Sify Managed WAN Services Proposal

Submitted To: <Customer Name>

Sify Technologies Ltd.

Contents

[Document History 4](#_Toc168669704)

[Sign-Off 4](#_Toc168669705)

[Document Title 4](#_Toc168669706)

[Preparation 4](#_Toc168669707)

[Release 4](#_Toc168669708)

[Distribution List 4](#_Toc168669709)

[Statement of Confidentiality 4](#_Toc168669710)

[Executive Summary 5](#_Toc168669711)

[About <CUSTOMER NAME> 5](#_Toc168669712)

[About Sify Technologies Ltd. 5](#_Toc168669713)

[Business Units 5](#_Toc168669714)

[Managed Network Services Portfolio 6](#_Toc168669715)

[Scale of Operations 6](#_Toc168669716)

[What does Sify bring to the table? 6](#_Toc168669717)

[Sify Managed Network Services 8](#_Toc168669718)

[Service Description 8](#_Toc168669719)

[Managed WAN Services (MWAN) 9](#_Toc168669720)

[Managed Customer Premise Equipment (MCPE) 10](#_Toc168669721)

[Sify MCPE on Other ISP Link 10](#_Toc168669722)

[MCPE Deployment Stages 11](#_Toc168669723)

[Managed Customer Owned Equipment (MCOE) 12](#_Toc168669724)

[Manpower-only Model 12](#_Toc168669725)

[Shared/ Hybrid Model 13](#_Toc168669726)

[Service Tiers 13](#_Toc168669727)

[Basic Tier 14](#_Toc168669728)

[Advanced Tier 17](#_Toc168669729)

[Premier Tier 19](#_Toc168669730)

[Managed SD-WAN Services (MSD-WAN) 21](#_Toc168669731)

[Supported Platforms 22](#_Toc168669732)

[Key Features of Sify SD-WAN 23](#_Toc168669733)

[Deep Observability: Cisco ThousandEyes 23](#_Toc168669734)

[Service Overview 24](#_Toc168669735)

[Network Performance Monitoring 24](#_Toc168669736)

[Application Performance Monitoring 24](#_Toc168669737)

[Cloud Performance Monitoring 25](#_Toc168669738)

[Reporting and Analytics 26](#_Toc168669739)

[Capabilities 26](#_Toc168669740)

[Service Components 27](#_Toc168669741)

[Service Tiers 28](#_Toc168669742)

[Essentials 28](#_Toc168669743)

[Premier 28](#_Toc168669744)

[Signature 29](#_Toc168669745)

[Sify’s Scope of Work 30](#_Toc168669746)

[Service Deliverables 31](#_Toc168669747)

[Transition Services 31](#_Toc168669748)

[Proactive Monitoring 31](#_Toc168669749)

[Link Management 32](#_Toc168669750)

[Router Management 33](#_Toc168669751)

[Service Desk 34](#_Toc168669752)

[Incident Reporting and Management 34](#_Toc168669753)

[Problem Management 35](#_Toc168669754)

[Configuration Management 35](#_Toc168669755)

[Inventory Management 36](#_Toc168669756)

[Change Management 36](#_Toc168669757)

[Security Management 36](#_Toc168669758)

[Online Reporting 37](#_Toc168669759)

[Performance Reporting 37](#_Toc168669760)

[Customer Premise Equipment Maintenance 38](#_Toc168669761)

[Next Business Day Response Maintenance Service 38](#_Toc168669762)

[Vendor coordination 38](#_Toc168669763)

[Network and Technology 39](#_Toc168669764)

[People and Process Requirements 39](#_Toc168669765)

[NOC Backend System Requirements 39](#_Toc168669766)

[Service Request Initiation & Resolution (Ticketing) 40](#_Toc168669767)

[Service Level Agreements 41](#_Toc168669768)

[SLA Exceptions and Exclusions 41](#_Toc168669769)

[Service Level Conditions 42](#_Toc168669770)

[Site Uptime SLA – Service Credits 42](#_Toc168669771)

[Site Uptime SLA - Penalty Exclusion 42](#_Toc168669772)

[Service Request 43](#_Toc168669773)

[Severity Level Definitions 43](#_Toc168669774)

[Ownership of Managed CPEs post contract period 44](#_Toc168669775)

[Faulty Managed CPEs Caused by Customer Site Conditions 44](#_Toc168669776)

[Addition of New Sites, Managed CPEs Post Contract Period 44](#_Toc168669777)

[RMA Process 45](#_Toc168669778)

[Device Warranties 45](#_Toc168669779)

[Sify Service Portal: AakaashTM 45](#_Toc168669780)

[Reviews 47](#_Toc168669781)

[Commercial Proposal 48](#_Toc168669782)

[Information Security Policy 49](#_Toc168669783)

[Standard Terms & Conditions 50](#_Toc168669784)

[General T&Cs 50](#_Toc168669785)

[Payment Terms 52](#_Toc168669786)

# Document History

## Sign-Off

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Company** | **Name** | **Designation** |
| **Author** |  |  |  |
| **Client Management** |  |  |  |
| **Project Owner** |  |  |  |
| **Project Sponsor** |  |  |  |

## Document Title

|  |  |
| --- | --- |
| **Customer** |  |
| **Title** | Sify Managed WAN Services Proposal |
| **Document Name** | .pdf |

## Preparation

|  |  |  |
| --- | --- | --- |
| **Action** | **Name** | **Date** |
| **Prepared By** | Solution Architect | June 2023 |
| **Reviewed By** |  |  |
| **Distributed By** |  |  |

## Release

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ver.** | **Release Date** | **Change Notice** | **Pages Affected** | **Remarks / Changes** |
| **v1.0** |  | NA | NA | NA |

## Distribution List

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Company** | **Name** | **Sections to Read** | **For Info** | **For Action** | **Released By** |
| <CUSTOMER NAME> |  | All |  | 🗹 |  |
|  |  | All | 🗹 | 🗹 |  |
|  |  | All | 🗹 | 🗹 |  |

## Statement of Confidentiality

|  |
| --- |
| This document contains proprietary trade secret and confidential information to be used solely for evaluating [“Sify”]. The information contained herein is to be considered confidential. by accepting this document, agrees that neither this document nor the information disclosed herein, nor any part thereof, shall be reproduced or transferred to other documents, or used or disclosed to others for any purpose except as specifically authorized in writing by Sify Technologies Limited. |

# Executive Summary

## About <CUSTOMER NAME>

< Content about the Customer>

## About Sify Technologies Ltd.

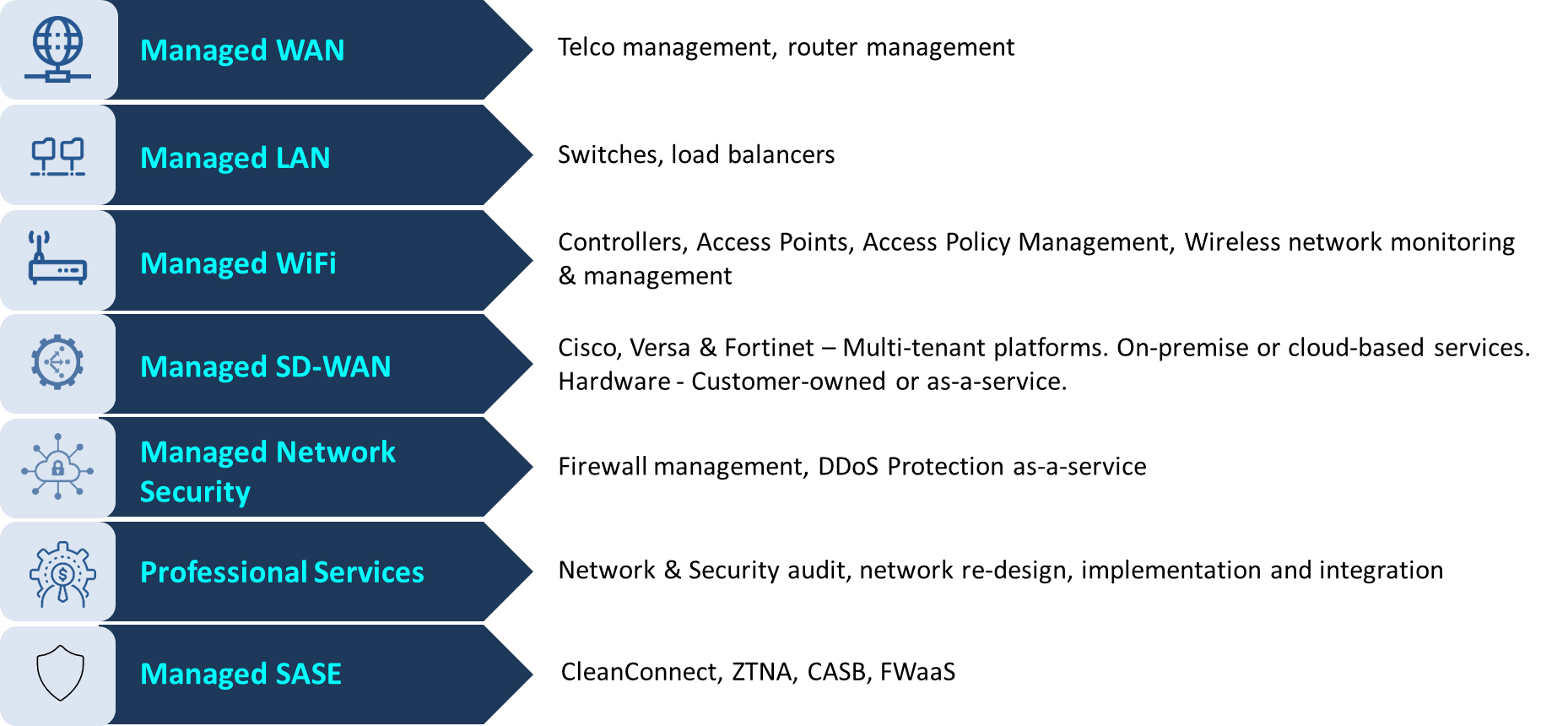
A Fortune 500 India company, Sify Technologies is India’s most comprehensive ICT service & solution provider. Sify being Digital at Core in our solutions portfolio, Sify is focused on the changing ICT requirements of the emerging Digital economy and the resultant demands from large, mid and small-sized businesses. Sify’s infrastructure comprising the largest MPLS network, top-of-the-line DCs, partnership with global technology majors, vast expertise in business transformation solutions modelled on the cloud make it the first choice of start-ups, incoming Enterprises, and even large Enterprises on the verge of a revamp,

More than 10000 businesses across multiple verticals have taken advantage of our unassailable trinity of Datacentres, Networks and Security services and conduct their business seamlessly from more than 1600 cities in India. Internationally, Sify has presence across North America, the United Kingdom and Singapore.

