Information Network 1
Network management

2012/5/25

Youki Kadobayashi

NAIST 奈良先端科学技術大学院大学

Network management

- Physical management
  - power supply, cabling, cooling, ...
- Configuration management
  - logical configuration of routers, hosts...
- Performance management
  - achieved bandwidth, observed loss rate...
- Operation management
  - operators assignment, day/night shift...

Network management matrix

	Planned	Measured	Analyzed	Improved
Physical management				
Configuration management				
Performance management				
Operation management				

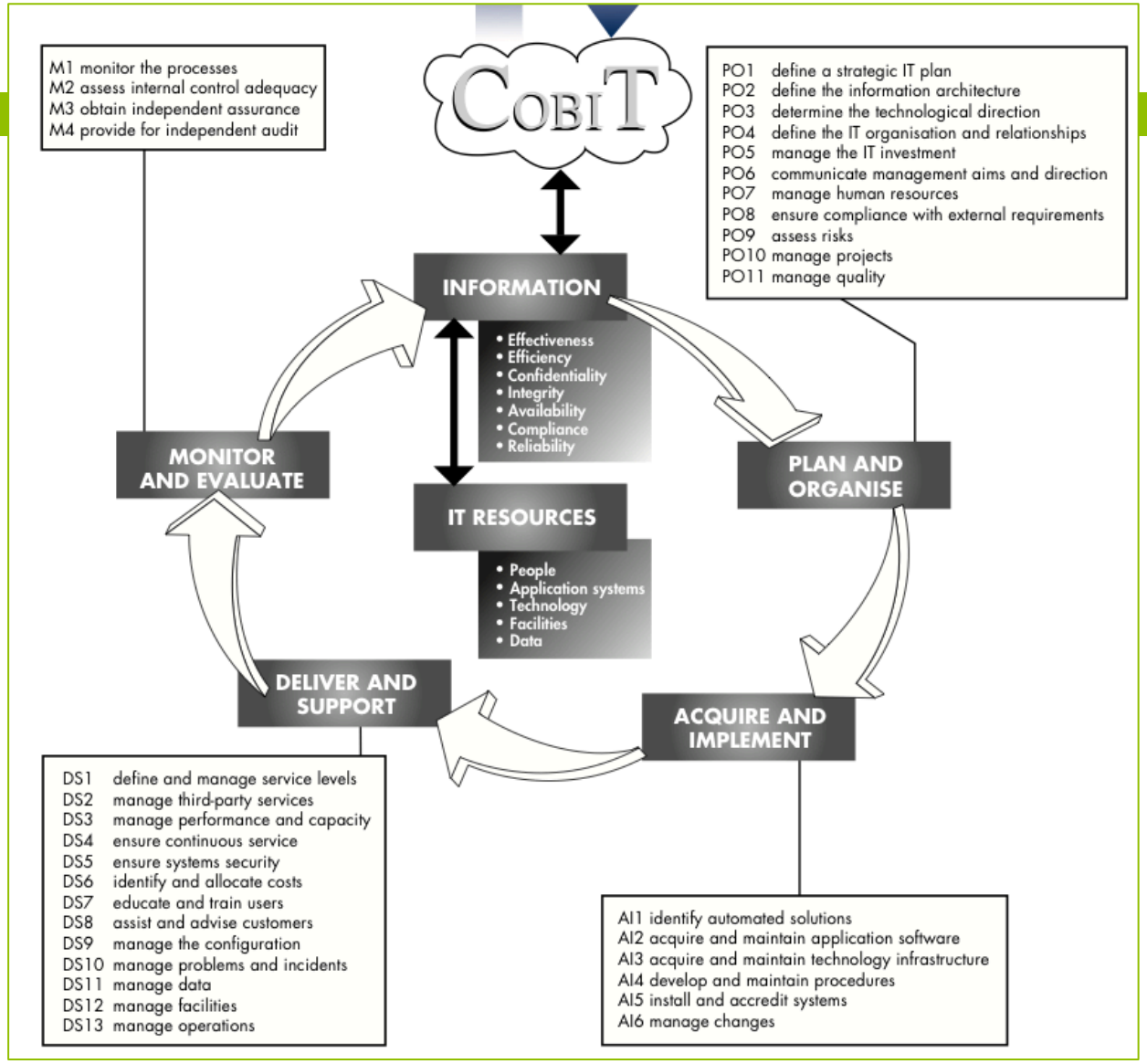
Issue tracking

 12/05/25

Focus of this lecture

	Planned	Measured	Analyzed	Improved
Physical management				
Configuration management				
Performance management				
Operation management				

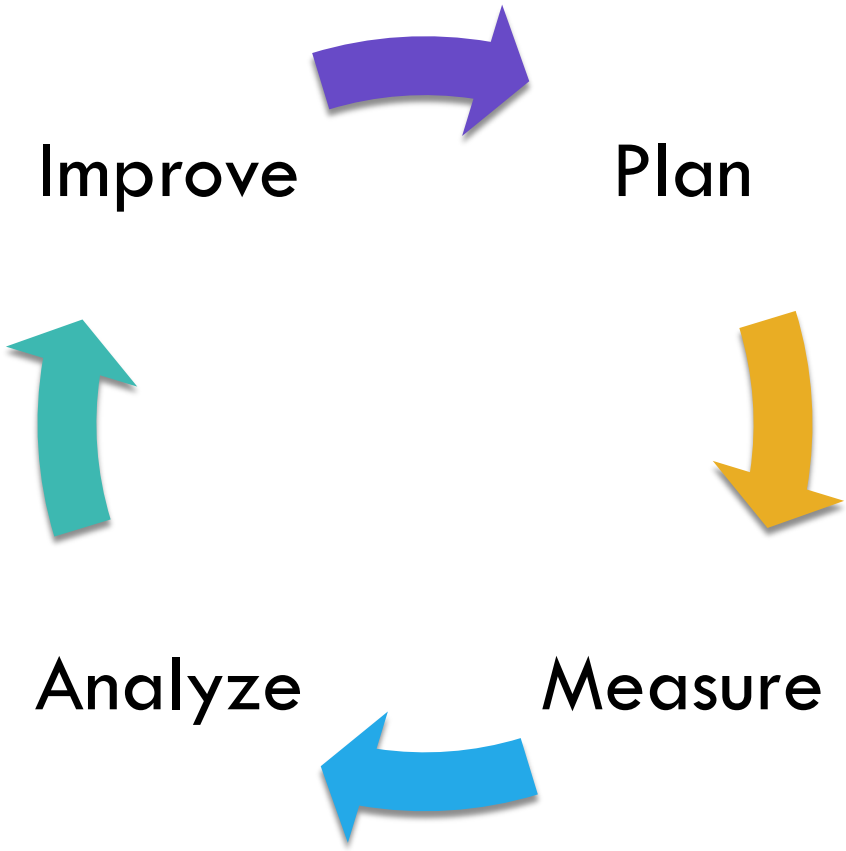
Network management in broader context: COBIT



Source:
COBIT Student Book, ITGI, available online.

