Hit the Ground Running with SNMP

LISA 2006, Washington, DC

Doug Hughes
doug@will.to

History

- First implementation (v1) in 1988 based on SGMP (97) standardized in 1990
  - get-request, set-request, get-next, get-response, trap
- SNMPv2(c) – 1996 (draft/experimental)
  - locking mechanism
  - 64 bit counters and error handling
  - bulk operations
  - improved Set
- SNMPv3 (standard in 2003, draft 1999)
  - security model
  - access model
  - privacy

The Challengers

- CMIP – OSI protocol ('nuff said)
- CORBA(OMG) – ITU still moving this way
- CMOT – life support (CMIP over TCP/IP RFC 1095)
- WBEM – based upon CIM (Sun, MS, Redhat)
- TL1 (Micromuse(IBM)/Telecordia)
- DMI (DMTF) – CIM – basis for things like IPMI
- TMN (ITU) – aligned with CMIP
- LDAP (really! - proposed as part of an initiative for directory enabled networks)

Concepts

- **Management Station**
- **Management Agent**
- **MIB**
- **OID** (Object identifier)
- Types
- Ports (161 & 162 UDP)
- Encoding
  - ASN.1
- Queries
- Traps
- Informs
- Versions
  - v1
  - v2c
  - v3

Stations and Agents

- Management Station – interface for the people/programs doing the querying of network devices. (e.g. HPOV, etc)
- Management Agent – software running on the device being managed. The Agent responds to requests and sends out traps and inform messages to management stations and other agents
- Management Information Base (MIB) – all managed information is represented with distinct objects (variables)

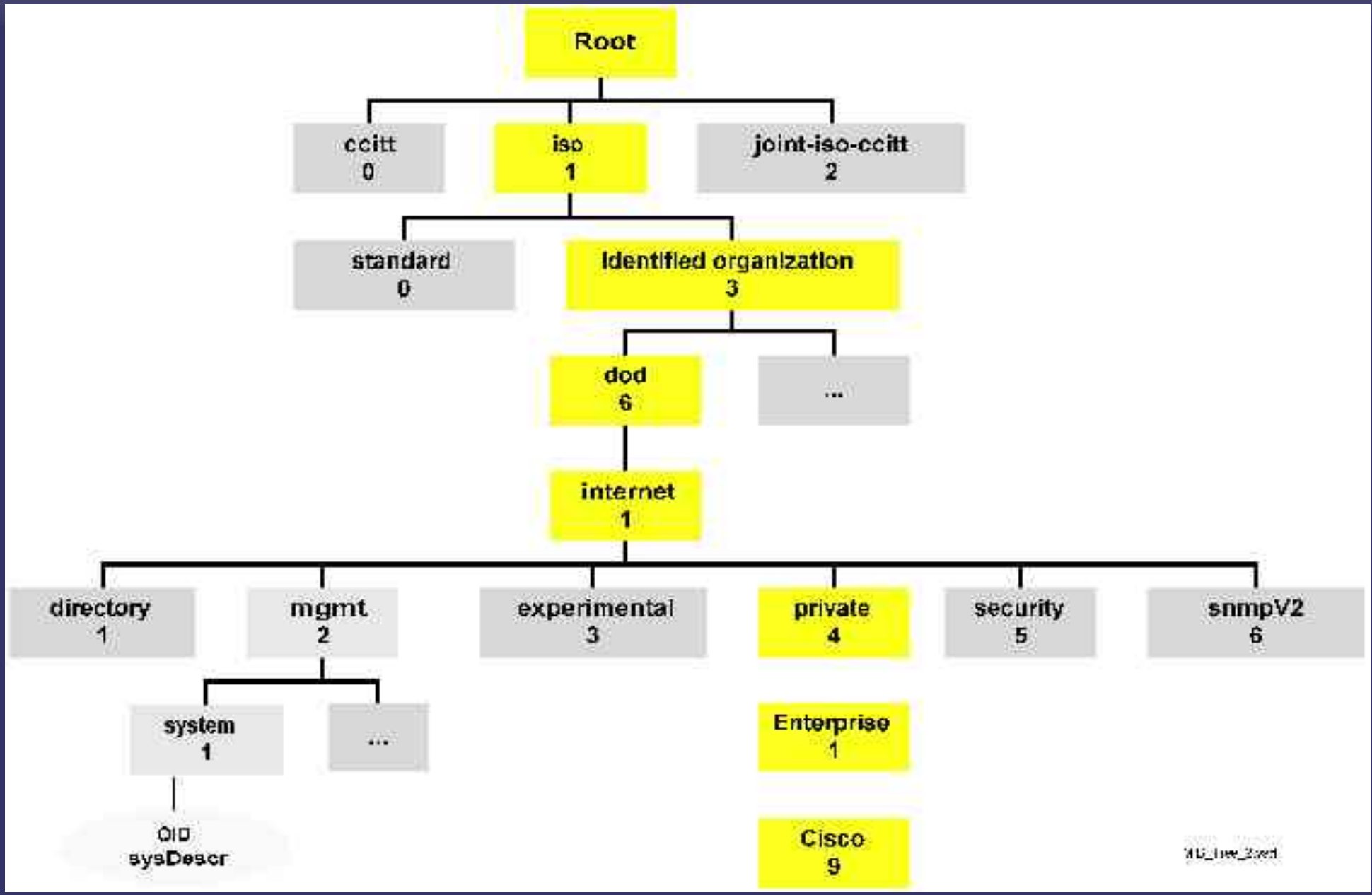
MIB

```
ipForwarding OBJECT-TYPE
    SYNTAX      INTEGER {
                    forwarding(1),    -- acting as a router
                    notForwarding(2)  -- NOT acting as a router
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The indication of whether this entity is acting as an IP
            router in respect to the forwarding of datagrams received
            by, but not addressed to, this entity.  IP routers forward
            datagrams.  IP hosts do not (except those source-routed via
            the host)."
    ::= { ip 1 }
```

