Network Models

Routers operate logically at Layer 3.

High-speed LANs typically use Ethernet in full duplex, using switches that operate at Layer 2.

WAN technologies include dedicated leased lines, which are a dedicated point-to-point connection that can use Point-to-Point Protocol (PPP) or High-Level Data Link Control (HDLC). Packet-switching networks include Frame Relay and ATM, which are used to create virtual circuits using frame relay and ATM switching. These are point-to-multipoint networks to create virtual circuits using frame relay and ATM switching. These are point-to-multipoint networks.

A virtual local area network (VLAN) is a network that is using third-party services (such as an Internet Service Provider) for connectivity across large geographic areas. A VLAN is a collection of a links connected over a long distance (farther than the LAN could provide).

VAN (Virtual Private Network) technologies include dedicated leased lines, which are a dedicated point-to-point connection that can use Point-to-Point Protocol (PPP) or High-Level Data Link Control (HDLC). Packet-switching networks include Frame Relay and ATM, which are used to create virtual circuits using frame relay and ATM switching. These are point-to-multipoint networks to create virtual circuits using frame relay and ATM switching. These are point-to-multipoint networks.

Physical components for a network include hosts, connections, switches, and routers. Physical components of the network include hosts, connections, switches, and routers.

Bandwidth is the speed at which data flows through the network. A network’s bandwidth is graphically displayed by the bandwidth meter on the network diagram. A bandwidth meter is a graphical representation of the network’s bandwidth.

Network Models

<table>
<thead>
<tr>
<th>Level</th>
<th>Name</th>
<th>Prefix</th>
<th>Default Mask</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IP</td>
<td>128.0.0.0</td>
<td>255.0.0.0</td>
<td>Masked</td>
</tr>
<tr>
<td>2</td>
<td>IP</td>
<td>192.0.0.0</td>
<td>255.255.0.0</td>
<td>Masked</td>
</tr>
<tr>
<td>3</td>
<td>IP</td>
<td>224.0.0.0</td>
<td>255.255.255.0</td>
<td>Masked</td>
</tr>
<tr>
<td>4</td>
<td>IP</td>
<td>232.0.0.0</td>
<td>255.255.255.255</td>
<td>Masked</td>
</tr>
<tr>
<td>5</td>
<td>IP</td>
<td>239.0.0.0</td>
<td>255.255.255.255</td>
<td>Broadcast</td>
</tr>
</tbody>
</table>

Networks

To create IP subnets, you take (starting on the leftmost bit of the subnet mask) the number of host bits (not used to identify the network) and subtract 2. If you have a network of 10.96, and so on.

Using the command log in the vty lines requires the user to provide a password when connecting on Telnet. That password is configured on the vty lines.

A remote server may be used to control the local server. For example, on a network with a Telnet user configured on the route.

You may use an access control list (ACL) and apply it to the vty lines to control which source addresses can connect. In addition, you can set restrictions for incoming sessions on the vty lines.

To remotely manage a switch, you need an IP address, subnet mask, and default gateway. The switch must be reachable on the port in the management VLAN.

The switch opens a connection between multiple, independent network domains to Layer 2.

Create separate broadcast domains in each switch, increasing the number of broadcast domains.

Span multiple switches using trunking. Alloagal broadcast domains are useful for broadcast domains.

To add new broadcast domains, use the following.

Route between VLANs requires a router or a Layer 3 switch.

Trunks carry traffic from multiple VLANs over the Layer 2 network. If a VLAN is tagged with 802.1Q ID is tagged using 802.1Q Q. Spanning Tree Protocol (STP) introduces multiple broadcast domains.

A Cisco device after it has IP addresses can use a Cisco device after it has IP addresses. You can use Telnet/SSH to remotely manage a switch. To access the command line of a switch, use the command show interface.

To remotely manage a switch, you need an IP address, subnet mask, and default gateway. The switch must be reachable on the port in the management VLAN.

Switches operate logically at Layer 3.

The VLAN must be created to create the VLAN. You can add VLANs to a switch.

To add a new VLAN, you need the following.