Management lifecycle

- PDCA etc.



 12/05/25

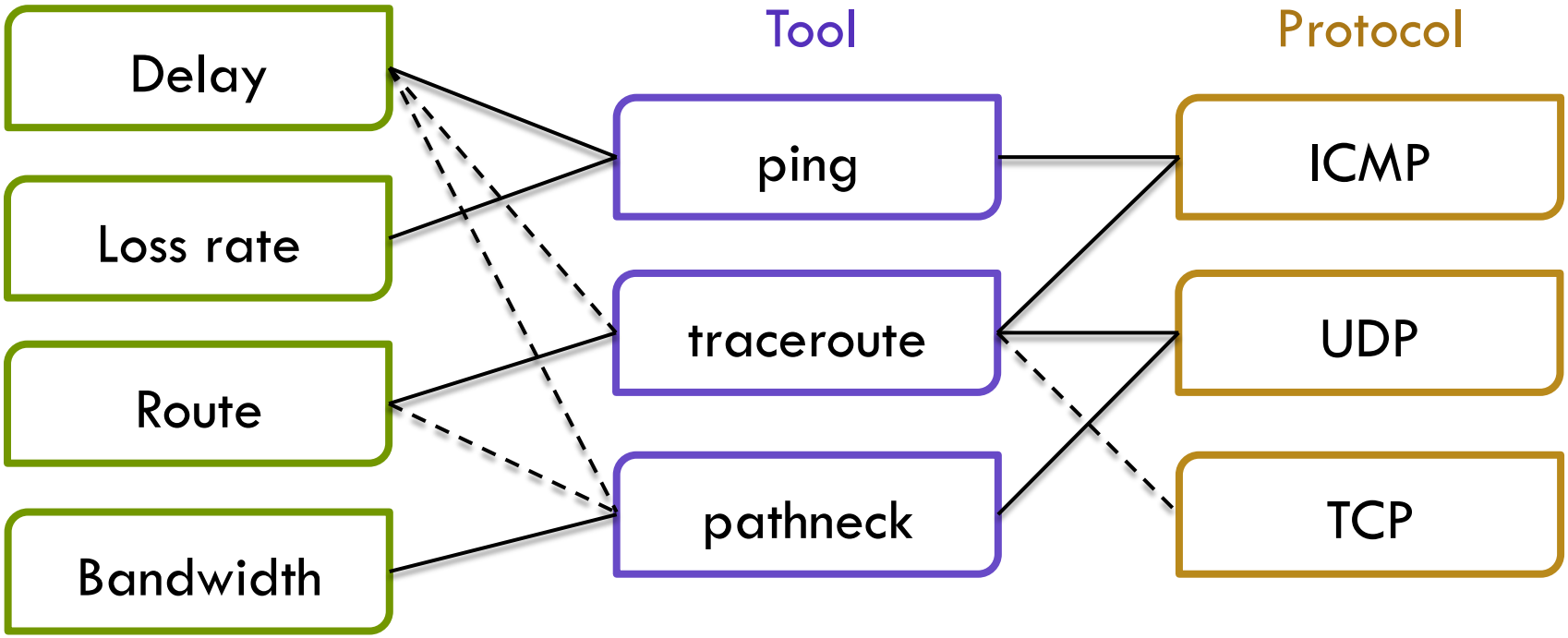
Key question

- How do we
  - plan for measurement?
  - measure state of the network?
  - detect and analyze problems?
  - improve the network?

Planning for measurement

	Active	Passive
End-to-end measurements		
Bandwidth	x	
Loss rate	x	
Delay	x	
Route	x	
Link-level measurements		
Bandwidth	x	x
Loss rate	x	x
Delay	x	
Route		x

End-to-end measurements



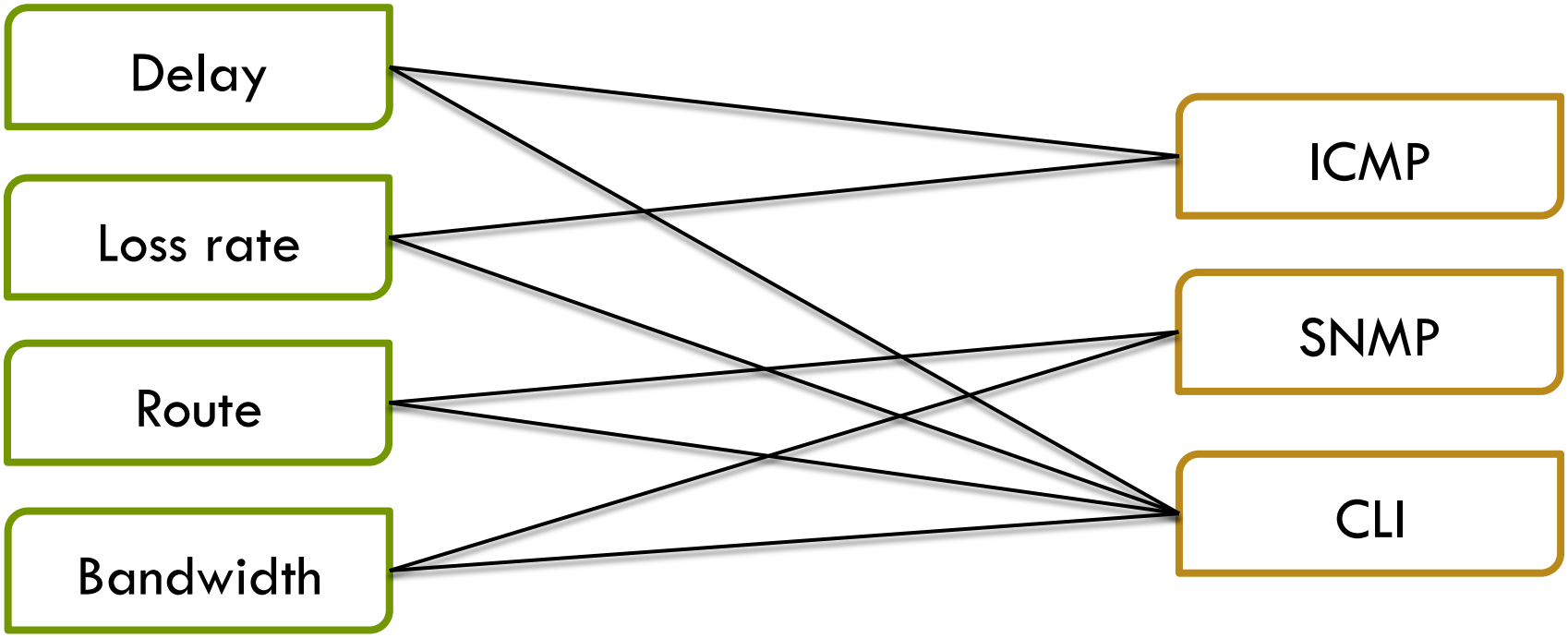
- Most of them are active
- Key design goal: minimum interference

