

Table 6-4 *Subnetworks for 172.17.0.0 with 255.255.240.0 Mask*

Third Octet	Subnetwork
00000000	172.17.0.0
00010000	172.17.16.0
00100000	172.17.32.0
00110000	172.17.48.0
01000000	172.17.64.0
01010000	172.17.80.0
01100000	172.17.96.0
01110000	172.17.112.0
10000000	172.17.128.0
10010000	172.17.144.0
10100000	172.17.160.0
10110000	172.17.176.0
11000000	172.17.192.0
11010000	172.17.208.0
11100000	172.17.224.0
11110000	172.17.240.0

The subnetwork 172.27.0.0/28 is used when the **ip subnet-zero** command is configured on the router. Each subnetwork has 12 bits for the host portion. This produces $(2^{12}) - 2 = 4096 - 2 = 4094$ hosts on each subnet. Two is subtracted for the subnet number and the broadcast address number. Looking at Table 6-5 with subnet 172.17.48.0, host addresses will range from 172.17.48.1 to 172.17.63.254, with the subnet broadcast address of 172.17.63.255. Notice that the subnetwork address has 12 0s, and the broadcast address has all 1s as the least significant bits (bolded in Table 6-5).

Table 6-5 *Subnetwork 172.17.48.0*

Type	Binary IP address	Dotted Decimal
Subnetwork	10101100 00010001 0011 0000 00000000	172.17.48.0
First host	10101100 00010001 00110000 00000001	172.17.48.1
Last host	10101100 00010001 00111111 11111110	172.17.63.254
Broadcast	10101100 00010001 0011 1111 11111111	172.17.63.255

Mask Nomenclature

Two ways exist by which to represent a subnet mask. The first format is dotted decimal—for example, 255.255.255.0. Recently, the bit mask number format has become popular. This format represents the subnet mask by using a slash with the number of bits with 1s in the mask. For example, the mask 255.255.255.0 is represented as /24. Table 6-6 shows some mask representations.

Table 6-6 *Subnet Masks*

Dotted Decimal	Bit Mask
255.0.0.0	/8
255.192.0.0	/10
255.255.0.0	/16
255.255.224.0	/19
255.255.240.0	/20
255.255.255.0	/24
255.255.255.128	/25
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

Variable-Length Subnet Masks

Using one of the subnets from Table 6-4 on a point-to-point serial link would be a waste of IP addresses. Only two addresses are needed on a point-to-point serial link; therefore, more than 4000 addresses would be wasted. Variable-length subnet masks (VLSMs) provide the capability to use different masks in a network for different segments. Large LANs could use a /23 mask, for example, for 510 hosts. A serial link could use a /30 mask for two hosts (routers). Not all routing protocols support VLSM; routing protocols will be covered in the “IP Routing Protocols” section later in this chapter.

Take subnet 172.17.48.0/20 from Table 6-4. Subdividing this network using a /23 mask produces eight subnetworks. Table 6-7 displays the results of this example; the bolded bits indicate the 3 bits used to determine subnets

Table 6-7 *VLSM Subnetwork*

Third Octet	Subnetwork
0011 0000	172.17.48.0/23
0011 0010	172.17.50.0/23
0011 0100	172.17.52.0/23

Table 6-7 *VLSM Subnetwork (Continued)*

Third Octet	Subnetwork
0011 0 110	172.17.54.0/23
0011 1 000	172.17.56.0/23
0011 1 010	172.17.58.0/23
0011 1 100	172.17.60.0/23
0011 1 110	172.17.62.0/23

Now take one of these subnetworks and use it for the serial links of the internetwork. Taking 172.17.62.0/23 and subdividing it using a /30 mask produces 128 subnetworks for serial links. Table 6-8 displays the subnets created for serial links. The bolded bits indicate the bits used to determine the subnet numbers.

Table 6-8 *VLSM Subnetworks for Serial Links*

Third Octet	Fourth Octet	Subnetwork
00111110	0000 0 000	172.17.62.0/30
00111110	0000 0 100	172.17.62.4/30
00111110	0000 1 000	172.17.62.8/30
00111110	0000 1 100	172.17.62.12/30
...
00111111	1111 0 100	172.17.63.244/30
00111111	1111 1 000	172.17.63.248/30
00111111	1111 1 100	172.17.63.252/30

To verify the addressing, take one of these subnets and break it down at the bit level. Table 6-9 shows the details for subnet 172.17.62.12/30.

