ICT networks

Pure Training Center

About the author

Holder of bachelor of science in telecommunication engineering With over 7 years of experience as practicing telecom engineer / manager, and as university lecturer

Author of the books

1.Statistics guide for students and researchers with SPSS illustration (ISBN-10:1656013657, ISBN-13:978-1656013651)

2. Microwave and cellular communication planning and design for engineers And managers (ISBN-13: 979-8737317263)

Website:www.puretrainingcenter.com
Business email:info@puretrainingcenter.com
Personal email:abdiasisjama1989@gmail.com
Skype ID:abdiasis.jama2
Tel/WhatsApp:+252906790027

NETWORKING CONCEPTS

Lesson five

Pure Training Center

Ethernet network components


Work station


Switch


Router


Wireless router


Twisted pair cable


Optical fiber cable

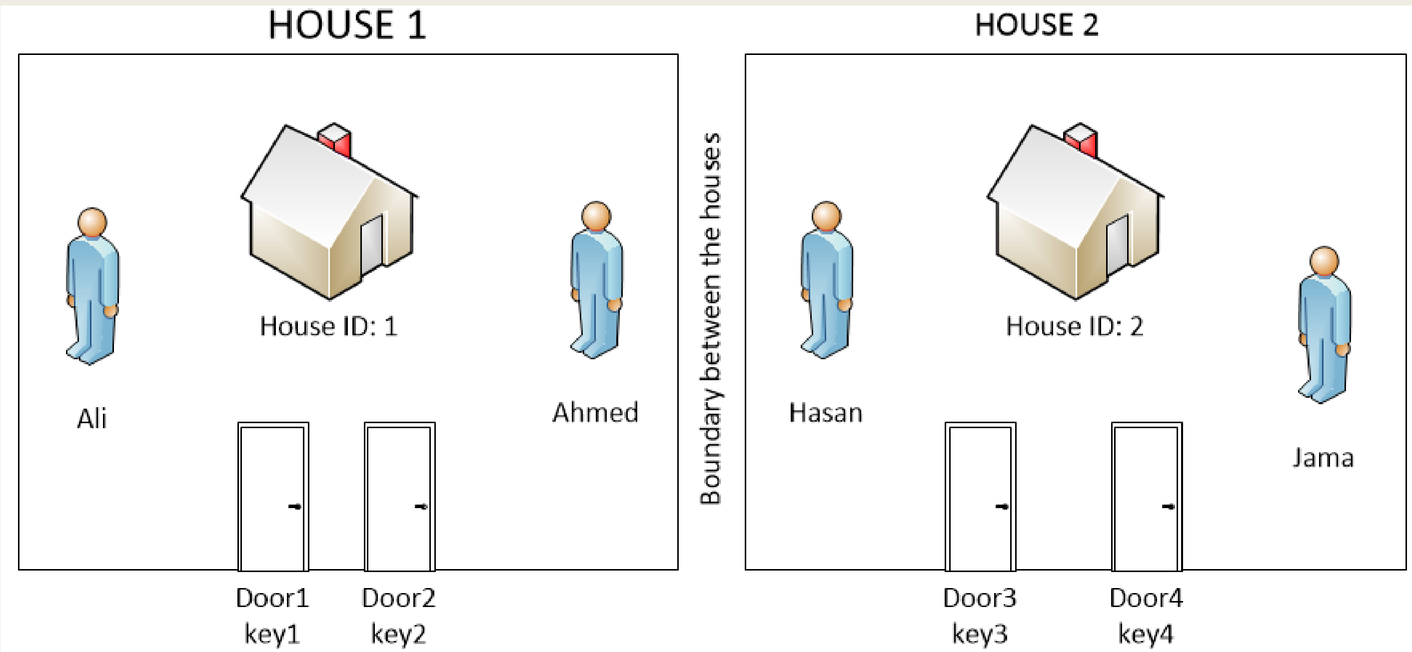

RJ-45 port

Fast Ethernet and Gigabit Ethernet

- Fast Ethernet is a technology that
  - *Can transfer data at 100Mbps over twisted-pair cable or optical fiber cable*
  - *Its uses full-duplex*
- Gigabit Ethernet is a technology that
  - *Is faster than fast Ethernet by transferring data at a rate of 1000Mbps*
  - *Most data center use optical fiber or CAT5e/6*
- Newer technologies also support 10G Ethernet that run on optical fiber lines

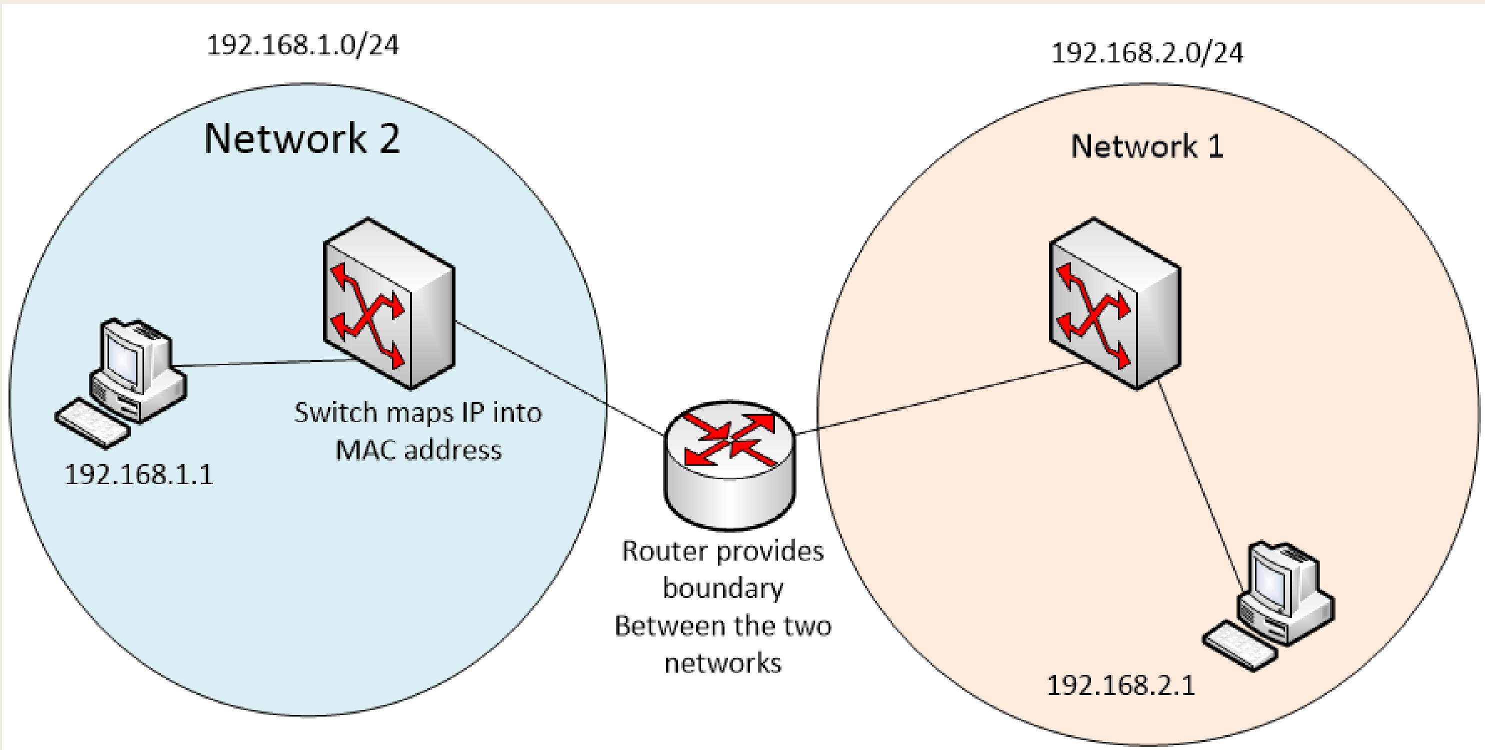
Addressing

- Consider two neighboring houses shown below



Person = computer
Person name = computer IP
Boundary wall = router
House = network
House owner = MAC
House ID = IP address
Door key = port number

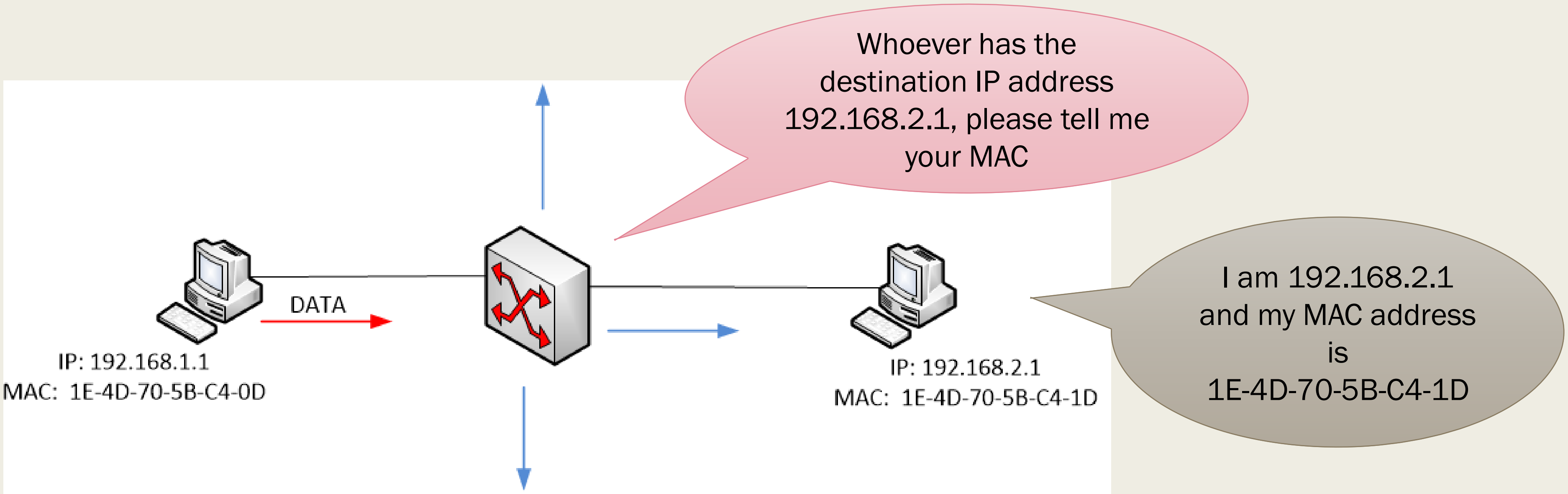
Network addressing



L2 communication

- L2 (layer 2) data communication means all computers are connected to switch
- Switches don't understand IP address but understand MAC addresses
- MAC address is already built-in into all network devices such as computers, but IP address is assigned manually by the ICT engineer or dynamically by DHCP server
- When computer 192.168.1.1 Sends data to destination computer 192.168.2.1, the switch broadcasts the received frame out of all its ports except the port it received using ARP protocol
- The destination computer then identifies to the switch with its MAC address. The switch then sends the data frame to destination MAC address

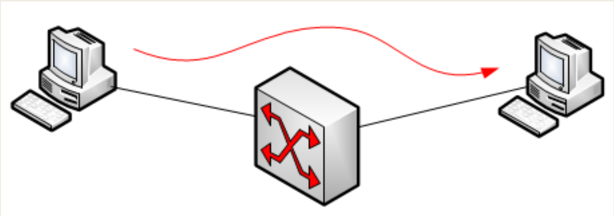
Address resolution protocol (ARP)



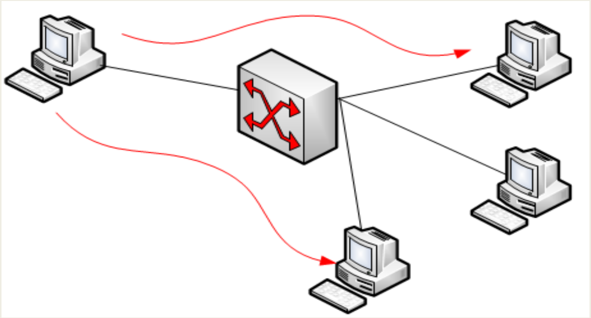

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0050.0fe4.dcd5    DYNAMIC     Fa0/1
   1    0090.2b97.548d    DYNAMIC     Fa0/2
```

Unicast, multicast, and broadcast

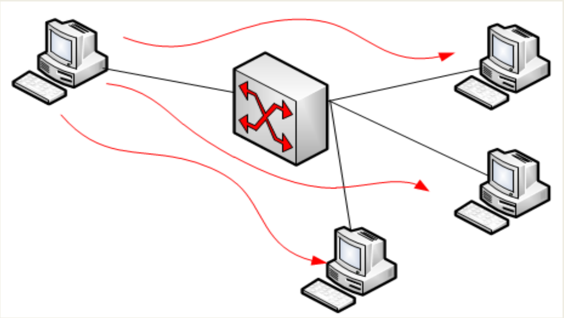
- Unicast is one-to-one communication (e.g. telephone call)
- Multicast is one-to-many communication (e.g. email)
- Broadcast is one-to-all (e.g. FM radio, cellular paging)



Unicast



Multicast



Broadcast

Broadcast domain

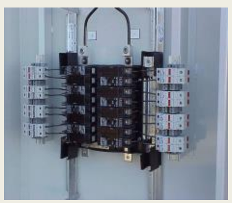
- L2 switch is one broadcast domain (meaning an Ethernet frame reaching one interface will reach all hosts connected to the switch except the sender)

- Broadcast domain = one subnet (one network)

- L3 router has broadcast domain in each interface (each interface is a separate network)

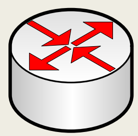
Redundancy

- To design high availability network, critical network components should have redundancy (one active component and one or several standby components)

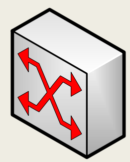


Power redundancy

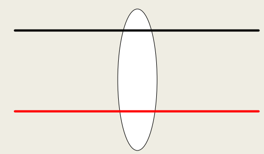
Server redundancy



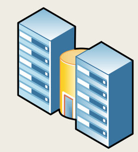
Gateway router redundancy



Aggregation Switch redundancy



Connection redundancy



Configuration backup

Kilobyte, Megabyte, Gigabyte

- Humans understand natural numbers (1, 2, 3, 4, 5, 6, 7, 8, 9, 10)
- Computers and other digital electronics understand binary numbers (0, 1)
- 8 bits of computer data form one byte (1 byte = 8 bits)
- 1 kilobyte = 1000 bytes (1kB = 1000B)
- 1 megabyte = 1000 kilobytes (1MB = 100kB)
- 1 gigabyte = 1000 megabytes (1GB = 1000MB)
- 1 terabyte = 1000 gigabytes (1TB = 1000GB)

Network characteristics

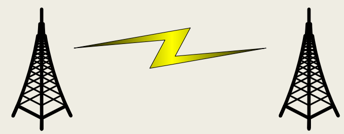
- Throughput / data rate / bit rate / speed … the speed at which a user can access network resources (measured in **bit per second**)
- Latency / delay … the round trip delay associated with when a user accesses network resources and get response from the network
- Bandwidth / capacity … total volume of data that can pass across the network at any given time (measured in byte)

Transmission media

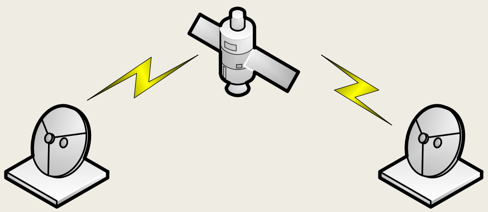
- LAN uses twisted pair and optical fiber cables
- WAN uses optical cables and wireless media

CAT5	100Mbps
CAT5e	1Gbps
CAT6	1Gbps

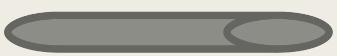
multimeter	Short connections in data center
Single mode	Long connections in backbone links



Fixed radio links

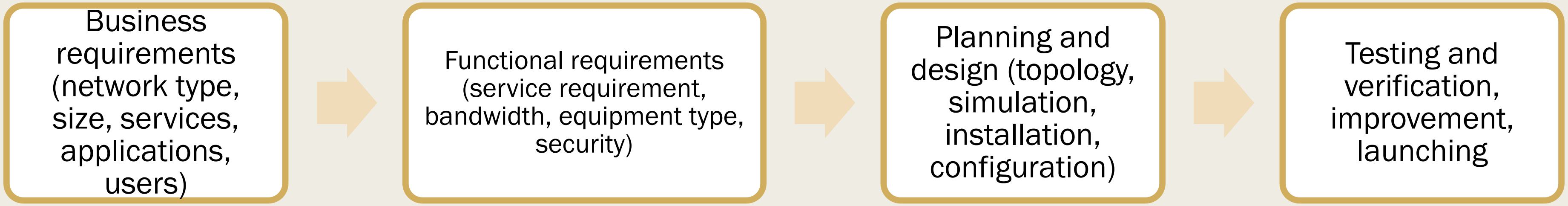


Satellite links



Single mode fiber

Network design requirements

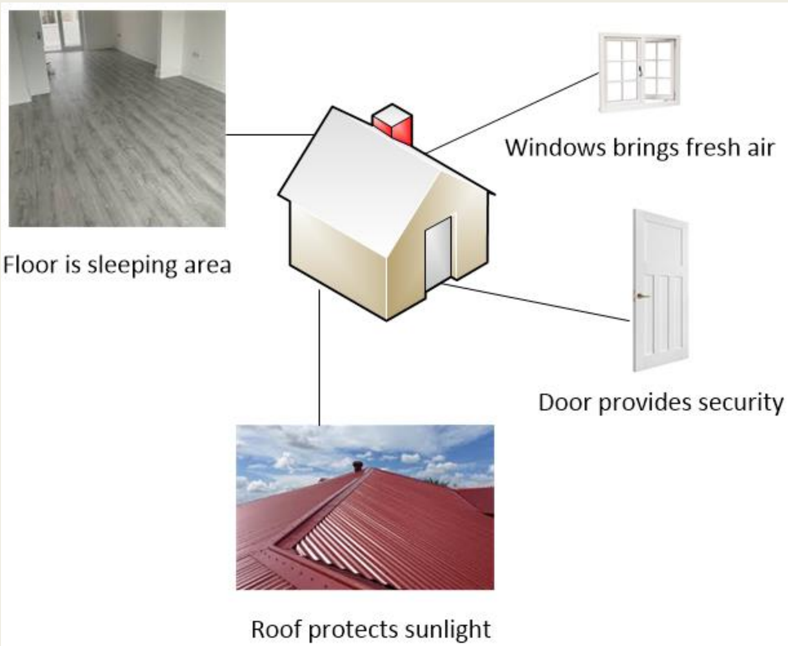


- The ICT engineer should understand business requirement of the client
- Transforming business requirements into functional requirements of the network
- Transforming functional requirements into planning and design
- Implementing the network, testing it, make changes where necessary and launching it

OSI MODEL

Networking standards

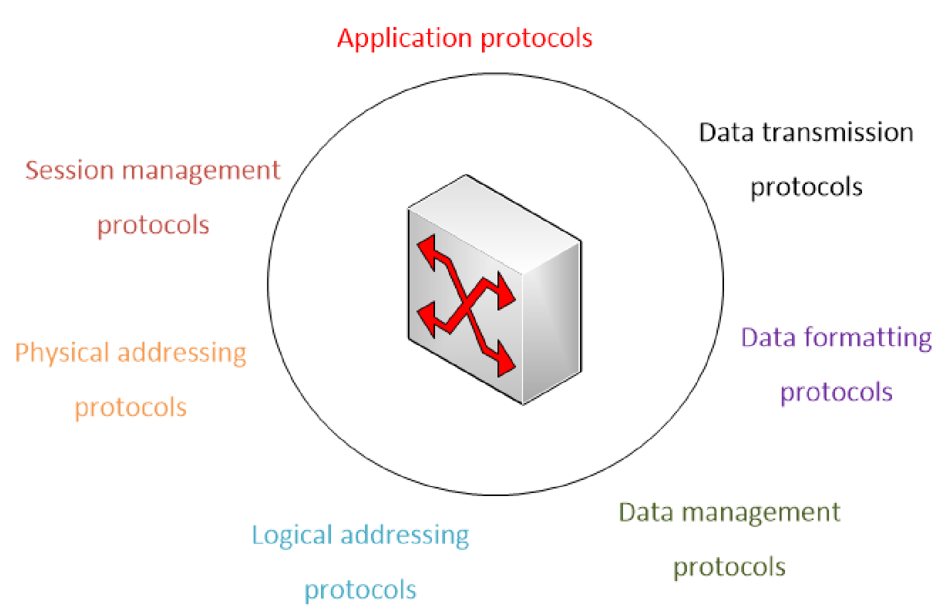
House model



	Layer	Function	Example
1	Roof	Protects sunlight	Metal
2	Window	Brings fresh air	Glass, wood
3	Door	Provides security	Metal, wood
4	Floor	Sleeping area	Cement, marble

Every house should have the above model, so that Construction suppliers produce same cement, same keys, Same ceilings, same doors, same windows

OSI model



	Layer	Function	Example of protocols
7	Application	Interface to user	HTTP/FTP
6	Presentation	Formatting and encryption	SSL
5	Session	Session for separate traffic	PPTP
4	Transport	Data segmentation	TCP/UDP
3	Network	Logical IP addressing	IPv4/IPv6
2	Data link	Physical MAC addressing	Ethernet
1	Physical	Bits for transmitting over the medium (e.g. microwave)	Microwave

Every network should follow the OSI model, in Oder for different manufacturers to produce Interoperable network equipment

Network equipment interoperability

- Since networking components (routers, switches, cables, servers, computers) are produced by different manufactures, they should work together at the end user level

Layer 1: Physical

- The physical layer (aka layer one or **L1**) defines the following
  - *Specifications on the interface between the network devices and the transmission network*
  - *Binary representation of data and encoding it into electrical or optical signal*
  - *Other characteristics defined by L1 include (duplex, shared or dedicated bandwidth, throughput, synchronization, aggregations, etc.)*

1101001011

Layer 2: Data link

- Its functions include (data framing, physical MAC addressing, error and flow control)
- Switches perform L2 functions by using MAC addresses of devices to establish communication between them
- VLAN is used in L2 to divide the switch into multiple separate networks (or subnets)

Layer 3: Network

- **Routing** is one of the main functions performed at L3. It enables sources and destinations to communicate over many different networks (or subnets)
- **Logical addressing** is another main function of L3 in which each device on the network is assigned an IP address that is unique
- IPv4 and IPv6 are used for logical addressing
- Types of routing protocols used (static, RIP, OSPF, EIGRP, BGP)

Layer 4: Transport

- **Port addressing** (different services run on a server at the same time such as HTTP, FTP, DNS). The client computer specifies which destination port number is being requested. Port numbers are added to the data by L4
- Example of port addressing are
  - *HTTP for port 80 and FTP for port 21*
- Other functions include
  - *Data segmentation into transport blocks*
  - *Connection control, flow control and error control*

Layer 5: Session

- As its name indicates, L5 establishes and maintains sessions between communicating devices. It also makes sure synchronization exists before starting communication

Layer 6: Presentation

- This layers performs data formatting such as
  - *Compression*
  - *Encryption*

Layer7: Application

- Its allows the user to access the network (user interface)

TCP/IP PROTOCOL SUITE

Networking standards

What is network protocol?

- A protocol is like a government that controls how ICT networks behave
- A single protocol can not do all the job. So many different protocols work together to control the network (**protocol suite**)
- TCP/IP is the most commonly implemented protocol suite in today's computer networks
- It has 4 layers in contrast with OSI that has 7 layers
- OSI is theoretically references while TCP/IP is used practically

TCP/IP vs OSI

Application	Application
Presentation	
Session	
Transport	Transport
Network	Internet
Data link	Network access
Physical	

TCP/IP layers

Layer	Example protocols
Application	HTTP, HTTPS, FTP, SMTP, DNS
Transport	TCP, UDP
Internet	IP, ICMP,
Network access	Ethernet, 802.x

Application layer

- This combines the OSI (application + presentation + session) layers

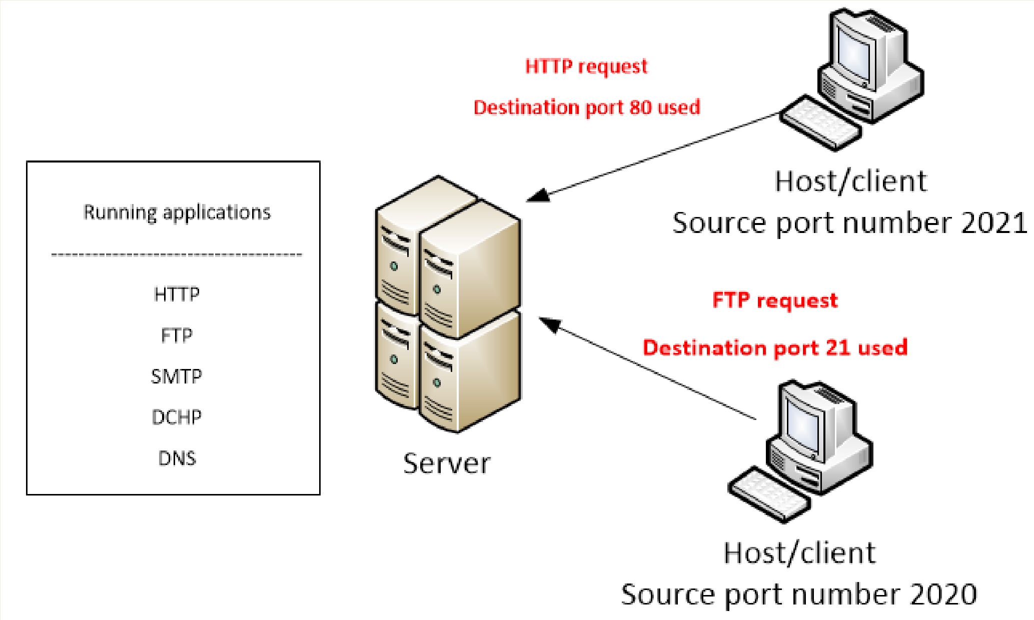
HTTP	Hyper text transfer protocol. It is used in web access web pages on the internet. For example Google chrome uses HTTP to transfer the web pages you request from remote server
HTTPS	Secure HTTP is more secure and used nowadays
FTP	File transfer protocol. It is used to transfer files (documents, audio, video, etc.) between networking devices
SMTP	Simple mail transfer protocol. It is used to send emails
DNS	Domain name service. It translates domain names into IP addresses
DHCP	Dynamic host configuration protocol. It provides IP addresses to network hosts automatically

Transport layer

- TCP (transmission control protocol) is used for connection-oriented which is reliable. UDP (user datagram protocol) is used for less reliable connections
- Port numbers for application

  layer protocols
- It segments data received from

  Application layer into segments



TCP header added by transport layer

