CCENT LAB

26 Basic Lab Documentation

update 05-07-2018

D ID IT AJI SEPTIA WAN

LIST OF CONTENTS

I. BAB 1 – TCP/IP 1

1. Basic Subnetting Calculation Lab..... .... 2 2. Fast Subnetting Calculation Lab .... 2 3. IPv4 Address Configuration Lab .... 4 4. IPv4 Subnetting Lab .... 6 5. Variables Lab Length Subnet Masking (VLSM) 7

6. Lab Pengenalan IPv6 12
7. Lab Soal IPv6 13
8. Lab Packet Tracer IPv6 14
9. Lab Dasar Command Line Interface Cisco 16

II. BAB 2 – SWITCHING 19

10. Lab Dasar Virtual Local Area Network (VLAN) 20
11. Lab VLAN Trunk 23
12. Lab Cisco Discovery Protocol 26
13. Lab Static Port Security 28

III. BAB 3 – ROUTING 31

14. Lab Inter-VLAN Routing Router-on-a-stick 32
15. Lab Static Routing IPv4 35
16. Lab Static Routing IPv6 39
17. Lab Routing Information Protocol version 2 (RIPv2) IPv4 41

IV. BAB 4 – INFRASTRUCTURE SERVICES 46

18. Lab DHCPv4 Server, DHCP Relay dan DHCP Client 47
19. Lab Standart AccessList (ACL) 48
20. Lab Static NAT 54
21. Lab Dynamic NAT 56
22. Lab NAT Overloaded atau Port Address Translation (PAT) 59

V. BAB 5 – INFRASTRUCTURE MAINTENANCE 65

23. Lab Devices Monitoring dengan Syslog 65
24. Lab Network Time Protocol (NTP) 67
25. Lab Backup dan Restore iOS TFTP 75
26. Lab Cisco Troubleshoot tools 77

CHAPTER 1

TCP/IP

Basic Subnetting Calculation Lab 2
Fast Subnetting Calculation Lab 2
IPv4 Address Configuration Lab 4
Lab Subnetting IPv4 6
Lab Variabel Length Subnet Masking (VLSM) 7
Lab Pengenacion IPv6 12
Lab Soal IPv6 13
Lab Packet Tracer IPv6 14
Lab Dasar Command Line Interface Cisco 16

1. Basic Subnetting Calculation Lab

Given the IP Address 192.168.10.0 with subnet 255.255.255.128 or CIDR /25, determine the subnet, Valid Subnet, Number of hosts per Subnet, Broadcast Address and Valid Address ?

Subnet: 255.255.255.128, where 128 if converted into binary numbers becomes 10000000, and to find the subnet/network, use the number 1 in powers of 2,
so 21=2

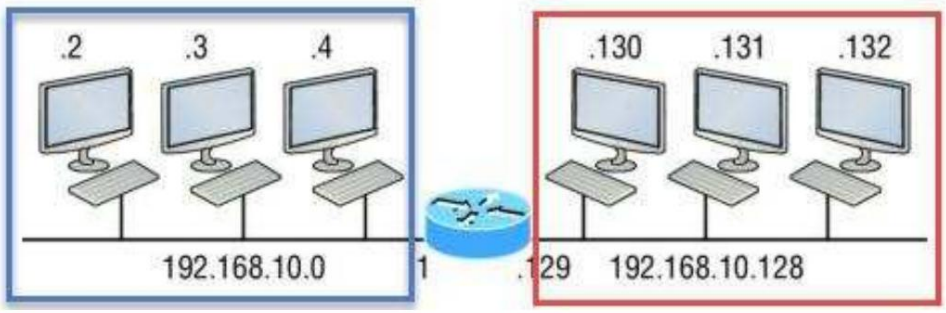
Valid Subnet: 256-128 = 128. Subnets always start from 0, so the first subnet is 0, and the second is 128

Number of hosts per subnet: 128 if converted to 10000000, because looking for a host the number 0 is used, so 27 -2 = 126 valid hosts

Table. Basic subnetting

Subnet's	1	2
Subnet Address 192.168.10.0		192.168.10.128
FirstValid	192.168.10.1	192.168.10.129
LastValid	192.168.10.126 192	168.10.254
Broadcast	192.168.10.127 192	168.10.255

If applied in a network



Picture. Application of subnetting on networks

The two blue and red networks cannot communicate with each other, because they have different subnet addresses.

2. Fast Subnetting Calculation Lab

Question : Determine which subnet/network the IP address is 192.168.93.210 with Subnet Mask 255.255.255.248 !

Is known

IP Address : 192.168.93.210

Subnetmask: 255.255.255.248 or /29

Answer

/32 -/29 = 3 = 23=8 # The number 32 is a fixed number!

210/8 = 26.25 # The number 210 is taken from the tail at address 192.168.93.210

26x8 = 208

Range = 192.168.93.208 – 192.168.93.215

Network = 192.168.93.208

Broadcast = 192.168.93.215

First Valid = 192.168.93.209

Last Valid = 192.168.93.214

So the network/subnet is at 192.168.93.208

Next class B in a fast way,

Question : Determine the broadcast address from 10.48.128.0 255.255.240.0!

Is known

IP Address : 10.48.128.0

Subnetmask: 255.255.240.0 or /20

Answer

/20+8 = /28 # The number 8 is a special fixed number in class B!

/32-/28 = 4 = 24 =16

Number of hosts = 16x256 = 4096 # The number 256 is a fixed number!

128/16 = 8 # The number 128 is taken from the address 10.48.128.0!

8x16 = 128

Range = 10.48.128.0 – 10.48.143.255

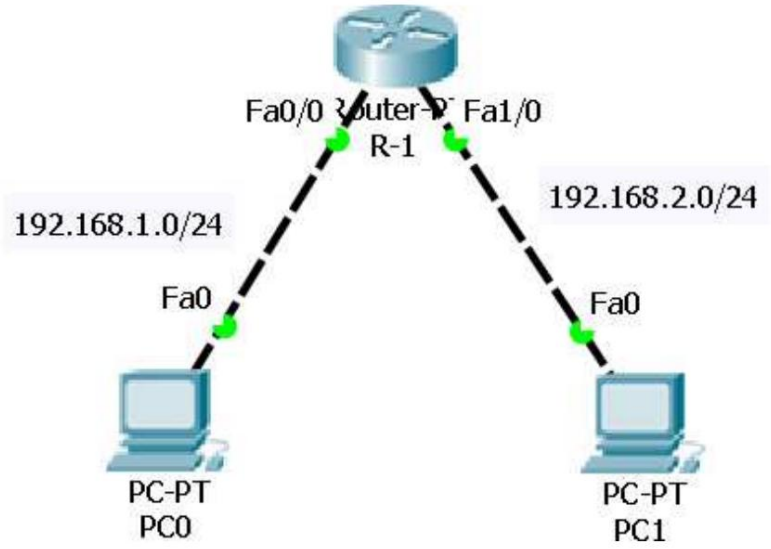
Network = 10.48.128.0

Broadcast = 10.48.143.255

First Valid = 10.48.128.1

Last Valid = 10.48.143.255

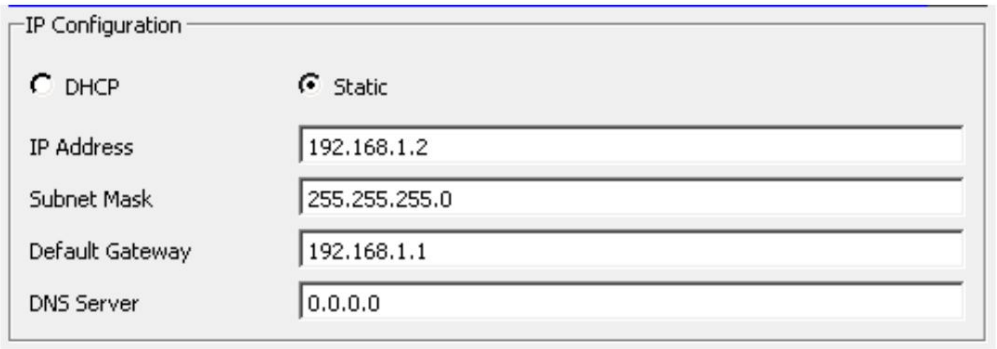
3. IPv4 Address Configuration Lab



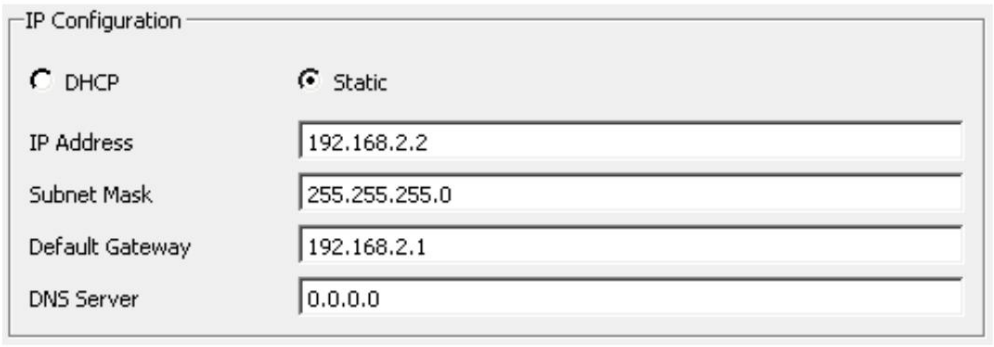
Picture. Basic network topology

R-1 configuration

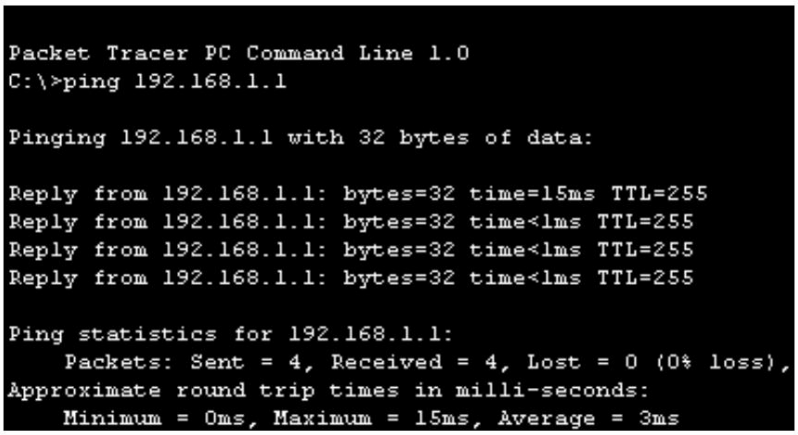
```
Router#configure terminal
Router(config)#hostname R-1
R-1(config)#
R-1(config)#interface fastEthernet 0/0
R-1(config-if)#ip address 192.168.1.1 255.255.255.0
R-1(config-if)#no shutdown
R-1(config)#interface fastEthernet 1/0
R-1(config-if)#ip address 192.168.2.1 255.255.255.0
R-1(config-if)#no shutdown
```



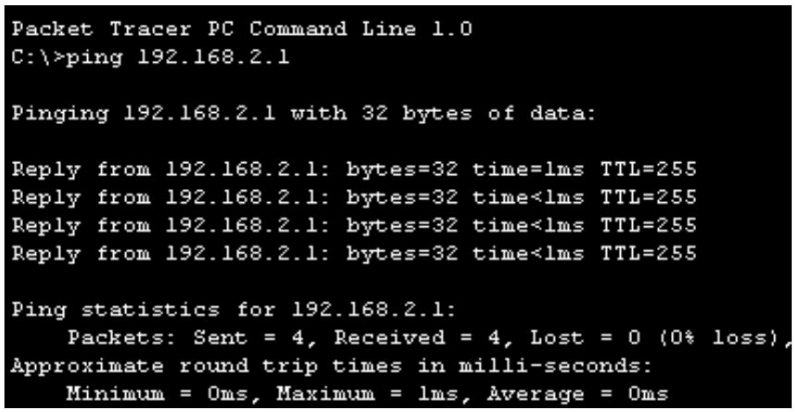
Picture. PC0 Configuration



Picture. PC1 configuration

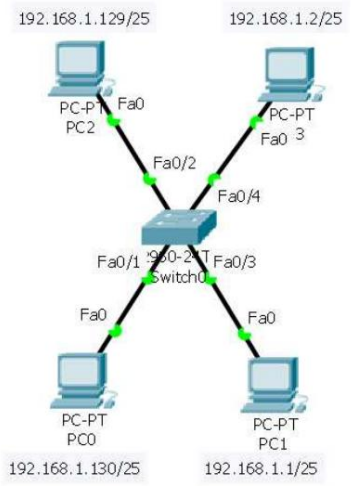


Picture. Testing from PC0 to R-1

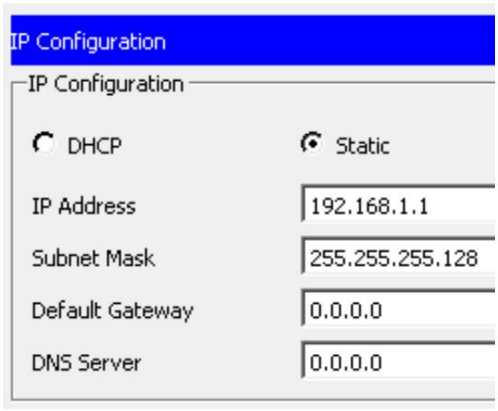


Picture. Testing from PC1 to R-1

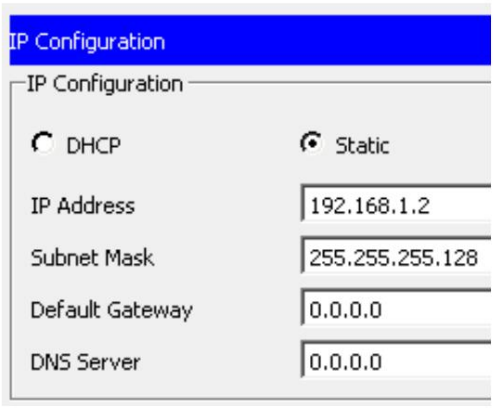
4. Lab Subnetting IPv4



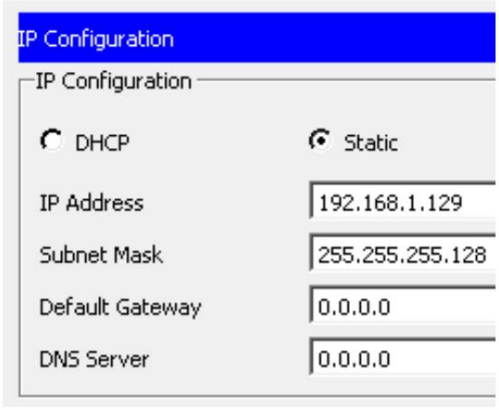
Picture. Subnetting uses /25



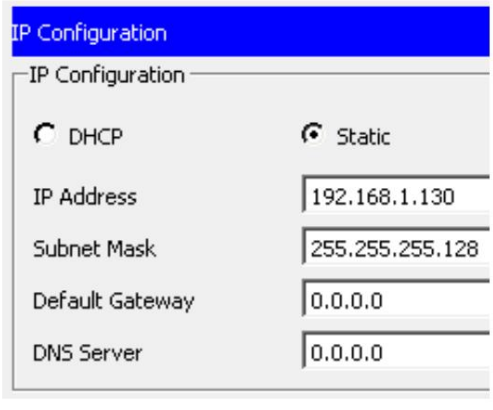
Picture. PC 1



Picture. PC 3



Picture. PC 2



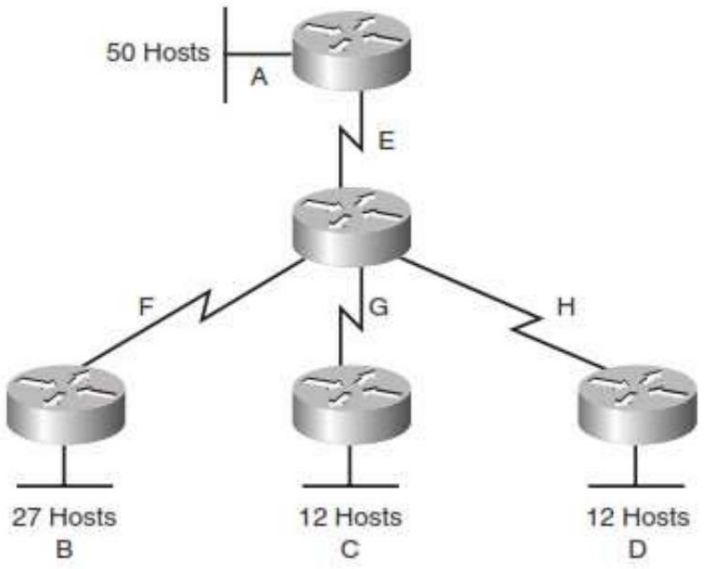
Picture. PC 4

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.130

Pinging 192.168.1.130 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.130:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Picture. Testing subnetting on other networks

An example of a test is pinging from 192.168.1.1 to 192.168.1.2 and the result should be "Reply from...". If you ping 192.168.1.130 the result is "Request timed out", because it has a different subnet mask/ different network.

