

Challenger in Gartner MQ for Managed Hybrid Cloud Hosting APAC 2017

Recognized in Market Guide for Public Cloud Managed & Professional Services Providers APAC 2020

Image result for cybermediaLeadership Award for Network Transformation 2019

**CIO Choice Awards**

Data Center Transformation Services 2018

Network Transformation Services 2018

*Submitted to:*

**Customer Name**

**Managed Network Services Proposal**

The Economic Times Iconic Brands 2020 Hybrid & Multi Cloud

**Date**

A picture containing icon

Description automatically generated

Table of Contents

[2. Document History 5](#_Toc172538933)

[2.1 Sign-Off 5](#_Toc172538934)

[2.2 Document Title 5](#_Toc172538935)

[2.3 Preparation 5](#_Toc172538936)

[2.4 Release 5](#_Toc172538937)

[2.5 Distribution List 5](#_Toc172538938)

[2.6 Statement of Confidentiality 5](#_Toc172538939)

[3. Executive Summary 6](#_Toc172538940)

[3.1 About <CUSTOMER NAME> 6](#_Toc172538941)

[3.2 About Sify Technologies Ltd. 7](#_Toc172538942)

[3.2.1 Business Units 7](#_Toc172538943)

[3.2.2 Differentiators 8](#_Toc172538944)

[3.2.3 Network Capabilities 9](#_Toc172538945)

[3.2.4 Scale of Operations 11](#_Toc172538946)

[3.2.5 What does Sify bring to the table? 11](#_Toc172538947)

[4. WAN Transformation 13](#_Toc172538948)

[4.1 The need of Transformation 13](#_Toc172538949)

[5. In-Scope Managed Services 15](#_Toc172538950)

[5.1 Overview 15](#_Toc172538951)

[5.2 Managed Network Services Description 16](#_Toc172538952)

[5.2.1 Tasks 17](#_Toc172538953)

[5.2.2 Proactive Monitoring 19](#_Toc172538954)

[5.2.3 Incident and Problem Management 20](#_Toc172538955)

[5.2.4 Change Management 21](#_Toc172538956)

[5.2.5 Configuration Management 22](#_Toc172538957)

[5.2.6 Performance Reporting 22](#_Toc172538958)

[5.2.7 Central Helpdesk / NOC 22](#_Toc172538959)

[5.2.8 Link Management 24](#_Toc172538960)

[5.2.9 Router Management 25](#_Toc172538961)

[5.2.10 Vendor Management 26](#_Toc172538962)

[5.2.11 CPE Routers Details 26](#_Toc172538963)

[5.3 Resource Deployment 27](#_Toc172538964)

[5.3.1 Roles & Responsibilities 28](#_Toc172538965)

[5.3.2 Communication Plan 28](#_Toc172538966)

[6. Service Level Agreement (SLA) 30](#_Toc172538967)

[6.1 Management SLA 30](#_Toc172538968)

[6.1.1 WAN Incident Management 30](#_Toc172538969)

[6.1.2 Severity Level Definitions 30](#_Toc172538970)

[6.1.3 Network Severity Categorization 31](#_Toc172538971)

[6.2 Service Window 32](#_Toc172538972)

[6.3 SLA Dependencies 32](#_Toc172538973)

[7. Tools & Processes 33](#_Toc172538974)

[7.1 BeaconTM NMS 33](#_Toc172538975)

[7.1.1 Architecture 34](#_Toc172538976)

[7.1.2 Auto-Discovery 34](#_Toc172538977)

[7.1.3 Topology Maps 35](#_Toc172538978)

[7.1.4 Fault Management 35](#_Toc172538979)

[7.1.5 Trouble Ticketing 35](#_Toc172538980)

[7.1.6 SNMP Traps 35](#_Toc172538981)

[7.1.7 Alerts and Escalation 36](#_Toc172538982)

[7.1.8 Event Viewer 36](#_Toc172538983)

[7.1.9 Performance Management 37](#_Toc172538984)

[7.1.10 Comprehensive Reporting 38](#_Toc172538985)

[7.1.11 SLA tracker 38](#_Toc172538986)

[7.1.12 Administration 39](#_Toc172538987)

[7.1.13 SNMP support 39](#_Toc172538988)

[7.1.14 Port monitoring 39](#_Toc172538989)

[7.1.15 Secure 39](#_Toc172538990)

[7.1.16 Data Persistence 39](#_Toc172538991)

[7.1.17 Simple 39](#_Toc172538992)

[7.1.18 Scalability 39](#_Toc172538993)

[7.1.19 Monitoring Parameters 40](#_Toc172538994)

[7.2 Sify’s Service Portal: Aakash 40](#_Toc172538995)

[7.2.1 Aakash: An Overview 40](#_Toc172538996)

[7.2.2 Aakaash: Service Screens 41](#_Toc172538997)

[8. Reviews 48](#_Toc172538998)

[9. Commercial Proposal 49](#_Toc172538999)

[10. Terms & Conditions 50](#_Toc172539000)

# Document History

## Sign-Off

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Company** | **Name** | **Designation** |
| Author | Sify Technologies Limited |  | Solution Architect |
| Client Management | Sify Technologies Limited |  | Account Manager |
| Project Owner | <CUSTOMER NAME> |  |  |
| Project Sponsor | <CUSTOMER NAME> |  |  |

## Document Title

|  |  |
| --- | --- |
| **Customer** | <CUSTOMER NAME> |
| **Title** | Approach Proposal document on WAN Transformation |
| **Document Name** | <CUSTOMER NAME> - WAN Transformation Approach v1.0.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 |  | þ |  |
| Sify Technologies Limited |  | All | þ | þ |  |
| Sify Technologies Limited |  | All | þ | þ |  |

## Statement of Confidentiality

|  |
| --- |
| This document contains proprietary trade secret and confidential information to be used solely for evaluating Sify Technologies Limited [“Sify”]. The information contained herein is to be considered confidential. <CUSTOMER NAME> 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

