System Admin

Class 6 - Networking
by Ian Robert Blair, M.Sc.

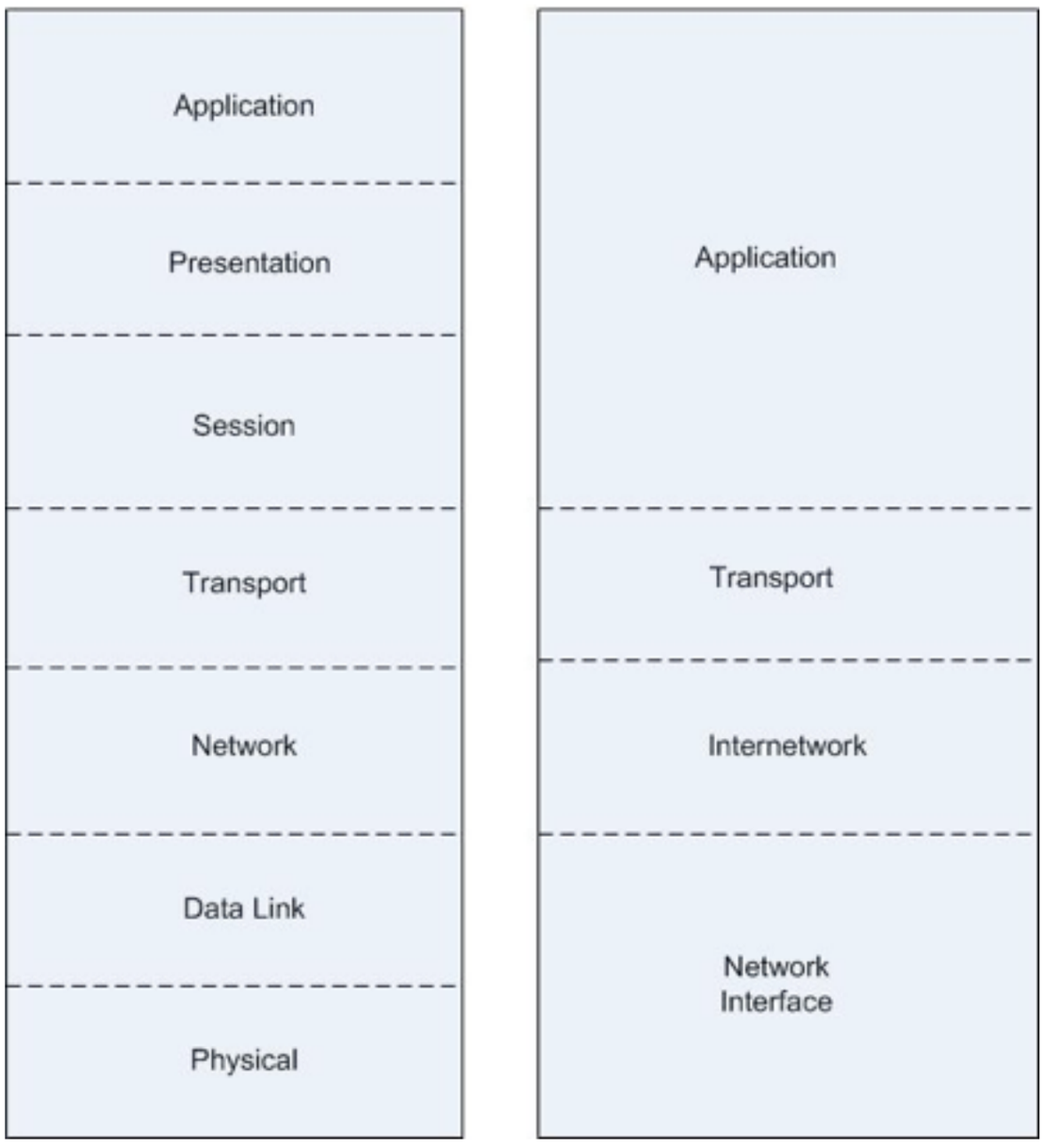
Agenda

- Networking
- DNS DHCP

Networking

OSI and TCP Models

Comparing The OSI Model And TCP / IP Architecture.



Networking Concepts 1

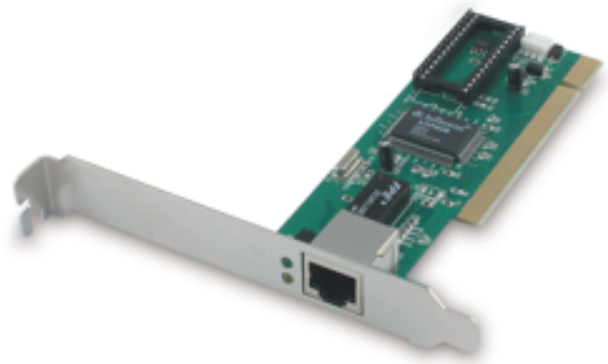
- The **Internet** is a loosely administered network of networks (an internetwork) that links computers on diverse LANs around the globe
- A related term, **intranet**, refers to the networking infrastructure within a company or other institution
- Intranets are usually **private (**protected by a **firewall)**
- An intranet can provide **database, email,** and **Web page** access to a limited group of people, regardless of their geographic location
- You can use an **extranet** (also called a **partner net**) or a **VPN** (virtual private network) to connect sites, partners, and employees securely

Networking Concepts 2

- VPN is also used to connect **remote users** (via the internet)
- A **WAN (wide area network)** covers a large geographic area (over a provider network)
- A **firewall** prevents certain types of traffic from entering or leaving a network
- A **VLAN (virtual local area network or virtual LAN)** is a logical network defined in software on a network device

Networking Concepts 3

- **Ethernet** is the most common topology used in **LANs**, speeds range from 10 megabits per second to 100 gigabits per second
- A modern Ethernet network transfers data using **copper/fiber-optic** cable or **wireless** transmitters and receivers
- Each **NIC(Network Interface Card)** on a system connected to a network has a unique identifier called a **MAC address**, sometimes referred to as an Ethernet address
- The terms 10BaseT, 100BaseT, and 1000BaseT refer to Ethernet over cat-3/4/5/5e/6/7 **UTP** (unshielded twisted pair) cable



Networking Concepts 4

- A **switch is a (Layer 2)** device that establishes a virtual path between source and destination hosts

- To reach a destination address is not on the local network, a packet must be passed on to another network by a **router (Layer 3)**

- A **layer-3** switch is equivalent to a router; it combines features of layer-2 switching and routing

