CSET 150

NETWORK DESIGN AND MANAGEMENT

EVENING MASTERS EDITION

DR. MAHBOOB QAOSAR

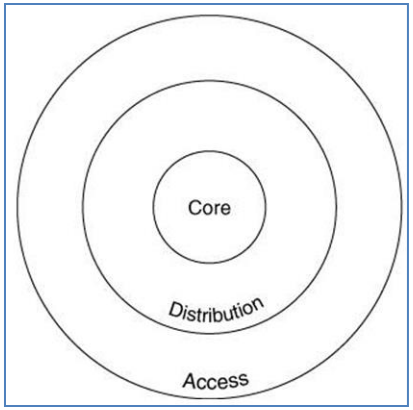
ASSOCIATE PROFESSOR, CSE, RU

SWITCHING DESIGN CONSIDERATIONS

- We Know:
  - the hierarchical network design model and
  - the Enterprise Composite Network Design model
- **Hierarchical ..:** the access layer, the distribution layer, and the core layer
- **Enterprise Composite Network** ..: Enterprise Campus, Enterprise Edge, and Service Provider Edge.
  - Each of these functional areas contains network modules, which in turn can include the hierarchical layers.

FOR THE ACCESS LAYER

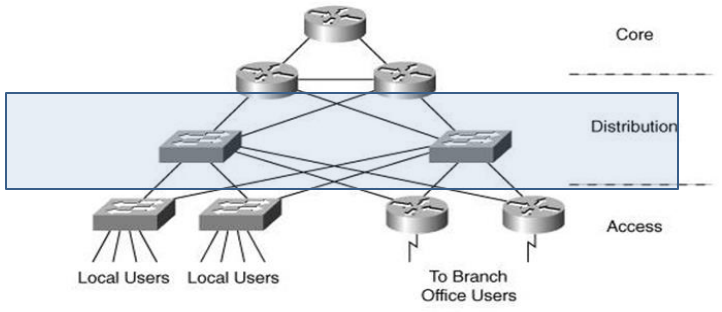
- For the access layer, design considerations include the following:
  - The **number of end-user devices** to be supported
  - The **applications** that are being used this defines some of the features required in the switches, as well as the performance and bandwidth needed
  - The **use of VLANs**, including whether trunks are required between switches
  - **Redundancy** requirements



FOR THE DISTRIBUTION LAYER

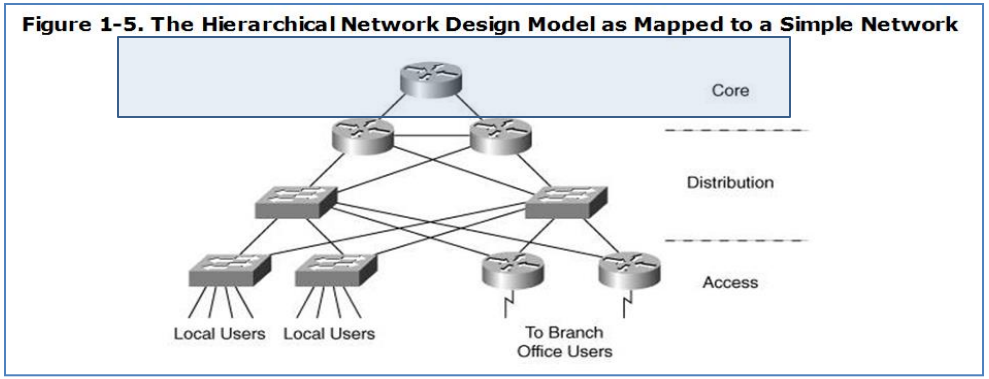
- For the distribution layer, design factors include the following:
  - The **number of access switches** to be aggregated
  - **Redundancy** requirements
  - **Features** required for **specific applications** to be supported
  - Required **interfaces** to the **core** layer
  - For **Layer 3 switches**, the **routing protocols** to be supported and whether sharing of information among **multiple routing protocols** is required