```
Transmission Control Protocol, Src Port: 80, Dst Port: 49830, Seq: 1, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 49830
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 3341623306
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 1535065940
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 237
    [Calculated window size: 237]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x2808 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [Timestamps]
```

Internet layer

- IP addressing and packet routing

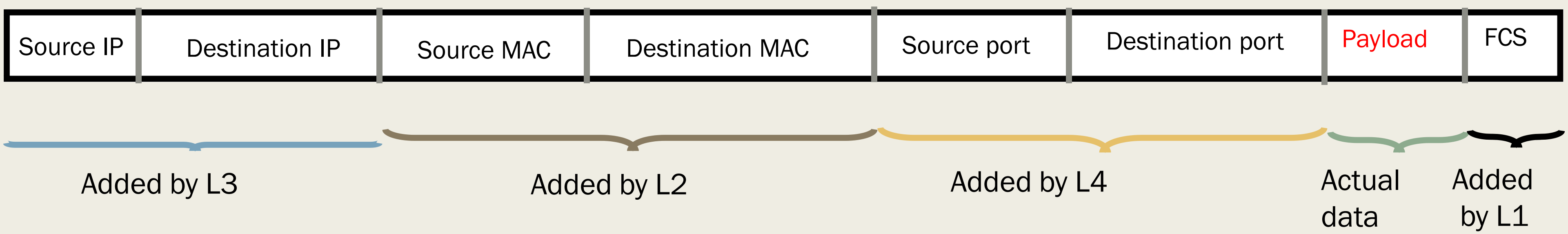
IP	Internet protocol. Forwards data packets across the network
ARP	Address resolution protocol. Maps IP addresses to MAC address at L2 networks
ICMP	Internet control message protocol. Used to ping remote devices for connectivity

Network access layer

- This layer combines data link and physical layers of the OSI model
- Examples of protocols that work at the network access layer include
  - *Ethernet*
  - *PPP*
  - *TDMA (PDH, SDH)*
  - *IEEE 802.x*

Data frame

- When sending data through TCP/IP network, all layers add header



NETWORK TOPOLOGY

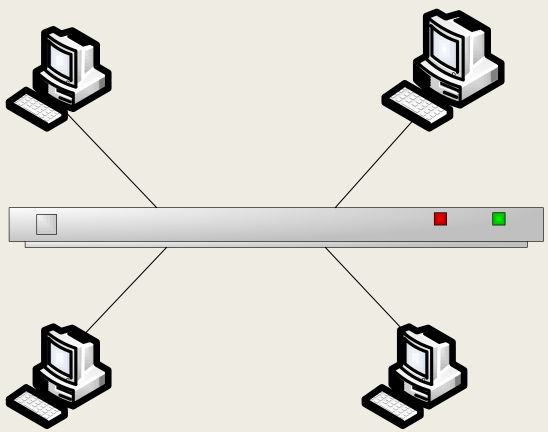
Design concepts

Business requirement

- Network engineer is responsible for designing networks according to client requirement

- Things to consider
  - *Which topology to use (star, ring, mesh)*
  - *Services to be supported by the network*
  - *Redundancy to avoid single point failure*

Star topology



All client machines connect to central access switch

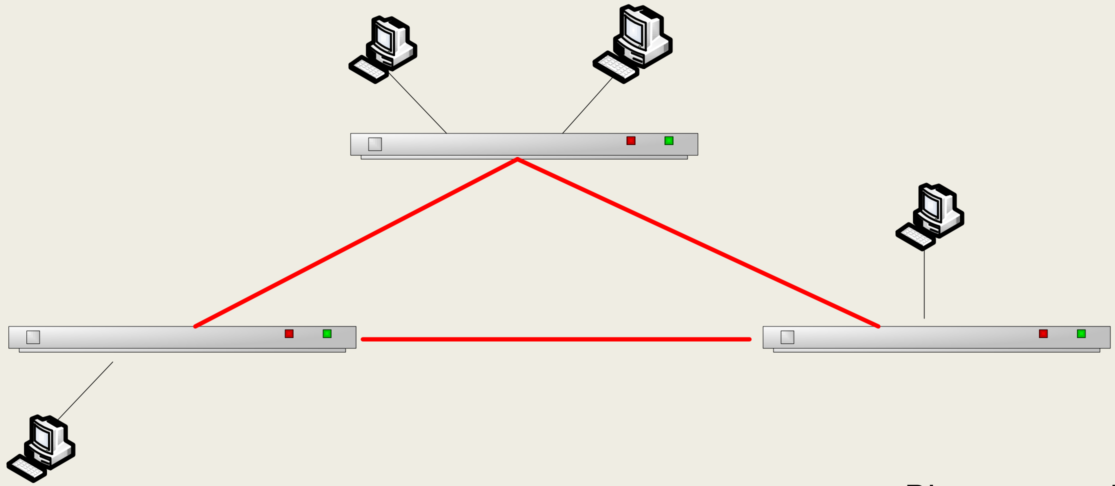
Advantage

Simple to design and implement

Disadvantage

There is single point failure (if the central switch fails. the whole network fails)

Ring topology



Ring connection is formed between company sites

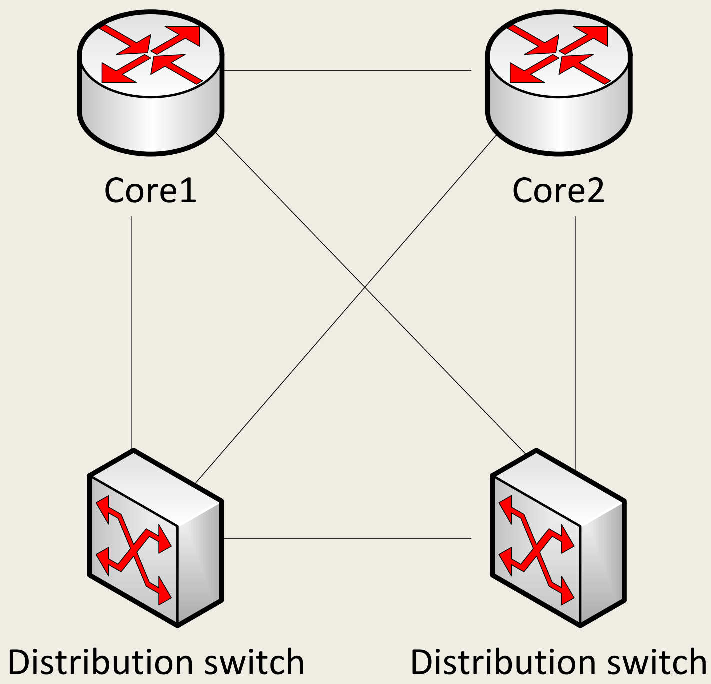
Advantage

Redundancy is provided (if one path fails, the other path takes over)

Disadvantage

Cost is increases. Switching loops may arise if the network is L2

Mesh topology



Every site is connected to every other site

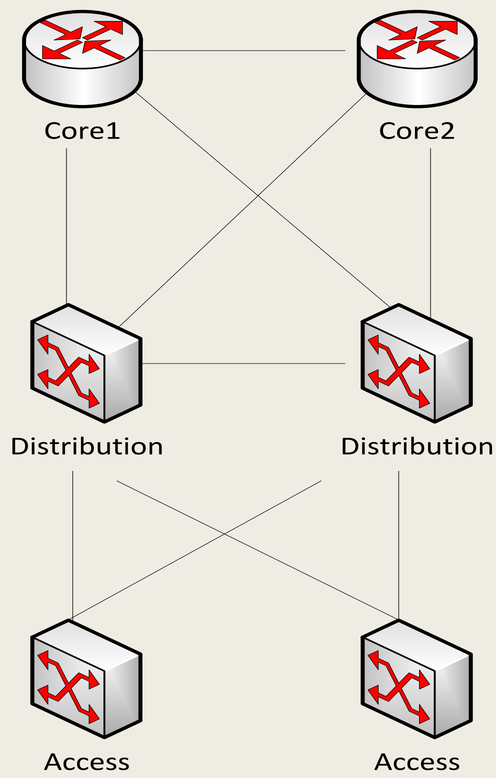
Advantage

Redundancy is provided (if one site fails, the other site takes over)

Disadvantage

Expensive and needs expertise to implement

Hierarchal design model



Connection to other networks
And internet

Aggregation switches in data center

Subnets in floors and offices

IP SUBNETTING

Internet protocol addressing

Binary and decimal numbers

- Binary number is base-2 system that take 2-value (0, 1)
- Decimal number is base-10 system that take 10-value (1, 2, 3, 4, 5, 6, 7, 8, 9, 10)
- To convert decimal number to binary we use the following table

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Examples

- Convert 255 into binary representation

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Add all numbers
That sum to 255

- 255 = 128 + 64 +32 + 16 + 8 + 4 + 2 + 1
- Because all numbers in the table are used to add to 255, we give all of them bit 1
- Hence 255 in binary is 11111111
- Any number in the table that do not take part the sum is given bit 0

IP address

- IP address is 32-bit identifier given to a network device for communication purpose
- The 32-bit length is divided into 4 pars each of 8 bits (A.B.C.D)
- The smallest digit an IP address can take is 0, the largest digit is 255
- The IP address consists of two parts (network part that identifies the network and host part that identifies network devices)

IP address classes

- The IP protocol used in today's network is called IPv4 and is 32-bit
- The next generation IP address is called IPv6 and is 128-bit
- There are four IP classes in IPv4

Class	First number address range	Comment
A	1 – 126	127 networks / 16 million hosts
B	127 - 191	16,000 networks / 65,000 hosts
C	192 – 223	2 million networks / 254 host
D	224 – 254	Reserved for multicast groups

Class A IP address examples

- We said an IP address has four numbers A.B.C.D
- For class A IP address the first number can take [(1-126).B.C.D]
- 121.43.1.2 is class A IP address because the first number 121 is between 1 – 126

Public and private IP address

- Public IP addresses are assigned for devices and services on the internet and can be used only once. Hence there are registered for the owner
- Private IP addresses are assigned for private LANs of organizations and can be re-used in different networks

Class	Private IP address range
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

Subnet mask

- The IP address is divided into two parts
  - ***Network part*** *that identifies the network (is like grandfather name that the family shares)*
  - ***Host part*** *that identifies the computer or other devices in the network (is like names of individual members of the family)*
- **Subnet mask** is the one that tells which part of the IP address is the network and which part is the host
- Therefore when assigning an IP address to host, subnet mask is also assigned to tell the computer the network address and host address

Classful and classless subnet masks

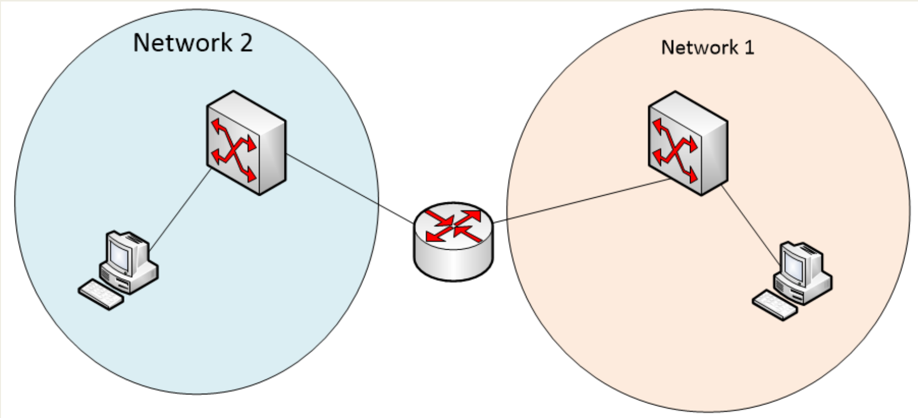
In classful addressing, fixed subnet mask can be used with IP addresses as shown below

Class	Classful subnet mask	Slash notation
A	255.0.0.0	/8
B	255.255.0.0	/16
C	255.255.255.0	/24

In classless addressing, variable subnet masks can be used which is very efficient

Classful IP subnets example

- Suppose you are given the classful IP one network 10.10.0.0/16
- You are asked to subnet it into **4** networks to plan for the following network



4 networks required

2 to address networks 1 and 2

The remaining 2 networks will
Be for future expansion

Classful IP subnet example

- 10.10.0.0/16 can also be written as 10.10.0.0 255.255.0.0
- 255.255.0.0 and /16 are the same
- 255 in binary is 11111111 and 0 in binary is 00000000
- Hence 255.255.0.0 in binary form is 11111111.11111111.00000000.00000000
- The part that contain 1 is the network while the 0 part is the host
- Hence 11111111.11111111.00000000.00000000 = network.network.host.host
- If you count all the 1s and 0s, it will total to 32-bit

First step in subnetting

- Convert the required number of networks into binary format (1)

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

- The value 4 is highlighted in the table
- Hence 4 in binary format is 00000100
- Removing leading zero we get 4 = 100 in binary
- Hence it takes 2 bits to get 4 networks

Second step in subnetting

- Convert the given subnet mask into binary, and steal the host portion number of bits equivalent to 4 networks (100)
- 255.255.0.0 = 11111111.11111111.00000000.00000000 is original subnet
- How many bits we need to get four networks? 2 bits (2 power 2)
- Steal this 2 bits from the host portion of the subnet mask to get
- 11111111.11111111.11000000.00000000 is new subnet mask

Third step in subnetting

- Find the new subnet mask after stealing 2 bits from the host portion of the original subnet mask
- New subnet mask is 11111111.11111111.11000000.00000000
- Now convert the new subnet mask into decimal

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

- 11000000 = 128 + 64 = 192 → hence new subnet mask is **255.255.192.0**

Fourth step in subnetting

- If the original network is 10.10.10.0 find the increment that has to be added to get the next networks
- Increment = last 1 bit of the new subnet mask
- New subnet mask is 11111111.11111111.11000000.00000000

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

- Hence increment = 64

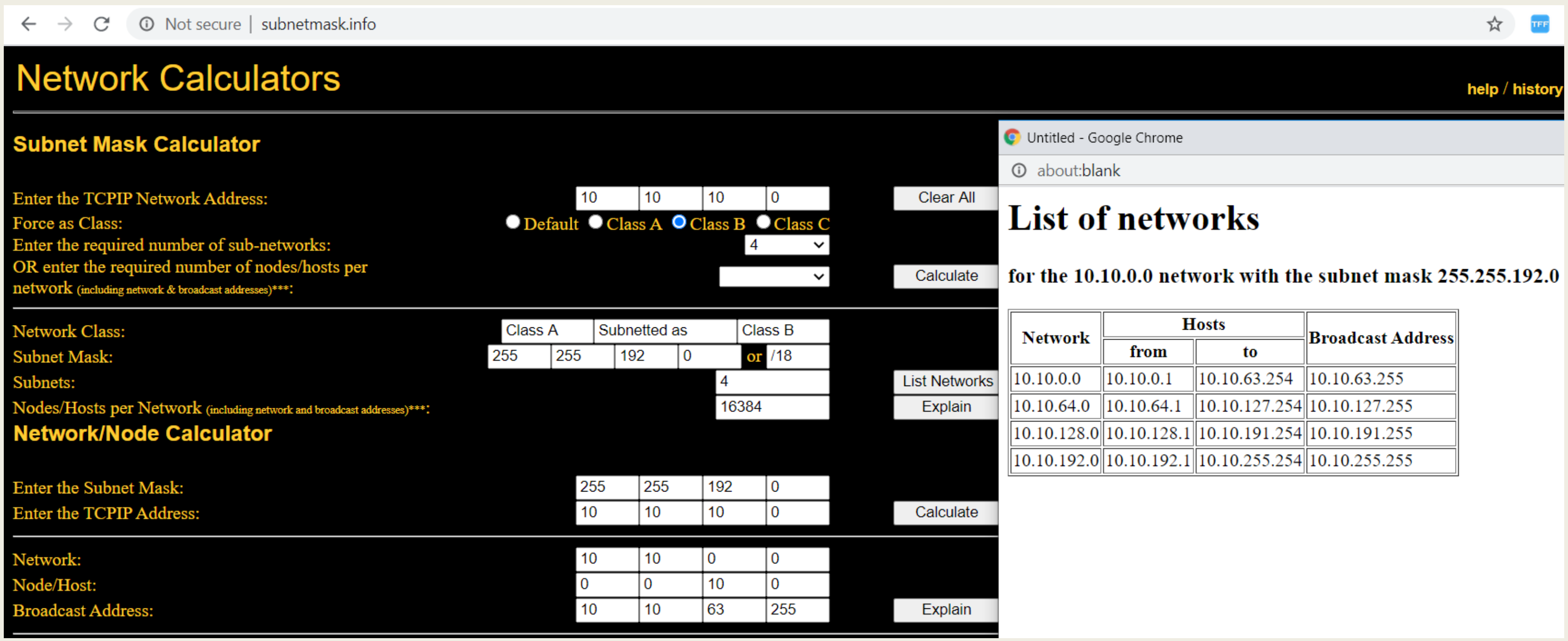
Final step in subnetting

- Using the increment create the networks

	Starting	Ending	Subnet mask
First network	10.10.0.0	10.10.63.255	255.255.192.0
Second network	10.10.64.0	10.10.127.255	255.255.192.0
Third network	10.10.128.0	10.10.191.255	255.255.192.0
Fourth network	10.10.192.0	10.10.255.255	255.255.192.0

Now you can assign the first two networks to the network design and save the Last two networks for future network growth and expansion

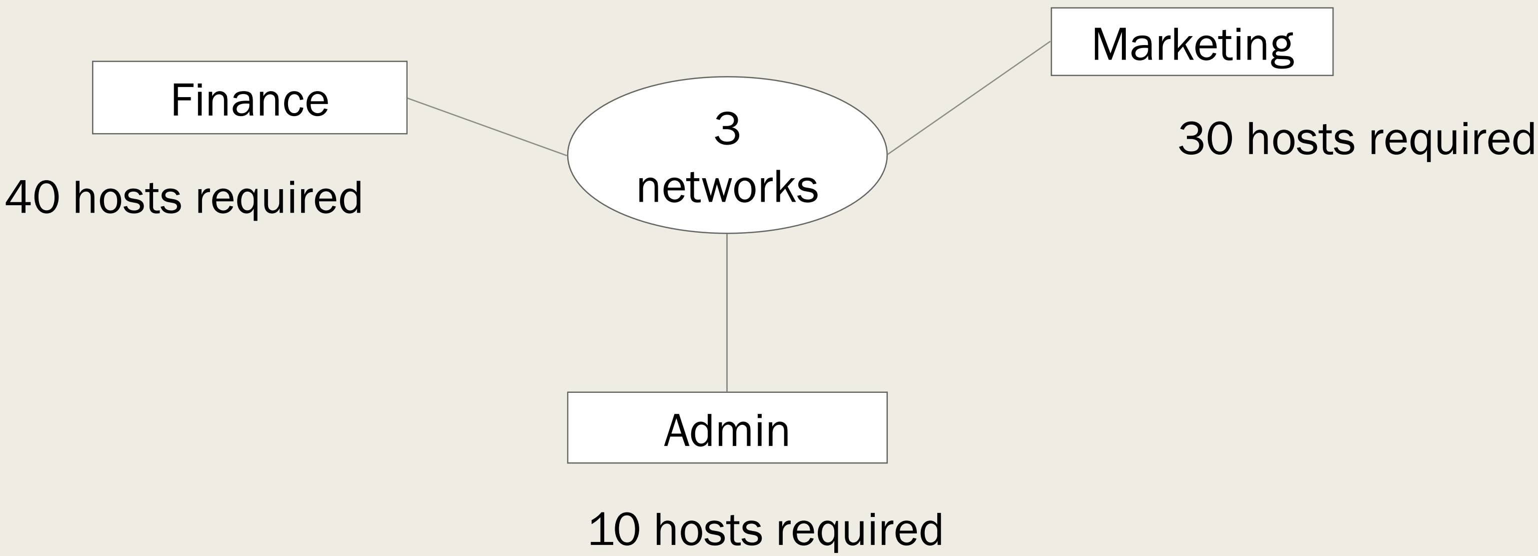
Using the online subnet calculator



Variable length subnet mask (VLSM)

Subnetting technique in which different subnets are designed based on required Hosts per subnet

As an example, you are given 192.168.50.0/24



VLSM for finance

Pure Training Center

- Convert the number of required 40 hosts into binary

128	64	32	16	8	4	2	1
0	0	1	0	1	0	0	0

It takes 6 bits
To get 40 hosts

- Convert the original subnet mask into binary

/24 = 255.255.255.0 = 11111111.11111111.11111111.00000000

- Find the new subnet mask by saving the number of hosts

11111111.11111111.11111111.11000000 = 255.255.255.192 = /26

- Find the increment

Increment is the last 1 bit = 64

192.168.50.0	192.168.50.63
192.168.50.64	

This subnet is sufficient
For 40 hosts

Hence finance network is 192.168.50.0/26 which supports 61 hosts

VLSM for Marketing

Pure Training Center

- Convert the number of required 30 hosts into binary

128	64	32	16	8	4	2	1
0	0	0	1	1	1	1	0

It takes 5 bits
To get 30 hosts

- Convert the original subnet mask into binary

/24 = 255.255.255.0 = 11111111.11111111.11111111.00000000

- Find the new subnet mask by saving the number of hosts

11111111.11111111.11111111.11100000 = 255.255.255.224 = /27

- Find the increment

Increment is the last 1 bit = 32

192.168.50.0	192.168.50.31
192.168.50.32	192.168.50.63
192.168.50.64	192.168.50.95
192.168.50.96	192.168.50.127

Taken by finance

This subnet is sufficient
For 30 hosts

Hence finance network is 192.168.50.64/27 which supports 30 hosts

VLSM for administration

Pure Training Center

- Convert the number of required 10 hosts into binary

128	64	32	16	8	4	2	1
0	0	0	0	1	0	1	0

It takes 4 bits
To get 10 hosts

- Convert the original subnet mask into binary

/24 = 255.255.255.0 = 11111111.11111111.11111111.00000000

- Find the new subnet mask by saving the number of hosts

11111111.11111111.11111111.11110000 = 255.255.255.240 = /28

- Find the increment

Increment is the last 1 bit = 16

192.168.50.64	192.168.50.79
192.168.50.80	192.168.50.95
192.168.50.96	192.168.50.111
192.168.50.112	192.168.50.127

Taken by marketing (192.168.50.64 – 192.168.50.95)

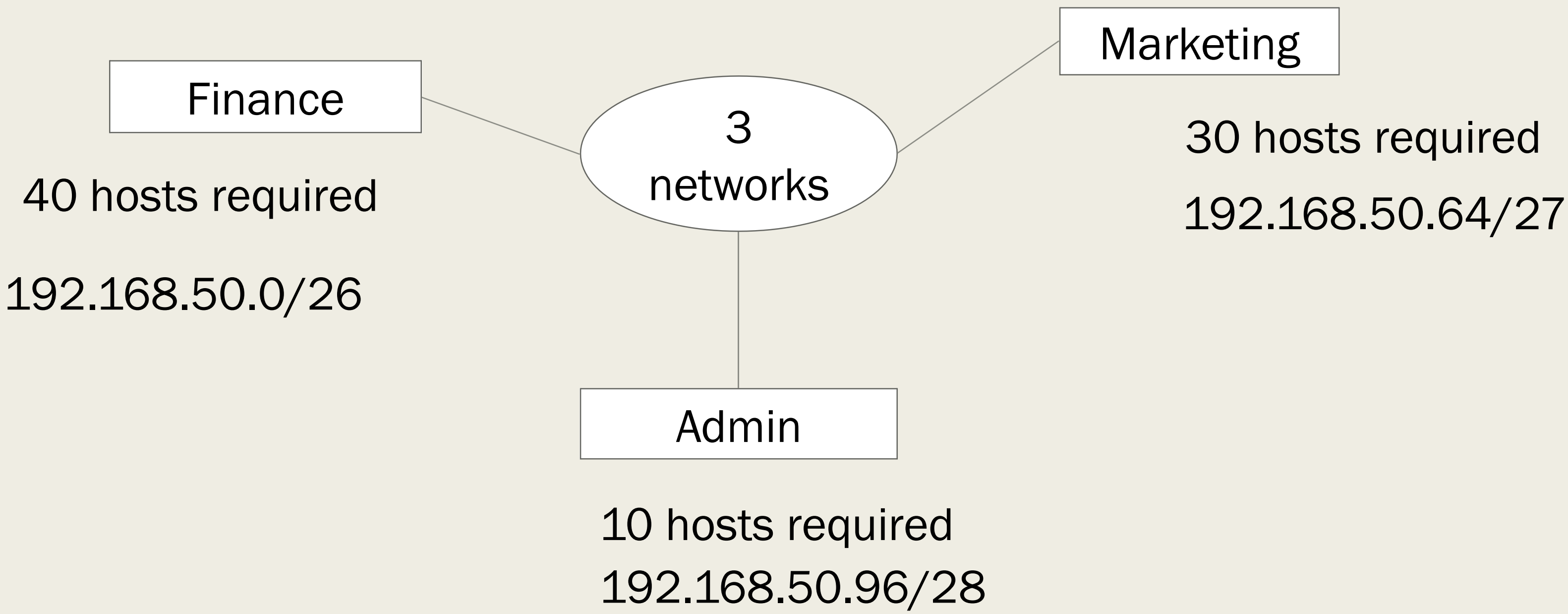
This subnet is sufficient
For 10 hosts (192.168.50.96 – 192.168.50.111)

Hence finance network is 192.168.50.96/28 which supports 30 hosts

Variable length subnet mask (VLSM) design

Subnetting technique in which different subnets are designed based on required Hosts per subnet

As an example, you are given 192.168.50.0/24



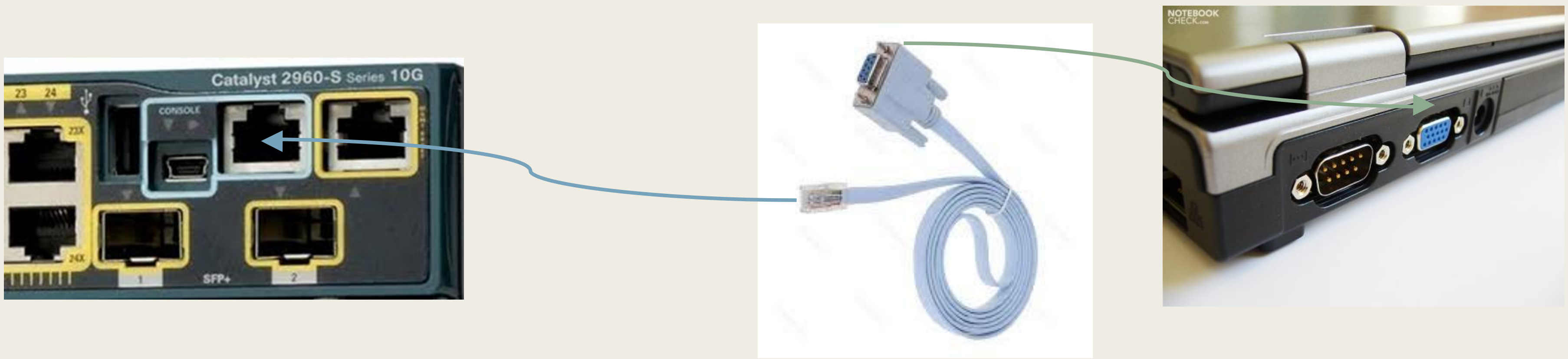
BASIC SWITCH CONFIGURATION

L2 networking

Pure Training Center

Connecting laptop to switch console port

Switch console port



Remote management using telnet

Switch Gigabit port
IP address assign

IP address

Basic configurations

Pure Training Center

- Hostname

