Campus Networking
Best Practices

UNIVERSITY OF OREGON

Week at a Glance

- Monday: Introduction and Cabling Systems
- Tuesday: Fiber Optic Termination Lab
- Wednesday: Layer 2 (in-building networks)
- Thursday: Layer 3 (campus core routing)
- Friday: Wireless LANs for campus

Daily Schedule

- 8:30am-10:30am Morning Session I
- 10:30am-11:00am Tea Break
- 11:00am-1:00pm Morning Session II
- 1:00pm-2:00pm Lunch
- 2:00pm-4:00pm Afternoon Session I
- 4:00pm-4:30pm Tea Break
- 4:30pm-6:00pm Afternoon Session II

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

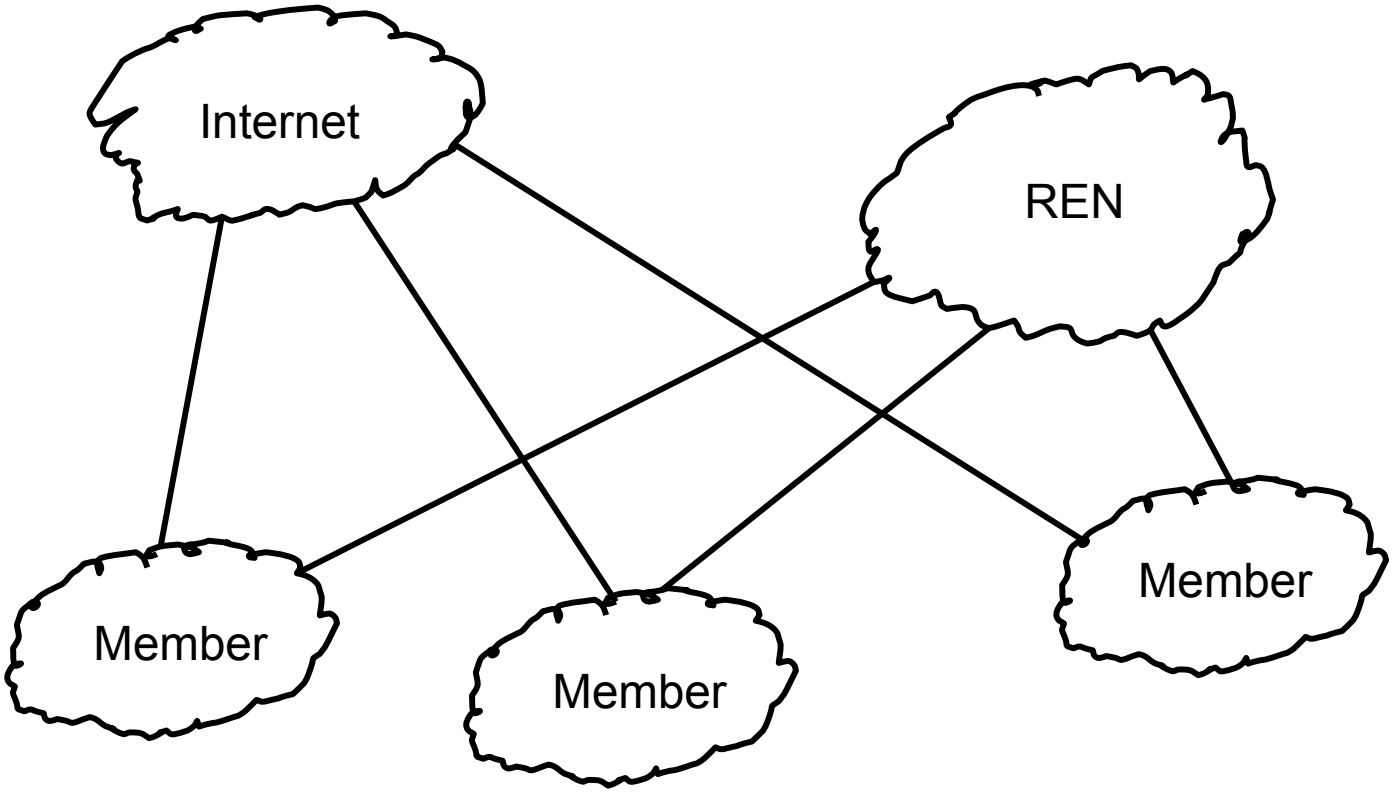
Why a REN?

- **Enable research or services that could not be accomplished otherwise**
- Cost Savings (buyers club)
- Vision of building alliances
- Successful RENs find that there are unanticipated benefits

