To design a network infrastructure and IPV4 addressing scheme for the company, we need to consider the following requirements:

1. The company has four departments – Finance/HR, Engineering, Sales, and Administration – and each department has a different number of computers.
2. The company requires five servers – Web, Email, DNS, Authorisation, and a File/Print server.
3. All office-based users should have access to all servers.
4. External users can access the company’s external website only.
5. The company allows staff to use a wireless network with their own devices to access the internet, but these devices should not be allowed to access the departmental networks.
6. The company would like to trial the use of IoT devices to monitor the server room.

Based on the above requirements, we can design the following network infrastructure:

1. VLANs:
2. We will create separate VLANs for each department to ensure network security and efficient network management. There will be a separate VLAN for the wireless network for staff devices. We will also create a VLAN for IoT devices used to monitor the server room.
3. Subnets:
4. We will assign a different subnet to each department VLAN. This will ensure that each department has a separate IP address range and can communicate with other departments through the router.
5. Servers:
6. We will install five servers in the server room – Web, Email, DNS, Authorisation, and a File/Print server. All servers will be connected to a switch in the server room, which will be connected to the router.
7. Wireless Network:
8. We will set up a wireless network for staff devices and assign it a separate VLAN. This network will be secured using WPA2 Enterprise authentication and will use RADIUS authentication with the Authorisation server. This will ensure that only authorised users can access the wireless network.
9. IoT Devices:
10. We will install IoT devices in the server room to monitor temperature, humidity, and other parameters. These devices will be connected to a separate VLAN to ensure security and efficient network management.
11. IP Addressing Scheme:
12. We will use the following IP addressing scheme:

* Finance/HR Department: 192.168.1.0/24
* Engineering Department: 192.168.2.0/24
* Sales Department: 192.168.3.0/24
* Administration Department: 192.168.4.0/24
* Wireless Network: 192.168.5.0/24
* IoT Devices: 192.168.6.0/24
* Servers: 192.168.7.0/24

We will assign IP addresses to the servers as follows:

* Web Server: 192.168.7.10
* Email Server: 192.168.7.20
* DNS Server: 192.168.7.30
* Authorisation Server: 192.168.7.40
* File/Print Server: 192.168.7.50

All computers and devices in each department will be assigned IP addresses from their respective departmental subnets.

In summary, we will design a network infrastructure with separate VLANs for each department, a wireless network for staff devices, and a separate VLAN for IoT devices. We will use a different subnet for each department VLAN and assign IP addresses to the servers and devices accordingly. This will ensure efficient network management, security, and effective communication between departments and servers.

The network infrastructure and IPV4 addressing scheme designed for the company is scalable and available because it allows for easy expansion and can handle increased traffic and users without causing downtime or performance issues.

Scalability:

The VLANs and subnets used in the network design provide scalability. If the company expands in the future, we can simply add new VLANs and subnets for new departments or groups of users. We can also add more switches and routers to expand the network and improve its performance. The IP addressing scheme allows for easy scalability, as we can simply allocate new IP addresses from a different subnet for new devices or users.

The use of a separate VLAN for IoT devices allows for easy scaling of the network monitoring capabilities. If the company decides to install more IoT devices in the future, we can simply assign them IP addresses from the IoT VLAN and connect them to the switch.

Availability:

The network infrastructure is also designed to provide high availability. All servers are connected to a switch, which is connected to a router, ensuring redundancy and fault tolerance. If one switch or router fails, the other switch or router can take over without causing downtime.

The use of multiple servers for Email, DNS, and File/Print services ensures high availability of these critical services. If one server fails, the other servers can take over without causing downtime or loss of data.

The use of RADIUS authentication with the Authorisation server and WPA2 Enterprise authentication for the wireless network ensures that only authorised users can access the network, improving its security and availability.

In conclusion, the network infrastructure and IPV4 addressing scheme designed for the company is scalable and available. It can handle future expansion, and its design ensures high availability, fault tolerance, and security.

