SANOG

Network Operations and Network Management

By
Aftab A. Siddiqui

aftabs@cyber.net.pk

Overview

- Network Management
- Network Operations Centre
- Network Monitoring Systems and Tools
- Network Management Protocol
- SNMP
- Stats and Accounting
- Network Flows
- Fault and Problem Management
- Configuration Management
- Archiving
- Log Management

Network Management

- System & Service monitoring
  - Reachability, availability
- Resource measurement/monitoring
  - Capacity planning, availability
- Performance monitoring (RTT, throughput)
- Stats & Accounting/Metering
- Fault Management
  - Fault detection, troubleshooting, and tracking
- Configuration/Change Management

Network Management

- Network is running smoothly and monitoring problems before hand.
  - Deliver projected SLAs (Service Level Agreements)
  - Depends on policy
    - Management expectations ?
    - Users expectations ?
    - Customers expectations ?
    - What does the rest of the Internet expect ?
  - Is 24x7x365 good enough ?
    - Can you Guarantee 100% uptime?

Network Management

- What does it take to deliver 99.9 % ?
  - 30,5 x 24 = 762 hours a month
  - (762 – (762 x .999)) x 60 = 45 minutes max of downtime a month!
- Need to shutdown 1 hour / week ?
  - (762 - 4) / 762 x 100 = 99.4 %
  - Remember to take planned maintenance into account in your calculations, and inform your users/customers if they are included/excluded in the SLA
- How is availability measured ?
  - In the core ? End-to-end ? From the Internet ?

Network Management

- Know when to upgrade
  - Is your bandwidth usage too high ?
  - Where is your traffic going ?
  - Do you need to get a faster line, or more providers ?
  - Is the equipment too old ?
- Keep an audit trace of changes
  - Record all changes
  - Makes it easier to find cause of problems due to upgrades and configuration changes
- Where to consolidate all these functions ?
  - In the Network Operation Center (NOC)

The Network Operations Center (NOC)

- Where it all happens
  - Coordination of tasks
  - Status on network and services
  - Fielding of network-related incidents and complaints
  - Where the tools reside (”NOC server”)
- One of the goals of this Tutorial…
  - Help you understand how to build a NOC box
  - It will be the most important machine on your network

Network monitoring systems and tools

- Two kinds of tools
  - **Diagnostic tools** – used to test connectivity, ascertain that a location is reachable, or a device is up – usually active tools
  - **Monitoring tools** – tools running in the background (”daemons” or services), which collect events, but can also initiate their own probes (using diagnostic tools), and recording the output, in a scheduled fashion.

Network monitoring systems and tools

- Active tools
  - Ping – test connectivity to a host
  - Traceroute – show path to a host
  - Combination of ping + traceroute
  - SNMP collectors (polling)
- Passive tools
  - log monitoring, SNMP trap receivers
- Automated tools
  - SmokePing – record and graph latency to a set of hosts, using ICMP (Ping)
  - MRTG – record and graph bandwidth usage on a switch port or network link, at regular intervals

Network monitoring systems and tools

- Network & Service Monitoring tools
  - Nagios – server and service monitor
    - Can monitor pretty much anything
    - HTTP, SMTP, DNS, Disk space, CPU usage, ...
    - Easy to write new plugins (extensions)
  - Basic scripting skills are required to develop simple monitoring jobs – Perl, Shellscript...
  - Many good Open Source tools
    - Zabbix, ZenOSS, etc ...
- Use them to monitor reachability and latency in your network
  - Parent-child dependency mechanisms are very useful!

Network monitoring systems and tools

- Monitor your critical Network Services
  - DNS
  - Radius/LDAP/SQL
  - SSH to routers
- Define notification method?
- Always collect logs!
  - Every network device (and UNIX and Windows servers as well) can report system events using syslog
  - You **MUST collect and monitor your logs!**
  - **Not doing so is one of the most common mistakes when doing network monitoring**

Network Management Protocols

- **SNMP – Simple Network Management Protocol**
  - **Industry standard, hundreds of tools exist to exploit it**
  - **Present on any decent network equipment**
    - Network throughput, errors, CPU load, temperature, ...
  - **UNIX and Windows implement this as well**
    - Disk space, running processes, ...
- **SSH and telnet**
  - **Always use secure connection to network device when available**
  - **It's also possible to use scripting to automate monitoring of hosts and services**

Enable SSH

- Avoid using telnet for your network devices
- Everything is clear text on the wire in telnet
- Most of the renowned vendor platforms support ssh

```
>show ip ssh
SSH Disabled - version 1.99
%Please create RSA keys (of atleast 768 bits size) to enable SSH v2.
Authentication timeout: 120 secs; Authentication retries: 3
```

Enable SSH

- There are four steps required to enable SSH support on a Cisco IOS router:
- Configure the **hostname** command.
- Configure the DNS domain.
- Generate the SSH key to be used.
- Enable SSH transport support for the virtual type terminal (vtys).

- hostname srilanka
- **aaa new-model** username sanog password 0 sanog
- ip domain-name sanog.org

Enable SSH

- (config)#crypto key generate rsa

```
The name for the keys will be: srilanka.sanog.org
Choose the size of the key modulus in the range of 360 to 2048 for your
 General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
```

- line vty 0 15 transport input SSH

SNMP

- SNMP – Simple Network Management Protocol
  - Industry standard, hundreds of tools exist to exploit it
  - Present on any decent network equipment
- Query – response based
  - GET / SET
- Tree hierarchy
  - Query for ”Object Identifiers” (OIDs)
- Concept of MIBs (Management Information Base)
  - Standard and vendor-specific (Enterprise)

SNMP

- UDP protocol, port 161
- Different versions
  - Originally, 1988
  - v1 – RFC1155, RFC1156, RFC1157
    - Original specification
  - v2 – RFC1901 … RFC1908 + RFC2578
    - Extends v1, new data types, better retrieval methods (GETBULK)
    - Really is version v2c (without security model)
  - v3 – RFC3411 … RFC3418
- Typically we use SNMPv2
- Terminology:
  - Manager (the monitoring ”client”)
  - Agent (running on the equipment/server)

