TCP/IP Protocol Suite and IP Addressing

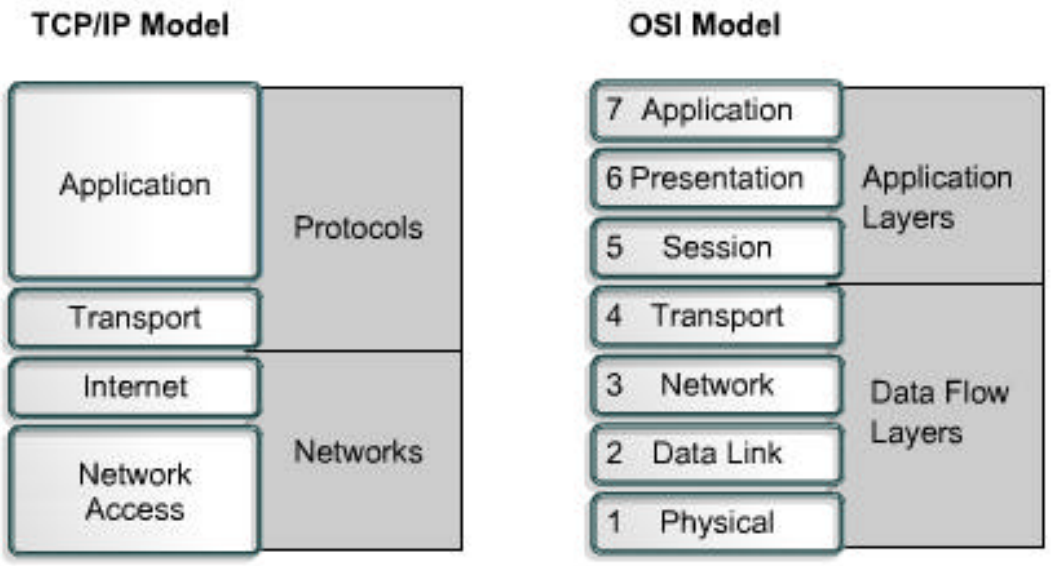
CCNA 1 v3 – Module 9

Introduction to TCP/IP

U.S. DoD created the TCP/IP model.

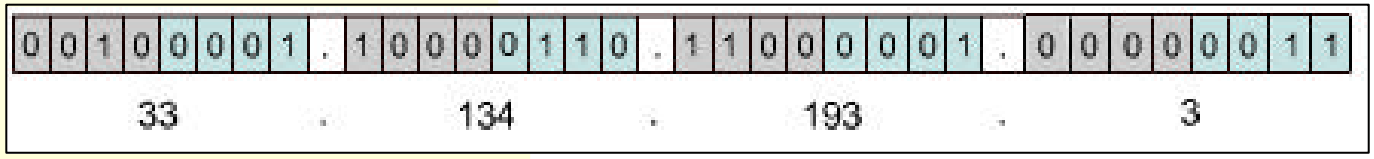
Provides **reliable** data transmission to any destination under any circumstance.

TCP/IP model has become the **Internet standard**.



TCP/IP v4 was standardized in **1981**.

IPv4 addresses are **32 bits** long **dotted decimal**.



IPv6 (IPng) standardized in **1992** by IETF.

IPv6 addresses are **128 bits** long written in hexadecimal with colons separating 16-bit fields. **Leading zeros** can be **omitted** in each field.

Example: **3FFE:1900:6545:3:230:F804:7EBF:12C2**

Application Layer

Handles high-level protocols, issues of **representation**, **encoding**, and **dialog control**. Protocols at this level include:

FTP **File Transfer Protocol**	Reliable, connection-oriented service using TCP to transfer files between systems. Supports bi-directional binary and ASCII file transfers.
TFTP **Trivial File Transfer Protocol**	Connectionless service using UDP. Used on routers to transfer configuration files and IOS images. Faster than FTP.
NFS **Network File System**	Distributed file system developed by Sun Microsystems. Allows file access to remote storage devices.
SMTP **Simple Mail Transfer Protocol**	Administers the transmission of e-mail over computer networks. Only provides support for plaintext.
Telnet **Terminal emulation**	Provides capability to remotely access another computer. Enables user to log in to remote host and execute commands.
SNMP Simple Network Management Protocol	Used to monitor and control network devices, to manage configurations, statistics collection, performance, and security
DNS **Domain Name System**	Used on Internet for translating domain names and their publicly advertised network nodes into IP addresses

Transport Layer

- Provides **transport services** from the source host to the destination host.
- Constitutes a **logical connection** between two endpoints.
- Two protocols:

1. **Transmission Control Protocol – connection oriented**
2. **User Datagram Protocol - connectionless**

- Transport services include all the following services:

TCP and UDP	TCP only
Segmenting upper-layer application data	
Sending segments from one end device to another end device	
	Establishing end-to-end operations
	Flow control provided by sliding windows
	Reliability provided by sequence numbers and acknowledgments

Internet Layer

Best path determination and **packet switching** occur at this layer.

