Network Monitoring and Management

Network Documentation & Netdot

Attribution

Based on materials from several presentations authored by:

- Carlos Vicente
  University of Oregon Network Services
  Principal author of Netdot
- Hervey Allen
  Network Startup Resource Center
- Dale Smith
  University of Oregon Network Services

Documentation

Have you ever 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!

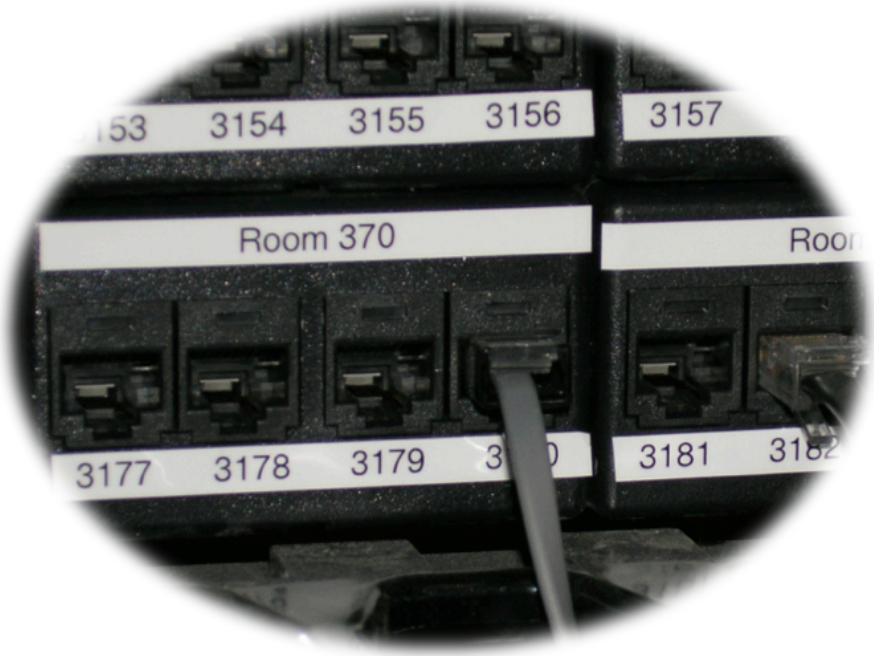
Documentation

Maybe this process should be automatic. Tools to help automate network documentation are something to consider.

- You can write local scripts (programs) to do this.
- Consider among several automated documenation systems for networks.
- You'll probably end up using and doing both.

Documentation: Labeling

Nice…



Problems with documentation

In most cases:

- Lack of clear procedures and methods
- Dispersion
- Lack of structure
- Lack of correlation
- Lack of tools… or, too many tools
- Lack of time and human resources

Requirements for a tool

- Open standards based
- Generic and flexible
- That uses a relational database
- Automates tasks
- Exports configurations
- Web and command-line interfaces (CLI)
- Authentication and authorization
- Reports
- Open source code
- Application programming interface (API)

Netdot: {net.} NETwork DOcumentation Tool

- Started in 2002. Required by the University of Oregon Network Services and NERO (http://www.nero.net)
- Nothing equivalent available as Open Source
- Started as something much simpler
- Quickly it became apparent that centralizing and correlating information was critical:
  - Topology
  - Cable plant
  - IP and Mac addresses
  - DNS, DHCP, etc.

Netdot: Design goals

- Reutilize components (don't reinvent the wheel)
  - There are Open Source packages that help to resolve many Network Management problems.
- Independent of the RDBMS using abstraction (http://www.masonhq.com)
  - MySQL, Postgres, etc.
- Use of Object Relations Mapper tools (ORM)
- Minimize the number of programming languages.
  - Perl and Javascript
- Low impact graphical interface.

{net.} NETwork DOcumentation Tool

Include functionality of other network documenation tools such as IPplan and Netdisco.

