Campus Network Design Workshop

Basic Campus Design Concepts

UNIVERSITY OF OREGON

Last updated 17th October 2016

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
- 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

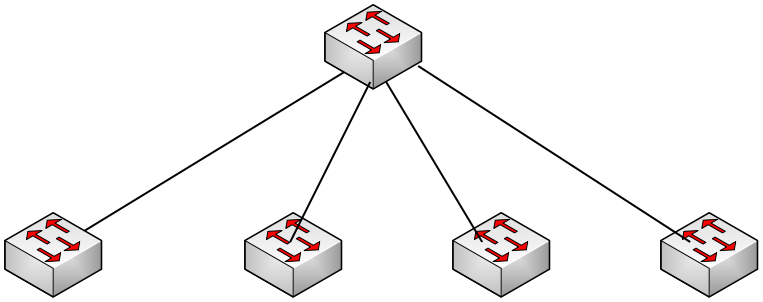
- Minimize number of network devices in any path
- Use standard solutions for common situations
- Build Separate Core and Edge Networks
- Provide services near the core
- Separate border routers from core
- Provide opportunities to firewall and shape network traffic

Core versus Edge

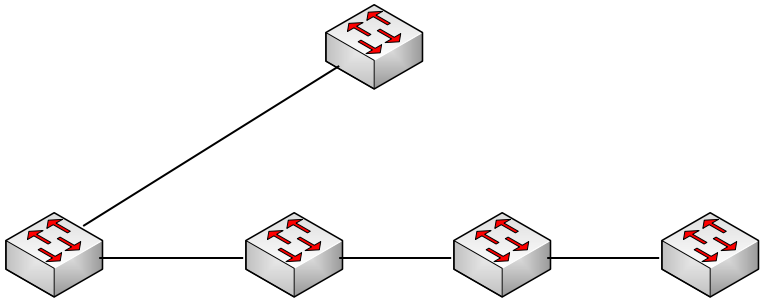
- Core network is the “core” of your network
  - Needs to have reliable power and air conditioning
  - May have multiple cores
  - Always route in the core
- Edge is toward the edges of your network
  - Provide service inside of individual buildings to individual computers
  - Always switch at the edge

Minimize Number of Network Devices in the Path

- Build star networks



- Not daisy chained networks

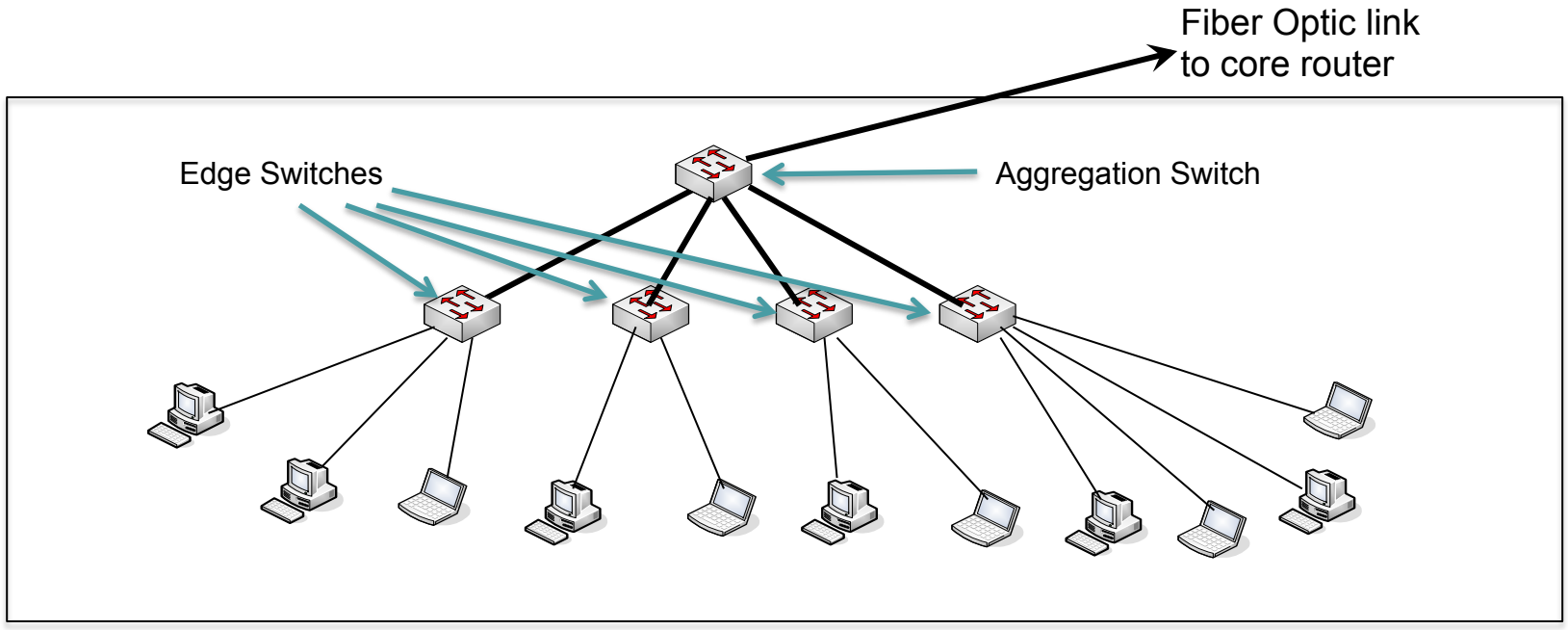


Edge Networks (Layer 2 LANs)