```
Switch(config)#hostname FINANCE
```

- Management VLAN and IP configuration

```
FINANCE(config)#int vlan 1
FINANCE(config-if)#ip address 192.168.50.1 255.255.255.192
```

- Remote management (telnet)

```
FINANCE(config)#line vty 0 15
FINANCE(config-line)#login local
FINANCE(config)#username jama privilege 15 secret cisco
FINANCE(config)#enable secret cisco
```

- Running-config and startup-config

```
FINANCE#copy running-config startup-config
```

VLAN

L2 switching

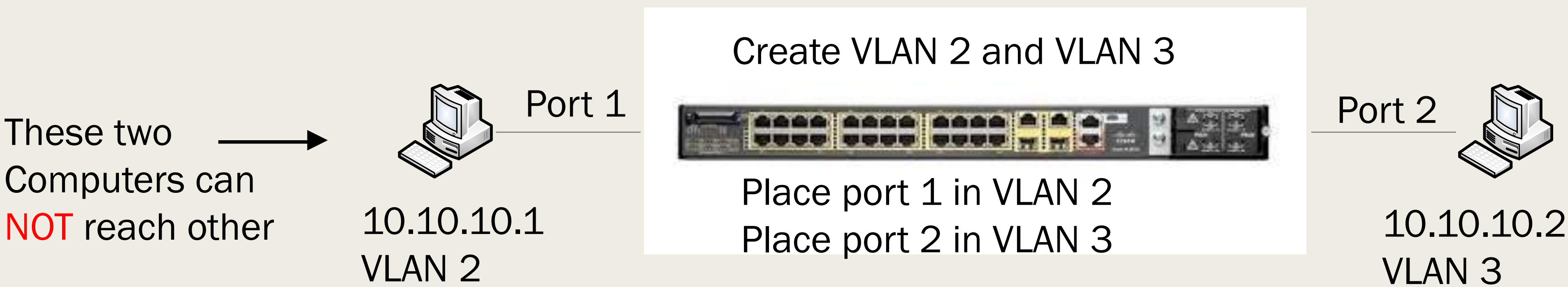
Introduction

- All ports (interfaces) of L2 switch are in default VLAN (VLAN 1)
- Thus all computers connected to the switch will be able to communicate provided they are assigned to same network (for example 10.10.10.0/16)

These two computers can reach other because they belong to same VLAN 1

What is a VLAN?

- VLAN is logical grouping of L2 switches
- By default, the switch is in one logical group (network) under VLAN 1
- It is possible to create other VLANs in the switch to logically separate the users connected to the switch



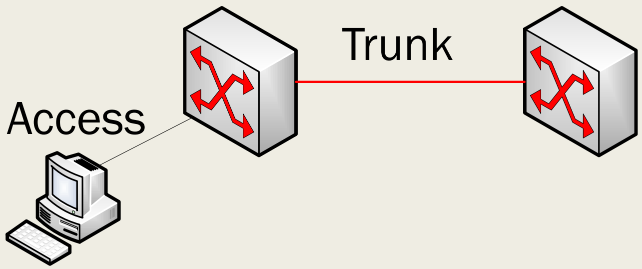
VLAN tag

- If a computer1 in VLAN5 wants to reach another computer2 in VLAN5 connected to the same switch, well how will the switch know the frame was actually sent to computer2 in VLAN5?
- The answer is that the switch labels the Ethernet frame with VLAN tag (identifier)
- If the frame has no VLAN tag, the switch then sends the frame on native VLAN (1 by default)

Header	**VLAN tag**	Payload	Trailer

Access and trunk ports

- A connection between a computer and switch is called access link
- A connection between two switches is called trunk
- An access port can carry only one VLAN
- A trunk port can carry all VLANs for tagged traffic and native VLAN for untagged traffic (by using dot1q protocol)



VLAN configuration on switch

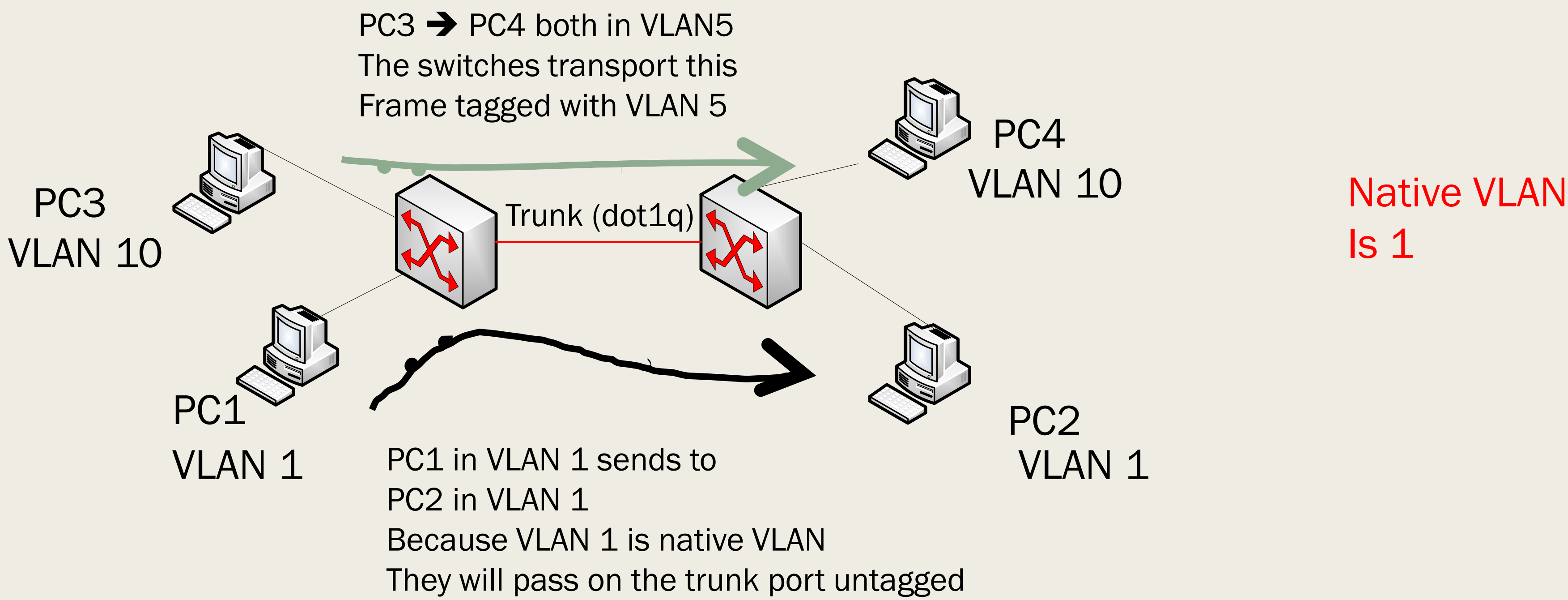
VLAN ID	NAME	MEMBER PORT	DESCRIPTION	MODE
100	10Mbps internet to certain hotel	G9	Port facing to aggregation switch	Trunk
101	10Mbps	GX	Port facing to ISP rack	access

Trunk setup between switches

- By default, most network switches come with dynamic auto negotiation protocol.
- A cross-over cable connected between two switches will dynamically setup as a trunk
- In real-life production network, dynamic trunking should be disabled by manually configured by the ICT engineer
- In Cisco networking, the dynamic trunk protocol (DTP) is used

Native VLAN

- If a switch receives a frame with NO VLAN tag on its trunk port, it assumes that frame belongs to the native VLAN (which is VLAN 1 by default)



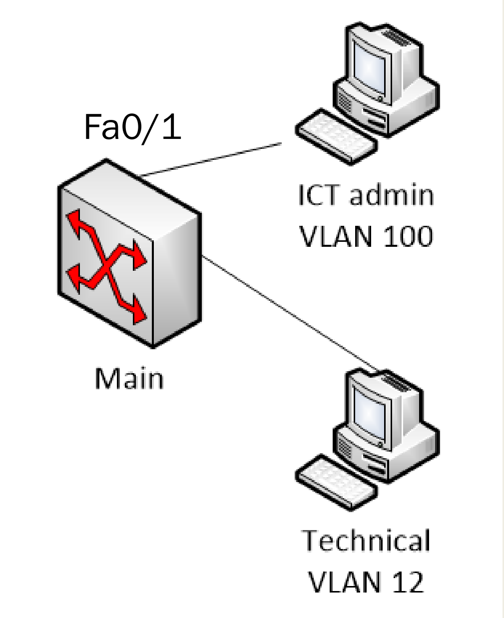
VLAN configuration

Setting management vlan to 100

```
Main(config)#vlan 100
Main(config-vlan)#name admin
Main(config)#int vlan 100
Main(config-if)#ip add 192.168.50.1 255.255.255.0
```

Main#show ip interface brief

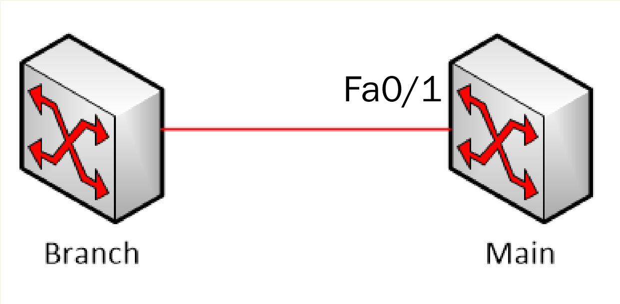
Interface	IP-Address	OK?	Method	Status	Protocol
Vlan100	192.168.50.1	YES	manual	up	down



Apply the created vlan to the switch port

```
Main(config)#int fa0/1
Main(config-if)#switchport mode access
Main(config-if)#switchport access vlan 100
```

Setting up trunk ports



New switches have dynamic trunk

Main#show interface fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)

Manual trunk configuration