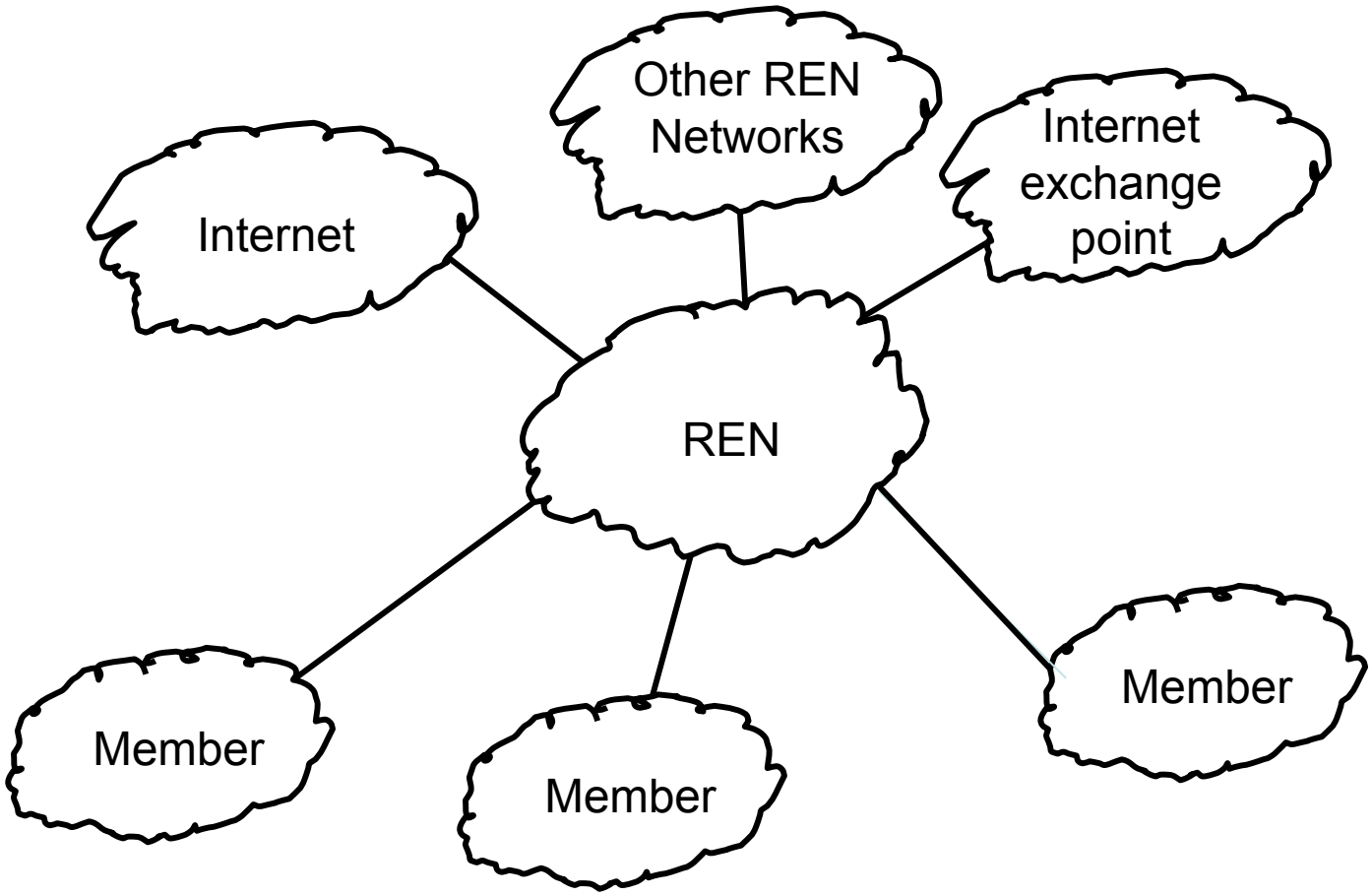
REN Services

- What services are provisioned? Various models:
  - REN provides all Internet connectivity
  - Peering network to exchange traffic between members
  - Advanced peering network that might
    - Develop or peer with a local commercial exchange
    - Provide international connections (GEANT, etc)
  - Other services (video conferencing)

REN as Peering Network



REN as Internet Service Provider



KENET

- KENET acts as your Primary Internet Service Provider
- KENET Carries traffic between customers
- KENET Carries traffic to Europe to connect to the Internet
- KENET Carries traffic to Europe to peer with other R&E Networks (GEANT, TENET, etc)

UNIVERSITY OF OREGON

Who Needs Public IP Space?

- **Every campus must have Public IP address space**
- KENET has public IP address space and will provide you with public IP space
- Large Universities can get provider independent IP space that would not be from KENET
- It will be by far the easiest to get your address space from KENT

Provider Independent IP Addresses

- What are provider independent IP addresses?
  - Public IP addresses that are not allocated to you by your Internet Service Provider.
- Can move between service providers without renumbering
- Space provided by KENET is not provider independent – if you move away from KENET, you must give back your addresses

NAT is a reality

- NAT is common technique to reduce number of public IP addresses required
- NAT makes some things hard.
  - NAT breaks things like SIP (standard-based VoIP), which you have to work around
  - NAT translation device needs to know about applications. Stifles innovation.
  - Makes it harder to track down viruses and hackers

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 uplinks, but moving to high speed external links, they start to fail.

Campus Network Personnel

- Every campus should have at least one person who does nothing but work on the network. Not email systems. Not course management systems. Just networks.
- Larger campuses will need more
- University of Oregon has 8 people just doing networking plus 3 doing security (26,000 network connections)
  - Started small 20 years ago with 2 people

UNIVERSITY OF OREGON

Why is This Stuff Important

- The 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
- Without a plan, how will you know where to make investments?

Campus Networking Design

UNIVERSITY OF OREGON

Campus Network Rules

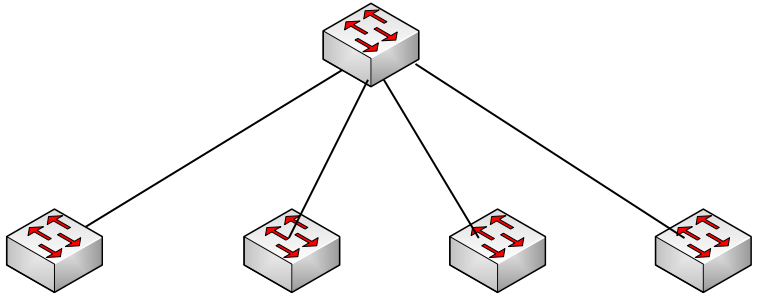
- Minimize number of network devices in any path
- Use standard solutions for common situations
- Build Separate Core and Edge Networks
- Provide services near the core
- Separate border routers from core
- Provide opportunities to firewall and shape network traffic

Core versus Edge

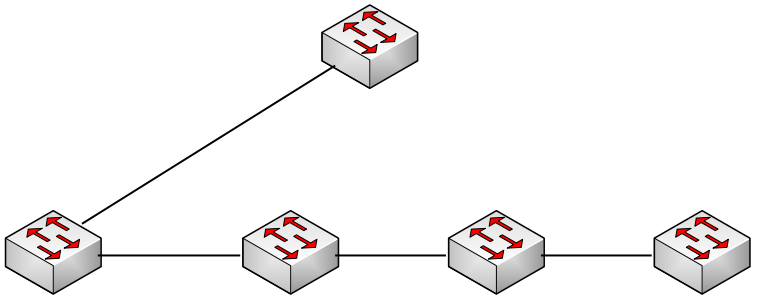
- Core network is the “core” of your network
  - Needs to have reliable power and air conditioning
  - May have multiple cores
  - Always route in the core
- Edge is toward the edges of your network
  - Provide service inside of individual buildings to individual computers
  - Always switch at the edge