End-to-end measurements: some examples

```
$ ping www.naist.jp
PING supernova.naist.jp (163.221.80.83): 56 data bytes
64 bytes from 163.221.80.83: icmp_seq=0 ttl=53 time=27.834 ms
64 bytes from 163.221.80.83: icmp_seq=1 ttl=53 time=17.071 ms
64 bytes from 163.221.80.83: icmp_seq=2 ttl=53 time=29.268 ms
^C
--- supernova.naist.jp ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 17.071/24.724/29.268/5.443 ms
```

```
$ traceroute www.k-opti.com
traceroute to www.k-opti.com (203.140.81.118), 64 hops max, 52 byte packets
 1  10.0.0.1 (10.0.0.1)  7.982 ms  0.743 ms  0.686 ms
 2  60.56.32.27 (60.56.32.27)  22.038 ms  22.145 ms  33.347 ms
 3  218.251.84.69 (218.251.84.69)  14.742 ms  10.565 ms  24.549 ms
 4  60.56.20.57 (60.56.20.57)  24.770 ms  7.168 ms  25.485 ms
 5  58.191.151.246 (58.191.151.246)  24.471 ms  9.047 ms  24.963 ms
 6  www.k-opti.com (203.140.81.118)  27.681 ms  32.329 ms  21.803 ms
```