Figure 1-5. The Hierarchical Network Design Model as Mapped to a Simple Network



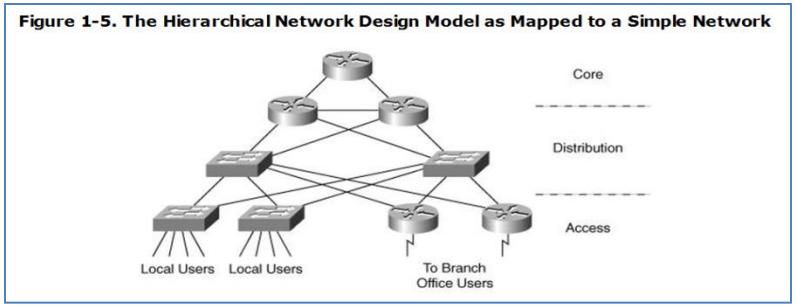
FOR THE CORE LAYER

- The role of the core layer is to provide a high-speed backbone.
- Thus, the **key requirement** is the **performance** needed to support all the access and distribution data.
- The number of ports to the distribution layer, and the protocols (for example, routing protocols) that need to be supported on those ports, are also important considerations.
- Redundancy in the core is a typical requirement, to meet the availability needs of the network



CISCO RECOMMENDATIONS

- Cisco current campus design recommendations include the followin:
  - **Layer 2** switches can be used at the **access layer**, with **Layer 3** switches at the **distribution and core layers.**
  - **VLANs** should **not** spread across the campus, because this can slow network convergence.
  - The **core and distribution** layers can be combined into one layer (called a **collapsed backbone**) for smaller networks.
  - **Larger** campuses should have a **separate** distribution layer to allow the network to grow easily.
  - **Redundancy** in the core, between the core and distribution layers, and between the distribution and access layers is also recommended.



Chapter 3: IPv4 Routing Design

Network Design: Design Principles, Determining Requirements, Analyzing the Existing Network, Preparing the Preliminary Design, Completing the Final Design Development, Deploying the Network, Monitoring and Redesigning, Maintaining, Design Documentation, Modular Network Design, Hierarchical Network Design, The Cisco Enterprise Composite Network Model.

Technologies - Switching Design: Switching Types, Spanning, Tree Protocol, Redundancy in Layer 2 Switched Networks, STP Terminology and Operation, Virtual LANs. Trunks. Inter VLAN Routing. Multilayer Switching. Switching Security and Design Considerations. IPv4 Address Design, Private and Public Addresses, NAT, Subnet Masks, Hierarchical IP Address Design, IPv4 Routing Protocols, Classification, Metrics, Routing Protocol Selection.

Network Security Design: Hacking, Vulnerabilities, Design Issues, Human Issues, Implementation Issues, Threats, Reconnaissance Attacks, Access Attacks, Information Disclosure Attacks, Denial of Service Attacks, Threat Defense, Secure Communication, Network Security Best Practices, SAFE Campus Design.

Wireless LAN Design: Wireless Standards, Wireless Components, Wireless Security, Wireless Security Issues, Wireless Threat Mitigation, Wireless Management, Wireless Design Considerations, Site Survey, WLAN Roaming, Wireless IP Phones, Quality of Service Design, QoS Models, Congestion Avoidance, Congestion Management.

Network Management: ISO Network Management Standard, Protocols and Tools, SNMP, MIB, RMON NetFlow, Syslog, Network Management Strategy, SLCs and SLAs, IP Service-Level Agreements, Content Networking Design, Case Study, Venti Systems.

IPv4 Routing Design

- **Determining How Many IP Addresses Are Required**
  - How many different locations in your network that need addresses:
    headquarters, branch and regional offices, telecommuters, and so forth.
  - The number of devices in each location must be counted, including:
    - the network devices such as routers, switches, and firewalls;
    - workstations;
    - IP phones;
    - network management stations;
    - servers; and so forth.

IPv4 Address Design

- For each of these devices,
  - determine **how many interfaces** need to be addressed and
  - whether **private** or **public** addresses will be used.

- Reserved address required ? how many
  - 10% to 20% suggested.

