high importance
mid importance
low importance

SRM Institute of Science and Technology

Department of Computer Science and Engineering

Delhi – Meerut Road, Sikri Kalan, Ghaziabad, Uttar Pradesh – 201204

Academic Year: 2024-25 (ODD)

CN UNIT II Notes

IPv4

An IPv4 address is a 32- bit binary value, which can be displayed as four decimal digits. The IPv4 address space offers about 4.3 billion addresses. Only billion addresses can only be assigned out of 4.3 billion address. The other addresses are conserved for specific purposes such as multicasting, private address space, loopback testing, and research.

IP version 4 (IPv4) uses Broadcasting for transferring packets from one computer to all computers; this probably generates problems sometimes.

Dotted-Decimal Notation of IPv4 128.11.3.31

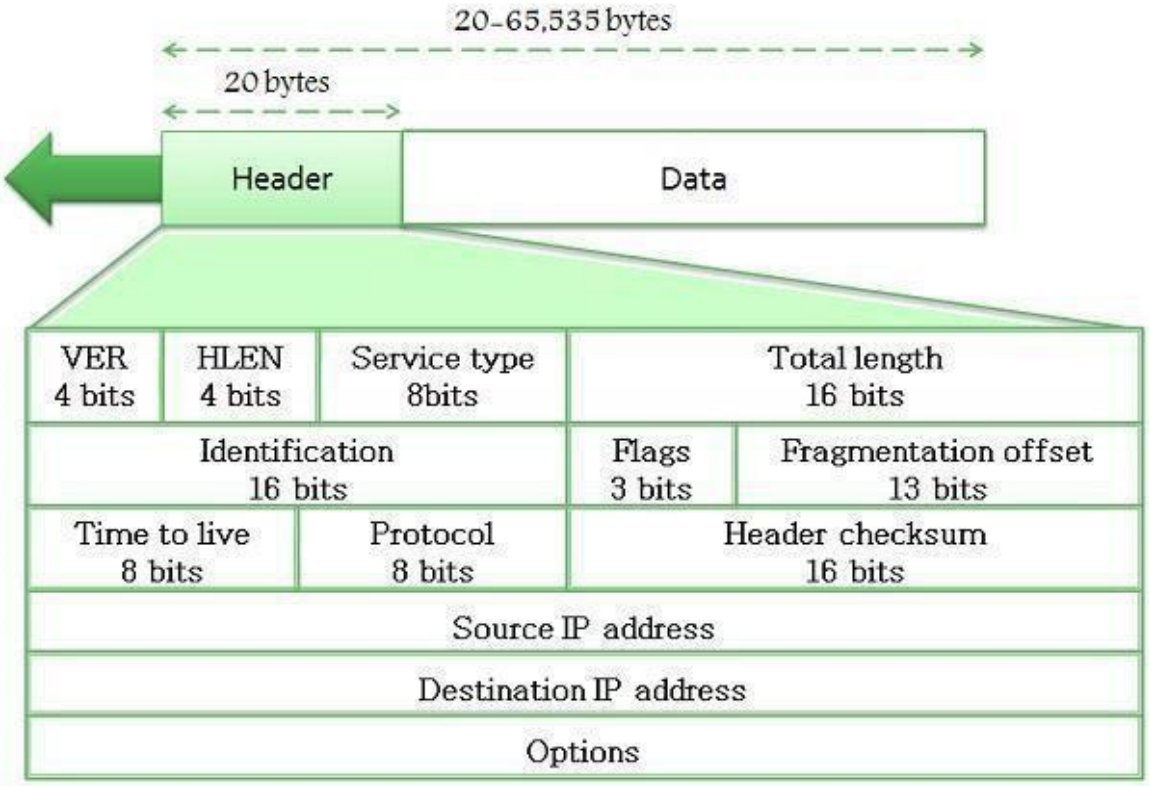
Packet Format

An IPv4 datagram is a variable-length packet comprised of a header (20 bytes) and data (up to 65,536 along with header). The header contains information essential to routing and delivery.

Base Header
Version: It defines the version number of IP, i.e., in this case, it is 4 with a binary value of 0100.
Header length (HLEN): It represents the length of the header in multiple of four bytes.

DSCP: differentiated services code point

Service type: It determines how datagram should be handled and includes individual bits such as level of throughput, reliability, and delay. **Total length:** It signifies the entire length of the IP datagram.
Identification: This field is used in fragmentation. A datagram is divided when it passes through different networks to match the network frame size. At that time each fragment is determined with a sequence number in this field.
Flags: The bits in the flags field handles fragmentation and identifies the first, middle or last fragment, etc.



Fragmentation offset: It's a pointer that represents the offset of the data in the original datagram.
Time to live: It defines the number of hops a datagram can travel before it is rejected. In simple words, it specifies the duration for which a datagram remains on the internet.
Protocol: The protocol field specifies which upper layer protocol data are encapsulated in the datagram (TCP, UDP, ICMP, etc.).
Header checksum: This is a 16-bit field confirm the integrity of the header values, not the rest of the packet.
Source address: It's a four-byte internet address which identifies the source of the datagram.
Destination address: This is a 4-byte field which identifies the final destination.
Options: This provides more functionality to the IP datagram. Furthermore can carry fields like control routing, timing, management, and alignment.

IPv4 is a two-level address structure (net id and host id) classified into five categories (A, B, C, D, and E).

IPv4 Addressing

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.

An IPv4 address is 32 bits long.

IPv4 addresses are unique. They are unique in the sense that each address defines one, and only one, connection to the Internet. Two devices on the Internet can never have the same address at the same time. We will see later that, by using some strategies, an address may be assigned to a device for a time period and then taken away and assigned to another device. On the other hand, if a device operating at the network layer has m connections to the Internet, it needs to have m addresses. We will see later that a router is such a device

The IPv4 addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet. The IPv4 addresses are unique and universal.

Address Space

A protocol such as IPv4 that defines addresses has an address space. An address space is the total number of addresses used by the protocol. If a protocol uses N bits to define an address, the address space is 2N because each bit can have two different values (0 or 1) and N bits can have 2N values. IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4 billion). This means that, theoretically, if there were no restrictions, more than 4 billion devices could be connected to the Internet. We will see shortly that the actual number is much less because of the restrictions imposed on the addresses.

The address space of IPv4 is 232 or 4,294,967,296.

Notations

There are two prevalent notations to show an IPv4 address: binary notation and dotted decimal

notation.

Binary Notation

In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address. The following is an example of an IPv4 address in binary notation:

01110101 10010101 00011101 00000010

Dotted-Decimal Notation

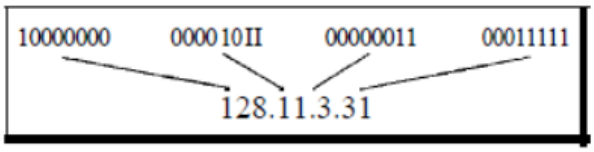
To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. The following is the dotted decimal notation of the above address:

117.149.29.2

Figure 19.1 shows an IPv4 address in both binary and dotted-decimal notation.

Note that because each byte (octet) is 8 bits, each number in dotted-decimal notation is a value ranging from 0 to 255.

Figure 19.1 *Dotted-decimal notation and binary notation for an IPv4 address*



An IP address is most often represented in decimal, in the following format:

158.80.164.3

An IP address is comprised of four octets, separated by periods:

First Octet	Second Octet	Third Octet	Fourth Octet
158	80	164	3

Each octet is an 8-bit number, resulting in a 32-bit IP address. The smallest possible value of an octet is 0, or 00000000 in binary. The largest possible value of an octet is 255, or 11111111 in binary.

