

Assignment 1: VLAN

What is the difference between 802.1q and ISL Trunking protocol? (4P)

ISL

- ISL is a Cisco proprietary protocol option for configuring Layer 2 trunk links.
- Supports multiple Layer 2 protocols (Ethernet, Token Ring, FDDI, and ATM).
- Supports PVST.
- Does not use a native VLAN, so it encapsulates every frame.
- Encapsulation process leaves original frames unmodified.
- No support for extended QoS.
- Protocol independent.

802.1Q

- The 802.1Q protocol, often referred to as "dot-1Q," offers the clear benefit of being the first IEEE standards-based trunking protocol for Ethernet. It allows multiple VLANs to traverse infrastructure equipment where cross vendor links exist.
- Support for Ethernet and Token Ring
- Support for 4096 VLANs
- Support for Common Spanning Tree (CST), Multiple Spanning Tree Protocol (MSTP), and Rapid Spanning Tree Protocol (RSTP)
- Point-to-multipoint topology support
- Support for untagged traffic over the trunk link via native VLAN
- Extended QoS support
- Growing standard for IP telephony links
- Protocol dependent.

Assignment 2: STP

Describe the characteristics of transparent bridge? (4P)

A transparent bridge has these characteristics:

- It must not modify the frames that are forwarded.
- It learns addresses by "listening" on a port for the source address of a device. When a source MAC address is read in frames coming into a specific port, the bridge assumes that the frames destined for that MAC address can be sent out of that port. The bridge then builds a table that records which source addresses are seen on which port. A bridge is always listening and learning MAC addresses in this manner.
- It must forward all broadcasts out of all ports, except for the port that initially received the broadcast.
- If a destination address is unknown to the bridge, it forwards the frame out of all ports, except for the port that initially received the frame. This is called unicast flooding.

Assignment 3: MULTILAYER SWITCHING

Explain the difference between the function of control plane and data plane in CEF based multilayer switching? (4P)

Layer 3 switching software employs a distributed architecture in which the control path and data path are relatively independent. The control path code, such as routing protocols, runs on the route processor, whereas most of the data packets are forwarded by the Ethernet interface module and the switching fabric.

Assignment 4: SWITCHING SECURITY

Explain Mac flooding attack with example and how to mitigate this attack? (4P)

A common Layer 2 or switch attack is MAC flooding, which causes a switch's CAM table to overflow, resulting in flooding regular data frames out all switch ports. A network intruder can maliciously flood a switch with a large number of frames from a range of invalid source MAC addresses. If enough new entries are made before old ones expire, new valid entries are not accepted. Then, when traffic arrives at the switch for a legitimate device that is located on one of the switch ports that was not able to create a CAM table entry, the switch must flood frames to that address out all ports. This has two adverse effects:

- Switch traffic forwarding is inefficient and voluminous.
- An intruding device can be connected to any switch port and capture traffic not normally seen on that port.

To mitigate against MAC flooding, port security is configured to define the number of MAC addresses that are allowed on a given port. Port security can also specify which MAC address is allowed on a given port.

Define AAA and what are the benefits of AAA? (4P)

Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which access control is set up on a switch. AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner.

Authentication

Verifies a user identity.

Authorization

Specify the permitted tasks for the users.

Accounting

Provide billing, auditing and monitoring.

Assignment 5: WIRELESS LAN SECURITY

Name all the key features of wireless LAN 802.1x authentication? (4p)

WLAN 802.1x has the following features.

- RADIUS and EAP encapsulate EAP packets within RADIUS.
- Supports multiple EAP types.
- Bases identification on the network access identifier (NAI).
- The standard supports roaming access in public spaces.
- Supports RADIUS for centralized AAA .
- This standard can be used with multiple encryption algorithms:
 - AES
 - WPA TKIP
 - WEP
- WEP keys are dynamic instead of static and do not require user intervention-based management.
- This standard is compatible with existing roaming technologies, enabling use in hotels and public places.

