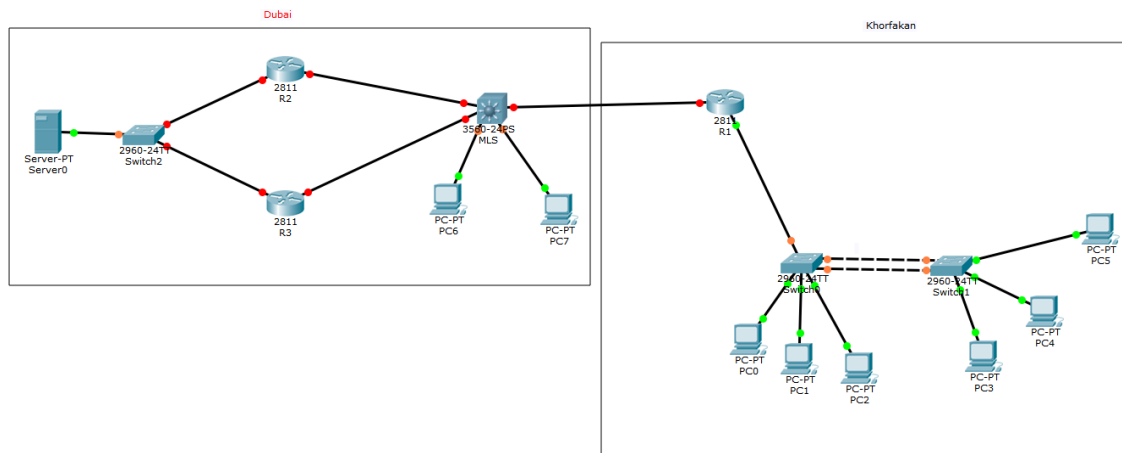


200-125 CCNA Lab 1

Your network divides to Two Segments

First segment is called “Khorfakan” , where you need to conduct the following tasks:

Part 1 SW1 & SW2

1-change switch 0 name to SW1 , switch 1 name to SW2 , both switches should belong to domain name “kh”

2-In SW1 & SW2 create vlan 2 , 3 and 4 with no names assigned to them.

3- In SW1 & SW2 assign interface f0/2 to vlan 2 , f0/3 to vlan 3 , f0/4 to vlan 4

4-Create Layer 2 etherchannel link between SW1 & SW2 G0/1 and G0/2 interfaces with following requirements:

- Use standard protocol to create your logical link number 1
- Make sure SW1 is the switch responsible to start up the etherchannel link negotiation
- Change port channel interface to trunk in both switches

5-Create Management interface in SW1 for VLAN 1 using IP address 1.0.0.50/8 and Default gateway 1.0.0.1

6- Create Management interface in SW2 for VLAN 2 using IP address 2.0.0.50/8 and Default gateway 2.0.0.1

7-Enable SSHv2 in SW1 & SW2 using username “kh” and password type 5 “cisco” , make sure only SSH allowed for remote connection to both switches

8-SW1 f0/24 will be connected to R1 for Inter VLAN Router on Trunk (Stick) so make sure its configured as trunk.

SW1

```
ena
config t
hostname sw1
ip domain-name kh

vlan 2
vlan 3
vlan 4

int range g0/1 - 2
channel-group 1 mode active
int port-channel 1
sw mo tr

int vlan 1
ip add 1.0.0.50 255.0.0.0
no sh
exit
ip default-gateway 1.0.0.1

username kh sec cisco
ena cisco
crypto key generate rsa
1024
line vty 0 4
login local
trans input ssh
exit
ip ssh version 2

int f0/24
sw mo tr

int f0/2
sw acc vlan 2
int f0/3
sw acc vlan 3
int f0/4
sw acc vlan 4
```

SW2

```
ena
config t
hostname sw2
ip domain-name kh

vlan 2
vlan 3
vlan 4

int range g0/1 - 2
channel-group 1 mode passive
int port-channel 1
sw mo tr

int vlan 2
ip add 2.0.0.50 255.0.0.0
no sh
exit
ip default-gateway 2.0.0.1

username kh sec cisco
ena cisco
crypto key generate rsa
1024
line vty 0 4
login local
trans input ssh
exit
ip ssh version 2

int f0/2
sw acc vlan 2
int f0/3
sw acc vlan 3
int f0/4
sw acc vlan 4
```

```
sw1#sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23
2	VLAN0002	active	Fa0/2
3	VLAN0003	active	Fa0/3
4	VLAN0004	active	Fa0/4
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
sw1#
```



```
sw1#sh interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Pol	on	802.1q	trunking	1
Fa0/24	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Pol	1-1005
Fa0/24	1-1005

Port	Vlans allowed and active in management domain
Pol	1,2,3,4
Fa0/24	1,2,3,4

Port	Vlans in spanning tree forwarding state and not pruned
Pol	1,2,3,4
Fa0/24	1,2,3,4

9-configure message of the day banner for SW1 & SW2 with message This is SW# where # is the id of the switch , banner should show to users whatever they connected with SSH or console

10-configure interfaces f0/2 , f0/3 and f0/4 with following requirements:

- Should move to forward state once cable connected to it
- Should not accept any BPDU frames
- Disable cisco proprietary discovery protocol
- Make sure Traffic coming only from one MAC address which should be saved in the switches even after reload , if violation happens interfaces should go to err-disable states

11-Console connection should be secured with same username and password we created in step 7

12-Disable exec Timeout for console and ssh

13- Prevents every logging output from immediately interrupting your console session.

14- Change the size of the history buffer for that session to 256 lines

SW1

