

## Business Case for Cisco SD-WAN

### Executive Summary

In today's digital age, where connectivity and network performance are critical to business success, Cisco Software-Defined Wide Area Network (SD-WAN) offers a transformative solution. This business case outlines the compelling reasons for adopting Cisco SD-WAN within our organization, including improved network performance, enhanced security, reduced costs, and simplified management.

### Problem Statement

Our organization faces several network-related challenges, including:

1. **Network Performance:** Our current Wide Area Network (WAN) infrastructure struggles to provide the required speed, reliability, and performance for our growing digital operations.
2. **Security:** Ensuring the security of data transmission between our remote locations and cloud-based applications is a significant concern.
3. **Cost Inefficiency:** Our existing WAN solutions involve high operating and maintenance costs, including expensive MPLS circuits.
4. **Complex Management:** Managing our current network infrastructure is complex and resource-intensive, making it challenging to adapt to changing business needs.

### Solution: Cisco SD-WAN

#### Key Features of Cisco SD-WAN

Cisco SD-WAN is a leading-edge solution designed to address these challenges and more:

1. **Network Optimization:** Cisco SD-WAN optimizes network performance by dynamically selecting the best path for data traffic, reducing latency and improving the user experience.
2. **Security:** It offers advanced security features, including firewall capabilities, intrusion detection, and encrypted communication to protect data across the WAN.
3. **Cost Savings:** By leveraging multiple connectivity options, including cost-effective internet links, Cisco SD-WAN can significantly reduce our WAN operating costs.
4. **Simplified Management:** The centralized management dashboard and automation capabilities simplify network configuration, monitoring, and troubleshooting.

### Benefits

1. **Improved Network Performance:** Cisco SD-WAN's traffic optimization and path selection ensure that critical applications perform consistently well, even over lower-cost internet connections.
2. **Enhanced Security:** With integrated security features, Cisco SD-WAN provides end-to-end encryption, threat detection, and security policies to safeguard our data.

3. **Cost Efficiency:** By eliminating the need for expensive MPLS circuits and optimizing network traffic, Cisco SD-WAN can lead to substantial cost savings.
4. **Simplified Management:** The centralized management console reduces the complexity of network management and enables faster response to changing business needs.

### Cost Analysis

While the initial investment in Cisco SD-WAN may be significant, the long-term benefits of improved network performance, reduced operating costs, and enhanced security outweigh the upfront expenses. The return on investment (ROI) is achieved through increased productivity, lower operational costs, and the ability to adapt to changing business demands.

### Conclusion

Cisco SD-WAN is the ideal solution to address our network performance, security, cost-efficiency, and management challenges. By adopting Cisco SD-WAN, we can significantly enhance our network capabilities, reduce costs, and improve security. This strategic investment positions our organization for future growth and success in the digital era.

## General SDWAN Knowledge

Software-Defined Wide Area Network (SD-WAN) is a technology that enhances the performance, security, and management of wide area networks (WANs) by leveraging software-driven and centralized control. Below, I'll explain the key components and features of SD-WAN to help customers understand what aspects are relevant to their specific needs:

### \*\*1. SD-WAN Components:

- **Edge Devices:** SD-WAN edge devices are deployed at branch offices, data centers, or remote locations. They play a crucial role in routing traffic, optimizing performance, and ensuring security. These devices are often referred to as SD-WAN appliances or routers.
- **Controller:** The SD-WAN controller is a centralized management platform that provides visibility, orchestration, and policy enforcement across the WAN. It allows administrators to configure and manage network policies, ensuring consistent performance and security.
- **Cloud or Data Center:** Some SD-WAN solutions leverage cloud-based controllers or data centers to centralize network management and provide scalability.

### 2. Key Features of SD-WAN:

- **Centralized Management:** SD-WAN offers a single point of control for network policies and configurations, making it easier to manage and optimize the entire WAN.
- **Dynamic Path Selection:** SD-WAN can intelligently route traffic over multiple network paths, such as MPLS, broadband, or cellular connections, based on real-time performance metrics. This ensures that critical applications receive the best possible network resources.
- **Application Visibility and Prioritization:** SD-WAN solutions can identify and classify applications on the network. Administrators can prioritize critical applications, ensuring they receive the necessary bandwidth and quality of service (QoS) levels.
- **Traffic Optimization:** SD-WAN can optimize traffic by using techniques like data compression, deduplication, and protocol acceleration to improve application performance over limited bandwidth.
- **Security:** SD-WAN solutions often include integrated security features such as firewalls, intrusion detection, and encryption to protect data traffic across the WAN.
- **Zero-Touch Provisioning:** SD-WAN edge devices can be deployed and configured remotely, reducing the need for on-site IT support and simplifying branch office setup.
- **Path Failover and Resilience:** SD-WAN automatically detects network issues and reroutes traffic to available paths, reducing downtime and ensuring business continuity.
- **Analytics and Reporting:** SD-WAN provides detailed visibility into network performance, allowing administrators to analyze trends, troubleshoot issues, and plan for capacity upgrades.