A Bring Your Own Device (BYOD) policy allows employees to use their personal devices, such as smartphones, laptops, and tablets, to access the corporate network. While there are potential benefits to implementing a BYOD policy, such as increased productivity and cost savings, there are also several legal and ethical implications that need to be considered:

Legal implications:

1. Data security: By allowing employees to use personal devices on the corporate network, the company risks exposing sensitive data to unauthorized access and theft. In case of a data breach, the company could be held liable for not taking adequate measures to secure its data.
2. Data retention: With personal devices accessing the corporate network, the company may struggle to retain control over its data. This could lead to potential legal issues related to data retention and e-discovery, which could result in significant fines and legal action.
3. Compliance: BYOD policies must be in compliance with various laws and regulations, such as HIPAA and GDPR, that govern the collection, storage, and use of personal data. Failure to comply with these laws could result in legal action, fines, and loss of reputation.

Ethical implications:

1. Employee privacy: A BYOD policy could violate employee privacy by allowing the company to access personal information on employees' devices. This could lead to mistrust and damage to employee morale.
2. Discrimination: A BYOD policy could lead to discrimination against employees who cannot afford the latest devices or those who prefer not to use their personal devices for work. This could lead to unequal treatment of employees and damage to the company's reputation.
3. Work-life balance: Allowing employees to use their personal devices for work could blur the line between work and personal life, leading to burnout and decreased job satisfaction.

In conclusion, while a BYOD policy has the potential to bring several benefits to a company, such as cost savings and increased productivity, it also poses several legal and ethical challenges. Companies should carefully consider the potential legal and ethical implications before adopting a BYOD policy and should take adequate measures to mitigate the risks associated with such a policy. This may include implementing security protocols, ensuring compliance with laws and regulations, and ensuring employee privacy and work-life balance.

The network includes a router that connects to the internet, a firewall providing NAT, and a switch that connects to the router and provides connectivity to the four departments. The switch is configured with VLANs for each department, with the Finance/HR department assigned VLAN ID 10, Engineering assigned VLAN ID 20, Sales assigned VLAN ID 30, and Administration assigned VLAN ID 40.

The network also includes five servers: Web, Email, DNS, Authorisation, and a File/Print server. There are 3 server machines for Email, DNS & file/ print server, which are accessible by all company computers and authorized wireless devices, providing shared services to authorized users. There is 1 server machine for authorisation server which authorizes users to logon to the internal company resources (servers and workstations). There is 1 web server machine which hosts an externally facing website accessible to any users.

Authorized wireless devices can access the servers, but not the departmental networks. Additionally, the network includes IoT devices used to monitor the server room.

he network design for the company consists of a simple topology with a router, firewall, switch, and separate VLANs for each department, including Finance/HR, Engineering, Sales, and Administration. The network includes a total of 395 desktop workstations spread across the departments, with 120 for Finance/HR, 50 for Engineering, 200 for Sales, and 25 for Administration.

In addition to the desktop workstations, the network includes five servers: Web, Email, DNS, Authorisation, and a File/Print server. There are three server machines for Email, DNS & file/print server, which are accessible by all company computers and authorized wireless devices, providing shared services to authorized users. There is one server machine for the authorisation server, which authorizes users to logon to the internal company resources (servers and workstations). There is one web server machine, which hosts an externally facing website accessible to any users.

The network isolation is achieved by using separate VLANs for each department. Each departmental VLAN is isolated from the others, preventing unauthorized access to departmental networks. In addition, wireless devices can access the servers but not be permitted to access the departmental networks, providing an additional layer of security.

The IP addressing scheme for the network is designed to provide a unique IP address to each device on the network. Each departmental VLAN is assigned a specific IP address range, which allows for efficient routing of network traffic. The network also includes a DHCP server, which is used to dynamically assign IP addresses and other network configuration settings to client devices on the network.

Overall, the network design is intended to provide a scalable, available, and secure network infrastructure that meets the needs of the company.