Assignment 6: QoS

Name all the drawbacks and benefits of QoS models? (4P)

Benefits and drawbacks of best effort model as follows:

- **Benefits:**
 - The model has nearly unlimited scalability. The only way to reach scalability limits is to reach bandwidth limits, in which case all traffic is equally affected.
 - You do not need to employ special QoS mechanisms to use the best-effort model. Best-effort is the easiest and quickest model to deploy.
- **Drawbacks:**
 - There are no guarantees of delivery. Packets will arrive whenever they can and in any order possible, if they arrive at all.
 - No packets have preferential treatment. Critical data is treated the same as casual e-mail is treated.

Benefits and Drawbacks of the IntServ Model:

- **Benefits:**
 - IntServ supports admission control that allows a network to reject or downgrade new RSVP sessions if one of the interfaces in the path has reached the limit (that is, if all bandwidth that can be reserved is booked).
 - RSVP signals QoS requests for each individual flow. In the request, the authorized user (authorization object) and needed traffic policy (policy object) are sent. The network can then provide guarantees to these individual flows.
 - RSVP informs network devices of flow parameters (IP addresses and port numbers). Some applications use dynamic port numbers, such as H.323-based applications, which can be difficult for network devices to recognize. Network-Based Application Recognition (NBAR) is a mechanism that complements RSVP for applications that use dynamic port numbers but do not use RSVP.

- **Drawbacks:**
 - There is continuous signaling because of the stateful RSVP architecture that adds to the bandwidth overhead. RSVP continues signaling for the entire duration of the flow. If the network changes, or links fail and routing convergence occurs, the network may no longer be able to support the reservation.
 - The flow-based approach is not scalable to large implementations, such as the public Internet, because RSVP has to track each individual flow. This circumstance makes end-to-end signaling difficult. A possible solution is to combine IntServ with elements from the DiffServ model to provide the needed scalability.

DiffServ model has several benefits and some drawbacks:

- **Benefits:**
 - Highly scalable
 - Provides many different levels of quality
- **Drawbacks:**
 - No absolute guarantee of service quality
 - Requires a set of complex mechanisms to work in concert throughout the network

What is the difference between classification and marking? (4P)

Classification is the process of identifying traffic and categorizing that traffic into classes. Classification uses a traffic descriptor to categorize a packet within a specific group to define that packet. Marking allows network devices to classify a packet or frame at the edge based on a specific traffic descriptor. QoS classification tools categorize packets by examining the contents of the frame, cell, and packet headers; whereas marking tools allow the QoS tool to change the packet headers for easier classification. Many QoS tools rely on a classification function to determine to which traffic the tool applies. Marking a packet or frame with its classification allows subsequent network devices to easily distinguish the marked packet or frame as belonging to a specific class. After the packets or frames are identified as belonging to a specific class, QoS mechanisms can be uniformly applied to ensure compliance with administrative QoS policies.

Name all queuing technologies. Explain the function of WFQ? (4P)

FIRST IN FIRST OUT

PRIORITY QUEUING

CUSTOM QUEUING

WEIGHTED FAIR QUEUING

CLASS BASED WFQ

LOW LATENCY QUEUING

WFQ uses a flow-based queuing algorithm that does two things simultaneously:

- It schedules interactive traffic to the front of the queue to reduce response time.
- It fairly shares the remaining bandwidth among the various flows to prevent high-volume flows from monopolizing the outgoing interface.

The basis of WFQ is to have a dedicated queue for each flow without starvation, delay, or jitter within the queue. Furthermore, WFQ allows fair and accurate bandwidth allocation among all flows with minimum scheduling delay. WFQ makes use of the IP precedence bits as a weight when allocating bandwidth. Low-volume traffic streams, which comprise the majority of traffic, receive preferential service, transmitting their entire offered loads in a timely fashion. High-volume traffic streams share the remaining capacity proportionally between them

What is the difference between traffic shaping and policing? (4P)

