Summary

Network Lab

2020/2021

contact us for any further information

Experiment 1

-in any computer network, computers and other network devices are connected together using cables.

- Unshielded twisted pair, or UTP for short, is the most common cable that is used for local area networks.

-The current standard for UTP cables is Category 5 Enhanced, better known as Cat5e.

-Cat5e: cable is available in several standards that suitable for different wiring applications.

-Cable runs are terminated with RJ45 connectors.

-Making network cables is a relatively simple process. In addition to cable and connectors, only a crimper wire trimmer is required.

UTP cable can be constructed to be:

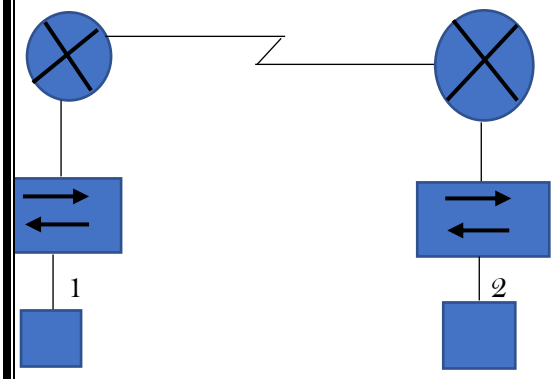
- Straight-through cable
- Crossover cable
- Rolled cable

1. Straight-through cable:
   A straight-through cable has connectors on each end that are terminated in similar manner in accordance with either the T568A or T568B standards. This means that the color of the wire on Pin 1 at One end of the cable will be the same for Pin 1 at the other end. Similarly Pin 2 will have the same color as Pin 2, and so on.
   Straight-through cables can be used to connect switch to router, switch to PC or server, and hub to PC or server.
2. Crossover cable:
   One end of the cable should be wired to the T568A standard. And the other end should be wired to the T568B standard. This crosses the transmit pairs and the receive pairs, the second and third pair, to allow Communication to take place.
   Crossover cables are used in cases, where we need to connect two devices that have the same interface. For example, connecting a switch to a switch, a hub to a hub, a PC to a PC, hub to switch, and a router directly to a host.
3. Rolled cable:
   Although rollover cable is not used to connect any Ethernet connections. It can be used to connect a PC to a router console serial communication (com) port in order to configure it.
   Rollover cables are probably the easiest cables to make because just cut the end off on one side straight-through cable and reverse it.

Experiment 2

*ما بصير يكون عنا جهازين بنفس النتورك و عليهم نفس ال IP

*IP overlap: "مشكلة معناها انه مستخدمين نفس النتورك ع أكثر من بورت للراوتر"



*ما بصير PC1 و PC2 يكونوا نفس ال IP مع انهم كل جهاز بنتورك بس لأنه النتورك مربوطين ببعض ما بصير

*IP: 172.16.10.100 / subnet mask: 255.255.0.0 then,

Network ID: 172.16.0.0 / from 172.16.0.0 to 172.16.255.255 in the same network

Ex: IP: 192.168.1.5 / subnet mask: 255.255.248.0, find the min and max IP of the network?

*طريقة الحل بعمل ANDing بين ال subnet mask و ال IP هيك بنتج عندي ال min

192.168. 0000 0001. 5 &&

255.255.1111 1000.0

Min: 192.168.0.0

*هسا عشان أطلع ال max بدي أحط بال min واحداات من عند نهاية ال prefix

Max: 192.168.0000 0111. 1111 1111

:192.168.7.255

EX:

IP: 10.10.10.10 / subnet mask: 255.255.128.0

10.10. 0000 1010. 10 &&

255.255.1000 0000.0

Min: 10.10.0000 0000. 0: 10.10.0.0

Max: 10.10.0111 1111.1111 1111: 10.10.127.255

*Note:

255.255.255.0 = /24

255.255.0.0 = /16

255.255.248.0 = /21

*أول IP بالنتورك هو : Network ID

*آخر IP بالنتورك هو : Broadcast IP

*الي بينهم هو : Host range

EX: 192.168.1.0 /24?

Network ID: 192.168.1.0

Broadcast IP: 192.168.1.255

Host Range: 192.168.1.1 to 192.168.1.254

EX: 172.16.5.10 /16?

Network ID: 172.16.0.0

Broadcast IP: 172.16.255.255

Host Range: 172.16.0.1 to 172.16.255.254

EX: 172.1.0.10 /8?

Network ID: 172.0.0.0

Broadcast IP: 172.255.255.255

Host Range: 172.0.0.1 to 172.255.255.254

*Note:

#of Hosts: 2^ (#of host portion bits) – 2

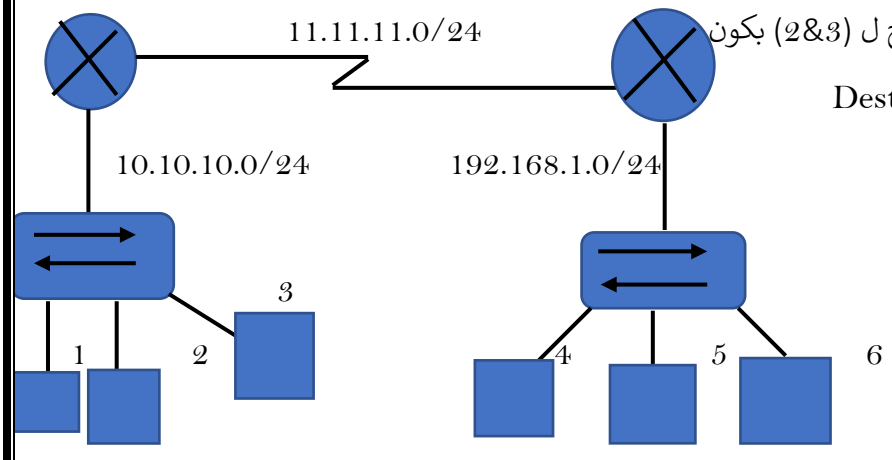
EX: 10.10.10.10 /18?

#of Hosts= 2^ (14) – 2 = 16382

*اذا كان ال Dest IP: 255.255.255.255 يعني Limited Broadcast (ببعت لكل الي معه بنفس النتورك) زي الماك ARP request بال FFFF..

*آخر IP بكل نتورك اسمه Direct Broadcast (ببعت من جهازي لكل الأجهزة الي بالنتورك الثانية)

EX:



*لو 1 بده يبعت ل (4&5&6) و ما يوصل المسج ل (2&3) بكون Dest IP: 192.168.1.255ال

أما لو من 1 ل (2&3) بس بكون ال Dest IP: 255.255.255.255

*Note:

*Range for multicast IP: 224.0.0.0 to 224.0.0.255

*اذا كان ال Dest IP بينهم يعني ابعت لكل الأجهزة التي تستخدم بروتوكول OSPF مثلا و هكذا

مثلا لو كان 224.0.0.5 : ابعت لكل الأجهزة الي شغالة على OSPF

*و هذه ال IP's محجوزة و تسمى (reserved link local IP's) و TTL لها هو 1

*أما من 224.0.1.0 to 239.255.255.255 بكونوا لل internet "مش مهم النا"

*Private & public IP's: "حفظ"

- 10.0.0.0/8
- 172.16.0.0 /12 to 172.31.255.255 /12
- 192.168.0.0 /16

*هذول ال Private IP بنستخدمهم زي ما بدنا داخل النتورك و مجانا

* بس اذا بدنا نطلع من النتورك لازم نحول ل public عن طريق (ISP(internet server provider بطريقة تسمى NATTING

(لما تشترك بالانترنت فبكون مقابل الحصول على public IP's

*To Know your IP:

Private: CMD -> ipconfig

Public: google -> my IP

**Remember:

- 255.255.255.255 -> limit Broadcast
- 0.0.0.0 -> default route "اذا ال اي بي الي بدك اياه مش موجود دور على هاد و اذا مش موجود اعمل دروب"
- 127.0.0.0/8 -> loop back
- 169.254.0.0/16 -> link local

* اذا الجهاز بكون فاصل و مش قادر يوصل لل DHCP serverو انا ما أعطيته static بوخذ IP من هاد و بختار واحد Randomly

- 192.0.2.0 /24 -> for testing " للناس الي اخترعت ال اي بي بس احنا ما راح نتعامل معه "

*IP Classes:

1. class A: 1.0.0.0/8 to 127.0.0.0/8
2. class B: 128.0.0.0/16 to 191.0.0.0/16
3. class C: 192.0.0.0/24 to 223.0.0.0/24
4. class D: 224.0.0.0/8 to 239.0.0.0/8 (multicast)

5.class E: 240.0.0.0/ to 250.0.0.0/ (Experimental ما بنستخدمهم)

*اذا استخدمنا IP بكلاس مع ال prefix تاعه بكون class full أما اذا ال prefix مختلف بكون class less

EX: 192.0.0.4/24 -> class full / 192.0.0.4/16 ->class less

.....