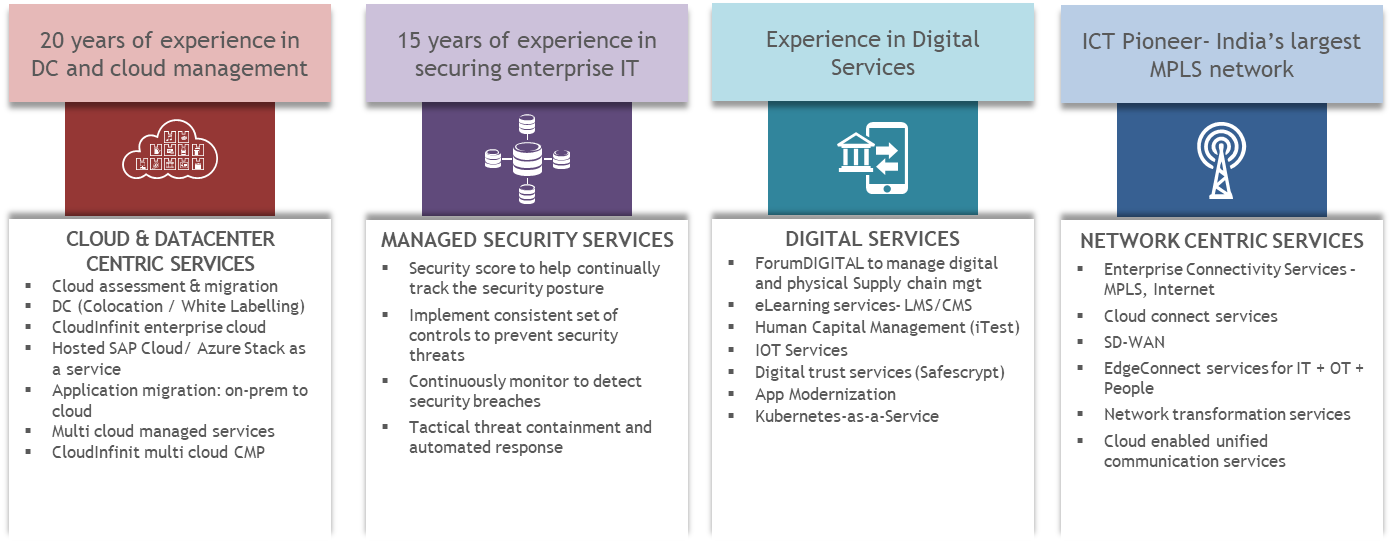
## About <CUSTOMER NAME>

## About Sify Technologies Ltd.

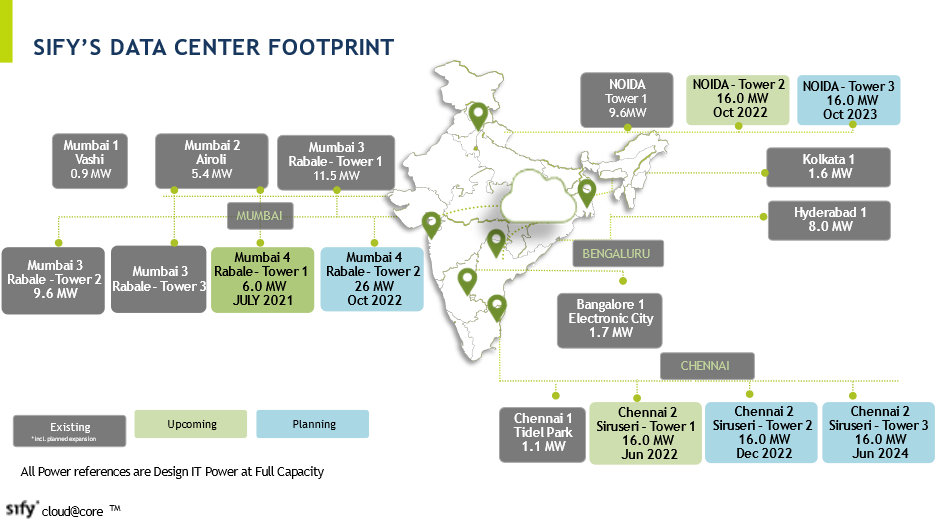
A Fortune 500 India company, Sify Technologies is India’s most comprehensive ICT service & solution provider. Sify being Digital at Core in our solutions portfolio, Sify is focused on the changing ICT requirements of the emerging Digital economy and the resultant demands from large, mid and small-sized 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 Data Centers, 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. .

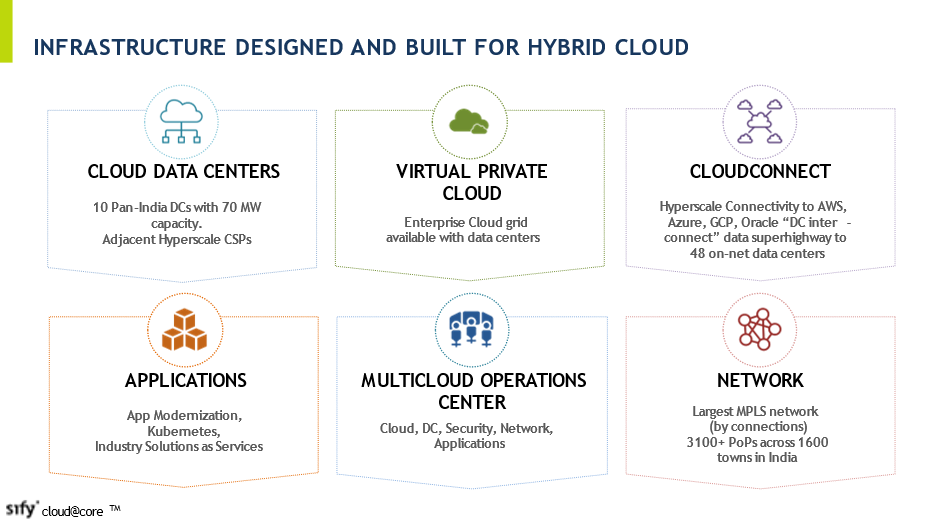
### Business Units

****

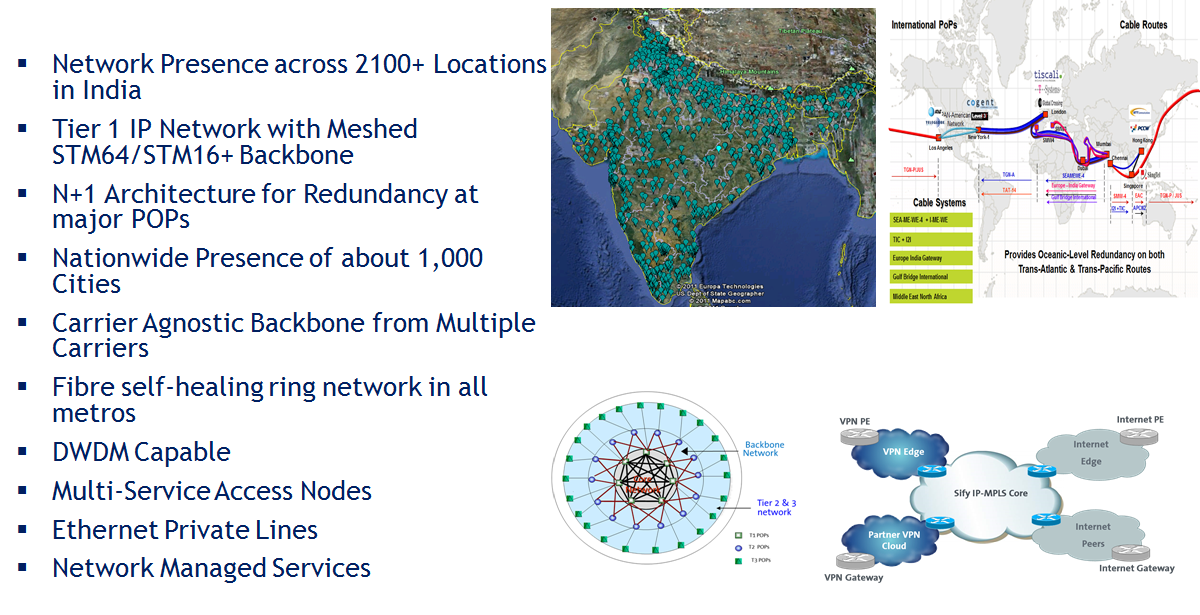
#### Sify’s Data Center Footprint



**Infrastructure designed and built for Hybrid Cloud**



#### Network Services



### Differentiators

Network Services

Pioneered in building and managing complex Networks. Managing 80000+ endpoints. Commissioned World’s largest MPLS Network.

