Sify Digital Services Ltd.

SD-WAN Product Requirement Document

Contents

[1 Executive Summary 2](#_Toc154767853)

[1.1 Overview 2](#_Toc154767854)

[2 Objectives 2](#_Toc154767855)

[2.1 Service Objectives 2](#_Toc154767856)

[3 Purpose, Scope & Stakeholders 3](#_Toc154767857)

[3.1 Business Drivers for the Product: 3](#_Toc154767858)

[3.2 Critical Success Factors: 3](#_Toc154767859)

[4 Features and Functionality 4](#_Toc154767860)

[5 Technical Specifications 4](#_Toc154767861)

[5.1 Platform Support 4](#_Toc154767862)

[5.2 Integration 4](#_Toc154767863)

[5.3 Scalability 4](#_Toc154767864)

[5.4 Performance 5](#_Toc154767865)

[6 Sify Deliverables 5](#_Toc154767866)

[7 Ordering & Billing 6](#_Toc154767867)

[8 CPQ Related Information 6](#_Toc154767868)

[8.1 Order Login Data for GUI 6](#_Toc154767869)

[8.2 Configuration options 7](#_Toc154767870)

[9 Terms and Conditions 8](#_Toc154767871)

[10 SLA 9](#_Toc154767872)

[10.1 Delivery SLA 9](#_Toc154767873)

[10.2 Operation SLA 9](#_Toc154767874)

[11 User Experience 9](#_Toc154767875)

[11.1 User Training and Documentation 9](#_Toc154767876)

[12 Regulatory and Compliance Considerations 10](#_Toc154767877)

[13 Timeline and Milestones 10](#_Toc154767878)

[13.1 Development Timeline 11](#_Toc154767879)

[14 Risks and Mitigation Strategies 11](#_Toc154767880)

[14.1 Potential Risks 11](#_Toc154767881)

[14.2 Mitigation Strategies 11](#_Toc154767882)

[15 Stakeholder Approval 11](#_Toc154767883)

[15.1 Review and Approval 11](#_Toc154767884)

[16 Appendices 12](#_Toc154767885)

[16.1 Glossary 12](#_Toc154767886)

# Executive Summary

## Overview

As enterprises transform their business processes to embrace greater digitization, cloud and mobility are combining to rapidly shift the application and data traffic profile within the enterprise. More enterprise applications are being delivered from the cloud, and more enterprise users are mobile and require anytime/anywhere access to applications. The network delivering application data to users must evolve. In distributed enterprises, such as those with several branches and remote workers, it is the wide area network (WAN) that requires an urgent transformation.

WAN transformation for a distributed Enterprise needs to address a diverse set of connection types, dispersed locations with different bandwidth needs, and the need to access applications both within the network and through the cloud. At the same time WAN transformation needs to look at simplifying networks, enhancing control, improving performance, visibility and driving efficiency.

Software-defined wide area network (SD-WAN) provides a solution to the WAN transformation.

SD-WAN solution promises the enablement of:

* Optimization of modern application delivery costs through the WAN in the face of future application traffic profile change and growth
* Greater flexibility and efficiency of network transport via cost-effective alignment of network connectivity options and bandwidth with application criticality
* Improved branch IT agility and efficiency through automated and agile service provisioning and reduced complexity
* Better customer engagement By enhancing cloud application reliability, availability, performance, and security
* Secure data traffic for all applications especially those hosted in the cloud

Sify’s SD-WAN service provides risk free WAN transformation service for Enterprises by offering

* A Hosted service to ease the costs of adoption.
* Experts guided Network deployment and migration.
* Orchestrating the network to meet the desired objectives of application performance.
* Transport services that enable a true Hybrid network.
* Better performance to the cloud hosted applications
* Comprehensive network management and monitoring.
* Service backed by comprehensive SLAs
* Leverage all Strategic and technical benefits that come from using Managed SD-WAN