OID

.1.3.6.1.2.1.1.1.0 = .iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0
.1.3.6.1.4.1.9 = .iso.org.dod.internet.private.enterprises.cisco
.1.3.6.1.1 = .iso.org.dod.internet.directory
.1.3.6.1.2 = .iso.org.dod.internet.mgmt
.1.3.6.1.3 = .iso.org.dod.internet.experimental
.1.3.6.1.4 = .iso.org.dod.internet.private
.1.3.6.1.5 = .iso.org.dod.internet.security
.1.3.6.1.6 = .iso.org.dod.internet.snmpV2

MIB Tree


Root
ccitt
0
iso
1
joint-iso-ccitt
2
standard
0
Identified organization
3
dod
6
...
internet
1
directory
1
mgmt
2
experimental
3
private
4
security
5
snmpV2
6
system
1
...
Enterprise
1
OID
sysDescr
Cisco
9

Protocol Features

- SNMP v1
  - RFC 1155, 1147, 1212, 1213
  - get, getnext, set, trap
- SNMPv2c
  - RFC 1901-1906
  - extended error codes
  - Getbulk
  - full conceptual row-table
  - improved set
  - limited rollback capability
  - bilingual to v1
- SNMP v3
  - limited availability
  - trilingual
  - RFCs 2570-2575
  - access control
  - authentication
  - privacy
  - views
  - encryption
  - optimized 2-pass SET

SNMP Operations

- PDU (Protocol Data Unit)
  - Get Request / Set Request
  - Get Response
  - GetNext Request
  - Traps
  - Informs (v2) (peer to peer)
  - GetBulk (v2)

Types

- Strings (octet strings)
- Integers (16bit, 32bit and unsigned)
- IP Addresses
- Timetick
- Counters (32bit and 64bit)
- OID
- custom/other

Queries

.iso.org.dod.internet.mgmt.mib-2.system children:
sysDescr sysObjectID sysUpTime sysContact sysName sysLocation

snmpwalk -c <community> -v <version> <host> <object>

```
# snmpget -v 2c -c abc123 myrouter .iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0
system.sysDescr.0 = Cisco Internetwork Operating System Software
IOS (tm) RSP Software (RSP-K4PV-M), Version 12.0(27)S5b, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Fri 12-Aug-05 14:
# snmpgetnext -v 2c -c abc123 myrouter .iso.org.dod.internet.mgmt.mib-2.system.sys-
Descr.0
system.sysObjectID.0 = OID: enterprises.9.1.46
```