5. Lab Variabel Length Subnet Masking (VLSM)



Picture. Example of implementing VLSM

Question :

Provided IP Address 192.168.77.0/24, determine the allocation of each Address according to the number of hosts required in the topology above,

Answer :

a. Create a table of the largest needs first, sorting them by the largest number of hosts

Table. Host requirements

No Network Jumlah Host		
1	A	50
2	B	27
3	C	12
4	D	12
5	AND	2
6	F	2
7	G	2
8	H	2

b. Provide a table like the following to aid understanding

Table. CIDR for class C networks

CIDR Subnetmask	Number of Subnets	Number of Hosts
/25 255.255.255.128 2 subnets /26 255.255.255.192 4		124
subnets /27 255.255.255.224 8 subnets /28		62
255.255.255.240 16 subnets /29 255.255.255.248 32		30
subnets /30 255.255.255.252 64 subnets		14
		6
		2

c. Look for a subnet with a number of hosts that can accommodate the host criteria above. On network A, it must be able to accommodate 50 hosts. Therefore, Subnet A is appropriate to use /26 62 hosts (see Table. CIDR for class C networks)

Tabel. /26 -- 4 Subnets -- 62 Hosts/Subnet Network #

IP Range Broadcast .1-.62 .65-.126		
.0		.63
.64		.127
.128	.129-.190	.191
.192	.193-.254	.255

d. Enter it into the main table, then the IP Address from 0-64 cannot be used anymore.

Subnet Name	Needed Size	Allocated Size	Address Mask Subnetmask		Assignable Range	Broadcast
A	50	62	192.168.77.0 /26 255.255.255.192	192.168.77.1 - 192.168.77.62		192.168.77.63

e. Next is 27 hosts, then /27 is suitable to use (see Table. CIDR for network class C).

Tabel./27 -- 8 Subnets -- 30 Hosts/Subnet

Network #	IP Range	Broadcast .1-.30
.0		.31
.32	.33-.62	.63
.64	.65-.94	.95
.96	.97-.126	.127
.128	.129-.158	.159
.160	.161-.190	.191
.192	.193-.222	.223
.224	.225-.254	.255

The part colored red means it can no longer be used, so use the next network

Subnet Name	Needed Size	Allocated Size	Address	Mask	Subnetmask	Assignable Range /	Broadcast
A	50	62	192.168.77.0	26	255.255.255.192	192.168.77.1 - 192.168.77.62	192.168.77.63
B	27	30	192.168.77.64 /27		255.255.255.224	192.168.77.65 - 192.168.77.94	192.168.77.95

f. Furthermore, 12 hosts can be accommodated by /28 (see Table CIDR for network class C).

Tabel./28 -- 16 Subnets -- 14 Hosts/Subnet

Network #	IP Range	Broadcast .0 .1-.14 .15
.16	.17-.30	.31
.32	.33-.46	.47
.48	.49-.62	.63
.64	.65-.78	.79
.80	.81-.94	.95
.96	.97-.110	.111
.112	.113-.126	.127
.128	.129-.142	.143
.144	.145-.158	.159
.160	.161-.174	.175
.176	.177-.190	.191
.192	.193-.206	.207
.208	.209-.222	.223
.224	.225-.238	.239
.240	.241-.254	.255

Enter into the main table

Subnet Name	Needed Size	Allocated Size	Address	Mask	Subnetmask	Assignable Range	Broadcast
A	50	62	192.168.77.0	/26	255.255.255.192	192.168.77.1 - 192.168.77.62	192.168.77.63

B	27	30	192.168.77.64	/27	255.255.255.224	192.168.77.65 - 192.168.77.94	192.168.77.95
C	12	14	192.168.77.96	/28	255.255.255.240	192.168.77.97 - 192.168.77.110	192.168.77.111
D	12	14	192.168.77.112	/28	255.255.255.240	192.168.77.113 - 192.168.77.126	192.168.77.127

g. Furthermore, the CIDR that can accommodate 2 hosts is /30. (see Table. CIDR for class C networks)

Tabel./30 -- 64 Subnets -- 2 Hosts/Subnet

Network #	IP Range	Broadcast .1-.2
.0		.3
.4	.5-.6	.7
.8	.9-.10	.11
.12	.13-.14	.15
.16	.17-.18	.19
.20	.21-.22	.23
.24	.25-.26	.27
.28	.29-.30	.31
.32	.33-.34	.35
.36	.37-.38	.39
.40	.41-.42	.43
.44	.45-.46	.47
.48	.49-.50	.51
.52	.53-.54	.55
.56	.57-.58	.59
.60	.61-.62	.63
.64	.65-.66	.67
.68	.69-.70	.71
.72	.73-.74	.75
.76	.77-.78	.79
.80	.81-.82	.83
.84	.85-.86	.87
.88	.89-.90	.91
.92	.93-.94	.95
.96	.97-.98	.99
.100	.101-.102	.103
.104	.105-.106	.107
.108	.109-.110	.111
.112	.113-.114	.115
.116	.117-.118	.119
.120	.121-.122	.123
.124	.125-.126	.127
.128	.129-.130	.131
.132	.133-.134	.135
.136	.137-.138	.139

.140	.141-.142	.143
.144	.145-.146	.147
.148	.149-.150	.151
.152	.153-.154	.155
.156	.157-.158	.159
.160	.161-.162	.163
.164	.165-.166	.167
.168	.169-.170	.171
.172	.173-.174	.175
.176	.177-.178	.179
.180	.181-.182	.183
.184	.185-.186	.187
.188	.189-.190	.191
.192	.193-.194	.195
.196	.197-.198	.199
.200	.201-.202	.203
.204	.205-.206	.207
.208	.209-.210	.211
.212	.213-.214	.215
.216	.217-.218	.219
.220	.221-.222	.223
.224	.225-.226	.227
.228	.229-.230	.231
.232	.233-.234	.235
.236	.237-.238	.239
.240	.241-.242	.243
.244	.245-.246	.247
.248	.249-.250	.251
.252	.253-.254	.255

Enter into the main table, so that the final results are obtained as in the table below

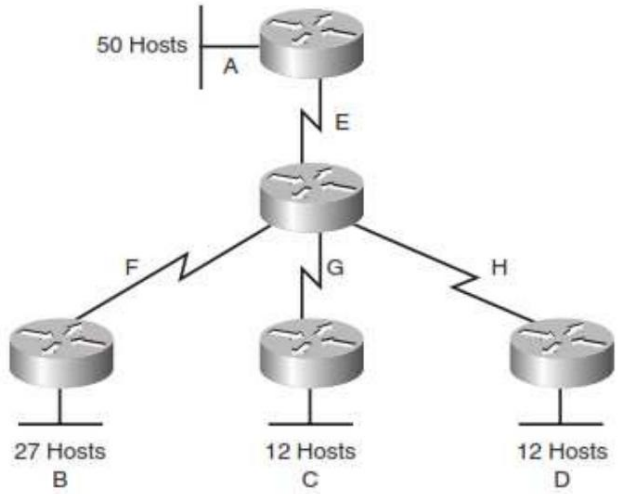


Table. Final results after performing VLSM

Subnet Name	Needed Size	Allocated Size	Address	Mask	Subnetmask	Assignable Range	Broadcast
A	50	62	192.168.77.0	/26	255.255.255.192	192.168.77.1 - 192.168.77.62	192.168.77.63
B	27	30	192.168.77.64	/27	255.255.255.224	192.168.77.65 - 192.168.77.94	192.168.77.95
C	12	14	192.168.77.96	/28	255.255.255.240	192.168.77.97 - 192.168.77.110	192.168.77.111
D	12	14	192.168.77.112	/28	255.255.255.240	192.168.77.113 - 192.168.77.126	192.168.77.127
AND	2	2	192.168.77.128	/30	255.255.255.252	192.168.77.129 - 192.168.77.130	192.168.77.131
F	2	2	192.168.77.132	/30	255.255.255.252	192.168.77.133 - 192.168.77.134	192.168.77.135
G	2	2	192.168.77.136	/30	255.255.255.252	192.168.77.137 - 192.168.77.138	192.168.77.139
H	2	2	192.168.77.140	/30	255.255.255.252	192.168.77.141 - 192.168.77.142	192.168.77.143

6. Lab Introduction to IPv6

IPv6 is the successor of IPv4. IPv6 is capable of providing addresses up to 3.402823669209384634633746074317 7e+38 addresses or 2 to the power of 128. Meanwhile IPv4 is only capable of 4294967296 addresses.

IPv6 emerged because of the limited number of IPv4, which was almost used up. Migration techniques to IPv6: Dual Stack, Tunneling, Translation.

IPv6 uses hexadecimal in its writing. Usually written x:x:x:x:x:x:x:x, where each X consists of 4 hexadecimals, or better known as hextets, for example 2001:0db8:0:1111::200

Simplification in IPv6:

A. The leading 0 may be omitted
- **a. 0012=12**
- **b. 0A0B=A0B**
- **c. 0B00=B00**

B. Replace the number 0 in a row with :: (double colon) or more often called compressed format.

There are 3 types of IPv6, namely Unicast, Multicast, and Anycast. For example, writing the prefix in IPv4 192.168.1.1/24, means that the IP address 192.168.1.1 has a subnet mask of 255.255.255.0. Meanwhile, IPv6, for example 2001:0db8:000a::/64, means that 2001:0db8:000a:: is the network address, and the rest (128-64=64) is for the interface ID or host ID.

7. Lab Soal IPv6

Solve the questions about IPv6 below.

1. A device has MAC Address bf-2c-73-fd-cf-28, specify the link address localnya

a.fe80::bf2c:73fd:cf28

b.fe80::bd2c:73ff:fefd:cf28

c.fe80::bf2c:73ff:fefd:cf28

d.ff02::bd2c:73ff:fefd:cf28

Is known

MAC Address : bf-2c-73-fd-cf-28

1. Take the first octet, namely bf

2. Change bf to binary, which is originally hexadecimal change to binary 3. B=11=1011,F=15=1111 4. Combine again, until it becomes 10111111 5. Flip the 7th bit, with the opposite number. If 0, change to 1, if 1 change to 0

6. Until the result 10111111 becomes 10111101 7. Change 10111101 to hexa 8. 101111012=BD16

9. Initial MAC bf-2c-73-fd-cf-28, after going through the conversion bd-2c-73-fd-cf-28

10. Change the writing of the MAC Address so that it becomes bd2c:73fd:cf28

11. Insert fffe into the middle of the MAC Address that has been changed earlier 12. bd2c:73fd:cf28 So that it becomes bd2c:73ff:fefd:cf28 13. Because the link is local, then using fe80::/10 14. The final result after merging fe80:: bd2c:73ff:fefd:cf28, so the correct answer is B

2. Ubah ke format awal IPV6 8bf9::e93:0:78d6:c920:b49b

Is known

IPv6 Address : 8bf9::e93:0:78d6:c920:b49b

1.Each hextet must consist of 4 nibles, check 1 by one,

2.8bf9::e93:0:78d6:c920:b49b so that if it is extended 8bf9::0e93:0000:78d6:c920:b49b

3. Count all the hextets, there should be 8 hextets, consisting of 32 nibles, so it should be 8bf9:0000:0000:0e93:0000:78d6:c920:b49b

3. How many subnets is /56 out of /52 ?

Answer :

2 56-52=16

4. Manakah penulisan IPV6 yang valid

a.2001:286b:f2f9:4c8b:537b:883a:c16d:5a75:b54c

b.2001:e69::9b29 | c. 2001:fef:a98c:ac53:e46d:bdb5

d.2001:d5ad::ddb7::46b1:cffd

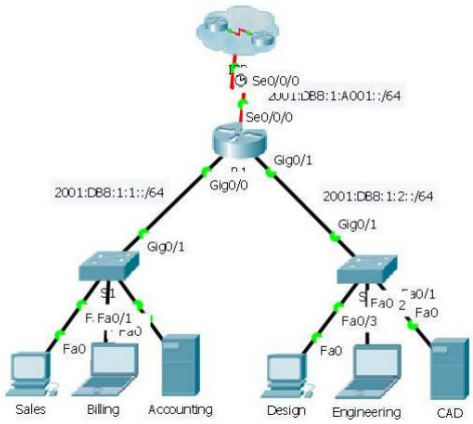
Answer :

a.2001:286b:f2f9:4c8b:537b:883a:c16d:5a75:b54c (Wrong, has 9 hextets, which should be 8 hextets) b.2001:e69::9b29

(Correct) c.2001:fef:a98c:

ac53:e46d:bdb5 (Wrong, only has 6 hextets, if it's still less than 8, give a double collon ::) d.2001:d5ad::ddb7::46b1:cffd (Wrong, double collon is only allowed used once)

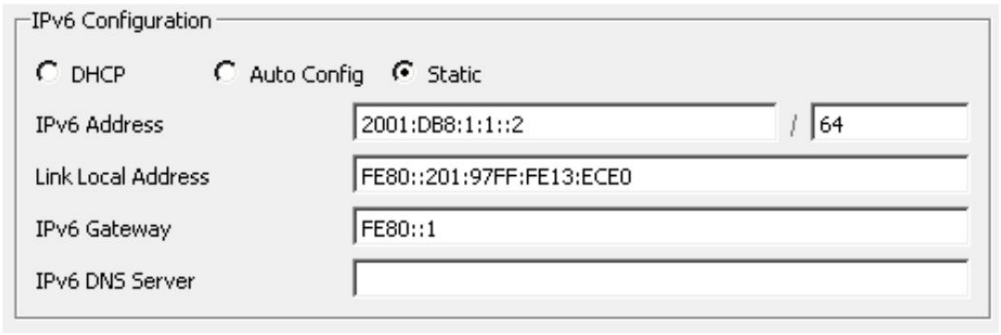
8. Lab Packet Tracer IPv6



Picture. IPv6 lab on packet tracer

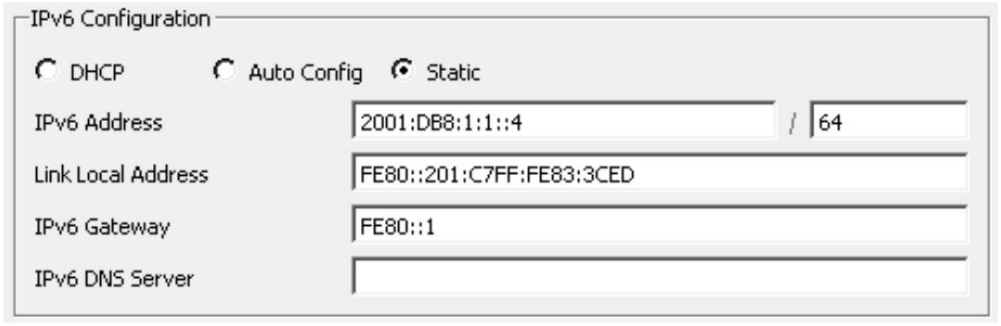
Configuration R-1

```
R1#configure terminal
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ipv6 address 2001:db8:1:1::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown
R1(config-if)#inter gigabitEthernet 0/1
R1(config-if)#ipv6 address 2001:db8:1:2::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown
R1(config)#ipv6 unicast-routing
R1(config)#inter serial 0/0/0
R1(config-if)#ipv6 add
R1(config-if)#ipv6 address 2001:db8:1:a001::2/64
R1(config-if)#no shutdown
```



Picture. Sales Configuration

Picture. Billing Configuration



Picture. Accounting Configuration

For the others it's more or less the same. Next is the testing stage. Testing is carried out using ping and browser.

```
C:\>ping 2001:DB8:1:2::2

Pinging 2001:DB8:1:2::2 with 32 bytes of data:

Reply from 2001:DB8:1:2::2: bytes=32 time=21ms TTL=127
Reply from 2001:DB8:1:2::2: bytes=32 time=11ms TTL=127
Reply from 2001:DB8:1:2::2: bytes=32 time=1ms TTL=127
Reply from 2001:DB8:1:2::2: bytes=32 time<1ms TTL=127

Ping statistics for 2001:DB8:1:2::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 21ms, Average = 8ms
```

Picture. Testing with Ping from Sales to Design

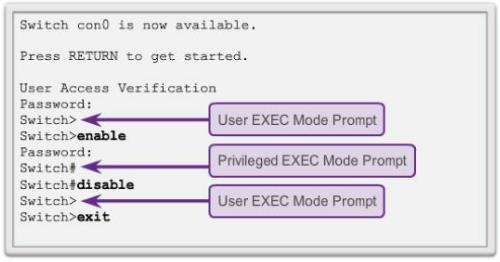
Picture. Browser Testing from Sales to CAD

9. Lab Dasar Command Line Interface Cisco

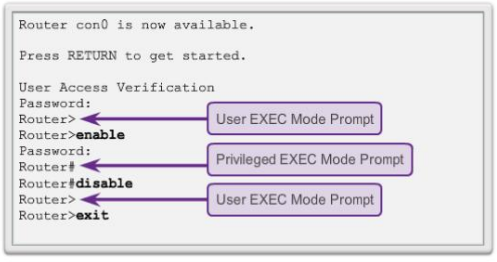
Operation Mode in Cisco for both Routers and Switches is divided into 3 overall, as in the table below:

Table. Modes in the Cisco CLI

No	mode	Sign
1	User Exec Mode	Router>
2	Privilege Mode	Router#
3	Global Configuration Mode	Router(config)#



Picture. Modes on Cisco Switches



Picture. Modes on Cisco Routers

The following is a list of basic commands in Cisco:

1. Switch from User to Priviledge mode and vice versa

The enable command is used to enter from User Exec Mode to Priviledge Mode, and to return it can be used to disable it

```
sRouter>enable
Router#
Router#disable
Router>
```

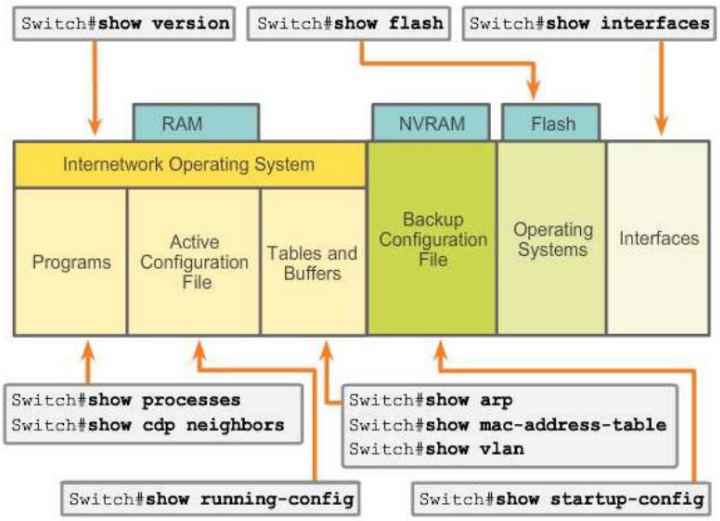
2. Exit/up one level

```
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

3. Displays certain information

To display the running configuration on the device, you can use the show running-config command in Priviledge Exec mode. Apart from that, there are many types of show commands. Can be seen in the image below.