Data Center Services

20+ years of experience in Build, Own, Operate Carrier-Neutral Data Centers. Truly carrier neutral, with multiple Internet Exchange ecosystem facilitating OTT and ISPs interconnect via portal.

Comprehensive Cloud Portfolio & Strategy

Cuts across, advisory, implementation & transformation.

Disaster Recovery

Experience of setting up / running disaster recovery infrastructure on a private / DRaaS model

Security Services

500 Devices, 140 Customers managed from SOC. Strong Information security and System Integration practice

Managed Services

20+ years’ experience in running DC, DR, Network, Security, Applications on Managed Services Model

Technical Skills

Credible partner with technical skills across the ICT spectrum, including software. Highly skilled team with expertise around all OEM products, Tools and services

Service Provider Agnostic

Neutral Player with Access to all Service Providers

Executive Commitment

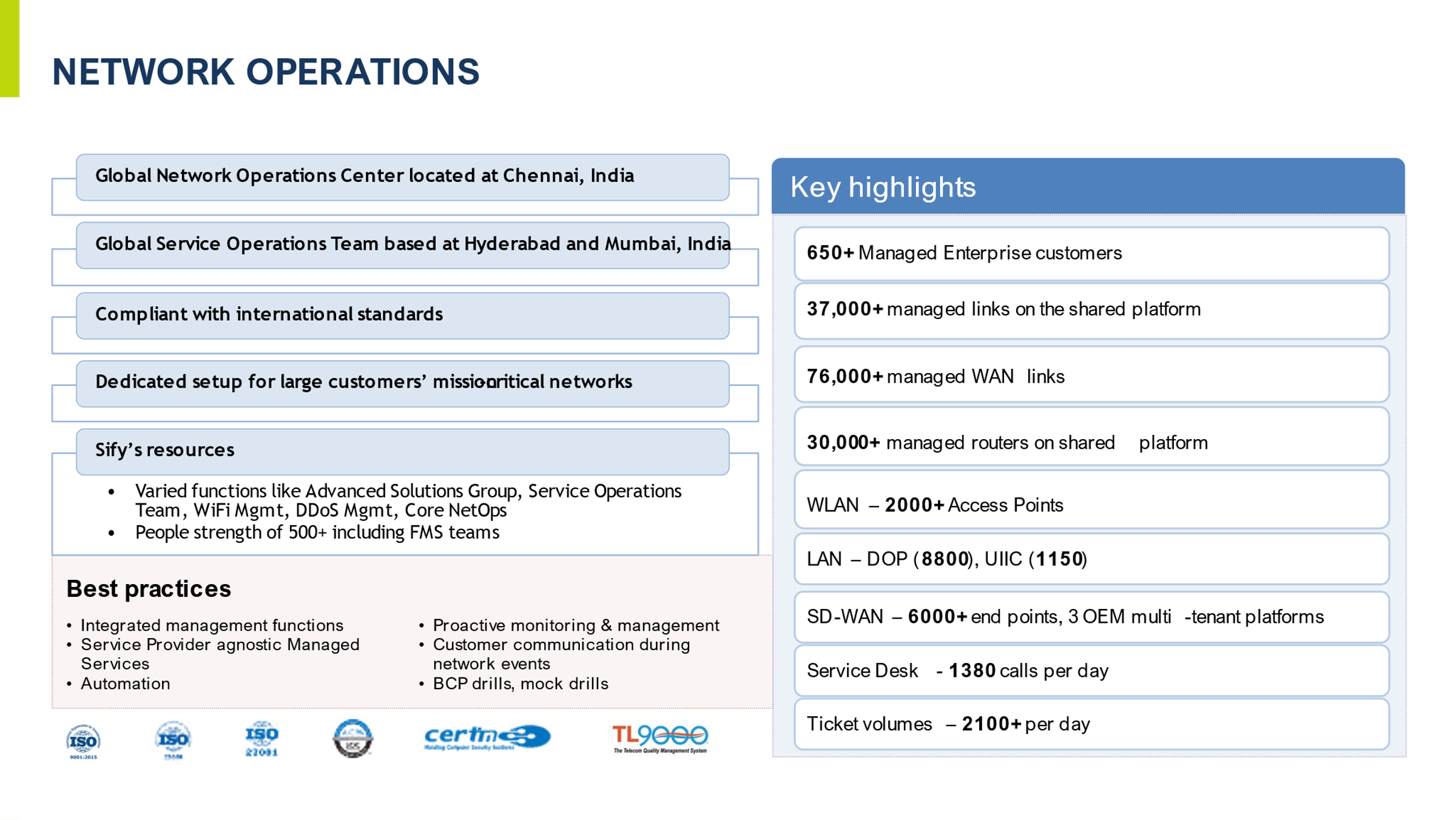
This engagement has the executive leadership commitment being led by the CEO

### Network Capabilities

Sify has developed expertise over a decade of designing, engineering, managing, and administering world-class networks. Our capabilities are detailed below.

|  |  |
| --- | --- |
| 1. Network Engineering & Design  * Requirement gathering, concept build * Project detailed SOW – develop and sign-off * Develop Network High Level Design * High Level Design Review * Develop Low Level Design * Documentation, Reviews * Project milestone reviews and sign-off * KPIs:   + Project Milestone based timelines   + Design compliance to gathered business input |  |
| 1. Network Implementation & Integration  * HLD documentation and review * Low Level Design documentation * Impact and risk assessment * LLD Review and Nodal Configuration development * Configuration testing at staging * Implementation and Integration * Design validation, UAT, Sign-off * KPIs:   + Project Milestone based timelines |  |
| 1. Network Migration & Transition  * Requirement gathering * Motivation, expectations – documentation * Pre-Migration statistics and configuration dump * Risk analysis and mitigation methodology * Rollback methodology * As-is and to-be documentations * Migration & transition * Post-Migration analysis, review and sign-off * KPIs:   + Project Milestone based timelines   + Compliance to expected results |  |
| 1. Network Audit & Optimization  * Network Study and documentation * Architectural review * Business expectations and known issues - doc * Audit reporting, analytics and compliance reports * Best practices and optimization recommendations * KPIs:   + Project Milestone based timelines |  |
| 1. Network Infra Management  * Central Network Operations Center – 24x7 * Fault Management * Incident & Problem Mgmt. * Proactive Monitoring – Device, Environ, back-bone links, NNI. * Problem, Change & Configuration Mgmt. * Vendor, Asset & Patch Mgmt. * Security, Accounting & Compliance Mgmt. * Tools – NMS, Incident handling, Service reporting * KPIs:   + Mean Time to Respond, Mean Time to Resolve   + Service portal and backend system availability   + Availability of NOC, Reactive vs. Proactive tickets | noc |
| 1. Advanced Technical Support  * Level-2 and Level-3 technical support * Subject matter expertise – Focused Technical Support * Vendor co-ordination, Vendor TAC - interfacing * On-site co-ordination for ATS program * Tools – Problem analysis and troubleshooting * Network Change review board * KPIs:   + Mean Time to Respond, Mean Time to Resolve,   + Change review – TAT |  |

