Network Addressing

Hydrosat Training Sessions

Abdallah Ibrahim
Technical Archtect & Cloud Cosultant
abdallah.cisco@gmail.com
abdallahcoptan.github.io

Addressing the network-IPv4

Each device on a network must be uniquely defined. At the Network layer, the packets of the communication need to be identified with the source and destination addresses of the two end systems. With IPv4, this means that each packet has a 32-bit source address and a 32-bit destination address in the Layer 3 header.

These addresses are used in the data network as binary patterns. Inside the devices, digital logic is applied for their interpretation. For us in the human network, a string of 32 bits is difficult to interpret and even more difficult to remember. Therefore, we represent IPv4 addresses using dotted decimal format.

For example, the address:

10101100000100000000010000010100

is expressed in dotted decimal as: 172.16.4.20

Types of addresses:

Network address - The address by which we refer to the network

Broadcast address - A special address used to send data to all hosts in the network

Host addresses - The addresses assigned to the end devices in the network

Network Prefixes :

When we express an IPv4 network address, we add a prefix length to the network address. The prefix length is the number of bits in the address that gives us the network portion. For example, in 172.16.4.0 /24, the /24 is the prefix length

Another address is used to detect network portion is called subnet mask where it either 1's or 0's.

Ex :

172.16.4.0/24

Host addresses 172.16.4.1→254

Broadcast address 172.16.4.255

Subnet mask 255.255.255.0

Ex :

172.16.4.00000000/25

Host addresses 172.16.4.1→126

Broadcast address 172.16.4.127

Subnet mask 255.255.255.128

Ex :

172.16.4.00000000/26

Host addresses 172.16.4.1→62

Broadcast address 172.16.4.63

Subnet mask 255.255.255.64

Ex :

169.252.22.129/27

169.252.22.10000001

Network address 169.252.22.128

Host addresses 169.252.22.129→158

Broadcast address 169.252.22.159

Subnet mask 255.255.255.224

Ex :

169.252.22.129/17

169.252.00010110.10000001

Network address 169.252.0.0

Host addresses 169.252.0.1→169.252.127.254

Broadcast address 169.252.127.255

Subnet mask 255.255.128.0

Types of communications:

In an IPv4 network, the hosts can communicate one of three different ways:

Unicast - the process of sending a packet from one host to an individual host

Broadcast - the process of sending a packet from one host to all hosts in the network

255.255.255.255

-Directed Broadcast

A directed broadcast is sent to all hosts on a specific network.

-Limited Broadcast

The limited broadcast is used for communication that is limited to the hosts on the local network.

Multicast - the process of sending a packet from one host to a selected group of hosts

Hosts that wish to receive particular multicast data are called multicast clients.

Each multicast group is represented by a single IPv4 multicast destination address. When an IPv4 host subscribes to a multicast group, the host processes packets addressed to this multicast address as well as packets addressed to its uniquely allocated unicast address. As we will see, IPv4 has set aside a special block of addresses from 224.0.0.0 to 239.255.255.255 for multicast groups addressing.

Reserved IPv4 address range:

Each multicast group is represented by a single IPv4 multicast destination address. When an IPv4 host subscribes to a multicast group, the host processes packets addressed to this multicast address as well as packets addressed to its uniquely allocated unicast address. As we will see, IPv4 has set aside a special block of addresses from 224.0.0.0 to 239.255.255.255 for multicast groups addressing.

1) Host addresses

Used for IPv4 hosts (0.0.0.0 to 233.255.255.255)

2) Multicast addresses

As previously shown, another major block of addresses reserved for special purposes is the IPv4 multicast address range 224.0.0.0 to 239.255.255.255.

the multicast address range is subdivided into different types of addresses:

1. reserved link local addresses:
   The IPv4 multicast addresses 224.0.0.0 to 224.0.0.255 are reserved link local addresses. These addresses are to be used for multicast groups on a

local network. Packets to these destinations are always transmitted with a time-to-live (TTL) value of 1

2. globally scoped addresses:
   The globally scoped addresses are 224.0.1.0 to 238.255.255.255. They may be used to multicast data across the Internet. For example, 224.0.1.1 has been reserved for Network Time Protocol (NTP) to synchronize the time-of-day clocks of network devices.