- **PROBLEM:** what if no reserved address available…

Private and Public Addresses

- Requests For Comments (RFC) 1918,
  - **"Address Allocation for Private Internets,"** defines the private IPv4 addresses as follows:

10.0.0.0	To	10.255.255.255
172.16.0.0	To	172.31.255.255
192.168.0.0	To	192.168.255.255

Private and Public Addresses

- Private addresses are for use only within a company's network;
- **Public addresses** must be used when communicating on the **public Internet.**
- Internal private addresses must be translated to public addresses when data is sent out to the Internet, and these public addresses must be translated back to the private addresses when packets come in from the Internet.

Private and Public Addresses

- Public addresses are required for the Internet connections and for servers that must be accessible from the Internet
  - for example, File Transfer Protocol (FTP) servers that contain publicly accessible data, and web servers.
- Other devices internal to the network can use private addresses they can connect to the Internet through a **NAT device**.
- NAT – network address translator

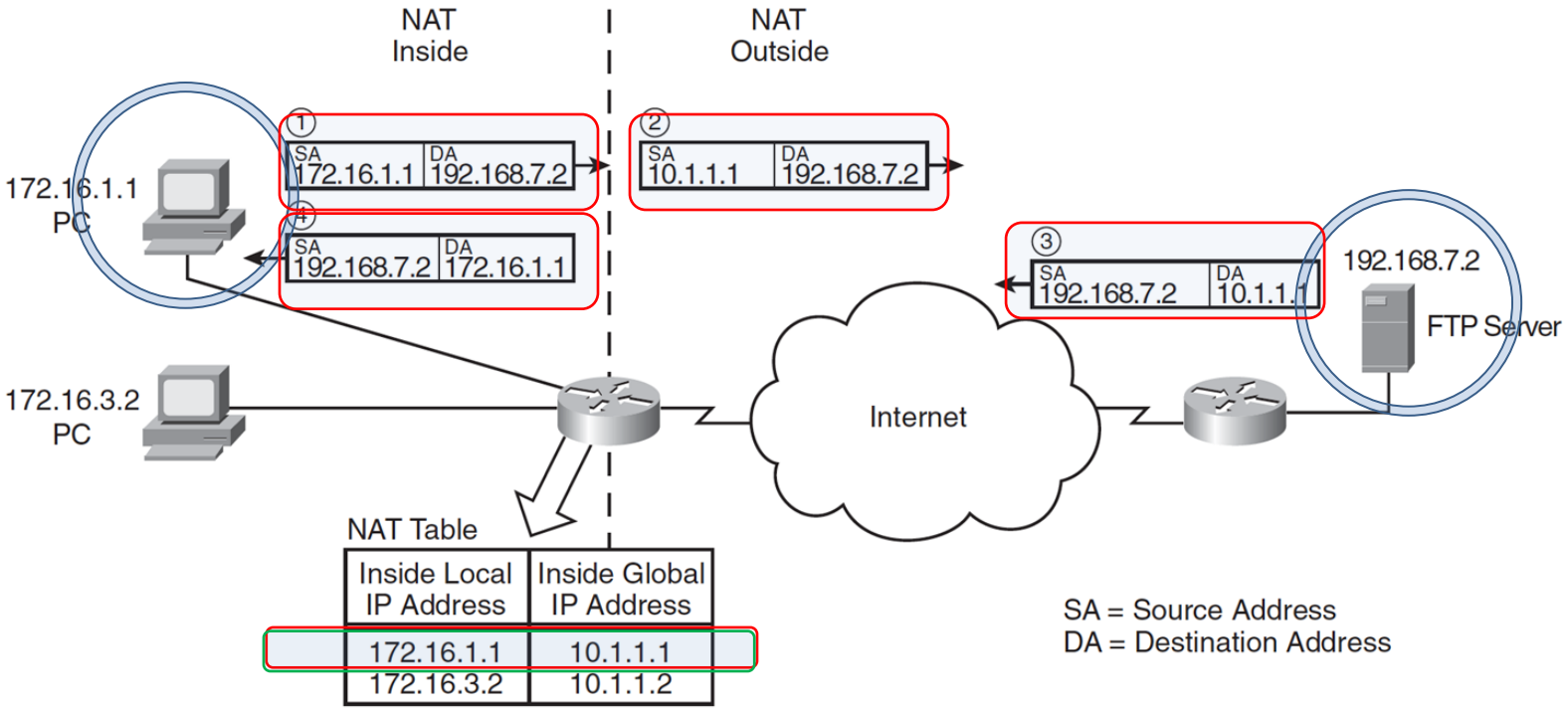
NAT (Network Address Translator)

- **To configure** NAT you first define **inside and outside** interfaces on the NAT device.
  - The inside **interface** connects to the **internal** network,
  - while the **outside** interface connects to the **Internet**.
  - You also define the addresses that are to be translated on each side.