### 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 the 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>.

# WAN Transformation

## The need of Transformation

Customers deploy their own tools internally within their data center or operations center for monitoring & management of the IT landscape. Here are seven signs that network management becomes too heavy for enterprise to handle on its own:

1. Lack of Management Tool or Low use

The proper selection, configuration, management, and use of network management tools require specialist skills. Poor use of these tools can result in, at best, a lack of diagnostic support information, and at worst, incorrect or misleading information, which defeats the object of having them. Management tools are also expensive to have in-house if large number of assets does not exist.

1. Use of Technology to its Fullest

IT division is just too small to properly run and manage all advanced technologies, so the return on those investments remains unrealized. The vendors who supplied these technologies can’t help either because their contracts don’t include operational management.

1. Lower Service Levels & Increased Downtime

IT division works in crisis mode all the time, so keeping network up and running leaves no time to make improvements. Of course, dedicating entire resources to improvement is out of the question because more resource deployment is constantly to fight fires. All of this leads to increased downtime, poor change and event management, and extended repair times when things go wrong.

1. Escalating Cost

It’s becoming more and more expensive to manage network in-house because of lack of scale in ICT division. Hiring expensive experts to deliver low-end services leads to budget constraints to make a distinction in skills levels. Everyone ends up doing everything with a higher risk of downtime.

1. Business Unit Head

Often, Business unit sources IT-as-a-service option directly from a provider without involving the ICT division. The perception is that the service business unit gets there is more responsive and prompt, and therefore suits their immediate requirements better.

1. Better ICT experience at Home

Today’s employees tend to be more technology savvy and connected at home than before. As a result, employees are more demanding and have a low tolerance for inconsistent services or underperforming technology.

1. Customer Complaints

Without improving infrastructure with strategic and tactical considerations in mind, it’s hard to keep competitive edge. IT Division starts to fall behind the market in terms of launching new service offerings to business.

# In-Scope Managed Services

## Overview

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-art 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 to its customers with a visibility to even the minute details of their infrastructure. The complete management service is offer from Sify's state-of-the-art Managed Services Operations Center [MSOC].

Sify monitoring interface will is available over internet as support portal for customer to logon 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. MSOC 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, MSOC would extend their support in the form of vendor coordination.

This service is offered to <CUSTOMER NAME> 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.

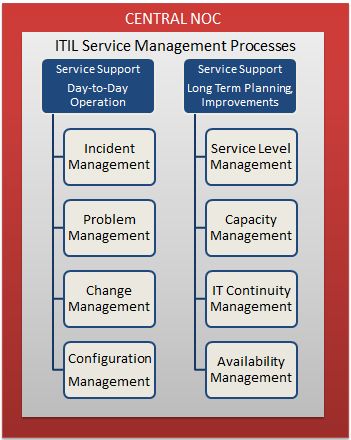
## Managed Network Services Description

Sify’s Managed Network Services offers 24x7 remote monitoring and management of Enterprise Customer Infrastructure. This service is delivered by Sify’s specialized technical team, to ensure that the infrastructure & services are always 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 outages.

Key Features

* Covers range of devices from leading vendors supporting various business needs
* Single point of ownership – end to end SLA
* 24x7 monitoring and management by specialized technical team

Sify’s skilled team of certified architects provide complete onsite and remote support for the management of customer’s infrastructure thus providing maximum assurance to service availability and performance. This offers the customers 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.



|  |  |
| --- | --- |
| **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 | |
| SLA Parameters | Mean time to Respond  Mean time to resolve  Service uptime |

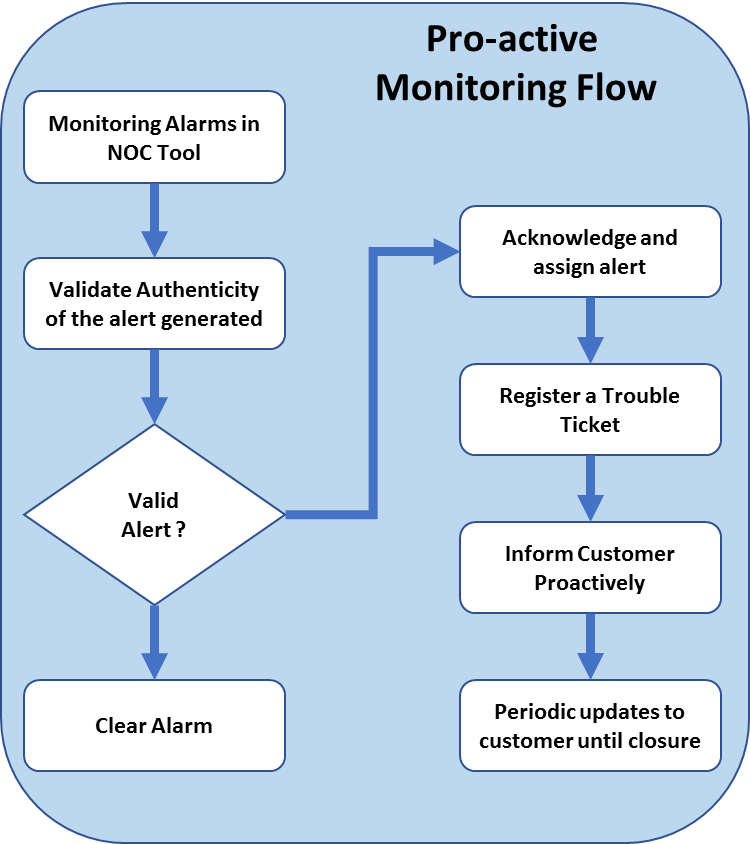
### Tasks

Tasks handled under proactive monitoring and management

* Implementation Services
  1. New Link
  2. Link Shifting
* Transition Services
  1. Service Migration
* Proactive Monitoring
  1. Problem Management
  2. Capacity Planning
* Service Desk, Incident Reporting & Management
  1. Trouble ticketing
  2. Fault Management
  3. Performance Management
* Inventory Management
  1. Asset Database
  2. Knowledgebase
* Change Management
  1. Change Management Database
  2. Configuration Management
* Reporting
  1. Online Reporting
  2. MIS Reporting
* Scheduled Maintenance
* Vendor Coordination
  1. Service Providers