```
Main(config)#int fa0/1
Main(config-if)#switchport mode trunk
Main(config-if)#switchport access vlan 100
```

Main#show interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1

Inter-vlan routing

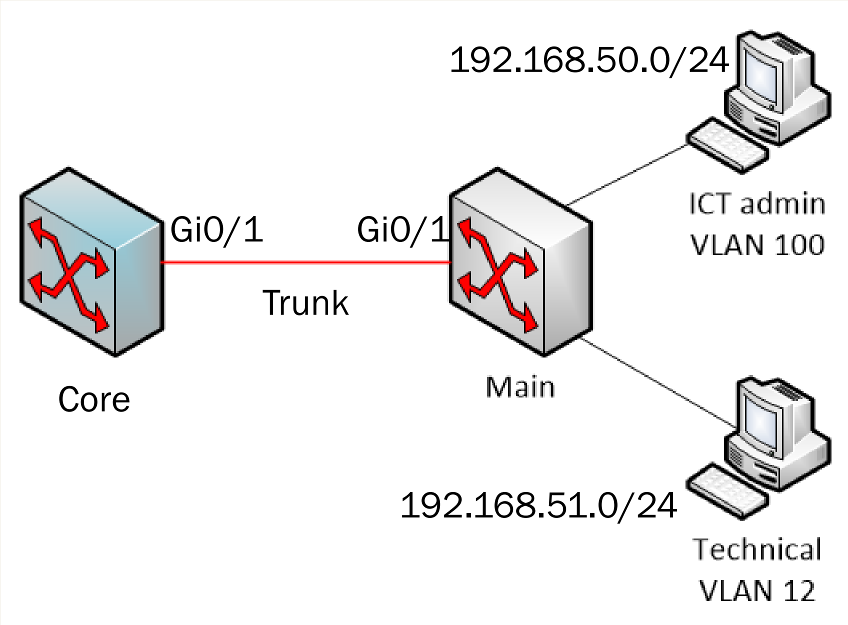
- Hosts in different vlans cannot reach other unless routing is configured
- In this example, we will use multi-layer switch to enable inter-vlan routing

Set interfaces vlans on the core multi-layer switch

core#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan100	192.168.50.1	YES	manual	up	up
Vlan 12	192.168.51.1	YES	manual	up	up

```
core(config)#ip routing
```



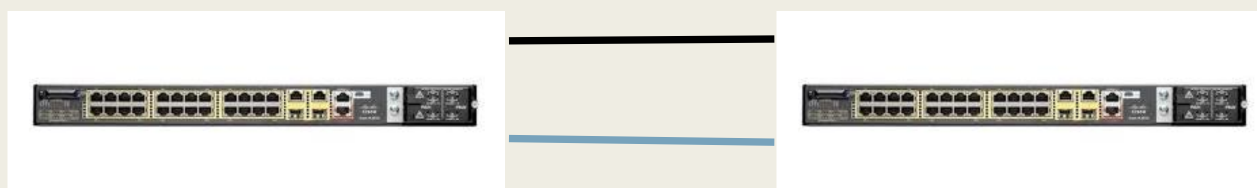
SPANNING TREE PROTOCOL

L2 switching

Introduction

- What happens when two links connect two switches?
  - *Loop (data frame will circulate in the loop formed by the two links and the network suffers broadcast storm)*
- Some cases we want to run two connection to provide redundancy (one link active and the other link passive)

STP (802.1D)
will prevent the loop and it
Is ON by default.



BPDU

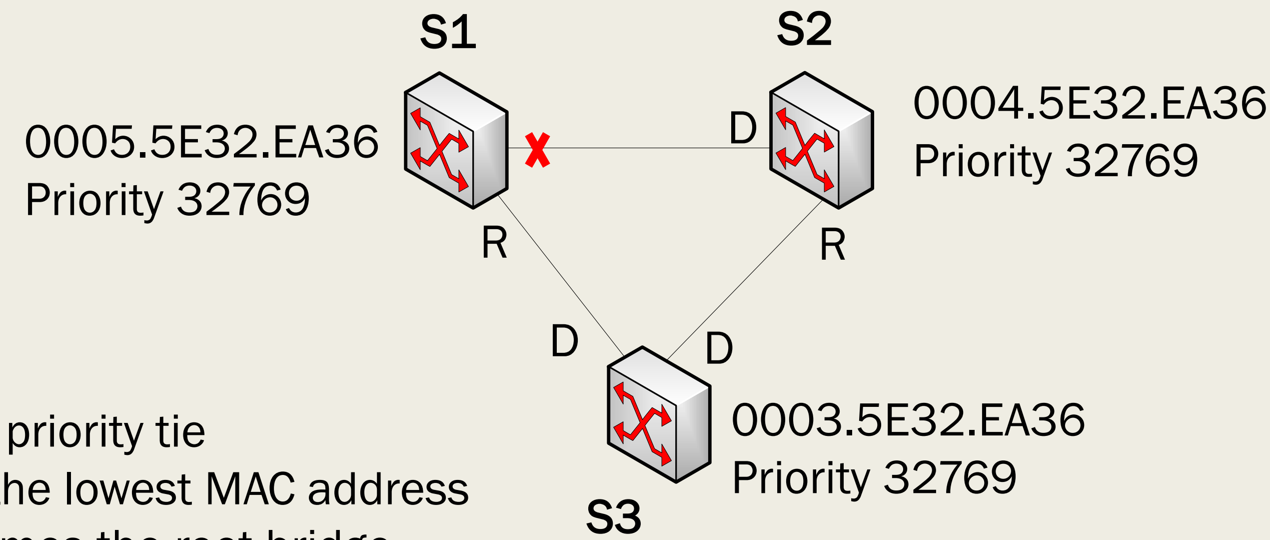
- Switches exchange BPDU (bridge packet data unit) messages every 2 seconds to detect loops

STP process

- Switches elect their "boss", called root bridge by
  - *Lowest priority (default 32768)*
  - *MAC address if there is priority tie (lower MAC wins)*
  - *It is best advised the ICT engineer to manually set the root bridge to the most important switch in the network*
- All other switches then identify their root ports (the fastest link to the root bridge)
- Switches then identify designated ports (forwarding ports) and ports to be blocked to prevent loop

Example

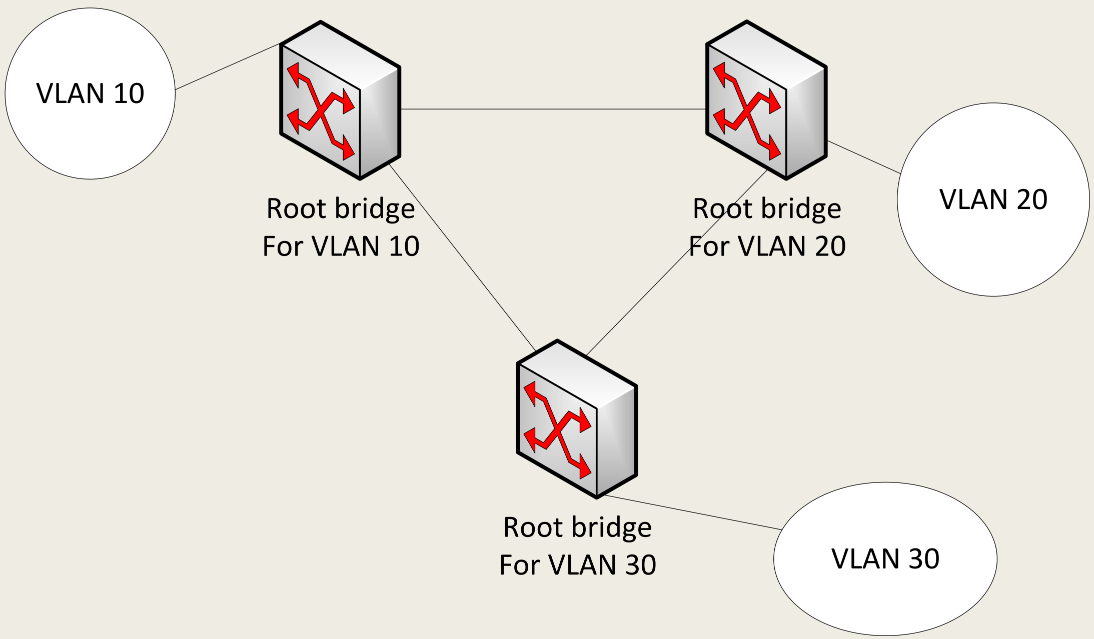
Link bandwidth	cost
10Gbps	2
1Gbps	4
100Mbps	19



1. There is priority tie
2. S3 has the lowest MAC address
3. S3 becomes the root bridge

Per VLAN STP

- It is possible to create different root bridges for each VLAN in cisco switches

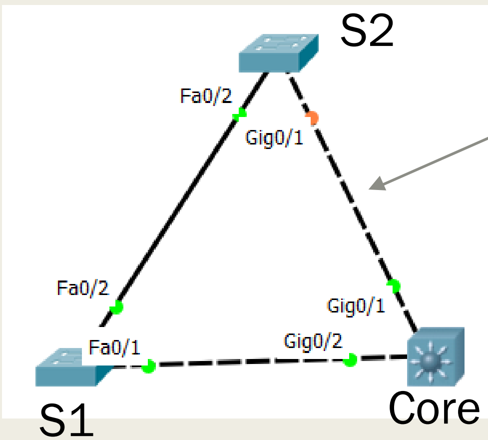


Rapid STP (802.1w)

- It is faster than the original STP
- Configured on all switches
- It enables faster convergence after network topology changes

Spanning tree lab

Assume all link are trunks



Spanning tree shuts down the fastest gigabit link in the network (not good)

```
core#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.6357.3074
             Cost        19
             Port        26(GigabitEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.FF25.7E47
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Root FWD 19        128.26   P2p
```

Root bridge is S1

Set the STP root bridge to core switch

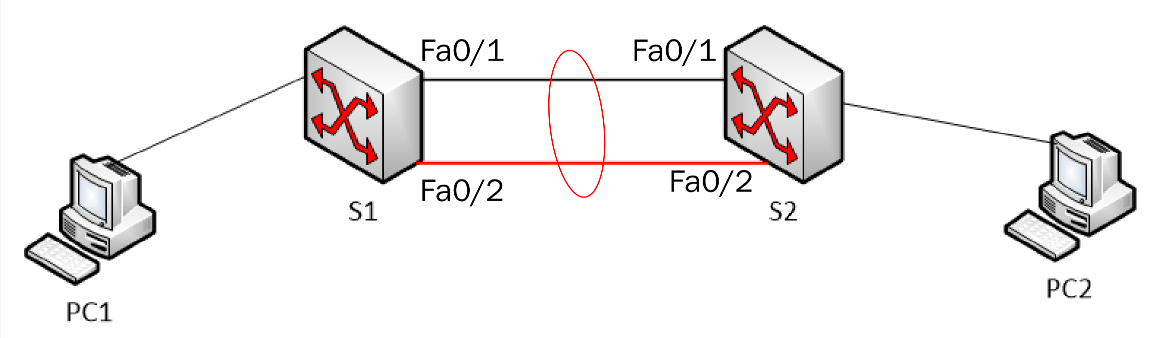
core(config)#spanning-tree Vlan 1 priority 4096

To speed up spanning mode transition stages (listening, learning, and forwarding) Enable rapid-STP as follows (for all switches in the network)

core(config)#spanning-tree mode rapid-pvst

Etherchannel

- Etherchannel is cisco proprietary link aggregation protocol
- The industry standard is IEEE 802.3ad L1LA
  - LACP (link aggregation control protocol) is the open protocol used for implementation
    - One side is active (starting aggregation) and the other passive (respond to aggregation)
- STP will treat the two aggregated links as one link




```
S1(config)#interface port-channel 1
S1(config)#interface range fa0/1-2
S1(config-if)#channel-group 1 mode active
```

```
S2(config)#interface port-channel 1
S2(config)#interface range fa0/1-2
S2(config-f)#channel-group 1 mode passive
```

```
Switch#show etherchannel summary

Group      Port-channel      Protocol      Ports
------+-------------+-----------+-----------------------------------------------
1          Po1(SU)           LACP          Fa0/1(P) Fa0/2(P)
```

Troubleshoot L2 networks

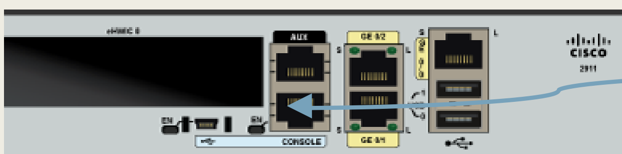
- Check switch port is enabled
- Verify VLAN and trunk configuration
- Check loops and STP configuration
- Check MAC-address table for learned devices
- Check port status, MTU and duplex
- Monitor traffic using interface counter statistics

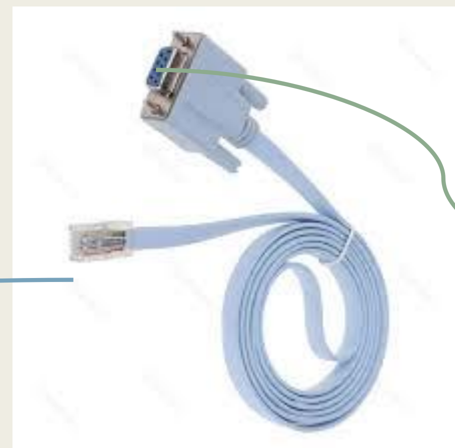
BASIC ROUTER CONFIGURATION

L3 networking

Connecting laptop to switch console port

Router console port





Remote management using telnet

Switch Gigabit port
IP address assign

Basic configurations

- Hostname

```
Switch(config)#hostname FINANCE
```

- Interface IP configuration

```
FINANCE(config)#int fa0/1
FINANCE(config-if)#ip address 192.168.50.1 255.255.255.192
```

- Remote management (telnet)

```
FINANCE(config)#line vty 0 15
FINANCE(config-line)#login local
FINANCE(config)#username jama privilege 15 secret cisco
FINANCE(config)#enable secret cisco
```

- Running-config and startup-config

```
FINANCE#copy running-config startup-config
```

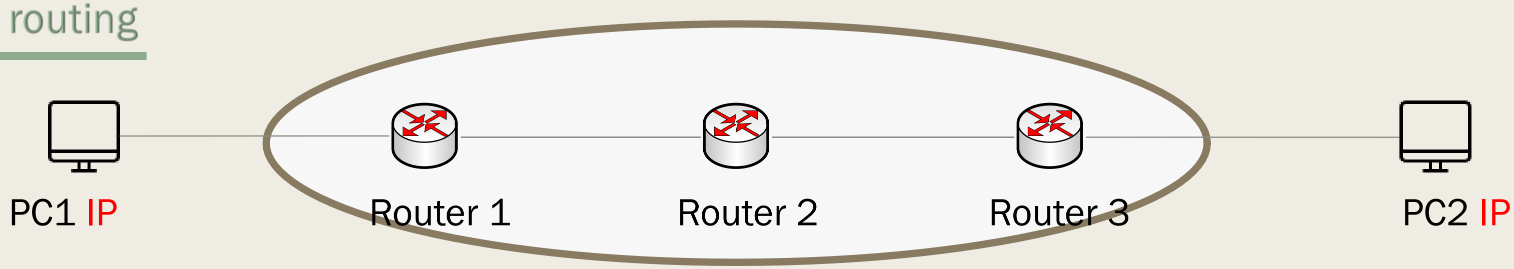
IP ROUTING

L3 networking

What is IP routing?

Mail routing

Data routing



Routing protocols types

- Routing protocols forward IP traffic from one router (hop) to the next neighboring router (hop) using the best path between source and destination
- Two types of routing protocols
  - ***Static routing*** *in which the ICT engineer manually configures*
  - ***Dynamic routing*** *protocols in which the routers dynamically configure themselves based on messages they exchanges. The ICT engineer only enables the routing protocols and adds the network addresses*

Which routing protocols we will learn

- Static routing
- OSPF (open shortest path first) which is dynamic routing protocol
- BGP (border gateway protocol)

Where do routers store the routing information?

- Router keeps routing database into routing tables

- In cisco networking, the most important command you need to remember is
  - *Show ip route*

Pure Training Center

Understand the routing table

```
     192.168.50.0/24 is variably subnetted, 5 subnets, 4 masks
S       192.168.50.0/26 [1/0] via 192.168.50.97
C       192.168.50.96/27 is directly connected, GigabitEthernet0/0
L       192.168.50.98/32 is directly connected, GigabitEthernet0/0
C       192.168.50.144/28 is directly connected, GigabitEthernet0/1
L       192.168.50.145/32 is directly connected, GigabitEthernet0/1
```

```
O          172.16.50.12/30 [110/2] via 172.16.50.17
```

OSPF

Destination network

AD

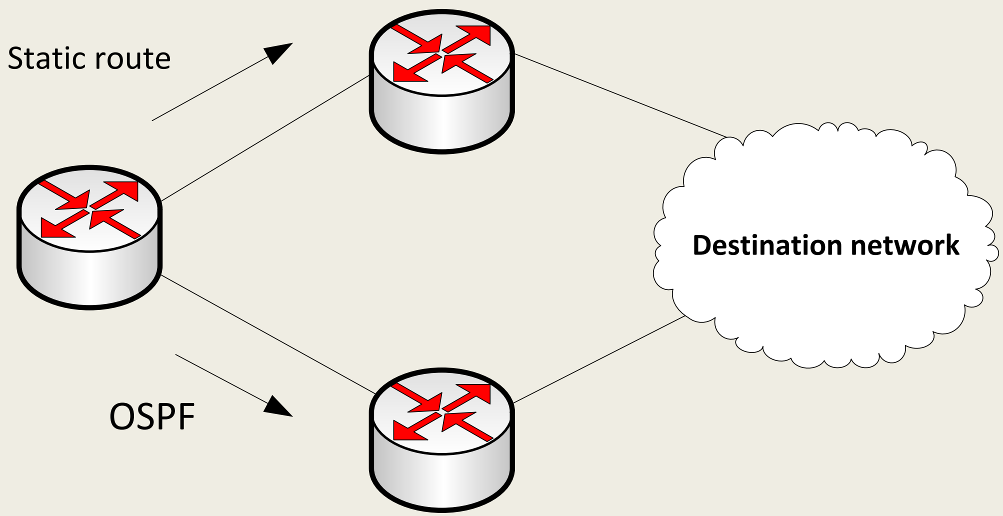
Next hop/ Exit gateway

The first thing the router places in its routing table is directly connected networks

Then router will learn only networks added by routing protocol and adds them on its routing table

Administrative distance (AD)

- It is a number which tells the best route to take when we have different routing protocols ➔ lowest AD wins

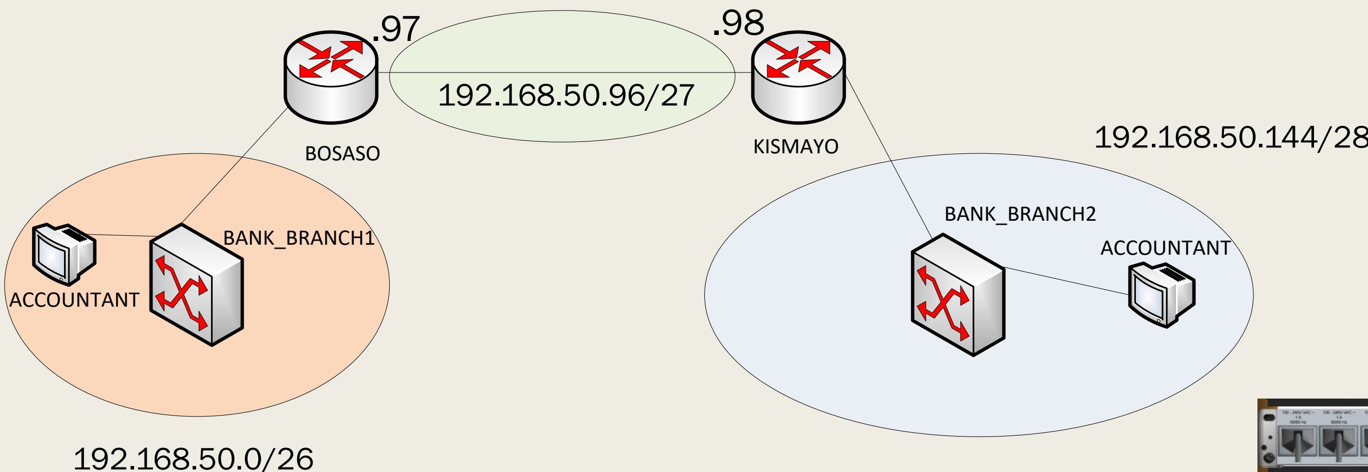


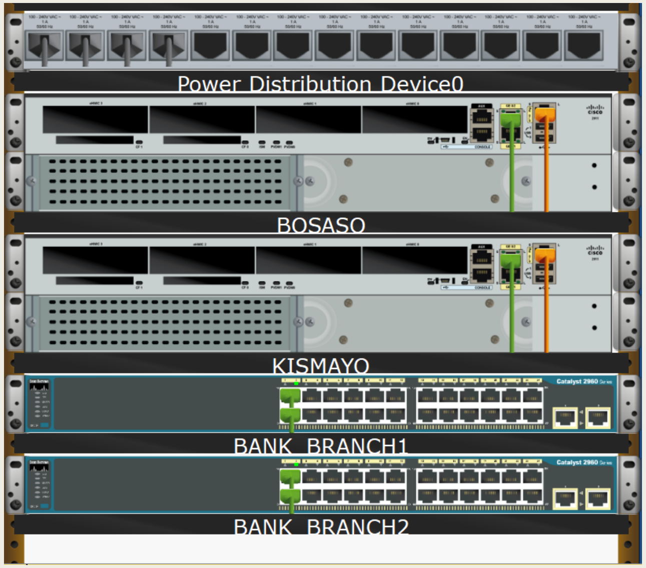
Routing protocol	AD
Directly connected	0
Static route	1
OSPF	110

STATIC ROUTING

IP routing

Static routing LAB





Ip route [destination network address] [destination subnet mask] [next hop]

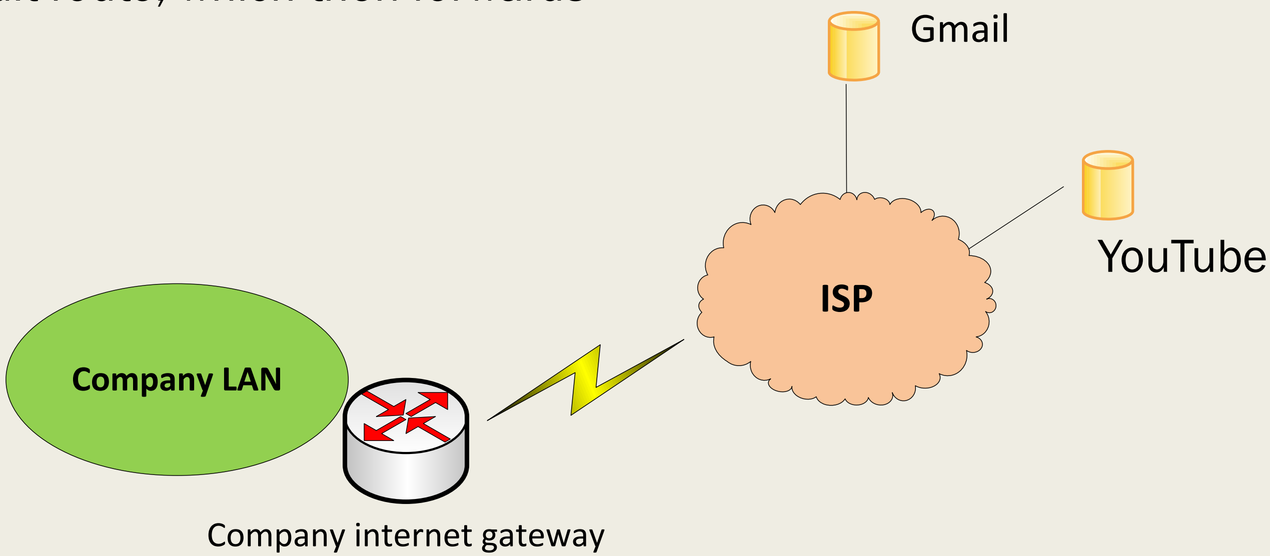
For example, to configure KISMAYO branch route to BOSASO router