Minimize Number of Network Devices in the Path

- Build star networks



- Not daisy chained networks



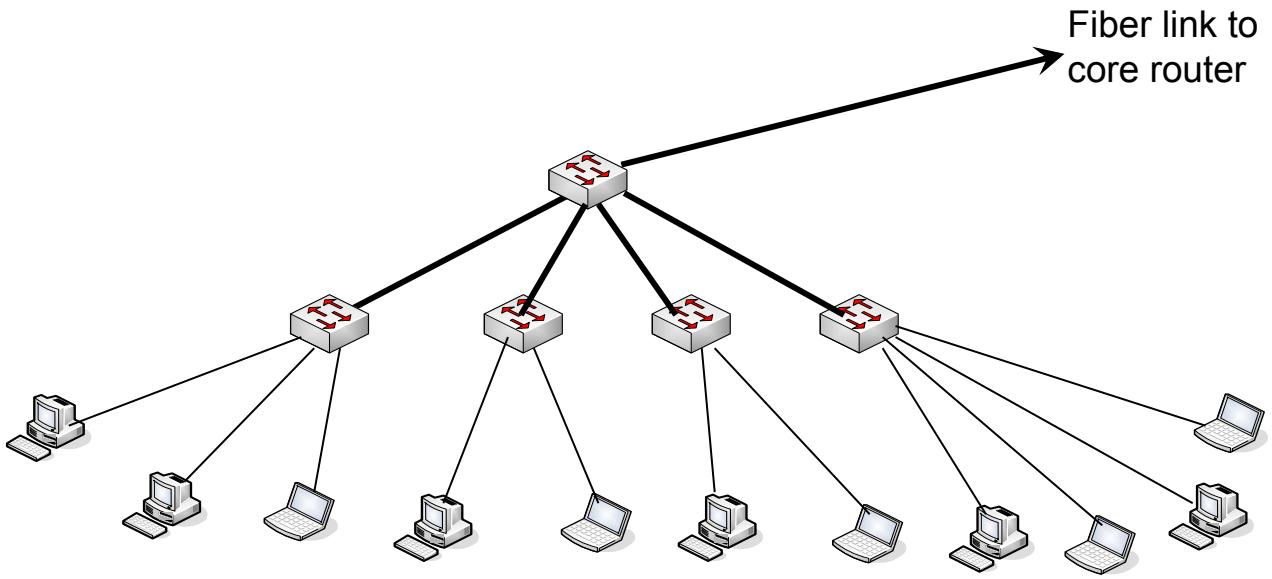
Edge Networks (Layer 2 LANs)

- 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!

UNIVERSITY OF OREGON

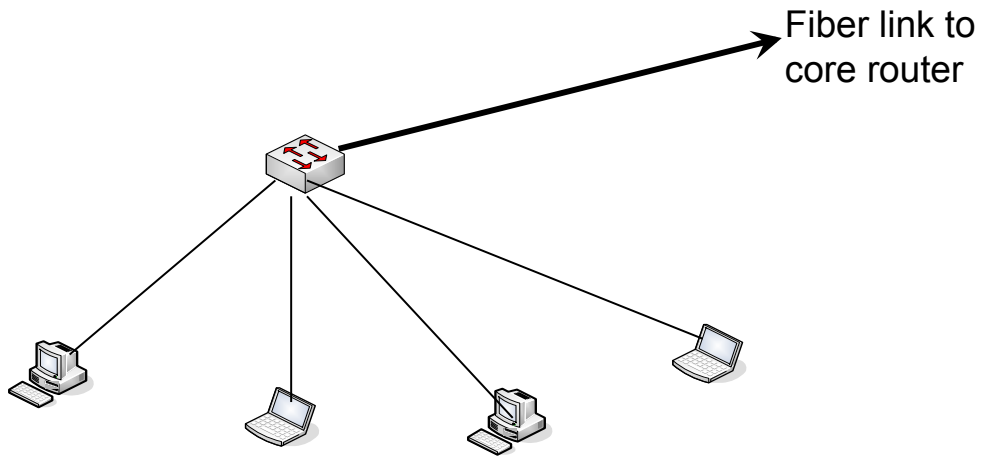
Edge Networks

- Make every network look like this:



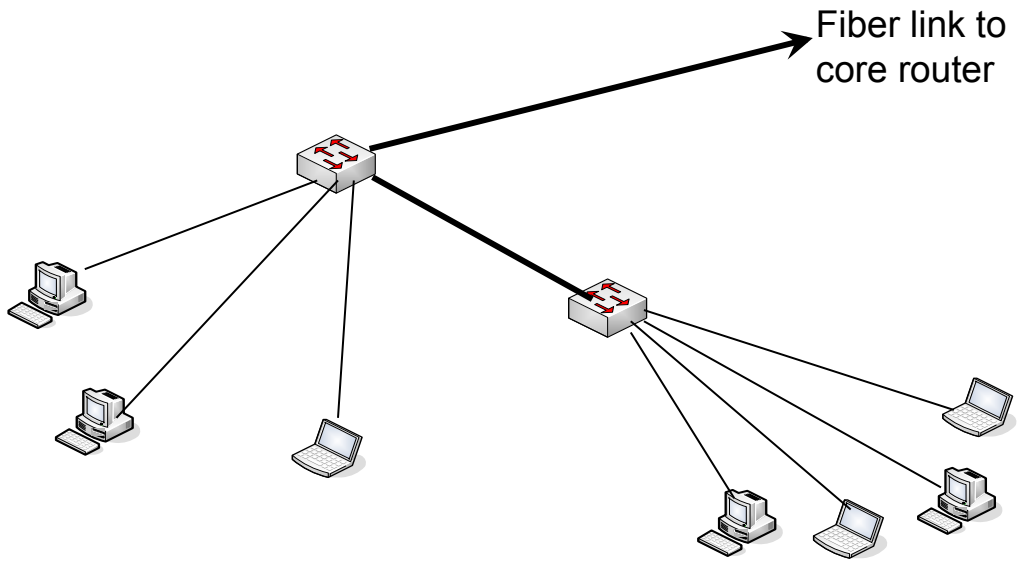
Edge Networks Continued

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



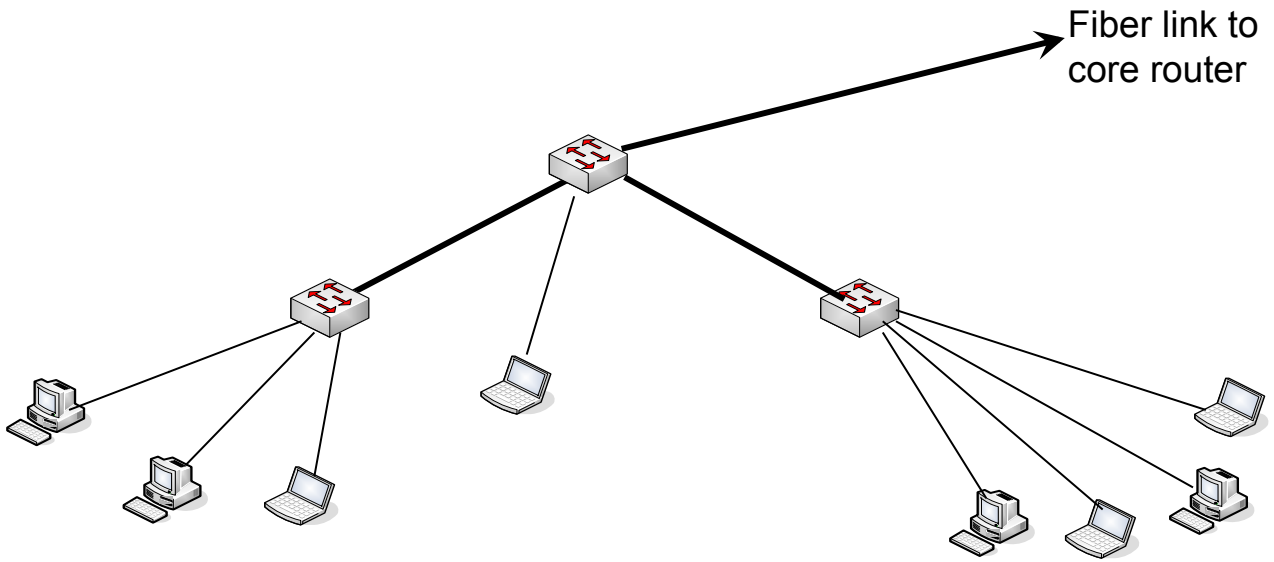
Edge Networks Continued

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



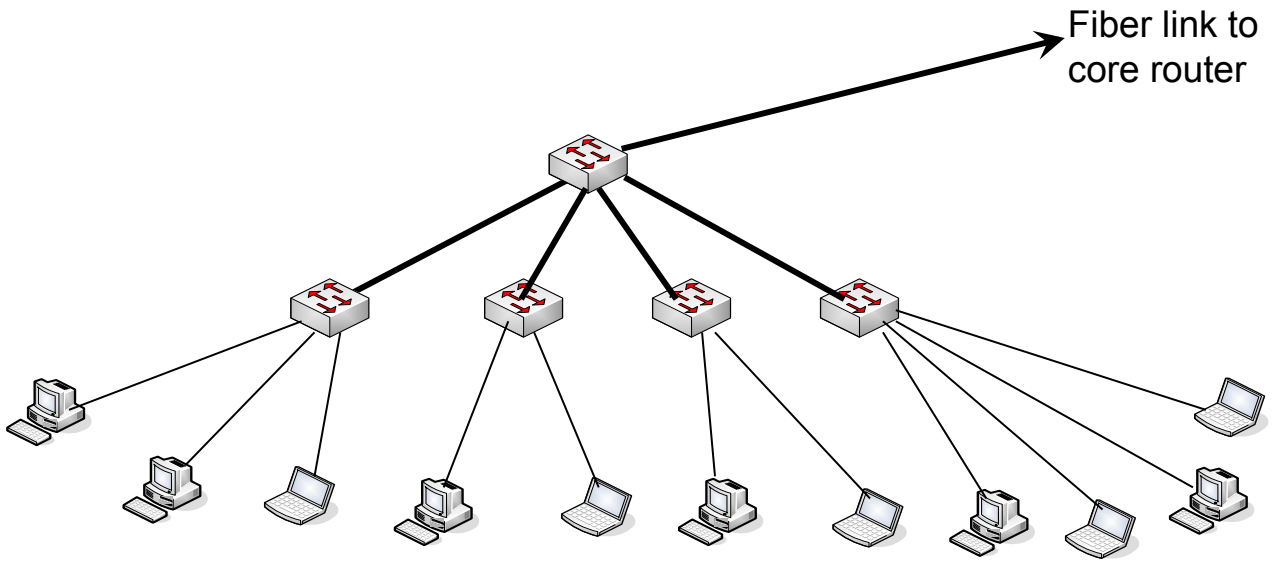
Edge Networks Continued

- And keep adding switches to get to the final configuration



