Network Management Introduction

Network Mgmt/Sec.

Jim Binkley

Outline

- OSI management functional areas
  - what is the problem?
- Network Management Systems
- QD (quick&dirty) tool survey
- what is the problem again?

OSI Management Functional Areas

- **Fault management**
  - how to detect/isolate/debug&correct “faults”
- Accounting management (not covered)
- **Configuration and name management** (some)
  - how to manage the namespaces (e.g., DNS/ip)
- **Performance management**
  - how to measure it
- **Security Management** - how to protect it

fault management

- a **fault**: an abnormal "broken" condition
  - an **error** need not be corrected
    - » an ethernet collision, lost packet
  - requires management attention
    - » too many ethernet collisions so work cannot get done
  - examples:
    - » failed router interface or router itself
    - » failed hard disk, etc.
    - » user complains that "network is slow"

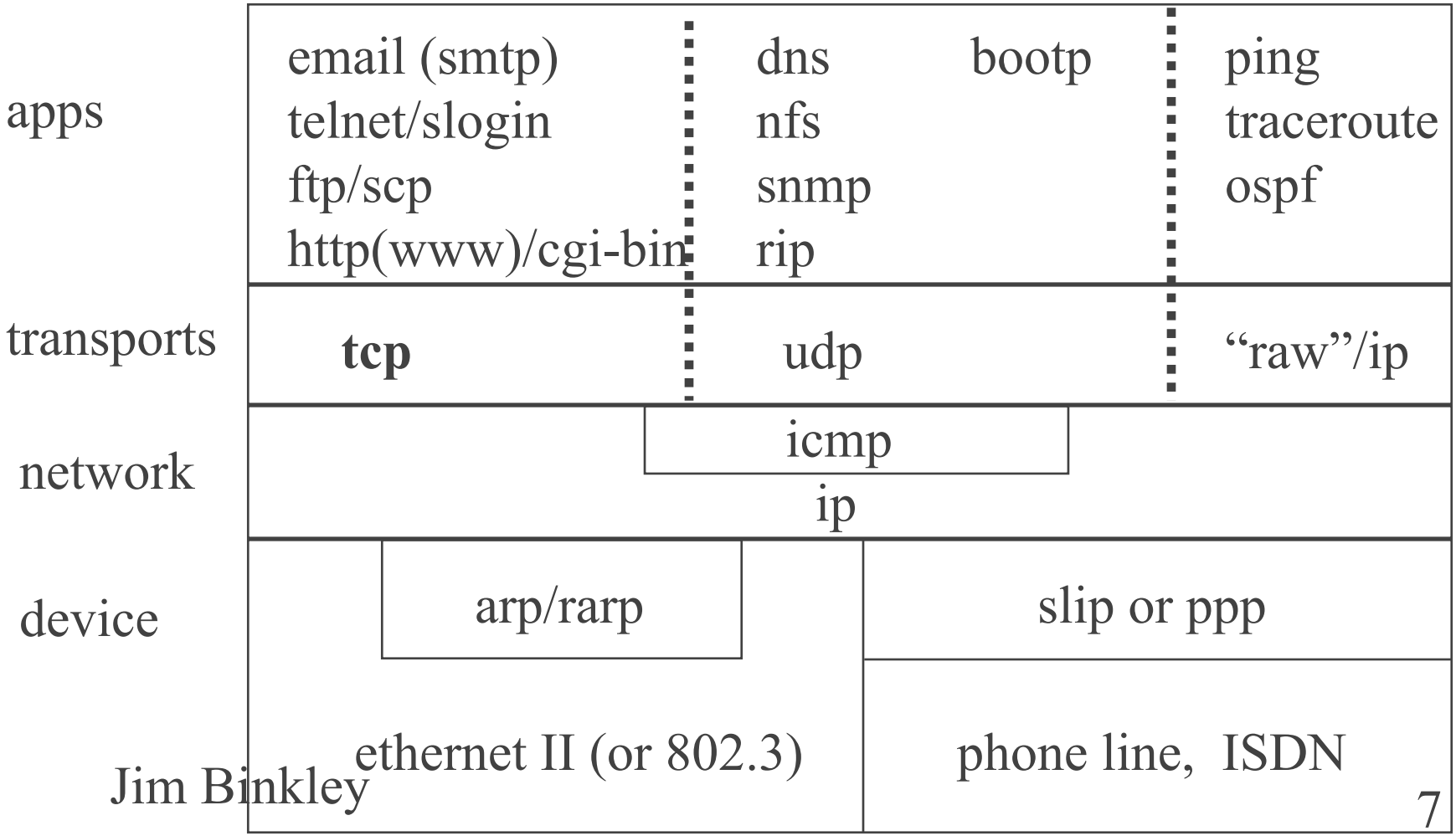
fault mgmt.