The protocols used in a network infrastructure can vary depending on the specific devices and applications used. However, based on the network described in the previous questions, here are some of the protocols that may be used:

1. TCP/IP: TCP/IP is the primary protocol used for communication on the internet and is the standard protocol used for most network communication. It is used for addressing, routing, and transmitting data across the network.
2. DNS: The DNS protocol is used to translate domain names into IP addresses. DNS servers are used to maintain a database of domain names and their associated IP addresses.
3. HTTP/HTTPS: The HTTP/HTTPS protocol is used for web browsing and is used to request and receive web pages and other content from web servers.
4. SMTP/IMAP/POP3: These are email protocols used for sending and receiving email messages. SMTP is used for sending email, while IMAP and POP3 are used for retrieving email messages from servers.
5. DHCP: The DHCP protocol is used for dynamically assigning IP addresses and other network configuration settings to client devices on the network.
6. VLAN: The VLAN protocol is used to create separate virtual networks within a physical network. This protocol is used to segment network traffic based on departments or other criteria, which increases network security and management.
7. SNMP: SNMP is used for network monitoring and management. It is used to collect and monitor data from network devices such as switches, routers, and servers.
8. RADIUS: RADIUS is used for user authentication and authorization in networks. It is used to control access to network resources and is commonly used in conjunction with wireless networks.

These are just a few of the many protocols that may be used in a network infrastructure. The specific protocols used can depend on the hardware and software used in the network, as well as the specific requirements of the network.

The IP addressing scheme for the network is designed to provide a unique IP address to each device on the network. The IP addressing scheme is divided into four octets, with each octet containing a value between 0 and 255. IP addresses are written in dotted-decimal notation, with each octet separated by a period. For example, an IP address of 192.168.1.1 is a common IP address used in private networks.

For the company described in the previous questions, each departmental VLAN is assigned a specific IP address range. The Finance/HR department has 120 computers, and it is assigned the IP address range of 192.168.10.0/24. This means that the IP addresses for the Finance/HR departmental VLAN will range from 192.168.10.1 to 192.168.10.254, with the subnet mask of 255.255.255.0.

The Engineering department has 50 computers and is assigned the IP address range of 192.168.20.0/24. This means that the IP addresses for the Engineering departmental VLAN will range from 192.168.20.1 to 192.168.20.254, with the subnet mask of 255.255.255.0.

The Sales department has 200 computers and is assigned the IP address range of 192.168.30.0/24. This means that the IP addresses for the Sales departmental VLAN will range from 192.168.30.1 to 192.168.30.254, with the subnet mask of 255.255.255.0.

The Administration department has 25 computers and is assigned the IP address range of 192.168.40.0/24. This means that the IP addresses for the Administration departmental VLAN will range from 192.168.40.1 to 192.168.40.254, with the subnet mask of 255.255.255.0.

The five servers are assigned static IP addresses within each departmental VLAN. Additionally, the router and firewall are assigned IP addresses within each departmental VLAN to enable routing and firewall functions.

Overall, the IP addressing scheme is designed to provide efficient routing of network traffic while ensuring that each device on the network has a unique IP address.

The network design described in the previous questions utilizes several technologies and protocols to provide network isolation, scalability, and security. Here's a summary of how each technology/protocol is utilized in the network:

1. VLANs: VLANs are used to provide network isolation between different departments in the company. Each department is assigned to a separate VLAN, which prevents network traffic from one department from interfering with another department. VLANs also enable better network management by allowing network administrators to group devices based on function or location.
2. Trunking: Trunking is used to carry traffic between switches for multiple VLANs. VLAN traffic is tagged with a VLAN identifier when it is transmitted between switches to ensure that it is delivered to the correct VLAN. Trunking enables better network management by reducing the number of physical connections required between switches.
3. Access control: Access control is used to restrict access to network resources based on user identity and role. An authorization server is used to authenticate users and grant them access to network resources based on their role in the organization. This ensures that only authorized users can access sensitive data and applications on the network.
4. DHCP: DHCP is used to automatically assign IP addresses to devices on the network. This reduces the need for manual IP address configuration and enables better management of IP address assignments. DHCP also reduces the risk of IP address conflicts by ensuring that each device is assigned a unique IP address.
5. STP: STP (Spanning Tree Protocol) is used to prevent network loops and ensure that there is a single path between switches. This improves network reliability by preventing network loops, which can cause broadcast storms and other network issues.
6. VTP: VTP (VLAN Trunking Protocol) is used to manage VLAN configurations between switches. It enables network administrators to make changes to VLAN configurations on one switch and have those changes automatically propagated to all other switches in the network.