- 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

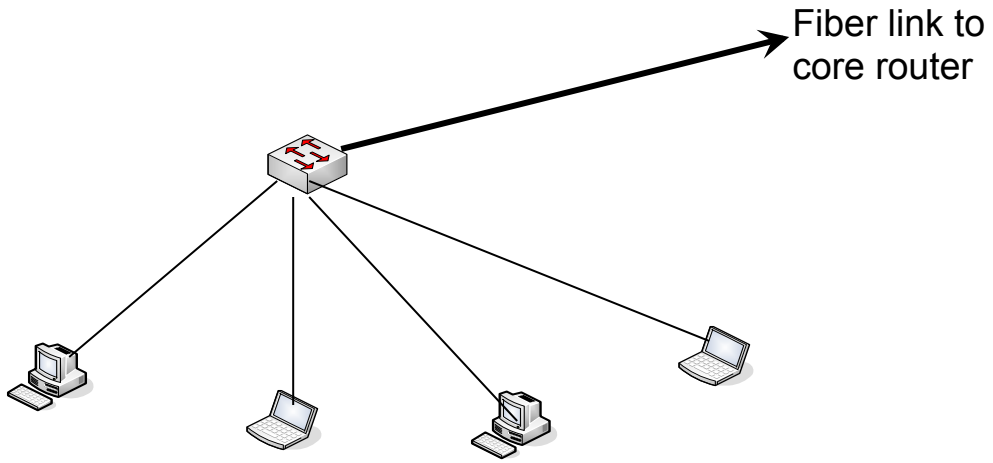
- Make every network in every building look like this:



One Building

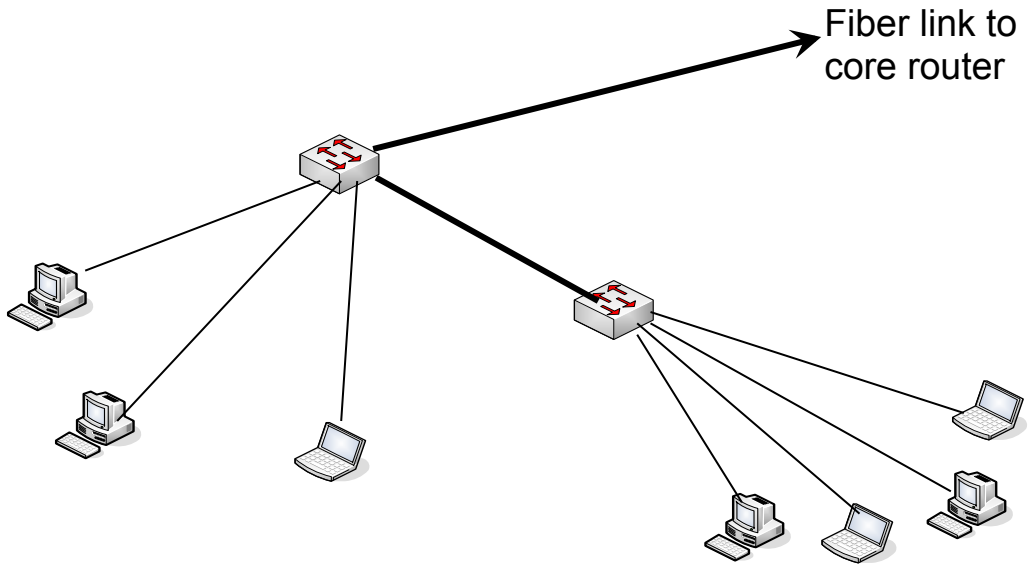
Edge Networks Continued

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



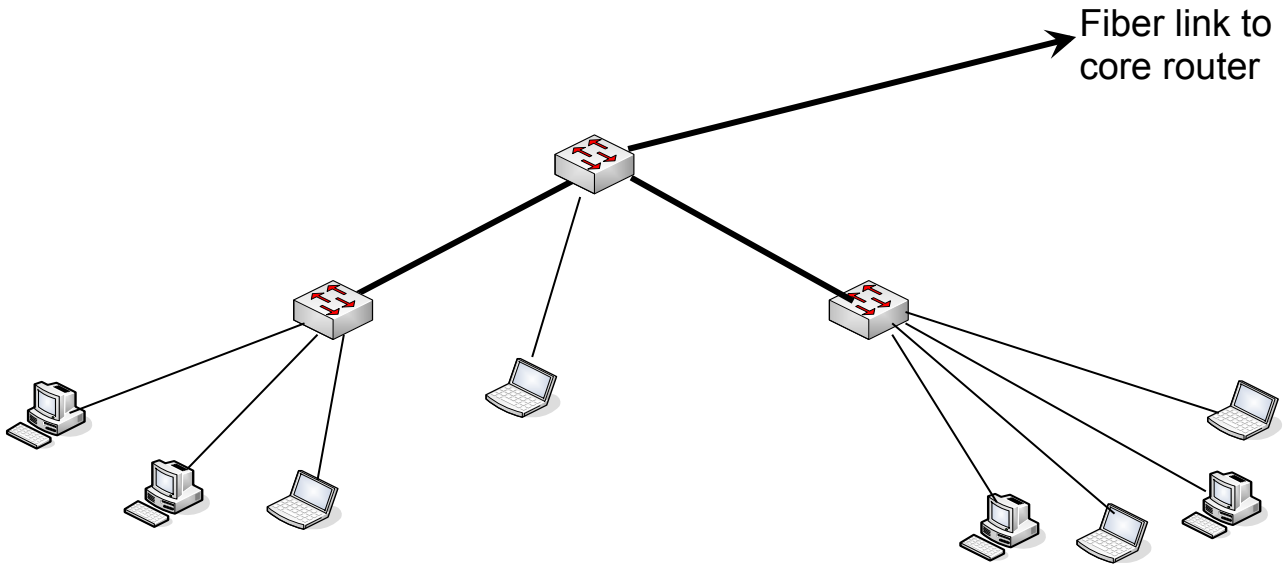
Edge Networks Continued

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



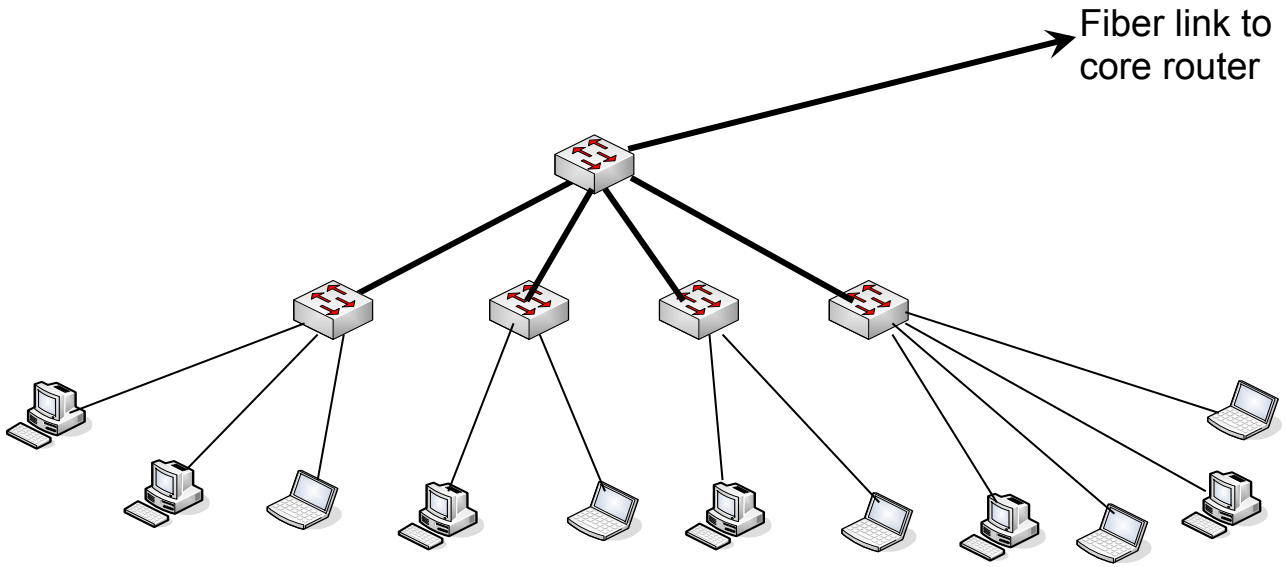
Edge Networks Continued

- And keep adding switches to get to the final configuration



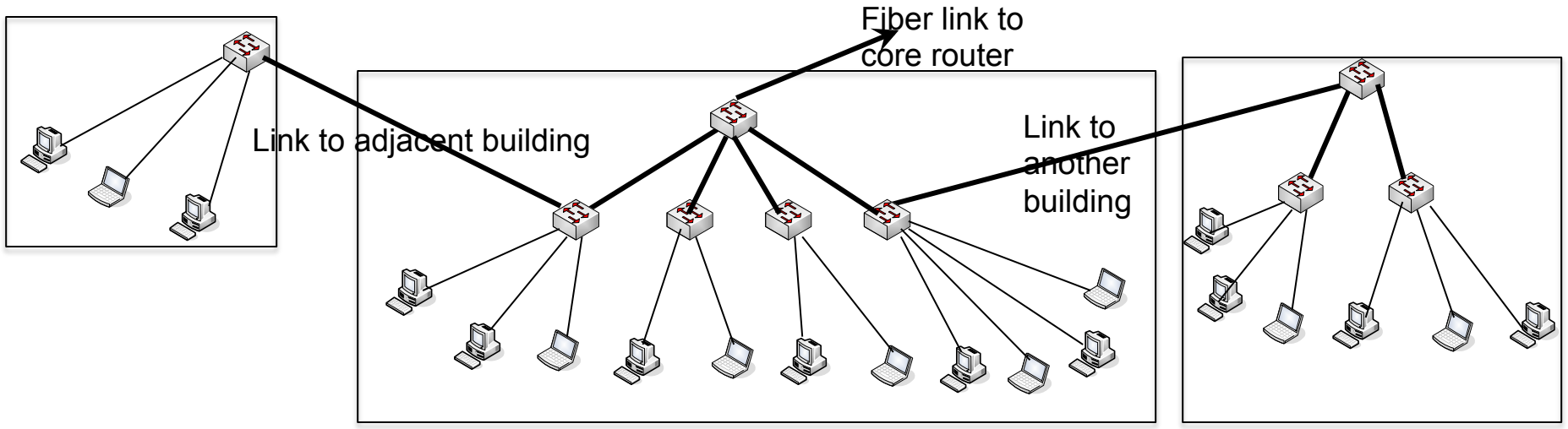
Edge Networks Continued

- And keep adding switches to get to the final configuration