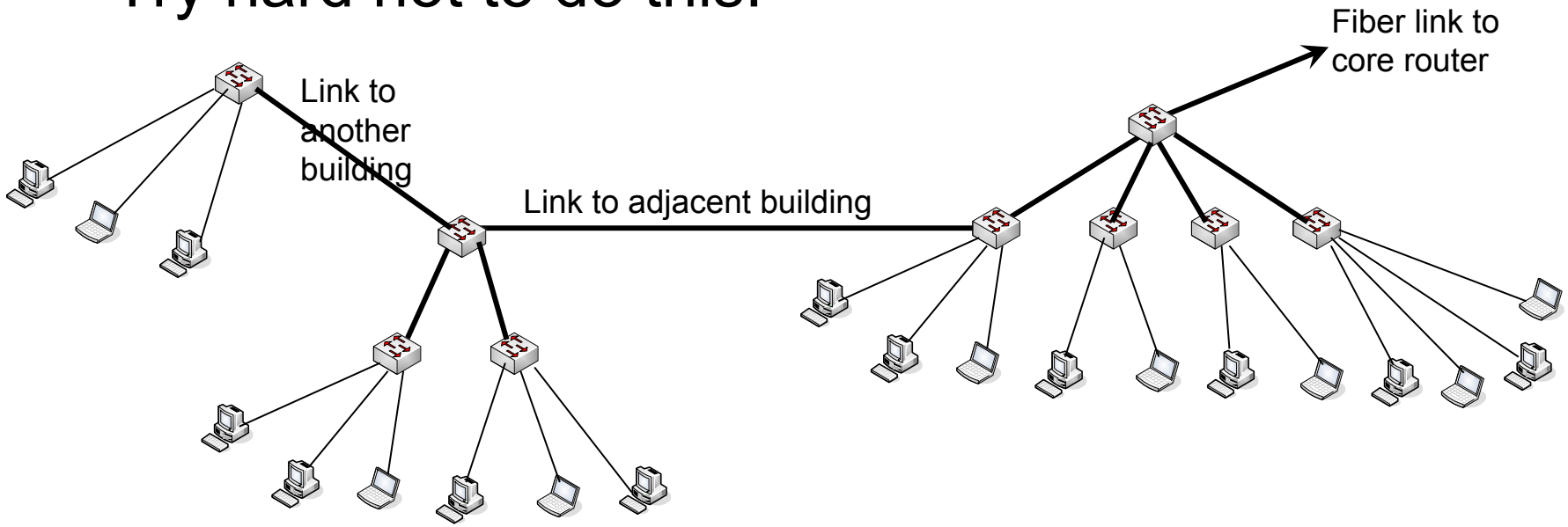
Edge Networks Continued

- And keep adding switches to get to the final configuration



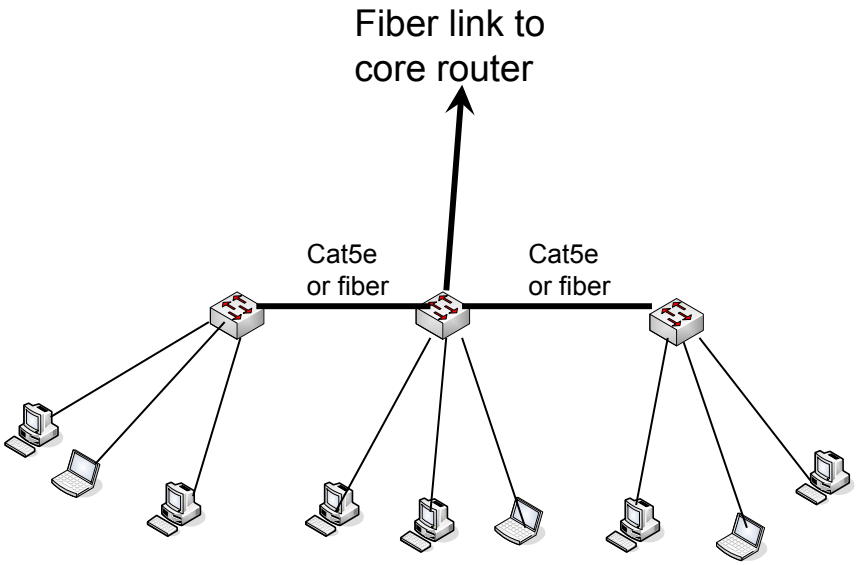
Edge Networks Continued

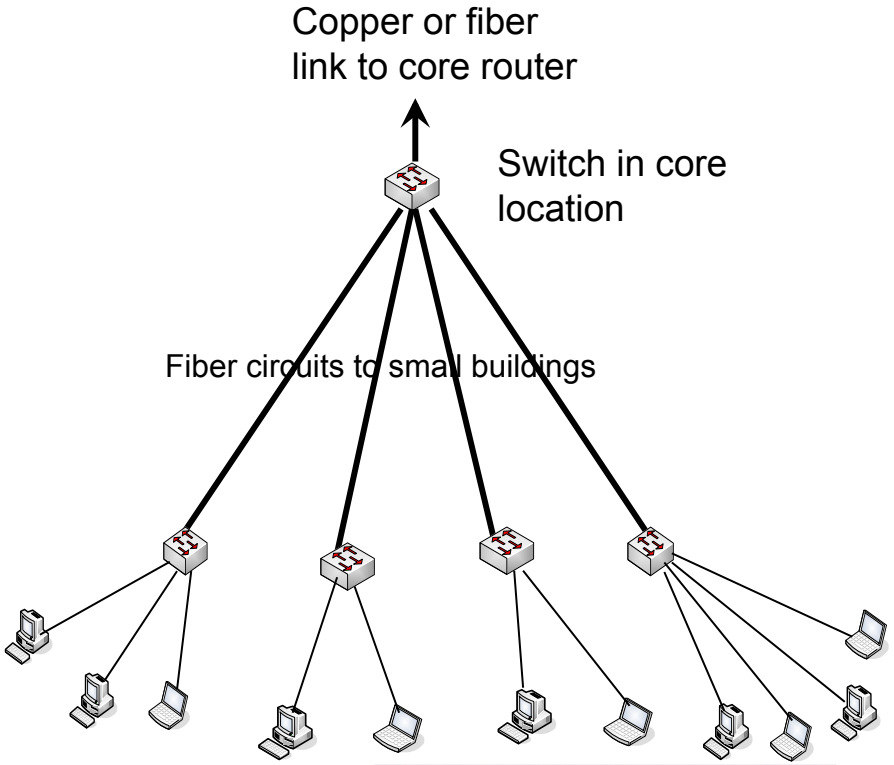
- Resist the urge to save money by breaking this model and daisy chaining networks or buildings together
- Try hard not to do this:



Edge Networks Continued

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





Selected Layer 2 Topics

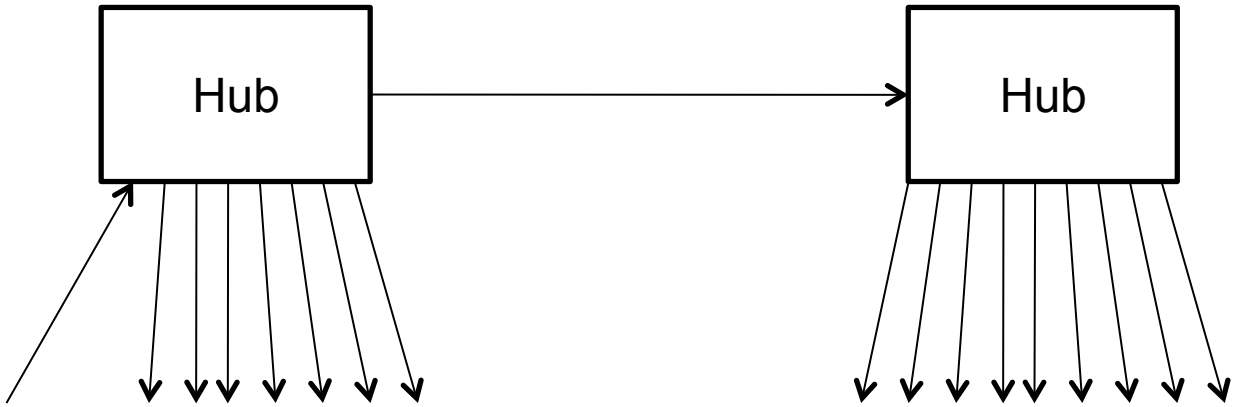
- Collision versus Broadcast Domain
- VLANs
- ARP – how it works
- DHCP - How it works
- Spanning Tree
- Link Aggregation
- Failure modes
  - 100 Mbs and Gigabit Duplex mismatch

Collision vs. Broadcast Domain

- Similar issues – affects performance of LAN
- Hubs (Repeaters)
  - Every packet goes to every port, irrespective of destination of packet
  - Every port is half duplex
  - Can only be one packet in transit – two transmitters = Collision

Collision vs. Broadcast Domain

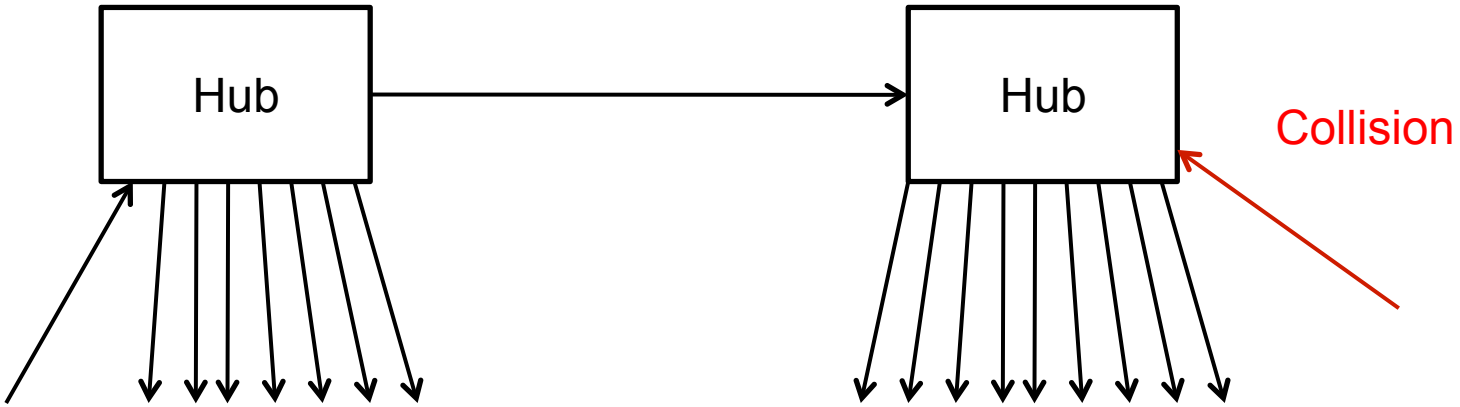
- Hubs/Repeaters



- Only One Packet at a time
- Every packet (even unicast) goes to every port

Collision vs. Broadcast Domain

- Hubs/Repeaters



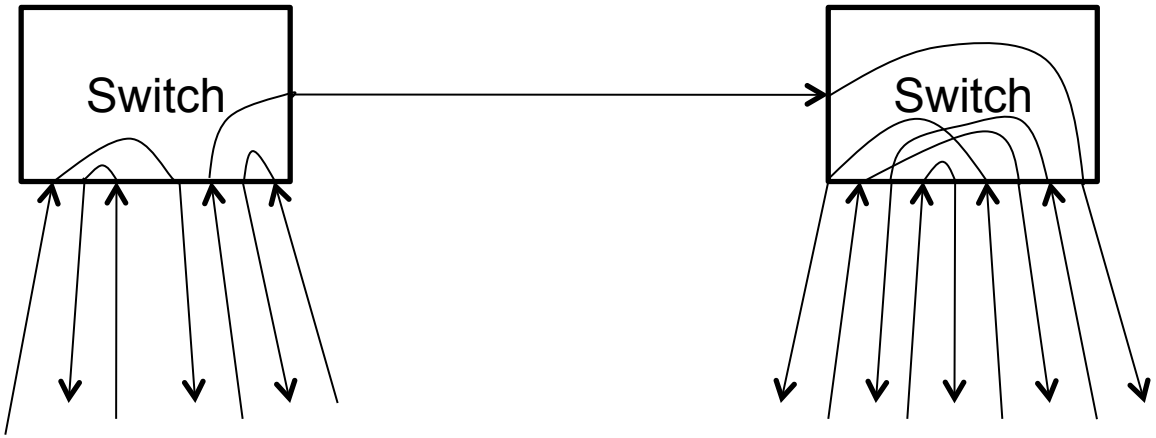
Two Transmitters = Collision

Collision vs. Broadcast Domain

- Switches
  - Switches learn where hosts are eavesdropping on traffic and building a forwarding table
  - Switches forward packets to correct port
  - Can only be many packets in transit
  - Broadcasts must go to all ports

