

Unit 7

Backbone Networks

Introduction

A **backbone network (BN)** is a high-speed network that connects many networks. BNs typically use higher-speed circuits to interconnect a series of LANs and provide connections to other BNs, MANs, WANs, and the Internet. A backbone that connects many BNs spanning several nearby buildings for a single organization is often called a **campus network**. A BN also may be called an **enterprise network** if it connects all networks within a company, regardless of whether it crosses state, national, or international boundaries.

Device	Operates At	Packets	Physical Layer	Data Link Layer	Network Layer
Switch	Data link layer	Filtered using data link layer addresses	Same or different	Same	Same
Router	Network layer	Routed using network layer addresses	Same or different	Same or different	Same
Gateway	Network layer	Routed using network layer addresses	Same or different	Same or different	Same or different

Fig: Backbone Network Devices

Components of Backbone Network

There are two basic components to a BN: the network cable and the hardware devices that connect other networks to the BN. The cable is often fiber optic to provide higher data rates. The hardware devices can be computers or special-purpose devices such as **switches, routers, and gateways**.

Switches

Most **switches** operate at the data link layer. They connect two or more network segments that use the **same** data link and network protocol. They understand only data link layer protocols and addresses. They may connect the **same or different** types of cable.

Routers

Routers operate at the network layer. They connect two or more network segments that use the **same or different** data link protocols but the **same** network protocol. They may connect the **same or different** types of cable. Routers are the “TCP/IP gateways” that strip off the data link layer packet, process the network layer packet, and forward only those messages that need to go to other networks on the basis of their network layer address. Routers may be special purpose devices or special network modules in other devices (e.g., wireless access points for home use often include a built-in router). One major feature of a router is that it can choose the “best” route between networks when there are several possible routes between them. Because a router knows its own location, as well as the packet’s final destination, it looks in a routing table to identify the **best route or path**.

Gateways

Gateways operate at the network layer and use network layer addresses in processing messages. Gateways are more complex than switches or routers because they are the interface between two or more dissimilar networks. Gateways connect two or more networks that use the **same or different** (usually different) data link and network protocols.

They may connect the *same or different* types of cable. Some gateways operate at the application layer as well. Gateways process only those messages explicitly addressed to them

and route those messages that need to go to other networks. Gateways translate one network layer protocol into another, translate data link layer protocols, and open sessions between application programs, thus overcoming both hardware and software incompatibilities. A gateway may be a stand-alone computer with several NICs and special software or a front-end processor connected to a mainframe computer.

Gateways used to be common, but as TCP/IP has become the dominant network protocol, they are quickly fading from use.

BACKBONE NETWORK ARCHITECTURES

The **backbone architecture** refers to the way in which the backbone interconnects the networks attached to it and how it manages the way in which packets from one network move through the backbone to other networks.

While there are an infinite number of ways in which network designers can build backbone networks, there are really only three fundamental architectures that can be combined in different ways. These architectures are:

1. **Routed Backbones:** routers that move packets on the basis of network layer addresses.
2. **Switched Backbones:** switches that move packets based on data link layer addresses.
3. **Virtual LANs:** switches that move packets through LANs that are built virtually, not using physical location.

Switched Backbones

Switched backbones are probably the most common type of BN used in the distribution layer (i.e., within a building); most new building BNs designed today use switched backbones. They also are making their way into the core layer as the campus backbone, but routed backbones still remain common. Switched backbone networks use a star topology with one switch at its center.

Figure below shows a switched backbone connecting a series of LANs. There is a switch serving each LAN (access layer) which is connected to the backbone switch at the bottom of the figure.

