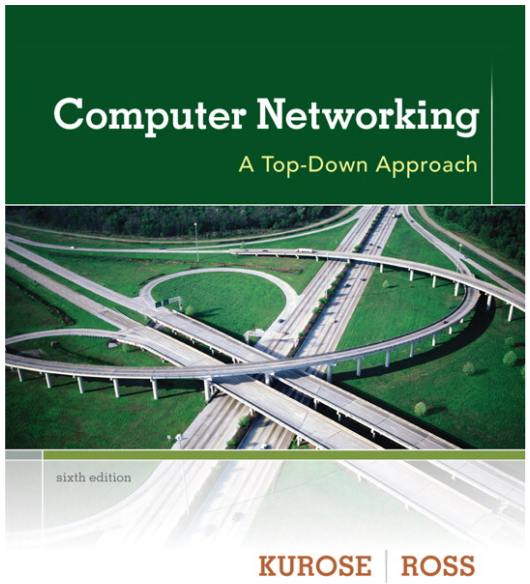
Chapter 9
Network Management



Computer Networking: A Top Down Approach
6th edition
Jim Kurose, Keith Ross
Addison-Wesley
March 2012

A note on the use of these ppt slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

Chapter 9: Network Management

Chapter goals:

- introduction to network management
  - motivation
  - major components
- Internet network management framework
  - MIB: management information base
  - SMI: data definition language
  - SNMP: protocol for network management
  - security and administration
- presentation services: ASN.1

What's UP?

- Can't access Facebook
- Can't access IITH web site
- Can't receive an e-mail
- Can't join VC session
- Remote login to lab server fails
- Paper download from IEEE fails

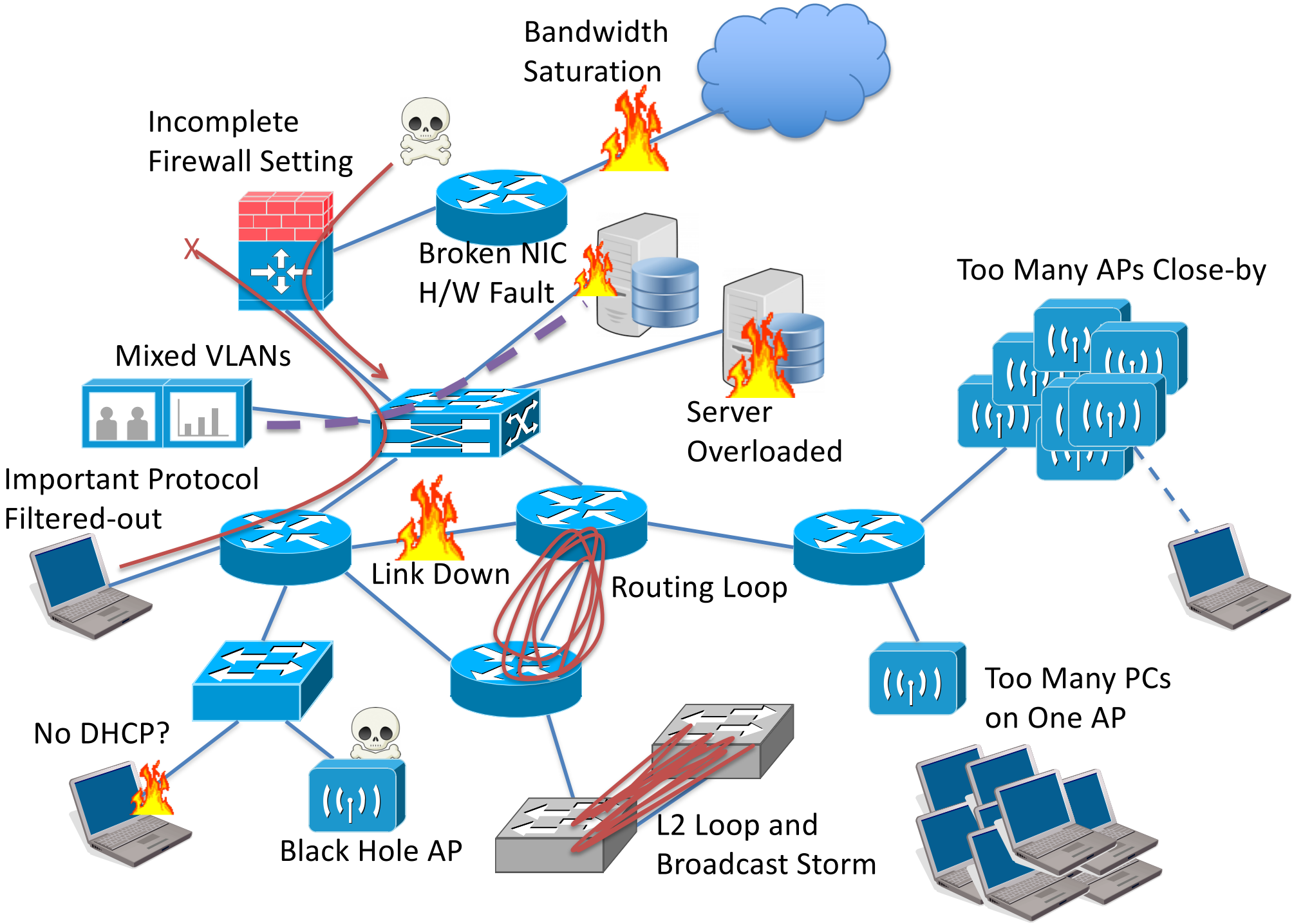
  …

  …
- Can't share a file with PC in next room

  …
- Anyway, network is sooooooooo slow
- Looks trouble, but no idea what's happening and who is on troubleshooting

Network gets disrupted

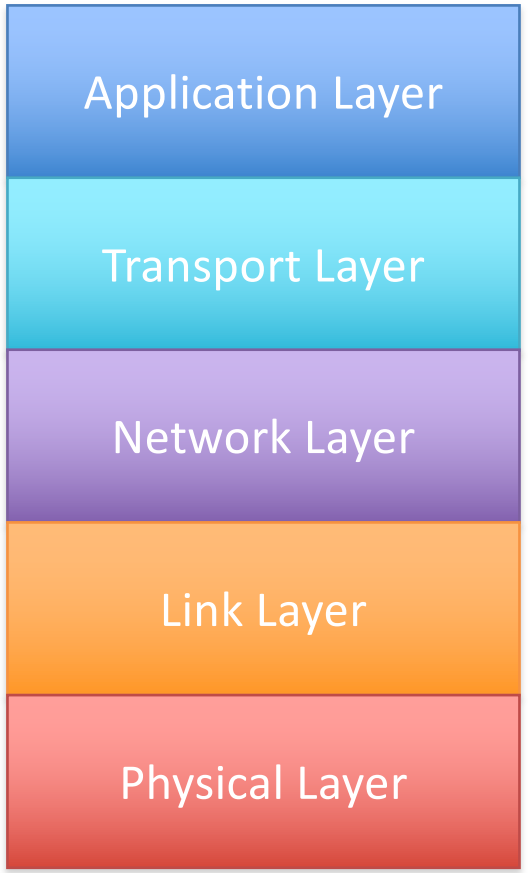
- Why?
  - Networking software has bugs
  - Networking hardware has its life time
  - People make mistakes
  - Systems have upper limit of performance
  - Bandwidth is limited and not free of charge
  - Network is always exposed to attackers and malwares
  - Natural disaster happens
  - Infrastructures are not perfect


Bandwidth
Saturation
Incomplete
Firewall Setting
X
Broken NIC
H/W Fault
Too Many APs Close-by
Mixed VLANs
Server
Overloaded
Important Protocol
Filtered-out
Link Down
Routing Loop
No DHCP?
Too Many PCs
on One AP
Black Hole AP
L2 Loop and
Broadcast Storm

Trouble?

- What is Happening?
- Where the trouble happens?
- Why and how does it happens?
- Since when did it happen?

- Can’t access to Google
  - Is your proxy setting correct?
  - Is TCP connection to proxy established?
  - Can your PC reach proxy?
  - Can proxy reach Facebook?
  - Does your PC have an appropriate IP address?
  - Are your PC really connected to LAN?



Long Way Before Troubleshooting

- Plan service and population
- Estimate required resource with appropriate capacity margin
- Design and implement networks
- Monitor service and network
- Know the normal situation
- Distinguish anomalies (Here we know a trouble!!)

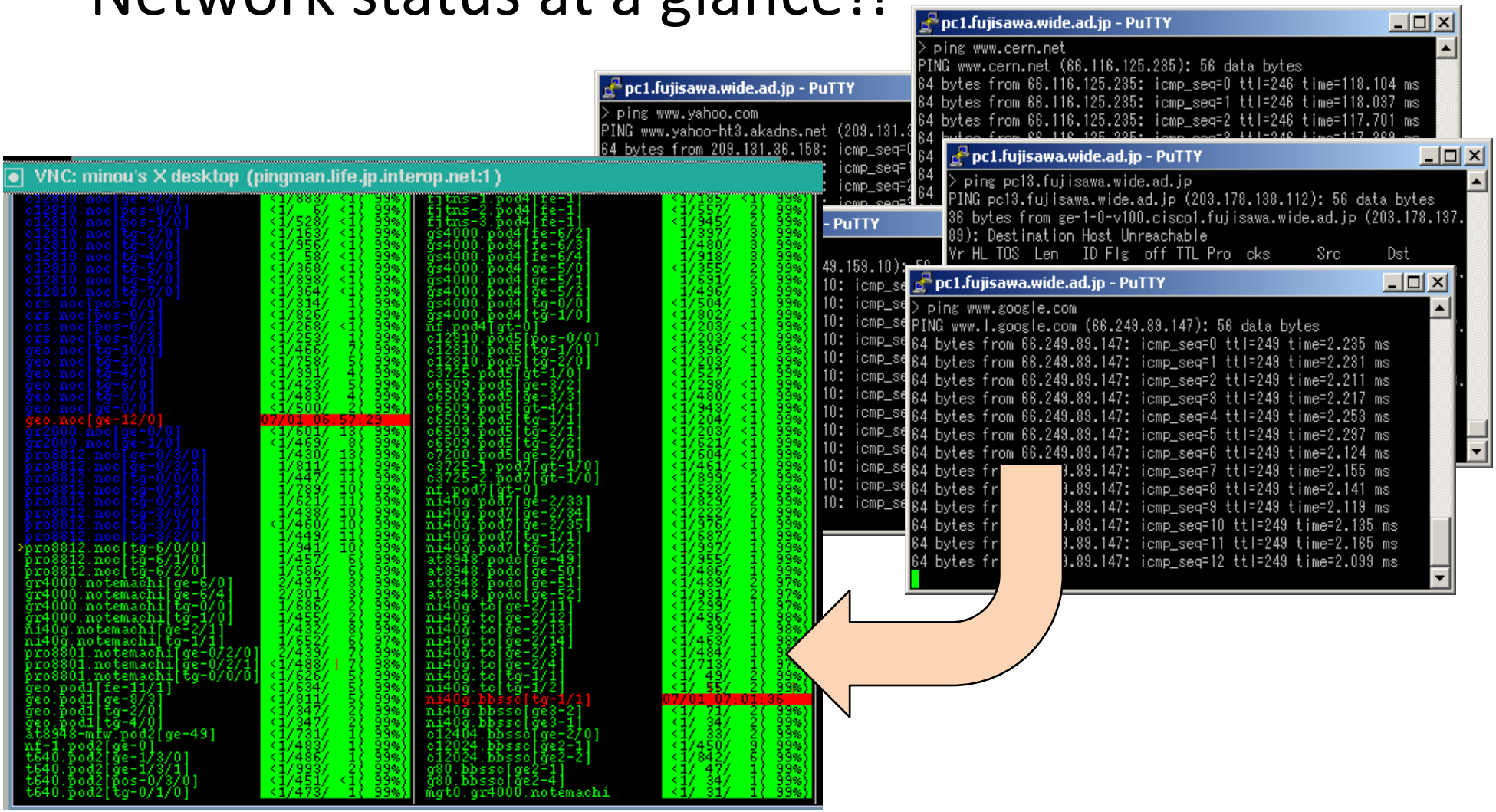
Very Basic Troubleshooting Tools

- ping
  - Does packet reach the destination and come back?
  - How long is RTT (Round-trip Time)?

- traceroute
  - Which path does packet go towards the destination?
  - Where it takes long time to pass through in the?
  - Helps to detect routing loop

Why is Visualizing Data Important?

