Campus Network Design Principles

Campus Network Design & Operations Workshop

These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license
(http://creativecommons.org/licenses/by-nc/4.0/)

UNIVERSITY OF OREGON

Last updated 30th September 2024

NSRC
Network Startup Resource Center

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
  - https://fasterdata.es.net/network-tuning/firewall-performance-issues

- Many are built with unmanaged network equipment that provide no ability for monitoring or tuning the network

How to Support R & E

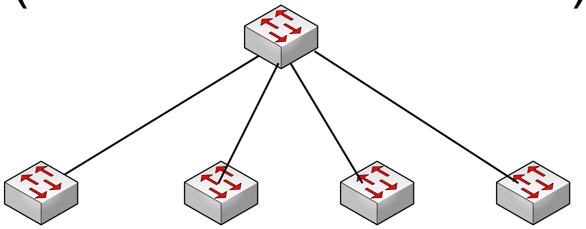
- Research and Education needs flexible and open networks
- Things to consider
  - NAT makes some things hard (H.323 video conferencing)
  - NAT requires state to be maintained (you may be using PAT)
  - NAT may require recalculation of checksums
  - Filtering makes it hard for researchers, teachers, and students to do interesting things
  - Your campus network must not be the bottleneck
- Make a plan for improvement – This lets you go step-by-step in a logical sequence to get where you want to be.

Campus Network Rules

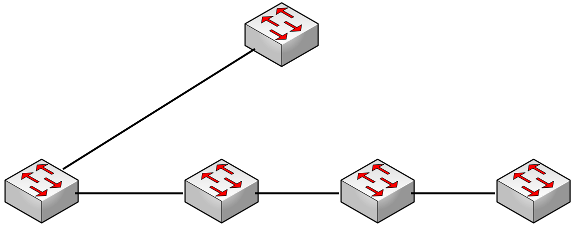
- Minimize number of network devices in any path
- Use the hub and spoke (star) configuration design pattern
- Segment your network with routers at the core/middle
- Provide services near the core
- Think carefully about where to firewall and where to NAT

Minimize Number of Network Devices in the Path

- Build hub and spoke (sometimes called star) networks



- Not daisy chained (sometimes called cascaded) networks



Hub and Spoke Design

- We will use this design pattern in two places in our network
  1. Between Buildings. We will run fiber optic cabling from a central location in a hub-and-spoke fashion to each remote building
  2. Inside of each building. We will run unshielded twisted pair (and possibly fiber) from the main rack in each building to all other racks.

Hub and Spoke at Campus Level

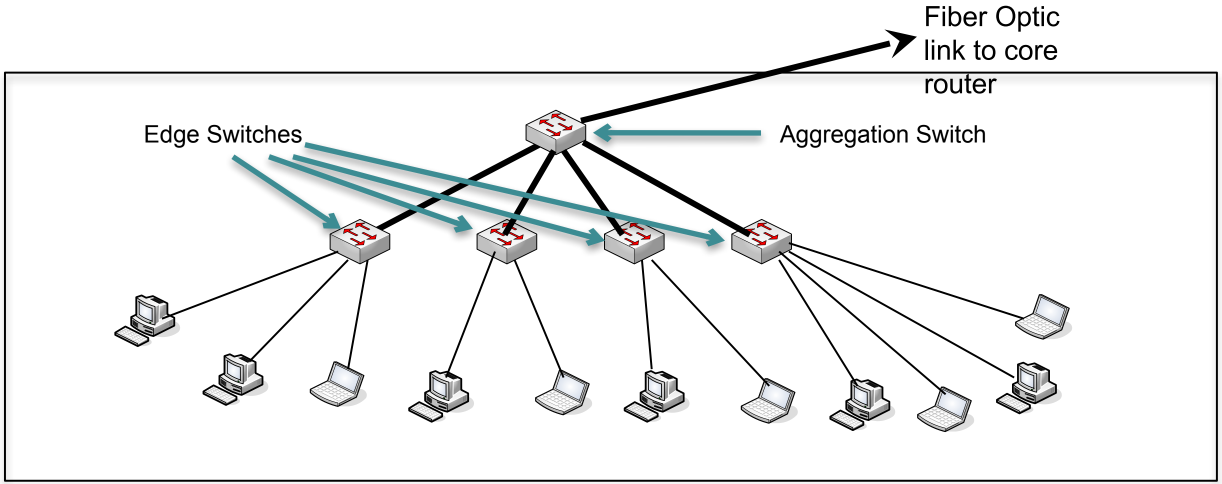
- At the campus level, best practices are to build hub and spoke networks
- The hub at the campus level is often called the core
- Best practices are to route at the core
  - This segments the network into independent subnets
  - Limits broadcasts

Hub and Spoke Networks Inside Buildings

- Inside of each building, we will also build a hub and spoke network.
- This hub and spoke network is what 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
- Often, the in-building portion is called the Edge of your network
- Always buy switches that are managed
  - no unmanaged switches!

