Basic Requirements of Campus Network

11 March 2019

Campus Network Best Practices – IT Center, University of Peradeniya

Dhammika Lalantha /
LEARN

Requirements Analysis

- The act of gathering and deriving requirements in order to understand system and network behaviors
- Need for requirement analysis:
  - May guide to the development of the network architecture and design you will need
  - Can be sure that everything from network performance, security, management requirements will be addressed
  - May result in a durable, expandable and upgradable network
  - Will make understand of issues of current network setup

Different types of requirements

- User requirements
  - Performance
    - Bandwidth
    - Throughput
    - Latency
    - Jitter
    - Error rate
  - Reliability and Resiliency
    - Service outages
    - Highly reliable and available network that can survive during any network component failure without any operator intervention

Different types of requirements

- Security
  - Guarantee of confidentiality, integrity and authenticity
  - Traffic isolation between the traffic of guests and internal staff.
- Affordability
  - Financial feasibility
- Functionality
  - Applications users need

Different types of requirements

- Application requirements
  - Mission-critical
    - Online business
  - Real-time and interactive
    - Multimedia applications
    - Should have predictable, guaranteed and high-performance delay requirements
  - Rate-critical
    - Network capacity
  - Meet industry regulations and corporate security policies

Different types of requirements

- Network requirements
  - Security
  - High availability
  - Scalability
  - Traffic isolation
    - Network segmentation
  - Quality of service

Thank You

Dhammika Lalantha/LEARN

Email: lalantha@learn.ac.lk

Network Fundamentals

11 March 2019

Campus Network Best Practices – IT Center, University of Peradeniya

Dhammika Lalantha /
LEARN

What is Your Campus network ?

- How large your network ?
  - Number of Network devices
  - Number of Client devices
- Is it a Flat network or Routed Network?
- Flat Network
  - Comprised of few switches and hubs
  - Shares a single broadcast domain
  - Poor security, Not scalable, Reduced speed
  - Not segmented, shares a single IP subnet

What is Your Campus network ?

- Routed Network
  - Comprised of Routers, Layer 3 switches and switches
  - Several broadcast domains
  - Better security, scalable network, better speed
  - Segmented, contains many many IP subnets

Network Segmentation

- Dividing a computer network into subnetworks.
- Why segment your network?
  - Stronger data security by separating your servers with sensitive data
  - Slow down attackers who breached your network
  - Reduced damage from successful attacks
  - Easier implementation of organization security policies
    - Applying firewall rules
  - Reduce impact from broadcasting including loops which could cause entire network to stop

Network Segmentation

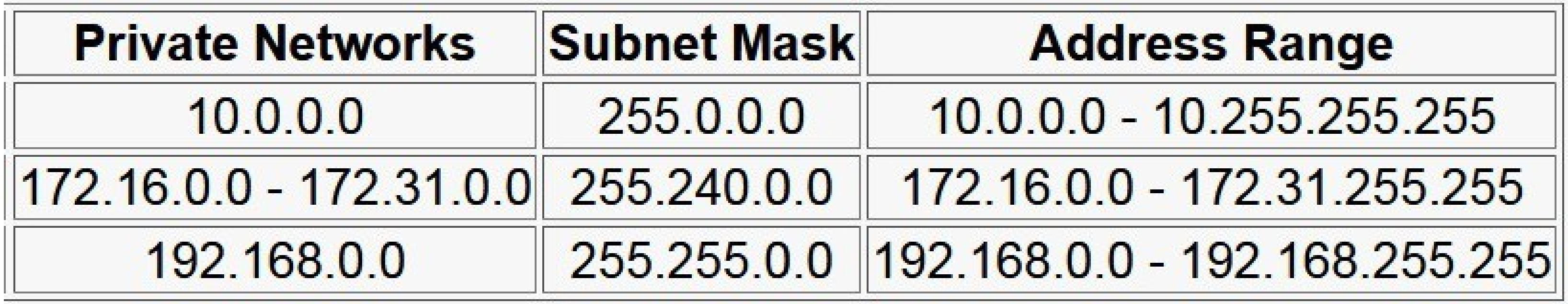
- Two basic methods
  - Subnetting (Layer 3)
  - VLANs (Layer 2)

Subnetting

- Partitioning a single physical network into several logical sub-networks.
- How to begin subnetting your network?
- A simple procedure :
  - Decide the number of client devices that need an IP address
  - Decide the number of subnets your network should have
  - Determine the number of host/client devices per each subnet
  - Choose a suitable Private IP block

Private IP addresses

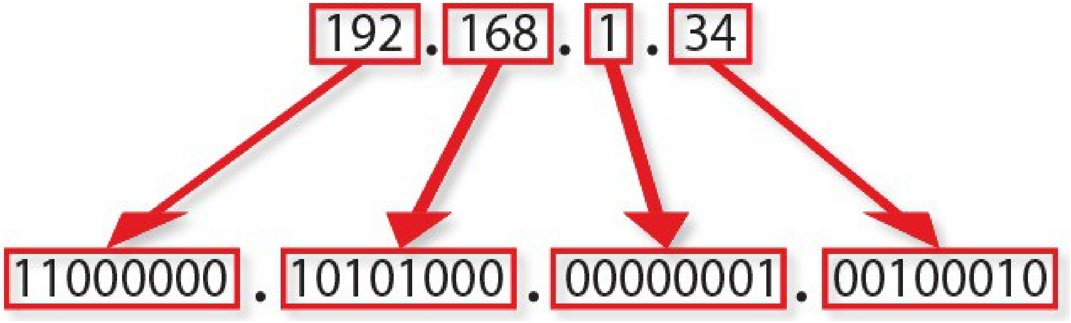
- Reserved by Internet Assigned Numbers Authority (IANA) for use within private networks



Private Networks	Subnet Mask	Address Range
10.0.0.0	255.0.0.0	10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.0.0	255.240.0.0	172.16.0.0 - 172.31.255.255
192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

IP addresses and Subnets

- Ex: IP address 192.168.1.34/24
- Binary representation

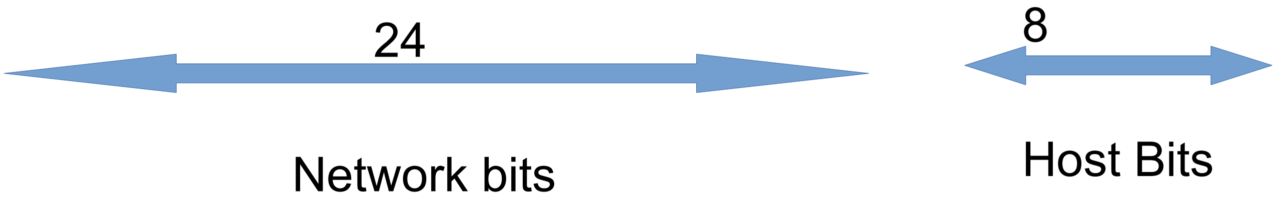


192 . 168 . 1 . 34

11000000 . 10101000 . 00000001 . 00100010

- Network and Host bits

11000000.10101000.00000001.00100010



24

8

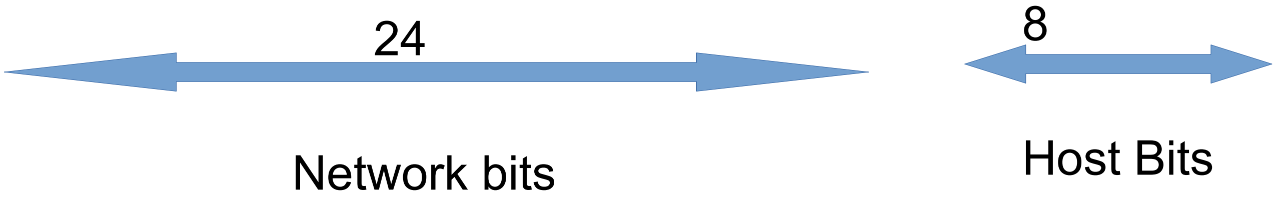
Network bits

Host Bits

IP addresses and Subnets

- Network address : 192.168.1.0

11000000.10101000.00000001.00000000



24

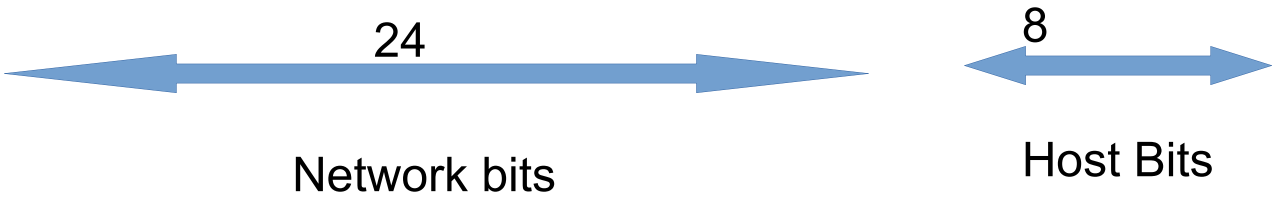
8

Network bits

Host Bits

- Broadcast address : 192.168.1.255

11000000.10101000.00000001.11111111



24

8

Network bits

Host Bits

IP addresses and Subnets

- Usable addresses within 192.168.1.34/24
    - $2^8 - 2 = 254$
- First valid host : 192.168.1.1
- Last valid host : 192.168.1.254
- Subnet mask : 255.255.255.0

