CpE654 / NIS654
Design and Analysis of Network Systems

Addressing and Routing Architecture

Readings!

McCabe's book: Chapter 6

Many texts referenced at the beginning of the course are also good references for Addressing and Routing Algorithms covered here.

Addressing

- Addresses are device identifiers to identify origin/destinations for routing data (packets, frames)
- Different addresses are assigned at different physical, data-link, and network layers.
- We'll focus here on network (IPv4) layer addressing.

Note that we only discuss IPv4 here. IPv4 address space (32 bits) is nearing exhaustion and you are encouraged to study about IPv6 (RFC 2460 and 429).

- IPv6 is128 bits long address, written as groups of four in hexs, separated by colons. Example: FAF6:AA98:7694:3310:ADEF:12AD:1011:FFAF
  - Note: hex FAF6 in binary is: 1111 1010 1111 0110
- Often leading zeros of a sections are omitted, 0063 can be written as 63 and 0000 can be written as 0. All zeros of a section can be replaced by double colons. Example:
- ABCD:0:0:0:0:FABC:0063:FFFF <=> ABCD::FABC:63:FFFF

Address Types

Address Type	Meaning
Local Addresses	Addresses that are recognized locally, at the LAN or subnet. Such addresses are usually at the data-link (e.g., Ethernet) layer.
Global Addresses	Addresses that are recognized worldwide. Such addresses are usually at the network (IP) layer.
Private Addresses	Network-layer addresses that are not routed through the public Internet. Private addresses are used in Network Address Translation (NAT).
Public Addresses	Network-layer addresses that are routed through the public Internet.
Temporary Addresses	Addresses that are assigned for a short duration of time, e.g., dynamically via the Dynamic Host Configuration Protocol (DHCP)
Persistent Addresses	Addresses that are assigned for a long duration of time or permanently configured within the device.

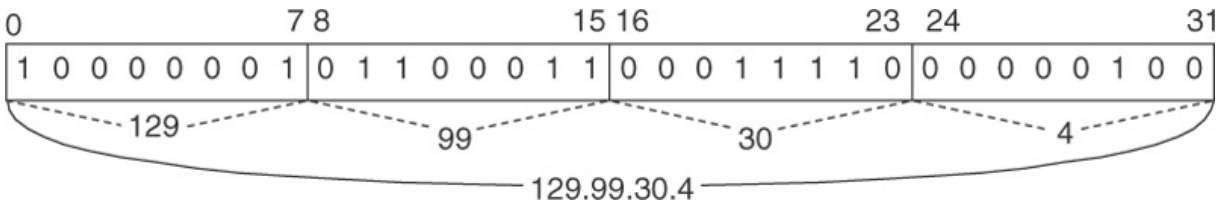
Examples:

- Ethernet address is a local address; format is six groups of two hexadecimal digits, separated by hyphens (-) or colons (:), in transmission order (e.g. 01-23-45-67-89-ab or 01:23:45:67:89:ab) (IEEE 802)
- IPv4 addresses (xxx.xxx.xxx.xxx) (or IPv6) could be global, public, temporary, and persistent.

IP Address Format

- We will focus on IPv4 addressing for this course.
- IP address consists of (1) address id and (2) an associated mask.
- They are given in dotted decimal or binary notation.
- Mask identifies which bits in the address applies to the network part and which apply to the device part. Thus, the address has2 parts – a network part and the other for the addresses within that network.
- Routers obtain the Network part of the address through the "AND" operation between the address and the mask,

Address id	Mask
129.99.30.4	255.255.240.0
10000001.01100011.00011110.00000100	11111111.11111111.11110000.00000000



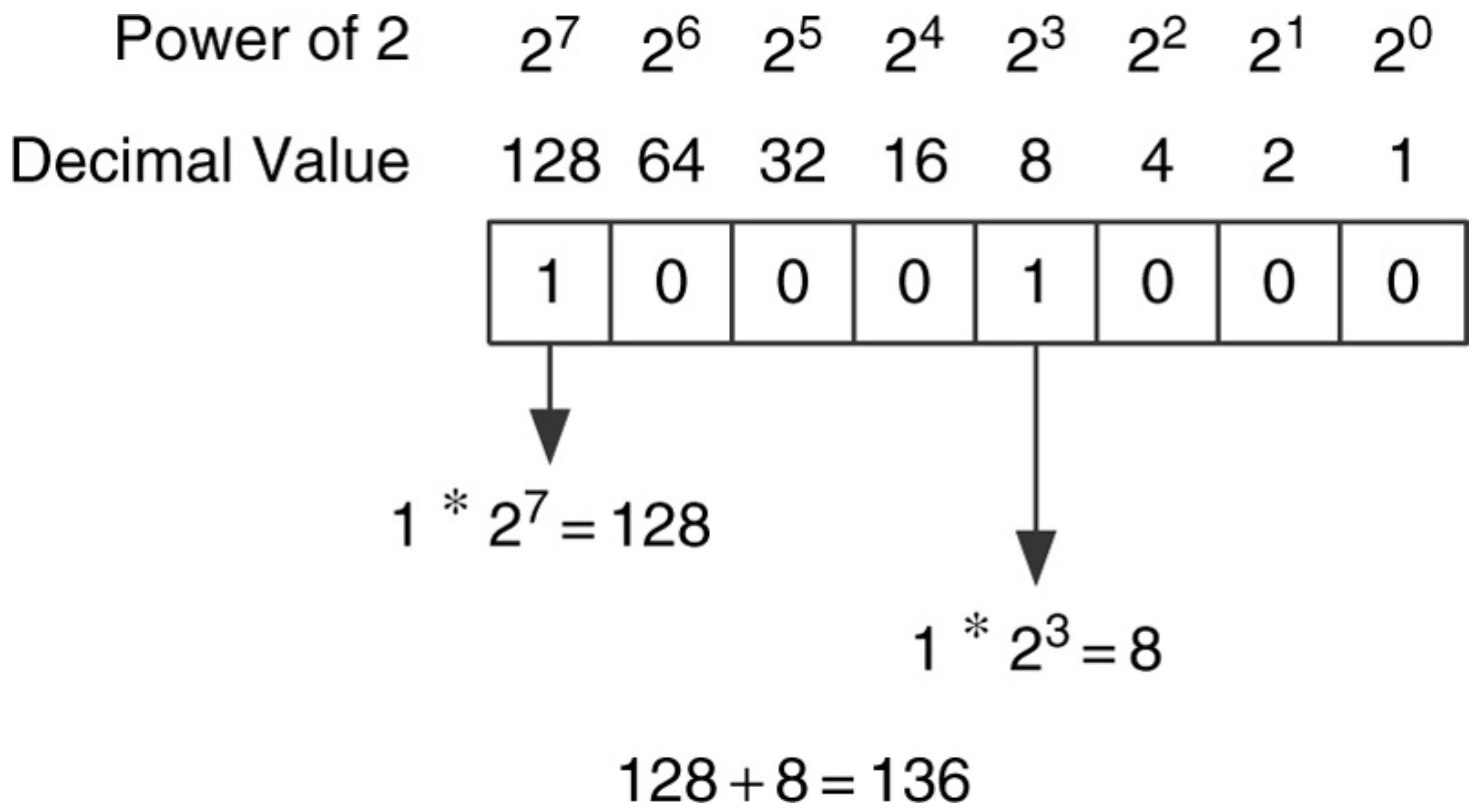
Address id

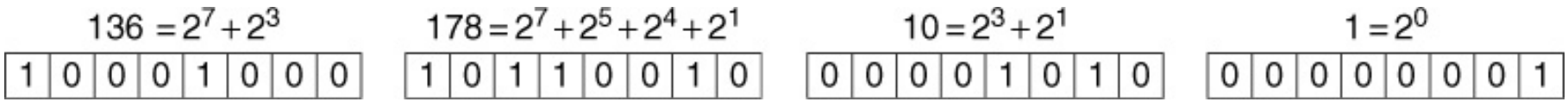
11111111.11111111.11110000.00000000

255 . 255 . 240 . 0

Mask

Binary vs. Decimal Numbering

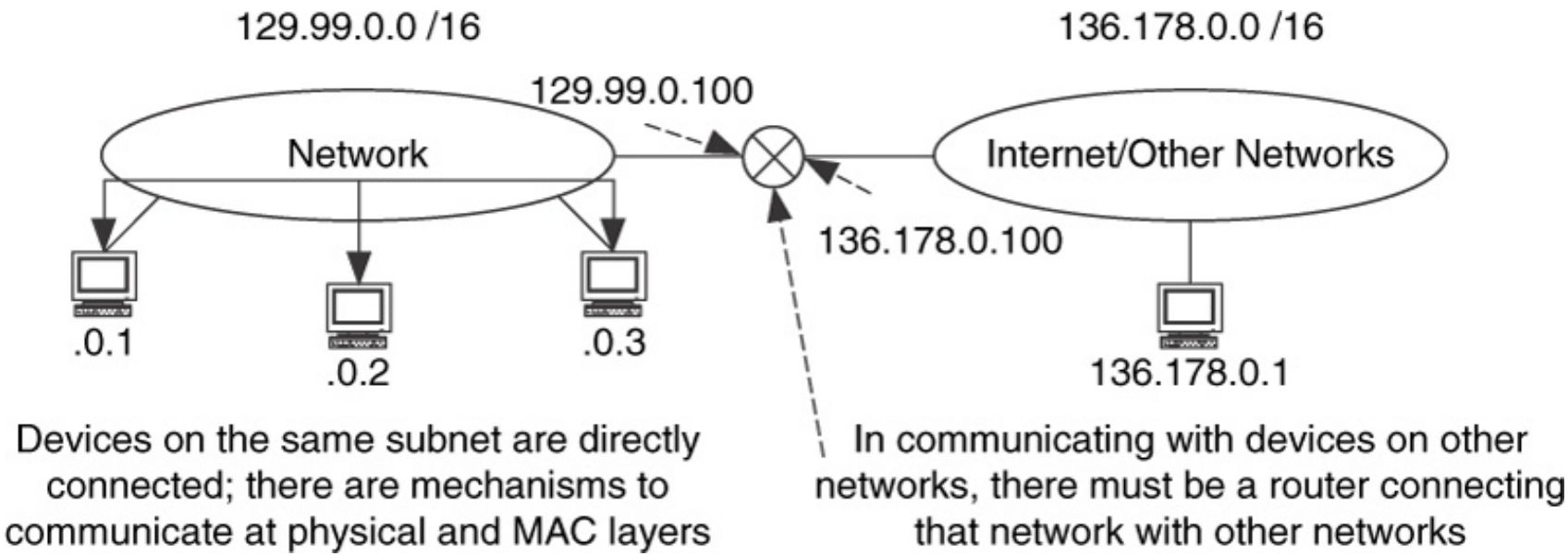




Addressing Mechanisms

- Classful addressing
- Subnetting
- Supernetting or classless inter-domain routing (CIDR)
- Variable-Length Subnetting
- Private Addressing
- Network Address Translation (NAT)

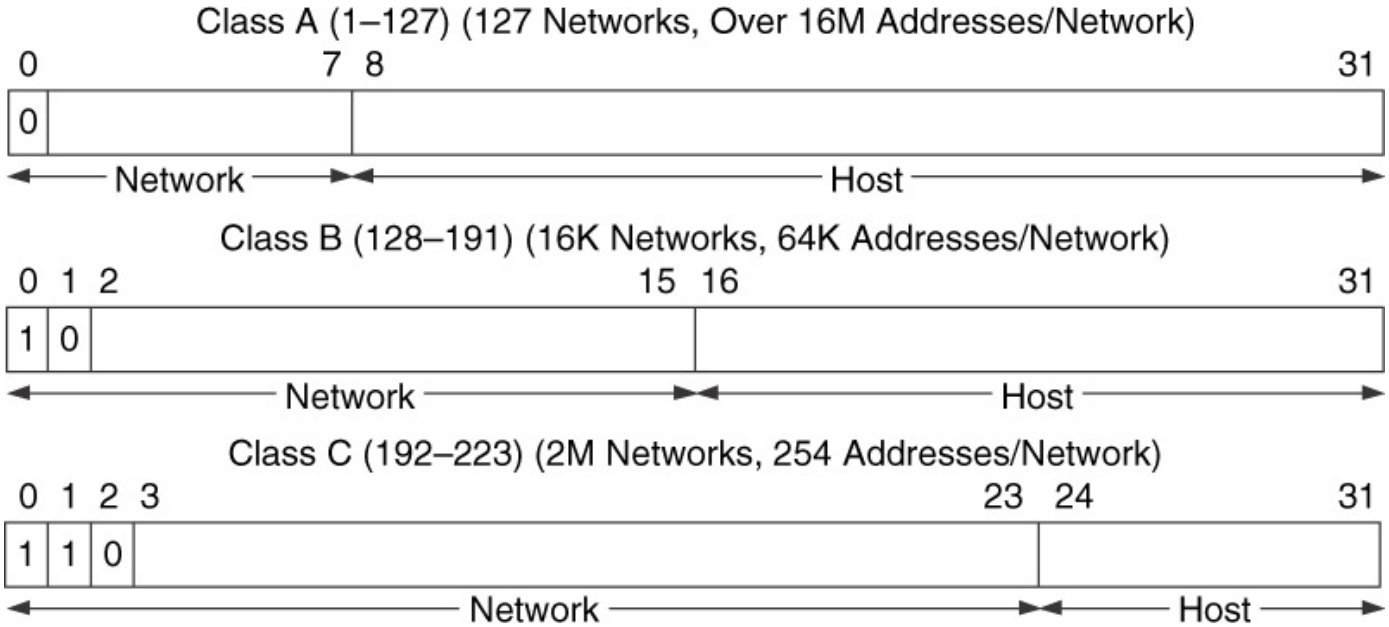
IP Routing
Intranet and Internet



Note:

- Each Router interface has an IP address which is part of the subnet in connects to
- In the figure above, two subnets are: 129.99.0.0/16 and 136.178.0.0/16
- IP address of the router interface to network 129.99.0.0/16 is 129.99.0.100
- IP address of the router interface to network 136.178.0.0/16 is 136.178.0.100

Classful IP Addressing



- Other classes: Class D (prefix1110) is for multicasting; Class E (prefix 1111) is for future use; 255.255.255.255 is a Broadcast Address
- Simple in concept but NOT very efficient
- Superseded by CIDR (Classless Inter Domain Routing)
- Properties of this address scheme:
  - ✓globally unique
  - ✓ hierarchical: Each IP address is divided into network address and host address
  - ✓A few set aside as private (10/8 prefix (00001010); 172.16/12 (172.00001100) prefix; and 192.168/16 prefix (192.168.0.0) Also look at NAT.

