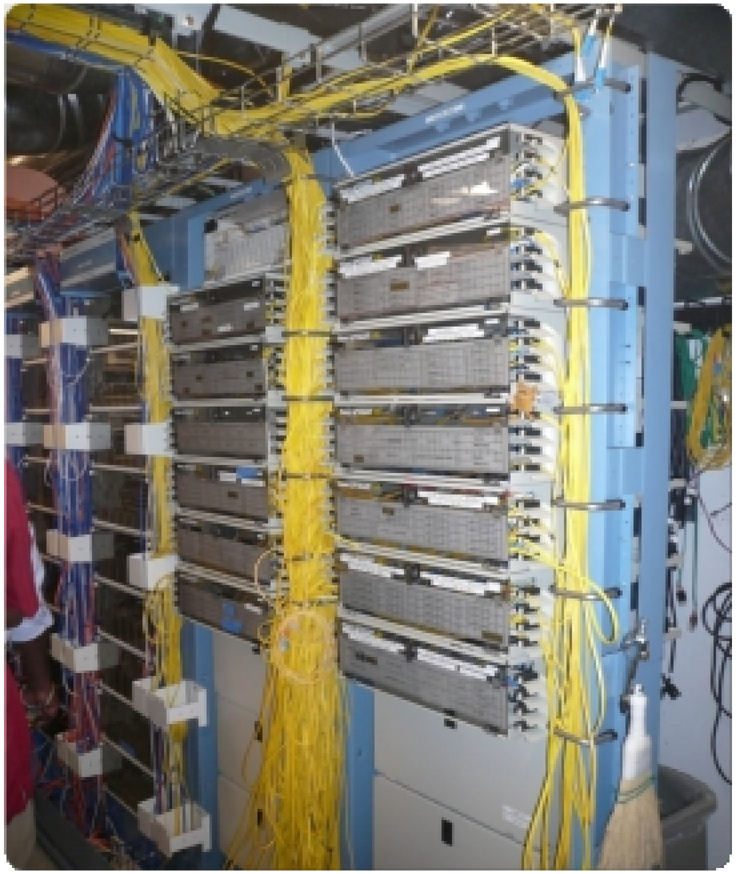
Part II: Details

Some details on the core concepts:

- Network documentation
- Diagnostic tools
- Monitoring tools
- Performance tools
- Active and passive tools
- SNMP
- Ticket systems
- Configuration and change management

Documentation

Maybe you've asked, "*How do you keep track of it all*?"...



Document, document, document...