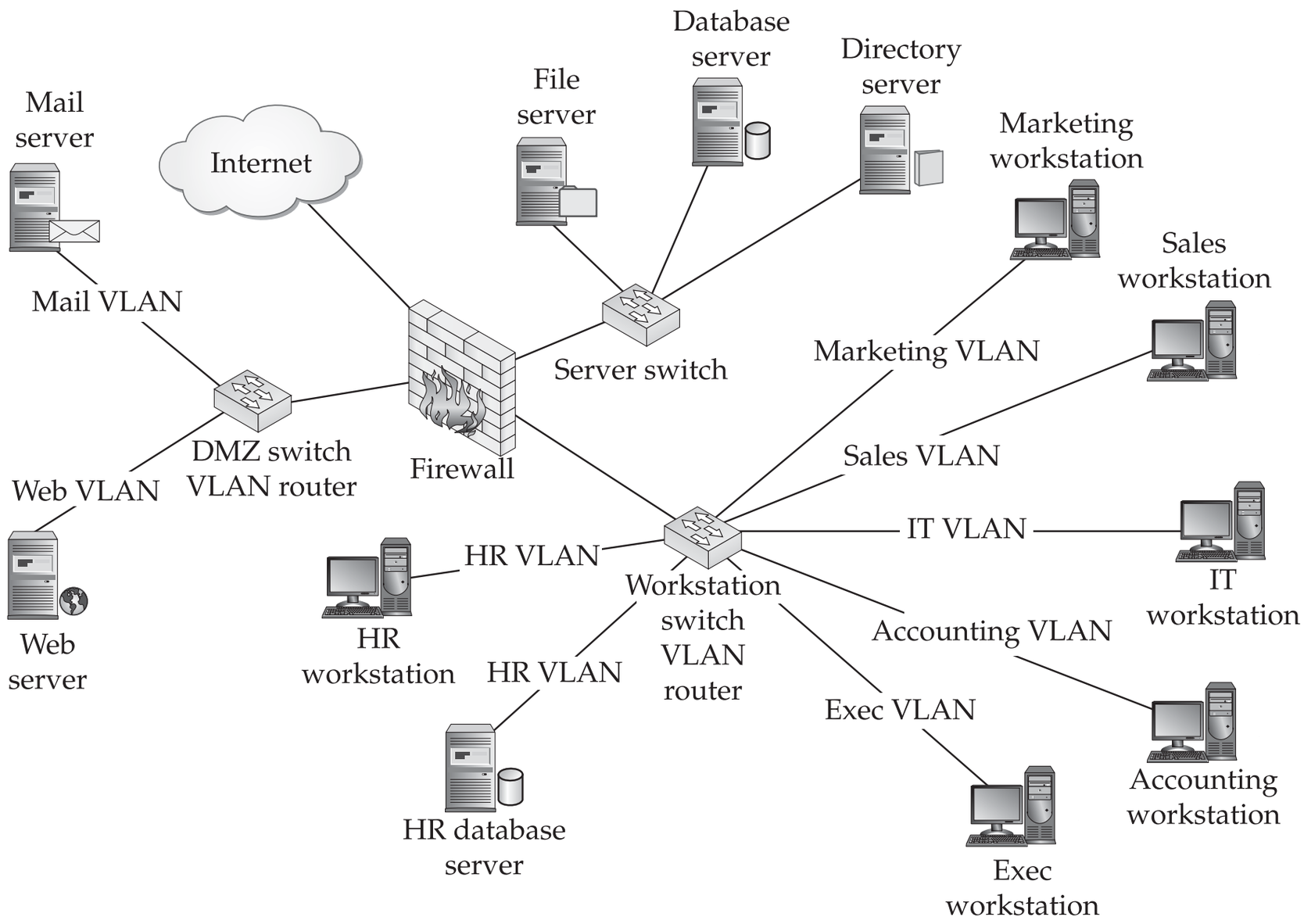
Cisco 3750
Network Switch

Cisco 2800
Network Router

Networking Concepts 5

- **Layer-4** switches inspect higher level packets to make decisions
- Most **Web load balancers** are layer-4 switches
- Network services that require highly reliable connections, such as **ssh** and **scp**, tend to use **TCP/IP** (Transmission Control Protocol)
- Network services that do not require guaranteed delivery but require timely delivery, such as video, audio, and time services, operate using the simpler **UDP/IP** (User Datagram Protocol)

Secure Network with VLANS

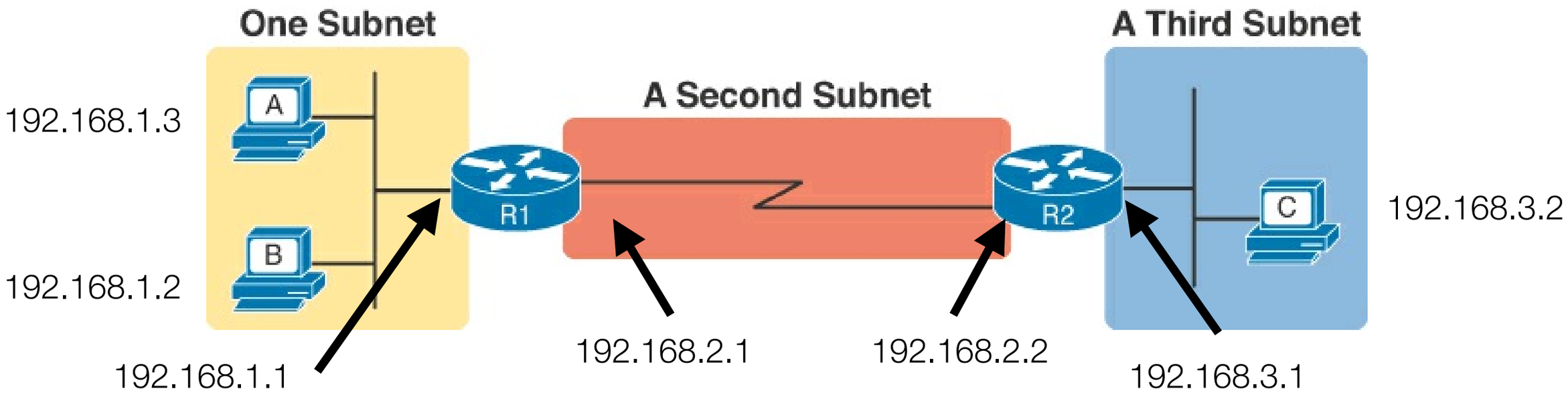


Networking Concepts 6

- Computers communicate over **IP** networks using unique addresses assigned by system software
- An **IP packet** includes the address of the **destination** and the **source** computer
- A **IPv4** network address is a **32-bit address** that is represented as one number broken into four octets separated by periods (for example, 192.168.184.5)
- IPv4 addresses can be divided into a **network**, **subnet**, and **host** sections
- A **subnet mask** (or network mask) is a bit mask that identifies which parts of an IP address correspond to the network address and the host portion of the address

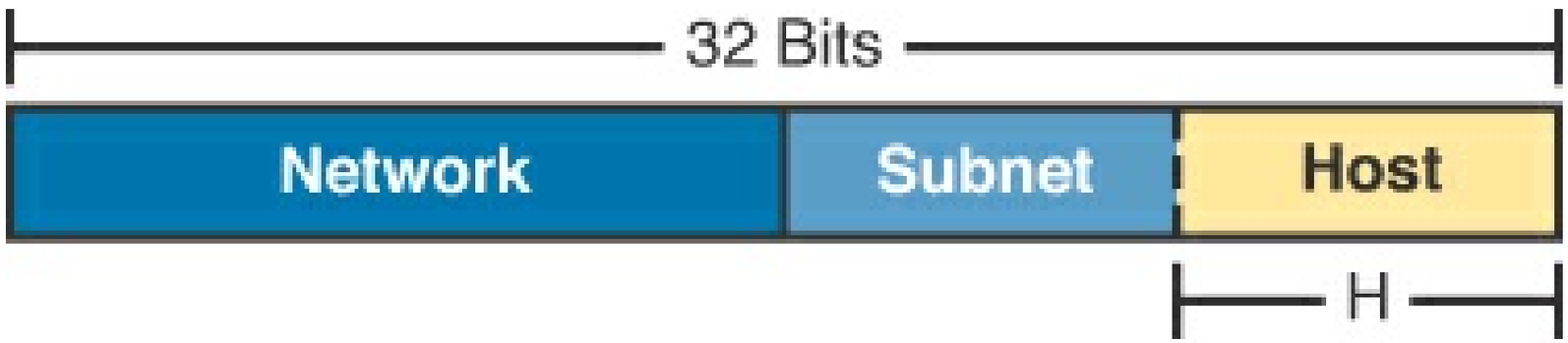
Network Addressing

- Every device that connects to an IP internetwork needs to have an IP address
- This includes:
  - Servers, mobile phones, laptops, desktops, IP phones, tables, routers, switches, firewalls, and network printers
- This network is divided into 3 different subnets



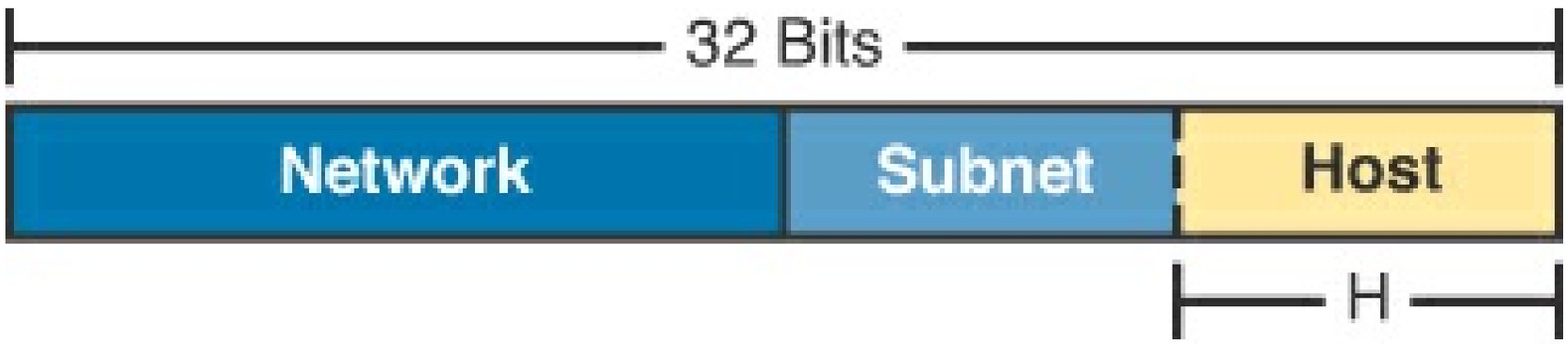
Number of Hosts per Subnet

- The subnet mask determines the size of the subnet
- The mask sets aside a number of host bits
- The number of hosts on a subnet is determined by 2^x-2
- So, a class B address with a subnet mask of 255.255.255.0
  - 16 bits for network
  - 8 bits for subnet
  - 8 for hosts = 2^8 - 2 = 254 possible host addresses



