Unit 2 VLAN

SEVEN MARKS:

1) What is Flat network? What are the drawbacks of flat network?

Ans: A flat network refers to a network architecture where all devices are on the same logical network segment, sharing the same broadcast domain. In a flat network, all devices can communicate with each other without the need for routers or network segmentation.

Drawbacks of a flat network include:

1. Broadcast Traffic: As the network grows, the amount of broadcast traffic increases. This can lead to network congestion and reduce network performance as all devices receive these broadcasts.

2. Security Concerns: In a flat network, there's a lack of inherent security controls. Any device within the same network segment can communicate with all other devices, potentially increasing the vulnerability to unauthorized access, data breaches, and attacks.

3. Scalability Issues: As the network expands, managing and maintaining a large, flat network becomes complex. The addition of new devices and services can lead to inefficiencies in managing IP addresses, subnets, and overall network traffic.

4. Difficulty in Isolating Issues: Troubleshooting network issues becomes challenging in a flat network. With all devices on the same segment, isolating and identifying problems can be more difficult.

For these reasons, modern network design often involves dividing the network into smaller, more manageable segments using techniques like VLANs, subnetting, and routing to mitigate the drawbacks associated with a flat network.

---

3) What are the different approaches of VLAN membership? explain.

Ans: VLAN Memberships

VLANs are typically created by an administrator, who then assigns switch ports to the VLAN. These are called static VLANs. If the administrator wants to do a little more work up front and assign all the host devices' hardware addresses into a database, the switches can be configured to assign VLANs dynamically

Static VLANs

Static VLANs are the typical way of creating VLANs and the most secure. The switch port that you assign a VLAN association always maintains that association until an administrator changes the port assignment. This type of VLAN configuration is easy to set up and monitor, working well in a net- work where the movement of users within the network is controlled. Using network management software to configure the ports can be helpful but is not mandatory.

Dynamic VLANs

Dynamic VLANs determine a node's VLAN assignment automatically. Using intelligent management software, you can enable hardware (MAC) addresses, protocols, or even applications to create dynamic VLANs. For example, suppose MAC addresses have been entered into a centralized VLAN management application. If a node is then attached to an unassigned switch port, the VLAN management database can look up the hardware address and assign and configure the switch port to the correct VLAN. This can make management and configuration easier for the administrator. If a user moves, the switch will automatically assign them to the correct VLAN. However, more administration is needed initially to set up the database.

Cisco administrators can use the VLAN Management Policy Server (VMPS) service to set up a database of MAC addresses that can be used for dynamic addressing of VLANs. VMPS is a MAC address–to–VLAN map- ping database.

---

5) What are the VLAN tagging method?

Ans: ISL and IEEE 802.1q

The VLAN tagging methods used in Ethernet networks include:

Inter-Switch Link (ISL) Proprietary to Cisco switches, it is used for FastEthernet and Gigabit Ethernet links only. Can be used on a switch port, router interfaces, and server interface cards to trunk a server. This server trunking is good if you are creating functional VLANs and don't want to break the 80/20 rule. The server that is trunked is part of all VLANs (broadcast domains) simultaneously. The users do not have to cross a layer-3 device to access a company-shared server.

IEEE 802.1q Created by the IEEE as a standard method of frame tagging. It actually inserts a

field into the frame to identify the VLAN. If you are trunking between a Cisco switched link and a different brand of switch, you have to use 802.1q for the trunk to work.LAN emulation (LANE) Used to communicate multiple VLANs over ATM.802.10 (FDDI) Used to send VLAN information over FDDI. Uses a SAID field in the frame header to identify the VLAN. This is proprietary to Cisco devices.

---

6) What are the link types & its significance with vlan?

Ans: There are two different types of links in a switched environment:

Access links:

Links that are only part of one VLAN and are referred to as the native VLAN of the port. Any device attached to an access link is unaware of a VLAN membership. This device just assumes it is part of a broadcast domain, with no understanding of the physical network. Switches remove any VLAN information from the frame before it is set to an access link device. Access link devices cannot communicate with devices outside their VLAN unless the packet is routed through a router.

Significance: Access links are used to connect end devices, like computers or printers, to a switch. Each access link typically carries traffic for a single VLAN. Devices connected to access links are unaware of VLAN tags; the switch port handles the VLAN assignment.

Trunk links:

Trunks can carry multiple VLANs. Originally named after trunks of the telephone system, which carries multiple telephone conversations, trunk links are used to connect switches to other switches, to routers, or even to servers. Trunked links are supported on Fast or Gigabit Ethernet only. To identify the VLAN that a frame belongs to with Ether- net technology, Cisco switches support two different identification techniques: ISL and 802.1q. Trunk links are used to transport VLANs between devices and can be configured to transport all VLANs or just a few. Trunk links still have a native, or default, VLAN that is used if the trunk link fails

Significance: Trunk links are used to interconnect switches or network devices and carry traffic for multiple VLANs simultaneously. They allow the transmission of VLAN-tagged frames between switches, enabling the transfer of traffic for different VLANs across the same physical link.