IP addresses are managed by a nonprofit corporation called ICANN (Internet Corporation for Assigned Names and Numbers)

IP Addressing - Classful

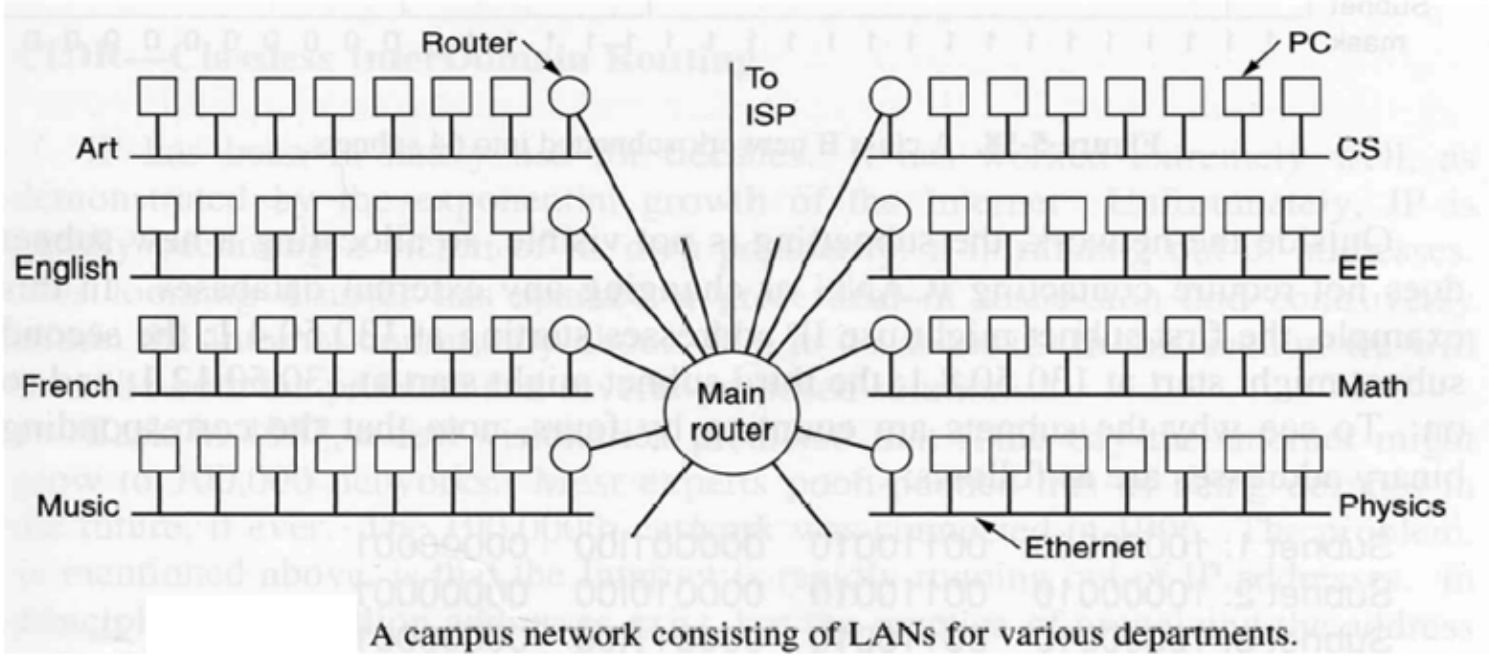
For each class, we can have different number of network addresses and different number of host addresses.

Class	No. of Networks	No. of Hosts per network
A	128	16 million
B	16K	64K
C	2 million	256

Classful IP Addressing

- Network and Device addresses don’t scale well for clients with different size networks
- As a clients’ need change, the address does not scale well since all the hosts in a network must have the same network number
- Masking allows network and device addresses to be grouped into subnets and supernets so that a client gets a network address suitable for its size and traffic to it can be routed based on its network address.

Subnetting

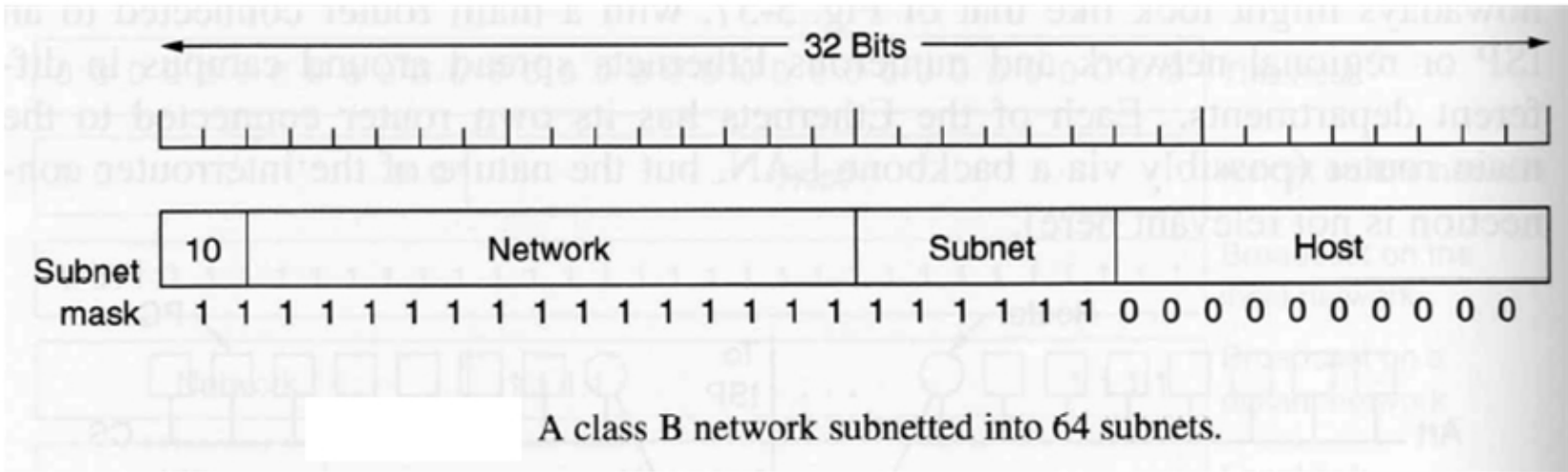


A campus network consisting of LANs for various departments.

- Divide the host field to create multiple networks (Subnets)
- Each subnet can support fewer hosts.
- Each subnet thus created has a subnet number.
- With each subnet, there are associated hosts.
- The router needs a subnet mask to identify which part of the address field is subnet address and which part is the host address.

Example - Subnetting

Instead of having a single class B address with 16 bits for the host number, the host number is divided into a 6-bit subnet numbers, giving a total of 2^6 = 64 subnets and a 10-bit host numbers (1024 hosts per network). This subnet mask can be written as 255.255.252.0. Three subnets are shown (130.50.4.0; 130.50.8.0; 130.50.12.0)



A class B network subnetted into 64 subnets.

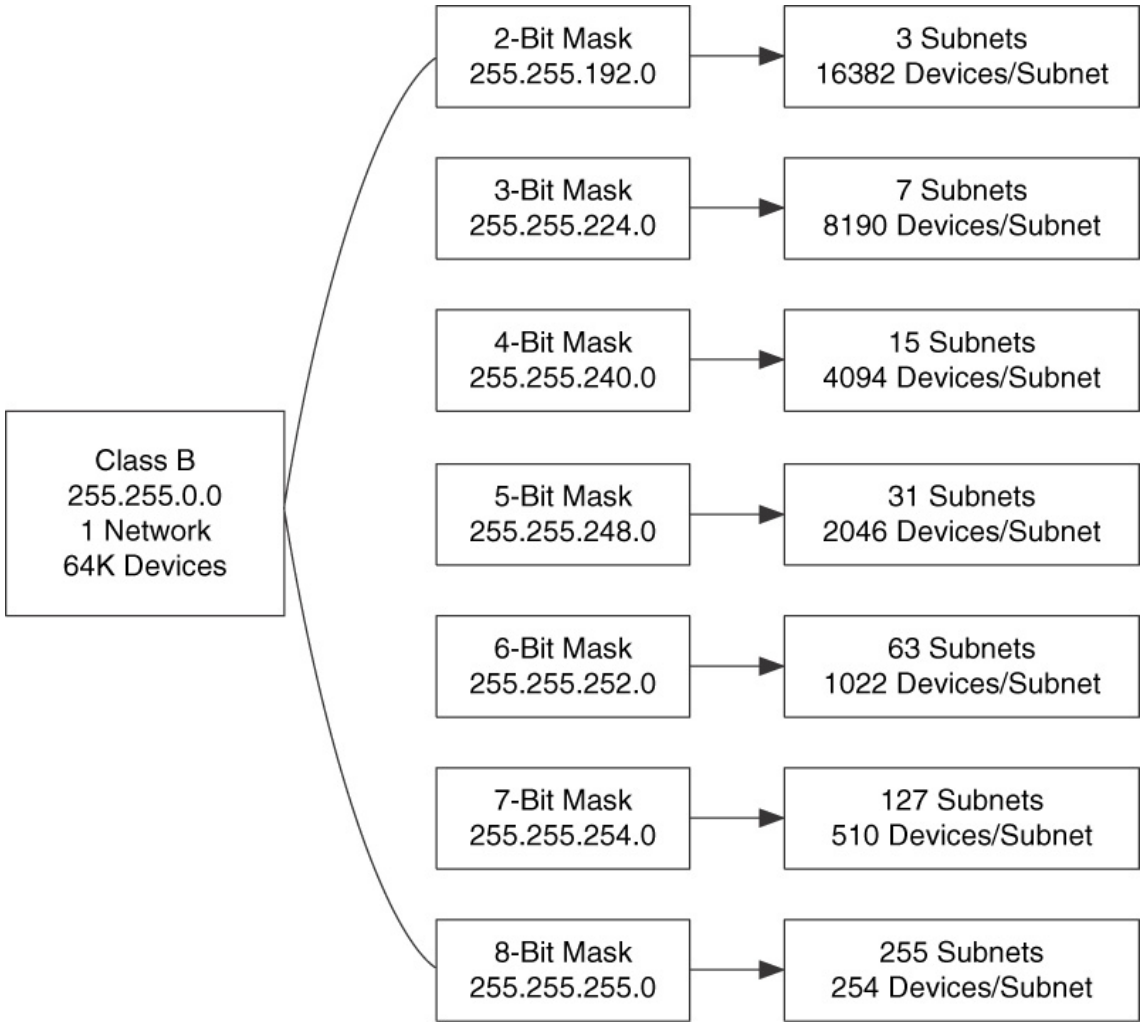
Subnet 1: 10000010 00110010 000001|00 00000001
Subnet 2: 10000010 00110010 000010|00 00000001
Subnet 3: 10000010 00110010 000011|00 00000001

Example - Subnetting

- Consider network address: 129.99.0.0
- It is class B network with natural mask of 255.255.0.0
- To create 7 subnets, increasing the mask by three bits into the third octet. The mask then becomes 255.255.224.0 (note: 224 in binary is 11100000)
- These 7 subnets are listed below with their addresses and masks

Subnet 1:	10000001	01100011	00100000	00000000	→	129.99.32.0	255.255.224.0
Subnet 2:	10000001	01100011	01000000	00000000	→	129.99.64.0	255.255.224.0
Subnet 3:	10000001	01100011	01100000	00000000	→	129.99.96.0	255.255.224.0
Subnet 4:	10000001	01100011	10000000	00000000	→	129.99.128.0	255.255.224.0
Subnet 5:	10000001	01100011	10100000	00000000	→	129.99.160.0	255.255.224.0
Subnet 6:	10000001	01100011	11000000	00000000	→	129.99.192.0	255.255.224.0
Subnet 7:	10000001	01100011	11100000	00000000	→	129.99.224.0	255.255.224.0

Subnetting Through Variable Size Masking



Variable-Length Subnetting

- Subnetting segments a network into a number of equal- sized subnets. This is inefficient.
- In variable-length subnetting, multiple variable-length subnet masks are used, creating subnets of different sizes.
- Examples: Consider the organization below which gets a Class B address. A subnet would be needed for it to provide block of addresses to its various groups.

Workgroup	Groups	Size/Group (Devices)
Engineering	3	400 (1200 total)
Marketing	1	1950
Administration	1	200
Sales	15	35–90 (1350 total)
Research and development (R&D)	1	150
Support	22	10–40 (880 total)
Total	43	5730

Variable Length Example Contd.

- The Class B address (136.178.0.0, mask 255.255.0.0).
- A Class B address can support 65,534 devices.
- We cannot implement subnets of equal size:
  - ✓ There are 1950 devices in Marketing group.
  - ✓ This means, we need 11-bit host addresses.
  - ✓ We have only a 5-bit for subnet mask.
  - ✓ A maximum of 31 possible subnets; however, we need 43 subnets.
- We have enough subnets, we can use a 6-bit subnet mask. This means we will have a maximum of 1023 devices per each subnet. This is not enough for Marketing group.

Variable Length Subnetting Example Contd.

- To solve this problem, we can use variable-length subnetting.
- We can use a combination of 4-bit and 8-bit subnet masks.
- With a 4-bit mask (255.255.240.0), we will have 15 subnets, each with a maximum of 4096 devices.This would be sufficient for Engineering and Marketing.
- The 8-bit mask (255.255.255.0) provides subnets that can have a maximum of 254 devices each. This is sufficient for each of the groups in Sales, R&D, and support.

- The subnet with 4-bit mask allocations are as following:

136.178.16.0	136.178.96.0	136.178.176.0
136.178.32.0	136.178.112.0	136.178.192.0
136.178.48.0	136.178.128.0	136.178.208.0
136.178.64.0	136.178.144.0	136.178.224.0
136.178.80.0	136.178.160.0	136.178.240.0

- ✓ Subnets (136.178.16.0, 136.178.32.0, and 136.178.48.0) are allocated to Engineering groups.
- ✓ Subnet (136.178.64.0) is allocated to Marketing.
- ✓ Subnet (136.178.80.0) is allocated to Administration.