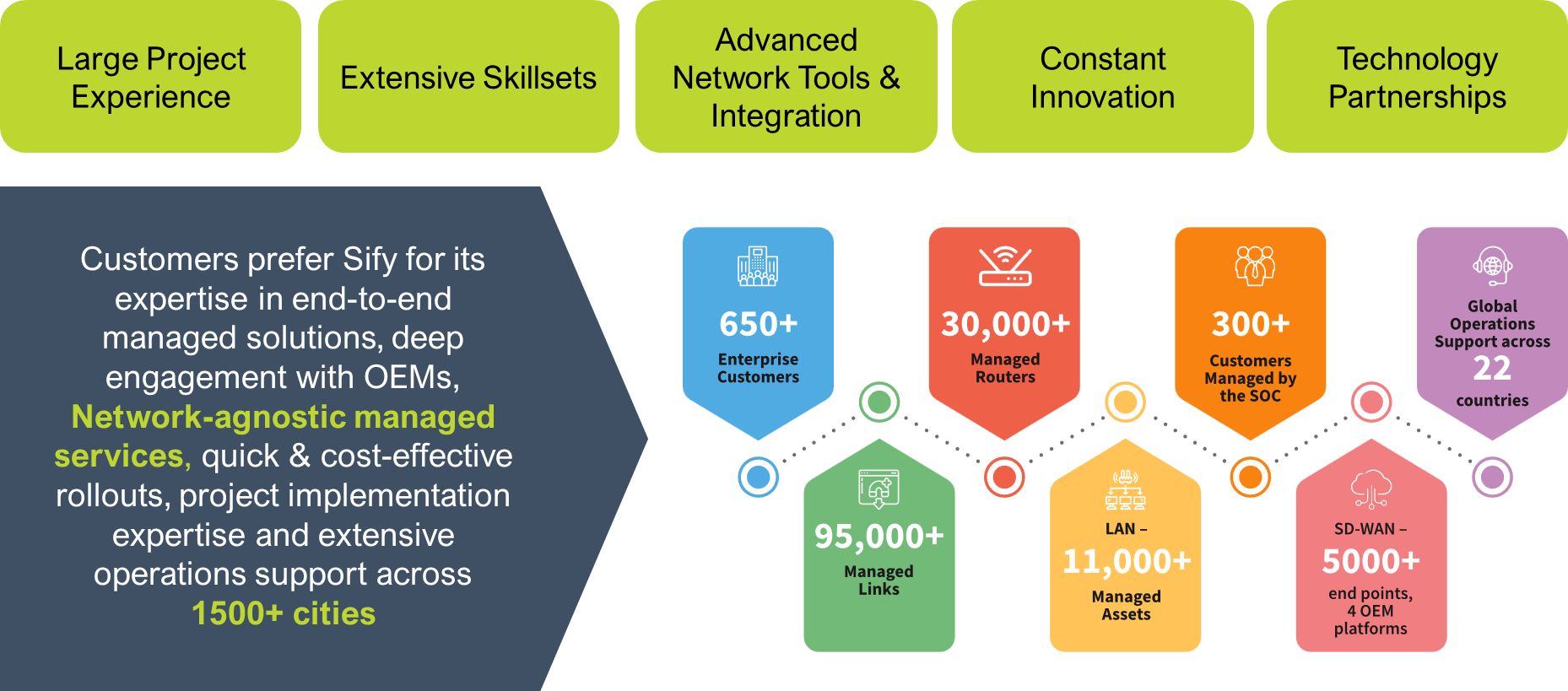
## Business Units



## Managed Network Services Portfolio



## Scale of Operations



## What does Sify bring to the table?

* Adherence to industry standards like ITILv3, ISO27001, ISO9001 and ISO20000 based service delivery
* Over 400 man-years of experience in management contributing to our core business
* Sify has optimal and right mix of services involved in system integration services including Network services, IT and security management, SOC
* Sify brings a strong Operational and Technical expertise in complex Infrastructure Management
* Extensive experience in delivering end-to-end network services concept creation – managing and delivering SLA adherence
* Sify has strategic relationships with OEM’s & Service Provider’s in the field of Compute, Network, Storage, Security, Operating Systems, Unified messaging & Applications, Enterprise Management Systems, Disaster Recovery Management & Replication, Power, Cooling, Building Management Systems, Passive components, MPLS Network, VPNoBB, Internet Bandwidth, Digital Certificates, etc.

Sify Technologies Limited (referred herein as “Sify”) has thoroughly understood the requirement and is pleased to submit the proposal to this. We are delighted at the possibility of partnering with <CUSTOMER NAME> in enhancing the adoption of technologies for efficient functioning of crucial business operations.

Sify is confident of offering a high-quality solution at a competitive price. We are equally confident that Sify’s awareness of the managed network services marketplace, its pioneering achievements in the field of providing high-quality managed network services to the Indian Corporate World, together with its unmatched expertise and experience in managing some of the country’s largest and mission-critical infrastructures can offer to <CUSTOMER NAME> a very unique and a distinct advantage which will clearly differentiate us and our solution from the rest of the competition. As a specialist and a leader in infrastructure management and services, we have also established our market leadership in the delivery of Managed Network Services, Data Center and Disaster Recovery services. It is this advantage of being a proven solution provider, which Sify wants to bring on board to <CUSTOMER NAME>.

To summarize this proposal, the response is divided into 2 parts, which addresses the following aspects of <CUSTOMER NAME> requirements as mentioned in the proposal.

Part 1: Technical Proposal

Part 2: Commercial Proposal

This document includes only Part 1 of the proposal. The document captures complete and comprehensive information about the proposed technical solution, its delivery capabilities and the support infrastructure/tools in place for management of the proposed solution offering based on adoption of industry-accepted ITIL standards. Part 2 is explained in a separate document, which is being submitted along with Part 1 to <CUSTOMER NAME>.

# Sify Managed Network Services

## Service Description

IT Infrastructure has become the lifeline for any business and there is a relentless drive towards automation and the focus on reducing manual intervention in processes, thereby achieving significant performance and productivity levels. Organizations are increasingly moving towards outsourcing their management of CPEs to Application Services to the service providers so that they can concentrate on their core business and thereby increase efficiency and productivity within the organization. Service provider not only brings rich and diversified experience but also enables a process-oriented approach ensuring smooth operations.

Sify monitors, manages, and administers customer’s infrastructure through redundant state-of-art Centralized Operations Centre at Mumbai, Chennai & Bangalore. Sify will manage the infrastructure proactively 24x7x365 days through the state-of-the-art Network Operations Centre. All the events will be proactively captured; analyzed and necessary actions will be taken through proper channel to rectify the errors, if any.

Proactive Monitoring and Management Service provided 24x7 proactive monitoring and management of WAN network, Security elements to offer performance and reporting with assured guarantees to Sify customers.

Driven by ITIL-based best practices, Sify's Monitoring and Management Services provide a comprehensive service offering its customers a visibility to even the minute details of their infrastructure. The complete management service is offered from Sify's state-of-the-art Managed Network Operations Centre [MNOC].

Sify monitoring interface will is available over the internet as a support portal for customers to log on with the provided credentials to view the status and statistics of the elements, request technical assistance regarding the in-scope infrastructure.

Apart from monitoring the customer’s network and its elements (under scope), this service will also cater to monitoring the business-critical application services from a network perspective. MNOC will act as a Single point of ownership for all Sify associated services, which includes, but not limited to, Sify’s communication services and Sify’s hardware AMC. However, in cases where there are third party vendors involved, MNOC would extend their support in the form of vendor coordination.

This service is offered to Customer’s who is looking for a trusted provider to outsource the monitoring and management functions of their infrastructure. This will help the customer to optimize their resources (tools and people) for administration of their infrastructure.

# Managed WAN Services (MWAN)

Sify’s Managed Services offers real-time monitoring and reporting of your network infrastructure as well as management of the network infrastructure. These services involve the use of network monitoring and reporting tools which can alert administrators when there is trouble on the network and help to develop trends in the health of the network by allowing complete visibility of the network through Sify’s own reporting portal – Aakaash. Sify MS offers effective resolution of network issues and problems through our MS-NOC.

|  |  |  |  |
| --- | --- | --- | --- |
| S. No. | Scenario | Link | CPE |
| 1 | Scenario 1 | Sify | Sify |
| 2 | Scenario 2 | Sify | COE |
| 3 | Scenario 3 | OSP | Sify |
| 4 | Scenario 4 | OSP | COE |

A screenshot of a computer

Description automatically generated with low confidence

|  |  |
| --- | --- |
| **Functional Specifications** | **Deliverables** |
| Managed Network Implementation Services | End to End |
| Transition Services | Applicable |
| Pro-active Monitoring | Applicable |
| Service Desk | Pro-active |
| Incident Reporting | Pro-active |
| Incident Management | Applicable. End to End |
| Problem Management | Applicable. End to End |
| Change Management | Applicable |
| Performance Management | Applicable. End to End |
| Inventory Management | Applicable |
| Service Provider Coordination | Applicable |
| Service Portal | Applicable. End to End |
| SLA Management | Applicable. End to End |
| SLA Parameters | Mean time to Respond.  Mean time to resolve.  Service uptime |

Sify MS offers 2 service variants to customers which are categorized as:

* Managed Customer Premise Equipment
  + Sify MCPE on Other ISP Link
* Managed Customer Owned Equipment
  + COE on Other ISP Link

## Managed Customer Premise Equipment (MCPE)

MCPE offers a managed solution that aims to manage and deliver best-fit Customer Premise Equipment to meet networking needs from device procurement to installation.