```
ena
config t
banner motd # This is SW1 #
```

SW2

```
ena
config t
banner motd # This is SW2 #
```

SW1 & SW2

```
int range f0/2 - 4
span portfast
span bpduguard enable
no cdp enable
sw mo acc
sw po
sw po max 1
sw po mac-address sticky
sw po vio sh
exit
```

```
line con 0
motd-banner
login local
exec-timeout 0
logging synchronous
history size 256
```

```
line vty 0 4
motd-banner
exec-timeout 0
logging synchronous
history size 256
```

```
sw1#show po
sw1#show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/2	1	1	0	Shutdown
Fa0/3	1	1	0	Shutdown
Fa0/4	1	1	0	Shutdown

```
sw1#sh run | begin interface
interface Port-channel 1
  switchport mode trunk
!
interface FastEthernet0/1
!
interface FastEthernet0/2
  switchport access vlan 2
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0007.EC3E.30A8
  no cdp enable
  spanning-tree portfast
  spanning-tree bpduguard enable
!
interface FastEthernet0/3
  switchport access vlan 3
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0006.2A3A.97A8
  no cdp enable
  spanning-tree portfast
  spanning-tree bpduguard enable
!
interface FastEthernet0/4
  switchport access vlan 4
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 00D0.BA0A.4501
  no cdp enable
  spanning-tree portfast
  spanning-tree bpduguard enable
!
```

Part2 R1

1-Assign R1 f0/1 to IP address 40.40.40.1/24

2-Configure R1 to support routing between VLAN 1,2,3,4 for SW1 &SW2 using the following requirements:

- For VLAN 1 , R1 IP address will be 1.0.0.1
- For VLAN 2 , R1 IP address will be 2.0.0.1
- For VLAN 3 , R1 IP address will be 3.0.0.1
- For VLAN 4 , R1 IP address will be 4.0.0.1

3-Configure R1 as DHCP server for any machine connected to VLAN 1 , 2 , 3 ,4 in SW1 & SW2 using the following requirements :

- For VLAN 1 , R1 DHCP IP address range will be from 1.0.0.100 to 1.0.0.200 ONLY
- For VLAN 2 , R1 DHCP IP address range will be from 2.0.0.100 to 2.0.0.200 ONLY
- For VLAN 3 , R1 DHCP IP address range will be from 3.0.0.100 to 3.0.0.200 ONLY
- For VLAN 4 , R1 DHCP IP address range will be from 4.0.0.100 to 4.0.0.200 ONLY