```
BOSASO#ip route 192.168.50.144 255.255.255.240 192.168.50.98
```

Default route

Default route is used to send traffic to any IP address on the internet

If a user in company LAN wants to reach the internet, the traffic is
Sent to the default route, which then forwards



Ip route 0.0.0.0 0.0.0.0 ISP link

IPv6

Introduction

- So far in this course we have been using IPv4 to address our networks and devices
- We learnt that IPv4 is 32-bit number that was divided into four parts each of 8-bits
- IPv4 address is divided into network part and host part. Subnet masks tell which part is network and which part is host

IPv6 is 128-bit address

4-bits form one hexadecimal (A = 1010)

IPv6 is thus 32-hexadecimal numbers

2001:1A45:2345:BC34:001A:0000:0000:000C

Hexadecimal system (base-16)

0	0000	8	1000
1	0001	9	1001
2	0010	A	1010
3	0011	B	1011
4	0100	C	1100
5	0101	D	1101
6	0110	E	1110
7	0111	F	1111

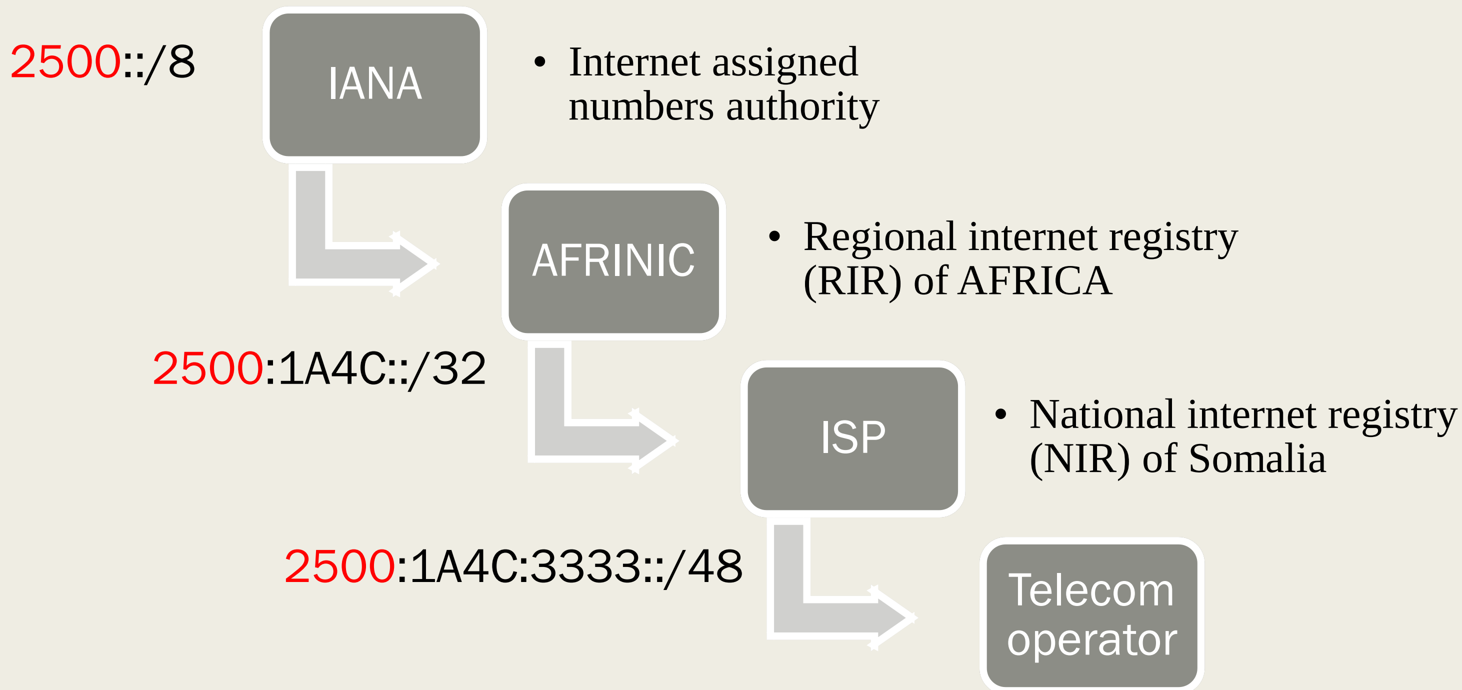
Writing IPv6 in simplified way

Omit leading zeros
Replace consecutive hex-0 with :: but only once

2001:1A45:2345:BC34:001A:0000:0000:000C = 2001:1A45:BC34:1A::C

Global unicast addresses

- IPv6 addresses that start with 2000::/3 prefix are called global unicast addresses
- These addresses are routable through the internet and can be assigned to hosts without NAT
- IANA assigns global unicast addresses



Subnet global unicast addresses

- From the previous slide, the telecom operator purchased the prefix 2500:1A4C:3333::/48
- But an IPv6 is 128-bits, this leaves 80 bits for the host
- When subnetting IPv6, the prefix is assigned /64 and the host /64

Hence we can create the following subnet prefix from our site prefix
2500:1A4C:3333:0001::/64
2500:1A4C:3333:0002::/64
2500:1A4C:3333:0003::/64
2500:1A4C:3333:0004::/64
…

Terminology

Registry prefix	2500::/8
ISP prefix	2500:1A4C::/32
Site prefix	2500:1A4C:3333::/48
Subnet prefix	2500:1A4C:3333:0001::/64

Pure Training Center

Assign global unicast addresses to network devices

For a host to communicate through network, it needs

- IP address, subnet mask, default gateway, DNS

Methods for IPv6 global unicast address assignment

	Prefix	Host	Default gateway	DNS
Stateful DHCPv6	DHCP	DHCP	Router using NDP	Stateful DHCP
Stateless autoconfig	Router using NDP	Derived from MAC	Router using NDP	Stateless DHCP
Static	Local	Local	Router using NDP	Stateless DHCP
Static with EUI-64	Local	Derived from MAC	Router using NDP	Stateless DHCP

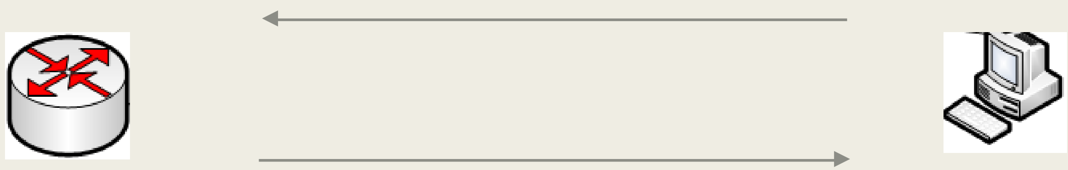
Stateful DHCPv6

- Stateful DHCPv6 keeps state information of each network host (leased IP address for example)
- Hosts send the multicast IPv6 address FF02::1:2/8 to find relay DHCP server

Stateless autoconfiguration

- Hosts learn prefix, prefix length and gateway using neighbor discovery protocol (NDP). The interface ID of the prefix is obtained using EUI-64 format
- An IPv6 configured router on the LAN receives RS (router solicitation) message from host and responds with RA (router advertisement) message

Sends IPv6 multicast RS message (FF02::2) to all IPv6 routers on the LAN



Router responds with RA listing prefix and its IPv6 as gateway
[Prefix is 2500:1A4C:3333:0001::/64
Gateway is 2500:1A4C:3333:0001::1/64]

Interface ID derived from host MAC
MAC is 48-bit ➔ expand to 64-bit
Insert 2-bytes into middle of MAC address to get 64-bit. Also flip 7th bit

MAC = 1C4D-705B-C40D
Interface ID = 1E4D:70FF:FE5B:C40D

Static IPv6

Network interface can obtain its IPv6 address statically by

- Statically configuring the entire 128-bit address
- Configuring the 64-bit prefix and calculating the interface ID using EUI-64

Other unicast addresses

Unique local

- Similar to IPv4 private addresses and are not routable through the internet
- Starts with FD00::/8 hexadecimal

FD	Random 40-bits	Subnet 16-bits	Interface ID using EUI-64

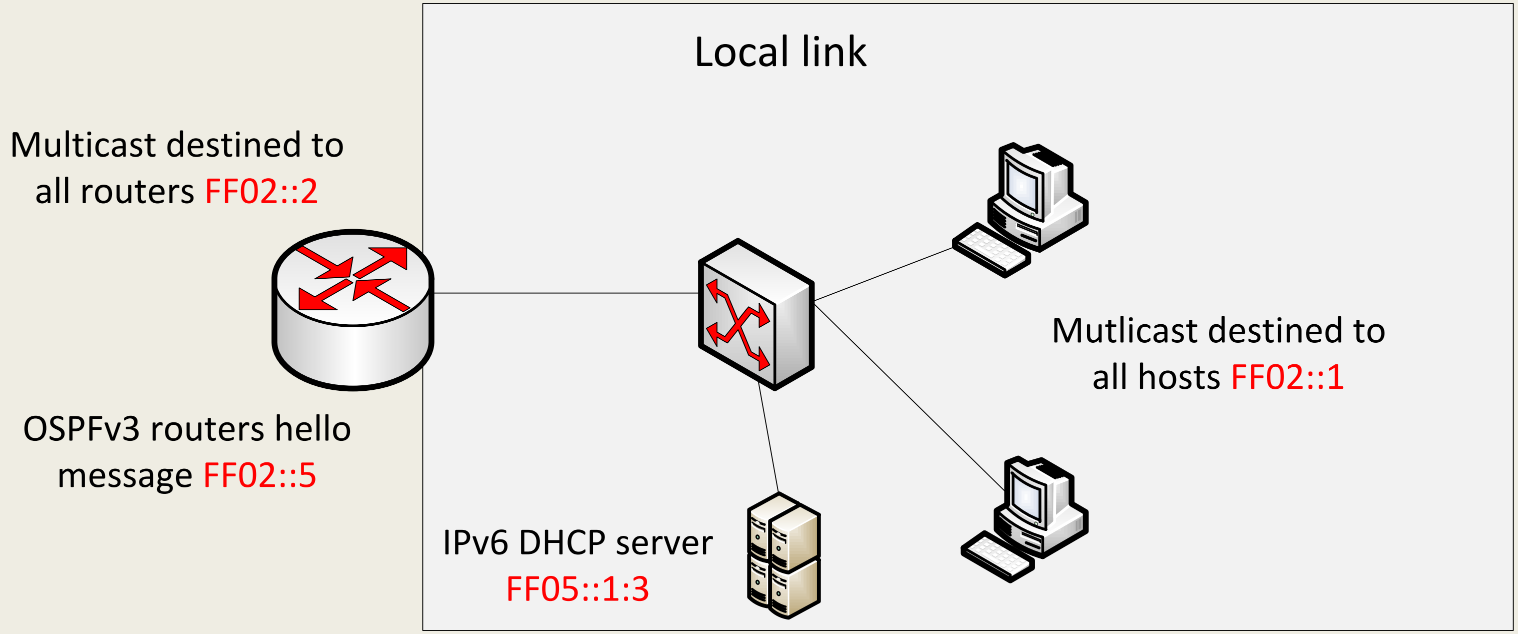
Link local

- Starts with FE80::/10 and used within local subnets (routers do not forward)
- All network devices automatically calculate it and used in the first packet transmission

FE80	54-bits all zeros	Interface ID using EUI-64

Special IPv6 multicast addresses

- IPv6 does not support broadcast as IPv4
- Common IPv6 multicast messages that start with FF are shown below

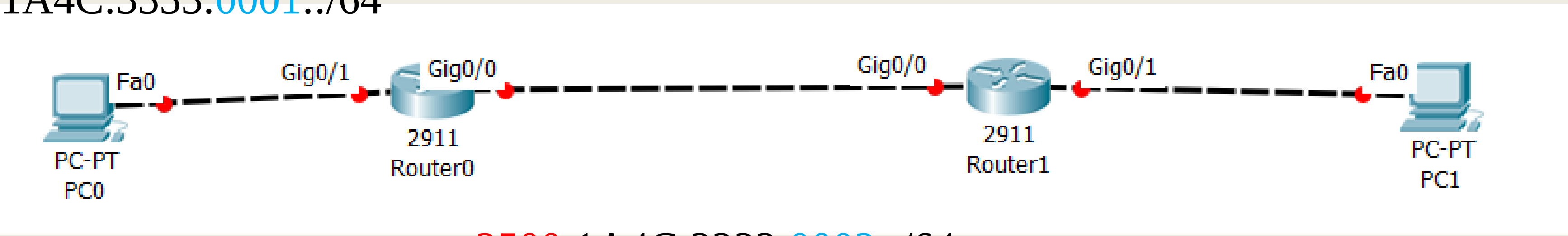


Example IPv6 configuration

For routers to forward IPv6 traffic the command ipv6 unicast-routing must be enabled

2500:1A4C:3333:0001::/64

2500:1A4C:3333:0003::/64



2500:1A4C:3333:0002::/64

```
Router0(config)#ip route ipv6 unicast-routing
Router0(config)#interface gi0/1
Router0(config-if)ipv6 address 2500:1a4c:3333:0001::/64 eui-64
```

```
Router0#show ipv6 interface brief
GigabitEthernet0/1                [up/up]
FE80::202:16FF:FE2D:6001
2500:1A4C:3333:1:202:16FF:FE2D:6001
GigabitEthernet0/2          [administratively down/down]
Vlan1                       [administratively down/down]
```

The remaining /64 is calculated from Router gi0/1 MAC address

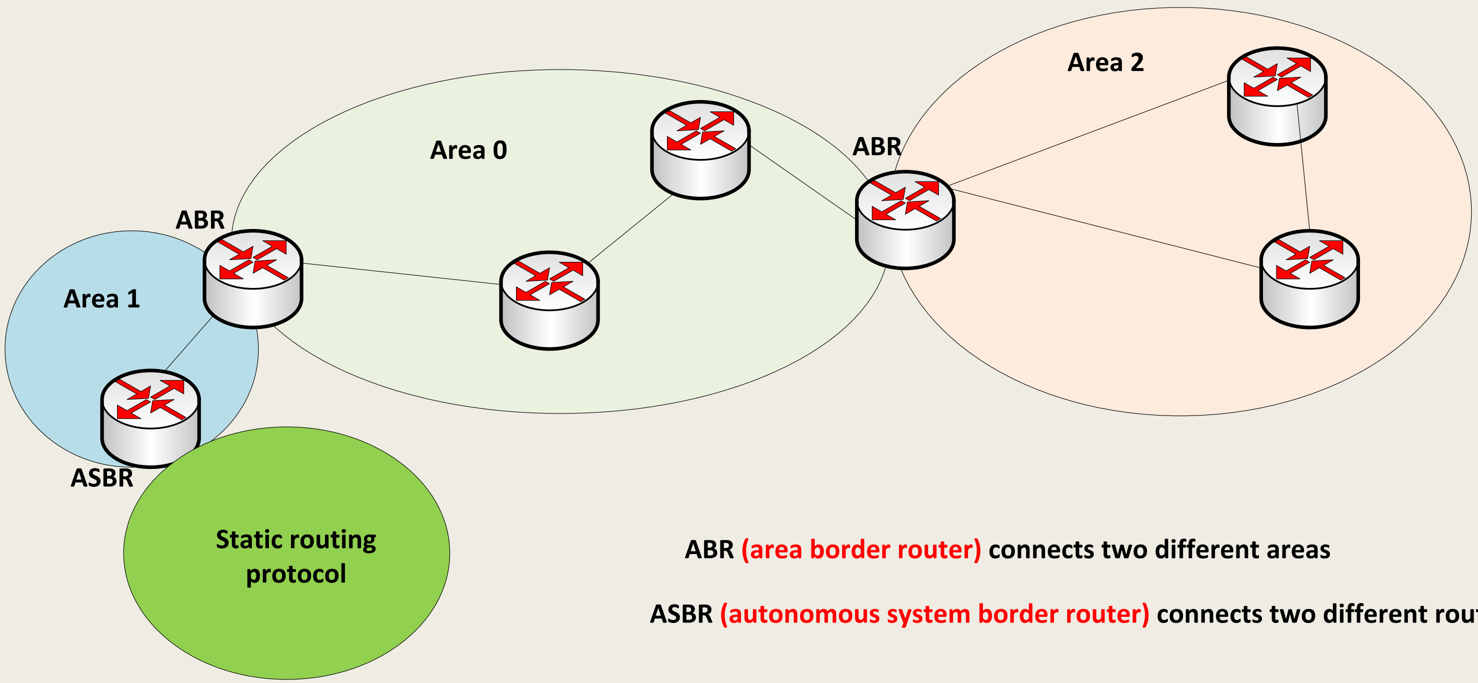
OSPF

Open shortest path first

What is OSPF?

- OSPF (open shortest path first) is an open routing protocol
- OSPF uses areas to logically group larger networks
- OSPF has area 0 in single area networks
- All other areas must connect to area 0
- OSPF routers use hello message to update routing table within area
  ➔ multicast to IP address 224.0.0.5
- OSPF supports VLSM

OSPF concepts



ABR (area border router) connects two different areas

ASBR (autonomous system border router) connects two different routing protocols

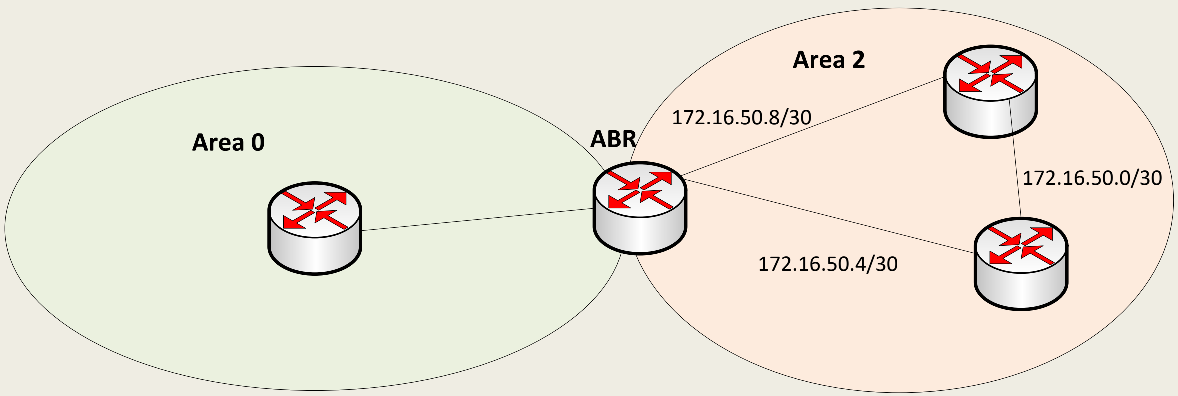
How OSPF routers form neighbors?

- Routers exchange hello messages once every 10 seconds for point-to-point links

Router ID:
Area ID:
Hello an dead timers:
Neighbors:
Subnet mask:

Route summarization (reverse of IP subnetting)

- In OSPF network where there are many routers, the routing table of each router gets large ➔ more processing power and memory
- Route summarization is the process of summarizing individual network addresses in an area into one network address ➔ done by ABR



172.16.50.0/24

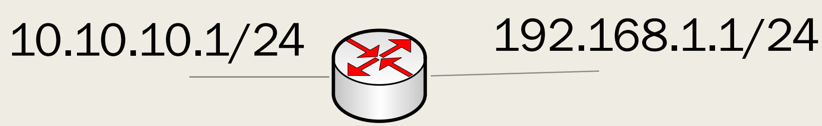
Wildcard bits

- OSPF uses wildcard instead of subnet mask when configuring
- Wildcard is the opposite of subnet mask
- Wildcard mask = 255.255.255.255 – subnet mask
- If the subnet mask is 255.255.0.0 the wildcard will be 0.0.255.255

- What is the wildcard of this subnet mask 255.255.255.252? 0.0.0.3
- 0.0.0.0 match everything (specific host)

Router ID

- Router ID is the OSPF name used to identify router running OSPF
- Best practice is to create loopback interface on the router and assigned designated IP address

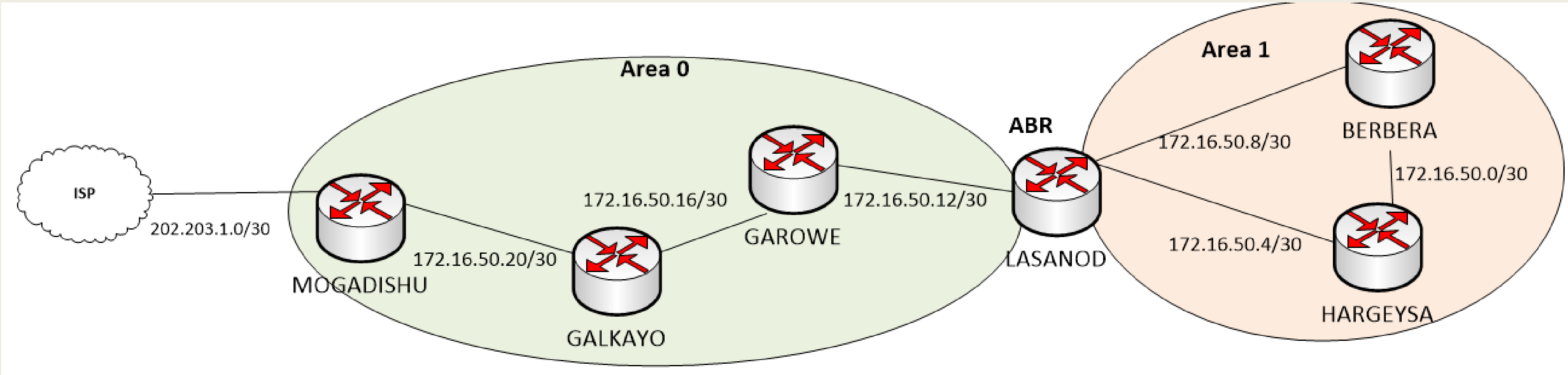


- The highest IP address on the physical interfaces becomes router ID
- If there is loopback interface, its IP address will become router ID

Useful show commands

Show ip route	To check routing table
Show ip protocols	To check which routing protocol is configured on router
Show ip interface brief	To check interfaces and IP assignments and status
Show ip ospf neighbor	To check formation of neighbors between routers in same area

OSPF lab



MOGADISHU(config)#router ospf 1
MOGADISHU(config)#network 172.16.50.20 0.0.0.3 area 0