Sify Managed CPE is offered as a Next Business Day (NBD) Service. Under NBD Service, repair coverage is offered Monday through Friday, 8:00 a.m. to 5:00 p.m. local time. If dispatch is required, a field engineer will arrive at the Customer premises no later than 5:00 p.m. on the next business day.

This service is available as a standard offering only to customers in Tier 1 and Tier 2 cities as per Sify considerations.

Sify shall provide installation, configuration, support, and maintenance, of hardware provided by Sify, as ordered in the Service order form.

## Sify MCPE on Other ISP Link

Proactive Monitoring & Management of Sify provided CPE on Other ISP link offers 24x7 remote monitoring and management of Enterprise Customer Networks. This service is delivered by Sify’s specialized technical team, to ensure that the network infrastructure is operational end to end. The service offers availability reports on monthly basis and ensures that proactive notification is provided to customer in case of any network outages.

Sify offers fully managed customer premise equipment (CPE) to its connectivity customers, who do not wish to own and manage the networking equipment at various locations. Sify extends tested and stable equipment, backed by end-to-end SLA thus ensuring high level of availability and single point of ownership. The service is available both on rental model as well as outright ownership model.

**Key Features**

* Covers range of CPE devices from leading vendors supporting various business needs
* Single point of ownership
* 24x7 monitoring and management by specialized network team.

Sify’s skilled team of certified network architects provide complete onsite and remote support for the management of customer’s network (LAN and WAN) thus providing maximum assurance to network availability and performance. This service is offered to customers who are looking for a trusted provider to outsource the monitoring and management functions of their infrastructure at a location where Sify is not currently providing them an active link. This service is offered to organizations who don’t want to invest heavily in the onetime capex for CPE.

SLA for hardware replacement will be governed basis the OEM support for the device procured by the customer.

## MCPE Deployment Stages

|  |  |  |
| --- | --- | --- |
| **#** | **Stakeholder** | **Activity** |
| 1 | Sales | Request for MCPE |
| 2 | Product Team | Request for quote from Vendor/ Commercial |
| 3 | Commercial Team | Quote Provided |
| 4 | Product Team | Validation of Quote |
| 5 | Product Team | Pricing of MCPE & BU Approval |
| 6 | Product Team | Request to raise PR with Business Process Team |
| 7 | Business Process Team | Raise PR |
| 8 | Commercial Team | Final negotiation with Vendor & Release PO |
| 9 | RSDM | Raise TR/ISO for MCPE |
| 10 | RSDM/ RSDE | Configure & Install MCPE |

## Managed Customer Owned Equipment (MCOE)

Proactive Monitoring & Management offers 24x7 remote monitoring and management of Customer Networks including the CPE. This service is delivered by Sify’s specialized technical team, to ensure that the network infrastructure is always operational end-to-end. This service is suitable for the customers those are using Sify’s connectivity services, and it will also be beneficial for the customers those are not using Sify’s connectivity service. The service offers availability reports on monthly basis and ensures that proactive notification is provided to customer in case of any network outages.

The service offerings include Configuration management, Incident Management, Problem management, Performance management, Change management and Helpdesk.

This service can be offered to customers who are looking to outsource monitoring and management functions of their infrastructure for self-owned CPEs. This service is beneficial to organizations looking to optimize their capital expenditure and operational expenditure involved in monitoring and administration of their network infrastructure.

**Key Features**

* Single point of ownership – end to end SLA.
* 24x7 monitoring and management by specialized network team.
* Configuration management features such as Storing of current configurations, online audit logs (30 days storage), Online backup.
* Vendor Management feature is also available as per need of customer.

Sify’s team provides complete Vendor support as a part of the management of customer’s network (LAN and WAN); this includes coordination with different vendors on behalf of customer to ensure maximum network availability and performance. The coordination with vendor can be extended to opening the trouble ticket at vendor’s end and follow-up with vendor. The service variants under this classification include,

* **Managed COE:** Proactive Monitoring & Management of links provided by Sify and having Customer Owned Equipment (COE).
* **Managed COE Other ISP:** Proactive Monitoring & Management of links not provided by Sify and having Customer Owned Equipment (COE).

## Manpower-only Model

Sify also offers Facility Management solutions for customers who require their network managers to be on site. These are the type of contracts in which the core deliverable from Sify’s end are highly trained personnel who are hired based on specific skillsets required to effectively manage the customer’s network.

In such kind of solutions, Sify will be responsible for hiring & managing the staff who would be deployed in the roles of engineers, project managers etc. on customer premises as dedicated resources. The idea behind providing dedicated resources is to ensure faster turnaround time for tickets and giving the customer “hands-and-feet” support on ground.

Manpower-only contracts could be of the following types –

* **Fully Dedicated Sify Resources:** Customer’s network is managed fully by a dedicated workforce on-site customer’s premises. Such kind of setups are minimally reliant on Sify’s shared NOC and most of the network management is done “in-house”.
* **Hybrid Model:** Sify provides a team of front-line staff to the customer who would be actively supported by shared resources in Sify’s central NOC.

**Outsourced Model:** In such arrangements, Sify might agree to manage the customer’s network in partnership with a 3rd party service provider. In this model, some of the low-level network personnel might be provided by the partner however, administration of the NOC, whether it is dedicated on site or hybrid will lie with Sify. This model will generally only be opted for in-case a large count of manpower is needed to be provided to a customer.

## Shared/ Hybrid Model

Sify offers a suite NextGen NOC tools & services along with manpower to efficiently manage the customer’s entire network. However, for cases where customer has already invested in a tool which they require a service provider to manage, Sify can also offer trained & experienced NOC resources, who would be able to takeover and run the customer’s network on their own tool. These resources will work in coordination with Sify NOC to manage the customer’s network.

## Service Tiers

|  |  |  |
| --- | --- | --- |
| **Basic** | **Advanced** | **Premier** |
| Fault Management | Fault Management | Fault Management |
| Performance Management | Performance Management | Performance Management |
| Configuration Management | Configuration Management | Configuration Management |
|  | Syslog | Syslog |
|  | Event Correlation | Event Correlation |
|  |  | Application Visibility on Network |
|  |  | AI/ ML (Optional Extra) |

## Basic Tier

Basic Tier network monitoring empowers Sify to optimize customer’s infrastructure performance with fault management, performance monitoring, and configuration management capabilities.

**Fault Management**

With our fault management service, clients benefit from real-time monitoring and rapid issue resolution, ensuring uninterrupted operations and minimized downtime.

Key benefits of the fault management feature are:

1. **Fault Detection**: The tool continuously monitors network devices, interfaces, and services to detect deviations from normal operation. This involves monitoring various parameters such as device availability, response times, error rates, and traffic patterns.
2. **Alarm Generation**: When a fault or abnormal condition is detected, the tool generates alerts or alarms to notify administrators. These alarms provide information about the nature of the fault, its severity, and the affected network components.
3. **Root Cause Analysis**: Once an alarm is generated, the tool performs root cause analysis to determine the underlying reason for the fault. This may involve analysing logs, event records, performance metrics, and configuration data to pinpoint the exact cause of the issue.
4. **Isolation and Localization**: The tool helps isolate the affected components and localize the problem to specific devices, interfaces, or network segments. This process helps minimize the impact of the fault and accelerates the resolution process.
5. **Resolution and Remediation**: Once the fault is identified and isolated, the tool facilitates the resolution process by providing guidance, automated actions, or workflows to rectify the issue. This may involve restarting services, reconfiguring devices, or implementing corrective actions to restore normal operation.

**Performance Management**

Additionally, our performance management features enable precise tracking of key performance metrics, facilitating resource optimization and enhanced system efficiency.

Key aspects of performance management are:

1. **Performance Monitoring**: Continuously monitoring key performance indicators (KPIs) such as bandwidth utilization, latency, packet loss, throughput, and error rates across network devices and links. This involves collecting performance data in real-time or through periodic polling.
2. **Performance Analysis**: Analysing collected performance data to identify trends, patterns, and anomalies that may impact network performance. This may involve comparing current performance metrics against historical data or predefined thresholds to detect deviations and potential issues.
3. **Capacity Planning**: Forecasting future network capacity requirements based on historical performance data, growth trends, and business needs. Performance management tools help predict resource utilization levels and plan for network expansion, upgrades, or optimizations to prevent congestion and scalability issues.
4. **Tuning and Optimization**: Optimizing network configurations, protocols, and settings to improve performance and efficiency. This may include adjusting Quality of Service (QoS) parameters, optimizing routing protocols, or fine-tuning network device settings to enhance performance for critical applications or services.
5. **Traffic Analysis**: Analysing network traffic patterns and flows to understand application usage, user behaviour, and resource consumption. The tool provides insights into traffic distribution, application performance, and bandwidth usage, enabling administrators to optimize network resources and prioritize critical traffic.
6. **SLA Compliance**: Ensuring compliance with service level agreements (SLAs) by monitoring performance metrics and meeting predefined service quality targets. The tool helps track SLA parameters such as availability, response times, and throughput, and provide reporting capabilities to demonstrate compliance to stakeholders.
7. **Troubleshooting and Diagnostics**: Assisting in troubleshooting performance issues by providing visibility into network behaviour, performance trends, and potential bottlenecks. The features include diagnostic tools, visualization capabilities, and root cause analysis features to expedite problem resolution and minimize downtime.

**Configuration Management**

Our configuration management service provides centralized control over network devices, servers, and applications, ensuring consistency, compliance, and reduced risk of errors.