- We will take the 4-bit subnet (136.178.96.0, or 136.178.01100000.0) and apply an 8-bit mask (255.255.255.0), we will get the following subnets:

136.178.97.0	136.178.102.0	136.178.107.0
136.178.98.0	136.178.103.0	136.178.108.0
136.178.99.0	136.178.104.0	136.178.109.0
136.178.100.0	136.178.105.0	136.178.110.0
136.178.101.0	136.178.106.0	136.178.111.0

✓Subnets {136.178.97.0 through 136.178.110.0} or {136.178.01100001.0 through 136.178.01101110.0} are allocated to Sales.

✓Subnet (136.178.111.0) is allocated to R&D.

• We need 22 subnets for Support; therefore, we will use the next two available 4-bit subnets (136.178.112.0 and 136.178.128.0). For 136.178.112.0:

136.178.113.0	136.178.118.0	136.178.123.0
136.178.114.0	136.178.119.0	136.178.124.0
136.178.115.0	136.178.120.0	136.178.125.0
136.178.116.0	136.178.121.0	136.178.126.0
136.178.117.0	136.178.122.0	136.178.127.0

For 136.178.128.0:

136.178.129.0	136.178.134.0	136.178.139.0
136.178.130.0	136.178.129.0	136.178.140.0
136.178.131.0	136.178.136.0	136.178.141.0
136.178.132.0	136.178.137.0	136.178.142.0
136.178.133.0	136.178.138.0	136.178.143.0

The remaining 4-bit and 8-bit subnets would be available for future growth.

Do Problem 6 for Practice
Addressing Requirements in Problem 6

AS Number	Location	Department	Users
1	Chicago Campus Building 1	Legal	120
		Accounting	370
	Chicago Campus Building 2	HQ	1580
		Engineering	200
2	Toronto	Sales	75
	Boston	Sales	110
3	Philadelphia	Operations1	2150
		Operations2	975
		Sales	575

Supernetting

- Consider a customer who needs more than one class C address but Class B address is too large or unavailable.
- How do you address this customer's need without wasting addresses by assigning this customer a Class B address even if they were available?
- The answer is supernetting.
- You can assign this customer a contiguous set of Class C addresses and through suitable masking create a supernet for routing with that network address.

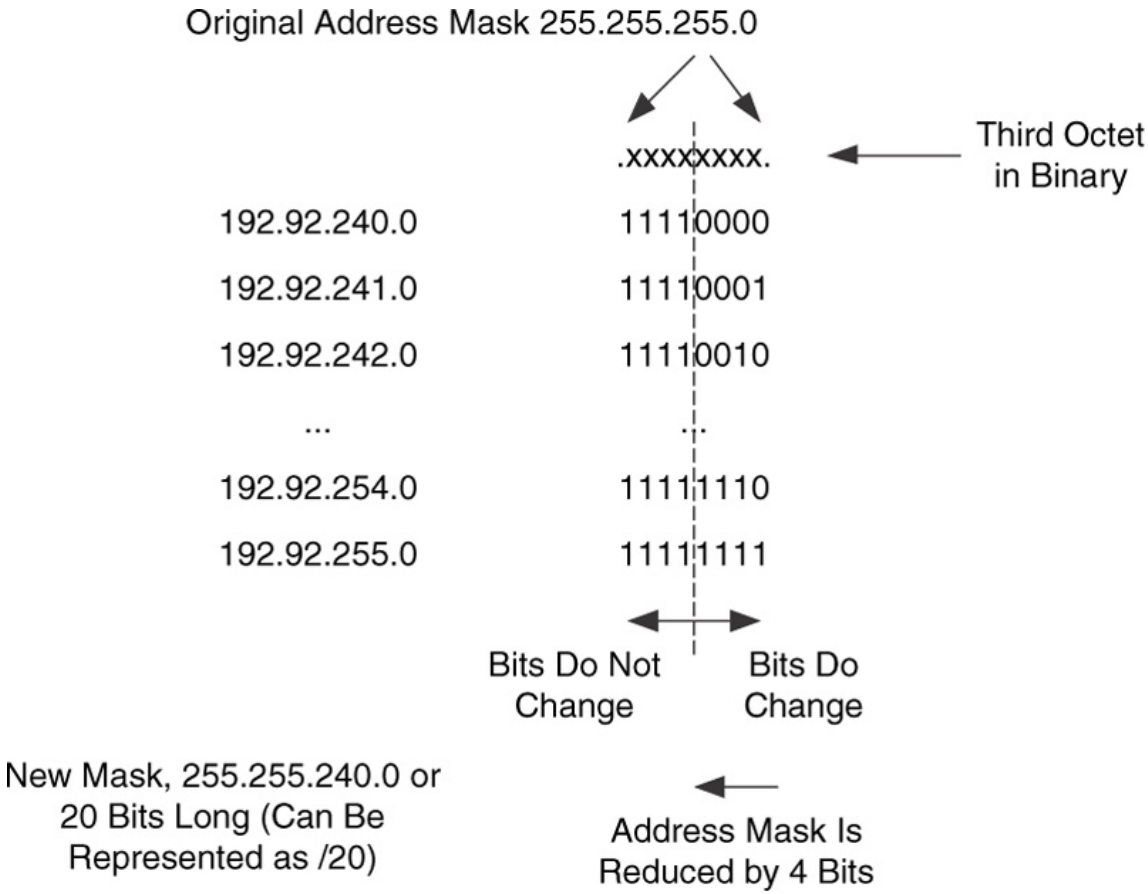
Question: Could you give this customer a number of disjoint Class C addresses which may be available. What will be the problem? See next slide for an insight into the problem.

Supernetting Contd.

- Consider a customer who needs 3,000 addresses and therefore Class B address is too large for this customer. However, contiguous Class C addresses: 192.92.240 (11110000).0 through 192.92.255(11111111).0 are available.
- If you assign this set of addresses to the customer, each router will need to translate 192.92.240.0 through 192.92.255.0, i.e.16 addresses, to route. Recall that these being class C addresses, the mask for these addresses is 255.255.255.0 and network address for them is given by the first three bytes.
- This is a lot of translation for the traffic going to the same place. We can do better through Supernetting.
- Look at the third byte of this set of class C addresses.

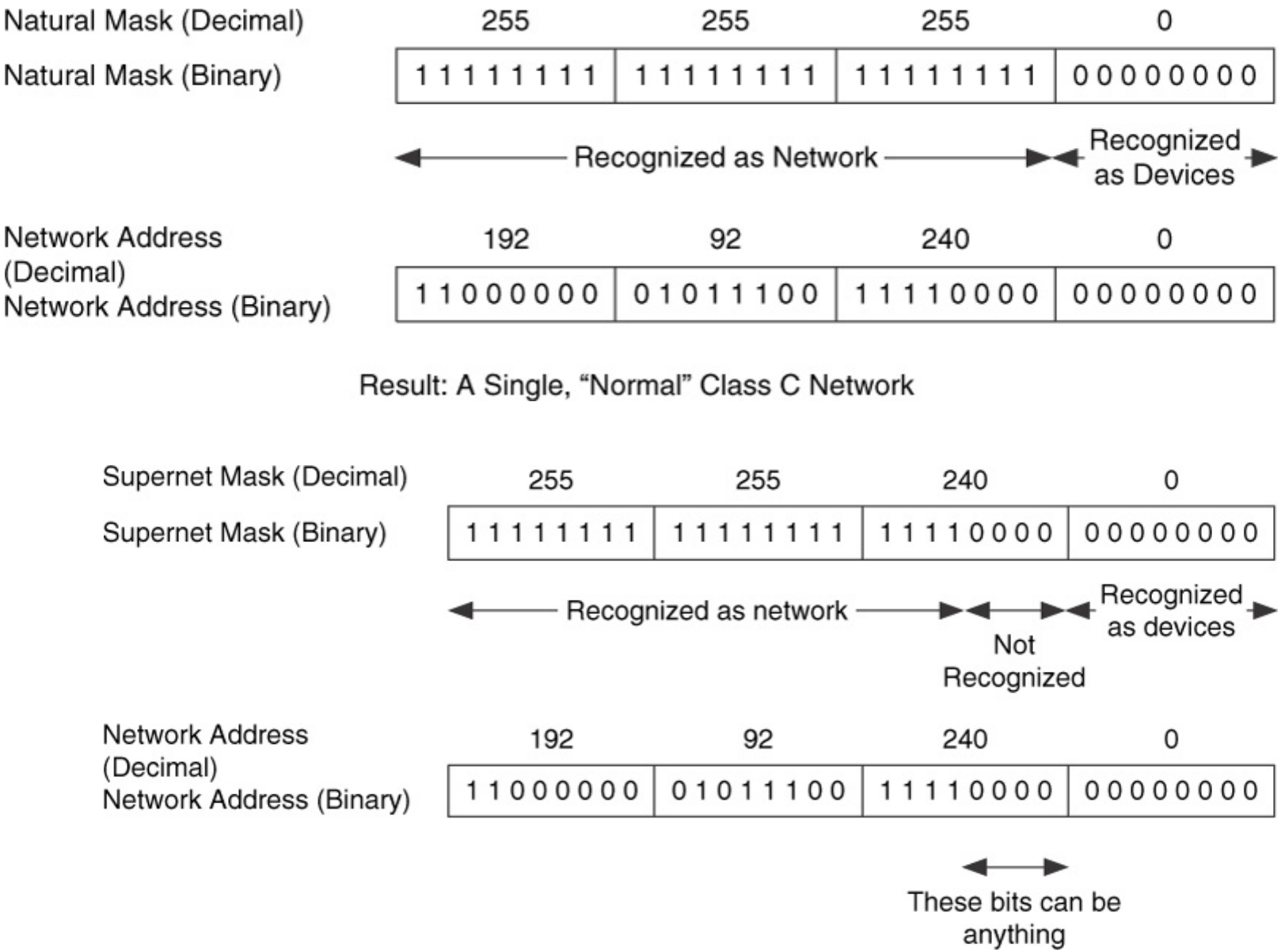
Superneting – Contd.

- Look at the third byte of this set of class C addresses. (192-92-240-0 to 192.92.255.0)



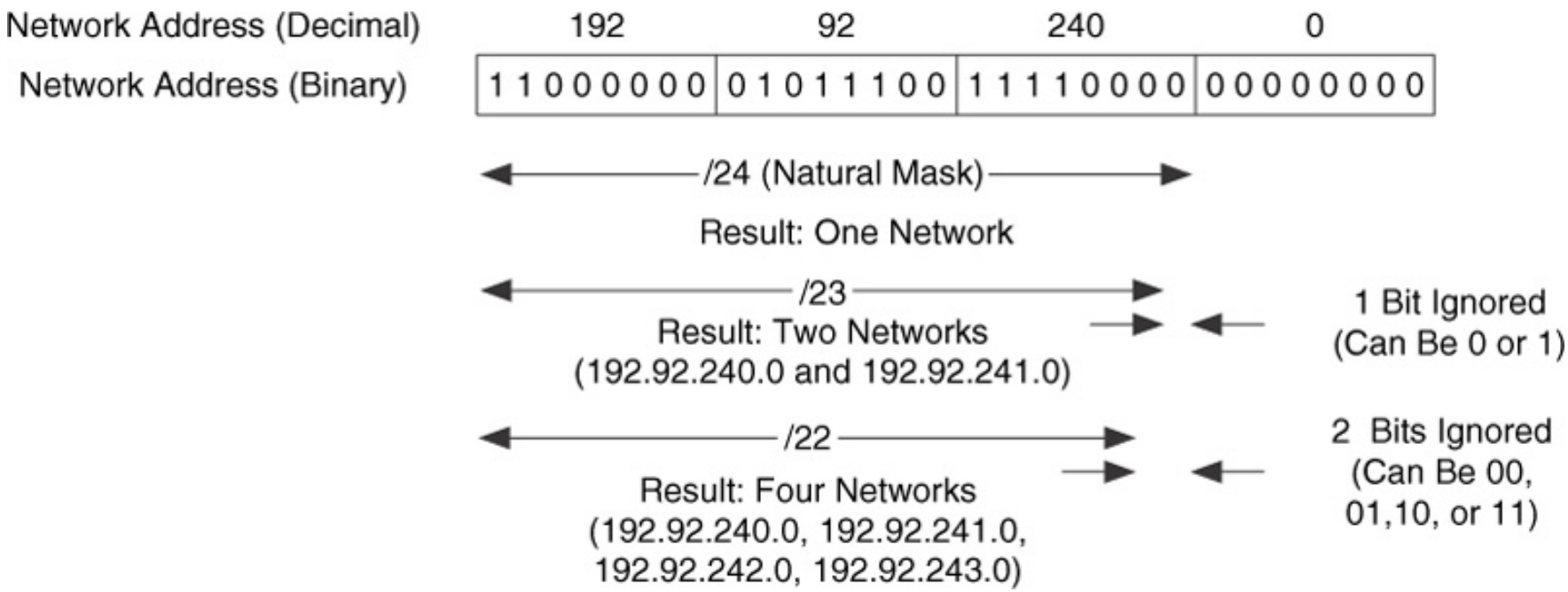
- You can see from above that we can create a new mask 255.255.240.0 thus creating a supernet with network address of 192.92.240.0 for routing since the first four bits of the third byte are all 1s.

Supernetting contd.



CIDR (Classless Inter-Domain Routing)

- The question then arises that subnetting and supernetting help arbitrarily divide the address into network part and device part, so why have classes?
- The answer is CIDR as shown.



CIDR Example

- Consider an organization which is granted a block of addresses and one of the addresses it has is: 205.16.37.39/28. We want to determine the network address for the organization and what host addresses are available to it.
- From above we see that the leftmost 28 bits defines the network address and the rightmost four bits are addresses available to this organization.
- Note that from /28 we know that only the rightmost octet is divided into network and host address and that the leftmost four bits define network address and the rightmost four the host addresses within the organization. This octet 39 in binary is: 00100111. From /28 then the network address here is: 205.16.37.32 (001000000) with associated mask od 255.255.255.240 (11110000) and the host addresses available to this organization are: 205.16.37.32 (00100000) to 205.16.37.47 (00101111).
- In summary, packets to this organization are routed based on the network address: 205.16.37.32xxxx and the organization has the liberty of addressing its hosts from the a block of: 205.16.37.32 (00100000) to 205.16.37.47 (00101111).