R1

```
ena
```

```
config t
```

```
ip dhcp excluded-address 1.0.0.1 1.0.0.99
```

```
ip dhcp excluded-address 1.0.0.201 1.255.255.255
```

```
ip dhcp excluded-address 2.0.0.1 2.0.0.99
```

```
ip dhcp excluded-address 2.0.0.201 2.255.255.255
```

```
ip dhcp excluded-address 3.0.0.1 3.0.0.99
```

```
ip dhcp excluded-address 3.0.0.201 3.255.255.255
```

```
ip dhcp excluded-address 4.0.0.1 4.0.0.99
```

```
ip dhcp excluded-address 4.0.0.201 4.255.255.255
```

```
ip dhcp pool vlan1
```

```
network 1.0.0.0 255.0.0.0
```

```
default-router 1.0.0.1
```

```
ip dhcp pool vlan2
```

```
network 2.0.0.0 255.0.0.0
```

```
default-router 2.0.0.1
```

```
ip dhcp pool vlan3
```

```
network 3.0.0.0 255.0.0.0
```

```
default-router 3.0.0.1
```

```
ip dhcp pool vlan4
```

```
network 4.0.0.0 255.0.0.0
```

```
default-router 4.0.0.1
```

```
int f0/0
```

```
no ip add
```

```
no sh
```

```
int f0/0.1
```

```
encap dot 1
```

```
ip add 1.0.0.1 255.0.0.0
```

```

int f0/0.2
encap dot 2
ip add 2.0.0.1 255.0.0.0
int f0/0.3
encap dot 3
ip add 3.0.0.1 255.0.0.0

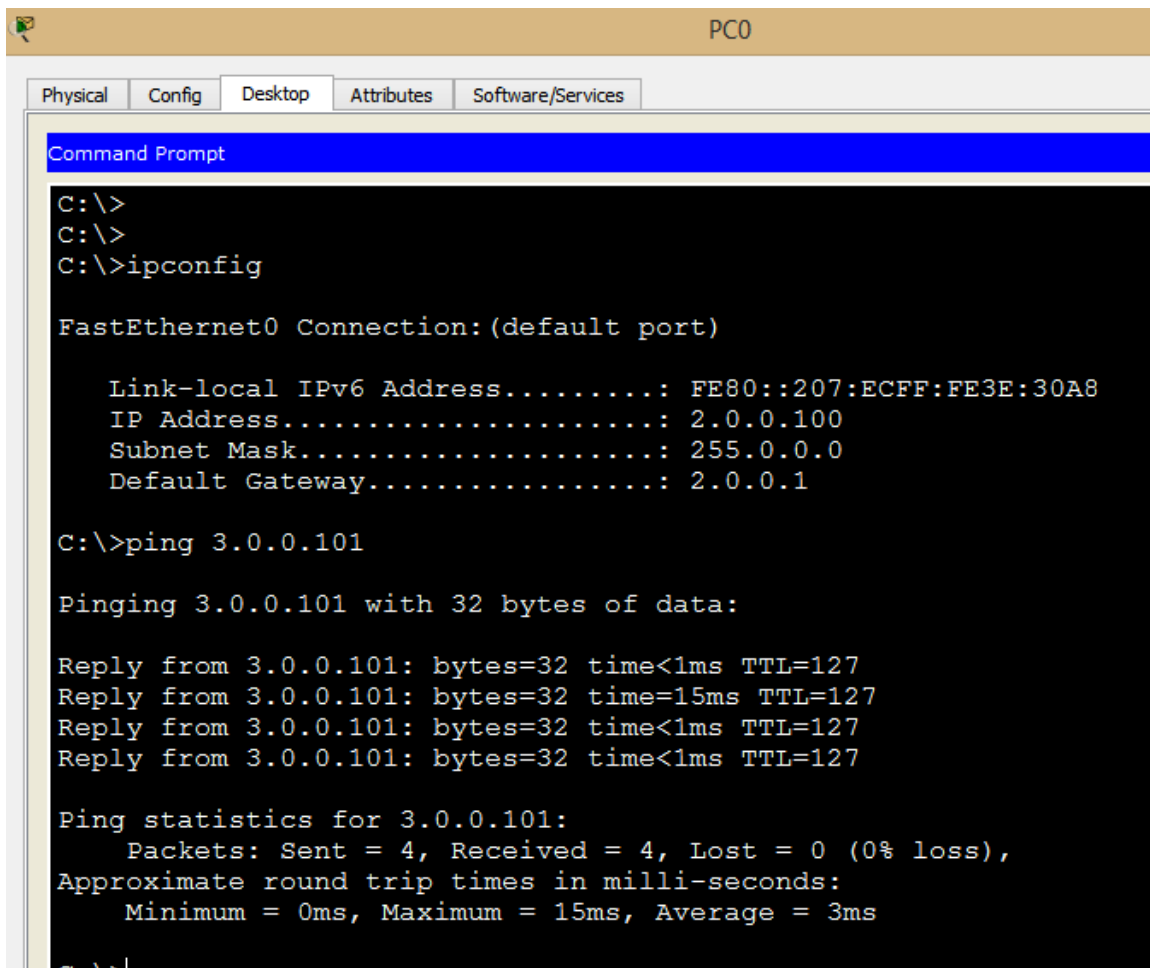
int f0/1
ip add 40.40.40.1 255.255.255.0
no sh

```

R1#sh ip dhcp binding

IP address	Client-ID/ Hardware address	Lease expiration	Type
2.0.0.100	0007.EC3E.30A8	--	Automatic
2.0.0.101	0090.0C93.A686	--	Automatic
3.0.0.100	0006.2A3A.97A8	--	Automatic
3.0.0.101	0003.E4C8.7D69	--	Automatic
4.0.0.100	00D0.BA0A.4501	--	Automatic
4.0.0.101	0002.176D.AD92	--	Automatic