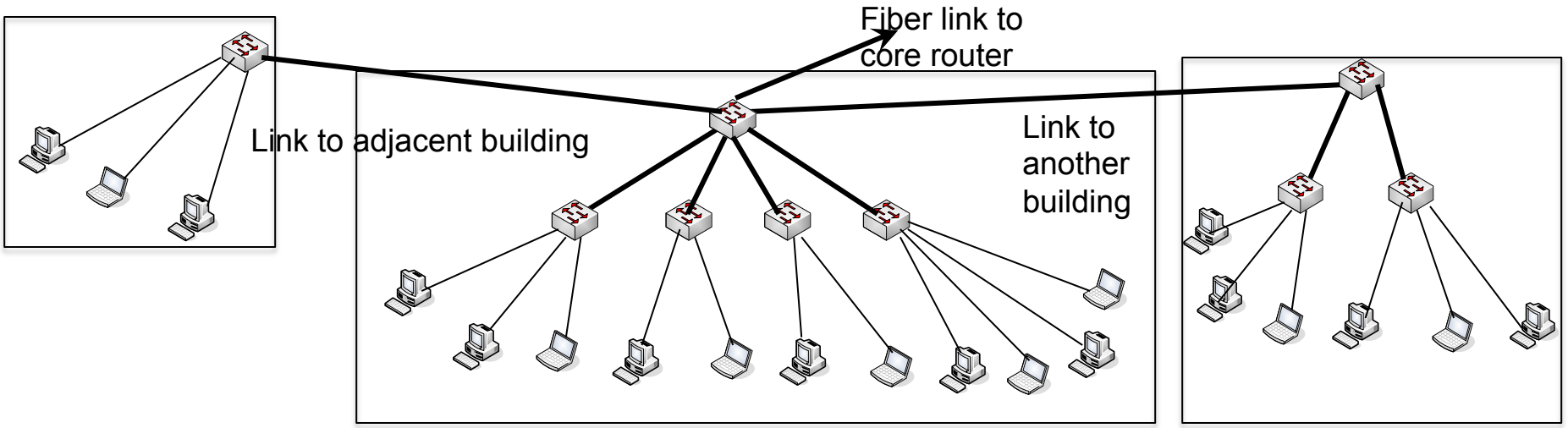
Edge Networks Continued

- 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

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

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

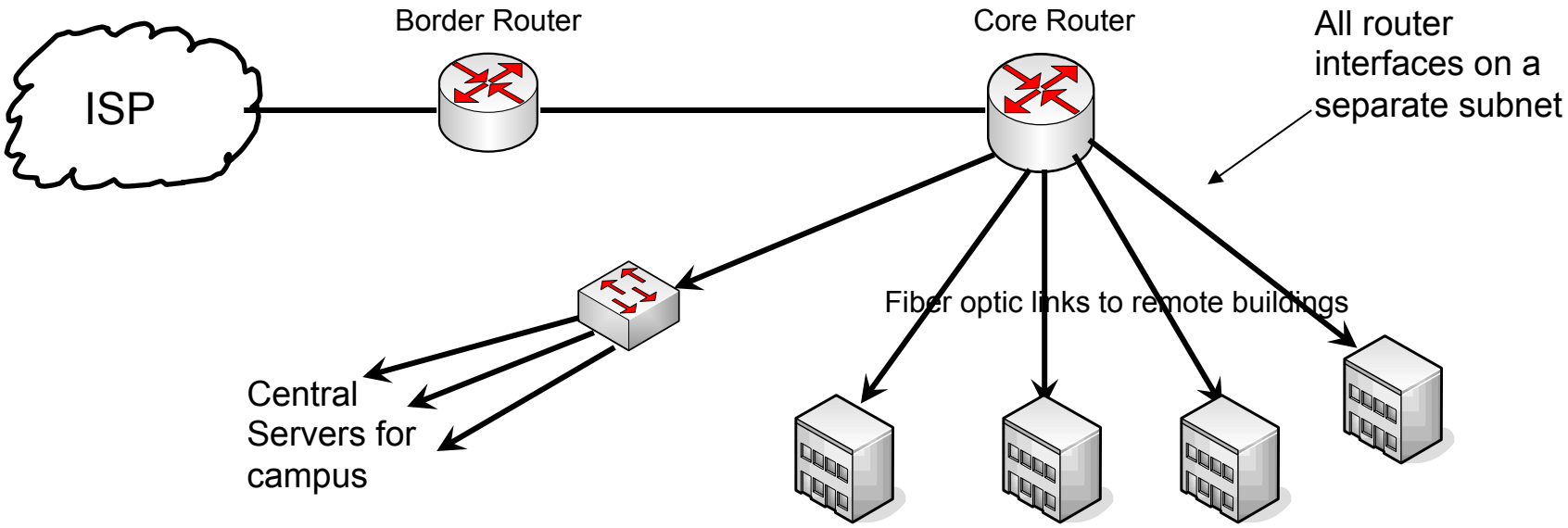
- Many vendors use the term “Layer 3 Switch”.
- These are contradictory terms
  - Layer 3 = Routing
  - Switch = Layer 2
- What vendors mean is that it is a device that can be configured as a router or a switch or possibly both at the same time.

