

Carnegie Mellon University
Computing Services

Campus Network Architecture, Management, and Monitoring

Steve Rhoton

1

Carnegie Mellon University
Computing Services

Agenda

- Campus Network architecture
- Campus Network size and statistics
- Managing and monitoring the network

2

Carnegie Mellon University
Computing Services

Network Architecture

- Design goals and standards:
 - Always redundant, everywhere possible
 - Redundant fiber pathways diverse as possible
 - Always plan for more capacity than needed
 - Network must be managed and monitored
 - We must be able to understand what is happening on the network

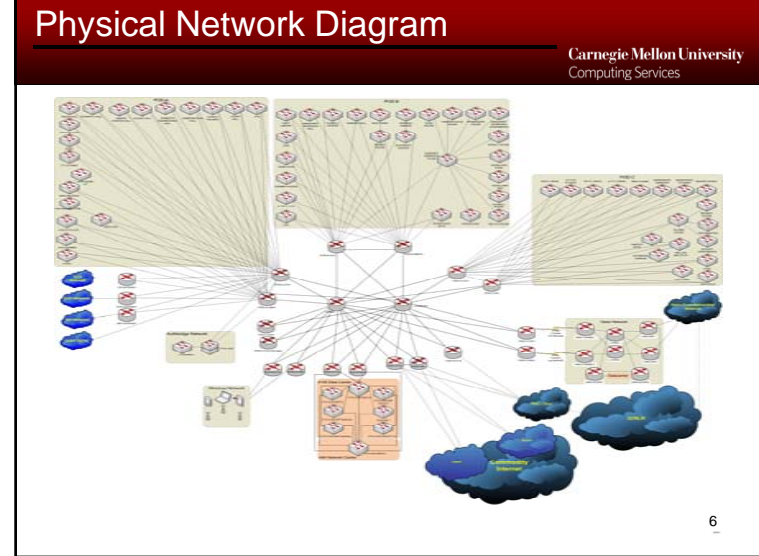
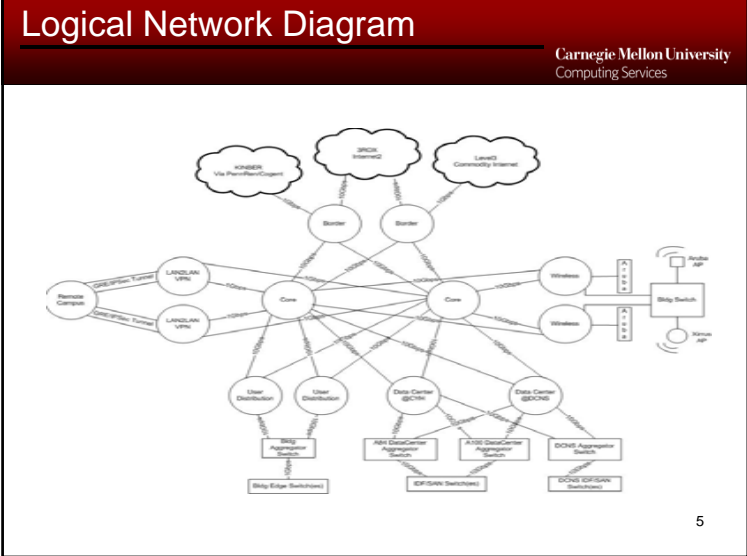
3

Carnegie Mellon University
Computing Services

Network Architecture

- “Border” routers connect to providers
- “Core” routers connect to border routers
- Wired network “distribution” routers connect to core routers
- Wireless “distribution” routers connect to cores
- Remote site VPN routers connect to cores
- Building switches connect to distribution routers
- User switches connect to building switches

4



- ### How Large is our Campus Network?
- Carnegie Mellon University
Computing Services
- 4 major sites around the world
 - ~90 buildings across main campus
 - 20 enterprise class routers
 - 1,000+ data switches
 - 50,000+ wired outlets
 - 71 miles of copper (connecting outlets to switches)
 - 531 miles of fiber
 - 3,000+ 802.11 wireless access points
 - 5,000,000+ square feet of indoor wireless coverage
 - 1-2 acres of outdoor wireless coverage (expanding in 2014)
- 7

