CHAPTER Four

Bridges and Layer-2 Switches

Merely putting together a local area network does not meet requirements of an organization. Very soon, the number of stations swells up, required geographic coverage goes beyond what is technically feasible and need arise to interconnect several local area networks to share common information base. LAN Bridge, Layer-2 Switch, and Router are the devices required to interconnect two or more local area networks.

5.1 Motivation for Using LAN Bridges

A local area network is the stand-alone network with capability to provide communication services to the end systems. There is however, always need to communicate with the stations connected on the other local area networks. Bridge is intermediary device that interconnect two or more local area networks. One would think that it should be simpler to form a bigger LAN that spans all the stations but it may not always be possible because:

- There is limit on the maximum number of stations that can be connected on a single LAN.
- The maximum physical size of a LAN is limited.
- Upgrading the existing infrastructure can be very costly and the investments already made are wasted.

Therefore, the solution is to interconnect two LANs as separate entitles using a bridge. At times, bridge installations may be done from a different perspective. There may be reasons to partition an existing LAN into several LANs using bridges. For example, if the performance of a LAN is poor because of too many collisions, it can be improved by partitioning a LAN into several interconnected LANs using Bridges. Bridge partitions the collision domain and therefore the performance improves.

A bridge is to be differentiated from a repeater and router .A repeater merely regenerates electrical signals and extends the physical medium domain of a LAN. It works at the physical layer level. Thus a network having repeaters still constitutes one single LAN and single collision domain.

Router is a packet switch implemented at the layer-3. The packets are routed and forwarded at layer-3.Thus all physical layers and data link layer protocol differences are taken care of. The addressing scheme at the layer-3 is structured. A layer-3 address is composed of two parts: - network part and host (end-system) part.

Therefore, unlike LAN networks, which work in broadcast mode, more intelligent and dynamic routing decisions are possible at layer-3 networks.

5.2 LAN Bridge

Bridge is the device that is attached to two or more local area networks .It takes MAC frames from one LAN and sends them across to the other LAN. Note the difference between a bridge and a repeater. A repeater does not look at the address field and regenerates all the frames.

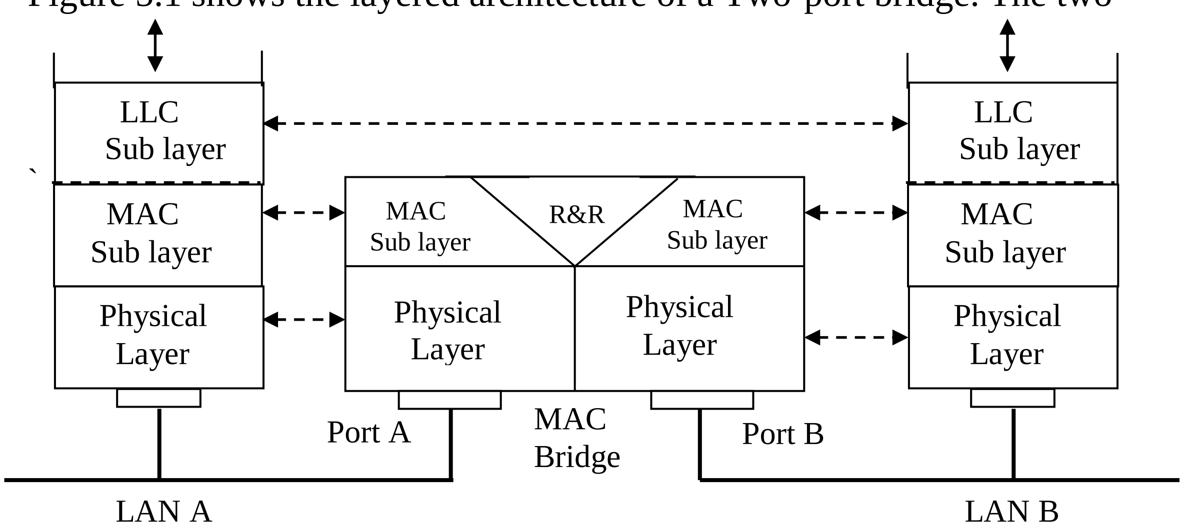
Due to the differences in the LAN technologies make it impractical to use the bridge to interconnect two dissimilar local area networks for the following reasons:

- Each type of LAN has its own MAC protocol and MAC frame format.
- The maximum size of MAC frame is different in LAN technologies.
- The data rates are different
- LAN management and priority management functions are different.

Therefore, Bridges generally interconnect LANs of the same MAC protocol type. Interconnection of dissimilar LAN types is nowadays dealt with using Router.

5.2.1 Bridge Architecture

Figure 5.1 shows the layered architecture of a Two-port bridge. The two



R & R: Relay and Routing functions.

Figure 5.1 Layered Architecture of a Bridge physical layers and MAC sub layers are matched (similar) with those of two LANs. The two MAC sub layers of the bridge have relay and routing functions between them.

When a MAC frame is received by the bridge at its one port, it examines its destination address .If the bridge decides that the frame should be transferred across, it forwards the frame to the other port using relay and routing function.

The decision whether to forward the frame or not is either taken by the bridge (transparent bridge) or alternatively, the MAC frame itself contains the routing instruction (source routing bridge). It is to be noted that:

- The bridged LANs maintain their identity although the user may not perceive so.
- A bridge does not extend the collision domain of one Ethernet to the other interconnected Ethernet.

5.2.2 Types of Bridges

The most widely deployed bridges are of two types:

- Transparent bridges
- Source routing bridges

Transparent bridges are also known as spanning tree bridges. They are used in Ethernet environment. Source routing bridges are used for Token Ring LANs. Source routing is part of IEEE 802.5 token ring specifications. Besides the protocol differences, these two types of bridge differ in the way the routing decisions is made. A transparent bridge is invisible to the stations in the network. The stations perceive the network as an extended network. The routing decisions are made by the bridge. A transparent bridge creates and maintains a comprehensive forwarding table of all destination stations.