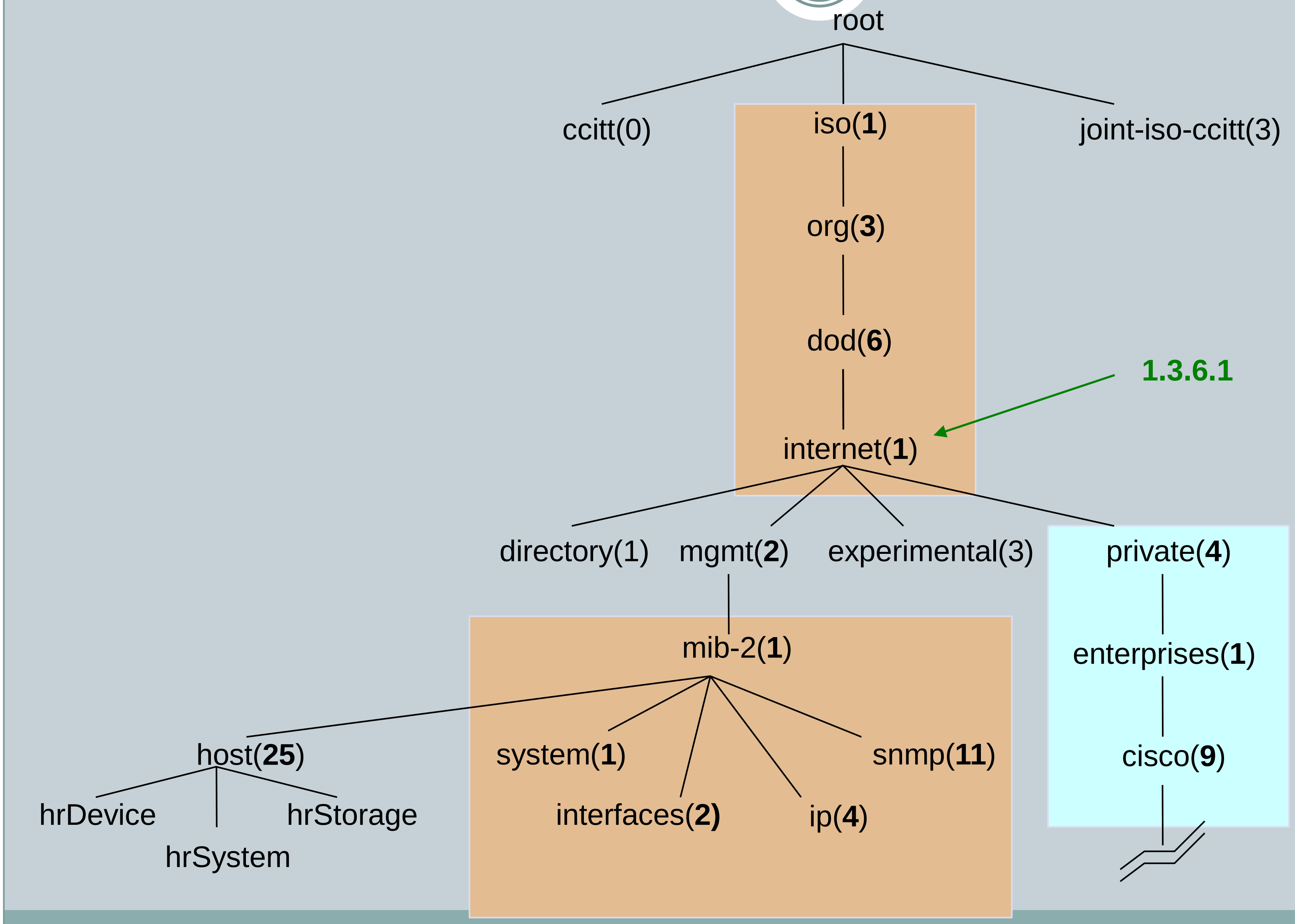
SNMP

- Typical queries
  - Bytes In/Out on an interface, errors
  - CPU load
  - Uptime
  - Temperature
  - …
- For hosts (servers or workstations)
  - Diskspace
  - Installed software
  - Running processes
  - …
- Windows and UNIX have SNMP

SNMP: Working

- Basic commands
  - GET (manager -> agent)
    - Query for a value
  - GET-NEXT (manager -> agent)
    - Get next value (list of values for a table)
  - GET-RESPONSE (agent -> manager)
    - Response to GET/SET, or error
  - SET (manager -> agent)
    - Set a value, or perform action
  - TRAP (agent -> manager)
    - Spontaneous notification from equipment (line down, temperature above threshold, ...)

The MIB tree



root

ccitt(0)

iso(**1**)

joint-iso-ccitt(3)

org(**3**)

dod(**6**)

internet(**1**)

1.3.6.1

directory(1)

mgmt(**2**)

experimental(3)

private(**4**)

mib-2(**1**)

enterprises(**1**)

host(**25**)

system(**1**)

snmp(**11**)

cisco(**9**)