- **Hybrid and Multi-Cloud Support:** SD-WAN can seamlessly connect branch offices to various cloud services, including public and private clouds, SaaS applications, and data centers.
- **Quality of Service (QoS):** SD-WAN allows for granular QoS policies to ensure that critical applications receive the necessary bandwidth and network resources.
- **Cost Optimization:** By using cost-effective internet connections alongside traditional MPLS circuits, SD-WAN can lead to significant cost savings.

### 3. Customization and Requirements:

- Customers should assess their specific network requirements and business goals when considering SD-WAN features. For example, an organization with a distributed workforce may prioritize secure remote access, while another company with latency-sensitive applications might focus on QoS and dynamic path selection.
- Security requirements may vary, so organizations should evaluate whether the SD-WAN solution provides the necessary security features or integrates with existing security solutions.
- Scalability and future growth plans should also be considered. A scalable SD-WAN solution can accommodate additional branch offices, users, and network resources as the organization expands.
- Customers should work closely with SD-WAN vendors and partners to customize their SD-WAN solution to meet their specific needs.

## Cisco SDWAN Knowledge

Cisco Software-Defined Wide Area Networking (SD-WAN) is a solution that simplifies the management and optimization of WAN connections, allowing organizations to connect remote offices and users securely and efficiently. Here's an overview of the major components, including hardware, software, and features of Cisco SD-WAN:

### Hardware Components:

#### 1. Cisco SD-WAN Routers:

- Cisco offers a range of SD-WAN routers, including the Cisco ISR 1000, ISR 4000, and ASR 1000 series routers, which serve as the primary hardware for SD-WAN deployments.

#### 2. Cisco Viptela vEdge Routers:

- These routers, now part of Cisco's SD-WAN portfolio, are purpose-built for SD-WAN deployments and provide connectivity for remote offices and branches.

#### 3. Cisco Catalyst Switches:

- Catalyst switches can be used as network access devices in SD-WAN deployments, providing Ethernet connectivity and Layer 2/Layer 3 functionality.

#### 4. Cisco Cloud Services Platform (CSP):

- Cisco CSP is a hardware appliance designed to host virtual network functions (VNFs) for SD-WAN services in the cloud or at the branch.

### Software Components:

#### 1. Cisco SD-WAN Software:

- Cisco's SD-WAN software includes the operating system and management software that run on SD-WAN routers and devices. It provides the intelligence and control for SD-WAN functionality.

#### 2. vManage:

- vManage is the centralized management and orchestration platform for Cisco SD-WAN. It offers a single pane of glass for provisioning, monitoring, and troubleshooting SD-WAN deployments.

#### 3. vSmart Controllers:

- vSmart controllers are responsible for the control plane in SD-WAN deployments. They enforce routing policies, distribute routes, and manage the SD-WAN overlay network.

#### 4. vBond Orchestrator:

- vBond is the orchestrator component that authenticates and brings SD-WAN devices online. It plays a critical role in the device onboarding process.

## 5. vEdge Cloud Router:

- The vEdge Cloud Router is a software-based router that can run as a virtual instance on x86 hardware. It extends SD-WAN connectivity to cloud-hosted applications and virtual environments.

### Key Features and Functionality:

#### 1. WAN Optimization:

- Cisco SD-WAN includes WAN optimization techniques such as data deduplication, compression, and caching to improve application performance and reduce bandwidth usage.

#### 2. Dynamic Path Selection:

- SD-WAN routers intelligently select the best path for traffic based on real-time network conditions, ensuring optimal application performance.

#### 3. Security Integration:

- Cisco SD-WAN integrates with security services, such as Cisco Umbrella and Cisco Cloud Security, to provide secure access to cloud-hosted applications and protect against threats.