Link-level measurements



- Most of them are passive
- Key design goal: reveal as much info as possible

 12/05/25

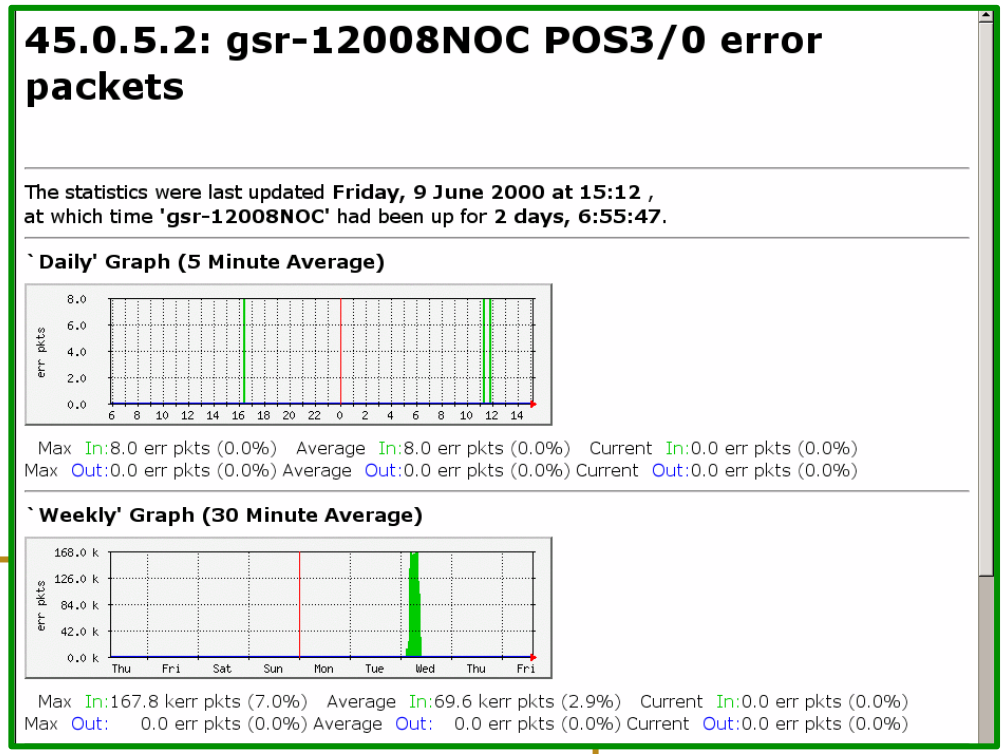
Link-level measurements: some examples

Loss rate
# of packets sent/received
Types of errors

CLI

show int Ether4/0 errors

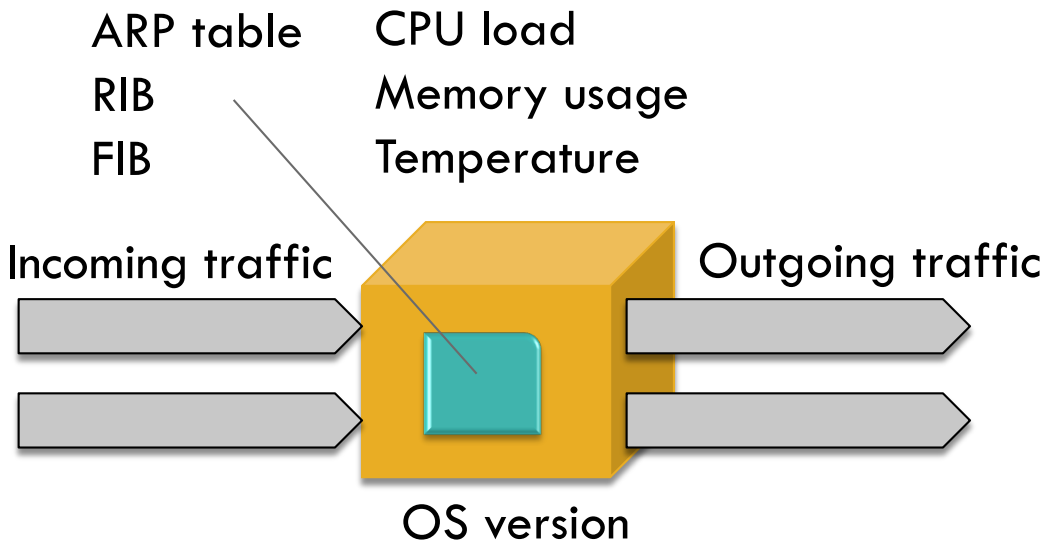
Ether4/0
  Internet address is 192.168.102.2/27
    412482 packets input, 101939884 bytes, 0 no buffer
    Received 43093 broadcasts, 8 runts, 0 giants
    69 input errors, 0 CRC, 61 frame, 0 overrun, 23 ignored, 0 abort



SNMP

 12/05/25

Challenges in the measurement of the state of network

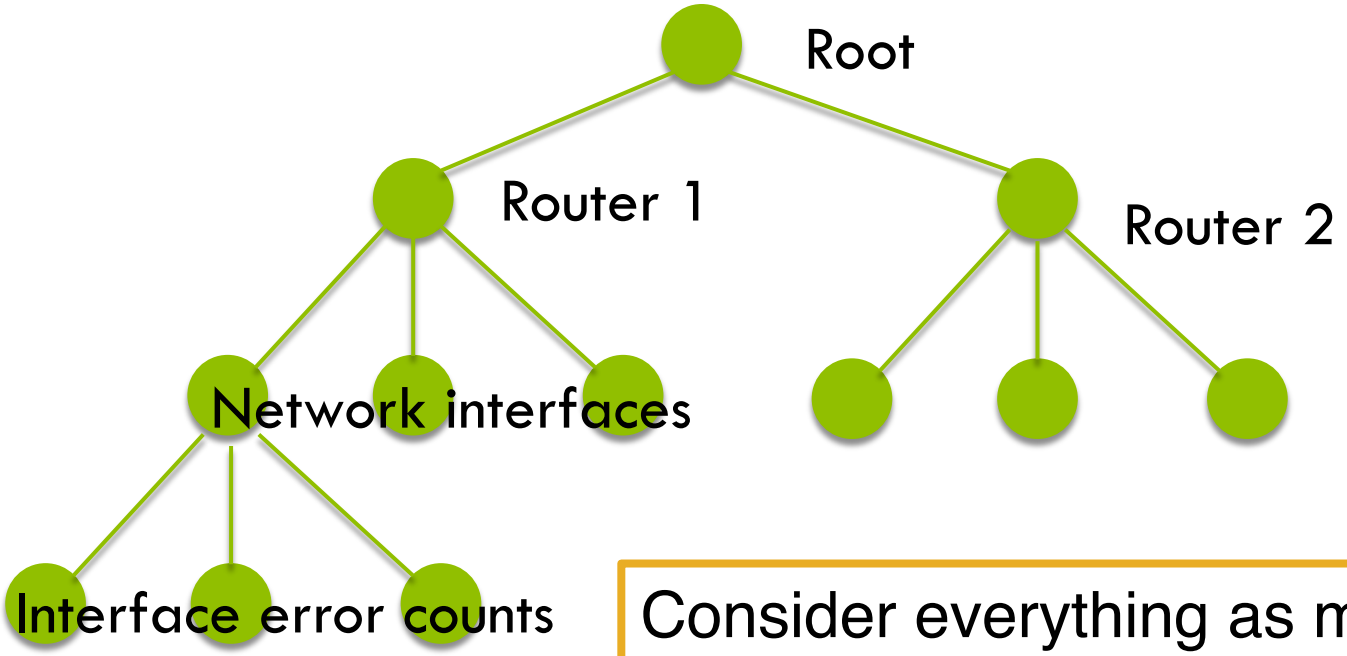


- Many data types
  - Number, string, array, IP address…
- Many measurement targets
  - Hundreds of interfaces, dozens of routers…

 12/05/25

Management Information Base (MIB)