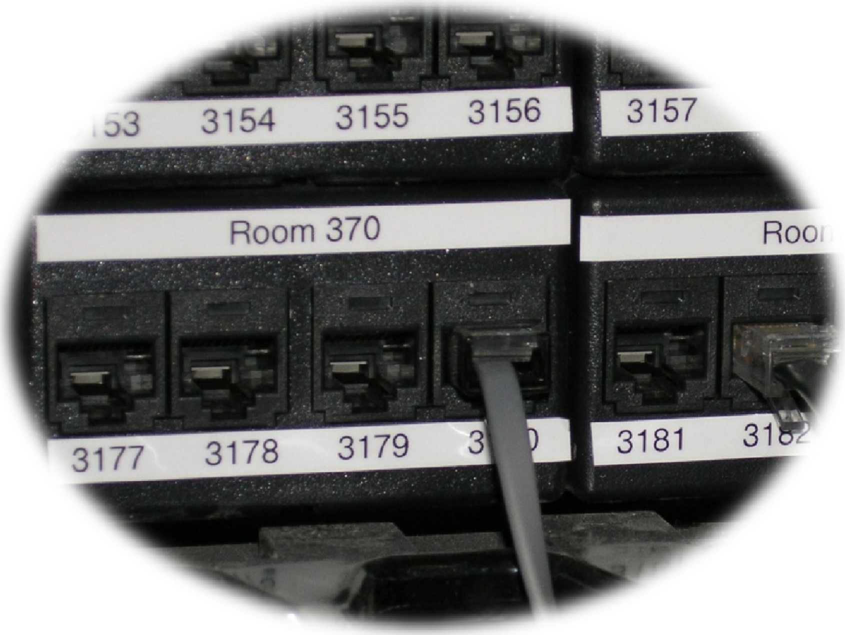
Documentation

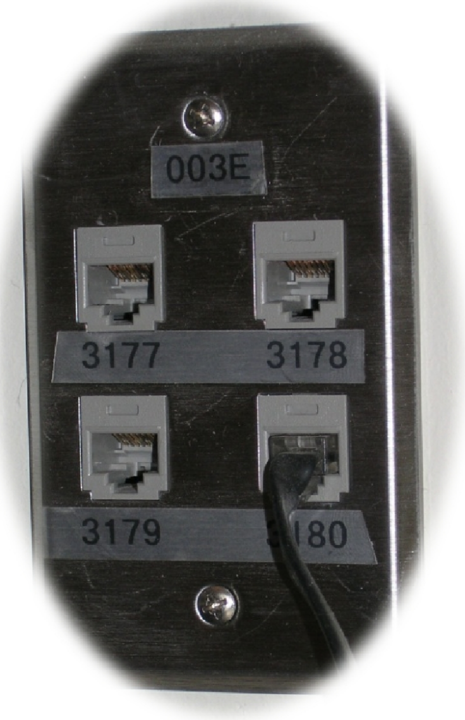
Basics, such as documenting your switches...

- What is each port connected to?
- Can be simple text file with one line for every port in a switch:
  - health-switch1, port 1, Room 29 – Director’s office
  - health-switch1, port 2, Room 43 – Receptionist
  - health-switch1, port 3, Room 100 – Classroom
  - health-switch1, port 4, Room 105 – Professors Office
  - …..
  - health-switch1, port 25, uplink to health-backbone
- This information might be available to your network staff, help desk staff, via a wiki, software interface, etc.
- Remember to label your ports!

Documentation: Labeling

Nice… ☺





Network Documentation

More automation might be needed. An automated network documentation system is something to consider.

- You can write local scripts to do this.
- You can consider some automated documentation systems.
- You’ll probably end up doing both.

Automated Systems

There are quite a few automated network documentation systems. Each tends to do something different:

- IPplan: http://iptrack.sourceforge.net/
- Netdisco: http://netdisco.org/
- Netdot: https://netdot.uoregon.edu/

IPplan:

From the IPplan web page:

“IPplan is a free (GPL), web based, multilingual, TCP IP address management (IPAM) software and tracking tool written in php 4, simplifying the administration of your IP address space. IPplan goes beyond TCPIP address management including DNS administration, configuration file management, circuit management (customizable via templates) and storing of hardware information (customizable via templates).”

Lots of screenshots:

http://iptrack.sourceforge.net/doku.php?id=screenshots

Netdisco:

- Project launched 2003. Version 1.0 released October 2009.
- Some popular uses of Netdisco:
  - **Locate** a machine on the network by MAC or IP and show the switch port it lives at.
  - **Turn Off** a switch port while leaving an audit trail. Admins log why a port was shut down.
  - **Inventory** your network hardware by model, vendor, switch-card, firmware and operating system.
  - **Report** on IP address and switch port usage: historical and current.
  - **Pretty pictures** of your network.

{net.} NETwork DOcumentation Tool

Netdot:

Includes functionality of IPplan and Netdisco and more. Core functionality includes:

- Device discovery via SNMP
- Layer2 topology discovery and graphs, using:
  - CDP/LLDP
  - Spanning Tree Protocol
  - Switch forwarding tables
  - Router point-to-point subnets
- IPv4 and IPv6 address space management (IPAM)
  - Address space visualization
  - DNS/DHCP config management
  - IP and MAC address tracking

