Campus Network
Best Practices:
Core and Edge Networks

Dale Smith
Network Startup Resource Center
dsmith@nsrc.org

This document is a result of work by the Network Startup Resource Center (NSRC at http://www.nsrc.org). This document may be freely copied, modified, and otherwise re-used on the condition that any re-use acknowledge the NSRC as the original source.
Campus Network Challenges

- Many are not structured properly and can’t effectively utilize high bandwidth connections
- Many make heavy use of NAT and firewalls that limit performance
- Many are built with unmanaged network equipment that provide no ability for monitoring or tuning the network
How to Best Support R & E

• Research and Education needs flexible and open networks

• Things to consider
  – NAT makes some things hard (H.323 video conferencing)
  – Filtering makes it hard for researchers, teachers, and students to do interesting things
  – Your campus network must not be the bottleneck

• Make a plan for improvement – without a plan, how will you get there.
Campus Network Rules

- Minimize number of network devices in any path
- Use standard solutions for common situations
- Build Separate Core and Edge Networks
- Provide services near the core
- Separate border routers from core
- Provide opportunities to firewall and shape network traffic
Core versus Edge

• Core network is the “core” of your network
  – Needs to have reliable power and air conditioning
  – May have multiple cores
  – Always route in the core

• Edge is toward the edges of your network
  – Provide service inside of individual buildings to individual computers
  – Always switch at the edge
Minimize Number of Network Devices in the Path

- Build star networks

- Not daisy chained networks
Edge Networks (Layer 2 LANs)

- Provides Service to end users
- Each of these networks will be an IP subnet
- Plan for no more than 250 Computers at maximum
- Should be one of these for every reasonable sized building
- This network should only be switched
- Always buy switches that are managed – no unmanaged switches!
Edge Networks

- Make every network look like this:

Fiber link to core router
Edge Networks Continued

• Build Edge network incrementally as you have demand and money
• Start Small:

Fiber link to core router
Edge Networks Continued

• Then as you need to add machines to the network, add a switch to get this:
Edge Networks Continued

• And keep adding switches to get to the final configuration
Edge Networks Continued

- And keep adding switches to get to the final configuration
Edge Networks Continued

• Resist the urge to save money by breaking this model and daisy chaining networks or buildings together

• Try hard not to do this:
Edge Networks Continued

- There are cases where you can serve multiple small buildings with one subnet.
- Do it carefully.
Core Network
Routing versus Switching
Layer 2 versus Layer 3

- Routers provide more isolation between devices (they stop broadcasts)
- Routing is more complicated, but also more sophisticated and can make more efficient use of the network, particularly if there are redundancy elements such as loops
Layer 3 Switches

• Many vendors use the term “Layer 3 Switch”.

• These are contradictory terms
  – Layer 3 = Routing
  – Switch = Layer 2

• What vendors mean is that it is a device that can be configured as a router or a switch or possibly both at the same time.
Switching versus Routing

These links must be routed, not switched
Core Network

• Reliability is the key
  – remember many users and possibly your whole network relies on the core
• May have one or more network core locations
• Core location must have reliable power
  – UPS battery backup (redundant UPS as your network evolves)
  – Generator
  – Grounding and bonding
• Core location must have reliable air conditioning
Core Network

- At the core of your network should be routers – you must route, not switch.
- Routers give isolation between subnets
- A simple core:
Where to put Firewalls

- Security devices must be placed “in line”
- This means that the speed of the firewall affects access to the outside world
- This is a typical design:

```
ISP
```

- Border Router
- Firewall/Traffic Shaper
- Core Router
- All router interfaces on a separate subnet
- Fiber optic links to remote buildings
- ISP

UNIVERSITY OF OREGON
Where to put Firewalls

- As Campus Networks have gotten better bandwidth, the firewall becomes a bottleneck.
- Can move part of your network from behind the firewall to allow full bandwidth, un-filtered access to the Internet.
- One configuration:
Where to put Servers?

- Servers should never be on the same subnet as users
- Should be on a separate subnet off of the core router
- Servers should be at your core location where there is good power and air conditioning
Where to put Servers?

- Sometimes you need servers that have public IP addresses.
- Can put directly off of a firewall with no NAT.
- Can have some servers with an interface on both the external network and an internal network.
Border Router

- Connects to outside world
- RENs and Peering are the reason you need them
- Must get Provider Independent IP address space to really make this work right
Putting it all Together
Alternative Core Designs

• Wireless Links versus Fiber
Layer 2 and 3 Summary

- Route in the core
- Switch at the edge
- Build star networks – don’t daisy chain
- Buy only managed switches – re-purpose your old unmanaged switches for labs
Questions?

This document is a result of work by the Network Startup Resource Center (NSRC at http://www.nsrc.org). This document may be freely copied, modified, and otherwise re-used on the condition that any re-use acknowledge the NSRC as the original source.
Symbols to use for diagrams