#Subnetting:

*لو عنا مثلا 192.168.1.0/24 و بدنا نشبك 2 Network مع بعض ما بقدر أعطي ال 2 Network نفس ال IP لانه الراوتر بربط بين ال 2 Network المختلفين لهيك اجت فكرة انه نستعير 1 bit من ال host portion لاضافة 2 Network و لو بدنا 4 Network بنضيف 2 bits حسب العلاقة :

2^ (#of bits) = #of Networks

بمثالنا 192.168.1.00000000 لو أعطينا هاد ال bit لل Network portion بصير عنا 2 Network :

1. 192.168.1.0(min)
   192.168.1.0111 1111(max)
2. 192.168.1.1000 0000(min)

   192. 168.1.1111 1111(max)

EX: We have 192.168.1.0/24, subnet it to 4 Networks

*للحصول على 4 Network نحن بحاجة الى 2 Bit من ال Host portion لانه 2^ (2)= 4

192.168.1. 0000 0000

1. 00 -> 192.168.1.00 00 0000

   192.168.1.00 11 1111

2. 01-> 192.168.1.01 00 0000

   192.168.1.01 11 1111

3. 10-> 192.168.1.10 00 0000

   192.168.1.10 11 1111

4. 11->192.168.1.11 00 0000

   192.168.1.11 11 1111

*every network has 2^ (6) – 2 = 62 host

.....

#VLSM:

*عملية تقسيم ال IP لأكثر من Network حسب عدد ال users المطلوبين و ليس عدد ال Networks

EX: 192.168.1.0/24, divide it to ENG department (100 users) / Marketing department (50 users)

IT department (20 users)?

192.168.1.0 000 0000

*نختار أكبر عدد users و هو 100 ثم نختار عدد ال bit المناسب 128 = (7) ^2 لكن هنا نأخذ 7 bit من اليمين و الي بظل عاليسار بنضيفه لل Network portion (بما انه ضفنا bit واحد لل Network portion يعني راح يطلع عندي 2 Network جداد)

1. 192.168.1.0/25

2. 192.168.1.128/25 -> 2^ (7) = 128 – 2 = 126 users for ENG

*ظل عنا النتورك رقم 1 فيها 126 Host بس بدنا نعمللها divide ل Network 2 و يكون وحدة مناسبة ل 50 users و وحدة ل 20 users

2^ (6) = 64

192.168.1.0/25

192.168.1.00 00 0000

1. 192.168.1.0/26 -> 62 users

2. 192.168.1.64/26 -> 62 users

*بنقدر نتركهم هيك و كل قسم يوخذ وحدة منهم و بنقدر نعطي ال 50 users وحدة و بنقسم الثانية و بصير عنا وحدة زيادة"بالحياة العملية بنتركهم هيك أما على الورق بنقسمهم للتدريب"

-أعطينا 2 لقسم ال Marketing و بدنا نقسم 1 "أسهل"

2^ (5) = 32

192.168.1.000 0 0000

1. 192.168.1.0/27 -> زيادة

2.192.168.1.32/27 -> for IT

Hashemite University
Faculty of Engineering and Technology
Computer Engineering Department

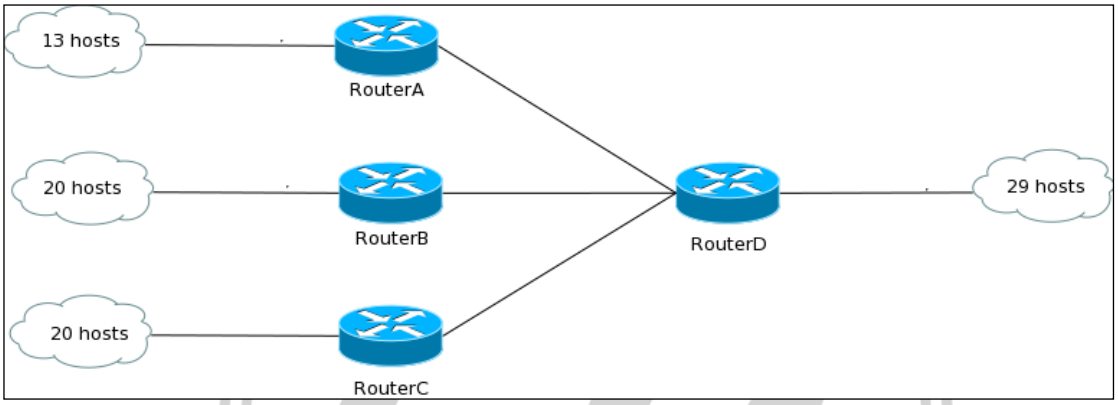
Homework Sheet

Experiment (2): Subnetting and VLSM

STUDENTS NAME: ID.: 1732930 PC NO:

Task1:

The organization has a network address of 172.30.0.0/14 to be divided as illustrated in the following topology. You must choose an addressing scheme that can accommodate the number of networks and hosts in the topology (including the networks between the routers).Note replace the XX in the given network address with the right most two digits of your ID, for example if your ID is 12345678, you need to replace the XX with 78.



Determine the number of subnets in Network Topology.

a. How many subnets are there? 7 subnets
b. How many bits should you borrow to create the required number of subnets? 3 bits
c. How many usable host addresses per subnet are in this addressing scheme? 32766
d. What is the new subnet mask in dotted decimal format? 255.255.128.0
e. How many subnets are available for future use? 1 subnet

Record the subnet information.

Fill in the following table with the subnet information:

Subnet Number	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0	172.28.0.0/17	172.28.0.1/17	172.28.127.254/17	172.28.127.255/17
1	172.28.128.0/17	172.28.128.1/17	172.28.255.254/17	172.28.255.255/17
2	172.29.0.0/17	172.29.0.1/17	172.29.127.254/17	172.29.127.255/17
3	172.29.128.0/17	172.29.128.1/17	172.29.255.254/17	172.29.255.255/17
4	172.30.0.0/17	172.30.0.1/17	172.30.127.254/17	172.30.127.255/17
5	172.30.128.0/17	172.30.128.1/17	172.30.255.254/17	172.30.255.255/17
6	172.31.0.0/17	172.31.0.1/17	172.31.127.254/17	172.31.127.255/17
7	172.31.128.0/17	172.31.128.1/17	172.31.255.254/17	172.31.255.255/17

Task2:

Develop a VLSM address scheme for the network displayed in the topology diagram in task1 using the same Network address, Fill in the following table with the subnet information:

Subnet Number	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0	172.28.0.0/27	172.28.0.1/27	172.28.0.30/27	172.28.0.31/27
1	172.28.0.32/27	172.28.0.33/27	172.28.0.62/27	172.28.0.63/27
2	172.28.0.64/27	172.28.0.65/27	172.28.0.94/27	172.28.0.95/27
3	172.28.0.96/28	172.28.0.97/28	172.28.0.110/28	172.28.0.111/28
4	172.28.0.112/30	172.28.0.113/30	172.28.0.114/30	172.28.0.115/30
5	172.28.0.116/30	172.28.0.117/30	172.28.0.118/30	172.28.0.119/30
6	172.28.0.120/30	172.28.0.121/30	172.28.0.122/30	172.28.0.123/30
7				

Experiment 3 & 4

The Cisco 2811 router is a multiple-chip standalone cryptographic module. The router has a processing speed of 350MHz. The interfaces for the router are located on the rear and front panels.