#### 4. Zero Trust Security:

- SD-WAN follows a Zero Trust security model, requiring authentication and encryption for all traffic, even on private networks.

#### 5. Application Visibility and Control:

- SD-WAN provides visibility into application usage and performance, allowing administrators to prioritize critical applications and enforce policies.

#### 6. Centralized Policy Management:

- vManage enables centralized policy creation and enforcement, making it easy to define and manage network and security policies across the entire SD-WAN deployment.

#### 7. Multi-Cloud Connectivity:

- SD-WAN allows organizations to connect to multiple cloud providers and SaaS applications securely and efficiently.

#### 8. WAN Monitoring and Reporting:

- Cisco SD-WAN provides comprehensive monitoring and reporting capabilities to track network performance, identify issues, and analyze traffic patterns.

#### 9. Scalability:

- SD-WAN is scalable to accommodate the needs of small branch offices or large enterprise networks, making it suitable for organizations of all sizes.

#### 10. Application-Aware Routing:

- Cisco SD-WAN routers use application-aware routing to make real-time decisions based on application requirements, ensuring consistent performance.

#### 11. Automatic Failover and Resilience:

- SD-WAN routers support automatic failover to backup links in case of network issues, ensuring high availability.

#### 12. Traffic Segmentation:

- SD-WAN allows for the segmentation of traffic into different classes, making it possible to prioritize mission-critical applications and ensure they receive the required bandwidth.

Cisco SD-WAN's combination of hardware, software, and features provides organizations with a flexible and efficient way to connect remote offices and users while optimizing network performance and enhancing security. It simplifies WAN management and enables better control over application traffic across the network.



## Question-based SDWAN awareness

1. Question: What feature in Cisco SD-WAN allows you to prioritize network traffic based on application requirements?

Feature: Application-aware traffic prioritization

Answer: Cisco SD-WAN uses application-aware QoS to prioritize network traffic based on application requirements.

2. Question: How does Cisco SD-WAN ensure network reliability in case of connectivity issues?

Feature: Automatic failover and dynamic path selection

Answer: Cisco SD-WAN automatically reroutes traffic and dynamically selects the best path to ensure network reliability in case of connectivity issues.

3. Question: Can Cisco SD-WAN seamlessly integrate with cloud-based applications and services?

Feature: Cloud integration for improved application performance

Answer: Yes, Cisco SD-WAN seamlessly integrates with cloud-based applications and services to improve application performance.

4. Question: What feature in Cisco SD-WAN provides a unified management interface for network administrators?

Feature: Centralized management and visibility

Answer: Cisco SD-WAN provides a centralized management interface for network administrators to monitor and control the entire network.

5. Question: How does Cisco SD-WAN protect against security threats and vulnerabilities?

Feature: Security features (encryption, firewall, threat detection)

Answer: Cisco SD-WAN includes security features such as encryption, firewall capabilities, and threat detection to protect against security threats and vulnerabilities.

6. Question: Does Cisco SD-WAN offer optimization for WAN traffic and applications?

Feature: WAN optimization and application acceleration

Answer: Yes, Cisco SD-WAN optimizes WAN traffic and accelerates applications to improve performance and reduce latency.

7. Question: Can Cisco SD-WAN efficiently manage multiple WAN connections and balance traffic across them?

Feature: Support for multiple WAN connections and load balancing

Answer: Cisco SD-WAN can efficiently manage multiple WAN connections and balance traffic across them for improved efficiency and reliability.



8. Question: Does Cisco SD-WAN provide secure connectivity for remote workers and branch offices?

Feature: Secure remote access for remote workers and branch offices

Answer: Yes, Cisco SD-WAN provides secure connectivity for remote workers and branch offices to ensure data privacy and compliance.

9. Question: How does Cisco SD-WAN help with network performance monitoring?

Feature: Analytics and reporting for network performance monitoring

Answer: Cisco SD-WAN offers analytics and reporting tools to monitor network performance and troubleshoot issues.

10. Question: Is Cisco SD-WAN compatible with various types of network transport options?

Feature: Transport flexibility and compatibility with various connectivity options

Answer: Yes, Cisco SD-WAN is compatible with a wide range of network transport options, including MPLS, broadband, and cellular networks.

## Current Network Challenges and Issues Without SD-WAN

### 1. Network Congestion:

- **Problem:** The existing network infrastructure faces constant congestion during peak hours, leading to sluggish application performance.
- **Impact:** Slow response times for critical business applications and frustrated employees.