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

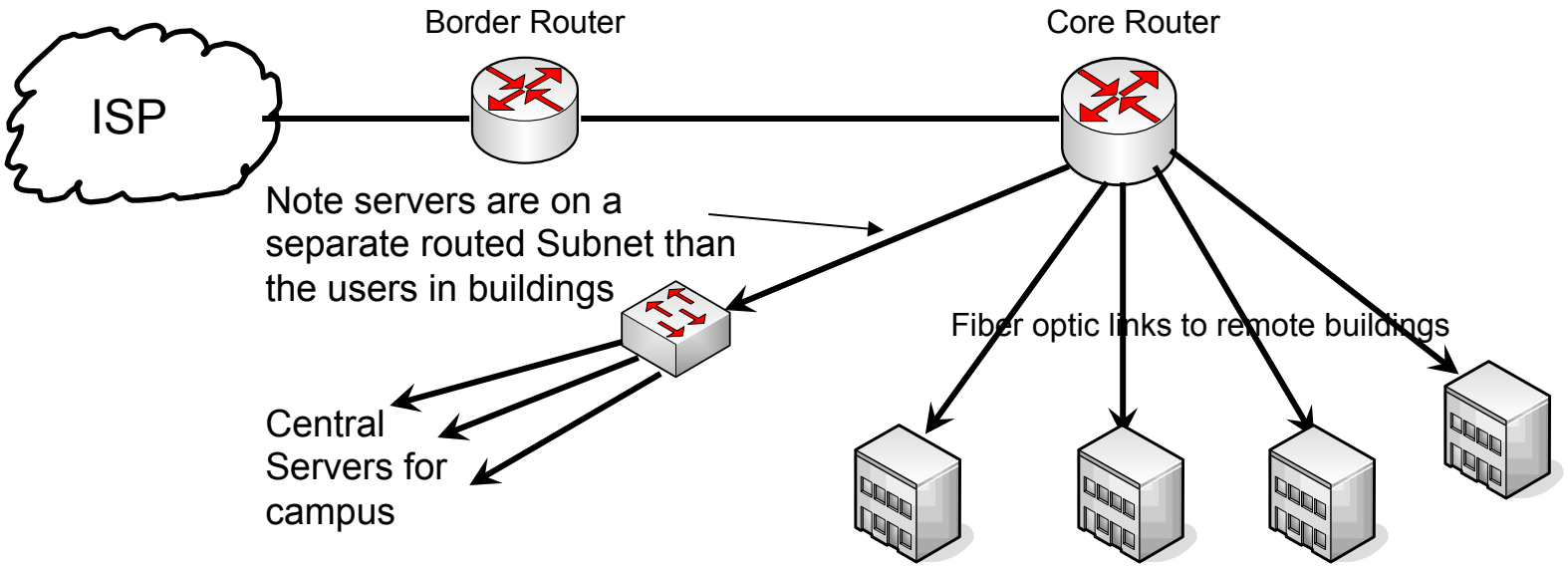
Core Network

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



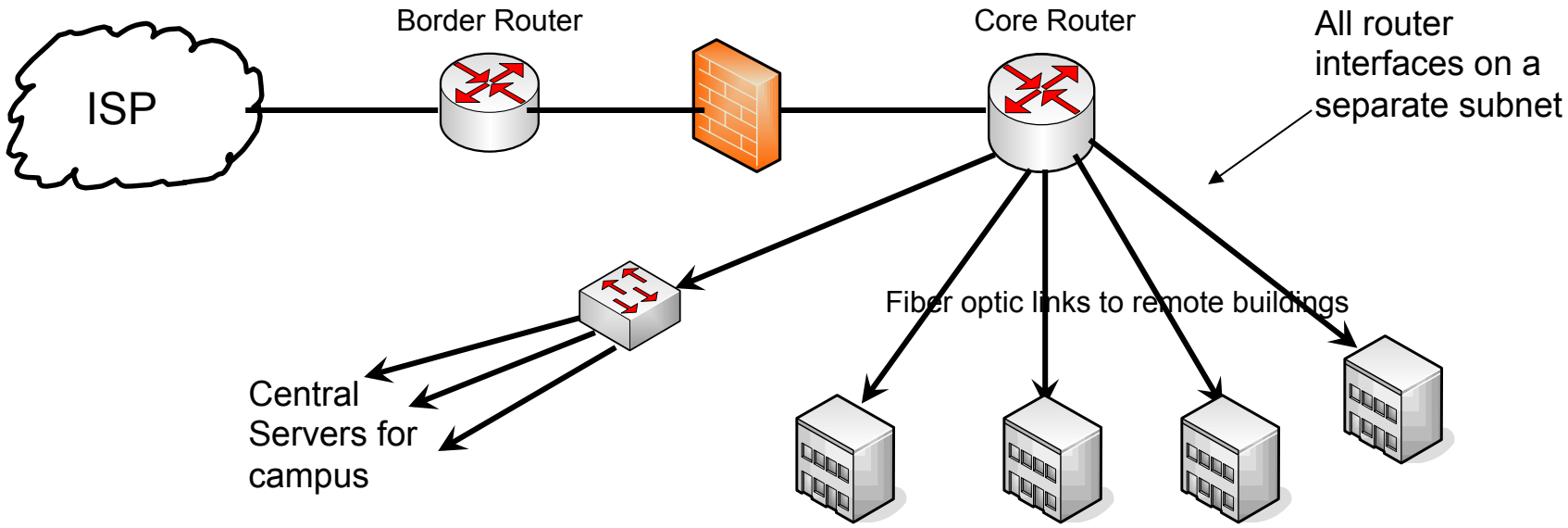
Where to put Servers?

