

Al-Mustaql University

College of Science

Intelligent Medical Systems Departement

Computer Networks - 3rd Class



جامعة المستقبل
AL MUSTAQL UNIVERSITY

Lecture 5: Designing IP addressing in the Networking II

Prof. Dr. Mehdi Ebady Manaa

Subnetting the Subnet

When contiguous 1s are added to the default mask, making the all-1s field in the mask longer, the definition of the network part of an IP address is extended to include **subnets**.

Adding bits to the network part of an address decreases the number of bits in the host part.

***The number of subnetworks created is calculated by the formula 2^s , where s is the number of bits by which the default mask was extended.

Subnetting the Subnet

**Suppose the IP address $172.16.0.0/16$, and there are 10 subnets required.

Select the appropriate subnet mask value that can accommodate 10 networks.

Assigned Address: $172.16.0.0/16$

In Binary $10101100.00010000.00000000.00000000$

Subnetting the Subnet

**Suppose the IP address 192.168.0.1 /24 , and there are 3 subnets required.

Select the appropriate subnet mask value that can accommodate 3 networks.

Assigned Address: 192.168.0.1/24

Determining the Size of the Network

The first step in designing an IP addressing plan is determining the size of the network to establish how many IP subnets and how many IP addresses are needed on each subnet. To gather this information, we need to answer the following questions:

- **How many locations does the network consist of ?:** The designer must determine the number and type of locations.
- **How many devices in each location need addresses?:** The network designer must determine the number of devices that need to be addressed, including end systems, router interfaces, switches, and any other devices.
- **What are the IP addressing requirements for individual locations?:** The designer must collect information about which systems will use dynamic addressing, which will use static addresses, and which systems can use private instead of public addresses.

Determining the Size of the Network

- **What subnet size is appropriate?:**Based on the collected information about the number of networks and planned switch deployment, the designer estimates the appropriate subnet size.

For example, deploying 48-port switches would mean that subnets with 64 host addresses would be appropriate, assuming one device per port.

Determining the Network Topology

The designer should acquire a general picture of the network topology; this will help determine the correct information to gather about network size and its relation to the IP addressing plan.

With this general network topology information, the designer determines the number of locations, location types, and their correlations.