- Key idea: organize managed information under a tree

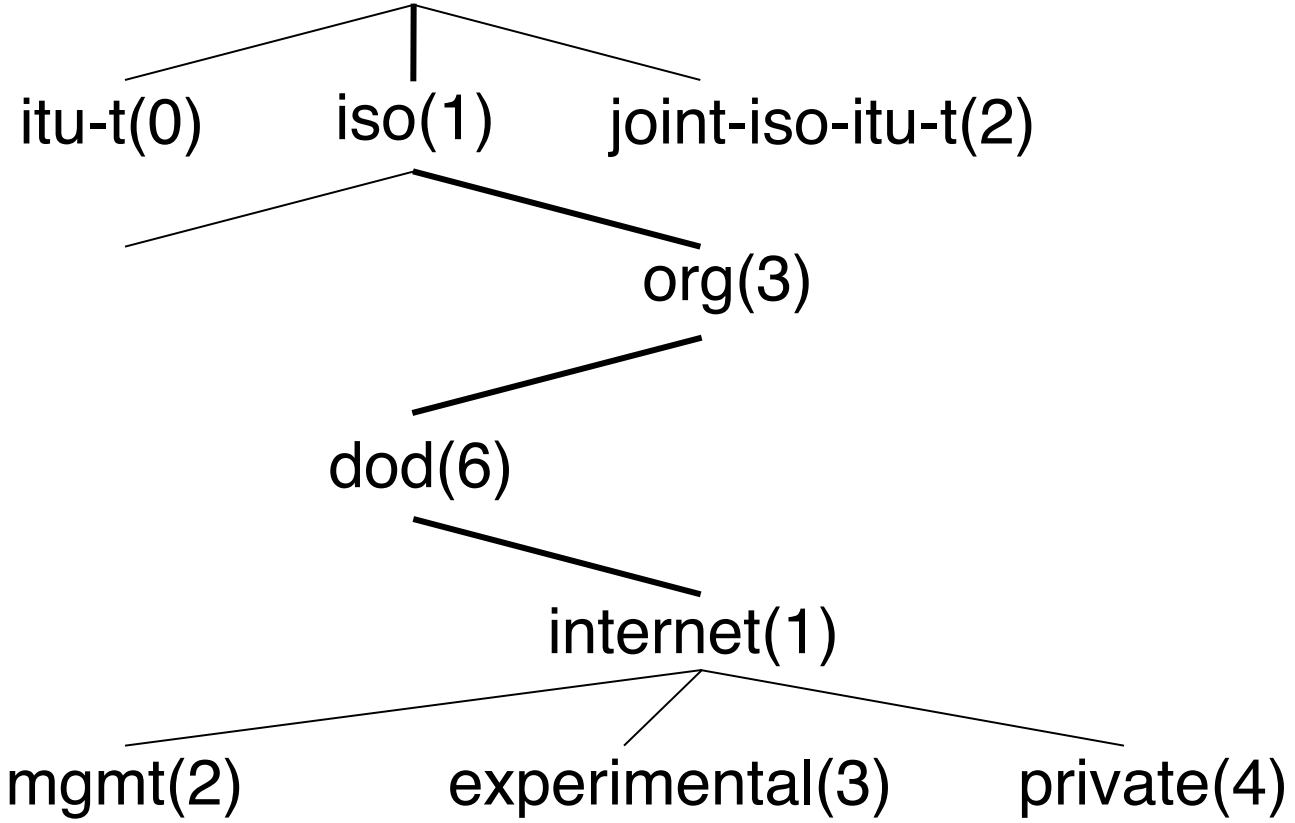


Consider everything as managed objects
Assign **object identifier** to every object

 12/05/25

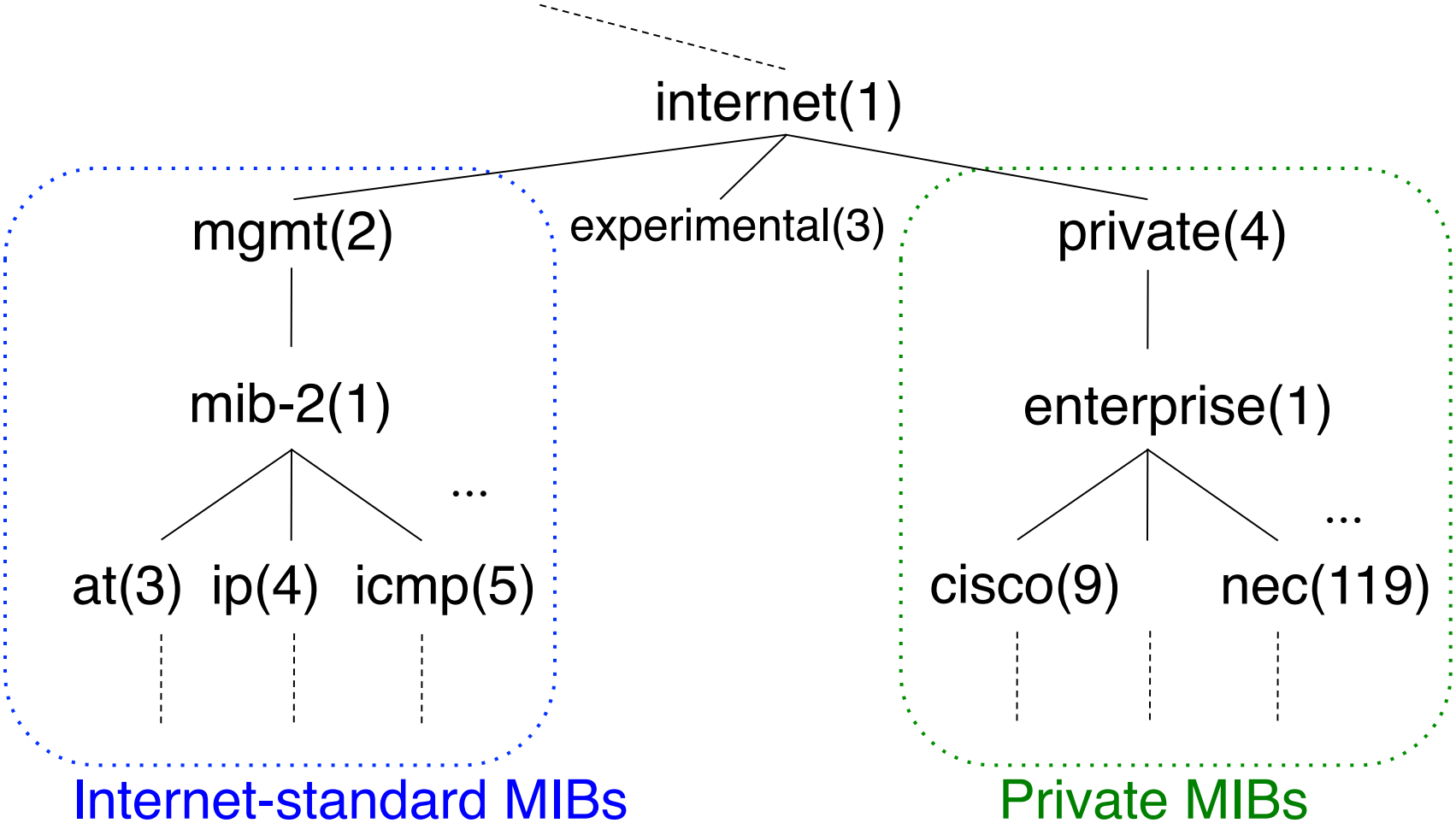
Object Identifier for the Internet

under the International standard OID root



 12/05/25

MIBs represent standard set of managed objects, as well as vendor-specific ones



 12/05/25

Inside 1.3.6.1.2.1: Standard MIBs (MIB-II)