Private Addressing

- Private IP addresses are those that cannot be advertised and forwarded by network devices in the public domain. Network routers with these addresses will drop the packets.
- Three are three blocks of private address space are:
  - 10/8 prefix i.e., 10.0.0.0 through 10.255.255.255. The leftmost 8 bits identify the network address.
  - 172.16/12 prefix, i.e., 172.16 (00010000).0.0 through 172.31(00011111).255.255, or 172.0001000.0.0 through 172.00011111.0.0. The leftmost 12 bits identify the network address.
  - 192.168/16 prefix, i.e., 192.168.0.0 through 192.168.255.255. The leftmost 16 bits identify the network address.
- Private addressing can be used for security, reusing addresses and for other reasons.

NAT (Network Address Translation)

NAT provides mechanism to translate addresses from the private address spaces to the public address space.

NAT creates bindings between addresses:

- One-to-one bindings (known as static NAT), used for servers.
- One-to-many address bindings (known as dynamic NAT), used for user devices.
- Address and port bindings (known as network address port translation [NAPT]).

Routing Algorithms

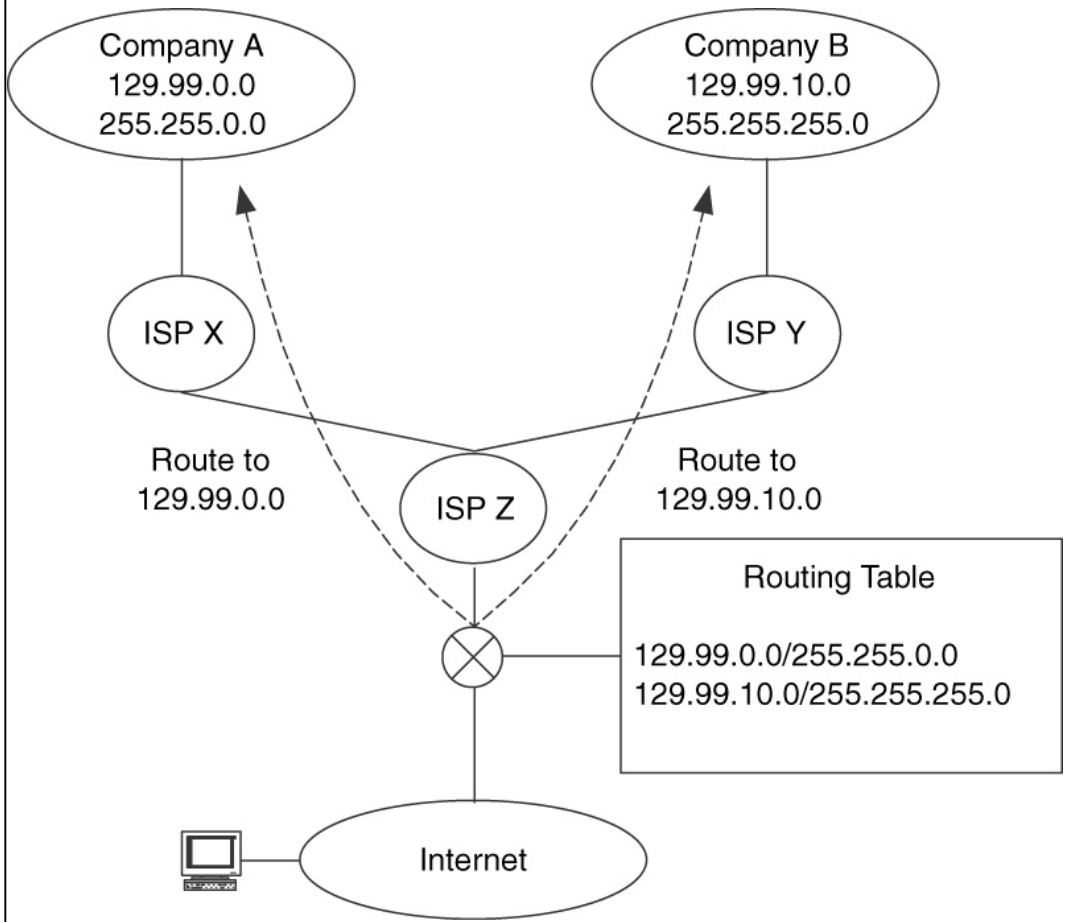
- Algorithm to decide which output line an incoming packet should be transmitted on.
- Routing consists of two main mechanisms:

1. **Path discovery and maintenance:**
   - Learning about reachability (i.e., which networks they are connected to and which networks)
   - Creates a **routing table**.
   - The ***default route*** (route of last resort.)
2. **Packet forwarding:**
   - applying the reachability information (routing table) to forward packets toward their destination

Packet Forwarding

- Where to forward a packet?
- Rather Simple: Packet is forwarded based on longest (most explicit) address match.
- Consider an IP packet arriving at ISP Z with a destination address of 129.99.10.1, Where should it be forwarded?
- Based on masks, match the company's network addresses with the packet address, and route with the longest address match, so route to router ISP Y
- Note "AND" operations on the company addresses with the packet address gets you the longest match.

Consider



Two Types of Routing Algorithms

- **Static routings:**
  - Computed in advance.
  - Independent of current traffic and topology.
- **Dynamic routings:** Routing to reflect changes in the traffic and topology.

Some of The Routing Algorithms

- Shortest Path Routing - Static
- Flooding - Static
- Distance Vector Routing
- Link State Routing
- Hierarchical
- Others such as Path Vector Routing used by Border Gateway Protocols

Shortest Path Routing (Static)

- Uses graphs to represent network components and finds shortest path from source to destination.
- Path length can be:
  - Number of hops
  - Physical Distance
  - Bandwidth
  - Measured delay
  - Other factors
- Dijkstra Algorithm can be used to find shortest path

Flooding (Static)

- Send every incoming packet on every outgoing link except the one it arrived on
- Flooding generates duplicated packets, to avoid it:
  - Use a hop counter. Discard after certain # of hops.
  - Keeping track of which packets have been flooded, to avoid sending them out a second time.
- Selective Flooding**:** Send incoming packets out on lines going approximately in the right direction.
- There are many strategies which are used for efficient flooding

Distance Vector Routing (Dynamic)

- Each router maintains a table giving the best known distance (the shortest path) to each destination and which line (next hop router) to use to get there. That is:
  - The tables contain one entry for each destination.
  - The preferred outgoing line (next hop) to use for that destination
- These tables are updated periodically by exchanging information with the neighbors.
- Uses Bellman-Ford Algorithm
- Router protocol RIP/RIPv2 (Routing Information Protocol), uses the distance-vector routing algorithm.

Distance Vector Routing Example

Consider that Node J wants to communicate with node G:

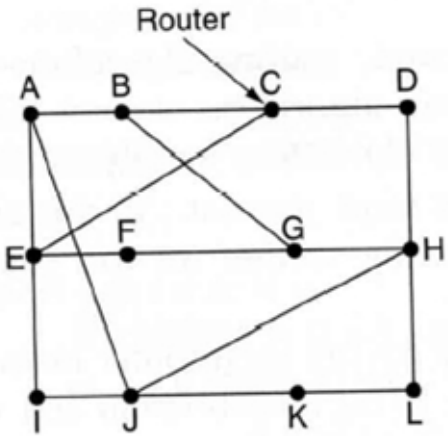
J first measures or estimates its delay to its neighbors, A, I, H, and K as 8, 10, 12, and 6 msec.

J will also receive four vectors from A, I, H, and K. These vectors tell J the delay to reach each destination from each of these neighbors.

Next J computes the delay to G via its four neighbors A, I, H, and K as 26 (8+18), 41 (10+31), 18 (12+6), and 37 (6+31) msec, respectively. Note that to reach G via A from the first vector is (8+18).

Once J has these distances from all its neighbors, it finds the minimum value, and the next hop router associated with that.

The best (minimum) value in this example is 18 msec (min(26, 41, 18, 37) with the associated next hop router H. J will send the packets via H.



New estimated delay from J

To	A	I	H	K	Line
A	0	24	20	21	8 A
B	12	36	31	28	20 A
C	25	18	19	36	28 I
D	40	27	8	24	20 H
E	14	7	30	22	17 I
F	23	20	19	40	30 I
G	18	31	6	31	18 H
H	17	20	0	19	12 H
I	21	0	14	22	10 I
J	9	11	7	10	0 –
K	24	22	22	0	6 K
L	29	33	9	9	15 K
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6	New routing table for J

Vectors received from J's four neighbors

Distance Vector Routing - Disadvantages

- On large networks, the table update process can take so long that at any given time the reported information does not represent the actual network status.
- It does not take line bandwidth into account when choosing routes.
- Algorithm related issues: Convergence, routing related traffic, etc. But it does work.
  - Count to infinity problem (limit counts- say to 16)
  - Split Horizon (Don’t pick link which provided the update)
  - Poisson reverse (put that link as distance of infinity)
- RIP and RIPv2 is based on this.
- For more, refer to RFC 1058 for instability.

Link State Routing (Dynamic)

- Link state routing requires more processing power than distance vector routing but provides more control over the routing process and responds faster to changes.
- Routing in Link State Routing can be based on:
- The avoidance of congested areas
- The speed of a line
- Or other various priorities.
- It uses Dijkstra’s algorithm
- The associated routing protocol is OSPF

Link State Routing (Contd.)

Each Router does the following:

•Compute the shortest path to every other router. One of the he algorithms used to compute short path from one node to another node is Dijkstra's shortest path algorithm.

• See its live demo of this (Dijkstra's) algorithm at:

http://optlab-server.sce.carleton.ca/POAnimations2007/DijkstrasAlgo.html

This algorithm computes shortest path from each node to every other node so that each node has a shortest route for every other node in its network.

•The algorithm need to run at each node.

•Then use the shortest path (to a destination) to route a packet to that destination.

Link State Routing - Disadvantages

As networks grow:

- the router routing tables grow, thus more memory and CPU power are consumed.
- more bandwidth is consumed to send updated information.

Solution:

•Organize the network in a tree-like structure and use localized routing within each branch or hierarchy.

•This solves the problems of link state routing in which routers can have and process less network information.

Routing Protocols

- RIP/RIPv2 (Routing Information Protocol), uses the distance-vector routing algorithm.
- OSPF (Open Shortest Path First), uses the link state algorithm, operates within an autonomous system.
- BGP (Border Gateway Protocol) - path-vector based. Policy dictates routing.
- MPLS (Multi-Protocol Label Switching): Use labels to route.

RIP, OSPF, and Static Routing Protocols

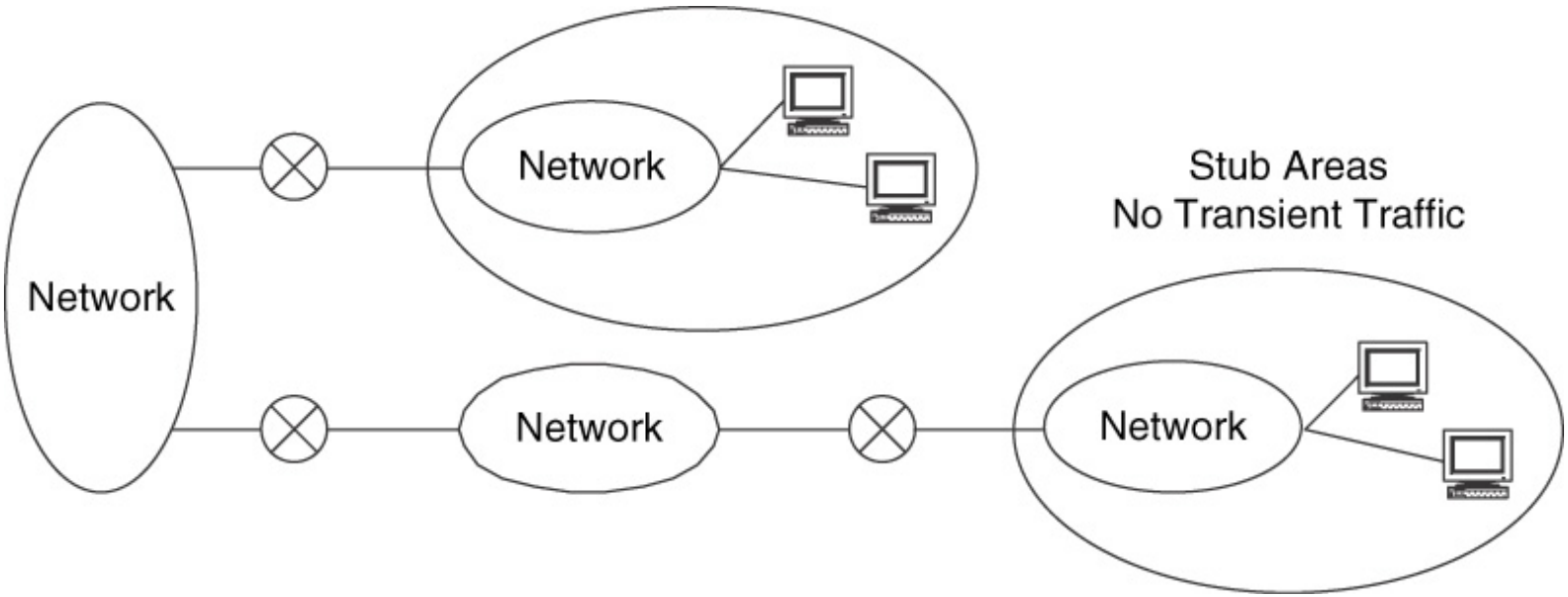
- RIP is a distant-vector routing protocol that is easy to use. It is good for small networks or within an autonomous system. However, it has few features and options. It has high overheads; slow to converge. Other issues as mentioned earlier.
- OSPF is a more complex protocol based on link-state routing, however, it provides area abstraction, rapid convergence, better performance. It is good for medium networks. OSPF is used in high hierarchy and diverse networks, with each segment running link state protocol.
- Static route is configured manually to force routing along certain paths. It is also applied as a default route between a stub network and the network to which the stub is connected.

BGP (Border gateway Protocol)

- Is a path-vector-based exterior gateway protocol for inter-domain routing, such as routing across Autonomous Systems. It is used where policy based path is more important in routing than cost (minimum) based.
- Use policies to determine actions to be taken on paths.
- BGP exchanges routing information establishing peering connections via TCP links.
- The complexity of BGP configuration depends on the complexity of your policy definitions.
- BGP is best-suited for inter-AS routing although it is also used within an AS in some cases.
- BGP can have two types of sessions:
  - IBGP (Interior BGP) to exchange routing information within an Autonomous System.
  - EBGP (Exterior BGP) to exchange information between two routers in two different Autonomous Systems.