Number of Networks per Subnet

- The number of networks on a subnet is determined by 2^x
- So, a class B address with a subnet mask of 255.255.255.0
  - 16 bits for network
  - 8 bits for subnet
  - 8 bits for subnet = 2^8 = 256 possible subnets



Broadcast and Range

- The **broadcast address** is a reserved number in each subnet that, when used as the destination address of a packet, is forwarded all hosts in that subnet
- The broadcast is the highest number in the subnet
- The **range** is the first usable IP address in a subnet to the last usable address
- So, for example:
  - If 192.168.1.0 is the network ID
  - **Subnet mask** is 255.255.255.0
  - The **broadcast** is 192.168.1.255
  - The **range** is 192.168.1.1 - 254

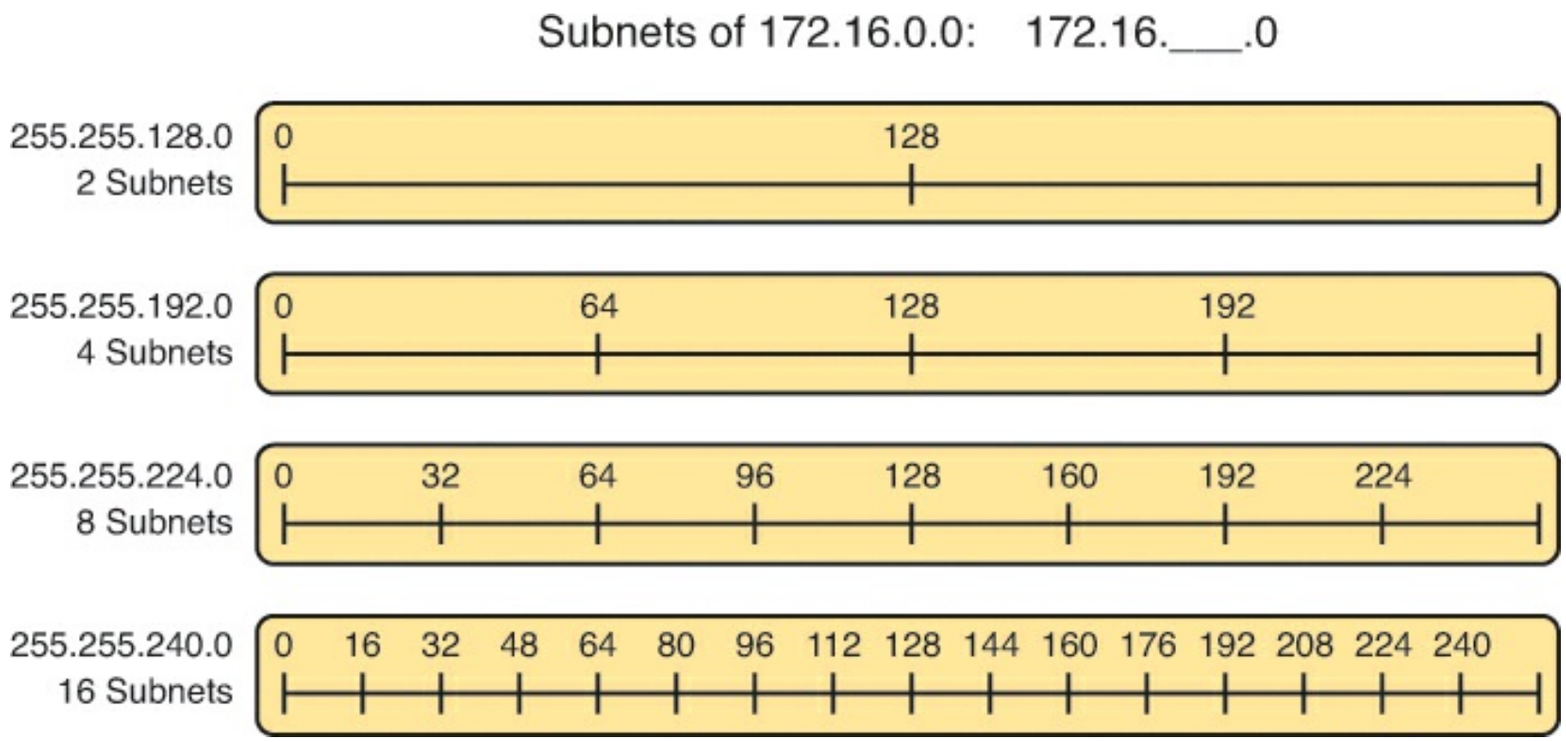
Practice 1

- What is the subnet ID, range, and broadcast for these IP Addresses?

192.168.6.54	255.255.255.0
10.77.3.14	255.255.0.0
172.22.55.77	255.255.0.0
1.99.53.76	255.0.0.0

Subnets, pt. 2

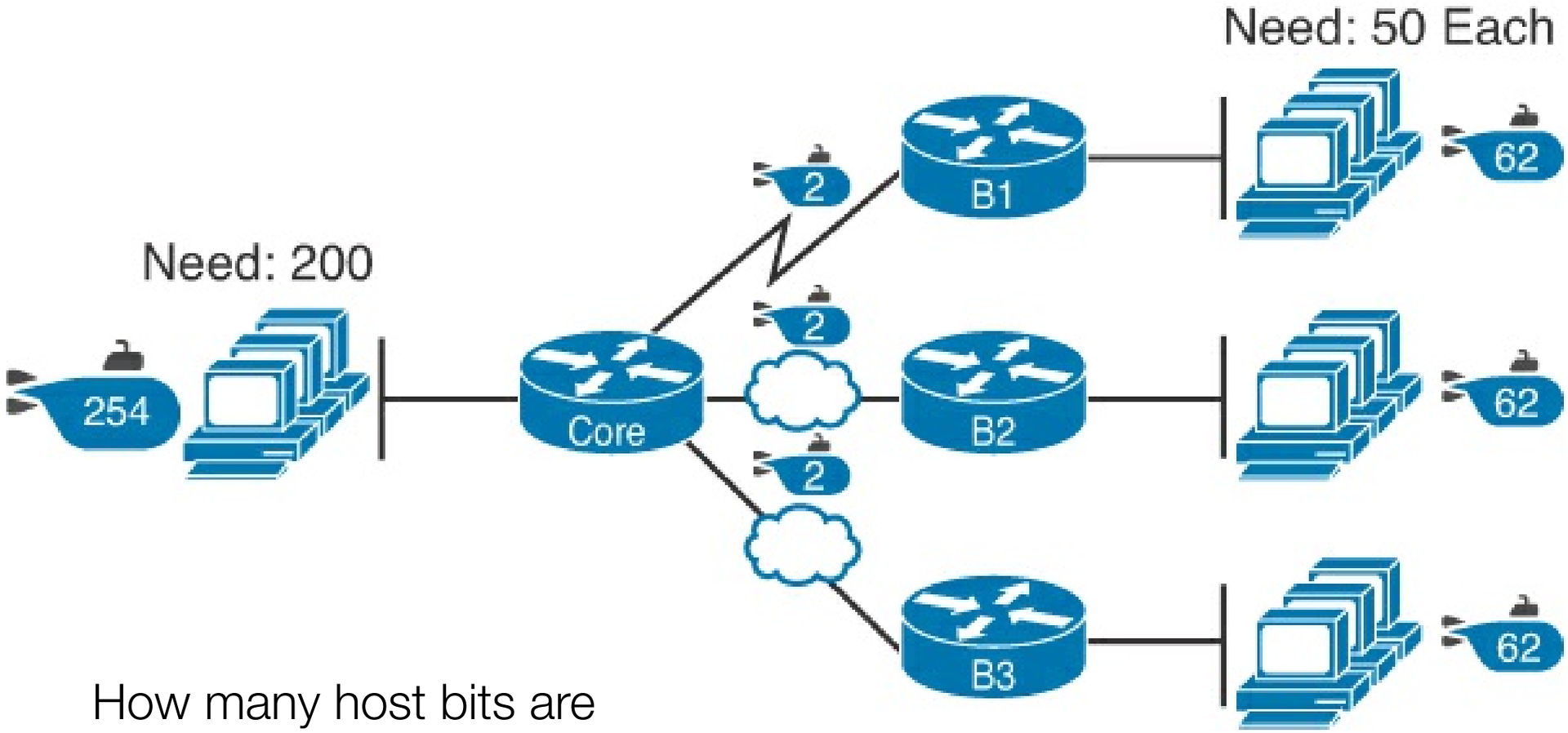
- To find a network ID for a more complex subnet, start with a IP address and mask
- Calculate the boundaries of the subnets (256 - mask)
- Locate the one that the address is within



Practice

Problem	IP Address	Mask	Subnet ID
1	10.77.55.3	255.248.0.0	
2	172.30.99.4	255.255.192.0	
3	192.168.6.54	255.255.255.252	
4	10.77.3.14	255.255.128.0	
5	172.22.55.77	255.255.254.0	
6	1.99.53.76	255.255.255.248	

Intro to VLSM



How many host bits are required for these subnets?

