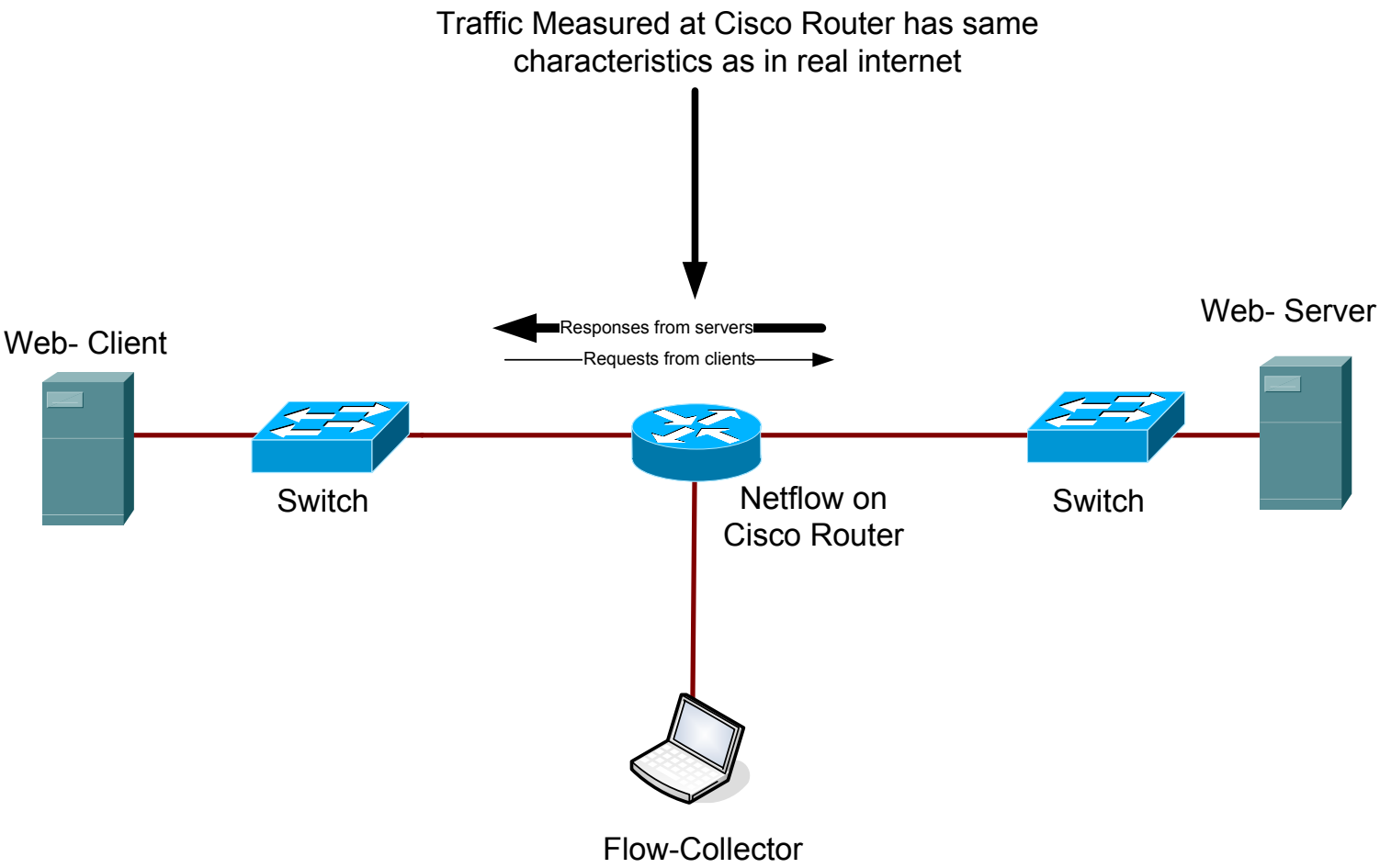
NETFLOW

- A Tool to get aggregated information from routers regarding volume of traffic.
- Cisco uses five tuple flow
  - Source ip
  - Source port
  - Destination ip
  - Destination port
  - Protocol

NETFLOW

- TCP Flows
  - Unidirectional.
  - One TCP connection has two flows.
  - They are exported on every FIN or RST
- UDP flows
  - Exported after some time.