NAT

A person at PC 172.16.1.1 wants to access data on the FTP server at 192.168.7.2.

Figure 3-1 *NAT Translates Between Inside and Outside Addresses*



A NAT device (in this case, a router) translates addresses on the inside network 172.16.0.0 to addresses on the outside network 10.1.0.0

N.B.: In practice, public addresses would be used on the Internet

NAT

- **A NAT device has a NAT table,**
  - created either dynamically or with static entries
  - configured by the network administrator

- Simple NAT table in the NAT router includes :
  - **Inside local IP address**
    - The address used by a host on the inside network
  - **Inside global IP address**
    - The address that represents an inside host on the outside network

How Routers Use Subnet Masks

- When you configure the IP address of a router's interface, you include the **address** and the **subnet mask.**
  - The router uses this information not only to address the interface but also to determine the address of the subnet to which the interface is connected.
- The router then puts this subnet address in its routing table, as a connected network on that interface.

How Routers Use Subnet Masks

To determine the network or subnet address to which a router is connected, the router performs a logical AND of the interface address and the subnet mask. Logically "ANDing" a binary 1 with any number yields that number; logically "ANDing" a binary 0 with any number yields 0.

Table 3-1 *Example Calculation of Subnet Address*

	Network	Subnet	Subnet	Host
Interface IP Address 10.5.23.19	00001010	00000101	00010111	00010011
Subnet Mask 255.255.255.0	11111111	11111111	11111111	00000000
Subnet Address 10.5.23.0	00001010	00000101	00010111	00000000

How Routers Use Subnet Masks

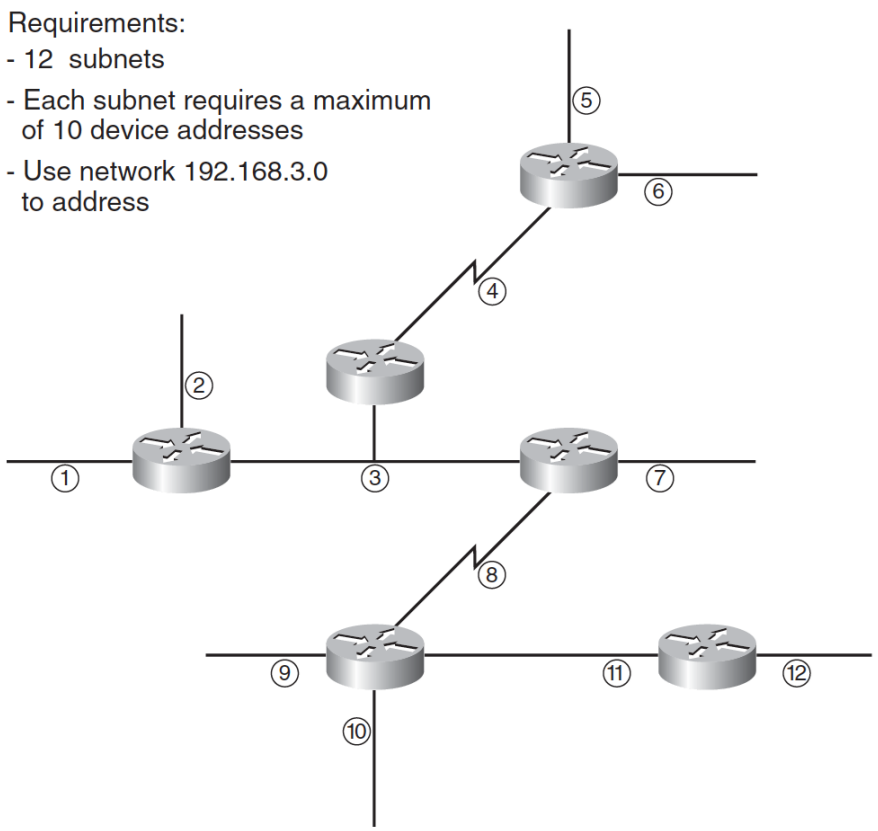
- **When a packet arrives at the router,**
  - the router analyzes the destination address of the packet to determine which network or subnet it is on.
  - The router looks up this network or subnet in its routing table to determine the interface through which it can best be reached;
  - the packet is then sent out of the appropriate router interface.
  - [If the router does not have a route to the destination subnet, the packet is rejected and an **Internet Control Message Protocol (ICMP)** error message is sent to the source of the packet.]

