



Network I Lab 04

IP & subnet Mask

Building simple star network with gateway

build Straight-Through Cable

Objective

- Understand the network ip resolution
- Understand gateway functionality

Back ground

IP addresses

An IP address is a 32-bit number that uniquely identifies a host (computer or other device, such as a printer or router) on a TCP/IP network.

IP addresses are normally expressed in dotted-decimal format, with four numbers separated by periods, such as 192.168.123.132. To understand how subnet masks are used to distinguish between hosts, networks, and subnetworks, examine an IP address in binary notation.

For example, the dotted-decimal IP address 192.168.123.132 is (in binary notation) the 32 bit number 110000000101000111101110000100. This number may be hard to make sense of, so divide it into four parts of eight binary digits.

These eight bit sections are known as octets. The example IP address, then, becomes 11000000.10101000.01111011.10000100. This number only makes a little more sense, so for most uses, convert the binary address into dotted-decimal format (192.168.123.132). The decimal numbers separated by periods are the octets converted from binary to decimal notation.

IP address has two parts. The first part of an IP address is used as a network address, the last part as a host address. If you take the example 192.168.123.132 and divide it into these two parts you get the following:

192.168.123.	Network
.132	Host

-or-

192.168.123.0	Network
0.0.0.132	Host

Subnet mask

The second item, which is required for TCP/IP to work, is the subnet mask. The subnet mask is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network.

In TCP/IP, the parts of the IP address that are used as the network and host addresses are not fixed, so the network and host addresses above cannot be determined unless you have more information. This information is supplied in another 32-bit number called a subnet mask. In this example, the subnet mask is 255.255.255.0. It is not obvious what this number means unless you know that 255 in binary notation equals 11111111; so, the subnet mask is:

11111111.11111111.11111111.00000000

Lining up the IP address and the subnet mask together, the network and host portions of the address can be separated:

11000000.10101000.01111011.10000100	IP address (192.168.123.132)
11111111.11111111.11111111.00000000	Subnet mask (255.255.255.0)

The first 24 bits (the number of ones in the subnet mask) are identified as the network address, with the last 8 bits (the number of remaining zeros in the subnet mask) identified as the host address. This gives you the following:

11000000.10101000.01111011.00000000	Network address (192.168.123.0)
00000000.00000000.00000000.10000100	Host address (000.000.000.132)

So now you know, for this example using a 255.255.255.0 subnet mask, that the network ID is 192.168.123.0, and the host address is 0.0.0.132. When a packet arrives on the 192.168.123.0 subnet (from the local subnet or a remote network), and it has a destination address of 192.168.123.132, your computer will receive it from the network and process it.

Almost all decimal subnet masks convert to binary numbers that are all ones on the left and all zeros on the right. Some other common subnet masks are:

Decimal	Binary
255.255.255.192	11111111.11111111.11111111.11000000
255.255.255.224	11111111.11111111.11111111.11100000

Network classes

IP addresses are divided into classes. The most common of these are classes A, B, and C. Classes D and E exist, but are not generally used by end users. Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet. Following are the ranges of Class A, B, and C Internet addresses, each with an example address:

- Class A networks use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.
- Class B networks use a default subnet mask of 255.255.0.0 and have 128-191 as their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.
- Class C networks use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

In some scenarios, the default subnet mask values do not fit the needs of the organization, because of the physical topology of the network, or because the numbers of networks (or hosts) do not fit within the default subnet mask restrictions. The next section explains how networks can be divided using subnet masks.

Default gateways

If a TCP/IP computer needs to communicate with a host on another network, it will usually communicate through a device called a router. In TCP/IP terms, a router that is specified on a host, which links the host's subnet to other networks, is called a default gateway. This section explains how TCP/IP determines whether or not to send packets to

its default gateway to reach another computer or device on the network.

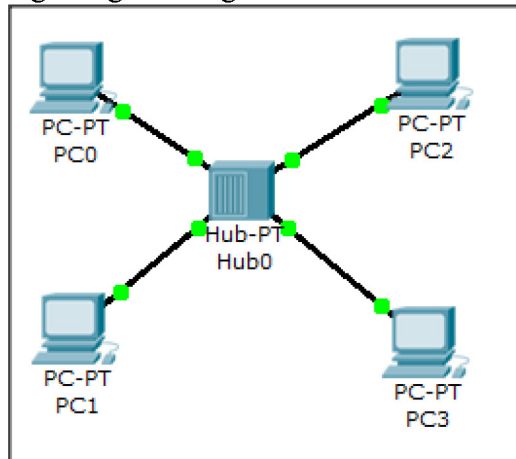
When a host attempts to communicate with another device using TCP/IP, it performs a comparison process using the defined subnet mask and the destination IP address versus the subnet mask and its own IP address. The result of this comparison tells the computer whether the destination is a local host or a remote host.

If the result of this process determines the destination to be a local host, then the computer will simply send the packet on the local subnet. If the result of the comparison determines the destination to be a remote host, then the computer will forward the packet to the default gateway defined in its TCP/IP properties. It is then the responsibility of the router to forward the packet to the correct subnet.

