Name : Adom Pokuaah

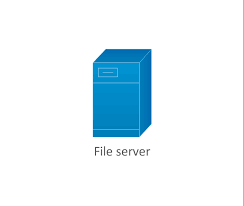
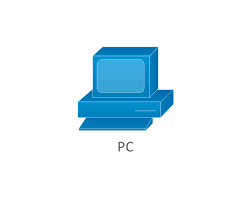
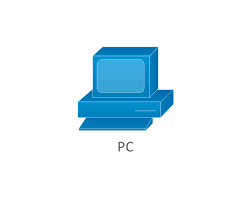
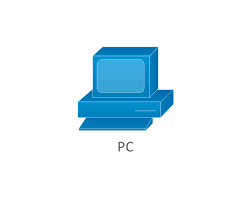
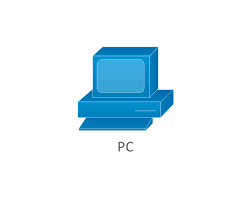
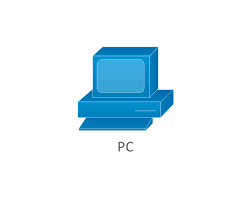
Index : 6825116

**Problems in the network**

1. Number of collision domain is one
2. Number of broadcast domain is one
3. There are too many hosts in a single broadcast domain
4. Too many host in the broadcast domain causes broadcast storm

**Scenario 1**

Eliminating all collisions by replacing all the hubs with switches and assume is on one Local Area Network with no internetwork.



3

2

1

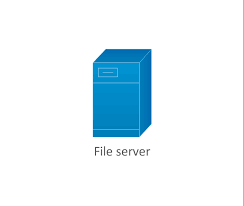
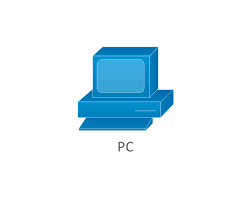
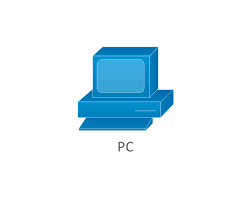
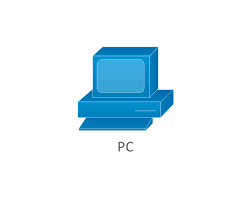
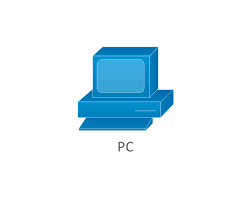
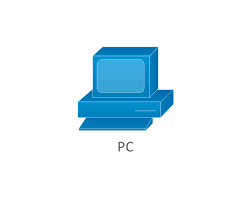
The switch ports break down the network into smaller collision domains. The smaller the collision domain, the fewer collisions that occur. Switches interpret the bits in the received frame so that they can typically send the frame out to the one required port, rather than all other ports. If a switch needs to forward multiple frames out the same port, the switch buffers the frames in memory, sending one at a time, thereby avoiding collisions.

The switch by default forwards multicast and broadcast messages because of that the network is still in one broadcast domain as such broadcast traffic might occur.

As a result of the switch operating in full duplex mode and port to port data transmission , frame collision is avoided in the network and more bandwidth is also provided to the host.

Scenario 2

Assuming we want to create two separate Local Area Networks and join them with a bridge.



**Segment A**

PC1

A

B

PC7

**Segment B**

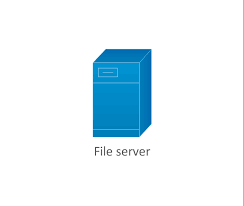
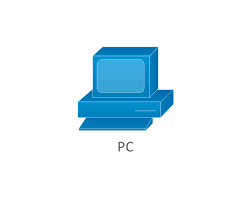
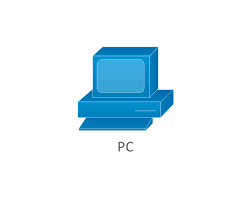
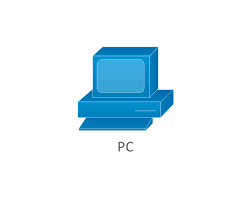
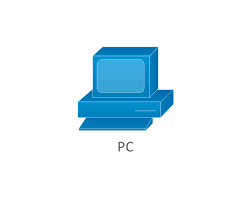
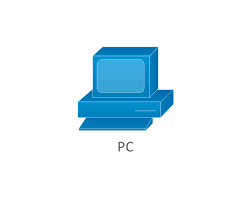
The network bridge divides the network into two segments – Segment A and Segment B. Each segment represent a separate collision domain, so the number of collisions on the network is reduced. Each collision domain has its own separate bandwidth, so a bridge also improves the network performance.