### 2. Application Prioritization Challenges:

- **Problem:** Without application-aware routing, all network traffic is treated equally, causing bottlenecks for mission-critical applications.
- **Impact:** Critical applications, such as VoIP and video conferencing, suffer from poor quality and interruptions.

### 3. Reliability and Downtime:

- **Problem:** Network reliability is a concern with frequent outages and downtime, disrupting operations.
- **Impact:** Lost revenue, decreased employee productivity, and customer dissatisfaction.

### 4. Inefficient Bandwidth Utilization:

- **Problem:** Inefficient utilization of expensive MPLS circuits leads to high operational costs.
- **Impact:** Rising operational expenses affecting the bottom line.

### 5. Complex Network Management:

- **Problem:** Managing a distributed network with multiple branch offices is challenging and time-consuming.
- **Impact:** Increased IT overhead and potential for misconfigurations and errors.

### 6. Security Vulnerabilities:

- **Problem:** Inadequate security measures leave the network vulnerable to cyber threats and data breaches.
- **Impact:** Potential loss of sensitive data, regulatory non-compliance, and damage to the company's reputation.

### 7. Limited Visibility:

- **Problem:** Lack of real-time network visibility makes it difficult to identify and address issues promptly.
- **Impact:** Extended downtime during troubleshooting, negatively affecting business operations.

### 8. Remote Work Challenges:

- **Problem:** Enabling secure remote access for employees is a cumbersome and insecure process.

- **Impact:** Increased security risks and remote workers struggling with unreliable connections.

#### 9. Scalability Limitations:

- **Problem:** The current network infrastructure is not scalable to support the addition of new branch offices.
- **Impact:** Delays in expanding operations and difficulties accommodating business growth.

**10. Compliance Concerns:** - **Problem:** Inadequate security and limited control over the network raise compliance concerns in highly regulated industries. - **Impact:** Risk of legal repercussions and fines for non-compliance.

In summary, the current network infrastructure faces a range of issues, including performance bottlenecks, reliability concerns, security vulnerabilities, and operational inefficiencies. The implementation of Cisco SD-WAN is poised to address these issues and provide a robust and efficient network solution.

## Statement of Work (SOW) - Cisco SD-WAN Implementation

### Project Overview:

This Statement of Work (SOW) outlines the requirements, scope, and implementation plan for deploying Cisco SD-WAN across 250 sites within ABC Corporation. The project aims to modernize the network infrastructure, enhance performance, and address critical network challenges using Cisco SD-WAN as the core solution.

### Project Objectives:

The primary objectives of this project are as follows:

1. Deploy Cisco SD-WAN to optimize network performance and reliability.
2. Enhance network security measures to protect sensitive data.
3. Simplify network management and troubleshooting processes.
4. Enable secure and efficient remote access for employees.
5. Prepare the network for future scalability and growth using Cisco SD-WAN.

### Project Scope:

#### 1. Cisco SD-WAN Implementation:

- Deploy Cisco SD-WAN appliances and software at all 250 existing sites.
- Configure Cisco SD-WAN devices to establish secure, high-performance connections.

#### 2. Quality of Service (QoS) Implementation:

- Develop and implement QoS policies within Cisco SD-WAN to prioritize critical applications.
- Optimize application performance for real-time data transmission.

#### 3. Security Enhancements:

- Implement end-to-end encryption within Cisco SD-WAN to protect data in transit.
- Configure Cisco SD-WAN's built-in security features, including firewall capabilities and threat detection mechanisms.

#### 4. Remote Work Enablement:

- Utilize Cisco SD-WAN to enable secure remote access for remote employees, ensuring secure connectivity and data protection.

#### 5. Scalability and Expansion:

- Design the Cisco SD-WAN network infrastructure to accommodate future growth and expansion.
- Ensure scalability without compromising network performance.

## 6. Centralized Management:

- Set up a centralized management console provided by Cisco SD-WAN for real-time network monitoring, configuration management, and troubleshooting.

## 7. Training:

- Provide training sessions for network administrators and IT staff on Cisco SD-WAN management and troubleshooting.

## 8. Documentation:

- Document the entire Cisco SD-WAN infrastructure, including configurations, policies, and procedures.