R1#



Part 3 MLS

- 1-Configure Multilayer Switch hostname to MLS
- 2-Enable Routing capabilities in MLS
- 3-Create VLAN 100 with name Sales_dept, VLAN 200 with name IT_dept
- 4- Assign interface f0/4 to VLAN 100 , f0/5 to VLAN 200
- 5- Enable routing between VLAN 100 & VLAN 200 using MLS SVI (Switch Virtual Interface) with following requirements:
VLAN 100 IP address 100.0.0.50 /8
VLAN 200 IP address 200.0.0.50/24
- 6-Change interfaces f0/1 , f0/2 and f0/3 to Layer 3 interfaces with following requirements:
F0/1 IP address 11.0.0.50/8
F0/2 IP address 12.0.0.50/8
F0/3 IP address 40.40.40.50/24

MLS

```
ena
config t
vlan 100
name Sales_dept
vlan 200
name IT_dept
ip routing
hostname MLS

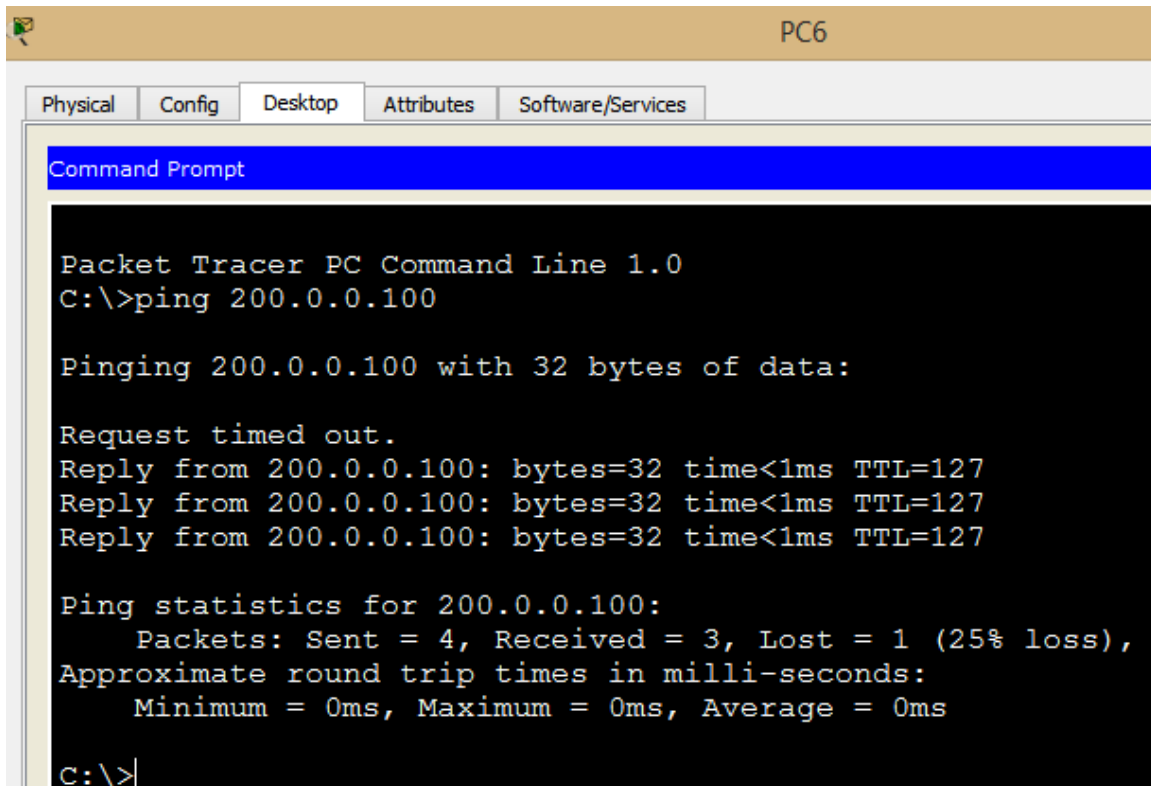
int f0/1
no sw
ip add 11.0.0.50 255.0.0.0
no sh
int f0/2
no sw
ip add 12.0.0.50 255.0.0.0
no sh
int f0/3
no sw
ip add 40.40.40.50 255.255.255.0
no sh
int vlan 100
ip add 100.0.0.50 255.0.0.0
no sh
int vlan 200
ip add 200.0.0.50 255.255.255.0
no sh
int f0/4
sw acc vlan 100
int f0/5
sw acc vlan 200
```

```
MLS#sh ip route c
```

```
C 11.0.0.0/8 is directly connected, FastEthernet0/1
C 12.0.0.0/8 is directly connected, FastEthernet0/2
C 40.40.40.0/24 is directly connected, FastEthernet0/3
C 100.0.0.0/8 is directly connected, Vlan100
C 200.0.0.0/24 is directly connected, Vlan200
```

```
MLS#sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
100	VLAN0100	active	Fa0/4
200	VLAN0200	active	Fa0/5
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	



Part 4 R2 & R3

1-Configure R2 interface f0/0 Ip address to 10.0.0.2/8 and f0/1 to 11.0.0.2/8

2-Configure R3 interface f0/0 Ip address to 10.0.0.3/8 and f0/1 to 12.0.0.3/8

3-Configure Cisco High availability protocol that normally use multicast address 224.0.0.102 for R2 & R3 with following requirements:

- Use group number 1
- Make sure R2 is the Primary Router while R3 is the secondary
- R2 will need to preempt R3 when it come back from down state
- Virtual IP should be 10.0.0.1
- R2 should track his interface connected to external networks

R2