• A VLAN name
• A VLAN ID
• An associated standard or extended access list

Sample VLAN Configuration

1. The VLAN must be created.
2. VLANs must be enabled on the switch.
3. The VLANs must be assigned to the desired port(s).

The VLAN is an independent network domain.

The VLAN is an independent network domain.

VLAN ID is tagged using 802.1Q.

VLANs carry traffic from multiple VLANs over the Layer 2 network. If a VLAN is tagged with 802.1Q ID is tagged using 802.1Q Q. Spanning Tree Protocol (STP) introduces multiple broadcast domains.

A Cisco device after it has IP addresses can use a Cisco device after it has IP addresses. You can use Telnet/SSH to remotely manage a switch. To access the command line of a switch, use the command show interface.

To remotely manage a switch, you need an IP address, subnet mask, and default gateway. The switch must be reachable on the port in the management VLAN.

Switches operate logically at Layer 3.

The VLAN must be created.

A VLAN name and password for local authentication to use Telnet. The switch must be reachable on a single connection (crossover cable). The Switch> enable.

Subnetting allows you to create additional subnets under your network. The formula is two to the power of the number of host bits.

To create IP subnets, you take (starting on the leftmost bit of the subnet mask) the number of host bits that you want to create. If you want to create two subnets, you would use 10.10.0.0/16. If you want to create two subnets, you would use 10.10.0.0/16. To create two subnets, you would use 10.10.0.0/16.

Using the command log in the vty lines requires the user to provide a password when connecting on Telnet. That password is configured on the vty lines.

A remote server may be used to control the local server. For example, on a network with a Telnet user configured on the route.

You may use an access control list (ACL) and apply it to the vty lines to control which source addresses can connect. In addition, you can set restrictions for incoming sessions on the vty lines.

To remotely manage a switch, you need an IP address, subnet mask, and default gateway. The switch must be reachable on the port in the management VLAN.

Switches operate logically at Layer 3.

The VLAN must be created.

A VLAN name and password for local authentication to use Telnet. The switch must be reachable on a single connection (crossover cable). The Switch> enable.

Subnetting allows you to create additional subnets under your network. The formula is two to the power of the number of host bits.

To create IP subnets, you take (starting on the leftmost bit of the subnet mask) the number of host bits that you want to create. If you want to create two subnets, you would use 10.10.0.0/16. If you want to create two subnets, you would use 10.10.0.0/16. To create two subnets, you would use 10.10.0.0/16.

Using the command log in the vty lines requires the user to provide a password when connecting on Telnet. That password is configured on the vty lines.

A remote server may be used to control the local server. For example, on a network with a Telnet user configured on the route.

You may use an access control list (ACL) and apply it to the vty lines to control which source addresses can connect. In addition, you can set restrictions for incoming sessions on the vty lines.

To remotely manage a switch, you need an IP address, subnet mask, and default gateway. The switch must be reachable on the port in the management VLAN.

Switches operate logically at Layer 3.

The VLAN must be created.

A VLAN name and password for local authentication to use Telnet. The switch must be reachable on a single connection (crossover cable). The Switch> enable.

Subnetting allows you to create additional subnets under your network. The formula is two to the power of the number of host bits.

To create IP subnets, you take (starting on the leftmost bit of the subnet mask) the number of host bits that you want to create. If you want to create two subnets, you would use 10.10.0.0/16. If you want to create two subnets, you would use 10.10.0.0/16. To create two subnets, you would use 10.10.0.0/16.

Using the command log in the vty lines requires the user to provide a password when connecting on Telnet. That password is configured on the vty lines.

A remote server may be used to control the local server. For example, on a network with a Telnet user configured on the route.

You may use an access control list (ACL) and apply it to the vty lines to control which source addresses can connect. In addition, you can set restrictions for incoming sessions on the vty lines.

To remotely manage a switch, you need an IP address, subnet mask, and default gateway. The switch must be reachable on the port in the management VLAN.

Switches operate logically at Layer 3.

The VLAN must be created.

A VLAN name and password for local authentication to use Telnet. The switch must be reachable on a single connection (crossover cable). The Switch> enable.

Subnetting allows you to create additional subnets under your network. The formula is two to the power of the number of host bits.