# Objectives

## Service Objectives

|  |
| --- |
| **Description** |
| Improve network efficiency by utilizing multiple connections simultaneously, reducing latency, and optimizing bandwidth usage. |
| Ensure high network availability and reliability by utilizing multiple paths, minimizing downtime, and automatically rerouting traffic in case of link failures. |
| Prioritize and route traffic based on application requirements, ensuring critical applications receive the necessary bandwidth and performance. |
| Optimize resource utilization, reduce reliance on expensive dedicated lines, and leverage cost-effective internet connections, leading to overall cost savings. |
| Enhance end-user experience by providing consistent and reliable access to applications and services, regardless of the user's location or network conditions. |
| Enable centralized control and management of the entire network through a unified interface, simplifying configuration, monitoring, and troubleshooting. |
| Implement advanced security features, such as encryption, firewalls, and intrusion detection, to safeguard data and ensure secure communication across the network. |
| Easily scale the network infrastructure to accommodate growing business needs and adapt to changing network requirements without significant disruptions. |
| Facilitate seamless integration with cloud-based applications and services, ensuring efficient and secure connectivity to resources hosted in public or private clouds. |
| Leverage the capabilities of multiple WAN links efficiently, distributing traffic intelligently to maximize performance and reliability for various applications. |
| Provide comprehensive real-time monitoring and analytics tools to track network performance, identify issues promptly, and make data-driven decisions for optimization. |
| Enforce corporate policies, compliance standards, and regulatory requirements consistently across the network, ensuring a secure and compliant operating environment. |
| Enable quick and efficient deployment of SD-WAN solutions, allowing organizations to adapt rapidly to changing network needs and business requirements. |

# Purpose, Scope & Stakeholders

Sify SD-WAN services should evaluate different SD-WAN OEM architecture and offer a wide variety of deployment option to the customer such as Cloud-based, On-premises or Hybrid. The offering should help customers optimize their network performance with SD-WAN by enhancing application performance and leveraging SD-WAN for intelligent traffic routing and dynamic path selection. The SD-WAN offering should integrate with cloud platforms such as AWS, Azure, Google Cloud, etc. The end customers should be able to address their security challenges with SD-WAN deployments with features such as threat detection, intrusion prevention and securing edge devices. The offering should be a Make in India product and the OEM should qualify as Local Content Class 1 supplier as per Govt of India Instructions for Make in India. The SD-WAN product should be a cost-effective solution which can be easily bundled with Sify connectivity offerings & have dynamic traffic steering and failover capabilities, which enhances network performance, delivering a seamless user experience for critical applications.

Sify’s scope would be to manage customer’s WAN infrastructure end to end. This would be further covered in the Deliverables section. Key stakeholders involved in the creation of this product include the OEM, as well as Sify Product, Engineering, Commercial, Service Delivery, Service Support & Infrastructure Services teams.

## Business Drivers for the Product:

|  |
| --- |
| **Business Drivers** |
| New Revenue streams - Converting un-managed customers to managed customers. |
| Value-add on top of connectivity offerings - Revenue retention of Sify’s network services. |
| Differentiation and Competitive Advantage. |
| Enhance market share by enabling customers to be SD-WAN ready or SD-WAN enabled. |
| Improved Customer Experience. |
| Reduced Operational Costs and Faster Time-to-Market. |
| GoI’s push for Make in India. |

## Critical Success Factors:

|  |
| --- |
| **Critical Success Factors** |
| SD-WAN Network architecture as per customer business objectives. |
| Vendor selection and evaluation. |
| High reliability with low failure rate. |
| Customizable hardware platform which can suit multiple customer scenarios. |
| Attractive price points with lower overall TCO. |
| Capability of zero touch provisioning and centralized management. |
| Enhanced Security and Compliance considerations. |
| Monitoring and Performance Management |

# Features and Functionality

These unique technical features are collectively required to address the complex requirements of modern networking environments.