In source routing bridges, as the name suggests, the routing is decided by the station sending a frame .The sending station incorporates the route to be followed to the destination in the frame. The bridge merely follows the routing instructions incorporated by the source. The source routing bridges, therefore, do not require any routing table for forwarding frames. Transparent bridges, therefore, are more complex than source routing bridges.

5.3 Transparent Bridges

A transparent bridge works in "Plug and Play" mode, i.e., when the bridge is attached to two Ethernet LANs it starts working. The network software configurations of the station need not be altered in any way. The bridge achieves this result by operating in promiscuous mode, i.e., it receives all the frames whether or not they are addressed to it. It builds a forwarding table by looking at the source address of the frame that hits its port. Based on the table, the bridge can, then, forward the frames from one Ethernet to the other. Thus the description of the operation the transparent bridge as consisting of the following two basic functions:

- Frame filtering and forwarding the frames based on the forwarding table.
- Learning the addresses of the stations and creating forwarding table.

5.3.1 Frame Filtering and Forwarding

As Ethernet LANs operate in broadcast mode, all the frames, irrespective of their destination, appear at the port of the bridge connect to the LAN, Figure 5.2. The bridge maintains a table of the MAC address of the all stations on the extended bridge network. The table is maintained port-wise. In other words, by looking at the table, it is possible to find out the port on which a particular destination address is available. When abridge receives a frame at any of its ports, it takes one of the following actions:

1. Filtering: If the destination address is available on the same port through which it received the frame, the bridge filters the frame.

2. Forwarding: If the bridge determines that the destination address is available on the different physical port than the one through which the frame was received, it forwards the frame onto that port. If the destination address on the frame is global address or multicast address, the bridge sends the frame on all its ports except the one from which it received the frame.

3. Flooding: If the bridge does not find the address in its forwarding table, it floods (sends) the frame on to all the physical ports except the one from which it received the frame.

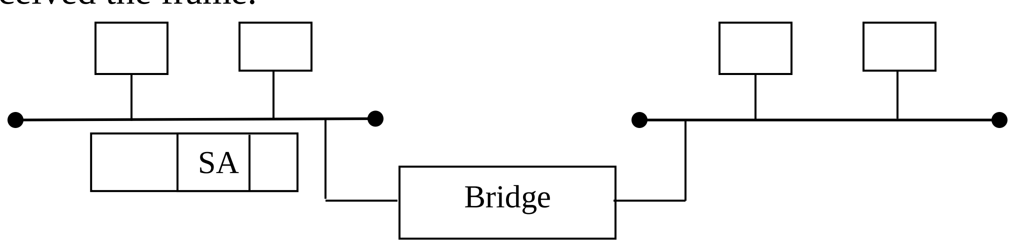


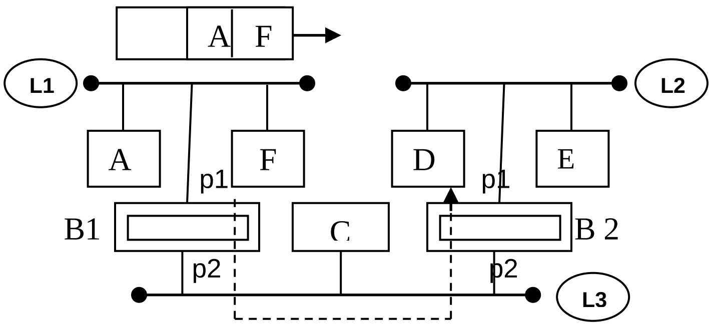
Figure 5.2 Bridged Ethernet LANs

5.3.2 Learning Address

When a bridge comes up for the first time, its forwarding table is empty. It builds up the address database by examining the source address field of the MAC frames that hits its ports. Whenever the bridge finds that the source address is not in its forwarding table, it updates the forwarding table with the source address and the identity of the port at which the frame was seen. Thus as the stations exchange the frames, the bridge gradually builds up its forwarding table. The process can be understood through the following example:

There are three LANs L1, L2, and L3, two bridges B1and B2, and five stations, A, C, D, E, and F on the networks, Figure5.3.

- To start with, the forwarding table of bridges B1, and B2 are empty. Station A sends a frame to station F on L1.
- Bridge B1 receives the frames on its port P1. It floods the frame through its port P2. It also adds updates to its forwarding table. It adds station A under port P1, Fig.5.3a.
- Bridge B2 receives the frame on its port P2. It floods the frame through its port P1. It also updates its forwarding table. It adds station A under port P2, Fig .5.3a.
- Station F replies to A on L1. Bridge B1 filters the frame because station A is available on the same LAN. It also updates its forwarding table. It adds station F under port P1, Fig.5.3b.
- Station F sends a frame to station E. Bridge B1 receives the frame on its ports P1. It floods the frame through its port P2, Fig.5.3c.
- Bridge B2 receives the frame on its port P2.It floods the frame through its port P1. It also updates its forwarding table. It adds station F under port P2. Fig 5.3c.
- Station E sends its reply to station F. Bridge B2 receives this frame on its port P1. It forwards the frame to L3 through its port P2 after consulting its forwarding table. It also updates its forwarding table. It adds station E under port P1, Fig. 5.3d.
- Bridge B1 receives the frame on its port P2. It forwards the frame on to L1, through its port P1 after consulting its forwarding table. It also updates its forwarding table. It adds station E under port P2, Fig.5.3d.
- The process continuous and the bridges build up their forwarding table, Fig.5.3e.