Size of Individual Locations

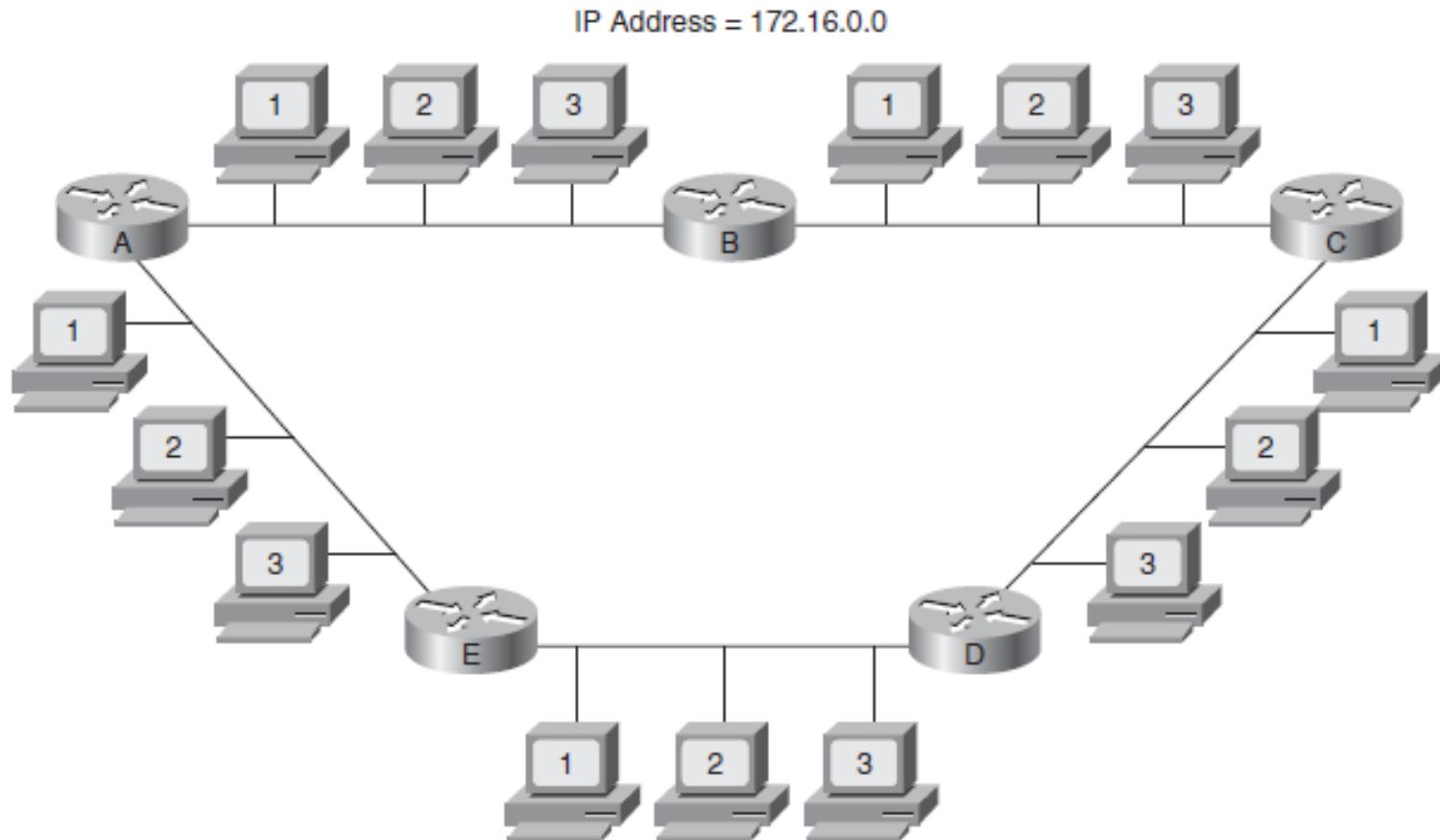
The network size, in terms of the IP addressing plan, relates to the number of devices and interfaces that need an IP address. To establish the overall network size in a simplistic way, the designer determines the approximate number of workstations, servers, router interfaces, and other network devices at each location.

This estimate provides the minimum overall number of IP addresses that are needed for the network.

Some additional addresses should be reserved to allow for seamless potential network growth. The designer should carefully discuss future network growth with the organization's representative to obtain a more precise estimate of the required resources.

Example

If we have the IP address 172.16.0.0, and you want to configure the network shown in the following figure.



Example

-- To establish the subnet mask, do the following:

Step 1/ Determine the number of networks (subnets) needed, the example has five networks.

Step 2/ Determine how many nodes per subnet must be defined. This example has five nodes (two routers and three workstations) on each subnet.

Step 3/ Determine future network and node requirements. For example, assume 100 percent growth.

Step 4/ Given the information gathered in Steps 1 to 3, determine the total number of subnets required. For this example, ten subnets are required.

Example

No mask accommodates exactly 10 subnets. Depending on your network growth trends, you might select **4 subnet bits**, resulting in a subnet mask of 255.255.240.0. The binary representation of this subnet mask is as follows:

11111111.11111111.**1111**0000.00000000

The additional 4 subnet bits would give you $2^4 = 16$ subnets.

Example

Assigned Address: 172.16.0.0/16

In Binary 10101100.00010000.00000000.00000000

Subnetted Address: 172.16.0.0/20

In Binary 10101100.00010000.XXXX0000.00000000

1st Subnet: 10101100 . 00010000 .0000 0000 . 00000000 = 172.16.0.0

2nd Subnet: 172 . 16 .0001 0000 . 00000000 = 172.16.16.0

3rd Subnet: 172 . 16 .0010 0000 . 00000000 = 172.16.32.0

4th Subnet: 172 . 16 .0011 0000 . 00000000 = 172.16.48.0

.