In-Building Edge Networks

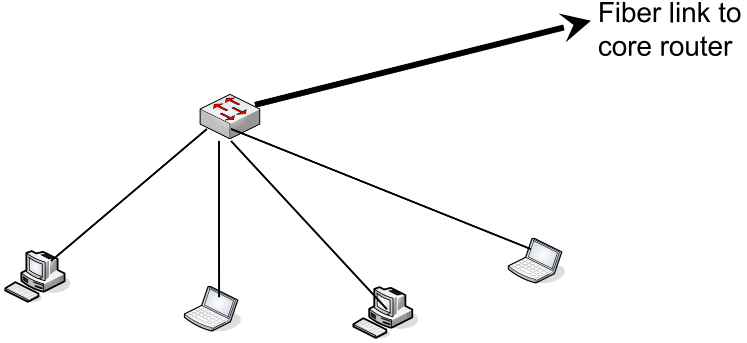
- Make every network in every building look like this:



One Building

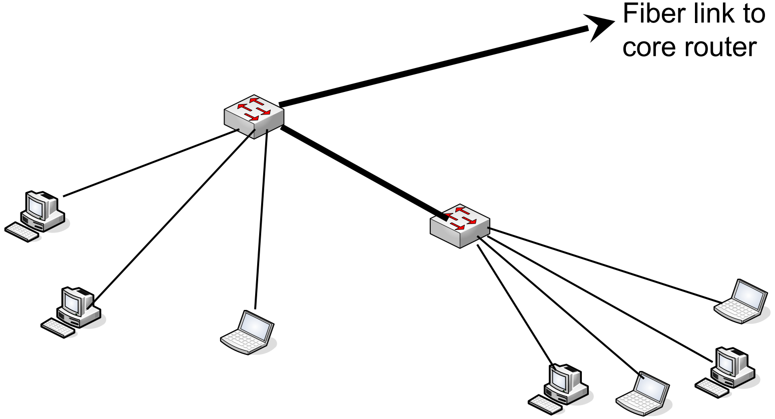
Edge Networks Continued

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



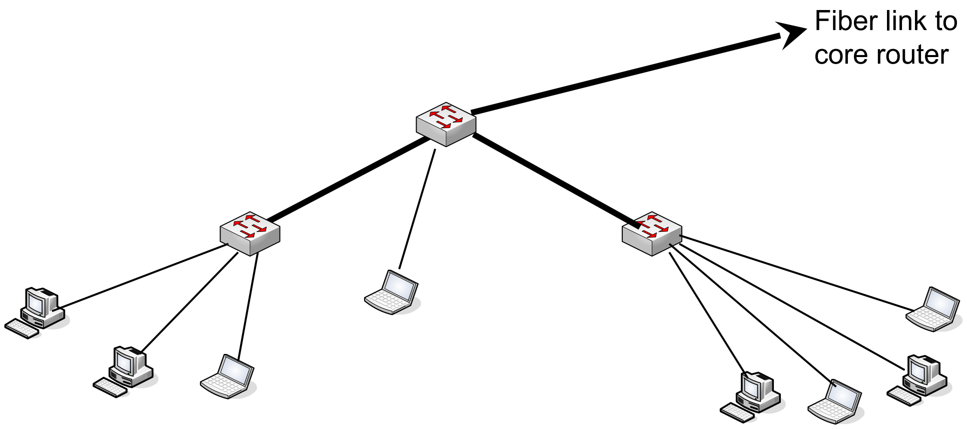
Edge Networks Continued

- Then as you need to add machines to the network, add a network rack and a switch to get this:



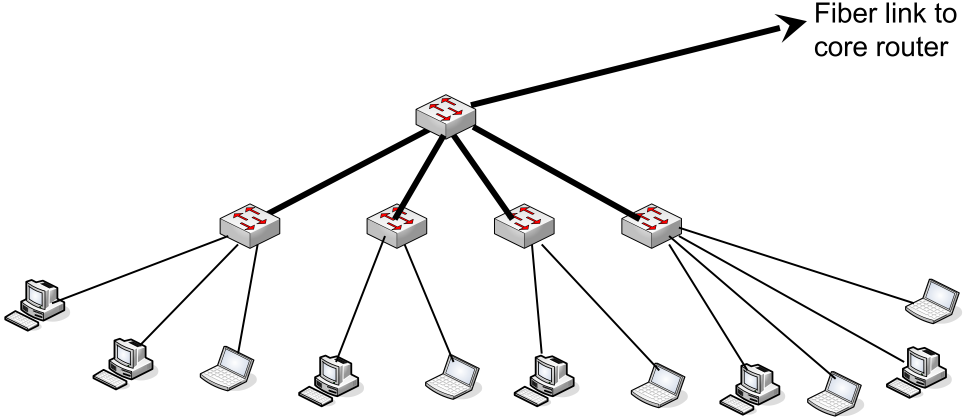
Edge Networks Continued

- And keep adding network racks and switches



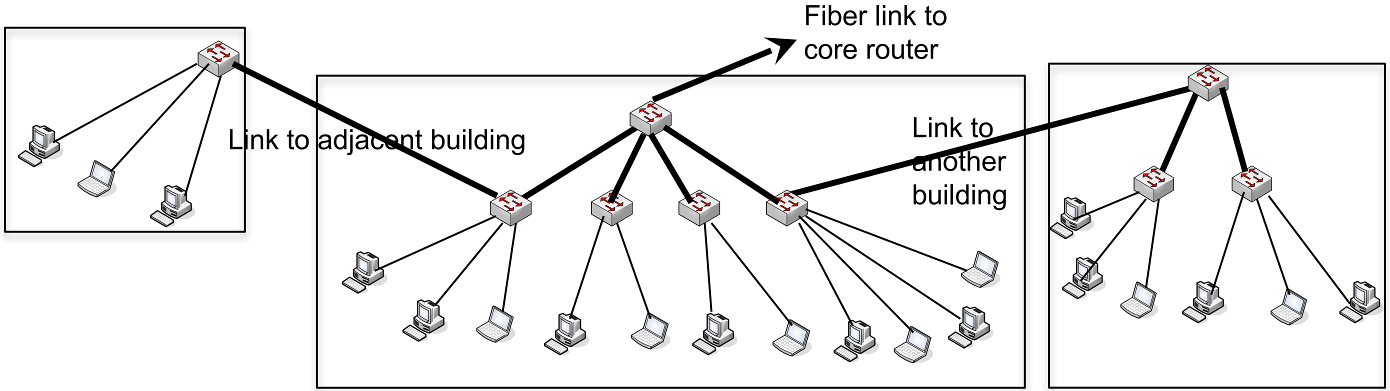
Edge Networks Continued

- Until you get to the final configuration



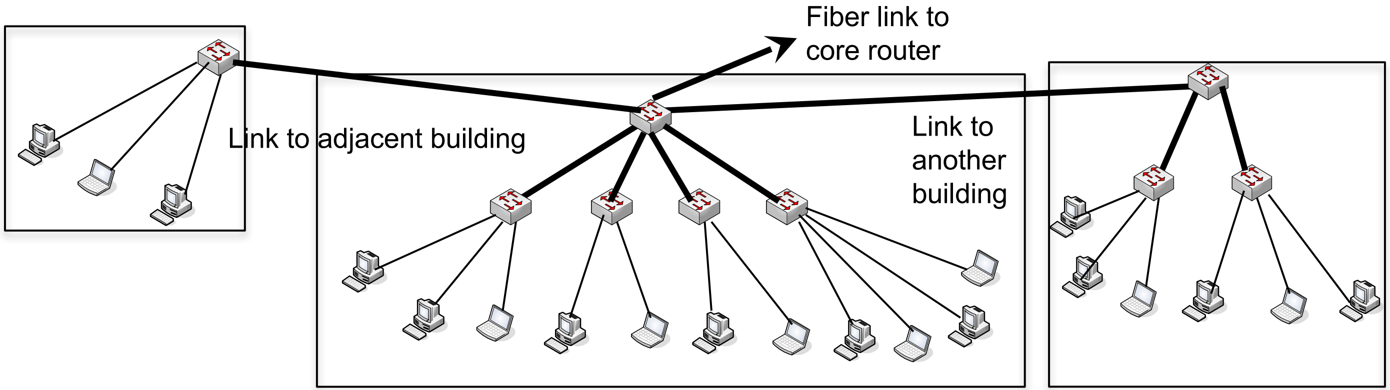
Edge Networks Continued

- 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. Keep the network diameter as small as possible and do as little daisy chaining as possible



