**Designing the Enterprise Branch**

The Cisco Enterprise Branch Architecture takes into account services such as voice, data, video, and security that customers want to deploy at their endpoints, no matter how far away the endpoints are or how they are connected. Using Borderless Networks, the Cisco Enterprise Branch Architecture should provide seamless connectivity.

An effective network design for enterprise branches and teleworkers requires knowledge of the campus technologies.

**Enterprise Branch Architecture**

The Cisco Enterprise Branch Architecture takes into account the services that customers want to deploy at their endpoints, no matter how far away the endpoints are or how they are connected.

Customers are seeking opportunities to protect, optimize, and grow their businesses by increasing security and consolidating voice, video, and data onto a single IP network. Additional concerns include investing in applications that will improve productivity and operating efficiencies. These services provide customers with new opportunities to reduce costs, improve productivity, and safeguard information assets.

The Cisco Enterprise Branch Architecture is an integrated, flexible, and secure framework for extending headquarters applications in real time to remote sites. It uses the Cisco Network Architectures for the Enterprise framework but applies it to the smaller scale of a branch location. Common network components that can be implemented in the branch include the following:

* Routers that provide WAN edge connectivity
* Switches that provide the LAN infrastructure
* Security appliances that defend the branch devices
* Wireless access points for device mobility
* Call-processing and video equipment for IP telephony and video support
* End-user devices, including IP phones and computers

**Enterprise Branch Design**

Requirements vary for different-sized branch offices. For the branch design, the following questions should be asked:

1. How many branch locations need to be supported?
2. How many existing devices (users, hosts, and network infrastructure) will be supported at each location?
3. What amount of scalability should be supported? (How much growth is expected at each location?)
4. What are the high-availability requirements at each location?
5. Which level of security should be integrated in the design?
6. Should security be managed locally or through the corporate location?
7. Are there any requirements for local server farms or network areas that sit between the internal network and an external network (a demilitarized zone [DMZ])?
8. Should network management be supported locally or through the corporate location?
9. What wireless services are needed, and how will they affect the clients, network, and environment?
10. What is the approximate available budget?

The number of devices that are supported is limited by the physical number of ports available. In addition to the scalability considerations, the high-availability requirements point to various design models as well.

It is recommended that branch offices be categorized based on the number of users as follows:

* **Small office:** Up to 50 users, single-tier design
* **Medium office:** Between 50 and 100 users, dual-tier design
* **Large office:** Between 100 and 200 users, three-tier design

Using this classification, the design models are described in the following sections. High availability, scalability, and migration to advanced services requirements also influence the model to be adopted.

**NOTE**

The remote teleworker (branch of one) design model is also discussed in this section.

The Integrated Services Router (ISR) at the WAN edge provides various voice, security, and data services that are integrated with the LAN infrastructure. Depending on the edge router, the following interfaces are available to integrate with the LAN:

* Integrated interfaces (10/100/1000)
* High-speed WAN interface card (WIC) Ethernet 10/100 interfaces
* Network modules
* Embedded security

**New Features on the ISR G2 Routers**

The Cisco Integrated Services Router Second Generation (ISR G2) portfolio builds upon the market success of the first generation of ISRs with new features that deliver greater enhancements for service virtualization, video-ready capabilities, and operational excellence. The Cisco ISR G2 innovations deliver the following:

* Video-ready branch office for a superior customer experience with new services that transform the branch-office workspace such as
  + Media engines that enable business-grade video applications that are based on high-density, video-ready digital signal processors (DSP) that deliver the medianet high-definition experience
  + Bandwidth-optimized and scalable video services, including media-rich video conferencing, video surveillance, video streaming, and digital signage
  + High-performance (up to 8x), nonstop branch office experience to meet your future WAN and services requirements
  + Cisco TelePresence capability to your midsize branch offices with T1/E1 links
* Service virtualization to deliver highly effective business innovation that achieves unparalleled service that includes
  + Cloud extensibility and services virtualization for mission-critical application survivability to remote sites
  + Broadest services offering to all branch-office sites, including security, unified communications, WAN optimization, application integration, and customizable virtual services
  + A revolutionary "on-demand" services delivery model that is enabled by the innovative Cisco Services Ready Engine (SRE)

**Small Branch Office Design**

Small branch office designs connect the access router with Layer 2 switch ports in one of three ways:

* **Integrated switching in the ISR or multiservice router:** This option has a lower port density and supports from 16 to 48 client devices on either a Cisco EtherSwitch network module or a Cisco EtherSwitch service module. This option provides a one-box solution that offers ease of management and uses the Cisco 3900 Series ISR or Cisco 2900 Series ISR for streamlined branch offices. Depending on the module, the integrated switch ports can provide power to end devices using Power over Ethernet (PoE).
* **Trunked network interface on the ISR to external switches or access points:** There is no link redundancy between the access switches or access points and the ISR. The access switches can provide power to end devices, including access points using PoE.
* **Logical EtherChannel interface between the ISR and access switches:** This approach uses a Cisco EtherSwitch module in the ISR to provide link redundancy to access layer switches. The access switches can provide power to end devices using PoE.