```
Router#show running-config Building
configuration...

Current configuration : 551 bytes

! version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
```



Pictures. Various show commands on the Cisco CLI

4. Configure the hostname or device name. The first
step in configuring the device is to provide a name/hostname. The name must be unique and able to represent the device.

Meanwhile, to delete, just use the hostname number.

```
Router#configure terminal
Router(config)#hostname R-Lantai-1
Router(config)#no hostname
Router#
```

5. Save the configuration
To save the configuration, use the write command.

```
Router#write Building
configuration...
 [OK]
```

CHAPTER 2

Switching

Lab Dasar Virtual Local Area Network (VLAN) 20

Lab VLAN Trunk 23

Lab Cisco Discovery Protocol 26

Lab Static Port Security 28

10. Lab Dasar Virtual Local Area Network (VLAN)

Every device connected to the switch will be on the same broadcast.

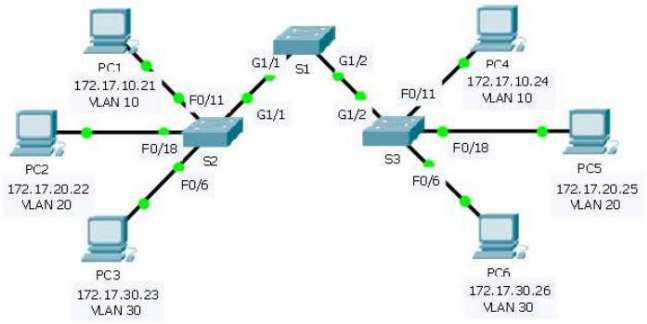
This means that each device will receive broadcast packets sent by other devices. We both know that broadcasts that are too large have a negative impact on network performance.

Picture. Separating broadcast domains using 2 switches

Initially, to break up the broadcast domain between devices, they were separated using different switches as above.

Picture. Separating broadcast domains using VLANs

With the VLAN feature, switches can divide broadcast domains without depending on other switches.



Picture. Basic VLAN topology

No VLAN	Nama Vlan	
1	10	Faculty/Staff
2	20	Student
3	30	Guest(Default)
4	99	Table

Management. VLAN naming

Device	Interface	IP Address	Subnet Mask	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	10
PC2	NIC	172.17.20.22	255.255.255.0	20
PC3	NIC	172.17.30.23	255.255.255.0	30
PC4	NIC	172.17.10.24	255.255.255.0	10
PC5	NIC	172.17.20.25	255.255.255.0	20
PC6	NIC	172.17.30.26	255.255.255.0	30

Tabel. IP Addressing

The following is the VLAN configuration on the CISCO Switch, according to topology, naming and IP Addressing.

1. Configure hostname

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S2
```

2. Configure the password that will be used when entering Global Configuration Mode

```
S2>enable
S2#configure terminal S2(config)#enable
secret cisco
S2(config)#exit
```

3. Konfiguarsi password line console

```
S2#configure terminal S2(config)#line
console 0 S2(config-line)#password
ciscocon
S2(config-line)#login S2(config-
line)#end
```

4. Configure vty line password

```
S2#configure terminal
S2(config)#line vty 0 15
S2(config-line)#password ciscovty
S2(config-line)#login
S2(config-line)#end
```

5. Configure the login banner

```
S2#configure terminal
S2(config)banner login # Authorized Personnel Only!#
```

6. Configure the Motd banner

```
S2#configure terminal
S2(config)banner motd # Maintenance is done every Saturday!#
```

7. Configure VLANs

```
S2#configure terminal
S2(config)#vlan 10
S2(config-vlan)#name Faculty/Staff
S2(config-vlan)#vlan 20
S2(config-vlan)#name Students
S2(config-vlan)#vlan 30
S2(config-vlan)#name Guest(Default)
S2(config-vlan)#vlan 99
S2(config-vlan)#name Management&Native
S2(config-vlan)#end
```

8. Configure VLAN according to port

```
S2#configure terminal
S2(config)#interface fastEthernet 0/11
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#exit
S2(config)#interface fastEthernet 0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#exit
S2(config)#interface fastEthernet 0/6
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
S2(config-if)#end
```

9. Check the VLAN that has been created

```
S2#show vlan brief
S2#show vlan id 10
S2#show interfaces fastEthernet 0/11 switchport
```

10. Displays the configuration configuration

```
S2#show running-config Building
configuration...

Current configuration : 1338 bytes

! version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

! hostname S2

! enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0




! ! ! ! ! spanning-tree mode pvst
spanning-tree extend system-id

! interface FastEthernet0/
```

11. Change the interface membership of the VLAN

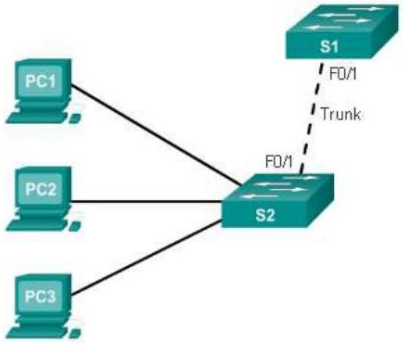
```
S2#configure terminal
S2(config)#interface fastEthernet 0/11
S2(config-if)#no switchport access vlan
S2(config-if)#do show vlan brief
VLAN Name Status Ports
----
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
```

```
F0/5, F0/7, F0/8, F0/9
F0/10, F0/11, F0/12, F0/13
F0/14, F0/15, F0/16, F0/17
F0/19, F0/20, F0/21, F0/22
Fa0/23, Fa0/24, Gig0/1, Gig0/2
10 Faculty/Staff active
20 Students active Fa0/18
30 Guest(Default) active Fa0/6
99 Management&Native active 1002 fddi-default
active
1003 token-ring-default active 1004 fddinet-default
active
1005 trnet-default active S2(config-if)#
```

12. Delete VLANs

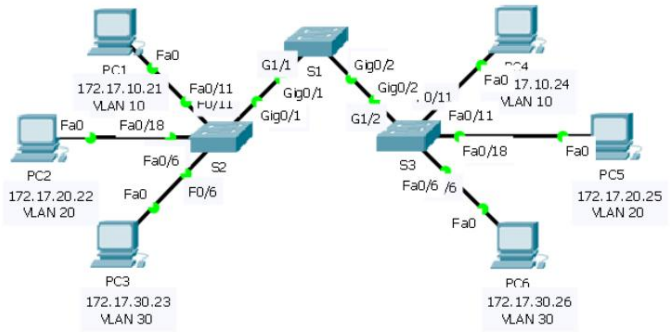
```
S2#configure terminal
S2(config)#no vlan 20
S2(config)#do show vlan brief

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
F0/5, F0/7, F0/8, F0/9
F0/10, F0/11, F0/12, F0/13
F0/14, F0/15, F0/16, F0/17
F0/19, F0/20, F0/21, F0/22
Fa0/23, Fa0/24, Gig0/1, Gig0/2
10 Faculty/Staff active
30 Guest(Default) active Fa0/6
99 Management&Native active 1002 fddi-default
active
1003 token-ring-default active 1004 fddinet-default
active 1005 trnet-default active

S2(config)#
```

11. Lab VLAN Trunk



Picture. Trunk VLANs

VLAN Trunk is a way to carry several VLANs on one link. For example in the image above, between switches, a vlan-trunk is used, so that each host with the corresponding vlan is connected to each other.



Picture. Trunk configuration between S1, S2 and S3

The configuration below aims to ensure that PC1 on VLAN10 can ping PC4 on VLAN10 too. The following is the VLAN Trunk configuration:

1. **Make sure each vlan is configured on S1, S2 and S3,**
   the following is an example in S2. Do it on S1 and S3.

```
S2#configure terminal
S2(config)#vlan 10
S2(config-vlan)#name Faculty/Staff
S2(config-vlan)#vlan 20
S2(config-vlan)#name Students
S2(config-vlan)#vlan 30
S2(config-vlan)#name Guest(Default)
S2(config-vlan)#vlan 99
S2(config-vlan)#name Management&Native
S2(config-vlan)#end
```

2. **Configure VLAN on the interface that is used as a trunk. If you look at S2, the interface leading to S1 is GigabitEthernet0/1**

```
S2#configure terminal
S2(config)#interface gigabitEthernet 0/1
S2(config-if)#switchport mode trunk
S2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
sw
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#switchport trunk allowed vlan 10,20,30
S2(config-if)#end
S2#
```

3. Do the same thing on S1

```
S1#configure terminal Enter
configuration commands, one per line. End with CNTL/Z.
S1(config)#interface gigabitEthernet 0/1 S1(config-if)#switchport
mode trunk S1(config-if)#switchport trunk native vlan 99
S1(config-if)#switchport trunk allowed vlan 10,20,30 S1(config-if)#end
S1(config)#interface gigabitEthernet 0/2 S1(config-if)#switchport mode trunk S1(config-
if)#switchport trunk native
vlan 99 S1(config-if)#switchport trunk allowed vlan 10,20,30
S1(config-if)#end 4. Menghapus allowed vlan dan native
vlan pada interface
```

```
S2#configure terminal
S2(config-if)#no switchport trunk native vlan
S2(config-if)#no switchport trunk allowed vlan
S2(config-if)#end
S2#
```

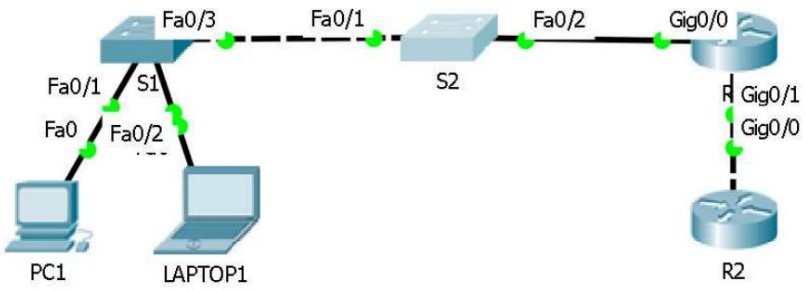
5. View configuration results/check trunk configuration

```
S2#show interfaces gigabitEthernet 0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Management&Native)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20,30
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
--More--
```

12. Lab Cisco Discovery Protocol

CDP is used to detect routers or switches that are directly connected to it. Cisco Discovery Protocol can display information in the form of hostname, IP Address, and running OS such as switches, routers and IP Phones.

CDP is a proprietary protocol from Cisco, while the Link Layer Discovery Protocol is an IEEE standard.



Picture. Cisco Protocol Discovery Lab

Here are the commands on the CDP and LLDP labs:

1. Displays CDP information on S2.

By using the show cdp neighbors command, S1 and R1 are visible.

For more detailed information, you can use show cdp neighbors detail

```
S2#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source
Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
S1 Fas 0/1 160 S 2960 Fas 0/3
R1 Fas 0/2 168 R C2900 Gig 0/0
```

2. View CDP details for a particular device

```
S2#show cdp entry R1

Device ID: R1
Entry address(es): IP address :
192.168.1.3
Platform: cisco C2900, Capabilities: Router
Interface: FastEthernet0/2, Port ID (outgoing port): GigabitEthernet0/0

Holdtime: 131

Version :
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
```

```
advertisement version: 2
Duplex: full
```

3. Use the results of show cdp neighbors to perform telnet

```
R2#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source
Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
R1 Gig 0/0 120 R C2900 Gig 0/1
Router#show cdp ent
Router#show cdp entry R1

Device ID: R1
Entry address(es): IP address :
192.168.2.1
Platform: cisco C2900, Capabilities: Router
Interface: GigabitEthernet0/0, Port ID (outgoing port): GigabitEthernet0/1

Holdtime: 170

Version :
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team

advertisement version: 2
Duplex: full

R2#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms


R2#telnet 192.168.2.1
Trying 192.168.2.1 ...Open

User Access Verification

Password:
R1>
```

4. Enable Link Layer Discovery Protocol (LLDP) on Cisco switches and routers

```
S2#configure terminal
S2(config)#lldp run
S2(config)#
```

5. Enable Link Layer Discovery Protocol (LLDP) on Cisco switches and routers

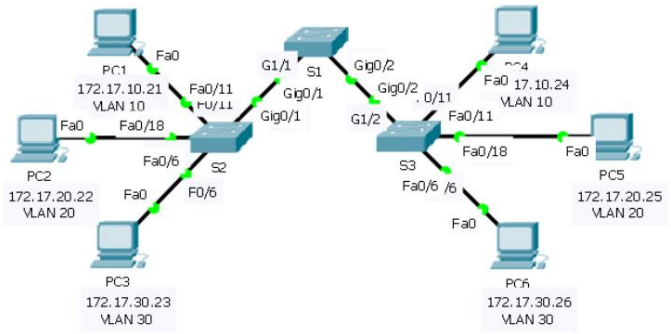
```
R2#show lldp neighbors
Capability codes:
 (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
 (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID Local Intf Hold-time Capability Port ID
R1 Gig0/0 120 R Gig0/1

Total entries displayed: 1
R2#
```

6. Disable the CDP or LLDP feature, this feature is often misused so if it is not very important you can disable it.

```
S2#configure terminal
S2(config)#no cdp run
S2(config)#no lldp run
S2(config)#end
S2#show cdp neighbors
% CDP is not enabled
S2#show lldp neighbors
% LLDP is not enabled
```

13. Lab Static Port Security

Each switch device must be secure before being used on the network. One way to secure a switch is to use the Port Security feature. Port Security will limit every MAC Address connected to that port.



Gambar. Lab port security

Port Security works based on Source MAC or origin MAC Address. For example, PC1 has MAC Address 0090.21DD.EA4B, connected to S2 via Port Fa0/11. By using Port Security, the MAC Address on PC1 can be determined whether it can send frames via Port Fa0/11 or not.

Port Security is carried out on each port on the switch. Each port can be determined by the maximum MAC address that can pass through. If the maximum MAC address has been exceeded, certain actions will be carried out.

There are 3 types of action or violation in port security, namely protect, restrict and shutdown with shutdown as the default option.

Option on the switchport port-security violation Command	Protect	Restrict	Shutdown*
Discards offending traffic	Yes	Yes	Yes
Sends log and SNMP messages	No	Yes	Yes
Increments the violation counter for each violating incoming frame	No	Yes	Yes
Disables the interface by putting it in an err-disabled state, discarding all traffic	No	No	Yes

Picture. Violation mode in Port Security

The first type of port security is static, meaning the MAC Address is entered manually by the network administrator.

1. **Enable port-security on the fastEthernet 0/11 interface. Enable the port security feature with the switchport port-security command. Tell fastEthernet 0/11 that there is a maximum of only 1 MAC address, namely 0090.21DD.EA4C. If it is detected instead of 0090.21DD.EA4C, then the action/violation is shutdown. This means that fastEthernet port 0/11 will die or shutdown.**

```
S2#configure terminal
S2(config)#interface fastEthernet 0/11
S2(config-if)#switchport port-security S2(config-if)#switchport
port-security maximum 1
S2(config-if)#switchport port-security violation shutdown S2(config-if)#switchport port-security
mac-address 0090.21DD.EA4C
```

2. **When MAC 0090.21DD.EA4C is not entered into fastEthernet port 0/11, according to the violation shutdown table, the packet will be dropped, a notification will appear on the screen, adding a counter to the violation incoming frame and disabling the fastEthernet 0/11 port or shutting down the fastEthernet 0**
   To return the port status to up, the network administrator needs to give a direct command to the shutdown switch followed by no shutdown.