The above IP address represented in binary would look as follows:

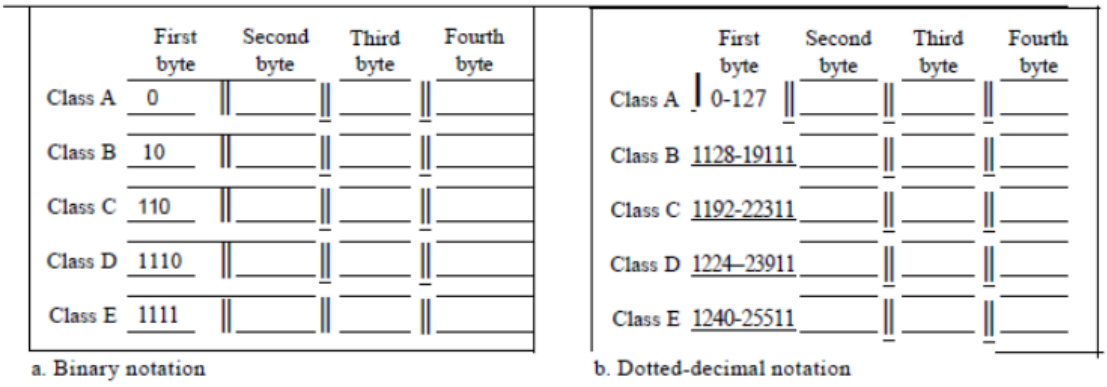
First Octet	Second Octet	Third Octet	Fourth Octet
10011110	01010000	10100100	00000011

Classful Addressing

IPv4 addressing, at its inception, used the concept of classes. This architecture is called classful addressing. Although this scheme is becoming obsolete, we briefly discuss it here to show the rationale behind classless addressing.

In classful addressing, the address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space. In classful addressing, the address space is divided into five classes:A, B, C, D, and E. We can find the class of an address when given the address in binary notation or dotted-decimal notation. If the address is given in binary notation, the first few bits can immediately tell us the class of the address. If the address is given in decimal-dotted notation, the first byte defines the class. Both methods are shown in Figure 19.2.

Figure 19.2 *Finding the classes in binary and dotted-decimal notation*



Limitations of classful addressing:

A block in class A address is too large for almost any organization. This means most of the addresses in class A were wasted and were not used.

• A block in class B is also very large, probably too large for many of the organizations that received a class B block.

• A block in class C is probably too small for many organizations.

• Class D addresses were designed for multicasting which means each address in this class is used to define one group of hosts on the Internet.

• The Internet authorities wrongly predicted a need for 268,435,456 groups. This never happened and many addresses were wasted here too.

And lastly, the class E addresses were reserved for future use; only a few were used, resulting in another waste of addresses

Classes and Blocks

One problem with classful addressing is that each class is divided into a fixed number of blockswith each block having a fixed size as shown in Table 19.1

Table 19.1 *Number ofblocks and block size in classfulIPv4 addressing*

Class	*Number ofBlocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Let us examine the table. Previously, when an organization requested a block of addresses, it was granted one in class A, B, or C. Class A addresses were designed for large organizations with a large number of attached hosts or routers. Class B addresses were designed for midsize organizations with tens of thousands of attached hosts or routers. Class C addresses were designed for small organizations with a small number of attached hosts or routers. We can see the flaw in this design. A block in class A address is too large for almost any organization. This means most of the addresses in class A were wasted and were not used. A block in class B is also very large, probably too large for many of the organizations that received a class B block. A block in class C is probably too small for many organizations. Class D addresses were designed for multicasting as we will see in a later chapter. Each address in this class is used to define one group of hosts on the Internet. The Internet authorities wrongly predicted a need for 268,435,456 groups. This never happened and many addresses were wasted here too. And lastly, the class E addresses were reserved for future use; only a few were used, resulting in another waste of addresses. In c1assfnl addressing, a large part of the available addresses was wasted.

Netid and Hostid

In classful addressing, an IP address in class A, B, or C is divided into netid and hostid. These parts are of varying lengths, depending on the class of the address. Figure 19.2 shows some netid and hostid bytes. The netid is in color, the hostid is in white. Note that the concept does not apply to classes D and E. In class A, one byte defines the netid and three bytes define the hostid. In class B, two bytes define the netid and two bytes define the hostid. In class C, three bytes define the netid and one byte defines the hostid.

Mask

Although the length of the netid and hostid (in bits) is predetermined in classful addressing, we can also use a mask (also called the default mask), a 32-bit number made of

Table 19.2 *Default masks for classful addressing*

Class	*Binary*	*Dotted-Decimal*	*CIDR*
A	11111111 00000000 00000000 00000000	255.0.0.0	*18*
B	11111111 11111111 00000000 00000000	255.255.0.0	*116*
C	11111111 11111111 11111111 00000000	255.255.255.0	*124*

Although the length of the netid and hostid is predetermined in we can also use a mask,

which is a 32-bit number made of contiguous 1s followed by contiguous 0s.

• The masks for classes A, B, and C are shown in below table.

• The mask can help us to find the netid and the hostid.

SUBNETTING

• Subnetting was introduced for classful addressing.

• If an organization was granted a large block in class A or B,

• Then, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called subnets) or, in rare cases, share part of the addresses with neighbors.

• Subnetting increases the number of Is in the mask

SUPERNETTING

• In supernetting, an organization can combine several class C blocks to create a larger range of addresses.

• In other words, several networks are combined to create a supernetwork or a supemet.

• An organization can apply for a set of class C blocks instead of just one.

• Ex: An organization that needs 1000 addresses can be granted four contiguous class C blocks. The organization can then use these addresses to create one supernetwork.

• Supernetting decreases the number of 1s in the mask. For example, if an organization is given four class C addresses, the mask changes from /24 to /22.

ADDRESS DEPLETION:

• The flaws in classful addressing scheme combined with the fast growth of the Internet led to the near depletion of the available addresses.

• Yet the number of devices on the Internet is much less than the 232 address space.

• We have run out of class A and B addresses, and a class C block is too small for most midsize organizations.

• One solution that has alleviated the problem is the idea of classless addressing

CLASSLESS ADRESSING:

• To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented.

• In this scheme, there are no classes, but the addresses are still granted in blocks.

ADDRESS BLOCKS:

• In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses.

• The size of the block (the number of addresses) varies based on the nature and size of the entity.

• Example, a household may be given only two addresses; a large organization may be given thousands of addresses.

An ISP, as the Internet service provider, may be given thousands or hundreds of thousands based on the number of customers it may serve.

NETWORK ADDRESSES:

When an organization is given a block of addresses, the organization is free to allocate the addresses to the devices that need to be connected to the Internet.

• The first address in the class, however, is normally (not always) treated as a special address.

• The first address is called the network address and defines the organization network.