Core Network
or
The Center of the Campus Level Hub and Spoke

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

Segmenting Your Network

- A single IP subnet that serves your entire campus puts your network at risk.
  - You cannot properly secure your hosts and protect them from a variety of attacks. How do you firewall your servers from students if they are on the same subnet?
  - Broadcasts on your network become a problem, including loops in the network that can stop the entire campus

Layer 3 Switches

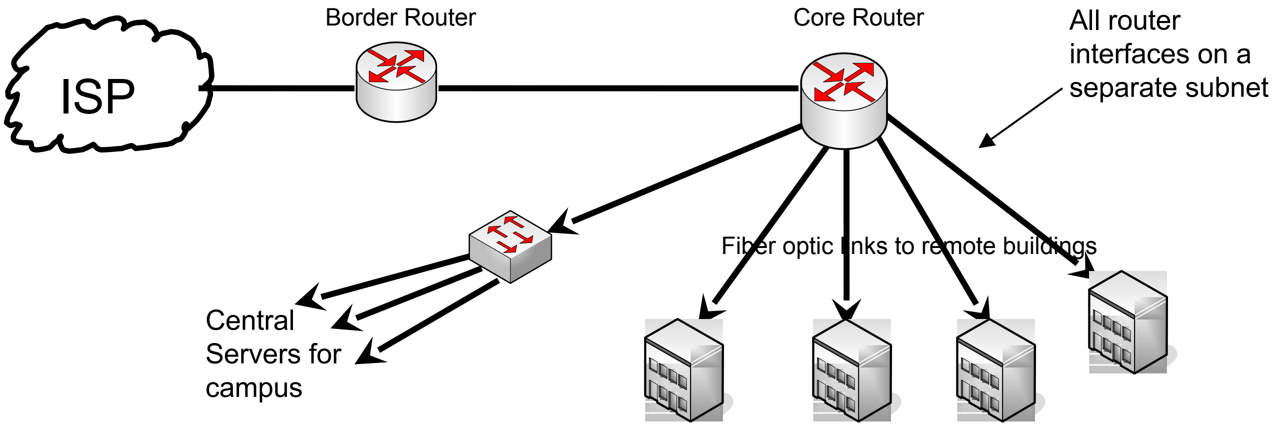
- Many vendors use the term “Layer 3 Switch”.
- These are contradictory terms
  - Layer 3 = Routing
  - Switch = Layer 2
- What vendors mean is that it is a device that can be configured as a router or a switch or possibly both at the same time.

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

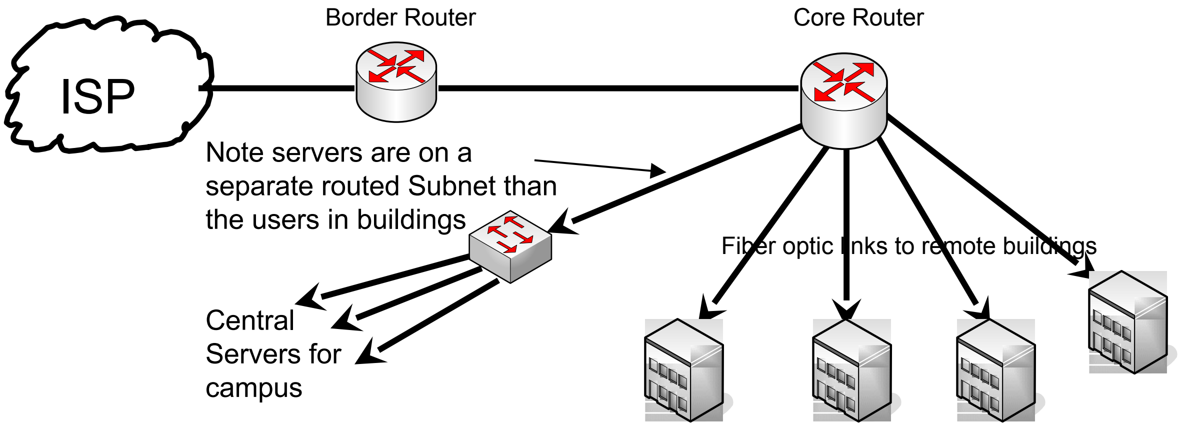
Core Network

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


Border Router
Core Router
ISP
All router interfaces on a separate subnet
Fiber optic links to remote buildings
Central Servers for campus

Where to put Servers?