Subnetting Example

- Given Network : 192.168.1.0/24
- Subnet mask of required subnets : 255.255.255.240 (/28)
  - Subnets? 2^4= 16
  - Usable Hosts? 2^4 – 2 = 14.
  - Broadcast address for each subnet?
  - Valid hosts?

Variable Length Subnet Mask (VLSM)

- Divide an IP address space into a hierarchy of subnets of different sizes without wasting the ip address space.
- Example network:
  - Administration staff – 12
  - Accounting staff – 5
  - Library staff – 6
  - Non-Academic staff - 35
  - Academic staff – 20
  - Students – 110
- How to design a network for above using VLSM if given network 192.168.100.0/24?

Variable Length Subnet Mask (VLSM)

- How to subnet your network with VLSM ?
- Follow the below simple procedure to subnet your network with the given requirements.
  - Sort the requirements of hosts per subnet in descending order.
  - Allocate the highest range of IPs to the highest requirement. Choose a suitable subnet mask to fill the requirement.
  - Next choose the next highest requirement and assign a subnet with with suitable subnet mask from the remaining network.
  - Do this until the all requirements are given a subnet.

Variable Length Subnet Mask (VLSM)

Answer:

User group	# of Hosts	Subnet
Students	110	192.168.100.0/25
Non-acadmeic	35	192.168.100.128/26
Academic	20	192.168.100.192/27
Administrative	12	192.168.100.224/28
Library	6	192.168.100.240/29
Accounting	5	192.168.100.248/29

Classless Inter Domain Routing (CIDR)

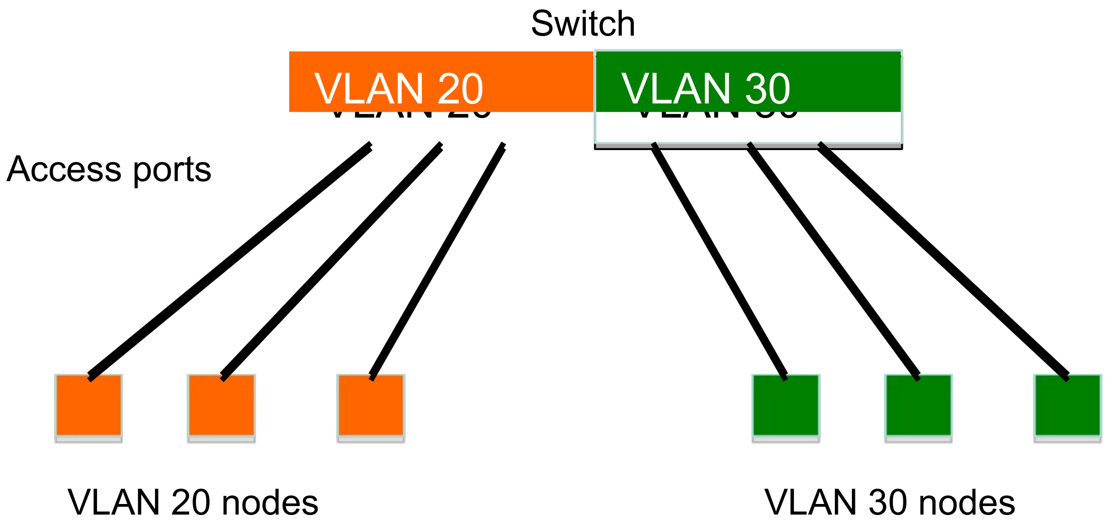
- Is a method of allocating IP addresses and IP routing
- Is a flexible way of allocating IP address in contrast to old classful IP addressing
- Efficiently use the available IP address space.
- Reduce the routing table entries
- Based on the concept of VLSM
- CIDR Notation
  - A.B.C.D/N
  - N – Network Prefix/IP prefix
  - Ex1 : 192.248.4.28/24
  - Ex2 : 192.168.3.23/27

Segmentation with VLANs

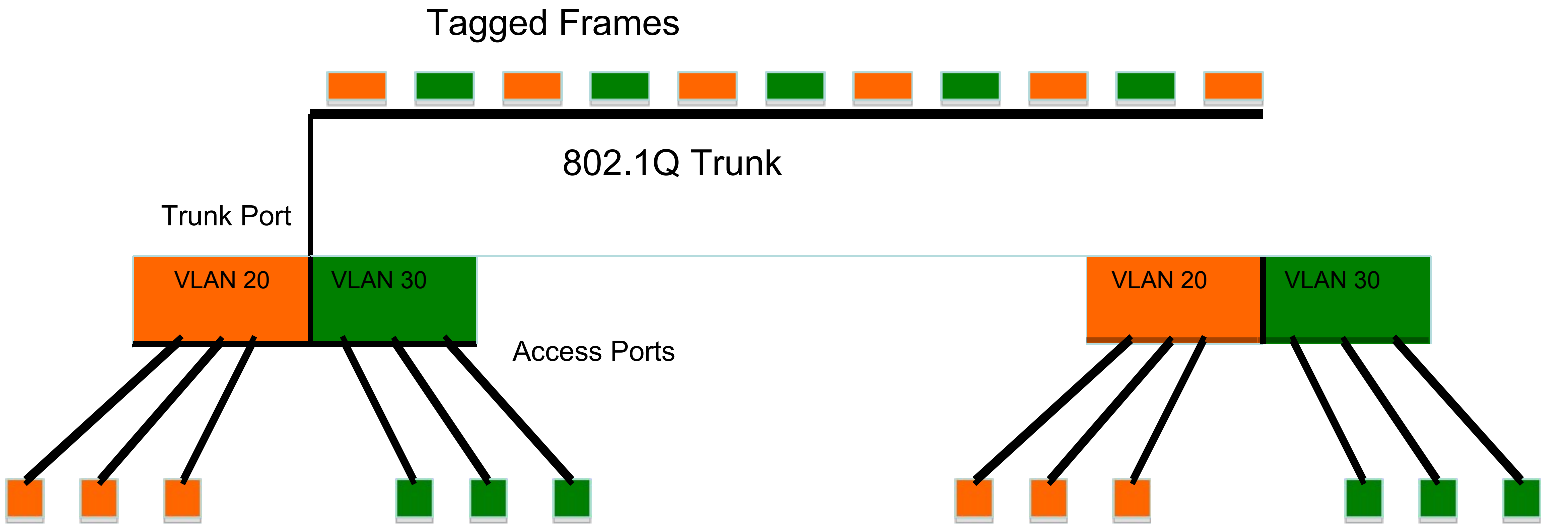
- What is a VLAN?
  - Any broadcast domain in a computer network partitioned/created at the data link layer (OSI layer 2)
  - It has same attributes as a physical LAN.
  - Allow to split switches into separate virtual switches
  - Inter-VLAN communication should happen through a layer 3 device (router, L3 switch)