The front panel contains the following:

(1) Power inlet

(2) Power switch

(3) Optional PRS input

(4) Console and auxiliary ports

(5) Two Universal Serial Bus (USB) ports.

(6) Compact Flash (CF) drive.

(7) Four LEDs that output status data about the system power, auxiliary power, system activity, and compact flash busy status.

The back panel contains the following:

(1) Ground connector
(2) Ethernet ports and LEDs
(3) 7 high-speed WAN interface card (HWIC) slots
(4) Enhanced Network Module (ENM) slot

** Although there are several different types and modules of routers, every router has the same general hardware components. Depending on the model. those components are located in different places inside the router. To see the internal router components, you must unscrew the metal cover and take it off the router. Usually you do not need to open the router unless you are upgrading memory.

#types of memory in Router:

1. CPU: The CPU executes operating system instructions, such as system initialization, routing function, and switching functions.

2. RAM: RAM stores the instructions and data needed to be executed by the CPU.

RAM is used to store these components:

- Operating System: The Cisco IOS (Internetwork Operating System) is copied into RAM during bootup.

-Running Configuration File: This is the configuration file that stores the configuration commands that the router IOS is currently using. With few exceptions, all commands configured on the router are stored in the running configuration file, known as running-config.

-IP Routing Table: This file stores information about directly connected and remote networks. It is used to determine the best path to forward the packet.

-ARP Cache: This cache contains the IPv4 address to MAC address mappings. The ARP cache is used on routers that have LAN interfaces such as Ethernet interfaces.

- Packer Buffe: Packets are temporarily stored in a buffer when received on an interface or before they exit an interface

** RAM is volatile memory and loses its content when the router is powered down or restarted.

3.ROM: ROM is a form of permanent storage. ROM used to store:

-The bootstrap instruction

-Basic diagnostic software

-Scaled-down version of IOS

ROM uses firmware, which is software that is embedded inside the integrated circuit.

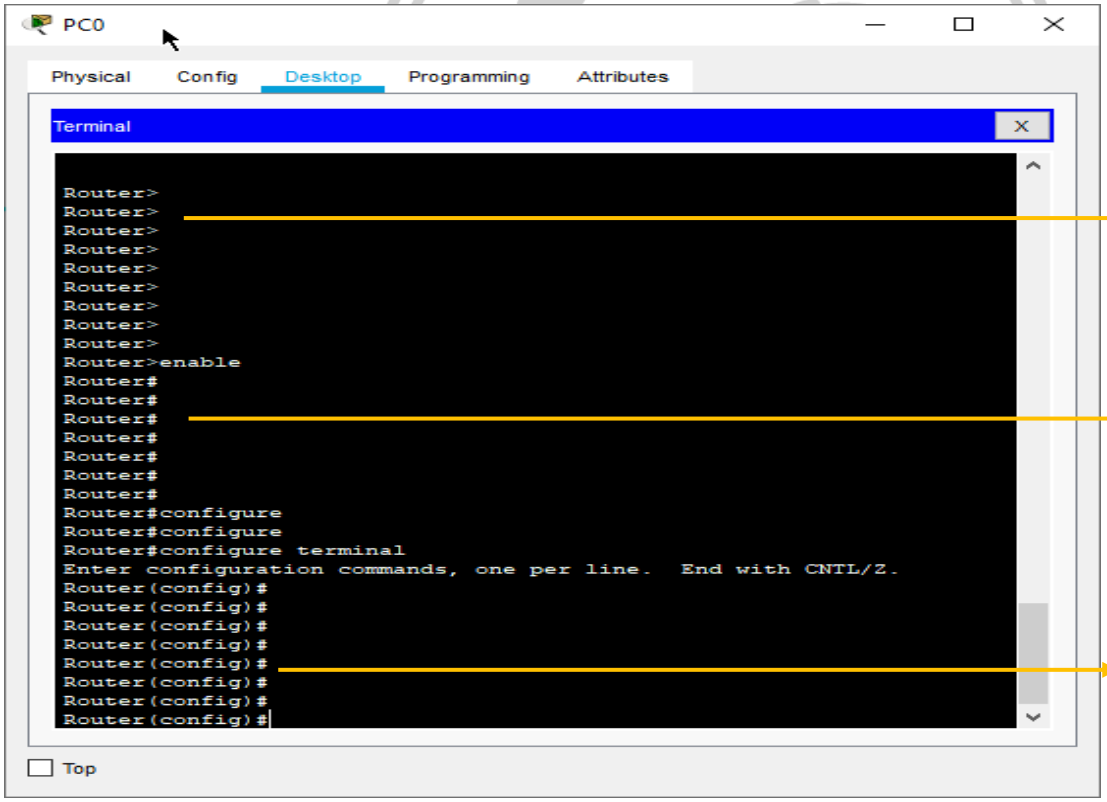
Firmware includes the software that does not normally need to be modified or upgraded, such as the bootup instructions. ROM does not lose its contents when the router loses power or is restarted.

4.Flash Memory: Flash memory is nonvolatile computer memory that can be electrically stored and erased. Flash is used as permanent storage for the operating system, Cisco IOS. In most models of Cisco routers, the IOS is permanently stored in flash memory and copied into RAM during the bootup process, where it is then executed by the CPU. Some older models of Cisco routers run the IOS directly from flash.

5.NVRAM: NVRAM (Nonvolatile RAM) does not lose its information when power is turned off. NVRAM is used as permanent storage for the startup configuration file (startup-config.) All configuration changes are stored in the running-config file in RAM, and with few exceptions, are implemented immediately by the IOS. To save those changes in case the router is restarted or loses power, the running-config must be copied to NVRAM, where it is stored as the startup-config file. NVRAM retains its contents even when the router reloads or is powered off.

.....

#Primary command modes:



User exec mode (allows limited commands)

Privilege mode (full access to all commands & troubleshoots)

Configuration mode (access for config option)

** لما أدخل للراوتر دائما بكتب no ل سؤال "do you want to enter initial config?"

** لما بدي أنتقل من mode ل mode مبين بالصورة شو أكتب

** لما بدي أرجع لل mode الي قبل بكتب exit

** اذا بدي أرجع لل privilege mode مباشرة بكتب end

Configuration mode

Global config mode	Line console & line VTY	Interface config mode
بأثر على كل ال router بدخل عليها by default	Line console 0 "لوضع باس وورد على الكونسول فقط "	Interface fast Ethernet 0/1 ال 1 تمثل رقم ال port الي بدي أدخل عليه
Router(config)#	Line VTY 0 15 ➔ to enable remote access	Router(config-if) #
	Router(config-line) #	

** لتجنب انه الجهاز يعلق لما أكتب كلمة غلط "no IP domain-lookup" Router(config)# "

** اذا بدي أغير اسم الراوتر "hostname ……." Router(config)# " طبعا شروط الاسم :

1. لازم يكون أكثر اشي 64 char
2. لازم يبلش ب char بس عادي بنتهي بـchar أو number
3. يحتوي على char , number and dashes only

** عشان أحط باسوورد عالراوتر :

Router(config)#line console 0 ⟶ Router(config-line) #password ……⟶ Router(config-line) #login

- Password Guidelines:
  - Use passwords that are more than eight characters in length.
  - Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.
  - Avoid using the same password for all devices.
  - Do not use common words because they are easily guessed.