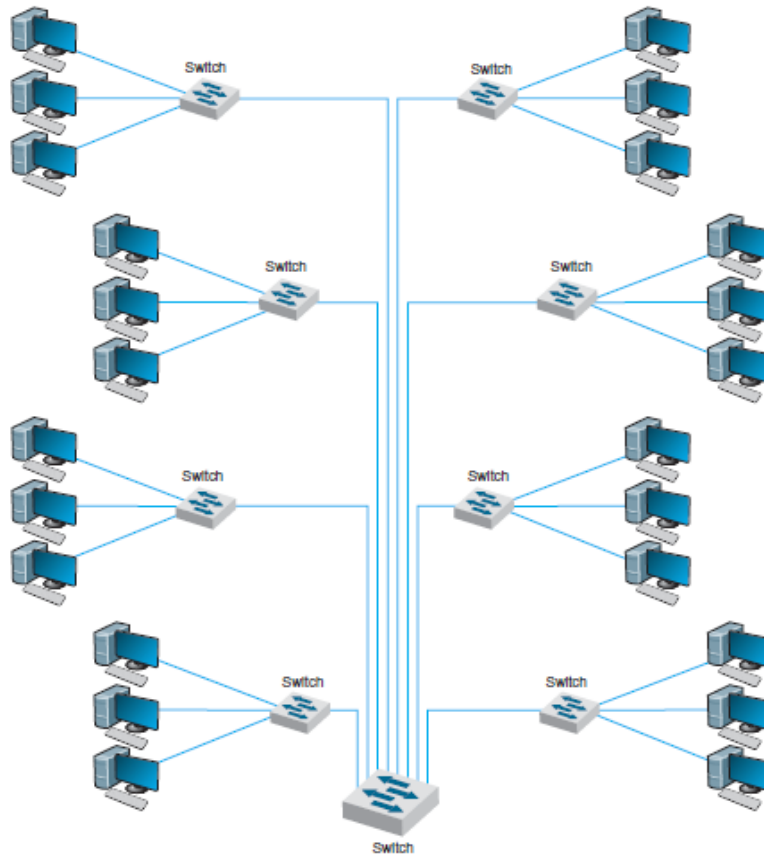


Fig: switched backbone network design

Some key **features and characteristics** of **switched backbones** are:

1. **Switching technology:** Network switches are intelligent devices that operate at Layer 2 or Layer 3 of OSI model. Switches are responsible for forwarding data packets based on MAC address.
2. **High Speed Connectivity:** Switched backbones are designed to provide high speed connectivity. This ensures data can flow quickly and efficiently between network segments.
3. **Segmentation:** Switched backbones are designed to enable network segmentation, which involves breaking down a large network into smaller and more manageable segments.
4. **Reduced Broadcast Traffic:** Switched backbone network effectively filter out unnecessary broadcast traffic reducing network congestion and improving overall performance.
5. **Improved Scalability:** Switched backbone network easily accommodate the addition of new devices and network segments making it highly scalable.
6. **Redundancy:** Redundant switches, links and failover mechanisms ensure network availability and minimize downtime incase of hardware failures.
7. **Security:** Advanced switched backbones can incorporate security features like access control lists, intrusion detection and encryption to protect the network from unauthorized access and threats.
8. **Centralized Management:** Network administrators can manage and monitor entire switched backbone from central location with efficient configurations and troubleshooting.
9. **Core of Data Center:** In data centre environments, switched backbones are a fundamental component. They connect servers, storage devices and other critical components.

Routed Backbones

Routed backbones move packets along the backbone on the basis of their network layer address (i.e., layer-3 address). Routed backbones are sometimes called **subnetted backbones** or **hierarchical backbones** and are most commonly used to connect different buildings within the same campus network (i.e., at the core layer).

Figure below shows a routed backbone used at the core layer. A routed backbone is the basic backbone architecture which is used to illustrate how TCP/IP worked. There are a series of LANs (access layer) connected to a switched backbone (distribution layer). Each backbone switch is connected to a router. Each router is connected to a core router (core layer). These routers break the network into separate subnets.

The primary advantage of the routed backbone is that it clearly segments each part of the network connected to the backbone. Each segment (usually a set of LANs or switched backbone) has its own subnet addresses that can be managed by a different network manager. Broadcast messages stay within each subnet and do not move to other parts of the network.

There are two primary disadvantages to routed backbones. First, the routers in the network impose time delays. Routing takes more time than switching, so routed networks can sometimes be slower. Second, routers are more expensive and require more management than switches.