The following protocols operate at the TCP/IP Internet layer:

IP	**Internet Protocol** provides connectionless, best-effort delivery routing of packets. IP is not concerned with the content of the packets but looks for path to destination.
ICMP	**Internet Control Message Protocol** provides control and messaging capabilities
ARP	**Address Resolution Protocol** determines the data link layer address (MAC address) for known IP addresses
RARP	**Reverse Address Resolution Protocol** determines IP addresses when the MAC address is known.

- IP defines **packets** and **addressing scheme**, transfers data **between Internet layer** and **network access layer** and **routes** packets to remote hosts.
- Calling IP an **unreliable** protocol simply means that IP does not perform error checking and correction. These are handled by upper layer protocols.

Network Access Layer

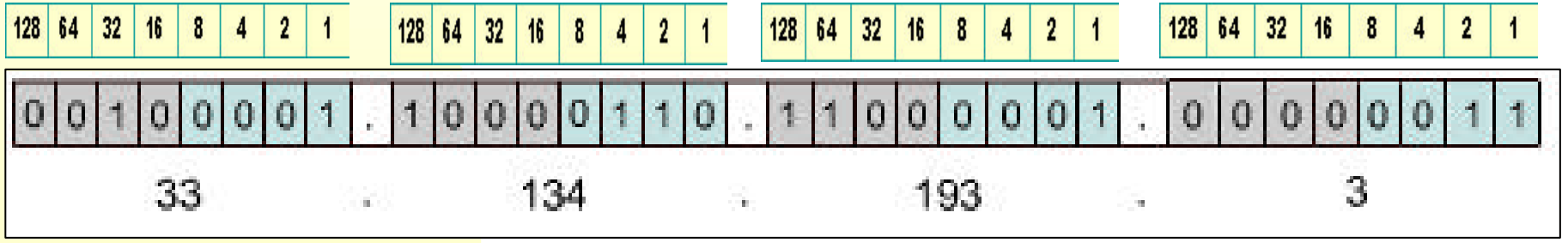
- Also called the **host-to-network** layer.
- Concerned with making a **physical link** to the **network media**.
- Includes LAN and WAN technology details, and all the details contained in the **OSI physical** and **data-link layers**.
- **Drivers** for software applications and **modem cards** operate here.
- Protocols such as **Serial Line Interface Protocol** and **Point to Point Protocol** provide modems network access.
- Intricate interplay of **hardware**, **software**, and **transmission-medium**.
- Maps IP addresses to **MAC addresses**.
- Encapsulates IP packets into **frames**.

Network Access layer protocols include:

Ethernet, Fast Ethernet, SLIP, PPP, FDDI, ATM, Frame-Relay, SMDS, ARP, Proxy ARP, RARP.

IP Addressing

- **Addresses** allow one computer to locate another computer on a network.
- Each computer in a TCP/IP network must be given a unique **IP address**. IP addresses operate at **Layer 3**.
- Each IP address is written as four parts separated by dots. Each part of the address is called an **octet** because it is made up of **eight bits**.
- Dotted decimal notation is easier for people to understand than **binary ones and zeros**.