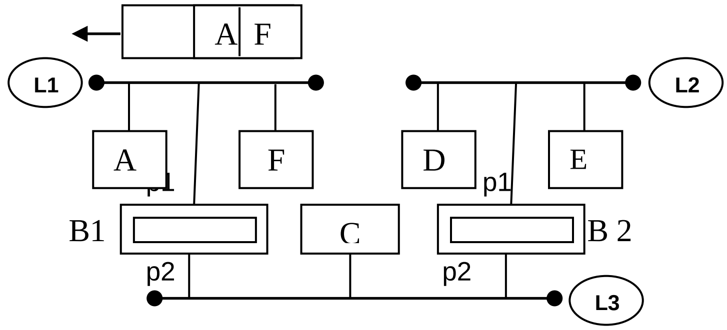
P1	P2
A	

Forwarding table of B1

P1	P2
	A

Forwarding table of B2

(a)



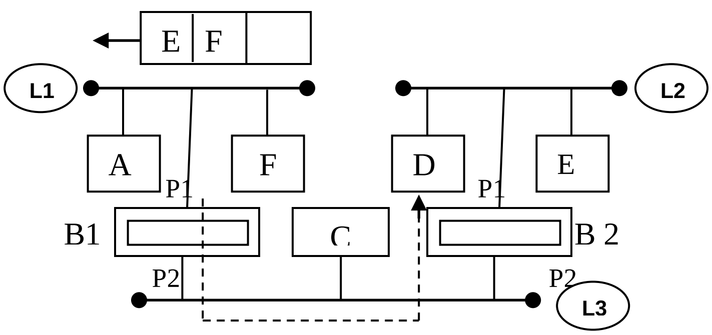
P1	P2
A	
F	

Forwarding table of B1

P1	P2
	A

Forwarding table of B2

(b)



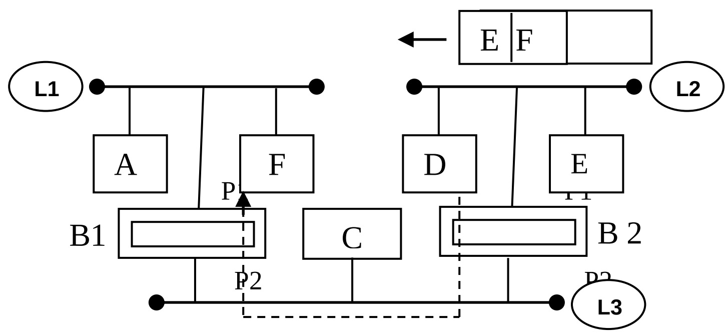
P1	P2
A	
F	

Forwarding table of B1

(c)

P1	P2
	A
	F

Forwarding table of B2



P1	P2
A	E
F	

Forwarding table of B1

(d)

P1	P2
E	A
	F

Forwarding table of B2

Forwarding table of B1

P1	P2
A	E
F	C
	D

(e)

P1	P2
E	A
D	F
	C

Forwarding table of B2

Fig. 5.3 Learning Address

If a station is moved from one Ethernet LAN to another, the old entry is deleted from the forwarding table and the new entry is rebuild automatically. Similarly, if a station is down, its entry is deleted from the table automatically.

5.3.3 Multiple Paths

If the topology of the interconnected Ethernet LANs has loops, there will be more than one path interconnecting two segments of a network. Multiple interconnecting paths can affect network operations in three ways:

- Confusion during address learning.
- Endless circulation of frames with unknown destination.
- Broadcast storm

Consider that there are two bridges B1 and B2, interconnecting two Ethernet LANs, L1 and L2, Figure 5.4.The forwarding tables of the bridges are empty to start with. When station A on LAN1 transmits a frame addressed to station B on LAN L2, both the bridges will take note that station A is available on their port P1. They will individually flood the frames to LAN2 through their port P2. These frames will be received by station B. Frame released by one bridge will also be received by the other bridge.

When the frame released by B2 on LAN L2 is received by B1, bridge B1 immediately updates its forwarding table again based on the source address contained in the received frame. It also transmits the frame through its port p1.the forwarding table now indicates that A is available on port P2.Bridge B2 also does the same when it receives the frame released by B1 on LAN L2.Although station A is on LAN L1,the forwarding tables of the two bridges do not indicate so. Thus, these two frames keep circulating in the ring and each time updates the entries of the forwarding table.

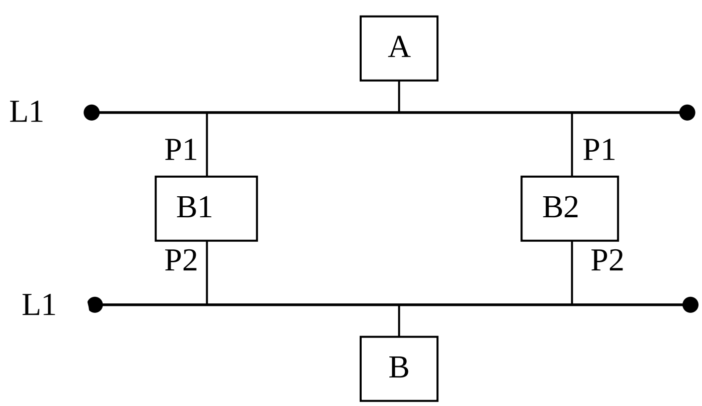


Figure 5.4 Multiple Paths Affect Address Learning

Figure 5.5 shows another situation where a broadcast frame creates a storm of frames. Station P on LAN L1 sends a broadcast frame. Bridge B3 receives two frame from bridges B1 and B2. Bridge B4 sends these two frames back to LAN L1. Bridges B1 and B2 forwards these two frames back to bridge B3 as four frames. Thus the number of frames gets multiplied as they go along the loop anticlockwise. We have not yet considered the storm that will be generated in clockwise direction by the first frame that hits bridge B4 directly.