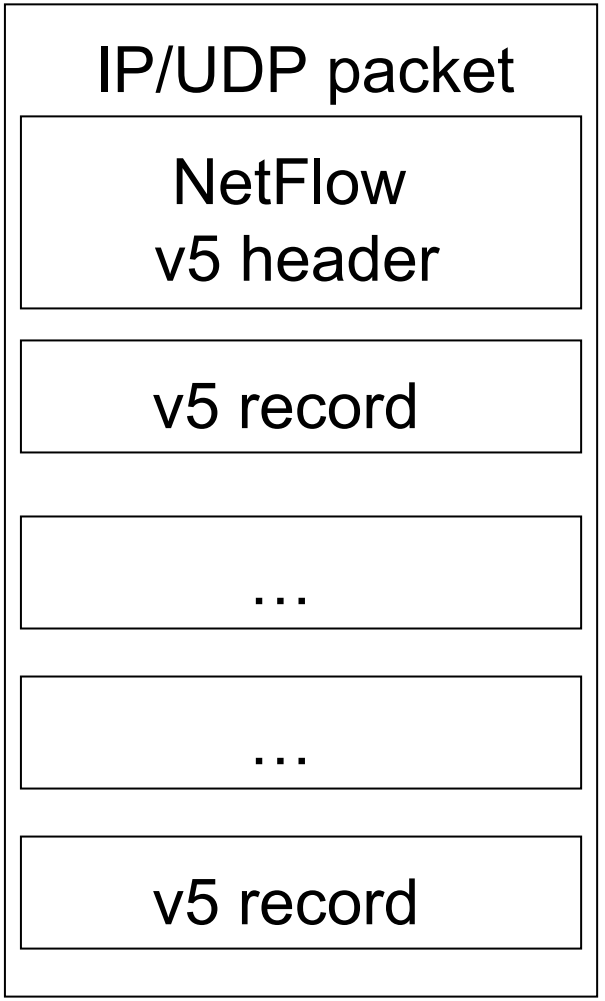
Basic Setup


Traffic Measured at Cisco Router has same characteristics as in real internet
Responses from servers
Requests from clients
Web- Client
Web- Server
Switch
Netflow on Cisco Router
Switch
Flow-Collector

Analysis of Netflow data

- Use linux utility *flow-tools*
- Flow-tools utilities
  - flow-capture
  - flow-report

NetFlow v5 Packet Example



flow-print

- Formatted output of flow files.

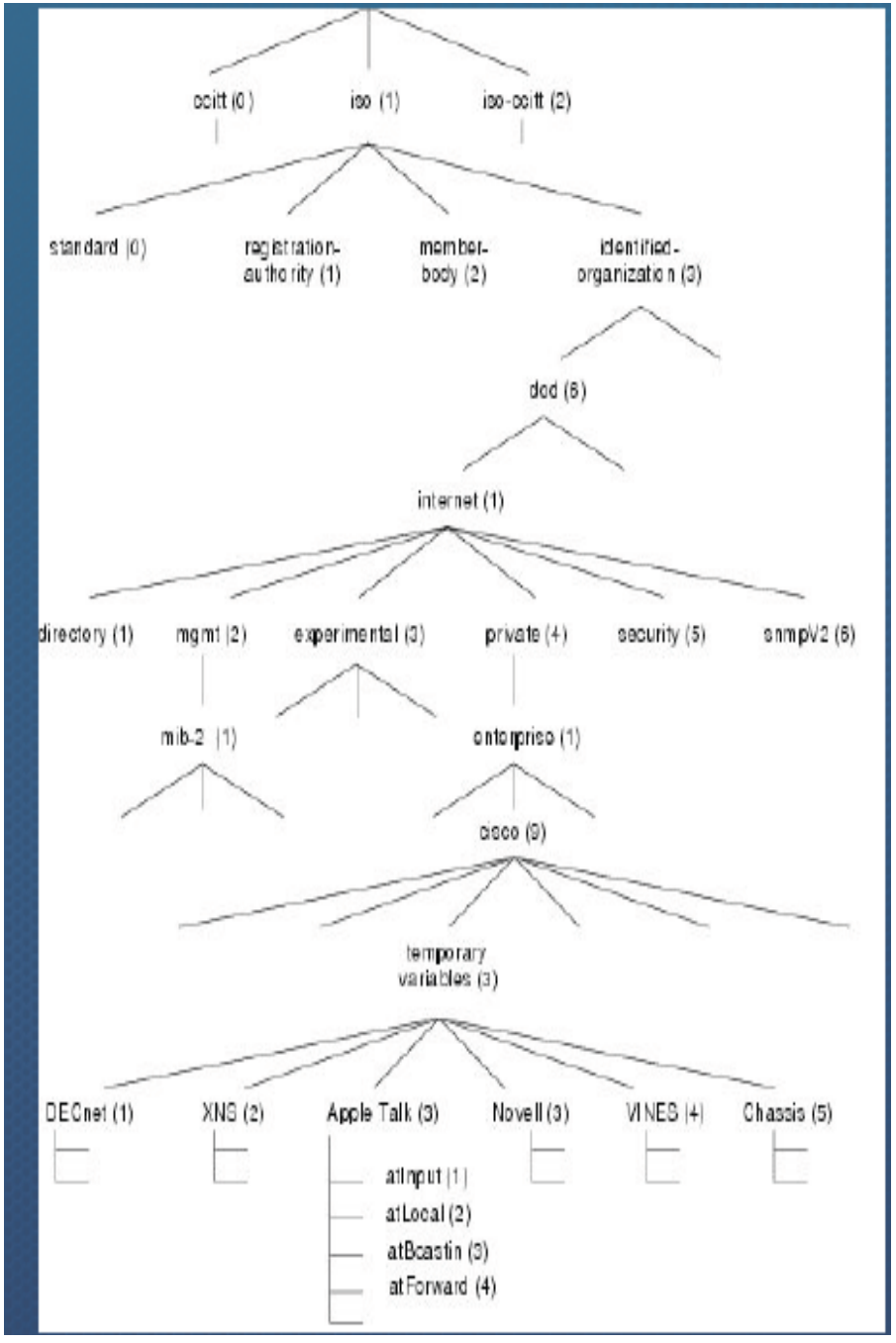
```
ng1:% flow-print < ft-v05.2002-01-21.093345-0500 | head -15
rcIP            dstIP            prot  srcPort  dstPort  octets packets
31.238.205.199  194.210.13.1     6     6346     40355    221          5
92.5.110.20     128.195.186.5    17    57040    33468    40           1
28.146.1.7      194.85.127.69    17    53       53       64           1
93.170.62.114   132.235.156.242  6     1453     1214     192          4
34.243.5.160    192.129.25.10    6     80       3360     654          7
32.235.156.242  193.170.62.114   6     1214     1453     160          4
30.206.43.51    130.101.99.107   6     3226     80       96           2
06.244.141.3    128.163.62.17    6     35593    80       739         10
06.244.141.3    128.163.62.17    6     35594    80       577          6
12.33.84.160    132.235.152.47   6     1447     1214     192          4
32.235.157.187  164.58.150.166   6     1214     56938    81           2
29.1.246.97     152.94.20.214    6     4541     6346     912         10
32.235.152.47   212.33.84.160    6     1214     1447     160          4
30.237.131.52   130.101.9.20     6     1246     80       902         15
```