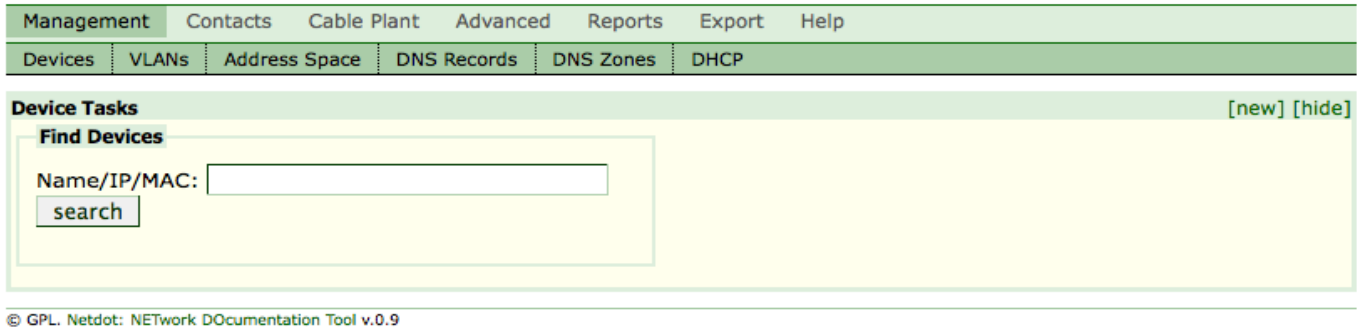
Core functionality includes:

- Discovery of network interfaces via SNMP
- Layer 2 topology discovery and graphics using:
  - CDP/LLDP
  - Spanning Tree protocol
  - Switches forwarding tables
  - Router point-to-point subnets
- IPv4 and IPv6 address management (IPAM)
  - Address space visualization
  - DNS and DHCP configuration managment
  - IP and Mac address correlation

{net.} NETwork DOcumentation Tool

Functionality cont.

- Cable plants (sites, fibre, copper, closes, circuits)
- Contacts (departments, providers, vendors, etc.)
- Export of data for various tools (Nagios, Sysmon, RANCID, Cacti, etc.)
  - For example, automate Cacti configuration
  - I.E., how to automate node creation in Cacti
- User access-level: admin, operator, user
- Ability to draw pretty pictures of your network.



Netdot components

SNMP::Info

http://snmp-info.sourceforge.net/

HTML::Mason

http://www.masonhq.com/

Class::DBI

http://search.cpan.org/~tmtm/Class-DBI/lib/Class/DBI.pm

Apache2::SiteControl

http://search.cpan.org/~awkay/Apache2-SiteControl-1.03/lib/Apache2/SiteControl.pm