hrDevice

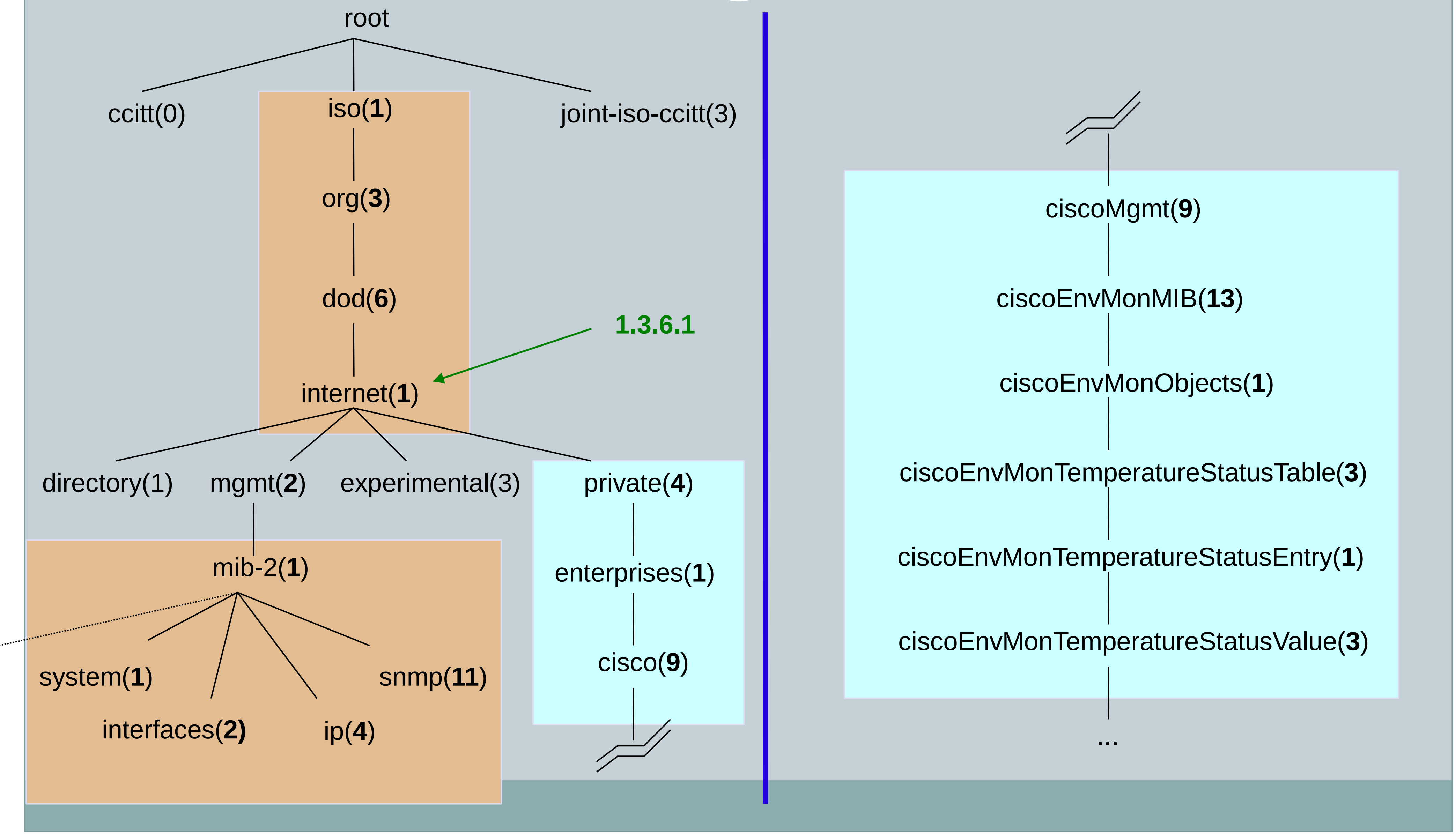
hrStorage

interfaces(**2**)

ip(**4**)

hrSystem

The MIB tree



root

ccitt(0)

iso(**1**)

joint-iso-ccitt(3)

org(**3**)

dod(**6**)

internet(**1**)

1.3.6.1

directory(1)

mgmt(**2**)

experimental(3)

private(**4**)

mib-2(**1**)

enterprises(**1**)

system(**1**)

snmp(**11**)

interfaces(**2**)

ip(**4**)

cisco(**9**)

ciscoMgmt(**9**)

ciscoEnvMonMIB(**13**)

ciscoEnvMonObjects(**1**)

ciscoEnvMonTemperatureStatusTable(**3**)

ciscoEnvMonTemperatureStatusEntry(**1**)

ciscoEnvMonTemperatureStatusValue(**3**)

...

OIDs and MIBs

- Navigate tree downwards
- OIDs separated by '.'
  - `1.3.6.1.4.1.9. ...`
- OID corresponds to a label
  - `.1.3.6.1.2.1.1.5 => sysName`
- The complete path:
  - `.iso.org.dod.internet.mgmt.mib-2.system.sysName`

MIBs

- MIBs are files defining the objects that can be queried, including:
  - Object name
  - Object description
  - Data type (integer, text, list)
- MIBS are structured text, using ASN.1
- Standard MIBs include:
  - MIB-II – (RFC1213) – a group of sub-MIBs
  - HOST-RESOURCES-MIB (RFC2790)
- MIBs also make it possible to interpret a returned value from an agent
  - For example, the status for a fan could be 1,2,3,4,5,6 – what does it mean ?

Querying SNMP agent

- Some typical commands for querying:
  - snmpget
  - snmpwalk
  - snmpstatus

- Syntax:

```
snmpXXX -c community -v1 host [oid]
snmpXXX -c community -v2c host [oid]
```

- Let's take an example
  - **snmpstatus -c public -v1 192.168.2.2**
  - **snmpget -c sanog -v1 192.168.2.2 .iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber.0**
  - **snmpwalk -c public -v1 ifDescr**

Querying SNMP agent

- Community:
  - A ”security” string (password) to define whether the querying manager will have RO (read only) or RW (read write) access
  - This is the simplest form of authentication in SNMP
- OID
  - A value, for example, .1.3.6.1.2.1.1.5.0, or it's name equivalent
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0

Stats & Accounting tools

- **Traffic accounting**
  - **what is your network used for, and how much**
  - **Useful for Quality of Service, detecting abuses, and billing (metering)**
  - **Dedicated protocol: NetFlow**
  - **Identify traffic ”flows”: protocol, source, destination, bytes**
  - **Different tools exist to process the information**
    - Flowtools, flowc
    - NFSen
    - ...