In all cases, the default gateway is on the ISR. The ISR provides Layer 3 services such as DHCP, firewall, and Network Address Translation (NAT).

If redundant access layer links and higher-bandwidth uplinks are required, only the second option, with higher-performance devices, can be used. The choice of the edge router also depends on the voice and Virtual Private Network (VPN) support that is needed.

The access switch supports Layer 2 services, and the Cisco ISR provides Layer 3 services. Typical access switches include the Cisco Catalyst 2960, 3560, and 3750 Series switches. To keep manageability simple, there are no loops in the topology.

**NOTE**

Although there are no Layer 2 loops in the planned design, spanning tree must be enabled and configured to protect the network from any accidental loops.

The recommended spanning-tree protocol is Rapid per-VLAN Spanning Tree Plus (RPVST+) for all Layer 2 deployments in a branch office environment. There is a default gateway for each VLAN configured in the topology. All the Layer 3 configurations are done on the ISR. The access switches must be configured with an IP address for management purposes.

Both the Cisco 2921 and 2951 ISRs support three integrated 10/100/1000 interfaces, which are Layer 3 native. Both the Cisco 2921 and 2951 ISRs support one slot for a network module. The Cisco 2921 and 2951 ISRs both support the 16-, 24-, and 48-port Cisco EtherSwitch network modules.

**Medium Branch Office Design**

The medium branch office topology is similar to the small office topology. One exception is that the WAN edge devices are larger, typically two Cisco 2921 or Cisco 2951 ISRs, and the access switches supporting LAN connectivity are external.

To scale up to 100 users, the following options are available:

* Use a higher-port-density external access switch.
* Use an ISR module that supports switched access ports that provide redundancy in the connection to the access switches through EtherChannel.

This design uses the integrated 10/100/1000 interfaces as Layer 3 trunks, providing the flexibility to use various access switches. The stackable Cisco Catalyst 3750 Series switch with an IP base image or an IP services image can be used as the access switch to support 24 or 48 users per switch. The IP base image feature set includes advanced quality of service (QoS), rate limiting, access control lists (ACL), and basic static and Routing Information Protocol (RIP) routing capability. The IP services image provides a richer set of enterprise-class features, including advanced hardware-based IP unicast and multicast routing.

An additional Advanced IP Services Software license is also available. This license is required for IP version 6 (IPv6) routing (Layer 3 switching).

With Cisco StackWise technology, customers can create a single, 32-Gbps switching unit with up to nine Cisco Catalyst 3750 Series switches. Cisco StackWise technology uses special stack-interconnect cables and stacking software. The stack behaves as a single switching unit that is managed by a master switch that is elected from one of the member switches. The master switch automatically creates and updates all the switching and optional routing tables. Support for the number of users needing PoE depends on the specific access switch that is used.

**Large Branch Office Design**

A large branch office design is like a small to medium campus design with 100 to 1000 users.

In addition to supporting more users, a large office might also need higher LAN switching capability if it is supporting a server farm or DMZ. Support for some of these services requires the use of appliance devices if higher throughput is required. To meet these requirements, a distribution layer is added to the small-office or medium-office topology by introducing a multilayer switch to provide the required LAN switching capabilities, port density, and flexibility to support additional appliances.

A stacked switch LAN topology is highly available, scalable, and manageable. High-availability requirements are met because link redundancy and device redundancy are built into the design. For high availability between the distribution and the edge layers, redundant links are used.

The port density of the stacked switches allows a number of access switches to be connected without compromising high availability. The distribution switches typically run the enhanced images, which support more features, including various routing protocols and advanced features, such as policy-based routing.

If Cisco Catalyst 3560 and 3750 Series switches are used at the access layers, other Layer 2 security features, such as DHCP snooping, Dynamic ARP Inspection (DAI), and IP Source Guard, can be enabled to provide additional security measures. The default gateways for all the VLANs at the access layer are configured on the distribution layer.

**Enterprise Teleworker (Cisco Virtual Office Solution) Design**

Another remote place in the enterprise network consists of the enterprise teleworkers. Organizations are constantly striving to reduce costs, improve employee productivity, and retain valued employees. These goals can be attained by providing employees with the ability to work from home with the same level of quality, function, performance, convenience, and security that is available in the office. With a work environment in the residence, employees can optimally manage their work schedules, allowing higher productivity (less affected by office distractions) and greater job satisfaction (flexibility in schedule). This transparent extension of the enterprise to employee homes is the objective of the Cisco Enterprise Teleworker (or Cisco Virtual Office solution) Architecture.