Routing protocol for Stub Network

- Stub networks have no transient traffic
- A static route is more appropriate for stub network
  - Simple to set up
  - No configuration
  - Less overhead traffic (no constant traffic to update routing tables)



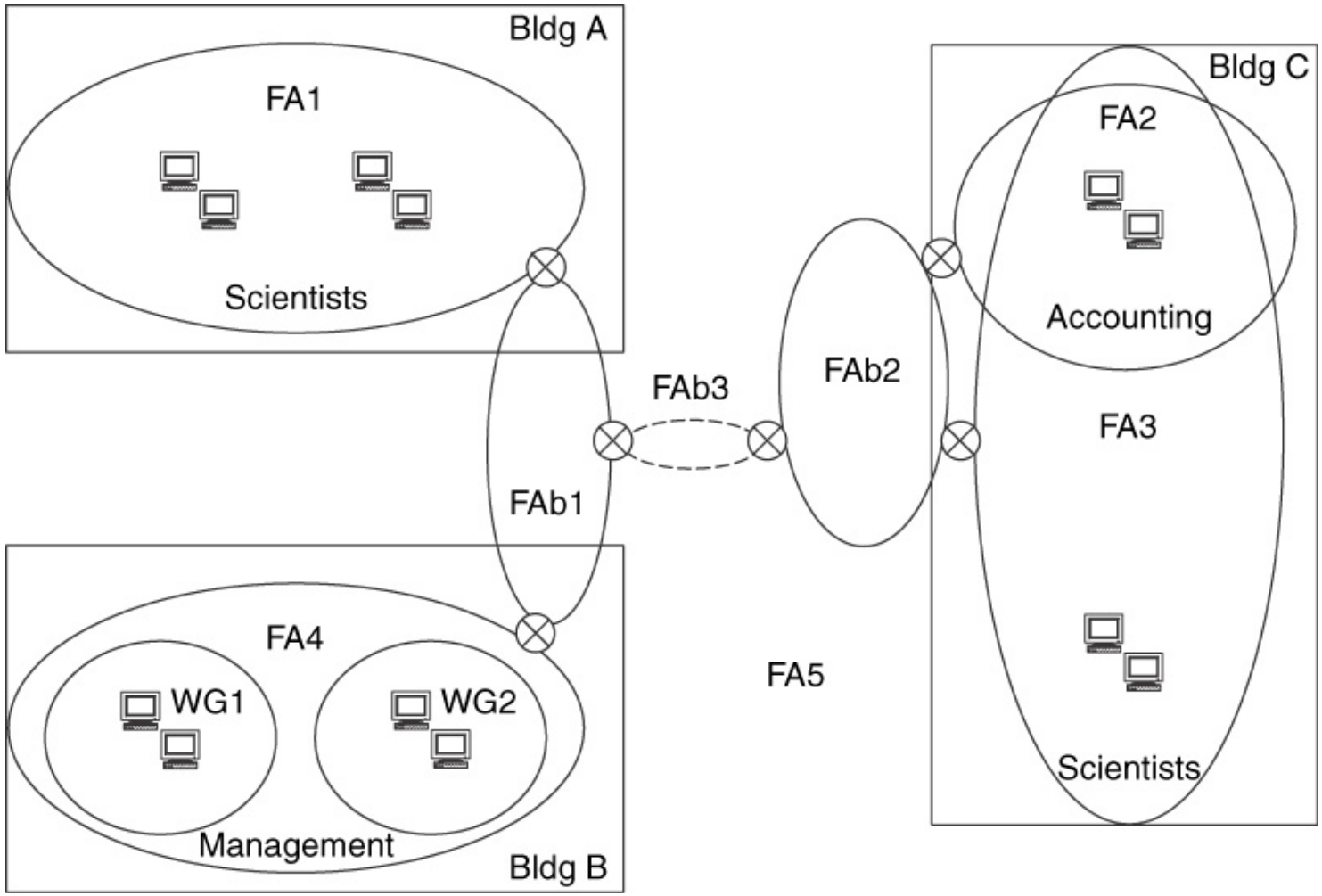
Routing Protocols Evolution

- Convergence times
- Complexity of the protocol
- The protocol overheads (bandwidth overhead, CPU utilization, memory utilization; their stability.
- Hierarchy and interconnectivity support
- Interoperability of the protocols

Establishing Routing Flows

- In this process the network segments into functional areas and workgroups, identifying boundaries between these areas, and then formatting the relationships between boundaries and routing flows.
- Function areas (FA) are groups within the system that share a similar function.
- Groups may be of users (workgroups), applications, or devices or combination of these, and they may share similar jobs/tasks, physical locations, or functions within the network.
- Workgroup (WG) are groups of users that have common locations, applications, and requirements, or that belong to the same organization.

An Example of Workgroups and Functional Areas



Routing Mechanisms

- Establishing Routing Flows
- Identifying and Classifying Routing
- Boundaries Manipulating Routing Flows

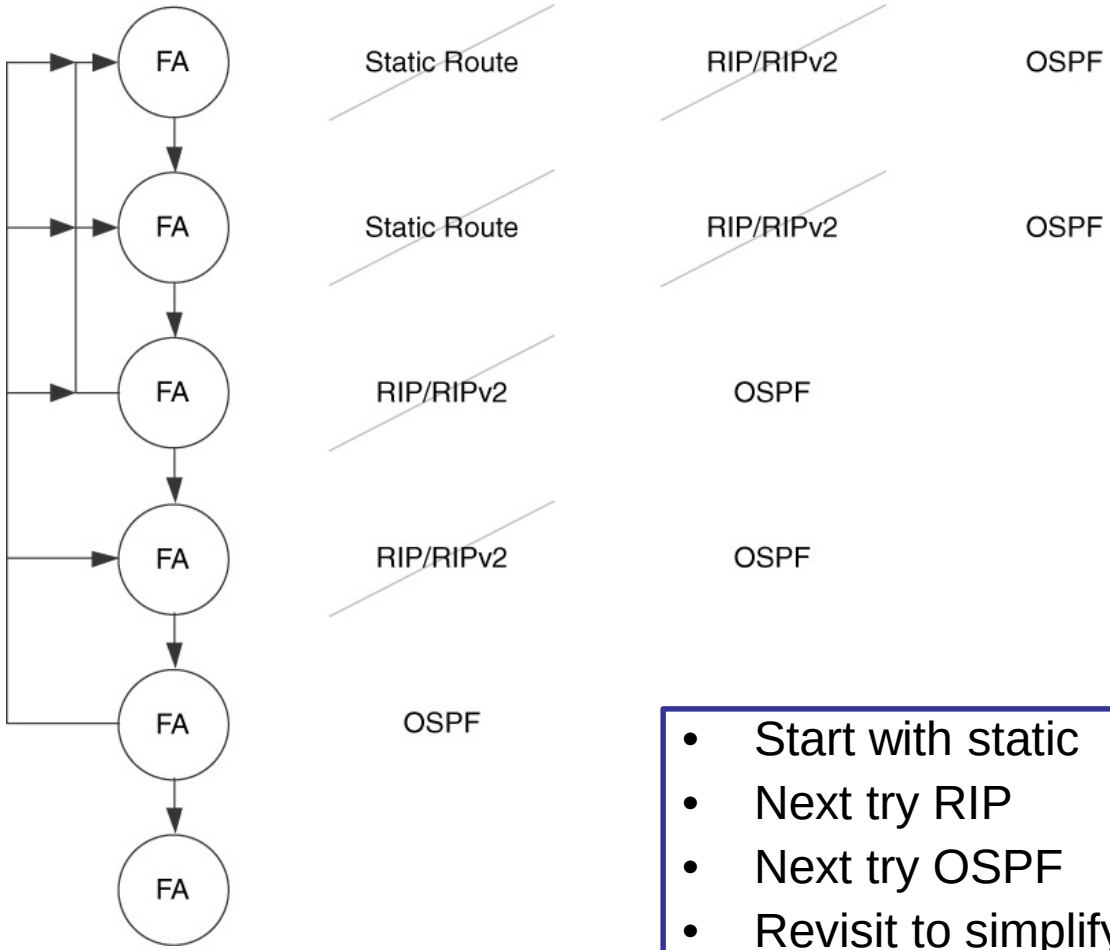
Manipulating Routing Flows

- A default route: is the route used when there is no other route for that destination.
- Default Route Propagation: is the technique used to inform network of the default path.
- Routing filtering: is the technique of applying route filters to hide networks from rest of an AS.
- A route filter: is a statement, configured in one or more routers, that identifies one or more IP parameters (e.g., an IP source or destination address) and an action (e.g. drop or forward) to be taken.
- Route aggregation: is the technique of exchanging routing information between ASs.
- Policies: are high-level abstractions of the route filtering technique

Choosing and Applying Routing Protocols

- Use “Keep It Simple Stupid (KISS)” principle
- Use minimal number of protocols through evaluation of hierarchy and diversity. Although at times, using different protocols at different areas is beneficial
- Start with simplest routing strategy and protocols
- If complexity increases then reevaluate.
- Note: Be aware of how information (e.g., network masks, policies, protocol metrics, AS information) is translated between protocols. These may be lost or mistranslated.

An Example of Iterative Evaluation of Routing Protocol KISS Concept



- Start with static
- Next try RIP
- Next try OSPF
- Revisit to simplify protocol implementation and minimize number of different protocols

Identify & Classify Routing Boundaries

Routing boundaries are physical or logical separations of a network, based on:

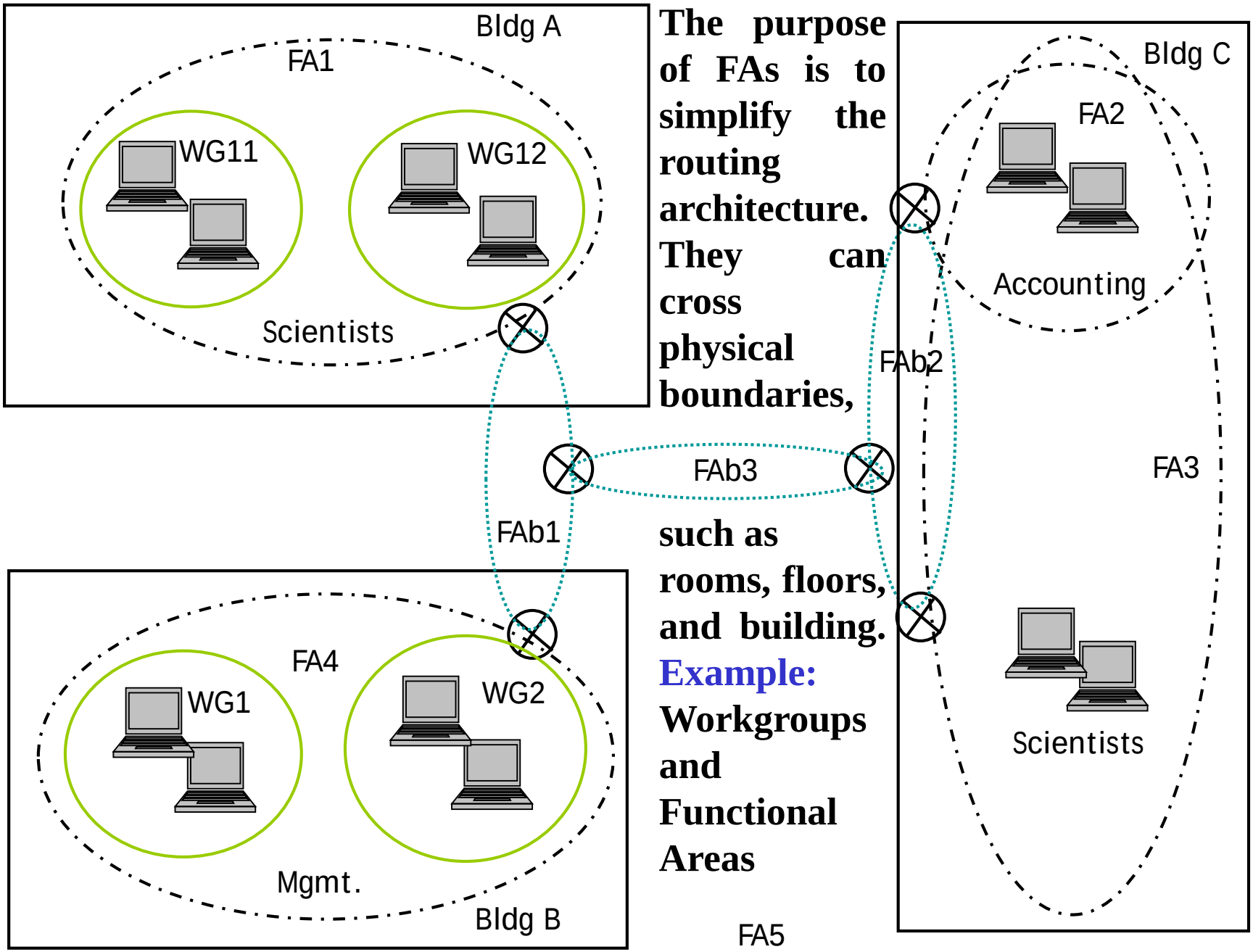
- requirements of that network
- administration of that network

Physical boundaries can be identified by

- isolation LANs (iLAN), also called demilitarized zones (DMZs),
- physical interfaces on network equipment,
- or physical security (based on the security devices location).

Logical boundaries can be identified by:

- FAs
- WGs
- administrative domain (i.e AS)
- routing management domains (a subset or a superset of one or more ASs).



The purpose of FAs is to simplify the routing architecture. They can cross physical boundaries, such as rooms, floors, and building.

Example: Workgroups and Functional Areas

Routing between Boundaries

Two type of routing protocol used to pass routing information among the boundaries.