|  |  |
| --- | --- |
| **Technical Feature** | **Description** |
| **WAN Link Load Balancing** | Distributes network traffic across multiple WAN links, optimizing bandwidth utilization and ensuring efficient use of available resources. |
| **Dynamic Path Control** | Monitors the performance of individual network paths in real-time and dynamically selects the best path for each application's traffic based on factors such as latency, jitter, and packet loss. |
| **Intelligent Traffic Steering** | Prioritizes critical applications by steering traffic over the most suitable paths, ensuring optimal performance and responsiveness for key business applications. |
| **Centralized Management and Orchestration** | Provides a centralized management platform for configuring, monitoring, and managing the entire network infrastructure. This simplifies network operations, reduces complexity, and enables policy-based orchestration of network resources. |
| **Zero-Touch Provisioning (ZTP)** | Supports zero-touch provisioning, allowing new branch sites or remote locations to be quickly and automatically provisioned without the need for manual configuration. |
| **WAN Optimization** | Features such as data deduplication, compression, and caching to reduce bandwidth consumption and improve application performance over wide area networks. |
| **Security Integration** | Integrates advanced security features to protect the network against cyber threats and vulnerabilities. This includes encryption, authentication, access controls, firewalling, intrusion prevention, and threat intelligence capabilities to safeguard sensitive data and applications. |
| **Cloud Connectivity** | Optimized connectivity to cloud services by enabling direct access to cloud applications and resources. This eliminates the need for backhauling traffic through data centers, reducing latency and improving performance for cloud-based applications. |
| **Quality of Service (QoS) Policies** | Allows administrators to define granular QoS policies based on application priorities, user profiles, and business requirements. |
| **Analytics and Reporting** | Built-in analytics and reporting capabilities to monitor network performance, track application usage, and analyze traffic patterns. This provides valuable insights into network behavior and performance trends, enabling proactive troubleshooting and optimization. |
| **Scalability and Flexibility** | Highly scalable and flexible architecture, allowing organizations to easily add new sites, users, and applications as their network requirements evolve. |
| **Failover and Redundancy** | Provides automatic failover and redundancy capabilities to ensure continuous connectivity in the event of a network link failure or degradation. |

# Technical Specifications

## Platform Support

|  |
| --- |
| **Platforms to Support** |
| Dedicated physical devices designed for SD-WAN deployment. |
| Software-based instances that can be deployed in virtualized environments. |
| Support for integration with various cloud platforms. |
| Capabilities to integrate with on-premises data center solutions. |
|  |

## Integration

|  |
| --- |
| **Integration** |
| Integration with various cloud platforms and services. |
| Compatibility with third-party security solutions for enhanced threat protection. |
| Integration with network monitoring and analytics tools for real-time visibility. |
| Compatibility with on-premises data center solutions for seamless integration. |
| Integration with WAN optimization tools for enhanced performance. |
| Support for integration with network management and orchestration platforms. |

## 

## Scalability

|  |
| --- |
| **Scaling Considerations** |
| Scalability in terms of supporting a growing number of branch offices, remote sites, or locations. |
| The ability to scale the SD-WAN solution to accommodate an increasing number of users and connected devices. |
| Scalability in handling higher volumes of network traffic as the organization grows. |
| The capability to efficiently manage a diverse set of applications and services over the network. |
| Scalability in connecting to and supporting a growing number of cloud services and applications. |
| The ability to easily expand available bandwidth to meet the increasing demands of the organization. |
| Scalability in integrating with existing network infrastructure, including legacy systems and technologies. |

## Performance

The managed SD-WAN product must deliver reliable, efficient, and secure internet connectivity for users across various scenarios and locations.

|  |
| --- |
| **Performance Metric** |
| Throughput |
| Latency |
| Jitter |
| Packet Loss |
| Link Utilization |
| Application Performance |
| Quality of Service (QoS) |
| Failover Time |
| Security Performance |
| Bandwidth Optimization |
| Real-time Monitoring and Analytics |

# Sify Deliverables

|  |  |
| --- | --- |
| **Requirement** | **Description** |
| Service portal | Portal to customer, able to view, configure, monitor WAN network performance of Sify and other providers |
| Capacity management | Measure WAN link utilization trends, create baselines and recommend customer on the actions taken – upgrade, downgrade |
| Transition and implementation services | Site survey, CRD, HLD and LLD. Deploy initial CPE devices across all sites. Perform MACD as and when changes required [bandwidth upgrade/downgrade, new features] |
| Proactive network monitoring | 24x7 Monitoring of network related faults and performance management. Able to view these alerts on self-service portal |
| Application visibility | Identify applications and sub-applications, report the performance of applications |
| Incident reporting and management | Trouble ticketing for all network related issues including other SP links. Detection of alerts from fault and performance management systems |
| Problem management | Diagnose, identify and isolate issues. Work on fix and workarounds with providers and SD-WAN vendors |
| Configuration management | Configuration of managed CPE devices, auditing, backup of configuration, template-based config |
| Inventory management | Manages inventory of CPE devices, resources – IP address, VLAN etc. |
| Vendor management | Co-ordinate with vendors for issue reporting and resolution, faulty hardware management, recommended best practices |
| Change management | Scheduled network changes – changing software based on EOL, proactive identification of network issues and resolution, MACD of WAN links and bandwidth |
| Service desk | 24x7 technical support team to co-ordinate with customer for issue reporting and resolution |
| Hardware replacement time | Replacement of faulty hardware and components |
| Support systems | IAM, NTP, OOB management systems |
| Root cause analysis | Analysis of issues and identify root causes – including CPE and provider links |