• It defines the organization itself to the rest of the world

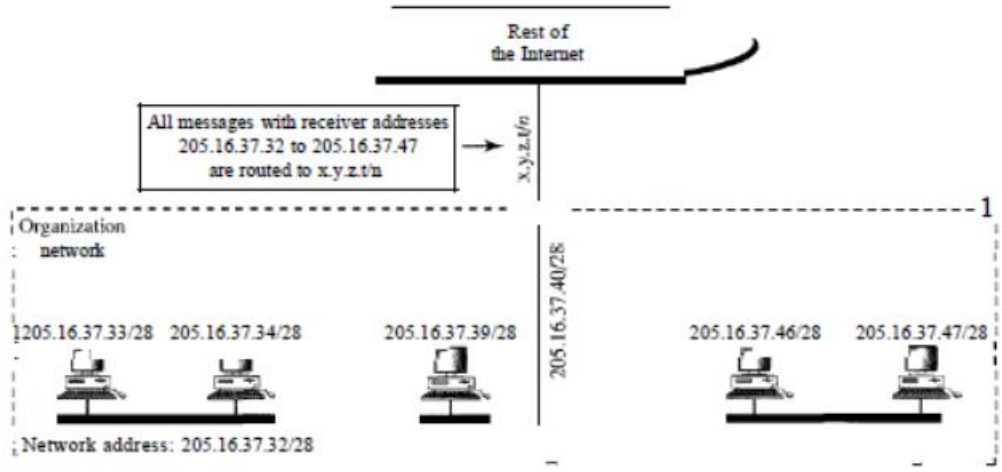
• The organization network is connected to the Internet via a router.

The router has two addresses. One belongs to the granted block; the other belongs to the network that is at the other side of the router.

• We call it as second address x.y.z.t/n because we do not know anything about the network it is connected to at the other side.

• All messages destined for addresses in the organization block (205.16.37.32 to 205.16.37.47) are sent, directly or indirectly, to x.y.z.t/n.

• We say directly or indirectly because we do not know the structure of the network to which the other side of the router is connected.



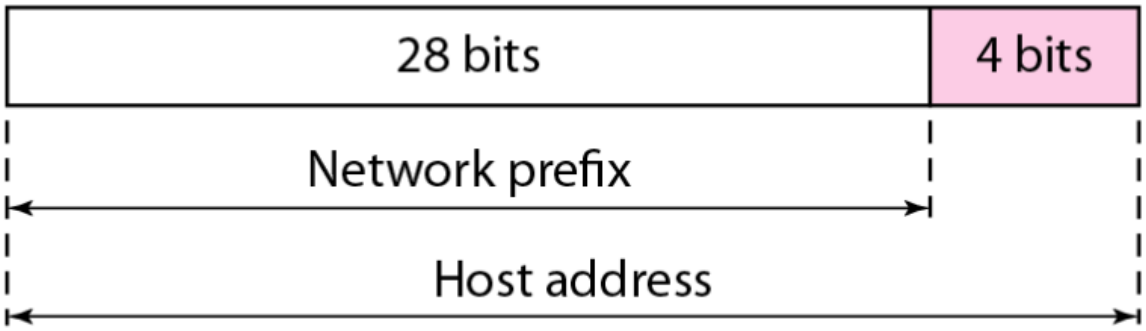
TWO-LEVEL HIERARCHY

• An IP address can define only two levels of hierarchy when not subnetted.

• The n leftmost bits of the address x.y.z.tJn define the network (organization network); the 32 – n rightmost bits define the particular host (computer or router) to the network.

• The two common terms are prefix and suffix.

• The part of the address that defines the network is called the prefix; the part that defines the host is called the suffix.



THREE-LEVEL HIERARCHY

An organization that is granted a large block of addresses may want to create clusters of networks (called subnets) and divide the addresses between the different subnets.

• The rest of the world still sees the organization as one entity; however, internally there are several subnets.

• All messages are sent to the router address that connects the organization to the rest of the Internet; the router routes the message to the appropriate subnets.

• The organization, however, needs to create small subblocks of addresses, each assigned to specific subnets.

• The organization has its own mask; each subnet must also have its own.

Figure 19.7 *Configuration and addresses in a subnetted network*

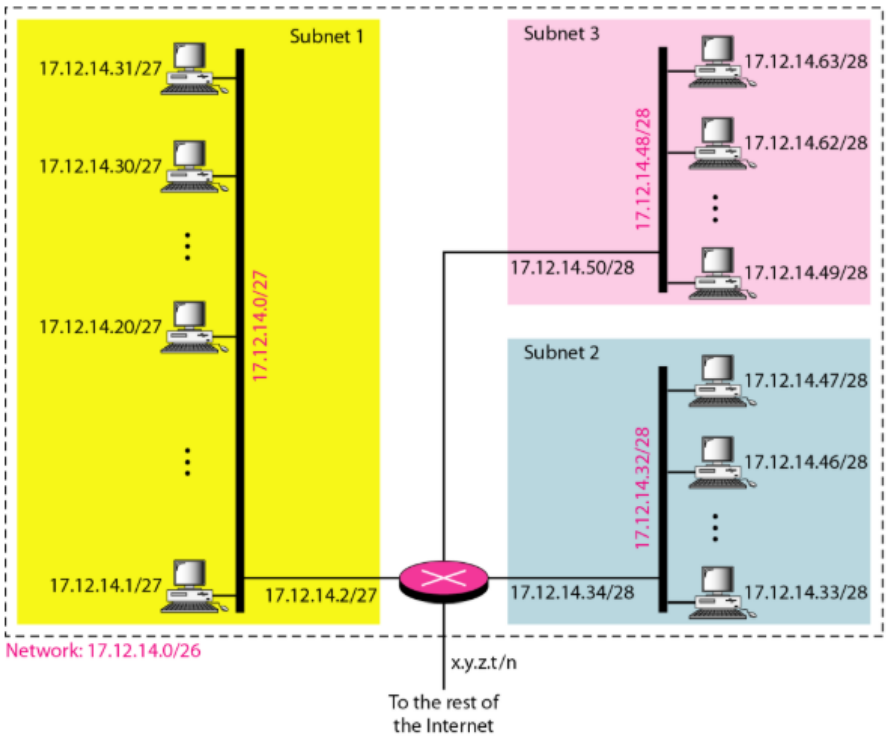
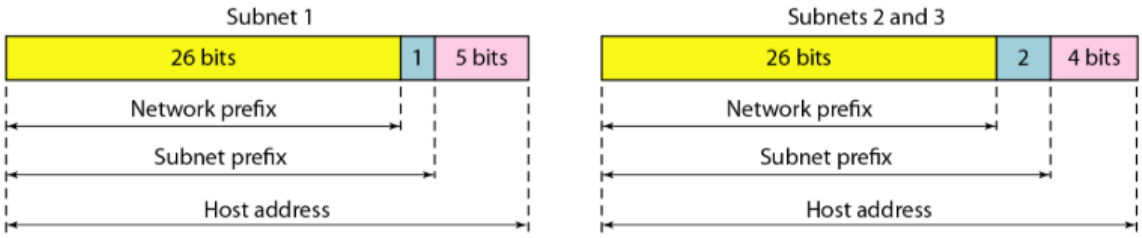


Figure 19.8 *Three-level hierarchy in an IPv4 address*



NETWORK ADDRESS TRANSLATION:

The number of home users and small businesses that want to use the Internet is ever increasing.

• In the beginning, a user was connected to the Internet with a dial-up line, which means that she was connected for a specific period of time.

• An ISP with a block of addresses could dynamically assign an address to this user. An address was given to a user when it was needed. But the situation is different today.

• Home users and small businesses can be connected by an ADSL line or cable modem.

• In addition, many are not happy with one address; many have created small networks with several hosts and need an IP address for each host.

• With the shortage of addresses, this is a serious problem-solution to this problem is called network address translation (NAT).

• NAT enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally.

The traffic inside can use the large set; the traffic outside, the small set.

• To separate the addresses used inside the home or business and the ones used for the Internet, the Internet authorities have reserved three sets of addresses as private addresses, shown in below table.

Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

Any organization can use an address out of this set without permission from the Internet

authorities.