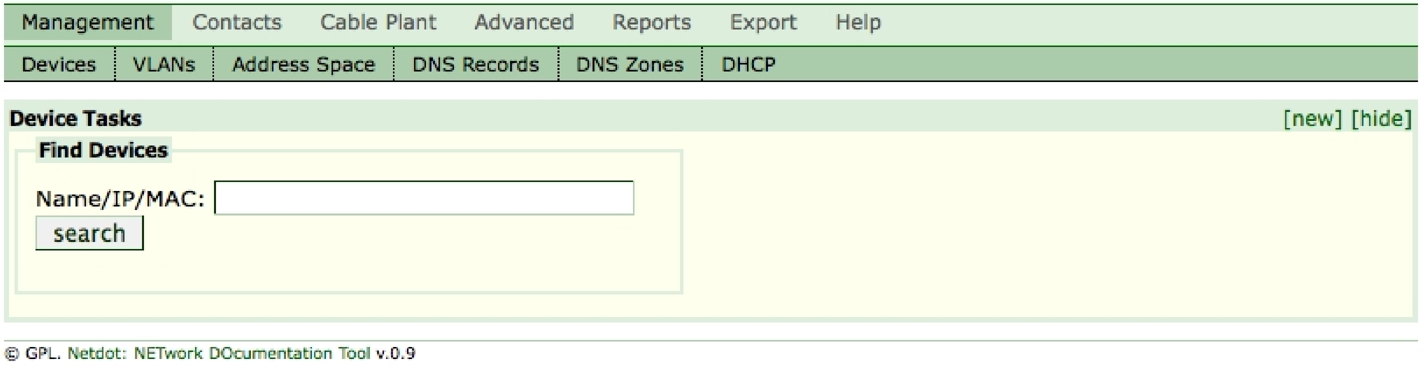
Continued ➔

{net.} NETwork DOcumentation Tool

Netdot:

Functionality continued:

- Cable plant (sites, fiber, copper, closets, circuits...)
- Contacts (departments, providers, vendors, etc.)
- Export scripts for various tools (Nagios, Sysmon, RANCID, Cacti, etc)
  - I.E., how we could automate node creation in Cacti!
- Multi-level user access: Admin, Operator, User
- It draws pretty pictures of your network