** لوضع IP لل PC ندخل على ال PC ثم desktop ثم IP config

#Commands:

1.كيف نشيك على ال IP address تبع ال PC :

Command prompt

C:\>ip config

2.كيف نشيك على ال MAC address تبع ال device : "الماك هو نفسه ال physical "

Command prompt

C:\>ip config “Space” \all

3.كيف تعطي hostname :

SW>enable

SW# config t

SW(config)#hostname ……

4.كيف بدي أعطي باسورد:

SW(config)#enable secret ……..

5.في عندي show command بفرجيني كل ال Interfaces الموجودة عل ى ال SW / كيف بعرف ال IP على ال SW :

SW# show IP interface brief

6.في عندي show command بفرجيني ال MAC address الي عندي:

SW# show mac address-table

**تعلموا الماك لانه ال devices الموجودة بالنتورك في بينهم traffic internally بروحوا و بيجو بين بعض

7.كيف بدي أعمل password لل console & telnet :

SW(config)# line console 0

SW(config-line)#password ……..

SW(config-line)#login

SW(config)# line vty 0 15

SW(config-line)#password …….

SW(config-line)#login

8.كيف بدي أعطي IP address "بدي أعمل remote management على ال SW :"

SW(config)# interface vlan 1

SW(config-if)#ip address ……. ……

IP address

subnet mask ……

SW(config-if)#no shutdown

9.عشان أعمل telnet لازم أعطي IP & gateway :

SW(config)#ip default-gateway …….

10.كيف بدنا نشوف ال running config :

SW# show running-config

11.كيف ممكن أخفي ال password بال running config :

SW(config)# service password-encryption

12.كيف بدنا نعمل save لل configuration :

SW# wr OR SW# copy running-config startup-config

13.كيف بحط رسالة ترحيبية :

SW(config)#banner motd * …….. *

14.كيف بدي أعطي ال IP للبورت في الراوتر من جهة نتورك معينه:

R(config)# interface g0/0 IP address subnet mask

R(config-if)#ip address . ……. …….

R(config-if)#no shutdown

15.كيف بشيك ال ARP table على الراوتر:

R# show arp

R# show IP route

Experiment 5 & 6

*A router can learn about remote networks in one of two ways:

Manually - Remote networks are manually entered into the route table using static routes.

Dynamically - Remote routes are automatically learned using a dynamic routing protocol like (RIP, Ospf and Eigrp).

Static Routes

Notes:

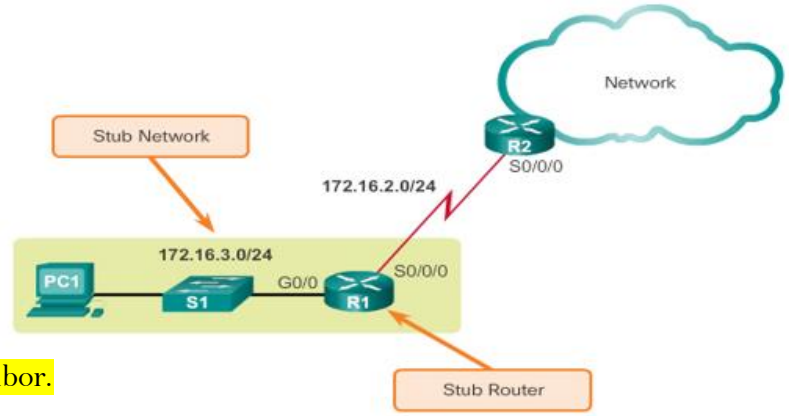
1- Unlike a dynamic routing protocol, static routes are not automatically updated and must be manually reconfigured any time the network topology changes.

2- A static route does not change until the administrator manually reconfigures it.

بالمختصر اي اضافة جديدة على النتوورك يحتاج الادمن لعمل تحديث على الراوترات.

When we use Static Route?

1- Small Network.
2- Stub Network.
3- Default route.



What is Stub Network?

A stub network is a network accessed by a single route, and the router has only one neighbor.

How to configure Static Route?

We use this command in global config mode:

Router(config)# ip route network-address subnet-mask {ip-address | exit-interface}

network-address: Destination network address of the remote network

subnet-mask: Subnet mask of the remote network

One or both of the following parameters must also be used:

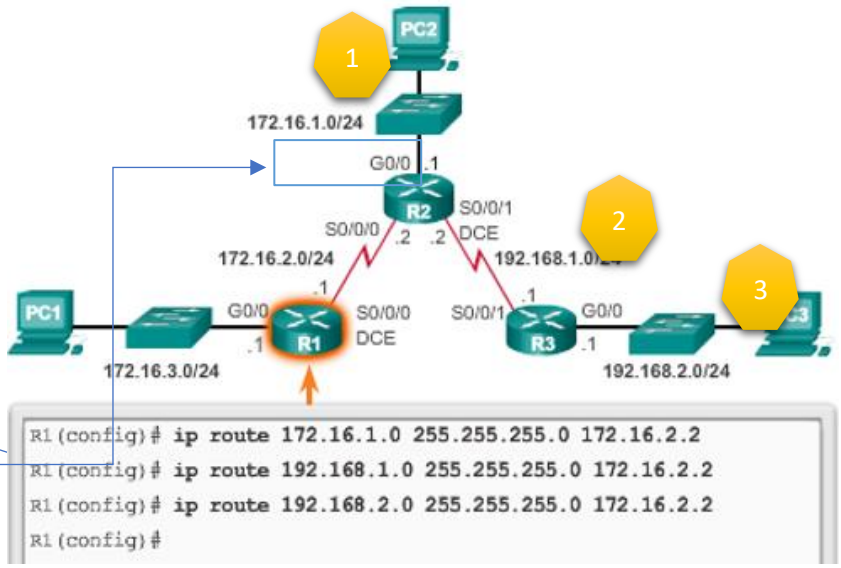
ip-address: Next-hop router's IP address. (Does not have to be next-hop.)

exit-interface: Outgoing or exit interface

Example of How to configure Static Route:

R1:

There is there network I want to reach via the S0/0/0 interface or my IP on that interface so we gonna use the IP as the following:



For the first line:

Ip route is the command

172.16.1.0 the network I want to reach

255.255.255.0 the subnet mask of it

172.16.2.2 the IP address of my next hop which is on my S0/0/0 interface.

*سؤال مشابه جدا في امتحان الميد ولكن المطلوب كان باستخدام ال exit interface

يكون الحل بنفس الطريقة ولكن بدل ال next hop نضع ال exit interface مثال:

R1 (config)# Ip route 192.168.1.0 255.255.255.0 S0/0/0

Now what is Default Route and how can we configure it?

Default Route: is the route that takes effect when no other route is available for an IP destination address.

وذلك يعني يلجئ الراوتر لاستخدام ال Default Route في حالة عدم وجود اي تطابق لعنوان المستقبل في routing table اي انه خيار الراوتر الاخير.

Configure it:

R1 (config)# Ip route 0.0.0.0 0.0.0.0 {Outgoing interface or Next hop address}

Static route Show commands:

1- show ip route
2- show ip route static
3- show ip route network

Dynamic Routing:

Is a networking technique that provides optimal data routing. Unlike static routing, dynamic routing enables routers to select paths according to real-time logical network layout changes.

الفرق الرئيسي بين الستاتك و الداينمك هو عند وجود اي تحديث بالنتوورك (اضافة او ازالة راوتر) الستاتيك يحتاج لادخال المعلومات الجديدة يدويا اما الداينمك يعمل تحديث اول باول بناءا على رسائل بين الراوترات باستخدام dynamic protocols المناسب.

*يفضل استخدام ال Dynamic protocols لتسهيل عملية ادارة الشبكات الكبيرة large Networks.

IP Routing Protocols:

RIP, OSPF, EIGRP, IGRP, ISIS and BGP.

Classification of Dynamic routing protocols:

1- Distance vector: The route with the least number of hops to the network is determined to be the best route. They send the entire routing table to directly connect neighbors.

2- Link-state: The route with lest cost. Link state protocols send updates containing the state of their own links to all other routers on the network.