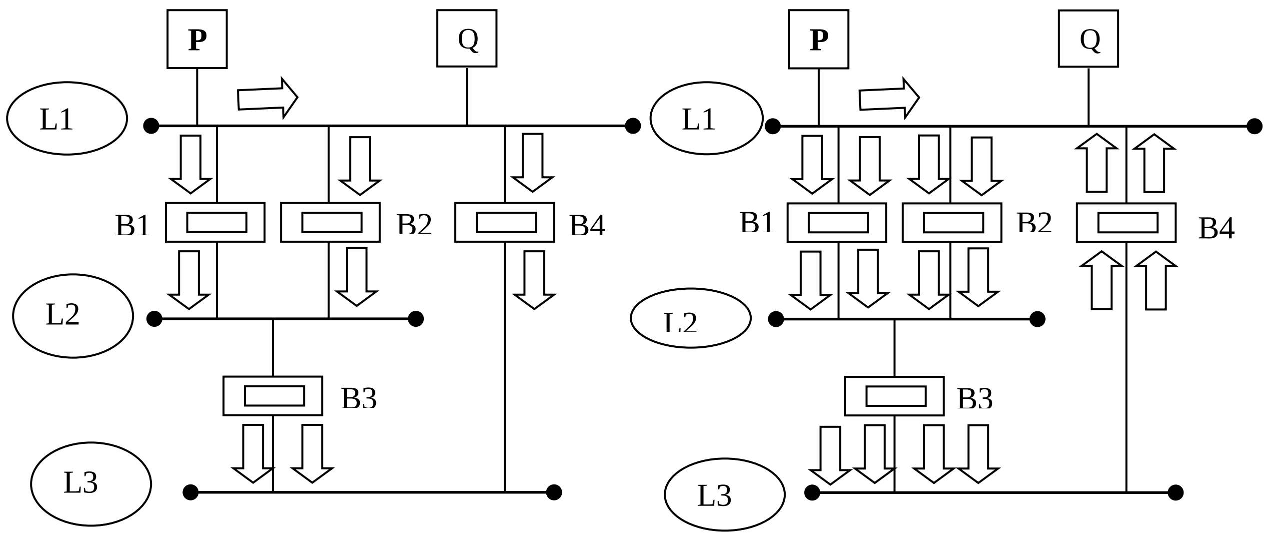


Figure 5.5 Frame Storm Due to Parallel Paths

Multiple paths are built into the network to improve network resilience against failure of segment or a bridge of a network. When one path fails, the alternative path takes over. But multiple paths can not be allowed to coexist. Therefore, what we need to ensure is that there is only one path interconnecting any two segments of network at any point of time in the network. If there is a failure in any section of the network, an alternative path is automatically built through the redundant network resources. This is achieved through the spanning tree protocol.

5.4 Spanning Tree Protocol

A spanning tree is a graph structure that includes all the bridges and stations on an extended network but it never has more than one active path connecting any two stations. Therefore, the complication of multiple path never occur. For example, Figure 5.6b shows the spanning tree topology of the network shown in Figure 5.6a. Note that all the multiple paths have been removed from the network.

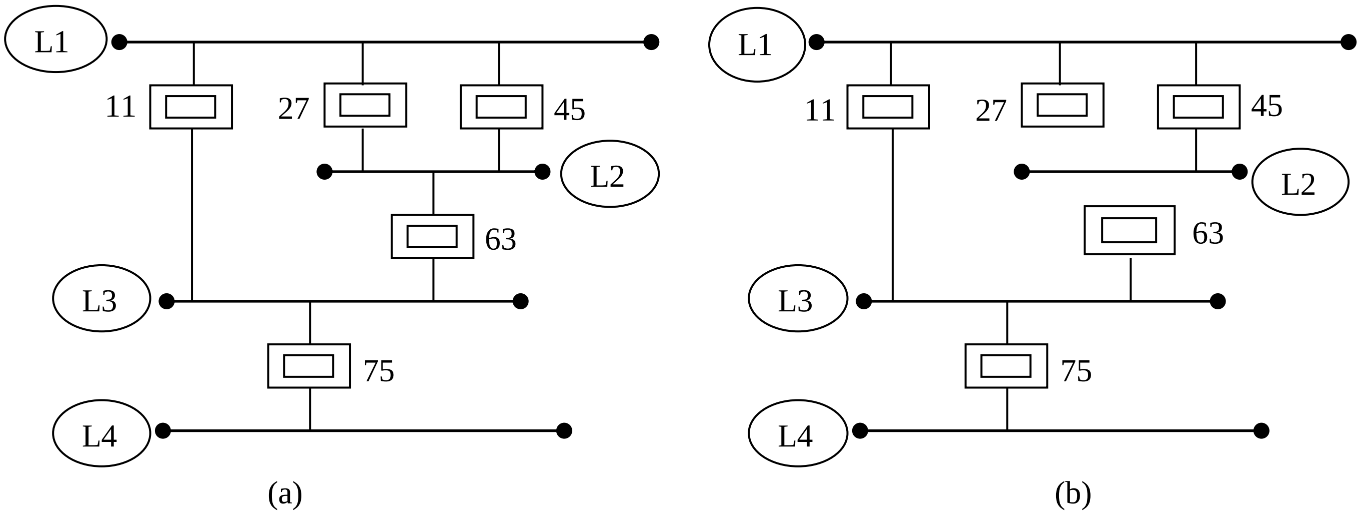


Figure 5.6 spanning tree topology

What we need is an algorithm by which the bridges will be able to drive the spanning tree automatically. The algorithm must be such that topological changes in the network due to additions, deletions of stations or faults are automatically discovered and spanning tree is reworked dynamically. Before we go to the algorithm, let us understand some of the definitions associated with the algorithm.

Root Bridge: the bridge with the lowest identifier is called the root bridge.

Port cost: each port of a bridge has an associated cost parameter, which is the cost of transmitting a frame through the particular port. The default value of the port cost is 1000/ (bit rate-Mbs). The port cost is associated with the bits transmission through a port. . Reception of bits through a port has no cost attached to it.

Root path cost: Root path cost is the cost associated with a path to a root bridge from a port of another bridge. It is the sum of all the intervening port cost parameters. Note that cost of the transmitting ports only is added to arrive at the root path cost.

Root port: A bridge may have several paths emanating from its ports to the root bridge. The port having the least root path cost is called "Root Port." If there are more than such ports, the port with the lowest port identification number is chosen as the root port.

Designated bridge: If there are several bridges connected to a LAN segment, one of the bridge is designated bridge for forwarding the data frames from that LAN segment. Selection of the designated bridge is based on the root path cost. The bridge that offers least root path cost from the LAN segment is selected as the designated bridge for that LAN segment. If more than one bridge have the same root path cost, the bridge with lower identifier number is chosen as the designated bridge.