Overall, the use of VLANs, trunking, access control, DHCP, STP, and VTP in this network design provides network isolation, scalability, security, and efficient network management.

Interfaces between components in a network can use either internal or external network addresses depending on the location of the components and the purpose of the interface. Here are some guidelines for when to use internal or external addresses:

1. Internal network addresses: These addresses are used for interfaces between components that are within the same network or subnet. For example, interfaces between PCs, switches, servers, and other network devices that are located within the company's network should use internal network addresses. Internal addresses are typically private IP addresses that are not routable over the internet. They are used for communication within a local network and are not accessible from outside the network.
2. External network addresses: These addresses are used for interfaces between components that are located in different networks or subnets. For example, interfaces between the company's web server and external clients should use external network addresses. External addresses are typically public IP addresses that are routable over the internet. They are used for communication between different networks and can be accessed from outside the network.

In the network design described in the previous questions, interfaces between the web server and external clients should use external network addresses. The web server is located in the company's internal network, but it provides services to external clients over the internet. Therefore, the web server needs to use an external IP address that is accessible from outside the network.

Interfaces between other components, such as switches, servers, and PCs, should use internal network addresses since they are located within the company's internal network. The authorization server, which is responsible for authenticating users and granting access to network resources, should also use internal network addresses since it is located within the company's internal network and is accessed only by authorized users within the network.

In the above network, we have four departments - Finance/HR, Engineering, Sales, and Administration, each having a specific number of computers. The IP addressing scheme for the network uses Class C addresses with a subnet mask of 255.255.255.0.

To assign IP addresses to the devices in each department, we need to create subnets. We can divide the Class C network address into smaller subnets using the subnet mask.

Here's how we can create subnets for each department:

1. Finance/HR: This department has 120 computers. We can use the IP address range 192.168.1.1 to 192.168.1.126 for this department. The subnet mask is 255.255.255.128, which gives us two subnets - 192.168.1.0/25 and 192.168.1.128/25.
2. Engineering: This department has 50 computers. We can use the IP address range 192.168.2.1 to 192.168.2.62 for this department. The subnet mask is 255.255.255.192, which gives us four subnets - 192.168.2.0/26, 192.168.2.64/26, 192.168.2.128/26, and 192.168.2.192/26.
3. Sales: This department has 200 computers. We can use the IP address range 192.168.3.1 to 192.168.3.254 for this department. The subnet mask is 255.255.255.0, which gives us one subnet - 192.168.3.0/24.
4. Administration: This department has 25 computers. We can use the IP address range 192.168.4.1 to 192.168.4.30 for this department. The subnet mask is 255.255.255.224, which gives us two subnets - 192.168.4.0/27 and 192.168.4.32/27.

In addition to these departmental subnets, we also need to allocate IP addresses to the servers, wireless devices, and IoT devices. We can use a separate subnet for each of these devices or group them together in a single subnet, depending on the specific requirements of the network.We can group the IOT and severs together

The IP addressing scheme in the network design uses Class C addresses because this class of IP addresses provides a sufficient number of addresses for the network's requirements while allowing for efficient use of IP address space.

Class C addresses provide 24 bits for the network portion of the address and 8 bits for the host portion, allowing for up to 254 hosts on each subnet. This is sufficient for most small to medium-sized networks, such as the one in the network design.

Using Class C addresses also allows for more efficient use of IP address space compared to higher classes, such as Class A or B, which provide more address space than is required for most small to medium-sized networks. By using Class C addresses, we can conserve IP address space and avoid wasting unused IP addresses.

Furthermore, Class C addresses are commonly used for LANs and provide a good balance between address space and network management complexity, making them a suitable choice for the network design's requirements.