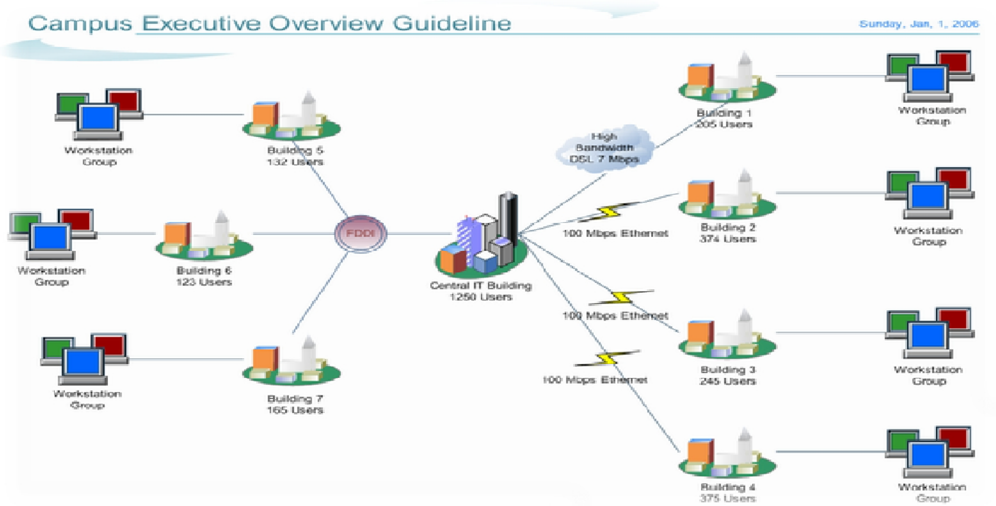
Device Tasks

Find Devices

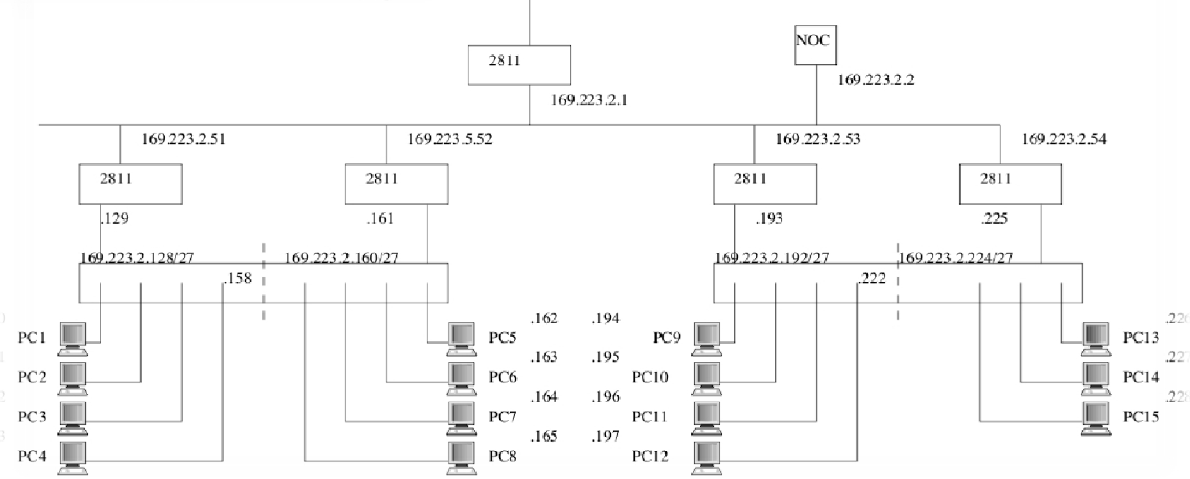
Name/IP/MAC:

© GPL. Netdot: NETwork DOcumentation Tool v.0.9

Documentation: Diagrams



Classroom layout at APRICOT 2008



Diagramming Software

Windows Diagramming Software

- Visio:

  http://office.microsoft.com/en-us/visio/FX100487861033.aspx

- Ezdraw:

  http://www.edrawsoft.com/

Open Source Diagramming Software

- Dia:

  http://live.gnome.org/Dia

- Cisco reference icons:

  http://www.cisco.com/web/about/ac50/ac47/2.html

- Nagios Exchange:

  http://www.nagiosexchange.org/

Network monitoring systems & tools

Three kinds of tools

1. **Diagnostic tools** – used to test connectivity, ascertain that a location is reachable, or a device is up – usually active tools

2. **Monitoring tools** – tools running in the background (”daemons” or services), which collect events, but can also initiate their own probes (using diagnostic tools), and recording the output, in a scheduled fashion.

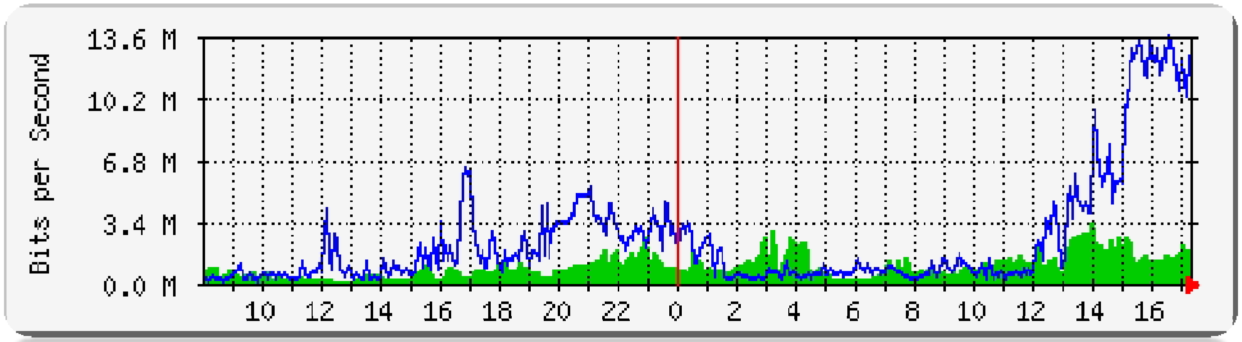
Network monitoring systems & tools

3. Performance Tools

Key is to look at each router interface (probably don't need to look at switch ports).

Two common tools:

- Netflow/NfSen: http://nfsen.sourceforge.net/
- MRTG: http://oss.oetiker.ch/mrtg/



MRTG = "Multi Router Traffic Grapher"

Network monitoring systems & tools

Active tools

- Ping – test connectivity to a host
- Traceroute – show path to a host
- MTR – combination of ping + traceroute
- SNMP collectors (polling)

Passive tools

- log monitoring, SNMP trap receivers, NetFlow

Automated tools

- SmokePing – record and graph latency to a set of hosts, using ICMP (Ping) or other protocols
- MRTG/RRD – record and graph bandwidth usage on a switch port or network link, at regular intervals