.

10th Subnet: 172 . 16 .1001 0000 . 00000000 = 172.16.144.0

Network Subnet Host

Interconnecting Private and Public Addresses

- * According to an organization needs, it can use both public and private addresses.
- * A router or firewall acts as the interface between the network's private and public sections.
- * When private addresses are used for addressing in a network and this network must be connected to the Internet, **Network Address Translation (NAT)** or **Port Address Translation (PAT)** must be used to translate from private to public addresses and vice versa.
- * NAT or PAT is required if accessibility to the public Internet or public visibility is required.

Interconnecting Private and Public Addresses

- * Static NAT is a one-to-one mapping of an unregistered IP address to a registered IP address.
- * Dynamic NAT maps an unregistered IP address to a registered IP address from a group of registered IP addresses.
- * NAT overloading, or PAT, is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address by using different port numbers.

Interconnecting Private and Public Addresses

- NAT or PAT can be used to translate the following:
 - **One private address to one public address:** Used in cases when servers on the internal network with private IP addresses must be visible from the public network. The translation from the server's private IP address to the public IP address is defined statically.
 - **Many private addresses to one public address:** Used for end systems that require access to the public network but do not have to be visible to the outside world.
 - **Combination:** It is common to see a combination of the previous two techniques deployed throughout networks.

Methods of Assigning IP Addresses

There are two basic IP address assignment strategies:

- Static assignment.
- Dynamic assignment.

Methods of Assigning IP Addresses

****Static Assignment****

An IP address is statically assigned to a system. The network administrator configures the IP address, default gateway manually.

Static address assignment is an extra burden for the administrator—especially on large-scale networks— who must configure the address on every end system in the network.

Methods of Assigning IP Addresses

****Dynamic Assignment****

- IP addresses are dynamically assigned to the end systems. Dynamic address assignment relieves the administrator of manually assigning an address to every network device. Instead, the administrator must set up a server to assign the addresses.
- On that server, the administrator defines the address pools and additional parameters that should be sent to the host such as the default gateway.
- On the host, the administrator enables the host to acquire the address dynamically; this is often the default.
- When IP address reconfiguration is needed, the administrator reconfigures the server, which then performs the host-renumbering task.
- Examples of available address assignment protocols include Reverse Address Resolution Protocol, and DHCP.

When to Use Static or Dynamic Address Assignment

To select either a static or dynamic end system IP address assignment method or a combination of the two, consider the following:

- **Node type:** Network devices such as routers and switches typically have static addresses. End-user devices such as PCs typically have dynamic addresses.
- **The number of end systems:** If there are more than 30 end systems, dynamic address assignment is preferred. Static assignment can be used for smaller networks.
- **Renumbering:** If renumbering is likely to happen and there are many end systems, dynamic address assignment is the best choice. With DHCP, only DHCP server reconfiguration is needed; with static assignment, all hosts must be reconfigured.

When to Use Static or Dynamic Address Assignment

- **Address tracking:** If the network policy requires address tracking, the static address assignment method might be easier to implement than the dynamic address assignment method. However, address tracking is also possible with dynamic address assignment with additional DHCP server configuration.
- **Additional parameters:** DHCP is the easiest solution when additional parameters must be configured. The parameters have to be entered only on the DHCP server, which then sends the address and those parameters to the clients.
- **High availability:** Statically assigned IP addresses are always available. Dynamically assigned IP addresses must be acquired from the server; if the server fails, the addresses cannot be acquired. To ensure reliability, a redundant DHCP server is required.
- **Security:** With dynamic IP address assignment, anyone who connects to the network can acquire a valid IP address, in most cases. This might be a security risk. Static IP address assignment poses only a minor security risk.

The use of one address assignment method does not exclude the use of another in a different part of the network.

Thank you