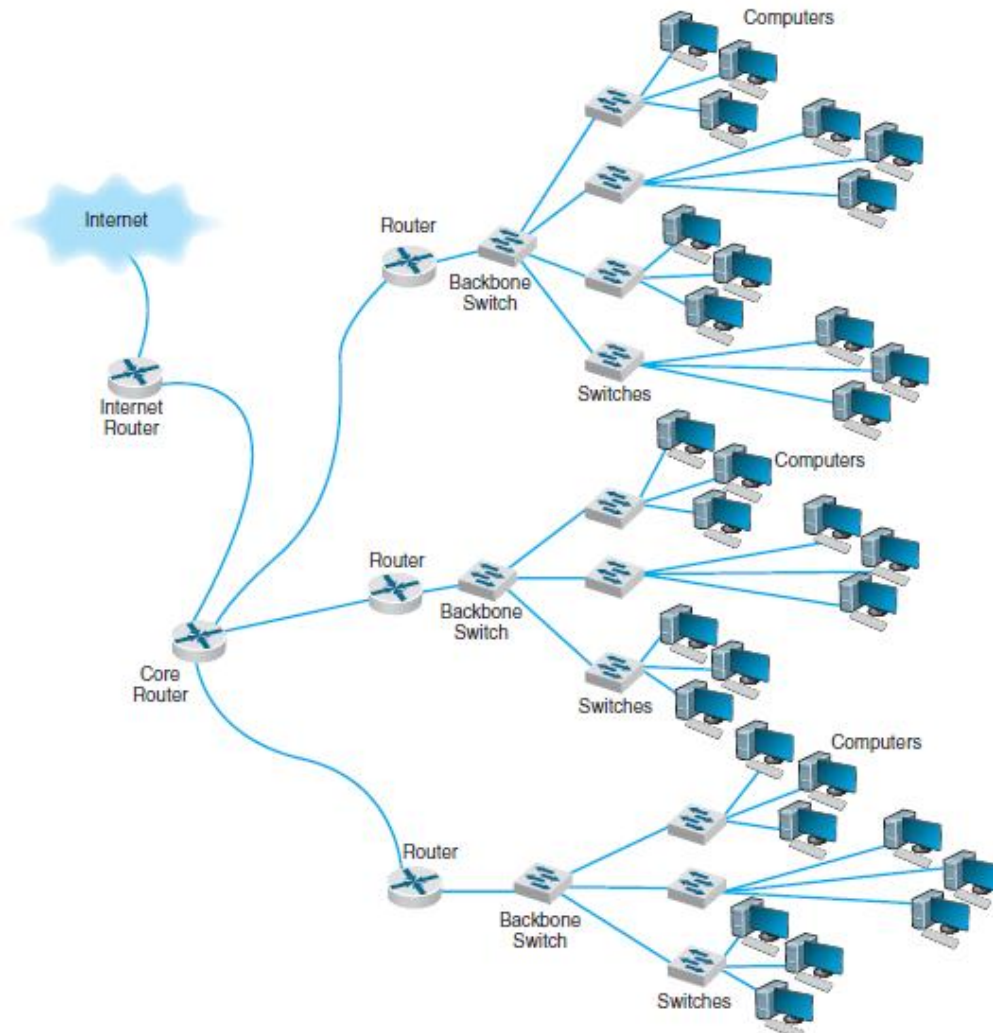


Fig: Routed backbone network

Routed Backbones are commonly used in larger networks, including enterprise networks. Also routed backbones provide the flexibility and control needed to meet the diverse requirements of today's complex networking environments.

Some **Key Features** and **Characteristics** of Routed Backbones are:

1. **IP Routing**
2. **Subnet Isolation**
3. **Interconnectivity**
4. **Traffic Filtering**
5. **Scalability**
6. **Optimized Routing**
7. **Internet Connectivity**
8. **Quality of Service**
9. **Security and Firewalling**



Consult your book for Elaboration

Virtual LANs

Virtual LANs are networks in which computers are assigned to LAN segments by software rather than by hardware. VLANs provide the same capability via software so that the network manager does not have to unplug and replug physical cables to move computers from one segment to another. Often, VLANs are faster and provide greater opportunities to manage the flow of traffic on the LAN and BN than do the traditional LAN and routed BN architecture. However, VLANs are significantly more complex, so they usually are used only for large networks.