3- Hybrid: Hybrid protocols use aspects of both distance vector and link state--for example, EIGRP.

RIPv2

The maximum hop counts that RIP protocol use is 15, and by default the RIP update messages sent every 30s.

Commands to enable RIP:

For RIPv1 we don't use it these days (in the global config mode):

Router (config)# router rip

Router (config-router)# network network IP(directly connected)

For RIPv2:

Router (config)# router rip

Router (config-router)# version 2

Router (config-router)# no auto summery

Router (config-router)# passive interface interface name

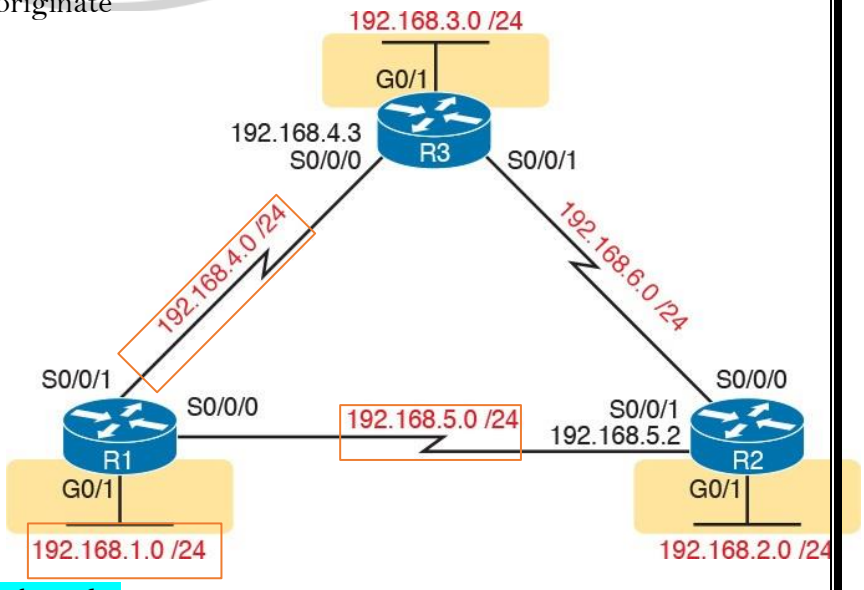
Passive interface: بالمختصر هي الانترفيس يلي ما بدي الراوتر يبعتلها رسائل ابديت

Router (config-router)# network network IP

Router (config-router)# default information originate

Example to configure RIPv2:

For R1 configuration:



R1(config)#router rip

R1(config-router)#version 2

R1(config-router)#network 192.168.1.0

R1(config-router)#network 192.168.4.0

R1 (config-router)#network 192.168.5.0

R1(config-router)#no auto-summary

V.I note: we use the directly connected networks only.

If R1 have a PC connected to G0/0 we can configure it as passive interface:

R1(config-router) #passive interface g0/0

Before we talk about EIGRP and OSPF we must know the definition of

Autonomous System:

(AS) is a set of Internet routable IP prefixes belonging to a network or a collection of networks that are all managed, controlled and supervised by a single entity or organization.

. Autonomous System وذلك يعني اي مجموعة من الاجهزة التي تمتلك IP و يتم التحكم فيها من جهاز رئيسي واحد او منظمة واحد يسمى ذلك

Types of AS:

Stub AS:

This AS is connected to only one other AS.

Transit AS:

This AS is connected to more than one other AS and can be used for transit traffic between autonomous systems. They are usually administered by large Internet service providers (ISPs).

Multihomed AS:

This AS is connected to more than one other AS but does not let transit traffic from another AS pass through itself.

.

EIGRP (Extreme Interior Gateway Protocols)

* Cisco private protocols. (Mean: just cisco device can use it.)

EIGRP protocols have 6 type of packets:

- Hello packets >> are used for neighbor discovery.
- Update packets >> have routing information and are sent reliable to whatever router that requires this information.
- Query packets >> when the router lose his information about network and have no backup routes .
- Reply packets >> response to Query packets
- Request packets >> request specific routing information.
- ACK packets >> This packet will acknowledge as a receipt of update, query, and replay packets.

Wild Card mask:

Think of a wildcard mask as the inverse of a subnet mask.

Example: if we have a network with the subnet mask 255.255.255.128, we can get the wild mask

$$255.255.255.255 - 255.255.255.128 = 0.0.0.127$$

EIGRP commands:

Router(config)# router eigrp autonomous-system (for AS in this course we use 1)

Network command:

Router(config-router)# network network-address [wildcard-mask]

Example to configure EIGRP:

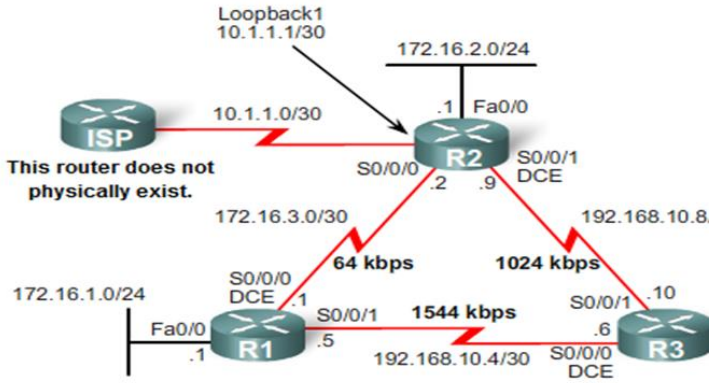
For R1 we can configure EIGRP as the following:

R1(config)# router eigrp 1

R1(config-router)# network 172.16.3.0 0.0.0.3

R1(config-router)# network 172.16.1.0 0.0.0.255

R1(config-router)# network 192.168.10.4 0.0.0.3



And ofc we can use the passive interface if we have one.

OSPF (Open Shortest Path Protocols)

أغلب معلومات في هذه التجربة كانت نظرية (كويزات وميد).

The OSPF maintains three tables:

Neighbor table: stores information about OSPF neighbors.

Topology table: stores the topology structure of a network.

Routing table: stores the best routes.

OSPF Router ID:

OSPF Router ID is an IPv4 address (32-bit binary number) assigned to each router running the OSPF protocol to provide a unique identity to the OSPF Router.

Ways to select the ID:

1- Any manually configured OSPF Router ID in OSPF Process
2- If there is no OSPF Router ID configured, the highest IP address on any of the Routers Loopback Interfaces is selected as the OSPF Router ID
3- If there is no Loopback Interfaces configured, the highest IP address on its active interfaces is selected as the OSPF Router ID.

On LANs, DR and BDR must be elected. Two rules are used to elect a DR and BDR:

DR: Designated Router \\ BDR: back up Designated Router.

1. Router with the highest OSPF priority will become a DR. By default, all routers have a priority of 1.

2. If there is a tie, a router with the highest router ID wins the election

The second highest ID became the BDR.

Quiz Question:

Mention the steps of OSPF:

1. Establish Router Adjacencies.
2. Elect the DR and the BBDR.
3. Discover Routes.
4. Select the best Routes.
5. Maintain Routing Table.

OSPF command:

Router(config)# router ospf ospf-prosessId (similar to AS in EIGRP)

Ex: Router(config)# router ospf 1 (similar to AS in EIGRP)

Network command:

Router(config-router)# network network-address [wildcard-mask] area (Number)

Ex: Router(config-router)# network 192.168.1.0 0.0.0.3 area 1

OSPF show commands:

Show OSPF

Show IP neighbor

Show OSPF interfaces

Experiment 7

ACL (Access Control List)

ACL: is a sequential collection of permit or deny statements that apply to addresses or upper-layer protocols.

بالمختصر الشديد لمفهوم ال ACL هي مجموعة من الاوامر التي قد تمنع او تسمح بمرور ال Layer 3 Packets او الاعلى.

هناك بعض الامور التي يجب الاخذ بها عند صنع ACL ومنها:

1- الترتيب مهم جدااا جدااا حيث ان الجملة الاولى لها اولوية التنفيذ من الثانية وكذلك الامر.