To meet the scalability and availability requirements and allow for future growth of the network, the following additional network components can be added:

1. Redundant routers and switches: Redundant routers and switches can be added to the network to provide high availability and fault tolerance. This can be achieved using protocols such as Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) to prevent network loops and ensure network availability in case of a failure.
2. Load balancers: Load balancers can be added to distribute traffic across multiple servers to prevent overloading of a single server and to ensure high availability. This can be achieved using protocols such as Virtual Router Redundancy Protocol (VRRP) or Hot Standby Router Protocol (HSRP) to provide redundancy and failover in case of a failure.
3. Virtualization: Virtualization can be used to create multiple virtual machines (VMs) on a single physical server to improve scalability and reduce hardware costs. This can be achieved using technologies such as Virtual LANs (VLANs) and Virtual Private Networks (VPNs) to create isolated networks and secure connections between VMs.
4. Dynamic routing protocols: Dynamic routing protocols can be used to automatically discover and learn about network changes and to select the best path for data transmission. This can be achieved using protocols such as Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP) to ensure efficient and reliable routing of data.
5. IPv6 addressing: IPv6 addressing can be used to provide a larger address space and to support future growth of the network. This can be achieved using protocols such as Neighbor Discovery Protocol (NDP) and Internet Control Message Protocol version 6 (ICMPv6) to support IPv6 addressing and routing.
6. Network management tools: Network management tools can be used to monitor and manage network performance and security. This can be achieved using technologies such as Simple Network Management Protocol (SNMP) and Network Configuration Protocol (NETCONF) to manage network devices and configurations.

Overall, adding these additional network components and using supporting technologies and protocols can improve the scalability and availability of the network and ensure that it can support future growth and changing requirements.

The core layer is the backbone of the network and provides high-speed connectivity between different parts of the network. In this network design, the core layer consists of the two redundant core switches.

The core switches are responsible for switching packets between different parts of the network, providing a high-speed, low-latency path for data to travel. As a result, they need to be highly available, scalable, and fast. They should also support advanced features such as QoS, VLANs, and routing protocols to provide optimal network performance.

At the core layer, there is typically minimal packet processing or manipulation, and traffic is typically forwarded based on destination address alone. This is done to minimize latency and ensure efficient traffic flow.

The core layer is also responsible for providing fault tolerance and redundancy to ensure the network is always available. In this design, both core switches are configured with HSRP to provide a virtual IP address for redundancy. The use of redundant links between the switches and the other layers of the network also ensures that there are no single points of failure.

Overall, the core layer is critical for ensuring a fast and reliable network infrastructure that can handle large amounts of traffic.

The distribution layer is responsible for aggregating traffic from access layer switches and providing connectivity to the core layer. In this network design, the distribution layer consists of several switches that are responsible for interconnecting the access layer switches and routing traffic to the core switches.

At the distribution layer, switches typically implement advanced features such as VLANs, Quality of Service (QoS), and Access Control Lists (ACLs) to provide better control over network traffic. The VLANs are used to segment the network into different logical groups to provide better security, manageability, and performance. QoS is used to prioritize and control bandwidth for specific types of traffic to ensure that mission-critical applications receive priority. ACLs are used to enforce security policies and control access to network resources.

The distribution layer is also responsible for implementing routing protocols to enable communication between different VLANs and subnets. This allows the network to scale and grow over time as new departments or users are added. In this design, the distribution layer switches are configured to use routing protocols such as OSPF or EIGRP to provide efficient routing and fault tolerance.

Overall, the distribution layer is critical for ensuring that the network scales and is designed to meet the needs of the various departments within the organization. It provides the necessary interconnectivity and security features to ensure that traffic is efficiently and securely routed to its destination.

The access layer is the edge of the network and is responsible for connecting end-user devices such as desktops, laptops, and printers to the network. In this network design, the access layer consists of switches that are located in each department and provide connectivity for the desktop workstations.

At the access layer, switches provide connectivity to end-user devices and enforce network policies such as VLAN membership, port security, and Quality of Service (QoS). The switches are also responsible for forwarding traffic to the distribution layer switches, which in turn route traffic to the core switches.

In this design, each department is assigned a separate VLAN to provide network isolation and security. Access layer switches are configured to ensure that only authorized devices are able to connect to the network. This is achieved through the use of port security and MAC address filtering, which ensures that only devices with authorized MAC addresses are allowed to connect to the network.

In addition, Quality of Service (QoS) is implemented at the access layer to prioritize traffic and ensure that mission-critical applications receive priority. This is particularly important in a network where there are multiple departments with different application requirements.

Overall, the access layer is responsible for providing connectivity to end-user devices while ensuring network security and performance. It is designed to be scalable and flexible, enabling the addition of new devices and departments as the organization grows over time.