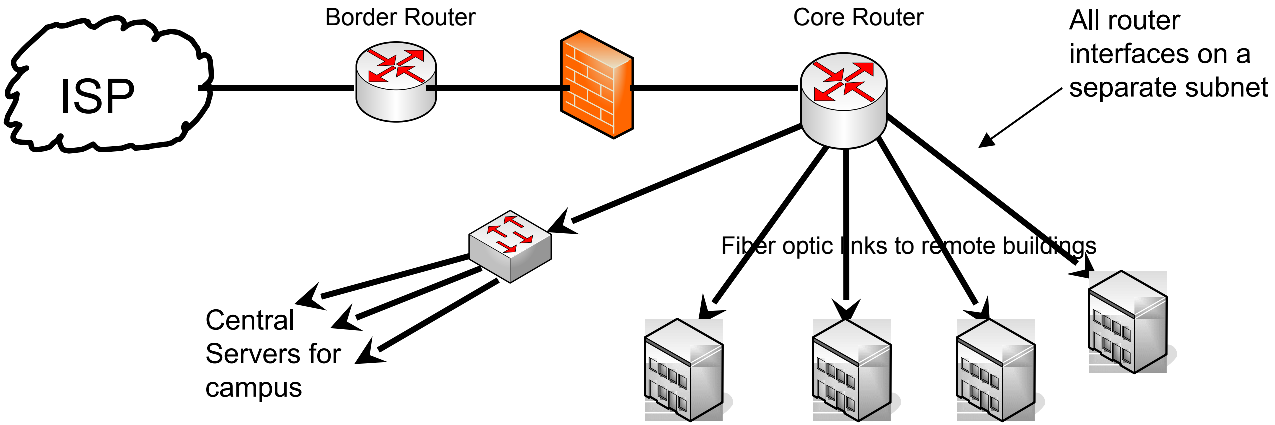
- Servers should never be on the same subnet as users
- Should be on a separate subnet off of the core router
- Servers should be at your core location where there is good power and air conditioning


Border Router
Core Router
ISP
Fiber optic links to remote buildings
Central Servers for campus

Note servers are on a separate routed Subnet than the users in buildings

Where to put Firewalls

- Security devices are often placed “in line”
- Campuses often take a corporate strategy to firewall all of their campus
- This is a typical design:

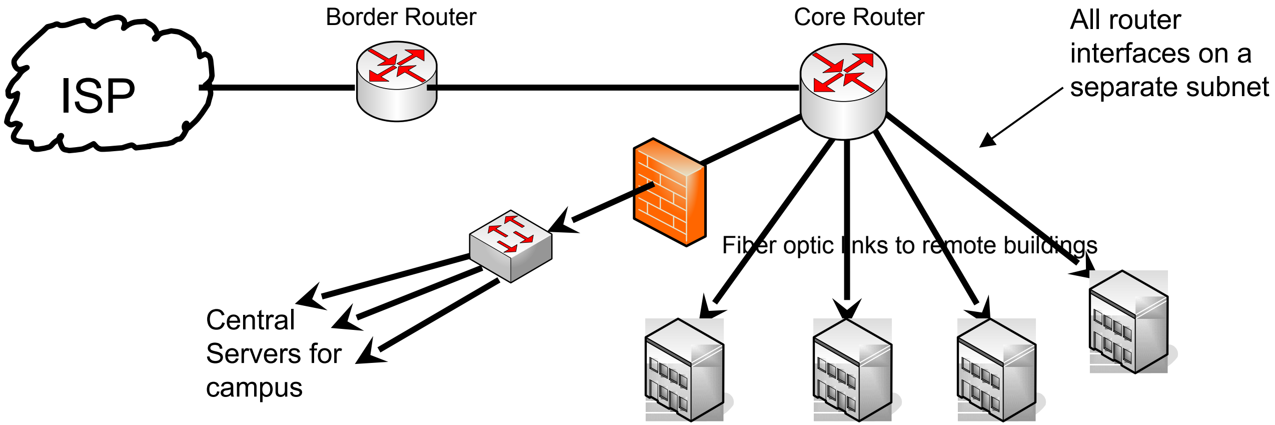

Border Router
Core Router
All router interfaces on a separate subnet
ISP
Fiber optic links to remote buildings
Central Servers for campus

Firewall Placement

- Campuses are not corporate environments
- Firewalls don’t protect users from getting viruses that come via two mechanisms
  - “clicked links” while web browsing
  - Email attachments
  - Both are encrypted and firewalls won’t help
- As bandwidth increases, in-line firewalls limit performance for all users. This gets to be a bigger problem at higher speeds.