3) Experimental addresses:

One major block of addresses reserved for special purposes is the IPv4 experimental address range 240.0.0.0 to 255.255.255.254, these addresses could be used for research or experimentation.

Public and Private addresses:

-Private Addresses

The private address blocks are:

10.0.0.0 to 10.255.255.255 (10.0.0.0 /8)

172.16.0.0 to 172.31.255.255 (172.16.0.0 /12)

192.168.0.0 to 192.168.255.255 (192.168.0.0 /16)

Hosts that do not require access to the Internet at large may make unrestricted use of private addresses.

With services to translate private addresses to public addresses, hosts on a privately addressed network can have access to resources across the Internet. These services, called Network Address Translation (NAT), can be implemented on a device at the edge of the private network. NAT allows the hosts in the network to "borrow" a public address for communicating to outside networks.

-Public Addresses

The vast majority of the addresses in the IPv4 unicast host range are public addresses. These addresses are designed to be used in the hosts that are publicly accessible from the Internet. Even within these address blocks, there are many addresses that are designated for other special purposes.

Special IPv4addresses:

There are certain addresses that cannot be assigned to hosts for various reasons. There are also special addresses that can be assigned to hosts but with restrictions on how those hosts can interact within the network.

1) Network and Broadcast Addresses
   Within each network the first and last addresses cannot be assigned to hosts.
2) Default Route
   0.0.0.0. The default route is used as a "catch all" route when a more specific route is not available. The use of this address also reserves all addresses in the 0.0.0.0 - 0.255.255.255 (0.0.0.0 /8) address block.
3) Loopback
   One such reserved address is the IPv4 loopback address 127.0.0.1. The loopback is a special address that hosts use to direct traffic to themselves. Although only the single 127.0.0.1 address is used, addresses 127.0.0.0 to 127.255.255.255 are reserved. Any address within this block will loop back within the local host. No address within this block should ever appear on any network.
4) Link-Local Addresses
   IPv4 addresses in the address block 169.254.0.0 to 169.254.255.255 (169.254.0.0 /16) are designated as link-local addresses. These addresses can be automatically assigned to the local host by the operating system in environments where no IP configuration is available
5) TEST-NET Addresses
   The address block 192.0.2.0 to 192.0.2.255 (192.0.2.0 /24) is set aside for teaching and learning purposes. These addresses can be used in documentation and network examples. Unlike the experimental addresses, network devices will accept these addresses in their configurations.

Classful addressing:

he unicast address classes A, B, and C defined specifically-sized networks as well as specific address blocks for these networks, as shown in the figure. A company or organization was assigned an entire class A, class B, or class C address block. This use of address space is referred to as classful addressing.

→Class A Blocks 0.0.0.0 /8 to 127.0.0.0 /8

- For large networks by 16 million host address.

- N.H.H.H with /8 prefix.

- Subnet mask 255.0.0.0

- 0NNNNNNN.H.H.H

- #network=2^N=2^7=128   #hosts=2^N-2

→Class B Blocks 128.0.0.0 /16 to 191.255.0.0 /16

- For moderate to large size networks with more than 65000 host.

- N.N.H.H with /16 prefix.

- Subnet mask 255.255.0.0

- 10NNNNNN.N.H.H

- #network=2^N=2^{14} #hosts=2^{16}

→Class C Blocks 192.0.0.0 /24 to 223.255.255.0 /24

- For small networks with a maximum of 254 hosts

- N.N.N.H with /24 prefix.

- Subnet mask 255.255.255.0

- 110NNNNN.N.N.H

- #network=2^N=2^{21} #hosts=2^8

→Class D NA(Multicast)

1110NNNN.N.N.H 224-239

→Class E NA(Experimental)

11110NNN.N.N.H 240-255

Classless Addressing

The system that we currently use is referred to as classless addressing. With the classless system, address blocks appropriate to the number of hosts are assigned to companies or organizations without regard to the unicast class.