Table 6-9 *Serial Link Subnet Detail*

Type	Binary IP address	Dotted Decimal
Subnetwork	10101100 00010001 00111110 00001100	172.17.62.12
Router 1	10101100 00010001 00111110 00001101	172.17.62.13
Router 2	10101100 00010001 00111110 00001110	172.17.62.14
Broadcast	10101100 00010001 00111110 00001111	172.17.62.15

Supernetting

Just as subnetting provides the capability to subdivide Class A, Class B, and Class C addresses into smaller groups, supernetting groups networks into larger supernets by borrowing bits from the network portion of the address. Say that you want a LAN network to have more than 254 hosts; a class C network is not sufficient. You can group two Class C networks using supernets to provide more IP addresses to the LAN segment without using secondary IP addresses on the router interface. Grouping classfull networks into supernets is considered classless routing.

Take networks 192.168.4.0/24 and 192.168.5.0/24, for example. These are Class C networks with a default mask of 255.255.255.0.

Notice from Table 6-10 that these networks are the same up to 23 bits. They are combined, or supernetted, into one network—192.168.4.0/23. The mask for the new network is 255.255.254.0. The first host address is 192.168.4.1. The last host address is 192.168.5.254. The broadcast address is 192.168.5.255.

Table 6-10 *Two Class C Networks Combined for Supernet*

Binary IP Address	Dotted Decimal
11000000 10101000 00000100 00000000	192.168.4.0
11000000 10101000 00000101 00000000	192.168.5.0

Address Aggregation

A set of classfull networks can also be summarized in routing entries by creating aggregate addresses at the supernet level. Figure 6-2 shows how address aggregation summarizes routes in which Router A sends only one route, 192.168.16.0/21, to its upstream router.

Classless Interdomain Routing

Classless interdomain routing (CIDR) is used in Internet Border Gateway Protocol (BGP) routing to reduce the number of Class C routes coming from an autonomous system. For example, ISPs can allocate blocks of 4, 8, or 16 Class C networks to a customer and use only one route for reachability. In Figure 6-3, the client has a CIDR block of four Class C networks, but Router A announces only 208.10.8.0/22 to the ISP router.

Figure 6-2 *Route Summarization*

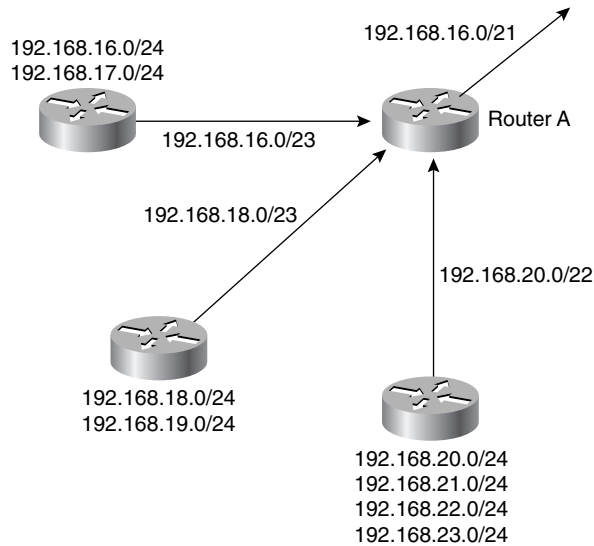
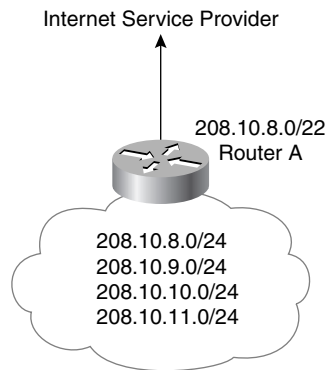


Figure 6-3 *Classless Interdomain Routing (CIDR)*



Addressing Scheme

When assigning addresses to areas, networks, subnetworks, and end stations, it is important to maintain an addressing scheme that can scale as the company grows. Hierarchical network design begins with the addressing scheme. Routers cannot summarize routes if the networks are not assigned within bit boundaries. Assume, for example, that network 172.17.0.0/16 will be used in a medium- to large-sized company with nine areas. Each area could have several sites.