---

8) Write a note on ISL protocol?

Ans:

Inter-Switch Link (ISL) Protocol

Inter-Switch Link (ISL) is a way of explicitly tagging VLAN information onto an Ethernet frame. This tagging information allows VLANs to be multiplexed over a trunk link through an external encapsulation method. By running ISL, you can interconnect multiple switches and still maintain VLAN information as traffic travels between switches on trunk links. ISL provides a low-latency, full wire-speed performance over FastEthernet using either half- or fullduplex mode.

Cisco created the ISL protocol, and therefore ISL is proprietary in nature to Cisco devices only. If you need a non-proprietary VLAN protocol, use the 802.1q, which is covered in the CCNP: Switching Study Guide. ISL is an external tagging process, which means the original frame is not altered but instead encapsulated with a new 26-byte ISL header. It also adds a second 4-byte frame check sequence (FCS) field at the end of the frame. Because the frame is encapsulated with information, only ISL-aware devices can read it. Also, the frame can be up to 1522 bytes long. Devices that receive an ISL frame may record this as a giant frame because it is over the maximum of 1518 bytes allowed on an Ethernet segment.

On multi-VLAN (trunk) ports, each frame is tagged as it enters the switch. ISL network interface cards (NICs) allow servers to send and receive frames tagged with multiple VLANs so the frames can traverse multiple VLANs without going through a router, which reduces latency. This technology can also be used with probes and certain network analyzers. It makes it easy for users to attach to servers quickly and efficiently, without going through a router every time they need to communicate with a resource. Administrators can use the ISL technology to include file servers in multiple VLANs simultaneously, for example.

It is important to understand that ISL VLAN information is added to a frame only if the frame is forwarded out a port configured as a trunk link. The ISL encapsulation is removed from the frame if the frame is forwardedout an access link.

9.What are the alternatives available to achieve Routing between two vlans?

Ans: There are several alternatives to achieve routing between two VLANs:

1. Router-on-a-Stick (RoAS): This method involves using a single physical router interface to route traffic between multiple VLANs. The router interface is configured as a trunk port that connects to a switch carrying traffic from multiple VLANs. The router then routes traffic between the VLANs.

2. Layer 3 Switch: A Layer 3 switch combines the functionality of a switch with that of a router. It can route traffic between VLANs by creating virtual interfaces (SVIs - Switched Virtual Interfaces) for each VLAN, enabling inter-VLAN routing directly on the switch.

3. Dedicated Router: Using a dedicated router with multiple physical interfaces, each connected to different VLANs, to perform inter-VLAN routing. Each interface on the router is assigned an IP address in different VLANs and handles the routing between them.

4. Virtual Router: Virtual routers or router appliances (e.g., virtual routers running on a server) can be used to route traffic between VLANs. These can provide the routing function while running on a virtualized environment.

5. Software-Defined Networking (SDN): SDN solutions, with centralized control over network resources, allow for routing and traffic segmentation between VLANs through software-based approaches.

These alternatives vary in terms of their cost, complexity, and scalability. The choice often depends on the specific needs, scale, and budget of the network infrastructure.

10.Write a note on VTP?

Ans: Cisco created VLAN Trunk Protocol (VTP) to manage all the configured VLANs across a switched internetwork and to maintain consistency throughout the network. VTP allows an

administrator to add, delete, and rename VLANs, which are then propagated to all switches.

VTP provides the following benefits to a switched network:

• Consistent VLAN configuration across all switches in the network.

• Allowing VLANs to be trunked over mixed networks, like Ethernet to ATM LANE or FDDI.

• Accurate tracking and monitoring of VLANs.

• Dynamic reporting of added VLANs to all switches .

• Plug-and-Play VLAN adding

To allow VTP to manage your VLANs across the network, you must first create a VTP server.

All servers that need to share VLAN information must use the same domain name, and a switch can only be in one domain at a time. This means that a switch can only share VTP domain information with switches configured in the same VTP domain.

A VTP domain can be used if you have more than one switch connected in a network. If all switches in your network are in only one VLAN, then you don't need to use VTP. VTP information is sent between switches via a trunk port.

Switches advertise VTP-management domain information, as well as a configuration revision number and all known VLANs with any specific parameters. You can configure switches to forward VTP information through trunk ports but not accept information updates, nor update their VTP database. This is called VTP transparent mode.

If you are having problems with users adding switches to your VTP domain, you can add passwords, but remember that every switch must be set up with the same password, which may be difficult.