Occasional remote users have much lighter application requirements than part-time and full-time teleworkers. They can connect through a wireless hotspot or as a guest network at a hotel, allowing them to have little control over network resiliency and availability.

The situation of enterprise teleworkers that are operating as a Cisco Virtual Office can be differentiated from other forms of work-at-home or telecommuting scenarios. The difference is that the emphasis is on delivering seamless managed accessibility to the complete range of applications and services that are critical to the operational effectiveness of enterprises. The Cisco Enterprise Teleworker Architecture is part of the overall secure Cisco Network Architectures for the Enterprise infrastructure. The Cisco Enterprise Teleworker Architecture gives companies the ability to integrate and securely manage their remote workers within the corporate network, while providing a high-quality end-user experience that supports a complete range of enterprise applications for the enterprise teleworker. The enterprise teleworker typically connects to an ISP through a DSL or cable modem and can use an analog dialup session to back up this connection.

The enterprise teleworker solution is implemented with a small ISR such as the Cisco 877, 878, and 888 Integrated Services Routers with integrated switch ports behind a broadband modem. The solution uses a transparent, always-on VPN tunnel back to the enterprise.

This architecture provides centralized management, where the customer can apply security policies, push configurations, and periodically test the connection through the broadband cloud and back to the corporate office. This allows the customer to see the latency, jitter, and packet loss that is being experienced at any given time. This solution can support advanced applications such as voice and video as part of the complete suite of enterprise services for the end user. For example, a teleworker can access the central-office IP telephone system from home, with comparable voice quality. The teleworker can also take advantage of higher-function IP telephony capabilities instead of using the public switched telephone network (PSTN).

An alternative solution is an unmanaged VPN approach, where the end user implements a software VPN from the PC across a generic broadband router, access point, or hub appliance. This alternate solution typically cannot support the level of feature integration, QoS, and managed support that is needed to deliver voice, video, multimedia, and traditional data to the end user in a reliable manner. The alternate solution is appropriate for occasional remote users, with their lighter application requirements.

**New ISRs for Small Offices and Teleworkers**

Cisco 860 and 880 Series ISRs deliver integrated services at broadband speeds to small offices and teleworkers or to service providers to deploy as part of their managed network services:

* Cisco 860 Series ISRs offer the following:
  + Concurrent broadband services for small offices and remote sites
  + Security features, including:
    - Stateful Inspection Firewall
    - IPsec VPNs (Triple Data Encryption Standard [3DES] or Advanced Encryption Standard [AES])
  + 4-port 10/100 Fast Ethernet managed switch with VLAN support
  + CON/AUX port for console or external modem
  + Secure IEEE 802.11g/n access-point option that is based on the IEEE 802.11n 2.0 standard
  + Easy setup, deployment, and remote management capabilities through web-based tools and Cisco IOS Software
* Cisco 880 Series ISRs offer the following:
  + High performance for broadband access in small offices and small branch-office and teleworker sites
  + Collaborative services with secure analog, digital voice, and data communication
  + Business continuity and WAN diversity with redundant WAN links: Fast Ethernet, symmetric high-bit-rate DSL (G.shdsl), asymmetric DSL (ADSL) 2/2+, very-high-data-rate DSL 2 (VDSL2), third-generation (3G), and ISDN
  + Survivable Remote Site Telephony (SRST) voice continuity for enterprise small branch-office and teleworker sites
  + Enhanced security, including:
    - Firewall: With advanced application and control for email, instant messaging (IM), and HTTP traffic
    - Site-to-site, remote-access and dynamic VPN services: IPsec VPNs (3DES or AES), Dynamic Multipoint VPNs (DMVPN), Group Encrypted Transport VPNs (GET VPN) with onboard acceleration, and Secure Socket Layer (SSL) VPNs
    - Intrusion prevention system (IPS): An inline, deep-packet inspection feature that effectively mitigates a wide range of network attacks
    - Content filtering: A subscription-based integrated security solution that offers category-based reputation rating, keyword blocking, and protection against adware, malware, spyware, and URL blocking
  + Four-port 10/100 Fast Ethernet–managed switch with VLAN support; two ports support Power over Ethernet (PoE) for powering IP phones or external access points
  + Secure IEEE 802.11g/n access-point option based on draft 802.11n standard with support for autonomous or Cisco Unified WLAN architectures
  + CON/AUX port for console or external modem
  + One USB 1.1 port for security eToken credentials, booting from USB, and loading configuration
  + Easy setup, deployment, and remote-management capabilities through web-based tools and Cisco IOS Software

Assignment:

Discuss & design the Enterprise network considering the following scenario

1.Ambo University for an enterprise design

2.Woliso campus for a campus design

Apply the suitable architecture (single/2/3 tier) & justify your tier selection, also demonstrate the same with appropriate diagrams.