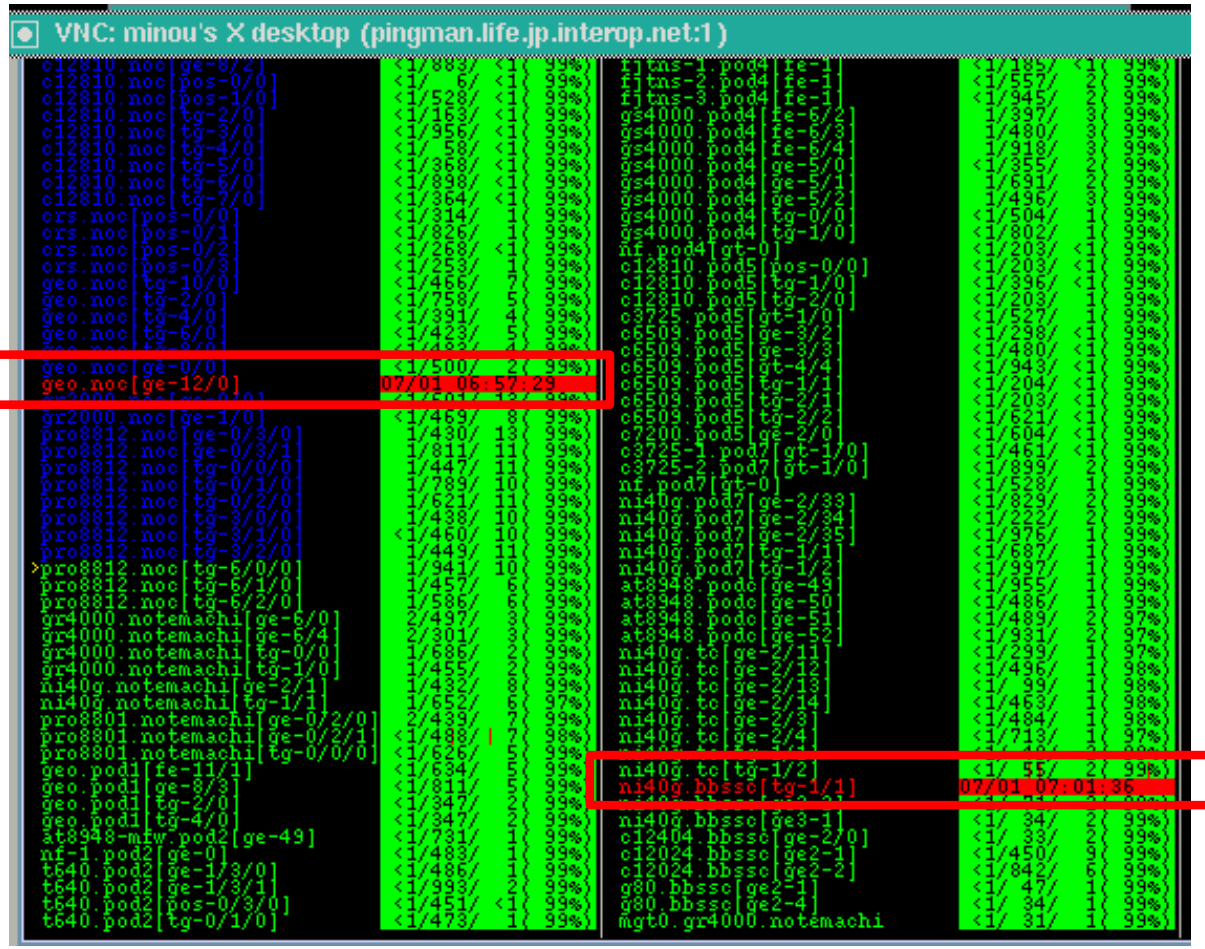
- Network status at a glance!!



Multi-point Monitoring

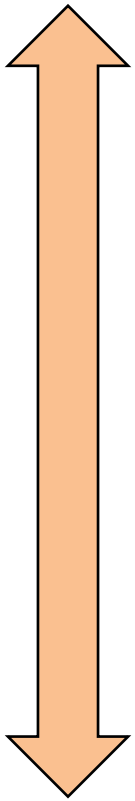
- Rough Monitoring (wide and many)
  - Reachability
  - Delay
  - Jitter
- Then we go for more details

Pingman



Granularity of Information

- Is service available?
- Is reachable?
- Is routing correct?
- Is topology correct?
- Is quality fine?
  - RTT, Jitter, Packet Loss
  - Throughput
- Is the contents of packet normal?



Rough and Low Cost

Preliminary Survey

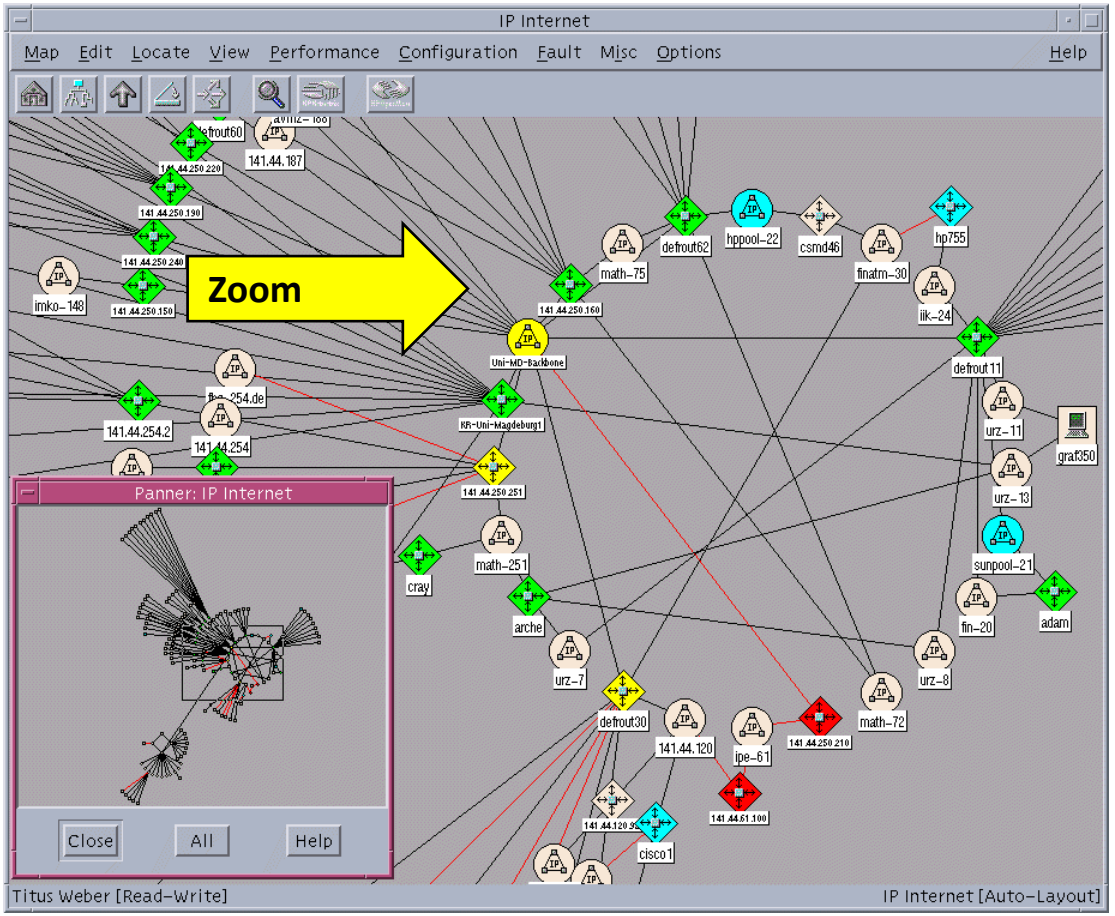
Fine and High Cost

Deep Inspection

Understanding Network topology

- Overview to Detail
  - Not reachable?
  - From where?
  - Beyond where?
- Scale of Impact?
- Why and where it happened?
- Identify problematic nodes

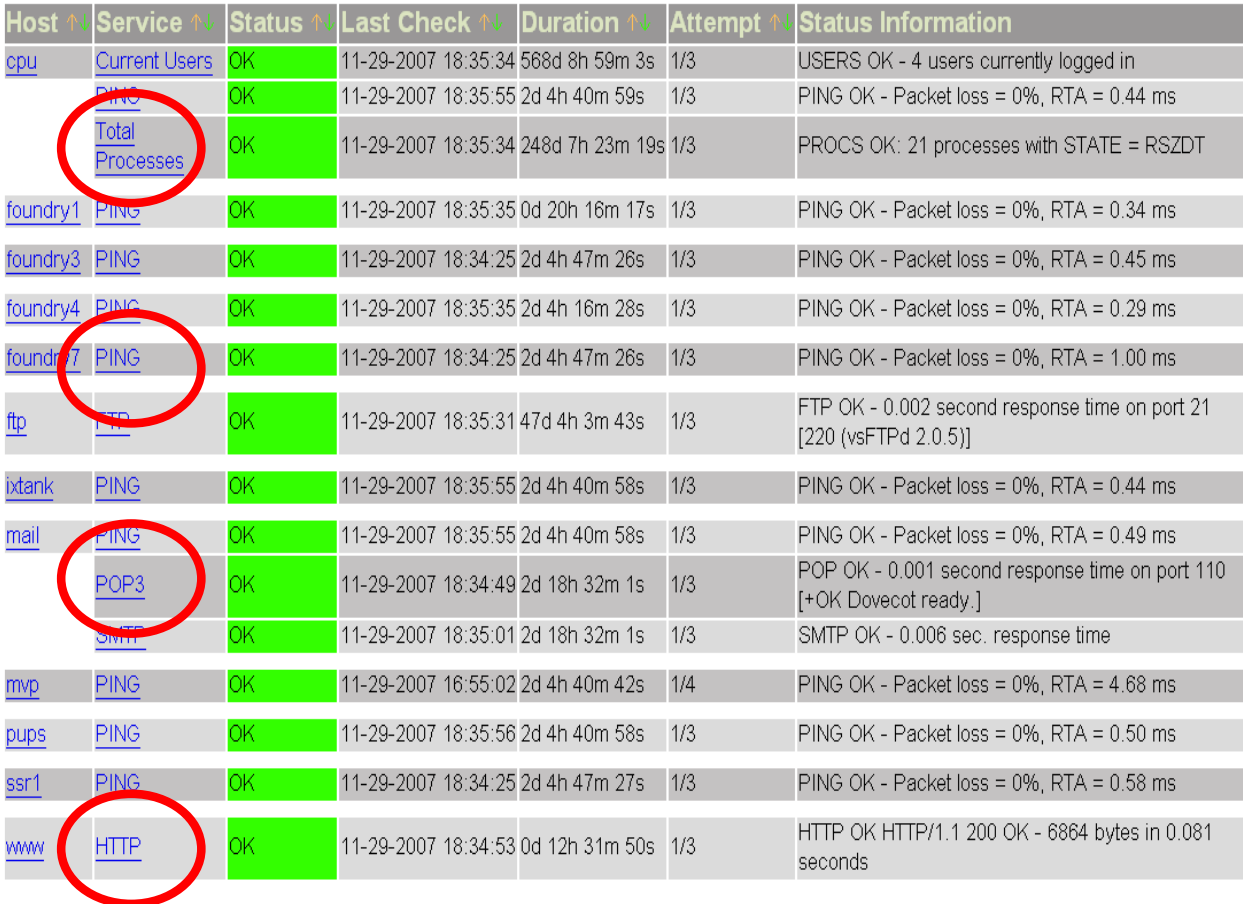
HP OpenView



http://ivs.cs.uni-magdeburg.de/sw-eng/us/CAME/pics/CAME.openview2.gifより引用

Service Monitoring

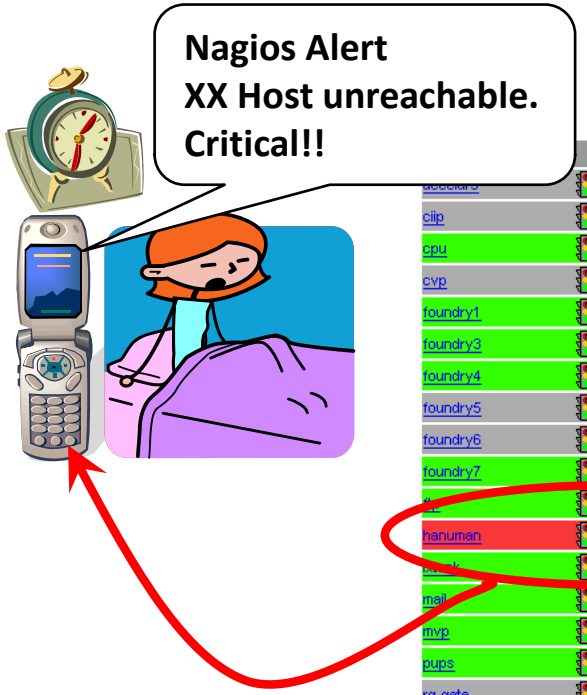
- Per Layer, Per Protocol
  - TCP + Application Protocol(ex. http get)
  - ICMP



Host	Service	Status	Last Check	Duration	Attempt	Status Information
cpu	Current Users	OK	11-29-2007 18:35:34	568d 8h 59m 3s	1/3	USERS OK - 4 users currently logged in
	PING	OK	11-29-2007 18:35:55	2d 4h 40m 59s	1/3	PING OK - Packet loss = 0%, RTA = 0.44 ms
	Total Processes	OK	11-29-2007 18:35:34	248d 7h 23m 19s	1/3	PROCS OK: 21 processes with STATE = RSZDT
foundry1	PING	OK	11-29-2007 18:35:35	0d 20h 16m 17s	1/3	PING OK - Packet loss = 0%, RTA = 0.34 ms
foundry3	PING	OK	11-29-2007 18:34:25	2d 4h 47m 26s	1/3	PING OK - Packet loss = 0%, RTA = 0.45 ms
foundry4	PING	OK	11-29-2007 18:35:35	2d 4h 16m 28s	1/3	PING OK - Packet loss = 0%, RTA = 0.29 ms
foundry7	PING	OK	11-29-2007 18:34:25	2d 4h 47m 26s	1/3	PING OK - Packet loss = 0%, RTA = 1.00 ms
ftp	FTP	OK	11-29-2007 18:35:31	47d 4h 3m 43s	1/3	FTP OK - 0.002 second response time on port 21 [220 (vsFTPd 2.0.5)]
ixtank	PING	OK	11-29-2007 18:35:55	2d 4h 40m 58s	1/3	PING OK - Packet loss = 0%, RTA = 0.44 ms
mail	PING	OK	11-29-2007 18:35:55	2d 4h 40m 58s	1/3	PING OK - Packet loss = 0%, RTA = 0.49 ms
	POP3	OK	11-29-2007 18:34:49	2d 18h 32m 1s	1/3	POP OK - 0.001 second response time on port 110 [+OK Dovecot ready.]
	SMTP	OK	11-29-2007 18:35:01	2d 18h 32m 1s	1/3	SMTP OK - 0.006 sec. response time
mvp	PING	OK	11-29-2007 16:55:02	2d 4h 40m 42s	1/4	PING OK - Packet loss = 0%, RTA = 4.68 ms
pups	PING	OK	11-29-2007 18:35:56	2d 4h 40m 58s	1/3	PING OK - Packet loss = 0%, RTA = 0.50 ms
ssr1	PING	OK	11-29-2007 18:34:25	2d 4h 47m 27s	1/3	PING OK - Packet loss = 0%, RTA = 0.58 ms
www	HTTP	OK	11-29-2007 18:34:53	0d 12h 31m 50s	1/3	HTTP OK HTTP/1.1 200 OK - 6864 bytes in 0.081 seconds