Subnet mask:

The prefix is a way to define the network portion that is human readable. the devices use a separate 32-bit pattern called a subnet mask.

The subnet mask is created by placing a binary 1 in each bit position that represents the network portion and placing a binary 0 in each bit position that represents the host portion.

Ex :

address 172.16.20.35

10101100.00010000.00010100.00100011

subnet mask 255.255.255.224

11111111.11111111.11111111.11100000

network address 172.16.20.32

10101100.00010000.00010100.00100000

Anding:

When an IPv4 packet is created or forwarded, the destination network address must be extracted from the destination address. This is done by a logic called AND. The IPv4 host address is logically ANDed with its subnet mask to determine the network address to which the host is associated. When this ANDing between the address and the subnet mask is performed, the result yields the network address.

Ex :	192.0.0.1	11000000.00000000.00000000.00000001 AND	
	255.255.0.0	11111111.11111111.00000000.00000000	
	Network	11000000.00000000.00000000.00000000	192.0.0.0

Sub netting:

Subnetting allows for creating multiple logical networks from a single address block. Since we use a router to connect these networks together, each interface on a router must have a unique network ID. Every node on that link is on the same network.

We create the subnets by using one or more of the host bits as network bits. This is done by extending the mask to borrow some of the bits from the host portion of the address to create additional network bits. The more host bits used, the more subnets that can be defined. For each bit borrowed, we double the number of sub networks available. For example, if we borrow 1 bit, we can define 2 subnets. If we borrow 2 bits, we can have 4 subnets. However, with each bit we borrow, fewer host addresses are available per subnet.

Formula for calculating subnets

- Use this formula to calculate the number of subnets:

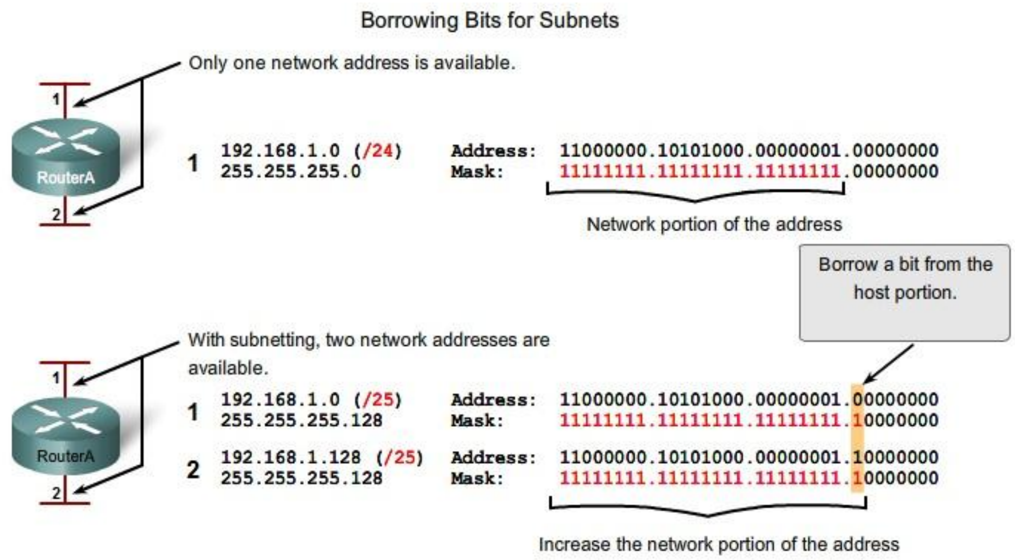
  2^n where n = the number of bits borrowed

- The number of hosts

  To calculate the number of hosts per network, we use the formula of 2^n - 2 where n = the number of bits left for hosts.