Alternative Suggestion

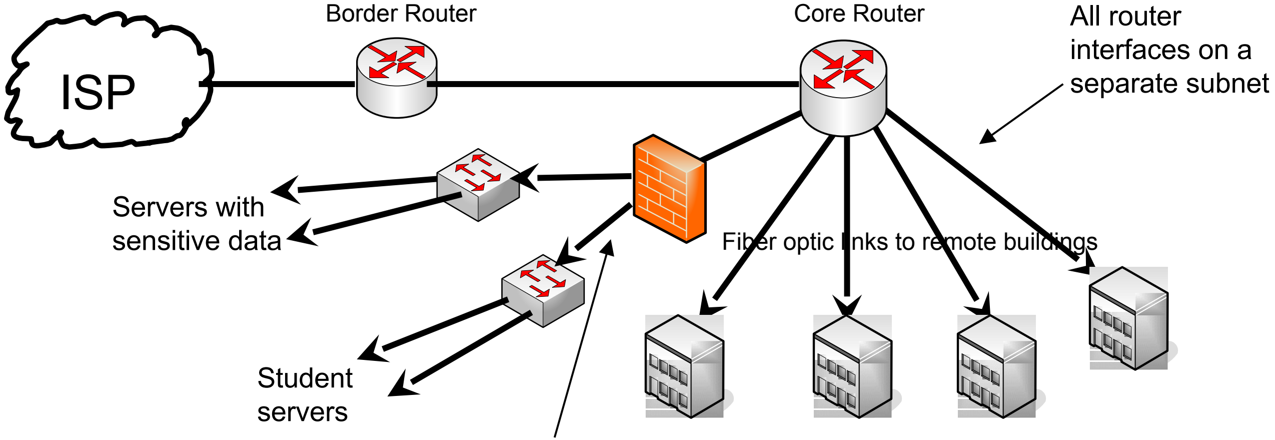
- Since Firewalls don’t really protect users from viruses, let’s focus on protecting critical server assets, even from campus users
- This is a typical design:



ISP
Border Router
Core Router
All router interfaces on a separate subnet
Fiber optic links to remote buildings
Central Servers for campus

Best Practices for Servers

- Not all servers are created equal. Some are accessed by students (Moodle, file & print, email).
- Others have sensitive data (payroll, financial systems, etc)
- Put different classes of servers on different subnets:

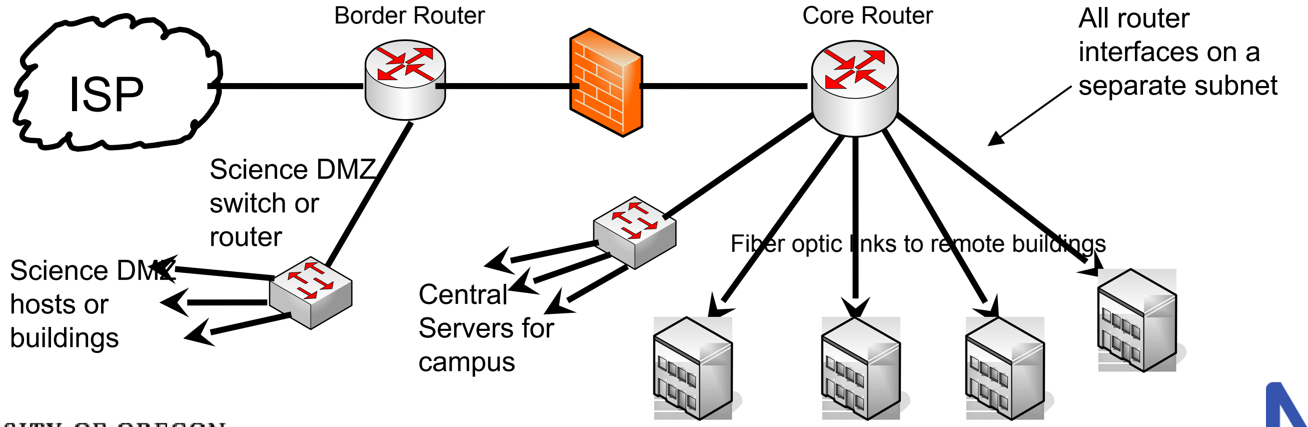

Border Router
Core Router
ISP
Servers with sensitive data
Student servers
Fiber optic links to remote buildings