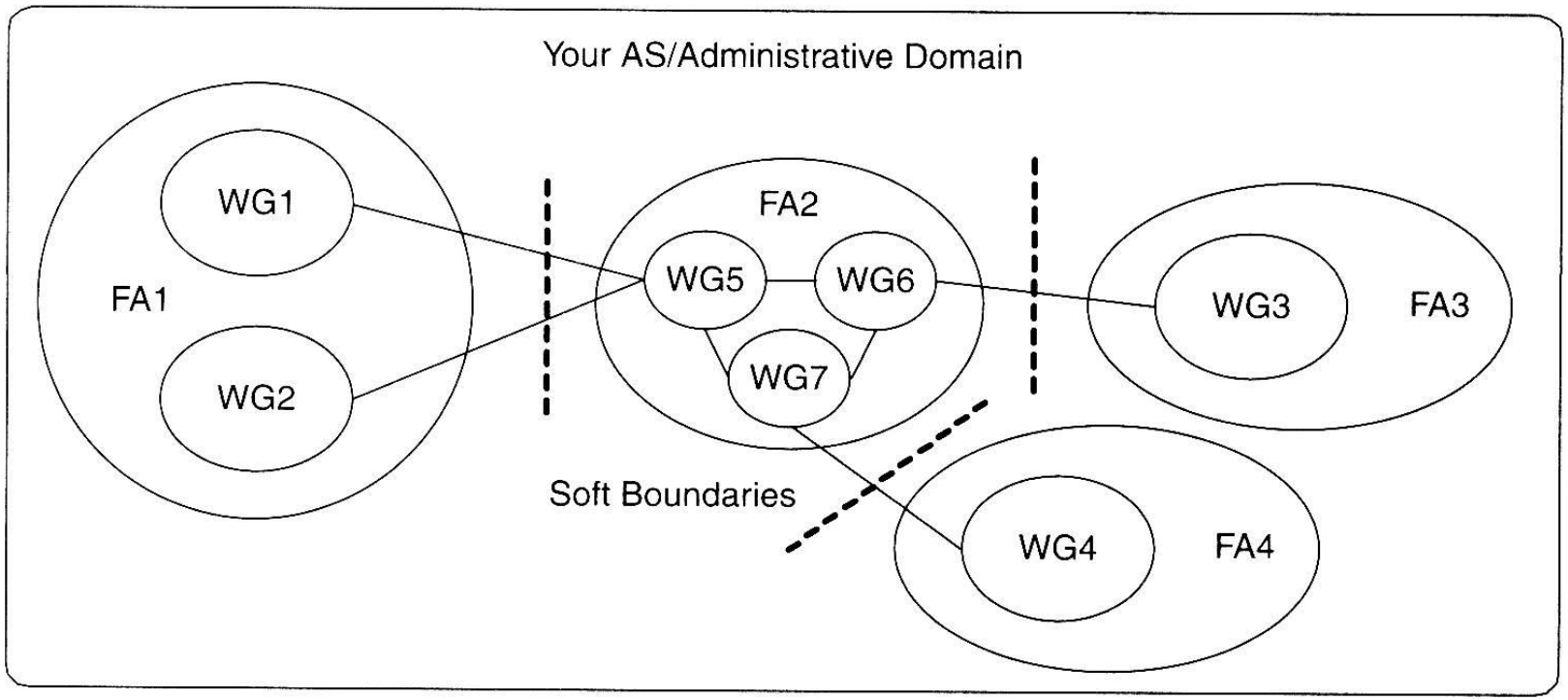
- Interior Gateway Protocols (IGPs), primarily within an AS. (IGPs can be used between ASs also, but rarely used that way)
- Exterior Gateway Protocols (EGPs), communicate routing information (reachability and metrics) primary between ASs, between an AS and external networks, between well-defined network boundaries within an AS, at ISP interfaces, and with DMZs.

Routing between boundaries:

- EGPs are used between Hard boundary:
- IGPs are used between Soft boundary

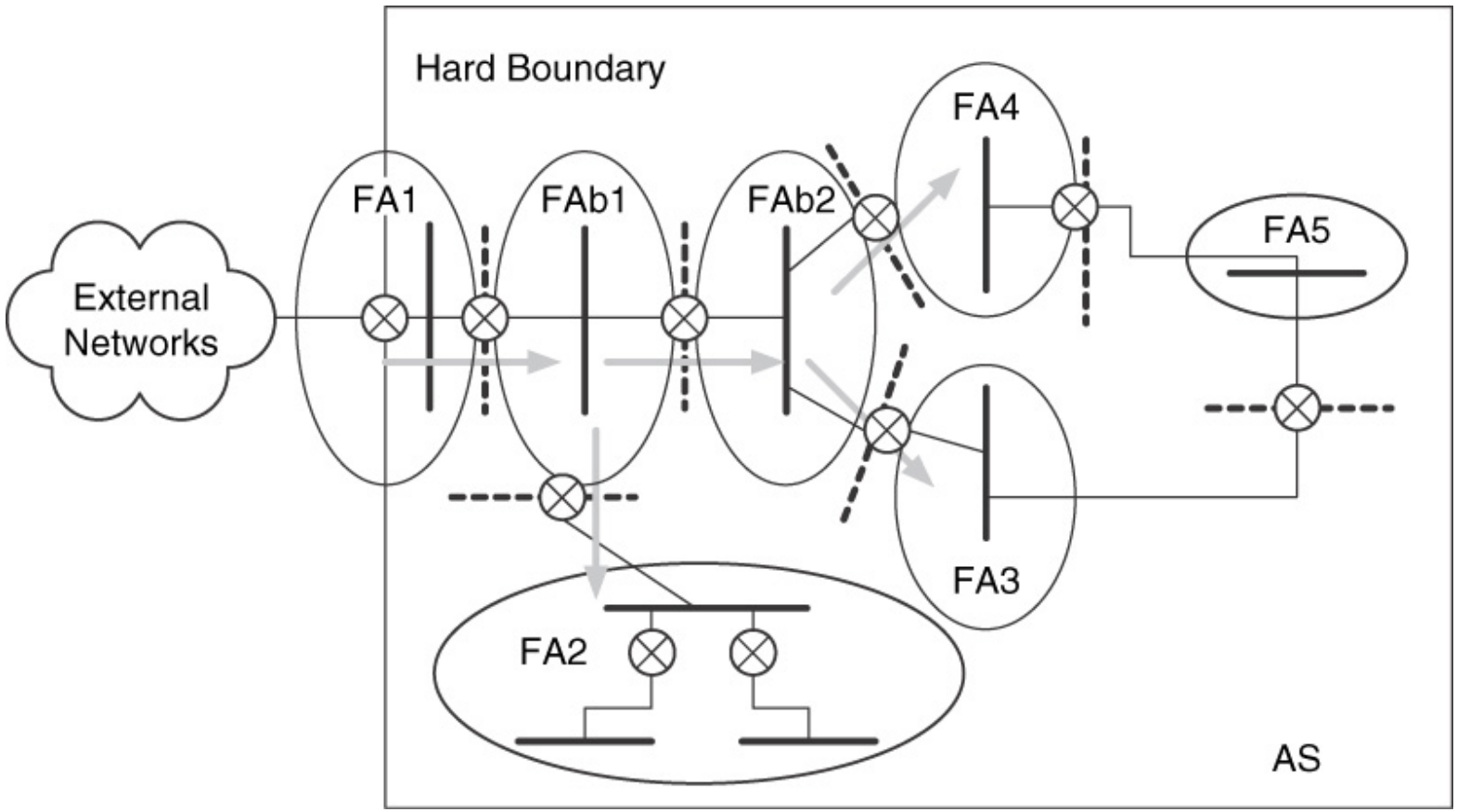
Soft Boundaries

- Used within a administrative area, but to separate workgroups and functional areas

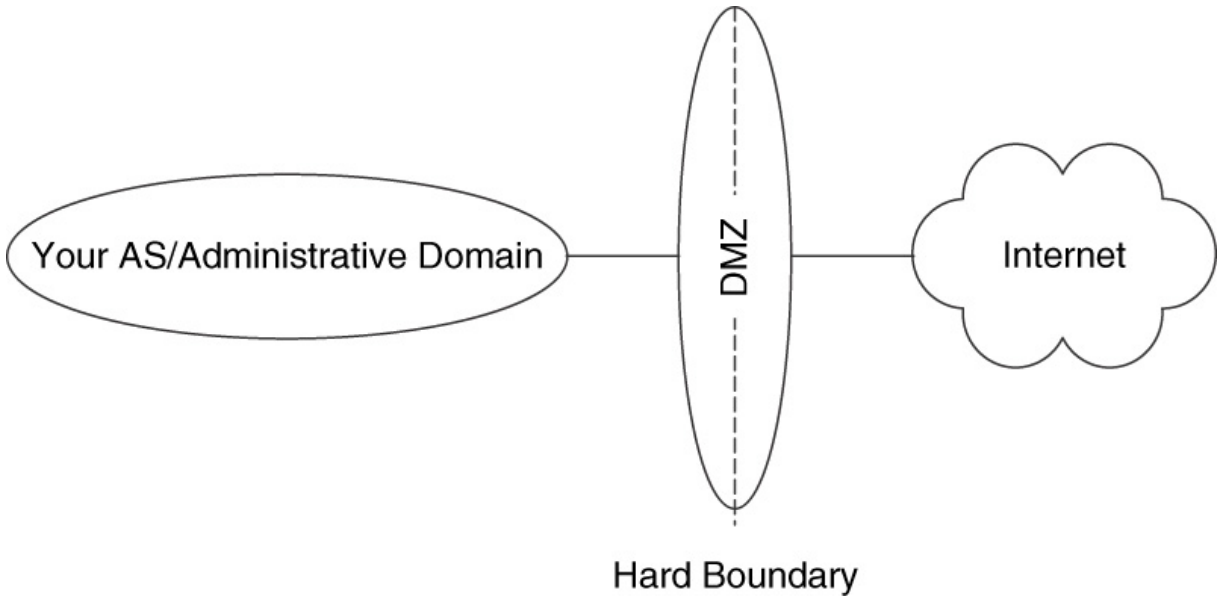


Hard Boundaries

- To protect your network (Autonomous System from outside networks



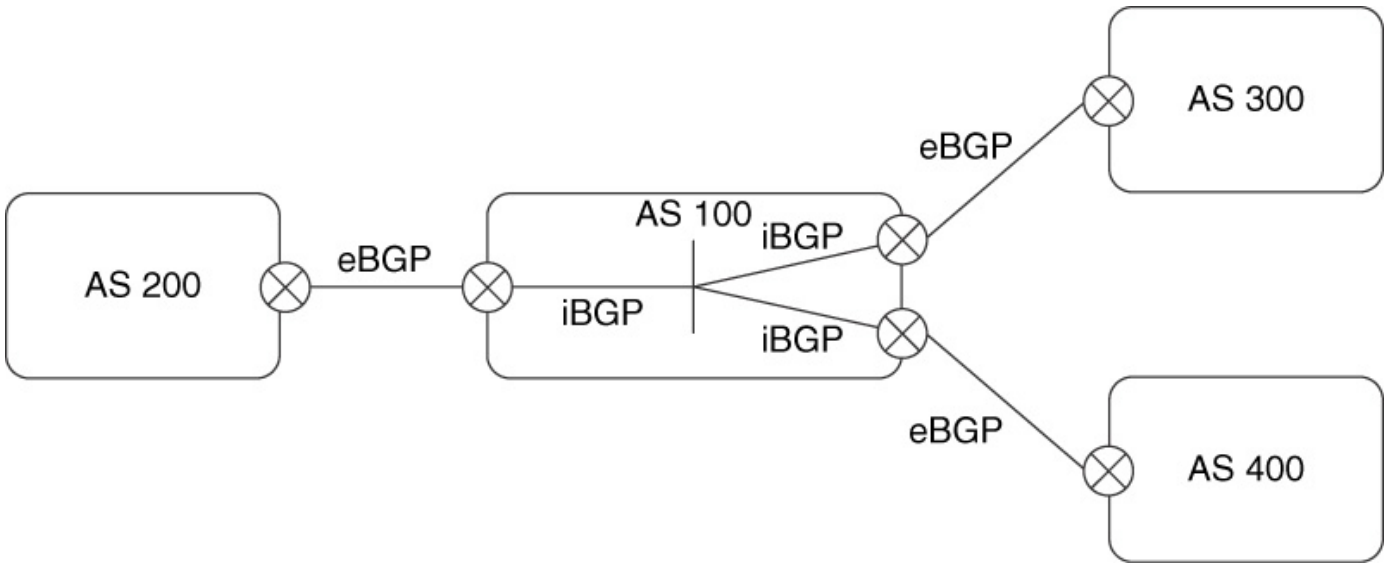
An Example of a Hard Boundary to Protect the Your Network from Outside - DMZ