• Everyone knows that these reserved addresses are for private networks.

• They are unique inside the organization, but they are not unique globally.

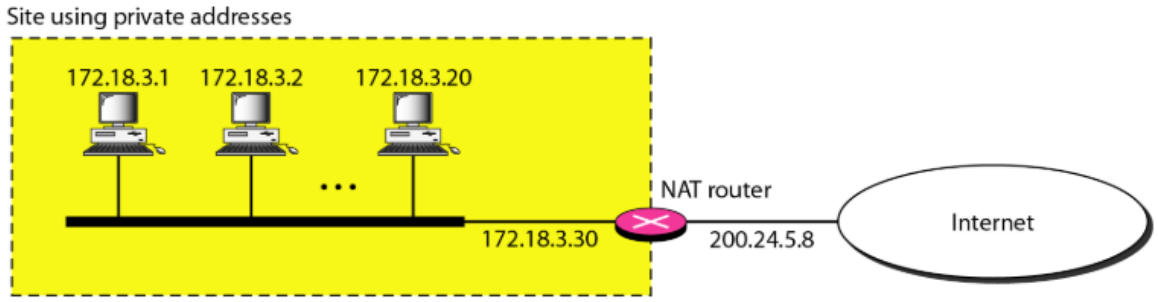
• No router will forward a packet that has one of these addresses as the destination address.

• The site must have only one single connection to the global Internet through a router that runs the NAT software. Below fig. shows a simple implementation of NAT.

The private network uses private addresses.

• The router that connects the network to the global address uses one private address and one global address.

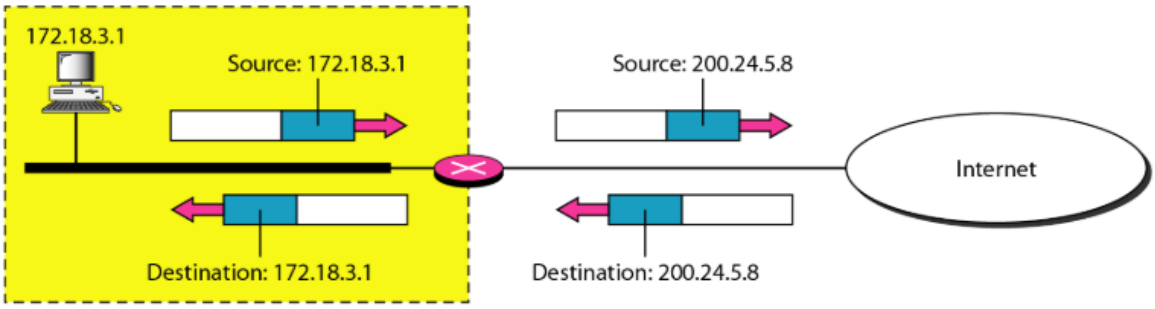
• The private network is transparent to the rest of the Internet; the rest of the Internet sees only the NAT router with the address 200.24.5.8



ADDRESS TRANSLATION:

• All the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address.

• All incoming packets also pass through the NAT router, which replaces the destination address in the packet (the NAT router global address) with the appropriate private address.



TRANSLATION TABLE:

• Translation table has only two columns: the private' address and the external address (destination address of the packet).

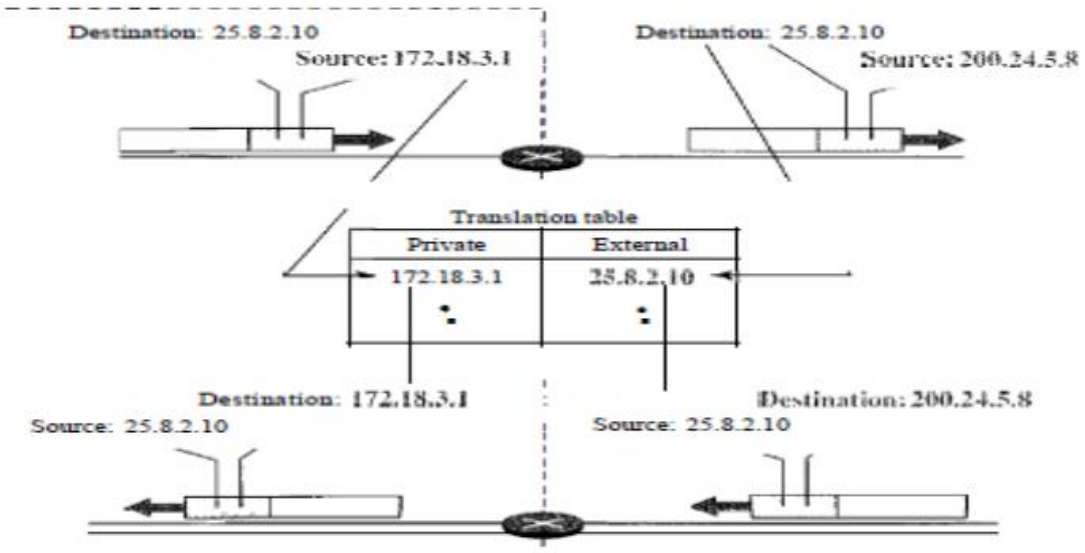
• When the router translates the source address of the outgoing packet, it also makes note of the destination address-where the packet is going.

• When the response comes back from the destination, the router uses the source address of the packet (as the external address) to find the private address of the packet.

POOL OF IP ADDRESSES

• As NAT router has only one global address, only one private network host can access the same external host.

To remove this restriction, the NAT router uses a pool of global addresses



USING BOTH IP ADDRESSES AND PORT NUMBERS

To allow a many-to-many relationship between private-network hosts and external server programs, we need more information in the translation table.

• For example, suppose two hosts with addresses 172.18.3.1 and 172.18.3.2 inside a private network need to access the HTTP server on external host 25.8.3.2.

• If the translation table has five columns, instead of two, that include the source and destination port numbers of the transport layer protocol, the ambiguity is eliminated.

Private Address	*Private Port*	*External Address*	*External Port*	*Transport Protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
. . .	. . .	. . .	. . .	. . .

Variable Length Subnet Mask (VLSM)

Variable Length Subnet Mask (VLSM) is a subnet -- a segmented piece of a larger network -- design strategy where all subnet masks can have varying sizes. This process of "subnetting subnets" enables network engineers to use multiple masks for different subnets of a single class A, B or C network.

With VLSM, an IP address space can be divided into a well-defined hierarchy of subnets with different sizes. This helps enhance the usability of subnets because subnets can include masks of varying sizes.

A subnet mask helps define the size of the subnet and create subnets with very different host counts without wasting large numbers of addresses.

Fixed-length subnet mask (FLSM)

A fixed-length subnet mask (FLSM) refers to a type of enterprise or provider networking where a block of IP addresses is divided into multiple subnets of equal length, i.e. an equal number of IP addresses. FLSM streamlines packet routing within the subnets of a proprietary network.

This differentiates FLSM from variable-length subnet mask (VLSM) or classless subnetting, where each subnet has different lengths, and includes different hosts and networks. VLSM may be considered the more modern and more efficient approach to subnetting.

In FLSM, once a packet arrives at an organization's main gateway with its network number, it is routed to its ultimate destination using a subnet number. The FLSM is usually a string of binary digits shown over the subnet number, telling the router which parts of the subnet number to look at.

A binary "1" over a particular digit in the subnet number says, "Pay attention to this digit." A "0" says, "Ignore this digit."

FLSM is also known as classful subnetting or traditional subnetting.