To create IP subnets, you take (starting on the leftmost bit of the subnet mask) the number of host bits that you want to create. If you want to create two subnets, you would use 10.10.0.0/16. If you want to create two subnets, you would use 10.10.0.0/16. To create two subnets, you would use 10.10.0.0/16.

Using the command log in the vty lines requires the user to provide a password when connecting on Telnet. That password is configured on the vty lines.

A remote server may be used to control the local server. For example, on a network with a Telnet user configured on the route.

You may use an access control list (ACL) and apply it to the vty lines to control which source addresses can connect. In addition, you can set restrictions for incoming sessions on the vty lines.
You can use the command show route to see the routes currently configured on the device. Routers using static routes configure their routes using the command:

```
Router(config)# ip route <subnet> <mask> <Gateway> [tag]
```

Routing between VLANs can be done through VLAN routing protocols (VRRP or IS-IS) or using static routes. Static routes are configured on a VLAN to point to another VLAN. To configure a VLAN, you may use the command:

```
interface VLAN 1
ip address 10.1.1.1 255.255.255.0
```

### Network Interfaces

- **VLAN 1**: This VLAN is used for connecting multiple networks. Each network is assigned a separate VLAN, and each VLAN is connected to a different switch.
- **VLAN 2**: This VLAN is used for connecting the switch to the router.
- **VLAN 3**: This VLAN is used for connecting the router to the internet.

### Route Configuration

Routing protocols are used to automatically discover and maintain routes to destinations. Common routing protocols include:

- **Routing Protocol**: These are protocols used between different autonomous systems (ASes).
- **Interior gateway protocols (IGPs)**: These are protocols used within a single AS, such as OSPF or RIP.
- **Exterior gateway protocols (EGPs)**: These are protocols used between different ASes, such as BGP.

### Troubleshooting Tools

- **Ping**: This tool is used to verify connectivity between two devices.
- **Trace Route**: This tool is used to determine the path a packet takes from one device to another.
- **Show Command**: Various show commands are used to view the current state of the network and its components.

### Dynamic Routing Protocols

- **OSPF (Open Shortest Path First)**
- **EIGRP (Enhanced Interior Gateway Routing Protocol)**
- **RIP (Routing Information Protocol)**

### Network Address Translation (NAT)

Network Address Translation (NAT) is used to translate private addresses to public addresses. NAT can be configured using the command:

```
ip nat inside source static <private_ip> <public_ip> [type]
```

### PPP (Point-to-Point Protocol)

PPP is a protocol used for establishing a connection between two devices. It uses the Link Control Protocol (LCP) to negotiate a connection, and then uses authentication protocols such as PAP or CHAP to verify the identity of the connecting parties.

### Packet Filtering

Packet filtering is used to control the flow of traffic on a network. Filters are defined using access lists (ACLs), which can be configured using the command:

```
access-list <list_name> permit <source_ip> <destination_ip> <protocol> <port_range>
```

### Network Time Protocol (NTP)

NTP is used to synchronize the time between devices on a network. It uses a time server to provide time synchronization.

### subnet and mask

- **subnet**: This is a group of devices that share a common network address.
- **mask**: This is a set of bits that specify the network address and the host address.

### Default Gateway

The default gateway is the router that a host uses to forward packets to destinations outside its local network. It is configured using the command:

```
default-gateway <ip_address>
```

### Static Routes

Static routes are manually configured by the administrator. They are used to provide connectivity to destinations that are not reachable through dynamic routing protocols.

```
interface Ethernet 0
ip address 10.1.1.1 255.255.255.0
```

### Summary

- **Routing Protocols**: OSPF, EIGRP, RIP
- **Network Address Translation**: NAT
- **Point-to-Point Protocol**: PPP
- **Packet Filtering**: Access Lists (ACLs)
- **Network Time Protocol**: NTP

### Conclusion

Understanding network configuration and troubleshooting is crucial for maintaining a stable and secure network environment. This includes configuring routes, managing access lists, and troubleshooting network issues. With the right tools and knowledge, network administrators can ensure that their networks operate efficiently and securely.