How can the network be divided allowing at least 2000 nodes per area? One method involves dividing the network into 16 areas at the /20 bit boundary. Notice that a /19 bit boundary would provide only eight areas, which would not be sufficient for this exercise. The areas can be classified as in Table 6-11, providing sufficient room for growth.

Table 6-11 *Area Network Assignments per Geographical Region*

Area	Range
Reserved	172.17.0.0/20
North America East	172.17.16.0/20
North America West	172.17.32.0/20
North America Central	172.17.48.0/20
South America	172.17.64.0/20
Japan	172.17.80.0/20
Singapore	172.17.96.0/20
Asia	172.17.112.0/20
Europe West	172.17.128.0/20
Europe East	172.17.144.0/20
Reserved	172.17.160.0/20
Reserved	172.17.176.0/20
Reserved	172.17.192.0/20
Reserved	172.17.208.0/20
Reserved	172.17.224.0/20
Reserved	172.17.240.0/20

Networks within the areas should be assigned based on the expected number of hosts and segments on the networks. Serial links should be assigned a /30 subnet. Using the America East network, 172.17.16.0/20, subdivide into two large LANs with around 1000 hosts each, four medium LANs with 200 hosts, five small LANs with 20 hosts, and reserved addresses for serial links; leave room for future medium and small LANs. Table 6-12 shows one way of how the network can be further divided.

Table 6-12 *America East Subnetwork Assignments*

Subnetwork	Range
Large LAN1	172.17.16.0/22
Large LAN2	172.17.20.0/22
Medium LAN1	172.17.24.0/24
Medium LAN2	172.17.25.0/24

Table 6-12 *America East Subnetwork Assignments (Continued)*

Subnetwork	Range
Medium LAN3	172.17.26.0/24
Medium LAN4	172.17.27.0/24
Medium LAN5 (future)	172.17.28.0/24
Small LAN1	172.17.29.0/27
Small LAN2	172.17.29.32/27
Small LAN3	172.17.29.64/27
Small LAN4	172.17.29.96/27
Small LAN5	172.17.29.128/27
Small LAN6 (future)	172.17.29.160/27
Small LAN7 (future)	172.17.29.192/27
Small LAN8 (future)	172.17.29.224/27
Reserved	172.17.30.0/24
Serial Link1	172.17.31.0/30
Serial Link2	172.17.31.4/30
Serial Link3	172.17.31.8/30
Serial Link4	172.17.31.12/30
Serial Link5	172.17.31.16/30
...	...

LAN Addressing

It is important to design the address assignment for LAN subnets as well. Reserve addresses for the network devices, such as routers, switches, and analyzers. Set aside a range of addresses for statically assigned servers. The rest can be used for dynamically assigned Dynamic Host Configuration Protocol (DHCP) devices. Table 6-13 shows an example.

Table 6-13 *LAN Device IP Assignment for Network 172.17.26.0/24*

Range	Assignment
.1	HSRP (default gateway)
.2	Router 1
.3	Router 2
.4 to .10	LAN switches

continues

Table 6-13 LAN Device IP Assignment for Network 172.17.26.0/24 (Continued)

.11	Protocol analyzer
.15 to .25	Servers
.26 to .34	Printers
.35 to .225	DHCP scope
.226 to .254	Reserved

IP Routing Protocols

The following CCDA objectives are covered in this section:

24	Identify scalability constraints and issues for IGRP, Enhanced IGRP, IP RIP, IPX RIP/SAP, NLSP, AppleTalk RTMP and AURP, static routing, and bridging protocols.
25	Recommend routing and bridging protocols that meet a customer's requirements for performance, security, and capacity.

Routing is the process by which a packet is forwarded from one network to another. Routers perform this function and also maintain tables of reachable networks and corresponding interfaces used to reach those networks. Such a table can be manually entered or dynamically created using information gathered by routing protocols.

This section covers IP routing protocol characteristics and differences.

Static Versus Dynamic Routing

Static routing is the method by which the network administrator manually enters routing entries on the router. The forwarding table is not learned by speaking with other routers on the network; these entries do not change unless the administrator alters them. The main benefit of static routing is that no routing protocol traffic is generated by the router. The drawback is that routers with static routes cannot react to network changes. Static routing is recommended for hub-and-spoke topologies with low bandwidth.

Dynamic routing protocols build routing tables from information received from other routers in the internetwork. In the event of a network change, they can recalculate the best routes to a destination.