Subnet Mask to Use

- **Determining the Subnet Mask to Use**
  - … depends on the number of **subnets required** and
  - the number of **host addresses** required on each of these subnets

Determining the Subnet Mask to Use

Figure 3-2 *The Number of Subnets and Hosts Required Determines the Subnet Mask to Use*



- A total of 12 subnets exist in this network;
- Each has a maximum of 10 device addresses.
- Some of the addresses are for router interfaces and some are for hosts (not shown in the figure);
- each device on each subnet needs to have its own IP address.

- Select a series : say 192.168.3…

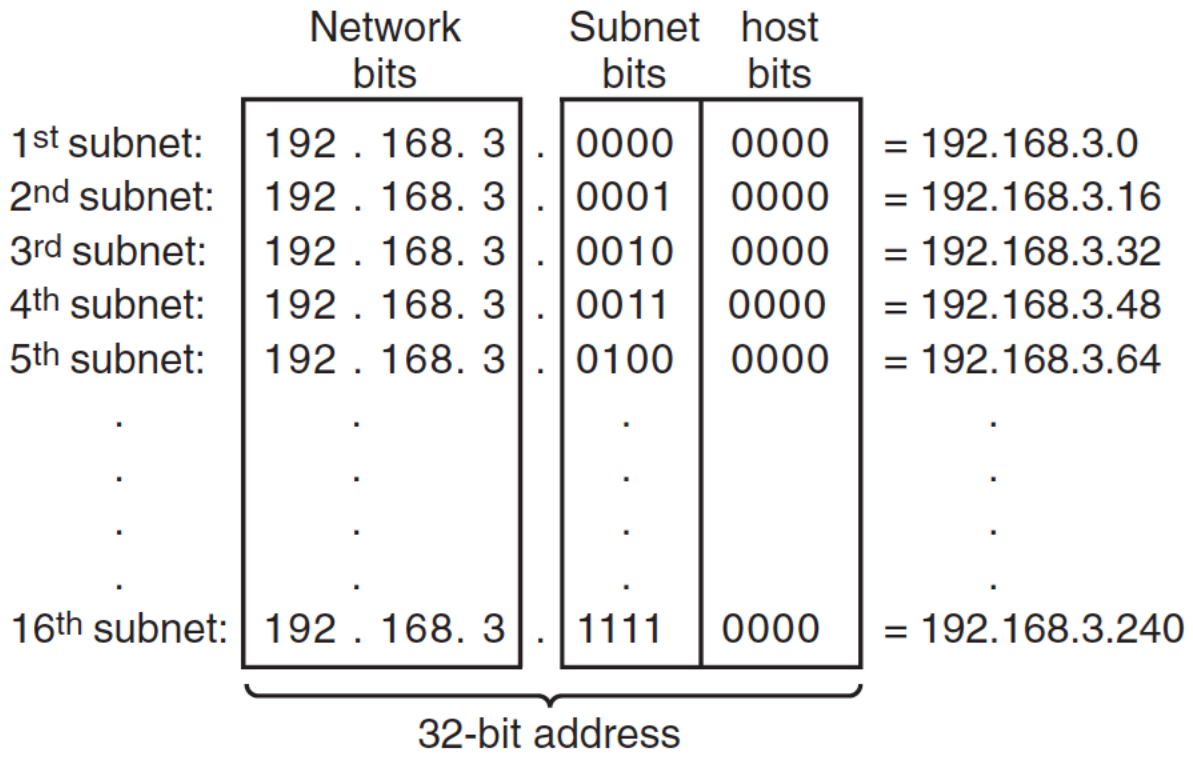
Determining the Subnet Mask to Use

- Number of subnet required 12 2^4 4 bits needed
- Number of host address required 10 2^4 4bit needed