In this network design, load balancers are used to distribute network traffic across multiple servers to improve the performance, scalability, and availability of network services.

There are several servers in the network, including web servers, email servers, DNS servers, and a file/print server. Each of these servers provides critical network services to users, and as such, must be highly available and scalable to meet demand.

To achieve this, load balancers are used to distribute traffic across multiple instances of each server, ensuring that no single server becomes overloaded with traffic. This not only improves performance and scalability but also ensures that if one server fails, traffic can be automatically redirected to a healthy server.

For example, the web server is used to host an externally facing website that is accessible to any user. To ensure that the website is always available and can handle high traffic volumes, load balancers are used to distribute traffic across multiple instances of the web server. This not only improves website performance but also ensures that if one web server fails, traffic can be automatically redirected to a healthy web server.

In addition, load balancers can also be used to perform SSL/TLS offloading, which improves the performance of encrypted traffic by offloading the CPU-intensive encryption process from the web server to the load balancer.

Overall, load balancers are an essential component of this network design, helping to ensure that critical network services are highly available, scalable, and performant.

Redundant routers and switches are essential components of this network design to ensure high availability and resiliency.

In this network, two core switches are used in a redundant configuration, connected to each other with multiple links, and both connected to the distribution layer switches. This provides redundancy at the core layer of the network, ensuring that if one core switch fails, the other can take over and continue to provide connectivity to the network.

At the distribution layer, two switches are also used in a redundant configuration, connected to each other with multiple links, and both connected to the access layer switches. This provides redundancy at the distribution layer of the network, ensuring that if one distribution switch fails, the other can take over and continue to provide connectivity to the network.

At the access layer, each access switch is connected to both distribution switches, providing redundant connectivity to the network. This also allows for load balancing of traffic between the two distribution switches, improving performance and resiliency.

Redundant routers are not explicitly mentioned in this network design, but they could be added at the network perimeter to provide redundancy for internet connectivity. For example, two routers from different ISPs could be used, each connected to a separate firewall, providing redundancy for internet connectivity.

Overall, redundant routers and switches are essential components of this network design, helping to ensure that critical network services are highly available and resilient to failures.

DHCP (Dynamic Host Configuration Protocol) is a protocol that can simplify IP address management in this network design by automating the process of assigning IP addresses to devices on the network.

With DHCP, a DHCP server can be configured to automatically assign IP addresses to devices on the network as they connect. This eliminates the need for manual IP address assignment, which can be time-consuming and error-prone in larger networks. DHCP can also simplify IP address management by providing a centralized location for managing IP address leases and making it easier to track IP addresses in use on the network.

In this network design, a DHCP server could be deployed to assign IP addresses to devices on each VLAN. The DHCP server would be configured with a range of IP addresses for each VLAN, along with other network settings such as DNS server and default gateway. When a device connects to the network, it would send a DHCP request to the DHCP server, which would then assign an available IP address from the appropriate VLAN range.

DHCP also supports the use of reserved IP addresses, which can be used to ensure that certain devices are always assigned the same IP address. This can be useful for devices that require a static IP address for configuration or management purposes.

Overall, using DHCP in this network design can simplify IP address management by automating the process of assigning IP addresses to devices on the network, providing a centralized location for managing IP address leases, and reducing the potential for errors when manually assigning IP addresses.

Access control and VLANs (Virtual Local Area Networks) can play an important role in improving security in this network design by limiting access to network resources based on specific criteria and isolating network traffic to prevent unauthorized access.

Access control is the process of regulating access to network resources based on specific criteria, such as user identity, device type, or network location. In this network design, access control can be implemented through the use of an authorization server, which can authenticate and authorize user access to network resources. This can help to prevent unauthorized access to sensitive data or critical network resources, and limit the potential impact of security breaches.

VLANs can also be used to improve security by isolating network traffic to prevent unauthorized access. In this network design, separate VLANs are created for each department, and each VLAN is configured to limit access to specific resources based on departmental requirements. This can help to prevent unauthorized access to sensitive data or critical network resources, and limit the potential impact of security breaches.

In addition, VLANs can also be used to segregate network traffic for specific purposes, such as IoT devices monitoring the server room. By isolating this traffic from other network traffic, it can help to reduce the potential impact of security breaches or attacks on these devices.

