Campus Network Best Practices: Campus Network Design Principles

Dale Smith
Network Startup Resource Center
dsmith@nsrc.org

UNIVERSITY OF OREGON

Why Are We Doing This?

- Our goal is to build networking capacity to support Research and Education
  - Remember: University = Research & Education
- The end game is regional, national, and larger Research and Education Networks (RENs)
- All RENs start with campus networks – they are the foundation of the REN

Why Focus on Campus Networks?

- The Campus Network is the foundation for all Research and Education activity
- Without a good campus network, the Research and Education Network can't work as well as it should
- Ad-hoc campus networks work OK with VSAT or low speed uplinks, but moving to high speed external links, they start to fail.

UNIVERSITY OF OREGON

Why Focus on Campus Networks?

- Your campus network is the foundation that all services are provisioned on
- Ad hoc networks just don't work well. They are unreliable and hard to maintain.
- If you don't have a plan, how will you know where are going?

What are Our Goals?

- Network Design Goals
  - Reliability/Resiliency
  - Performance
  - Manageability
    - Must have this to find problems and viruses
  - Scalability
    - Need to be able to grow as needs grow
- Need this in the campus and the REN

Campus Network Rules

- Separate layers of your network
- Minimize number of network devices in any path
- Use standard solutions for common situations
- Provision central services near the core
- Route near the core, switch at the edges
- Separate core router functions from border router functions
- Use DHCP centrally
- Separate DNS server duties

UNIVERSITY OF OREGON

Campus Network Design

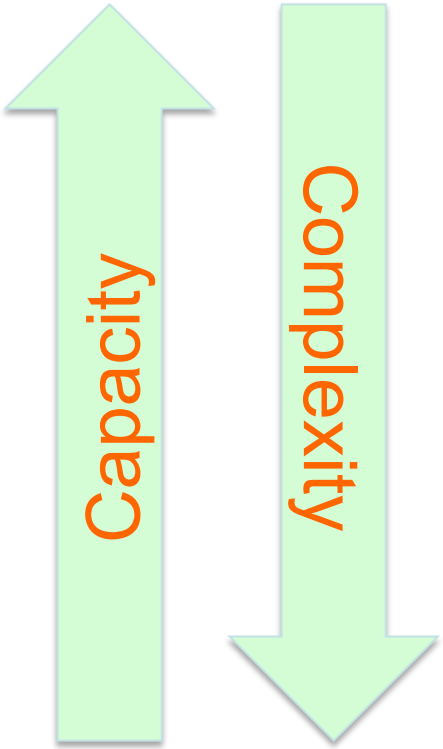
- A good network design is modular and hierarchical, with a clear separation of functions:
  - **Core**: Resilient, few changes, few features, high link and high CPU capacity
  - **Distribution**: Aggregation, redundancy
  - **Access**: Port density, affordability, security features, many adds, moves and changes