# Ordering & Billing

|  |
| --- |
| Billing T&C |
| OT: One Time, 100% within 30 days of invoicing to the customer. |
| RC1 Option: Quarterly in Advance, within 30 days of invoicing to the customer. |
| RC2 Option: Yearly in Advance, within 30 days of invoicing to the customer. |

# CPQ Related Information

## Order Login Data for GUI

Key configuration information will be:

1. Managed SDWAN Service and SDWAN Build offerings from XXX as defined OEM Platforms

|  |
| --- |
| P1 – XXX  P2 – YYY  P3 – ZZZ  P4 – AAA  P5 – BBB |

1. Payment Terms agreed with the customer.
   1. OTC – One-time and upfront within 30 days of invoicing
   2. Recurring Charges – Quarterly/Annually in Advance within 30 days of invoicing
2. Characteristics (attributes) of the product that may alter the price

|  |  |  |
| --- | --- | --- |
| **#** | **Attributes** | **Details** |
| 1 | Order Type | <New/Upgrade/Shift> |
| 2 | Contract Term (in years) | <As per PO> |
| 3 | Office Type | <Controller/Branch> |
| 4 | Platform Type | <P5> |
| 5 | Hardware/License Vendor | <OEM> |
| 6 | Device Owner | <Sify/Customer> |
| 7 | Deployment Type | <HA/Standard> |
| 8 | Feature Tier | <As per PO> |
| 9 | Device Type | <As per PO> |
| 10 | Throughput License | <As per PO> |
| 11 | ARC – Managed Services | <As per PO> |
| 12 | ARC – Others | <As per PO> |
| 13 | OTC – Implementation | <As per PO> |
| 14 | OTC – Professional Services | <As per PO> |
| 15 | OTC – Hardware | <As per PO> |
| 16 | OTC – Licence | <As per PO> |
| 17 | OTC – AMC | <As per PO> |

1. Product information (attributes) that is agreed with customer which will be delivered by Sify
2. Identify attributes that need to be printed in proposal
3. Validations on attributes or price

## Configuration options

# Terms and Conditions

1. All pricing provided are exclusive of applicable taxes.
2. PO should be in name of SDSL, Chennai.
3. The contract period will be for 3 years or 5 years (applicable as per the PO).
4. The project delivery timelines will be 12 - 14 weeks from the date of Sify’s acceptance of a customer PO. Any delays caused due to Customer premises or infrastructure not being ready will result in extension of delivery timelines.
5. Additional Charges are applicable for any additional cabling requirements.
6. Any physical hardware damage caused by customer will incur hardware charges for replacement of faulty hardware (OTC). Customer must provide UPS Power and earthing for the SD-WAN devices.
7. Early Termination charges are applicable for any services terminated within the contract period.
   1. In the event of performance degradation in Sify’s scope of work, which is brought to the notice of Sify in writing, Sify shall use all means available to rectify the same immediately and communicate to the customer on the action taken.
   2. If the performance degradation is not rectified within one month (1 month) from the time Sify acknowledges the customer complaint in writing/mail and if this performance degradation is repeated for the same site / network element for 3 consecutive times within a calendar quarter after Sify has taken necessary corrective measures, Customer has the option of terminating the contract with 1 month notice period for the affected site / network element.
   3. If the Customer chooses to terminate the entire contract for convenience or any other reason other than performance degradation of the service, the customer is liable to pay the annual recurring charges for the remaining period of the contract on a pro-rata basis. These charges will pertain to any Hardware and/or Software Licenses that have been specifically deployed for the use of the customer.
8. Any requirement of changing the SD-WAN feature tier will result in associated change of commercials.
9. Any changes to the Solution design and configuration will result in the design change along with the revised commercials.
10. Cancellation or reschedule of site visits (for international locations) within 48 hours’ notice will incur additional charges.
11. The provisioning/commissioning of any unmanaged or managed network security services (apart from anything included within SD-WAN Solution) is considered out of scope.
12. All Payment will be as per Sify's payment terms and conditions.
13. 24\*7 proactive monitoring and management of the network as defined in the solution document is included.
14. The customer will sign a scope of work document along with the PO and that will be considered as the reference for sign off on delivery of the project. Any scope not explicitly mentioned in the SOW will be considered out of scope of the project.
15. Only one site visit is factored for all on-site deployments and implementation for international locations, any additional site visits required will incur additional charges.
16. Installation SOW - basic rack & stack, uploading IOS/config file.
17. For International locations, Field Engineering services are factored for during business hours (9 AM - 5.00 PM Local Time Business Days). Out of business hours and Weekends and holidays will incur additional charges.
18. All Internal Cabling needs to be completed within 5 business days from the date of Service Readiness communicated by Sify. Failure to comply with the timeline will lead to the initiation of the billing for the SD-WAN service automatically from the Sixth day.”