- IPv4 32 bit – 8 bit . 8 bit . 8 bit . **8 bit**
- 8 bit . 8 bit . 8 bit . **4 bit (Subnet) + 4 bit (Host)**
- **255. 255 . 255. 1111000 255.255.255.240 –** network mask or subnet mask

Determining the Subnet Mask to Use

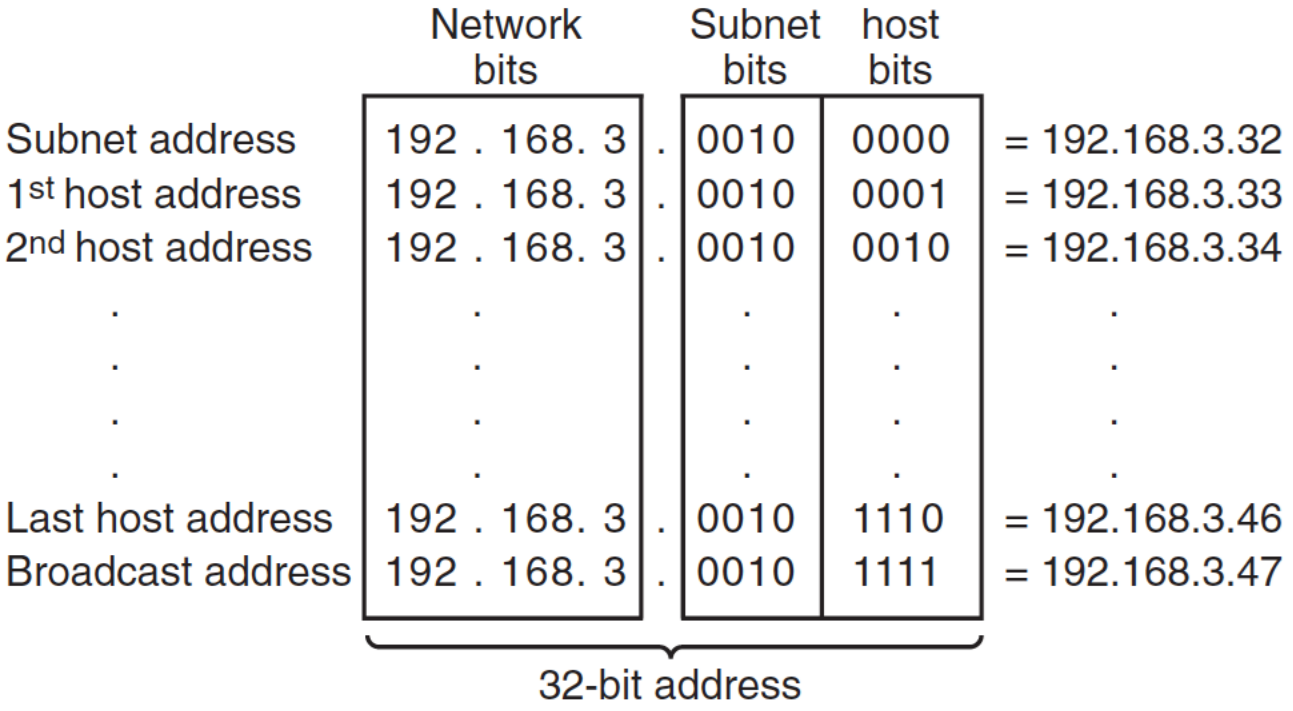
Figure 3-3 *Calculating Subnet Addresses*



Thus, the first subnet address that can be used with a mask of 255.255.255.240 is 192.168.3.0; this can also be written as 192.168.3.0/28. The second subnet is 192.168.3.16/28, and so on.

Determining the Subnet Mask to Use

Figure 3-4 *Calculating Device Addresses*



Remember that the address in which all host bits are 0 is the subnet address, and the address in which all host bits are 1 is the broadcast address