Queries...

```
# snmpwalk -v 2c -c abc123 myrouter .iso.org.dod.internet.mgmt.mib-2.inter-
faces.ifTable.ifEntry.ifDescr
interfaces.ifTable.ifEntry.ifDescr.1 = FastEthernet0/1/0
interfaces.ifTable.ifEntry.ifDescr.2 = POS1/0/0
interfaces.ifTable.ifEntry.ifDescr.3 = ATM4/0/0
interfaces.ifTable.ifEntry.ifDescr.4 = Serial5/1/0
interfaces.ifTable.ifEntry.ifDescr.5 = Serial5/1/1
interfaces.ifTable.ifEntry.ifDescr.6 = FastEthernet10/1/0
interfaces.ifTable.ifEntry.ifDescr.7 = POS11/0/0
interfaces.ifTable.ifEntry.ifDescr.8 = Serial12/0/0
interfaces.ifTable.ifEntry.ifDescr.9 = Serial12/0/1
interfaces.ifTable.ifEntry.ifDescr.10 = ATM4/0/0-atm layer
interfaces.ifTable.ifEntry.ifDescr.11 = ATM4/0/0.0-atm subif
...
```

SNMP Read-write

Warning: without SNMPv3 or encrypted transport this information is passed over the network in clear-text

```
# snmpset -c readwrite -v 2c myhost system.sysContact.0 s \
"noc@mycorp.net"
SNMPv2-MIB::sysContact.0 = STRING: noc@mycorp.net
#
```

Tool Evolution

- ISODE – very heavy, hard to port. compiler generated code
- CMU SNMP – yay! easy to use!
- UCD SNMP – attempt to support security in v2 (evolution of CMU) and cross-platform compilation
- Net-SNMP – rename of UCD in 2000, open source
- Perl, Tcl, Python, Awk(!), commercial (e.g. Castle Rock, HPOV, Netcool), scotty, etc

Tools

- Perl (Net::SNMP)
- Tcl (Scotty)
- scli (command line snmp interface with tabular display)
- MRTG/RRDTool
  - 1995 first release of MRTG – 100% Perl, scalability issues
  - Development of round-robin databases (RRD) for time-series data.

Scotty

```
% set s [snmp session]
% $s configure -address myrouter -version SNMPv2c -community abc123
% mib successor system
sysDescr sysObjectID sysUpTime sysContact sysName sysLocation sysServices sysOR-
LastChange sysORTable
% mib parent system
mib-2
% $s get sysUpTime.0
{1.3.6.1.2.1.1.3.0 TimeTicks {173d  8:54:55.25}}
% mib oid ifName.0
1.3.6.1.2.1.31.1.1.1.1.0
% mib syntax ifName.0
DisplayString
```

ASN.1

- formal language for defining message syntax for device communication
- The basis for MIBS
- complaints that it is as complex or more than the problem space it is trying to solve
- "*ASN.1 is complicated, and the testing is never thorough enough*" - Steve Bellovin

```
ifNumber OBJECT-TYPE
   SYNTAX      INTEGER32
   MAX-ACCESS read-only
   STATUS      current
   DESCRIPTION
         "The number of net-
    work interfaces (re-
    gardless of their cur-
    rent state) present"
:: = { interfaces 1 }
```