The simplest example is a **single-switch VLAN**, which means that the VLAN operates only inside one switch. The computers on the VLAN are connected into the one switch and assigned by software into different VLANs. The network manager uses special software to assign the dozens or even hundreds of computers attached to the switch to different VLAN segments. The VLAN segments function in the same way as physical LAN segments or subnets; the computers in the same VLAN act as though they are connected to the same physical switch or hub in a certain subnet. Because VLAN switches can create multiple subnets; they act like layer-3 switches or routers, except the subnets are *inside* the switch, not between switches. Therefore, broadcast messages sent by computers in one VLAN segment are sent only to the computers on the same VLAN.

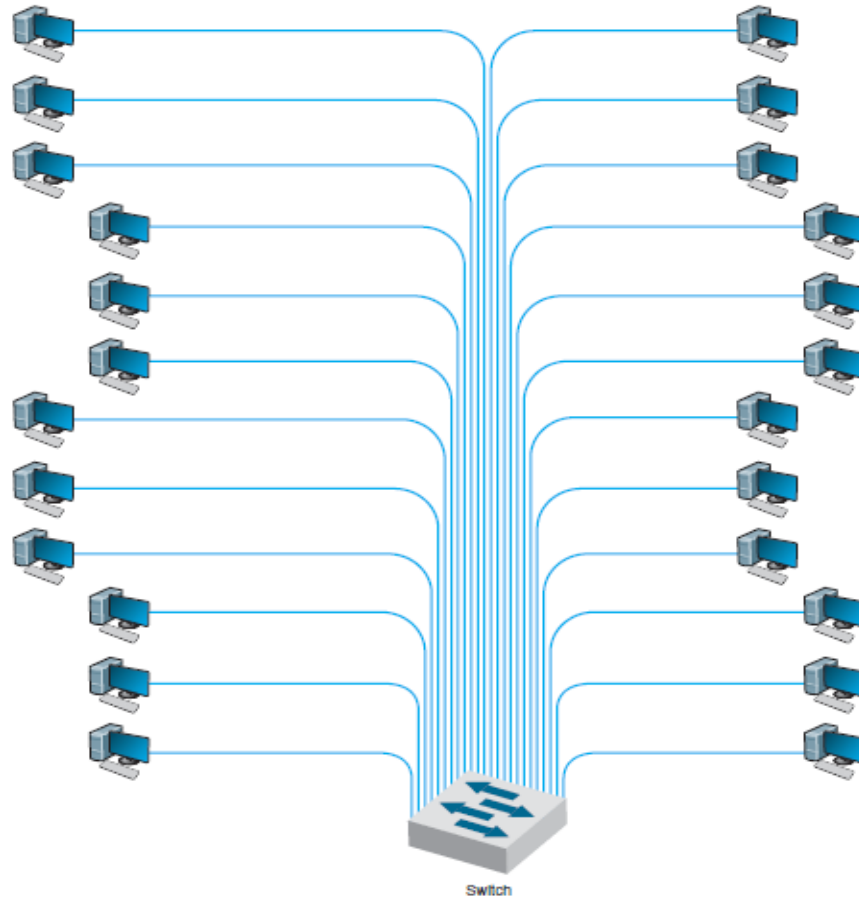


Fig: VLAN based backbone Network Design

Benefits of VLANs

Historically, we have assigned computers to subnets based on geographic location; all computers in one part of a building have been placed in the same subnet.

With VLANs, we can put computers in different geographic locations in the same subnet. For example, in Figure above a computer in the lower left could be put on the same subnet as one in the upper right—a separate subnet from all the other computers.