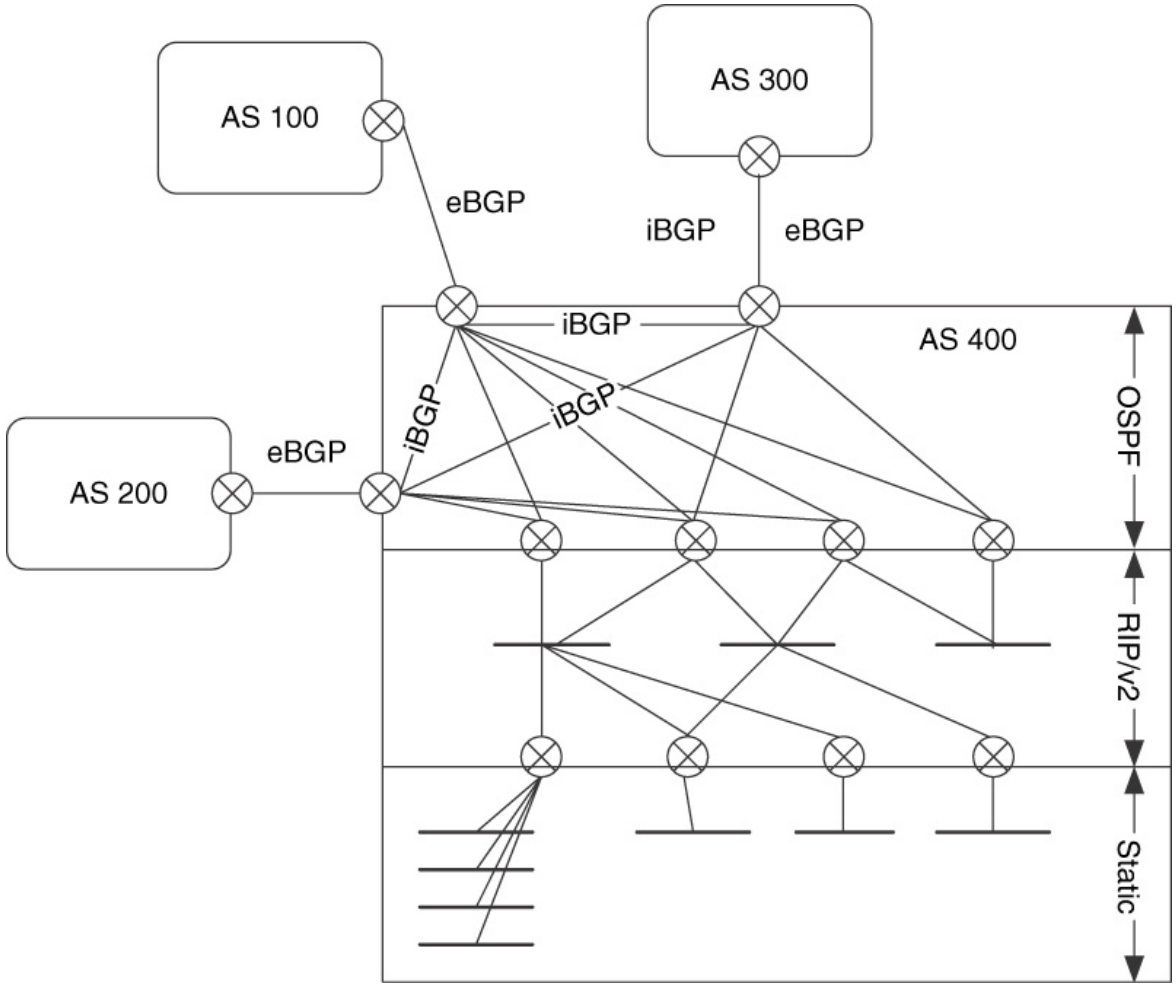
Application of Internal BGP (iBGP) and External BGP (eBGP)

There are two types of Border gateway Protocols (BGP):

- External BGP (eBGP) for applications between Autonomous Systems
- Internal BGP (iBGP) for applications within an AS

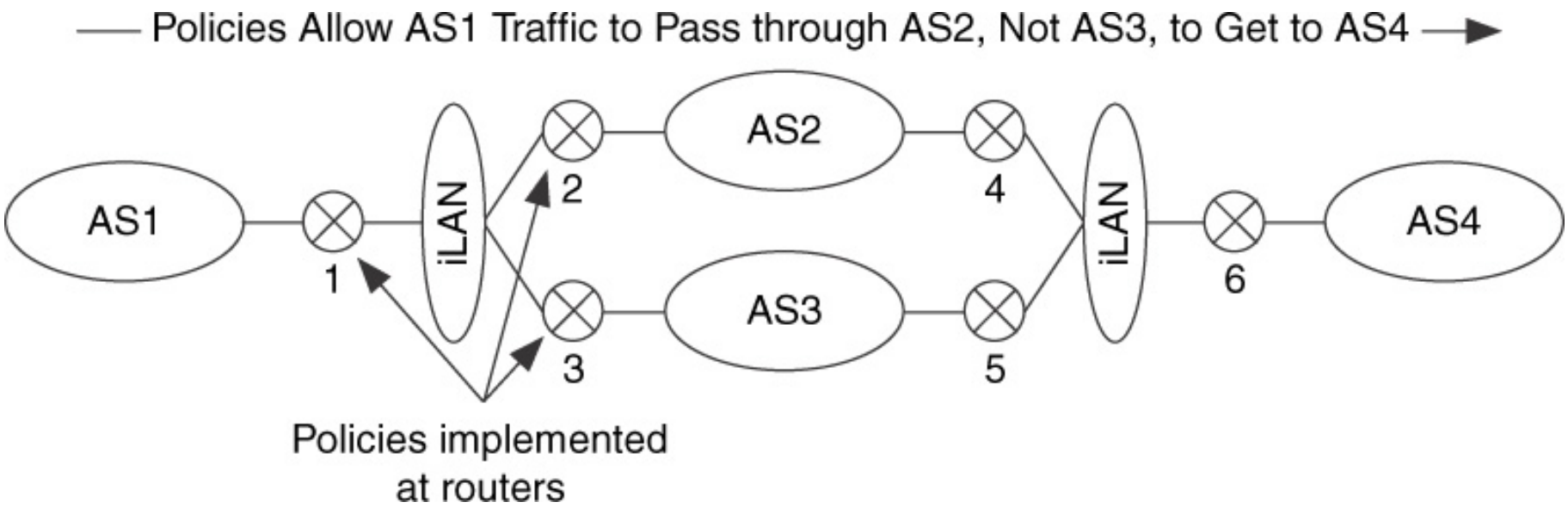


An Example Application of Static Routes, iBGP, eBGP in a Network



Policy enforcement between autonomous systems
An Example

- Routers 2 and 3 enforce a policy that traffic from AS1 must transit AS2 in order to get to AS4, and this traffic cannot transit AS3.



iLAN = isolation LAN

An example of Route Manipulation Technique

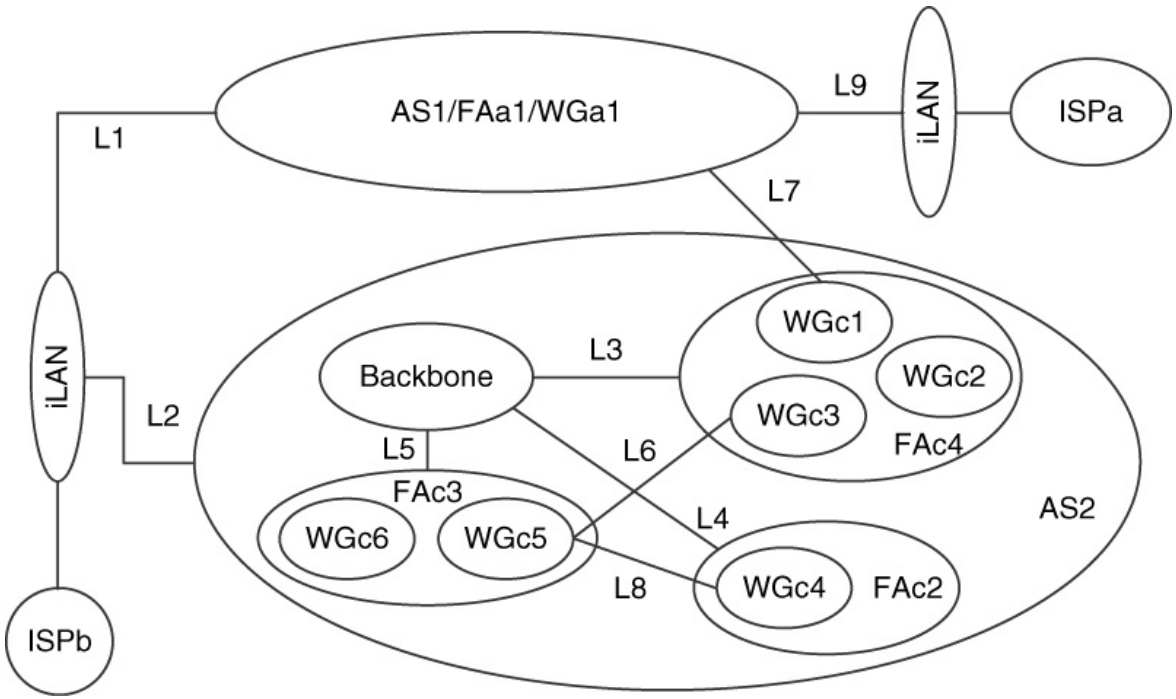
The routing requirements for AS1 are as follows:

1.1. Provide primary Internet access for AS1 through ISPa.

1.2. Provide redundant (secondary) Internet access for AS1 through IPSb.

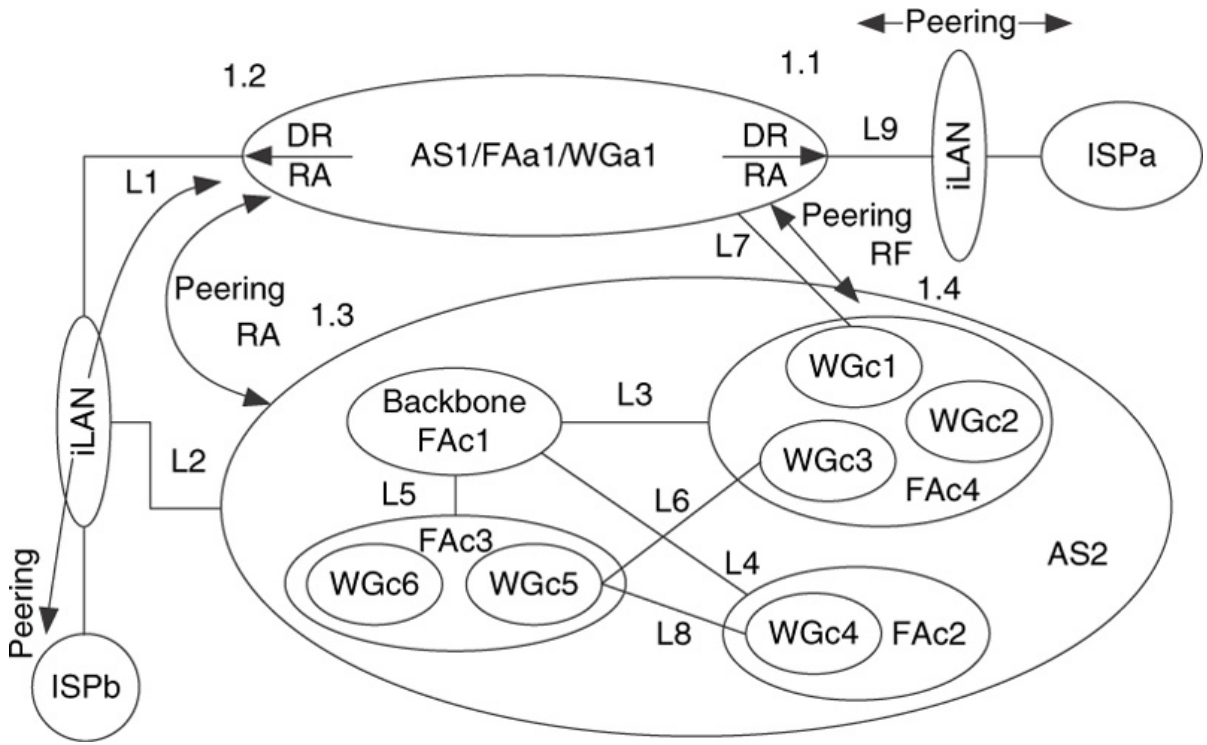
1.3. Allow AS2 traffic to transit AS1 to get redundant Internet access via ISPa.

1.4. Only allow communication between WGa1 in AS1 and WGc1 in AS2 via link L7.



An Example for Route Manipulation Technique – Contd. Route Manipulation Applied to AS1.

- Requirements 1.1. and 1.2. are solved by establishing peering agreements with both ISPa and ISPb. This agreement specifies that ISPa should propagate a default route to AS1 with a lower routing cost than the default route from ISPb to AS1.
- Requirement 1.3. is solved by establishing a peering agreement between AS1 and AS2 via links L1 and L2. AS1 accepts aggregate routes from AS2 and passes them to ISPa at higher cost than through ISPb
- Requirement 1.4. is solved by establishing a peering agreement between AS1 and AS2 via link L7. AS1 accepts route advertisements fromAS2/WGc1 via link L7. Route filter is applied to accept only traffic between WGa1 and WGc1.



1.1. Provide primary Internet access for AS1 is through ISPa.

1.2. Provide redundant (secondary) Internet access for AS1 is through IPSb.

1.3. Allow AS2 traffic to transit AS1 to get redundant Internet access via ISPa.

1.4. Only allow communication between WGa1 in AS1 and WGc1 in AS2 via link L7.

An Example for Route Manipulation Technique-Contd.

The routing requirements for AS2 are as follows:

2.1 Workgroup WGc5 can only communicate with workgroup WGc4 via link L8

2.2 Allow only traffic fromAS1 that is received over link L7 and is destined for workgroup WGc1 to pass; block other traffic