2- بنهاية كل ACL يوجد امر منع لجميع الاتصالات غير المذكورة ب ACL لذلك في بعض الاحيان نحتاج لختم ال ACL بامر سماح لكل الاتصالات (يعتمد على السؤال)

Access Lists Types:

1- Standard access lists: mainly based on source IP address.

2- Extended access lists: can be evaluate using source and destination IP and protocol field in the Network layer header, and port number at the Transport layer header.

These are the two main types of ACL.

BUT in case we want to categorize the ACL from Functional aspects there is 2 more types:

1- Numbered access lists
2- Named access lists

Both could be Standard or Extended but each of them have it unique commands.

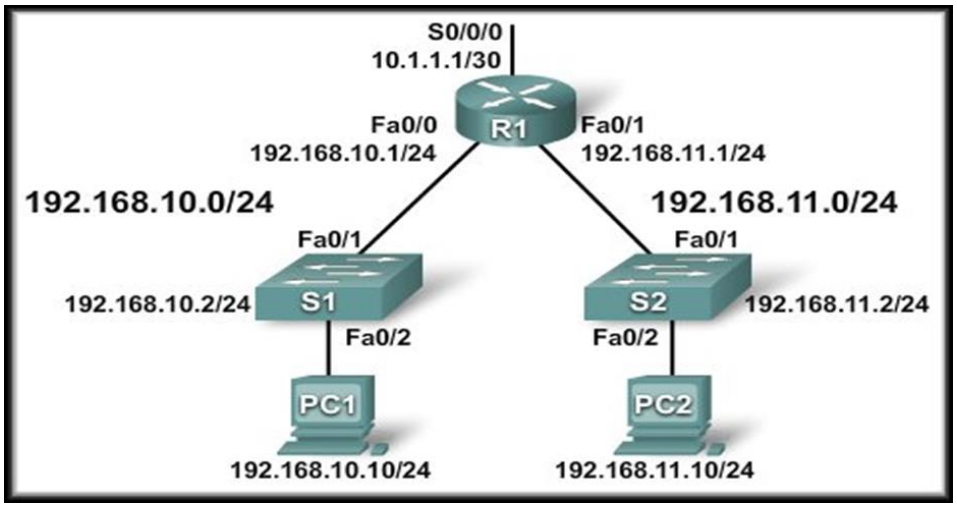
Configure Standard ACL:

```
Router(config)#access-list access-list-number
                          [deny | permit | remark]
                          source [source-wildcard]
```

Example of Standard ACL:

Example 1:

Allow only traffic from network 192.168.10.0 to exit the network on S0/0/0. Block any traffic from any other network.



Sol:

```
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#deny any

R1(config)#interface s0/0/0
R1(config-if)# ip access-group 1 out
```

Creating Standard Named ACL:

```
Router(config)# ip access-list [standard | extended] name

Router(config-std-nacl)# [permit | deny | remark] {source [source-
wildcard]} [log]

Router(config-if)#ip access-group name [in | out]
```

Example:

```
R1(config)#ip access-list standard NO_ACCESS

R1(config-std-nacl)#deny host 192.168.11.10
R1(config-std-nacl)#permit 192.168.11.0 0.0.0.255
R1(config-std-nacl)#deny any
R1(config-std-nacl)#end

R1(config)#interface Fa0/1
R1(config-if)# ip access-group NO_ACCESS out
```

Extended ACL:

Can be evaluate using source and destination IP and protocol field in the Network layer header, and port number at the Transport layer header.

So how can we configure it?

The main command in global configure mode:

```
router(config)#access-list access-list-number {deny | permit} protocol source source-wildcard destination destination-wildcard [port-number number]
```

note: any thing after the wild mask of the dst host is optional.

protocol: name of layer 3 protocols or could be (any)which mean all protocols.

source source-wildcard: IP and it wild mask like 192.168.1.0/30 192.168.1.0 0.0.0.3

destination destination-wildcard: same but for the destination host.

Or could be an Extended Named access list like:

```
router(config)#ip access-list extended {access-list-name}

router(config-ext-nacl)# {deny | permit} protocol source source-wildcard destination destination-wildcard [port-number number]
```

HW.3

PT Activity: 00:15:38

Packet Tracer - Skills Integration Challenge

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	G0/0	172.16.127.254	255.255.192.0	N/A
	G0/1	172.16.63.254	255.255.192.0	N/A
	S0/0/0	192.168.0.1	255.255.255.252	N/A
	S0/0/1	64.104.34.2	255.255.255.252	64.104.34.1
Branch	G0/0			N/A
	G0/1			N/A
	S0/0/0	192.168.0.2	255.255.255.252	N/A
HQ1	NIC	172.16.64.1	255.255.192.0	172.16.127.254
HQ2	NIC	172.16.0.2	255.255.192.0	172.16.63.254
HQServer.pka	NIC	172.16.0.1	255.255.192.0	172.16.63.254
B1	NIC			
B2	NIC	172.16.128.2	255.255.240.0	172.16.143.254
BranchServer.pka	NIC	172.16.128.1	255.255.240.0	172.16.143.254

Scenario

In this challenge activity, you will finish the addressing scheme, configure routing, and implement named access control lists.

Requirements

a. Divide 172.16.128.0/19 into two equal subnets for use on **Branch**.
   1) Assign the last usable address of the second subnet to the Gigabit Ethernet 0/0 interface.
   2) Assign the last usable address of the first subnet to the Gigabit Ethernet 0/1 interface.
   3) Document the addressing in the Addressing Table.
   4) Configure **Branch** with appropriate addressing

b. Configure **B1** with appropriate addressing using the first available address of the network to which it is attached. Document the addressing in the Addressing Table.

c. Configure **HQ** and **Branch** with OSPF routing according to the following criteria:
   - Assign the process ID 1.
   - Advertise all three attached networks. Do not advertise the link to the Internet.
   - Configure appropriate interfaces as passive.

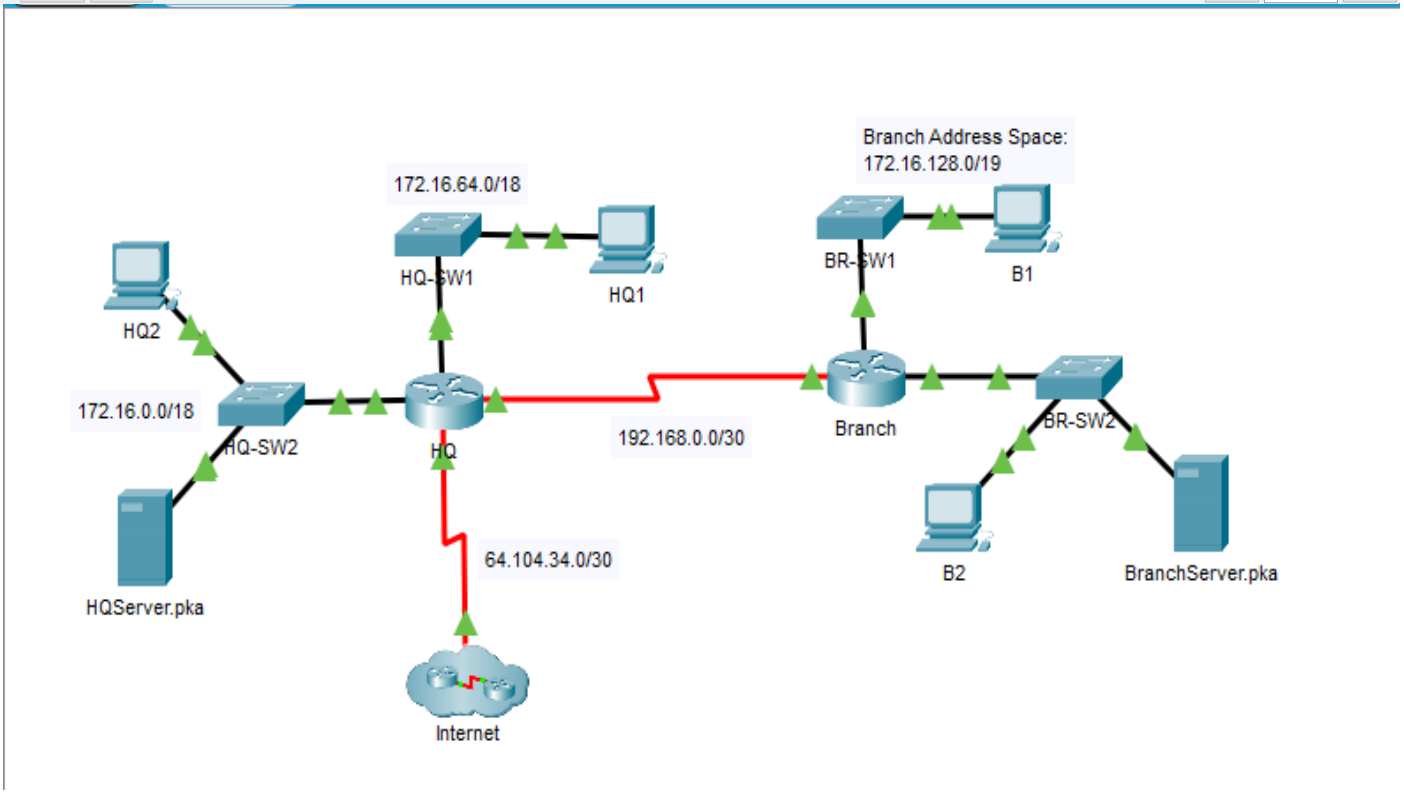
d. Set a default route on **HQ** which directs traffic to S0/0/1 interface. Redistribute the route to **Branch**.

