1. **Implement IP SLA**

IP SLA (Internet protocol service level agreement) is a feature of the Cisco Internetwork Operating System (Cisco IOS) that allows an IT professional to collect information about network performance in real time. IP SLAs are especially useful for wide area networks (WANs) that connect multiple geographies and needs to be monitored from one central location. An IP SLA Router is capable of generating traffic and reporting on it in real time. IP SLA can be configured in such a way that it can report on statistics such as:

* Jitter
* Response time
* Packet loss
* Voice Quality Scoring (MOS)
* Connectivity
* Server or website responses and downtime
* Delay

1. **Implement IPv4 ACLS - 1. Standard 2. Extended**

An Access Control List (ACL) is a list of network traffic filters and correlated actions used to improve security. The IPv4-based ACL is a list of sources IPv4 addresses that use Layer 3 information to permit or deny access to traffic. IPv4 ACLs restrict IP-related traffic based on the configured IP filters. A filter contains the rules to match an IP packet, and if the packet matches, the rule also stipulates if the packet should be permitted or denied. There are two types of IPv4 ACLs:

* Standard ACLs: These ACLs permit or deny packets based only on the source IPv4 address.
* Extended ACLs: These ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports, and more.

1. **1. Implement SPAN Technologies (Switch Port Analyzer) 2. Implement SNMP and Syslog 3. Implement Flexible NetFlow**

**SPAN** stands for switchport analyzer .it is also called port mirroring. To analyze network traffic passing through the port by using span.

It will send a copy of the traffic to another port on the switch. Span monitors received or sent (both) traffic on one or more source ports to a destination port for analysis. Only traffic that is entered or leaves source ports can be monitored.

**SNMP** (*Simple Network Management Protocol*) is an application-layer protocol for monitoring and managing network devices on a local area network (LAN) or wide area network (WAN). The purpose of SNMP is to provide network devices, such as routers, servers and printers, with a common language for sharing information with a network management system (NMS).

***Syslog*** stands for System Logging Protocol and is a standard protocol used to send system log or event messages to a specific server, called a syslog server. It is primarily used to collect various device logs from several different machines in a central location for monitoring and review.

***Flexible Netflow*** : NetFlow is a Cisco IOS technology that provides statistics on packets flowing through the router. NetFlow is the standard for acquiring IP operational data from IP networks. NetFlow provides data to enable network and security monitoring, network planning, traffic analysis, and IP accounting. Flexible NetFlow improves on original NetFlow by adding the capability to customize the traffic analysis parameters for your specific requirements. Flexible NetFlow facilitates the creation of more complex configurations for traffic analysis and data export through the use of reusable configuration components.

1. **Implement GRE Tunnel, VTP, NAT**

**Generic Routing Encapsulation, or GRE**, is a protocol for encapsulating data packets that use one routing protocol inside the packets of another protocol. "Encapsulating" means wrapping one data packet within another data packet, like putting a box inside another box. GRE is one way to set up a direct point-to-point connection across a network, for the purpose of simplifying connections between separate networks. It works with a variety of network layer protocols. The original IP packet enters a router, travels in encrypted form and emerges out of another GRE configured router as original IP packet like they have travelled through a tunnel. Hence, this process is called GRE tunneling.

**VTP (VLAN Trunking Protocol)** is a Cisco proprietary protocol used by Cisco switches to exchange VLAN information. With VTP, you can synchronize VLAN information (such as VLAN ID or VLAN name) with switches inside the same VTP domain. A VTP domain is a set of trunked switches with the matching VTP settings (the domain name, password and VTP version). All switches inside the same VTP domain share their VLAN information with each other.

**Network Address Translation (NAT)** is a process that enables one, unique IP address to represent an entire group of computers. In network address translation, a network device, often a router or NAT firewall, assigns a computer or computers inside a private network a public address. The NAT process helps with the conservation of IP addresses and provides better security.

1. **Implement Inter VLAN Routing**

Inter-VLAN routing can be defined as a way to forward traffic between different VLAN by implementing a router in the network. As we learnt previously, VLANs logically segment the switch into different subnets, when a router is connected to the switch, an administrator can configure the router to forward the traffic between the various VLANs configured on the switch. The user nodes in the VLANs forwards traffic to the router which then forwards the traffic to the destination network regardless of the VLAN configured on the switch. Inter-VLAN routing is the ability to route, or send, traffic between VLANs that are normally blocked by default.

1. **Observe STP topology changes and implement RSTP.**

* **Implement Advanced STP Modifications and Mechanism**
* **Implement MST**

**Spanning tree protocol (STP)** is predominantly used to prevent layer 2 loops and broadcast storms and is also used for network redundancy. It was developed around the time where recovery from an outage that took upwards of a minute or more was acceptable.

STP evolved into **rapid spanning tree protocol (RSTP)**, which offers several improvements over STP (802.1D). It has new port states and port roles and, more importantly, faster convergence times. RSTP works by adding an alternative port and a backup port compared to STP. These ports are allowed to immediately enter the forwarding state rather than passively wait for the network to converge. Both STP or RSTP are critical to having a healthy network and an administrator would benefit from using RSTP over STP.

**Multiple Spanning Tree (MST)** was created to allow for multiple spanning tree topologies while preserving scalability. MST enables an administrator to map an arbitrary number of VLANs to a single MST instance, resulting in the minimum number of instances needed to satisfy a design.