Being Alerted Anyware

- Know the outage of critical service quickly
- Need the guideline who handle the alert



Nagios Alert

	Status	Last Check	Duration	Status Information
[illegible]	PENDING	N/A	188d 2h 42m 35s+	Host has not been checked yet
ciip	PENDING	N/A	188d 2h 42m 35s+	Host has not been checked yet
cpu	UP	11-27-2007 13:54:55	19d 7h 15m 7s	PING OK - Packet loss = 0%, RTA = 0.50 ms
cvp	PENDING	N/A	188d 2h 42m 35s+	Host has not been checked yet
foundry1	UP	11-28-2007 22:19:37	2d 13h 27m 36s	PING OK - Packet loss = 0%, RTA = 0.37 ms
foundry3	UP	11-27-2007 13:48:45	19d 5h 45m 41s	PING OK - Packet loss = 0%, RTA = 0.28 ms
foundry4	UP	11-27-2007 14:19:30	2d 13h 57m 28s	PING OK - Packet loss = 0%, RTA = 0.36 ms
foundry5	PENDING	N/A	188d 2h 42m 35s+	Host has not been checked yet
foundry6	PENDING	N/A	188d 2h 42m 35s+	Host has not been checked yet
foundry7	UP	11-27-2007 13:48:45	19d 7h 20m 44s	PING OK - Packet loss = 0%, RTA = 0.30 ms
[illegible]	UP	[illegible]13-2007 14:33:06	47d 13h 13m 7s	PING OK - Packet loss = 0%, RTA = 0.18 ms
hanuman	DOWN	05-26-2[illegible]7 01:01:38	188d 8h 27m 37s	CRITICAL - Plugin timed out after 10 seconds
[illegible]	UP	[illegible]-27-2007 13:54:55	10d 2h 56m 22s	PING OK - Packet loss = 0%, RTA = 0.49 ms
mail	UP	11-27-2007 13:54:55	3d 3h 41m 31s	PING OK - Packet loss = 0%, RTA = 0.53 ms
mvp	UP	11-27-2007 13:55:25	2d 13h 50m 46s	PING OK - Packet loss = 0%, RTA = 7.76 ms
pups	UP	11-27-2007 13:54:56	4d 11h 8m 8s	PING OK - Packet loss = 0%, RTA = 0.65 ms
rg-gate	PENDING	N/A	188d 2h 42m 35s+	Host has not been checked yet
shonan	UP	05-16-2006 06:15:48	568d 18h 6m 44s	PING OK - Packet loss = 0%, RTA = 0.39 ms
ssr1	UP	11-27-2007 13:48:45	19d 7h 22m 24s	PING OK - Packet loss = 0%, RTA = 0.45 ms

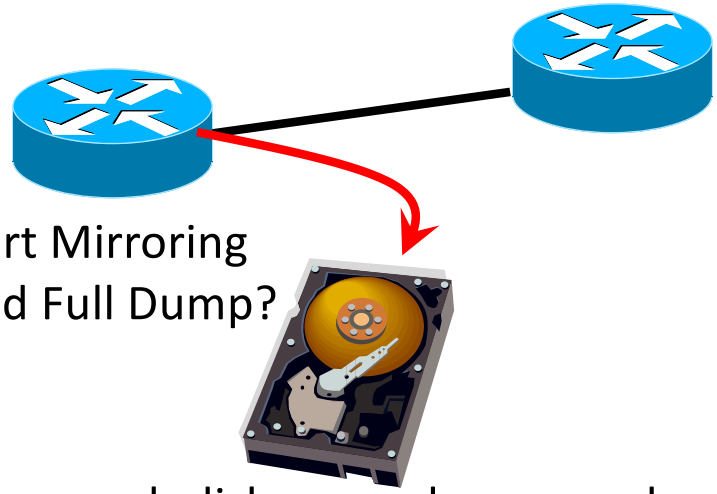
Spec, Limitation and Planning

- If you procure a backbone router, what kind of information should we carefully check?

- Packet processing performance
- Backplane capacity
- Power consumption
- Heat emission
- Dimension and weight

Monitoring Uses Resources

- What is the cost of monitoring?
  - Additional CPU load to equipment
  - Network bandwidth to transmit monitoring data
  - Disk space to store data
  - Additional HW and SW for monitoring purpose

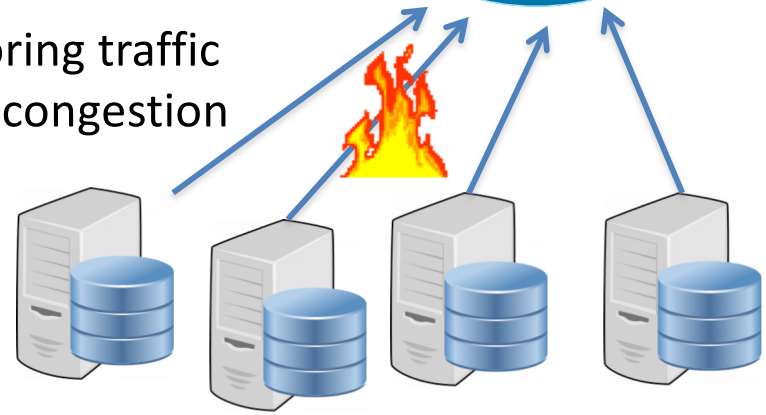


Port Mirroring
and Full Dump?

How much disk space do we need
for taking full dump of 100Mbps link?

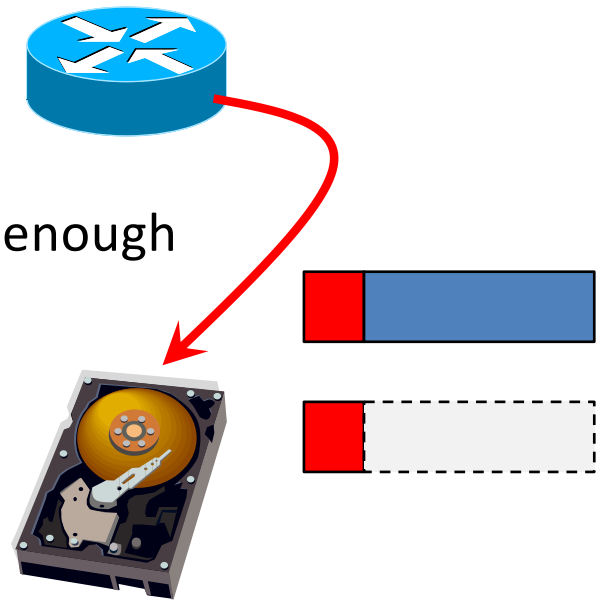
Monitoring target gets
busy to answer queries

Monitoring traffic
causes congestion



Defining “What we want to know”

- Total volume of traffic
  - Traffic counter on I/F serves very well
- Trend of network flow
  - Sampling (1 packet out of 100, for example) is enough
  - Depends on the traffic volume
- Distribution of protocols
  - First 128 of entire packet is enough



- We can know a lot of things without storing huge packet capture data, at the same time
- We need packet capture for some purposes
  - R&D, Security, Troubleshooting, etc…

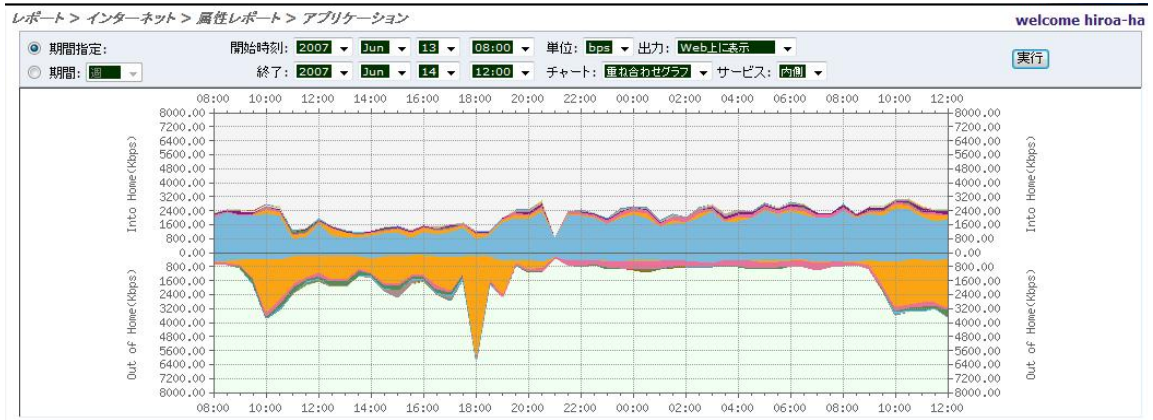
Some Questions

- Which data are we going to keep?
- How fast does its size glow?
- How long do we keep that data?

- Need to watch carefully
  - Tcpdump data, Squid log, HTTP access log, ….

Flow-based Monitoring

- Sampling
  - Statistically analyze the traffic trend
  - Capture 1 out of N packets, only headers
  - sFlow/NetFlow



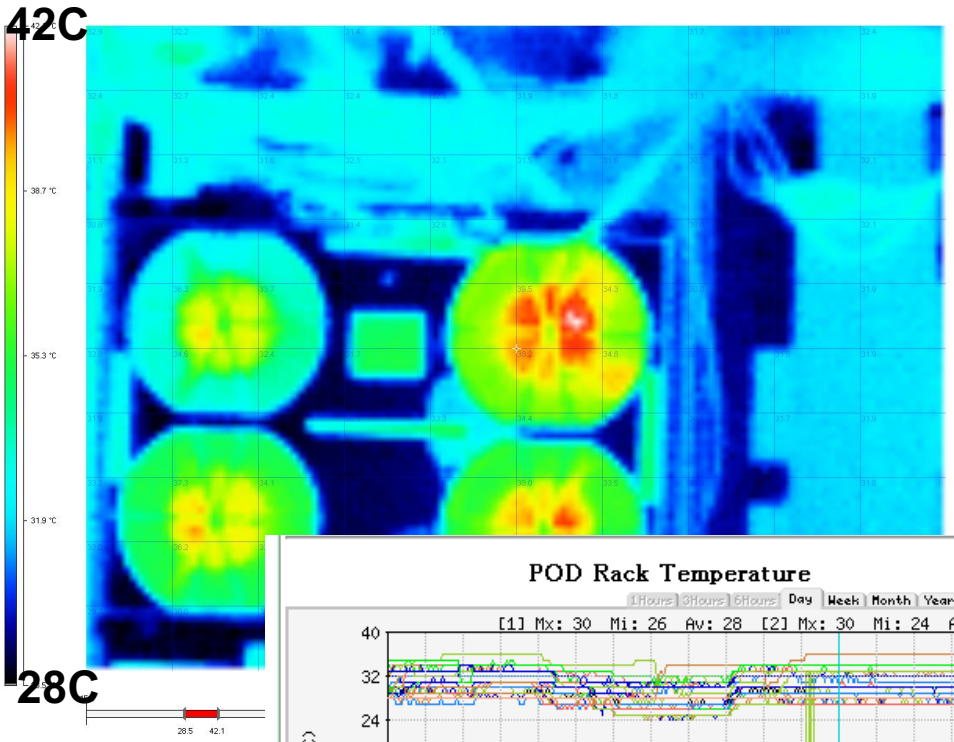
ダウンロードExcel-XML

平均値 | 現在値 | 最大値

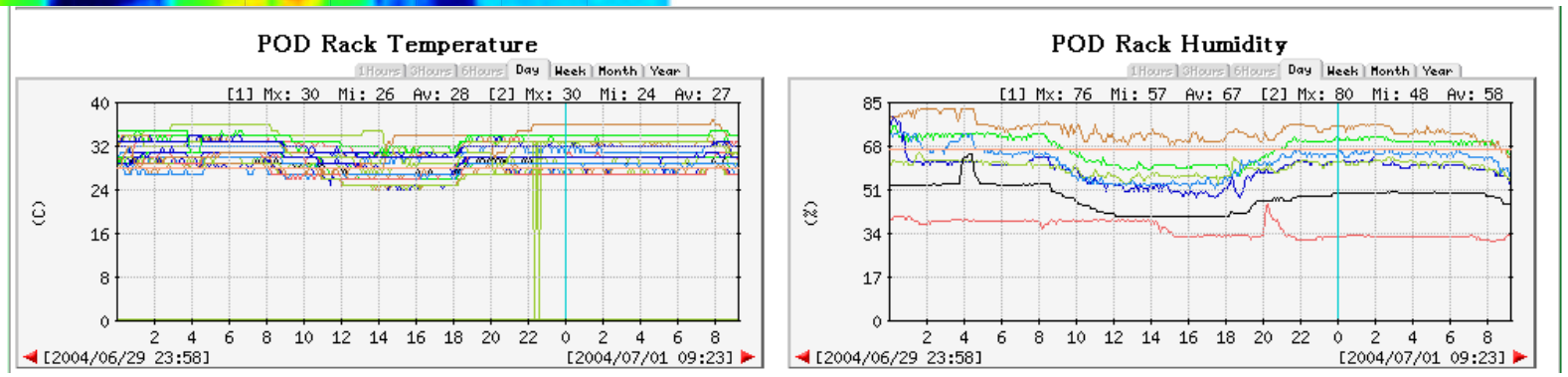
All	アプリケーション	ホームネットワークへ	ホームネットワークから	総和	トータル(%)
	Sasser.Sasser	1,710.47K	383.14K	2,093.61K	2.26%
	HTTP	131.51K	838.88K	970.39K	1.05%
	DNS	108.85K	228.36K	337.21K	0.36%
	HTTPS	17.05K	88.73K	105.78K	0.11%
	Slammer.Slammer	62.78K	0.00	62.78K	0.07%
	TELNET	28.49K	1,632.12	30.08K	0.03%
	WINS.Vulnerability	27.19K	1,074.69	28.24K	0.03%
	POP	887.00	21.61K	22.48K	0.02%
	Blaster.Blaster	15.04K	6,267.35	21.16K	0.02%
	RTSP	232.26	20.08K	20.31K	0.02%
	NetBIOS Service	14.48K	5,647.14	19.99K	0.02%
	SNMP	9,175.35	0.00	9,175.35	0.01%
	FTP.Data	1,024.47	6,607.58	7,632.06	0.01%