- ### How Large is our Campus Network?
- Carnegie Mellon University
Computing Services
- 578 VLANs
 - 884 Subnets
 - 3,000+ Users
 - 170,000+ Registered Machines
- 8

Protocols We Rely On

Carnegie Mellon University
Computing Services

- OSPF
- BGP
- Rapid Spanning-Tree
- CDP
- IPv4/v6
- TCP
- UDP
- ARP
- ... and many others

9

Network Monitoring - Goals

Carnegie Mellon University
Computing Services

- To clearly understand who is doing what on your network at any time.

10

Identifying Devices

Carnegie Mellon University
Computing Services

- Information that allows a device to work on the network (Layer 2, Layer 3)
- Information about what a device is doing on the network (Layer 3)
- Information about the device itself (Layers 4-7)

11

Identifying Devices - Layer 2

Carnegie Mellon University
Computing Services

- MAC Address
 - Found in:
 - DHCP requests
 - ARP and CAM data
 - Radius Data
 - Useful for:
 - Uniquely identifying the machine
 - Possibly identifying the machine manufacturer

12

Identifying Devices – Layer 3

Carnegie Mellon University
Computing Services

- IP Address
 - Found in:
 - DNS Requests
 - ARP and CAM data
 - Useful for:
 - Uniquely identifying the machine with its network and subnet
 - Must be tied to external tool (DHCP, IPAM, Radius) to get more accounting information

13

Identifying Devices – Layer 3

Carnegie Mellon University
Computing Services

- Network Switch and Routing Information
 - Found in:
 - Switch / Router Configs and SNMP
 - Useful for:
 - Finding Real-time connection and network path information

14

Identifying Devices – Layer 3

Carnegie Mellon University
Computing Services

- Network Flow Data
 - Found in:
 - Netflow v5 and v9 data
 - Various other applications (Argus, tcpdump)
 - Useful for:
 - Discovering traffic to and from a host
 - Finding the protocols a machine is using
 - Find throughput for a machine

15

Identifying Devices – Layer 7

Carnegie Mellon University
Computing Services

- Machine Registration
 - External Application That Maintains IP addresses for specific machines
- Payload Capture
 - Netflow v9, Argus
 - Complete Packet Payload

16

Identifying Users

Carnegie Mellon University
Computing Services

- IPAM Registration
 - IP/MAC -> User Mapping
- User Based Network Access (Radius)
 - VPN
 - 802.1x
 - WPA
- Syslog
 - MAC/IP User Information

17

CMU Custom Network Monitoring Applications

Carnegie Mellon University
Computing Services

- NetReg – IPAM, DNS, DHCP Management
- Bandwidth – Netflow and Bandwidth Tool
- DNS
- DHCP
- Radius
- Netinform/NLS – Network Archive Tool
- NISC – Incident Management Tool
- BKAD – Network Telemetry Data

18

NetReg

Carnegie Mellon University
Computing Services

Network Registration

Main

[Main](#) [Search Machines](#) [Search Outlets](#) [Reports](#) [Help](#) [Signoff](#)

[Activations](#) [Attributes](#) [Buildings](#) [Cables](#) [Dept Cntrl](#) [DHCP](#) [DNS](#)
[Networks](#) [Outlet Types](#) [Protections](#) [Services](#) [Scheduler](#) [Subnets](#)
[Telecom](#) [Trunk Set](#) [Users/Groups](#) [Vlans](#) [Zones](#)

Registered machines and outlets for: Stephen Rhoton

Registered Machines [Help](#)

[Register New Machine](#) [Search Your Machines](#) [View Expiring Machines](#)

Select a column heading to sort by the column field.