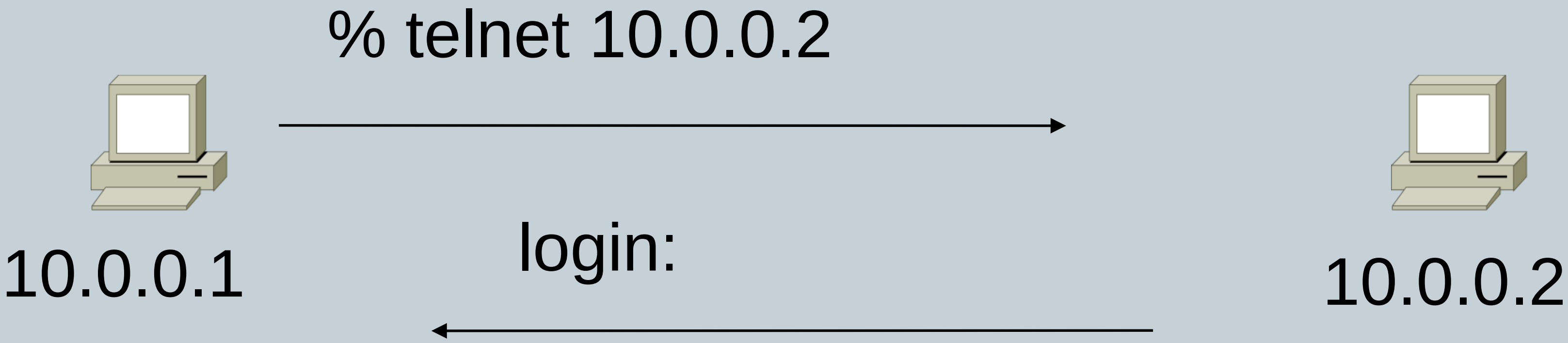
Network Flows

- Packets or frames that have a common attribute.
- Creation and expiration policy – what conditions start and stop a flow.
- Counters – packets,bytes,time.
- Routing information – AS, network mask, interfaces.

Network Flows

- Unidirectional or bidirectional.
- Bidirectional flows can contain other information such as round trip time, TCP behavior.
- Application flows look past the headers to classify packets by their contents.
- Aggregated flows – flows of flows.

Unidirectional Flow with Source/Destination IP Key



% telnet 10.0.0.2

login:

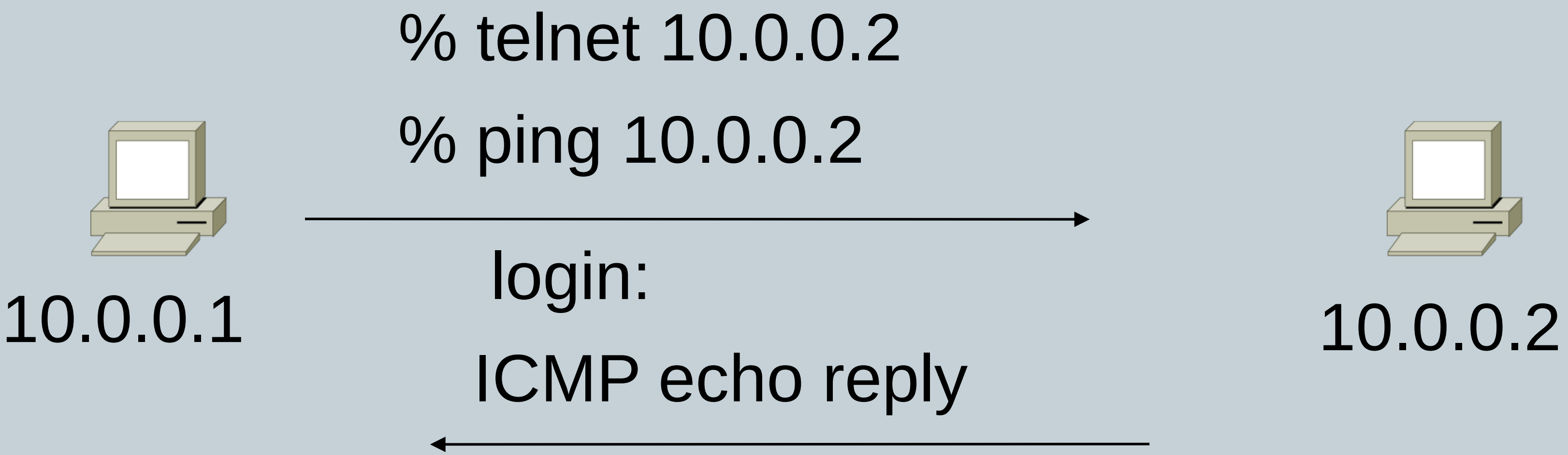
10.0.0.1

10.0.0.2

Active Flows

Flow	Source IP	Destination IP
1	10.0.0.1	10.0.0.2
2	10.0.0.2	10.0.0.1

Unidirectional Flow with Source/Destination IP Key



% telnet 10.0.0.2

% ping 10.0.0.2

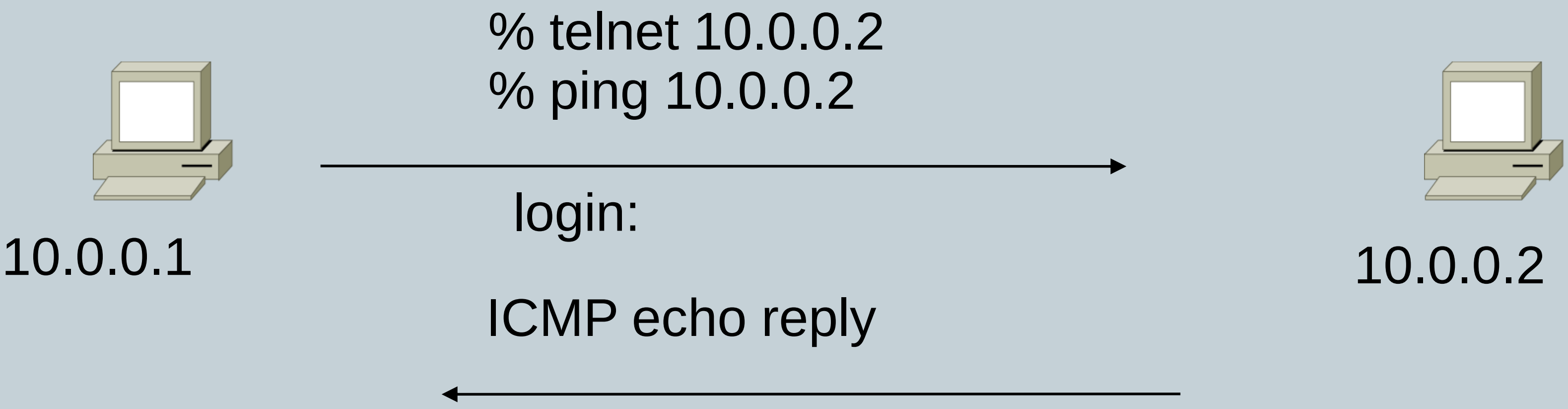
login:

ICMP echo reply

Active Flows

Flow	Source IP	Destination IP
1	10.0.0.1	10.0.0.2
2	10.0.0.2	10.0.0.1

Unidirectional Flow with IP, Port, Protocol Key



% telnet 10.0.0.2
% ping 10.0.0.2

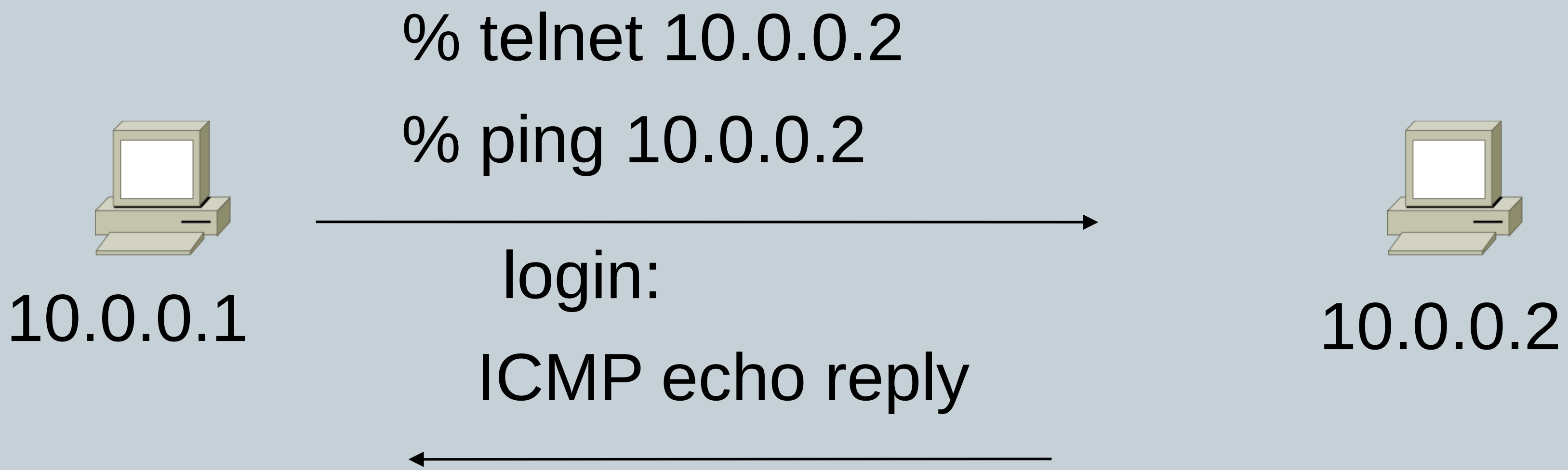
login:

ICMP echo reply

Active Flows

Flow	Source IP	Destination IP	prot	srcPort	dstPort
1	10.0.0.1	10.0.0.2	TCP	32000	23
2	10.0.0.2	10.0.0.1	TCP	23	32000
3	10.0.0.1	10.0.0.2	ICMP	0	0
4	10.0.0.2	10.0.0.1	ICMP	0	0

Bidirectional Flow with IP, Port, Protocol Key



% telnet 10.0.0.2

% ping 10.0.0.2

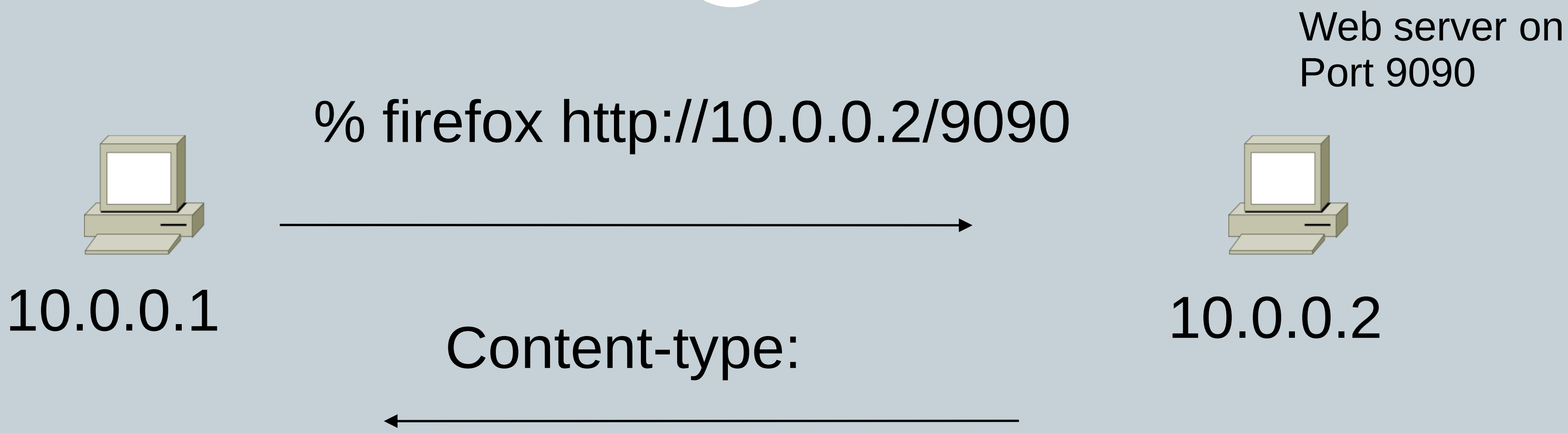
login:

ICMP echo reply

Active Flows

Flow	Source IP	Destination IP	prot	srcPort	dstPort
1	10.0.0.1	10.0.0.2	TCP	32000	23
2	10.0.0.1	10.0.0.2	ICMP	0	0

Application Flow



Web server on
Port 9090

% firefox http://10.0.0.2/9090

10.0.0.1

10.0.0.2

Content-type:

Active Flows

Flow	Source IP	Destination IP	Application
1	10.0.0.1	10.0.0.2	HTTP

Aggregated Flow

Main Active flow table

Flow	Source IP	Destination IP	prot	srcPort	dstPort
1	10.0.0.1	10.0.0.2	TCP	32000	23
2	10.0.0.2	10.0.0.1	TCP	23	32000
3	10.0.0.1	10.0.0.2	ICMP	0	0
4	10.0.0.2	10.0.0.1	ICMP	0	0

Source/Destination IP Aggregate

Flow	Source IP	Destination IP
1	10.0.0.1	10.0.0.2
2	10.0.0.2	10.0.0.1

Working with Flows

- Generating and Viewing Flows
- Exporting Flows from devices
  - Types of flows
  - Sampling rates
- Collecting it
  - Tools to Collect Flows - Flow-tools
- Analyzing it
  - More tools available, can write your own

Flow Descriptors

- A Key with more elements will generate more flows.
- Greater number of flows leads to more post processing time to generate reports, more memory and CPU requirements for device generating flows.
- Depends on application. Traffic engineering vs. intrusion detection.