- i.e., the world is not simple
- you understand all apps
- you understand your network setup
  - including routers/switches/wiring
  - you know where the wires are
- you know how your equipment works
- you made sure it all speaks SNMP ...
- judgement/experience/deity-level knowledge

time for a small rant

- **“the network is broken”**
- means what ... exactly? ...
  - your host apps
  - your host os
  - your host NIC card
  - your local ethernet segment
  - .all routers/segments in-between?..
    - » including NAT/MAEs
  - their web server/os/nic card

Internet Protocols make ...



protocol soup including new/old

- 802.3z, 802.3u
- 802.11, 802.10, 802.15
- 802.1P, 802.1Q, 802.1d
- RSVP/MBONE/DVMRP/multicast/PIM
- Diff-serve/MPLS/CDP/ISL
- or CIDR/IPSEC/SSL/SNMPv3
- appletalk/ipx/DECNET/SNA/CIPATM

performance management

- networks and hosts but we care about networks here
  - network = infrastructure PLUS hosts
  - however performance is wholistic
    - » bad hark disk doesn't help "net" performance
- performance?
  - per network type
  - through a router or switch, aggregation?
  - hosts can usually blast 100BASE ethernet fine
    - » if they are of recent vintage
    - » or concurrent tcp/web accesses?

distinguish two kinds of performance measurements

- **baselined data** - data collected over a long time period (mrtg: at least 5 minutes)
  - possibly stored in a database for later query analysis
  - focus being how things are changing over time?
- (near) **real-time data** and questions therein
  - » what is happening right now? define *now*,
  - » and define what ...

example:

- 1. mrtg/snmp interface thruput measurements for WAN T1 (whatever) i/f
  - do we need more WAN capacity?
- versus
- 2. real-time comparison of amount of multicast vs unicast traffic
  - might see with **rmon** or P.D. tool like **trafshow** (PSU student work "**ourmon**")
  - important question: how long is sample size?

security management

- question: do we defend ALL hosts on individual basis
  - can we afford to do this?
  - 5000 hosts and 1000 OS? plus apps ...
    - » patches plus diff. os releases make this hard
- or do we defend network at a few single points (secure enclave/firewall approach)
  - and **centralize** management (only a few network mgrs)
  - distributed system approach to host mgmt. is crucial
  - and yet hard - vendors/users are often host-oriented

configuration management

- network =
  - wiring, structured or spaghetti
  - hubs
  - switches
  - routers (some routers are cards in switches)
  - network monitor/s (management console)
  - hosts
    - » servers (web/NEWS/file/computer)
    - » PCs running Wxx, UNIX, APPLE
- can't see forest for trees?