NetAddr::IP

http://search.cpan.org/dist/NetAddr-IP/IP.pm

DBI

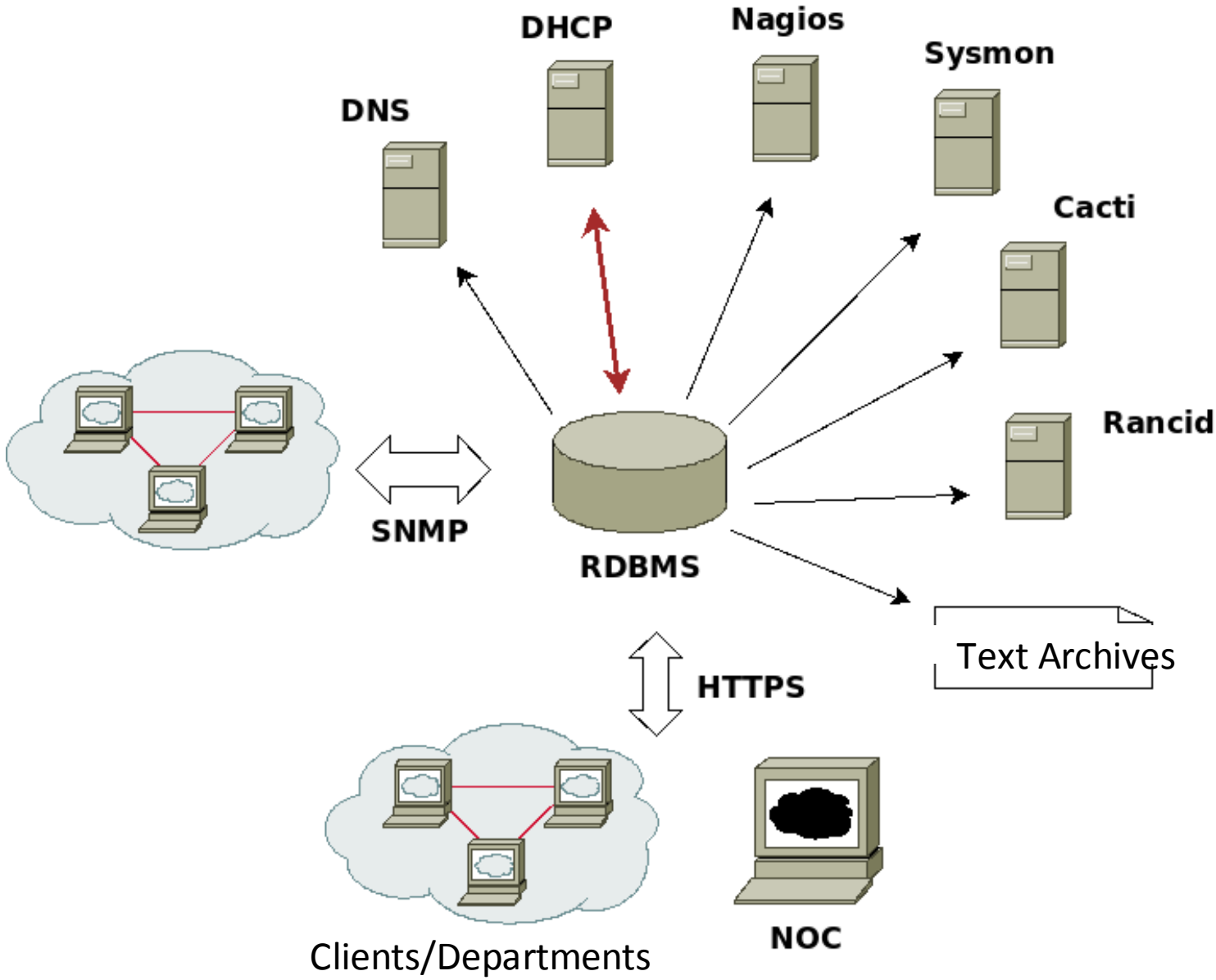
http://dbi.perl.org/

http://search.cpan.org/~timb/DBI/DBI.pm

MySQL

http://dev.mysql.com/doc/refman/5.1/en/

Netdot: NETwork DOcumentation Tool



Network devices

- Can be added via SNMP (preferred) or manually
- Automatic updates via SNMP
- Manufacturer, model, software version, name and domain, dates
- Maintenance contracts, out of band access, SNMP version and community
- Interfaces, VLANs, IP addresses, BGP peers
  - ARP tables (routers), redirection tables (switches)
- Topology
- Images, comments, change history

Topology

Netdot uses all possible sources of topological information:

- CDP and LLDP protocols
- Analyze redirection tables
- Spanning Tree protocol
- Point-to-point networks

Topology example

Netdot can draw the topology of a network or a segment of a network dynamically.

IP Space: Addresses and Blocks

- Hierarchical (*drill-down)* and graphical representation
- Support for IPv4 and IPv6
- Classification in:
  - Block
    - Container
    - Subnet
    - Reserved
  - Address
    - Static
    - Dynamic
    - Reserved

Visualization of IP space

IP Space: Blocks and Addresses

- Subnets are discovered from router interfaces
- From ARP tables we can know:
  - Addresses in use in each subnet
  - Mapping of IP to MAC
- Information added for blocks (or subnets)
  - Group that uses the block
  - Group that administers the block
  - Percent utilization of addresses (subnet)
  - Percent utilization of sub-divisions (containers)
- Information added for addresses
  - First and and last time seen
  - interface and device
  - Services to monitor with Nagios (HTTP, DNS, SSH, DHCP, Radius, LDAP, etc.)