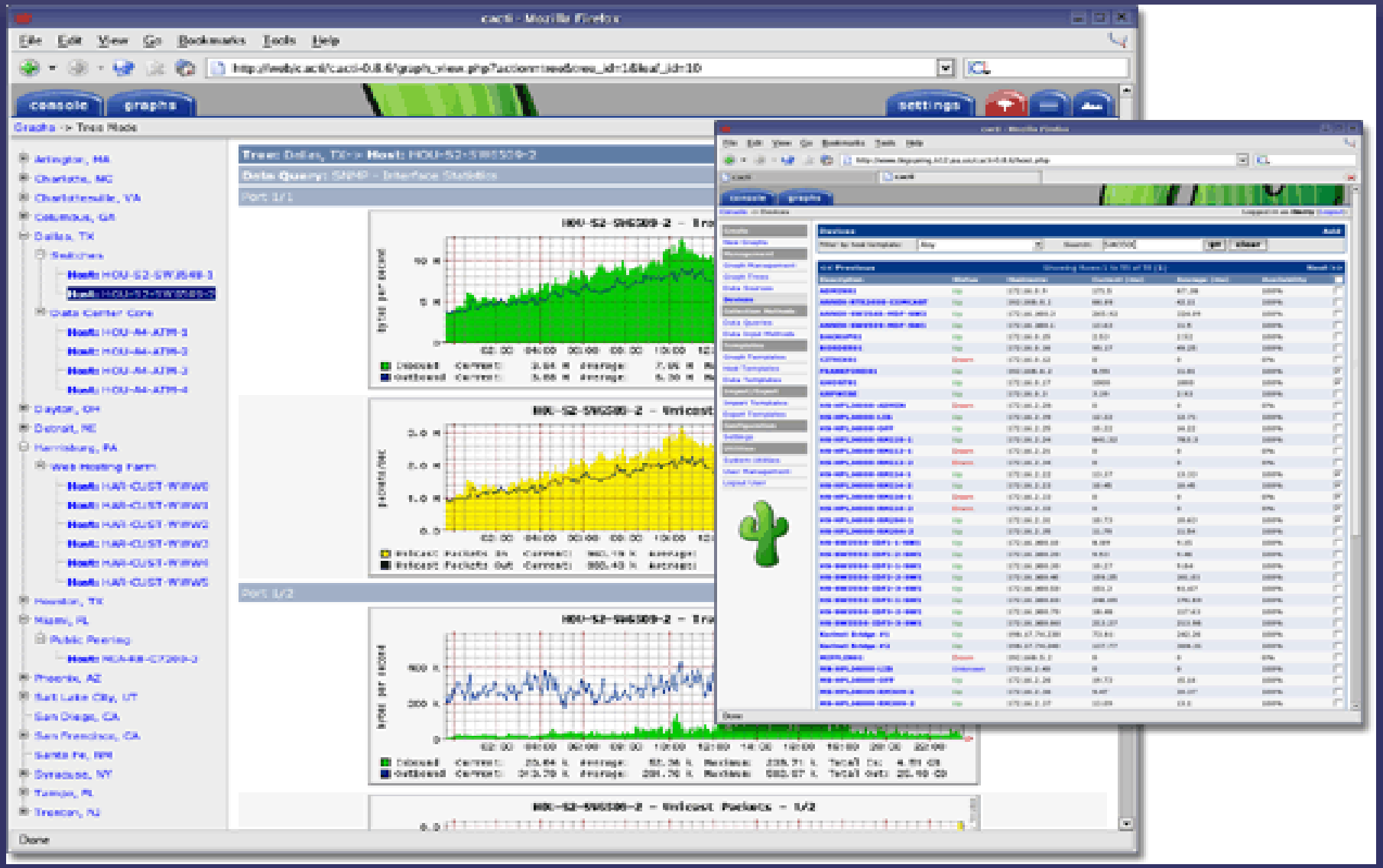
Useful things you can manage

- Router stats
  - Interface stats (load, packets, bits, drops, errors, rates)
  - CPU stats
  - FRUs
  - environmentals
  - acl hits/policers
  - thresholds
  - much much more
- System stats
  - process thresholds
  - load
  - logins
  - environmentals
  - FRU failures
  - CPU (load and user/system/wait/idle)
  - reboots and uptime
  - more...

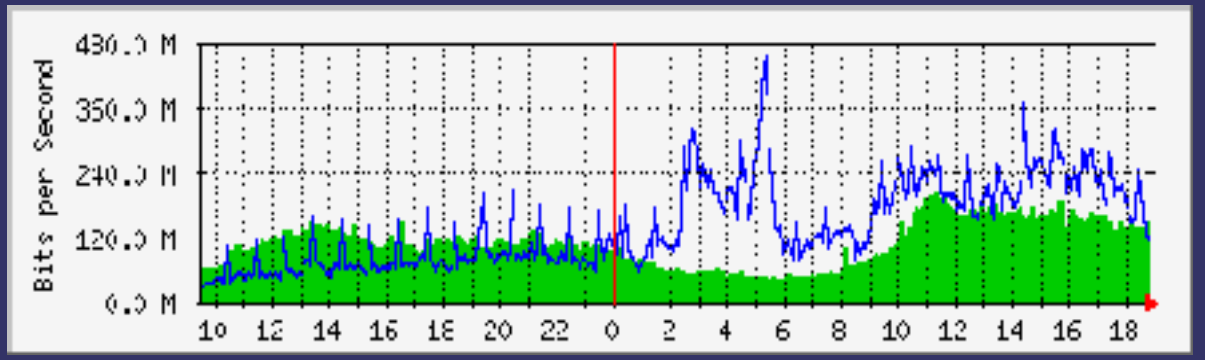
Things that make pretty graphs (and stuff)