```
MOGADISHU#show ip protocols

Routing Protocol is "ospf 1"  Protocol is OSPF
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 202.203.1.2  Router ID
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.50.20 0.0.0.3 area 0  Network being advertised in area 0
```

```
MOGADISHU#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.50.21      1   FULL/BDR        00:00:30    172.16.50.21    GigabitEthernet0/2
```

BGP

IP routing

Border gateway protocol (BGP)

- BGP is the routing protocol used by ISPs on the internet
- BGP is called exterior gateway routing protocol (EGP) as opposed to interior gateway protocols (IGP) such as OSPF

Differences between BGP which is an EGP and OSPF which is an IGP are summarized below

OSPF	BGP
Neighbors dynamically form between routers using hello message	Neighbors configured explicitly
Within an autonomous system	Between different autonomous systems
Hello multicast message	Uses TCP protocol port 179
Link state routing protocol	Path-vector routing protocol
Best path selection based on cost metric	Best path selection based on path attributes (PA)

Public IP address assignment

IANA

- Internet assigned numbers authority

41.223.0.0/16

AFRINIC

- Regional internet registry (RIR) of AFRICA

41.223.0.1/24

ISP

- National internet registry (NIR) of Somalia

41.223.0.1/29

Telecom operator

Public Autonomous system numbers (ASN) follow similar procedure of assignment (1 – 64511)

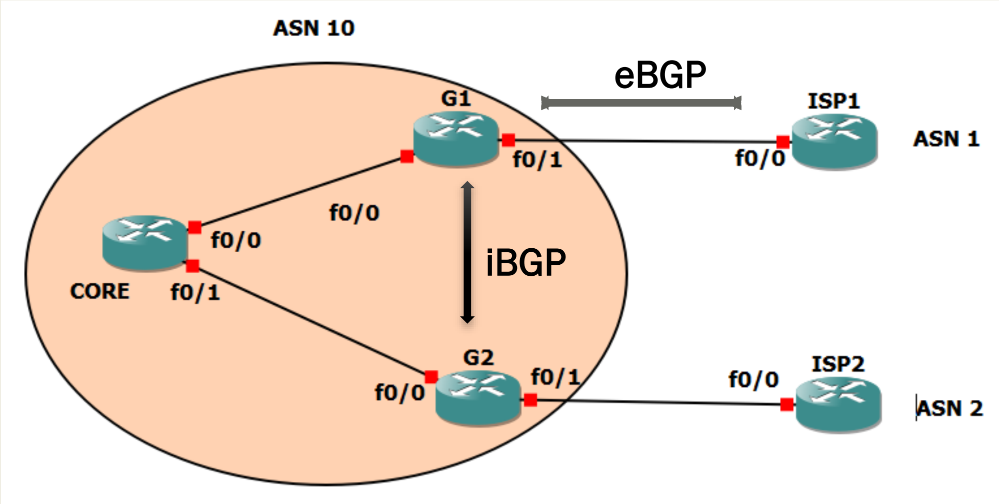
eBGP and iBGP

- eBGP is exterior border gateway protocol
- Used between different autonomous systems

G1(config)#router bgp asn 10
G1(config-router)#neighbor 1.1.1.1 remote-asn 1 (ISP1)

- iBGP is interior border gateway protocol
- Used within single autonomous system

G1(config)#router bgp asn 10
G1(config-router)#neighbor 2.2.2.2 remote-asn 10 (G2)



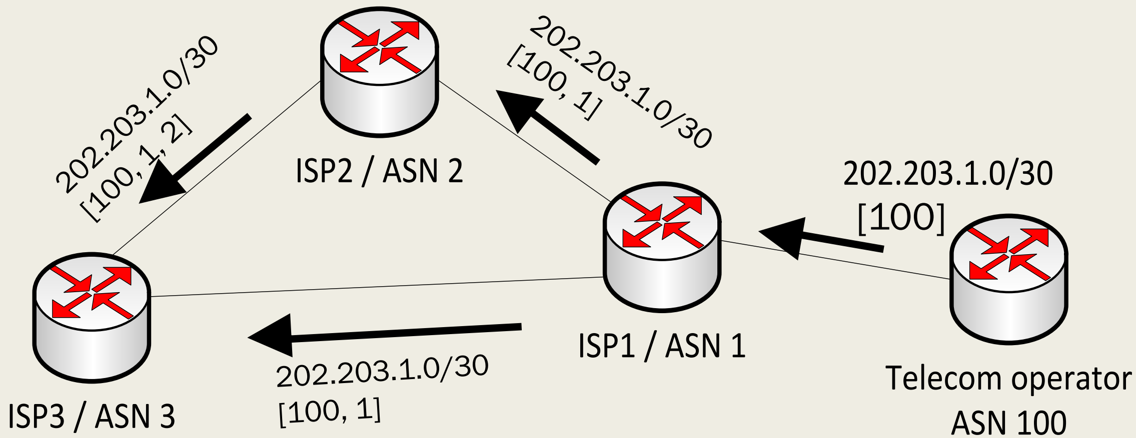
BGP path attributes (PA)

- IGP protocols such as OSPF use metric to determin best path. OSPF uses metric based on link bandwidth
- BGP uses more than just metric to determine best route
- When BGP is initially configured, by default routers used AS_SEQ PA to select the best route towards a prefix
- BGP PA are summarized in the table below

Next hop	How many hops the prefix is away?
AS_Path	How many ASNs the prefix is away?
Local preference	Used to influence best outbound route for all routers inside ASN
Origin	Routes injected from IGP
Multi-exit discriminator (MED)	Routers in different ASNs can influence in terms of BGP decisions

BGP route advertisement using AS_PATH PA

When a BGP router is adverting route through eBGP it addes on its ASN

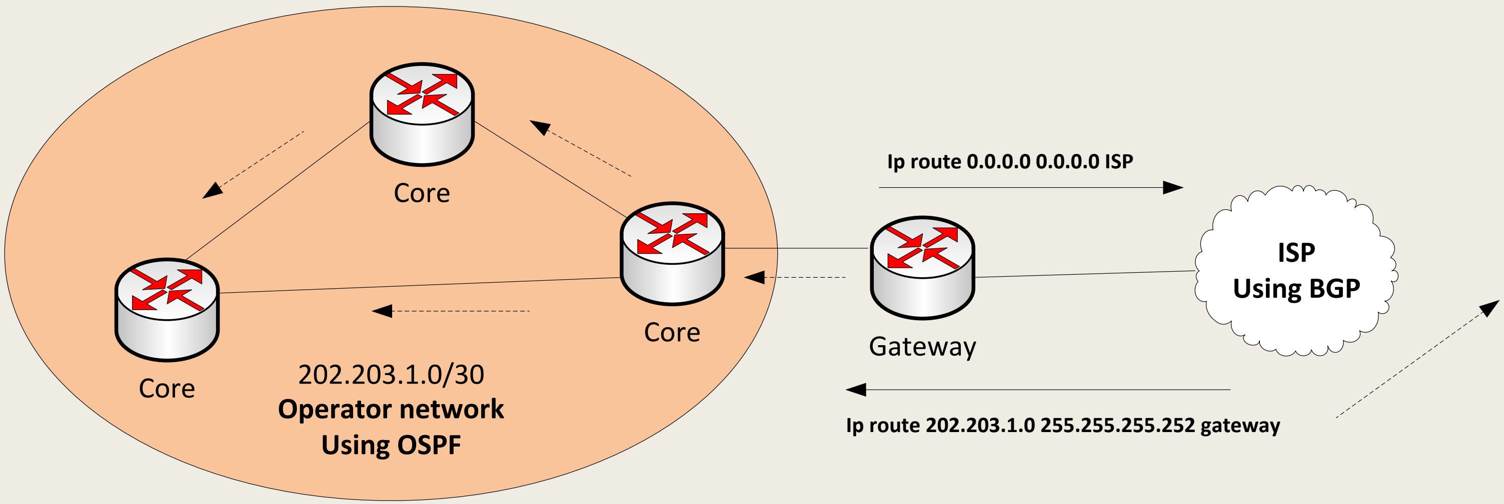


ISP3 learn two route for the prefix 202.203.1.0/30
It add the lower route to its BGP table as best path because it has small number of ASN [100,1]

Rationale for using BGP between enterprise and ISP

Case A: single outbound route towards the internet

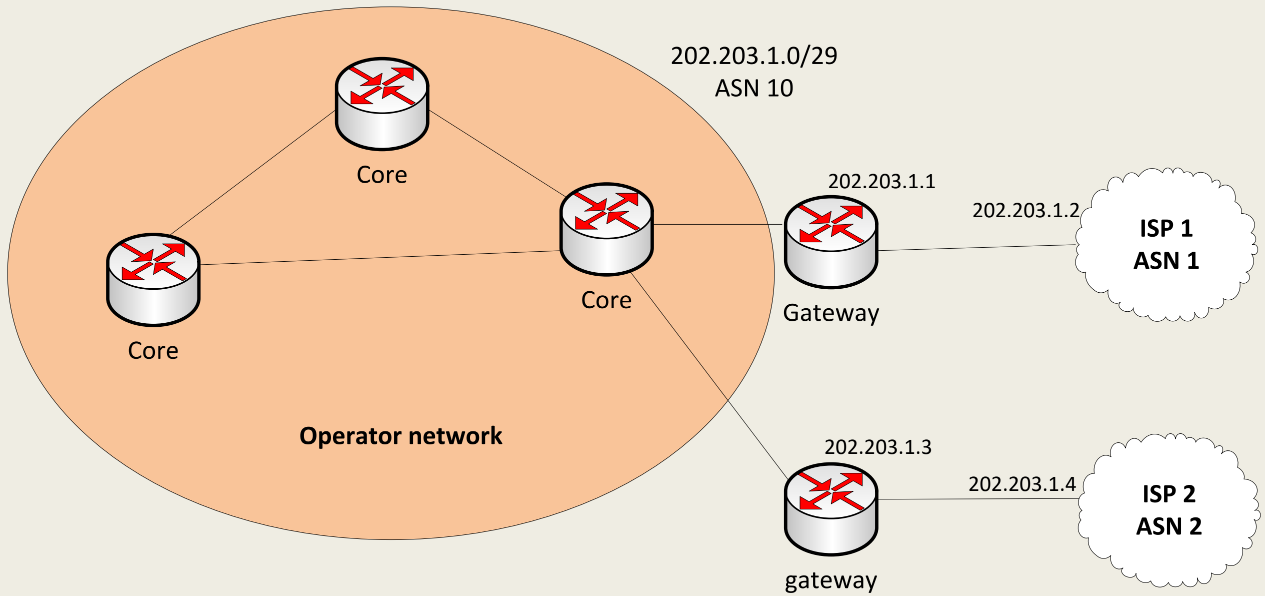
In this case static route and default route would be enough, and BGP is not necessary



Rationale for using BGP between enterprise and ISP

Case B: more that two outbound routes towards the internet

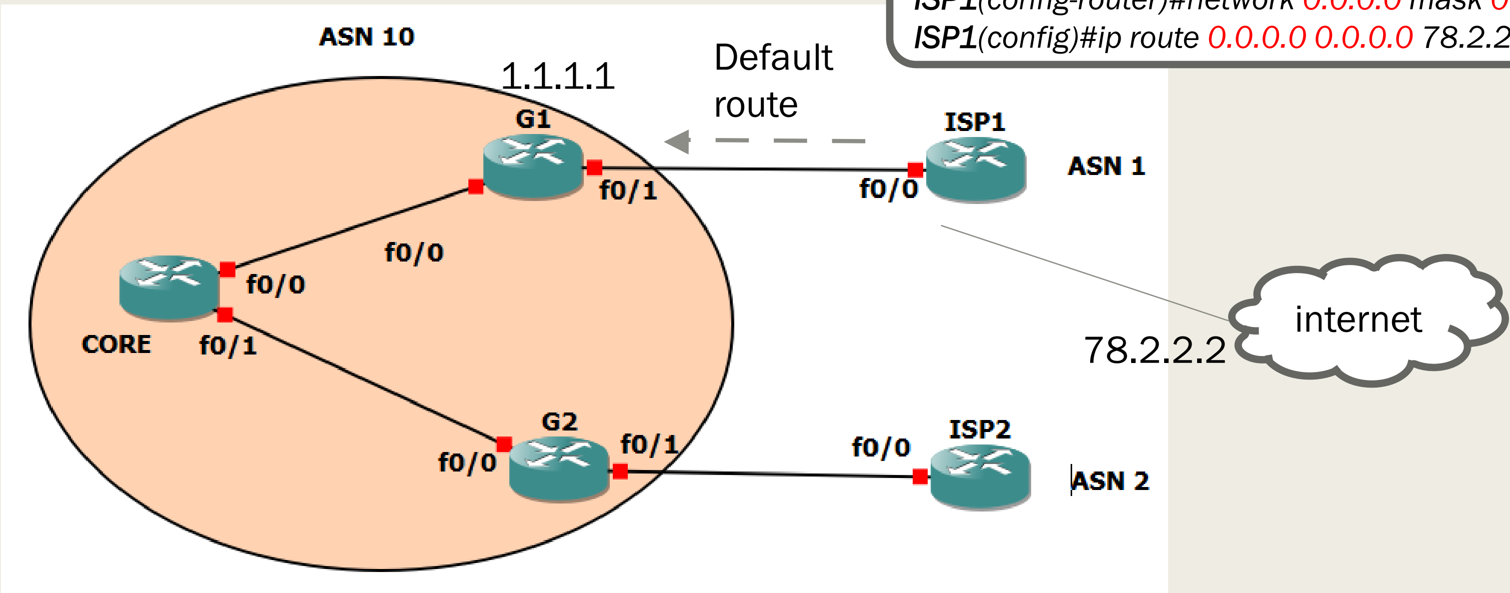
BGP normally used when there is more than one outbound
Route towards the internet, and one path is to be preferred
Over another for specific destinations in the internet

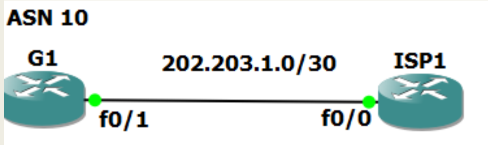


Internet default route update by ISP through BGP

- In our example, the enterprise has contracted to get default route through BGP from both ISP1 and ISP2
- We only show for ISP1, but the configuration is similar for ISP2

```
ISP1(config)#router bgp 1
ISP1(config-router)#neighbor 1.1.1.1 remote-asn 10
ISP1(config-router)#network 0.0.0.0 mask 0.0.0.0
ISP1(config)#ip route 0.0.0.0 0.0.0.0 78.2.2.2
```





Internet default route update by ISP through BGP

ISP1#show ip route

Gateway of last resort is 78.2.2.2 to network 0.0.0.0

```
     202.203.1.0/30 is subnetted, 1 subnets
C       202.203.1.0 is directly connected, FastEthernet0/0
     78.0.0.0/30 is subnetted, 1 subnets
C       78.2.2.0 is directly connected, Loopback0
S*   0.0.0.0/0 [1/0] via 78.2.2.2
```

G1#show ip route

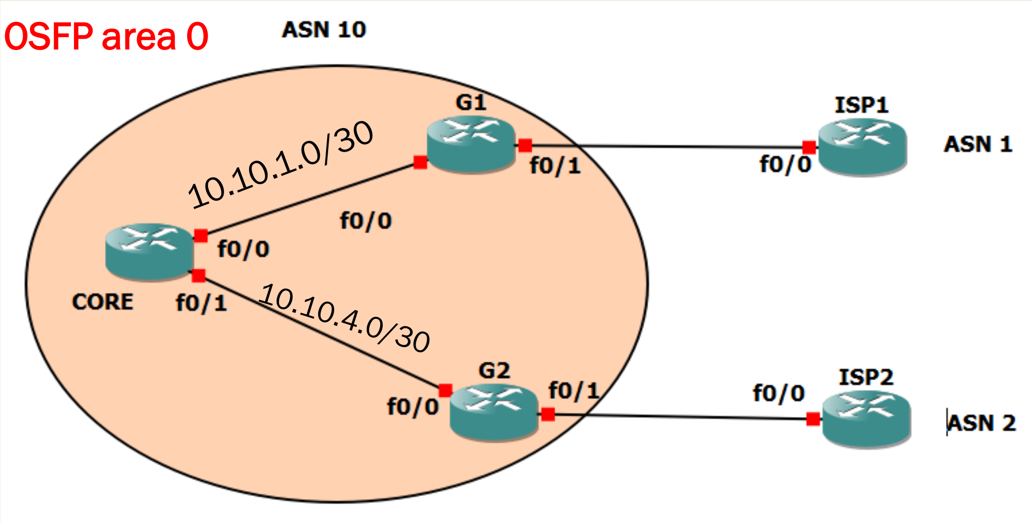
Gateway of last resort is 202.203.1.2 to network 0.0.0.0

```
     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/11] via 10.10.1.1, 02:16:33, FastEthernet0/0
     2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2 is directly connected, Loopback0
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/21] via 10.10.1.1, 02:16:23, FastEthernet0/0
     202.203.1.0/30 is subnetted, 1 subnets
C       202.203.1.0 is directly connected, FastEthernet0/1
     10.0.0.0/30 is subnetted, 2 subnets
C       10.10.1.0 is directly connected, FastEthernet0/0
O       10.10.1.4 [110/20] via 10.10.1.1, 02:16:35, FastEthernet0/0
B*   0.0.0.0/0 [20/0] via 202.203.1.2, 01:48:15
```

Advertising inbound routes to the ISP

- The ISP needs to learn public IP prefix the customer is using ➔ the customer advertises that prefix to the BGP
- The customer is using IGP such as OSPF internally ➔ OSPF redistribution into BGP