Collision vs. Broadcast Domain

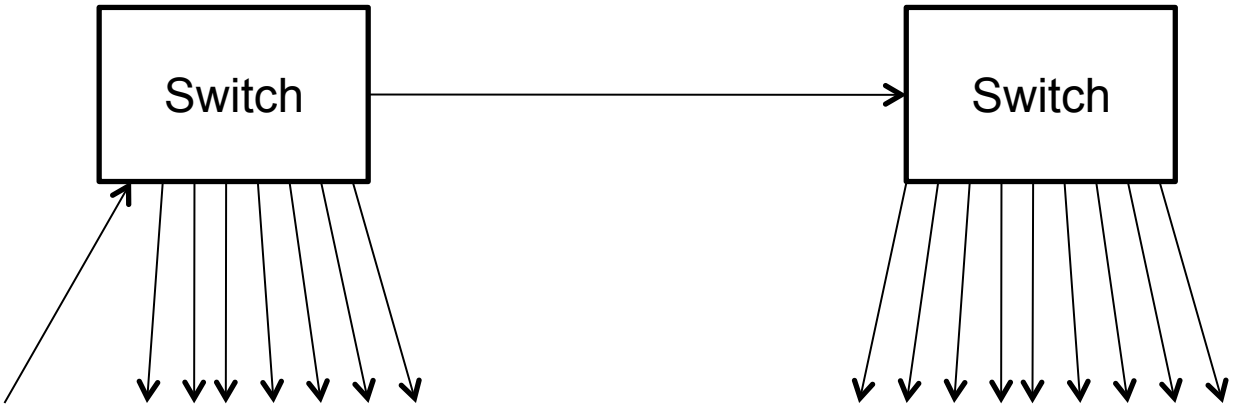
- Switches



- Many packets can be in flight – store and forward
- Unicast Packets go to intended destination

Collision vs. Broadcast Domain

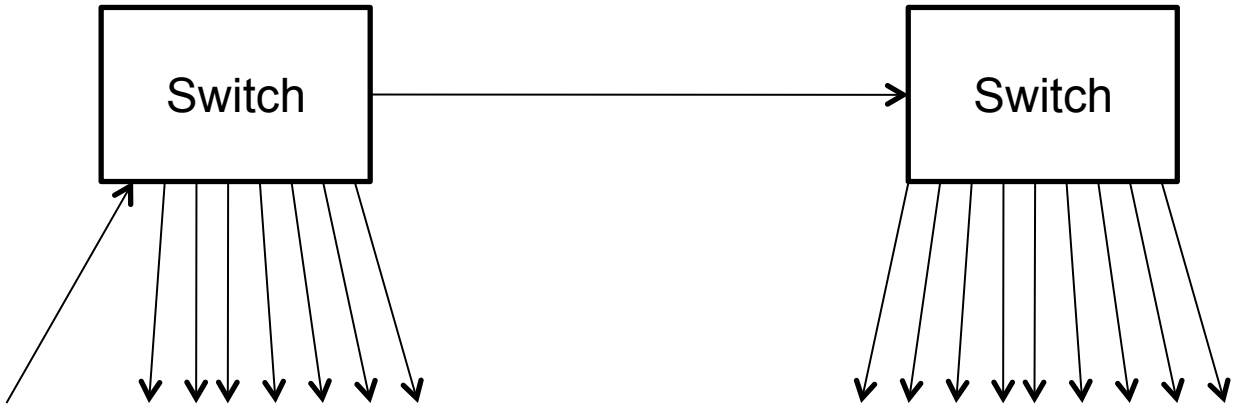
- Switches



- Broadcasts go to all ports (notice this looks like the hubs picture some slides ago)