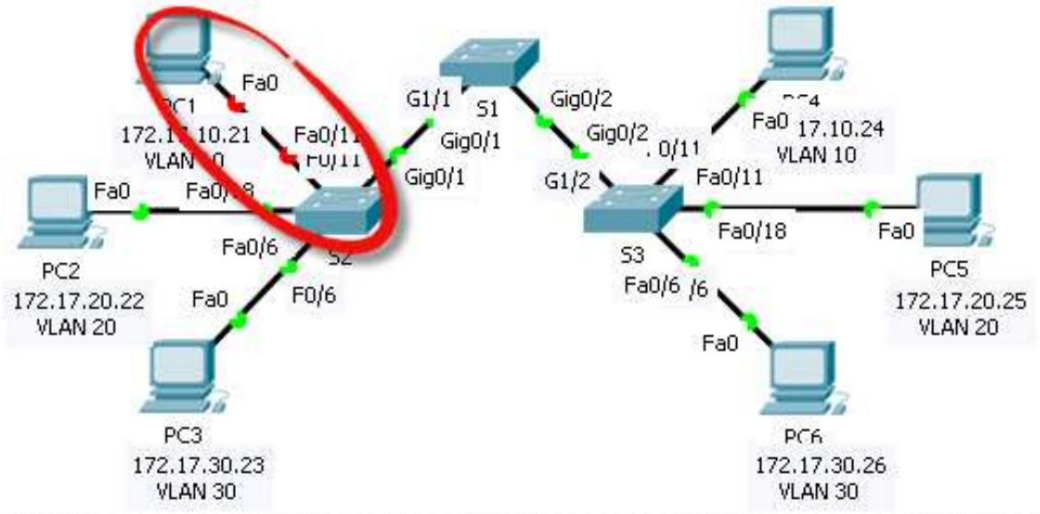
```
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down


%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/11, changed state to down
```

3. **View the port security status on fastEthernet 0/11**

```
S2#show port-security interface fastEthernet 0/11
Port Security : Enabled
```

```
Port Status : Secure-shutdown
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0090.21DD.EA4B:10
Security Violation Count : 1
```

4. The port on fastEthernet 0/11 changes from UP to down



5. Reactivate the shutdown port, then the fastEthernet 0/11 interface will be UP again

```
S2(config)#interface fastEthernet 0/11
S2(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

S2(config-if)#no shutdown
S2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/11, changed state to up
```

CHAPTER 3

Routing

BAB 3 – ROUTING 31

Lab Inter-VLAN Routing Router-on-a-stick 32

Lab Static Routing IPv4 35

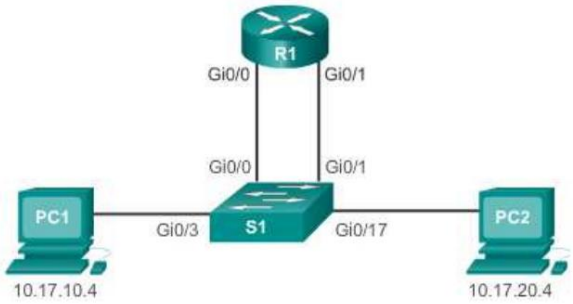
Lab Static Routing IPv6 39

Lab Routing Information Protocol version 2 (RIPv2) IPv4 41

14. Lab Inter-VLAN Routing Router-on-a-stick

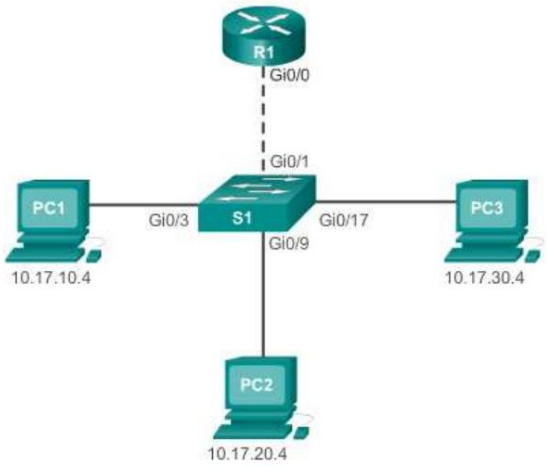
Networks that use VLAN will certainly have different subnets/segments.
Layer 3 is needed to forward traffic between these segments.

Apart from using a router, to connect subnets/segments to one another, you can use the interface in a switch or in other words, use a layer 3 switch.



Picture. Legacy inter-vlan

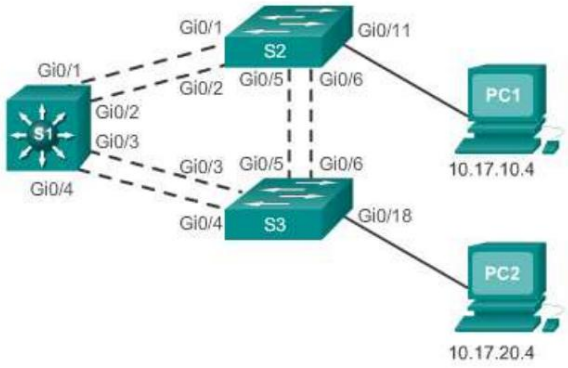
The initial method or legacy method, R1 uses 2 cables to connect network 10.17.10.4 with 10.17.20.4



Gambar. Router-on-a-stick

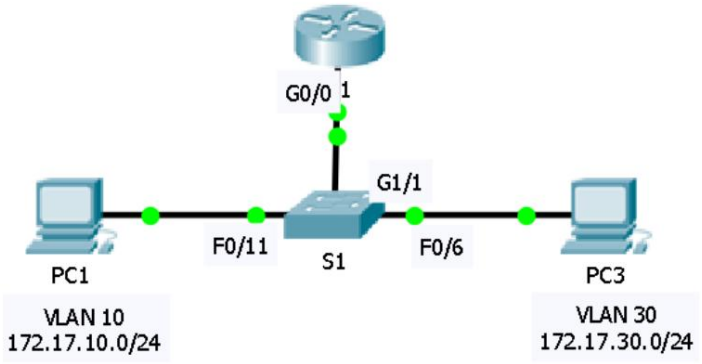
R1 simply uses 1 cable to connect several networks, or in other words uses virtual ports or subinterfaces. Subinterfaces are known as software-based virtual interfaces, where each subinterface can be assigned an IP address and subnet mask.

When you want to configure the Router-in-a-Stick, make sure that the interface that will be used as a subinterface is connected to the interface that has been set as a trunk.



Picture. Multilayer Switches

Using a multilayer switch, which can play a role at layer 2 and layer 3, thereby eliminating the role of the router.



Picture. Router-in-a-Stick Topology

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0.10	172.17.10.1	255.255.255.0	N/A
	G0/0.30	172.17.30.1	255.255.255.0	N/A
PC1	NIC	172.17.10.10	255.255.255.0	172.17.10.1
PC2	NIC	172.17.30.10	255.255.255.0	172.17.30.1

Picture. IP Addressing for Router-in-a-Stick topology

Lab objectives:

- **Configure subinterfaces**
- **Router-in-a-stick configuration**
- **PC1 can connect to PC2**

Here's the Router-in-a-Stick configuration:

1. Configure VLAN and access ports for F0/11 and F0/6

```
S1#configure terminal
```

```
S1(config-vlan)#vlan 10
S1(config-vlan)#vlan 30
S1(config)#interface fastEthernet 0/11
S1(config-if)#switchport access vlan 10
S1(config-if)#exit
S1(config)#interface fastEthernet 0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1#show vlan brief

VLAN Name Status Ports
____ ___ ___ ___

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
F0/5, F0/7, F0/8, F0/9
F0/10, F0/12, F0/13, F0/14
F0/15, F0/16, F0/17, F0/18
F0/19, F0/20, F0/21, F0/22
Fa0/23, Fa0/24, Gig0/1, Gig0/2
10 VLAN0010 active Fa0/11
30 VLAN0030 active Fa0/6
1002 fddi-default active 1003 token-ring-
default active 1004 fddinet-default active

1005 trnet-default active
S1(config)#interface gigabitEthernet 0/1
S1(config-if)#switchport mode trunk
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

S1(config-if)#
```

2. Configure subinterfaces and assign IP addresses to each subinterface

```
R1#configure terminal
R1(config)#interface gigabitEthernet 0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface gigabitEthernet 0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#no shutdown
```

3. Checking is done by pinging from PC1 172.17.10.10 to PC3 172.17.30.10

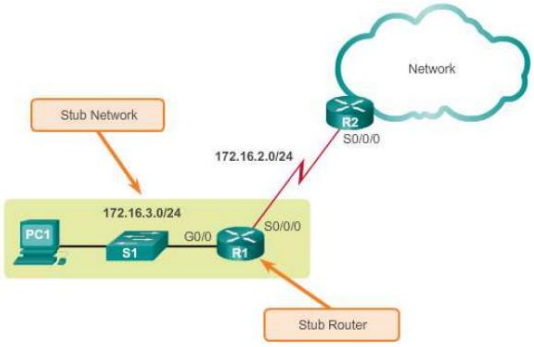
```
C:\>ping 172.17.30.10
```

```
Pinging 172.17.30.10 with 32 bytes of data:

Reply from 172.17.30.10: bytes=32 time=1ms TTL=127
Reply from 172.17.30.10: bytes=32 time=1ms TTL=127
Reply from 172.17.30.10: bytes=32 time<1ms TTL=127
Reply from 172.17.30.10: bytes=32 time<1ms TTL=127

Ping statistics for 172.17.30.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

15. Lab Static Routing IPv4

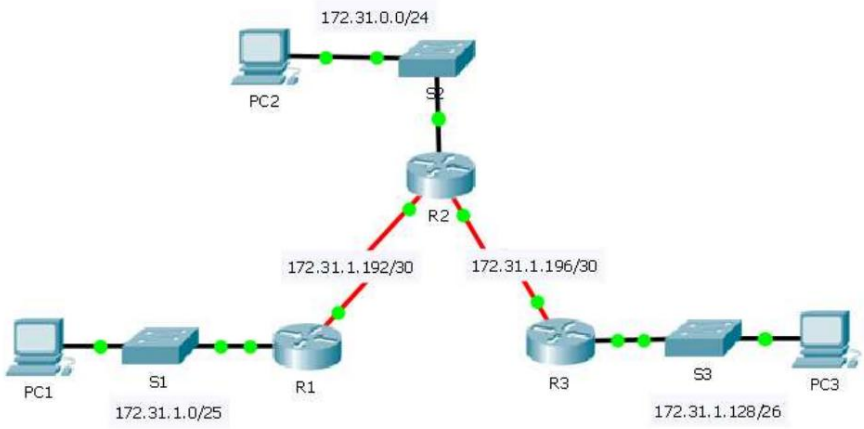
Routers can connect subnets/segments to each other in 2 ways, namely manual and dynamic. A Network Administrator can determine how a network connects to other networks.

Static routing has many advantages when applied in small scale networks, but is not suitable for application on a large scale.



Gambar. Stub network

Static routing is suitable for application in stub networks, meaning there is only 1 destination network, for example the need for internet access in the office.



Picture. Static routing topology

Even though the topology above uses IP 172.31.1.x, it uses different subnets. For example, PC1 and R1 are different from PC3 and R3. For more details, see the IP address table.

The syntax used in this lab is next-hop-static route, which means using IP Address

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0	172.31.1.1	255.255.255.128	N/A
	S0/0/0	172.31.1.194	255.255.255.252	N/A
R2	G0/0	172.31.0.1	255.255.255.0	N/A
	S0/0/0	172.31.1.193	255.255.255.252	N/A
	S0/0/1	172.31.1.197	255.255.255.252	N/A
R3	G0/0	172.31.1.129	255.255.255.192	N/A
	S0/0/1	172.31.1.198	255.255.255.252	N/A
PC1	NIC	172.31.1.126	255.255.255.128	172.31.1.1
PC2	NIC	172.31.0.254	255.255.255.0	172.31.0.1
PC3	NIC	172.31.1.190	255.255.255.192	172.31.1.129

Gambar. IP Addressing static route

Lab objectives:

- **Konfigurasi static routing mode next hop route ip address**
- **All PCs are connected**

The following is a static IPv4 routing lab according to the topology and IP address above:

1. Configure R1 static routing

```
R1#configure terminal
R1(config)#ip route 172.31.0.0 255.255.255.0 172.31.1.193
R1(config)#ip route 172.31.1.196 255.255.255.252 172.31.1.193
R1(config)#ip route 172.31.1.128 255.255.255.192 172.31.1.193
R1#show ip route Codes: L
- local, C - connected, S - static, 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

172.31.0.0/16 is variably subnetted, 7 subnets, 5 masks
S 172.31.0.0/24 [1/0] via 172.31.1.193
```

```
C 172.31.1.0/25 is directly connected, GigabitEthernet0/0
L 172.31.1.1/32 is directly connected, GigabitEthernet0/0
S 172.31.1.128/26 [1/0] via 172.31.1.193
C 172.31.1.192/30 is directly connected, Serial0/0/0
L 172.31.1.194/32 is directly connected, Serial0/0/0
S 172.31.1.196/30 [1/0] via 172.31.1.193

R1#
```

2. Configure static routing on R2

```
R2#show ip interface brief
Interface IP-Address OK? Method Status Protocol GigabitEthernet0/0 172.31.0.1 YES
manual up up GigabitEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 172.31.1.193 YES manual up up Serial0/0/1 172.31.1.197 YES manual up up Vlan1 unassigned YES unset

administratively down down


R2#configure terminal
R2(config)#ip route 172.31.1.0 255.255.255.128 172.31.1.194
R2(config)#ip route 172.31.1.128 255.255.255.192 172.31.1.198
R2#show ip route Codes:
L - local, C - connected, S - static, 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

 172.31.0.0/16 is variably subnetted, 8 subnets, 5 masks
C 172.31.0.0/24 is directly connected, GigabitEthernet0/0
L 172.31.0.1/32 is directly connected, GigabitEthernet0/0
S 172.31.1.0/25 [1/0] via 172.31.1.194
S 172.31.1.128/26 [1/0] via 172.31.1.198
C 172.31.1.192/30 is directly connected, Serial0/0/0
L 172.31.1.193/32 is directly connected, Serial0/0/0
C 172.31.1.196/30 is directly connected, Serial0/0/1
L 172.31.1.197/32 is directly connected, Serial0/0/1

R2#
```

3. Configurais static route di R3

```
R3#configure terminal R3(config)#ip
route 172.31.0.0 255.255.255.0 172.31.1.197
R3(config)#ip route 172.31.1.192 255.255.255.252 172.31.1.197
R3(config)#ip route 172.31.1.0 255.255.255.128 172.31.1.197
```

```
R3#sh ip route
Codes: L - local, C - connected, S - static, 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

172.31.0.0/16 is variably subnetted, 7 subnets, 5 masks S 172.31.0.0/24 [1/0] via 172.31.1.197
S 172.31.1.0/25 [1/0] via 172.31.1.197 C 172.31.1.128/26 is directly
connected, GigabitEthernet0/0 L 172.31.1.129/32 is directly
connected, GigabitEthernet0/0 S 172.31.1.192/30 [1/0] via 172.31.1.197 C 172.31.1.196/30 is directly
connected, Serial0/0/1 L 172.31.1.198/32 is directly connected, Serial0/0/1
```

4. Test ping from R1 to R3

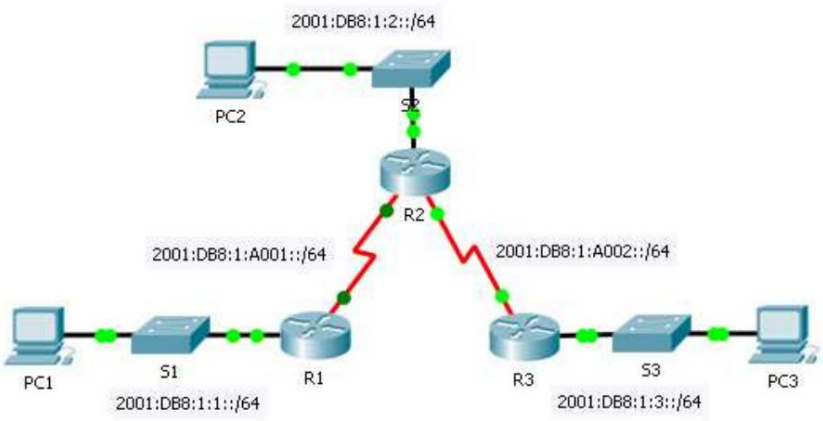
```
R1#ping 172.31.1.198

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.1.198, timeout is 2 seconds: !!!!!


Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/11 ms


R1#
```

5. Test ping from PC3 to PC1

```
C:\>ping 172.31.1.126

Pinging 172.31.1.126 with 32 bytes of data:

Reply from 172.31.1.126: bytes=32 time=13ms TTL=125 Reply from 172.31.1.126:
bytes=32 time=13ms TTL=125 Reply from 172.31.1.126: bytes=32 time=3ms TTL=125
Reply from 172.31.1.126: bytes=32 time=12ms TTL=125


Ping statistics for 172.31.1.126: Packets: Sent = 4,
Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum
= 3ms, Maximum = 13ms, Average = 10ms


C:\>
```

16. Lab Static Routing IPv6

The principles of static routing in IPv6 are the same, and should not cause problems. You need to activate a feature that functions to allow packets to be forwarded with the ipv6 unicast-routing command.



Gambar. Static routing ipv6

Device	Interface	IPv6 Address/Prefix	Default Gateway
R1	G0/0	2001:DB8:1:1::1/64	N/A
	S0/0/0	2001:DB8:1:A001::1/64	N/A
R2	G0/0	2001:DB8:1:2::1/64	N/A
	S0/0/0	2001:DB8:1:A001::2/64	N/A
	S0/0/1	2001:DB8:1:A002::1/64	N/A
R3	G0/0	2001:DB8:1:3::1/64	N/A
	S0/0/1	2001:DB8:1:A002::2/64	N/A
PC1	NIC	2001:DB8:1:1::F/64	FE80::1
PC2	NIC	2001:DB8:1:2::F/64	FE80::2
PC3	NIC	2001:DB8:1:3::F/64	FE80::3

Picture. Addressing Table

Lab objectives:

- **Enable the Routing feature on IPv6 with ipv6 unicast-routing**
- **Connect all PCs**

The following is a static routing configuration using IPv6 according to the topology and addressing table above:

1. Configure R1 static routing

```
R1#configure terminal
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 route 2001:DB8:1:2::/64 2001:DB8:1:A001::2
R1(config)#ipv6 route 2001:DB8:1:A002::/64 2001:DB8:1:A001::2
R1(config)#ipv6 route 2001:DB8:1:3::/64 2001:DB8:1:A001::2
R1#show ipv6 route
```

```
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
C 2001:DB8:1:1::/64 [0/0]
via GigabitEthernet0/0, directly connected
L 2001:DB8:1:1::1/128 [0/0]
via GigabitEthernet0/0, receive
S 2001:DB8:1:2::/64 [1/0]
via 2001:DB8:1:A001::2
S 2001:DB8:1:3::/64 [1/0]
via 2001:DB8:1:A001::2
C 2001:DB8:1:A001::/64 [0/0]
via Serial0/0/0, directly connected
L 2001:DB8:1:A001::1/128 [0/0]
via Serial0/0/0, receive
S 2001:DB8:1:A002::/64 [1/0]
via 2001:DB8:1:A001::2
L FF00::/8 [0/0]
```

2. Configure static routing on R2

```
R2#configure terminal R2(config)#ipv6
unicast-routing R2(config)#ipv6 route 2001:DB8:1:1::/64
2001:DB8:1:A001::1
R2(config)#ipv6 route 2001:DB8:1:3::/64 2001:DB8:1:A002::2
```

3. Configurais static route di R3

```
R3#configure terminal
R3(config)#ipv6 unicast-routing
R3(config)#ipv6 route 2001:DB8:1:2::/64 2001:DB8:1:A002::1
R3(config)#ipv6 route 2001:DB8:1:A001::/64 2001:DB8:1:A002::1
R3(config)#ipv6 route 2001:DB8:1:1::/64 2001:DB8:1:A002::1
```

4. Test ping from R1 to R3

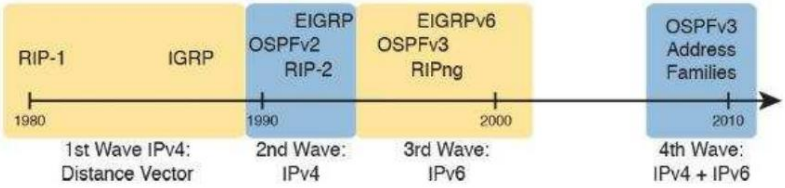
```
R1#ping 2001:DB8:1:A002::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1:A002::2, timeout is 2 seconds:

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/4 ms


R1#
```

5. Test ping from PC3 to PC1

```
C:\>ping 2001:DB8:1:1::F

Pinging 2001:DB8:1:1::F with 32 bytes of data:

Reply from 2001:DB8:1:1::F: bytes=32 time=12ms TTL=125
Reply from 2001:DB8:1:1::F: bytes=32 time=16ms TTL=125
Reply from 2001:DB8:1:1::F: bytes=32 time=11ms TTL=125
Reply from 2001:DB8:1:1::F: bytes=32 time=13ms TTL=125

Ping statistics for 2001:DB8:1:1::F:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 16ms, Average = 13ms
```

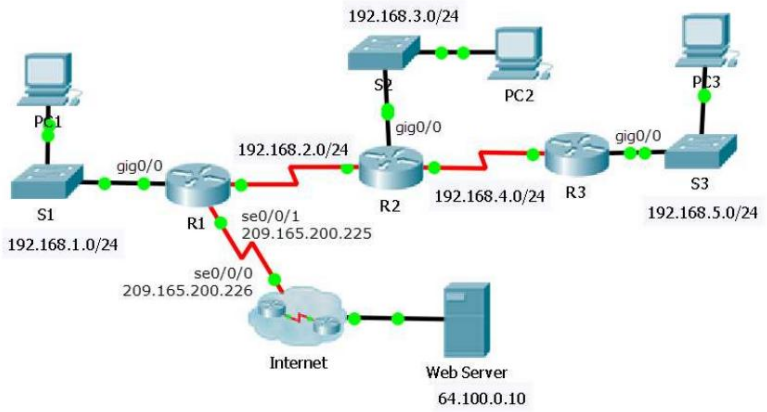
17. Lab Routing Information Protocol version 2 (RIPv2) IPv4

When the network becomes more complicated, a Network Administrator cannot rely on static routing on the network. The latest technology is needed, namely Dynamic Routing.



Routing Information Protocol Version 2, is a dynamic routing that is suitable for use on medium-scale networks only. Network Administrator Simply enable RIPv2 on each router. Once active on all routers, an exchange of route tables will occur, so that each route recognizes each route table.

RIP is a distance vector, which calculates the destination network based on hop count. Meanwhile, protocols such as OSPF use cost parameters. When the network topology changes, the dynamic route will automatically adapt to the change.



Picture. RIPv2 topology

Lab objectives:

- **RIPv2 configuration on R1, R2 and R3 • No autosummary • Passive interface on networks that do not require RIP updates • Default Route or gateway only on R1 interface Se0/0/1 with gateway address 209.165.200.226**
- **Verify RIPv2 with show ip protocol and show ip route**
- **Until finally all clients can access the server at address 64.100.0.10**

The following is a static routing configuration using IPv6 according to the topology and addressing table above:

1. **R1 static routing configuration R1 is an internet gateway, therefore the default route must be advertised on the network through information exchange between routers.**
   So when other routers exchange information, they will also add a default gateway to R1.

```
R1#configure terminal
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.2.0
R1(config-router)#network 192.168.1.0
R1(config-router)#passive-interface gigabitEthernet 0/0
R1(config-router)#no auto-summary R1(config-
router)#default-information originate R1#show ip route Codes: L - local, C -
connected, S - static, 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 209.165.200.226 to network 0.0.0.0

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.1/32 is directly connected, Serial0/0/0
R 192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:04, Serial0/0/0
R 192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:04, Serial0/0/0
R 192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:04, Serial0/0/0
```

```
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/30 is directly connected, Serial0/0/1
L 209.165.200.225/32 is directly connected, Serial0/0/1
S* 0.0.0.0/0 [1/0] via 209.165.200.226

R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 16 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
Interface Send Recv Triggered RIP Key-chain
Serial0/0/0 2 2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
192.168.1.0
192.168.2.0
Passive Interface(s): GigabitEthernet0/0
Routing Information Sources:
Gateway Distance Last Update
192.168.2.2 120 00:00:17
Distance: (default is 120)
R1#
```

2. Configure static routing on R2

```
R2#configure terminal R2(config-
router)#version 2
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.3.0
R2(config-router)#network 192.168.4.0
R2(config-router)#passive-interface gigabitEthernet 0/0
R2(config-router)#no auto-summary
```

3. Configure static route on R3

```
R3#configure terminal
R3(config)#router rip R3(config-
router)#version 2
R3(config-router)#no auto-summary R3(config-
router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#passive-interface gigabitEthernet 0/0
```

4. Results of configuration verification on R2

```
R2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 17 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
```

```
Incoming update filter list for all interfaces is not set Redistributing: rip Default version control: send
version 2, receive 2 Interface Send
Recv Triggered RIP Key-chain Serial0/0/1 2 2 Serial0/0/0 2 2 Automatic network summarization
is not in effect Maximum path: 4 Routing for Networks: 192.168.2.0




192.168.3.0
192.168.4.0
Passive Interface(s): GigabitEthernet0/0
Routing Information Sources:
Gateway Distance Last Update 192.168.2.1 120
00:00:19 192.168.4.1 120 00:00:24 Distance: (default
is 120)



R2#show ip route Codes: L -
local, C - connected, S - static, 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 192.168.2.1 to network 0.0.0.0

R 192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:01, Serial0/0/0 192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0 L 192.168.2.2/32 is directly connected, Serial0/0/0
192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.3.0/24 is directly connected,
GigabitEthernet0/0 L 192.168.3.1/32 is directly connected, GigabitEthernet0/0 192.168.4.0/24 is
variably subnetted, 2 subnets, 2 masks C 192.168.4.0/24 is directly connected, Serial0/0/1 L 192.168.4.2/32
is directly connected, Serial0/0/1 R 192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:09, Serial0/0/1 R* 0.0.0.0/0
[120/1] via 192.168.2.1, 00:00:01, Serial0/0/0




R2#
```

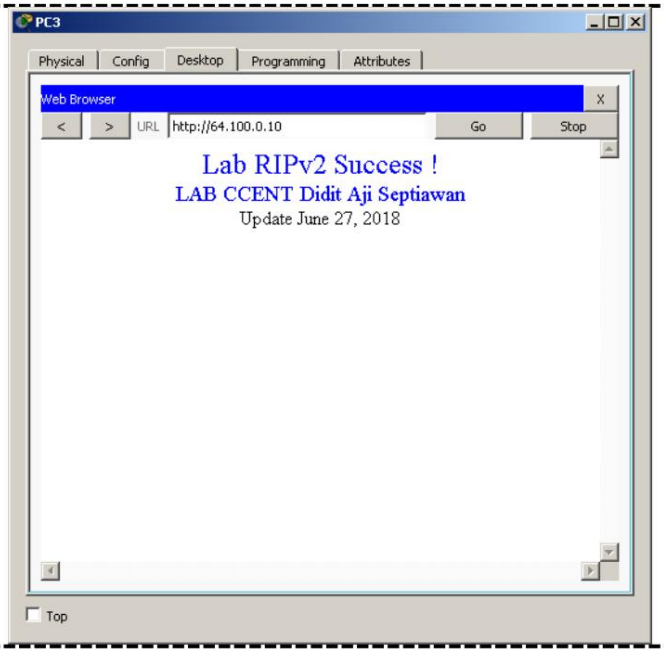
5. Test ping from PC3 to Web server 64.100.0.10, and use a browser

```
C:\>ping 64.100.0.10

Pinging 64.100.0.10 with 32 bytes of data:
```

Reply from 64.100.0.10: bytes=32 time=4ms TTL=124 Reply from 64.100.0.10: bytes=32 time=13ms TTL=124 Reply from 64.100.0.10: bytes=32 time=11ms TTL=124 Reply from 64.100.0.10: bytes=32 time=11ms TTL=124

Ping statistics for 64.100.0.10: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 4ms, Maximum = 13ms, Average = 9ms

C:\>



CHAPTER 4

Infrastructure Services

Lab DHCPv4 Server, DHCP Relay dan DHCP Client 47

Lab Standart AccessList (ACL) 48

Lab Static NAT 54

Lab Dynamic NAT 56

Lab NAT Overloaded atau Port Address Translation (PAT) 59

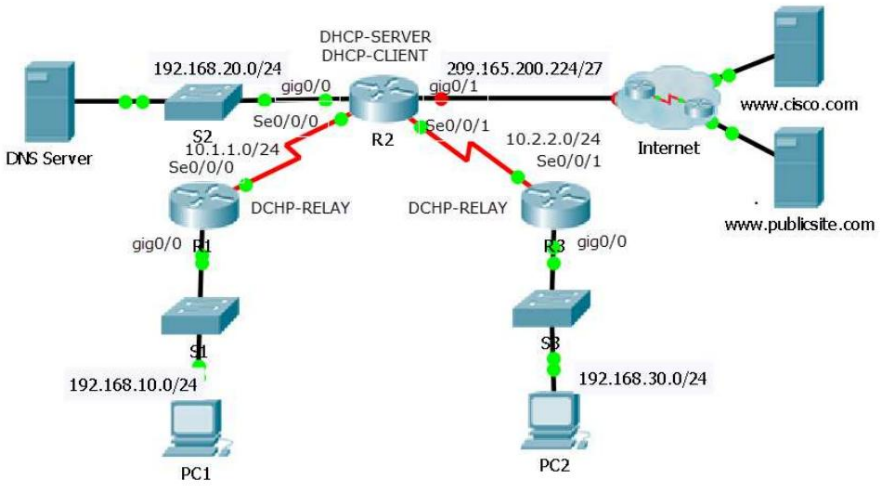
18. Lab DHCPv4 Server, DHCP Relay dan DHCP Client

Dynamic Host Configuration Protocol v4 (DHCPv4) is a standard for automatically assigning IP addresses. By providing IP addresses automatically, it will certainly help the network administrator's task in configuring many clients.

DHCP works by sending messages into the network. There are 4 messages including DHCPDiscover, DHCPOffer, DHCPRequest, DHCP Acknoledgement, more easily called DORA.

DHCP Server can distribute IP addresses, subnet masks, gateways, DNS and options.

IP Pool is a range of IPs that will be given to clients, it can be configured using the ip dhcp pool command. If there are some ranges that you don't want to give to the client, you can use IP DHCP Exlcude-Address
DHCP Relay is used if the network to which the IP will be assigned is not on the same subnet. Configure DHCP Relay using the ip helper-address command.
To configure as a DHCP Client, or receive an IP Address, simply use the ip address dhcp command.



Picture. DHCP Server, DHCP Relay, and DHCP Client topologies

Lab objectives:

• R2 will act as a DHCP-Server for PC1 and PC2. • Undistributed IP Address 192.168.10.1-192.168.10.10 and 192.168.30.1-192.168.30.10

• The pool name for network 192.168.10.0 is R1-LAN • The pool name for network 192.168.30.0 is R3-LAN • R2 interface gig0/1 plays the role of DHCP-Client • R1 and R3 act as DHCP-Relay • All PCs can access the Internet

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	G0/0	192.168.20.1	255.255.255.0	N/A
	G0/1	DHCP Assigned	DHCP Assigned	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
R3	G0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.0	N/A
PC1	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned
PC2	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned
DNS Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Picture. Addressing table

1. Configure exclude-address and pool address

```
R2#configure terminal R2(config)#ip
dhcp excluded-address 192.168.10.1 192.168.10.10
R2(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.10
R2(config)#ip dhcp pool R1-LAN
R2(dhcp-config)#network 192.168.10.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.10.1
R2(dhcp-config)#dns-server 192.168.20.254
R2(dhcp-config)#exit
R2(config)#ip dhcp pool R3-LAN
R2(dhcp-config)#network 192.168.30.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.30.1
R2(dhcp-config)#dns-server 192.168.20.254
R2(dhcp-config)#exit
R2(config)#
```

2. Configure DHCP-Relay on R1

```
R1#configure terminal
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip helper-address 10.1.1.2
R1(config-if)#end
```

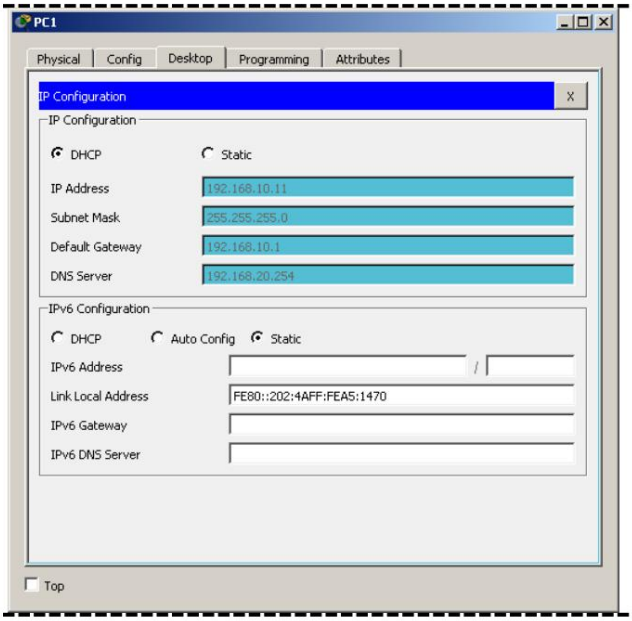
3. Configure DHCP-Relay on R3

```
R3#configure terminal
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ip helper-address 10.2.2.2
R3(config-if)#end
R3#
```

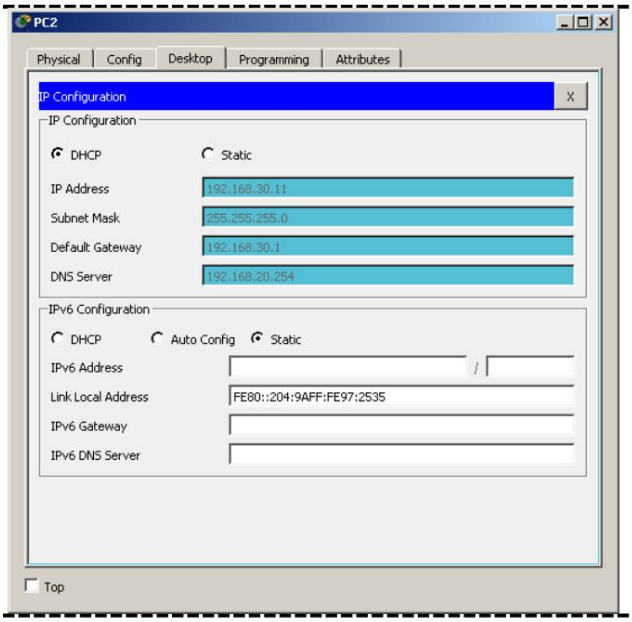
4. Configure the GigabitEthernet0/1 interface as DHCP-CLIENT