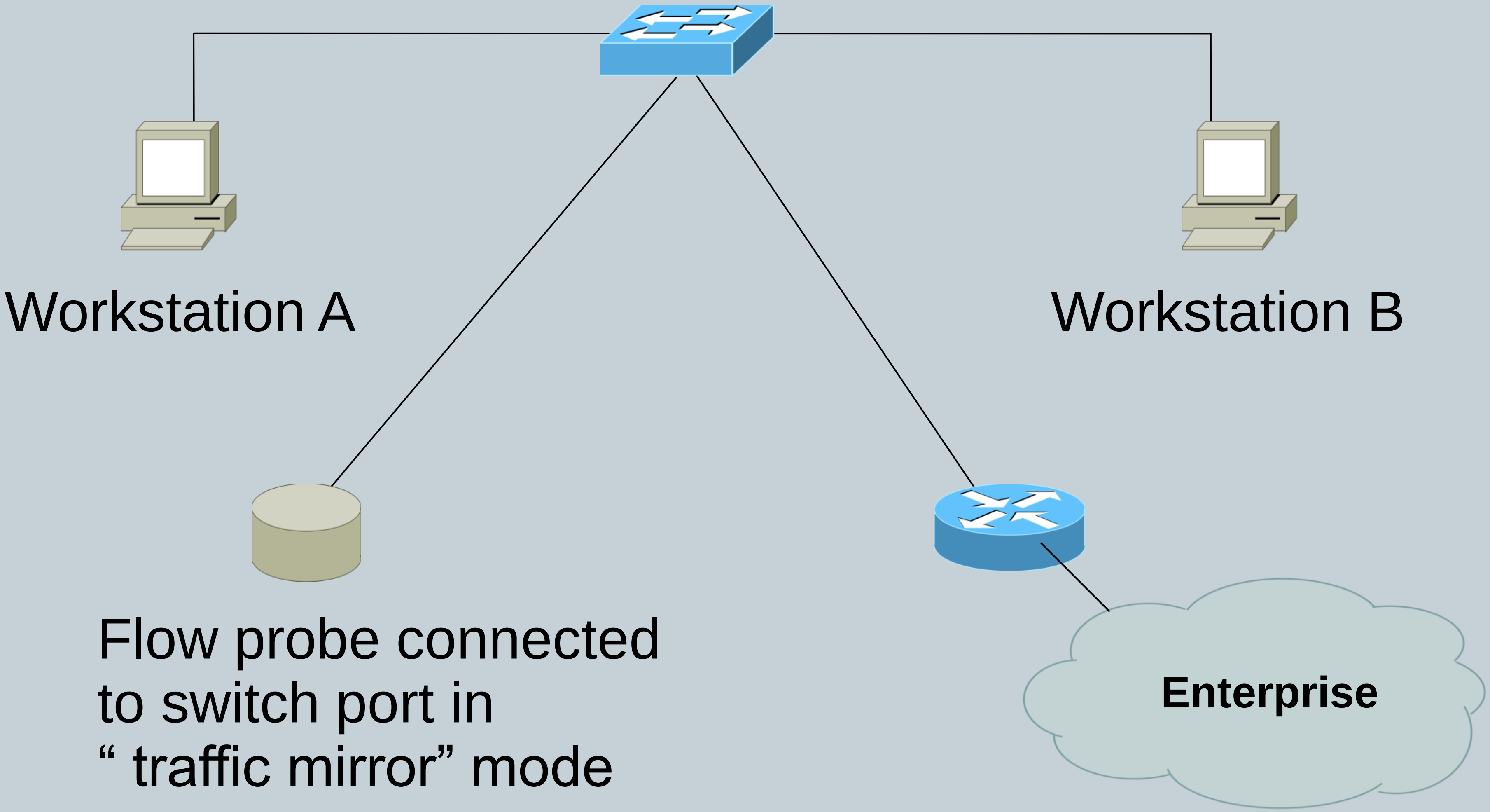
Flow Accounting

- Accounting information accumulated with flows.
- Packets, Bytes, Start Time, End Time.
- Network routing information – masks and autonomous system number.

Flow Generation/Collection

- Passive monitor
  - A passive monitor (usually a unix host) receives all data and generates flows.
  - Resource intensive, newer investments needed
- Router or other existing network device.
  - Router or other existing devices like switch, generate flows.
  - Sampling is possible
  - Nothing new needed

Passive Monitor Collection



Workstation A

Workstation B

Flow probe connected to switch port in “ traffic mirror” mode

Passive Monitor

- Directly connected to a LAN segment via a switch port in “mirror” mode, optical splitter, or repeated segment.
- Generate flows for all local LAN traffic.
- Must have an interface or monitor deployed on each LAN segment.
- Support for more detailed flows – bidirectional and application.

Router Collection

- Router will generate flows for traffic that is directed to the router.
- Flows are not generated for local LAN traffic.
- Limited to “simple” flow criteria (packet headers).
- Generally easier to deploy – no new equipment.

Cisco NetFlow

- Unidirectional flows.
- IPv4 unicast and multicast.
- Aggregated and unaggregated.
- Flows exported via UDP.
- Supported on IOS and CatOS platforms.

Cisco NetFlow Versions

- 4 Unaggregated types (1,5,6,7).
- 14 Aggregated types (8.x, 9).
- Each version has its own packet format.
- Version 1 does not have sequence numbers – no way to detect lost flows.
- The "version" defines what type of data is in the flow.
- Some versions specific to Catalyst platform.