Policing can be applied to either the inbound or outbound direction, while shaping can be applied only in the outbound direction. Policing drops nonconforming traffic instead of queuing the traffic like shaping. Policing also supports marking of traffic. Traffic policing is more efficient in terms of memory utilization than traffic shaping because no additional queuing of packets is needed. Both traffic policing and shaping ensure that traffic does not exceed a bandwidth limit, but each mechanism has different impacts on the traffic:

- Policing drops packets more often, generally causing more retransmissions of connection-oriented protocols, such as TCP.
- Shaping adds variable delay to traffic, possibly causing jitter. Shaping queues excess traffic by holding packets in a shaping queue. Traffic shaping is used to shape the outbound traffic flow when the outbound traffic rate is higher than a configured rate. Traffic shaping smoothes traffic by storing traffic above the configured rate in a shaping queue. Therefore, shaping increases buffer utilization on a router and causes unpredictable packet delays. Traffic shaping can also interact with a Frame Relay network, adapting to indications of Layer 2 congestion in the WAN.

Describe shortly DSCP per hop behavior of diffserv model. Give examples of each behavior? (6P)

A PHB is a description of the externally observable forwarding behavior of a DiffServ node applied to a particular DiffServ behavior aggregate (BA). PHBs may be specified in terms of their resource (for example, buffer, bandwidth) priority relative to other PHBs, or in terms of their relative observable traffic characteristics (for example, delay, loss). These PHBs may be used as building blocks to allocate resources and should be specified as a group (PHB group) for consistency. PHB groups will usually share a common constraint applying to each PHB within the group, such as a packet scheduling or buffer management policy. The DiffServ architecture defines the DiffServ (DS) field, which supersedes the ToS field in IPv4 to make per-hop behavior (PHB) decisions about packet classification and traffic conditioning functions, such as metering, marking, shaping, and policing.

- **Default PHB:** Used for best-effort service (bits 5 to 7 of DSCP equal 000).
- **Expedited Forwarding (EF) PHB:** Used for low-delay service (bits 5 to 7 of DSCP equal 101).
- **Assured Forwarding (AF) PHB:** Used for guaranteed bandwidth service (bits 5 to 7 of DSCP equal 001, 010, 011, or 100).
- **Class-selector PHB:** Used for backward compatibility with non-DiffServ-compliant devices (bits 2 to 4 of DSCP equal 000).

Assignment 7: Redundancy

How VRRP (virtual router redundancy protocol) differs from HSRP (hot standby router protocol)? (4P)

- VRRP is a Cisco proprietary protocol.
- The active router is referred to as the master virtual router.
- The master virtual router may have the same IP address as the virtual router group.
- Multiple routers can function as backup routers.
- VRRP is supported on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces, and with Multiprotocol Label Switching (MPLS), virtual private networks (VPNs), and VLANs.

Assignment 8: VOIP

Name all the steps of analog to digital conversion and describe them shortly? (4P)

Step 1 Sampling: The DSP periodically samples the analog signal. The output of the sampling is a pulse amplitude modulation (PAM) signal measured in volts.

Step 2 Quantization: The DSP matches the PAM signal to a segmented digital scale. This scale measures the amplitude (height or voltage) of the PAM signal.

Step 3 Compression: The DSP compresses voice samples to reduce bandwidth requirements.

8

PACKETIZATION Size =

$$30 \text{ ms} = \frac{30}{1000} \text{ Sec}$$

$$= \frac{30}{1000} \times 8000$$

$$= 240 \text{ bits}$$

$$= \frac{240}{8} = 30 \text{ byte}$$

Packet Rate =

1 Packet = 30 ms of voice

$$1 = \frac{30}{1000}$$

$$1 \text{ Packet} = \frac{1}{33.33} \text{ Sec}$$

$$33.33 \text{ Packet} = 1 \text{ second}$$

$$\text{PPS} = 33.33$$

Total Voice Packet Size

$$= \text{IP} + \text{UDP} + \text{RTP} + \text{Payload Size} + \text{L2H}$$

$$= 40 + 22 + 30$$

$$= 92 \text{ Byte}$$

Required BW =

$$= \frac{92 * 8 \text{ Kbps}}{30}$$

$$= 24.5 \text{ Kbps}$$