Possible Subnet Values

Binary Mask Octet	Decimal Equivalent	Number of Binary 1s
00000000	0	0
10000000	128	1
11000000	192	2
11100000	224	3
11110000	240	4
11111000	248	5
11111100	252	6
11111110	254	7
11111111	255	8

Sample Conversions

Binary Mask	Logic	Decimal Mask
11111111 11111111 11000000 00000000	11111111 maps to 255 11000000 maps to 192 00000000 maps to 0	255.255.192.0
11111111 11111111 11111111 11110000	11111111 maps to 255 11110000 maps to 240	255.255.255.240
11111111 11111000 00000000 00000000	11111111 maps to 255 11111000 maps to 248 00000000 maps to 0	255.248.0.0

Decimal Mask	Logic	Binary Mask
255.255.192.0	255 maps to 11111111 192 maps to 11000000 0 maps to 00000000	**11111111 11111111 11**000000 00000000
255.255.255.240	255 maps to 11111111 240 maps to 11110000	**11111111 11111111 11111111 1111**0000
255.248.0.0	255 maps to 11111111 248 maps to 11111000 0 maps to 00000000	**11111111 11111**000 00000000 00000000

Networking Concepts 7

- **IPv6** uses a **128-bit address** space, expressed as eight sets of four hexadecimal digits, each set separated from the next by a colon (IPv6 address 2001:4860:800a: 0000:0000:0000:0000:0067 or 2001:4860:800a::67)
- IPv6, the **network prefix** is always **64 bits**, and the **host section** is always the remaining **64 bits** (last 16 bits of the network prefix can be used for subnet)

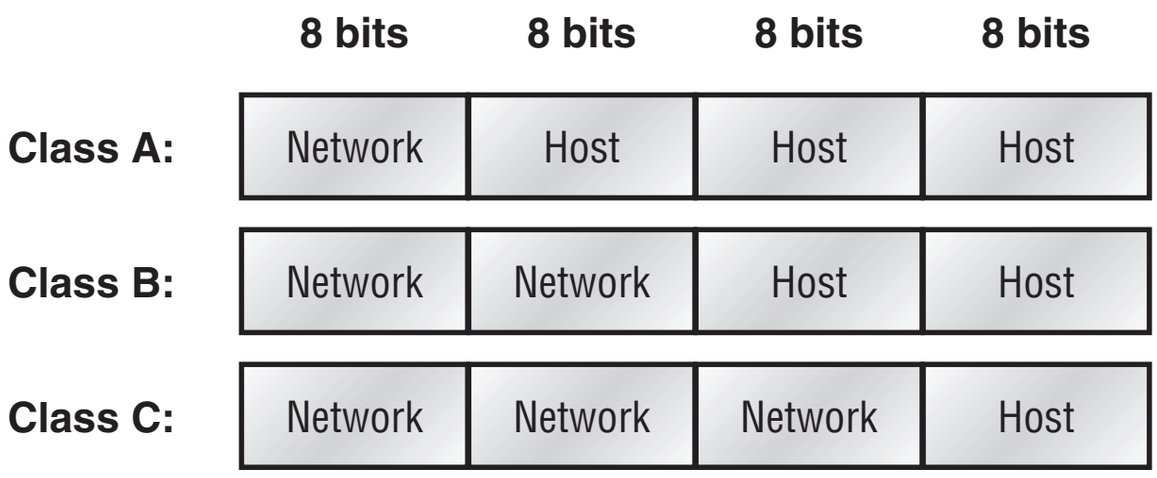
Networking Concepts 8

- **ARP (Address Resolution Protocol)** is a method for finding a host's MAC (Ethernet) address from its IP address on the same subnet
- Each host builds an **ARP cache** that holds a map that translates IP addresses into MAC addresses
- Packets that have a destination on another network are sent to the **router (default gateway)** on the local network
- A **static IP address** is one that always remains the same (servers)
- A **dynamic IP address** is one that is allocated (leased) to a client and that has a defined expiration time (clients)

Networking Concepts 9

- **Ports** are logical channels (numbered from 1 to 65,535)
- **Services** are associated with specific ports, generally with numbers less than 1024 (privileged ports)
- Commonly used ports include:
  - 22(SSH), 23 (TELNET), 80 (HTTP), 20/1(FTP), 25 (SMTP), 53 (DNS), 67/8 (DHCP), 69 (TFTP), 110 (POP3), 115 (SFTP), 123 (NTP), 61 (SNMP), 143 (IMAP), 389 (LDAP), 443 (HTTPS), 636 (LDAPS), 993 (IMAPS), 995 (POP3S)

IPv4 Address Ranges



Class D: Multicast

Class E: Research

Class	Range	Networks	Hosts
A	0-127	126	16,777,216
B	128-191	16,384	65,534
C	192-223	2,097,152	254
D	224-239	n/a	n/a
E	240-255	n/a	n/a

IPv4 Private Addresses

- Class A
  - 10.0.0.0 through 10.255.255.255
- Class B
  - 172.16.0.0 through 172.31.255.255
- Class C
  - 192.168.0.0 though 192.168.255.255

IPv4 Why Subnet?

- Sub-netting allows you to take one larger network and break it into a bunch of smaller networks
- It has the following benefits:
  - Reduced Network Traffic
  - Optimized network performance
  - Simplified management
  - Facilitated spanning of large geographical distances

Classless Inter-Domain Routing (CIDR)

- A /8
- B /16
- C /24

Name Resolution

- Linux provides several ways to associate hostnames with IP addresses:
  - **/etc/hosts file**
  - DNS Server

More Important Files 3

- **/etc/resolv.conf** - lists DNS servers, domain search path
- **/etc/services** - lists system services
- **/etc/sysconfig** - (directory) contains a hierarchy of system configuration files

Information and Location Commands

Usage	Description	Popular Options
`telnet`	used to open a remote console, is older than ssh and is **not secure**, but some legacy devices do not support ssh (network devices and terminals)	
`ping and ping6`	utilities send an ECHO_REQUEST packet to a remote computer to test connectivity	`-c (count)`
`w, who, finger user`	Displays detailed information about users	
`hostname`	Displays the name of the local system	
`Traceroute/ traceroute6`	utilities trace the route that an IP packet follows to its destination (called network hops)	
`ssh user@host`	secure shell client	

Configure Network

- Configuration for each server system: IP address, network mask, gateway address, DNS server addresses, system hostname
- Right-click the **NetworkManager** applet to display a menu that allows you to configure networking (nmtui, text mode)
- You can perform the same task by by editing the appropriate configuration file in **/etc/sysconfig/network-scripts**
  - `vi /etc/sysconfig/network-scripts/ifcfg-Auto_eth0`

Network Configuration (Manual)

```
DEVICE="eth0"
HWADDR="00:21:70:10:7E:CD"
NM_CONTROLLED="no"
ONBOOT="yes"
BOOTPROTO=static
# BOOTPROTO=dhcp
IPADDR=10.16.1.106
NETMASK=255.255.255.0
#   the GATEWAY is sometimes in: /etc/sysconfig/network
GATEWAY=10.16.1.1
```

/etc/sysconfig/network (Manual Config)

```
HOSTNAME=acme.example.com
DNS1=10.16.1.112
DNS2=8.8.8.8
## DNS2=76.242.0.28
SEARCH=example.com
```