Local VLANs

- Two or more VLANs within a single switch



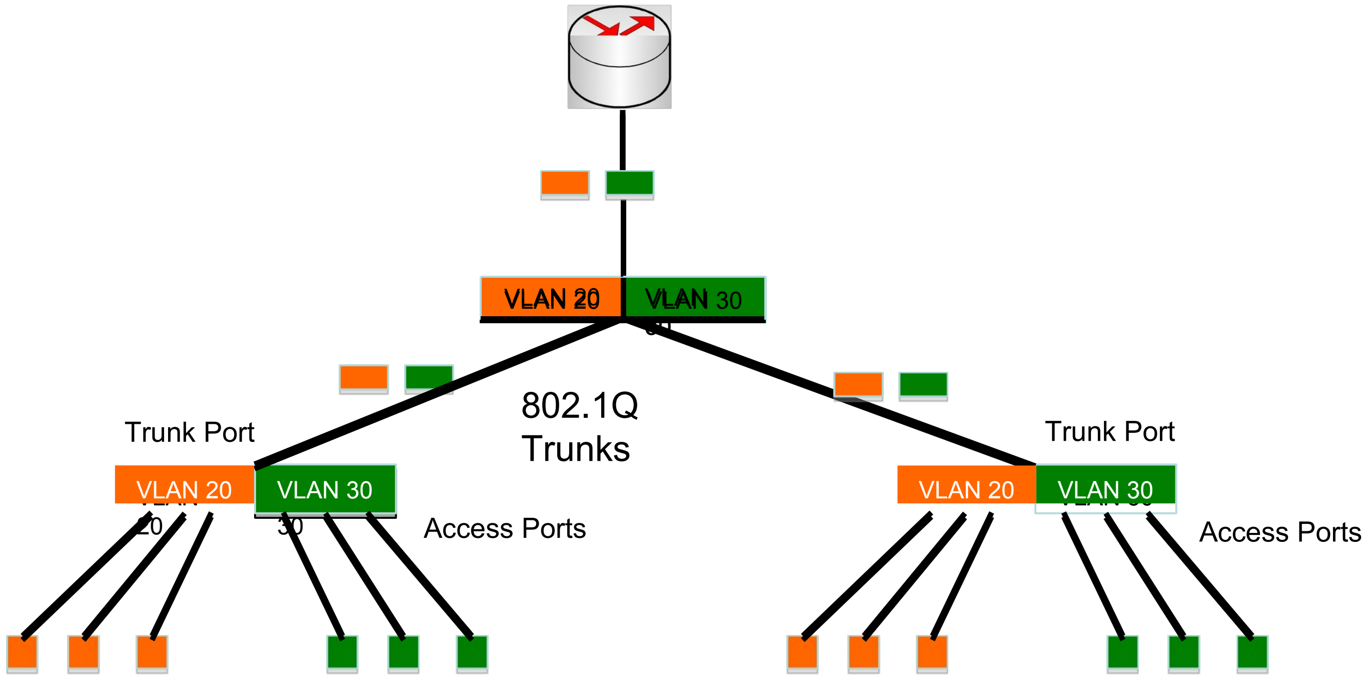
VLAN across switches



This is called “VLAN Trunking”

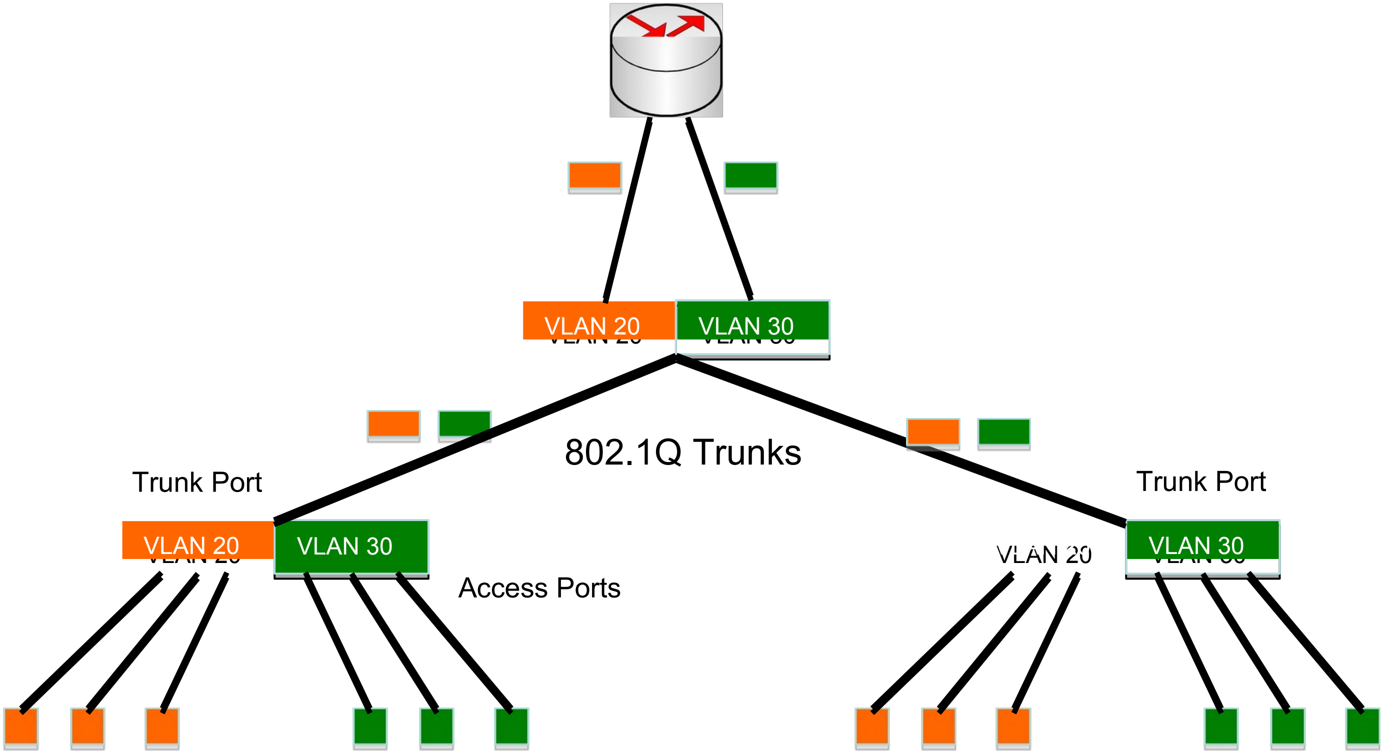
Routing Inter-VLAN traffic

- Single interface on the router used as a trunk



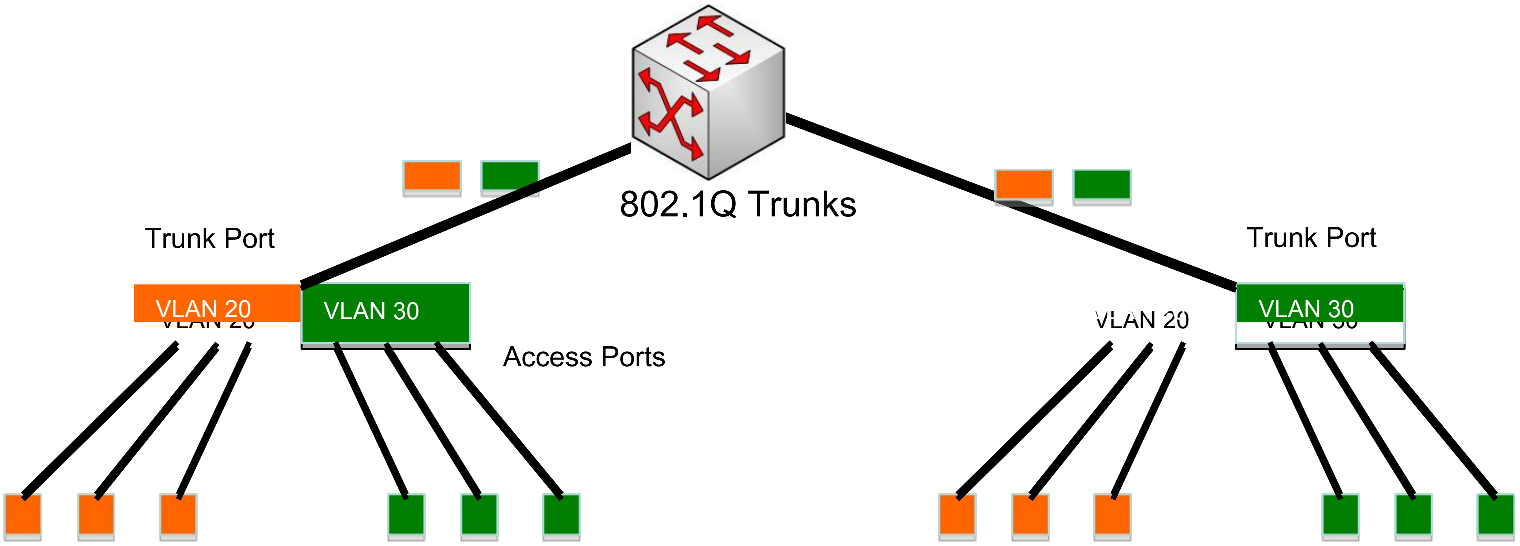
Routing Inter-VLAN traffic

Separate interfaces for each VLAN



Routing Inter-VLAN traffic

Can use a 802.1Q compliant Layer-3 switch to do switching as well routing



Benefits of Segmentation with VLANs

- Why use VLANs over Subnetting for network segmentation
  - Logical grouping of hosts that are physically dispersed on network
  - Reduce the need to have routers deployed on network
  - Cost effective since Routers are costlier than switches
  - Flexibility of expanding a network