- 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 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:

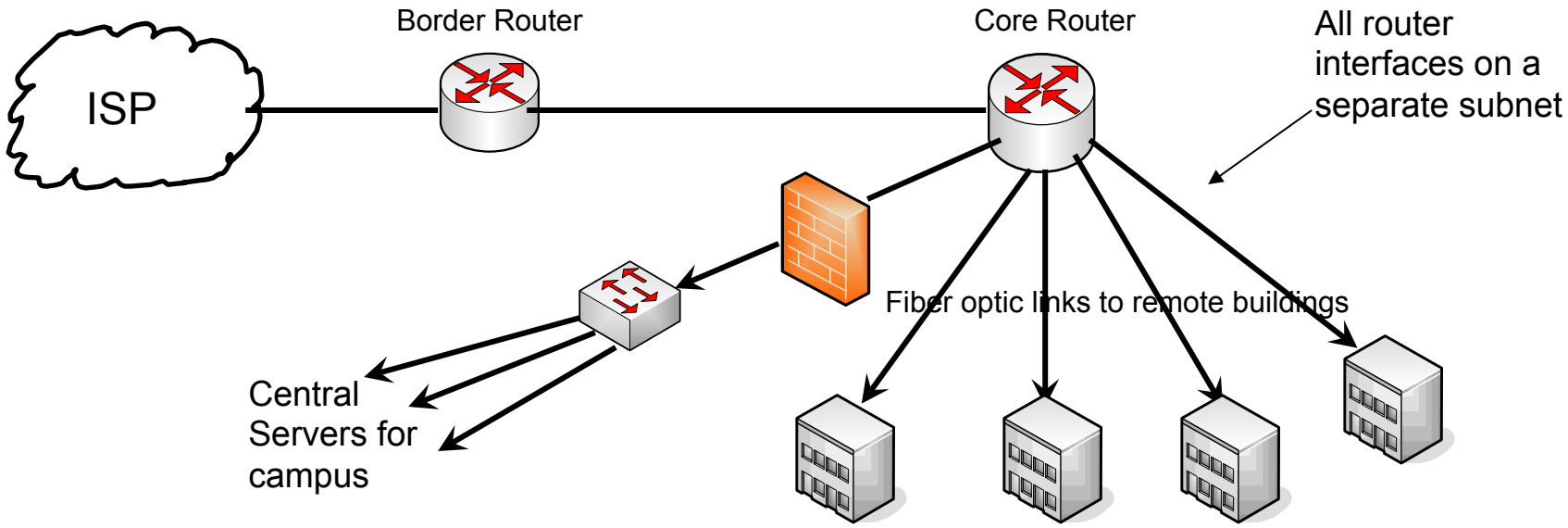


Firewall Placement

- 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.

