# **Guide for Network Design Plan**

A network design plan is a comprehensive document that outlines the structure, components, and configuration of a computer network. It serves as a blueprint for building, expanding, or upgrading a network infrastructure. The plan includes various elements and considerations to ensure the network meets the organization's requirements and supports its operations effectively. Here are some key components typically included in a network design plan:

1. Network Goals and Objectives: Clearly define the purpose and goals of the network design, such as enhancing performance, improving security, supporting scalability, or accommodating future technology advancements.

* Performance: The network should be designed to meet the organization's performance requirements, such as bandwidth and latency requirements.
* Security: The network design should incorporate security measures that are appropriate for the organization's needs, such as firewalls, access control, intrusion detection/prevention, and encryption protocols.
* Scalability: The network should be designed to accommodate the expected growth of the organization and be flexible enough to manage future technological advancements.
* Reliability: The network design should be reliable and provide high availability to ensure that critical applications and services are always accessible.
* Manageability: The network should be designed with management in mind, including configuration management, device backups, and incident response procedures.
* Cost: The network design should consider the organization's budget and cost constraints, while still meeting the requirements outlined above.

1. Network Topology: Identify the network's physical and logical layout, including the placement of routers, switches, servers, and other network devices. This may involve selecting the appropriate network architecture, such as wired and wireless networks.

* Physical Layout: Define the physical layout of the network, including the location of network devices and cabling infrastructure. This may involve a floor plan or schematic diagram of the building or campus where the network will be deployed.
* Logical Layout: Define the logical layout of the network, including the network hierarchy and how devices will be connected to each other. This may involve a network diagram that shows the relationships between network devices and their IP addresses.
* Network Architecture: Determine the appropriate network architecture for the organization's needs. This may involve selecting between wired and wireless networks, or between different types of wireless technologies such as Wi-Fi, Bluetooth, or Zigbee.
* Redundancy and High Availability: Consider the need for redundancy and high availability in the network design. This may involve deploying redundant network devices and links to minimize downtime and ensure network availability.
* Scalability: Consider the potential for future growth and scalability of the network. This may involve designing the network with expansion in mind and selecting network devices that can accommodate future growth.
* Traffic Segmentation: Consider how traffic will be segmented within the network. This may involve creating separate VLANs for different departments or implementing Quality of Service (QoS) policies to prioritize certain types of traffic.

1. IP Addressing Scheme: Define the IP addressing scheme to be used within the network, including IP ranges, subnets, and allocation of addresses to network devices. This ensures efficient routing and management of network resources.

* When it comes to the IP addressing scheme, you need to determine how IP addresses will be assigned and managed within the network. This includes defining the range of IP addresses to be used and the subnet mask used to identify the network and host portions of the IP address.
* You will need to decide on a private IP addressing scheme that will be used internally within the organization. You may want to consider using RFC 1918 private IP addresses that are reserved for private networks, such as 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.
* You will also need to consider the allocation of IP addresses to network devices, such as servers, printers, and other network infrastructure. This may involve using static IP addresses for critical devices that require a consistent address, while using dynamic IP addresses for other devices that can be assigned an address automatically by a DHCP server.
* By having a well-defined IP addressing scheme, you can ensure efficient routing and management of network resources, as well as enable devices to communicate with each other across the network.

1. Network Segmentation: Determine how the network will be segmented into smaller subnets or virtual LANs (VLANs) to enhance security, optimize network performance, and isolate network traffic. Think about zones of security to separate less secure devices and users from more secure devices and users. Network access control lists to allow/restrict specific types of traffic (see #7) between different networks (external to internal, VLAN to VLAN).

* Determine the network's security requirements: Determine the types of data and applications being used and identify the most critical systems. Identify the users who require access to these systems and data, and those who do not. This will help you determine the zones of security for your network.
* Create VLANs: VLANs allow you to segment your network without having to physically separate it. By creating separate VLANs for different groups of users, you can control which devices are able to communicate with one another, and which traffic is allowed or denied between VLANs.
* Use Access Control Lists (ACLs): ACLs can be used to allow or restrict traffic between different VLANs, or between different networks (external to internal).
* Use Network Address Translation (NAT): NAT allows you to hide the IP addresses of your internal network from the external network. This adds an extra layer of security to your network, making it more difficult for attackers to identify and exploit vulnerable devices.
* Use Firewalls: Firewalls can be used to restrict traffic between different networks, or between different VLANs. They can also be used to monitor traffic and alert you to potential security threats.
* Monitor Network Traffic: Regularly monitor your network traffic to identify any abnormal activity or traffic patterns that could indicate a security breach.
* Use Best Practices for Network Design: Implement best practices for network design to ensure that your network is secure and efficient. This includes using strong passwords, keeping software and firmware up-to-date, and regularly backing up important data.