Adding Routes

- Temporary routes can be added with:
  - `ip route add 192.0.2.1 via 10.0.0.1`
- Persistent routes can be added via `/etc/sysconfig/network-scripts/route-enp0s3`:
  - `default via 192.168.1.1`
  - `10.10.10.0/24 via 192.168.1.1`

IP Command

- `ip addr show`
- `ip route show`
- `ip link show`
  - `ip -s link`
- `ifconfig and route (deprecated)`

Other Commands

- `ethtool`
- `ifdown, ifup`
  - For example, use the command, `ifup enp0s3,` to bring it up
- When you make changes to the network configuration, you must bring the interface down, then up or use: `systemctl restart network`

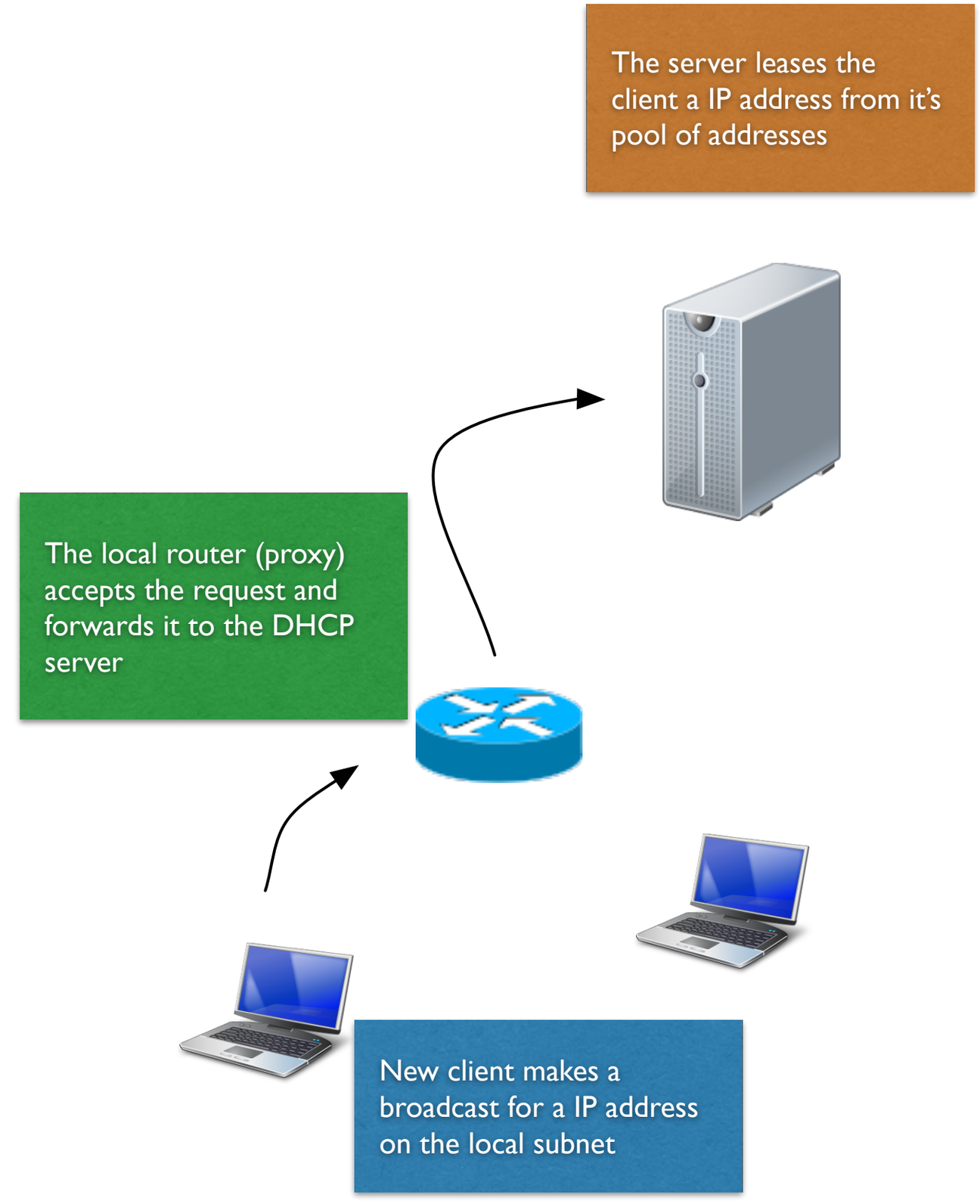
Netstat

- **Netstat** command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, and multicast memberships
  - List all ports use, `netstat -a`
  - List all tcp/udp ports use, `netstat -at(u)`
  - List only listening TCP Ports use, `netstat -lt`
  - Show statistics for all ports use, `netstat -s`
  - `-p` option will add the “PID/Program Name” to the netstat output

DHCP/DNS

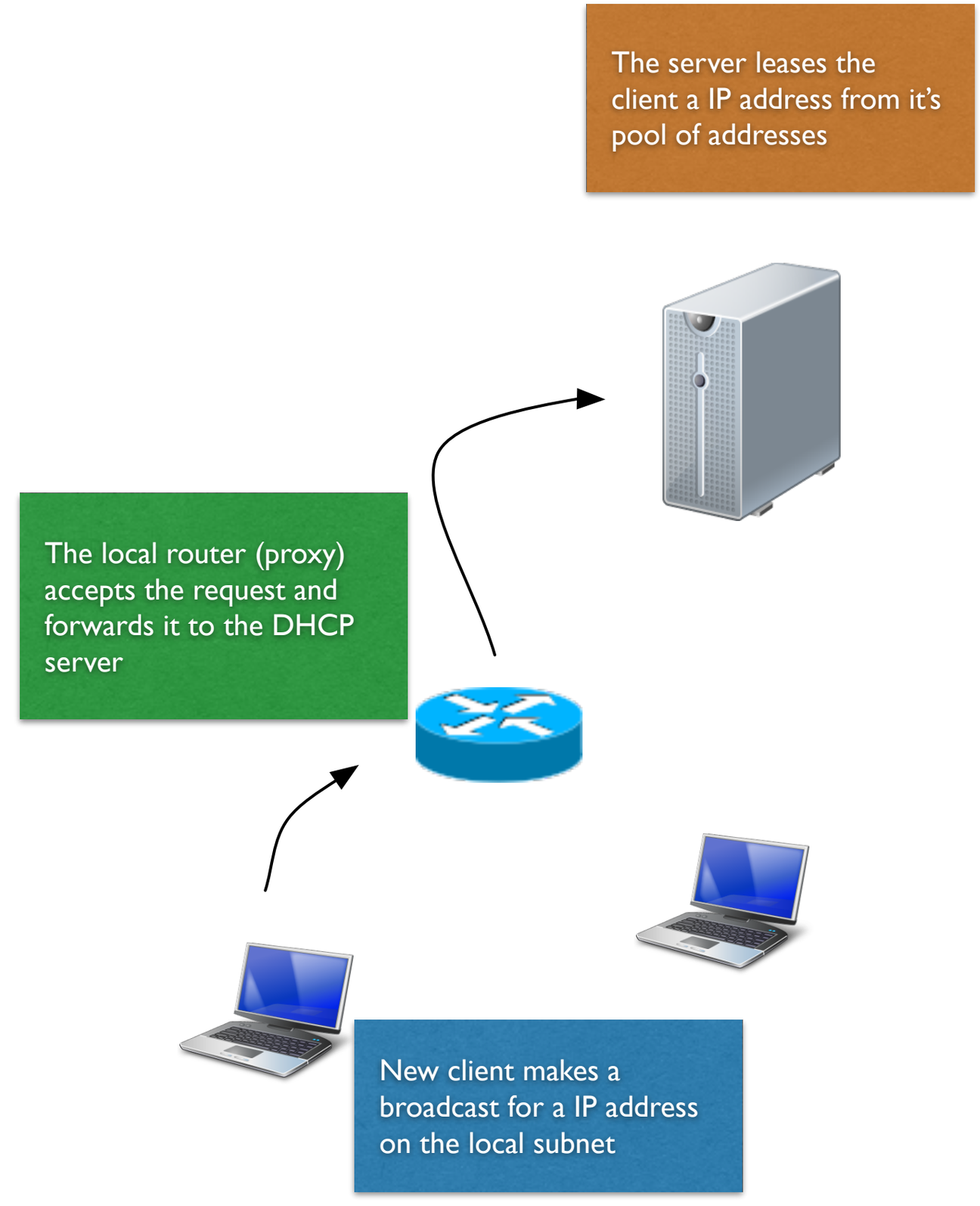
DHCP

- The **dhclient (dhclient package)** contacts the server daemon, dhcpd, to obtain the IP address, netmask, broadcast address, nameserver address, and other networking parameters
- The **server (dhcp package)** leases an IP address to the client
- Once a DHCP client has requested and established a lease, it stores the lease information in a file named **dhclient-*-interface.lease**, which resides in the `/var/lib/dhclient` directory