This differentiates FLSM from variable-length subnet mask (VLSM) or classless subnetting, where each subnet has different lengths, and includes different hosts and networks. VLSM may be considered the more modern and more efficient approach to subnetting.

In FLSM, once a packet arrives at an organization's main gateway with its network number, it is routed to its ultimate destination using a subnet number. The FLSM is usually a string of binary digits shown over the subnet number, telling the router which parts of the subnet number to look at.

A binary "1" over a particular digit in the subnet number says, "Pay attention to this digit." A "0" says, "Ignore this digit."

FLSM is also known as classful subnetting or traditional subnetting.

Benefits and drawbacks of FLSM

When it was first introduced, FLSM was simply known as "subnetting." Its biggest benefit is that it validates the idea of borrowing bits from an IP address host field to create locally-significant subnet identification addresses.

The use of FLSM saves a router the task of having to handle an entire IP address, because the router deals only with the digits selected by the mask. Further, it divides the address space into an adequate number of subnets and can therefore meet the needs of large LANs.

In IP classes of IPv4 addresses, there are fixed subnets with a fixed number of hosts and networks. For example, a class C IP address has a 24-bit network part and an 8-bit host part. Similarly, Class A addresses have an 8-bit network part and a 24-bit host part.

What this means is that in this method of subnet masking, subnets are rarely filled to capacity. This results in the inefficient use of IP address space, and a significant waste of unused addresses.

To overcome these challenges, a VLSM is better. In networks with many unassigned IP addresses, VLSM uses IP address space more efficiently, and thus prevents waste

Network Devices

In this section, we divide connecting devices into five different categories based on the layer in which they operate in a network, as shown in Figure 15.1. The five categories contain devices which can be defined as in Table 1:

Table 1: Connecting Devices

S. No.	Device	Layer(s)
1.	Passive hub	*below the physical layer*
2.	Repeater/Active hub	*at the physical layer*
3.	Bridge/Two-layer switch	*at the physical and data link layers*
4.	Router/Three-layer switch	*at the physical, data link, and network layers*
5.	Gateway	*at all five layers*

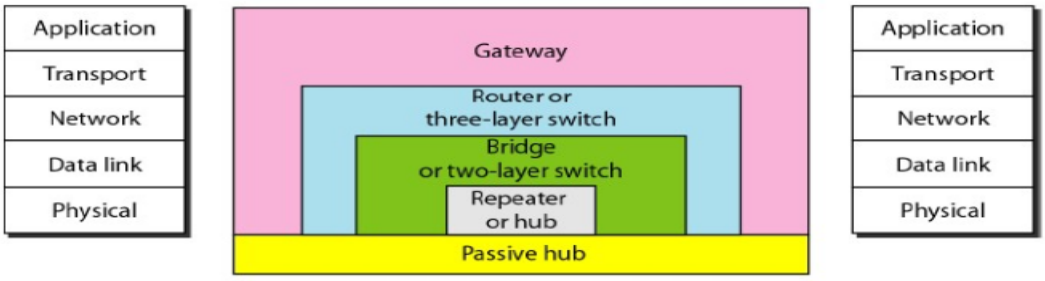


Figure 15.1 Five categories of connecting devices

Passive Hubs

A passive hub is just a connector. It connects the wires coming from different branches. In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point. This type of a hub is part of the media; its location in the Internet model is below the physical layer.

Repeaters

A repeater is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern. The repeater then sends the refreshed signal. A repeater can extend the physical length of a LAN, as shown in Figure 15.2.

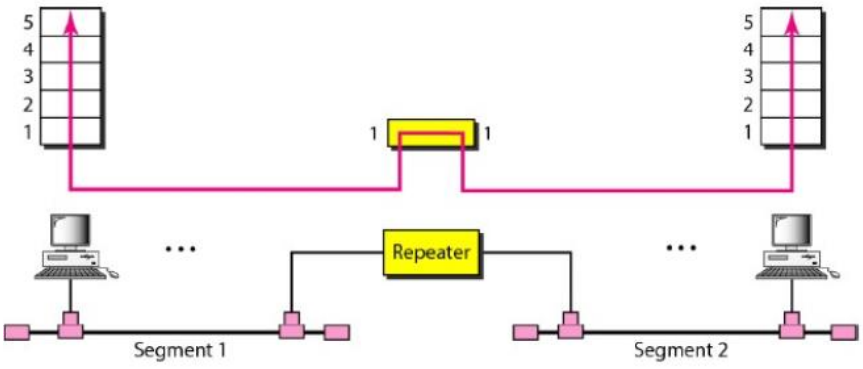


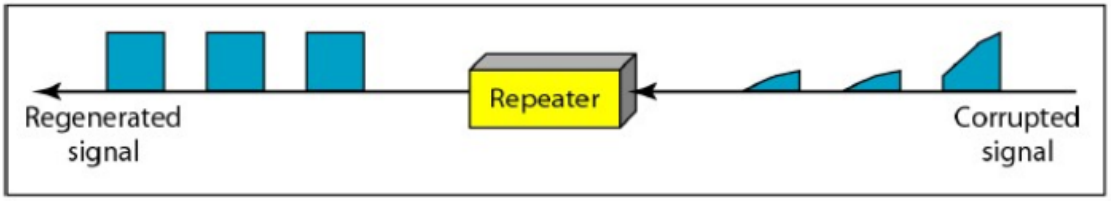
Figure 15.2 A repeater connecting two segments of a LAN

A repeater does not actually connect two LANs; it connects two segments of the same LAN. The segments connected are still part of one single LAN. A repeater is not a device that can connect two LANs of different protocols.

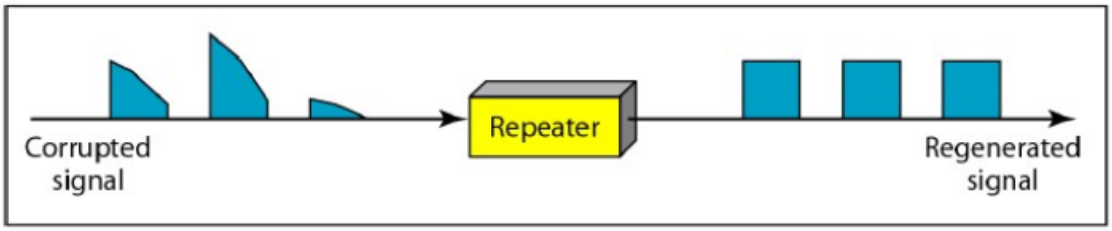
• A repeater can overcome the 10Base5 Ethernet length restriction. In this standard, the length of the cable is limited to 500 m. To extend this length, we divide the cable into segments and install repeaters between segments. Note that the whole network is still considered one LAN, but the portions of the network separated by repeaters are called segments.

• The repeater acts as a two-port node, but operates only in the physical layer. When it receives a frame from any of the ports, it regenerates and forwards it to the other port.

• A repeater forwards every frame; it has no filtering capability.



a. Right-to-left transmission.



b. Left-to-right transmission.

Figure 15.3 Function of a repeater

Active Hubs

An active hub is actually a multipart repeater. It is normally used to create connections between stations in a physical star topology. We have seen examples of hubs in some Ethernet implementations (10Base-T, for example). However, hubs can also be used to create multiple levels of hierarchy, as shown in Figure 15.4. The hierarchical use of hubs removes the length limitation of 10Base-T (100 m).