Temperature and Humidity

- Check CPU temperature using SNMP
- Put thermometer on top of rack
- Monitor with infra-red sensors

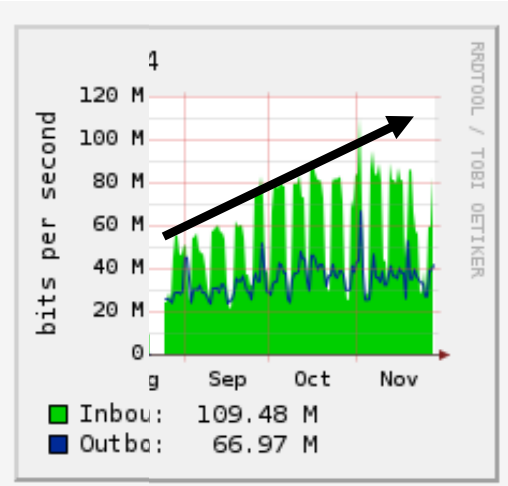


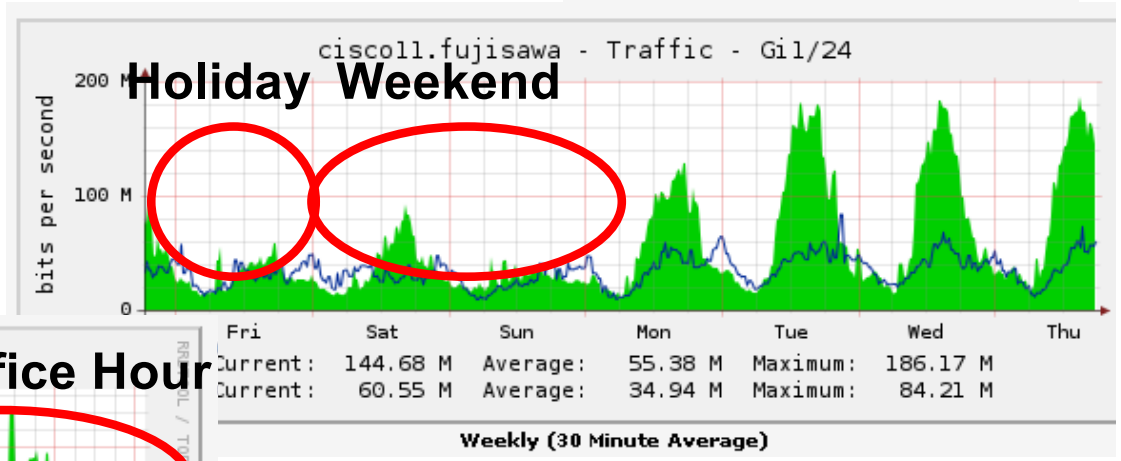
Which way we go?

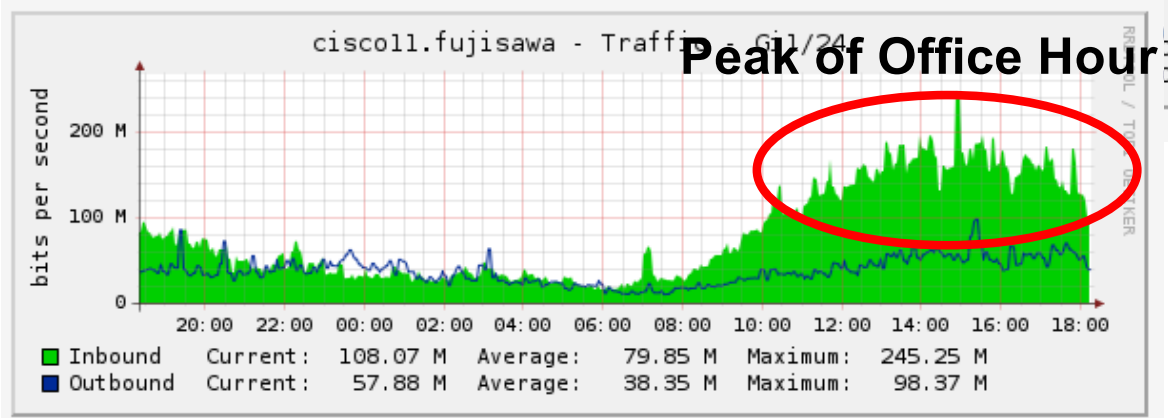


Knowing Peaks, Trends and Estimating Future from Data

- Daily Observation
  - When is the network busiest?
- Weekly Observation
  - On what kind of day is vacant and busy
- Long-term Observation
  - Is the network demand increasing?
  - How much?

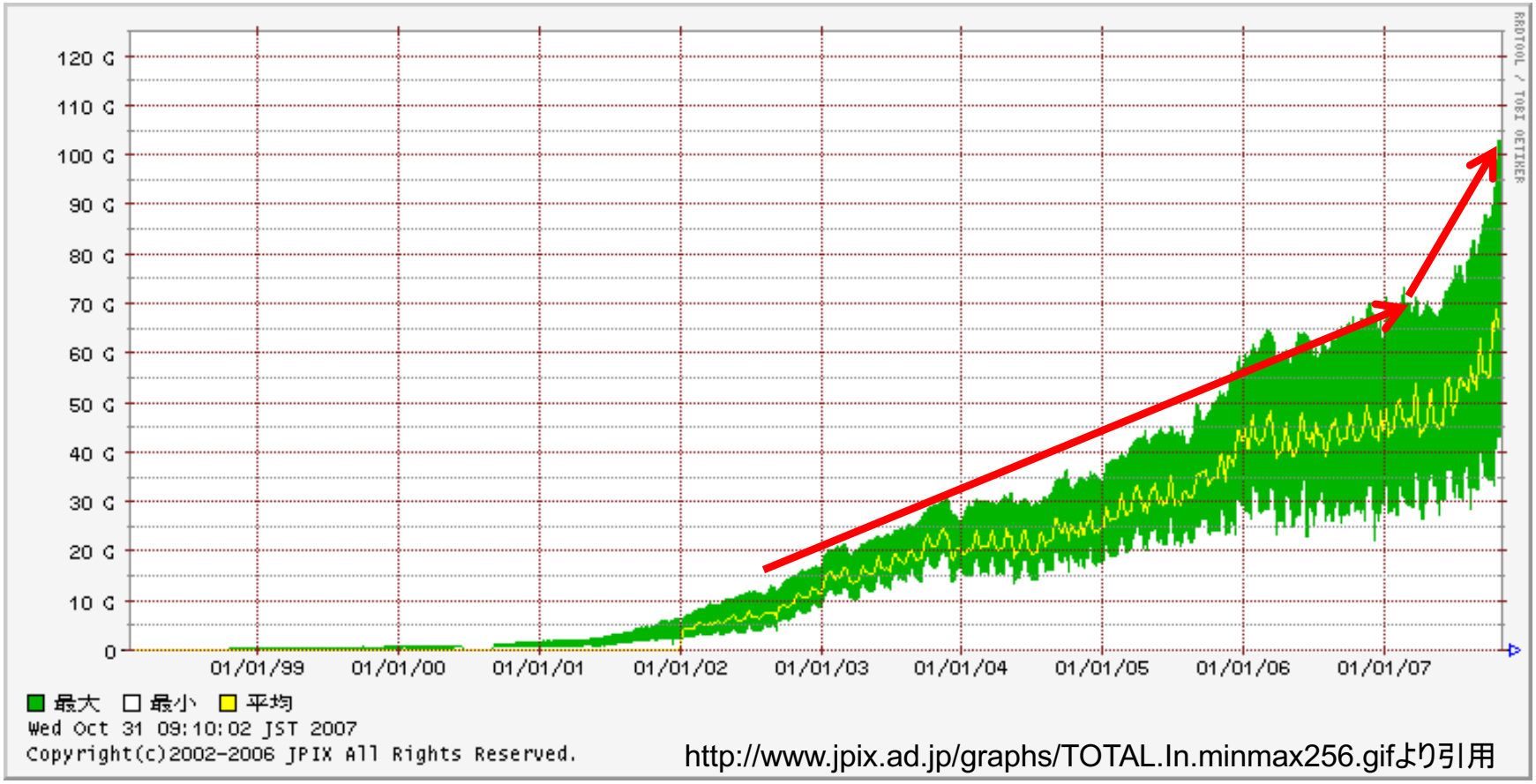






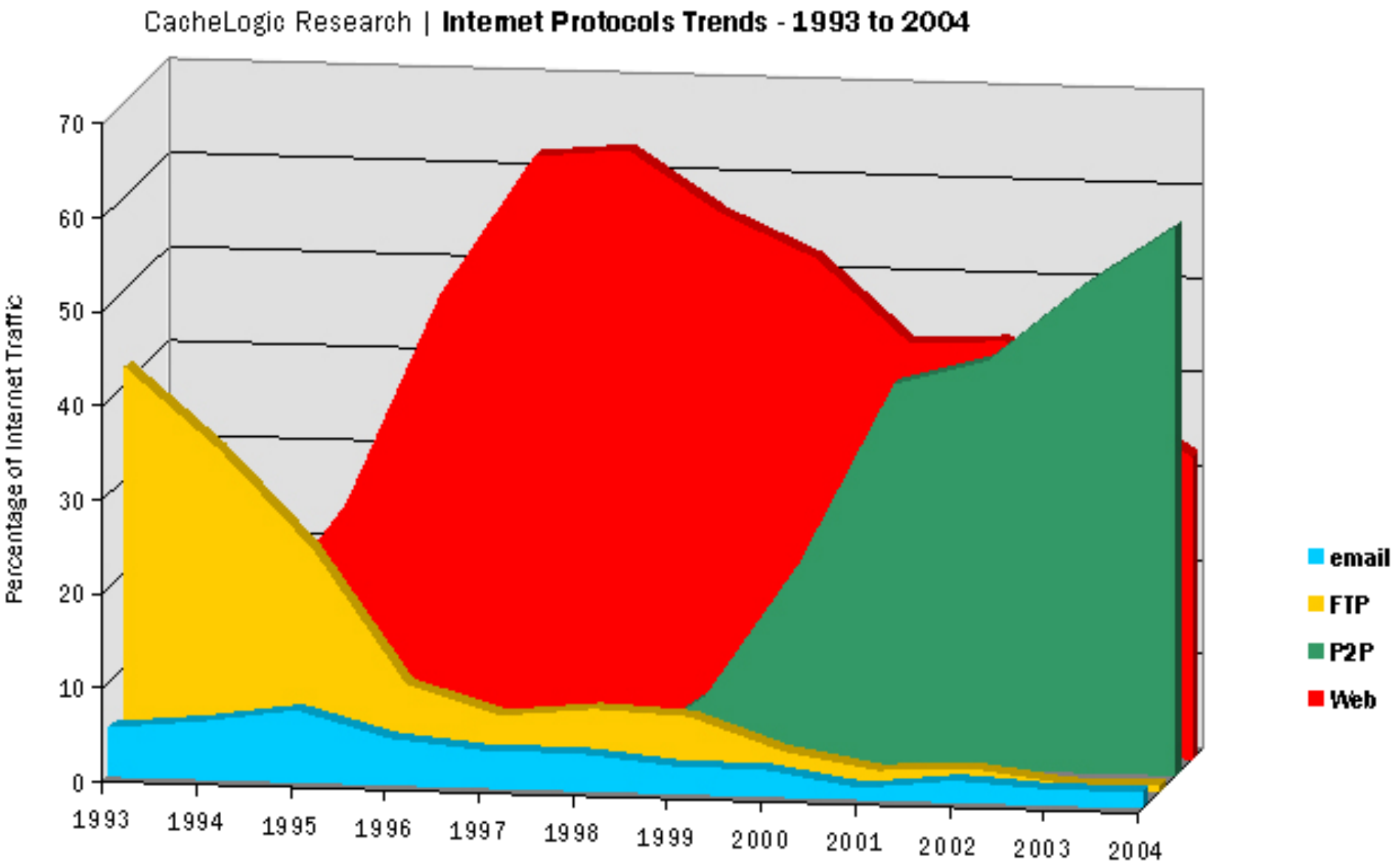
Traffic Growth in IX

- IX: Internet Exchange = Core of the Internet
- Application Breakthrough, Infrastructure breakthrough