# SLA

Sify’s service offerings are SLA-driven and offer a good value proposition to corporations seeking to improve the return on their IT investments.

Network SLA

Uptime: > 99.50%

## Delivery SLA

The project delivery timelines will be 12 - 14 weeks from the date of Sify’s acceptance of a customer PO. Any delays caused due to Customer premises or infrastructure not being ready will result in extension of delivery timelines.

## Operation SLA

**Incident Management**

|  |  |
| --- | --- |
| **SLA Attributes** | **SLA Indicators** |
| Incident Notification | Severity 1 - 15 mins  Severity 2 - 30 mins  Severity 3 – Online |
| Incident Response | Severity 1 - 15 mins  Severity 2 - 30 mins  Severity 3 – 120 mins |
| Incident / Problem Resolution | Severity 1 – 4 Hours  Severity 2 – 8 hours  Severity 3 – 24 hours |
| Sify GNOC Availability | >99.90% |
| Sify Service Portal Availability | >99.50% |

**Note:** \* From the time of call / trouble ticket logged on to Sify’s portal

**Change Management**

|  |  |
| --- | --- |
| **SLA Attributes** | **SLA Indicators** |
| Any changes to the network / SD-WAN setup | Customer will be informed 24 hours in advance or Customer must make a request 24 hours in advance of the changes to be executed (does not include hardware replacements) |
| Change Resolution | Severity 1 – 4 hours  Severity 2 – 8 hours  Severity 3 – 48 hours |

# User Experience

## User Training and Documentation

|  |  |
| --- | --- |
| **Component** | **Description** |
| Certification Programs | - Enrolling Engineering, Solutions, BD & Sales for certification programs. |
| Documentation | - Tiered & focused training decks to be created for different roles of stakeholders. |
| Regular Updates | - Keep training materials and documentation up to date with product releases. |
| Training Schedule | - Plan training sessions for different roles of stakeholders.  - Provide recordings for on-demand access. |
| Integration with LMS | - Integrate training modules with existing Learning Management System. |

# 

# Regulatory and Compliance Considerations

|  |  |
| --- | --- |
| **Regulatory & Compliance Considerations** | **Description** |
| Data Protection Laws | Adhere to India's data protection laws, including the Personal Data Protection Bill, ensuring the secure processing and storage of personal and sensitive information within the office-in-a-box product. |
| Cybersecurity Regulations | Comply with cybersecurity regulations and standards issued by the government or regulatory bodies. Implement robust cybersecurity measures to protect the office-in-a-box product from cyber threats and attacks. |
| IT Act, 2000 and Amendments | Align with the Information Technology Act, 2000, and its subsequent amendments. Ensure legal compliance with provisions related to electronic signatures, data protection, and electronic records. |
| Telecom Regulatory Authority of India (TRAI) Guidelines | Comply with TRAI guidelines, especially if the office-in-a-box product involves telecommunications services. Ensure adherence to regulations related to telecommunication and consumer protection. |
| Goods and Services Tax (GST) Compliance | Ensure compliance with GST regulations for invoicing and taxation if the office-in-a-box product involves the sale of goods or services. Adhere to GST guidelines and maintain accurate records for tax purposes. |
| Intellectual Property Rights (IPR) | Respect intellectual property rights, including patents, copyrights, and trademarks. Avoid unauthorized use of third-party intellectual property within the office-in-a-box product to prevent legal complications. |
| Local and State Regulations | Stay informed about local and state-specific regulations that may impact the operation of the office-in-a-box product. Comply with licensing requirements and other regional regulations applicable to the business. |
| Health and Safety Regulations | If applicable, adhere to health and safety regulations, especially if the office-in-a-box product involves physical components or equipment. Ensure a safe working environment for users. |
| Environmental Compliance | Consider environmental regulations and implement eco-friendly practices if the office-in-a-box product involves hardware components. Adhere to waste disposal guidelines and minimize environmental impact. |