Ex ample: 192.168.1.0/24 need 2 network, 255.255.255.0

Hop count=256-128=128



Borrowing Bits for Subnets

Only one network address is available.

```
1  192.168.1.0 (/24)    Address: 11000000.10101000.00000001.00000000
   255.255.255.0        Mask:    11111111.11111111.11111111.00000000
```

Network portion of the address

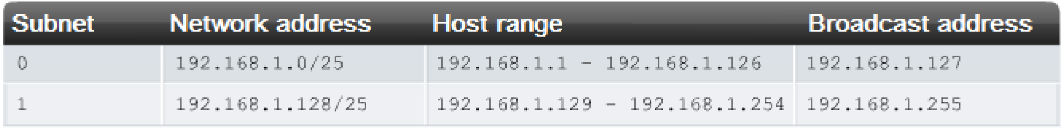
Borrow a bit from the host portion.

With subnetting, two network addresses are available.

```
1  192.168.1.0 (/25)    Address: 11000000.10101000.00000001.00000000
   255.255.255.128      Mask:    11111111.11111111.11111111.10000000
2  192.168.1.128 (/25)  Address: 11000000.10101000.00000001.10000000
   255.255.255.128      Mask:    11111111.11111111.11111111.10000000
```

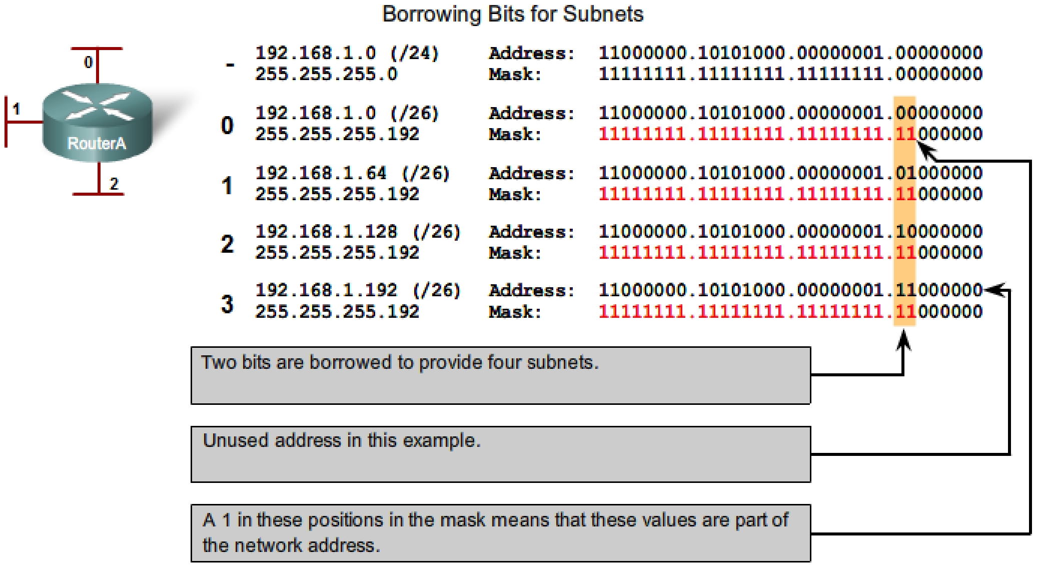
Increase the network portion of the address

Addressing Scheme: Example of 2 networks



Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255

Ex ample: 192.168.1.0/24 need 3 network, 255.255.255.0



Borrowing Bits for Subnets

```
-  192.168.1.0 (/24)    Address: 11000000.10101000.00000001.00000000
   255.255.255.0        Mask:    11111111.11111111.11111111.00000000
0  192.168.1.0 (/26)    Address: 11000000.10101000.00000001.00000000
   255.255.255.192      Mask:    11111111.11111111.11111111.11000000
1  192.168.1.64 (/26)   Address: 11000000.10101000.00000001.01000000
   255.255.255.192      Mask:    11111111.11111111.11111111.11000000
2  192.168.1.128 (/26)  Address: 11000000.10101000.00000001.10000000
   255.255.255.192      Mask:    11111111.11111111.11111111.11000000
3  192.168.1.192 (/26)  Address: 11000000.10101000.00000001.11000000
   255.255.255.192      Mask:    11111111.11111111.11111111.11000000
```