Layers Features

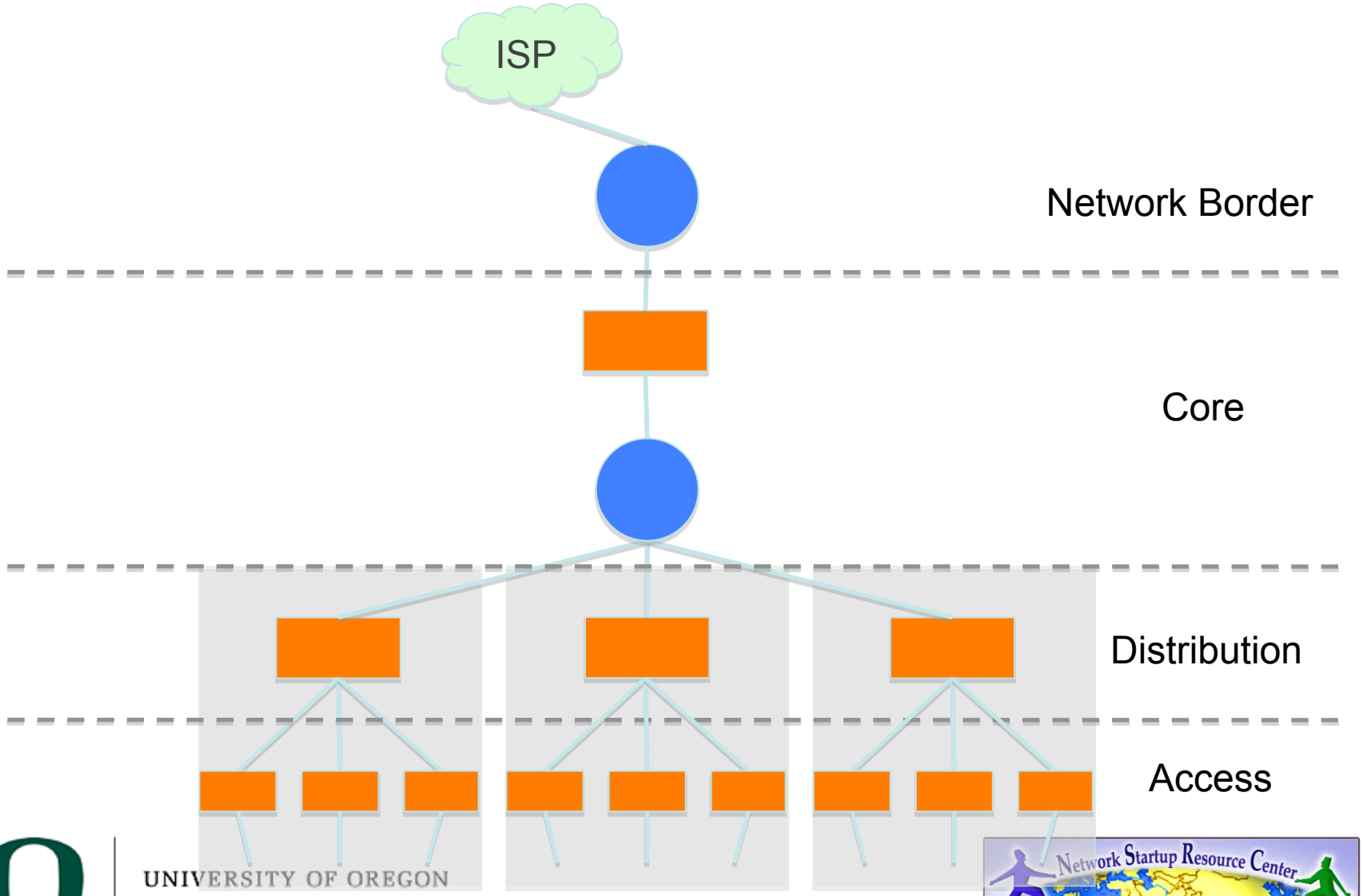
Core

Distribution

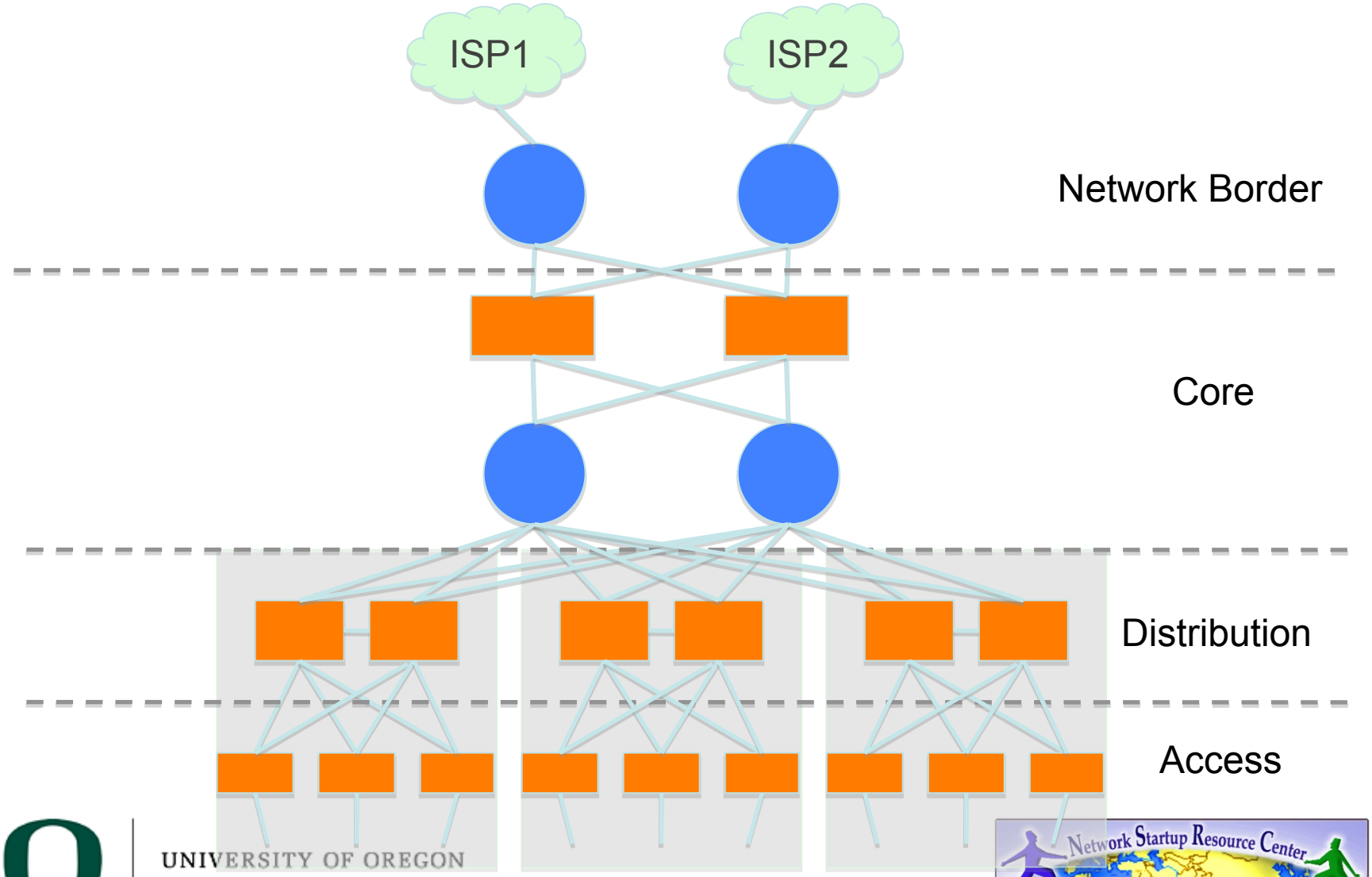
Access



Campus Network Design - Simple

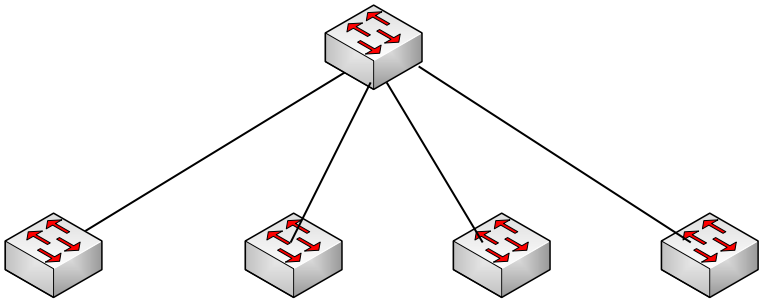


Campus Network Design - Redundant

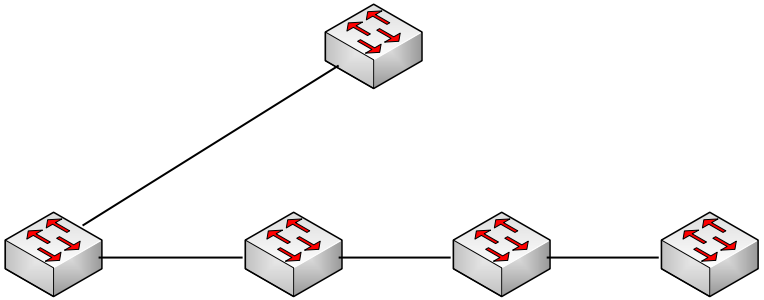


Minimize Number of Network Devices in the Path

- Build star networks



- Not daisy chained networks



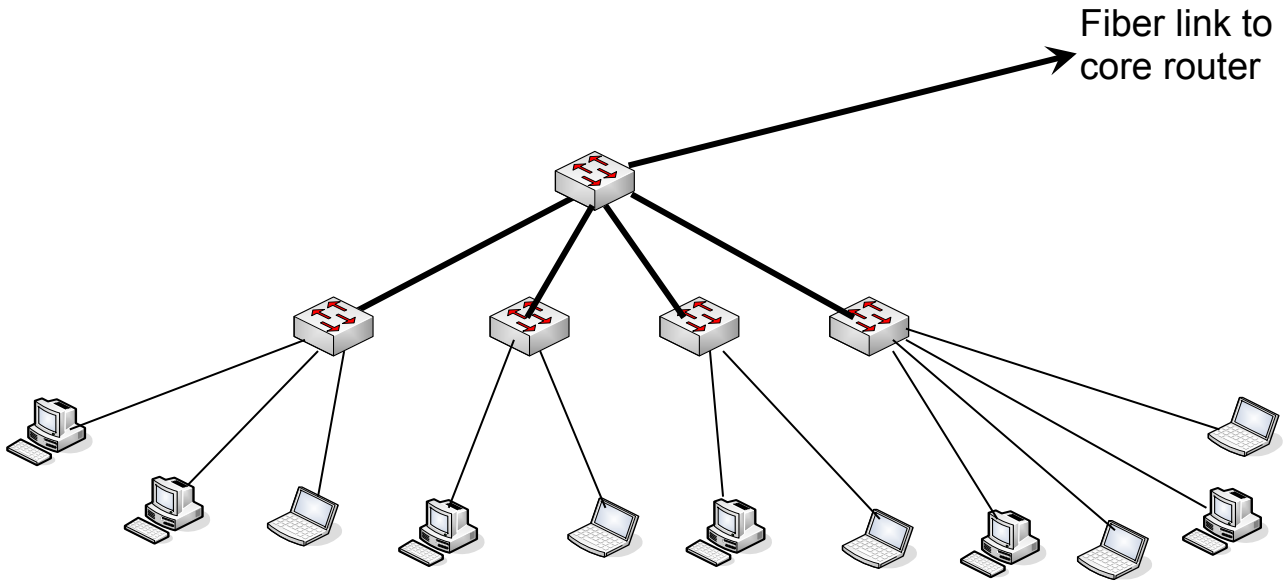
Edge Networks (Layer 2 LANs)

- 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!

UNIVERSITY OF OREGON

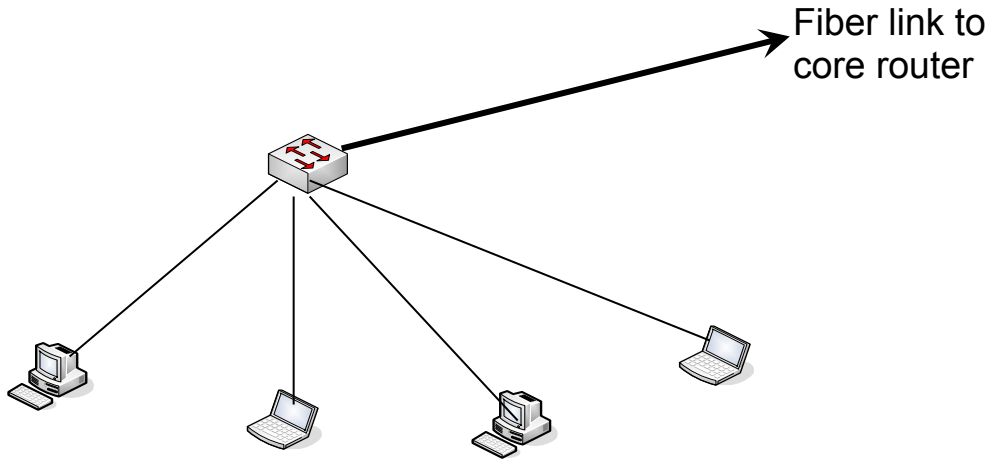
Edge Networks

- Make every network look like this:



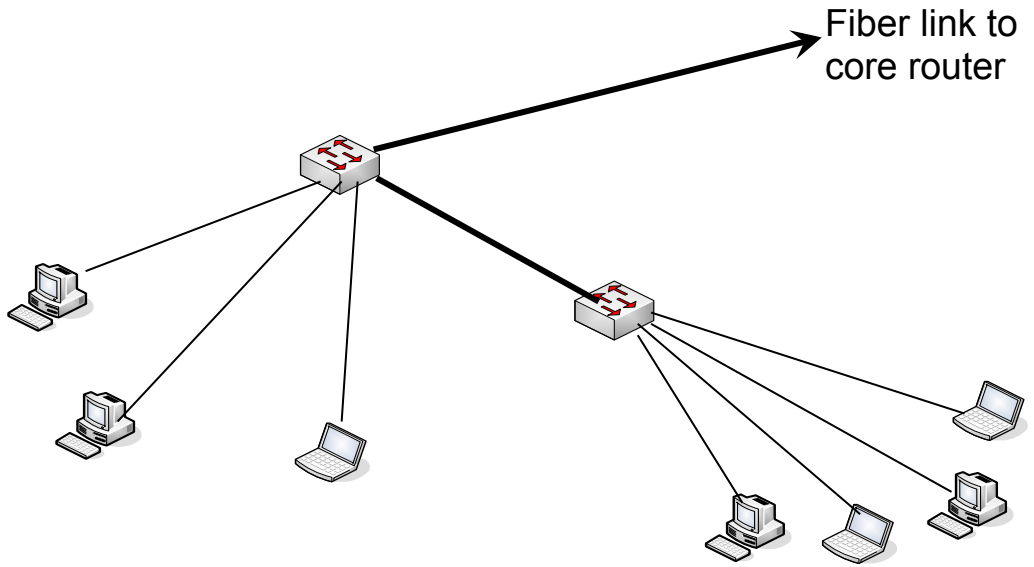
Edge Networks Continued

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



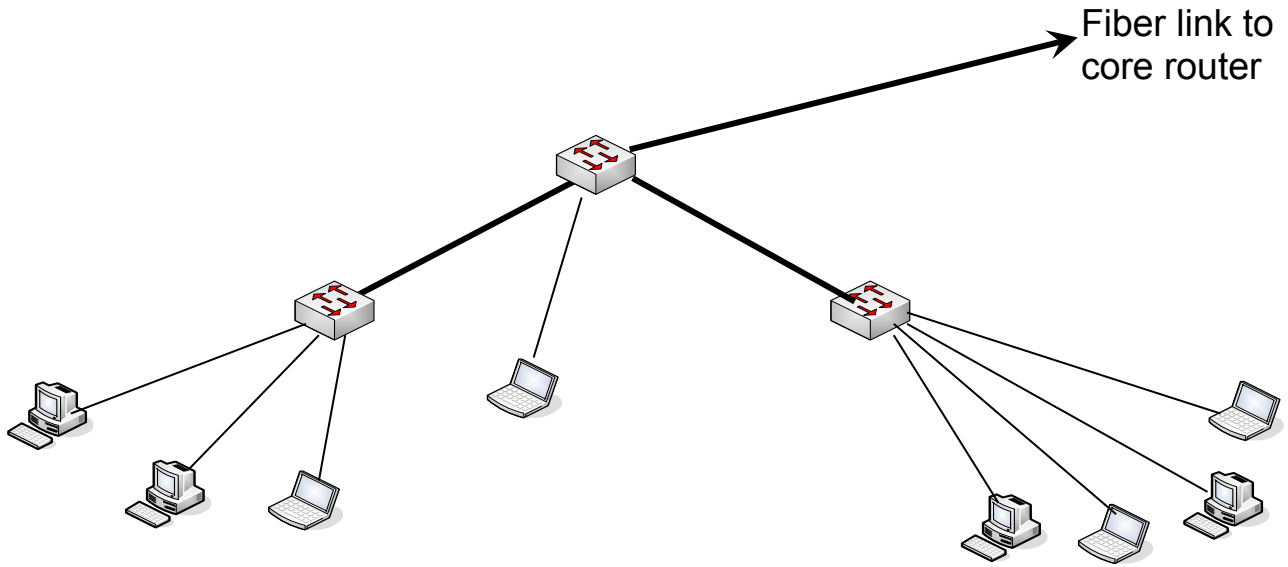
Edge Networks Continued

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



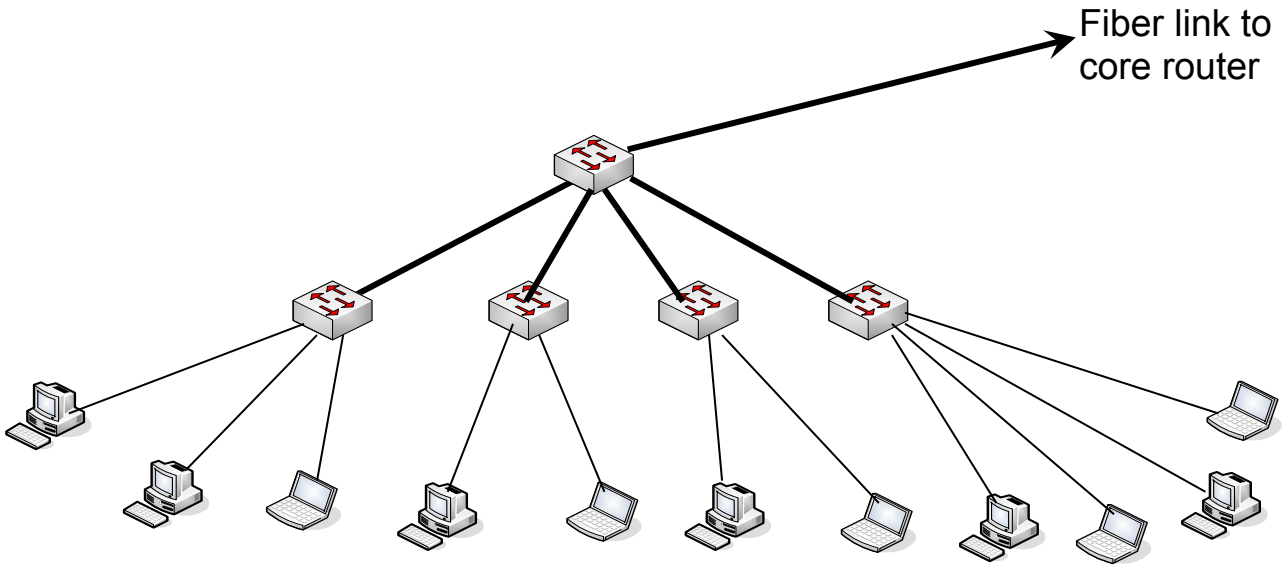
Edge Networks Continued

- And keep adding switches to get to the final configuration



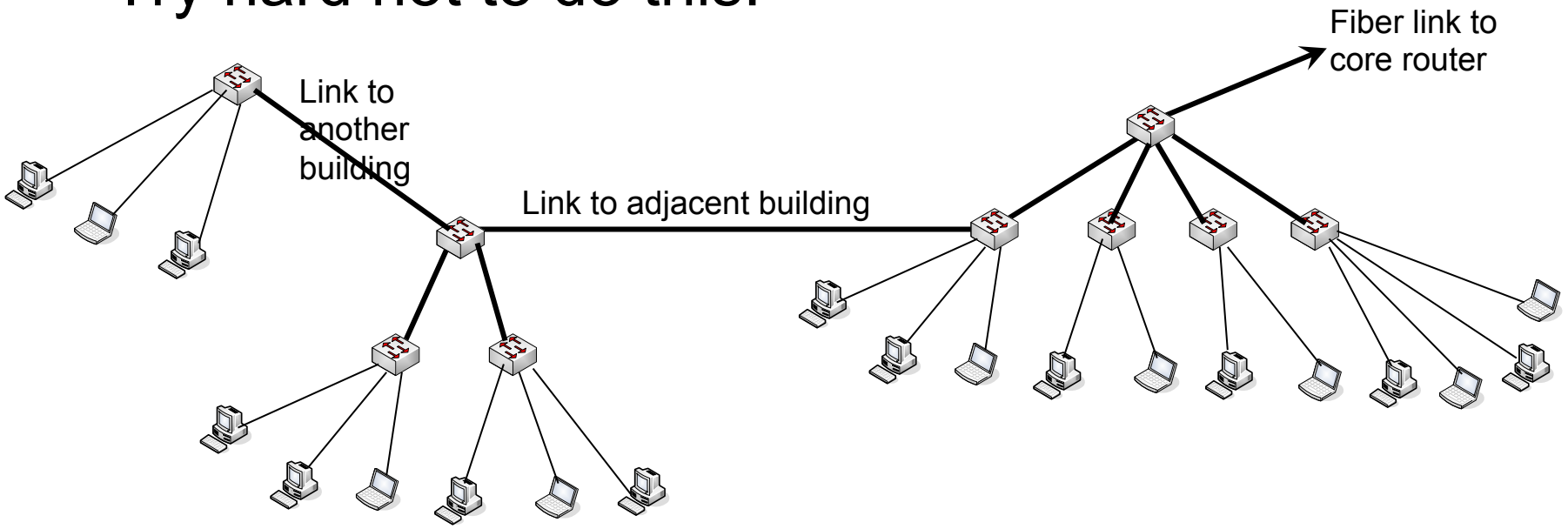
Edge Networks Continued

- And keep adding switches to get to the final configuration



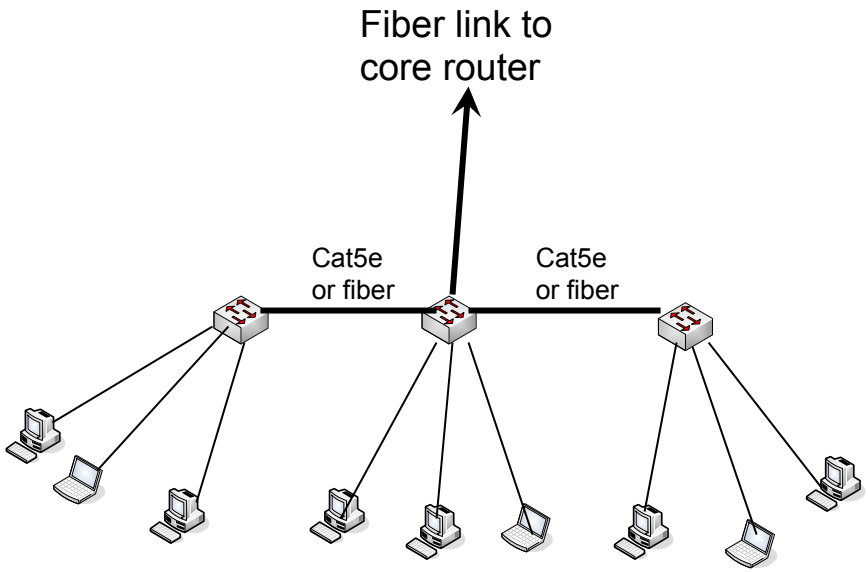
Edge Networks Continued

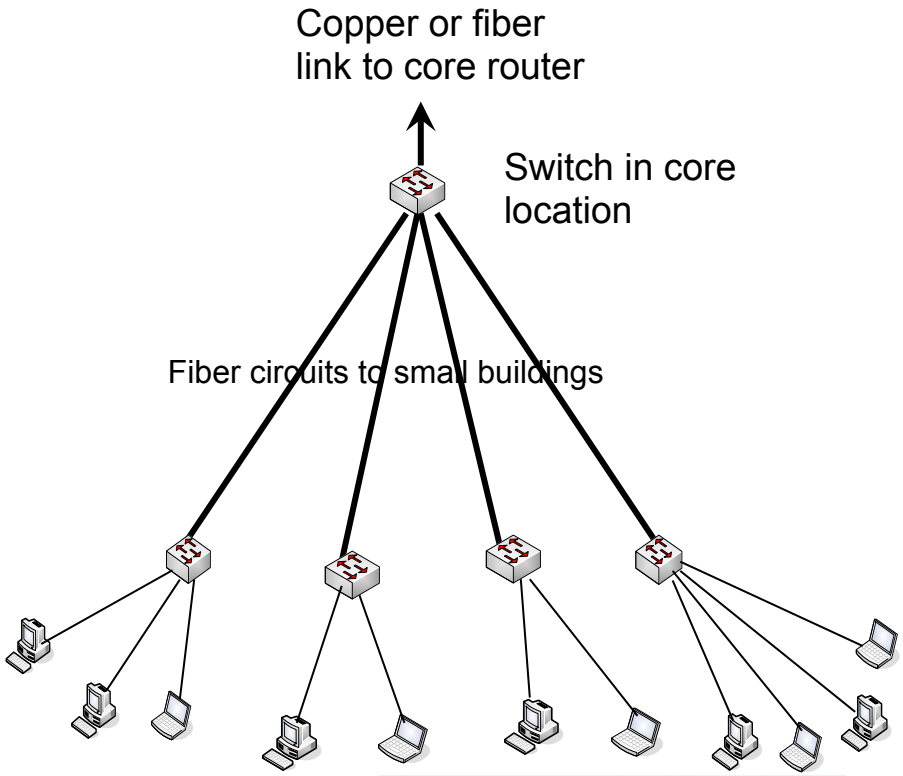
- Resist the urge to save money by breaking this model and daisy chaining networks or buildings together
- Try hard not to do this:



Edge Networks Continued