Thank You

Dhammika Lalantha/LEARN

Email: lalantha@learn.ac.lk

Basic Campus Design Principles

11 March 2019

Campus Network Best Practices – IT Center, University of Peradeniya

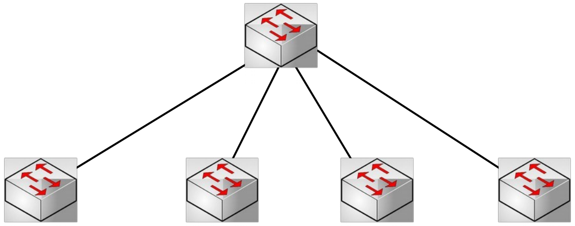
Dhammika Lalantha /
LEARN

Campus Network rules

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

Choosing Network Topology

A good topology to begin with is Hub and Spoke (sometimes called Star)



Advantages of Hub and Spoke topology

- Low startup cost
- Easier to expand the network with disruption to the network
- Easy to troubleshoot and isolate network problems
- It has a faster performance

Hub and Spoke Design

We will use this design pattern in two places in our network

1. Between Buildings(may be a Faculties or Department).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 between Buildings

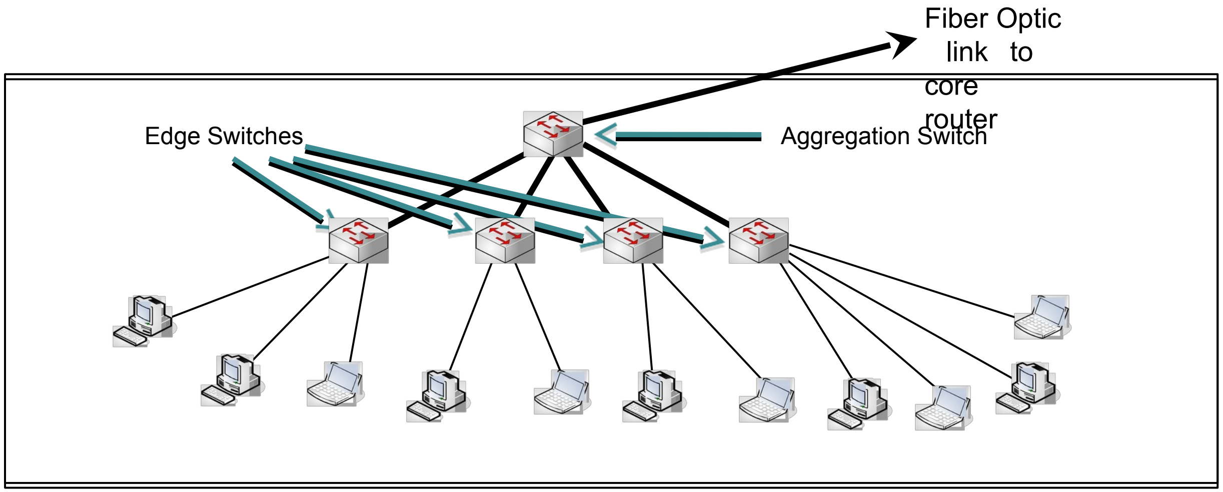
- The hub at the campus level (core network) is often called the core is a Layer 3 device
- Best practices are to route at the core
  - This segments the network into independent subnets
  - Limits broadcasts

Hub and Spoke Networks Inside of 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
  - i.e. Do not go beyond 24 subnet mask length for user subnets
- 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:

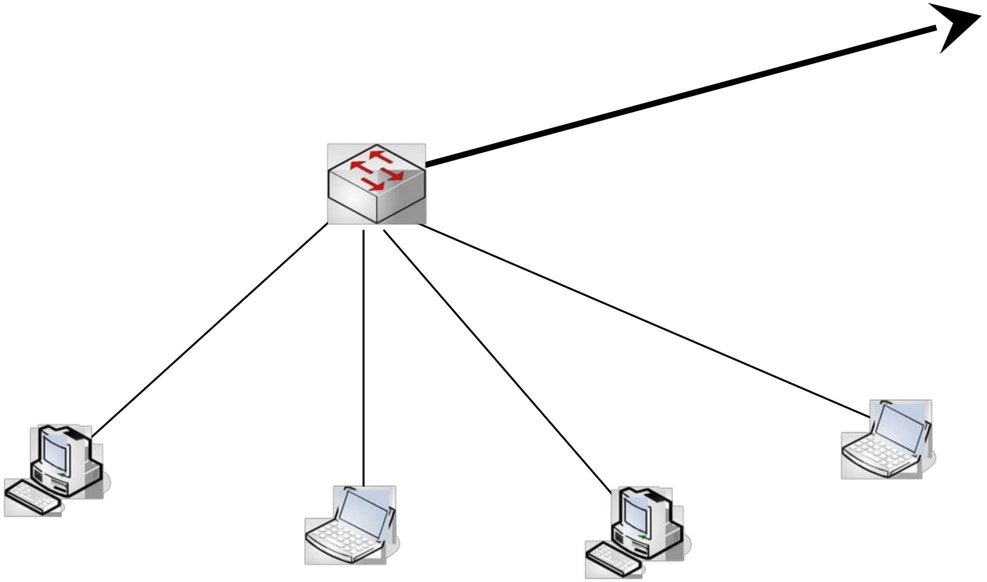


One Building

Edge network continued

Build Edge network incrementally as you have demand and money

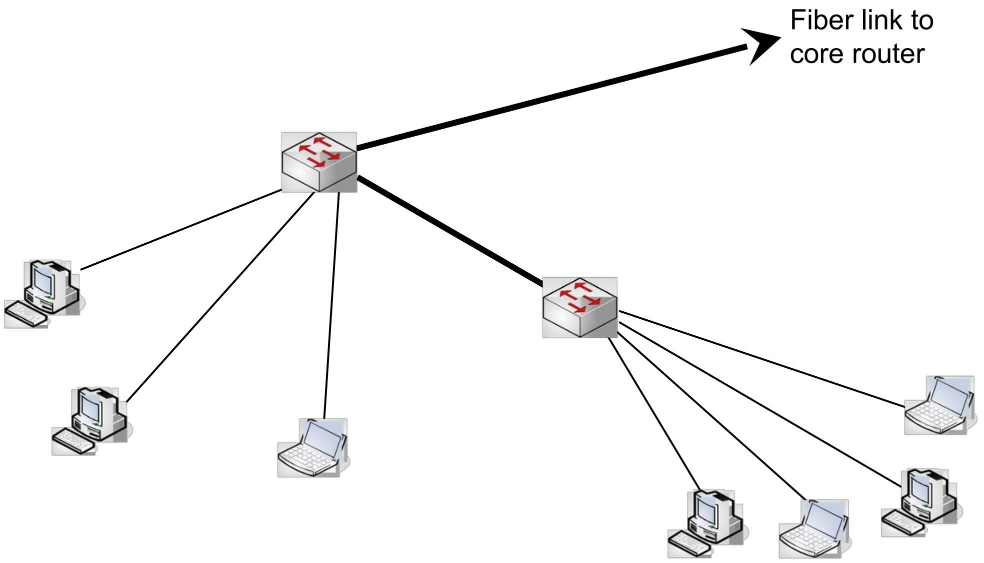
Start Small:



Fiber link to core router

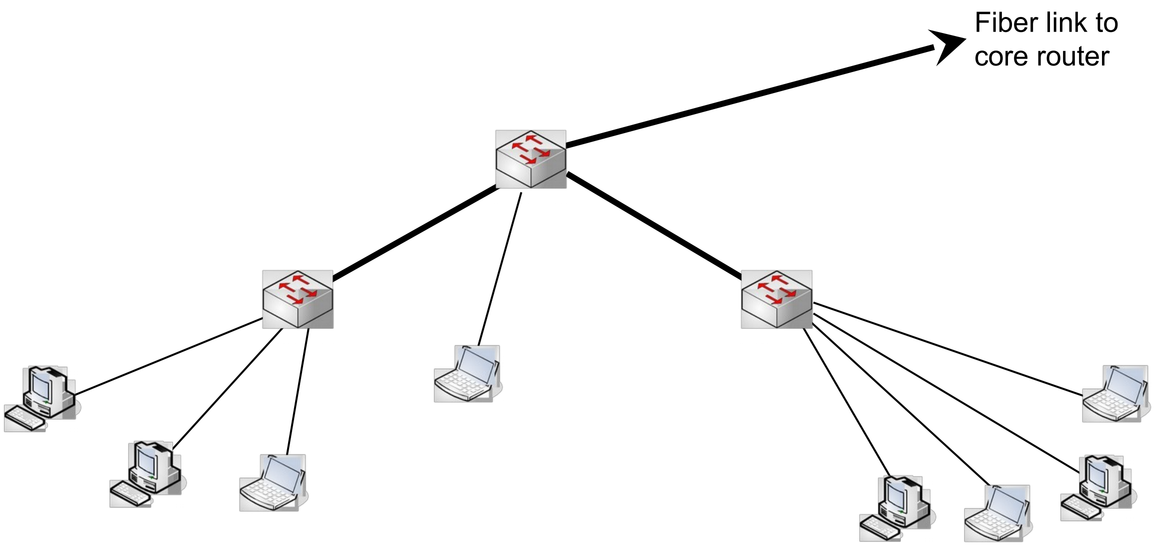
Edge network continued

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



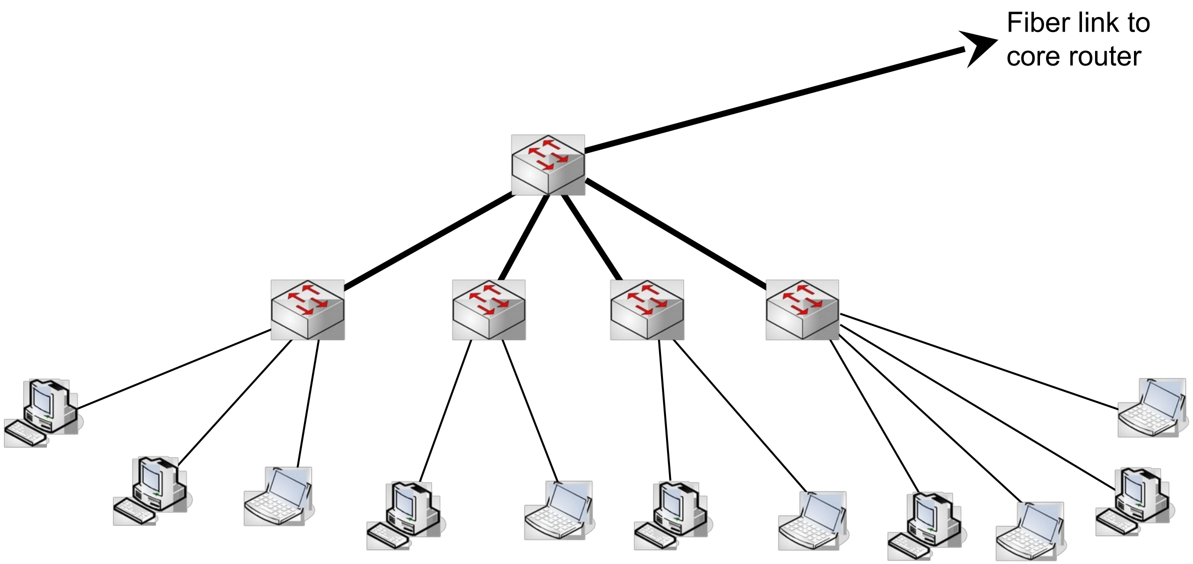
Edge Networks Continued

And keep adding network racks and switches



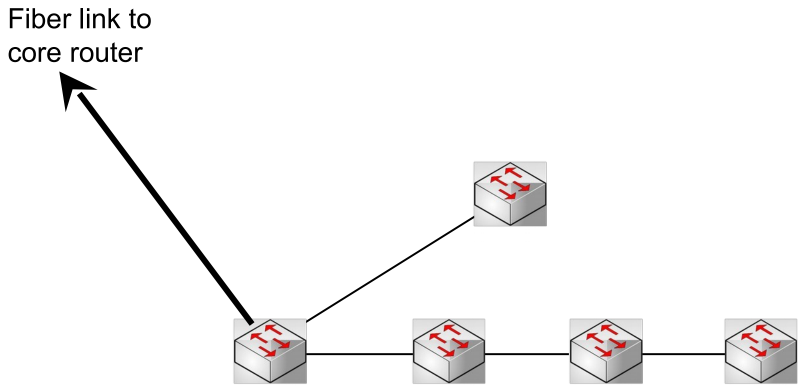
Edge Networks Continued

Until you get to the final configuration



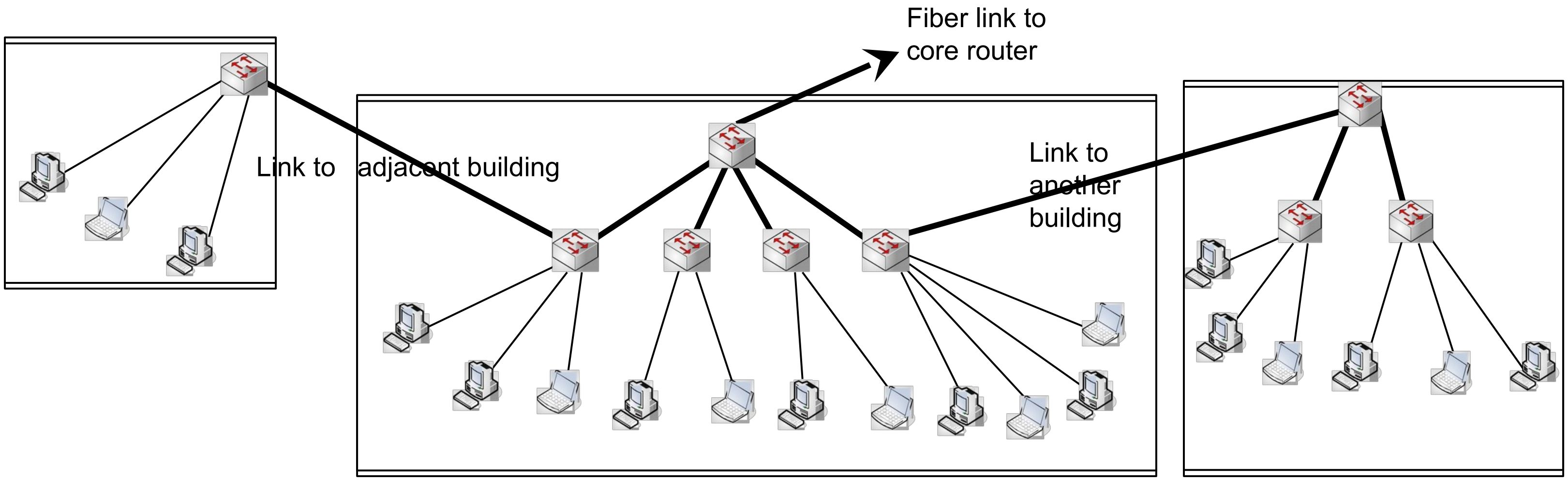
Edge Networks Continued

Avoid daisy chained (sometimes called cascaded) networks



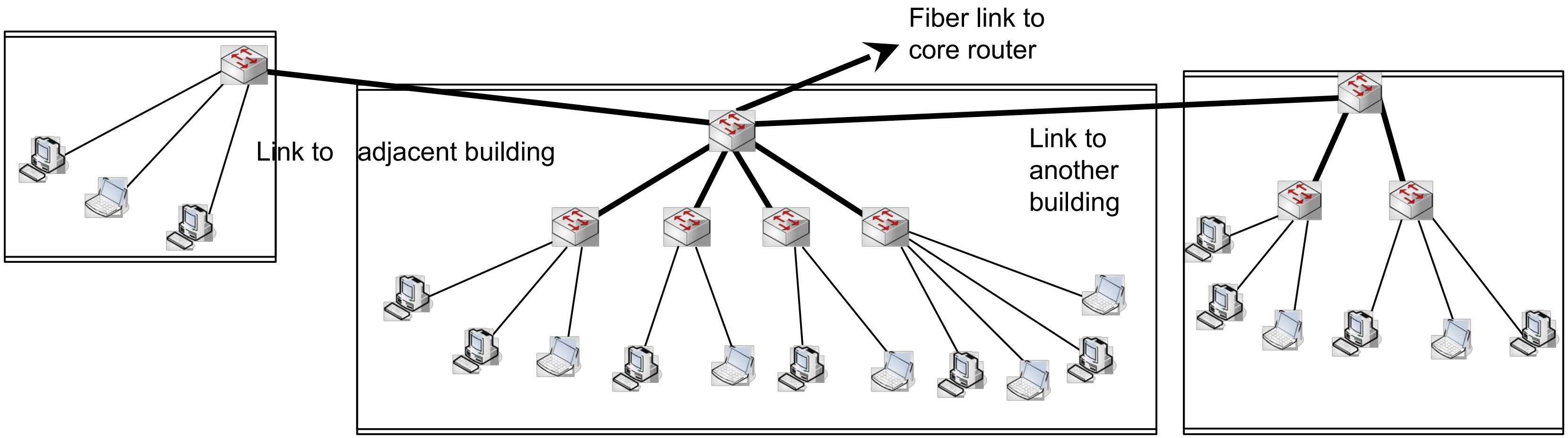
Edge Networks Continued

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