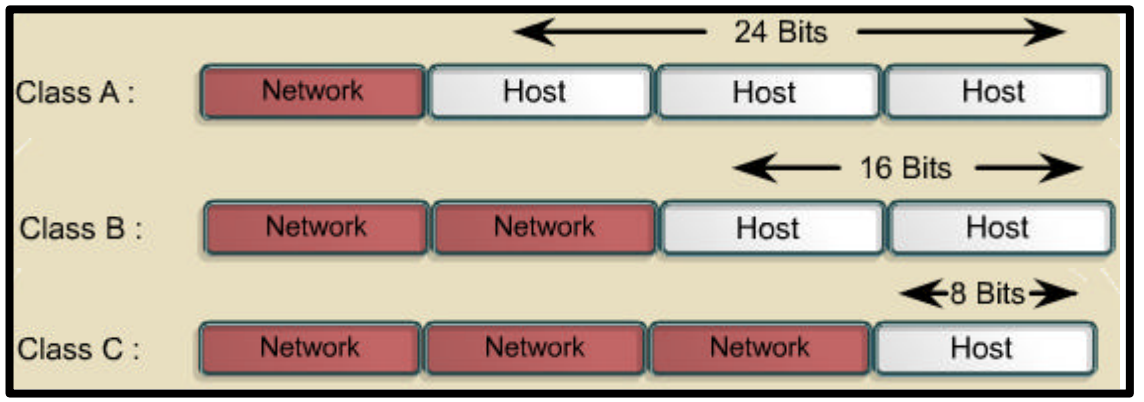
Every IP address has two parts:

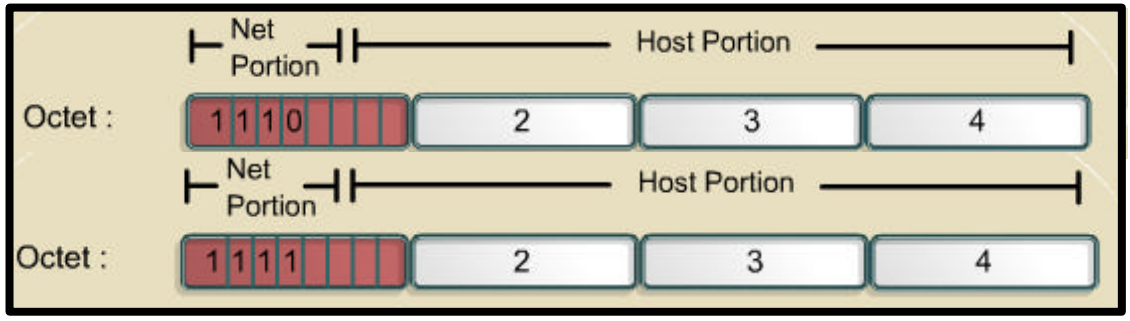
1. Network
2. Host

IP addresses are divided into classes A,B and C to define large, medium, and small networks.

The Class D address class was created to enable multicasting.

IETF reserves Class E addresses for its own research.





Address Class	High-Order Bits	First Octet Address Range	Number of Bits in the Network Address	Number of Networks	Number of Hosts per Network
Class A	0	0-127	8	126	16,777,216
Class B	10	128-191	16	16,384	65,536
Class C	110	192-223	24	2,097,152	254
Class D	1110	224-239	28	N/A	N/A

Certain host addresses are reserved and cannot be assigned to devices on a network:

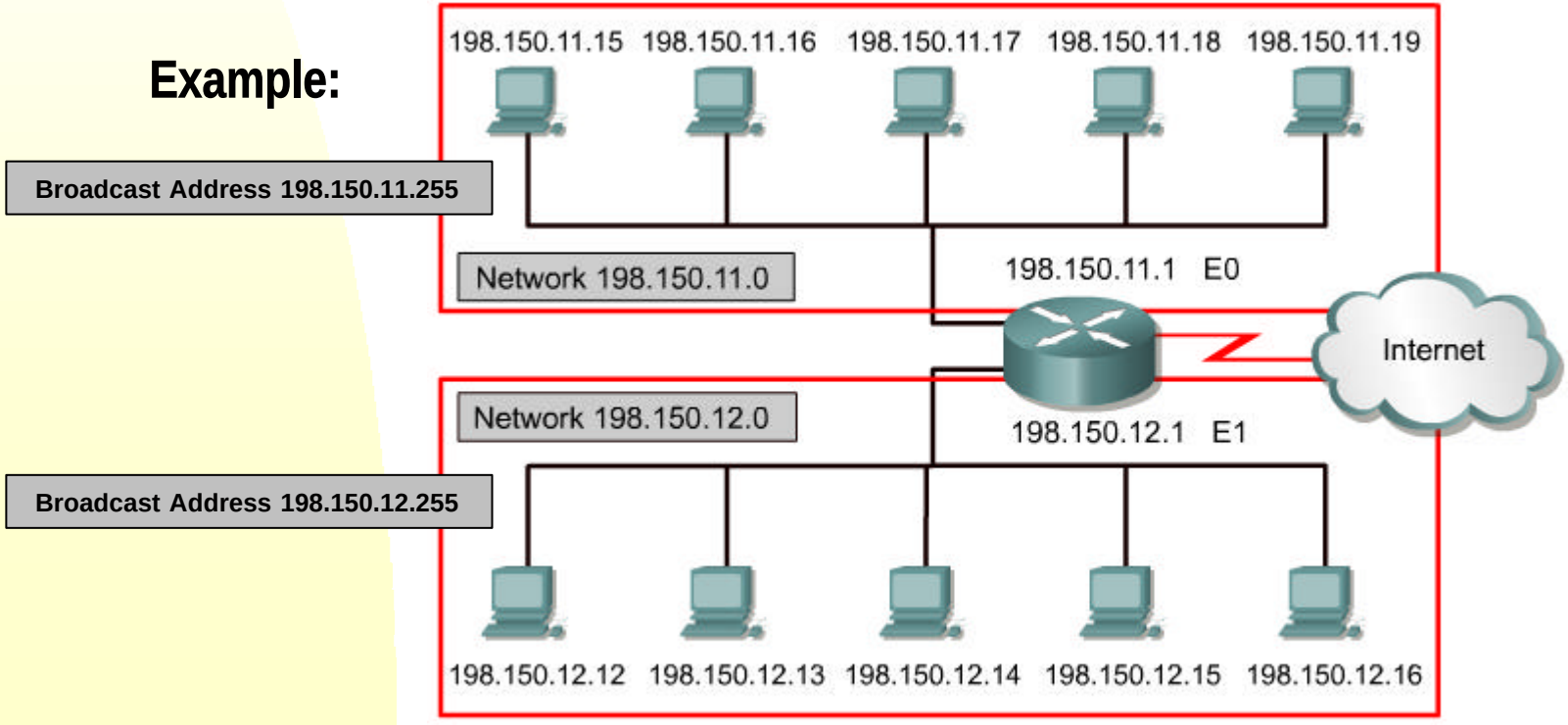
Network address – Used to identify the network itself

- An IP address that has binary 0s in all host bit positions is reserved for the network address

Broadcast address – Used for broadcasting packets to all the devices on a network

- Broadcast IP addresses end with binary 1s in the entire host part of the address.

Example:



IP Private Addresses

- **IANA** manages the remaining supply of **Public IP addresses** to ensure that duplication does not occur. Public IP addresses are unique and must be obtained from an ISP or a registry.
- **Private IP addresses** are a solution to the problem of the exhaustion of public IP addresses. Addresses that fall within these **ranges** are not routed on the Internet backbone:

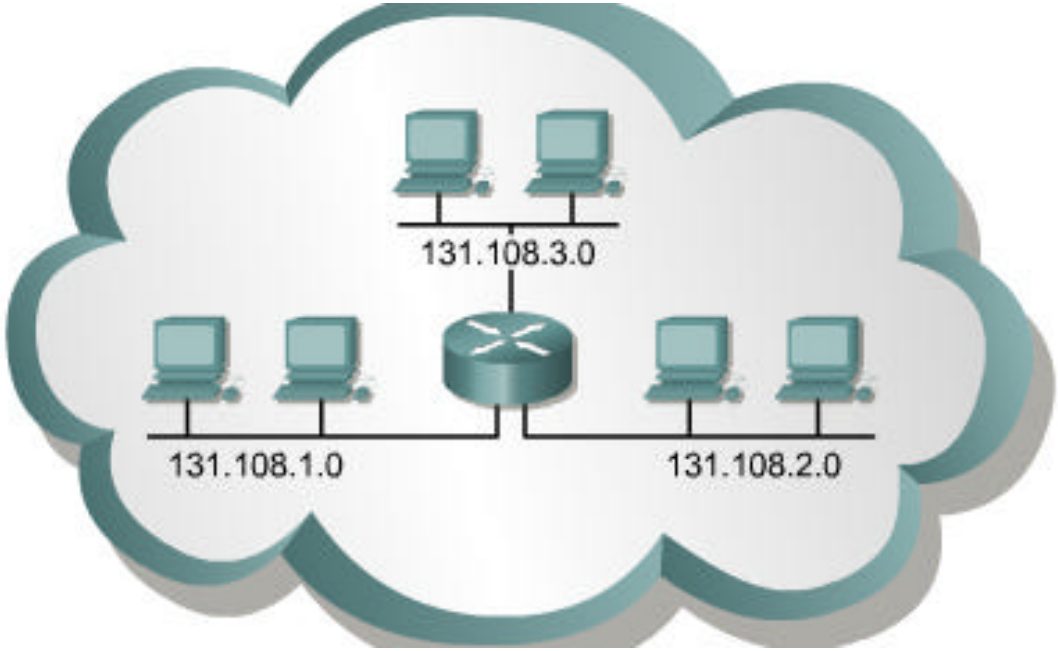
Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

- Connecting a network using private addresses to the Internet requires **translation** of the private addresses to public addresses (NAT).