## Cisco SD-WAN Migration and Implementation Plan

### Phase 1: Project Initiation (Week 1-2)

#### 1.1. Project Kickoff:

- Hold a kickoff meeting to ensure all stakeholders are aligned with project objectives and scope.
- Identify the project team and assign roles and responsibilities.

#### 1.2. Requirements Analysis:

- Review the existing network infrastructure documentation.
- Collect specific requirements from business units and stakeholders.
- Determine key performance metrics and objectives.

#### 1.3. Risk Assessment:

- Identify potential risks and challenges related to the migration.
- Develop a risk mitigation strategy.

#### 1.4. Resource Procurement:

- Procure Cisco SD-WAN appliances, licenses, and any required hardware.
- Ensure availability of skilled personnel and third-party vendors if needed.

### Phase 2: Network Assessment and Planning (Week 3-8)

#### 2.1. Current Network Assessment:

- Perform an in-depth assessment of the existing network infrastructure.
- Document network topology, device configurations, and traffic patterns.
- Identify network bottlenecks and performance issues.

#### 2.2. Design and Architecture:

- Develop a detailed design plan for the Cisco SD-WAN deployment.
- Create network diagrams and configurations for each site.
- Define routing policies, QoS settings, and security policies.

#### 2.3. Site Readiness Assessment:

- Evaluate the readiness of each site for Cisco SD-WAN deployment.
- Identify any necessary site-specific changes or upgrades.

### Phase 3: Pre-Deployment (Week 9-12)

#### 3.1. Hardware and Software Preparation:

- Configure and stage Cisco SD-WAN appliances and software.
- Ensure all required licenses are activated.

### 3.2. Test Environment Setup:

- Set up a test environment to validate configurations and policies.
- Conduct thorough testing of Cisco SD-WAN functionalities.

### 3.3. Security Configuration:

- Configure security features, including encryption and firewall rules.
- Establish secure connectivity for remote workers and branch offices.

## Phase 4: Deployment (Week 13-32)

### 4.1. Site Deployment:

- Begin site-by-site deployment of Cisco SD-WAN appliances.
- Install hardware and ensure proper connectivity.
- Apply site-specific configurations and policies.

### 4.2. Configuration Verification:

- Verify that each site is operational and meets design specifications.
- Test failover and redundancy mechanisms.

### 4.3. Performance Tuning:

- Fine-tune QoS settings to optimize application performance.
- Monitor and adjust routing policies as needed.

### 4.4. User Training:

- Provide training to network administrators and IT staff on Cisco SD-WAN management and troubleshooting.

## Phase 5: Post-Deployment (Week 33-36)

### 5.1. Monitoring and Optimization:

- Implement continuous network performance monitoring and reporting using Cisco SD-WAN analytics.
- Continuously optimize configurations based on real-world performance data.

### 5.2. Documentation and Knowledge Transfer:

- Document the entire Cisco SD-WAN infrastructure, including configurations and procedures.



- Conduct knowledge transfer sessions for internal IT teams.

### 5.3. Final Testing and Validation:

- Perform final testing to ensure all sites are fully operational and meeting performance objectives.

### 5.4. Project Closure:

- Conduct a project closure meeting to review project goals and deliverables.
- Archive project documentation and lessons learned.

## Phase 6: Ongoing Maintenance and Support (Ongoing)

### 6.1. Network Operations:

- Implement ongoing support, monitoring, and maintenance as needed.
- Stay current with software updates and security patches.

### 6.2. Performance Optimization:

- Continuously optimize the network for evolving requirements.
- Conduct periodic security audits and updates.

### 6.3. Scalability and Growth:

- Plan for future scalability and accommodate additional sites or network expansion as required.

## Test Cases for Cisco SD-WAN Features

### Feature 1: Application-Aware Routing

**Objective:** To verify that Cisco SD-WAN effectively prioritizes and routes network traffic based on application requirements.

#### Test Steps:

1. Define test environment with Cisco SD-WAN deployed.
2. Identify a set of applications with different priorities (e.g., video conferencing, email, web browsing).
3. Define QoS policies for each application type within Cisco SD-WAN.
4. Generate network traffic for identified applications and measure network performance.
5. Confirm that critical applications receive preferential treatment and optimal performance.
6. Introduce network failures or congestion and verify dynamic rerouting.

### Feature 2: Dynamic Path Selection and Failover

**Objective:** To ensure that Cisco SD-WAN can automatically reroute traffic and maintain network connectivity in case of link failures or congestion.