NetFlow v1

- Key fields: Source/Destination IP, Source/Destination Port, IP Protocol, ToS, Input interface.
- Accounting: Packets, Octets, Start/End time, Output interface
- Other: Bitwise OR of TCP flags.

NetFlow v5

- Key fields: Source/Destination IP, Source/Destination Port, IP Protocol, ToS, Input interface.
- Accounting: Packets, Octets, Start/End time, Output interface.
- Other: Bitwise OR of TCP flags, Source/Destination AS and IP Mask.
- Packet format adds sequence numbers for detecting lost exports.

NetFlow v8

- Aggregated v5 flows.
- Not all flow types available on all equipments
- Much less data to post process, but loses fine granularity of v5 – no IP addresses.

NetFlow v8

- AS
- Protocol/Port
- Source Prefix
- Destination Prefix
- Prefix
- Destination
- Source/Destination
- Full Flow

NetFlow v9

- Record formats are defined using templates.
- Template descriptions are communicated from the router to the NetFlow Collection Engine.
- Flow records are sent from the router to the NetFlow Collection Engine with minimal template information so that the NetFlow Collection Engine can relate the records to the appropriate template.
- Version 9 is independent of the underlying transport (UDP, TCP, SCTP, and so on).

NetFlow Packet Format

- Common header among export versions.
- All but v1 have a sequence number.
- Version specific data field where N records of data type are exported.
- N is determined by the size of the flow definition. Packet size is kept under ~1480 bytes. No fragmentation on Ethernet.

Cisco IOS Configuration

- Configured on each input interface.
- Define the version.
- Define the IP address of the collector (where to send the flows).
- Optionally enable aggregation tables.
- Optionally configure flow timeout and main (v5) flow table size.
- Optionally configure sample rate.

Cisco IOS Configuration

```
interface FastEthernet0/0
 description Access to backbone
 ip address 192.168.0.1 255.255.255.0
 ip route-cache flow
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description Access to local net
 ip address 192.168.2.1 255.255.255.0
 ip route-cache flow
 duplex auto
 speed auto


ip flow-export version 5
ip flow-export destination 192.168.2.2 9996
```

Cisco IOS Configuration

- Change in command in newer IOS

```
interface FastEthernet0/0
 ip route-cache flow      ! Prior to IOS 12.4
 ip flow [ingress|egress]! From IOS 12.4
```

- If CEF is not configured on the router, this turns off the existing switching path on the router and enables NetFlow switching (basically modified optimum switching).
- If CEF is configured on the router, NetFlow simply becomes a "flow information gatherer" and feature accelerator—CEF remains operational as the underlying switching process

Cisco IOS Configuration

```
gw-192-168-2-0#sh ip flow export
Flow export v5 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  192.168.2.2 (9996)
  Version 5 flow records
  55074 flows exported in 3348 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

Cisco IOS Configuration

```
gw-192-168-2-0#sh ip cache flow
IP packet size distribution (3689551 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .483 .189 .014 .002 .003 .001 .000 .000 .000 .000 .000 .000 .000 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .000 .008 .002 .288 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  26 active, 4070 inactive, 55206 added
  1430681 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25800 bytes
  26 active, 998 inactive, 55154 added, 55154 added to flow
  0 alloc failures, 0 force free
  1 chunk, 2 chunks added
  last clearing of statistics never
```

Cisco IOS Configuration

```
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet        3357      0.0        35    92      1.3       0.5      11.5
TCP-FTP            128      0.0        19    97      0.0       0.6       1.5
TCP-FTPD           128      0.0       105   771      0.1       0.2       1.5
TCP-WWW          13462      0.1       125   962     19.3       7.0       5.9
TCP-X              269      0.0         1    40      0.0       0.0      14.3
TCP-other         9107      0.1       154    62     16.1       6.9       8.2
UDP-DNS           2248      0.0         1    73      0.0       0.8      15.4
UDP-NTP           3132      0.0         1    76      0.0       0.0      15.4
UDP-TFTP            24      0.0         6    49      0.0      30.0      15.3
UDP-Frag             6      0.0         1    32      0.0       0.0      15.5
UDP-other         6700      0.0         9   104      0.7       2.2      15.5
ICMP             16661      0.1        23    87      4.5      18.5      15.4
Total:           55222      0.6        66   480     42.3       8.8      11.6

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/1         192.168.2.195   Fa0/0         202.128.0.7     01 0000 0800     4
Fa0/1         192.168.2.195   Fa0/0         218.185.127.204 01 0000 0800     4
Fa0/1         192.168.2.2     Fa0/0         192.168.15.102  06 0016 C917    89
Fa0/1         192.168.2.2     Local         192.168.2.1     06 DB27 0016   120
Fa0/1         192.168.2.195   Fa0/0         202.128.31.179  01 0000 0800     4
Fa0/0         208.81.191.133  Fa0/1         192.168.2.194   06 0050 8452     3
```

Cisco IOS Configuration

```
ip flow-top-talkers
 top 10
 sort-by bytes


gw-192-168-2-0#sh ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Fa0/1         192.168.2.2     Fa0/0         192.168.11.33   06 0050 0B64  3444K
Fa0/1         192.168.2.2     Fa0/0         192.168.11.33   06 0050 0B12  3181K
Fa0/0         192.168.11.33   Fa0/1         192.168.2.2     06 0B12 0050    56K
Fa0/0         192.168.11.33   Fa0/1         192.168.2.2     06 0B64 0050    55K
Fa0/1         192.168.2.2     Local         192.168.2.1     01 0000 0303    18K
Fa0/1         192.168.2.130   Fa0/0         64.18.197.134   06 9C45 0050    15K
Fa0/1         192.168.2.130   Fa0/0         64.18.197.134   06 9C44 0050    12K
Fa0/0         213.144.138.195 Fa0/1         192.168.2.130   06 01BB DC31  7167
Fa0/0         192.168.15.102  Fa0/1         192.168.2.2     06 C917 0016  2736
Fa0/1         192.168.2.2     Local         192.168.2.1     06 DB27 0016  2304
10 of 10 top talkers shown. 49 flows processed.
```

Cisco command summary

- Enable CEF
  - `ip cef`
- Enable flow on each interface