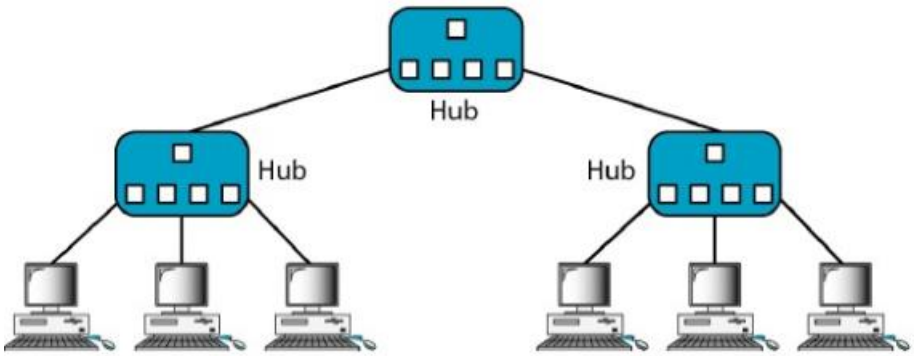


Figure 15.4 A hierarchy of hubs

Bridges

A bridge operates in both the physical and the data link layer. As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame.

What is the difference in functionality between a bridge and a repeater?

A bridge has filtering capability. It can check the destination address of a frame and decide if the frame should be forwarded or dropped. If the frame is to be forwarded, the decision must specify the port. A bridge has a table that maps addresses to ports. Let us give an example. In Figure 15.5, two LANs are connected by a bridge. If a frame destined for station 712B13456142 arrives at port 1, the bridge consults its table to find the departing port.

According to its table, frames for 71:2B:13:45:61:42 leave through port 1; therefore, there is no need for forwarding, and the frame is dropped. On the other hand, if a frame for 71:2B:13:45:61:41 arrives at port 2, the departing port is port 1 and the frame is forwarded. In the first case, LAN 2 remains free of traffic; in the second case, both LANs have traffic. In our example, we show a two-port bridge; in reality a bridge usually has more ports.

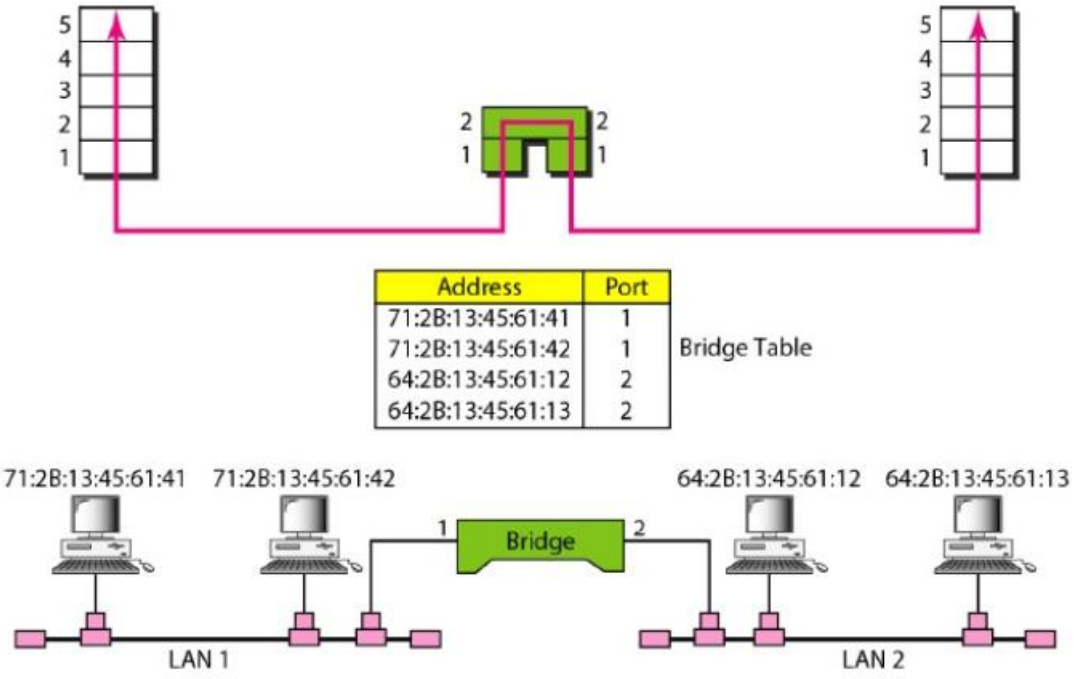


Figure 15.5 A bridge connecting two LANs

Note: A bridge does not change the physical addresses contained in the frame.

Transparent Bridges

A transparent bridge is a bridge in which the stations are completely unaware of the bridge's existence. If a bridge is added or deleted from the system, reconfiguration of the stations is unnecessary. According to the IEEE 802.1d specification, a system equipped with transparent bridges must meet three criteria:

- Frames must be forwarded from one station to another.
- The forwarding table is automatically made by learning frame movements in the network.
- Loops in the system must be prevented.

The earliest bridges had forwarding tables that were static. The systems administrator would manually enter each table entry during bridge setup. Although the process was simple, it was not practical. If a station was added or deleted, the table had to be modified manually. The same was true if a station's MAC address changed, which is not a rare event. For example, putting in a new network card means a new MAC address.

A better solution to the static table is a dynamic table that maps addresses to ports automatically. To make a table dynamic, we need a bridge that gradually learns from the frame movements. To do this, the bridge inspects both the destination and the source addresses. The destination address is used for the forwarding decision (table lookup); the source address is used for adding entries to the table and for updating purposes. Let us elaborate on this process by using Figure 15.6.

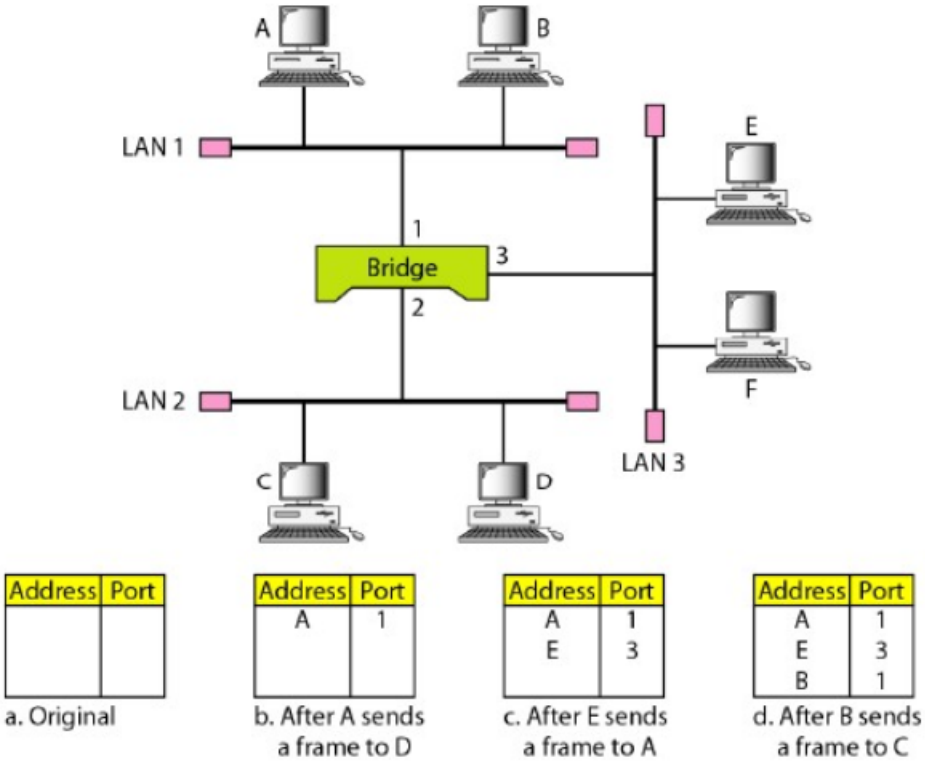


Figure 15.6 A learning bridge and the process of learning

1. When station A sends a frame to station D, the bridge does not have an entry for either D or A. The frame goes out from all three ports; the frame floods the network. However, by looking at the source address, the bridge learns that station A must be located on the LAN connected to port 1. This means that frames destined for A, in the future, must be sent out through port 1. The bridge adds this entry to its table. The table has its first entry now.
2. When station E sends a frame to station A, the bridge has an entry for A, so it forwards the frame only to port 1. There is no flooding. In addition, it uses the source address of the frame, E, to add a second entry to the table.
3. When station B sends a frame to C, the bridge has no entry for C, so once again it floods the network and adds one more entry to the table.