DHCP

- The DHCP client configuration file (optional), `/etc/dhcp/dhclient.conf`, is required only for custom configurations
- DHCP server configuration in `/etc/dhcp/dhcpd.conf`
- Server leases can be found in `/var/lib/dhcpd`



DHCP Options

- Subnet mask
- Router
- DNS Servers
- Domain name
- Lease time

DHCP Configuration

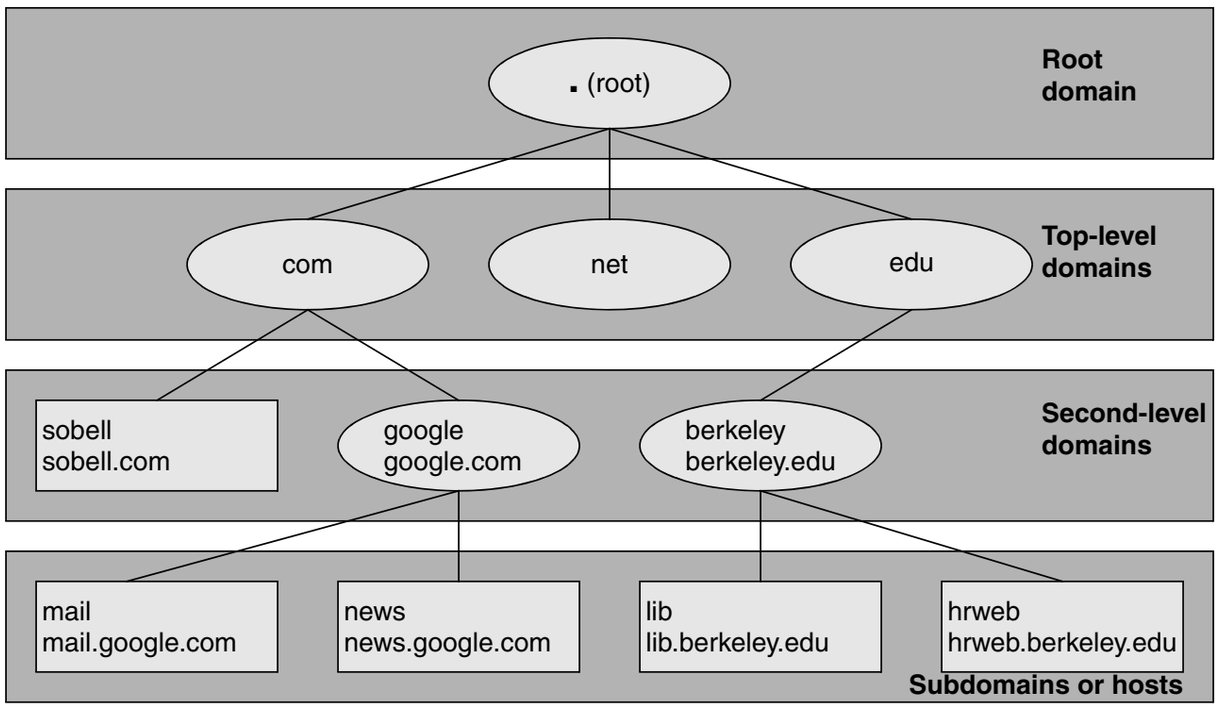
```
default-lease-time 600;
max-lease-time 7200;

shared-network name {
    option domain-search                "test.company.com";
    option domain-name-servers      ns1.company.com, ns2.company.com;

    subnet 192.168.1.0 netmask 255.255.252.0 {
        option routers                      192.168.1.254;
        range 192.168.1.50 192.168.1.253;
    }
    subnet 192.168.2.0 netmask 255.255.252.0 {
        option routers                      192.168.2.254;
        range 192.168.2.50 192.168.2.253;

         host laser-printer-lex1 {
                hardware ethernet 08:00:2b:4c:a3:82;
                fixed-address 192.168.2.120;
        }
    }
```

DNS 1

- **DNS (Domain Name System)** maps domain names to IP addresses, and vice versa
- DNS provides a means for routing email
- Under DNS, name servers work with clients, called resolvers, to distribute host information in the form of resource records in a timely manner as needed
- DNS is:
  - Hierarchical, DNS has a root, branches, and nodes
  - Distributed, so it offers fast access to servers
  - Replicated, to enhance reliability
- DNS was specified in 1983 and BIND (most popular) became part of BSD in 1985

DNS 2

- In addition, DNS is:
  - Secure, so your browser or email is directed to the correct location
  - Flexible, so it can adapt to new names, deleted names, and names whose information changes
  - Fast, so Internet connections are not delayed by slow DNS lookups



DNS 3

- A **fully qualified domain name (FQDN)** is a pointer that positively locates a host or a domain on the Internet or network
- Put the domain names, in the order you want them tried, after the search keyword in `/etc/resolv.conf`
- Hostnames can contain characters from the set a–z, A–Z, 0–9, and –, in addition can include various accents, umlauts, and so on (c. 2004)
- DNS considers uppercase and lower-case letters to be the same (it is not case sensitive)

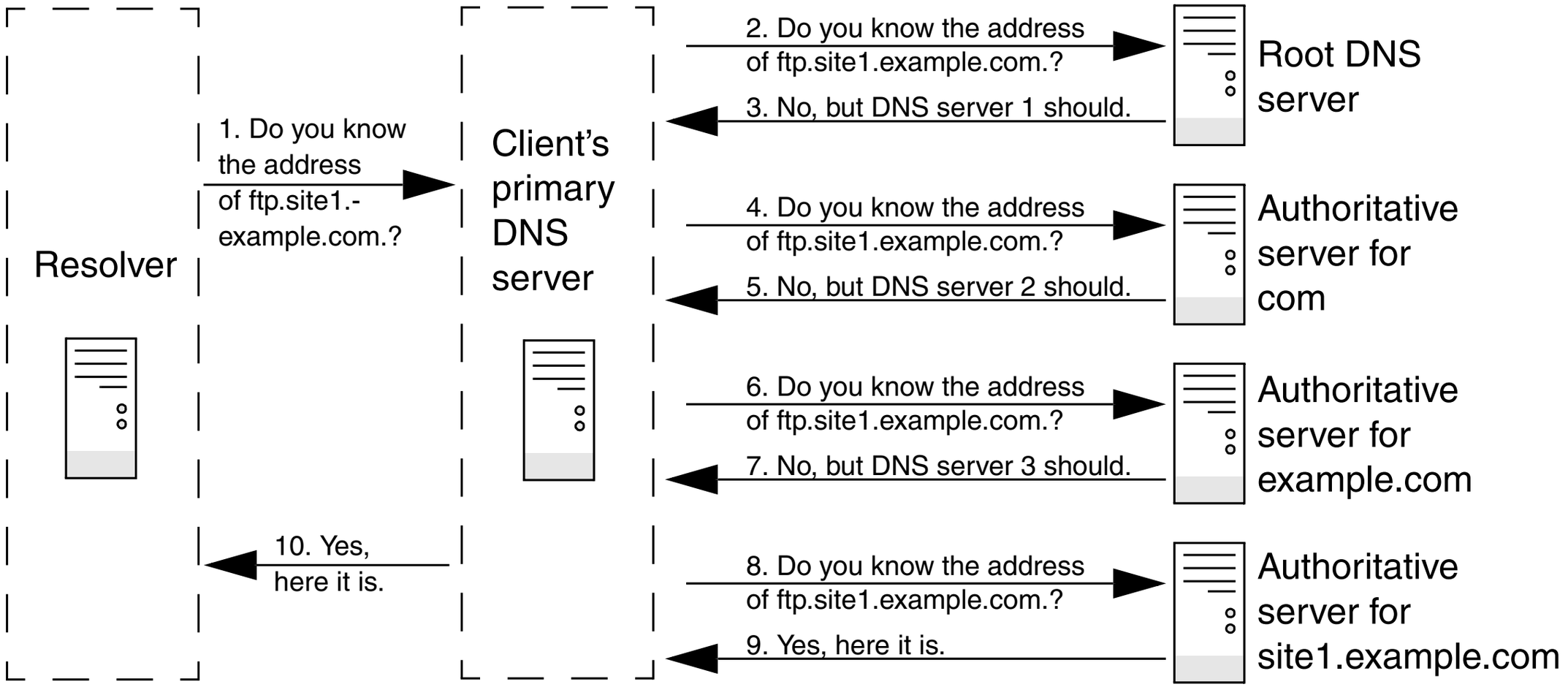
DNS Zones

- For administrative purposes, domains are grouped into **zones** that extend downward from a domain
- Information about zones originates in **zone files**, one zone per file
- Each zone has at least one **authoritative** DNS server which holds all information about the zone
- A DNS **query** returns information about a domain and specifies which DNS server is authoritative for that domain