- There are cases where you can serve multiple small buildings with one subnet.
- Do it carefully.
- Two basic models:





Core Network

UNIVERSITY OF OREGON

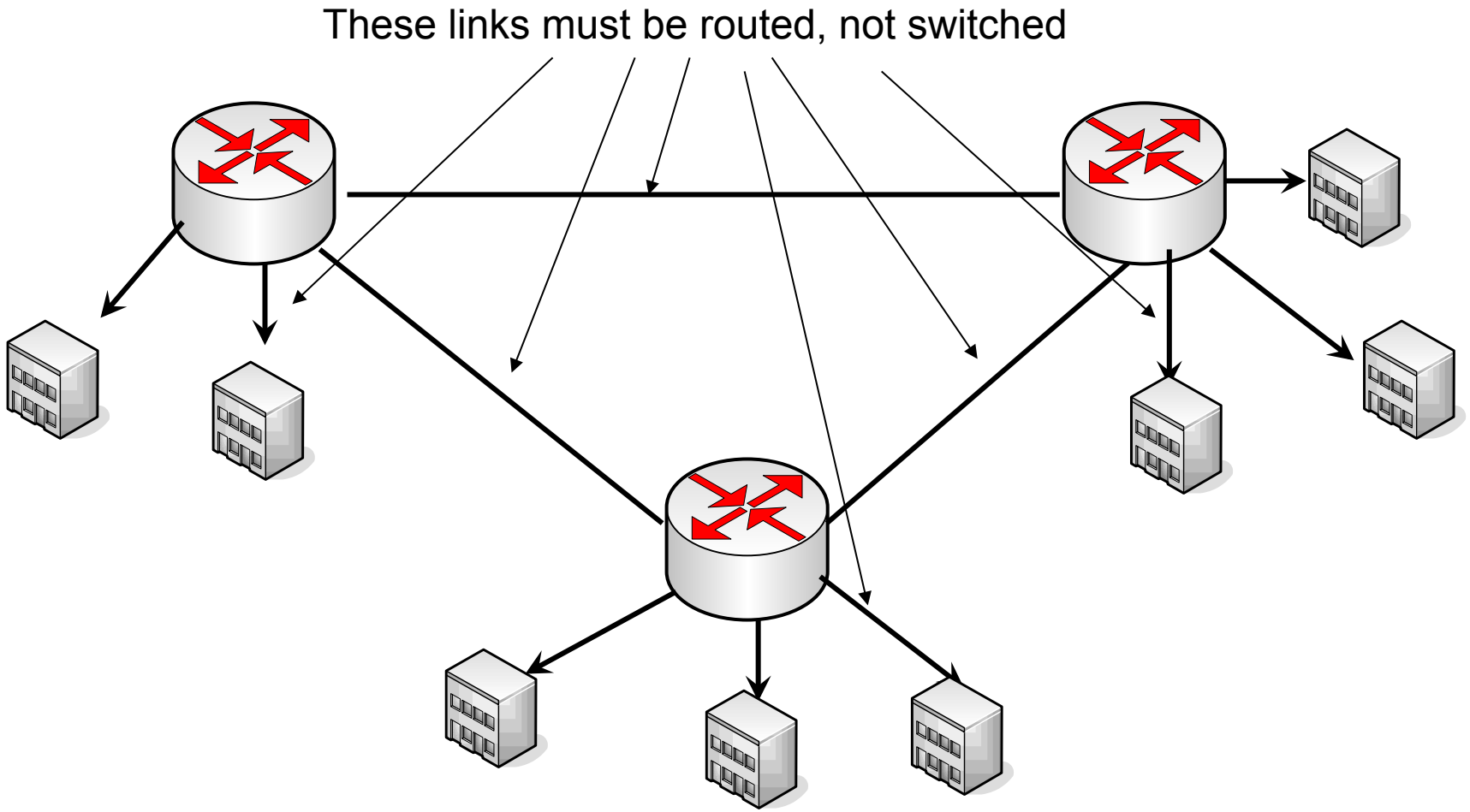
Core Layer

- Core network is the "core" of your network
  - Reliability is key
    - Keep it simple!
  - Always route (not switch) in the core
  - Reliable power and air conditioning
  - As you grow:
    - Add more devices for redundancy or better performance
    - Use dual power supplies fed from separate UPSs

Routing versus Switching
Layer 2 versus Layer 3

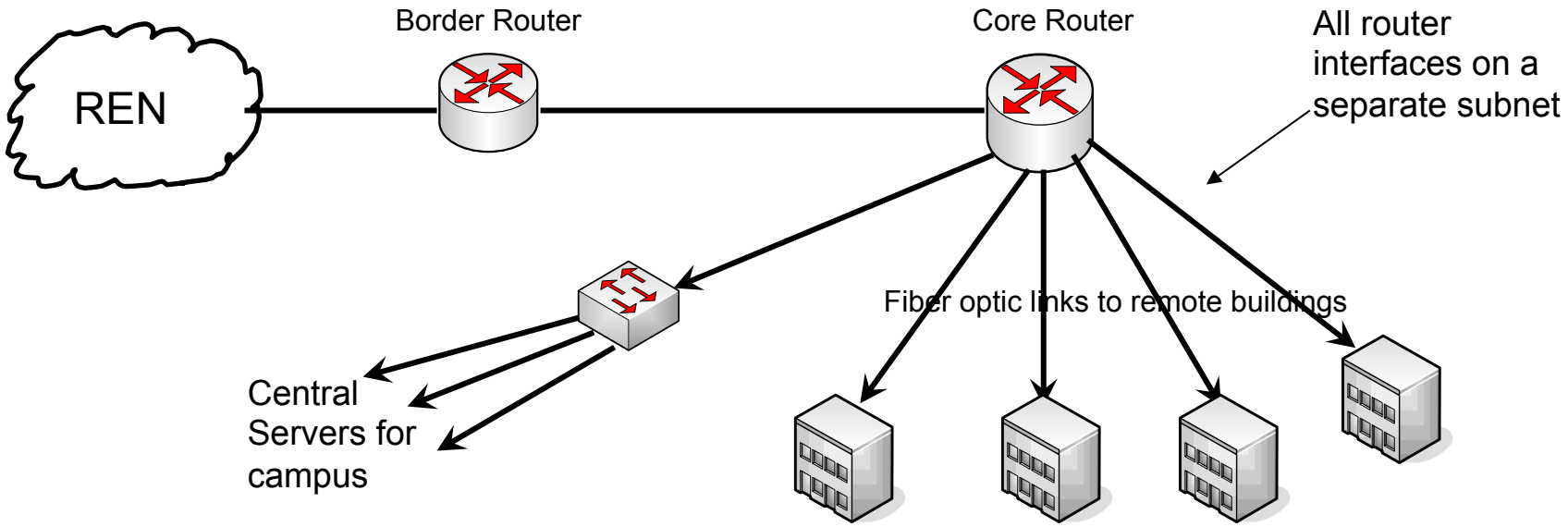
- Routers provide more isolation between devices (they stop broadcasts)
- Routing is more complicated, but also more sophisticated and can make more efficient use of the network, particularly if there are redundancy elements such as loops