```
ip route cache flow OR
ip flow ingress
ip flow egress
```

- View flows
  - `show ip cache flow`
  - `show ip flow top-talkers`

Cisco Command Summary

- Exporting Flows to a collector

```
ip flow-export version 5 [origin-as|peer-as]
ip flow-export destination x.x.x.x <udp-port>
```

- Exporting aggregated flows

```
ip flow-aggregation cache as|prefix|dest|source|proto
  enabled
  export destination x.x.x.x <udp-port>
```

Fault & problem management

- Is it transient ?
  - Overload, temporary resource shortage
- Is it permanent ?
  - Equipment failure, link down
- Error detection ?
  - Monitoring!
  - Customer complaints
- Log Log Log….
  - Open ticket to track an event (planned or failure)
  - Define dispatch/escalation rules
    - Who handles the problem ?
    - Who gets it next if no one is available ?

Configuration Management

- Record changes to equipment configuration, using *revision control (also for configuration files)*
- *Inventory management (equipment, IPs, interfaces, etc.)*
- *Use version control!*
  - *As simple as: ”cp named.conf named.conf.20070827-01”*
- *For plain configuration files:*
  - *CVS, Subversion*
  - *Mercurial*

Configuration Management

- *Traditionally, used for source code (programs)*
- *Works well for any text-based configuration files*
  - *Also for binary files, but less easy to see differences*
- *For network equipment:*
  - *RANCID (Automatic Cisco configuration retrieval and archiving, also for other equipment types)*
  - *Archive (Cisco IOS feature)*

Archiving

- Cisco IOS archive command can help you automatically save configuration after every change.
- This command can also show you the difference between any two configurations saved.
- These archives can also be created manually as per requirement.
- This command can also be used to automatically log all commands entered by any user.
- This command was introduced with IOS 12.3(4)T. Later it was integrated into IOS Release 12.2(25)S.

Archiving : Cisco IOS Command

```
Router(config)# archive
Router(config-archive)#?
```

Archive configuration commands:

default	Set a command to its defaults
exit	Exit from archive configuration mode
log	Logging commands
maximum	maximum number of backup copies
no	Negate a command or set its defaults
path	path for backups
time-period	Period of time in minutes to automatically archive the running-config
write-memory	Enable automatic backup generation during write memory

Archiving: Example

- In case you want to archive configuration on an ftp server than following configuration will be used. This will backup config on every “write mem” and periodically after every 15 days.

- ip ftp username sanog
- ip ftp password testing
- archive
- path ftp://202.163.x.x/switchesconfig/$h
- write-memory
- time-period 21600

Archiving: Example

- Router #show archive
- The next archive file will be named ftp://202.163.x.x/switchesconfig/asw01-cc-syb-8flr-14
- Archive # Name
- 0
- 1 ftp://202.163.x.x/switchesconfig/asw01-cc-syb-8flr-1
- 2 ftp://202.163.x.x/switchesconfig/asw01-cc-syb-8flr-2
- 3 ftp://202.163.x.x/switchesconfig/asw01-cc-syb-8flr-3
- 4 ftp://202.163.x.x/switchesconfig/asw01-cc-syb-8flr-4
- 5 ftp://202.163.x.x/switchesconfig/asw01-cc-syb-8flr-5
- 6 ftp://202.163.x.x/switchesconfig/asw01-cc-syb-8flr-6
- 7 ftp://202.163.x.x/switchesconfig/asw01-cc-syb-8flr-7
- 8 ftp://202.163.x.x/switchesconfig/asw01-cc-syb-8flr-8
- 9 ftp://202.163.x.x/switchesconfig/asw01-cc-syb-8flr-9
- 10 ftp://202.163.x.x/switchesconfig/asw01-cc-syb-8flr-10
- 11 ftp://202.163.x.x/switchesconfig/asw01-cc-syb-8flr-11
- 12 ftp://202.163.x.x/switchesconfig/asw01-cc-syb-8flr-12
- 13 ftp://202.163.x.x/switchesconfig/asw01-cc-syb-8flr-13 <- Most Recent

Log Management

- What is log management and monitoring ?
- It's about keeping your logs in a safe place, putting them where you can easily inspect them with tools
- Keep an eye on your log files
- They tell you something important…
  - Lots of things happen, and someone needs to keep an eye on them…
  - Not really practictal to do it by hand!

Log Management

- On your routers and switches
  - Nov 12 17:28:44.301 PKT: %BGP-5-ADJCHANGE: neighbor 192.168.241.44 Down BGP Notification sent
  - Nov 12 17:28:44.301 PKT: %BGP-3-NOTIFICATION: sent to neighbor 192.168.241.44 4/0 (hold time expired) 0 bytes
  - Nov 12 18:28:47.036 PKT: %BGP-5-ADJCHANGE: neighbor 192.168.0.50 vpn vrf maha-sec Down BGP Notification sent
  - Nov 12 18:28:47.036 PKT: %BGP-3-NOTIFICATION: sent to neighbor 192.168.0.50 4/0 (hold time expired) 0 bytes
  - Nov 12 18:43:21.066 PKT: %LDP-5-NBRCHG: LDP Neighbor 58.65.219.254:0 (1) is DOWN (Session KeepAlive Timer expired)
  - On your servers as well
  - Aug 31 17:53:12 ubuntu nagios2: Caught SIGTERM, shutting down...
  - Aug 31 19:19:36 ubuntu sshd[16404]: Failed password for root from 192.168.1.130 port 2039 ssh2

Log Management

- First, need to centralize and consolidate log files
- Log all messages from routers, switches and servers to a single machine – a logserver
- All logging from network equipment and UNIX servers is done using syslog
- Windows can be configured to use syslog as well, with some tools
- Log locally, but also to the central server

Configuring centralized logging

- Cisco equipment
  - Minimum:
    - logging <ip.of.log.host>
- UNIX host
  - Edit /etc/syslog.conf
  - Add a line ”*.*   @ip.of.log.host”
  - Restart syslogd
- Other equipments have similar options
  - Options to control facility and level

Questions ?

?