Key aspects of configuration management include:

1. **Configuration Repository**: Storing and maintaining a centralized repository of device configurations, including backup copies of configuration files and version history. This repository serves as a single source of truth for all network device configurations, facilitating easy access, tracking, and restoration of configurations when needed.
2. **Configuration Automation**: Automating the process of configuring network devices to ensure consistency and reduce human errors. This provides automation capabilities for tasks such as device provisioning, software updates, and configuration changes, streamlining deployment and management workflows.
3. **Configuration Templates**: Creating and managing configuration templates or profiles for different types of network devices and services. These templates define standard configurations and best practices for device settings, ensuring uniformity and compliance with organizational policies and industry standards.
4. **Change Management**: Implementing change management processes to track and control configuration changes throughout their lifecycle. This helps manage change requests, approvals, and audits, ensuring that all configuration modifications are documented, authorized, and properly implemented to minimize disruptions and security risks.
5. **Compliance Monitoring**: Monitoring device configurations for compliance with predefined configuration standards, regulatory requirements, and security policies. It can perform automated compliance checks, compare device configurations against baseline configurations or regulatory standards, and generate reports to demonstrate compliance to auditors and stakeholders.
6. **Configuration Auditing and Reporting**: Conducting regular audits of device configurations to identify discrepancies, unauthorized changes, or deviations from standard configurations. This includes reporting capabilities to generate audit trails, configuration change logs, and compliance reports for analysis and review.
7. **Rollback and Recovery**: Facilitating configuration rollback and recovery procedures to restore devices to a known, stable configuration in case of configuration errors, failures, or security incidents. The tool has rollback mechanisms, configuration snapshotting, and backup/restore functionalities to revert configurations to previous states and minimize service disruptions.

## Advanced Tier

In the Advanced Tier, in addition to the features provided in the Basic Tier, Sify delivers advanced Syslog and Event correlation capabilities through Everest InfraOn.

**Syslog Management**

With our Syslog service, clients can collect and centralize log data from various devices and applications, enabling comprehensive monitoring and analysis for proactive issue detection and resolution.

Key aspects of syslog management in Sify’s network monitoring tool are:

1. **Message Collection**: Captures syslog messages generated by various devices and systems within the network, including routers, switches, firewalls, servers, and applications.
2. **Centralized Storage**: Syslog messages are stored in a centralized repository or database for easy access, search, and analysis. Centralized storage enables administrators to maintain a comprehensive log history and correlate events across different devices and systems.
3. **Message Parsing**: Parses syslog messages to extract relevant information, such as timestamps, severity levels, source IP addresses, error codes, and message content. Parsing allows for structured storage and efficient analysis of syslog data.
4. **Alerting and Notification**: Provides alerting and notification mechanisms to inform administrators about critical events, errors, or anomalies detected in syslog messages. Alerts can be configured based on predefined thresholds, severity levels, or specific message patterns.
5. **Log Analysis and Reporting**: Offers log analysis and reporting capabilities to analyse syslog data, identify trends, patterns, and anomalies, and generate reports for compliance, troubleshooting, and security analysis purposes.
6. **Data Aggregation**: Aggregation capabilities allow for the consolidation of syslog data from distributed sources into a single view for centralized analysis.
7. **Retention and Archiving**: Supports syslog message retention and archiving policies to comply with regulatory requirements, internal policies, and audit standards. Retention settings determine how long syslog messages are retained in the system before being archived or purged.

**Event Correlation**

Our Event correlation feature further enhances this capability by intelligently correlating related events to provide deeper insights into system performance and potential threats.

Key aspects of the event correlation feature are:

1. **Aggregation**: Collecting and consolidating event data from multiple sources, such as network devices, servers, applications, and security appliances, into a centralized repository for analysis.
2. **Normalization**: Standardizing event data formats, attributes, and metadata across different sources to facilitate consistent analysis and correlation.
3. **Pattern Recognition**: Identifying recurring patterns, trends, or anomalies within event data to detect potential issues or abnormalities. This involves analysing event timestamps, severity levels, message content, and other attributes to identify correlations.
4. **Root Cause Analysis**: Determining the underlying cause or trigger of correlated events by tracing the sequence of events leading up to an issue. This may involve analysing event dependencies, causal relationships, and impact propagation across the network.
5. **Event Deduplication**: Eliminating duplicate or redundant events to reduce noise and false positives in correlation analysis. Event deduplication ensures that only unique events are considered for correlation to avoid unnecessary alerting and confusion.
6. **Temporal Correlation**: Correlating events based on their temporal relationships, such as sequences, time intervals, or concurrency. Temporal correlation helps identify related events that occur within a specific timeframe or follow a particular sequence, indicating potential cause-and-effect relationships.
7. **Hierarchical Correlation**: Correlating events at multiple levels of abstraction, such as correlating low-level network events with higher-level application or business events. Hierarchical correlation enables administrators to understand the impact of network events on business operations and prioritize response efforts accordingly.
8. **Dynamic Thresholding**: Adjusting correlation thresholds dynamically based on changing network conditions, traffic patterns, or environmental factors. Dynamic thresholding helps adapt correlation algorithms to evolving network behaviours and performance baselines.
9. **Automated Remediation**: Implementing automated response actions or remediation workflows based on correlation analysis results. Automated remediation helps streamline incident response processes and mitigate issues proactively before they impact network performance or service availability.

## Premier Tier

An upgrade to the Premier Tier delivers unparalleled Application Visibility on Network and cutting-edge AI/ML features through Everest InfraOn in addition to all the features provided in the Advanced Tier.

**Application Visibility on Network**

With our Application Visibility service, clients gain deep insights into network traffic, allowing for precise monitoring and management of critical applications. Leveraging advanced AI/ML algorithms, Everest InfraOn intelligently analyses network data to detect anomalies, predict potential issues, and automate response mechanisms, ensuring proactive threat mitigation and seamless operations.

Key aspects of application visibility on the network include:

1. **Traffic Monitoring**: Monitoring network traffic to identify and classify application flows based on protocols, ports, and application signatures. This allows network administrators to gain visibility into which applications are consuming network bandwidth and how they are being used.
2. **Protocol Decoding**: Analysing network packets to decode application-layer protocols and extract information about application sessions, transactions, and data payloads. Protocol decoding enables detailed analysis of application behaviour and performance characteristics.
3. **Application Performance Monitoring (APM)**: Monitoring application performance metrics such as response times, latency, throughput, and error rates to assess the quality of user experience and troubleshoot performance issues. APM capabilities provide visibility into how applications are performing from the perspective of end users and clients.
4. **User Behaviour Analysis**: Analysing application traffic patterns to understand user behaviour, preferences, and usage trends. User behaviour analysis helps identify popular applications, detect anomalies, and optimize network resources based on user demands.
5. **Application Dependency Mapping**: Mapping dependencies between applications, servers, and network components to understand the flow of application traffic and identify dependencies that may impact application performance or availability. Application dependency mapping helps optimize network design and troubleshooting efforts.
6. **Quality of Service (QoS) Management**: Prioritizing application traffic based on business requirements and service level agreements (SLAs) to ensure that critical applications receive adequate network resources and QoS guarantees. QoS management enhances application performance and user satisfaction by minimizing latency and packet loss for important applications.
7. **Security Monitoring**: Identifying and monitoring potentially risky or unauthorized applications on the network to detect security threats, data exfiltration attempts, or policy violations. Security monitoring capabilities provide visibility into application-level threats and enable proactive threat detection and response.
8. **Application Performance Optimization**: Optimizing application performance by identifying and addressing network-related issues that impact application delivery, such as network congestion, packet loss, or latency. Application performance optimization techniques help improve application responsiveness and reliability.

**AI/ML Capabilities (Add-on option)**

AI (Artificial Intelligence) and ML (Machine Learning) significantly enhances the tool’s capabilities by providing advanced analytics, automation, and predictive capabilities. Here's how AI/ML makes monitoring better:

1. **Anomaly Detection**: Analyse historical network data to establish baseline behaviour and detect anomalies indicative of network issues or security threats. This allows for early detection and proactive response to abnormal behaviour, minimizing downtime and security breaches.
2. **Predictive Analytics**: By analysing patterns and trends in network data, the tool can predict potential network failures or performance degradation before they occur. Predictive analytics enable proactive maintenance and capacity planning, reducing the likelihood of service disruptions.
3. **Intelligent Alerting**: Enhance alerting mechanisms by correlating events, prioritizing alerts based on severity and impact, and reducing false positives. This helps focus attention on critical issues and avoid alert fatigue among IT teams.
4. **Automated Remediation**: Automate remediation actions in response to detected issues. For example, the tool can identify optimal configuration changes or reroute traffic to mitigate congestion, reducing manual intervention and accelerating problem resolution.
5. **Dynamic Network Optimization**: Optimize network configurations and resource allocation dynamically based on changing traffic patterns, user behaviour, and application requirements. This improves network performance, efficiency, and resource utilization.
6. **Behavioural Analysis**: AI/ML techniques can analyse device behaviour on the network to identify deviations from normal patterns and detect insider threats or unauthorized activities. Behavioural analysis enhances network security by flagging suspicious behaviour for further investigation.
7. **Traffic Prediction and Management**: AI/ML algorithms can predict future network traffic patterns and adjust network policies and configurations accordingly to optimize bandwidth utilization and ensure quality of service (QoS) for critical applications.
8. **Root Cause Analysis**: The tool can perform advanced root cause analysis by correlating multiple data sources and identifying the underlying causes of network issues more accurately and efficiently.

# Managed SD-WAN Services (MSD-WAN)

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.

Sify’s Managed 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

Sify has extensive experience in delivering high-quality SD-WAN solutions for our customers in the following industries –

• FMCG

• Manufacturing

• Private BFSI

• Public BFSI

• Retail & Distribution

• Pharma & Healthcare

• Utilities & Infrastructure

Some of our success stories with Managed SD-WAN –

* Achieved centralized policy enforcement across all locations, dashboard-based monitoring and control of the entire WAN for one of India’s largest electricity PSU with 750 locations.
* Significant improvement in application performance with internet-based access for one of India’s leading pharmaceutical companies
* Single ownership with Sify for installation and 24x7 monitoring & management. Significant cost reduction with LTE/broadband as fallback for non-critical traffic/locations & zero touch unified security policies across pan India 250+ locations.
* Application based routing & QoS with rate limiting for selected applications. No capex & risk with new technology implementation for one of the National Co-operative Banks with 55 locations.