Steps

Part 1: Simple 4 PCs star network contains two different logical network

1. Connect 4 PCs sing straight through cables to hub as shown.



2. Apply the following configuration to PCs

PC name	PC01
IP	192.168.1.101
Subnet mask	255.255.255.0
Gateway	-
DNS	-

PC name	PC02
IP	192.168.1.102
Subnet mask	255.255.255.0
Gateway	-
DNS	-

PC name	PC03
IP	192.168.1.103
Subnet mask	255.255.255.0

Gateway	-
DNS	-

PC name	PC04
IP	192.168.1.1040
Subnet mask	255.255.255.0
Gateway	-
DNS	-

3. Test communication between pcs sing ping command

```
PC1>Ping 192.168.1.102
PC1> ping 192.168.1.103
PC1> ping 192.168.1.104
```

Conclusion

All pcs belongs to one network 192.168.1.0
Any PCs can access all other PCs in the network

4. Now change configuration as follows

PC name	PC01
IP	192.168.1.101
Subnet mask	255.255.255.0
Gateway	-
DNS	-

PC name	PC02
IP	192.168.1.102
Subnet mask	255.255.255.0
Gateway	-
DNS	-

PC name	PC03
IP	192.168.2.101
Subnet mask	255.255.255.0
Gateway	-
DNS	-

PC name	PC04
IP	192.168.2.102
Subnet mask	255.255.255.0
Gateway	-
DNS	-

5. Test connectivity between PCs using ping command

```
PC1> ping 192.168.1.102
PC1> ping 192.168.2.103
PC1> ping 192.168.2.104
PC2> ping 192.168.1.101
PC2> ping 192.168.2.103
```

PC2> ping 192.168.2.104

Conclusion

There are two different class C network 192.168.1.0, and 192.168.2.0
PC1, and PC2 on the first network can communicate with each other
PC3, and PC4 on the second network can communicate with other
Network 1 PCs can't communicate with network 2 PCs

6. Change configuration again as follows

PC name	PC01
IP	192.168.1.101
Subnet mask	255.255.0.0
Gateway	-
DNS	-

PC name	PC02
IP	192.168.1.102
Subnet mask	255.255.0.0
Gateway	-
DNS	-

PC name	PC03
IP	192.168.2.101
Subnet mask	255.255.0.0
Gateway	-
DNS	-

PC name	PC04
IP	192.168.2.102
Subnet mask	255.255.0.0
Gateway	-
DNS	-

7. Test connectivity between PCs using ping command

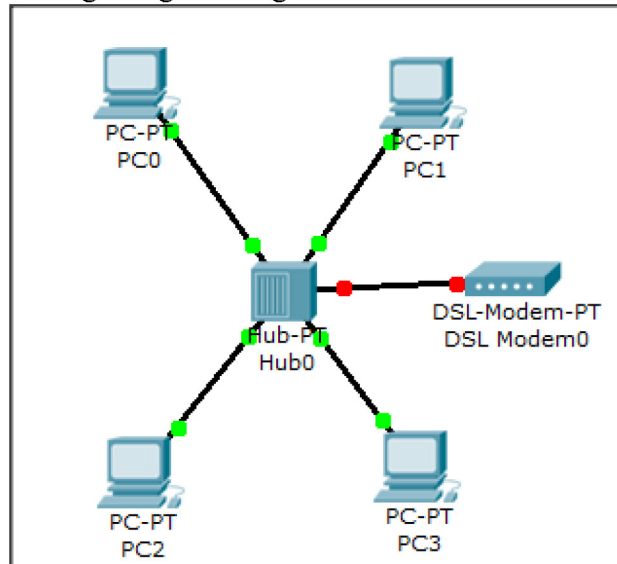
PC1> ping 192.168.1.102
PC1> ping 192.168.2.103
PC1> ping 192.168.2.104
PC2> ping 192.168.1.101
PC2> ping 192.168.2.103
PC2> ping 192.168.2.104

Conclusion

There only one class B network 192.168.0.0,
Any PCs can access all other PCs in the network

Part2: Simple 4 PCs star network with gateway using automatic configuration

1. Connect 4 PCs sing straight through cables to hub as shown.



2. Apply the following configuration to internet Gateway

IP	192.168.1.1
Mask	255.255.255.0
DHCP range	192.168.1.100 ~ 192.168.1.200

3. Apply the following configuration to PCs

PC name	PC01
IP	auto
Subnet mask	-
Gateway	-
DNS	-

PC name	PC02
IP	auto
Subnet mask	-
Gateway	-
DNS	-

PC name	PC03
IP	Auto
Subnet mask	-
Gateway	-
DNS	-

PC name	PC04
IP	Auto

Subnet mask	-
Gateway	-
DNS	-

4. Get configurations from PCs using ipconfig command

PC1> ipconfig

5. Test connectivity between PCs using ping command

PC1> ping 192.168.1.102
PC1> ping 192.168.1.103
PC1> ping 192.168.1.104
PC2> ping 192.168.1.101
PC2> ping 192.168.1.103
PC2> ping 192.168.1.104