Switching versus Routing



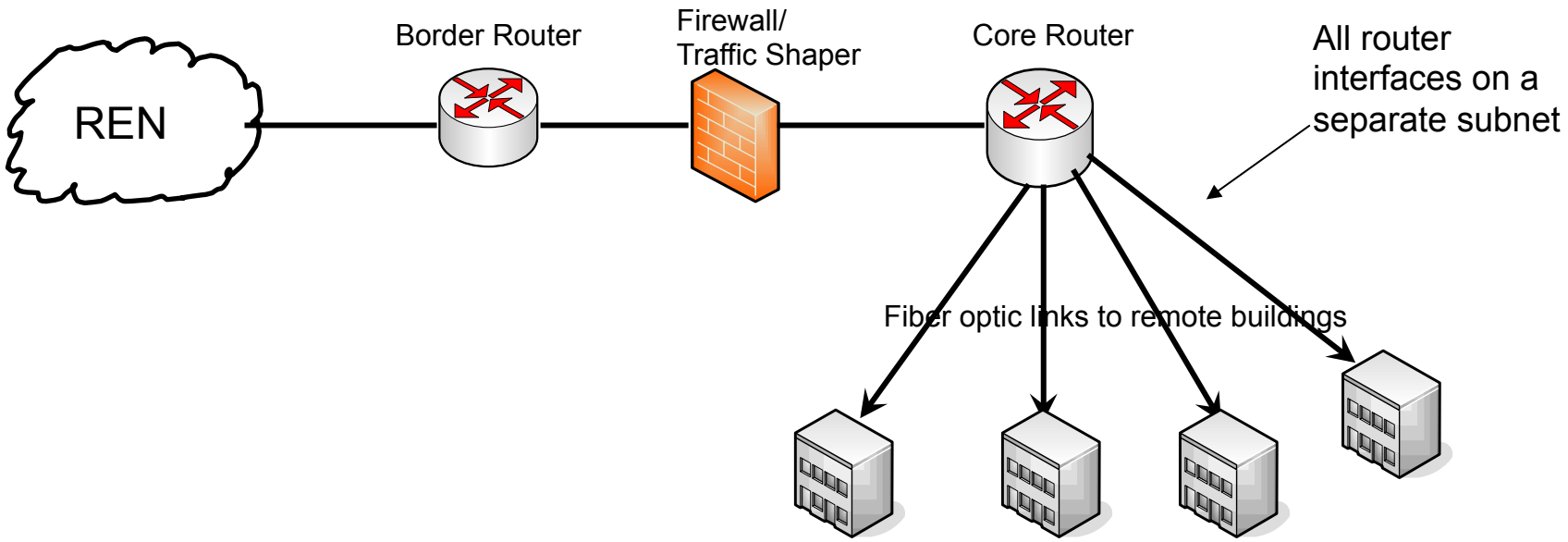
Core Network

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



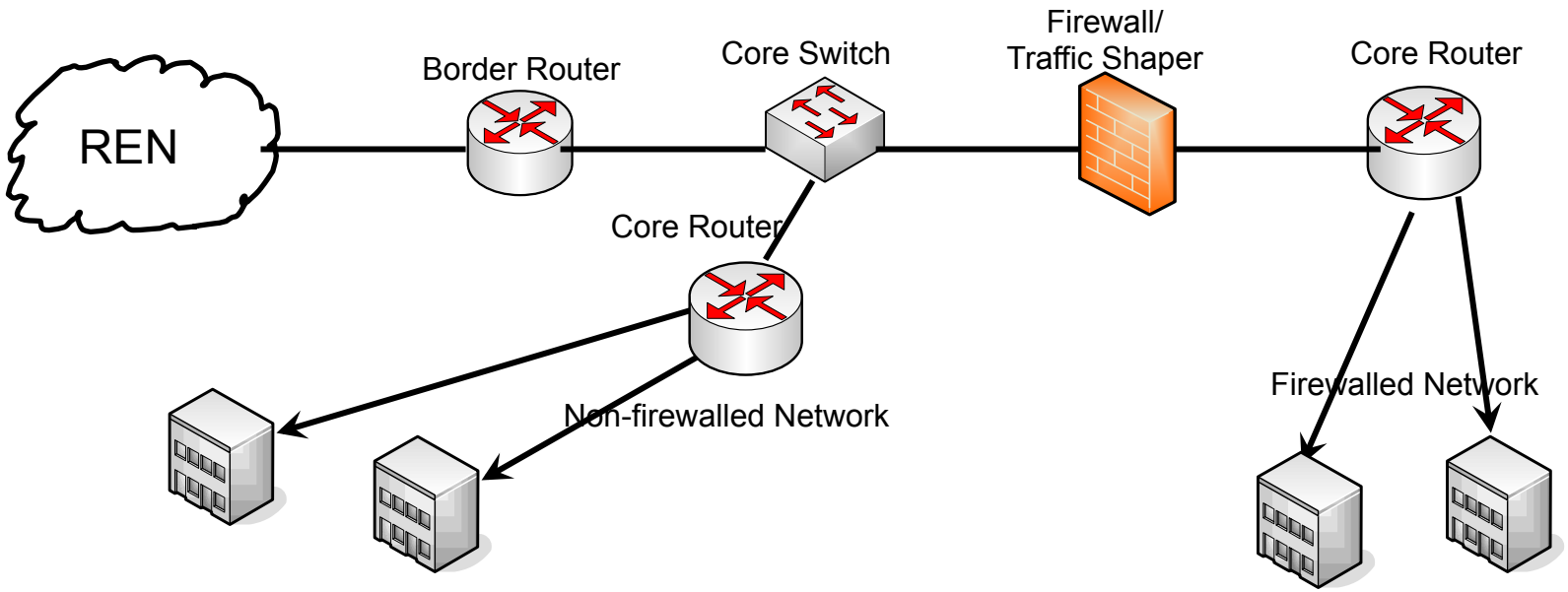
Where to put Firewalls or NAT

- Firewalls or NAT devices must be placed “in line”
- This means that the speed of this device affects access to the outside world
- This is a typical design, but think about alternatives



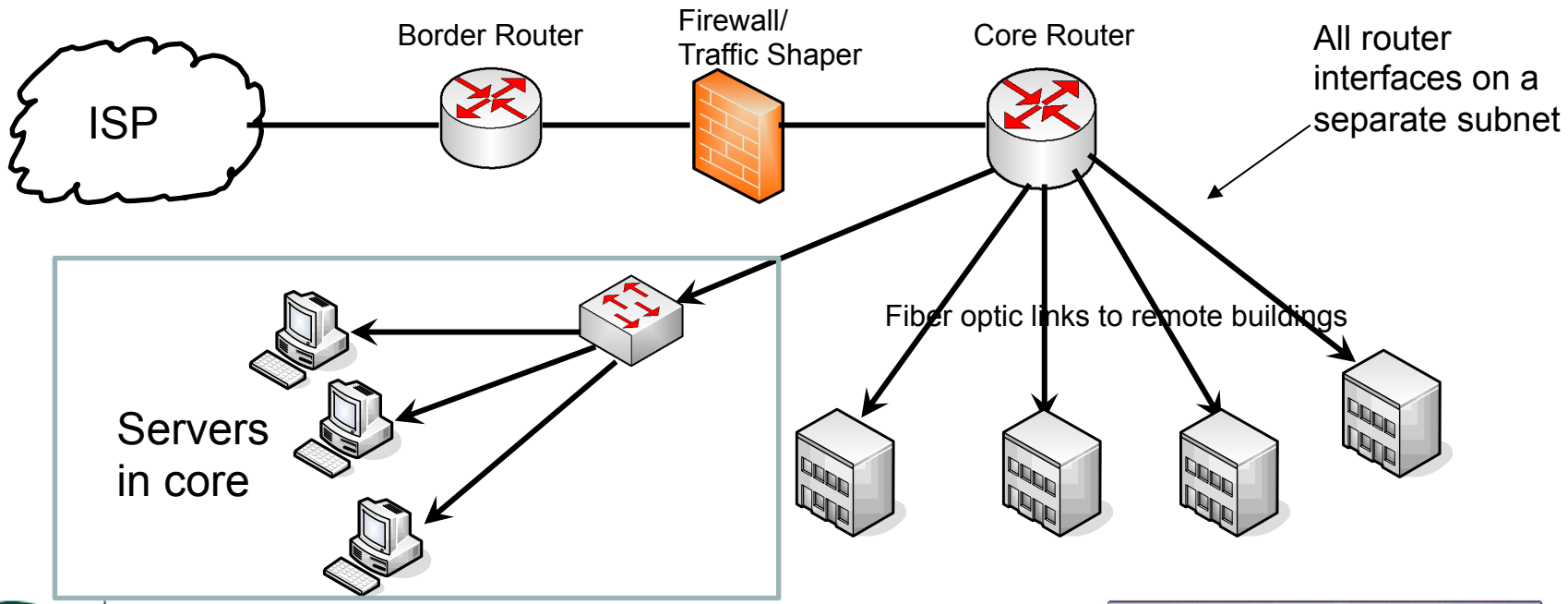
Where to put Firewalls

- Try to have parts of your network non-firewalled, non NATed
- This will allow full bandwidth, un-filtered access to the Internet
- Simple configuration:



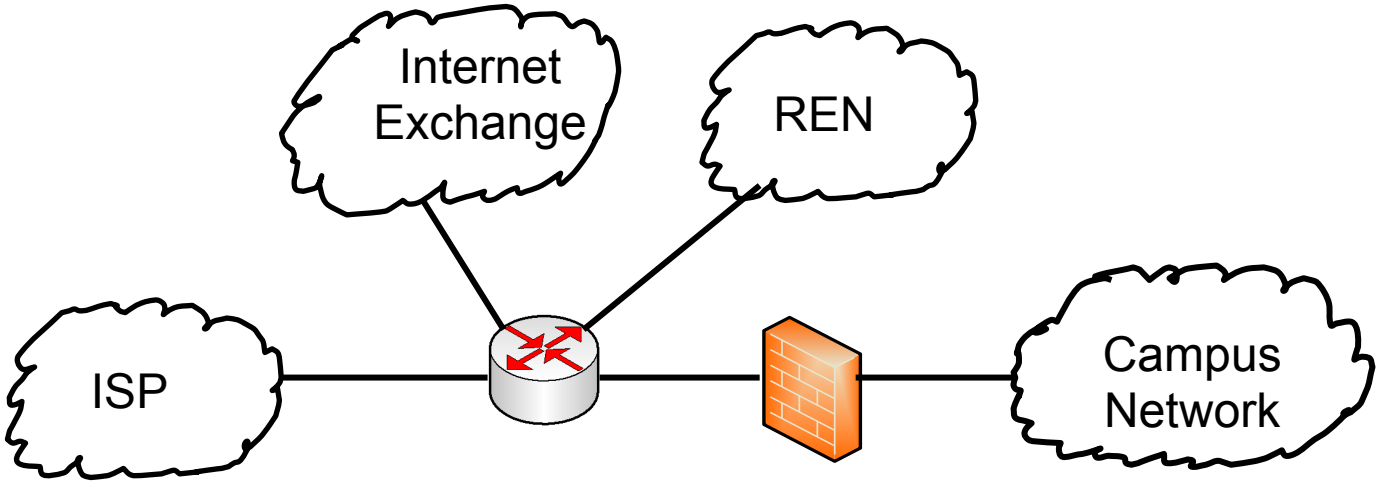
Where to put Servers?

- Servers should be on a high speed interface off of your core router
- Servers should be at your core location where there is good power and air conditioning

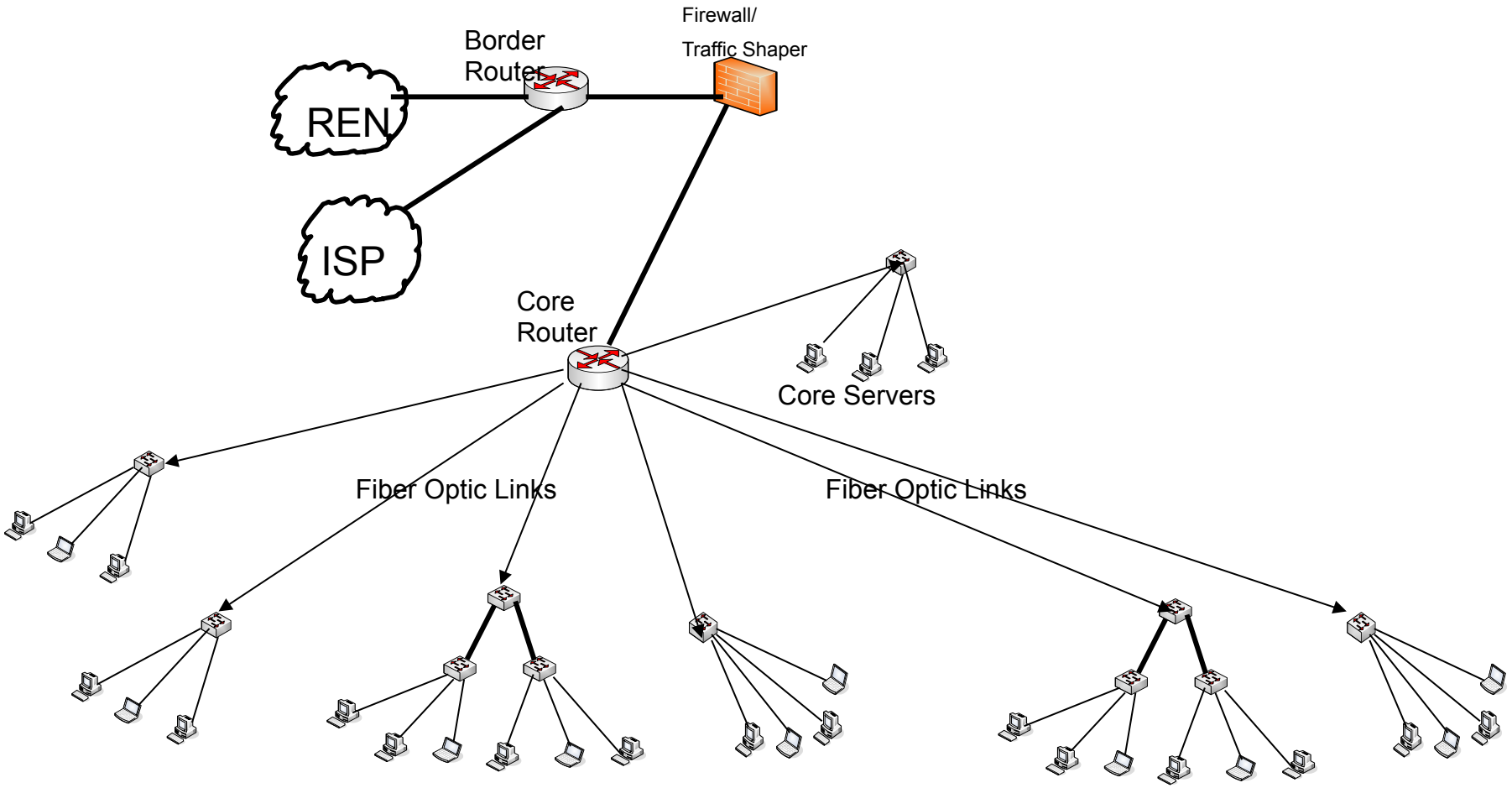


Border Router

- Connects to outside world
- RENs and Peering are the reason you need them
- Must get Provider Independent IP address space and Autonomous System Number and run BGP to really make this work right