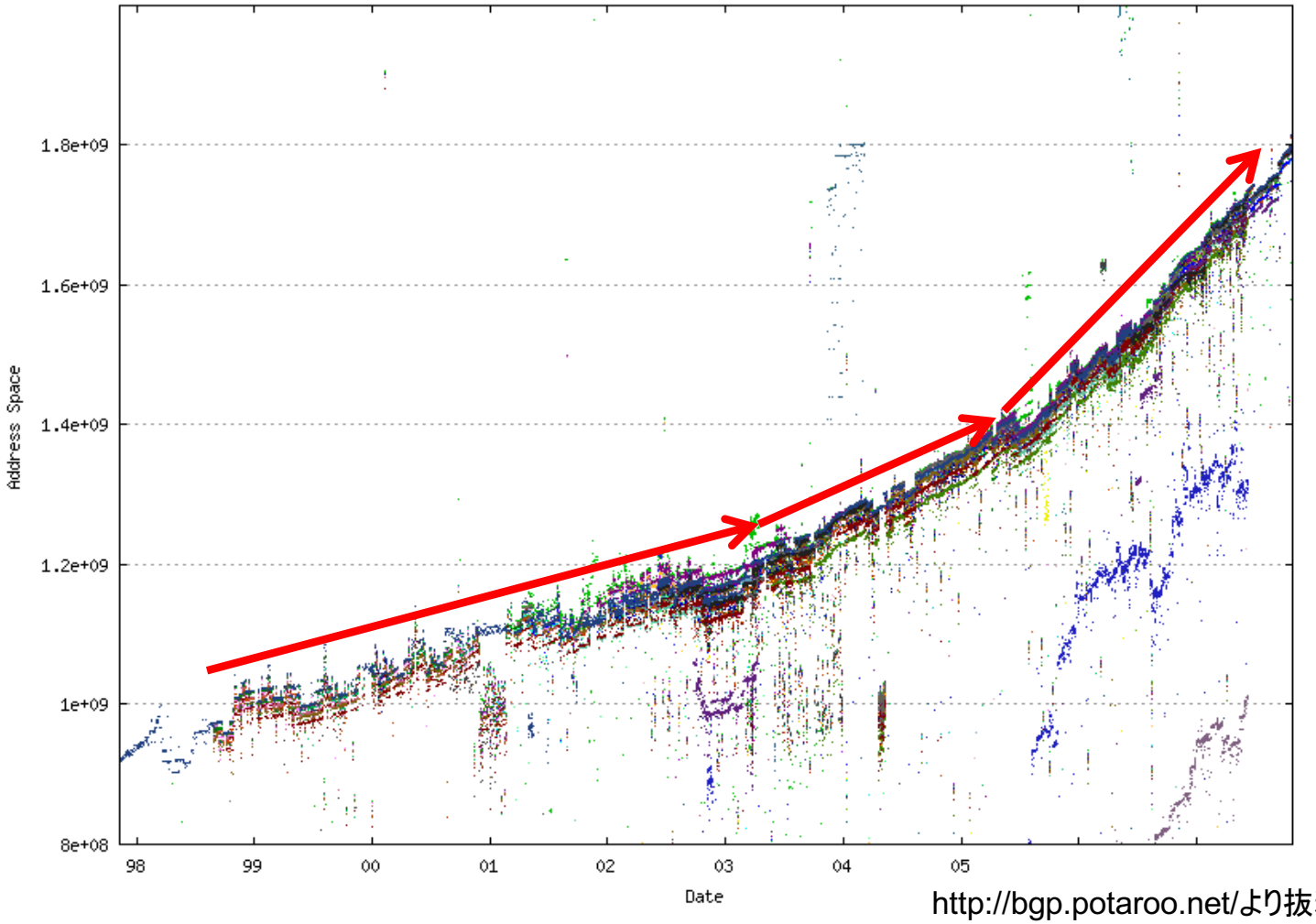
http://www.jpix.ad.jp/graphs/TOTAL.In.minmax256.gifより引用

Change of Application Trends



Number of BGP Full Route

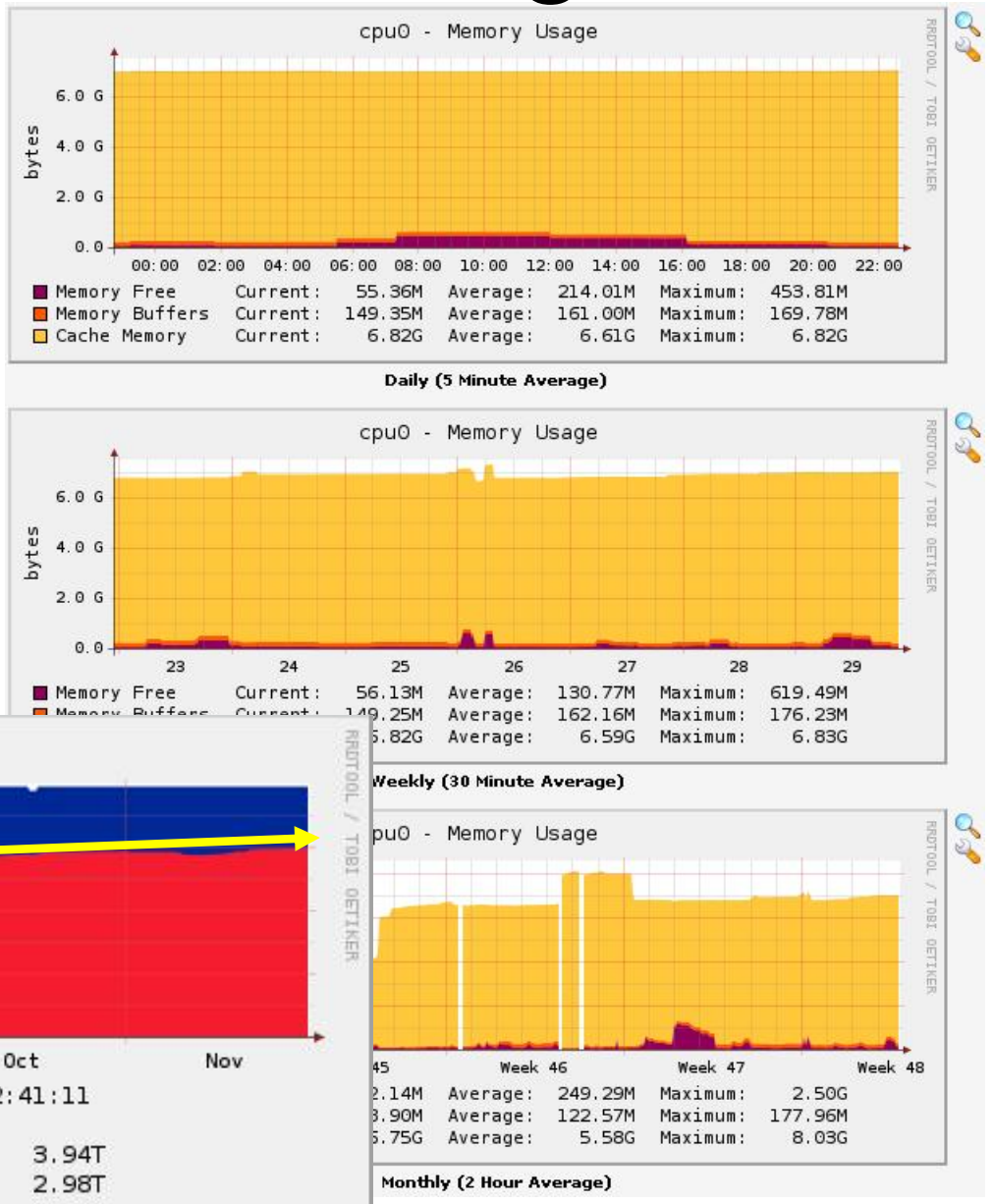
- Is the memory of routers enough?



http://bgp.potaroo.net/より抜粋

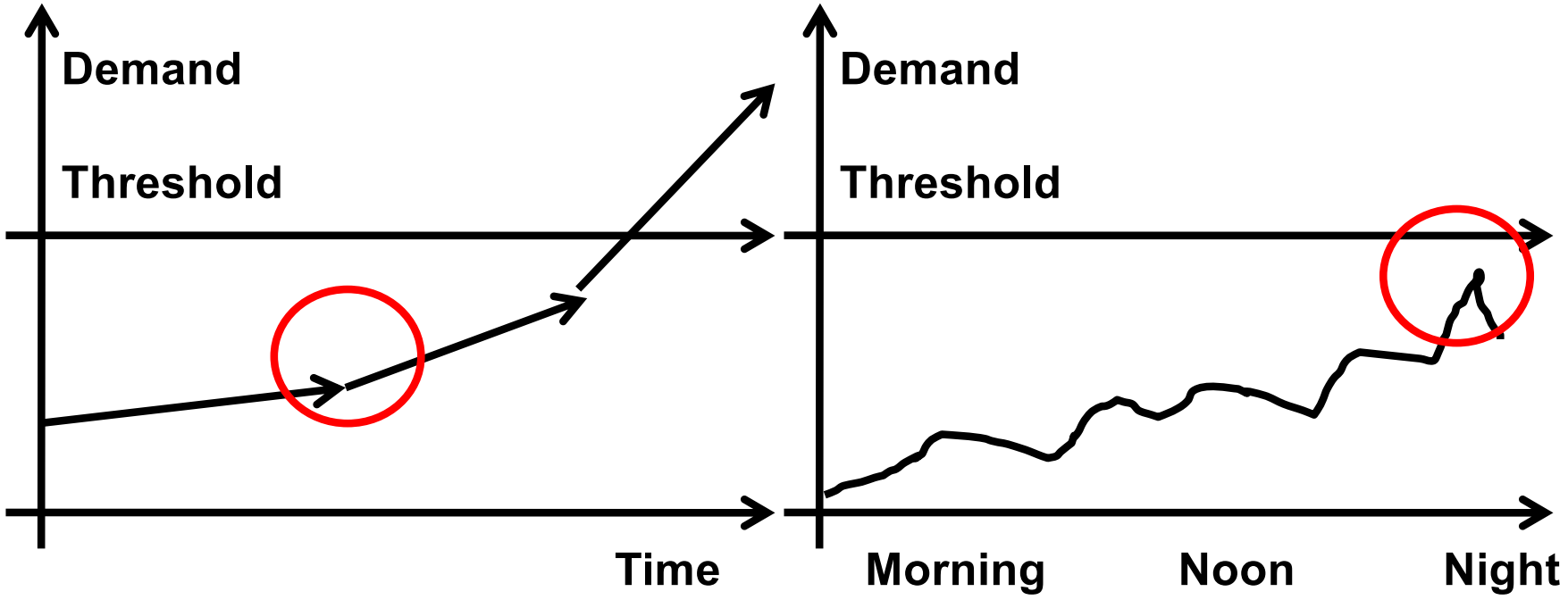
Is demand increasing?

- Very slow growth



How to estimate demand increase?

- Increasing demand glows even more rapidly
- Stay aware of demand increase
- Do consider the peak demand



Intermediate Summary

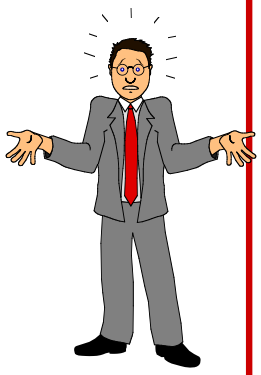
- Monitoring Services and Networks
  - “broader overview” and “deep inspection”
  - “Just reach” or “Appropriately reach”
  - Importance of visualization
  - Tradeoffs between monitoring granularity and cost
- Make feedback from statistic evidence to the operation in next stage
  - What kind of difficulty will we face in the future??
  - When does it happens?
  - Let’s be prepared with some solutions before it happens!!

Chapter 9 outline

- What is network management?
- Internet-standard management framework
  - Structure of Management Information: SMI
  - Management Information Base: MIB
  - SNMP Protocol Operations and Transport Mappings
  - Security and Administration
- ASN.1

What is network management?

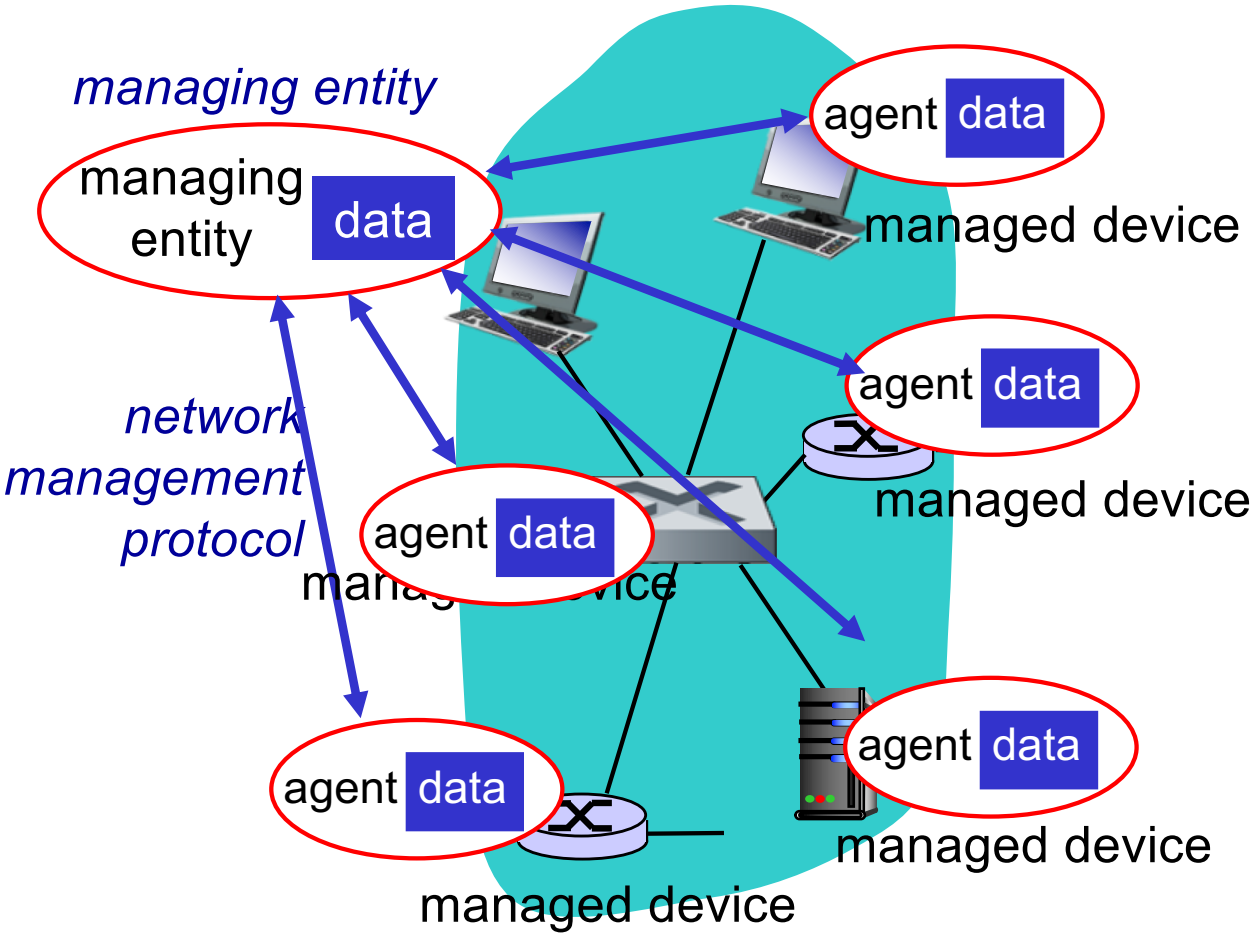
- autonomous systems (aka "network"): 1000s of interacting hardware/software components
- other complex systems requiring monitoring, control:
  - jet airplane
  - nuclear power plant
  - others?