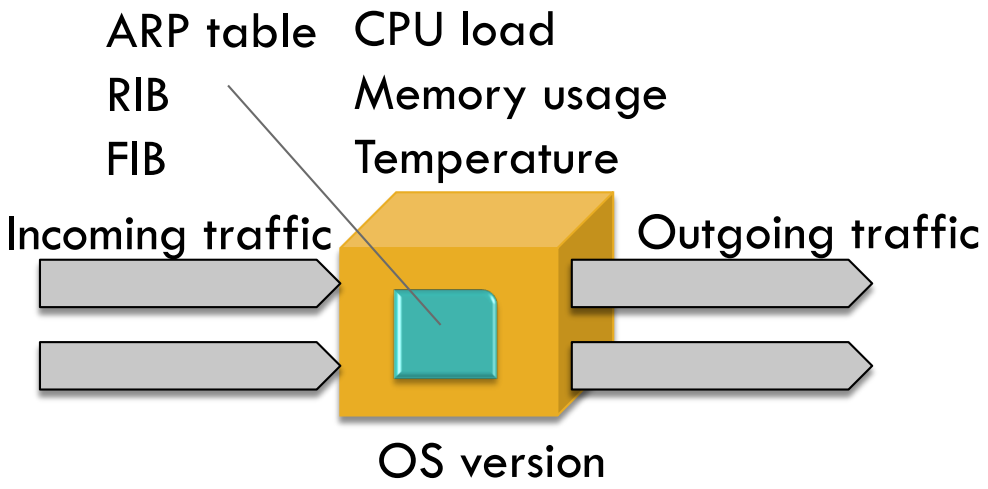
Sibling	ID	Usage examples
system	1	OS version
interfaces	2	Number of packets sent / received
at	3	ARP table
ip	4	Interface IP address, Routing table
icmp	5	ICMP message counts by type
tcp	6	TCP packet counts, errors, connection table
udp	7	UDP packet counts, errors
transmission	10	Statistics for datalink
snmp	11	SNMP packet counts, errors

These are actually defined in RFCs 1213, 2011, 4022, 4113: “Management Information Base for Network Management of TCP/IP-based internets: MIB-II”

More MIBs under mib-2 tree

Sibling	ID	Type of MIB	Defined in
ospf	14	OSPF MIB	RFC 1253
bgp	15	BGP MIB	RFC 4273
bridge	17	Bridge MIB	RFC 4188
ifMIB	31	Interface MIB	RFC 2863
ipv6MIB	55	IP version 6 MIB	RFC 2465

Result:
These measurements can be represented by standard MIBs



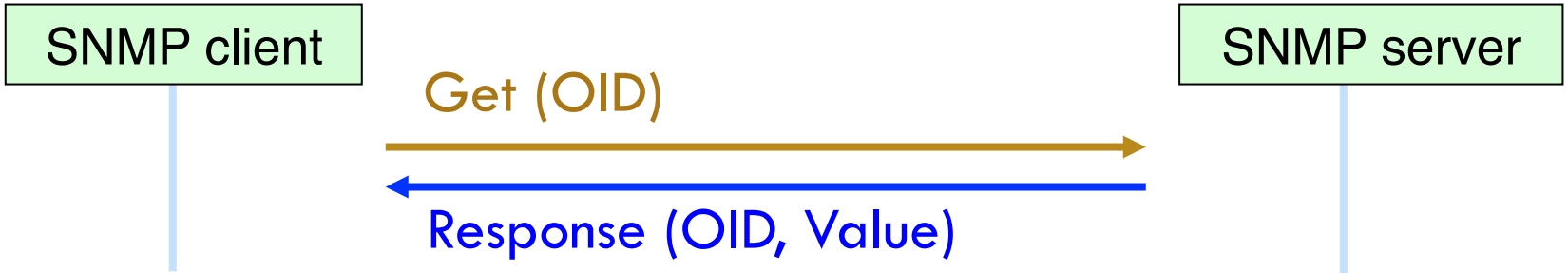
Representing many kinds of data: ASN.1

ITU-T X.680: Information technology – Abstract Syntax Notation One (ASN.1)

- A variant of (tag, length, value)
  - tag: ASN.1 type
  - length: size of the ASN.1 value
  - value: ASN.1 value
- Data types in ASN.1
  - INTEGER
  - OCTET STRING
  - OBJECT IDENTIFIER
  - SEQUENCE (array)

SNMP conveys MIBs

Simple Network Management Protocol version 2, RFC1448



- SNMP characteristics
  - Data types: defined in ASN.1, SMIv2
    - "Structure of Management Information Version 2 (SMIv2)" - RFC2578
  - OID space management: MIB tree + IANA Registry
    - http://www.iana.org/assignments/smi-numbers
  - Rich set of tools: libraries, management tools

 12/05/25

SNMP example: net-snmp

```
# snmptranslate -On -IR sysDescr
.1.3.6.1.2.1.1.1
```

OID hierarchy from the root

```
# snmptranslate -Onf -IR sysDescr
.iso.org.dod.internet.mgmt.mib-2.system.sysDescr
```

Object names from the root

```
# snmptranslate -Td -IR sysDescr
SNMPv2-MIB::sysDescr
sysDescr OBJECT-TYPE
  -- FROM       SNMPv2-MIB, RFC1213-MIB
  -- TEXTUAL CONVENTION DisplayString
  SYNTAX       OCTET STRING (0..255)
  DISPLAY-HINT  "255a"
  MAX-ACCESS    read-only
  STATUS       current
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) system(1) 1 }
```

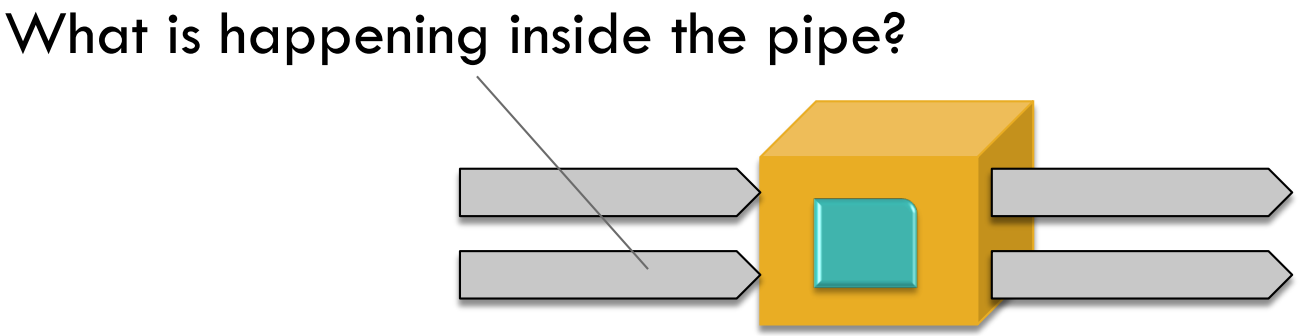
Data type definition of the object

```
# snmpgetnext -IR -v 1 -c sample 203.178.142.3 sysDescr
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Internetwork Operating System Software
IOS (tm) GS Software (GSR-P-M), Experimental Version 12.0(20020720:053512) [akr-v3-isp2 105]
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Fri 09-Aug-02 22:07 by akr
```