SNMP

- Simple Network Management Protocol
  - Runs on UDP
  - client-server
  - Participants
    - 1 manger/Management Station (e.g. router/switch)
    - management agents

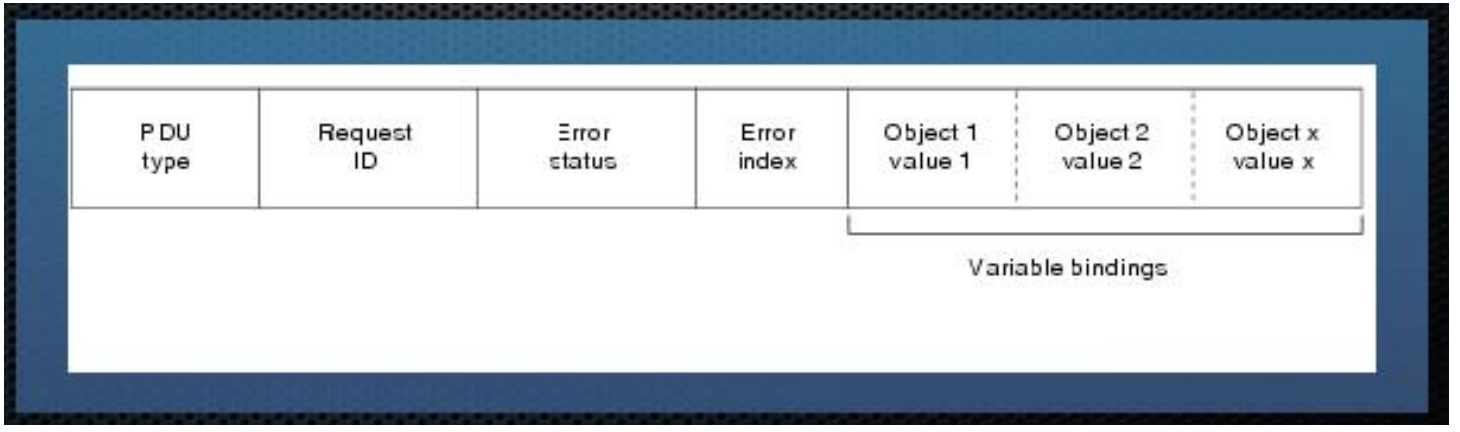
SMNP

- Operations: get , set, (trap) , (traversal)
- Security: By a simple shared secret (community)
- SNMP MIB
  - MIB: Management Information Base
  - Groups the managed objects into hierarchal namespace.
  - Individual objects addressed via OID (Object Identifier)


ccitt (0)
iso (1)
iso-ccitt (2)
standard (0)
registration-authority (1)
member-body (2)
identified-organization (3)
dod (6)
internet (1)
directory (1)
mgmt (2)
experimental (3)
private (4)
security (5)
snmpV2 (6)
mib-2 (1)
enterprise (1)
cisco (9)
temporary variables (3)
DECnet (1)
XNS (2)
Apple Talk (3)
Novell (3)
VINES (4)
Chassis (5)
atInput (1)
atLocal (2)
atBcastin (3)
atForward (4)

SNMP Packet

- Is called PDU (protocol data unit)
- Contains: command, Request ID, Error status, variables



Tools

- snmpget : query a specific object variable
- snmpset : set a specific object variable
- snmpwalk: hierarchically list MIB sub tree