Cabling

- Inter-building cabling (backbone)
  - Buildings and closets where cabling starts and stops.
  - Type of fiber, length, quantity of fibers
- Fibers
  - Interconnections (splicing) and sequences
  - Measurements, tests, interfaces, circuits
  - Status

Cabling

- Intra-building cabling (interior cabling)
  - Closet where it begins
    - Level
      - Building
  - Interface (port) where it is connected
  - Outlet where it terminates (id)
    - Office number or room
      - Level
        - » Building

Cabling: Closets

- Physical data
  - Dimensions, number and types of panels, type of ventilation, number of copper pairs, number of racks, etc.
- Cabling that terminates in the closet
  - Fiber and twisted pair
- Photos

Closet photos

Entities

- Branch
- Customer
- Department
- Manufacturer
- Peer (BGP)
- Provider
- Vendor

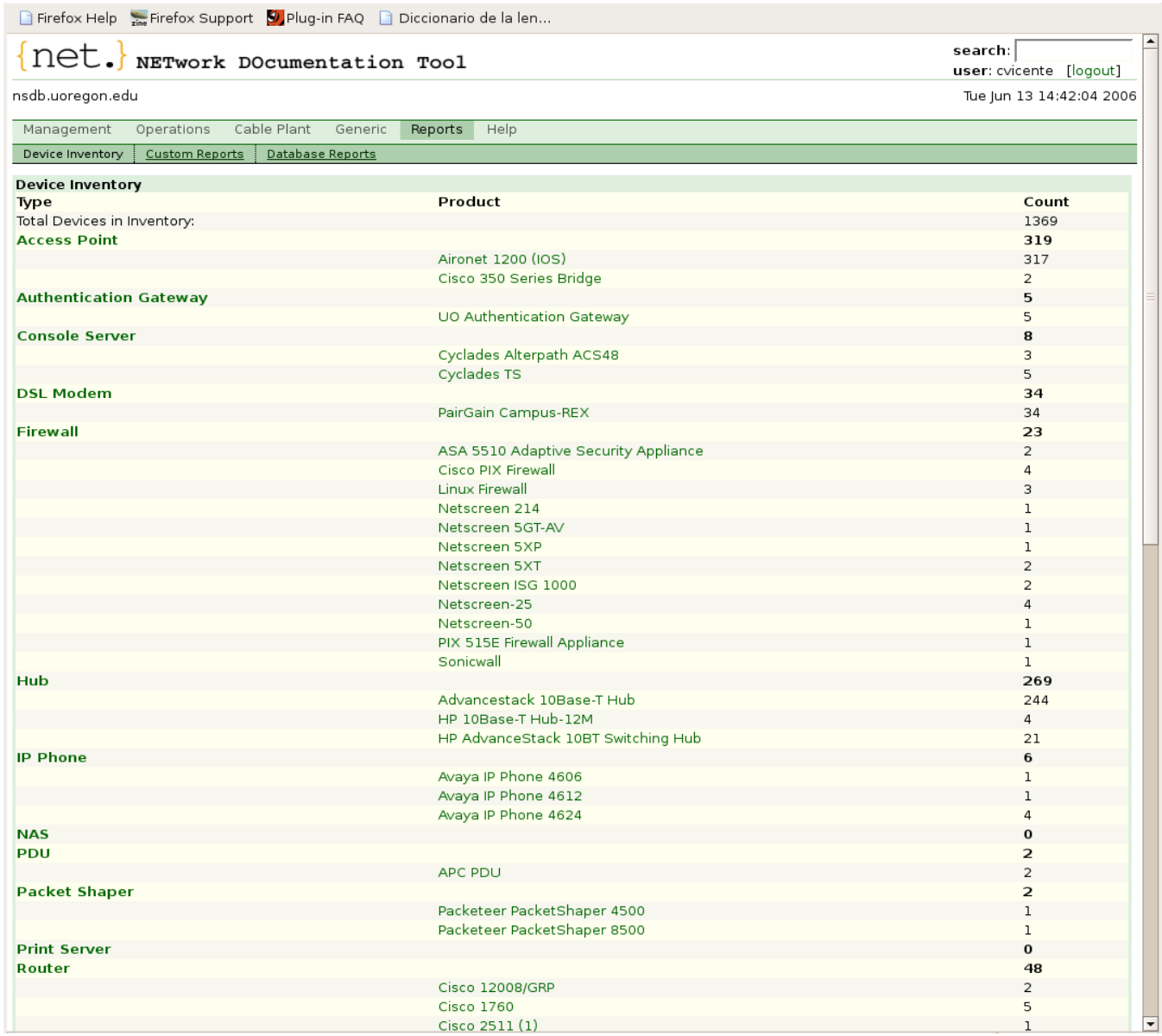
Contacts

- Based in individuals and roles (Person & Contact)
  - Information by individual
    - Contact data
      - Locations, position, telephone, e-mail, beeper
    - Roles
      - Administrative contact, technical, etc.
      - Notification schedule and levels
    - Contact lists
      - Assigned to different resources
        - » Devices, subnets, cabling, etc.

Reports

- Devices
  - By category and by product
  - Out-of-date firmware
  - Duplex mismatches
- Most used MAC codes (Manufacturers)
- From the database
  - SQL table utilization reports

Inventory and Devices



Device Inventory

Type	Product	Count
Total Devices in Inventory:		1369
Access Point		**319**
	Aironet 1200 (IOS)	317
	Cisco 350 Series Bridge	2