#### Test Steps:

1. Set up a test environment with multiple network paths and Cisco SD-WAN.
2. Generate network traffic and confirm proper path selection.
3. Simulate link failures and congestion.
4. Verify that Cisco SD-WAN dynamically selects alternative paths.
5. Confirm uninterrupted network connectivity during failures.

### Feature 3: WAN Optimization and Application Acceleration

**Objective:** To test Cisco SD-WAN's ability to optimize WAN traffic and accelerate application performance.

#### Test Steps:

1. Define a test environment with bandwidth limitations.
2. Generate network traffic for applications with high data transfer needs.
3. Measure application performance without Cisco SD-WAN optimization.
4. Enable WAN optimization features and measure performance improvements.
5. Confirm reduced latency and enhanced data transfer speeds.

#### Feature 4: Cloud Integration

**Objective:** To validate Cisco SD-WAN's seamless integration with cloud-based applications and services.

**Test Steps:**

1. Establish connections to cloud-based applications (e.g., Office 365, Salesforce).
2. Generate network traffic for cloud-based applications.
3. Measure application performance and response times.
4. Confirm that Cisco SD-WAN optimizes cloud application traffic.

#### Feature 5: Centralized Management and Visibility

**Objective:** To ensure that the centralized management interface provides efficient network monitoring and control.

**Test Steps:**

1. Access the centralized management console.
2. Monitor network performance and device status.
3. Modify network configurations from the centralized interface.
4. Confirm real-time visibility and control over the network.

#### Feature 6: Security Enhancements

**Objective:** To verify that Cisco SD-WAN provides robust security measures, including encryption, firewall, and threat detection.

**Test Steps:**

1. Configure security policies within Cisco SD-WAN.
2. Generate network traffic with security testing tools.
3. Verify that Cisco SD-WAN enforces security policies.
4. Monitor for any intrusion attempts or security breaches.

#### Feature 7: Support for Multiple WAN Connections and Load Balancing

**Objective:** To test Cisco SD-WAN's ability to efficiently manage multiple WAN connections and balance traffic.

**Test Steps:**

1. Set up multiple WAN connections (e.g., MPLS, broadband, cellular).
2. Generate network traffic and measure load balancing effectiveness.
3. Confirm that traffic is evenly distributed across WAN connections.

4. Introduce network failures and verify failover and load balancing.

## SD-WAN Implementation sample questions and answers

### 1. Business Objectives and Requirements:

- What are the primary business objectives for implementing Cisco SD-WAN?
- Are there specific requirements related to network performance, reliability, or application availability?

### 2. Network Assessment:

- Have you conducted a thorough assessment of your existing network infrastructure?
- What are the key performance bottlenecks or issues in your current WAN?

### 3. Site Locations and Topology:

- How many branch offices or remote sites need to be connected to the SD-WAN?
- What is the geographical distribution of these sites?
- Do you have data centers that need to be integrated into the SD-WAN?

### 4. Bandwidth Requirements:

- What are the bandwidth requirements for each branch or site?
- Are there variations in bandwidth needs for different applications or user groups?

### 5. Application Prioritization:

- Do you have critical applications that require prioritization over the network?
- How do you plan to prioritize and optimize application traffic?

### 6. Redundancy and High Availability:

- What level of redundancy and high availability is required for your SD-WAN solution?
- Are you planning for dual WAN connections at each site?

### 7. Security and Compliance:

- What security measures and compliance requirements need to be addressed within the SD-WAN architecture?
- How will you handle encryption and data protection for traffic between sites?

### 8. Integration with Existing Infrastructure:

- Are there existing routers, firewalls, or other networking components that need to be integrated into the SD-WAN solution?
- Do you plan to retain any part of your current network infrastructure?

## 9. Cloud Integration:

- Do you have applications hosted in cloud environments (e.g., AWS, Azure, Google Cloud) that need to be accessed via the SD-WAN?
- How will the SD-WAN solution integrate with your cloud strategy?

**10. Vendor Selection:** - Have you chosen Cisco as your SD-WAN vendor, or are you considering multiple vendors for evaluation? - What criteria are you using to evaluate SD-WAN vendors?

**11. Deployment Models:** - Are you planning for a full SD-WAN overlay or a hybrid approach with existing MPLS circuits? - How do you envision the SD-WAN architecture (Hub and Spoke, Full-Mesh, etc.)?