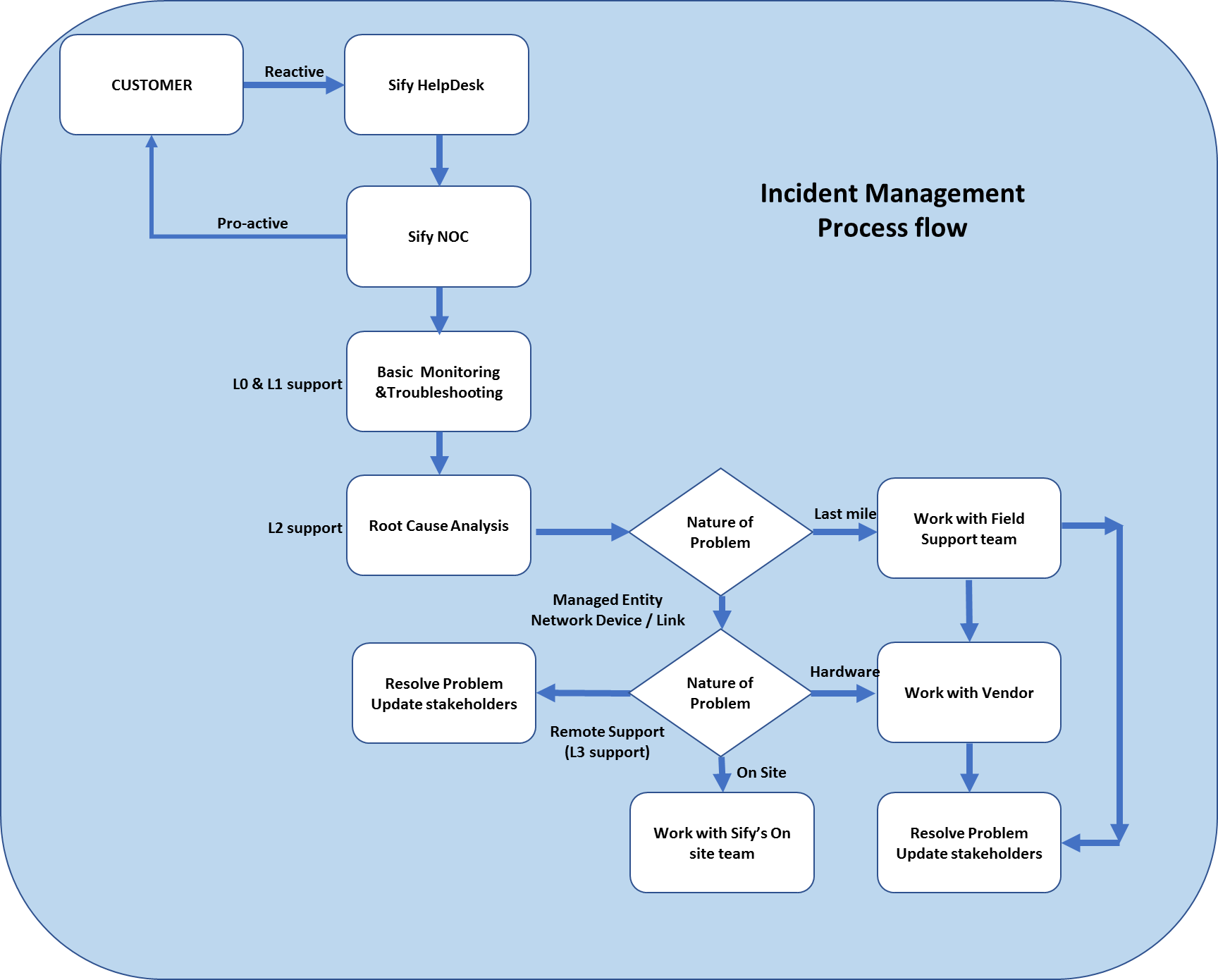
### Proactive Monitoring

* Monitor all <CUSTOMER NAME> related infrastructure using the Network Management System.
* Monitoring the availability of the Network.
* Register a trouble ticket with the help desk for pro-actively identified outages / anomalies.