Authentication Gateway		**5**
	UO Authentication Gateway	5
Console Server		**8**
	Cyclades Alterpath ACS48	3
	Cyclades TS	5
DSL Modem		**34**
	PairGain Campus-REX	34
Firewall		**23**
	ASA 5510 Adaptive Security Appliance	2
	Cisco PIX Firewall	4
	Linux Firewall	3
	Netscreen 214	1
	Netscreen 5GT-AV	1
	Netscreen 5XP	1
	Netscreen 5XT	2
	Netscreen ISG 1000	2
	Netscreen-25	4
	Netscreen-50	1
	PIX 515E Firewall Appliance	1
	Sonicwall	1
Hub		**269**
	Advancestack 10Base-T Hub	244
	HP 10Base-T Hub-12M	4
	HP AdvanceStack 10BT Switching Hub	21
IP Phone		**6**
	Avaya IP Phone 4606	1
	Avaya IP Phone 4612	1
	Avaya IP Phone 4624	4
NAS		**0**
PDU		**2**
	APC PDU	2
Packet Shaper		**2**
	Packeteer PacketShaper 4500	1
	Packeteer PacketShaper 8500	1
Print Server		**0**
Router		**48**
	Cisco 12008/GRP	2
	Cisco 1760	5
	Cisco 2511 (1)	1

Configuration exports

The information contained within Netdot enables the automatic generation of configurations for software packages.

- Monitoring devices and servces
  - Nagios, Sysmon
- Monitoring configurations
  - RANCID
- Traffic analysis
  - Cacti
- Services
  - DNS (Bind)
  - DHCP

Exporting configurations

Recommendation:

- Netdot updates Subversion or CVS
- Puppet (replaces Cfengine) distributes configurations, restarts services, etc.

Other automated systems

There are several. Each one does something different:

Open Source

- IPplan:
  http://iptrack.sourceforge.net/
- Netdisco
  http://netdisco.org/
- RackTables
  http://racktables.org/

Commercial

- HP OpenView
- IBM Tivoli and Netcool
- SolarWindows

[[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.