1. Hardware and Software Requirements: Specify the hardware devices and software applications needed to support the network design, including routers, switches, firewalls, servers, network monitoring tools, and any specialized network equipment. Restrict non-approved services (e.g., cloud, software-as-a-service, etc.) and only allow approved services (policy to prevent “shadow IT”). Only approved devices.

* Specify the hardware devices: Identify the hardware devices required to build the network, such as routers, switches, firewalls, servers, storage devices, and other network appliances. Consider the network topology and the number of devices needed to support the organization's operations. Choose devices that can handle the required bandwidth and traffic loads.
* Specify the software applications: Identify the software applications needed to manage and monitor the network, such as network monitoring tools, configuration management tools, and security management software. Choose software that is compatible with the hardware devices and meets the organization's requirements.
* Restrict non-approved services: Identify services that are not approved for use on the network, such as cloud-based services and software-as-a-service applications. Develop a policy to prevent "shadow IT," which refers to employees using unauthorized software and services that can introduce security risks or compatibility issues. Only allow approved services and applications that meet the organization's requirements.
* Only allow approved devices: Establish a policy for the types of devices that are allowed on the network, such as laptops, desktops, and mobile devices. Specify the operating systems and versions that are supported and ensure that security measures are in place to protect against unauthorized access and malware. Consider using network access control (NAC) to enforce device compliance before granting network access.

1. Security Measures: Outline the security measures to be implemented within the network, such as firewalls, intrusion detection systems (IDS), virtual private networks (VPNs), access controls, and encryption protocols (in-transit), network access control. Monitoring of ingress and egress traffic.

* Firewalls: Firewalls are an essential component of any network security strategy. They help to control access to the network by blocking unauthorized traffic while allowing legitimate traffic to pass through. Firewalls can be hardware-based or software-based and should be configured to restrict traffic based on specific rules and policies.
* Intrusion Detection Systems (IDS): IDS systems are designed to monitor network traffic for signs of potential security threats, such as hacking attempts or malware infections. IDS systems can be used to detect and alert network administrators to potential security threats so they can act to prevent them.
* Virtual Private Networks (VPNs): VPNs provide a secure way to connect remote users or sites to the network. VPNs use encryption to protect data in transit and ensure that only authorized users can access the network.
* Access Controls: Access controls are used to limit access to network resources based on user roles and permissions. Access controls can be implemented at various levels, including the network, application, and data layers.
* Encryption Protocols: Encryption protocols are used to protect data in transit by scrambling the data so that authorized parties can only read it. Common encryption protocols include Transport Layer Security (TLS).
* Network Access Control: Network access control (NAC) is used to ensure that only authorized devices can connect to the network. NAC systems can be used to enforce policies such as requiring up-to-date anti-virus software, enforcing strong passwords, and blocking unauthorized devices.
* Monitoring: Network monitoring is an essential part of network security. Monitoring tools can be used to track network traffic, detect potential security threats, and alert network administrators to potential issues. Ingress and egress traffic should be monitored for signs of malicious activity.

1. Network Services: Identify the required network services, such as DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), email, file sharing, remote access, and any other network services critical to the organization's operations. List and identify only the approved ports, protocols, and services.

* Identifying the required network services is a critical step in the network design plan, as it ensures that the network can support the organization's operations and meets its business requirements. Here are some additional details about this step:
* DHCP (Dynamic Host Configuration Protocol): DHCP is a protocol that allows network administrators to automatically assign IP addresses and other network configuration information to devices on the network. This is an essential service for any network, as it simplifies the process of managing IP addresses and reduces the risk of conflicts or configuration errors.
* DNS (Domain Name System): DNS is a system that translates domain names into IP addresses, allowing users to access websites and other network resources using easy-to-remember names rather than complex IP addresses. DNS is a critical service for any network, and its availability and reliability are essential for maintaining network operations.
* Email: Email is a fundamental service for most organizations, and it requires specialized software and hardware to manage effectively. Email services should be configured to ensure that messages are delivered securely, and that sensitive information is protected.
* File sharing: File sharing allows users to share files and collaborate on projects, making it a critical service for many organizations. However, file sharing must be managed carefully to prevent unauthorized access to sensitive data.
* Remote access: Remote access allows employees to access network resources from outside the organization's physical location. This service requires robust security measures, such as VPNs and two-factor authentication, to protect against unauthorized access.

1. Network Management and Monitoring: Define the processes and tools for network management and monitoring, including network performance monitoring, configuration management, device backups, and incident response procedures.