e. Design a named access list **HQServer** to prevent any computers attached to the Gigabit Ethernet 0/0 interface of the **Branch** router from accessing **HQServer.pka**. All other traffic is permitted. Configure the access list on the appropriate router, apply it to the appropriate interface and in the appropriate direction.

f. Design a named access list **BranchServer** to prevent any computers attached to the Gigabit Ethernet 0/0 interface of the **HQ** router from accessing the HTTP and HTTPS service of the **Branch** server. All other traffic is permitted. Configure the access list on the appropriate router, apply it to the appropriate interface and in the appropriate direction.

Time Elapsed: 00:15:38 Completion: 100/100

Top | Check Results | Reset Activity | < | 1/1 | >



Sol:

****router branch

branch>enable

branch# config t

branch(config)#int g0/0

#ip add 172.16.159.254 255.255.240.0

#ex

branch(config)#int g0/1

#ip add 172.16.143.254 255.255.240.0

#ex

****pc B1

بندخل عليه من desktop

بعدين IP configuration

عبي هدول

IP: 172.16.144.1

Subnet: 255.255.240.0

Gateway: 172.16.159.254

***router branch

branch(config)#router OSPF 1

#network 172.16.144.0 0.0.0.31 area 0

#network 172.16.128.0 0.0.15.255 area 0

#network 192.168.0.0 0.0.0.3 area 0

#passive-interface g0/0

#passive-interface g0/1

#ex

**router HQ

HQ>enable

HQ# config t

HQ (config)#router OSPF 1

#network 172.16.0.0 0.0.63.255 area 0

#network 172.16.64.0 0.0.63.255 area 0

#network 192.168.0.0 0.0.0.3 area 0

#passive-interface g0/0

#passive-interface g0/1

#passive-interface S0/0/1

#exit

HQ(config)#ip route 0.0.0.0 0.0.0.0 S0/0/1

#router OSPF 1

#default-information originate

#ex

***router branch

branch(config)#ip access-list extended HQServer

#deny ip any host 172.16.0.1

#permit ip any any

#ex

branch(config)#int g0/0

#ip access-group HQServer in

****router HQ

```
HQ(config)#ip access-list extended BranchServer
        #deny tcp any host 172.16.128.1 eq 80
        #deny tcp any host 172.16.128.1 eq 443
        #permit ip any any
        #ex
HQ(config)#int g0/0
        #ip access-group BranchServer in
```

Experiment 8 & 9

*Broadcast storm:

- انه مسج يكون broadcast و يوصل لما يكون كل الشركة على switches فبتظلها تنتشر لتوصل للكل

- بال default بكونوا كل ال ports ال switch موجودين بنفس النتورك بكونوا كلهم تابعين ل VLAN1 كل VLAN الها رقم و اسم

** فائدة ال VLAN: تقسيم ال switch لأكثر من نتورك (أكثر من LAN)

** بال default بكونوا كلهم ب VLAN 1 و بنفس النتورك

**VLAN benefits:

1. Reduce cost
2. Split Broadcast domain
3. Network design flexibility
4. Security
5. Better management
6. Higher performance

**Range of VLAN 1 to 4096:

1.Normal Range: [1 to 1005] -> For traditional networks saved in flash (VLAN.dat)

- في خصائص خاصة بال Normal بس مثل VTP

2.Extended Range: [1006 to 4096] -> For ISP (Internet service protocol) saved in Running-config and then to Startup-config after(wr) / NO VTP

Note**:

- يعني لو نعمل VLAN 5 و VLAN 2000 و نكتب show running-config راح يطلعلنا بس ال 2000 لانه ال 5 مخزن بال flash

- VLAN 1 موجودة default بس بنقدر نستخدمها و ما بنقدر نمسحها

- Maximum #of VLAN in switch 2960: 255 VLANs

**VLAN types:

1. Data VLAN: that have DATA like (PCs, Servers)
2. Default VLAN: like VLAN 1
3. Management VLAN: for telnet & SSH
4. Voice VLAN: contain IP phones

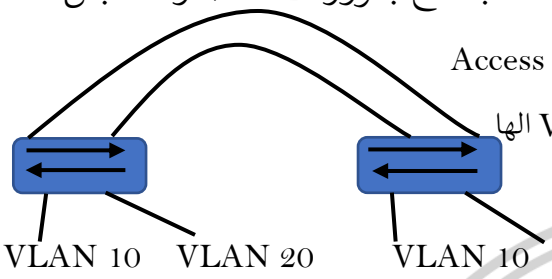
5. Native VLAN: Native بكون tag بكون VLAN عادي أما الي بدون tag بكون عليه الي

**بعد ما يدخل ال Frame على ال switch يميزه و هو بتعامل معه انه لأي VLAN بطبع عليه tag برقم ال VLAN تبعه و قبل ما يطلع من ال Switch على ال VLAN تبعه بشيل ال tag عنه

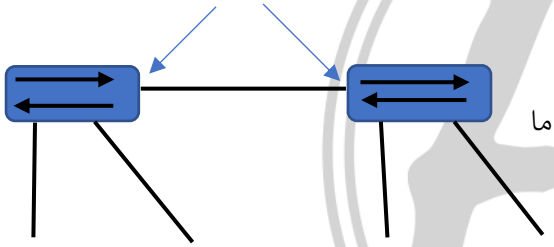
**ال Native VLAN ما بنحط عليه tag فبتكون مميزة انه الي ما عليها tag هي ال Native و بتكون by default هي VLAN 1 بس الأحسن انه نغيرها

#Access port & Trunk port:

بسمح بمرور VLAN واحد بس بسمح بمرور multi VLAN



-بهاي الرسمة مستخدمين Access port بين SW1 وSW2 حيث كلAccess port بسمح بنقلVLAN واحد فقط و هون بصير عملية tagging لأنه كل VLAN الها Access port خاص فيها



-لو PC موجود ب VLAN 10 الي ب SW1 بده يبعت ل PC موجود ب VLAN 10 ب SW2 : لما يوصل الفريم من VLAN 10 ل SW1 راح يحط عليه tag خاص بVLAN 10 و ببعته عن طريق ال Trunk لل SW2 و بدون ما يشيل ال tag ل غاية ما يوصل لل Access port الي بتوديه ل VLAN 10 الي ب SW