Actual value associated with the object

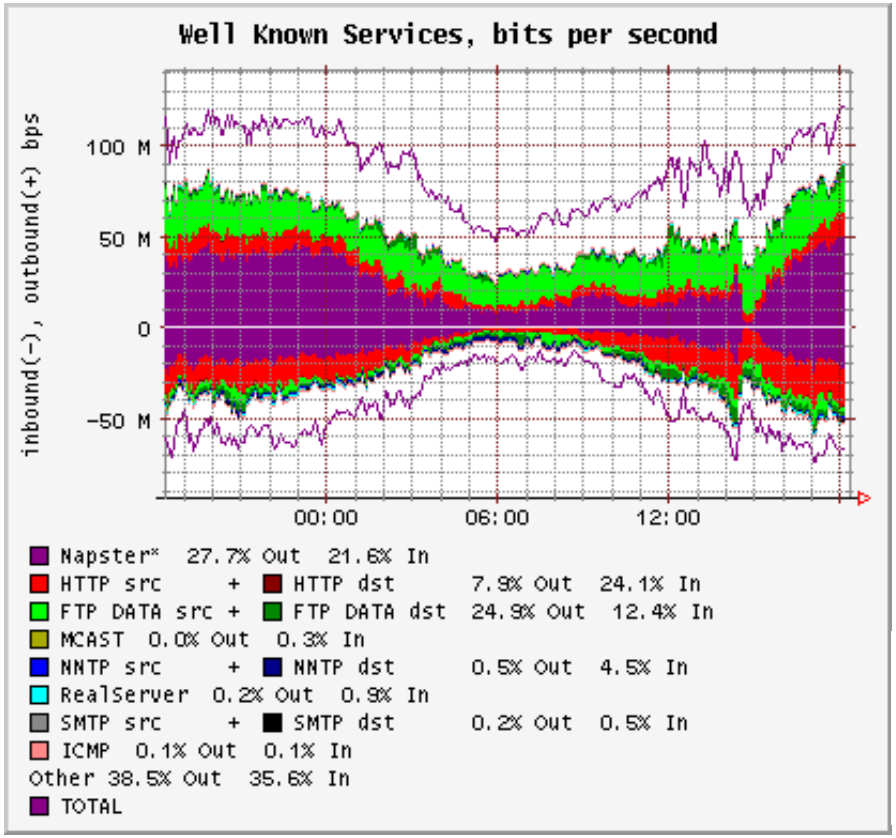
The need for more fine-grained measurement

- Fair-share principle is only ideal
  - Alpha flows (big experiments, events, …)
  - Buggy devices
  - Misconfigurations
  - Attacks



Packet and flow sampling

- sFlow (RFC3176), PSAMP (RFC5476)
- NetFlow (RFC3954)



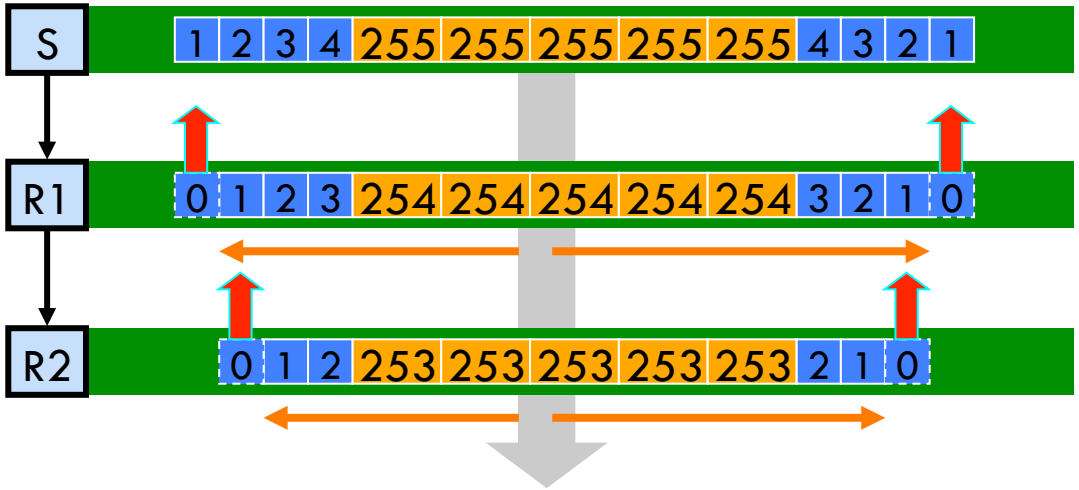
Source: FlowScan -- Network Traffic Flow Visualization and Reporting Tool, CAIDA

How do we detect and analyze problems?

- Bottleneck point?
- Surge of traffic?

Detecting and analyzing bottleneck

Pathneck (N. Hu et al., SIGCOMM'04)