Loop Problem

Transparent bridges work fine as long as there are no redundant bridges in the system. Systems administrators, however, like to have redundant bridges (more than one bridge between a pair of LANs) to make the system more reliable. If a bridge fails, another bridge takes over until the failed one is repaired or replaced. Redundancy can create loops in the system, which is very undesirable. Figure 15.7 shows a very simple example of a loop created in a system with two LANs connected by two bridges.

1. Station A sends a frame to station D. The tables of both bridges are empty. Both forward the frame and update their tables based on the source address A.
2. Now there are two copies of the frame on LAN 2. The copy sent out by bridge 1 is received by bridge 2, which does not have any information about the destination address D; it floods the bridge. The copy sent out by bridge 2 is received by bridge 1 and is sent out for lack of information about D. Note that each frame is handled separately because bridges, as two nodes on a network sharing the medium, use an access method such as CSMA/CD. The tables of both bridges are updated, but still there is no information for destination D.
3. Now there are two copies of the frame on LAN 1. Step 2 is repeated, and both copies flood the network.
4. The process continues on and on. Note that bridges are also repeaters and regenerate frames. So in each iteration, there are newly generated fresh copies of the frames.

Solution of Loop Problem

To solve the looping problem, the IEEE specification requires that bridges use the spanning tree algorithm to create a loopless topology.

Spanning Tree

In graph theory, a spanning tree is a graph in which there is no loop. In a bridged LAN, this means creating a topology in which each LAN can be reached from any other LAN through one path only (no loop). We cannot change the physical topology of the system because of physical connections between cables and bridges, but we can create a logical topology that overlays the physical one. Figure 15.8 shows a system with four LANs and five bridges.

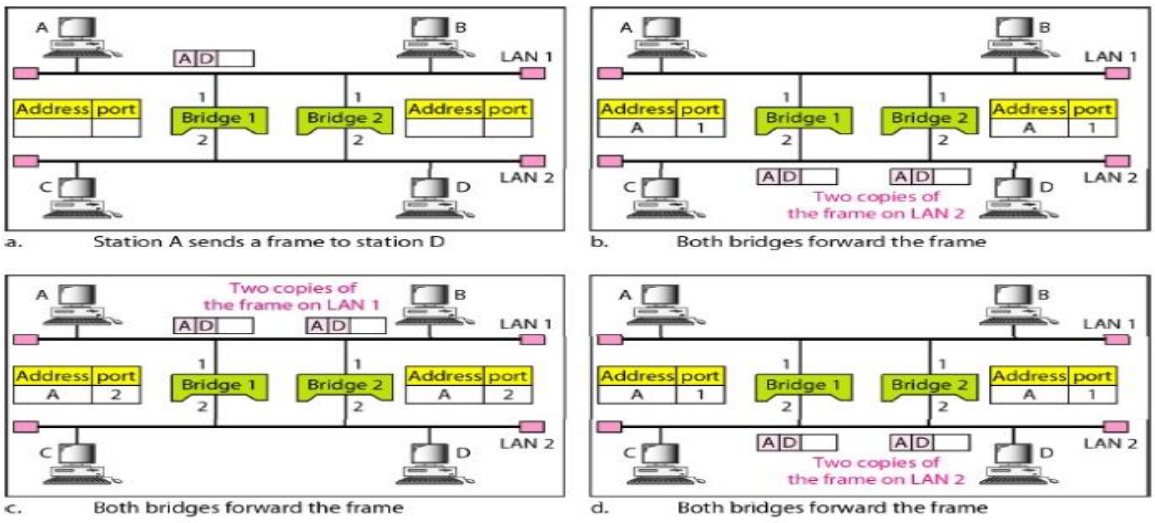
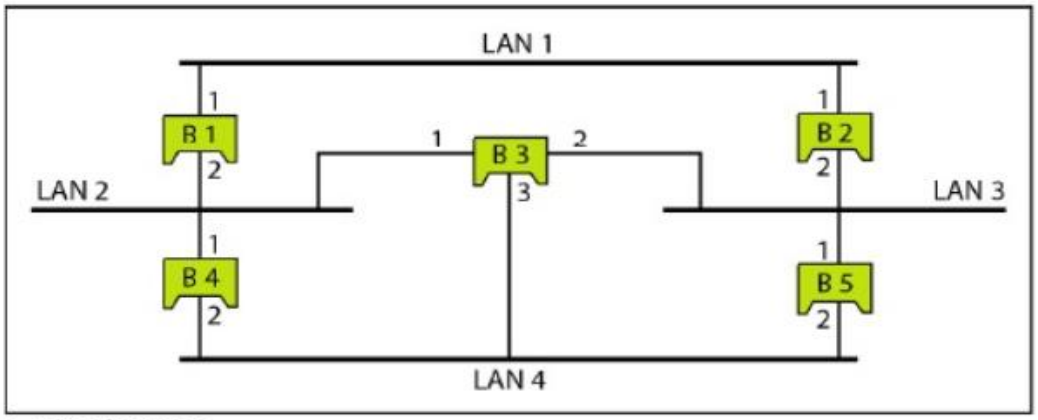


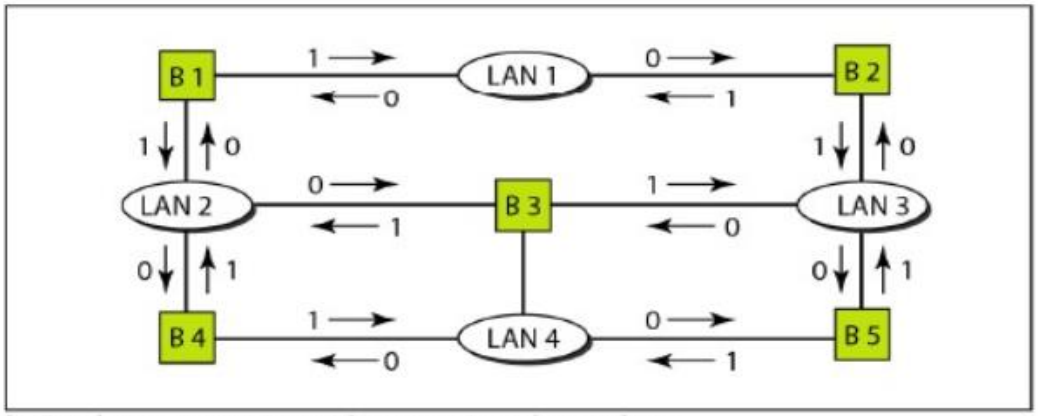
Figure 15.7 Loop problem in a learning bridge

We have shown the physical system and its representation in graph theory. We have shown both LANs and bridges as nodes. The connecting arcs show the connection of a LAN to a bridge and vice versa.