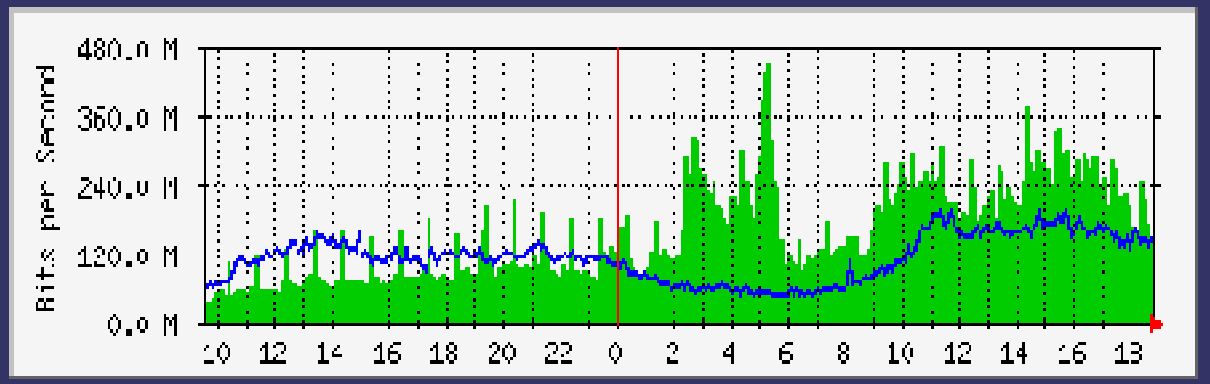
- Cacti
- MRTG
- SolarWinds
- netdisco (total network discovery)
- HPOV
- Netcool (ISM, SSM, SLAmanager, Precision, etc)
- Zenoss