```
R2#configure terminal Enter
configuration commands, one per line. End with CNTL/Z.
R2(config)#interface gigabitEthernet 0/1
R2(config-if)#ip address dhcp R2(config-if)#no
shutdown
```

5. Configure DHCP on PC1



6. Configure DHCP on PC2



7. Verify the DCHP server on R2 See the

excluded IP address and the assigned IP address

```
R2#show running-config | include dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp pool R1-LAN
ip dhcp pool R3-LAN
ip address dhcp
```

```
R2#show ip dhcp binding IP address
Client-ID/ Lease expiration Type
Hardware address
192.168.10.11 0002.4AA5.1470 -- Automatic
192.168.30.11 0004.9A97.2535 – Automatic
R2#show ip interface brief Interface IP-Address
OK? Method Status Protocol GigabitEthernet0/0 192.168.20.1 YES manual up up
GigabitEthernet0/1 209.165.200.231 YES DHCP up up Serial0/0/0 10.1.1.2 YES manual up up
Serial0/0/1 10.2.2.2 YES manual up up Serial0/1/0 unassigned YES unset down down Serial0/1/1
unassigned YES unset down down Vlan1 unassigned YES unset
administratively down down



R2#
R2#show dhcp lease Temp IP
addr: 209.165.200.231 for peer on Interface: GigabitEthernet0/1

Temp sub net mask: 255.255.255.224
DHCP Lease server: 209.165.200.225 DHCP Transaction , state: Bound
id: 7BE08E2A
Lease: 86400 secs, Renewal: 43200 secs, Rebind: 75600 secs
Temp default-gateway addr: 0.0.0.0
Next timer fires after: 11:45:46
Retry count: 0 Client-ID:cisco-00D0.BCDA.3902-Gig0/1
Client-ID hex dump: 636973636F2D303044302E424344412E
33930322D476967302F31
Hostname: R2
```

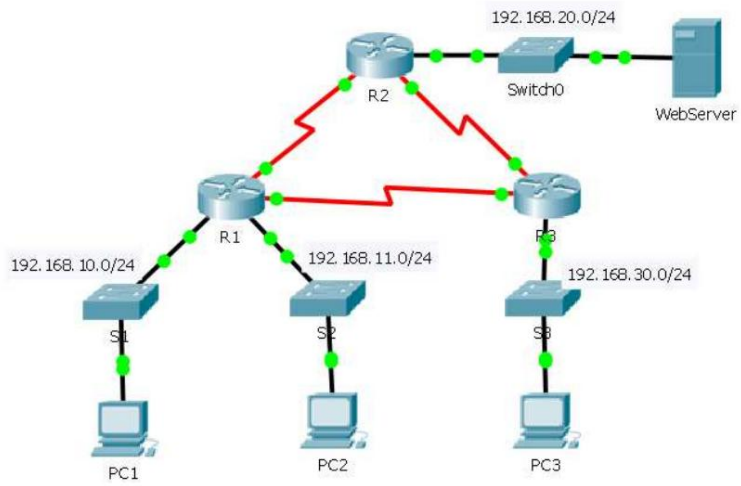
8. Verify the DHCP-RELAY configuration on R1 and R3

```
R1#show ip interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 192.168.10.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is 10.1.1.2
Directed broadcast forwarding is disabled
R3#show ip interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 192.168.30.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is 10.2.2.2
Directed broadcast forwarding is disabled
```

19. Lab Standart AccessList (ACL)

ACL has the same function as the firewall feature on the proxy. ACLs are used to filter packets, both incoming and outgoing. The ACL analogy is like a security guard in a house. Security is given the task of allowing and denying someone to enter the house with orders given by their master.

There are 2 types of ACL operations at Cisco, namely Standard ACL and Extended ACL. This lab uses the ACL standard. The ACL standard only uses the Source Address as a consideration for denying or permitting.



Picture. ACL standards lab

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	F0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	F0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Picture. Addressing table

Previously the IP Address had been set and R1, R2 and R3 had been connected using RIPv2. The RIPv2 configuration can be checked in the previous lab.

Lab objectives:

• Network 192.168.11.0/24 cannot access the webserver.

So that only 192.168.11.0/24 cannot access the webserver and does not interfere with other networks, this ACL is suitable to be applied to R2, with an outbound interface to the

webserver. • Network 192.168.10.0/24 must not communicate with 192.168.30.0/24.

Similar to before, so that only the network is denied, the ACL rule is placed on the router closest to the destination, namely R3, the outbound interface facing PC3.

• ACL configuration on R2 uses standard numbered ACL, namely between 1-99 (number)

• Configure ACLs in R3 using named ACLs (text)

1. Configure numbered ACL on R2 with numbered ACL 10

Deny 192.168.11.0/24

Permit any

So, every packet originating or Source Address 192.168.11.0/24 that will go out to the WebServer network will be blocked, apart from Source Address 192.168.11.0/24 that's allowed.

```
R2#configure terminal
R2(config)#access-list 10 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 10 permit any
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip access-group 10 out R2(config-if)#end

R2#
R2#show access-lists Standard IP
access list 10 10 deny 192.168.11.0 0.0.0.255
(11 match(es))
20 permit any (27 match(es))

R2#show ip interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 192.168.20.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is 10
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
```

IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled

The command above is quite clear, by creating a numbered access-list on R2, numbered 10, with the rule that if the network 192.168.11.0-192.168.11.254 passes through the router it will rejected/deny, Apart from that,

permit 2. Configure named ACL on R3 with the name NO_ACCESS

Deny 192.168.10.0/24

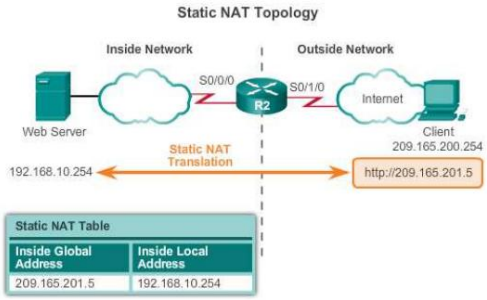
Permit any

So, every packet originating from Source Address 192.168.10.0/24 that will go out to the PC3 network will be blocked, apart from the Source Address 192.168.10.0/24 which is allowed.

```
R3#configure terminal R3(config)#ip
access-list standard NO_ACCESS
R3(config-std-nacl)#deny 192.168.10.0 0.0.0.255
R3(config-std-nacl)#permit any R3(config-std-
nacl)#exit
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ip access-group NO_ACCESS out R3(config-if)#end

R3#
R3#show access-lists Standard
IP access list NO_ACCESS
10 deny 192.168.10.0 0.0.0.255
20 permit any

R3#show access-lists Standard
IP access list NO_ACCESS
10 deny 192.168.10.0 0.0.0.255 (3 match(es))
                                20 ermit any
```

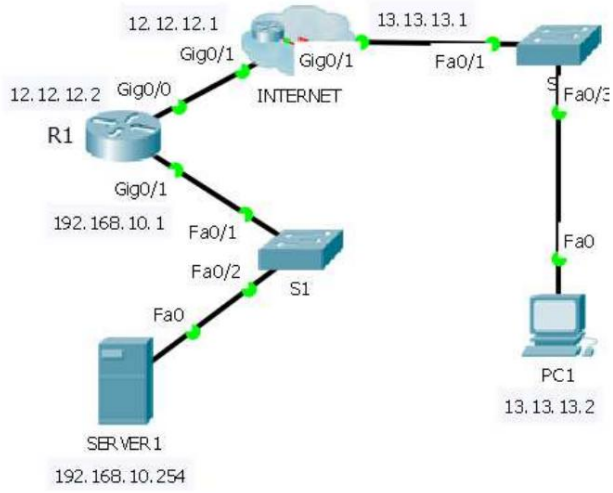
20. Lab Static NAT

Network Address Translation arises because of the limitations of IPv4. With NAT, Private IP is translated into Public IP. Using NAT saves IPv4 allocation, if there was no NAT, IPv4 might have run out before 2000.



Picture. Static nat topology

Static nat is often called One-to-one mapping. Usually used on a server so that it can be accessed from the internet, for example a website that is on a local web server at school which can be accessed from anywhere via the internet.



Picture. Static nat topology in packet tracer

In this lab, PC1 appears to be connected to the internet and gets a public IP, namely 13.13.13.2. Then R1 has a public IP, namely 12.12.12.2. Server1 is under R1 with a private IP address 192.168.10.254.

Table. NAT mapping

Inside local	**192.168.10.254 Private LAN**	
Inside global	**12.12.12.2**	**Public Internet**

Lab objectives:

- **PC1 can access the server by accessing 12.12.12.2**

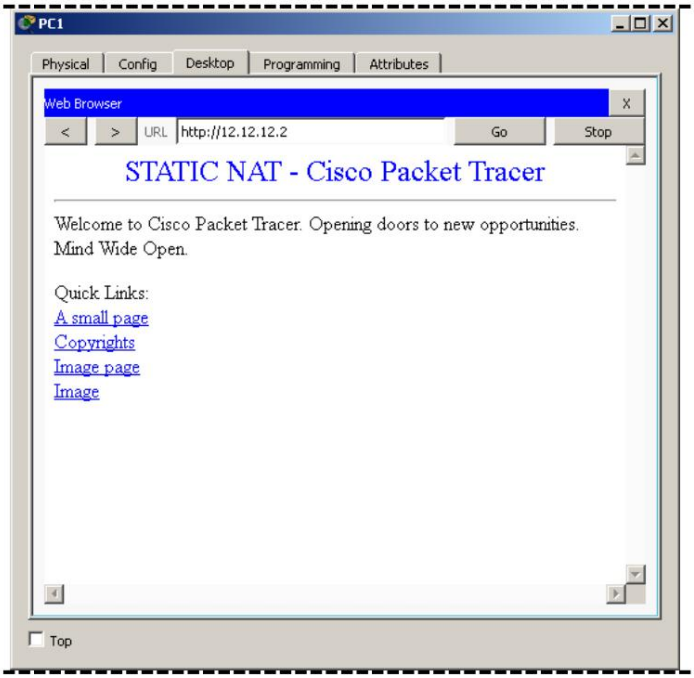
• Static nat configuration

The following is the One-to-one NAT configuration:

1. Configure Static NAT on R1

```
R1#configure terminal R1(config)#ip
nat inside source static 192.168.10.254 12.12.12.2
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip nat outside R1(config-if)#exit

R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ip nat inside R1(config-if)#end

R1#
```

2. Access from PC1 to the webserver



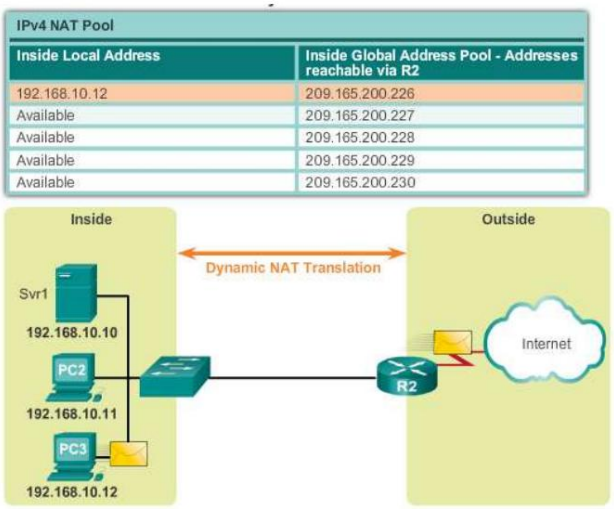
3. Verify the static nat configuration on R1

```
R1#show ip nat translations Pro Inside global
Inside local Outside local Outside global
--- 12.12.12.2 192.168.10.254 --- ---

R1#show ip nat translations Pro Inside global
Inside local Outside local Outside global
icmp 12.12.12.2:1 192.168.10.254:1 13.13.13.2:1 13.13.13.2:1
icmp 12.12.12.2:2 192.168.10.254:2 13.13.13.2:2 13.13.13.2:2
icmp 12.12.12.2:3 192.168.10.254:3 13.13.13.2:3 13.13.13.2:3
icmp 12.12.12.2:4 192.168.10.254:4 13.13.13.2:4 13.13.13.2:4
--- 12.12.12.2 192.168.10.254 --- ---
tcp 12.12.12.2:80 192.168.10.254:80 13.13.13.2:1025 13.13.13.2:1025
```

```
tcp 12.12.12.2:80 192.168.10.254:80 13.13.13.2:1026 13.13.13.2:1026


R1#show ip nat statistics
Total translations: 7 (1 static, 6 dynamic, 6 extended)
Outside Interfaces: GigabitEthernet0/0
Inside Interfaces: GigabitEthernet0/1
Hits: 17 Misses: 6
Expired translations: 0
Dynamic mappings:
Router#
```

IP translation results after passing through the router, which was originally Private IP 192.168.10.254 was translated one-to-one NAT with 12.12.12.2

21. Lab Dynamic NAT

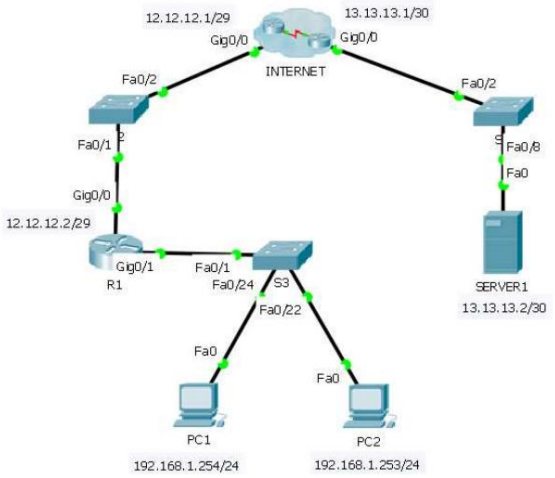


Picture. Example of Dynamic NAT

In contrast to static NAT which is only used 1:1, meaning 1 private IP to 1 private public, dynamic NAT uses POOL (collection/range of IPs). Dynamic NAT is a combination of POOL with ACL. ACLs allow which IP addresses can be translated to the internet.

Even though Dynamic NAT is limited and rarely used due to the increasingly limited IPv4, it will still be discussed.

For example, as in the picture above, a company has a Public IP from 209.165.200.226 to 209.165.200.230. Dynamic NAT will serve clients who are on the inside. If there is a client who will access the internet, the Router will work to map the available Public IP with the Private IP in the previously permitted ACL.



Picture. Dynamic NAT Labs

The topology above R1 has a Public IP allocation from 12.12.12.3-5, it will be used by 2 clients namely PC1 and PC2 to access Server1 which uses Public IP 13.13.13.2.

Lab objectives:

- **Create a dynamic lab**
- **Determine the Public IP Pool**
- **Determine ACLs that can use Public IP**

The following is the complete Dynamic NAT configuration:

1. Configure Dynamic NAT on R1

```
R1#configure terminal
R1(config)#ip nat pool DHCP1 12.12.12.3 12.12.12.5 netmask 255.255.255.248

R1(config)#access-list 1 permit 192.168.1.254
R1(config)#access-list 1 permit 192.168.1.253
R1(config)#ip nat inside source list 1 pool DHCP1
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip nat outside R1(config-if)#exit

R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ip nat inside R1(config-if)#end
```

DHCP1 holds the Private IP that will be used by the client. The clients that are allowed have been defined in access-list 1. Next, determine which ip nat outside (the part connected to the internet) and ip nat inside (local or private LAN).

2. Test the ping from the client

```
C:\>ping 13.13.13.2

Pinging 13.13.13.2 with 32 bytes of data:

Request timed out.
Reply from 13.13.13.2: bytes=32 time=13ms TTL=125
Reply from 13.13.13.2: bytes=32 time=11ms TTL=125
Reply from 13.13.13.2: bytes=32 time=13ms TTL=125

Ping statistics for 13.13.13.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 13ms, Average = 12ms

C:\>
```

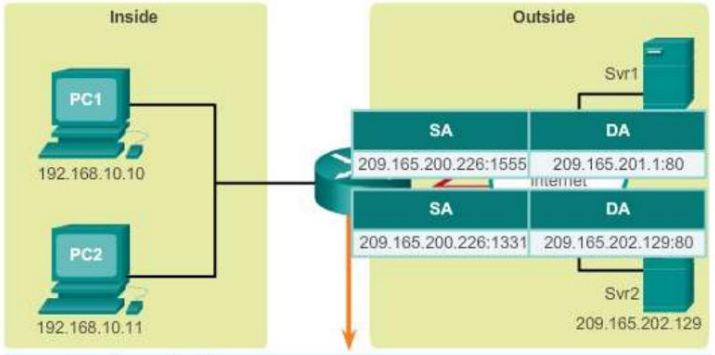
3. Verify the Dynamic NAT configuration on R1