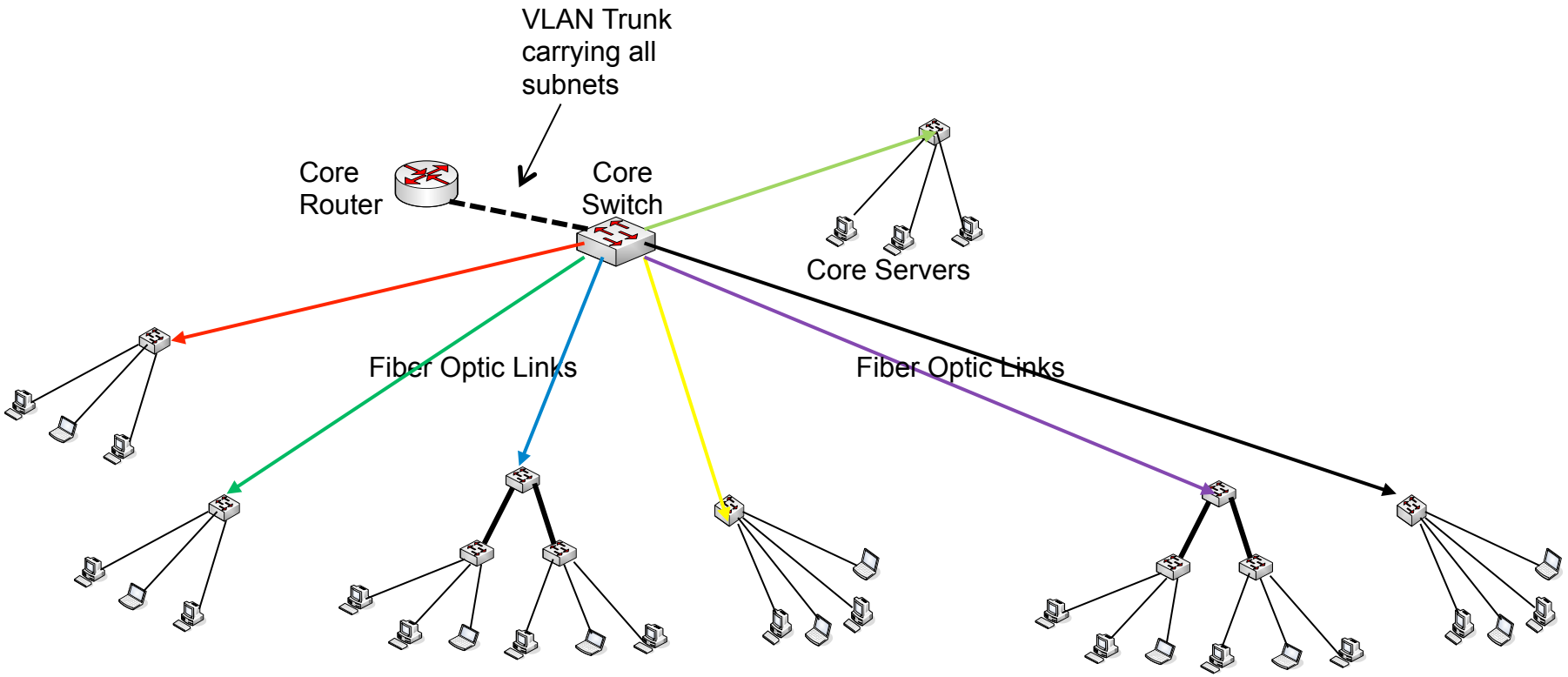


Putting it all Together



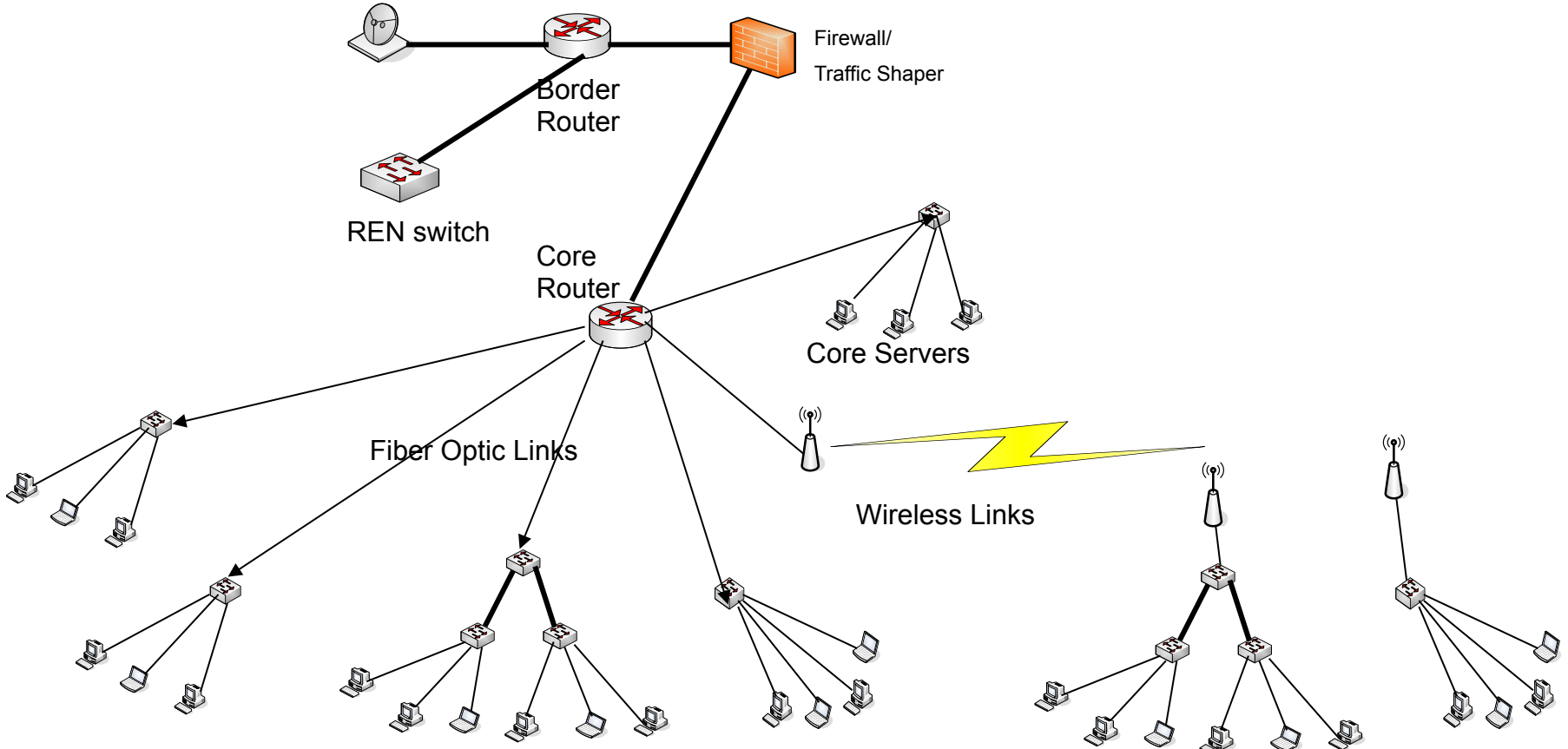
Alternative Core Designs

- One Armed Router for Core



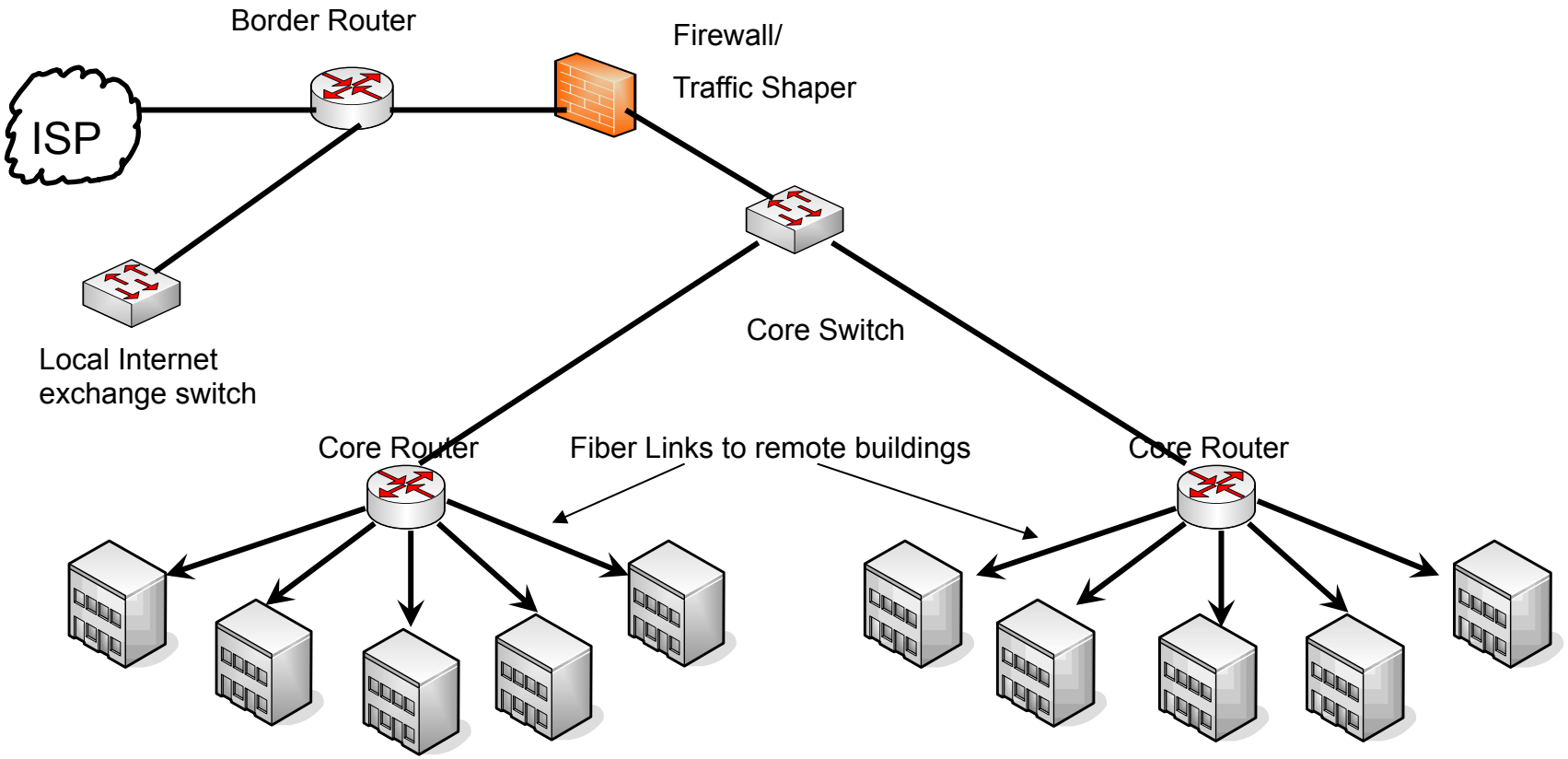
Alternative Core Designs

- Wireless Links versus Fiber

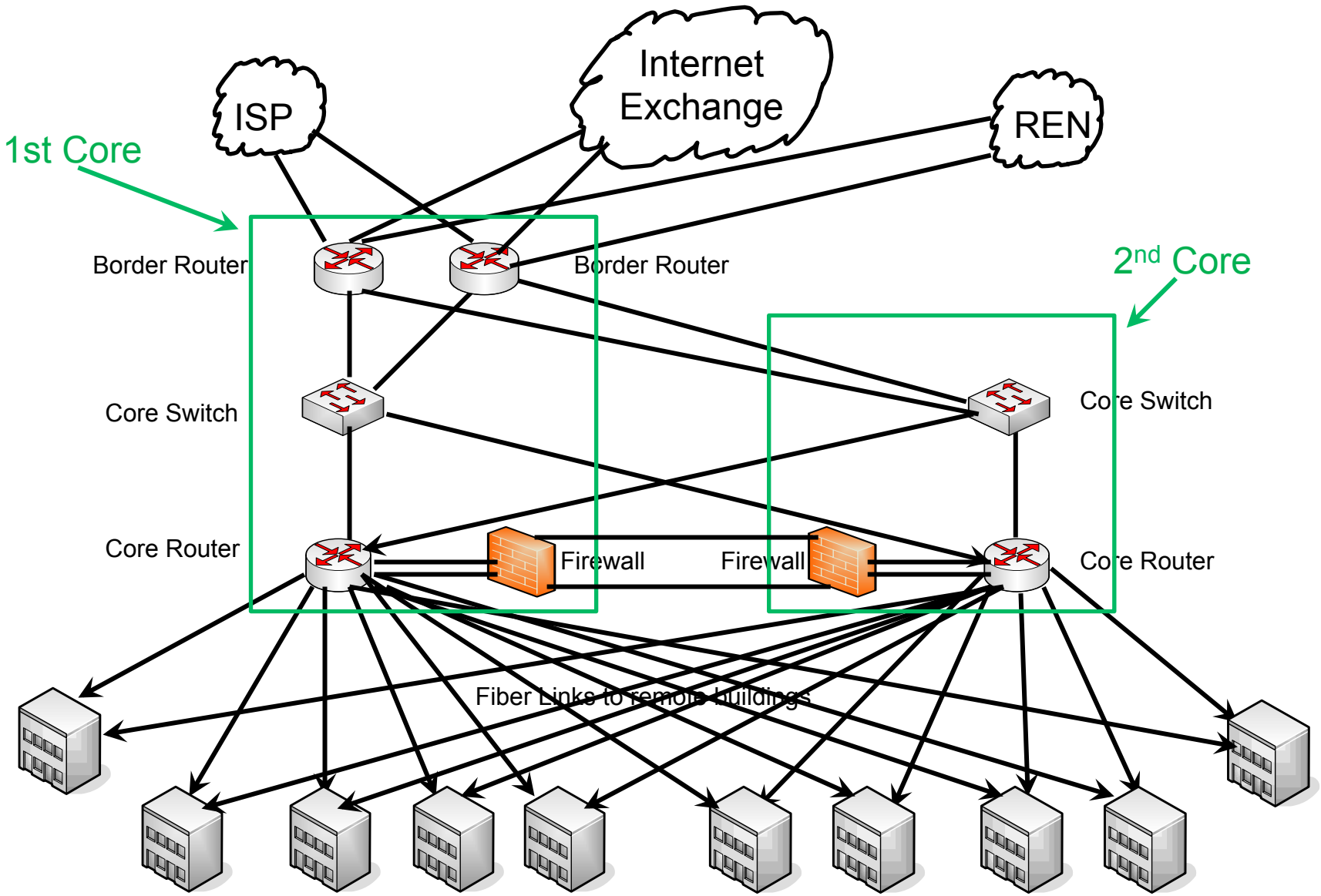


Complex Core Designs

- Multiple Core Routers



More Complex Core Designs



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

DHCP

- Dynamic Host Configuration Protocol
  - Used to assign IP address and provide basic IP configuration to a host.
- Simplifies your life greatly
  - Faster
  - Fewer mistakes
  - Easier renumbering
- Should be provisioned centrally
  - Requires relaying across layer 3 networks

Central DHCP

- In order to centralize your DHCP service, you need a DHCP relay on each subnet