Designated Port: the port of the designated bridge that connects to the LAN segment is called designated port.

5.4.1 Bridge Protocol Data Unit (BPDU)

To construct the spanning tree and for other management functions, a control frame called configuration Bridge Protocol Data Unit (BPDU) is exchanged by the bridges. Configuration BPDUs are generated by the bridges and have MAC multicast address. A configuration BPDU generated by a bridge contains the following fields:

- Bridge Identifier(B-ID)
- Root Identifier(R-ID) as perceived by bridge
- Root Path Cost (RPC)of the bridge.
- Port Identifier(P-ID)
- Any other information

The format of BPDU is shown in Figure 5.7.

2	1	1	1	8	4	8	2	8	→Bytes
Protocol Id	Port ver	BPDU type	Other	R-Id	RPC	B-Id	p-Id	other	

Figure 5.7 Format of BPDU

5.4.2 Constructing the Spanning Tree

Constructing the spanning tree involves the following steps:

1. Identification of the root bridge,
2. Identification of the root ports,
3. Selecting of the designated bridges for every LAN.

After the above steps are carried out, the root ports and the designated ports of the bridges are set in forwarding mode and all other ports are retained in blocked mode. In forwarding mode, a port becomes active for the data frames. Once this is done, the goal of spanning tree algorithm is achieved and there will be only one path from any station in the network.

To understand the spanning tree algorithm, consider a network as shown in Figure 5.8. It consists of 4 LAN segments and 5 bridges having identifiers, (B-Id), 11, 27, 45, 63, and 75. The port cost (C) associated with each port is also indicated in the figure.

To begin with, all the ports of all the bridges are in blocked mode. A port in blocked mode does not accept any data frame but it accepts BPDUs.

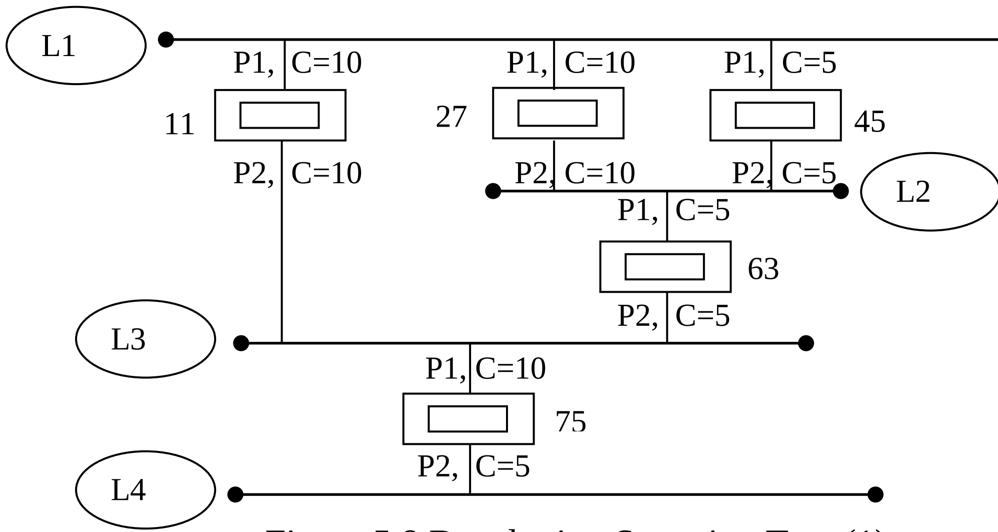


Figure 5.8 Developing Spanning Tree (1)

Selection of the root bridge

The bridge with the lowest bridge identifier (B-Id) is selected as Root Bridge. Root Bridge is identified as follows:

- Each bridge asserts that it is the root bridge by sending configuration BPDU on all its ports, Figure 5.9. It indicates its identity(B-Id), root bridge identity(R-Id) which is its own identity, root path cost(RPC) which is zero and port identity(P-Id) in the BPDUs.