Cacti

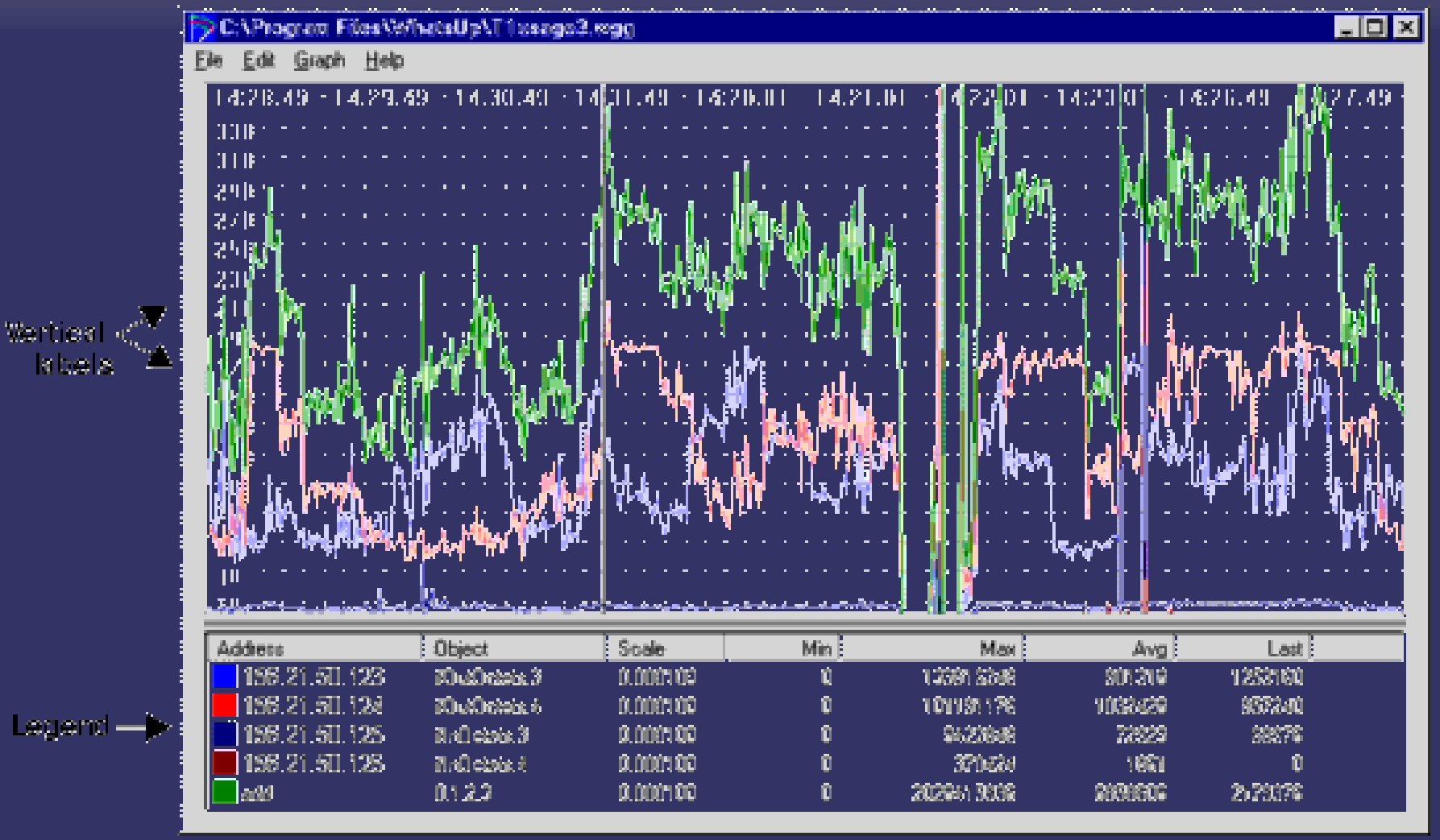

cacti - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
console
graphs
settings
Graphs -> Tree Mode
Arlington, MA
Charlotte, NC
Charlottesville, VA
Columbus, GA
Dallas, TX
Switches
Data Center Core
Dayton, OH
Detroit, NE
Harrisburg, PA
Web Hosting Farm
Houston, TX
Miami, FL
Public Peering
Phoenix, AZ
Salt Lake City, UT
San Diego, CA
San Francisco, CA
Santa Fe, NM
Syracuse, NY
Tampa, FL
Trenton, NJ
Tree: Dallas, TX -> Host:
Data Query: SNMP - Interface Statistics
Port: 1/1
Port: 1/2
Done