## Supported Platforms

Sify supports end-to-end proactive monitoring & management of the below listed SD-WAN platforms –

* Versa
* Cisco Catalyst
* Fortinet
* Aruba
* FatPipe

## Key Features of Sify SD-WAN

* Application visibility and control: Applications can be prioritized based on business policies, and visibility is provided through the centralized cloud-based network management application.
* Dynamic WAN selection: Minimum performance benchmarks can be set on a per-application basis and can be adjusted automatically.
* Application optimization: The service allows the customer to continuously monitor and improve network paths based on performance bench-marks and includes forward error correction and jitter buffering.
* Secure network deployment: The SD-WAN service automatically sets up IPSec tunnels with end-to-end encryption, enabling dynamic branch-to-branch connectivity.
* Stateful firewall: An integrated stateful firewall allows for the deployment and management of security policies, which can be managed centrally with options for edge overrides by location. In addition, application layer filtering provides some next-generation firewalling capabilities.
* Network analytics: Real-time analytics allow for policy creation and troubleshooting and provide insights into application utilization and bandwidth consumption.

# Deep Observability: Cisco ThousandEyes

Cisco ThousandEyes is a network intelligence platform designed to provide comprehensive visibility into the performance of applications and services delivered over the internet. Its purpose is to empower organizations with insights into their network, helping them monitor, analyse, and optimize performance across various environments, including internal infrastructure, cloud services, and internet connections.

Cisco ThousandEyes serves as a crucial tool for organizations seeking to optimize their network performance, enhance security, and deliver a seamless digital experience to end-users.

## Service Overview

Cisco ThousandEyes will provide comprehensive visibility into network, application, cloud & security performance, including real-time monitoring and historical data analysis.

### Network Performance Monitoring

|  |  |
| --- | --- |
| **Feature** | **Description** |
| Network Path Visualization | Visualize end-to-end network paths, including hops, latency, and packet loss. |
| Internet and Cloud Monitoring | Monitor connectivity and performance to cloud services and internet-based applications. |
| BGP Monitoring | Monitor Border Gateway Protocol (BGP) routing to identify issues affecting network reachability. |
| DNS Monitoring | Monitor DNS resolution and identify issues impacting domain resolution and website access. |
| Web Transaction Monitoring | Monitor web transactions to identify issues affecting the user experience of web applications. |
| Network Device Monitoring | Monitor the performance of network devices, such as routers and switches, to detect issues. |
| Network Metrics and Analytics | Collect and analyze various network metrics, including latency, jitter, and throughput. |
| Enterprise and Endpoint Agents | Deploy agents across the enterprise and on endpoints to monitor network performance from different locations. |
| Multi-Cloud Visibility | Gain insights into network performance across multiple cloud providers. |
| Network Topology Mapping | Automatically map the network topology to understand the relationships between different components. |
| Historical Performance Data | Store and analyze historical network performance data to identify trends and patterns over time. |
| Collaboration and Reporting | Facilitate collaboration among teams and provide reporting capabilities for network insights. |

### Application Performance Monitoring

Key application performance monitoring features that ThousandEyes offers:

|  |  |
| --- | --- |
| **Feature** | **Description** |
| Network Path Visualization | Visualize the end-to-end network path, including hops, latency, and packet loss. |
| Internet and Cloud Monitoring | Monitor connectivity and performance to cloud services and internet-based applications. |
| DNS and Web Transaction Monitoring | Monitor DNS resolution and web transactions to identify issues affecting application performance. |
| Network Metrics and Analytics | Collect and analyze various network metrics, such as latency, jitter, and throughput. |
| Synthetic Transaction Monitoring | Simulate user transactions to proactively identify performance problems before end-users are affected. |
| Enterprise and Endpoint Agents | Deploy agents across the enterprise and on endpoints to monitor performance from different locations. |
| Multi-Cloud Visibility | Gain insights into application performance across multiple cloud providers. |
| Historical Performance Data | Store and analyze historical performance data to identify trends and patterns over time. |
| Collaboration and Reporting | Facilitate collaboration among teams and provide reporting capabilities for performance insights. |

### Cloud Performance Monitoring

Cisco ThousandEyes will support and integrate with various cloud platforms, ensuring seamless monitoring in hybrid and multi-cloud environments.

|  |  |
| --- | --- |
| **Feature** | **Description** |
| Cloud Service Monitoring | Monitor the performance and availability of cloud services, including popular cloud providers. |
| Multi-Cloud Visibility | Gain insights into application and network performance across multiple cloud platforms. |
| Internet Service Provider (ISP) Cloud Monitoring | Monitor and analyze the performance of connections to internet service providers and cloud services. |
| Cloud Provider-Specific Metrics | Capture and analyze metrics specific to various cloud service providers (e.g., AWS, Azure, GCP). |
| Direct Cloud Connectivity Monitoring | Monitor the performance of direct connections to cloud services without reliance on VPNs or other intermediaries. |
| Cloud-Based Application Monitoring | Monitor the performance of applications hosted in the cloud and their interactions with users. |
| Synthetic Transactions in the Cloud | Perform synthetic transactions to assess and monitor the performance of cloud-hosted applications. |
| Integration with Cloud APIs | Utilize APIs provided by cloud service providers for deeper integration and data retrieval. |
| Cloud Resource Utilization Monitoring | Monitor the utilization of cloud resources such as virtual machines, storage, and databases. |
| Cloud Security and Compliance Monitoring | Assess and monitor security and compliance measures within cloud environments. |
| Cloud Cost and Billing Integration | Integrate with cloud providers for visibility into cost and billing related to cloud resources. |
| Alerting and Reporting | Set up alerts and generate reports based on cloud performance and availability metrics. |

### Reporting and Analytics

Cisco ThousandEyes offers reporting capabilities, including customizable dashboards, trend analysis, and alerting mechanisms for network and application performance.

|  |  |
| --- | --- |
| **Feature** | **Description** |
| Real-Time Dashboards | Create customizable dashboards to visualize real-time data on network and application performance. |
| Historical Performance Analysis | Analyze historical data to identify trends, patterns, and changes in network and application behavior. |
| Reporting and Alerting | Generate reports on performance metrics and set up alerts based on specific conditions or thresholds. |
| API Access | Access data programmatically using APIs to integrate with other systems and extract customized insights. |
| Multi-Layered Data Visualization | Utilize various visualization techniques for a comprehensive view of network and application performance. |
| Drill-Down Capabilities | Drill down into specific data points to investigate and troubleshoot performance issues in more detail. |
| Path Visualization and Tracing | Visualize end-to-end network paths and trace the route of packets to identify performance bottlenecks. |
| Synthetic Transaction Reports | View reports on synthetic transactions to assess and monitor the performance of applications. |
| Cloud and Internet Connectivity Reports | Gain insights into connectivity and performance to cloud services and the internet. |
| Role-Based Access Control (RBAC) | Implement RBAC to control access to reporting and analytics features based on user roles. |
| Export and Share Reports | Export reports for offline analysis and share them with stakeholders for collaborative troubleshooting. |
| Integration with Third-Party Tools | Integrate with third-party tools and services to enhance reporting and analytics capabilities. |

## Capabilities

* **Comprehensive Visibility:** The ability of ThousandEyes to provide end-to-end visibility into the entire network path, including internal infrastructure, cloud services, and internet connections, is a critical success factor. Organizations benefit from a holistic view of their network, helping them identify and address performance issues effectively.
* **Real-Time Monitoring:** Real-time monitoring capabilities are crucial for identifying and responding to network issues promptly. ThousandEyes' ability to provide up-to-the-minute data on network performance enables IT teams to take proactive measures to maintain a high level of service availability.
* **Cloud and Internet Intelligence:** As organizations increasingly rely on cloud services and internet connectivity, the ability to monitor and gain intelligence into the performance of these services is essential. ThousandEyes provides insights into how applications are performing across various cloud platforms and internet service providers.
* **Digital Experience Monitoring:** Success with ThousandEyes involves leveraging its digital experience monitoring capabilities. This allows organizations to understand how end users are experiencing applications and services, enabling them to optimize performance and enhance user satisfaction.
* **Advanced Diagnostics and Troubleshooting:** The platform's diagnostic tools play a crucial role in troubleshooting network issues. Successful implementation involves utilizing these tools effectively to identify and resolve problems quickly, whether they originate within the organization's infrastructure or externally.
* **Security Insights:** Security is a critical success factor, and ThousandEyes provides visibility into internet traffic, helping organizations detect and respond to security threats. Integrating security monitoring and response strategies with ThousandEyes enhances overall network security.
* **Scalability:** The ability of ThousandEyes to scale with the organization's needs is essential. As networks grow and evolve, the platform should be able to handle increased data volume and monitor a growing number of endpoints without sacrificing performance.
* **User-Friendly Interface:** A user-friendly interface facilitates effective use of the platform by network administrators. A well-designed and intuitive interface streamlines the monitoring and troubleshooting processes, contributing to the overall success of the implementation.
* **Integration Capabilities:** Successful deployment often involves integrating ThousandEyes with other network management and security tools. Integration with other Cisco products, as well as third-party solutions, enhances the overall effectiveness of the organization's network management strategy.

## Service Components

ThousandEyes as a service typically consists of following components:

* Customer’s existing network landscape, consisting of –
  + Routers
  + Switches
  + Firewalls
  + Load balancers
  + Servers
  + Access points
  + Links, etc.
* Sify’s underlying connectivity products (MPLS/ ILL/ Broadband).
* Service Desk & Escalation Engineers trained on ThousandEyes.
* ThousandEyes licenses of required tier included as an add-on service on top of standard Sify Managed Services offerings.