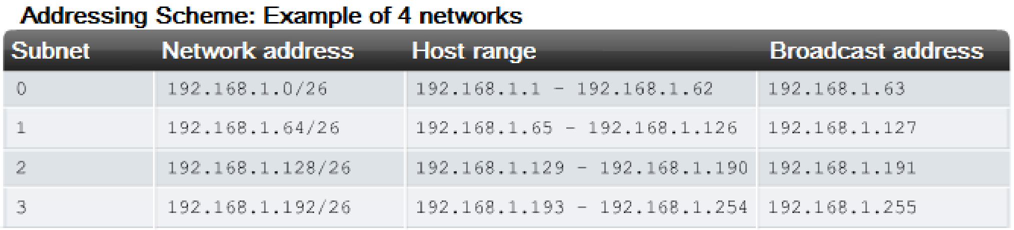
Two bits are borrowed to provide four subnets.

Unused address in this example.

A 1 in these positions in the mask means that these values are part of the network address.

More subnets are available, but fewer addresses are available per subnet.

Hop count=256-192=64

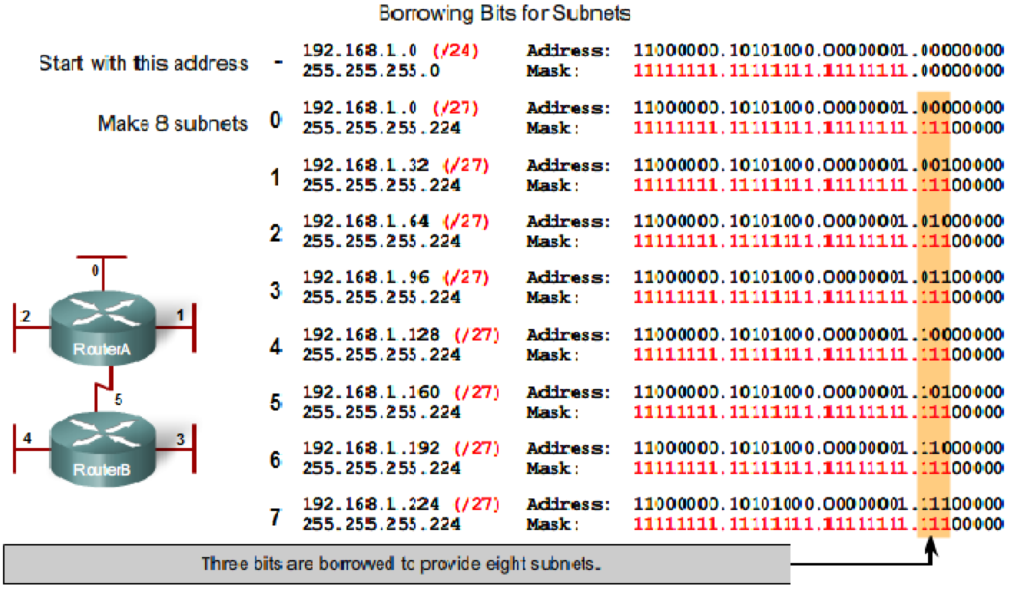


Addressing Scheme: Example of 4 networks

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

Ex ample: 192.168.1.0/24 need 6 network, 255.255.255.0

Hop count=256-224=32



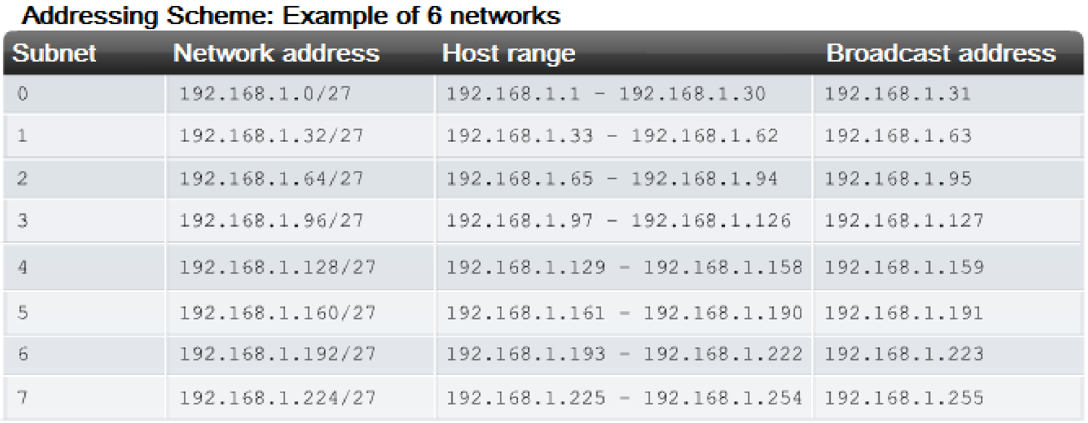
Borrowing Bits for Subnets

```
Start with this address  -  192.168.1.0 (/24)     Address: 11000000.10101000.00000001.00000000
                            255.255.255.0         Mask:    11111111.11111111.11111111.00000000

Make 8 subnets  0  192.168.1.0 (/27)     Address: 11000000.10101000.00000001.00000000
                   255.255.255.224       Mask:    11111111.11111111.11111111.11100000
                1  192.168.1.32 (/27)    Address: 11000000.10101000.00000001.00100000
                   255.255.255.224       Mask:    11111111.11111111.11111111.11100000
                2  192.168.1.64 (/27)    Address: 11000000.10101000.00000001.01000000
                   255.255.255.224       Mask:    11111111.11111111.11111111.11100000
                3  192.168.1.96 (/27)    Address: 11000000.10101000.00000001.01100000