# Timeline and Milestones

## Development Timeline

|  |  |
| --- | --- |
| **Milestones** | **Timeline** |
| Product Requirement Document | TBD |
| Internal Deck | TBD |
| Customer Facing Deck | TBD |
| Proposal Format | TBD |
| Price Book | TBD |
| Onboarding on CPQ | TBD |

# Risks and Mitigation Strategies

## Potential Risks

|  |  |  |
| --- | --- | --- |
| **Risk Category** | **Potential Risks** | **Impact** |
| Regulatory Risks | - Non-compliance with data protection regulations. | - Legal penalties and reputational damage. |
| - Data localization requirements. | - Impact on cross-border data transfers. |
| Project Management | - Scope creep and changing requirements. | - Delays, increased costs, and resource strain. |
| - Untrained or poorly trained implementation/ support resources | - Deadline overruns, service outages and penalties |
| Vendor/Partner Risks | - Dependence on a single OEM for product delivery. | - Delays and potential disruptions. |
| Adoption Risks | - Resistance to adoption of the product among end-users. | - Poor adoption rates and underutilization. |

## Mitigation Strategies

|  |  |  |
| --- | --- | --- |
| **Risk Category** | **Potential Risks** | **Mitigation Strategies** |
| Regulatory Risks | - Non-compliance with data protection regulations. | - Stay informed about relevant regulations and ensure compliance. |
| - Data localization requirements. | - Implement data localization strategies and legal compliance. |
| Project Management | - Scope creep and changing requirements. | - Establish a robust change control process and communicate changes. |
| - Untrained or poorly trained implementation/ support resources | - Ensure availability of trained resources for each project. |
| Vendor/Partner Risks | - Dependence on a single OEM for product delivery. | - Maintain constant communication with OEM on product lifecycle. |
| Adoption Risks | - Resistance to adoption of the product among end-users. | - Conduct user training programs and create awareness campaigns. |

# Stakeholder Approval

## Review and Approval

|  |  |
| --- | --- |
| Document Owners | Suresh Gummaraju |
| Saurabh Kumar Acharya |
| Approved By | Pranesh Babu Khyatasandra |
| Ramakrishna Kotha |
| Anuj Malhotra |
| Joseph Abraham |
| Mohan Raj S |
| Hari Hara Moorthy |
| Suresh Gummaraju |

# Appendices

## Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Quality of Service (QoS) | A set of techniques used to manage network resources, prioritize certain types of traffic, and ensure a consistent level of service for critical applications. |
| Regulatory Compliance | Adherence to laws, regulations, and industry standards related to data protection, privacy, and other relevant requirements. |
| Cyber Threats | Malicious activities and attacks aimed at exploiting vulnerabilities in computer systems, networks, and data. |
| Centralized Management | The ability to monitor, configure, and control network devices from a central location, providing efficiency and ease of administration. |
| Scalability | The capability of a system or network to handle increased demand by adding resources or adapting to accommodate a growing user base. |
| Reliability | The ability of a system or network to consistently perform its intended functions without failures or interruptions. |
| Analytics and Reporting | Tools and capabilities for collecting and analyzing data, generating reports, and gaining insights into network performance and user behavior. |
| Compliance Adherence | Conforming to established rules, regulations, and standards relevant to a specific industry or jurisdiction. |
| Digital Transformation | The integration of digital technologies into various aspects of business operations, often leading to fundamental changes in how businesses operate and deliver value. |
| IoT (Internet of Things) | The network of interconnected devices and objects that can communicate and exchange data, contributing to automation and smart functionality. |
| Remote Work | Work conducted away from a traditional office environment, often facilitated by digital technologies and connectivity. |
| Mesh Networking | A network topology where each node (device) is connected to multiple other nodes, forming a flexible and resilient communication infrastructure. |
| Managed Service Provider (MSP) | An organization or company that provides managed services, such as managed SD-WAN, to clients, often on a subscription or contractual basis. |
| 5G Technology | The fifth generation of cellular technology, offering increased data transfer speeds, lower latency, and improved connectivity for mobile devices. |

Top of Form