## Service Tiers

The Tiers are differentiated from each other by the following 2 parameters –

* Type of Tests
* Frequency of Tests

### Essentials

Base ThousandEyes tier. Targeted towards customers looking for long term reviews of a business-critical service from campus sites. Key value propositions are -

* Uncover gradual degradation or improvements in long term performance, enabling you to proactively address issues or capitalize on positive trends.
* Establish benchmarks and identify areas where performance falls below expectations. This information is used to prioritize optimization efforts.
* See how the application performance compares to peers in customer’s industry or market and get data driven recommendations.

**Metrics**

* Web Layer: Availability, Response Time, DNS Time, Connect Time, SSL Negotiation Time, Wait Time, Receive Time
* Network Layer: Campus-to-Application Loss, Campus-to-Application Latency, Campus-to-Application Jitter
* Metrics collection Interval: 60 Minutes

### Premier

Targeted/ upsold to customers who need real-time & deep visibility of critical applications over any network from campus sites. Keep value propositions are –

* Know when app/networks are not available before users start complaining about poor experience.
* Faster proving of app vs. network issues, reducing wasted time in troubleshooting incidents.
* Get data driven evidence of 3rd party ISP/Application issues that are affecting your campus users**.**

**Metrics**

* Web Layer: Page Load, Availability, Response Time, DNS Time, Connect Time, SSL Negotiation Time, Wait Time, Receive Time, transaction, FTP.
* Network Layer: Campus-to-Application Loss, Campus-to-Application Latency, Campus-to-Application Jitter
* BGP Layer: Prefix Reachability, Path Changes, BGP Updates
* Voice: SIP Server, Availability, RTP, MOS
* Metrics collection Interval: 5 Minutes
* End User Metrics: DNS & Gateway Loss/Latency, Wi-Fi Quality, CPU, Memory, VPN Loss/Latency

### Signature

Targeted/ upsold to high volume customers operating mission critical applications over any network for a hybrid workforce. Key value propositions are –

* Quantitative understanding of employee connectivity experience to drive investment decisions instead of relying on subjective user feedback.
* Know when app/networks are not available before users start complaining about poor experience.
* Better fault domain isolation (WiFi, PC, Campus, ISP, SaaS) reducing the number of unnecessary responders.

**Metrics**

* Web Layer: Availability, Response Time, DNS Time, Connect Time, SSL Negotiation Time, Wait Time, Receive Time
* Network Layer: Campus-to-Application Loss, Campus-to-Application Latency, Campus-to-Application Jitter
* BGP Layer: Prefix Reachability, Path Changes, BGP Updates
* Metrics collection Interval: 2 Minutes
* End User Metrics: DNS & Gateway Loss/Latency, Wi-Fi Quality, CPU, Memory, VPN Loss/Latency

## Sify’s Scope of Work

* **Implementation and Configuration**
  + Agent Installation in customer campus/cloud and end user machines.
  + Set up and configure Cisco ThousandEyes according to the client's requirements and network infrastructure to ensure proper integration with existing systems and applications.
* **Monitoring and Performance Management**
  + Continuous monitoring of network performance, application delivery, and user experience.
  + Real-time visibility into latency, packet loss, and other key performance metrics.
  + Proactive identification and resolution of network issues to maintain optimal performance.
* **Security Monitoring and Threat Detection**
  + Detect and alert security threats, ensuring the protection of sensitive data and infrastructure.
  + Regular security assessments and updates to address evolving cybersecurity challenges.
* **Collaborative Intelligence and Reporting**
  + Providing end-to-end network visibility.
  + Generate comprehensive reports on network performance, application health, and security threats.
  + Collaborate with client teams to interpret data and provide actionable insight.
* **Troubleshooting and Issue Resolution**
  + Swift identification and resolution of network issues to minimize downtime.
  + Root cause analysis for recurring problems and implementation of preventive measures.
* **Optimization and Recommendations**
  + Provide recommendations for optimizing network and application performance.
  + Advise on improvements to enhance the overall digital experience for end-users.
  + Assess scalability and suggest adjustments to accommodate changing business needs.
* **Regular Health Checks and Audits**
  + Perform regular health checks to ensure the ongoing effectiveness of the solution.
  + Conduct audits to assess adherence to security best practices and compliance requirements.

# Service Deliverables

## Transition Services

**Study & Design** - Transition teams within Sify MS-NOC will create device level configuration to prepare the network in scope for network management and monitoring services of MSNOC. At this stage the design activities are specific to the management of the network limited to the services of Sify MS-NOC. A basic study on the applications used and its critical paths on the network will be done at this stage based on FAQ and interview discussions with the customer representatives to facilitate a complete proactive approach to MS-NOC services.

**Implementation** – MS-NOC representatives will load the device specific configurations per site and perform transport and device level implementation and testing.

## Proactive Monitoring

Managed Services NOC (MS-NOC) will provide proactive monitoring services to identify any outages as well as service degrades. MS-NOC would use Sify’s Fault, Performance, and configuration compliance features of its Next Generation Operations Support System to deliver the proactive management services.

* Real time and round the clock monitoring of devices in scope
  + WAN routers and the associated links
  + LAN Switches (if defined as part of the scope)
  + Monitor at 5 minutes interval (Standard)
  + Ability to monitor at 1-minute intervals (Premium)
* Provide multiple notification option to the customer (Customer to choose)
  + E-mail
  + SMS
  + Call from the network monitoring team.
  + Notify the following to the customer.
    - Occurrence of an incident
    - Periodic status updates to customer
* Pro-active incident management
  + Incident ticket raised pro-actively by Sify for last mile link issues.
  + Resolution of incident ticket
* Status of Escalation of the incident ticket
* Monitor availability of resources in-scoped
* Monitor performance of resources
* Monitor performance of network
* Monitor back up status of devices.

## Link Management

WAN links is another of the important and critical component to connect the remote branches the centralized datacentre for application services. It requires proactive monitoring to ensure maximum uptime. Sify will remotely monitor, manage, and configure the Routers as per customized requirement of clients.

|  |  |  |  |
| --- | --- | --- | --- |
| **Service** | **Task** | **Deliverables** | **Service Trigger** |
| 24x7 Monitoring | Monitor customer’s link for  Availability  Bandwidth utilization  Packet Loss  Latency  Jitter | Utilization Reports  Availability Reports  Performance Reports | Based on alerts |
| Error logs and port errors | Monitoring for error logs and port errors. | Notification through Email / Phone | Based on alerts |
| Link Configuration | Configure and troubleshoot link & router interface. | Notification through Email / Phone | As per service request |
| Root Cause Analysis | Do the Root Cause Analysis for problems and give the permanent solution. | Notification through Email / Phone | As needed |
| Bandwidth troubleshooting | Analyze and fix the problems due to high bandwidth utilization and port errors. | Notification through Email / Phone | Based on alerts |
| Vendor Coordination | Coordinate with the service provider for  Service levels  Performance related issues  New link deployments  Configuration changes  Router failures | Notification through Email/Phone | On customer request.  As needed |

## Router Management

WAN infrastructure is one of the important and critical components to connect to the outside world and internet. It requires proactive monitoring to ensure maxim uptime. Sify will remotely monitor, manage, and configure the Routers as per customized requirement of clients.

|  |  |  |  |
| --- | --- | --- | --- |
| **Service** | **Task** | **Deliverables** | **Service Trigger** |
| 24x7 Monitoring | Monitor customer’s Router.  Device Availability  CPU Threshold  Memory Thresholds  Bandwidth utilization  Ethernet/WAN Interfaces availability | Utilization Reports  Availability Reports | Based on alerts |
| Error logs and port errors | Monitoring for error logs and port errors. | Notification through Email / Phone | Based on alerts |
| Router interface Configuration | Configure and troubleshoot router interface configurations. | Notification through Email / Phone. | As per change request |
| Access control | Configure ACLs depending on the requirement.  AAA | Notification through Email / Phone. | As per service request |
| High availability Configuration | Configuring HSRP, VRRP, GLBP and troubleshoot related issues | Notification through Email / Phone. | As per service request |
| Routing | Configure the routing protocol as per requirement, new routes, route redistribution and route summarization.  Configure and troubleshoot multicasting as per requirement. | Notification through Email / Phone. | Change request through AAKAASH. |
| QOS | Implementing Quality of Service for improving performance | Notification through Email / Phone. | Change request through AAKAASH. |
| MPLS | Configuring and troubleshooting MPLS as per customer requirement. | Notification through Email / Phone. | As per service request |
| Backup Management | Take the running configuration backup at regular intervals | Notification through Email / Phone. | As per service request |
| IOS upgrades | Upgrade the current IOS to latest IOS | Notification through Email / Phone. | As on needed. |
| Root Cause Analysis | Do the Root Cause Analysis for problems and give the permanent solution. | Notification through Email / Phone. | As on needed. |
| Security Management | Defining strong authentication methods for the users who have access.  SNMP security | Notification through Email / Phone. | As on needed |

## Service Desk

MS-NOC would serve as the single point of contact for Proactive Monitoring & Management services. MS-NOC will be manned 24x7x365 and can be accessed through a Universal Access Number. Additionally, customers can also reach the NOC through E-mails and the Service Portal.

## Incident Reporting and Management

Sify MS-NOC delivers an online designated web portal for reporting all incidents associated with its services. This will be a primary single point of contact for customers while the MS Helpdesk accessed through a Toll-free universal access number would be secondary.

* Trouble Ticket Handling – A trouble ticket number will be assigned for every trouble the customer logs in online or calls for. For each trouble reported Sify will maintain information about the trouble, the steps taken to resolve and the final disposition of it online. An RCA will be created for trouble reported based on customer request.
* Incident management: Sify will also login all incidents triggered from its proactive management system and maintain information about the trouble and the steps taken to resolve them.
* Fault Management – Services include detection, isolation, diagnosis, correction, and customer notification of network troubles. MS-NOC operates a SNMP based management system that provides real-time and back-in time graphic oriented network management of customer premises devices and associated communication links.
* Performance management – Services include monitoring of health and utilization of devices, communication links and other SP services part of customer WAN or VPN under the scope of management.