MRTG

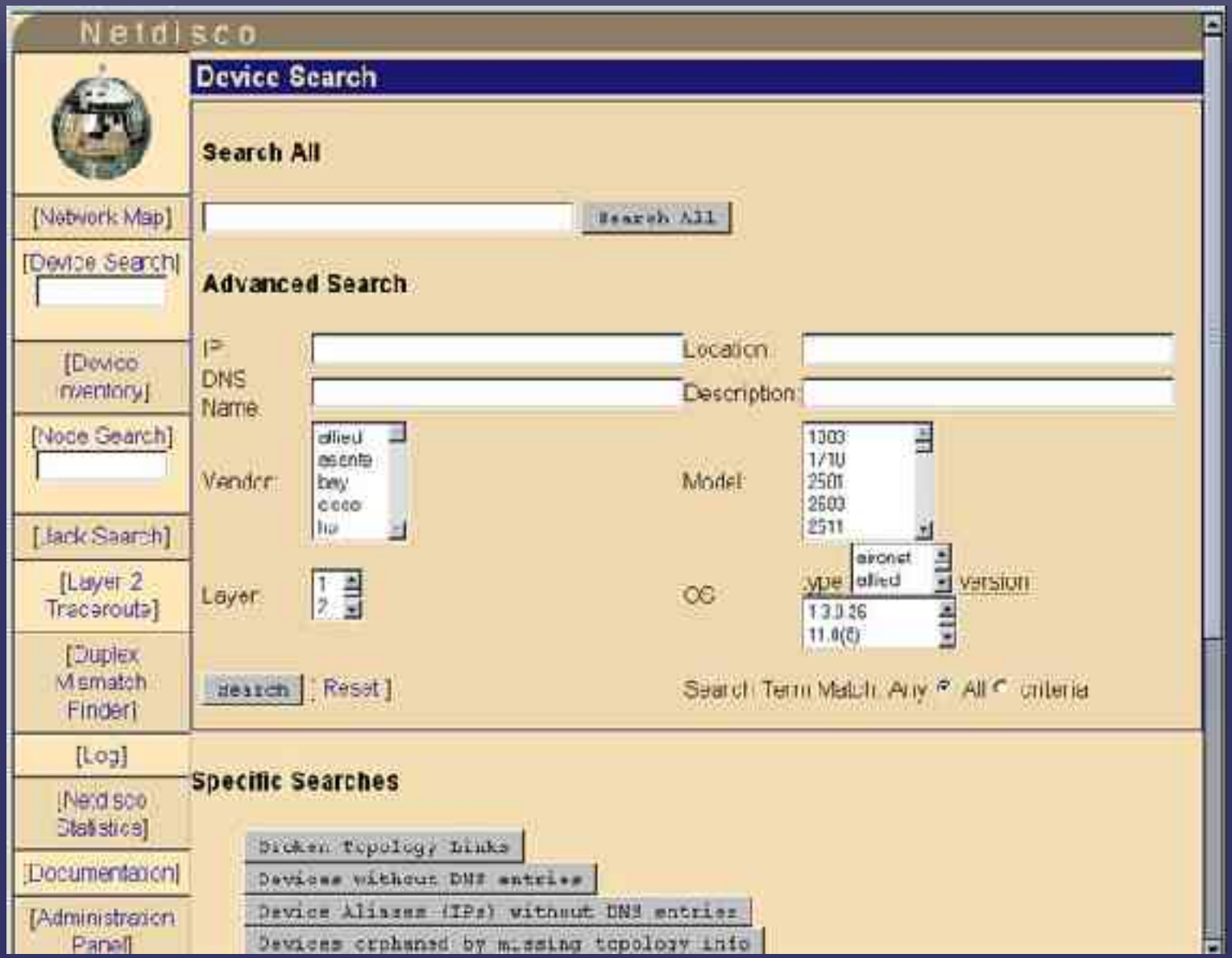

Bits per Second
480.0 M
360.0 M
240.0 M
120.0 M
0.0 M
10 12 14 16 18 20 22 0 2 4 6 8 10 12 14 16 18


Bits per Second
480.0 M
360.0 M
240.0 M
120.0 M
0.0 M
10 12 14 16 18 20 22 0 2 4 6 8 10 12 14 16 18