```
R1#show ip nat translations Pro Inside global
Inside local Outside local Outside global
icmp 12.12.12.3:113 192.168.1.254:113 13.13.13.2:113 13.13.13.2:113
icmp 12.12.12.3:114 192.168.1.254:114 13.13.13.2:114 13.13.13.2:114
icmp 12.12.12.3:115 192.168.1.254:115 13.13.13.2:115 13.13.13.2:115
icmp 12.12.12.3:116 192.168.1.254:116 13.13.13.2:116 13.13.13.2:116
icmp 12.12.12.3:117 192.168.1.254:117 13.13.13.2:117 13.13.13.2:117
icmp 12.12.12.3:118 192.168.1.254:118 13.13.13.2:118 13.13.13.2:118
icmp 12.12.12.3:119 192.168.1.254:119 13.13.13.2:119 13.13.13.2:119
icmp 12.12.12.3:120 192.168.1.254:120 13.13.13.2:120 13.13.13.2:120
icmp 12.12.12.3:121 192.168.1.254:121 13.13.13.2:121 13.13.13.2:121
icmp 12.12.12.3:122 192.168.1.254:122 13.13.13.2:122 13.13.13.2:122
icmp 12.12.12.3:123 192.168.1.254:123 13.13.13.2:123 13.13.13.2:123
icmp 12.12.12.3:124 192.168.1.254:124 13.13.13.2:124 13.13.13.2:124
icmp 12.12.12.3:125 192.168.1.254:125 13.13.13.2:125 13.13.13.2:125
icmp 12.12.12.3:126 192.168.1.254:126 13.13.13.2:126 13.13.13.2:126
icmp 12.12.12.4:1019 192.168.1.253:1019 13.13.13.2:1019 13.13.13.2:1019
icmp 12.12.12.4:1020 192.168.1.253:1020 13.13.13.2:1020 13.13.13.2:1020
icmp 12.12.12.4:1021 192.168.1.253:1021 13.13.13.2:1021 13.13.13.2:1021
icmp 12.12.12.4:1022 192.168.1.253:1022 13.13.13.2:1022 13.13.13.2:1022
icmp 12.12.12.4:1023 192.168.1.253:1023 13.13.13.2:1023 13.13.13.2:1023
icmp 12.12.12.4:1024 192.168.1.253:1024 13.13.13.2:1024 13.13.13.2:1024
icmp 12.12.12.4:1025 192.168.1.253:1025 13.13.13.2:1025 13.13.13.2:1025
icmp 12.12.12.4:1026 192.168.1.253:1026 13.13.13.2:1026 13.13.13.2:1026
icmp 12.12.12.4:1027 192.168.1.253:1027 13.13.13.2:1027 13.13.13.2:1027
icmp 12.12.12.4:1028 192.168.1.253:1028 13.13.13.2:1028 13.13.13.2:1028
icmp 12.12.12.4:1029 192.168.1.253:1029 13.13.13.2:1029 13.13.13.2:1029
```

R1#sh ip nat statistics Total translations:
79 (0 static, 79 dynamic, 79 extended)
Outside Interfaces: GigabitEthernet0/0
Inside Interfaces: GigabitEthernet0/1
Hits: 1344 Misses: 1346
Expired translations: 1267
Dynamic mappings:
-- Inside Source
access-list 1 pool DHCP1 refCount 79
pool DHCP1: netmask 255.255.255.248
start 12.12.12.3 end 12.12.12.5
type generic, total addresses 3 Testing can use the . allocated 2 (66%), misses 0

show ip nat translation command. You can see the IP addresses in the defined pool used 12.12.12.3 and 12.12.12.4.

22. Lab NAT Overloaded atau Port Address Translation (PAT)



NAT Table with Overload

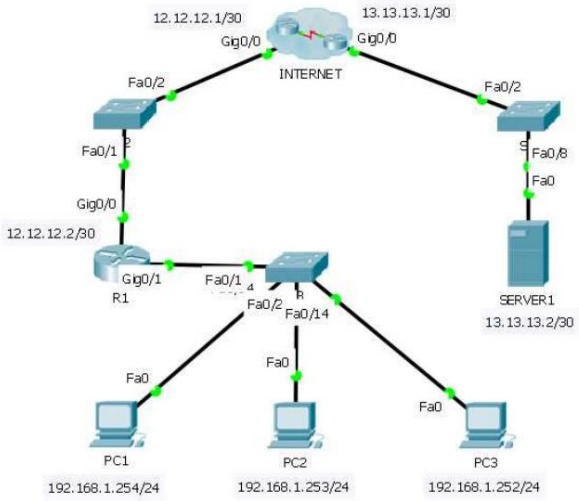
Inside Global IP Address	Inside Local IP Address	Outside Local IP Address	Outside Global IP Address
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.11:1331	209.165.202.129:80	209.165.202.129:80

Pictures. PAT

By using NAT Overloading/PAT, with only 1 Public IP, you can translate many Private IPs. This can be found in the RT/RW net or SOHO scale internet. As in the picture above, PC1 and PC2 are connected to a router, where the router only has 1 IP address, namely 209.165.200.226.

PC1 wants to access web services located at 209.165.201.1, while PC2 goes to 209.165.202.129. Because it only has 1 Public IP, namely 209.165.200.226, it is suitable to use NAT Overloading.

When PC1 and PC2 access their respective destinations, it is as if the router is accessing those destinations. SA or Source Address shows that 209.165.200.226 with a different DA Destination Address. The router differentiates using the port attached to its Public IP.



Gambar. Lab NAT Overloaded

The topology above, with only the Public IP installed on the R1 side, namely 12.12.12.1, all PC1, PC2 and PC3 clients can access the internet.

Lab objectives:

- **Determine the ACL of the NAT-allowed clients**
- **Overloaded NAT configuration**

The following is the Overloaded NAT configuration:

23. Configure nat on R1

```
R1#configure terminal
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#ip nat inside source list 1 interface gigabitEthernet 0/0 overload R1(config)#interface gigabitEthernet 0/0


R1(config-if)#ip nat outside R1(config-if)#exit

R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ip nat inside R1(config-if)#end

R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#sho
```

ACL 1 defines the IP range that is permitted/allowed to use NAT.
GigabitEthernet 0/0 is an exit interface/interface that is connected to the internet/public IP.

24. Test the ping from the client

```
C:\>ping 13.13.13.2

Pinging 13.13.13.2 with 32 bytes of data:

Request timed out.
Reply from 13.13.13.2: bytes=32 time=13ms TTL=125
Reply from 13.13.13.2: bytes=32 time=11ms TTL=125
Reply from 13.13.13.2: bytes=32 time=13ms TTL=125

Ping statistics for 13.13.13.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 13ms, Average = 12ms

C:\>
```

25. Verify NAT Overloaded configuration on R1

R1#show ip nat statistics

Total translations: 75 (0 static, 75 dynamic, 75 extended)

Outside Interfaces: GigabitEthernet0/0

Inside Interfaces: GigabitEthernet0/1

Hits: 2286 Misses: 2300

Expired translations: 2214

Dynamic mappings:

R1#show ip nat translations Pro Inside global

Inside local Outside local Outside global

icmp 12.12.12.2:10 192.168.1.252:10 13.13.13.2:10 13.13.13.2:10

icmp 12.12.12.2:11 192.168.1.252:11 13.13.13.2:11 13.13.13.2:11

icmp 12.12.12.2:12 192.168.1.252:12 13.13.13.2:12 13.13.13.2:12

icmp 12.12.12.2:13 192.168.1.252:13 13.13.13.2:13 13.13.13.2:13

icmp 12.12.12.2:14 192.168.1.252:14 13.13.13.2:14 13.13.13.2:14

icmp 12.12.12.2:15 192.168.1.252:15 13.13.13.2:15 13.13.13.2:15

icmp 12.12.12.2:16 192.168.1.252:16 13.13.13.2:16 13.13.13.2:16

icmp 12.12.12.2:17 192.168.1.252:17 13.13.13.2:17 13.13.13.2:17

icmp 12.12.12.2:18 192.168.1.252:18 13.13.13.2:18 13.13.13.2:18

icmp 12.12.12.2:19 192.168.1.252:19 13.13.13.2:19 13.13.13.2:19

icmp 12.12.12.2:2019 192.168.1.253:2019 13.13.13.2:2019 13.13.13.2:2019

icmp 12.12.12.2:2020 192.168.1.253:2020 13.13.13.2:2020 13.13.13.2:2020

icmp 12.12.12.2:2021 192.168.1.253:2021 13.13.13.2:2021 13.13.13.2:2021

icmp 12.12.12.2:2022 192.168.1.253:2022 13.13.13.2:2022 13.13.13.2:2022

icmp 12.12.12.2:2023 192.168.1.253:2023 13.13.13.2:2023 13.13.13.2:2023

icmp 12.12.12.2:2024 192.168.1.253:2024 13.13.13.2:2024 13.13.13.2:2024

icmp 12.12.12.2:2025 192.168.1.253:2025 13.13.13.2:2025 13.13.13.2:2025

icmp 12.12.12.2:2026 192.168.1.253:2026 13.13.13.2:2026 13.13.13.2:2026

icmp 12.12.12.2:2027 192.168.1.253:2027 13.13.13.2:2027 13.13.13.2:2027

```
icmp 12.12.12.2:2028 192.168.1.253:2028 13.13.13.2:2028 13.13.13.2:2028

icmp 12.12.12.2:2029 192.168.1.253:2029 13.13.13.2:2029 13.13.13.2:2029

icmp 12.12.12.2:2030 192.168.1.253:2030 13.13.13.2:2030 13.13.13.2:2030

icmp 12.12.12.2:2031 192.168.1.253:2031 13.13.13.2:2031 13.13.13.2:2031

icmp 12.12.12.2:2032 192.168.1.253:2032 13.13.13.2:2032 13.13.13.2:2032

icmp 12.12.12.2:2033 192.168.1.253:2033 13.13.13.2:2033 13.13.13.2:2033

icmp 12.12.12.2:2034 192.168.1.253:2034 13.13.13.2:2034 13.13.13.2:2034

icmp 12.12.12.2:2035 192.168.1.253:2035 13.13.13.2:2035 13.13.13.2:2035

icmp 12.12.12.2:2036 192.168.1.253:2036 13.13.13.2:2036 13.13.13.2:2036

icmp 12.12.12.2:2037 192.168.1.253:2037 13.13.13.2:2037 13.13.13.2:2037

icmp 12.12.12.2:2038 192.168.1.253:2038 13.13.13.2:2038 13.13.13.2:2038

icmp 12.12.12.2:2039 192.168.1.253:2039 13.13.13.2:2039 13.13.13.2:2039

icmp 12.12.12.2:2040 192.168.1.253:2040 13.13.13.2:2040 13.13.13.2:2040

icmp 12.12.12.2:2041 192.168.1.253:2041 13.13.13.2:2041 13.13.13.2:2041

icmp 12.12.12.2:2042 192.168.1.253:2042 13.13.13.2:2042 13.13.13.2:2042

icmp 12.12.12.2:2043 192.168.1.253:2043 13.13.13.2:2043 13.13.13.2:2043

icmp 12.12.12.2:2044 192.168.1.253:2044 13.13.13.2:2044 13.13.13.2:2044

icmp 12.12.12.2:2045 192.168.1.253:2045 13.13.13.2:2045 13.13.13.2:2045

icmp 12.12.12.2:2046 192.168.1.253:2046 13.13.13.2:2046 13.13.13.2:2046

icmp 12.12.12.2:2047 192.168.1.253:2047 13.13.13.2:2047 13.13.13.2:2047

icmp 12.12.12.2:2048 192.168.1.253:2048 13.13.13.2:2048 13.13.13.2:2048

icmp 12.12.12.2:2049 192.168.1.253:2049 13.13.13.2:2049 13.13.13.2:2049

icmp 12.12.12.2:2050 192.168.1.253:2050 13.13.13.2:2050 13.13.13.2:2050

icmp 12.12.12.2:2051 192.168.1.253:2051 13.13.13.2:2051 13.13.13.2:2051

icmp 12.12.12.2:20 192.168.1.252:20 13.13.13.2:20 13.13.13.2:20
icmp 12.12.12.2:217 192.168.1.254:217 13.13.13.2:217 13.13.13.2:217
icmp 12.12.12.2:218 192.168.1.254:218 13.13.13.2:218 13.13.13.2:218
```

```
icmp 12.12.12.2:219 192.168.1.254:219 13.13.13.2:219 13.13.13.2:219 icmp 12.12.12.2:21 192.168.1.252:21
13.13.13.2:21 13.13.13.2:21 icmp 12.12.12.2:220 192.168.1.254:220 13.13.13.2:220 13.13.13.2:220 icmp
12.12.12.2:221 192.168.1.254:221 13.13.13.2:221 13.13.13.2:221 icmp 12.12.12.2:222 192.168.1.254:222 13.13.13.2:222
13.13.13.2:222 icmp 12.12.12.2:223 192.168.1.254:223 13.13.13.2:223 13.13.13.2:223 icmp 12.12.12.2:224
192.168.1.254:224 13.13.13.2:224 13.13.13.2:224 icmp 12.12.12.2:225 192.168.1.254:225 13.13.13.2:225 13.13.13.2:225
icmp 12.12.12.2:226 192.168.1.254:226 13.13.13.2:226 13.13.13.2:226 icmp 12.12.12.2:227 192.168.1.254:227
13.13.13.2:227 13.13.13.2:227 icmp 12.12.12.2:228 192.168.1.254:228 13.13.13.2:228 13.13.13.2:228 icmp
12.12.12.2:229 192.168.1.254:229 13.13.13.2:229 13.13.13.2:229 icmp 12.12.12.2:22 192.168.1.252:22 13.13.13.2:22
13.13.13.2:22 icmp 12.12.12.2:230 192.168.1.254:230 13.13.13.2:230 13.13.13.2:230 icmp 12.12.12.2:231
192.168.1.254:231 13.13.13.2:231 13.13.13.2:231 icmp 12.12.12.2:232 192.168.1.254:232 13.13.13.2:232 13.13.13.2:232
icmp 12.12.12.2:233 192.168.1.254:233 13.13.13.2:233 13.13.13.2:233 icmp 12.12.12.2:234 192.168.1.254:234
13.13.13.2:234 13.13.13.2:234 icmp 12.12.12.2:235 192.168.1.254:235 13.13.13.2:235 13.13.13.2:235 icmp
12.12.12.2:236 192.168.1.254:236 13.13.13.2:236 13.13.13.2:236 icmp 12.12.12.2:237 192.168.1.254:237
13.13.13.2:237 13.13.13.2:237 icmp 12.12.12.2:238 192.168.1.254:238 13.13.13.2:238 13.13.13.2:238 icmp
12.12.12.2:239 192.168.1.254:239 13.13.13.2:239 13.13.13.2:239 icmp 12.12.12.2:23 192.168.1.252:23 13.13.13.2:23
13.13.13.2:23 icmp 12.12.12.2:240 192.168.1.254:240 13.13.13.2:240 13.13.13.2:240 icmp 12.12.12.2:241
192.168.1.254:241 13.13.13.2:241 13.13.13.2:241 icmp 12.12.12.2:242 192.168.1.254:242 13.13.13.2:242 13.13.13.2:242
icmp 12.12.12.2:243 192.168.1.254:243 13.13.13.2:243 13.13.13.2:243 icmp 12.12.12.2:244 192.168.1.254:244
13.13.13.2:244 13.13.13.2:244 icmp 12.12.12.2:245 192.168.1.254:245 13.13.13.2:245 13.13.13.2:245 icmp
12.12.12.2:246 192.168.1.254:246 13.13.13.2:246 13.13.13.2:246 icmp 12.12.12.2:247 192.168.1.254:247 13.13.13.2:247
13.13.13.2:247 icmp 12.12.12.2:248 192.168.1.254:248 13.13.13.2:248 13.13.13.2:248 icmp 12.12.12.2:249
192.168.1.254:249 13.13.13.2:249 13.13.13.2:249 icmp 12.12.12.2:24 192.168.1.252:24 13.13.13.2:24 13.13.13.2:24
icmp 12.12.12.2:250 192.168.1.254:250 13.13.13.2:250 13.13.13.2:250 icmp 12.12.12.2:251 192.168.1.254:251
13.13.13.2:251 13.13.13.2:251 icmp 12.12.12.2:252 192.168.1.254:252 13.13.13.2:252 13.13.13.2:252 icmp
12.12.12.2:253 192.168.1.254:253 13.13.13.2:253 13.13.13.2:253 icmp 12.12.12.2:254 192.168.1.254:254 13.13.13.2:254
13.13.13.2:254 icmp 12.12.12.2:25 192.168.1.252:25 13.13.13.2:25 13.13.13.2:25 icmp 12.12.12.2:26 192.168.1.252:26
13.13.13.2:26 13.13.13.2:26 icmp 12.12.12.2:5 192.168.1.252:5 13.13.13.2:5 13.13.13.2:5 icmp 12.12.12.2:6
192.168.1.252:6 13.13.13.2:6 13.13.13.2:6 icmp 12.12.12.2:7 192.168.1.252:7 13.13.13.2:7 13.13.13.2:7 icmp
12.12.12.2:8 192.168.1.252:8 13.13.13.2:8 13.13.13.2:8 icmp 12.12.12.2:9 192.168.1.252:9 13.13.13.2:9 13.13.13.2:9
```

R1#

Testing shows that 3 IP addresses, namely 192.168.1.252, 192.168.1.253 and 192.168.1.254, are translated into 12.12.12.2 with a random port.

CHAPTER 5

Infrastructure Maintenance

Lab Devices Monitoring dengan Syslog 65

Lab Network Time Protocol (NTP) 67

Lab Backup dan Restore iOS TFTP 75

Lab Cisco Troubleshoot tools 77

23. Lab Devices Monitoring dengan Syslog

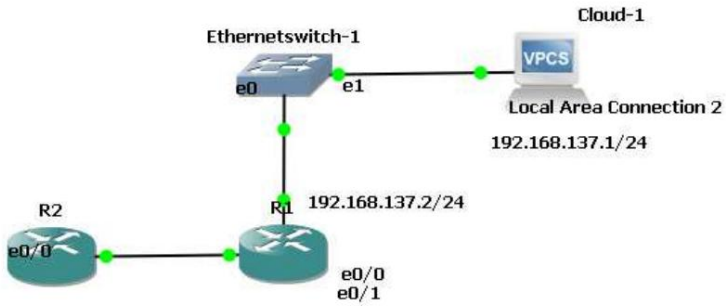
Syslog is used by Network Administrators to view logs that occur on network devices. Syslog is defined in RFC 3164 using UDP port 514.

Syslog is generally used for monitoring, troubleshooting, and saving logs on a device to the syslog server. Logs sent to the syslog server have several warning levels, from level 1 to 7.

Syslog server is installed on the computer connected to the device to be monitored. There are many syslog servers that you can try, including the following:

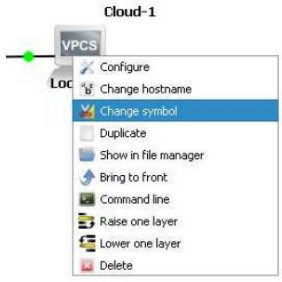
Picture. Various types of syslog server applications

In this lab, Syslog Server 1.2.3 is used. Then the topology uses GNS3, where Syslog Serer 1.2.3 is installed on the laptop.



Picture. Syslog lab topology

The VPCS in the topology above only changed its symbol, which was originally Cloud.
Then make sure the laptop has a loopback interface. Connect the loopback with the cloud whose symbol has been changed earlier. Next, set the IP address
192.168.137.x.



Picture. Change cloud symbol to pc

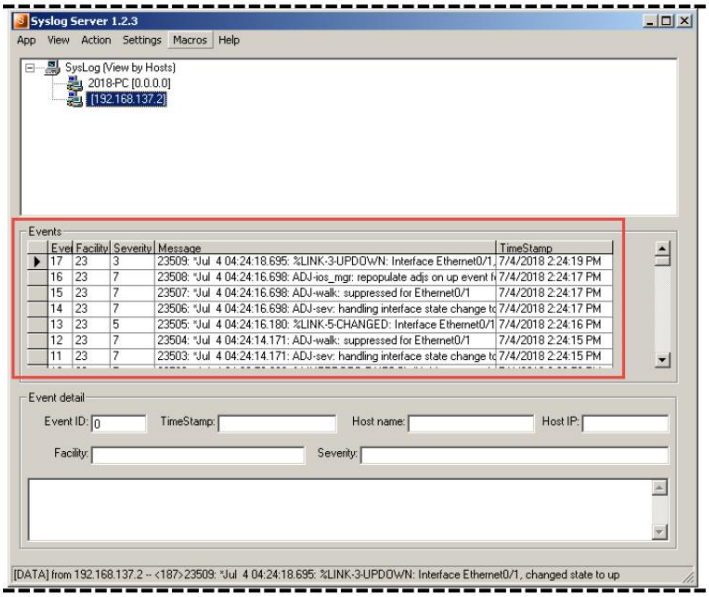
After installing Syslog Server 1.2.3, make sure they are connected to each other. After that, continue with the Router configuration for which the log will be captured. The following is the configuration on R1:

1. Configure logging