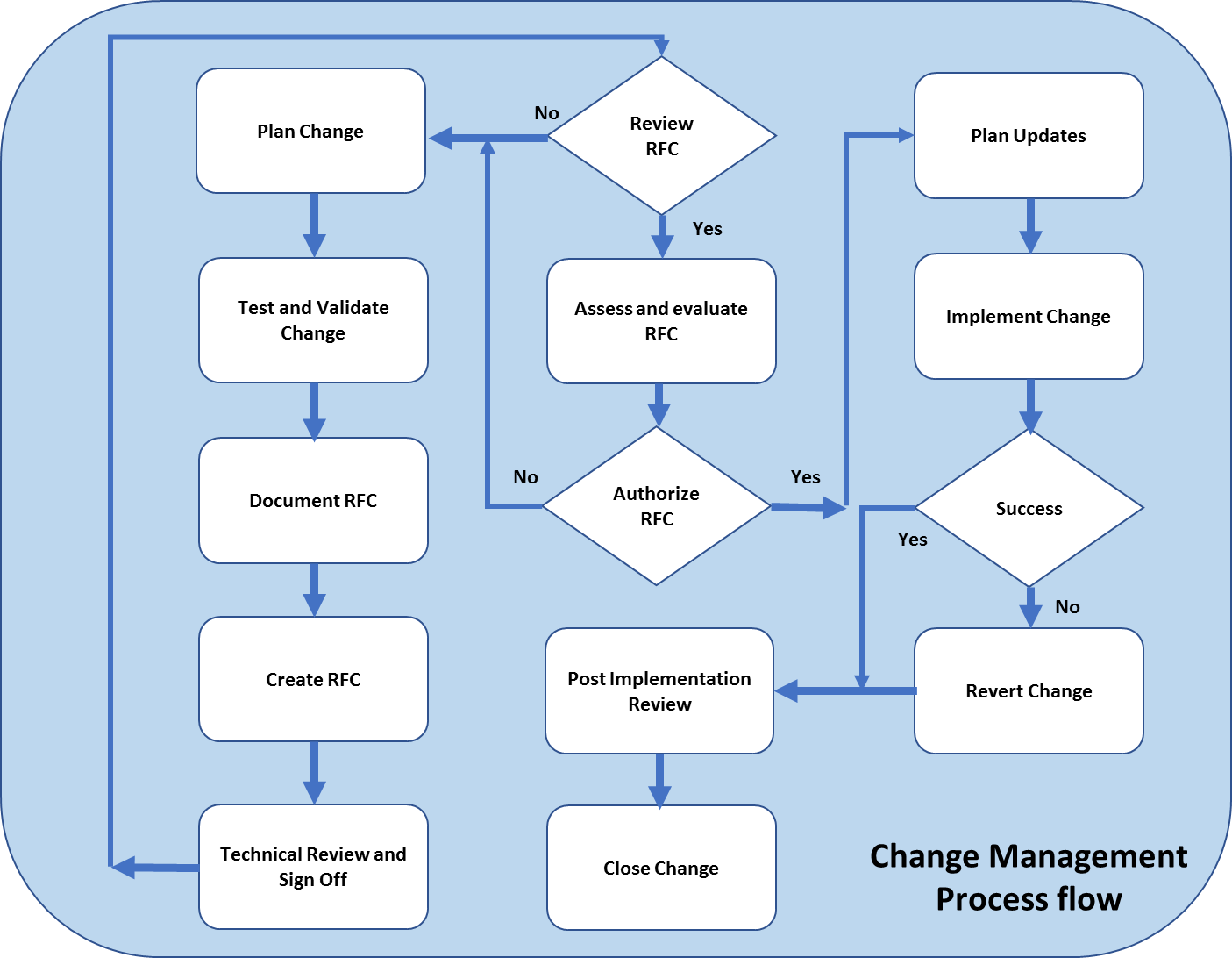
### Incident and Problem Management

* Handle all trouble tickets that have been pro-actively registered
* Incident handling and problem resolution
* Root cause analysis and RCA reporting
* Work with SP vendors, as applicable, for achieving the SLA
* Provide regular reports on Network Operations as requested by <CUSTOMER NAME>
* Work with vendors, field operations, <CUSTOMER NAME> internal or any other interface to restore outages to the network



### Change Management

* Initiate change requests
  1. All change requests would be initiated through the ticketing portal and customer would be intimated for his due approval
* Communicate change requests to the customer for approval
* Perform scheduled and emergency changes as applicable
* Perform post implementation review
* Carrying out changes in the Network as approved in the Change Management
* Increasing or decreasing the Bandwidth
* The following activities, in coordination with the field operations team will be performed:
  1. De-commissioning of Networks where <CUSTOMER NAME>’s office operations cease
  2. Shifting of offices – necessary movement of equipment, shifting of circuits etc.
  3. Addition of new offices to the Network



### Configuration Management

* Periodic back up of device configuration
* Maintaining a backup library
* Online auditing of configuration changes per device
* Configuration restoration

### Performance Reporting

* Provide performance reports on the following metrics
  1. Device statistics

1. CPU and Memory performance
   1. Link statistics
2. Bandwidth utilization
3. Threshold violations
4. Errors
   1. Service statistics
5. Latency
6. Packet Loss
7. Jitter

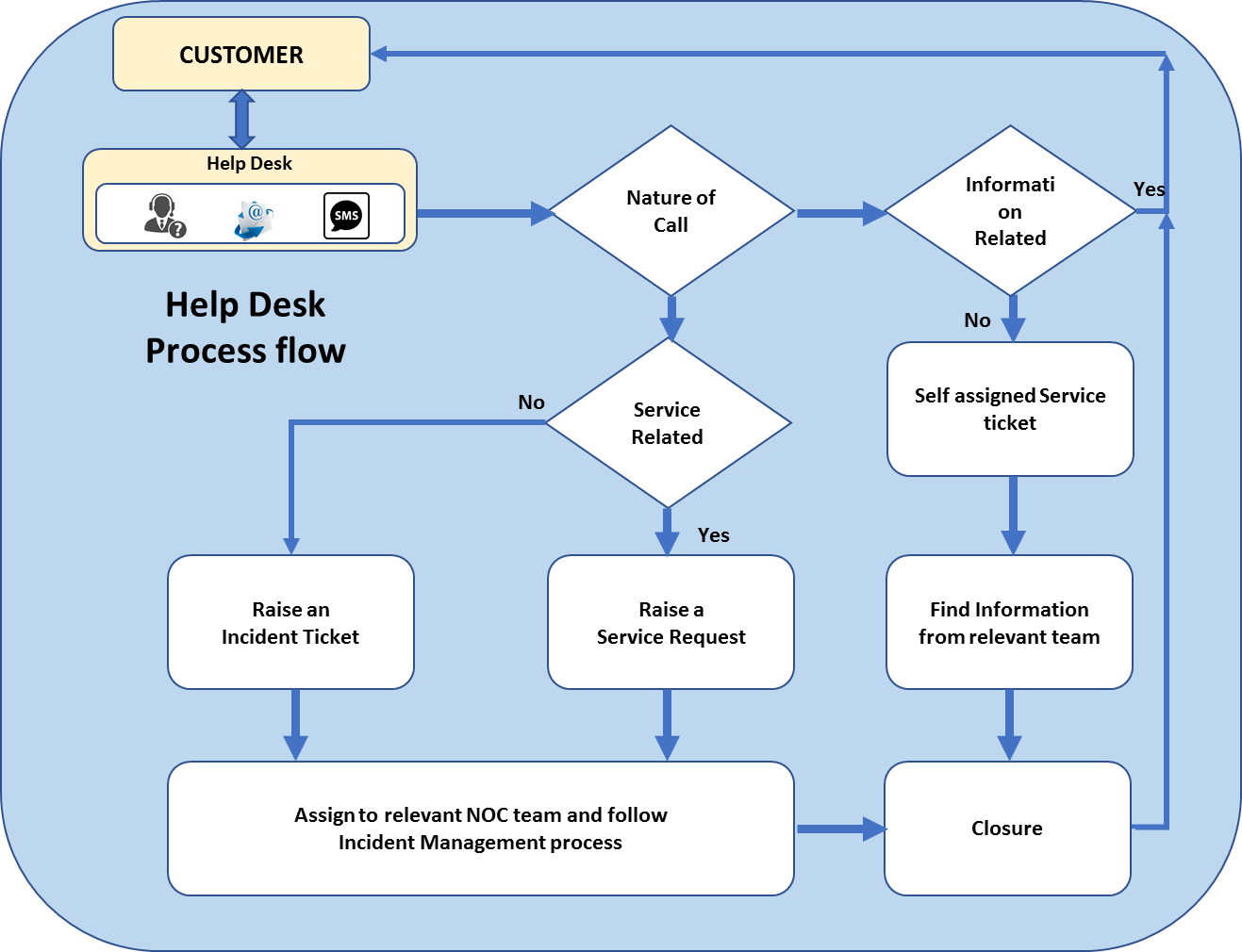
* Provide regular reports on network utilization and trending analysis
* Availability reporting will be made available through the trouble ticket system.

### Central Helpdesk / NOC

* The central helpdesk will be the first point and single point of contact for all issues in the network
* The helpdesk team will be responsible to registering trouble tickets in the ticketing system pro-actively / reactively, as required
* The team will be responsible for internal / external escalations to ensure a reported incident is resolved quickly

Besides all the above activities, the NOC team will also be responsible for the following activities:

1. Inventory Management
2. Establishing a process of regular tests on redundant links and submit reports on their stability, convergence times etc.
3. Service Providers Vendor Coordination
4. Other activities as decided & mutually agreed between <CUSTOMER NAME> & Sify.