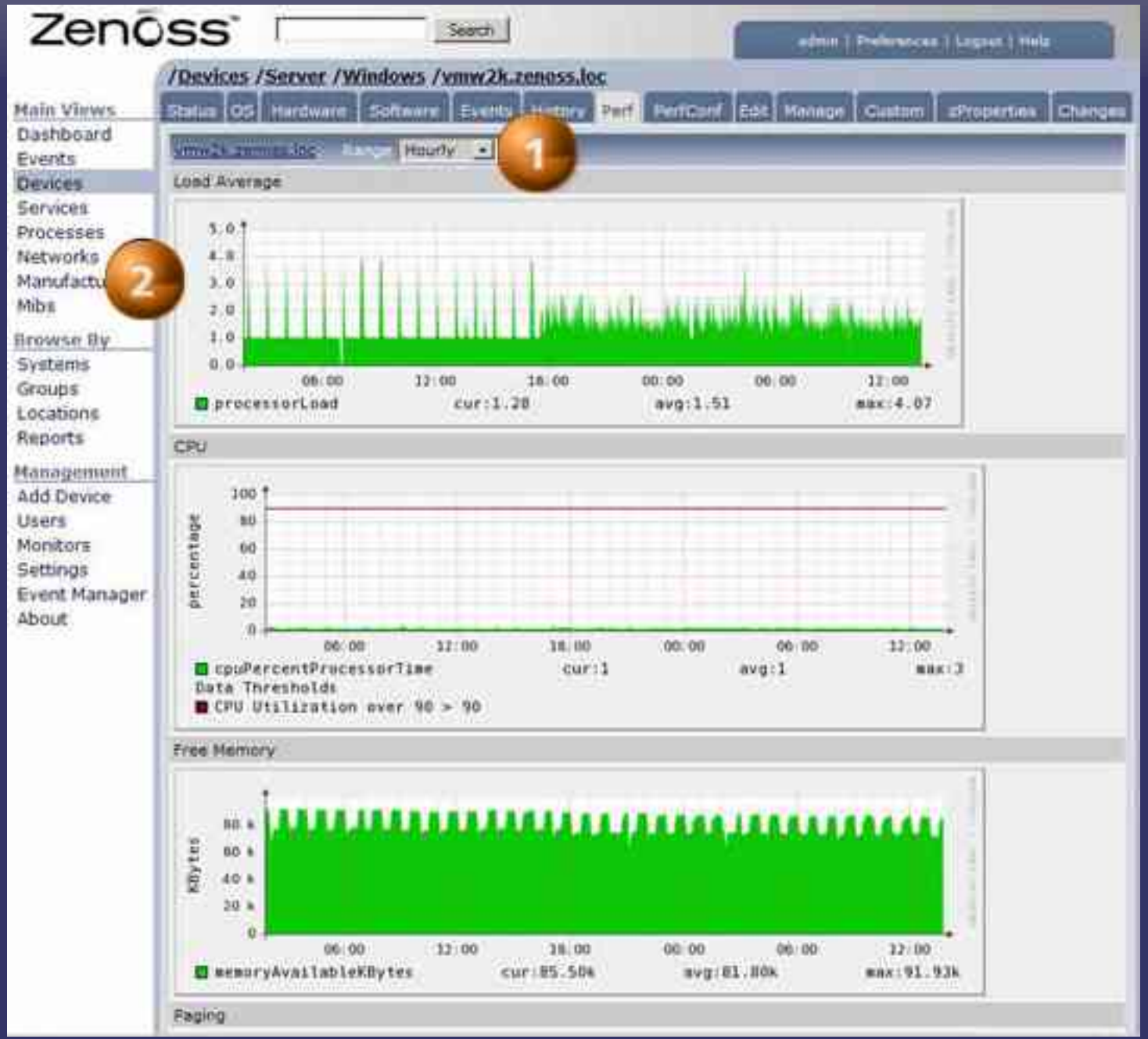
WhatsUp Gold



Netdisco


Netdisco
Device Search
Search All
[Network Map]
[Device Search]
[Device Inventory]
[Node Search]
[Jack Search]
[Layer 2 Traceroute]
[Duplex Mismatch Finder]
[Log]
[Netdisco Statistics]
[Documentation]
[Administration Panel]
Search All
Advanced Search
IP
DNS Name
Location
Description
Vendor:
Model:
Layer
OS
Type
Version
search
Reset
Search Term Match: Any All criteria
Specific Searches
Broken topology links
Devices without DNS entries
Device Aliases (IPs) without DNS entries
Devices orphaned by missing topology info

Zenoss


Zenoss
Search
admin | Preferences | Logout | Help
/Devices /Server /Windows /vmw2k.zenoss.loc
Main Views
Dashboard
Events
Devices
Services
Processes
Networks
Manufactu
Mibs
Browse By
Systems
Groups
Locations
Reports
Management
Add Device
Users
Monitors
Settings
Event Manager
About
Status
OS
Hardware
Software
Events
History
Perf
PerfConf
Edit
Manage
Custom
zProperties
Changes
Hourly
1
2
Load Average
5.0
4.0
3.0
2.0
1.0
0.0
06:00
12:00
18:00
00:00
06:00
12:00
processorLoad
cur:1.28
avg:1.51
max:4.07
CPU
percentage
100
80
60
40
20
0
cpuPercentProcessorTime
cur:1
avg:1
max:3
Data Thresholds
CPU Utilization over 90 > 90
Free Memory
KBytes
80 k
60 k
40 k
20 k
0
memoryAvailableKBytes
cur:85.50k
avg:81.80k
max:91.93k
Paging

SNMP Traps

- Traps sent to one or more management stations
- Components
  - Source device
  - Agent (for relayed traps)
  - Enterprise (the OID sending the trap)
  - varbind list ($1, $2, ... $n)
    - a list of OIDs with values which map to objects in the device MIB
    - as if the values had been polled with snmpget or snmpgetnext

Trap example

- SNMP trap
  - OID1 = .1.3.6.1.2.1.15.3.1.14.152.97.234.114 = “” - bgp last error
  - OID2 = .1.3.6.1.2.1.15.3.1.2.152.97.234.114 = “1” - bgp peer state
  - enterprise 1.3.6.1.2.1.15.7 = bgp traps
  - generic-trap 6 (6 = generic traps are most often 6 = enterprise specific)
  - specific-trap 2
  - community = 10011-1-Fujitsu-L3VPN@TRAPS (from information specific to the router config for the bgp session experiencing session transition)

RMON

- Remote Monitoring – standard on most enterprise routers (Cisco and Juniper for sure) -
- RFC 1271 (1992), RFC 1757 (1995) – draft standard
- RMON Groups
  - statistics – statistics for each monitored interface
  - history – periodic samples from configured managed network
  - alarm – check particular variables and alarm when they threshold
  - host – statistics associated with discovered hosts
  - HostTopN – rate-based statitics for traffic among talk talkers
  - Packet Capture – capture interface traffice remotely
  - Events – control event generation and notification (SNMP traps)

Things you probably didn't know you could do with SNMP or were too afraid to try

- Reconfig/recover a router with SNMP-RW strings that has lost telnet/ssh access
- dump a full CAM table and correlate with host MAC addresses (cammer.pl et al.)
- SNMP traceroute including interface name, bandwidth, next hop, speed and loading
- GET FRU failures for fans, power supplies, temperature threshold crossings, and more from Sun Netras and other NEMS devices.
- Monitor high and low threshold crossings with hysteresis for **any** variable that is monitorable via SNMP (RMON)