Subnetting

Example:
All three segments are part of the Class B network:
Address space 131.108.0.0
Default network mask 255.255.0.0

Individual subnets are created:
Subnet mask 255.255.255.0



- Subnetting a network means to use the **subnet mask** to break a large network up into smaller, more efficient and manageable **subnets**.
- With subnetting, the network is not limited to Class A, B, or C masks
- To create a subnet address, **borrow bits** from the **host field** and designate them as the **subnet field**.
- There are three parts to subnet addresses:

1. **Network**
2. **Subnet**
3. **Host**

Obtaining an IP Address

Two methods to assign IP addresses:

1. **Static**
   - Manually configured on the host by Network Administrator
   - Can be used for hosts on **small, infrequently changing networks**
   - Assign to **printers**, **servers**, and **routers**
2. **Dynamic**
   - Host discovers its IP address by asking another network device
   - Using **RARP**, **BOOTP** or **DHCP**

RARP

- **Reverse ARP** associates a known **MAC address** with an **IP address**.
- RARP requests are **broadcast** onto the LAN and are responded to by the **RARP server** (usually a router).
- RARP uses the same packet format as ARP.
- The RARP packet format has an empty source IP addresses field, and **destination MAC** address set to **FFFFFFFFFFFF**.
- Workstation running RARP have codes in ROM that start the process.

BOOTP

Bootstrap Protocol only requires a **single packet exchange** to obtain IP information.

BOOTP packets can include:

- **IP address**
- **Router address**
- **Server address**
- Vendor-specific information.

Network administrator creates a file specifying parameters for each device.
Each host must have a **BOOTP profile** with an IP address assignment.
No two profiles can have the same IP address.
BOOTP uses **UDP** to carry messages.

BootP process:

1. Host sends a **broadcast IP packet** - destination **255.255.255.255**.
2. BOOTP server receives the broadcast and then sends back a broadcast.
3. Client finds its own MAC address in the destination address field of the server's broadcast and accepts the IP address and other information.

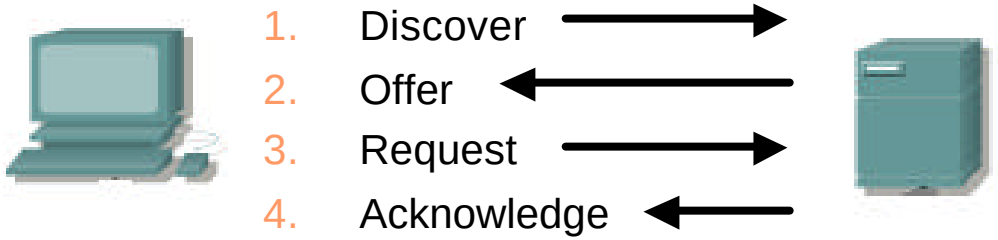
DHCP

Dynamic Host Configuration Protocol is BOOTP's successor.

Host can obtain IP address dynamically **without** a network administrator having to set up **individual profiles**.

Range of IP addresses is defined on a **DHCP server**.

Four part process:



DHCP Offer includes IP address, default-gateway, subnet mask and **lease information**.

DHCP allows users to be **mobile**.

DHCP leases an IP address to a device and then reclaims that IP address for another user after the first user releases it.

DHCP offers a one to many ratio of IP addresses.

ARP

Address Resolution Protocol maps **IP** to **MAC addresses**.

ARP automatically obtains MAC addresses on **local** segment.

Proxy ARP provides the MAC address of an intermediate device for transmission **outside** the **LAN**.

ARP tables are stored in **RAM** and maintained automatically on each device.

When a network device wants to send data across the network, it uses information from the ARP table.

There are two ways that devices can gather MAC addresses:

1. **Monitoring** traffic occuring on the local network segment.
2. **Broadcasting** an **ARP request**