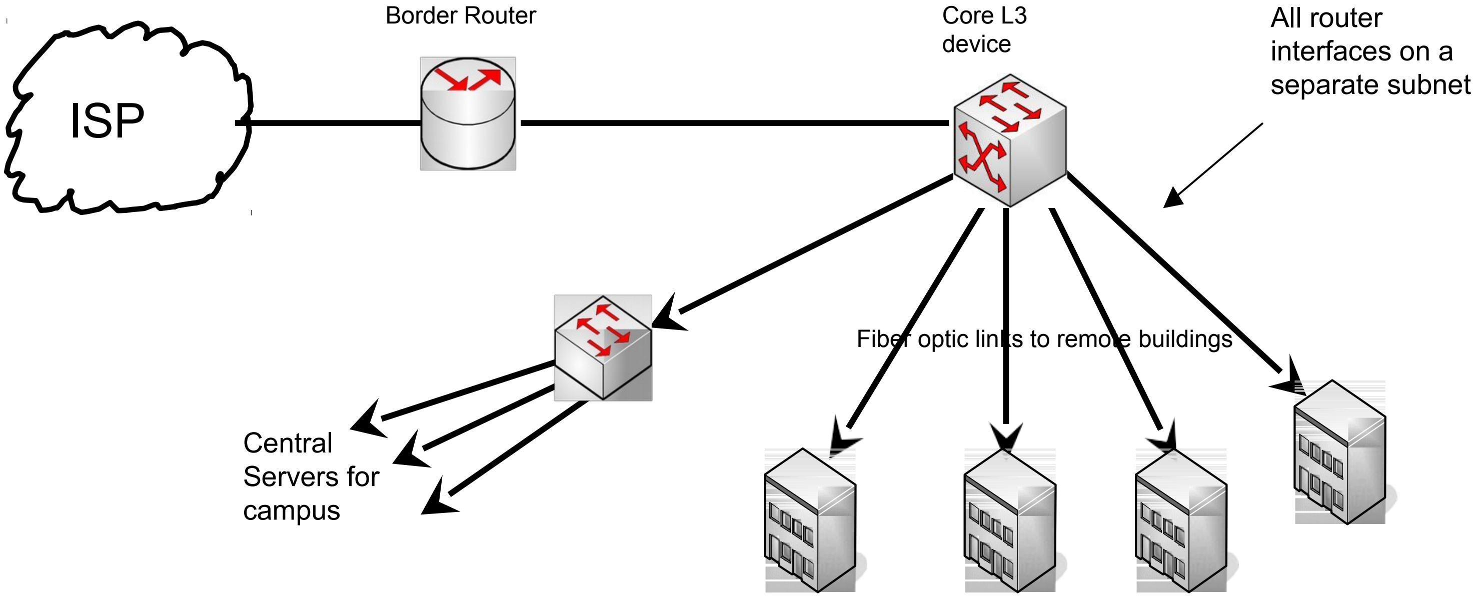


Segmenting Your Network

- 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

Core Network

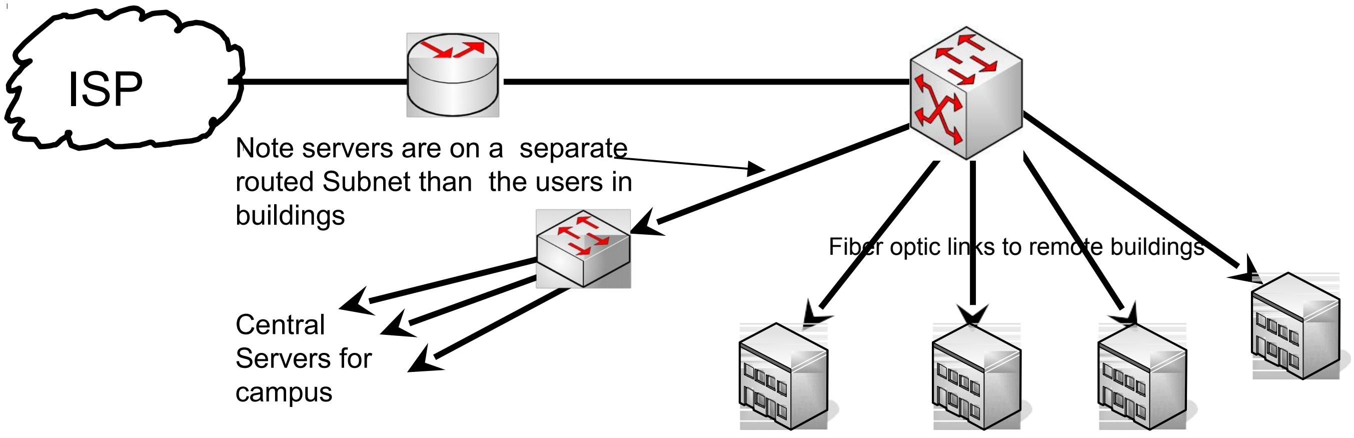
- At the core of your network should be routers – you must route, not switch. Routers give isolation between subnets
- A simple core:


Border Router
Core L3 device
All router interfaces on a separate subnet
ISP
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

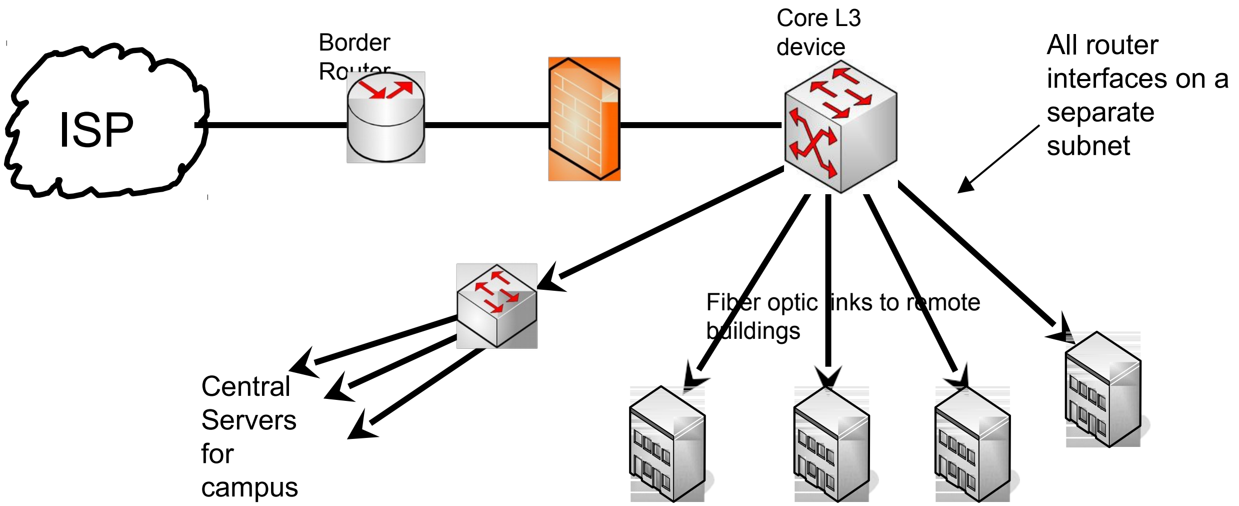
Servers should be at your core location where there is good power and air conditioning