- To find the spanning tree, we need to assign a cost (metric) to each arc. The interpretation of the cost is left up to the systems administrator.
- It may be the path with minimum hops (nodes), the path with minimum delay, or the
- path with maximum bandwidth.
- If two ports have the same shortest value, the systems administrator just chooses one. We have chosen the minimum hops.
- The hop count is normally 1 from a bridge to the LAN and 0 in the reverse direction.



a. Actual system



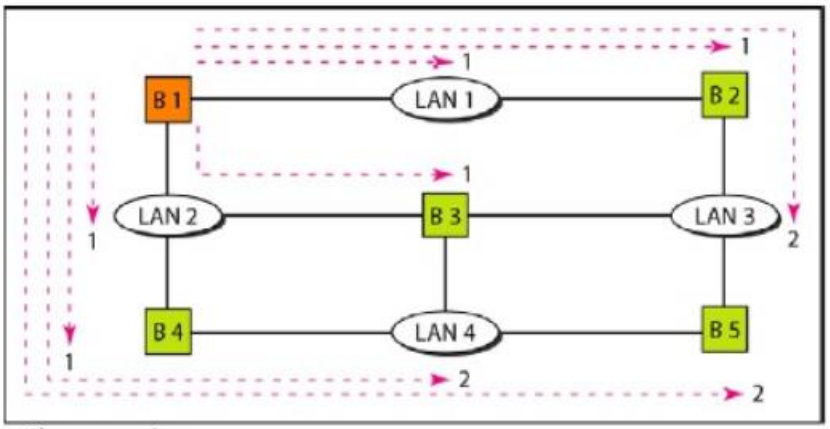
b. Graph representation with cost assigned to each arc

Figure 15.8 A system of connected LANs and its graph representation

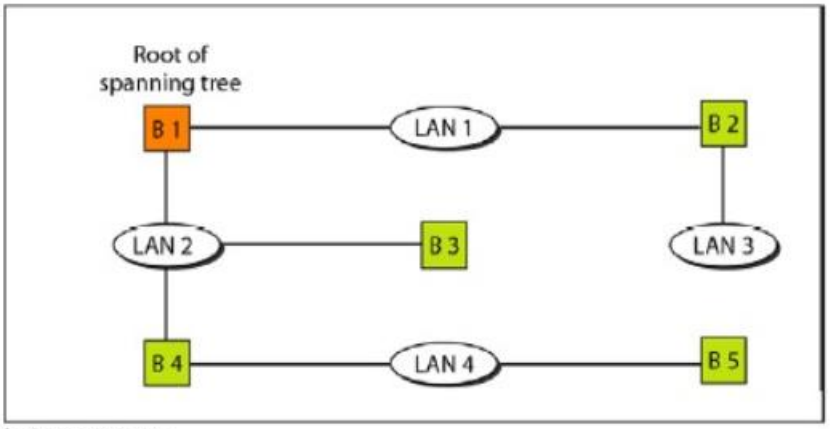
The process to find the spanning tree involves three steps:
1. Every bridge has a built-in ID (normally the serial number, which is unique). Each bridge broadcasts this ID so that all bridges know which one has the smallest ID. The bridge with the smallest ID is selected as the root bridge (root of the tree). We assume that bridge B1 has the smallest ID. It is, therefore, selected as the root bridge.
2. The algorithm tries to find the shortest path (a path with the shortest cost) from the root bridge to every other bridge or LAN. The shortest path can be found by examining the total cost from the root bridge to the destination. Figure 15.9 shows the shortest paths.
3. The combination of the shortest paths creates the shortest tree, which is also shown in Figure 15.9.
4. Based on the spanning tree, we mark the ports that are part of the spanning tree, the forwarding ports, which forward a frame that the bridge receives. We also mark those ports that are not part of the

spanning tree, the blocking ports, which block the frames received by the bridge. Figure 15.10 shows the physical systems of LANs with forwarding points (solid lines) and blocking ports (broken lines).

Note that there is only one single path from any LAN to any other LAN in the spanning tree system. This means there is only one single path from one LAN to any other LAN. No loops are created. You can prove to yourself that there is only one path from LAN 1 to LAN 2, LAN 3, or LAN 4. Similarly, there is only one path from LAN 2 to LAN 1, LAN 3, and LAN 4. The same is true for LAN 3 and LAN 4.



a. Shortest paths



b. Spanning tree

Figure 15.9 Finding the shortest paths and the spanning tree in a system of bridges

Switches

When we use the term switch, we must be careful because a switch can mean two different things. We must clarify the term by adding the level at which the device operates. We can have:

- Two-layer switch: performs at the physical and data link layers.
- Three-layer switch. is used at the network layer; it is a kind of router.

A two-layer switch is a bridge, a bridge with many ports and a design that allows better (faster) performance. A bridge with a few ports can connect a few LANs together. A bridge with many ports may be able to allocate a unique port to each station, with each station on its own independent entity. This means no competing traffic (no collision, as we saw in Ethernet).

- A two-layer switch, as a bridge does, makes a filtering decision based on the MAC address of the frame it received.

- However, a two-layer switch can be more sophisticated. It can have a buffer to hold the frames for processing.
- It can have a switching factor that forwards the frames faster. Some new two-layer switches, called cut-through switches, have been designed to forward the frame as soon as they check the MAC addresses in the header of the frame.

A three-layer switch is a Routers, a router is a three-layer device that routes packets based on their logical addresses (host-to-host addressing).

- Router is faster and more sophisticated. The switching fabric in a router(three-layer switch) allows faster table lookup and forwarding.
- A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route.
- The routing tables are normally dynamic and are updated using routing protocols.

Figure 15.11 shows a part of the Internet that uses routers to connect LANs and WANs.

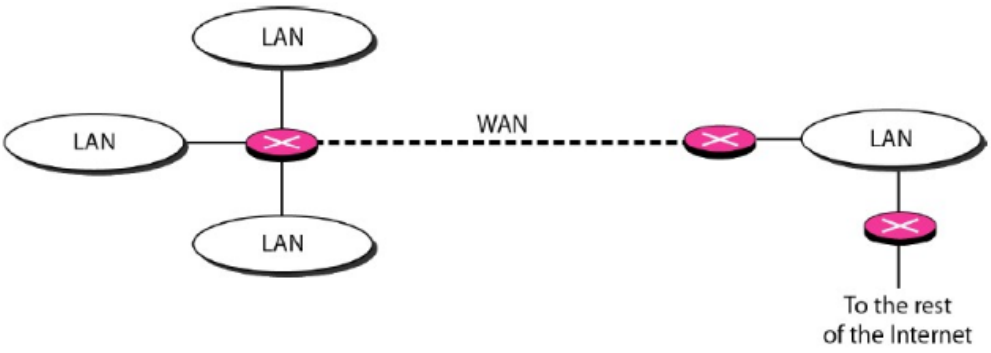


Figure 15.11 Routers connecting independent LANs and WANs

Router

Although some textbooks use the terms gateway and router interchangeably, most of the literature distinguishes between the two.

- A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model.
- A gateway takes an application message, reads it, and interprets it.
- This means that it can be used as a connecting device between two internetworks that use different models. For example, a network designed to use the OSI model can be connected to another network using the Internet model.
- The gateway connecting the two systems can take a frame as it arrives from the first system, move it up to the OSI application layer, and remove the message.
- Gateways can provide security. The gateway is also used to filter unwanted application-layer messages**.**