```
ena
```

```
config t
```

```
int f0/1
```

```
ip add 11.0.0.2 255.0.0.0
```

```
no sh
```

```
int f0/0
```

```
ip add 10.0.0.2 255.0.0.0
```

```
no sh
```

```
standby 1 ip 10.0.0.1
```

```
standby 1 priority 120
```

```
standby 1 preempt
```

```
standby 1 track fastEthernet 0/1
```

R3

```
ena
```

```
config t
```

```
int f0/1
```

```
ip add 12.0.0.3 255.0.0.0
```

```
no sh
```

```
int f0/0
```

```
ip add 10.0.0.3 255.0.0.0
```

```
no sh
```

```
standby 1 ip 10.0.0.1
```

```
R3#sh standby
FastEthernet0/0 - Group 1
  State is Standby
    10 state changes, last state change 00:00:49
  Virtual IP address is 10.0.0.1
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.44 secs
  Preemption disabled
  Active router is 10.0.0.2, priority 120 (expires in 7 sec)
    MAC address is 0000.0C07.AC01
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Fa0/0-1 (default)
R3#
```

Part 5 Routing Protocol EIGRP

Configure EIGRP AS number 100 in R1 , R2 , R3 and MLS

Verify by making Server connected to R2 & R3 subnet 10.0.0.0/8 to SSH SW1 and SW2

R1

```
ena
config t
router eigrp 100
no auto
network 1.0.0.0 0.255.255.255
network 2.0.0.0 0.255.255.255
network 3.0.0.0 0.255.255.255
network 4.0.0.0 0.255.255.255
network 40.40.40.0 0.0.0.255
```

MLS

```
ena
config t
router eigrp 100
no auto
network 11.0.0.0 0.255.255.255
network 12.0.0.0 0.255.255.255
network 100.0.0.0 0.255.255.255
network 40.40.40.0 0.0.0.255
network 200.0.0.0 0.0.0.255
```

R2

```

ena
config t
router eigrp 100
no auto
network 11.0.0.0 0.255.255.255
network 10.0.0.0 0.255.255.255

```

R3

```

ena
config t
router eigrp 100
no auto
network 12.0.0.0 0.255.255.255
network 10.0.0.0 0.255.255.255

```