[First Page](#) | [Next Page](#)

Hostname	Hardware Address	Mode	IP Address	Subnet
260-2.IBM.COM		static	128.2.6.140	NetDev
ALICE3.PBWORKS.COM		reserved	0.0.0.0	NetDev
APERTURE-SQL.ANDREW.CMU.EDU	000C29358878	static	128.2.6.54	NetDev
APERTURE-TEST.ANDREW.CMU.EDU	000C297F43E3	static	128.2.6.49	NetDev

19

Bandwidth

Carnegie Mellon University
Computing Services

Date	Total In (MB)	Total Out (MB)	Greatest Value (MB)
2011-03-28	6942 MB	105 MB	6942 MB
2011-03-29	3643 MB	85 MB	3643 MB
2011-03-30	14 MB	1 MB	14 MB
2011-03-31	2506 MB	70 MB	2506 MB
2011-04-01	926 MB	66 MB	926 MB
Total:	14031 MB	327 MB	Five Day Running Avg: 2866.2 MB

20

NetInform/NLS

Carnegie Mellon University
Computing Services

- Collects DNS, DHCP and Switch Information
- ARP, MAC Data
- Time-based

21

NetInform/NLS

Carnegie Mellon University
Computing Services

The screenshot shows the NetInform/NLS interface for IP 128.2.6.231. It displays the hostname as TROPOI.NET.CMU.EDU and provides networking information including MAC address (00:23:DF:FF:12:AA), IP address (128.2.6.231), subnet (Network Development), group members (jpy@andrew.cmu.edu, camp@andrew.cmu.edu, swhot@andrew.cmu.edu, swhot@andrew.cmu.edu), and owners (jpy@andrew.cmu.edu).

22

NISC

Carnegie Mellon University
Computing Services

Created At	Created By	Updated At	Updated By	Machines	Users	Watchers
2011-03-24 15:31:47	admin	2011-03-24 15:52:03	admin	172.31.50.232	swhot@OC4D6444-8300-11C	
2011-03-29 11:28:22	omnies@ANDREW	2011-03-29 11:32:57	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		
2011-03-29 14:20:21	omnies@ANDREW	2011-03-29 14:26:24	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		
2011-03-29 14:35:49	omnies@ANDREW	2011-03-29 14:42:27	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		
2011-03-29 14:44:11	omnies@ANDREW	2011-03-29 14:55:31	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		
2011-03-29 14:56:38	omnies@ANDREW	2011-03-29 15:08:35	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		
2011-03-29 16:01:37	omnies@ANDREW	2011-03-29 16:14:59	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		
2011-03-29 16:16:40	omnies@ANDREW	2011-03-29 16:28:04	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		
2011-03-29 08:30:25	omnies@ANDREW	2011-03-29 16:42:11	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		
2011-03-29 16:42:55	omnies@ANDREW	2011-03-30 11:36:56	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		
2011-03-30 09:24:59	lerchey@ANDREW	2011-03-30 09:26:37	lerchey@ANDREW	128.237.144.170	lerchey@00000000-0000-1000	
2011-03-30 07:31:30	omnies@ANDREW	2011-03-30 16:21:45	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		
2011-03-30 12:22:23	omnies@ANDREW	2011-03-30 16:23:16	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		
2011-03-30 16:24:29	omnies@ANDREW	2011-03-30 16:36:20	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		
2011-03-30 13:00:53	omnies@ANDREW	2011-03-30 17:01:43	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		
2011-03-30 13:02:02	omnies@ANDREW	2011-03-30 17:10:59	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		
2011-03-31 10:10:45	lerchey@ANDREW	2011-03-31 10:33:24	lerchey@ANDREW	128.2.161.236	lerchey@remote	help@cs.cmu.edu, sco-remote
2011-03-31 10:47:24	lerchey@ANDREW	2011-03-31 10:50:43	lerchey@ANDREW	128.237.144.221	lerchey@00000000-0000-1000	
2011-03-31 10:53:30	lerchey@ANDREW	2011-03-31 10:56:52	lerchey@ANDREW	172.31.50.46	lerchey@00000000-0000-1000	
2011-03-31 10:54:51	omnies@ANDREW	2011-03-31 10:55:52	omnies@ANDREW	128.2.125.191 58.80.35.F3.7		