"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."

Infrastructure for network management

definitions:



managed devices contain *managed objects* whose data is gathered into a *Management Information Base (MIB)*

Network management standards

OSI CMIP

- Common Management Information Protocol
- designed 1980's: *the* unifying net management standard
- too slowly standardized

SNMP: Simple Network Management Protocol

- Internet roots (SGMP)
- started simple
- deployed, adopted rapidly
- growth: size, complexity
- currently: SNMP V3
- *de facto* network management standard

Chapter 9 outline

- What is network management?
- Internet-standard management framework
  - Structure of Management Information: SMI
  - Management Information Base: MIB
  - SNMP Protocol Operations and Transport Mappings
  - Security and Administration
- ASN.1

SNMP overview: 4 key parts

- Management information base (MIB):
  - distributed information store of network management data
- Structure of Management Information (SMI):
  - data definition language for MIB objects
- SNMP protocol
  - convey manager<->managed object info, commands
- security, administration capabilities
  - major addition in SNMPv3

SMI: data definition language

Purpose: syntax, semantics of management data well-defined, unambiguous

- base data types:
  - straightforward, boring
- OBJECT-TYPE
  - data type, status, semantics of managed object
- MODULE-IDENTITY
  - groups related objects into MIB module

Basic Data Types

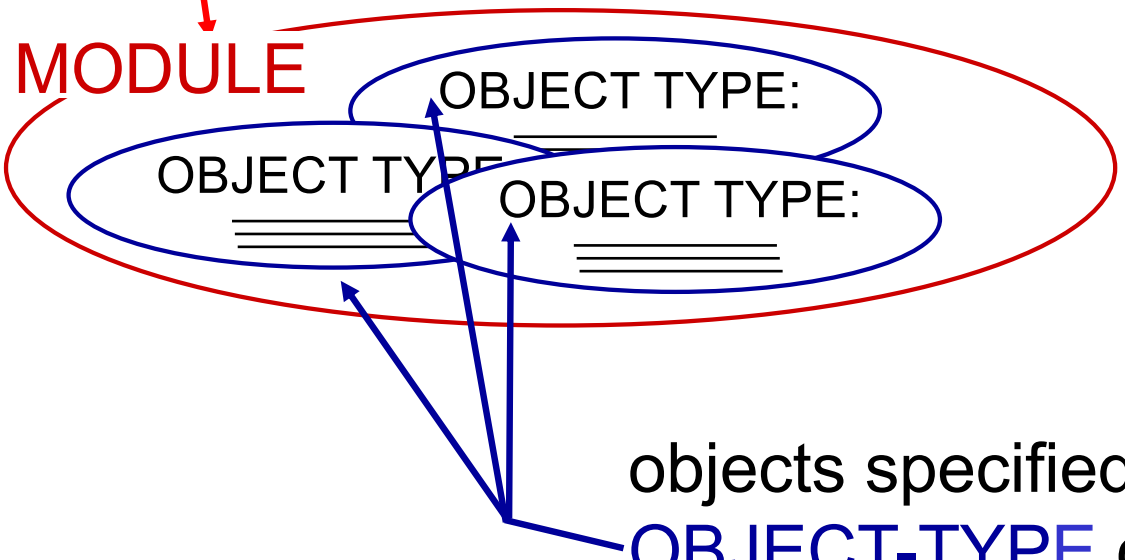
INTEGER
Integer32
Unsigned32
OCTET STRING
OBJECT IDENTIFIED
IPaddress
Counter32
Counter64
Guage32
Time Ticks
Opaque

SNMP MIB

MIB module specified via SMI

MODULE-IDENTITY

(100 standardized MIBs, more vendor-specific)



objects specified via SMI

OBJECT-TYPE construct

SMI: object, module examples

OBJECT-TYPE: ipInDelivers

```
ipInDelivers OBJECT TYPE
  SYNTAX       Counter32
  MAX-ACCESS   read-only
  STATUS   current
  DESCRIPTION
     "The total number of input
      datagrams successfully
      delivered to IP user-
      protocols (including ICMP)"
::= { ip   9}
```

MODULE-IDENTITY: ipMIB

```
ipMIB MODULE-IDENTITY
  LAST-UPDATED "941101000Z"
  ORGANZATION "IETF SNPv2
          Working Group"
  CONTACT-INFO
     " Keith McCloghrie
          "
     ……
  DESCRIPTION
     "The MIB module for managing
IP
     and ICMP implementations, but
     excluding their management of
     IP routes."
  REVISION "019331000Z"
 ……
::= {mib-2 48}
```

MIB example: UDP module

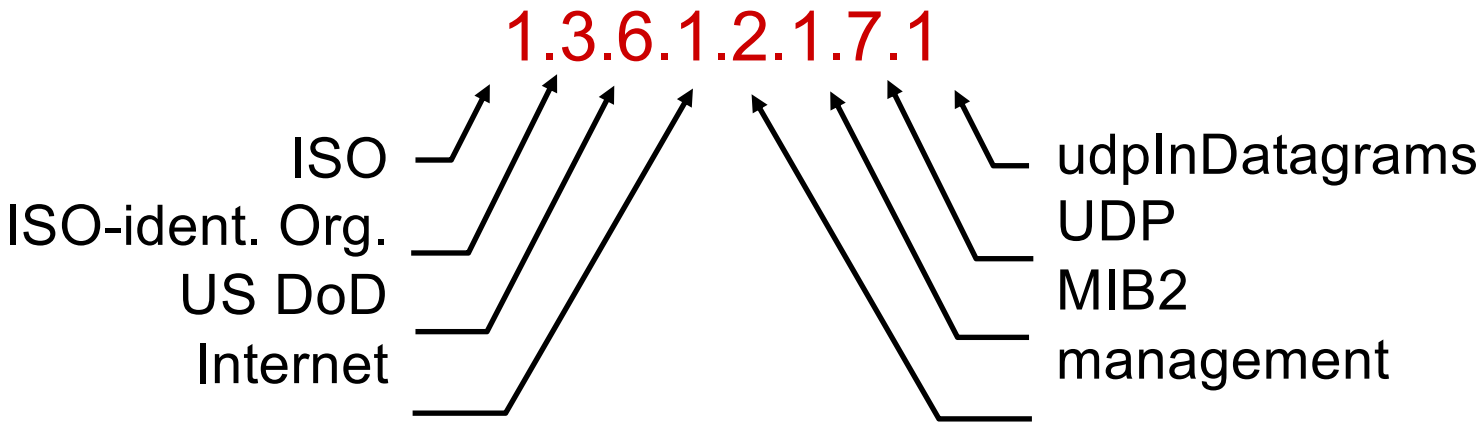
Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	total # datagrams delivered at this node
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	# underliverable datagrams: no application at port
1.3.6.1.2.1.7.3	UDInErrors	Counter32	# undeliverable datagrams: all other reasons
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	# datagrams sent
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	one entry for each port in use by app, gives port # and IP address

SNMP naming

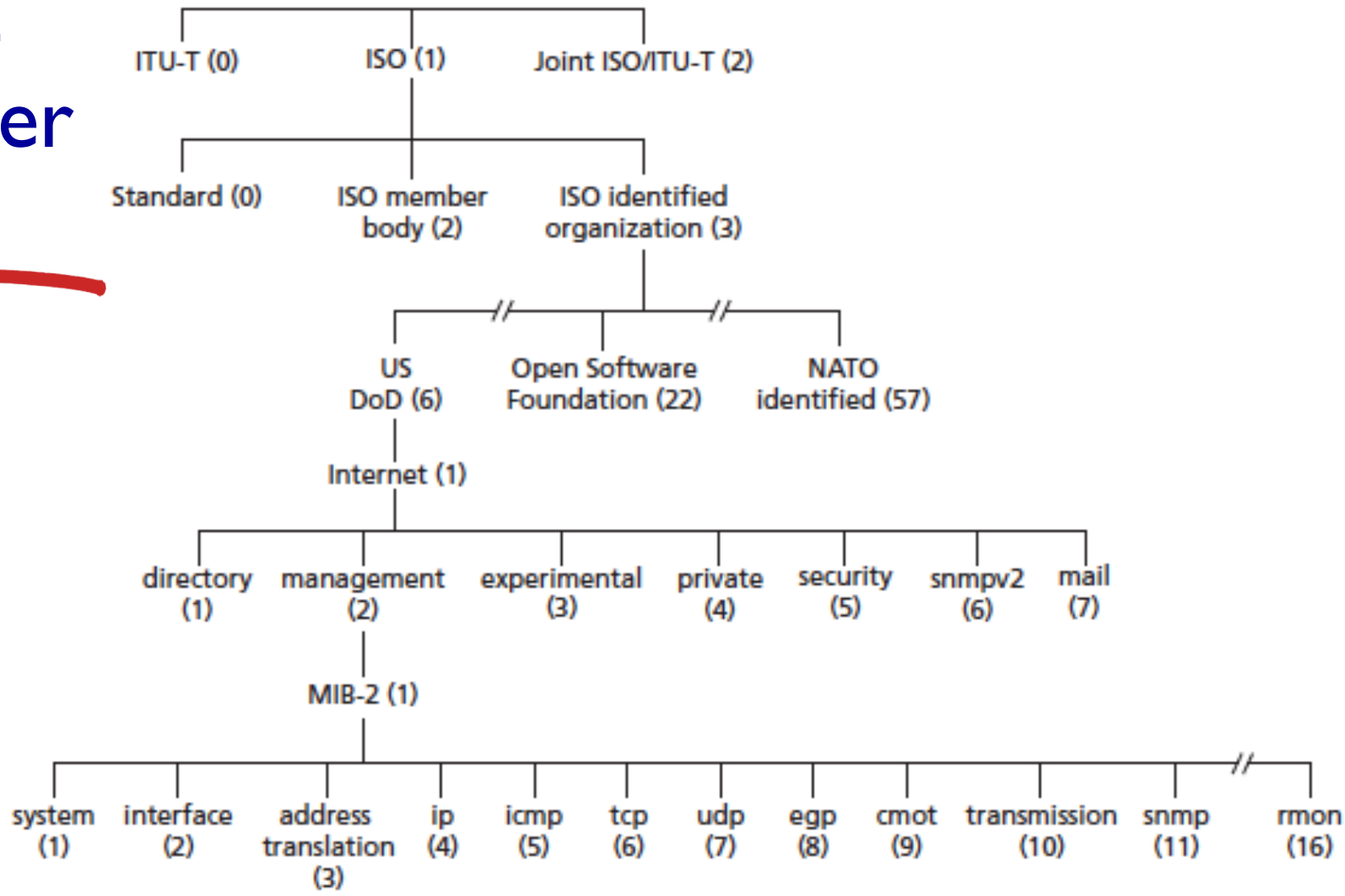
question: how to name every possible standard object (protocol, data, more..) in every possible network standard??