```
R2#sh ip route
```

```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

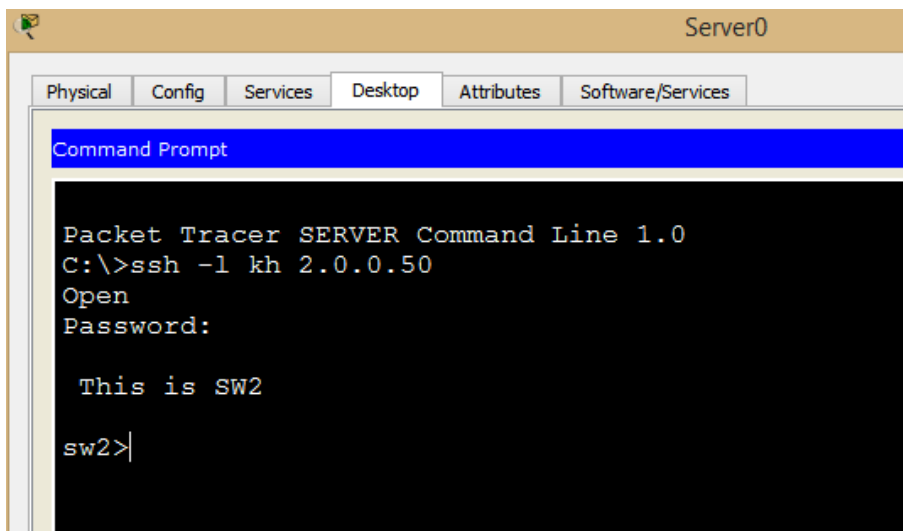
```

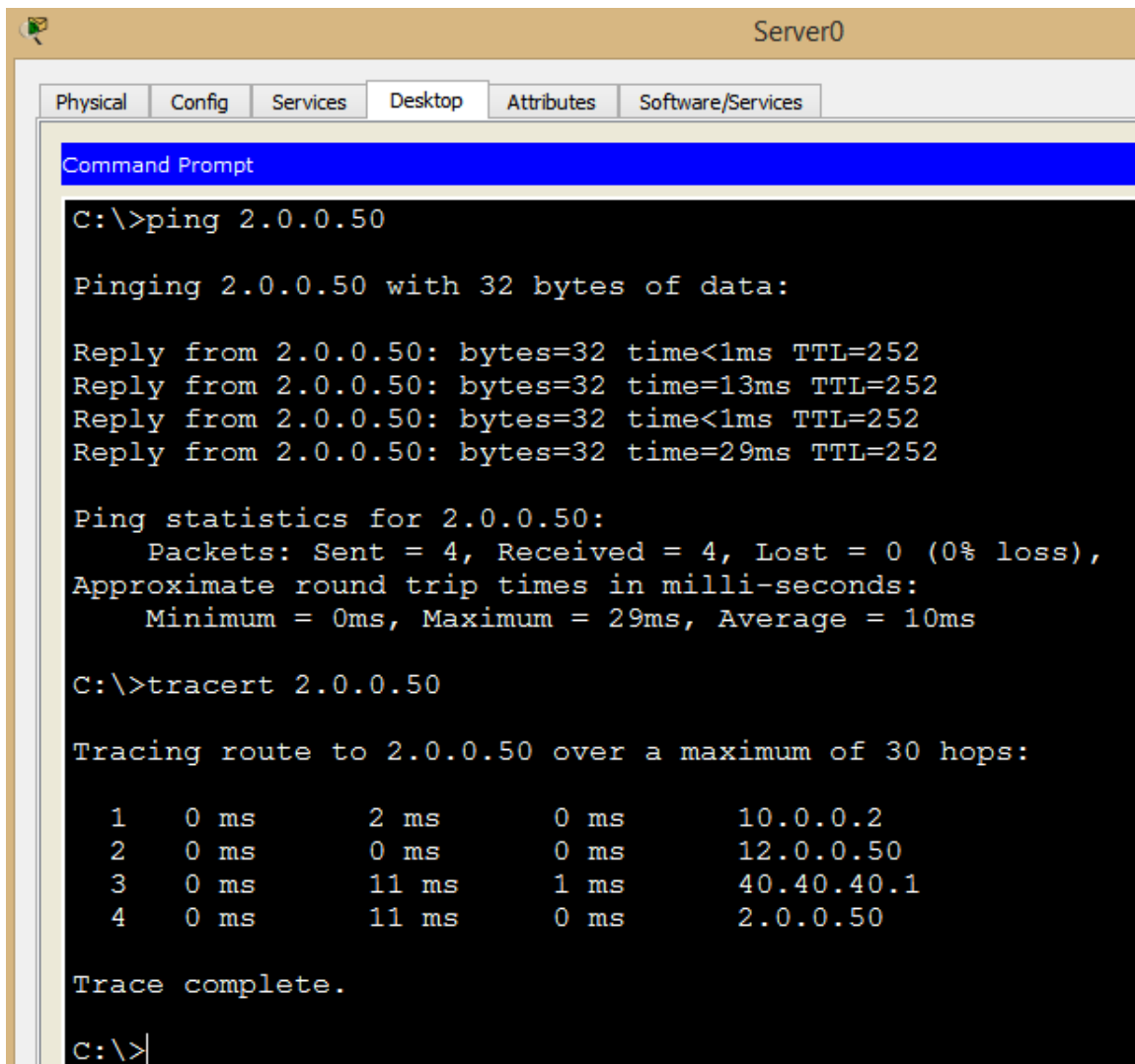
```
Gateway of last resort is not set
```

```

D    1.0.0.0/8 [90/33280] via 11.0.0.50, 00:06:20, FastEthernet0/1
D    2.0.0.0/8 [90/33280] via 11.0.0.50, 00:06:20, FastEthernet0/1
D    3.0.0.0/8 [90/33280] via 11.0.0.50, 00:06:20, FastEthernet0/1
D    4.0.0.0/8 [90/33280] via 11.0.0.50, 00:06:20, FastEthernet0/1
C    10.0.0.0/8 is directly connected, FastEthernet0/0
C    11.0.0.0/8 is directly connected, FastEthernet0/1
D    12.0.0.0/8 [90/30720] via 11.0.0.50, 00:06:20, FastEthernet0/1
     [90/30720] via 10.0.0.3, 00:05:48, FastEthernet0/0
D    40.0.0.0/24 is subnetted, 1 subnets
     40.40.40.0 [90/30720] via 11.0.0.50, 00:06:20, FastEthernet0/1
D    100.0.0.0/8 [90/25628160] via 11.0.0.50, 00:06:20, FastEthernet0/1
D    200.0.0.0/24 [90/25628160] via 11.0.0.50, 00:06:20, FastEthernet0/1

```





Server0

Physical Config Services Desktop Attributes Software/Services

Command Prompt