DNS Queries

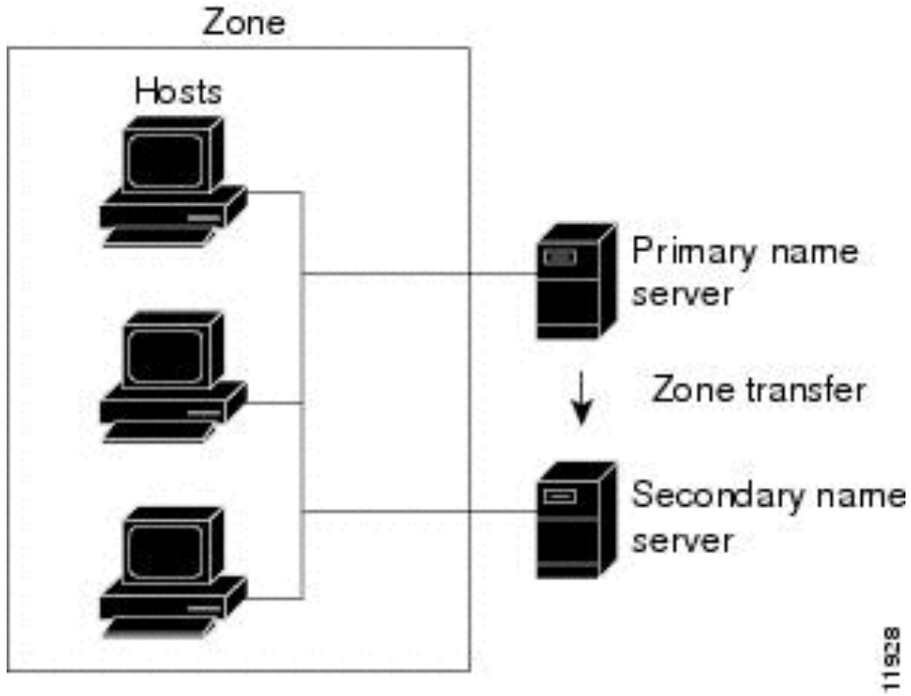
- There are two types of DNS queries: **iterative** and **recursive**
- **Nameservers** (DNS Servers) typically send each other iterative queries
- An **iterative** query sends a domain name to a DNS server and asks the server to return either the IP address of the domain or the name of the DNS server that is authoritative for the domain or one of its parents
- A **recursive** query sends a domain name to a DNS server and asks the server to find the IP address of the domain by querying other servers to get the answer

DNS Resolving



DNS Server Types

- A **primary master** server, also called a primary server or master server, is the authoritative server that holds the master copy of zone data
- **Slave servers**, also called secondary servers, are authoritative and copy zone information from the primary master server or another slave server
- When information on the primary master server changes, the primary master server **notifies** the slave servers (executes a zone transfer to copy the new zone information)



DNS Server Types

- **DNS caches**, also called caching-only servers, are not authoritative
- When a DNS cache receives a query, it answers it from cache (memory) if it can
- If the DNS cache does not have the answer in cache, it forwards the query to an authoritative server

Resource Record Types, pt. 1

- **A** - IPv4 Address
  - `ns IN A 192.168.0.1`
- **AAAA** - IPv6 Address
  - `ns IN AAAA 2001:630:d0:131:a00:20ff:feb5:ef1e`
- **CNAME** - Canonical Name Maps an alias or nickname to a domain name
  - `ftp IN CNAME www.sam.net.`
- **MX** - Mail Exchange Specifies a destination for mail addressed to the domain
  - `speedy IN MX 10 mail`
  - `IN MX 20 mail.sam.net.`
- **NS** - Nameserver Specifies the name of the system that provides domain service (DNS records) for the domain
  - `peach IN NS ns.max.net.`

Resource Record Types, pt. 2

- **PTR** - Pointer Maps an IP address to a domain name and is used for reverse name resolution
    - `3 IN PTR peach`
- **SOA** - Start of Authority Designates the start of a zone

```
@ IN SOA ns.zach.net. mgs@sobell.com. (
                  2010111247 ; serial
                  8H                  ; refresh
                  2H                  ; retry
                  4W                 ; expire
                  1D)                 ; minimum
```

Resource Record Types, pt. 3

- The **$TTL** directive specifies the default zone TTL (the maximum amount of time data stays in a slave server's cache)

- **TXT** - Text Associates a character string with a domain

  - `zach.net. IN TXT "Sobell Associates Inc."`

Linux/Unix Network Utilities

- **host** utility looks up an IP address for a hostname, or vice versa
  - `host 209.157.128.22`
- **Dig** (domain information groper) utility queries DNS servers and individual machines for information about a domain
  - `dig @127.0.0.1 www.sobell.com`
  - `dig -x 209.157.128.22`

Install Bind

- Install bind, bind-utils, system-config-bind (gui), bind-chroot (for chrooted bind) packages, and run:
  - `systemctl enable bind`
  - `systemctl start bind`

- **Reload** named configuration files without disturbing clients connected to the server
- The named server accepts queries on TCP and UDP port **53**
- **bind-chroot** package sets up named to run in a chroot jail
- Named configuration file `/etc/named.conf`
- Messages generally appear in `/var/log/messages`

named.conf, pt. 1

- allow-query {IP-list}, Allows queries from IP-list only
- allow-recursion {IP-list}, Specifies systems for which this server will perform recursive queries
- allow-transfer {IP-list}, Specifies systems that are allowed to perform zone transfers from this server
- directory path, Specifies the absolute pathname of the directory containing the zone files.
- forward ONLY|FIRST, ONLY forwards all queries and fails if it does not receive an answer. FIRST forwards all queries and, if a query does not receive an answer, attempts to find an answer using additional queries
- forwarders {IP [port] [; ...]}, Specifies IP addresses and optionally port numbers that queries are forwarded to

named.conf, pt. 2

- notify YES|NO, YES sends a message to slave servers for the zone when zone information changes
- recursion YES|NO, YES (default) provides recursive queries if the client requests. NO provides iterative queries only

  The Following are within the Zone clause:

- allow-update {IP-list}, Specifies systems that are allowed to update this zone dynamically
- file filename, Specifies the zone file—the file that specifies the characteristics of the zone.
- masters (IP-list), Specifies systems that a slave zone can use to update zone files. Slave zones only.
- type ztyp,Specifies the type of zone defined by this clause (forward, hint, master, slave)

Zone File

- By default, the zone files reside in `/var/named`
- Slave zone files should be kept in `/var/named/slaves`, which is owned by named and is writable by processes running with a UID of named
- For chrooted named, `/var/named/chroot/etc/named.conf` and `/var/named/chroot/var/named`

Zone File

```
$TTL  86400 ; 24 hours could have been written as 24h or 1d
$ORIGIN example.com.
@  1D  IN    SOA ns1.example.com.   hostmaster.example.com. (
               2002022401 ; serial
               3H ; refresh
               15 ; retry
               1w ; expire
               3h ; minimum
              )
       IN  NS     ns1.example.com. ; in the domain
       IN  NS     ns2.smokeyjoe.com. ; external to domain
       IN  MX  10 mail.another.com. ; external mail provider
; server host definitions
ns1    IN  A      192.168.0.1  ;name server definition
www    IN  A      192.168.0.2  ;web server definition
ftp    IN  CNAME  www.example.com.  ;ftp server definition
; non server domain hosts
bill   IN  A      192.168.0.3
fred   IN  A      192.168.0.4
```