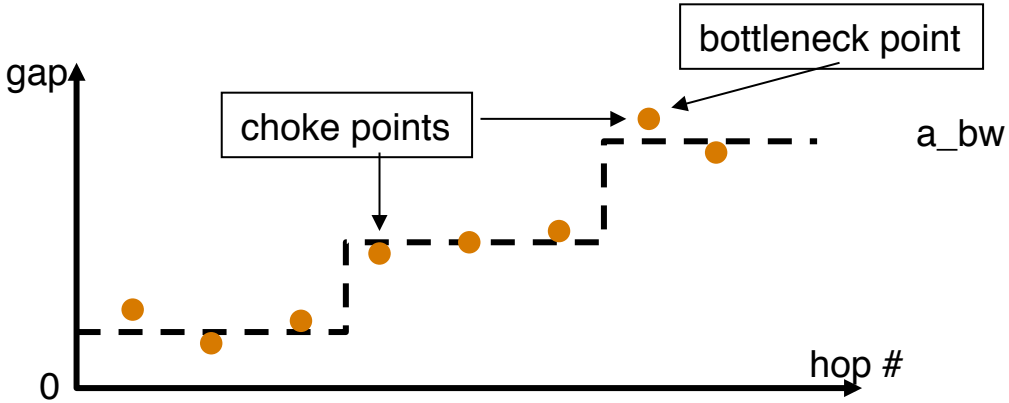


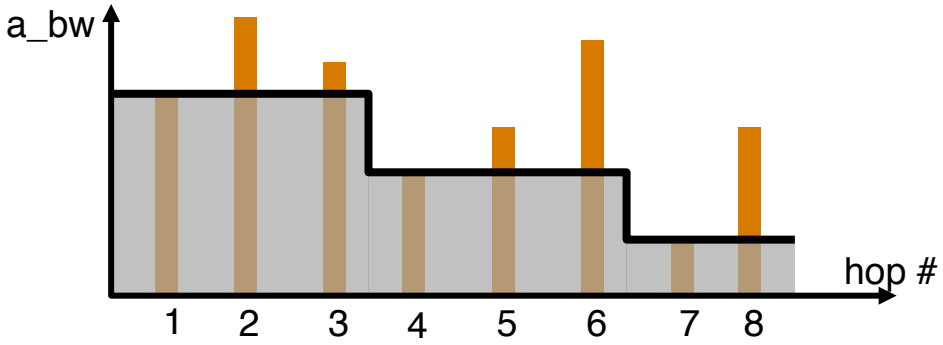
Recursive Packet Train:

- Load packets (orange)
- Measurement packets (blue)

with different TTLs.

ICMP time exceed message from head & tail of the train.





 12/05/25

Detecting and analyzing bottleneck

Pathneck (N. Hu et al., SIGCOMM'04)

- Actual measurement results from pathneck
  - Note: tool claims ~70% accuracy; result not verified

```
$ ./pathneck -xo ftp.isi.edu
1306302074.013198 128.9.176.20 500 60 0
(...)
     RTT    IP               gap   gap-s c  est.bw
05   1.319 203.178.136.169   2751   2722 1  87.237 ub ve-7.cisco2.dojima.wide.ad
.jp
06   9.986 203.178.136.237   2722   2722 .  88.170 lb ve-61.cisco2.notemachi.wid
e.ad.jp
07   9.943 203.178.133.141   2722   2722 .  88.170 lb apan-jp.t-lex.net
08 123.764 192.203.116.145   2582   2582 2   0.000 uk losa-tokyo-tp2.transpac2.n
et
09 123.963 207.231.240.129   2495   2495 .  96.190 lb cenichpr-1-lo-jmb-702.lsan
ca.pacificwave.net
10 126.192  137.164.27.254    659   2365 3   0.000 uk 137.164.27.254
11 124.773    198.32.16.29   2365   2365 . 101.475 lb 198.32.16.29
conf = 0.125 0.054 0.055

rtt = 124.806 ( 128.9.176.20 )
```


Detecting and analyzing surge of traffic

Mark Crovella et al., "Diagnosing Network-Wide Traffic Anomalies", SIGCOMM 2004

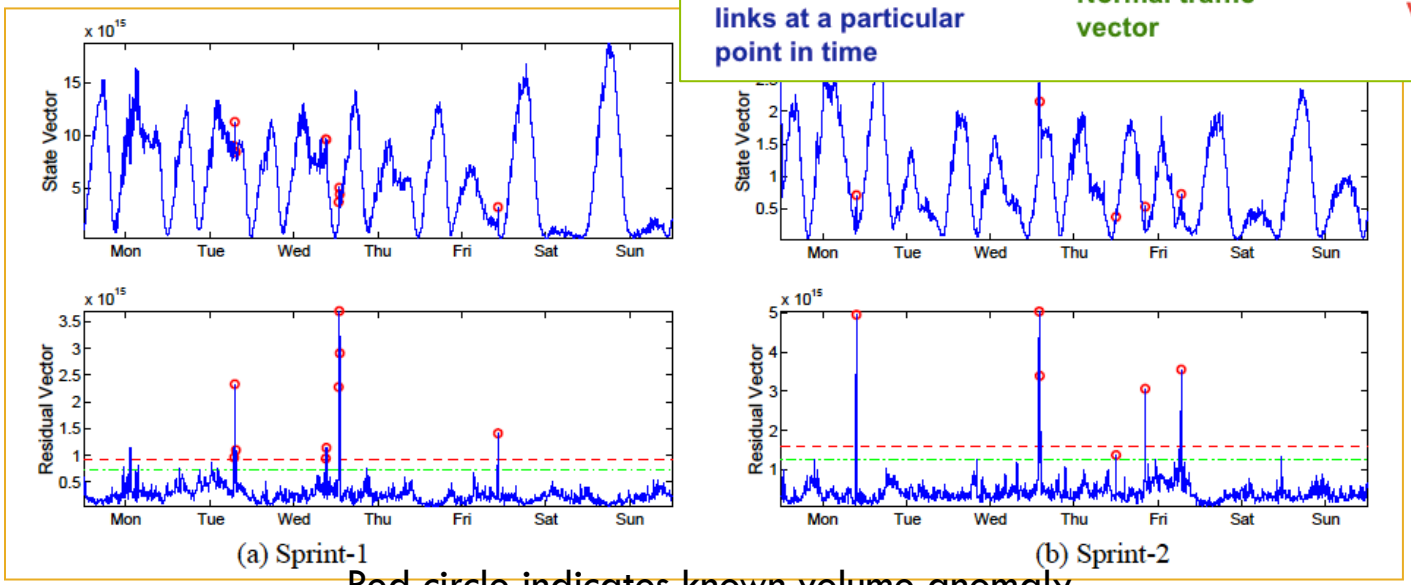
- Employ PCA to delineate normal traffic from anomalous traffic
  - Preprocessed with EWMA, Fourier

$$\mathbf{y} = \hat{\mathbf{y}} + \tilde{\mathbf{y}}$$

Traffic vector of all links at a particular point in time

Normal traffic vector

Residual traffic vector



Red circle indicates known volume anomaly.

 12/05/25

Summary

- Network management and ICT management
- Performance management
- Information model for network management
  - MIB
- Analysis of collected information