Collision vs. Broadcast Domain

- Switches



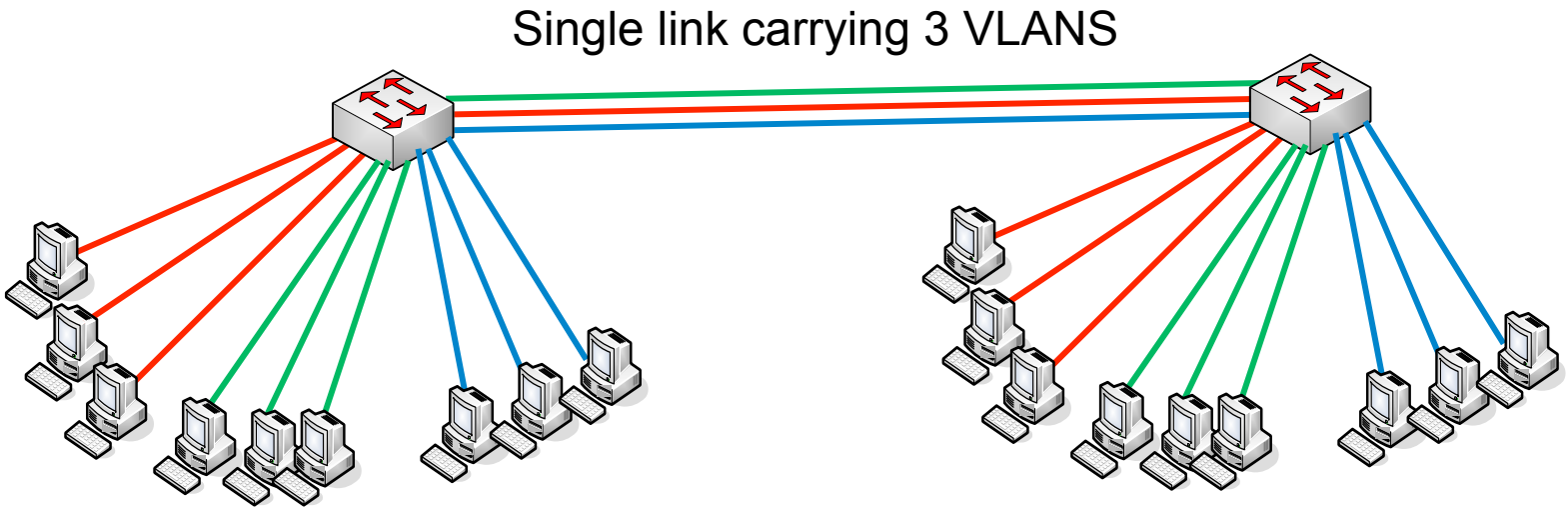
- Switches need to know about multicast

VLANs

- Virtual LANs – reduce scope of broadcast domain and separate traffic
- Tagging – identifying the VLAN associated with a packet. Ports are configured as Tagged or untagged.
- Trunking – Carrying traffic for multiple VLANs on a single link. Must use tagging.

VLANs

- Tagging on Trunks – must tag

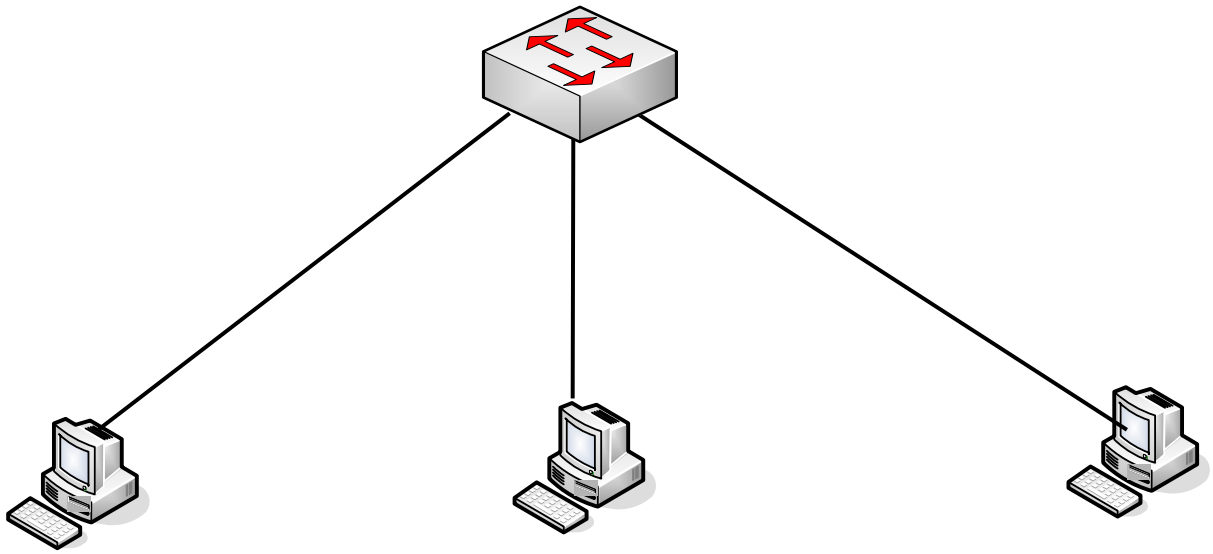


ARP

- Address Resolution Protocol
- Builds a mapping of IP address to Ethernet Address
- ARP Protocol
  - Broadcast ARP Request (who has this IP?)
  - Owner of IP address in ARP Request issues ARP reply
- Pathology: anyone can issue an ARP reply at any time

UNIVERSITY OF OREGON

ARP



10.0.0.1
00:00:11:00:00:aa

10.0.0.2
00:00:11:00:00:bb

10.0.0.3
00:00:11:00:00:cc

DHCP

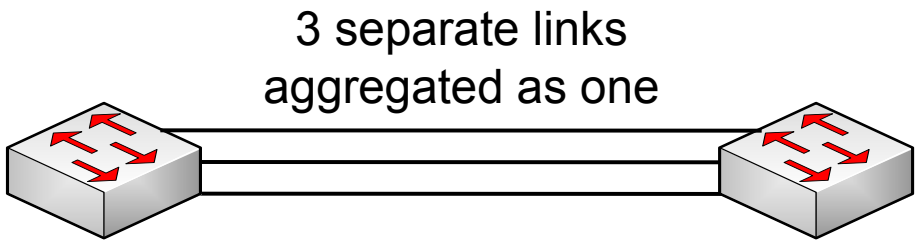
- Dynamic Host Configuration Protocol
- Used to assign IP address and provide basic IP configuration to a host.
- Simple protocol
  - Client broadcasts a DHCP DISCOVER
  - Server(s) unicast back a DHCP OFFER
  - Client selects an offer and sends a REQUEST
  - Server sends back a DHCP ACK to client
- Managed switches can block rogue DHCP

Spanning Tree

- Eliminates loops in Layer 2 networks
- Several flavors
  - Original Spanning Tree 802.1D
  - Rapid Spanning Tree (RSTP) 802.1w
  - Multiple Spanning Tree (MSTP) 802.1s and 802.1Q-2003
- Modern managed switches can do all of the above
- Lots of discussion about this Wednesday

Link Aggregation

- Bonds multiple channels together to provide more bandwidth
- Issues:
  - Compatibility
  - How traffic is scheduled



Failure Modes

- Loops in your network
- Rogue DHCP servers
- Duplex mis-match
  - 100Mbs – late collisions and CRC
  - 1000Mbs – can't establish link
- Need managed switches to correct these

Thanks

Questions?

UNIVERSITY OF OREGON

Symbols to use for diagrams