answer: *ISO Object Identifier tree:*

- hierarchical naming of all objects
- each branchpoint has name, number

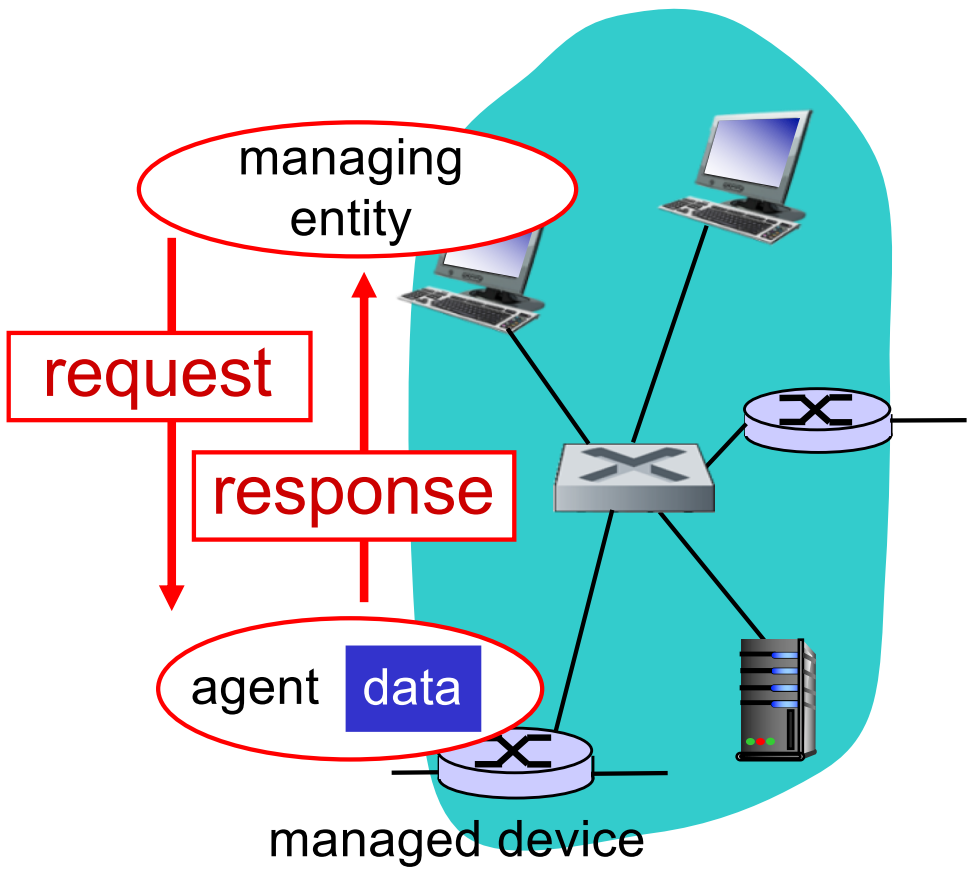


OSI Object Identifier Tree

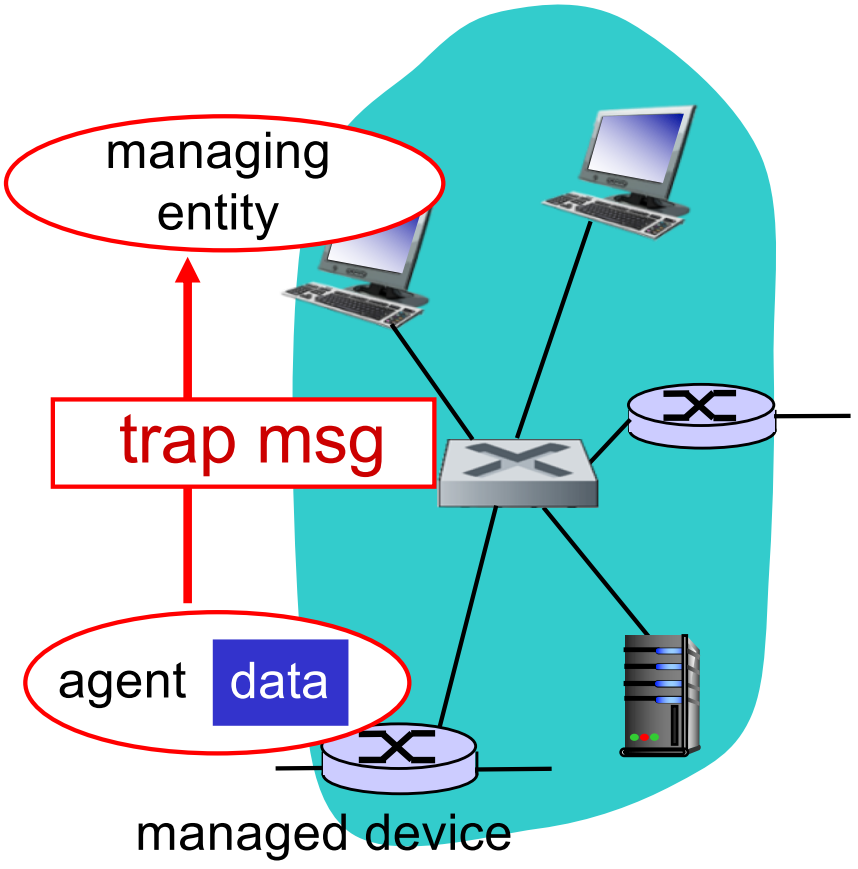


SNMP protocol

Two ways to convey MIB info, commands:



request/response mode

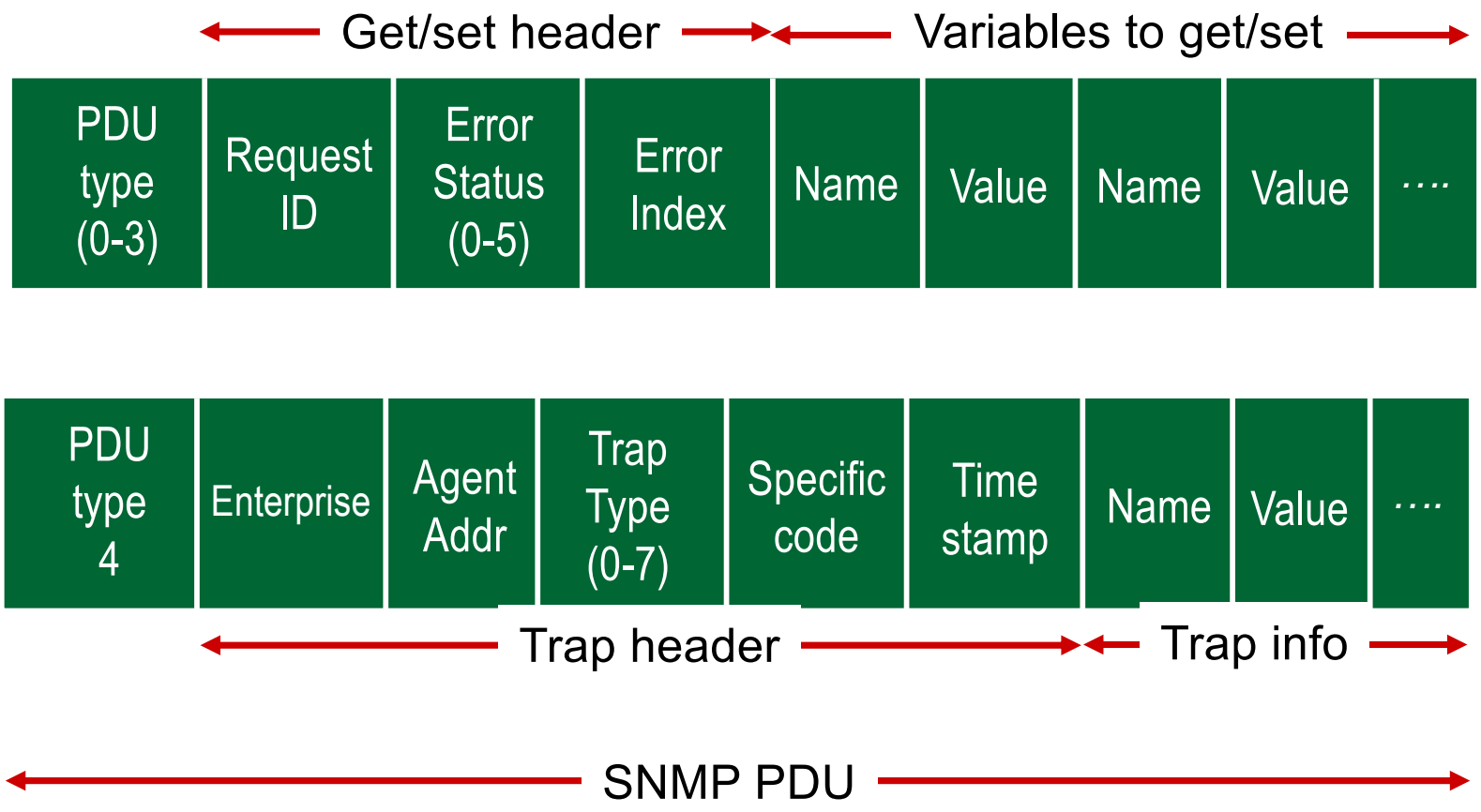


trap mode

SNMP protocol: message types

Message type	Function
GetRequest GetNextRequest GetBulkRequest	Mgr-to-agent: "get me data" (instance,next in list, block)
InformRequest	Mgr-to-Mgr: here's MIB value
SetRequest	Mgr-to-agent: set MIB value
Response	Agent-to-mgr: value, response to Request
Trap	Agent-to-mgr: inform manager of exceptional event

SNMP protocol: message formats



SNMP security and administration

- encryption: DES-encrypt SNMP message
- authentication: compute, send MIC(m,k): compute hash (MIC) over message (m), secret shared key (k)
- protection against playback: use nonce
- view-based access control:
  - SNMP entity maintains database of access rights, policies for various users
  - database itself accessible as managed object!

Chapter 9 outline

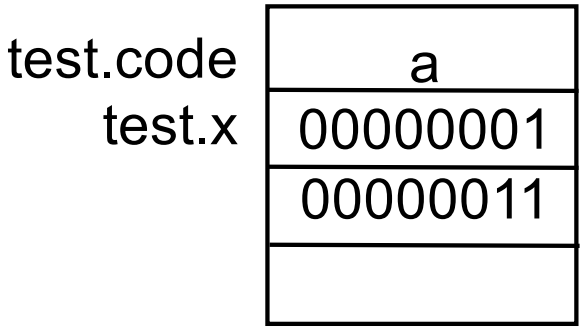
- What is network management?
- Internet-standard management framework
  - Structure of Management Information: SMI
  - Management Information Base: MIB
  - SNMP Protocol Operations and Transport Mappings
  - Security and Administration
- The presentation problem: ASN.1

The presentation problem

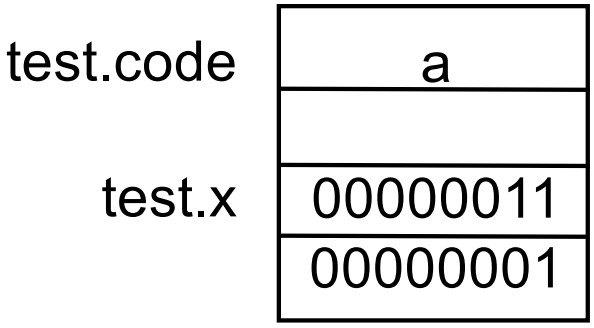
Q: does perfect memory-to-memory copy solve "the communication problem"?

A: not always!

```
struct {
   char code;
    int x;
    } test;
test.x = 256;
test.code= 'a'
```



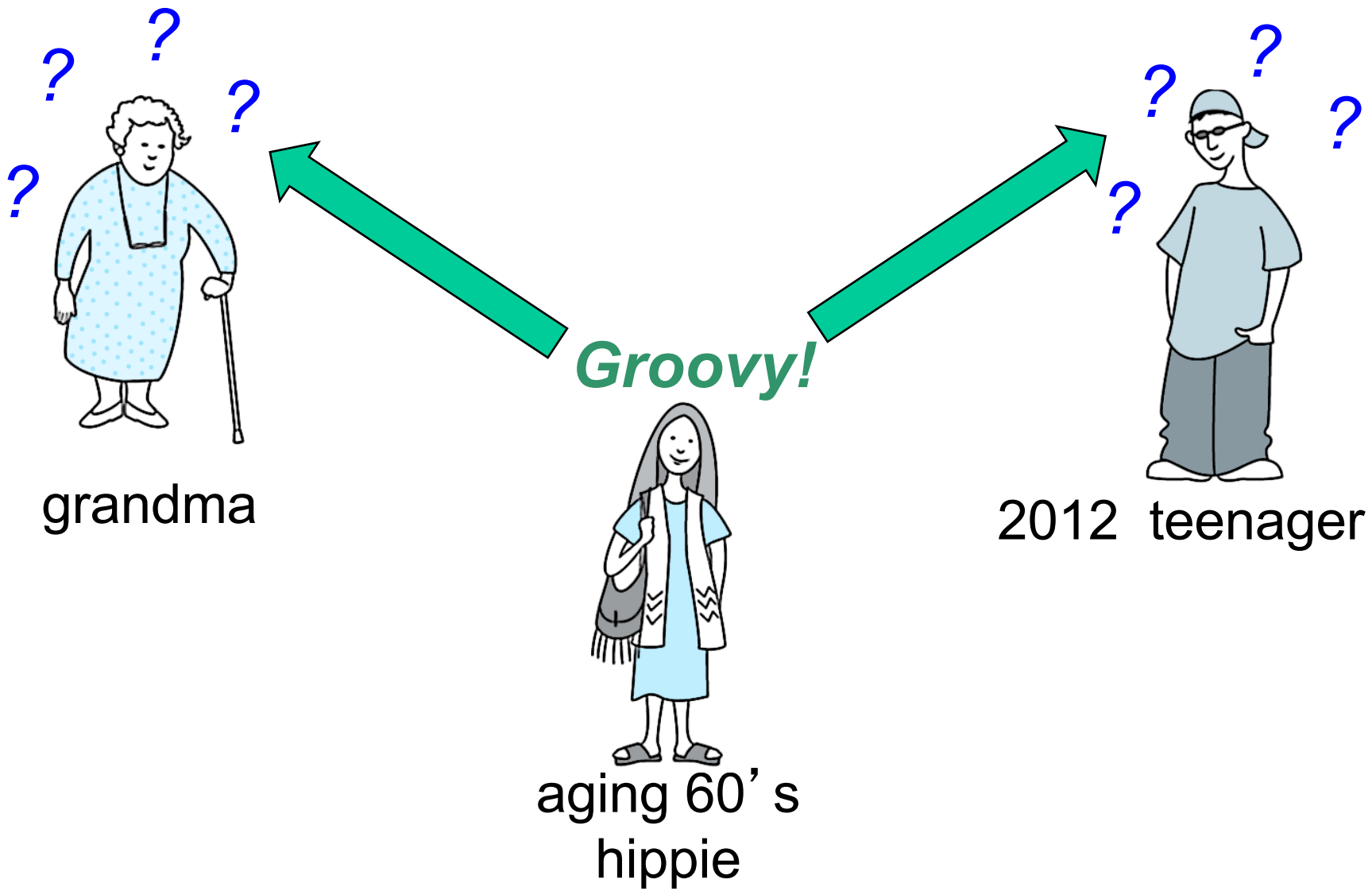
host 1 format



host 2 format

problem: different data format, storage conventions

A real-life presentation problem:

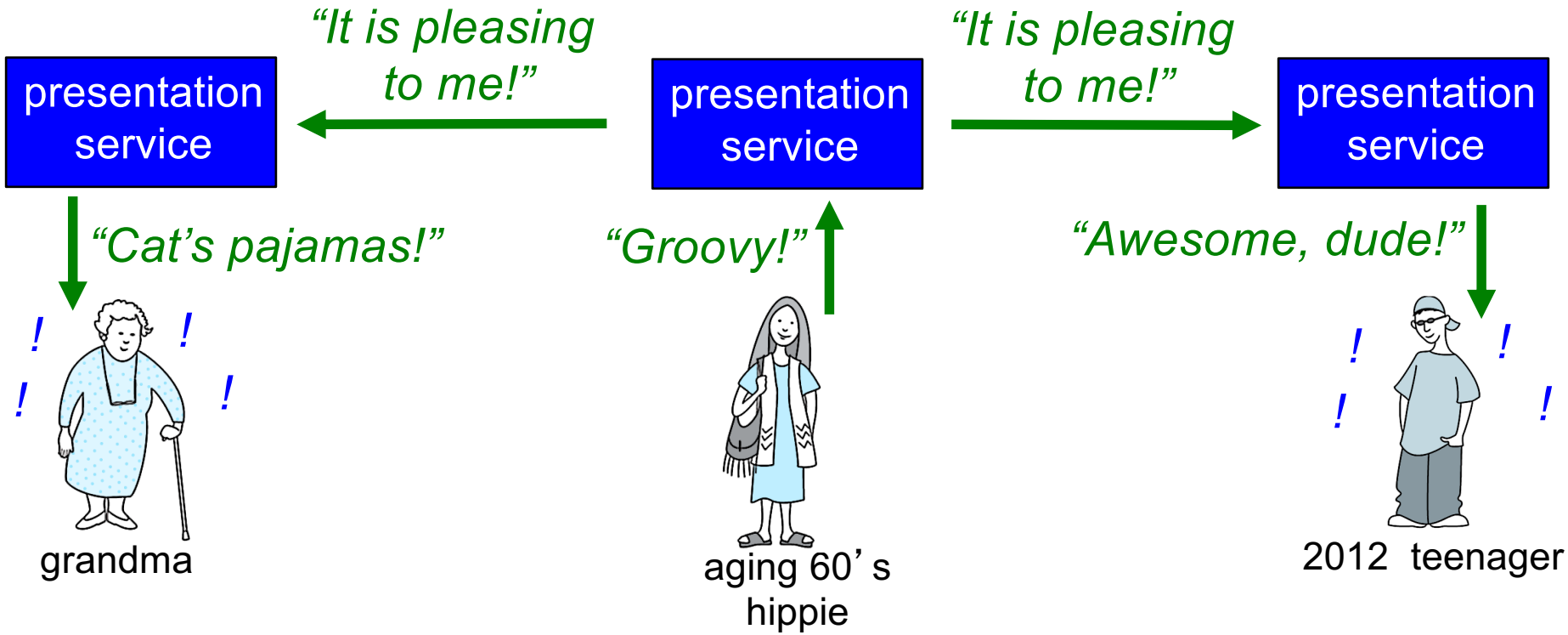


Presentation problem: potential solutions

1. Sender learns receiver's format. Sender translates into receiver's format. Sender sends.
   - real-world analogy?
   - pros and cons?
2. Sender sends. Receiver learns sender's format. Receiver translate into receiver-local format
   - real-world-analogy
   - pros and cons?
3. Sender translates host-independent format. Sends. Receiver translates to receiver-local format.
   - real-world analogy?
   - pros and cons?

Solving the presentation problem

1. Translate local-host format to host-independent format
2. Transmit data in host-independent format
3. Translate host-independent format to remote-host format



ASN.1: Abstract Syntax Notation 1

- ISO standard X.680
  - used extensively in Internet
  - like eating vegetables, knowing this "good for you"!
- defined data types, object constructors
  - like SMI
- BER: Basic Encoding Rules
  - specify how ASN.1-defined data objects to be transmitted
  - each transmitted object has Type, Length, Value (TLV) encoding

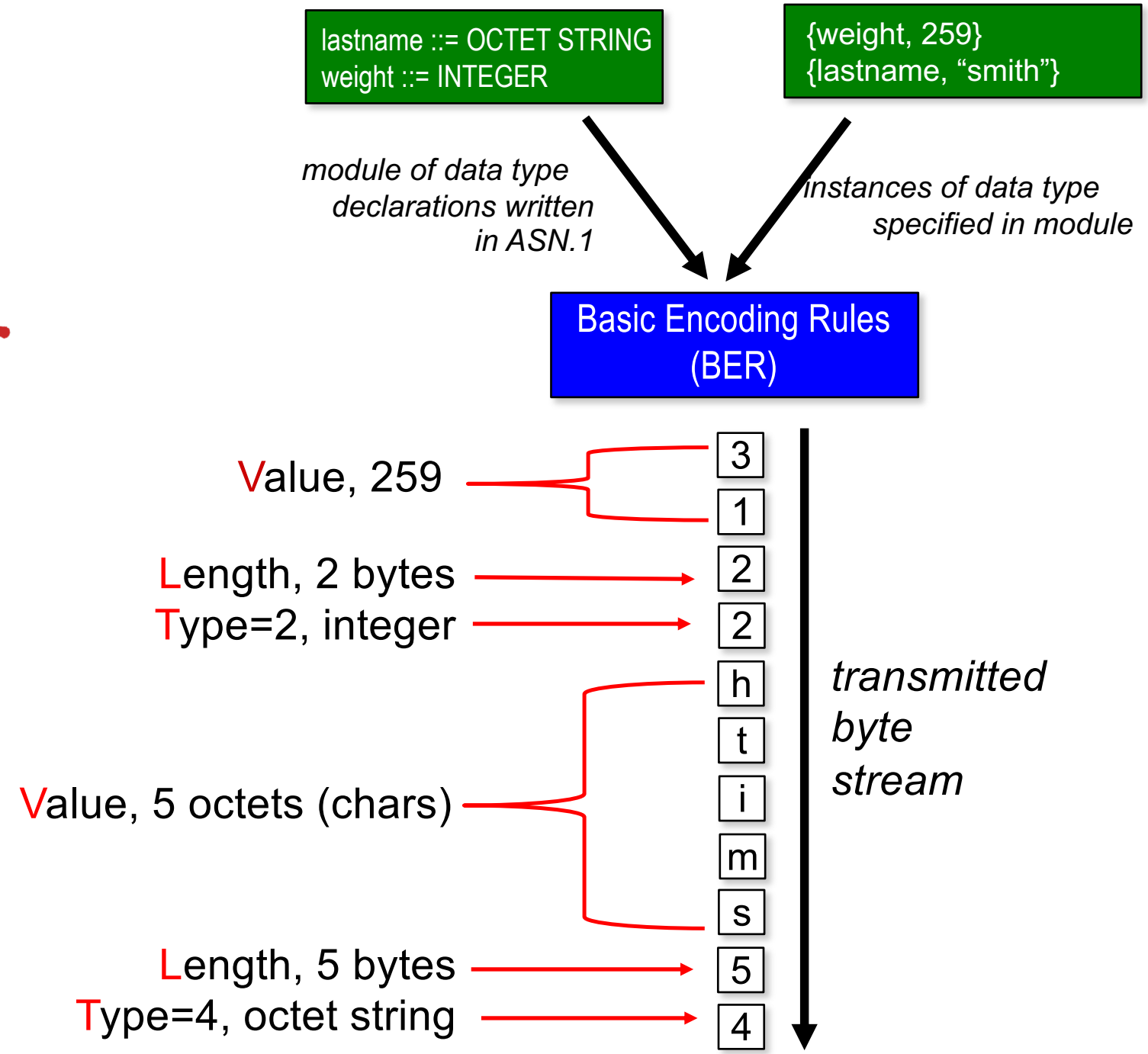
TLV Encoding

Idea: transmitted data is self-identifying

- T: data type, one of ASN.1-defined types
- L: length of data in bytes
- V: value of data, encoded according to ASN.1 standard

Tag Value	Type
1	Boolean
2	Integer
3	Bitstring
4	Octet string
5	Null
6	Object Identifier
9	Real

TLV encoding: example

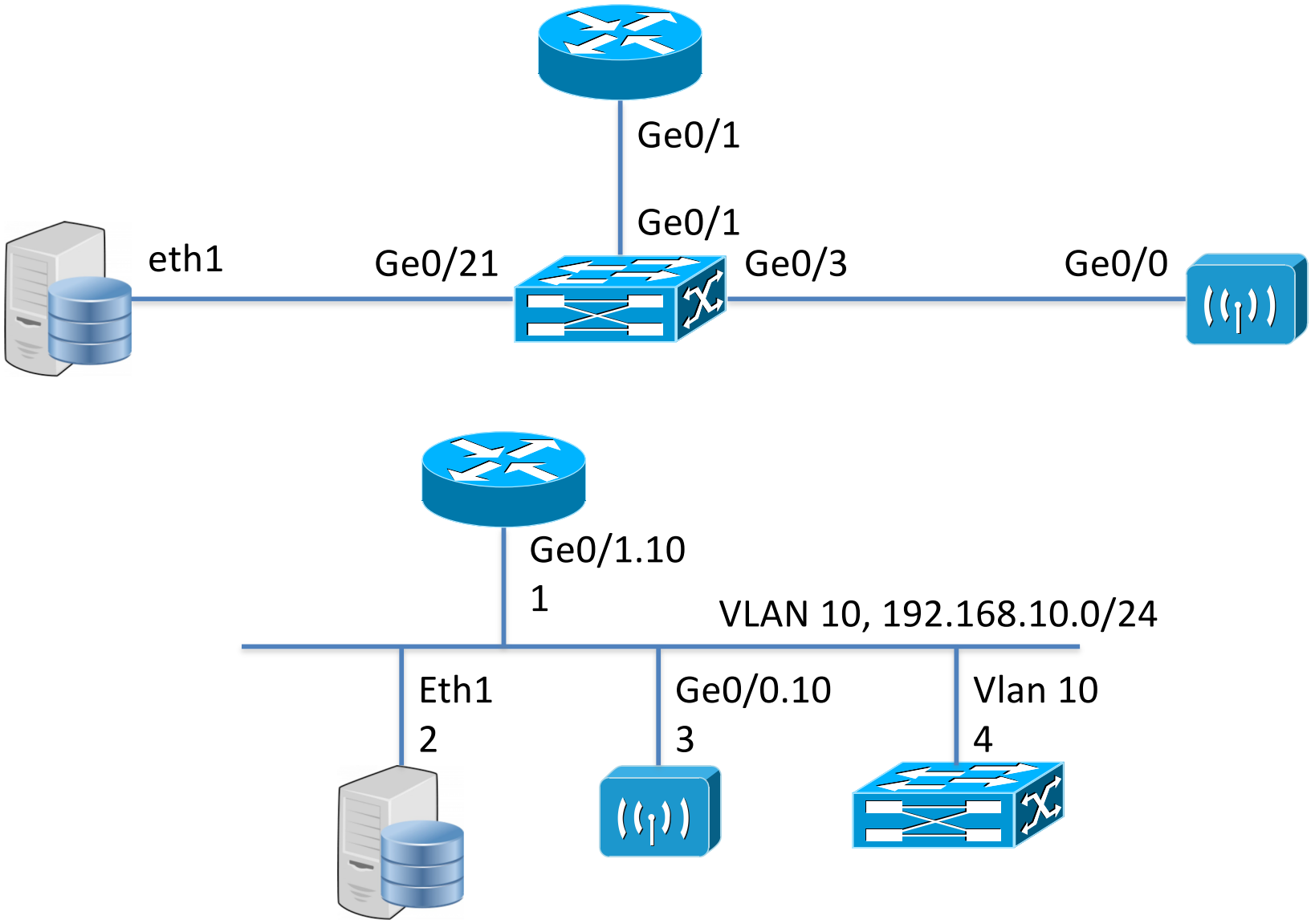


Network management: summary

- network management
  - extremely important: 80% of network "cost"
  - ASN.1 for data description
  - SNMP protocol as a tool for conveying information
- network management: more art than science
  - what to measure/monitor
  - how to respond to failures?
  - alarm correlation/filtering?

SNMP Hands-on

Layer1/2/3 Setup



SNMP: Monitoring Networks and Servers

- Packet loss? No answer to ping and telnet? Routing table is not calculated?
  - Bandwidth saturates
  - CPU load is too high
  - Available memory is out
- Configure SNMPv3 service on network equipment, servers and end user devices
- And more information

Enabling SNMPv3 on Cisco Router and Switch

- Same setting to be applied to router and switch
  - User Name: iith
  - Group Name: iithauth
  - Password: iithsnmp
  - Authentication Protocol: MD5

- Configuration

```
switch1(config)#snmp-server engineID local 192168010004
switch1(config)#snmp-server group iithauth v3 auth
switch1(config)#snmp-server user iith iithauth v3 auth md5 iithsnmp
```

- Get information from Cat 2960

```
$ snmpwalk -v 3 -u iith -l authNoPriv -A iithsnmp 192.168.10.4
```

Enabling SNMPv3 on Linux Server

- Give same configuration to Linux server
- Edit /etc/snmp/snmpd.conf

```
# vi /etc/snmp/snmpd.conf
createUser iith MD5 iithsnmp
rwuser iith auth

# AGENT BEHAVIOR
# Comment for Local system
# Uncomment for all interfaces
agentAddress udp:161,udp6:[::1]:161
```

- Restart snmpd

```
# service snmpd restart
```

- Get system information from your friends