## Problem Management

Sify delivers problem management services that includes,

* Maintenance of known error database
* Check known error database for workarounds before applying resolution to a particular incident.
* Update KEDB every time a new workaround is provided to an incident.
* Provide root cause analysis for every P1 incident.
* Track all recurring incidents. Any recurrence of 4 in the last 30 days should be considered a problem.
* Provide RCA and necessary resolution for identified problems and provide possible inputs to Change Management

## Configuration Management

Sify MS-NOC delivers configuration management services that includes,

* Archiving back up of all the device configurations
* Ensuring changes made to a device is backed up and archived.
* Maintain last known good configuration to roll back changes to a previous configuration if results are unsatisfactory.
* Detect changes to configuration in real time.
* Maintain authentication, authorization and accounting while allowing for configuration changes.
* Ensure compliance of all configuration changes.
* Maintain a configuration management database with updated configuration items and the relationship between each of the assets.
* Maintain device software and hardware inventory.

## Inventory Management

Sify MS-NOC delivers inventory management services that includes,

* Capturing and maintaining inventory of network devices within the scope of the managed network per customer location.
* Maintaining customer site contact information and IP address details.

## Change Management

Post implementation Sify MS-NOC will handle all customer-initiated Move/Add/Change/Delete (MACD) requests through an online change management module. All Sify-initiated changes would be managed by Sify with an approval from the customer representative based on the criticality and the extent of impact to services.

* Perform emergency changes as part of providing immediate resolution to an identified incident. These changes cannot be planned and scheduled at a specific time because of service impact.
* Perform change management task based on inputs from the problem management process.
* Perform change management task based on inputs from incident management process.
* Perform change management task after following the required approval process.
  + Initiated by change initiator.
  + Reviewed by change manager.
  + Reviewed and approved by Sify and the customer.
* Post implementation review and clearance by the PIR team

## Security Management

Sify MS-NOC delivers security management Services within scope of network under management limited to,

* Performing device software updates and loads including one free device software update [within the same train or feature set] per year upon customer request.
* Proactive software updates to fix software bugs & security flaws. (Applicable for bundled CPE only).
* Mapping access control of all devices under its management to a Sify controlled AAA system.

## Online Reporting

Customer can utilize a designated web portal to access reports on the services online. It will include,

* Reports on number of incidents handled by the Sify MS-NOC per site and per device.
* Analysis Reports performance data from different sites based on various parameters.
* Health and Utilization reports on devices and communication links.
* Inventory report – listing the assets within the network under the scope of management.
* Availability reports – Service availability and score cards.

## Performance Reporting

Performance reporting services include.

* Provide Network Performance Report on
  + Latency
  + Packet Loss
  + Jitter
* Provide Bandwidth report.
  + Last Mile Bandwidth Utilization
  + Last Mile volume utilization
* Provide Resource related reporting.
  + CPU utilization
  + Memory utilization
* Alarms and Traps report
* CIO Dashboard
* Ticket Based Reporting
  + Total Open Tickets.
  + Total Open tickets violating SLA.
  + Weekly / Monthly Reports.

## Customer Premise Equipment Maintenance

Sify Proactive Network Management services would include customer premises equipment maintenance for services with bundled CPE. It would also be applicable for other categories if subscribed.

## Next Business Day Response Maintenance Service

For Proactive Network Management, Sify will provide Next Business Day Response maintenance service for Equipment, 8 x 5 excluding Sify-designated holidays. When Sify verifies that a problem is covered under its services and it requires on-site support, Sify will respond to customer’s affected site by next business day if the problem is verified by Sify before 3:00 p.m. Next Business Day Response is subject to geographic availability on a site-by-site basis.

## Vendor coordination

In case customer Networks involving third-party services like IP Service Provider communication links, VPN/DIA services, system Integrator delivered hardware maintenance etc., one of the following options would be applicable.

* **Customer-owned CPE’s vendor management** – Sify MS-NOC upon detecting trouble pertaining to services offered by third-party vendors will open a trouble ticket in its system and communicate the same to customer representatives. Sify would continue to follow-up with the customer representatives for further updates on such trouble report until closure. Seldom would Sify interface with the third-party vendors directly.
* **Sify managed CPE’s vendor co-ordination** – Sify in its initial transition process would understand, document and sign-off on the vendor co-ordination processes with the customer. Sify MS-NOC upon detecting trouble pertaining to services offered by third-party vendors will open a trouble ticket in its system and follow the signed-off process for incident handling directly with the documented vendor interface.
  + Sify MS-NOC personnel will act as a customer representative and report vendor’s progress in resolving the trouble online in its system.
  + Sify will not be directly responsible for non-performance of any third-party vendor services.
  + Sify will report vendor’s incident handling performance reports monthly online.

## Network and Technology

To offer proactive network management services with the deliverables defined above, the following MS-NOC backend system, process, people, and tools will address it.

### People and Process Requirements

A dedicated managed network solutions – Network Operations Centre manned with Level-1 and Level-2 technical support engineers attending to the first call (reactive) or detecting the trouble and correcting them proactively (proactive). This team will be dedicated and outside of the service helpdesk handling Sify enterprise solutions customers.

Processes will be aligned with the service delivery and support teams to ensure smooth transition of a customer; be it existing, new or under migration. The processes will ensure that the customer if opted for managed network services should have one helpdesk and one account/engagement manager to work with.

### NOC Backend System Requirements

To fulfil the service deliverables discussed above, the following supporting systems are as a backend for operating the MS-NOC.

* AAA system – A deployment of Authentication, Authorization and Accounting system in a virtualized mode of deployment is a must to support access-controls on the network devices at various customer deployments in a secure manner. Virtualization in this environment is to address multi-tenancy.
* NTP system – A stratum-1 NTP clock source serving multiple customers network deployments is required to synchronize the clocks across all the network devices for event correlation.
* Out-of-band Management – System to remotely access a network isolated due to communication link failure is required for cases with critical network deployments. Customer supplied fixed-line modem and the fixed line would be used in this case.

## Service Request Initiation & Resolution (Ticketing)

Service Requests for Customers are raised in the following ways:

* Pro-active alerts by the Global Network Management Centre for Managed Customers after validation. Customers also have the option of raising a trouble ticket in the following manner.
* Reactively by Customers can raise Service Requests in the following ways,
* Call Helpdesk - 1800 419 2929 / +91-044-66022400
* Email Helpdesk - [helpdesk@sifycorp.com](mailto:helpdesk@sifycorp.com)
* Raise a ticket on Aakaash portal (“information ON infrastructure”) which can be accessed using Customer “username” and “password”.
* Proactive alerts are populated in Beacon (Sify’s monitoring tool).
* Reactive requests are populated in Sify Oracle CRM.

Service Requests for Customers are resolved in the following ways:

* Service Request handling for Managed Customers - Requests are handled by GNMC Service Operations Team centrally and are co-ordinated till closure.
  + L1 engineers will co-ordinate with customer and perform 1st level trouble shooting (FLT) and if required, arrange a field visit till resolution is achieved.
  + For wider issues, our engineers co-ordinate with Network Operations and update customer accordingly till resolution is achieved.
  + For core network related issues, team will co-ordinate with Advanced Support Group (ASG) till resolution is achieved.
* Service Request handling for Non-Managed Customers - Requests are handled by Regional Service Operations Team for North, South, West and East.
  + L1 engineers will co-ordinate with customer and perform 1st level trouble shooting (FLT) and if required, arrange a field visit till resolution is achieved.
  + For wider issues, co-ordinate with Network Operations and update customer accordingly till resolution is achieved.
  + For core related issues, team will co-ordinate with Advanced Support Group till resolution is achieved.

# Service Level Agreements

The Service Level Agreements (“SLAs”) available for Managed Network Services are as follows for Sify provided links + CPE & Sify provided links + COE.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Service Features** | **Specifications** | **COE** | **MCPE** |
| 1 | Service Availability Guarantee - Link | (Tier 1/Tier 2/Tier 3) | > 99.9 / >99.5 / > 99% | > 99.9 / >99.5 / > 99% |
| 2 | Service Availability Guarantee - Device | (Tier 1/Tier 2/Tier 3) (Will exclude hardware replacement time) | > 99.9 / >99.5 / > 99% | > 99.9 / > 99.5 / > 99% |
| 3 | Service portal Availability |  | 99.99% | 99.99% |
| 4 | Packet Loss | (Tier 1/Tier 2/Tier 3) | < 0.5% / < 1% / < 1.5% | < 0.5% / < 1% / < 1.5% |
| 5 | Jitter | (Tier 1/Tier 2/Tier 3) | 15/20/25 ms (Diamond class of service only) | |
| 6 | Delivery time | Hardware delivery time | NA | 7 Days |
| 7 | Mean Time to Resolve (MTTR) | for severity 1/2/3 | 4 hrs. / 4 hrs. / 24 hrs. | 4 hrs. / 4 hrs. / 24 hrs. |
| 8 | Hardware Replacement Time | Replacement of Faulty Hardware according to Tier 1/Tier 2/Tier 3 ('Same Day' is only applicable for Tier 1 Cities) | NA | NBD |
| 9 | Mean Time to Respond | for severity 1/2/3 | 15s/ 30 / 60 mins | 15s/ 30 / 60 mins |
| 10 | Incident Response Rate |  | 99.90% | 99.90% |

## SLA Exceptions and Exclusions

Sify is not responsible for failure to meet an SLA where Sify’s failure results, in whole or in part, from:

* Negligence of the Customer or its representatives.
* Any Force Majeure event that prevents Sify, or vendor from providing Service or affecting restore or repair.
* Failures in performance caused by any national or local holiday.
* Any case in which Sify or vendor agents are available to repair within the Service Level commitment, but Customer reschedules to a different time or date.
* No access (Sify or vendor Agents rare available to repair within the Service Level commitment but the Customer does not provide Site access)

Interruptions or delays caused by the failure of power, equipment, services, or systems (at Customer premises) not provided by Sify including, but not limited to UPS Backup power; Generators; or Air conditioning/Heating.