                   255.255.255.224       Mask:    11111111.11111111.11111111.11100000
                4  192.168.1.128 (/27)   Address: 11000000.10101000.00000001.10000000
                   255.255.255.224       Mask:    11111111.11111111.11111111.11100000
                5  192.168.1.160 (/27)   Address: 11000000.10101000.00000001.10100000
                   255.255.255.224       Mask:    11111111.11111111.11111111.11100000
                6  192.168.1.192 (/27)   Address: 11000000.10101000.00000001.11000000
                   255.255.255.224       Mask:    11111111.11111111.11111111.11100000
                7  192.168.1.224 (/27)   Address: 11000000.10101000.00000001.11100000
                   255.255.255.224       Mask:    11111111.11111111.11111111.11100000
```

Three bits are borrowed to provide eight subnets.

0
1
2
RouterA
5
4
3
RouterB



Addressing Scheme: Example of 6 networks

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/27	192.168.1.1 - 192.168.1.30	192.168.1.31
1	192.168.1.32/27	192.168.1.33 - 192.168.1.62	192.168.1.63
2	192.168.1.64/27	192.168.1.65 - 192.168.1.94	192.168.1.95
3	192.168.1.96/27	192.168.1.97 - 192.168.1.126	192.168.1.127
4	192.168.1.128/27	192.168.1.129 - 192.168.1.158	192.168.1.159
5	192.168.1.160/27	192.168.1.161 - 192.168.1.190	192.168.1.191
6	192.168.1.192/27	192.168.1.193 - 192.168.1.222	192.168.1.223
7	192.168.1.224/27	192.168.1.225 - 192.168.1.254	192.168.1.255