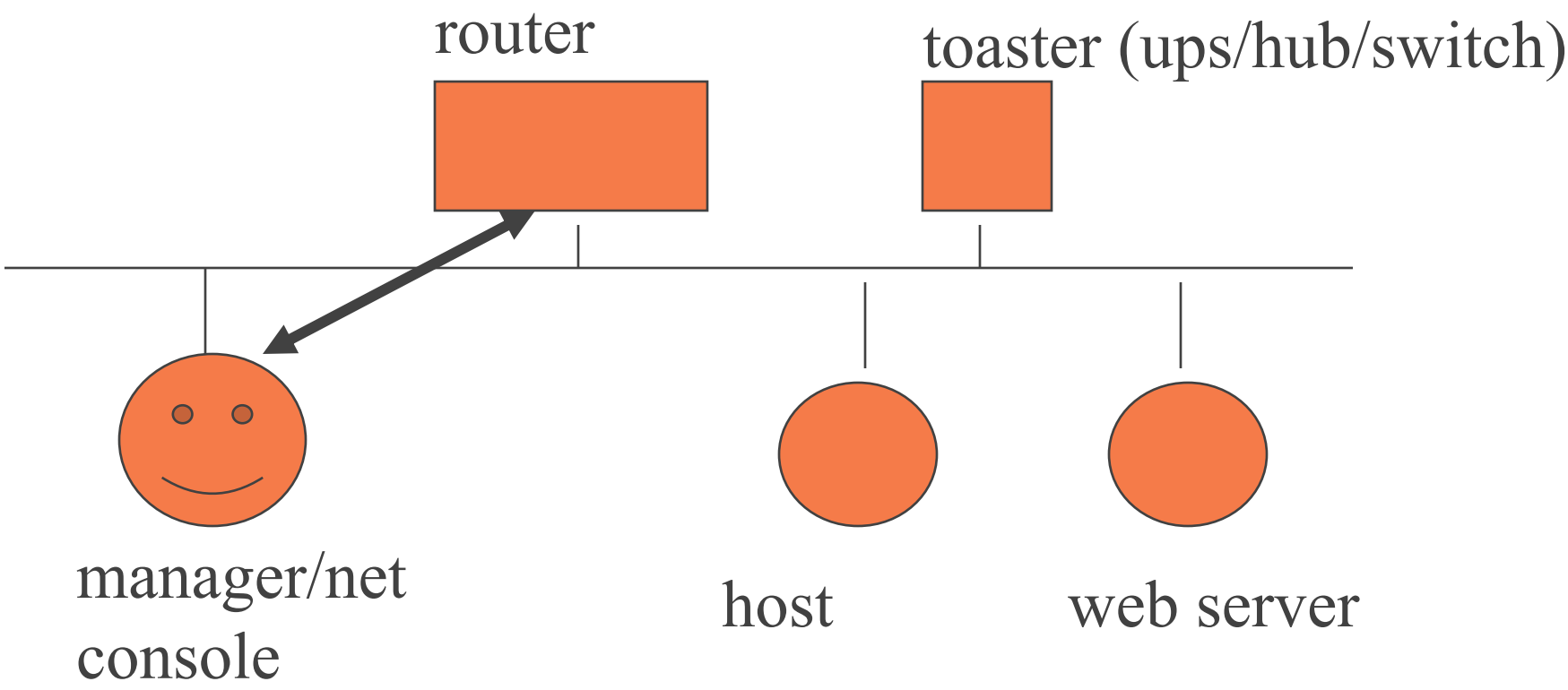
criticism of ISO model

- they don't talk about growing the network
  - we have to have some feel to know how to grow it
  - we need to compare ourselves to others
    - » case studies can be useful
  - get info in a reasonable way and
  - manage both the network, the management tools, and the growth of both

ideal Network Mgmt. System

- distributed approach
- one node is manager/all other nodes are managed
  - irony here is that you have single point of failure problem
- nice wonderful GUI
  - X/Windows/web (web is becoming more common) (note: either os-centric, or *not*)

e.g., SNMP approach



manager polls all nodes (send/response) with SNMP/displays data

if it moves, manage it

"If networking management is viewed as an essential aspect, then it must be universally deployed on the largest possible collection of devices in the network"

Marshall Rose

SO

- **unmanaged hubs** are not a good thing
  - maybe a necessary evil
  - **managed** in SNMP-speak means has SNMP
  - managed always costs more
- one may aim for all routers/switches and core infrastructure boxes
  - and do a less good job on the hosts/servers
  - SNMP on hosts/servers less good anyway
  - very hard to deal with *ALL* host os/all apps

examples of distributed tools:

- HPOpenView Network Node Manager
  - "framework"; i.e., can layer 3rd party products on it
  - e.g., Ciscoworks/Netmetrix/etc. with more specific functions
  - has own basic functionality
- MRTG - multi router traffic grapher - free
  - *now rrdtool/cricket, etc.*
- Big Brother (not SNMP) - free
- *nagios and other ping monitors, is server up?*

HPOV NNM major functions

- router+subnet network map view
  - if a node or net is red -- that's *bad*
- event management
  - catch SNMP traps and pass high-level judgement on other happenings (events)
  - send email/page notification
- SNMP mib browser
- realtime graphs for selected SNMP items

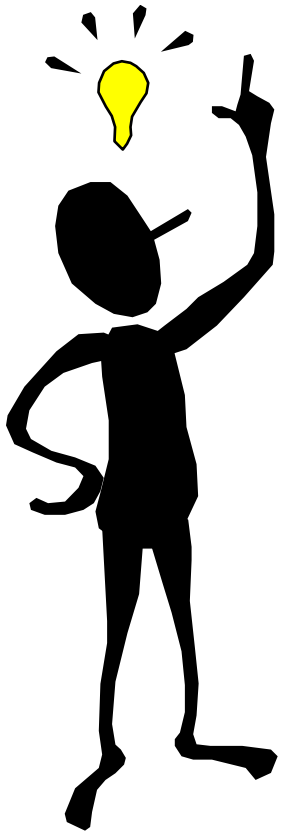
non-distributed, point-focus tools

- **line testers - hw POV**
  - is the wire broken?
- **network analyzers - packet POV**
  - public-domain like tcpdump/solaris snoop
  - or expensive like from network general
  - or part of RMON spec
- not to rule out basic tools
  telnet/dig/nslookup/ping/traceroute/ngrep, a web browser, and maybe netcat ?!

yes ... telnet

- telnet might be the most important tool
- can you telnet to it ... (even the UPS)
  - and what kind of interface do you have when
  - you get there
  - Cisco IOS for routers
    - » switches
    - » other people's switches
    - » MENU-driven (faugh!)

the human brain <-- the tool



some real problems

- too many hosts - not enough time/money
- march of technology --> too many useless details
- distributed nature of problem
  - user X can't talk to web-site Z
- security as a never-ending nightmare
  - hackers have tools - do net mgrs have tools?
- every-growing complexity - especially at link layer

tools we will look at:

- HPOV (if we can, commercial tool)
- ucd-snmp tools (PD)
  - snmp server
  - snmpget/snmpset/snmpwalk
- MRTG and newgen rrdtool/cricket
- big-brother
- tcpdump/trafshow/nmap

tools you should already know

- ping - Packet INternet Groper
- whois (or the web version)
- host/nslookup (DNS)
- dig (DNS, better)
- traceroute
- telnet, yes, telnet
- UNIX: netstat -rn (dump routing table)
- UNIX: arp -a (dump arp table)

final thought

- big network - requires focus on network; ie.., **network engineers don't care about hosts (can't...)**
- toolbase and brain **need distributed focus**, not point focus on individual host
  - we don't have time for individual hosts
  - need distributed picture of network
- netscape or IE may be most important tool soon (right now it is HPOV or telnet)