All router interfaces on a separate subnet

Different subnets with different firewall rules – block students from accessing sensitive data

Science DMZ

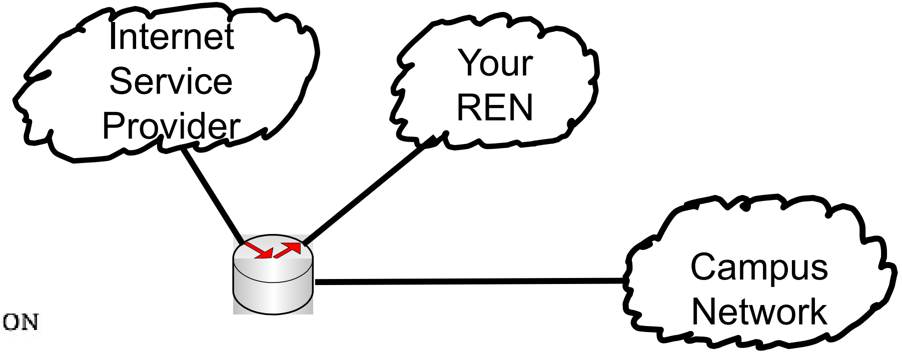
- Some campuses can't develop the political backing to remove firewalls for the majority of the campus
- Consider moving high bandwidth devices from behind firewall (this is sometimes called the Science DMZ)
- Recommended Configuration:



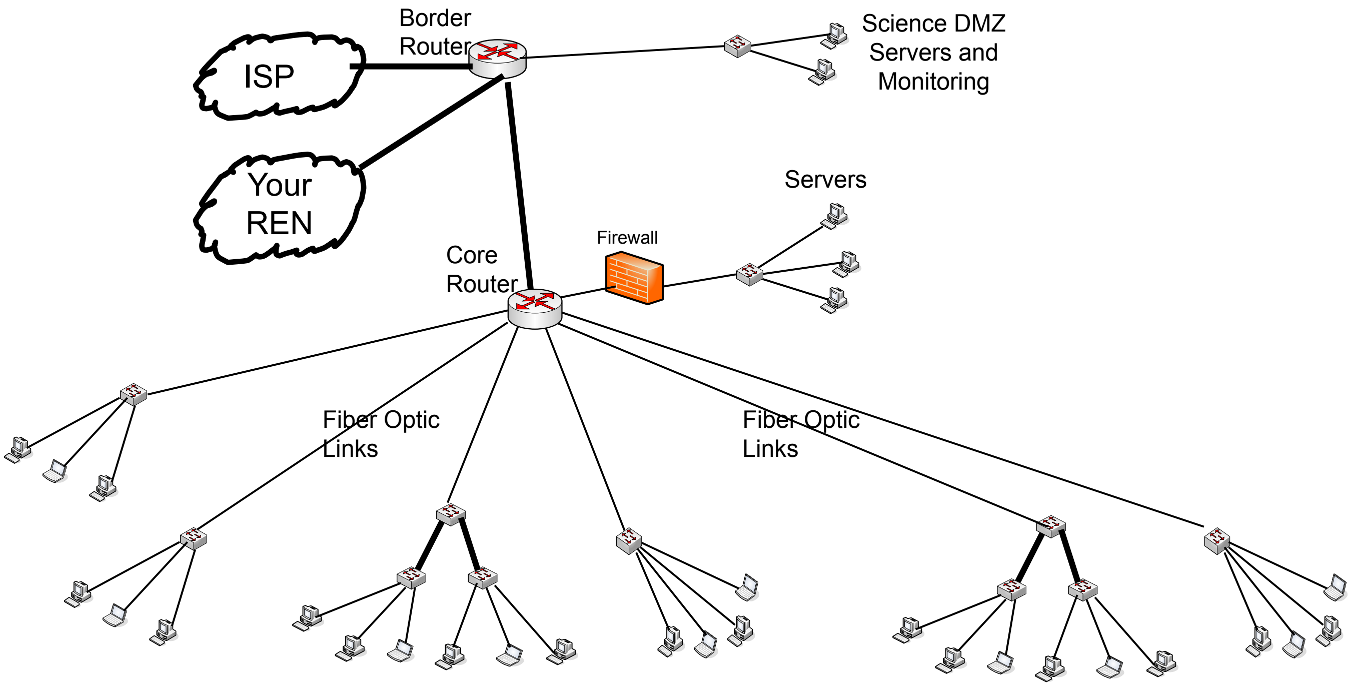
Border Router
Core Router
All router interfaces on a separate subnet
ISP
Science DMZ switch or router
Science DMZ hosts or buildings
Central Servers for campus
Fiber optic links to remote buildings