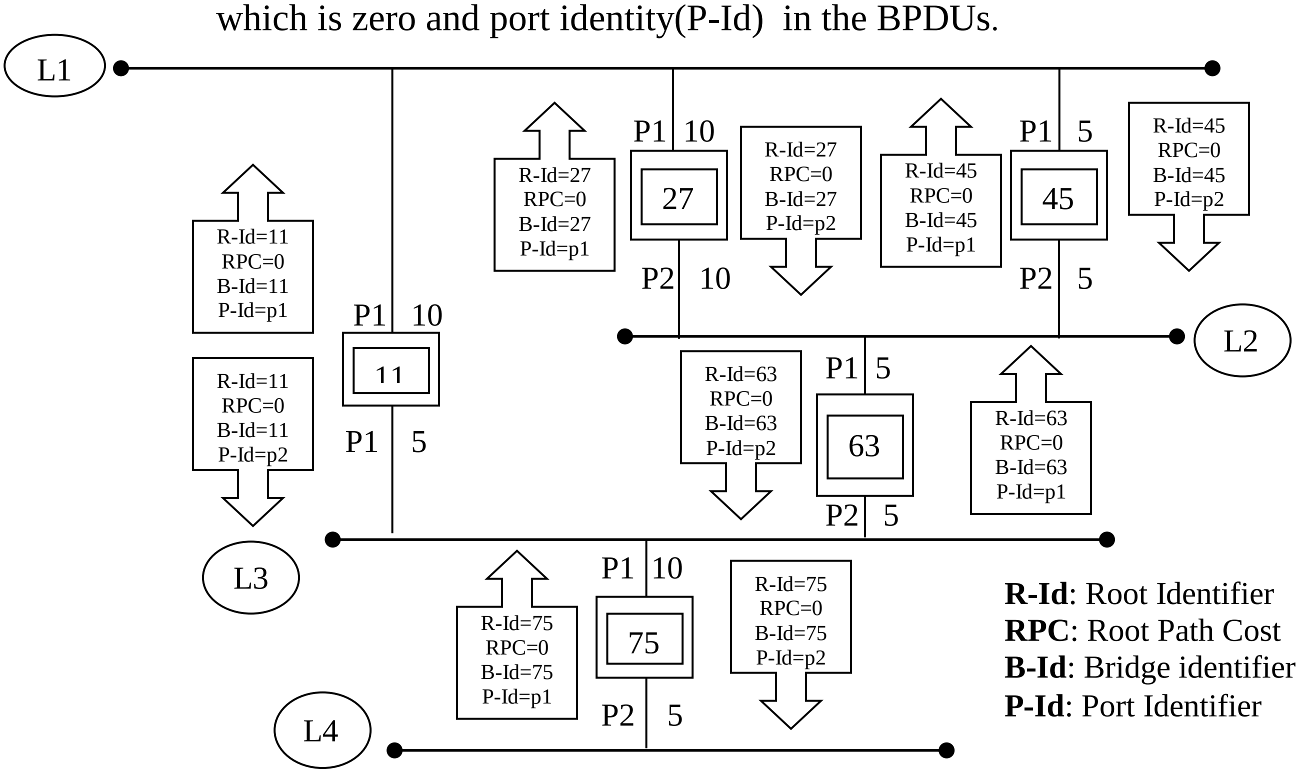


Figure 5.9 Developing Spanning Tree (2).

- If a bridge receives a configuration BPDU with lower root bridge identity than its own identity (R-Id < B-Id) on any of its ports, it stops sending its configuration BPDU and forwards the received BPDU on its other ports. When forwarded by a bridge, a BPDU undergoes the following changes:
    - The bridge puts its own identity in the (B-Id) field.
    - The bridge puts its own port identity in the (P-Id) field.
    - The root path cost is incremented by the cost of the port through which the BPDU is received because later it will be transmitting through this port. The root bridge identity (R-Id) is retained as it is.
- If a bridge receives a configuration BPDU with higher root bridge identity (R-Id) than its own identity (B-Id) on a port, it continues sending its configuration BPDUs.

Thus all the bridges except bridge 11 stop sending their configuration BPDUs. Bridge 11 is identified as the root bridge by all the other bridges.

Identification of the root ports

Every bridge other than the root bridge determines its root port, which is the port with the lowest root path cost. It involves the following steps:

- The configuration BPDUs generated by the root bridge are forwarded by all the other bridges on their ports. After making the necessary changes in the B-Id, P-Id, and RPC fields, Figure 5.10. The root path cost is incremented by the cost of the port through which the BPDU is received.
- Each bridge determines which of its ports has the lowest root path cost and that port is selected as the root port. For example, bridge 27 receives three BPDUs, one from Root Bridge 11 on port P1, second from bridge 45 on port P2, and the third from bridge 63 also on port P2. It calculates the root path cost as 10, 15, and 15 from these BPDUs, respectively. It decides P1 as its root port. If there is a tie, the port with the lower port identifier is selected as root port.
- The root ports are put in the forwarding mode. Other ports remain in the blocked mode.

Selection of the designated bridges and the designated ports

A bridge is designated for each LAN segment to carry its data frame to the other LAN segments. If there are several bridges connected to a LAN, the bridge that has the lowest RPC is selected as the designated bridge. For example, LAN2 has three bridges 27, 45, and 63attached to it, bridge 45 is the designated bridge for LAN2. Port, P2, of bridge 45 that connects to LAN2, is called the designated port.

The decision of selecting the designated bridge is made by the bridges themselves. For example, in case of LAN2 the bridges 27, 45, 63 decide as follows:

- When bridge 45 receives BPDUs offering RPC of 10 from bridge 27 and RPC of 5 from bridge 63, it decides as follows:
    - Bridge 27 has higher RPC and therefore it can not be the designated bridge for LAN2.
    - Bridge 63 has the same RPC but it has higher B-Id and therefore it can not be designated bridge for LAN2.