RackTables

Web site:

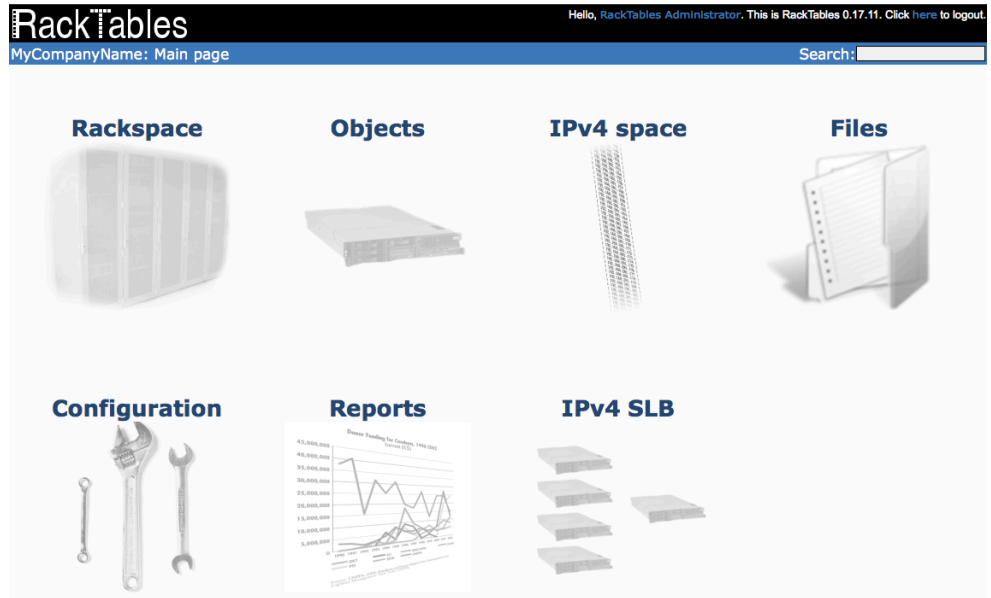
http://racktables.org/

From the RackTables web site

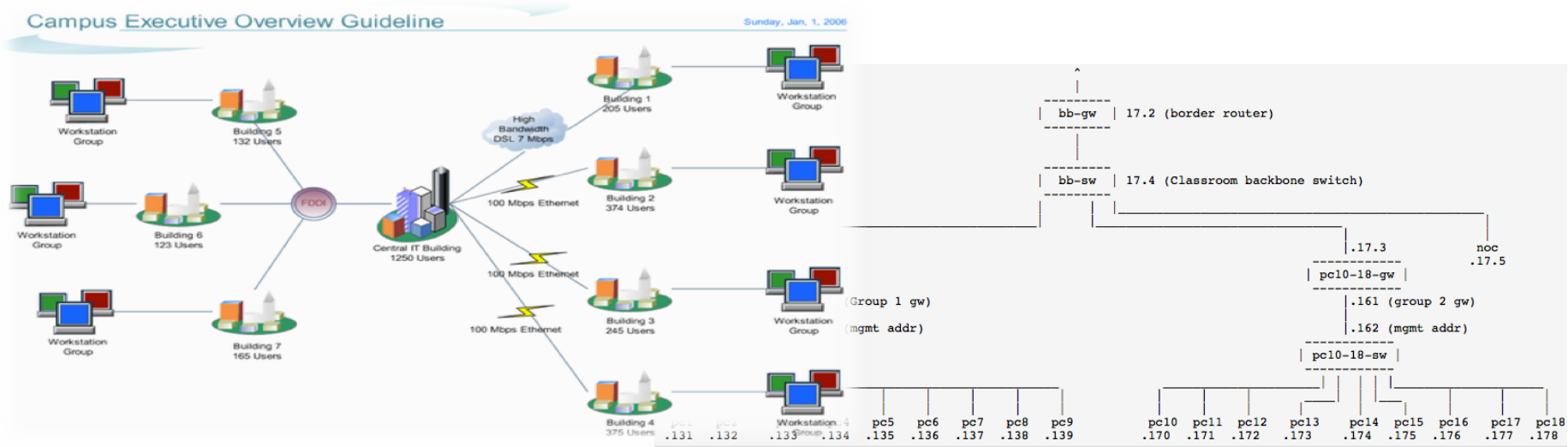
"Racktables is a nifty and robust solution for datacenter and server room asset management. It helps document hardware assets, network addresses, space in racks, networks configuration and much much more!"