**Trunk:

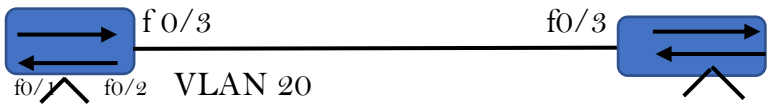
1. 802.1 q :

-موجود بكل مكان تقريبا و يستخدم لأجهزة cisco و غيرها بعمل tagging

-اذا في tag بصير ماكس حجم الفريم 1522بايت بدل 1518 بايت

2. ISL: Legacy, for cisco devices only, No tagging

EX:



VLAN 10 VLAN 10 VLAN 20

Sol:

SW1(config)# VLAN 10

#name ENG

#VLAN 20

#name management

#int f 0/1

#switchport mode access

#switchport access VLAN 10

#int f 0/2

#switchport mode access

#switchport access VLAN 20

#int f 0/3

#switchport mode trunk

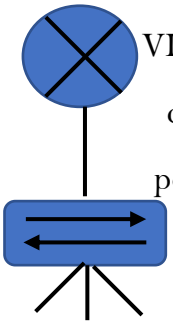
#switchport trunk native VLAN 900

- بنستخدم ال command التالي لعرض تفاصيل ال port الي مشغلينه trunk :

SW# show interface trunk

** و بنعمل نفس هاي الكوماندات عال SW2

**VLAN Routing:(Sub Interface / Router on a Stick)



- الفكرة انه لو الراوتر عليه مثلا 2 ports و عندي switch عليه 50 VLAN مش راح أقدر أشبكهم كل VLAN على الراوتر خاص فيه و اذا ما كان لكل VLAN بورت خاص فيها مش راح يكون في default gateway Port لأنه البورت الي عليه IP واحد راح يكون لنتورك وحدة. فالحل انه نعمل تقسيم لهاي ال interface لعدة ports حسب حاجتنا و حسب كمية الاستخدام و تعمل الراوتر للداتا

#Config on Switch:

SW1(config)# VLAN 10

#name ENG

#VLAN 20

#name management

#int f 0/1

#switchport mode access

#switchport access VLAN 10

#int f 0/2

#switchport mode access

#switchport access VLAN 20

#int f 0/3

#switchport mode access

#switchport access VLAN 30

#int f 0/4

#switchport mode trunk

#switchport trunk native VLAN 900

#Config on Router:

R(config)# int g0/0

no shutdown

int g0/0.10

encapsulation dot1q 10

IP address ……IP…… ……Subnet MASK……

int g0/0.20

encapsulation dot1q 30

IP address ……IP…… ……Subnet MASK……

int g0/0.30

encapsulation dot1q 30

IP address ……IP…… ……Subnet MASK……

**Layer 3 Switch:

- جهاز بشتغل ك Switch و ك Router بنفس اللحظة
- بكون عليه Routing table & ARP table & MAC table
- حاليا هو الأكثر استخداما عند ال customers لأنها بتوفر استخدام راوتر وSwitch

HashemiteUniversity
FACULTY of Engineering and Technology
COMPUTER Engineering Department

Homework Sheet

Introduction to VLANs/Inter-VLAN routing

STUDENTS NAME:_____, ID.:_____PC NO_____.

Basic VLAN Configuration

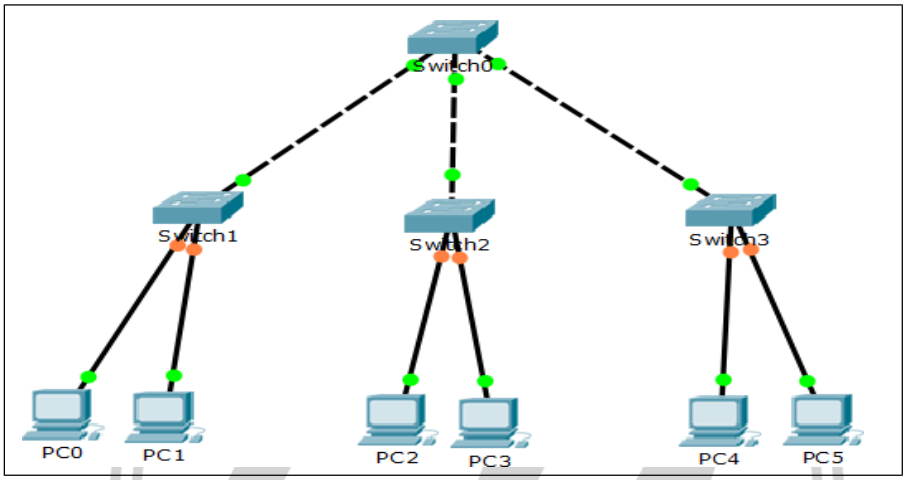


Figure (1): Topology Diagram

Device	IP Address	Subnet Mask	Default Gateway
PC0	192.168.1.2	255.255.255.0	192.168.1.1
PC1	192.168.2.2	255.255.255.0	192.168.2.1
PC2	192.168.1.3	255.255.255.0	192.168.1.1
PC3	192.168.3.2	255.255.255.0	192.168.3.1
PC4	192.168.2.3	255.255.255.0	192.168.2.1
PC5	192.168.3.3	255.255.255.0	192.168.3.1

Table (1): Addressing Table.

VLAN	Name	PCs
10	DEV	PC0, PC2
11	HR	PC1, PC4
20	ACC	PC3, PC5
90	NATIVE	--------

Table (2): VLANs Table.

Task: Prepare the Network

Cable a network that is similar to the one in the topology diagram. Assign the IP addresses and configure the VLANs as shown in the tables so the PCs in the same VLAN can communicate, then make the necessary modifications to enable Inter-VLAN routing using router on stick method.

Sol:

****on Switch 1

SW1(config)# VLAN 10

#name DEV

#VLAN 11

#name HR

#VLAN 20

#name ACC

#VLAN 90

#name Native

#int f 0/1

#switchport mode access

#switchport access VLAN 10

#int f 0/2

#switchport mode access

#switchport access VLAN 11

#int f 0/3

#switchport mode trunk

#switchport trunk native VLAN 90

****on Switch 2

SW2(config)# VLAN 10

#name DEV

#VLAN 11

#name HR

#VLAN 20

#name ACC

#VLAN 90

#name Native

#int f 0/1

#switchport mode access

#switchport access VLAN 10

#int f 0/2

#switchport mode access

#switchport access VLAN 20

#int f 0/3

#switchport mode trunk

#switchport trunk native VLAN 90

****on Switch 3

SW3(config)# VLAN 10

#name DEV

#VLAN 11

#name HR

#VLAN 20

#name ACC

#VLAN 90

#name Native

#int f 0/1

#switchport mode access

#switchport access VLAN 11

#int f 0/2

#switchport mode access

#switchport access VLAN 20

#int f 0/3

#switchport mode trunk

#switchport trunk native VLAN 90

****on Switch 4

SW4(config)# VLAN 10

#name DEV

#VLAN 11

#name HR

#VLAN 20

#name ACC

#VLAN 90

#name Native

#int f 0/1

#switchport mode trunk

#switchport trunk native VLAN 90

#int f 0/2

#switchport mode trunk

#switchport trunk native VLAN 90

#int f 0/3

#switchport mode trunk

#switchport trunk native VLAN 90

***on Router

#Config on Router:

R(config)# int g0/0

no shutdown

int g0/0.10

encapsulation dot1q 10

IP address 192.168.1.1 255.255.255.0

int g0/0.11

encapsulation dot1q 11

IP address 192.168.2.1 255.255.255.0

int g0/0.20

encapsulation dot1q 20

IP address 192.168.3.1 255.255.255.0

****PCs

بندخل عليه من desktop

بعدين IP configuration

عبي هدول

IP: ……..

Subnet: ……

Gateway: ……