A more common implementation is a **multiswitch VLAN**, in which several switches are used to build the VLANs (**Figure below**). VLANs are most commonly found in building backbone networks (i.e., access and distribution layers) but are starting to move into core backbones between buildings. In this case, we can now create subnets that span buildings.

Virtual LANs offer other **two major advantages** compared to the other network architectures. The **first lies in their ability to manage the flow of traffic on the LAN and backbone very precisely**. VLANs make it much simpler to manage the broadcast traffic that has the potential to reduce performance and to allocate resources to different types of traffic more precisely. The bottom line is that VLANs often provide faster performance than the other backbone architectures.

The **second advantage is the ability to prioritize traffic**. The VLAN tag information included in the Ethernet packet defines the VLAN to which the packet belongs and also specifies a priority code on the **IEEE 802.1q** standard.

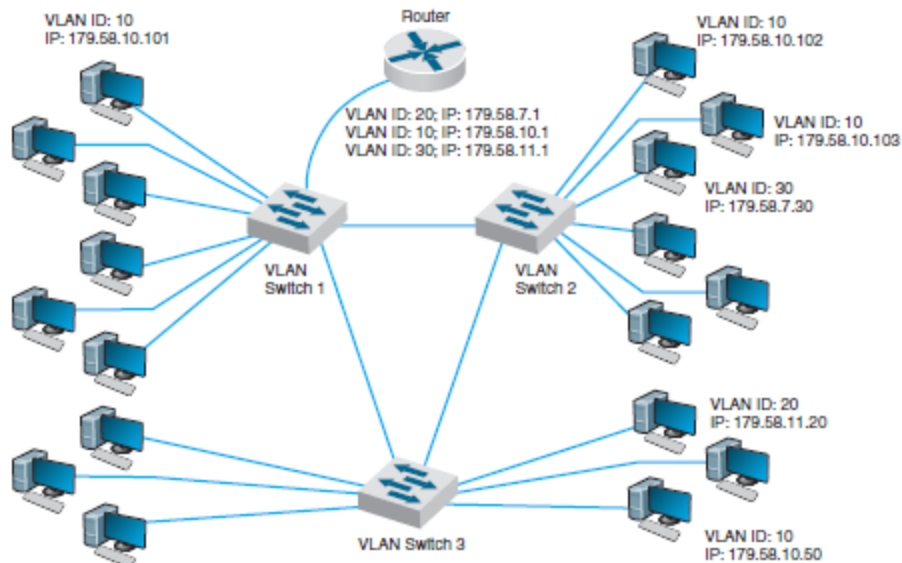


Fig: Multiswitch VLAN based backbone network design

Some other advantages are:

1. Network Segmentation
2. Cost and Time Reduction
3. Improved Security
4. Optimized Traffic Flow
5. Simplified Network Management
6. Reduced Broadcast Traffic
7. Flexibility and Scalability
8. Geographical Flexibility
9. Resource Optimization
10. Virtual Routing
11. Disaster Recovery
12. Guest Networking
13. Compliance and Regulations

Consult your book for Elaboration

How VLANs Work

VLANs work by logically dividing a physical network into multiple isolated virtual networks. Following points illustrates how VLAN works

1. **Creation and Configuration of VLANs:** Network administrators configure VLANs on network switches or routers that support VLAN functionality. They assign a unique VLAN ID to each VLAN. VLAN can be created based on various criteria such as department, function, security requirements etc.
2. **Port Assignments:** Administrator assign individual switch ports to specific VLANs based on the connected devices and their locations. Devices connected to a specific port are considered part of the VLAN associated with that port.
3. **VLAN Tagging:** When a device connected to a VLAN- configured port sends network traffic, the switch adds a VLAN tag (called 802.1Q tag) to the Ethernet frames. This tag contains the VLAN ID, which identifies the associated VLAN. The VLAN tag allows switches to distinguish which VLAN the traffic belongs to.