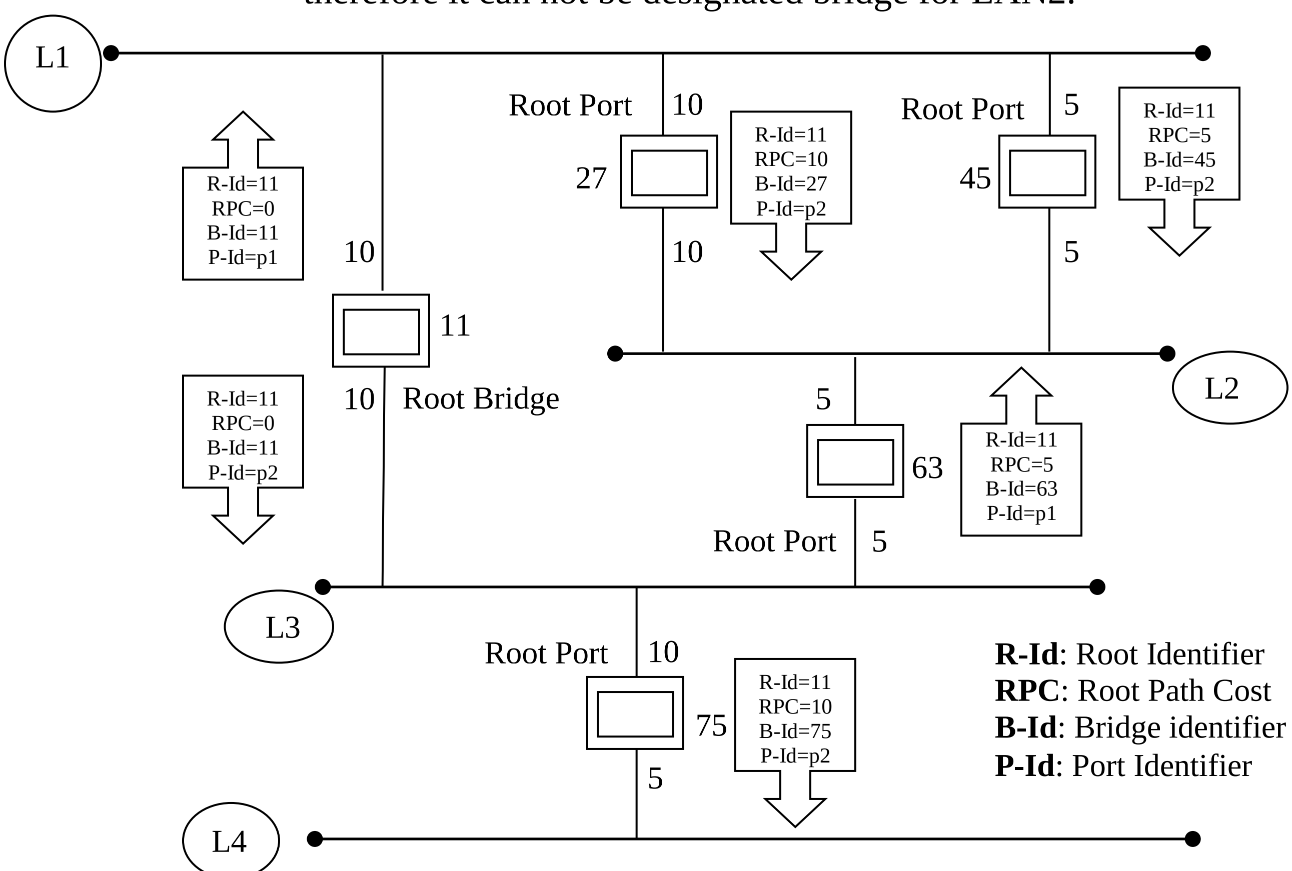


Figure 5.10 Developing Spanning Tree (3)

Having carried out this exercise, bridge 45 assumes the role of the designated bridge and puts its port P2 (designated port) in the forwarding mode.

- Bridges 27 and 63 carry out similar exercise and decides to keep their ports that connect to LAN2 in the blocked mode.

The ultimate network scenario is shown in Figure 5.11. The dotted lines the blocked link. Note that the root bridge is the designated bridge for all the LANs connected to it directly. From this moment onwards, normal network operation is possible. Every station will have only one path to any other station on the network.

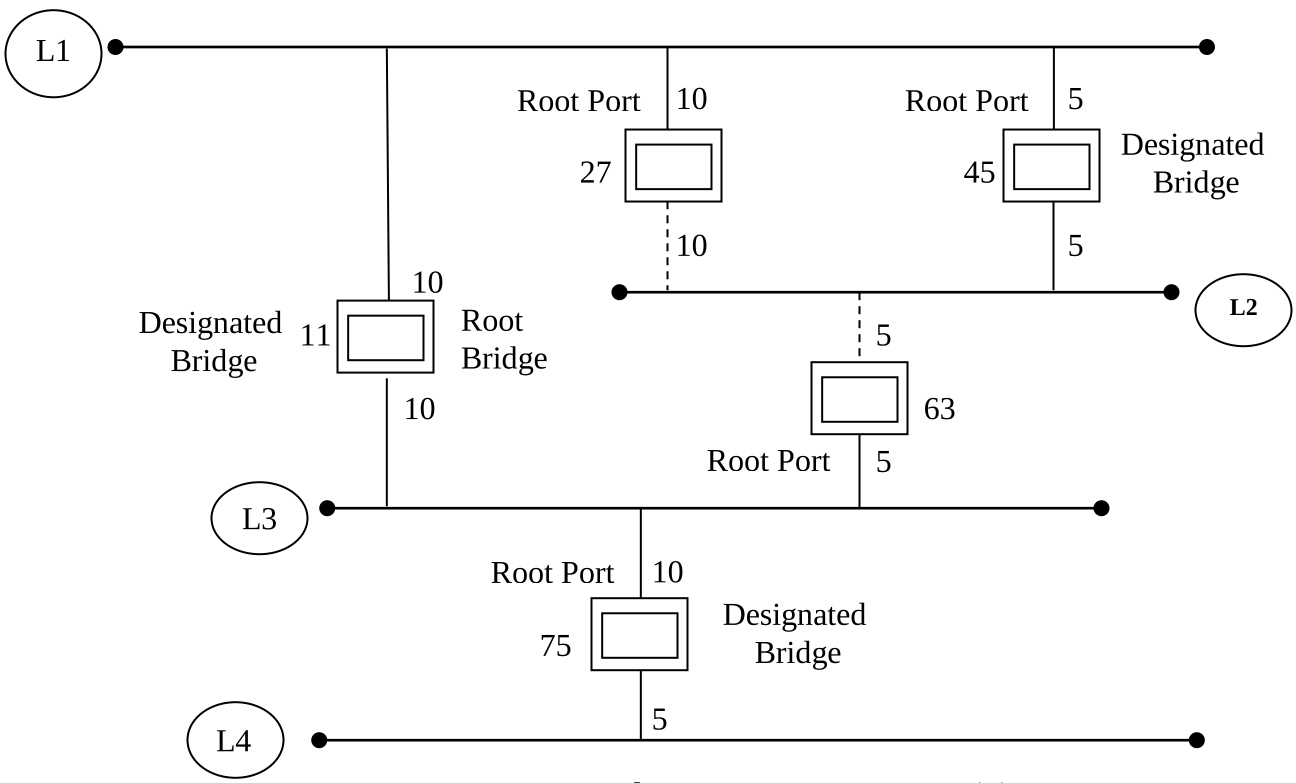


Figure 5.11 Developing Spanning Tree (4)

5.5 Layer 2 Ethernet Switches

We have seen three types of Ethernet devices so far-repeater, hub, and transparent bridge. These devices are required when there is need to expand a local area network in terms of the number of stations and their geographic distribution. During 1990s, these Ethernet devices replaced by Ethernet switches, also called layer-2 switches.

5.5.1 Motivations Behind Ethernet Layer-2 Switches.

Layer-2 switches were introduced in the network when the required data rate, geographic coverage, and number of stations could not be supported on the Ethernet. In the following there are some issues involved and how layer -2 switches could address these issues.