23

BKAD

Carnegie Mellon University
Computing Services

The screenshot shows the BKAD interface with a search for a device (MAC: 128.2.6.12) and a table of Syslog Data. The Syslog Data table contains the following entries:

Timestamp	Message
2014/10/19 11:46:54	Oct 19 11:46:54 pod-t-fu1.gvu.cmu.net %FWSM-4-106023: Deny udp src OUTSIDE:162.212.181.242/19639 dst SIXNET:128.2.6.12/53 by access-group 'OUTSIDE_IN' [0x0, 0x0]
2014/10/19 11:56:49	Oct 19 11:56:49 pod-t-fu1.gvu.cmu.net %FWSM-4-106023: Deny tcp src OUTSIDE:128.0.114.184/6000 dst SIXNET:128.2.6.12/3388 by access-group 'OUTSIDE_IN' [0x0, 0x0]
2014/10/19 12:11:24	Oct 19 12:11:24 pod-t-fu1.gvu.cmu.net %FWSM-4-313004: Denied ICMP type=3, from laddr: 193.34.70.10 on interface OUTSIDE to 128.2.6.12: no matching session
2014/10/19 12:12:55	Oct 19 12:12:55 pod-t-fu1.gvu.cmu.net %FWSM-4-106023: Deny tcp src OUTSIDE:93.174.93.51/42969 dst SIXNET:128.2.6.12/60383 by access-group 'OUTSIDE_IN' [0x0, 0x0]
2014/10/19 12:13:41	Oct 19 12:13:41 pod-t-fu1.gvu.cmu.net %FWSM-4-106023: Deny tcp src OUTSIDE:71.6.145.200/43603 dst SIXNET:128.2.6.12/62078 by access-group 'OUTSIDE_IN' [0x0, 0x0]
2014/10/19 12:13:57	Oct 19 12:13:57 pod-t-fu1.gvu.cmu.net %FWSM-4-106023: Deny tcp src OUTSIDE:190.190.131.2/6096 dst SIXNET:128.2.6.12/443 by access-group 'OUTSIDE_IN' [0x0, 0x0]
2014/10/19 12:13:59	Oct 19 12:13:59 pod-t-fu1.gvu.cmu.net %FWSM-4-106023: Deny tcp src OUTSIDE:190.190.131.2/6096 dst SIXNET:128.2.6.12/443 by access-group 'OUTSIDE_IN' [0x0, 0x0]
2014/10/19 12:19:36	Oct 19 12:19:36 pod-t-fu1.gvu.cmu.net %FWSM-4-106023: Deny tcp src OUTSIDE:168.190.131.2/6096 dst SIXNET:128.2.6.12/443 by access-group 'OUTSIDE_IN' [0x0, 0x0]
2014/10/19 12:41:19	Oct 19 12:41:19 pod-t-fu1.gvu.cmu.net %FWSM-4-106023: Deny udp src OUTSIDE:162.212.181.242/7940 dst SIXNET:128.2.6.12/53 by access-group 'OUTSIDE_IN' [0x0, 0x0]
2014/10/19 14:19:27	Oct 19 14:19:27 pod-t-fu1.gvu.cmu.net %FWSM-4-106023: Deny udp src OUTSIDE:162.212.181.242/29432 dst SIXNET:128.2.6.12/53 by access-group 'OUTSIDE_IN' [0x0, 0x0]

24

CMU Commercial Network Monitoring Applications

Carnegie Mellon University
Computing Services

- NetMRI
(<http://www.infoblox.com/en/products/netmri.html>)
- NetQoS
(<http://www.ca.com/content/Integration/netqos.aspx>)
- AirWave
(<http://www.arubanetworks.com/products/management-security-software-2/airwave/>)
- Nagios (<http://www.nagios.org/>)

25

Q&A

Carnegie Mellon University
Computing Services

- Questions?

26