Border Router

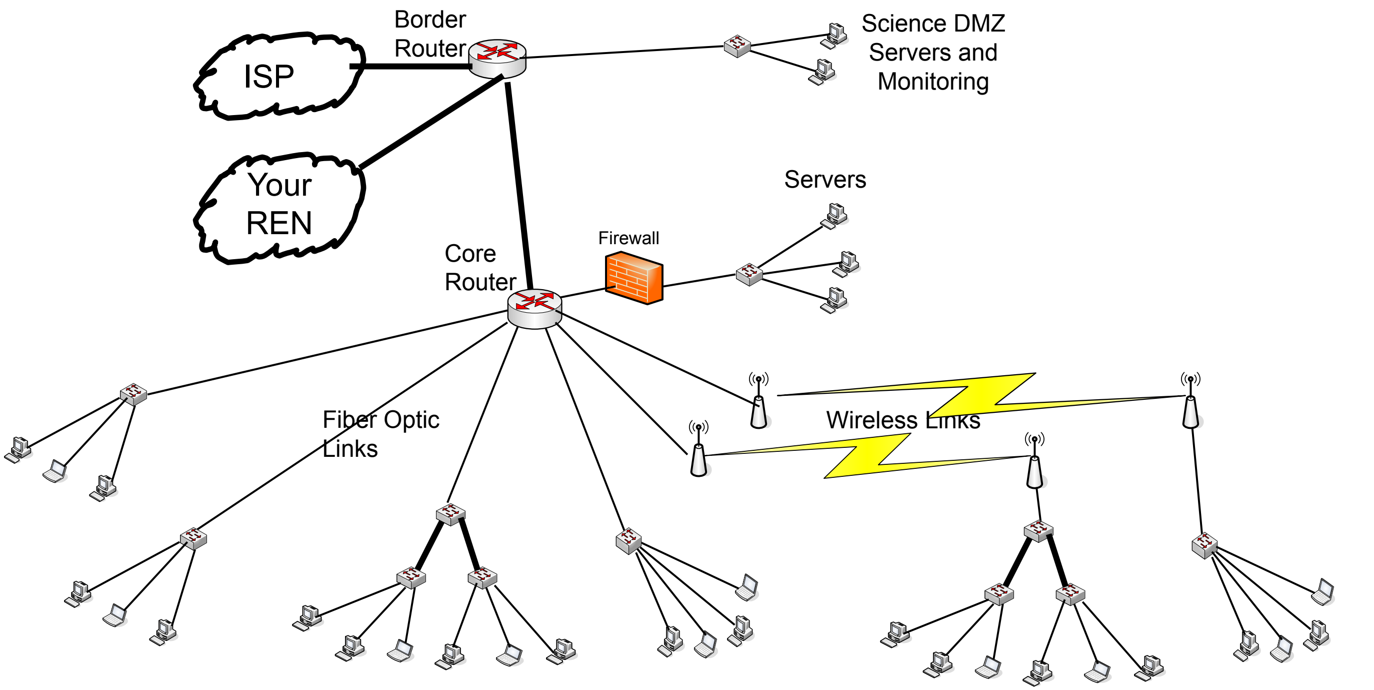
- Connects campus to outside world
- If you are dual homed, you must have a border router
  - Dual homing takes more effort to make work properly
- Many campuses in emerging regions will do NAT on this device that connects the campus to the outside world.
  - Most of them use a firewall for this function
  - Dual homing with a NAT firewall isn't really dual homing



Putting it all Together



Wireless Links Instead of Fiber



Layer 2 and 3 Summary

- Build Hub and Spoke Networks
  - Don’t daisy chain
- Route at the core of the campus network
- Switch at the edge of the campus network
- 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.

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center