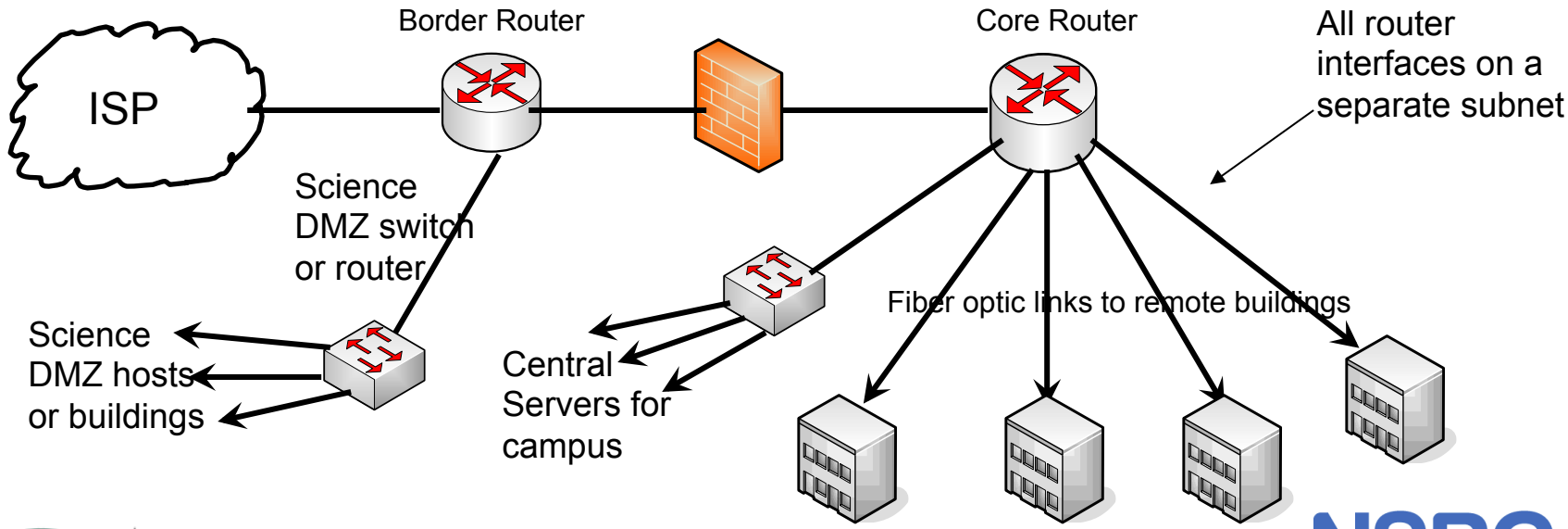
Alternative Suggestion

- Since Firewalls don't really protect users from viruses, let's just think about protecting critical server assets
- This is a typical design:



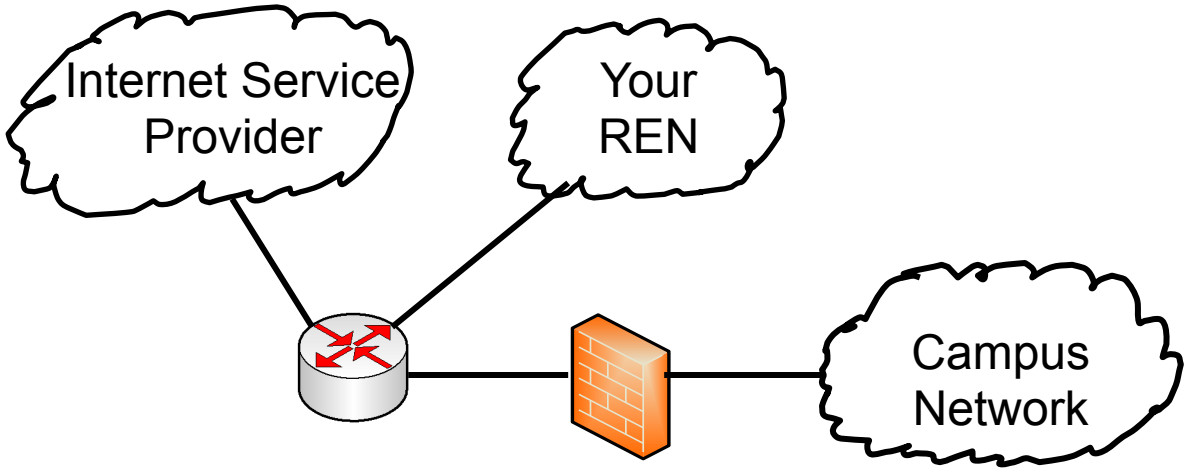
Science DMZ

- 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:

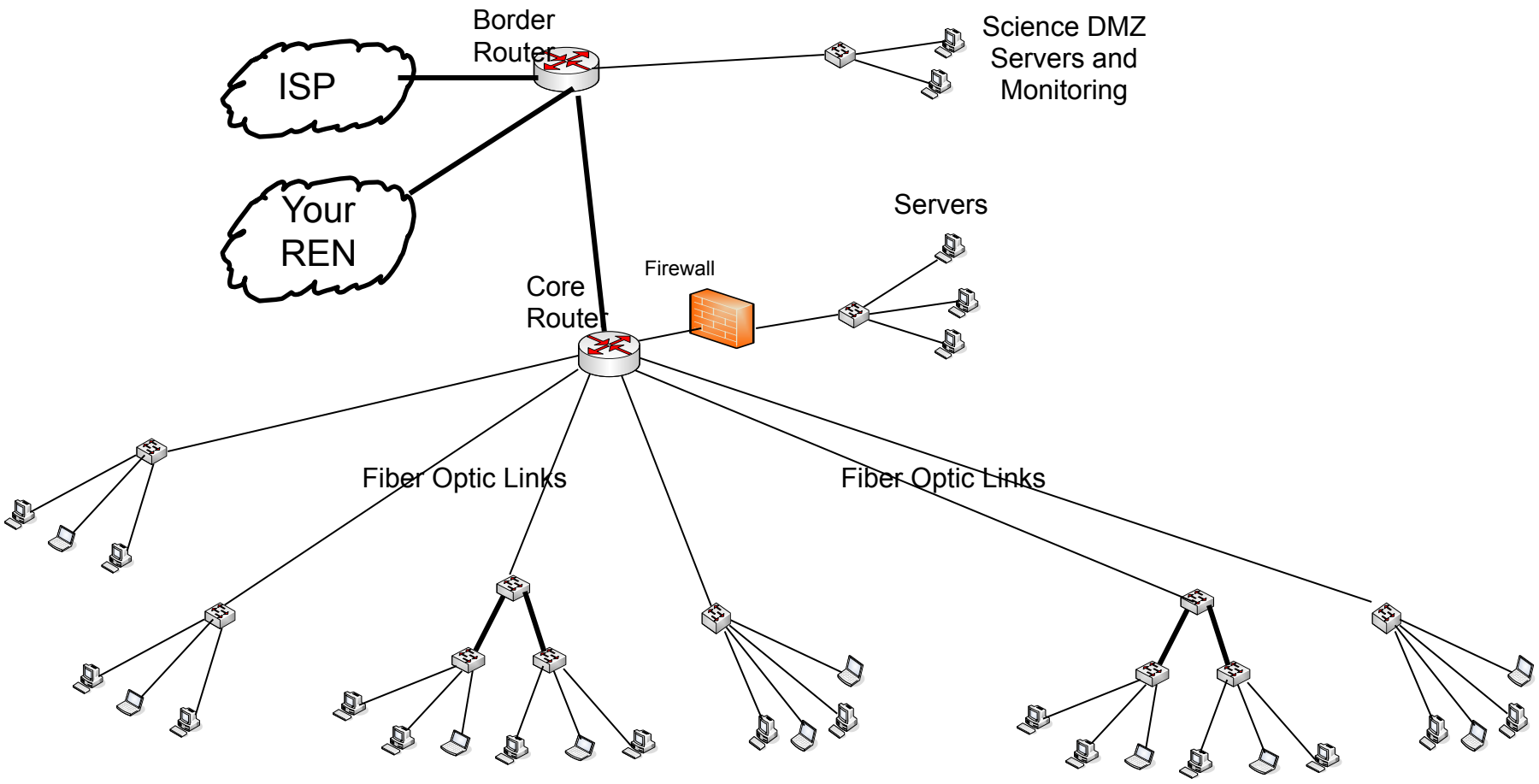


Border Router

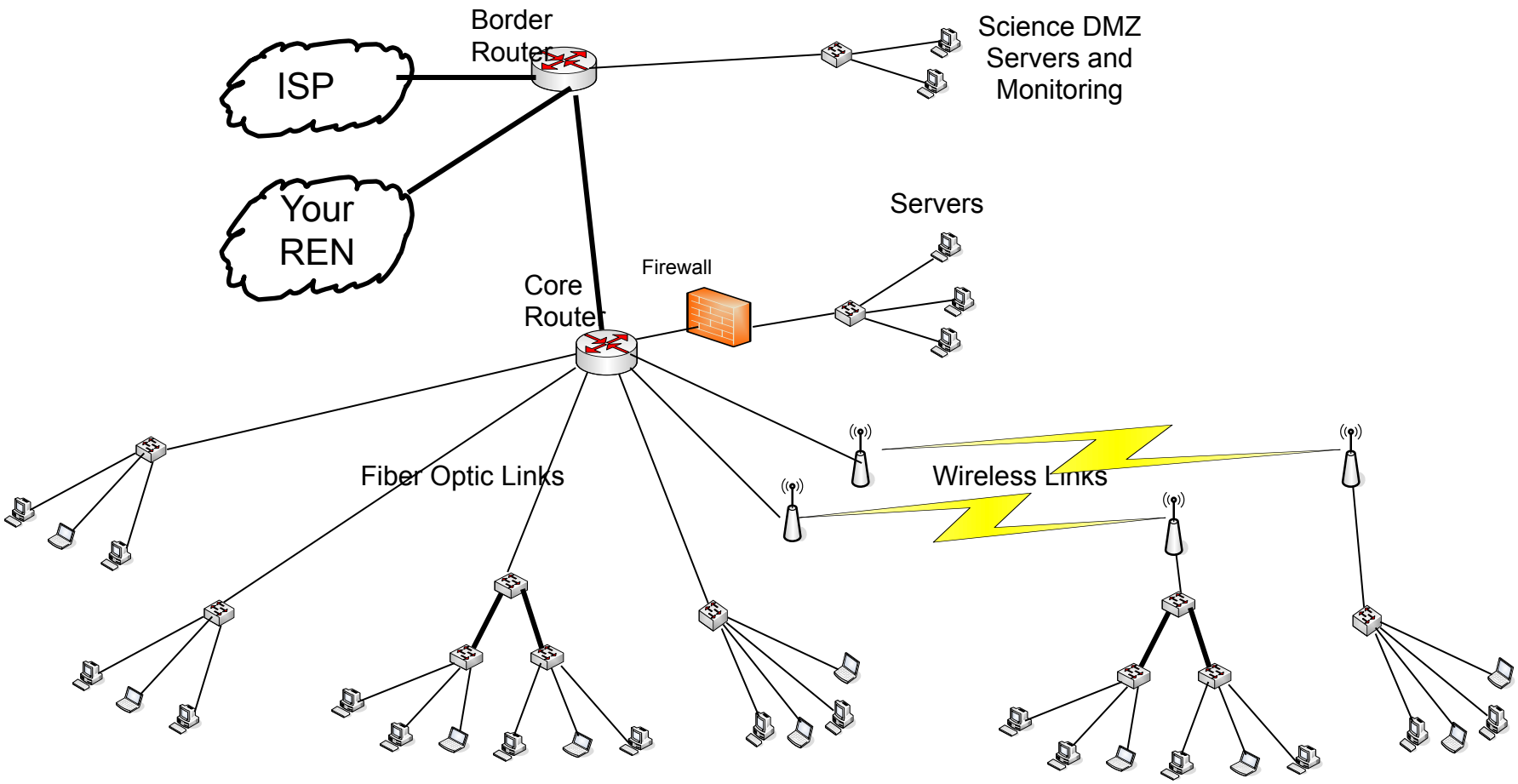
- Connects to outside world
- Many campuses in emerging regions will do NAT on these border routers.
- If you are dual home, you **must** have a border router (dual homing is hard to make it work right)



Putting it all Together



Wireless Links Instead of 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?

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Symbols to use for diagrams