**12. Network Monitoring and Management:** - What tools and solutions do you plan to use for monitoring and managing the SD-WAN environment? - How will you ensure network visibility and troubleshooting capabilities?

**13. Quality of Service (QoS):** - What QoS policies are needed to ensure the performance of critical applications? - How will you define and enforce QoS policies across the SD-WAN?

**14. Deployment Timeline and Phases:** - Do you have a specific timeline for deploying SD-WAN across all sites? - Are you planning to deploy in phases, starting with specific sites or regions?

**15. Training and Skills:** - Have you identified the need for training your IT staff on SD-WAN management and troubleshooting? - How will you ensure your team has the necessary skills for SD-WAN operation?

**16. Budget and Cost Considerations:** - Have you established a budget for the SD-WAN project, including hardware, software, and ongoing operational costs? - Are you exploring cost-saving opportunities through SD-WAN deployment?

**17. Vendor Support and SLAs:** - What level of support and service level agreements (SLAs) are you expecting from Cisco or your chosen SD-WAN vendor? - How will support and maintenance be handled?

**18. Disaster Recovery and Business Continuity:** - What measures are in place to ensure business continuity and data recovery in case of network failures or disasters? - Have you considered redundancy and failover mechanisms?

**19. User Experience and Feedback:** - How will you gather feedback from end-users to ensure that the SD-WAN implementation meets their expectations? - Do you have plans for ongoing user satisfaction monitoring?

**20. Project Governance:** - What project management and governance structure will be in place to oversee the SD-WAN implementation from start to finish? - Who are the key stakeholders involved in decision-making?

## Sample Answers

### 1. Business Objectives and Requirements:

- Our primary business objective is to enhance network performance and reliability while reducing costs. We aim to achieve better application availability and optimize the use of WAN resources.

### 2. Network Assessment:

- Yes, we have conducted a comprehensive assessment of our existing network infrastructure. We have identified areas of congestion, latency, and performance bottlenecks.

### 3. Site Locations and Topology:

- We have 50 branch offices across the country that need to be connected to the SD-WAN. Our sites are geographically distributed, and we have two data centers.

### 4. Bandwidth Requirements:

- Bandwidth requirements vary across our sites. Some require high bandwidth for data-intensive applications, while others need lower bandwidth for basic operations.

### 5. Application Prioritization:

- We have critical applications like VoIP and video conferencing that require prioritization. We plan to use Quality of Service (QoS) to achieve this.

### 6. Redundancy and High Availability:

- We require a high level of redundancy and availability. Each branch will have dual WAN connections for failover.

### 7. Security and Compliance:

- Security is a top priority. We need encryption for all traffic between sites and compliance with industry-specific regulations.

### 8. Integration with Existing Infrastructure:

- We have existing routers and firewalls that we plan to integrate into the SD-WAN solution. We want to leverage our current investments.

### 9. Cloud Integration:

- Yes, we have applications hosted in AWS and Azure. We need seamless integration with these cloud environments.

**10. Vendor Selection:** - We are evaluating multiple SD-WAN vendors, including Cisco, based on criteria such as performance, scalability, and ease of management.



**11. Deployment Models:** - We plan to deploy a full SD-WAN overlay across all sites while gradually phasing out our existing MPLS circuits.

**12. Network Monitoring and Management:** - We will use Cisco's SD-WAN vManage for monitoring and management, ensuring visibility into network performance.

**13. Quality of Service (QoS):** - We will define QoS policies to prioritize critical applications and ensure optimal performance.

**14. Deployment Timeline and Phases:** - Our timeline is to complete the deployment within 12 months, starting with a pilot phase at select branches.

**15. Training and Skills:** - We have identified the need for training our IT staff on SD-WAN management. Cisco will provide training and certification programs.

**16. Budget and Cost Considerations:** - Our budget includes hardware, software licensing, professional services, and ongoing operational costs. We aim to achieve cost savings through SD-WAN.

**17. Vendor Support and SLAs:** - We expect 24/7 support from Cisco with defined SLAs for incident response and issue resolution.

**18. Disaster Recovery and Business Continuity:** - We have implemented redundancy and failover mechanisms to ensure business continuity and data recovery in case of network failures.

**19. User Experience and Feedback:** - We plan to gather user feedback through surveys and monitoring tools to continually improve the user experience.

**20. Project Governance:** - We have established a dedicated project management team to oversee the implementation, and key stakeholders from IT and business units are involved in decision-making.