```
C:\>ping 2.0.0.50

Pinging 2.0.0.50 with 32 bytes of data:

Reply from 2.0.0.50: bytes=32 time<1ms TTL=252
Reply from 2.0.0.50: bytes=32 time=13ms TTL=252
Reply from 2.0.0.50: bytes=32 time<1ms TTL=252
Reply from 2.0.0.50: bytes=32 time=29ms TTL=252

Ping statistics for 2.0.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 29ms, Average = 10ms

C:\>tracert 2.0.0.50

Tracing route to 2.0.0.50 over a maximum of 30 hops:

  0  0 ms    2 ms    0 ms    10.0.0.2
  1  0 ms    0 ms    0 ms    12.0.0.50
  2  0 ms   11 ms    1 ms    40.40.40.1
  3  0 ms   11 ms    0 ms    2.0.0.50

Trace complete.

C:\>
```

Part 6 ACL

1-Configure SW2 to accept SSH connections from Server 10.0.0.100 and PC 2.0.0.100 ONLY

2-Configure PC 2.0.0.100 to be the only machine in VLAN 2 allowed to access Web server 10.0.0.100

3-Configure R2 & R3 to be able to ping any machine but never respond to ping requests coming from any machine.

SW2

```
ena
config t
access-list 1 permit host 10.0.0.100
access-list 1 permit host 2.0.0.100
line vty 0 4
access-class 1 in
```

R1

```
ena
config t
access-list 100 permit tcp host 2.0.0.100 host 10.0.0.100 eq 80
access-list 100 deny tcp 2.0.0.0 0.255.255.255 host 10.0.0.100 eq 80
access-list 100 permit ip any any
```

```
interface FastEthernet0/0.2
ip access-group 100 in
```

R2 & R3

```
ena
config t
access-list 100 permit icmp host 10.0.0.100 any echo
access-list 100 deny icmp host 10.0.0.100 any echo-reply
access-list 100 permit ip any any
int f0/0
ip access-group 100 in
```

Part 7 GRE

- 1-Create loopback interface 1 in R1 with IP address 192.168.101.1/24
- 2-Create loopback interface 3 in R3 with IP address 192.168.103.3/24
- 3-make sure R1&R3 will advertise these loopbacks to each other's using RIPv2
- 4-RIPv2 should be running in R1 & R3 ONLY
- 5-IP address if using tunnels should 200.200.200.#/24 where # is the router id
- 6-use extended ping to verify that R1 loopback can ping R2 loopback

R1

```
ena
config t
int loop 1
ip add 192.168.101.1 255.255.255.0
```

```
int tunnel 1
ip add 200.200.200.1 255.255.255.0
tunnel source f0/1
tunnel destination 12.0.0.3
```

```
router rip
ver 2
no auto
network 192.168.101.0
network 200.200.200.0
```

R3

```
ena
config t
int loop 3
ip add 192.168.103.3 255.255.255.0
```

```
int tunnel 1
ip add 200.200.200.3 255.255.255.0
tunnel source f0/1
tunnel destination 40.40.40.1
```

```
router rip
ver 2
no auto
network 192.168.103.0
network 200.200.200.0
```

Extended ping

```
Protocol [ip]:
Target IP address: 192.168.103.3
Extended commands [n]: y
Source address or interface: 192.168.101.1
```


Part 8 network management

- 1-Configure R1 ,R2 ,R3 & MLS to use server 10.0.0.100 as secure NTP server using key 1 "cisco" & Syslog server
- 2-Enable SNMP in R2 & R3 using password "cisco" for set and get messages
- 3-Enable telnet in R3 using server 10.0.0.100 as AAA server as first authentication method and in case it down R3 should use local username and password
- 4-Configure R2 to use server 10.0.0.100 as FTP server using username "cisco" & password "cisco"
- 5-Send copy of R2 running configuration to server 10.0.0.100 using FTP protocol
- 6-Send copy of R3 running configuration to server 10.0.0.100 using TFTP protocol
- 7-Make sure you do not use any boot system commands in R3
- 8-Make sure R2 can ping or telnet R3 using name "standby"
- 9-Change local username in R3 to "Yasser" instead of "kh" using password recovery procedures

R1 ,R2 ,R3 & MLS