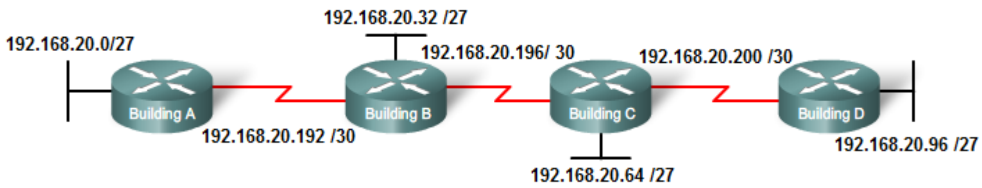
Sub netting a subnet

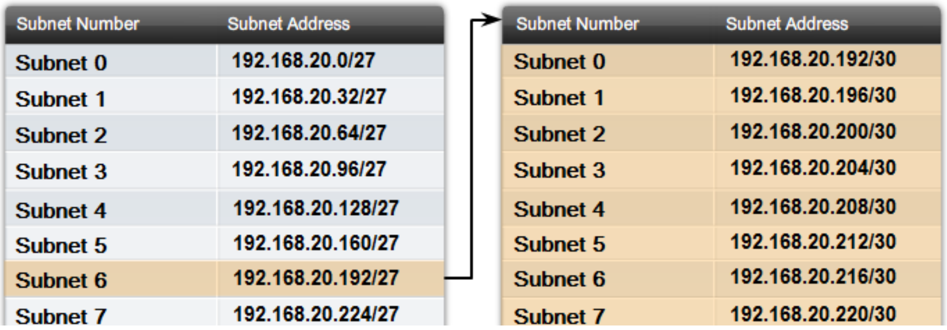
Sub netting a subnet, or using Variable Length Subnet Mask (VLSM) was designed to maximize addressing efficiency. When identifying the total number of hosts using traditional subnetting, we allocate the same number of addresses for each subnet. If all the subnets have the same requirements for the number hosts, these fixed size address blocks would be efficient. However, most often that is not the case.

Example:

We need 7 nets from 192.168.20.0/24   255.255.255.0

Hop count = 256-224=32 we borrow 3bit





Subnet Number	Subnet Address
Subnet 0	192.168.20.0/27
Subnet 1	192.168.20.32/27
Subnet 2	192.168.20.64/27
Subnet 3	192.168.20.96/27
Subnet 4	192.168.20.128/27
Subnet 5	192.168.20.160/27
Subnet 6	192.168.20.192/27
Subnet 7	192.168.20.224/27

Subnet Number	Subnet Address
Subnet 0	192.168.20.192/30
Subnet 1	192.168.20.196/30
Subnet 2	192.168.20.200/30
Subnet 3	192.168.20.204/30
Subnet 4	192.168.20.208/30
Subnet 5	192.168.20.212/30
Subnet 6	192.168.20.216/30
Subnet 7	192.168.20.220/30

s

We make sub netting by borrow 3 bits so there 5 bits for hosts so,we have 30 hosts,

If we have net with only 2 hosts ,so the other 28 hosts are wasted so, this is inefficient for classfull addresses, so

The solution of this is to make sub netting to the subnets 192.168.20.192/27 by hop count= 256-252=4

Solve:

192.168.1.0/24

1) 2 subnets has 50 host

2) 3 subnets has 24 host

3) 2 subnets has 2 host

Solve:

192.168.1.0/24

1) subnet has 72 host

2) subnet has 30 host

3) subnet has 24 host

4) 2 subnets has 2 host

Solve:

192.168.1.0/24

- Without VLSM

- With VLSM

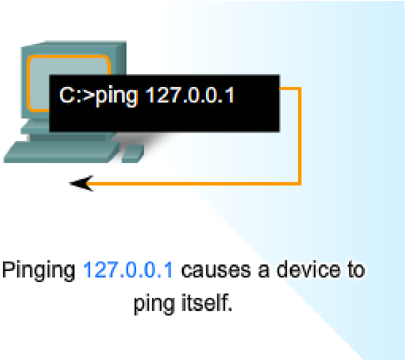
1) subnet has 30 host

2) subnet has 15 host

3) 2 subnets has 2 host

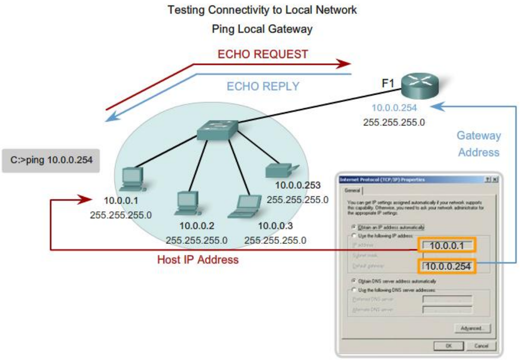
Testing the network layer:

1) Ping to the host itself

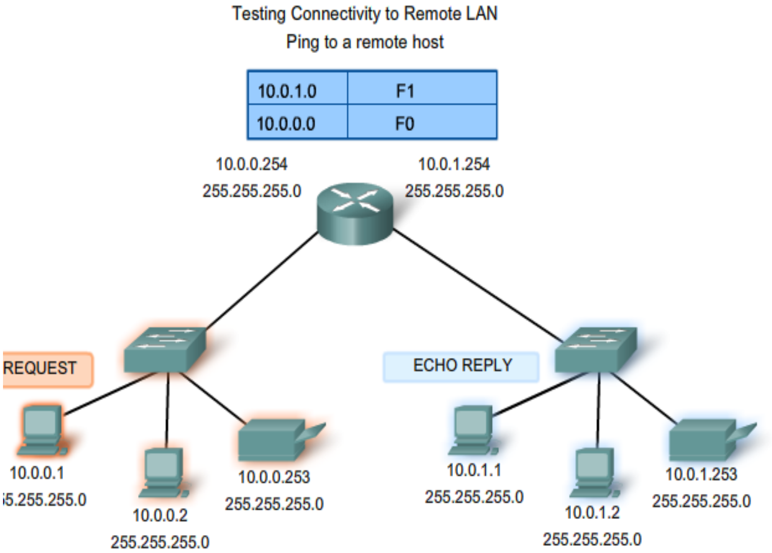


Pinging 127.0.0.1 causes a device to ping itself.

2) Ping to test local network test getway



3) Ping to remote host test remote local network



10.0.1.0	F1
10.0.0.0	F0

4) Testing the path of the packet by tracerout(tracert)
Traceroute (tracert) is a utility that allows us to observe the path between these hosts. The trace generates a list of hops that were successfully reached along the path.
→ Round Trip Time (RTT)

The round trip time (RTT) is the time a packet takes to reach the remote host and for the response from the host to return. An asterisk (*) is used to indicate a lost packet.
→ Time to Live (TTL)
Traceroute makes use of a function of the Time to Live (TTL) field in the Layer 3 header and ICMP Time Exceeded Message. The TTL field is used to limit the number of hops that a packet can cross. When a packet enters a router, the TTL field is decremented by 1. When the TTL reaches zero, a router will not forward the packet and the packet is dropped.

ICMP v4 protocol:

Although IPv4 is not a reliable protocol, it does provide for messages to be sent in the event of certain errors. The purpose of these messages is to provide feedback about issues related to the processing of IP packets under certain conditions, not to make IP reliable. ICMP messages are not required and are often not allowed for security reasons.

ICMP messages that may be sent include:

→ Host Confirmation

An ICMP Echo Message can be used to determine if a host is operational.

→ Unreachable Destination or Service

The ICMP Destination Unreachable can used to notify a host that the destination or service is unreachable.

The Destination Unreachable packet will contain codes that indicate why the packet could not be delivered.

Among the Destination Unreachable codes are:

0 = net unreachable

1 = host unreachable

2 = protocol unreachable

3 = port unreachable

→ Time Exceeded

An ICMP Time Exceeded message is used by a router to indicate that a packet cannot be forwarded because the TTL field of the packet has expired.

→ Route Redirection

A router may use the ICMP Redirect Message to notify the hosts on a network that a better route is available for a particular destination.

→ Source Quench

The ICMP Source Quench message can be used to tell the source to temporarily stop sending packets. If a router does not have enough buffer space to receive incoming packets, a router will discard the packets. If the router has to do so, it may also send an ICMP Source Quench message to source hosts for every message that it discards.

A destination host may also send a source quench message if datagrams arrive too fast to be processed.