A bridge works at the Data link layer (Layer 2) of the OSI model. It inspects incoming traffic and decide whether to forward it or filter it. Each incoming frame is inspected for destination MAC address. If the bridge determines that the destination host is on another segment of the network, it forwards the frame to that segment.

**Scenario 3 – Subnetting Approach**

Eliminating collisions in the network by creating two separate networks with routers and switches and assume you want to create an internetwork. And assuming you have been given a subnet of 10.128.0/18 to subdivide into 8 subnets.

After subneting number of host on that each subnet can support is 6.



**Mac Address: 9**

**IP Address : 10.128.208.3/21**

**Interface : e1/1/1**

**Mac Address: A**

**IP Address : 10.128.200.0/21**

**Interface : e2/1/1**

**Mac Address: A**

**IP Address : 10.128.208.0/21**

Printer 1

**Mac Address: 8**

**IP Address : 10.128.208.1/21**

1

**Mac Address: 7**

**IP Address : 10.128.208.2/21**

**Mac Address: 4**

**IP Address : 10.128.208.4/21**

**Mac Address: 3**

**IP Address : 10.128.200.3/21**

**Mac Address: 1**

**IP Address : 10.128.200.1/21**

14

74

4

3

2

1

**Mac Address: 2**

**IP Address : 10.128.200.2/21**

Here we have a router with two interfaces: **e1/1/1** (which I'll refer to as *E1*) and **e1/1/2** (which I'll refer to as *E2*).

The router's two interfaces are in separate subnets, separate collision domain as well as broadcast domain. When data arrives from one of the segment the router decides according to its routing table to which network to forward the data. By default it doesn’t forward broadcast. Subnetting ensures that traffic destined for a device within a subnet stays in that subnet, which reduces congestion.

E1 is connected to subnet: **10.128.200.0/21**

E2 is connected to subnet: **10.128.208.0/21**

Now, suppose Pc1 (with IP address **10.128.200.1/21** and therefore in subnet **10.128.200.0/21**) sends a message to Pc4 (with IP address **10.128.208.4/21** and therefore in subnet **10.128.208.0/21**)

1. The Switch examines the source address of the frame and creates an address and port number entry for PC1 in its Mac Address Table..
2. The Switch examines the destination address of the frame and does not find it in its Mac Address Table so it floods it to all other ports
3. Once that packet arrives at the router, the following happens:
4. Packet arrives on interface E1with subnet **10.128.200.0/21**
5. Router determines the destination address is **10.128.208.4/21**
6. Router examines its routing table to determine where the packet should go based on the NetId
7. The routing table indicates interface E2 is connected to subnet **10.128.208.0/21**
8. The router prepares the packet for transmission on interface E2.
9. The new packet is transmitted on interface E2

Once the packet is sent to the network segment connected to router interface E2 it is received by the switch which checks its Mac Address table for the destination Mac address. The frame is then forward to the Port on which Pc4 is on if the Mac address is on the Mac address table.

**RECOMMENDATIONS AND CONCLUSIONS**

It is recommended you subnet the network, as it allows you to control the growth of the network by calculating the number of host each subnet can support. But subnetting enables you to ensure that information remains in the subnetted network or broadcast domain, which allows other subnets to maximize their speed and effectiveness. Subnetting also divides your network’s broadcast domains, enabling you to better control traffic flow, thus increasing network performance.

It is also recommended to use Switches instead of a bridge or hub as Switches support many ports, operates at wire speed in terms of switching of frames and also each device on a switch is individually to a port on a switch.

In conclusion, use the best network devices and network arrangement better suited for your organization. As each network device or network topology has its pros and cons.