Overall, access control and VLANs can improve security in this network design by limiting access to network resources based on specific criteria, isolating network traffic to prevent unauthorized access, and segregating network traffic for specific purposes. This can help to reduce the potential impact of security breaches and protect critical network resources.

In this network design, separate VLANs are created for each department - Finance/HR, Engineering, Sales, and Administration. Each VLAN is assigned a specific VLAN ID, and all devices within that VLAN are assigned IP addresses from the corresponding subnet.

To configure VLANs, network switches must be configured to support VLANs, typically using protocols such as Virtual LAN Trunking Protocol (VTP) or Multiple VLAN Registration Protocol (MVRP). Once configured, VLANs can be created by assigning specific ports on the switch to a particular VLAN, or by using 802.1Q tagging to assign a VLAN ID to traffic on a specific port.

In this network design, each switch is configured with separate VLANs for each department, and ports on each switch are configured to belong to the appropriate VLAN. For example, all ports connected to devices in the Finance/HR department are configured to belong to the Finance/HR VLAN, and all traffic on those ports is tagged with the corresponding VLAN ID.

In addition, to allow communication between VLANs, a Layer 3 switch or a router is configured with virtual interfaces for each VLAN. This allows the switch or router to route traffic between VLANs, while also enforcing access control policies to restrict access to resources based on departmental requirements.

Overall, configuring VLANs involves assigning specific ports on switches to VLANs, assigning VLAN IDs to traffic on specific ports using 802.1Q tagging, and configuring Layer 3 switches or routers with virtual interfaces for each VLAN. This allows for the isolation of network traffic, better security through access control, and more efficient use of network resources.

1. Network Topology:

We will use a hierarchical network topology with a core, distribution, and access layer. Each department will have its own access layer switch, which will connect to a distribution layer switch. The distribution layer switches will be connected to the core layer switch. The servers will be connected to the distribution layer switches. Wireless access points will be connected to the access layer switches.

1. VLANs:

We will create the following VLANs to separate the traffic:

* VLAN 10: Finance/HR Department
* VLAN 20: Engineering Department
* VLAN 30: Sales Department
* VLAN 40: Administration Department
* VLAN 50: Wireless Network
* VLAN 60: IoT Devices
* VLAN 70: Servers

1. Access Control:

We will use access control lists (ACLs) to control access to the servers and departmental networks. We will configure ACLs to allow access to the servers from authorised wireless devices and the authorisation server, but not from the IoT devices or departmental networks. We will configure ACLs to allow access to the external website from all networks.

The approach taken is to create a separate VLAN for each department to ensure that each department's network is separated from other departments. We will also create a separate VLAN for wireless devices and IoT devices. The five servers will be connected to all VLANs except for the departmental VLANs. The router will be used to interconnect the VLANs and provide Internet connectivity.

We will use the following routing and addressing protocols:

* Routing Protocol: We will use a dynamic routing protocol such as OSPF or EIGRP to exchange routing information between the router and switches.
* Addressing Protocol: We will use DHCP to automatically assign IP addresses to the workstations and wireless devices.

1. Additional Network Components for Scalability and Availability:

To meet the scalability and availability requirements, we can add the following network components:

* Load Balancers: Load balancers can be added to distribute traffic across multiple servers, improving performance and availability.
* Redundant Links: Redundant links can be added between the switches and router to provide redundancy and improve network availability.
* Virtualization: Virtualization can be used to consolidate multiple servers

Network Diagram

The above network diagram represents the network design for the given scenario. The network components used in the network are as follows:

Router: Used to connect different networks and perform routing functions.

Switch: Used to connect devices within the same network segment and forward data between them.

Firewall: Used to provide security by filtering incoming and outgoing traffic.

Server: Used to host services such as Web, Email, DNS, Authorization, and File/Print.

Wireless Access Point: Used to provide wireless access to staff-owned devices.

IoT Devices: Used to monitor the server room temperature and door.

Each departmental network is separated from other departments using VLANs. The wireless network and IoT devices are also separated from other networks using VLANs. The interfaces between the components use internal addresses, except for the interface between the router and the Internet, which uses an external address.