## Service Level Conditions

The Service Levels defined above are subject to the conditions that for all Service Level Types mentioned above, Customer must provide on-site personnel & hardware to replace the failed device with a replacement device.

## Site Uptime SLA – Service Credits

The total of all Service Credits provided by Sify is limited to a maximum of 5% of the Quarterly Service Charge for the affected Service and Location. The Site Uptime Service Credit will be applicable as per the Site Type deployment (as mentioned within SLA table). Service credits shall be Customer’s sole remedy for a breach of the applicable service level agreement.

## Site Uptime SLA - Penalty Exclusion

No Service penalty is payable by Sify, if the failure to meet the Service Level is attributable to:

* Suspension of Services due to the Customer’s breach of the Agreement
* Alleged Service Level failure which cannot be verified by Sify's systems.
* Acts or omissions of the Customer, its subcontractors or any third party acting on the Customer’s behalf.
* Scheduled Maintenance
* Emergency Maintenance (where the emergency has not been caused by the negligence or wilful misconduct of Sify)
* Previously identified Problem that is awaiting a Change Window to be approved by the Customer to Resolve the Problem
* Any malfunction, Incident, defect, or failure in the Customer’s equipment
* Power failure at the Customer Location
* Force Majeure Events

## Service Request

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Service Feature** | **Severity** | **Metric** |
| 1 | Mean Time to Respond | For Severity 1/2/3/4 | 15 mins/ 30mins / 60 mins/1 Business Day\* |
| 2 | Incident Response Rate |  | 99.90% |

\* Indicates all time mentioned as Business Hours

## Severity Level Definitions

* **Severity 1**: An existing infrastructure is down or there is a critical impact on the Customer’s business operation. (Business Critical or Emergency)
  + System Unusable
  + Immediate Action Needed
  + Critical Condition
* **Severity 2**: Operation of an existing infrastructure is severely degraded, or significant aspects of the Customer’s business operation are being negatively impacted by unacceptable infrastructure performance. Operational performance of the infrastructure is impaired, but most business operations remain functional. (Major)
  + Error Condition
  + Warning condition
  + Normal but significant condition
* **Severity 3**: Changes to the infrastructure elements to activate / provision new services to end users. (Minor)
  + Change management request.
* **Severity 4**: Information is required on software capabilities, installation, or configuration. There is clearly little or no impact on the Customer’s business operation. (Low)
  + Informational message only
  + Debugging

## Ownership of Managed CPEs post contract period

* All Sify owned Managed CPE will continue to be under Sify’s ownership for the entire lifecycle of the product.
* Ownership of such devices will not change even if the project reaches the end of contract duration.
* Ownership of the Managed CPE can be transferred to the customer at the end of the contract only if the customer agrees to procure the device the residual value decided by Sify.
* Ownership of the Managed CPE can be transferred to the customer before the end of contract only if the customer agrees to procure the device at the transfer rate decided by Sify.

## Faulty Managed CPEs Caused by Customer Site Conditions

The customer will be charged for any damage or fault occurring to a Sify owned device due to poor hygiene at location or device burnout due to insufficient Earthing & lack of UPS power. Customer will be charged for replacement of device even if the damage occurs due to unpredictable disasters such as fire or flooding. The price for replacement of the device will be decided by Sify and will depend on device type.

Addition of New Sites, Managed CPEs During Contract Period

Any new sites added over the course of the contract should have the same scope and deliverables as the original set of sites. Customer will need to release separate PO for the additional sites. Sify will aim to protect the price of new locations up to a maximum period of 6 months, post which any new sites added will be subject to price update.

Any change in solution will be treated as a separate opportunity & will have no bearing on the running contract.

## Addition of New Sites, Managed CPEs Post Contract Period

Addition of new sites, devices post the contract period will be considered as a new opportunity. The price of deliverables in the previous contract cannot be used as a reference even if there is no change in the solution.

## RMA Process

The scope of RMA will cover the services under MCPE with Proactive Network Monitoring and Management i.e. hardware provided by Sify & managed by Sify.

## Device Warranties

* The RMA process is undertaken to ensure the return of a faulty product to receive a replacement of repair during the product’s warranty period.
* As standard process, all managed CPE are procured with minimum 1 year of warranty. Any project specific procurements are done with warranty scope as per project.
* Faulty CPE are classified as Dead-on-Arrival (DOA) if a fault is detected during installation within specified period from date of delivery.
* RMA can only be raised when device is in-warranty. Devices are treated as in-warranty during the RMA process even if the actual warranty runs out before the RMA process ends.

# Sify Service Portal: AakaashTM

Sify Aakash is our integrated service platform for our customers and is developed in-house. The capability of the proposed platform today is limited to the Service desk and reporting functionality to Customer and its users.

Sify Aakash Portal is also a customer facing portal that offers integrated view of the Service requests, Network performance Reports, Inventory and trouble tickets that have been registered for the issues reported and identified pro-actively. It allows for seamless flow of information between various reports. This is a web-based portal access to which will be extended to the customer.

The system is completely built on the ITIL model, offering all the functionalities of the FCAPS model. All the incidents and changes are recorded through the system for customer visibility as well as for analysis. The system offers enhanced real-time and scheduled reporting based on defined configuration.

There will be two types of accounts for customers.

* **Admin Account**
  + User Management – This module to onboard and manage site accounts with required features and reports.
  + SLA Management (Monthly SLA Reporting)
  + Service management (Incident / Service / Change Requests)
  + Performance Reporting
  + Topology
  + Dashboards
  + Asset Management
* **User Operator Account**
  + Performance Reporting
  + Reports pertaining only to that site.
  + Asset Information specific to network
  + Device and Link asset details of that specific site
  + Service management
  + Raise incidents / service requests specific to their site.

# Reviews

<CUSTOMER NAME> & Sify shall conduct reviews with preset periodicity along with the Project In-charge, Support Engineers, and Account Manager to review & ascertain the performance of the team & in-scope infrastructure.

# Commercial Proposal

**<<<<<<<<<<<<<< INCLUDE CUSTOMER PRICING >>>>>>>>>>>>>>**

# Information Security Policy

Information is a critical asset for Sify, and it is essential to protect it from unauthorized access, disclosure, alteration, and destruction. This Information Security Policy outlines the principles, guidelines, and responsibilities necessary to maintain the confidentiality, integrity, and availability of information within the organization.

**Policy Scope:** This policy applies to all employees, contractors, third-party vendors, and any other personnel who have access to Sify's information resources.

**Information Classification:** All information assets must be classified based on their sensitivity and criticality. The classification levels are:

* Public: Information that can be freely shared with the public.
* Internal: Information for internal use only, not to be shared outside the organization.
* Confidential: Sensitive information requiring strict controls and limited access.

**Access Controls:** Access to information resources shall be based on the principle of least privilege. Access rights will be granted on a need-to-know basis, considering the employee's role and responsibilities. User access accounts must be promptly deactivated upon termination or change of roles.

**Physical Security:** Physical access to information assets, datacentres, and server rooms must be restricted and monitored. All devices containing sensitive information must be securely stored, and access to these areas must be logged and monitored.

**Network Security:** All network connections to the [Company Name] infrastructure must be secure and compliant with industry best practices. Firewalls, intrusion detection/prevention systems, and other security measures must be implemented and regularly updated.

**Data Encryption:** Sensitive data must be encrypted during transmission and storage. Encryption protocols must align with industry standards, and encryption keys must be securely managed.

**Malware Protection:** All endpoints must have up-to-date antivirus software, and regular scans should be conducted to detect and remove malware. Employees should be educated on the risks of phishing and other social engineering attacks.

**Incident Response:** A documented incident response plan shall be in place to address security incidents promptly. Employees must report any suspected security incidents to the IT department immediately.

**Security Awareness Training:** All employees must undergo regular security awareness training to stay informed about the latest security threats, policies, and best practices.

**Compliance with Laws and Regulations:** Sify is committed to complying with all applicable laws, regulations, and industry standards related to information security.

**Policy Review and Updates:** This Information Security Policy will be reviewed annually and updated as necessary to address emerging threats and changes in the business environment.

**Enforcement:** Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or legal action.

# Standard Terms & Conditions

## General T&Cs

* All pricing provided are exclusive of applicable taxes.
* The contract period will be applicable as per the PO.
* 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.
* Additional Charges are applicable for any additional cabling requirements.
* 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 managed devices.
* Early Termination charges are applicable for any services terminated within the contract period.
  + 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.
  + 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.
  + 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.
* Any requirement of changing the feature tier (if applicable) will result in associated change of commercials.
* Any changes to the Solution design and configuration will result in the design change along with the revised commercials.
* Cancellation or reschedule of site visits (for international locations) within 48 hours’ notice will incur additional charges.
* The provisioning/commissioning of any unmanaged or managed network security services (apart from anything included within the Solution) is considered out of scope.
* All Payment will be as per Sify's payment terms and conditions.
* 24\*7 proactive monitoring and management of the network as defined in the solution document is included.
* 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.
* 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.
* Installation SOW - basic rack & stack, uploading IOS/config file.
* 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.

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 service automatically from the Sixth day.”

## Payment Terms

|  |  |  |
| --- | --- | --- |
| **Billing T&C** | **Notice Period** | **Billing Dispute** |
| Direct Sale: 100% on delivery | 30 days in advance | Billing Disputes to be raised within 15 days of invoice submission. No claims raised later would not be accepted |
| Recurring Charge: Quarterly in Advance | 30 days in advance | Billing Disputes to be raised within 15 days of invoice submission. No claims raised later would not be accepted |

**<<<<<<<<<<<<<<<<<<<<<<< END OF DOCUMENT >>>>>>>>>>>>>>>>>>>>**