```
R1#configure terminal
R1(config)#logging 192.168.137.1
R1(config)#logging trap 7 R1(config)#logging
source-interface ethernet 0/0
R1(config)#interface loopback 0
R1(config-if)#shutdown
R1(config)#no shutdown
R1(config)#end
R1#
```

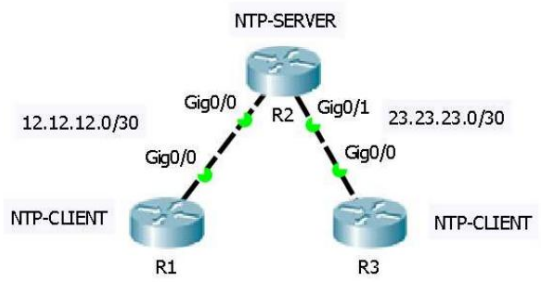
The command above tells the router to direct the loggi to the syslog server located at address 192.168.137.1. To test whether it works or not, experiment by activating and deactivating the loopback interface.

2. Results on server syslog



24. Lab Network Time Protocol (NTP)

So that log results are accurate, correct time configuration is required. This lab is about Clock configuration followed by NTP Client.



Picture. NTP Topoogy

Lab objectives:

- **Configure time on R2**
- **Configure NTP Client on R1 and R3**

1. Konfig clock

```
R2#
R2#clock set 11:23:59 04 July 2018
R2#show clock
11:24:2.172 UTC Wed Jul 4 2018
R2#
```

2. Configure NTP Client

```
R3#configure terminal Enter
configuration commands, one per line. End with CNTL/Z.
R3(config)#ntp server 23.23.23.1
R3(config)#exit
R3#
```

25. Lab Basic Device Hardening

Securing devices on a network is the first effort carried out by a network administrator. There are many ways to do device hardening. Here are several ways to secure devices on a network:

1. Password

Use a password with at least 8 characters, or more. Even if it could be a 10 character password. Make the password more complicated, namely with a combination of letters, numbers, characters, symbols and even spaces. Don't use commonly used passwords such as @dmin or p@ssw0rd. Change your password regularly and lastly, don't write/save your password in a place where other people can access it freely.

2. Enable password to enter Priviledge Mode

```
R1#configure terminal
R1(config)#enable password cisco
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show running-config Building
configuration...

Current configuration : 627 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

! hostname R1

!!

! enable password cisco
!

!!

!!

! ip cef
no ipv6 cef

R1#exit



R1 con0 is now available

Press RETURN to get started.

R1> one
Password:
R1#
```

The enable password command will restrict users from entering Priviledge Mode. The disadvantage of enabling passwords is that passwords are not encrypted, so it is more advisable to use the enable secret command

3. Enable secret (more secure than enable password)

```
R1#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable secret ciscosec
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit



R1 con0 is now available

Press RETURN to get started.

R1> one
Password:

R1#show running-config Building
configuration...

Current configuration : 674 bytes

! version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
'
hostname R1
'


! ! enable secret 5 $1$mERr$thF1sEHJ9Dl2J3WzXxyZ1/
enable password cisco

! ip cef

R1#
```

The enable secret command will encrypt the password when viewed using show running-configuration. By executing the enable secret command, even though the enable password has been executed automatically, what is used by the system is the enable secret

4. Secure the line console

```
R1#configure terminal
R1(config)#line console 0
R1(config-line)#password ciscocon
R1(config-line)#login
R1(config-line)#end
R1#exit
```

```
R1 con0 is now available

Press RETURN to get started.


User Access Verification

Password:

R1>one
Password:
R1#

R1#show running-config Building
configuration...

Current configuration : 700 bytes

! version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

! hostname R1

''

! enable secret 5 $1$mERr$thF1sEHJ9Dl2J3WzXxyZ1/
enable password cisco


! ! ip cef
no ipv6 cef


! ! license udi pid CISCO1941/K9 sn FTX1524YU4U
'

! spanning-tree mode pvst

! interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown

! interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
```

```
shutdown

! interface Vlan1
no ip address
shutdown

! ip classless
'
ip flow-export version 9
'


''


''


! ! line con 0
password ciscocon
login

! line to 0
'

R1#
```

When someone accesses the router/switch via the console port, they automatically have to enter the line console password. If you check with show running-config, you can see there the console line using the password ciscocon. The login option forces the router/switch to use a previously set password if you want to enter the system.

5. Secure the vty line

```
R1#configure terminal Enter
configuration commands, one per line. End with CNTL/Z.
R1(config)#lin
R1(config)#line vt
R1(config)#line vty 0 15
R1(config-line)#password ciscovty
R1(config-line)#login
R1(config-line)#end
```

VTY line is the line used to access Cisco devices using Telnet.
Generally Cisco supports up to 16 VTY lines. The ciscovty password will only be used when the administrator wants to access cisco devices using telnet.

6. Encrypt semua pasword dengan service password-encryption

The passwords for the console line and vty line above, if you look at the show running-config, will be clearly visible. Therefore, use the password-encryption service to encrypt all passwords.

```
R1#configure terminal R1(config)#service
password-encryption R1(config)#end

R1#show running-config Building
configuration...

Current configuration : 801 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption

! hostname R1

! enable secret 5 $1$mERr$thF1sEHJ9Dl2J3WzXxyZ1/
enable password 7 0822455D0A16

! ip cef
no ipv6 cef

! license udi pid CISCO1941/K9 sn FTX1524YU4U
!

spanning-tree mode pvst

! interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown

! interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless

! ip flow-export version 9
```

```
! line con 0
password 7 0822455D0A1606181C
login

! line to 0

! line vty 0 4
password 7 0822455D0A1613030B
login
line vty 5 15
password 7 0822455D0A1613030B
login
!
!!
end

R1#
```

All passwords will change to encrypted for both the console, VTY and the device.

7. Use banners as reminders

Even though using an encrypted password secures Cisco devices, it is important to send a message to anyone who tries to access devices they don't have access to.

Messages like "Welcome to R1" and so on are not suitable for use. It should be something like "This device is monitored by the system, all forms of unauthorized access are subject to applicable law!"

```
R1#configure terminal Enter
configuration commands, one per line. End with CNTL/Z.
R1(config)#banner login # You access R1, this device is monitored by the system, any form of unauthorized access
is subject to applicable law.!#

R1(config)#banner motd # Backup devices every Saturday, 03.00 am #

R1(config)#end
```

The login banner and motd banner both provide warnings to users who want to access the system either via console or telnet. Motd banners are more specifically used as messages that can change over time.

8. SSH configuration

SSH promises more security than Telnet.

```
Router#configure terminal
```

```
R2(config)#hostname R2
R2(config)#ip domain-name didit.com
R2(config)#crypto key generate rsa
The name for the keys will be: R2.didit.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R2(config)#username didit privilege 15 secret didit
R2(config-line)#transport input telnet
R2(config-line)#transport input ssh
R2(config-line)#login local R2(config-line)#end
```

SSH requires a unique domain on the network, so the first step is setting the hostname then the domain.

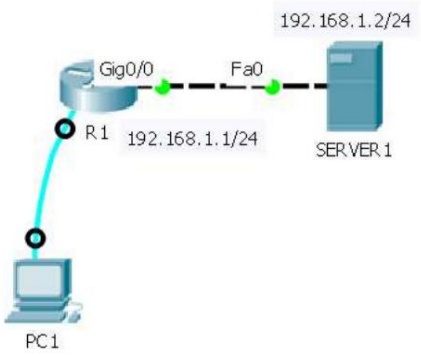
Next, generate encryption on SSH with the command crypto key generate rsa general-key, the higher the modulus, the more secure the encryption.

Create a local username database with the username command

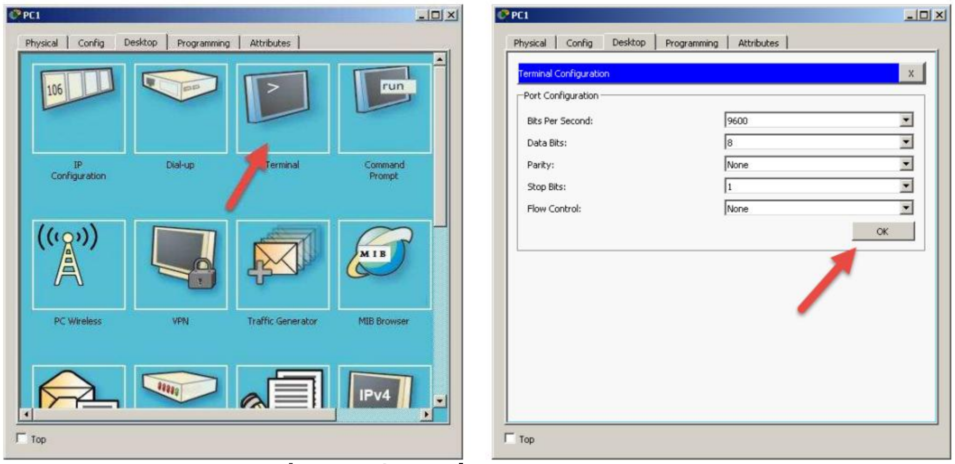
Make the line vty use the local database

26. Lab Backup dan Restore iOS TFTP

To perform a backup, you need a TFTP program that has been installed on the client and server side. TFTP is used to upgrade iOS, backup iOS, restore iOS, backup running-configuration, startup-configuration etc.



Picture. Backup topology with TFTP server



Picture. Console access to Router

Here are the steps to backup iOS to tftp server:

1. Check connectivity from the Router to the server

```
Router#configure terminal
Router(config)#hostname R1
R1(config)#
R1#
%SYS-5-CONFIG_I: Configured from console by console
ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms


R1#
```

Make sure you can ping each other between the Router and Server 2. Backup to TFTP Server

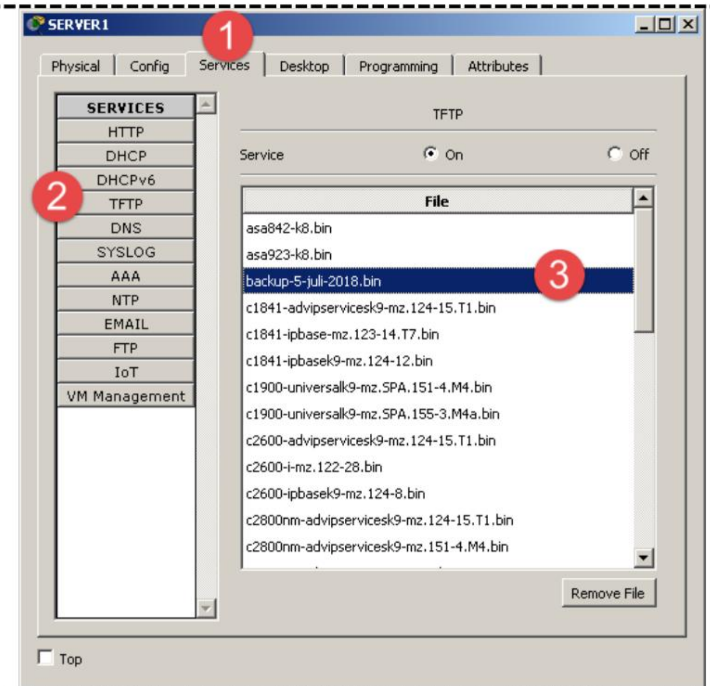
```
R1#copy tftp: flash:
Address or name of remote host []? 192.168.1.2
Source filename []? backup-july-5-2018.bin
Destination filename [backup-5-juli-2018.bin]? c1900-
universalk9-mz.SPA.151-4.M4.bin

Accessing tftp://192.168.1.2/backup-5-juli-2018.bin...
Loading backup-5-juli-2018.bin from 192.168.1.2: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

!!!
!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 0.683 secs (5163977 bytes/sec)

Copy from flash: to tfpt server

3. Check the TFTP Server



Service on the TFTP server, which accommodates copy results from Cisco devices

4. To restore, just go to the command line, match the name in TFTP

R1#copy tftp: flash:
Address or name of remote host []? 192.168.1.2
Source filename []? backup-july-5-2018.bin
Destination filename [backup-5-july-2018.bin]?

Accessing tftp://192.168.1.2/backup-5-juli-2018.bin...
Loading backup-5-juli-2018.bin from 192.168.1.2: !!!

!!!
!!!
!!!
!!!
!!!
[OK - 33591768 bytes]

```
33591768 bytes copied in 0.676 secs (5217451 bytes/sec)
R1#
```

27. Lab Cisco Troubleshoot tools

To carry out troubleshooting on a network, several commands are needed as below:

Tabel. CLI Troubleshoot cisco devices

show version Displays the iOS version show ip interface brief Displays the configuration on	
the interface briefly show interfaces fastethernet0/0 Displays information on FastEthernet0/0 show ip route Displays the routing table	
show protocols Displays the protocol used show arp Displays arp show running-config Displays the current configuration	
running show vlan Showing vlan Testing connectivity to 192.168.1.1 Testing the route taken to	
get to 192.168.11 Remotely 192.168.1.1	
ping 192.168.1.1 traceroute	
192.168.1.1	
telnet 192.168.1.1	
debug	Enables debug/log features
show ip access-list	Displays running ACLs