Switches detect the additional VLANs within a VTP advertisement and then prepare to receive information on their trunk ports with the newly defined VLAN in tow. The information would be VLAN ID, 802.10 SAID fields, or LANE information. Updates are sent

out as revision numbers that are the notification plus 1. Anytime a switch sees a higher revision

number, it knows the information it is receiving is more current and will overwrite the current database with the new one.

Ten Marks Questions:

1. Design network with 3 VLANs for a organization. Use a router to implement inter VLAN routing, using IOS commands.

Use the 1900 switch, connect 6 nodes A,B,C,D,E,F through ports 1 to 6

with ip address 10.0.0.1 to 10.0.0.6, Mask 255.0.0.0

/* check the connectivity between each nodes from A to F

Ping 10.0.0.2, 3,4,5,6

/* Observe the vlans if any

Switch1900#sh vlan

/* Define vlans in switch 1900

CISCO#config terminal

CISCO(config)#vlan 10 name HR

CISCO(config)#vlan 20 name Sales

CISCO(config)#vlan 30 name IT

/* Observe the vlans

Switch1900#sh vlan

/* Assign membership to vlan

CISCO(config)#int e0/1

CISCO(config-if)#vlan-membership static 10

CISCO(config)#int e0/2

CISCO(config-if)#vlan-membership static 10

CISCO(config)#int e0/3

CISCO(config-if)#vlan-membership static 20

CISCO(config)#int e0/4

CISCO(config-if)#vlan-membership static 20

CISCO(config)#int e0/5

CISCO(config-if)#vlan-membership static 30

CISCO(config)#int e0/6

CISCO(config-if)#vlan-membership static 30

CISCO#sh vlan

/* check the connectivity between each nodes from A to F

Ping 10.0.0.2, 3,4,5,6

---

2. What are the different VLAN Tagging methods? Explain each of then in brief.

Ans: The VLAN tagging methods used in Ethernet networks include:

Inter-Switch Link (ISL) Proprietary to Cisco switches, it is used for FastEthernet and Gigabit Ethernet links only. Can be used on a switch port, router interfaces, and server interface cards to trunk a server. This server trunking is good if you are creating functional

VLANs and don’t want to break the 80/20 rule. The server that is trunked is part of all VLANs (broadcast domains) simultaneously. The users do not have to cross a layer-3 device to access a company-shared server.

IEEE 802.1q Created by the IEEE as a standard method of frame tagging. It actually inserts a field into the frame to identify the VLAN. If you are trunking between a Cisco switched link and a different brand of switch, you have to use 802.1q for the trunk to work.LAN emulation (LANE) Used to communicate multiple VLANs over ATM.802.10 (FDDI) Used to send VLAN information over FDDI. Uses a SAID field in the frame header to identify the VLAN. This is proprietary to Cisco devices.

3.What are the methods to achieve inter VLAN routing? Explain

Ans:

Inter-VLAN routing enables communication between different VLANs within a network. There are several methods to achieve inter-VLAN routing:

1. Router-on-a-Stick (RoAS):

- Explanation: This method involves using a single router interface to route traffic between multiple VLANs. The router interface is configured as a trunk port that connects to a switch carrying traffic from multiple VLANs. The router then routes traffic between the VLANs.

- Configuration: Each VLAN is configured as a subinterface on the router, and the router performs the inter-VLAN routing between these subinterfaces.

2. Layer 3 Switch:

- Explanation: A Layer 3 switch performs routing functions at the network layer. It can route traffic between VLANs using virtual interfaces (SVIs - Switched Virtual Interfaces) associated with each VLAN.

- Configuration: The switch is configured with SVIs for each VLAN, enabling it to route traffic between VLANs directly without the need for an external router.

3. Dedicated Router:

- Explanation: A dedicated router with multiple physical interfaces is used to perform inter-VLAN routing. Each interface on the router is assigned to different VLANs, and the router routes traffic between these interfaces.

- Configuration: Each interface on the router is assigned an IP address in different VLANs, and appropriate routing configurations are made to enable traffic flow between these interfaces.

4. Virtual Router:

- Explanation: Utilizing virtual routers or router appliances, typically running on virtualized environments or servers, to perform inter-VLAN routing functions.

- Configuration: These virtual routers operate similarly to physical routers, allowing for the configuration of VLAN interfaces and routing protocols to manage traffic flow between VLANs.

5. Software-Defined Networking (SDN):

- Explanation: SDN solutions provide a centralized and software-based approach to network management. This can involve using a controller to manage traffic flows between VLANs in a more dynamic and programmable manner.

- Configuration: SDN requires specific software-defined configurations and protocols to manage inter-VLAN routing dynamically.

Each method has its advantages and is chosen based on the network architecture, hardware availability, scalability, and specific requirements of the network infrastructure.