* Network Performance Monitoring: This involves using network monitoring tools to monitor the performance of the network. The tools can be used to track traffic patterns, identify bottlenecks, and troubleshoot network issues. The information gathered from network monitoring can be used to optimize network performance and improve the user experience.
* Configuration Management: This involves managing the configurations of network devices such as routers, switches, and firewalls. This is important to ensure that the network is functioning correctly and to prevent unauthorized changes to the network. Configuration management involves maintaining accurate documentation of the network devices, their configurations, and any changes made to them.
* Device Backups: Backups are essential to ensure that the network can be quickly restored in case of a failure or disaster. Backups can be performed at regular intervals and should be stored offsite to prevent data loss in case of a physical disaster.
* Incident Response Procedures: Incident response procedures are put in place to ensure that the network is quickly and effectively restored in case of an incident such as a security breach or a failure. The procedures should outline the roles and responsibilities of the different members of the IT team and include detailed steps for addressing incidents.

1. Scalability and Redundancy: Consider the potential growth and scalability of the network, as well as the need for redundancy and failover mechanisms to ensure network availability and minimize downtime. End-of-life/end-of-support must be considered due to risk for scalability and redundancy.

* Scalability: When designing a network, it is important to consider potential growth and scalability. This means ensuring that the network can handle increased traffic and additional devices as the organization grows. To ensure scalability, the network design should be flexible and adaptable, with room for expansion.
* Redundancy: Redundancy refers to the ability of the network to continue operating even if one or more components fail. This can be achieved through redundancy mechanisms such as backup power supplies, redundant network links, and redundant network devices.
* Failover mechanisms: In addition to redundancy, it is also important to have failover mechanisms in place to minimize downtime in the event of a failure. This can include automatic failover to a redundant system, load balancing, and network virtualization.
* End-of-life/end-of-support: When designing a network, it is important to consider the lifecycle of the network components, including hardware and software. Components that are approaching end-of-life or end-of-support can pose a risk to scalability and redundancy, as they may not be able to support new features and may not receive security updates. Therefore, it is important to plan for the replacement of these components as part of the network design.

1. Implementation Plan: Provide a detailed roadmap for deploying the network design, including timelines, tasks, resource allocation, and any dependencies or considerations for integration with existing infrastructure.

Here are some key factors to consider in developing an implementation plan:

* Timeline: Develop a timeline that includes key milestones, deadlines, and deliverables. This timeline should be realistic and achievable and should consider any external factors that may impact the implementation schedule.
* Resource allocation: Identify the resources needed for the implementation, including personnel, hardware, software, and other equipment. Assign roles and responsibilities to team members and ensure that all resources are available when needed.
* Dependencies: Identify any dependencies or constraints that may impact the implementation. These could include hardware or software compatibility issues, procurement delays, or other external factors.
* Integration: Consider how the new network design will integrate with existing infrastructure. This may involve testing and verifying compatibility with existing systems and ensuring that the new network design does not disrupt existing operations.
* Testing: Develop a comprehensive testing plan that includes functional, performance, and security testing. This will help ensure that the new network design meets the requirements and performs as expected.
* Training: Develop a training plan for end-users and IT personnel. This should include training in new equipment, software, and processes. It is essential to ensure that end-users understand how to use the new network and that IT personnel are well-equipped to support and maintain the new network.
* Documentation: Develop documentation to support the implementation, including network diagrams, configuration files, and procedures for maintenance and troubleshooting.
* Monitoring: Develop a plan for monitoring and maintaining the network after implementation. This includes ongoing performance monitoring, incident response procedures, and regular backups.

1. Support Services: Consider internal IT/managed service providers/telecom providers, vendor risk management (e.g., are they meeting security requirements), and service level agreements.

* Support services are a critical component of any network design plan. It is important to consider how the network will be supported and maintained over time, and what resources will be necessary to ensure its continued operation.
* One key consideration is the level of internal IT support that will be needed to maintain the network. This may include dedicated staff for network management, or it may involve contracting with a managed service provider to handle these tasks. It is important to assess the capabilities of the existing IT team and determine whether additional resources are needed to support the new network.
* Another consideration is the involvement of external vendors in the network design and implementation. When working with vendors, it is important to perform a vendor risk assessment to ensure that they are meeting security requirements and have appropriate measures in place to protect sensitive data.
* In addition, service level agreements (SLAs) should be established with any external providers to ensure that they are meeting performance standards and can respond quickly to any issues that may arise. These SLAs should include metrics such as uptime guarantees, response times, and resolution times, and should be reviewed and updated as needed.
* Finally, ongoing monitoring and maintenance of the network should be established, including regular performance monitoring, software and hardware updates, and regular backups to ensure data is protected and recoverable in case of any issues. A clear support and maintenance plan should be established and communicated to all stakeholders to ensure that everyone understands their roles and responsibilities in maintaining the network.

A well-prepared network design plan serves as a guide for network administrators, engineers, and IT teams involved in building, operating, and maintaining the network infrastructure. It helps ensure a consistent and optimized network design that aligns with the organization's requirements, security policies, and future growth plans.