```
ena
config t
ntp authentication-key 1 md5 cisco
ntp authenticate
ntp trusted-key 1
ntp server 10.0.0.100 key 1

logging on
logging host 10.0.0.100
service timestamps log datetime msec
service timestamps debug datetime msec
```

R2 & R3

```
ena
config t
snmp-server community cisco rw
```

R3

```
ena
config t
username kh sec cisco
ena cisco
line vty 0 4
login authentication default
exit
aaa new-model
aaa authentication log default group radius local
radius-server host 10.0.0.100
```

R2

```
ip ftp username cisco
ip ftp password cisco
ip host standby 10.0.0.3
```

```
R2#ping standby
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

```
R2#copy run ftp
```

```
Address or name of remote host []? 10.0.0.100
```

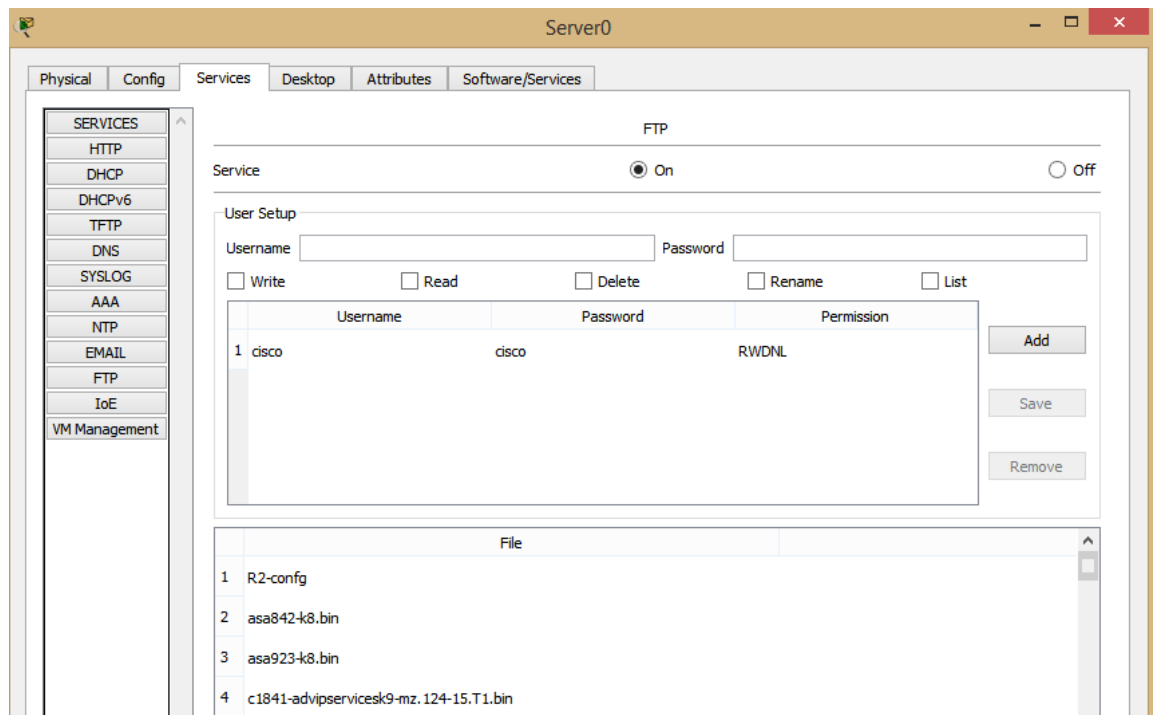
```
Destination filename [R2-config]?
```

```
Writing running-config...
```

```
[OK - 800 bytes]
```

```
800 bytes copied in 0.043 secs (18000 bytes/sec)
```

```
R2#
```



R3

- 1-connect your router using console cable
- 2-turn off turn on your router
- 3-press ctrl+pause break
- 4-**confreg to 0x2142**
- 5-**reset**
- 6-n
- 7-ena
- 8-**copy start run**
- 9-config t
- 10- no username kh secret cisco
- 11- username Yasser secret cisco
- 12-**confreg-register 0x2102**
- 13-exit
- 14-copy run start

See you in Lab 2 where we will cover the following topics:

- Cisco Router as DHCP relay agent
- OSPFv2 multiple areas
- NAT static, dynamic and PAT
- BGP
- PPP with CHAP
- IOS 15 Licensing

Later Lab3 we will cover IPv6 with OSPFv3 and EIGRPv6

Finally this series should finished with Lab4 Troubleshooting with 10 Tickets to solve , each ticket will have at least two faults

Good Luck

CCIE & CCSI: Yasser Auda

<https://www.facebook.com/YasserRamzyAuda>

<https://learningnetwork.cisco.com/people/yasserramzy/content>

<https://www.youtube.com/user/yasserramzyauda>