### Link Management

WAN links is another of the important and critical component to connect the remote branches the centralized data center 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 the access * SNMP security | * Notification through Email / Phone. | As on needed |

### Vendor Management

All projects are executed with the help of Service Provider & OEMs. Each vendor plays a very important role in the project and is a very important stakeholder in the success of the project. Each vendor ideally should be handled as a separate project as they need to be evaluated on a continuous basis and scoping and controlling becomes a continuous part of vendor management. 90% of the components are vendor driven which is why it is obvious that any lapses in vendor management can skew the project. Sify has a proven evaluation process and separate set of specialized people who are focused on Service Provider relationships on an ongoing basis.

This scope is considered only for the Service Provider as a vendor. The router AMC and its vendor management or <CUSTOMER NAME> SI partner will continue by <CUSTOMER NAME>. Sify will notify <CUSTOMER NAME> team for any hardware related problem.

### CPE Routers Details

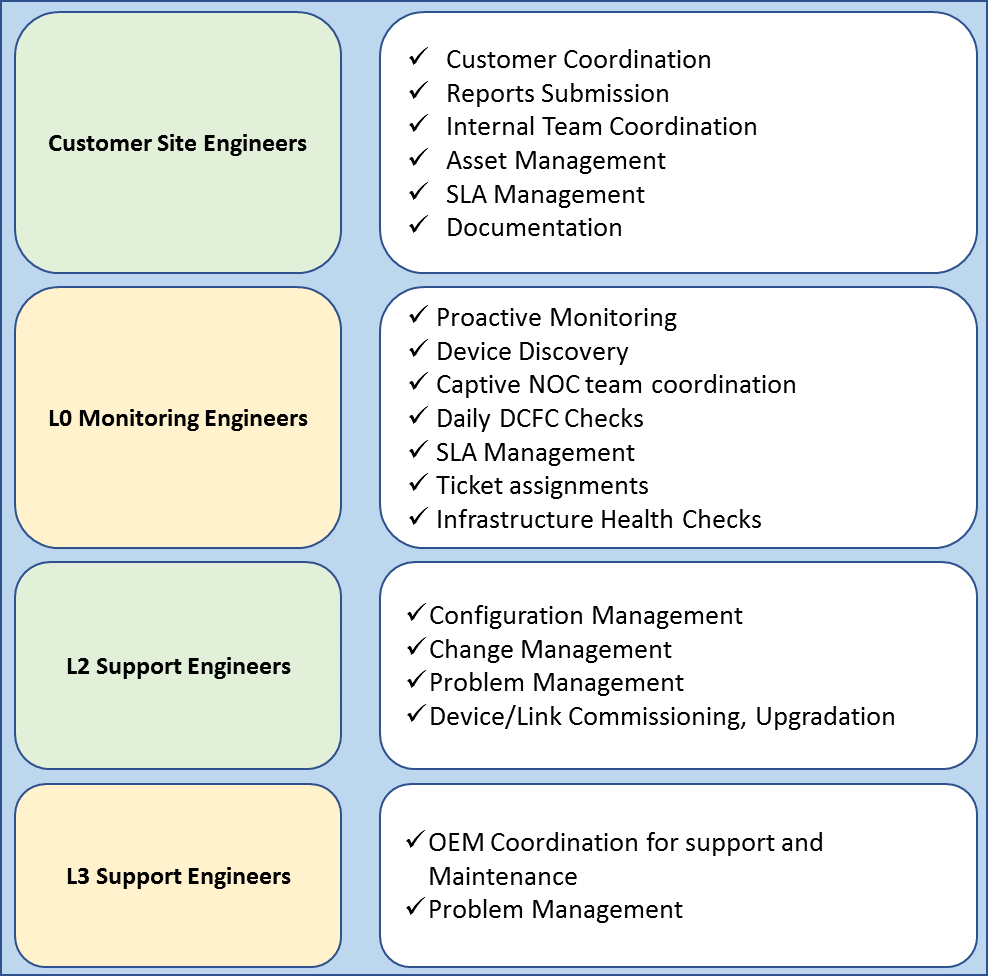
As per the inputs shared by the <CUSTOMER NAME>, every remote site and the Service Center sites are provisioned with single CPE router. Appropriate WAN modules with serial interface for the BSNL links and RJ45 Ethernet handoff for WAN & LAN are considered in the present CPE Routers.

|  |  |
| --- | --- |
| **Total CPE Router Details** | |
| **Remote Sites + Service Center** | |
| Make & Model | Count |
| Cisco ISR4431/K9 & Cisco ISR4431-SEC/K9 | xxxxxx |
| CiscoRV042 | xxxxxx |
| Grand Total | xxxxxx |

## Resource Deployment

Project execution directly depends on the quality and quantity of the resources keeping in mind the costs. Too many or too less resources can affect the delivery adversely. Hence, a careful selection of experienced people coupled with the right combination would ensure expected results. Finally, it is the ability of the project manager to bring all these skilled resources to deliver the desired result with the help of proven methodology. The Sify project team for this project and their roles are included below.

|  |  |
| --- | --- |
| **Position** | **Role** |
| Sify Project Manager | Responsible for reaching the goals and fulfilling the objectives of the project, within the time limits, costs defined by the <CUSTOMER NAME> and Sify management.  During the project, the Project Manager is the first line interface between <CUSTOMER NAME> and Sify Management. The Project Manager will therefore act diligently and honestly in all such dealings and will encourage, motivate project team members to act likewise. Project Manager will also do a timely escalation to the sponsors of the project |
| Central Helpdesk | First level of contact for day-to-day operations of the network for onsite engineers.  Escalates to appropriate level within the stipulated time frame on non-compliance of agreed service levels. |
| Onsite Engineer (L1) | First level local contact for customer.  Provide remote hands & feet support to NOC.  Initial troubleshooting of the network issues.  Report generation based on <CUSTOMER NAME> requirement / reporting frequency. |
| Field Support Engineers | Remote hands support for Onsite Transition Engineers.  Responsible for on-field support for SLA adherence.  Service Provider coordination for troubleshooting & fixing up errors & failures. |
| Sify Sales Account Manager | Overall relationship is maintained between <CUSTOMER NAME> and Sify during the project. The Account Manager will also be responsible for ensuring any commercial change arises due to change in scope to be taken up with <CUSTOMER NAME>. Actively participates in review process. |



### Roles & Responsibilities

Each resource in the project team on either side is designed to carry out specific tasks. If not communicated well, the project can go for a toss. Hence, before we begin execution, clear definition of roles & responsibilities on either side is a must.

### Communication Plan

All communication between the NOC and the other internal teams within Sify will happen through the Trouble ticketing system. The NOC team of Sify would have access enabled and extended to the Sify trouble ticketing system through which all incidents will be recorded. Any assistance required from the field teams and the off-site NOC team will be directed to the respective teams through the reassignment of the ticket to the relevant teams in the system.