Collision domain

As shown in the Figure 5.12, in case of repeater or a hub, there is one Ethernet and one collision domain. As the numbers of stations and transmission rate increases, so does the collisions and eventually a stage comes the throughput performance deteriorates. At this stage it becomes necessary to partition the local area network using a bridge.

A bridge has buffer and it uses a store and forward mechanisms to send the frames. Store and forward mechanism does not allow frames on one segment of the network to collide with the frames on the other segment of the network.

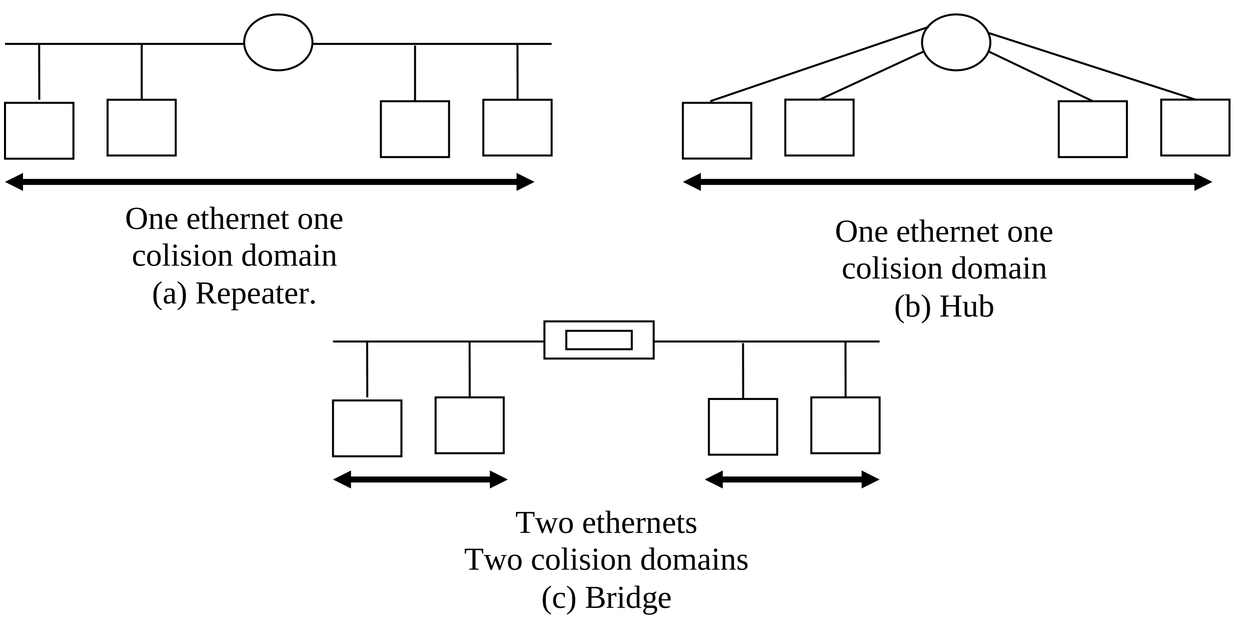


Figure 5.12 Collision Domain in a Network Having a Repeater, a Hub or a Bridge

Therefore, a bridge effectively partitions the network into separate Ethernets, each having its own collision domain. Thus the constraint of supporting large number of stations on one local area network is overcome. But a bridge has limitations of number of ports. It can partition a LAN in a few segments, say two or four, which does not meet the requirement.

Layer-2 switch is functionally a multi-port bridge. It can have a number of ports ranging from 12 to a few hundreds. With such large number of ports it is possible to create big collision free network. Each station is connected to the switch on point-to-point full duplex Ethernet link.

Multi-rate adaptation

Repeaters and hub do not support different speeds at their ports, i.e., 10 Mbps Ethernet can not be interconnected with100 Mbps Ethernet using a hub or repeater. A transparent bridge can do this because it has buffer to store the frames temporarily. But this capability is fully made use of in layer-2 switches.

5.5.2 Latency in Ethernet Layer-2 Switch

When a frame is received on a port of a switch , the source address is added to the forwarding table, if it is not already there. The destination address in the frame is searched in the forwarding table for determining the output port of the switch. The frame is put in the queue for subsequent transmission on that port. Such layer2 switch is categorized as store and forward switch.

In a store and forward switch, the latency time is the time taken from ingress of the frame to its egress from switch. Minimum latency will be when there are no frames in the queue. For a 1500 octets frame at 10 Mbps the latency comes to over 1ms. Latency of the switch can be reduced by starting to forward the frame on the output port as soon as the source and the destination address have been received. Such layer-2 switch is called ***cut-through*** switch and it reduces the switch latency to less than 50µs.

However, there are several situations where cut-through switching will not work or may not be desirable. For example:

- If the destination port is busy, the frame must put in the queue, so there is no advantage gained.
- The source and the destination ports must be operating at the same data rate for cut-through to work.
- If an error is detected in a frame, a store and forward switch will filter the frame but a cut-through switch will not. Therefore, if error rate is above a defined threshold, the cut-through switches are designed to change over to store and forward mode.

5.5.3 Basic Features of Ethernet Layer-2 Switch

Considering that layer-2 switch is functionally similar to a multiple port bridge, so the basic features of layer-2 switch can be summarized as follows:

1. Layer -2 switches operate in the same way as transparent bridges for functions like address learning, filtering, and forwarding frames. They also have forwarding tables like bridges.
2. Spanning tree protocol is used to remove multiple paths between two stations.
3. Most of the stations are connected to switches on full duplex point to point links.
4. They support rate adaptation, i.e., a switch can send with the transmission rate at 100 Mbps on a port to another port of rate 10 Mbps.
5. The network is collision free if only point-to-point full duplex links are used.
6. a switch can have large number of ports. Several switches can be interconnected to meet the port requirements.

As compared to a bridge, a switch is faster because several of its functions are implemented in hardware. The current implementation of layer-2 networks use switches instead of bridges.