  - Most routers provide this feature
    - Also possible on Linux routers using ISC DHCPD as relay
  - The central server knows which subnet queries are coming from, and assigns addresses from the right pool
- As you grow, add another server and run as a failover pair

DNS

- DNS reliability is essential to your network
  - No DNS == No services
- Server location
  - On different subnets, off of different routers
  - Air conditioned, dual power supplies, etc.
- Separate duties
  - Authoritative and recursive on different machines

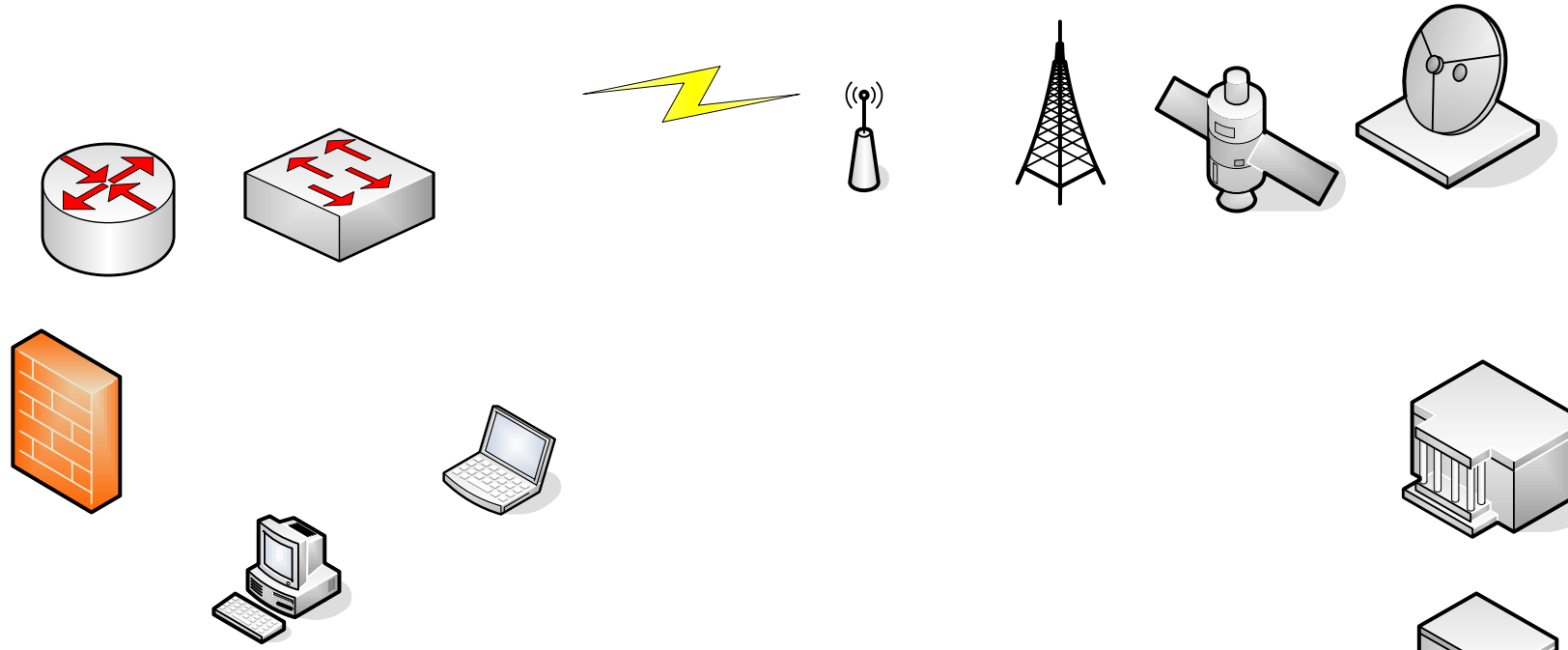
DNS Authoritative vs. Recursive

Server Function	Information	Target audience
Authoritative	Your domains	The Internet
Recursive	All other domains	Your users

Questions?

UNIVERSITY OF OREGON

Symbols to use for diagrams



UNIVERSITY OF OREGON