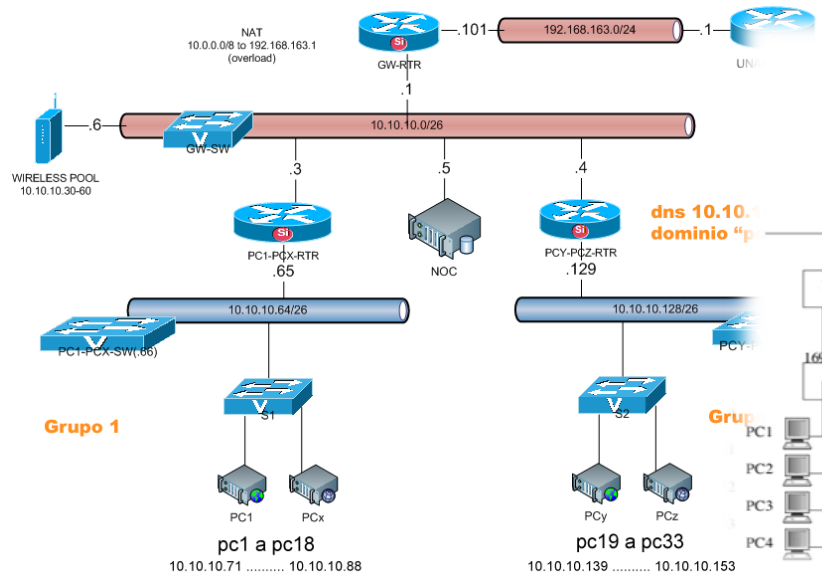
There is a demo system:

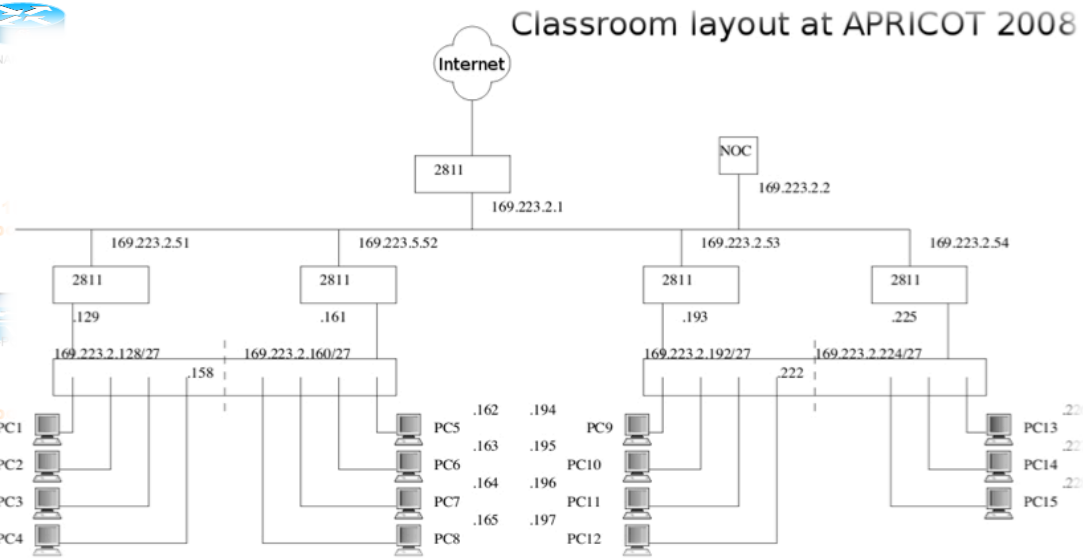
http://racktables.org/demo.php



Documentation: Diagrams







Diagramming Software

Windows

- Visio:
  http://office.microsoft.com/en-us/visio/FX100487861033.aspx
- Ezdraw:
  http://www.edrawsoft.com/

Open Source

- ASCII:
  http://www.ascii-art.org/
- 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/

Netdot demo

Assuming there is time we will now give a short demonstration of a running copy of Netdot

Netdot can be found at:

http://netdot.uoregon.edu/