Conclusion

Gateway and DHCP automatically assign ip addresses to connected clients

6. Turn off gateway, check configuration and connectivity again

PC1> ipconfig
PC1> ping 192.168.1.102
PC1> ping 192.168.2.103
PC1> ping 192.168.2.104
PC2> ping 192.168.1.101
PC2> ping 192.168.2.103
PC2> ping 192.168.2.104

7. Turn off PCs network adaptor, after a while turn it back on, check configuration and connectivity again

PC1> ipconfig
PC1> ping 192.168.1.102
PC1> ping 192.168.2.103
PC1> ping 192.168.2.104
PC2> ping 192.168.1.101
PC2> ping 192.168.2.103
PC2> ping 192.168.2.104

Conclusion

Regarding LAN gateway and DHCP is only responsible of assigning IP addresses to PCs

Part3: Simple 4 PCs star network with gateway using manual configuration

1. Apply the following configuration to internet Gateway

IP	192.168.1.1
Mask	255.255.255.0
DHCP range	192.168.1.100 ~ 192.168.1.200

2. Apply the following configuration to PCs

PC name	PC01
IP	192.168.1.101
Subnet mask	255.255.255.0
Gateway	-
DNS	-

PC name	PC02
IP	192.168.1.102
Subnet mask	255.255.255.0
Gateway	-
DNS	-

PC name	PC03
IP	192.168.1.103
Subnet mask	255.255.0.0
Gateway	-
DNS	-

PC name	PC04
IP	192.168.1.104
Subnet mask	255.255.0.0
Gateway	-
DNS	-

3. Get configurations from PCs using ipconfig command

PC1> ipconfig

4. Test connectivity between PCs using ping command

PC1> ping 192.168.1.102
PC1> ping 192.168.1.103
PC1> ping 192.168.1.104
PC3> ping 192.168.1.101
PC3> ping 192.168.1.103
PC3> ping 192.168.1.104

Conclusion

Regarding LAN the main function of gateway and DHCP server is to automatically assign IP for each PC inside the network. But the communication between PCs established behind that gateway, but you need to give these PCs a static IP first.

Part4: Testing gateway functionalities I

1. Apply the following configuration to internet Gateway

IP	192.168.1.1
Mask	255.255.0.0
DHCP range	192.168.1.100 ~ 192.168.1.200

2. Apply the following configuration to PCs

PC name	PC01
IP	192.168.1.101
Subnet mask	255.255.255.0
Gateway	192.168.1.1
DNS	192.168.1.1

PC name	PC02
IP	192.168.1.102
Subnet mask	255.255.255.0
Gateway	-
DNS	-

PC name	PC03
IP	192.168.1.103
Subnet mask	255.255.255.0
Gateway	192.168.1.1
DNS	192.168.1.1

PC name	PC04
IP	192.168.1.104
Subnet mask	255.255.255.0
Gateway	-
DNS	-

3. Get configurations from PCs using ipconfig command

PC1> ipconfig

4. Test connectivity between PCs using ping command

PC1> ping 192.168.1.102
PC1> ping 192.168.1.103
PC1> ping 192.168.1.104
PC1> ping 8.8.8.8
PC2> ping 192.168.1.101
PC2> ping 192.168.1.103
PC2> ping 192.168.1.104
PC2> ping 8.8.8.8
PC3> ping 192.168.1.101
PC3> ping 192.168.1.102
PC3> ping 192.168.1.104
PC3> ping 8.8.8.8
PC4> ping 192.168.1.101
PC4> ping 192.168.1.102
PC4> ping 192.168.1.103
PC4> ping 8.8.8.8

Conclusion

Internal LAN is accessible without defining the gateway address
Internet WAN is not accessible without defining gateway address

Part5: Testing gateway functionalities II

Get the gateway of internet router for example "163.121.170.83"

1. Test connectivity between PCs using ping command

PC1> tracert 163.121.170.83

PC3> tracert 163.121.170.83

```
C:\Windows\system32\cmd.exe
-4 Force using IPv4.
-6 Force using IPv6.

C:\Users\Ahmed ElShafee>tracert 163.121.170.83

Tracing route to 60CT2-R06C-GZ-EG [163.121.170.83]
over a maximum of 30 hops:
  0  6 ms   2 ms   2 ms  192.168.1.1
  1  16 ms  14 ms  14 ms  60CT2-R06C-GZ-EG [163.121.170.83]
  2  15 ms  14 ms  14 ms  host-163.121.217.10.tedata.net [163.121.217.10]
  3  17 ms  15 ms  14 ms  host-163.121.217.10.tedata.net [163.121.217.10]
  4  15 ms  16 ms  16 ms  host-163.121.216.254.tedata.net [163.121.216.254]
  5  21 ms  20 ms  18 ms  host-163.121.211.102.tedata.net [163.121.211.102]
  6  19 ms  16 ms  18 ms  host-163.121.160.166.tedata.net [163.121.160.166]
  7  20 ms  17 ms  23 ms  60CT2-R06C-GZ-EG [163.121.170.83]

Trace complete.
C:\Users\Ahmed ElShafee>
```

Conclusion

Internet consists of interconnected routers each router has its own gateway. Packets are being transferred from node to node till reaching destination