Reverse Zone

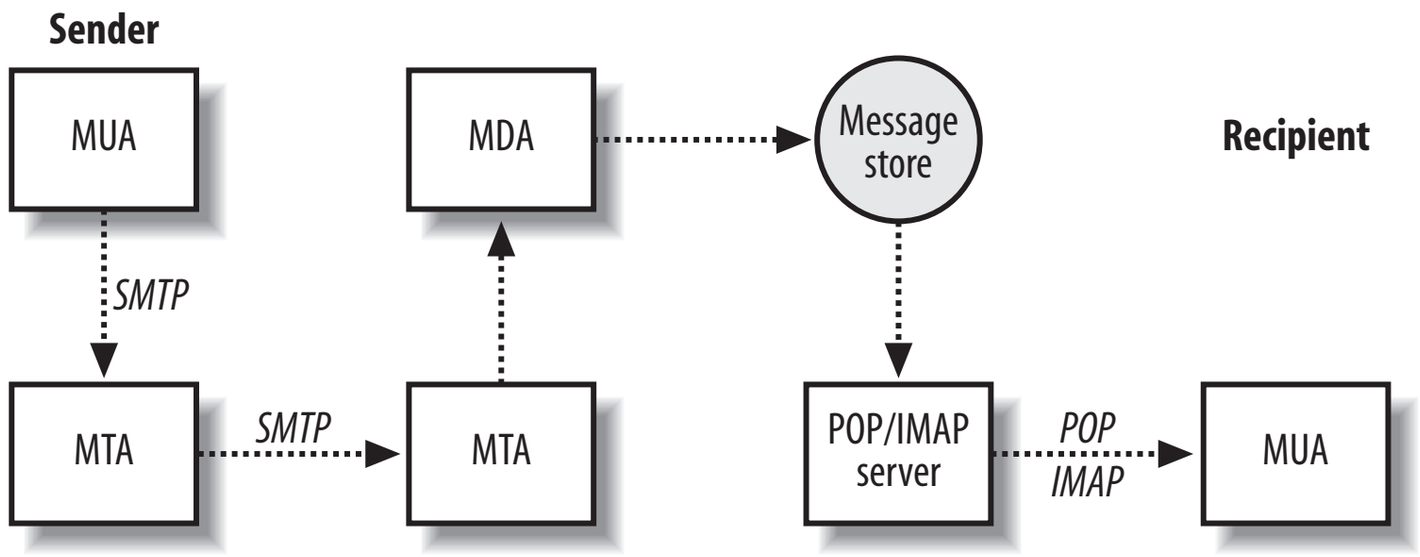
```
$TTL  86400 ; 24 hours could have been written as 24h or 1d
$ORIGIN 0.168.192.IN-ADDR.ARPA.
@  1D  IN    SOA ns1.example.com.   mymail.example.com. (
               2002022401 ; serial
               3H ; refresh
               15 ; retry
               1w ; expire
               3h ; minimum
              )
; server host definitions
1       IN  PTR    ns1.example.com.
2       IN  PTR    www.example.com.
; non server domain hosts
3       IN  PTR    bill.example.com.
4       IN  PTR    fred.example.com.
```

TSIGs

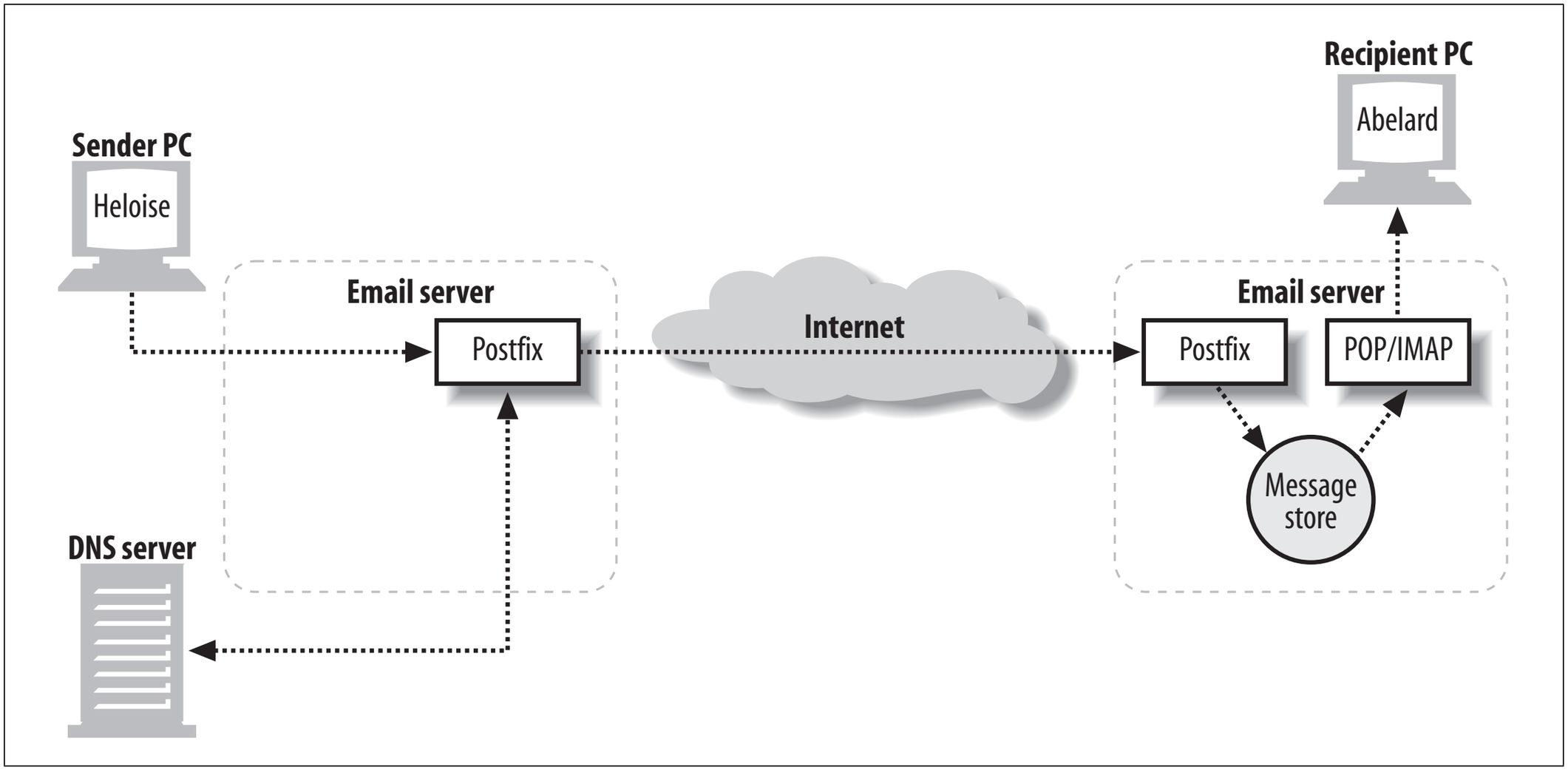
- BIND supports **transaction signatures (TSIGs)**, which allow two systems to establish a trust relationship by using a shared secret key to defend against IP spoofing
  - `dnssec-keygen -r /dev/urandom -a hmac-md5 -b 512 -n HOST keyname`
- The next step is to tell the nameservers about the shared secret by inserting the following code in the `/etc/named.conf` file on both servers
- Once both servers know about the key, use a **server** statement in named.conf to tell them when to use it

Email, pt. 1

- Sending and receiving email require four pieces of software:
  - MUA (mail user agent) - Client application (ie. outlook, evolution)
  - MTA (mail transfer agent) - Server (ie. sendmail, postfix)
  - MDA (mail delivery agent) - Mailbox agent (ie. procmail)
  - POP3/IMAP Server - Deliver mail to client
- By default, SMTP uses port 25



Email, pt. 2


Sender PC
Heloise
Email server
Postfix
Internet
Recipient PC
Abelard
Email server
Postfix
POP/IMAP
Message store
DNS server

Lab Assignments

- Build two or three linux machines (shell only uses less resources)
- Rename machines, and assign static IP addresses to each vm
- Edit the /etc/host files so you can ping each machine by simple name
- Install a DHCP server on one VM, use it dynamically assign addresses to the other two hosts
- Configure ssh so that you can authenticate automatically (without password) when logging in to each host
- Use SCP and rsync to copy directories between hosts

Homework

- Read Chapter 19, 26
- Do page 403, Exercises 1-3, 8, 9
- Do page 699, Exercises 6

Contact

Ian Robert Blair, MSc.

ian.robertblair@icloud.com

QQ: 2302412574