```
G1(config)#ip prefix-list 10-10 seq 5 permit 10.10.1.0/29 le 31
G1(config)#route-map PUBLIC permit 10
G1(config-route-map)#match ip add prefix-list 10-10
G1(config)#router bgp 10
G1(config-router)#redistribute ospf 1 route-map PUBLIC
G1(config-router)##aggregate-address 10.10.1.0 255.255.255.248 summary-only
```



ISP1#show ip bgp

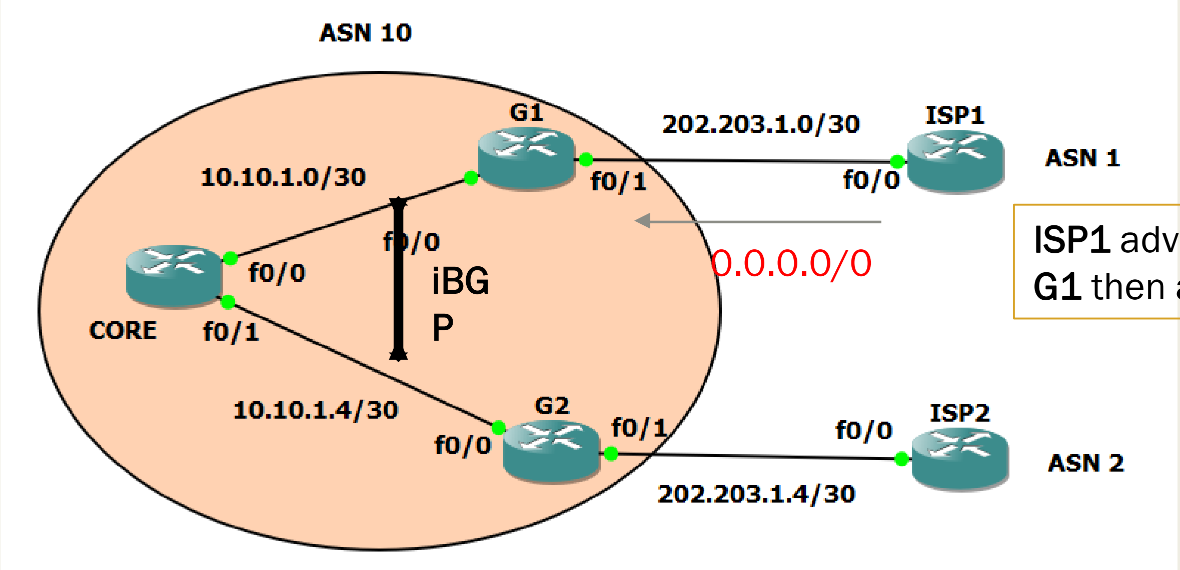
Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.10.1.0/30	202.203.1.1	0		0	10 ?
*> 10.10.1.4/30	202.203.1.1	20		0	10 ?

To learn single route for the entire prefix, the Aggregate-address will give

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.10.1.0/29	202.203.1.1	0		0	10 i

Pure Training Center

Next hop reachability with iBGP



ISP1 advertises default route to **G1** using eBGP
G1 then advertises default route to **G2** using iBGP

```
G2#    Network          Next Hop            Metric LocPrf Weight Path
     * i0.0.0.0         202.203.1.2              0    100      0 1 i
```

202.203.1.2 is the fa0/0 of **ISP1**

```
G2#ping 202.203.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.203.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

→ Reachability fail

NAT

Network address translation

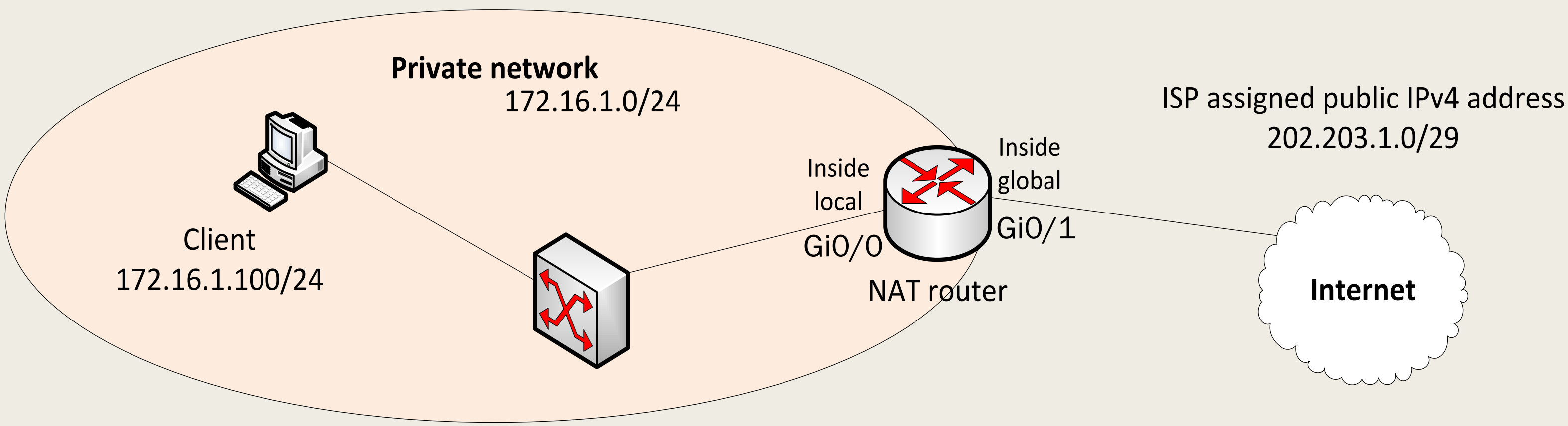
Private and public IPv4 addresses

- Private IP addresses are not routable on the internet. They are used within the organization

Class	Private IP address range
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

- Public IP addresses are used on the internet. NAT translates private IP to public IP when going to the internet

IP NAT Lab




```
NAT(config)#router ospf 1
NAT(config)#interface gi0/0
NAT(config-if)#ip nat inside
NAT(config)#interface gi0/1
NAT(config-if)#ip nat outside
NAT(config)#access-list 1 permit 172.16.1.0 0.0.0.255
NAT(config)#ip nat inside source list 1 interface gi0/1 overload
```

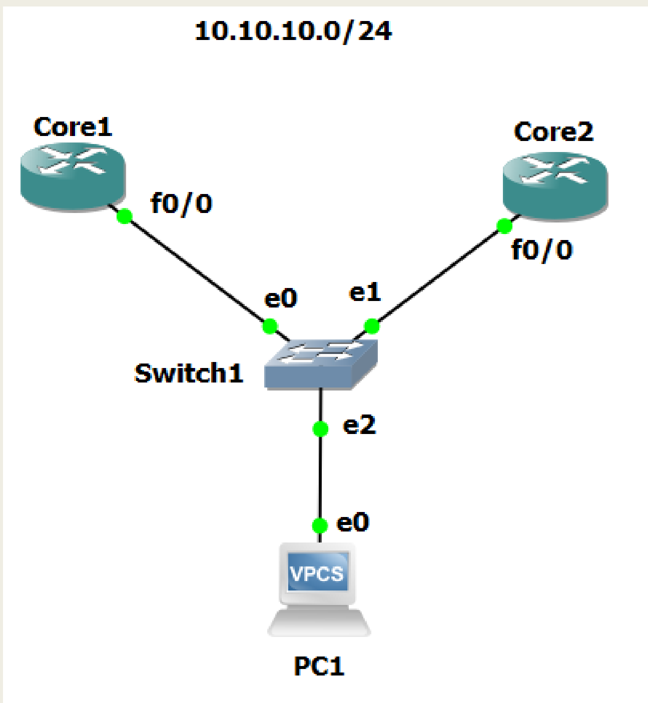
```
NAT#show ip nat translations
Pro  Inside global      Inside local        Outside local       Outside global
icmp 202.203.1.1:1      172.16.1.100:1      202.203.1.2:1       202.203.1.2:1
icmp 202.203.1.1:2      172.16.1.100:2      202.203.1.2:2       202.203.1.2:2
```

L3 TROUBLESHOOTING

IP routing

VRRP

- Virtual router redundancy protocol (VRRP) is open standard protocol for designing redundancy L3 networks
- One router becomes **master** and the other **backup**
- The router with the highest IP address or priority becomes master
- Widely used in telecommunication networks to establish redundant gateways facing the internet




```
core1(config)#interface fa0/0
Core1(config-if)#vrrp 1 ip 10.10.10.3

core2(config)#interface fa0/0
Core2(config-if)#vrrp 1 ip 10.10.10.3
```

```
Core1#show vrrp brief
Interface      Grp  Pri  Time  Own  Pre    State    Master addr    Group addr
Fa0/0            1  100  3609        Y     Backup   10.10.10.2     10.10.10.3
```

L3 IP troubleshooting

Issue	Solution
Destination host unreachable	Check routing table if destination network is missing Check PC default gateway
No internet connection	Check default route to the ISP
Request timeout	Firewall blocking return traffic
Other IP related issues	Check interface IP configuration and status

WIRELESS NETWORKING

Wireless LAN controller

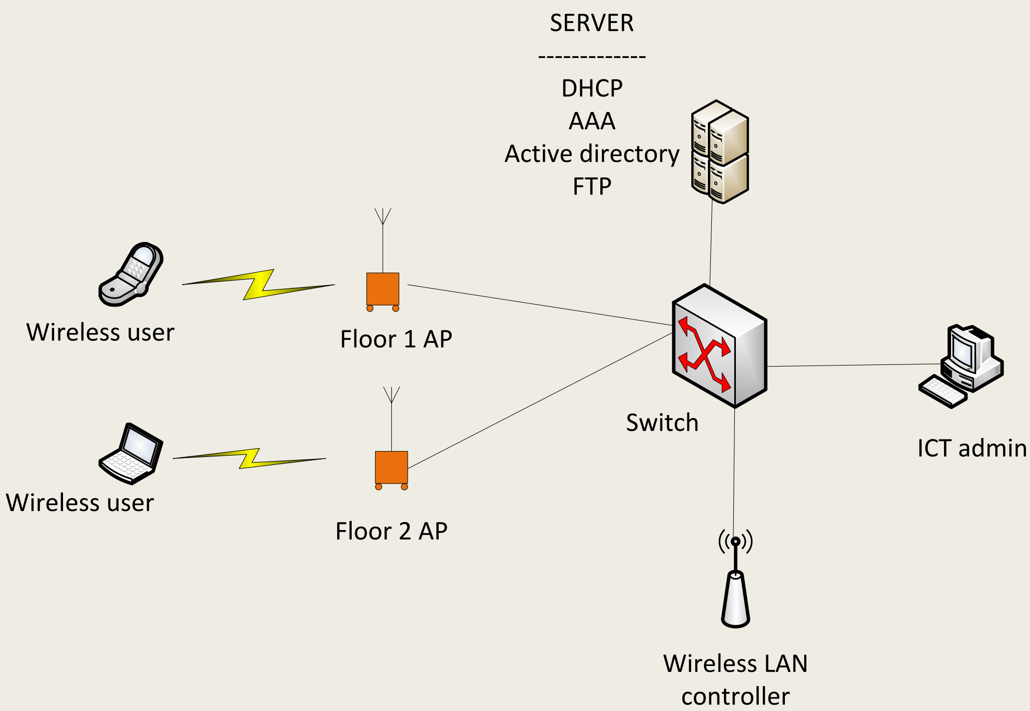
Objectives

Requirements

Continuous wireless internet coverage throughout the enterprise building

The objective is to have one WIFI controller, and several Access points placed at different floors of the enterprise Building.
As user moves within the building, seamless handover Between access point will take place.

LAB



Subnet to use 10.10.10.0/24

Server --- 10.10.10.1/24
Controller --- 10.10.10.2/24

DHCP
10.10.10.30 – 10.10.10.80

DHCP

- DHCP (dynamic host configuration protocol) is a service that automatically assigns an IP address to network client

- In production network, you can setup DHCP on
  - *Firewall*
  - *Windows server*

SECURITY

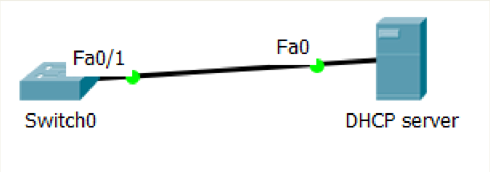
Network security

Network security systems

- AAA
  - *Authentication (username and password)*
  - *Authorization (what activities the user is allowed to do)*
  - *Accounting (auditing what a user has done on the network)*
- Firewall
- IPS (intrusion prevention system)
- Proxy server
- VPN (site-to-site, remote access)

DHCP snooping

- An illegal DCHP server assigns IP addresses to network clients



This configuration will allow only port fa0/1
Of the switch for DHCP server connection

```
switch0(config)#ip dhcp snooping
switch0(config)#interface fa0/1
Switch0(config-if)#ip dhcp snooping trust
```

Port security

Switch is a L2 device that learns and forwards MAC addresses
Switches store learned MAC address in MAC-address-table

The switch has limited memory to learn
And store MAC addresses

```
Switch0#show port-security interface fa0/1
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Restrict
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 5
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

In this configuration, maximum 5 MAC addresses
Will be allowed to be learnt on interface fa0/1

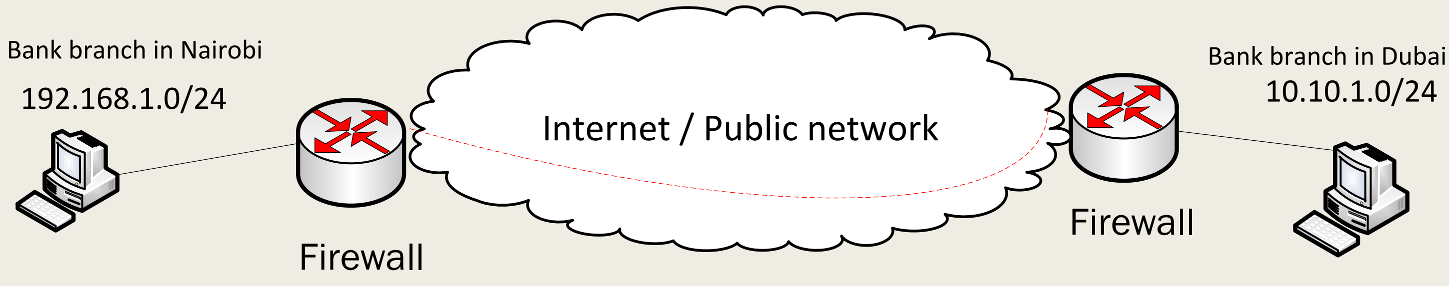
```
switch0(config)#interface fa0/1
Switch0(config-if)#switchport mode access
Switch0(config-if)#switchport port-security
Switch0(config-if)#switchport port-security maximum 5
Switch0(config-if)#switchport port-security violation Restrict
```

VPN

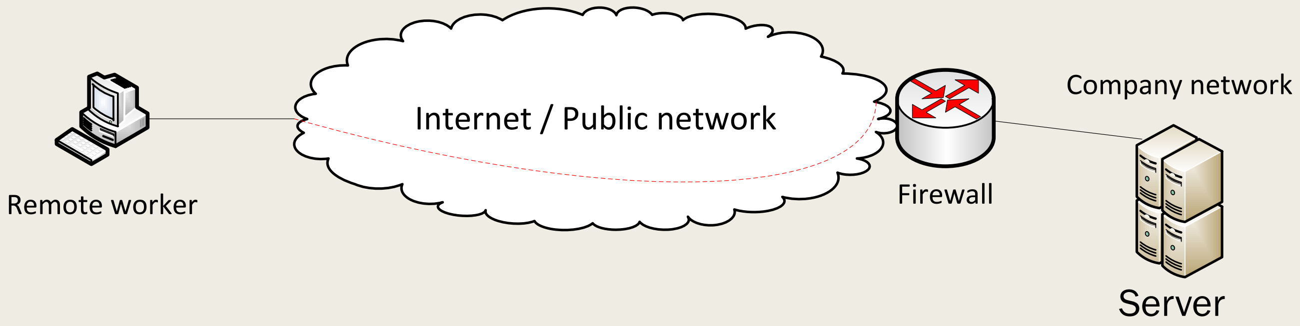
- VPN (virtual private network) is used to encrypt traffic passing through shared network such as the internet
- Two types
  - *Site-to-site VPN for encrypting traffic flowing between two company branches*
  - *Remote access VPN when accessing company internal server from the internet*

VPN types

Site-to-site VPN connecting two branches of the company over the internet

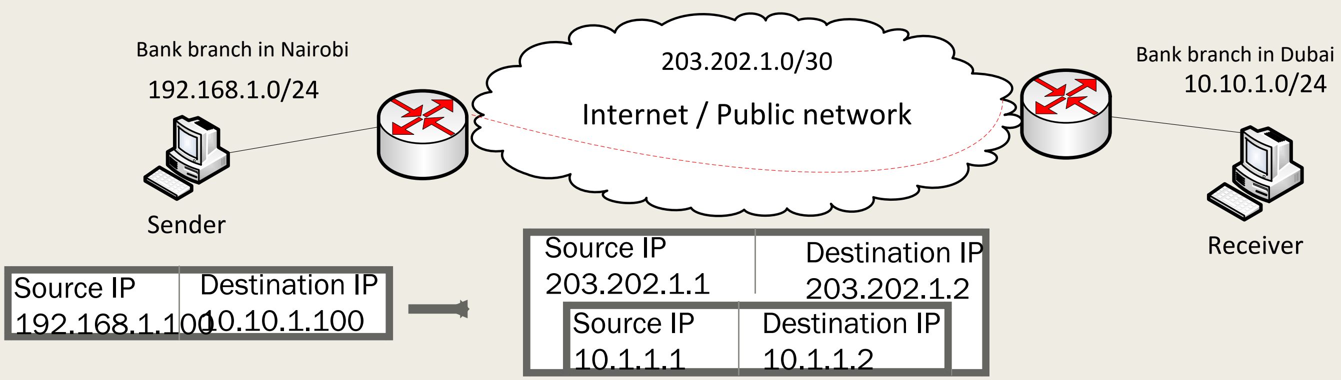


Remote access VPN for remote worker to access and manage internal server



Encapsulation

- GRE (generic routing encapsulation) is used to encapsulate private IP address inside public IP address over the VPN
- It does not provide security on the data

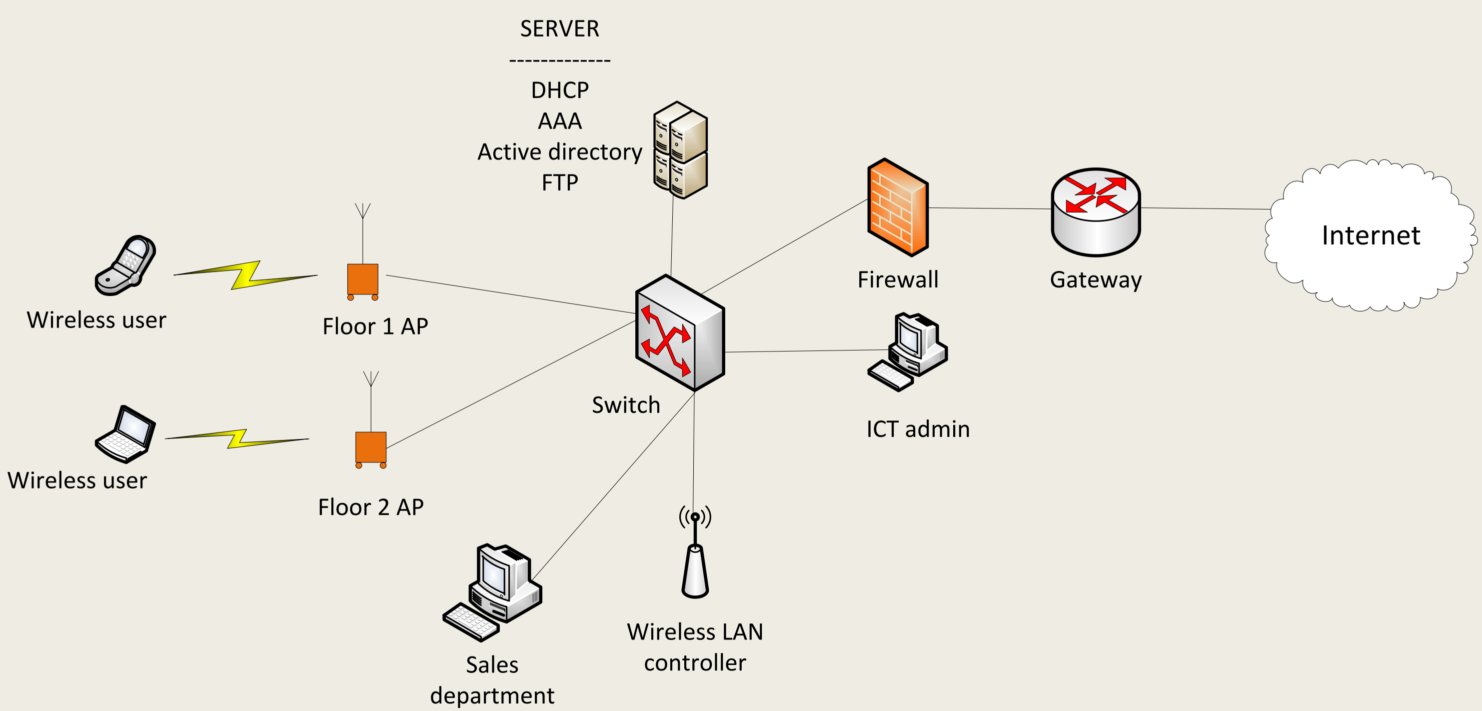


IPSEC

- IPSEC is used to secure data over the GRE tunnel (GRE tunnel sent over the IPSEC tunnel) ➔ VPN with IPSEC is secure VPN
- IPSEC is a collection of protocols that provide encryption and hashing over the VPN tunnel

Security feature	Definition
Confidentiality	Encryption using key
Integrity	Data not modified using MD5 for example
Authentication	Verification
Anti-replay	No duplicate packets

Firewall, IPS, proxy server



ACCESS LISTS

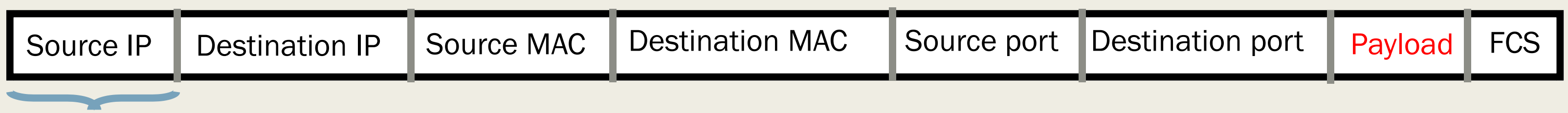
Security

What is an access list?

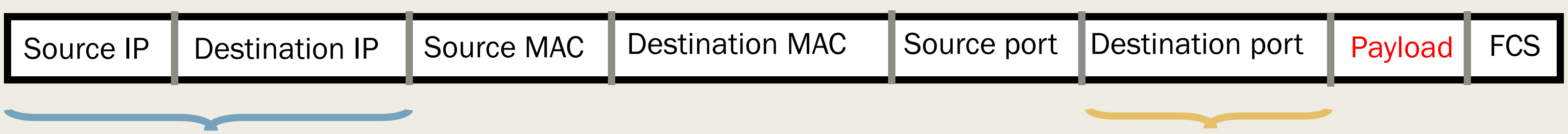
- ACL is filtering IP traffic
- Two types
  - *Standard ACL which filters IP traffic based on source IP address only ➔ applied close to the destination*
  - *Extended ACL which filters IP traffic based on source IP address, destination IP address, and destination port number ➔ applied close to the source*

Standard ACL vs extended ACL

- Standard ACL

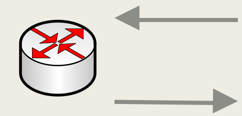


- Extended ACL



Access list rules

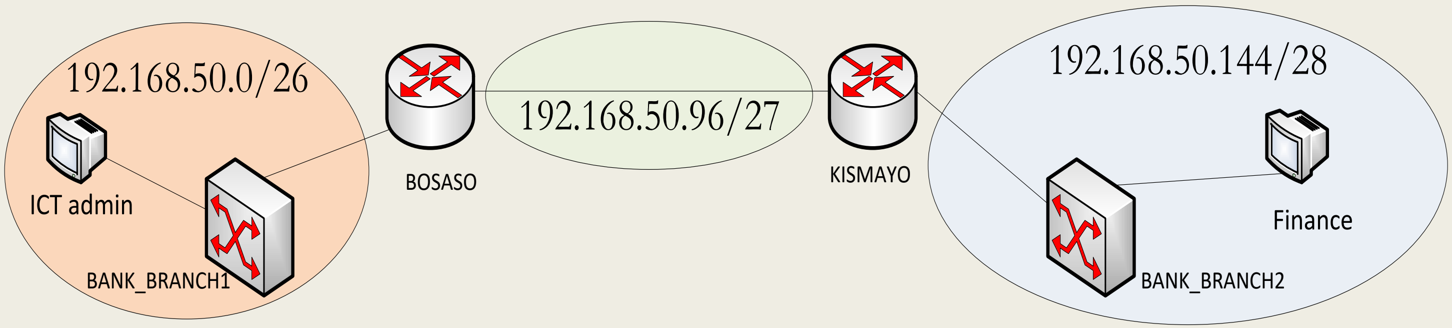
- One access list per interface, per protocol, per direction
- Direction
  - *Inbound (filter packets as they arrive at router interface)*
  - *Outbound (filer packets as they leave from router interface)*



- ACLs are processed from top to bottom ➔ there is implicit "deny any" at the bottom that will deny all traffic if you don't add permit statements on top

Standard access list example

- Deny/permit specific host or network to telnet to the router
- For example, permit only ICT admin to telnet to KISMAYO and BOSASO routers and deny another other telnet



Permit/deny [source IP] [source subnet]

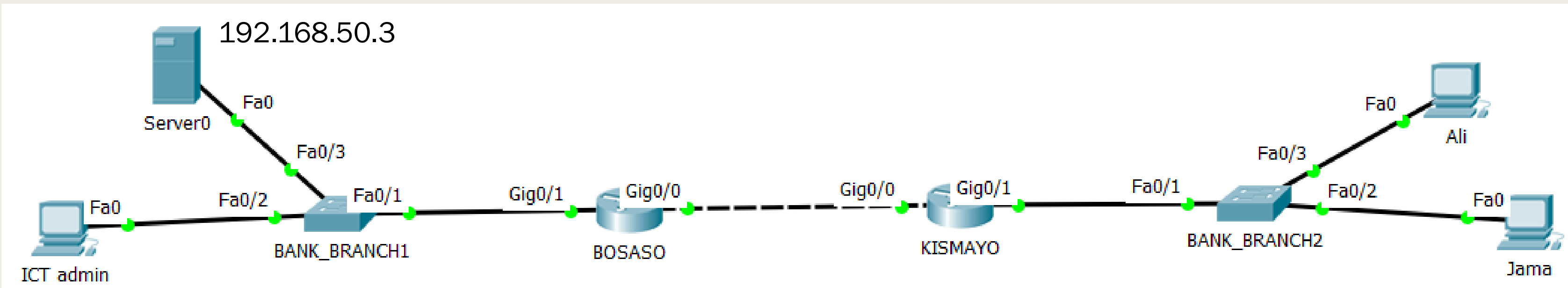
```
BOSASO(config)#ip access-list standard DENY_TELNET
BOSASO(config-std-nacl)#permit host 192.168.50.2
BOSASO(config)#line vty 0 15
BOSASO(config-line)#access-class DENY_TELNET in
```