ISP
Note servers are on a separate routed Subnet than the users in buildings
Fiber optic links to remote buildings
Central Servers for campus

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:

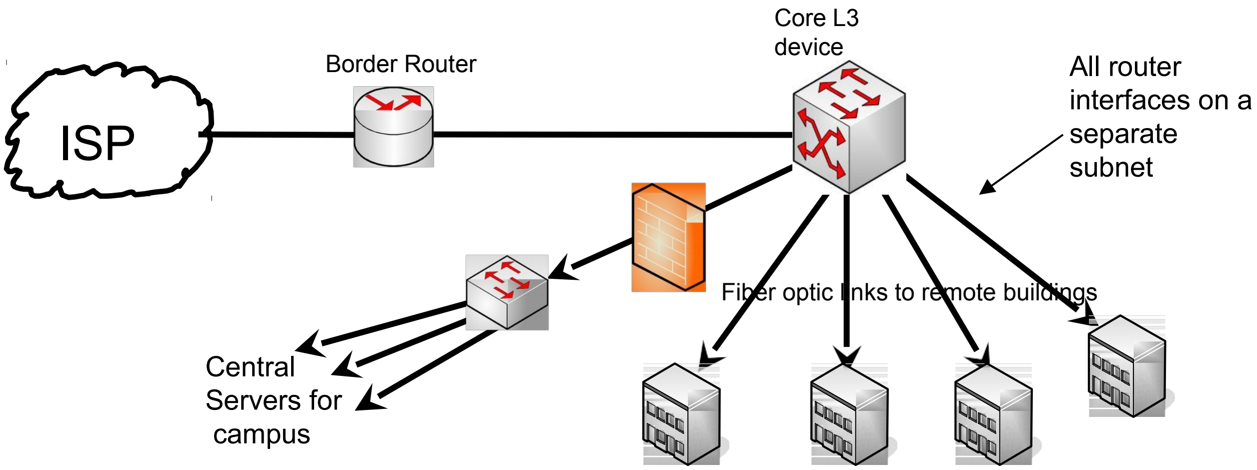

ISP
Border Router
Core L3 device
All router interfaces on a separate subnet
Fiber optic links to remote buildings
Central Servers for campus

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.

Firewall Placement - 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:

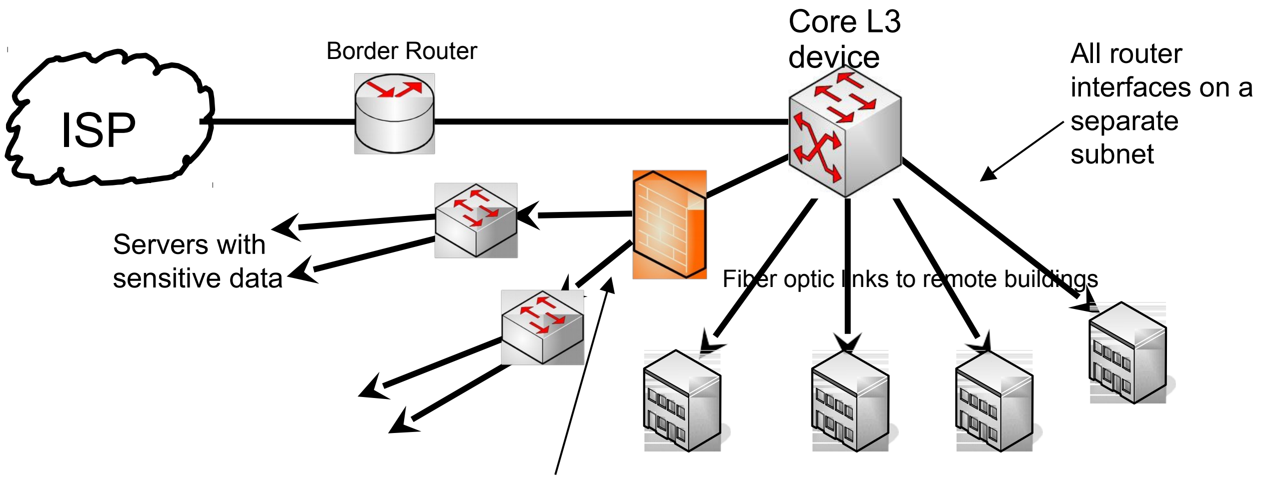


Best Practices for Servers

Not all servers are created equal. Some are accessed by students (Moodle, file & print, email).

Others have sensitive data (payroll, financial systems, etc)

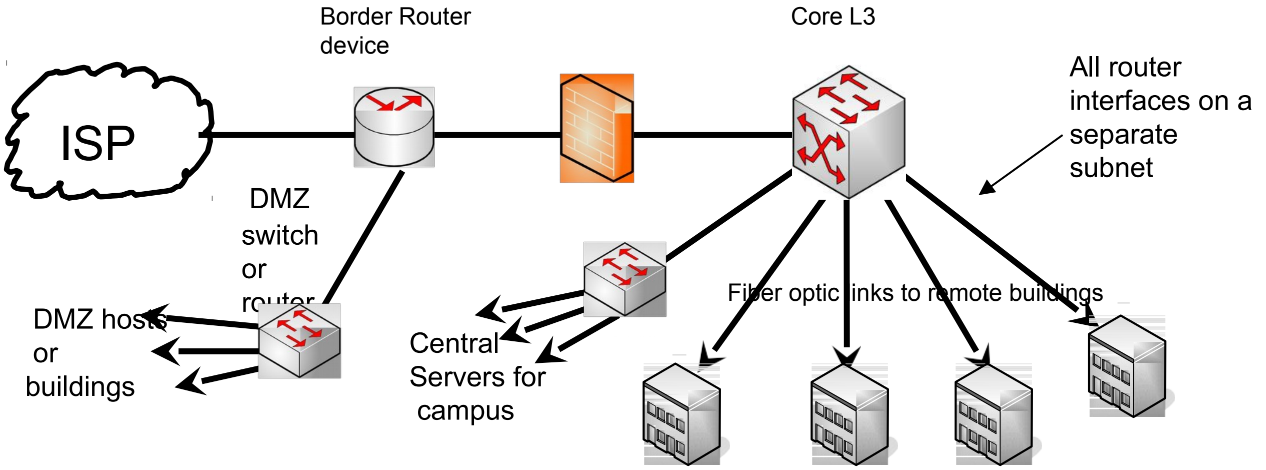
Put different classes of servers on different subnets


ISP
Border Router
Core L3 device
All router interfaces on a separate subnet
Servers with sensitive data
Fiber optic links to remote buildings

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

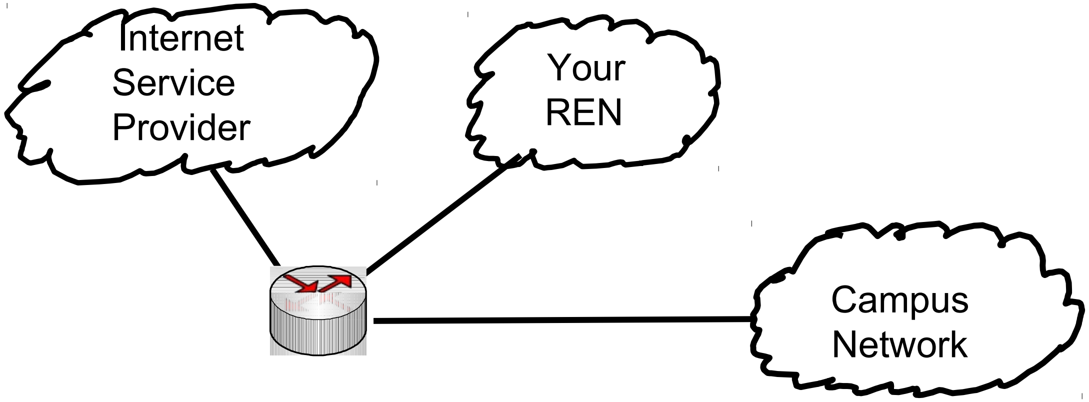
Science DMZ

- Science DMZ is network optimized for high-performance scientific applications
- 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
- Recommended Configuration:

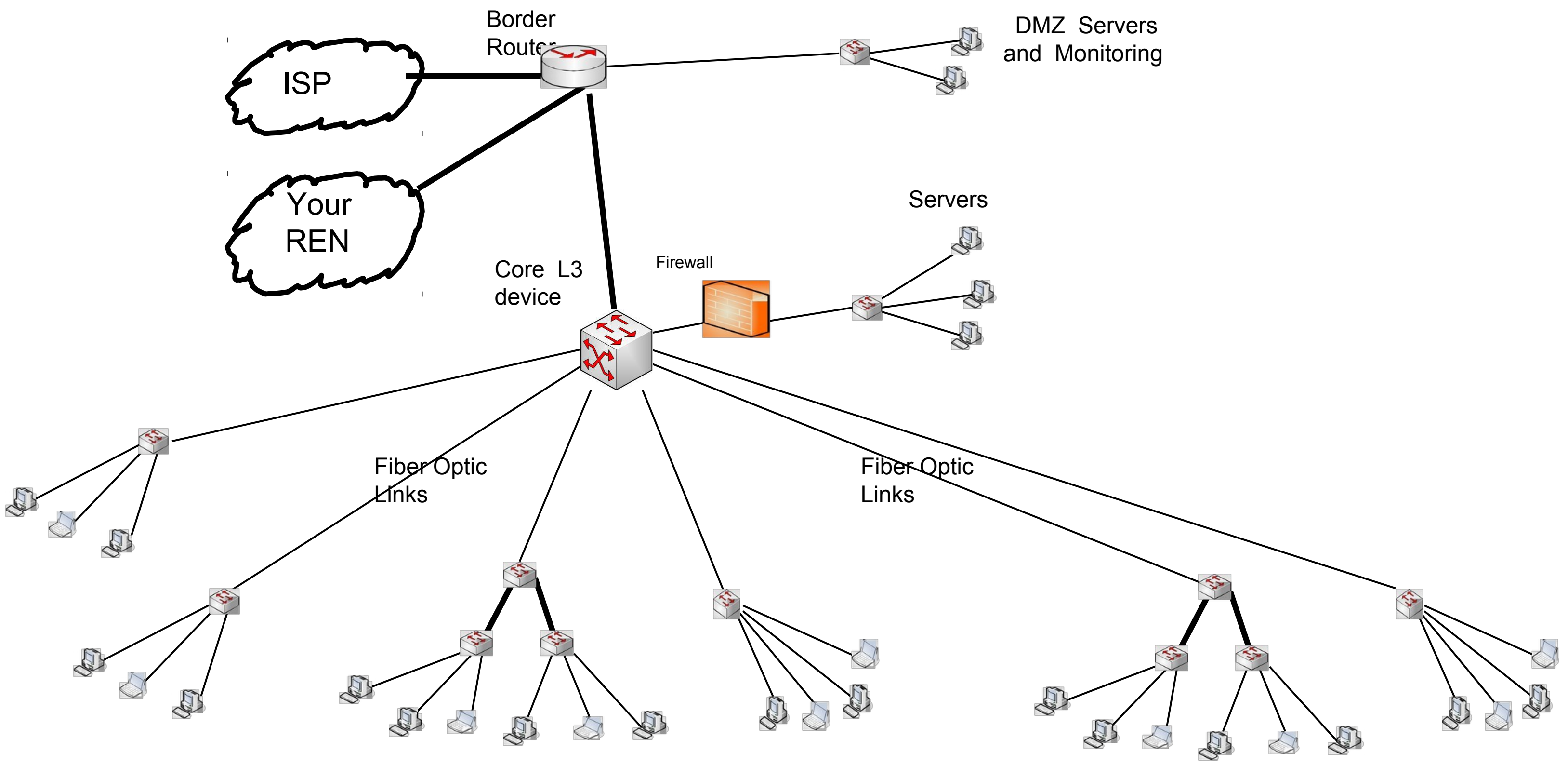

Border Router device
Core L3
ISP
All router interfaces on a separate subnet
DMZ switch or router
DMZ hosts or buildings
Central Servers for campus
Fiber optic links to remote buildings

Border Router

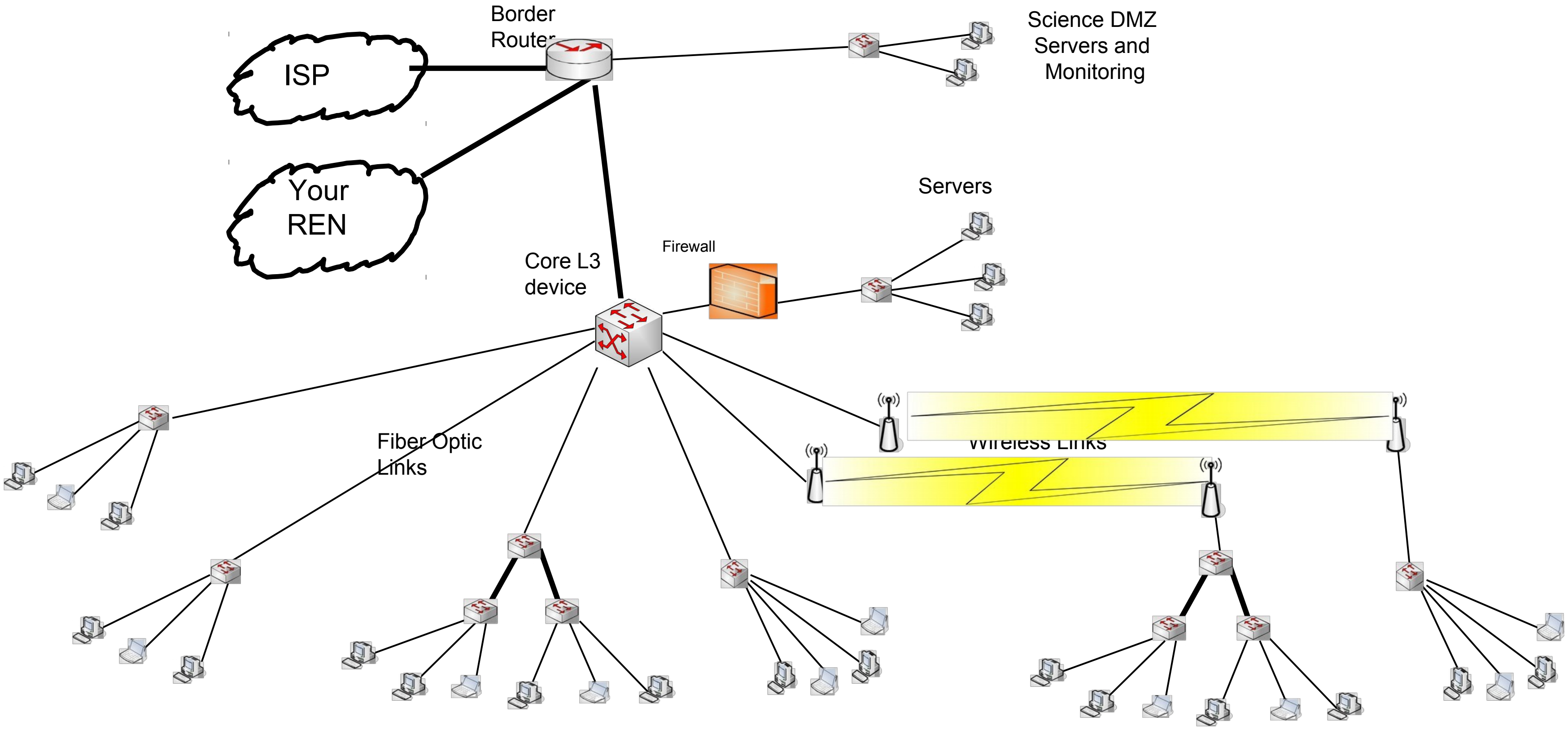
- Connects campus to outside world
- If you are dual homed, you must have a border router
  - dual homing is hard to make it work right
- Many campuses in emerging regions will do NAT on this device that connects the campus to the outside world.
  - Most of them use a firewall for this function



Putting it all Together



Wireless Links Instead of Fiber



Thank You

Dhammika Lalantha/LEARN

Email: lalantha@learn.ac.lk