2.3 Allow functional area FAc3 to use functional areaFAc4 as an alternate path to the Internetvia link L6

2.4 Do not allow functional area FAc2 to use functional area FAc3 as an alternate path to the Internet via link L6

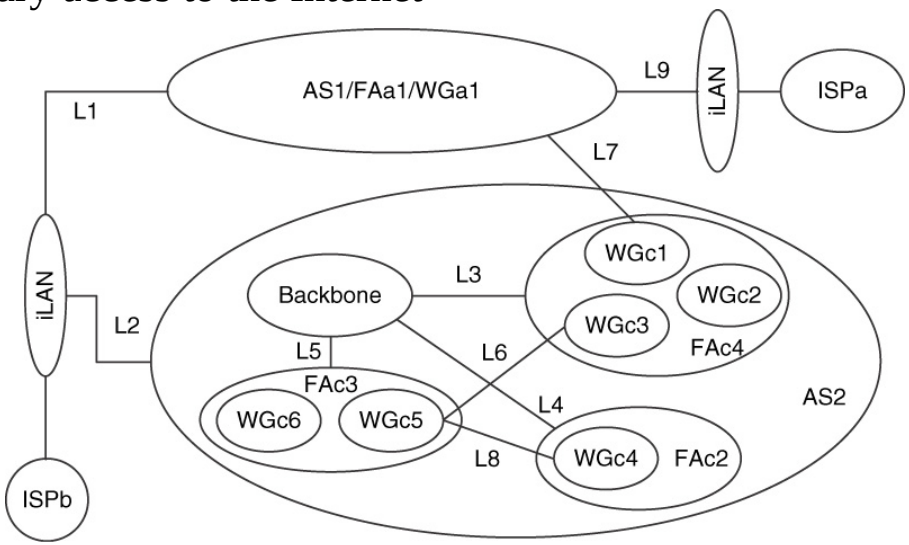
2.5 Do not advertise workgroup WGc2

2.6 Workgroup WGc1 can only communicate withAS1/WGa1 via link L7

2.7 All other functional area must use functional area FAc1 as the default path

2.8 Use AS1 as a transient AS for redundant access to the Internet via ISPa

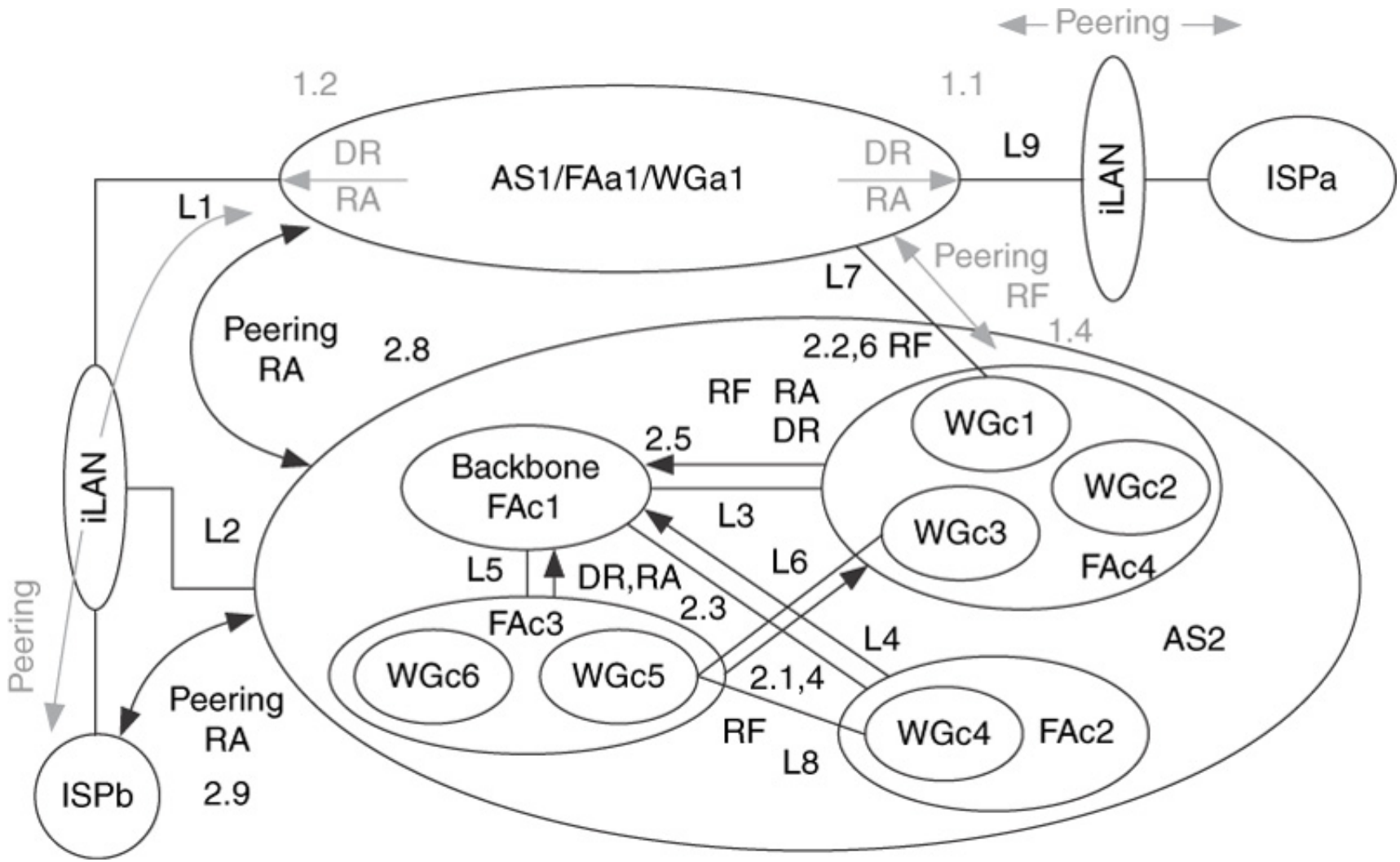
2.9 Use ISPb as a primary access to the Internet



An Example for Route Manipulation Technique – Contd.
Route Manipulation Applied to AS2.

- Requirement 2.1 is solved by applying route filtering at both workgroups WGc5 and WGc4 to force this routing to take place and to prevent other workgroup using link L8
- For requirement 2.2 a peering agreement with AS1 is established , and route filtering is applied at link L7.
- Requirement 2.3 is solved by having functional area FAc4 propagate a default route via link L6 to functional area FAc3 with a higher cost than functional area FAc3 is getting from FAc1.
- In requirement 2.4, route filtering is applied to functional areas FAc2 and FAc3, as was done in problem 2.1.
- For requirement 2.5. route filters are applied at routers that connect to the workgroupWGc2, in order to keep that workgroup from being advertised.
- In requirement 2.6,route filtering is used again, this time to force communications via link L7 Be careful to not allow workgroup WGc1 to use link L7 as access to the Internet.
- In requirements 2.7, FAc1 propagates a default route to all functional areas. All functional areas will appregate route advertisements at the soft boundaries.
- For requirement 2.8 another peering agreement is established with AS1 to allow AS2 to use AS1 as a transit AS to access ISPa in the event that ISPb fails. AS2 must advertise aggregate routes to AS1 with a higher cost than to ISPb.
- In requirement 2.9, a peering agreement is established between ISPb and AS2. AS2 will advertise aggregate routes to ISPb, ISPb will advertise a default to AS2, and ISPb will propagate AS2’s routes to the Internet.

The result of Route Manipulation Technique Applied to AS2



Addressing Strategies

•During the requirements analysis process, you must gather information about devices growth expectations. **Why?**

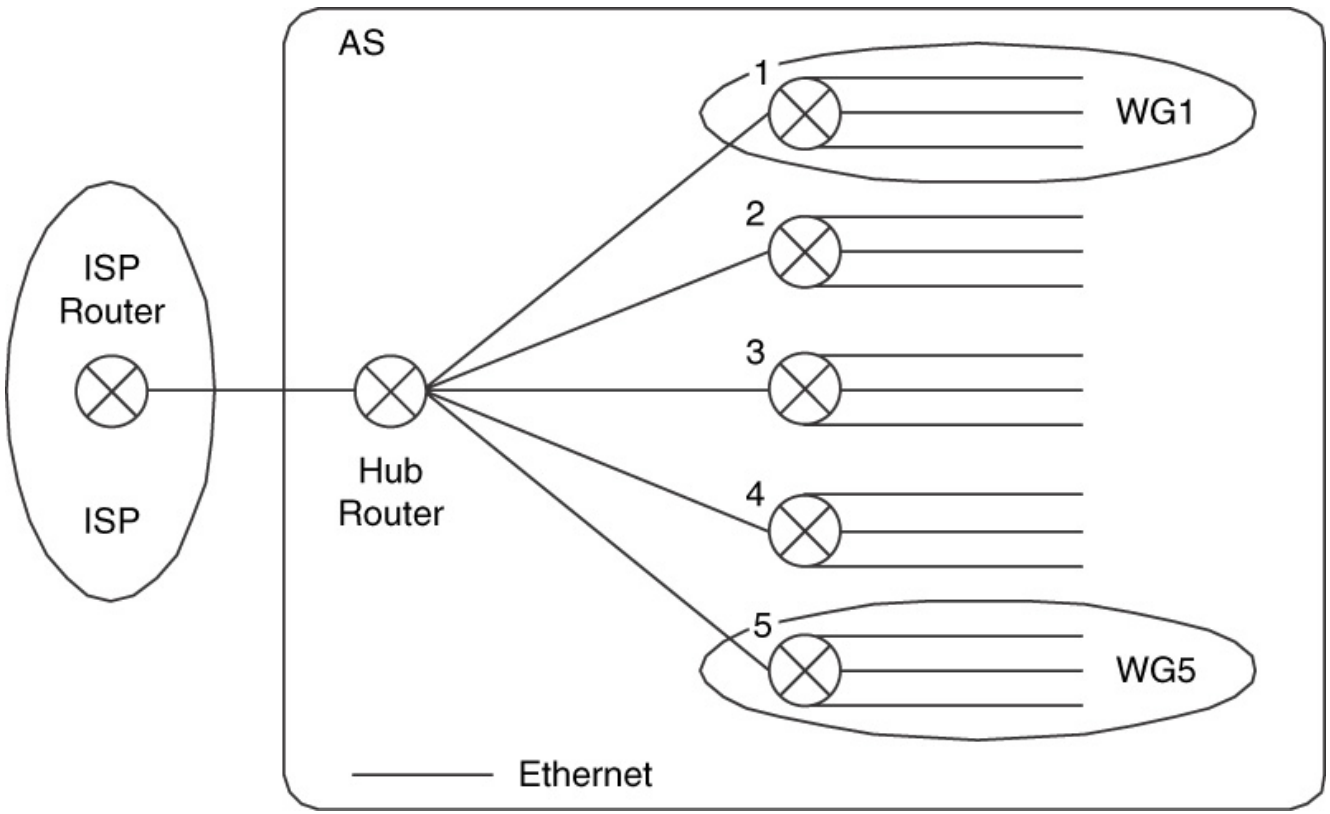
•When applying subnetting, NAT, dynamic addressing, etc. the addressing, masks, and the overall strategy will scale to size as per analysis process.

•To scale the network addressing, we can use one or more of the following addressing strategies where the network is broken into addressing areas along with variable length addressing:

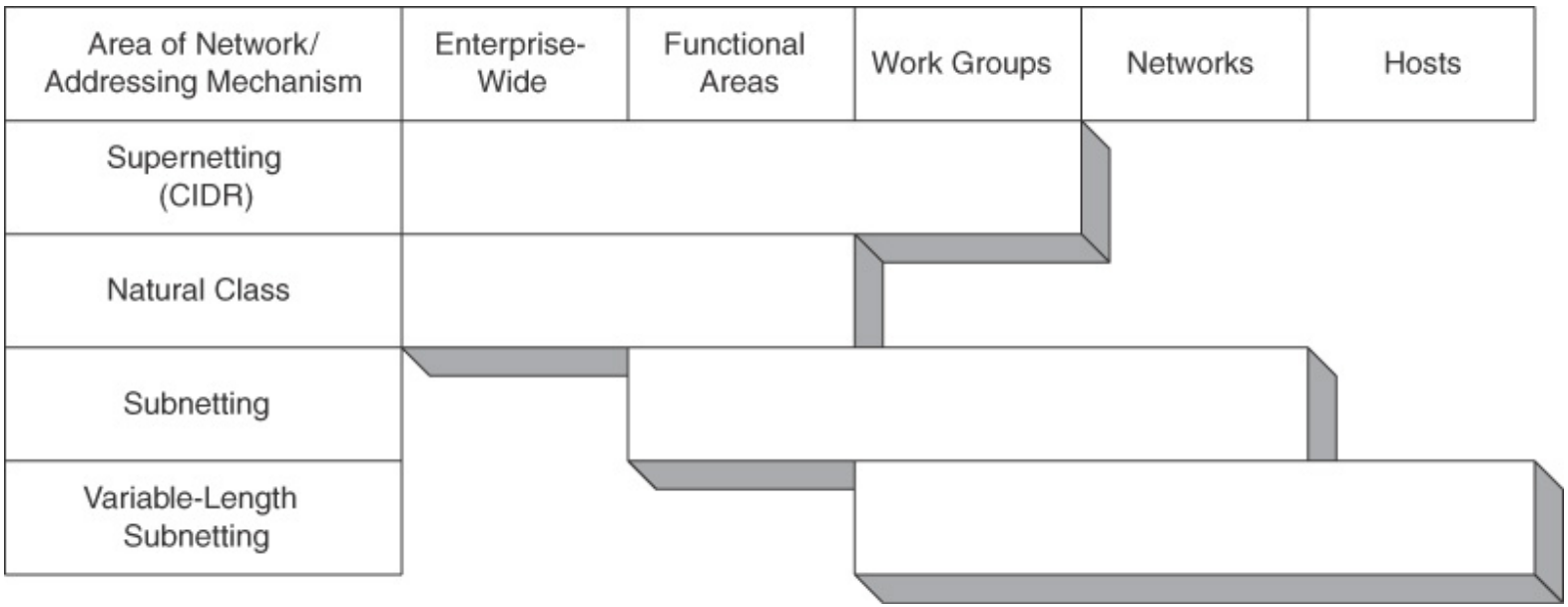
- ✓ use FAs as growth entities within the network
- ✓ Use WGs within each FA as growth entities
- ✓ Use appropriate Subnets within each FA
- ✓ Use total number of subnets (current and future) in the organization for growth
- ✓Use total number of devices (current and future) within each subnet
- ✓Use variable-length subnetting
- ✓Use hierarchies of variable length subnetting (CIDR blocks for growth areas)

Example of Addressing Strategies

- the network is broken into work groups where each group uses variable length subnetting for growth
- Hub router connected to five WGs has the capacity to connect to more, say 10 networks.



Addressing Strategies Application region in Network



Architecture Considerations

- Service-provider networks generally focus on mechanisms such as supernetting, multicasting, routing policies, and peering.
- Enterprise networks generally focus on mechanisms such as NAT, subnetting, VLANs, switching, and the choice and locations of routing protocols.

  Areas of the network where dynamic addressing, private addressing, and NAT mechanisms are applied will affect how routing will (or will not) be provided in those areas.

Architecture Considerations

Internal Relationships

- Depending on the type of network being developed, the set of candidate addressing and forwarding mechanism for a component architecture can be different.
- Addressing and forwarding mechanisms influence the choice of routing protocols and where they are applied.

Architecture Considerations Contd.

External Relationships

•Interactions between Addressing/Routing and Network Management:

- Addressing/routing can be used to configure boundaries for network management.

•Interaction between Addressing/Routing and Performance:

- both can be closely coupled with some mechanisms such as MPLS, resource reservation protocol, and IPv6.

•Interaction between Addressing/routing and Security

Architecture Considerations Contd
External Relationships.

Interactions between Addressing/Routing and Security:

- ✓ Security mechanisms are often intrusive
- ✓Security may require change in routing
- ✓NAT can be used to enhance security and provide private addressing space for a network.
- ✓ Addressing/Routing can affect security in these ways:
  - In terms of accessing the network from the outside (Firewalls, NAT)
  - How protective measures are implemented on servers (e.g., access control lists, restricted access based on IP address and subnet)
  - Ability to trace an attack (the use of dynamic addressing can create problems in tracing network events).