```
BOSASO#show ip access-lists
Standard IP access list DENY_TELNET
        10 permit host 192.168.50.2
```

Pure Training Center

Extended access list example

- Deny KISMAYO branch network from accessing web server in BOSASO network



192.168.50.0/26

192.168.50.144/28

Permit/deny [source IP] [source subnet] [destination IP] [destination subnet] [protocol]

```
KISMAYO(config)#ip access-list extended DENY_HTTP
KISMAYO(config-ext-nacl)#deny tcp 192.168.50.144 0.0.0.15 host 192.168.50.3 eq 80
KISMAYO(config-ext-nacl)#permit ip any any
KISMAYO(config)#interface gi0/1
KISMAYO(config-if)#ip access-group DENY_HTTP in
```

VLAN TRAFFIC OVER CARRIER ETHERNET

WAN technologies

Introduction

Service providers can use Carrier Ethernet to interconnect different sites at different locations such as

- Mobile backhaul
- Remote site connection
- Internet service to customers

Traffic is carried across the CE by using VLANs. All other L2 protocols apply including STP

Other features of CE include

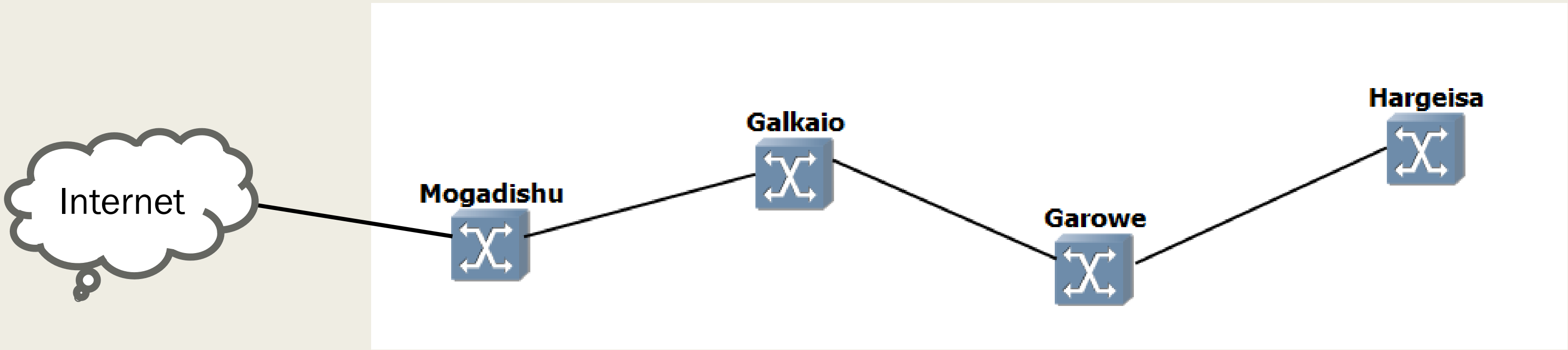
- OAM (operation, administration and maintenance)
- Scalability
- High speed (multi-gigabit)

Practice exercise

Requirement

The operator is connected to the internet at Mogadishu. It has been decided to deliver internet to Hargeisa

Configure VLAN 100 for transporting 20Mbps internet from Mogadishu to Hargeisa



Hint

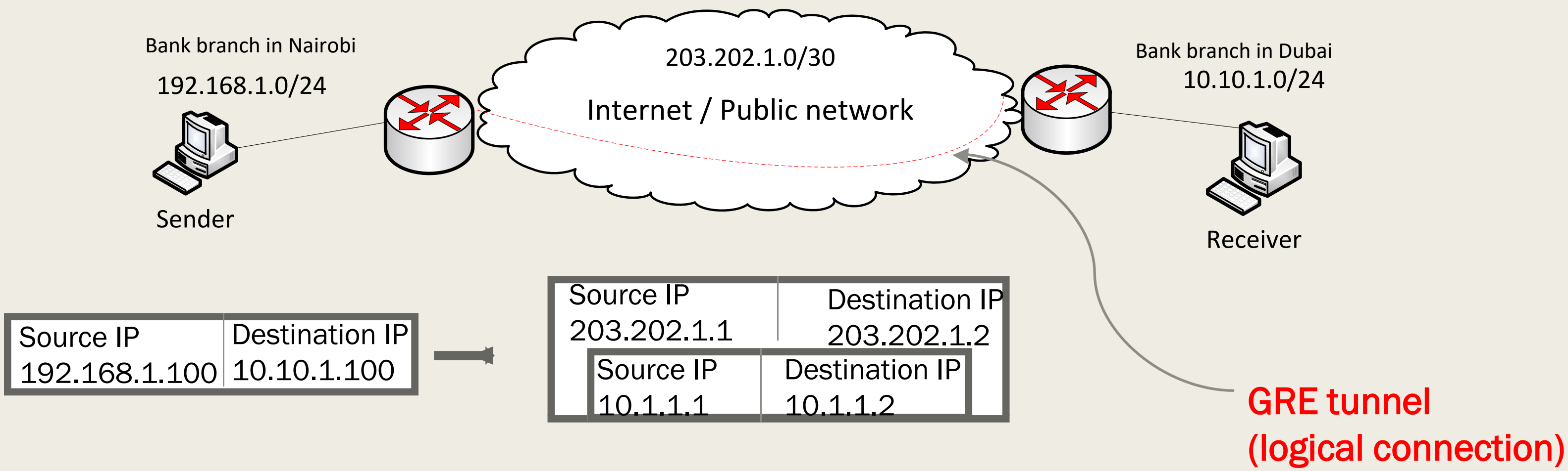
- Set all trunk ports
- Set VLAN on switch and apply it
- Test internet connection by connecting PC to Hargeisa switch

IPSEC OVER GRE

WAN technologies

GRE tunnel

- GRE (generic routing encapsulation) is used to encapsulate private IP address inside public IP address over the VPN
- It does not provide security on the data



IPSEC

- GRE tunnel is a VPN connection but with no security
- IPSEC adds security layer to the GRE logical connection
  - Adds authentication, encryption, and hashing

To establish IPSEC two phases are used

- Phase 1 an ISAKMP session is enabled (policy for each tunnel and transform sets)
- Phase 2 an IPSEC tunnel is formed that will be protected by phase 1

MPLS L3 VPN

WAN technologies

Introduction

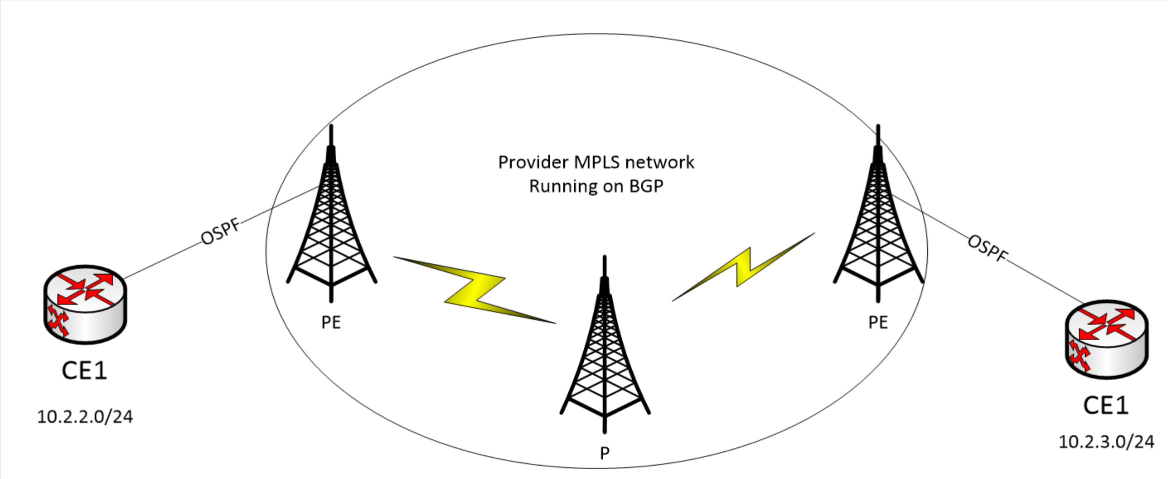
- MPLS (multi-protocol label switching) is WAN technology that provides faster connection than IP network
- It is multiprotocol because it supports various protocols such as IPv4 and IPv6
- MPLS routers forward traffic by switching label across the network instead of looking at routing table

MPLS applications

- To create L3 VPN for customer over the provider MPLS network
- Traffic engineering and management

MPLS network components

- Customer edge (CE) router that is located on the customer premises
- Provider edge (PE) router that labels the IP packets from the customer.
- P (Provider router) in the core network of the WAN operator and will switch the MPLS label across the MPLS core network

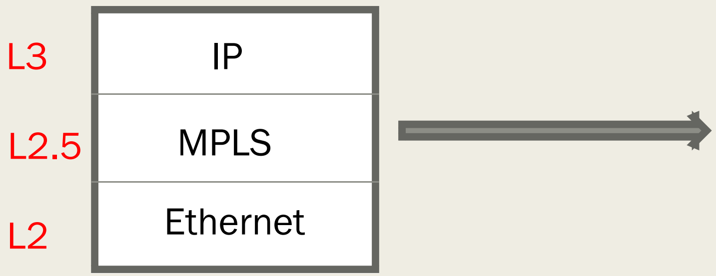


Other facts

- PE router has two interfaces, one to the customer and another to the MPLS network
- MPLS labels are used only in the core MPLS network (P, PE)

MPLS header

MPLS header is a 32-bit header inserted in between L2 and L3 ➔ hence regarded as L2.5



MPLS header

```
MultiProtocol Label Switching Header, Label: 17, Exp: 0, S: 1, TTL: 255
    0000 0000 0000 0001 0001 .... .... .... = MPLS Label: 17
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 1111 1111 = MPLS TTL: 255
```

MPLS label is used between PE and P router, it is not used between PE and CE link

MPLS label is unidirectional ➔ different label used for forward and return traffic

Label distribution protocol (LDP)

- MPLS speaking routers establish relationship through label distribution protocol
- Labels are used only in the core MPLS network
- MPLS L3 VPN uses two labels ➔ one to indicate next hop MPLS route and another which customer traffic is going to
- LDP routers listen to TCP connection port 646

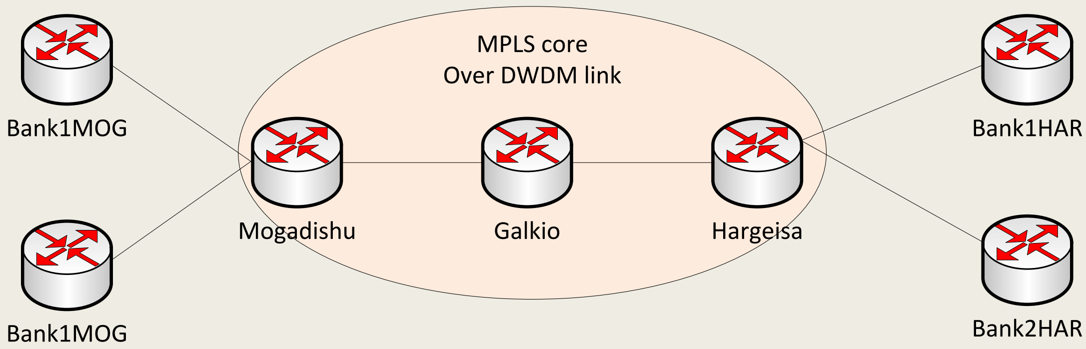
MPLS L3 VPN deployment scenario

Project requirement

- Deploy MPLS L3 VPN over DWDM link between Mogadishu and Hargeisa sites of smart telecom company
- Because of the cost involved in MPLS infrastructure, the MPLS core network will be placed on Mogadishu, Hargeisa and Galkio. L2 carrier Ethernet will extend in intermediate sites

Customer requirement

- Bank1 and Bank2 each has offices in Mogadishu and Galkio and want VPN reliable connection



Equipment requirement

2 PE routers
1 P router
4 CE routers

You need to buy these licenses MPLS and BGP from vendor

Design objectives

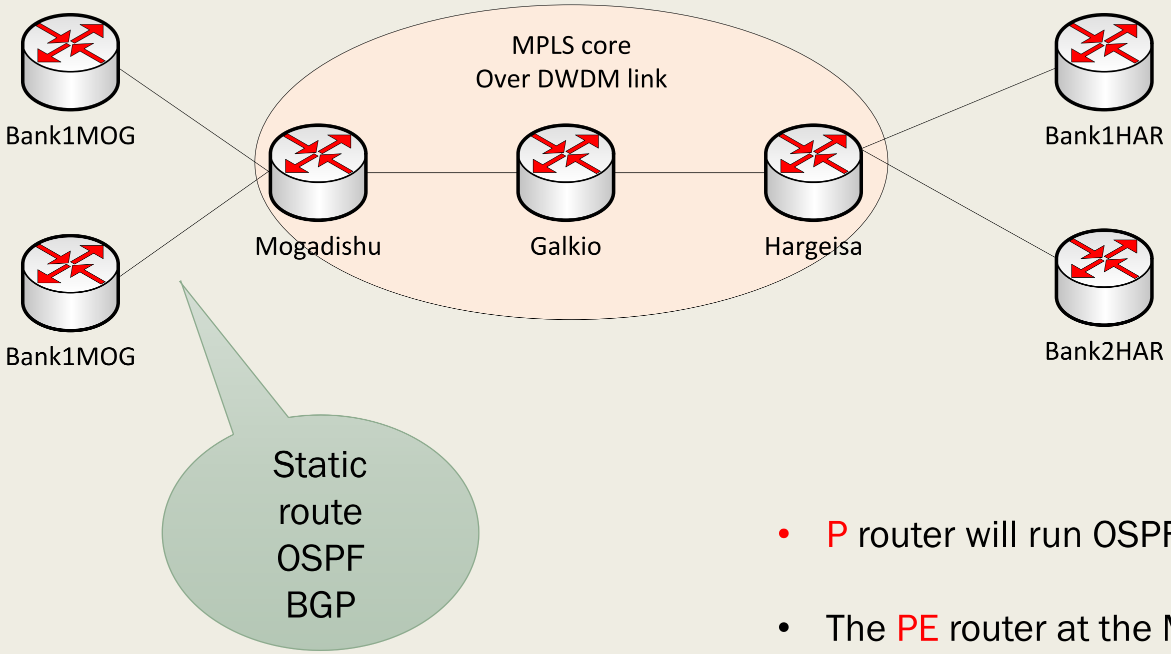
- Customer router should not see provider MPLS core network and cannot inject routes
- Customer network should not be able to access (telnet, SSH, traceroute, ping) the MPLS core

⇓

Hide core MPLS from customers

- Customers can use same subnets to connect to the MPLS core

What routing protocols to use in L3 VPN?



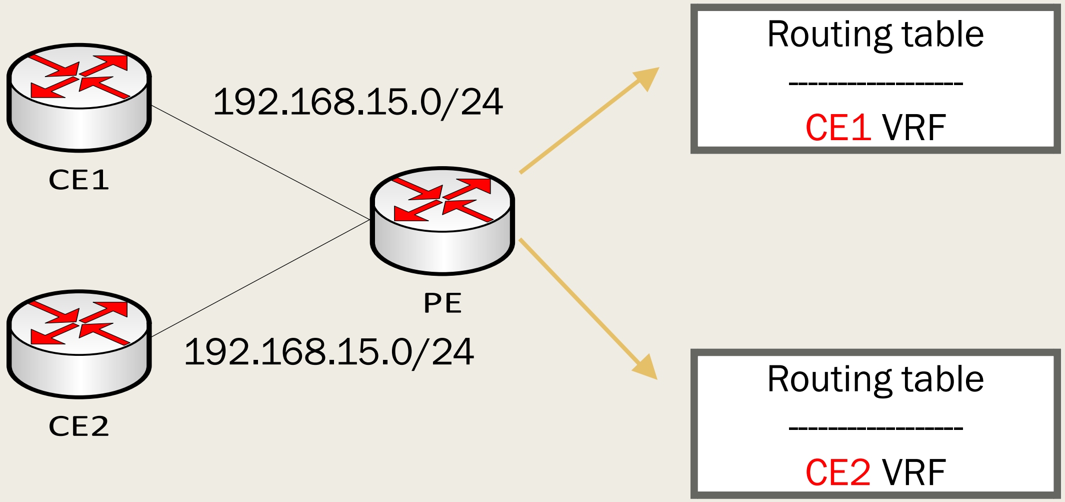
Multiple routes for different VRFs

- P router will run OSPF ➔ could use other IGP protocol
- The PE router at the MPLS edge will use internal BGP
- OSPF and BGP should be redistributed to each other

Virtual routing and forwarding

- VRF is a way of creating different IP routing tables within a single physical router
- In that way different customer traffic are separated within the router

  by assigning each customer network to different VRF



MPLS L3 VPN configuration steps

- Configure MPLS on core routers on the provider network
- Configure customer VRF on PE routers
- Configure OSPF instance for each customer
- Configure iBGP on PE routers
- Redistribute OSPF and BGP so that end-to-end L3 VPN works
- Hide core MPLS from customers to prevent customer route injection
- Verification and testing