4. **Isolation and Broadcast Control:** Devices within the same VLAN can communicate with each other directly, as if they are on same physical network segment. This is accomplished by the switch forwarding traffic only to devices within same VLAN. Broadcast traffic is confined (restricted) to the VLAN, preventing it from crossing VLAN boundaries. This controls network congestion and security risks associated with unnecessary broadcast traffic.
5. **Inter- VLAN Routing:** If devices in different VLAN need to communicate, a router or layer 3 switch is used. These devices act as gateways between VLANs.
6. **Security and Access Control:** VLANs provide network segmentation, which enhances security. Network administrators can control and secure traffic between VLANs using access control lists or firewall rules applied at the router or layer 3 switch.
7. **Management and Monitoring:** Network administrators can manage and monitor each VLAN separately. This allows for individual control over configuration settings, security policies and performance monitoring each virtual network.
8. **Dynamic VLAN Assignment:** In some scenarios VLANs can be assigned dynamically based on user authentication or specific device characteristics.
9. **Quality of Service:** VLANs can be used to implement Quality of Service (QoS) policies ensuring that specific types of traffic receive priority over others, optimizing network performance for critical applications.

The Best Practice Backbone Design

The past few years have seen radical changes in the backbone, both in terms of new technologies (e.g., gigabit Ethernet) and in architectures (e.g., switched backbones, VLANs). Fifteen years ago, the most common backbone architecture was the routed backbone, connected to a series of shared 10Base-T hubs in the LAN.

Today, the most effective architecture for the distribution layer in terms of **cost** and **performance** is a **switched backbone** (either rack-mounted or using a chassis switch) because it provides the best performance at the least cost. For the **core layer**, most organizations use a **routed backbone**. Many large organizations are now implementing VLANs, especially those which have departments spread over multiple buildings, but VLANs add considerable cost and complexity to the network.

Improving Backbone Performance

The method for improving the performance of BNs is similar to that for improving LAN performance. First, find the bottleneck, then solve it or, more accurately, move the bottleneck somewhere else. The performance of the network can be improved by improving the performance of the computers and other devices in the network, by upgrading the circuits between computers, and by changing the demand placed on the network

1. Improving Device Performance

The primary functions of computers and devices in BNs are routing and protocol translations. If the devices and computers are the bottleneck, routing can be improved with faster devices or a faster routing protocol. **Distance vector routing** is faster than **dynamic routing** but obviously can impair circuit performance in high-traffic situations.

Link state routing is usually used in WANs and MANs because there are many possible routes through the network. BNs often have only a few routes through the network, so link state routing may not be too helpful since it will delay processing and increase the network traffic because of the status reports sent through the network. **Distance Vector Routing** will often simplify processing and improve performance.

Most backbone devices are store-and-forward devices. One simple way to improve performance is to ensure that they have sufficient memory. If they don't, the devices will lose packets, requiring them to be retransmitted.

2. Improving Circuit Capacity

If network circuits are the bottlenecks, there are several options. One is to increase overall circuit capacity (e.g., by going from 100Base-T Ethernet to gigabit Ethernet). Another option is to add additional circuits alongside heavily used ones so that there are several circuits between some devices. In many cases, the bottleneck on the circuit is only in one place—the circuit to the server. A switched network that provides 100 Mbps to the client computers but a faster circuit to the server (e.g., 1000Base-T) can improve performance at very little cost.

3. Reducing Network Demand

One way to reduce network demand is to restrict applications that use a lot of network capacity, such as desktop videoconferencing, medical imaging, or multimedia. In practice, it is often difficult to restrict users. Nonetheless, finding one application that places a large demand on the network and moving it can have a significant impact. Much network demand is caused by broadcast messages, such as those used to find data link layer addresses. Some application software packages and

NOS modules written for use on LANs also use broadcast messages to send status information to all computers on the LAN. For example, broadcast messages inform users when printers are out of paper, or when the server is running low on disk space. When used in a LAN, such messages place little extra demand on the network because every computer on the LAN gets every message. This is not the case for routed backbones because messages do not normally flow to all computers, but broadcast messages can consume a fair amount of network capacity in switched backbones. In many cases, broadcast messages have little value outside their individual LAN. Therefore, some switches and routers can be set to filter broadcast messages so that they do not go to other networks. This reduces network traffic and improves performance.