Once reassigned, the regular Sify trouble ticketing process would be followed by the respective teams. Any updates made in the trouble ticket will be visible to the NOC team at the HO.

Over and above the trouble ticketing system, the teams will also interact through E-mails and telephone calls, as needed and applicable.

The process the NOC team would follow in handling an incident is detailed below at a high level. All the communication between the NOC team and the other respective teams (Off site) will happen through the trouble ticketing system.

All escalations to the <CUSTOMER NAME> requiring their action will be done through an E-mail and a telephone call. All such tickets that require <CUSTOMER NAME> attention will be tagged as “Awaiting <CUSTOMER NAME> response” status. If the activity requiring <CUSTOMER NAME> escalation is out of the scope of the NOC team, the corresponding ticket will be closed and the issue will be pursued separately on E-mails.

# Service Level Agreement (SLA)

## Management SLA

During the transition phase, Sify will create the SLA for ongoing service delivery based on the achievement feasibility and review.

### WAN Incident Management

|  |  |
| --- | --- |
| **SLA Attributes** | **SLA Indicators** |
| Incident Notification | Severity 1 - 15 mins  Severity 2 - 30 mins  Severity 3 – 60 mins  Severity 4 – Online |
| Incident Response | Severity 1 - 15 mins  Severity 2 - 30 mins  Severity 3 - 60 mins  Severity 4 – 120 mins |
| Service Level Adherence | > 98% |
| Sify GNOC Availability | > 99.90% |
| Sify AAKAASH Service Portal Availability | > 99.50% |

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

### 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

### Network Severity Categorization

|  |  |
| --- | --- |
| **Incident** | **Severity** |
| Severity 1 | * Outage Network Down (WAN)   1. Power issue at the site   2. Router failure   3. Link Down (cable failure) |
| Severity 2 | * Line Closure * Line Upgrade * New Line * Performance Issue   1. Link Latency   2. Link Reliability   3. Packet Drops * Routers   1. HA Configuration at the site   2. IOS Upgrades |
| Severity 3 | * Configuration Issue   1. Route Addition   2. Route Deletion   3. ACL’s |
| Severity 4 | * Reports Generation |

## Service Window

* 24 x 7 x 365 remote monitoring and management for network devices.

## SLA Dependencies

All incidents and problems will be resolved within the time frames as described in the section above. The resolution time frame is not applicable if the resolution is dependent on the following:

* External providers
* Due to delays in response or request from users
* Hardware [Routers] / Software failures or replacements or upgrades
* If the resolution requires a change and the change request is pending for approval.

# Tools & Processes

Industry-standard, well-accepted processes and frameworks govern each aspect of Sify’s service offerings. The adoption of all these tools and processes ensures that Sify makes a palpable difference to customers in its continual quest towards attaining higher levels of security, network management and service delivery standards.

Sify’s processes conform to the ITIL framework for service management. ITIL provides for a cohesive set of best practices drawn from the public and private sectors internationally. First introduced in the 1980’s, ITIL is now the defacto global standard for IT service management. These processes have been developed for the special requirements involved in running mission-critical IT infrastructure that needs to be operational 24x7x365. The processes are exhaustively documented and Sify is certified in ISO 9001:2000 in Network Operations, Data Center Operations and Customer Relationship Management. Sify has achieved process maturity through an unrelenting commitment towards constant enhancement of the customer experience. The ISO 9001:2000 certification is an affirmation of our commitment to continuing excellence in our quality management processes. We have Six Sigma initiatives ongoing in our customer support division as part of our goal to ensure customer delight.

Sify’s service delivery methodology, developed and honed through engagements with global clients, comprehensively covers service level management, capacity and availability management and continuity management. Clearly documented processes for service support, covering configuration management, change management, release management, incident management and problem management, complement this.

Sify supports all leading infrastructure management platforms and has a diverse pool of engineers with hands on experience in infrastructure management. Sify uses powerful customizable tools and applications along with methodologies and processes to deliver high-quality services to increase network/data availability and optimize performance.

Sify follows Six Sigma program to achieve quality for the services it provides to customers. It is a measure of quality that strives for near perfection. Six Sigma is a disciplined, data-driven approach and methodology for eliminating defects in any process. Sify uses the statistical representation of Six Sigma to describe how a process is performing. Using the Six Sigma methodology, Sify has implemented a measurement-based strategy that focuses on process improvement and variation reduction through the application of Six Sigma improvement projects.

Sify uses six sigma tools like failure mode effect analysis (FMEA) to identify potential failure modes for a product or process, to access risk associated with those failure modes, to rank the issues in terms of importance and to identify and carry out corrective actions to address the most serious concerns. Sify ensures proper and stable service delivery by analyzing potential risks and addressing them on time.

## BeaconTM NMS

BeaconTM is one such tool, which is born out of Sify’s quest of continued adoption of industry-standard practices and tools. It is Sify’s in-house developed, comprehensive network management solution (NMS). Beacon™ provides an expertise driven approach that combines best-in-class network management software with process know-how and training.

### Architecture

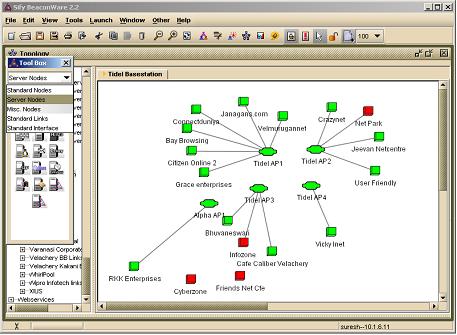
The NMS consists of the following modules:

* NMS Station
* NMS Data Poller
* NMS Database
* NMS Client
* NMS Web Server

The NMS Station is an NMS server, which acts as the nerve center for the entire network management system. It houses the database also. NMS Data Pollers, installed at various optimal points of the network, are responsible for checking the health and performance of a set of devices, links and applications and reporting this back to the NMS Station. The decision to install the number of pollers is a function of the number of devices being monitored and the reachability of the devices from the central location. NMS clients will enable remote access to the NMS server for configuration, administration and for monitoring real time the state of the network. The Client part of the software can be installed at each of the locations and is used to view the state of the network.

### Auto-Discovery

Once installed, NMS will setup your network map. It will automatically discover all network devices, links and associated interfaces. These are then mapped diagrammatically as a topology. The discovery can be for a range of IPs or for specific IP addresses. The discovery mechanism does an SNMP walk and ping sweep of the entire network. The utility also classifies the discovered devices and application according to name and type. This utility comes of great use when configuring a complex network for monitoring. This facility of Auto-discovery can be used to map out all the devices to be monitored in the network without any effort. Auto-discovery process also grabs the details of the various ports of the devices and the details linked to the same.



### Topology Maps

Multiple topologies consisting of resources and their linkages can be setup in the system for reducing the visual complexity of the network. A background image can also be setup to provide a geographical basis for the network map. Drill down topology is possible. Herein the top-level topology can be mapped out and then hyper linked to the detailed topology, which forms the downstream part of the network. This results in easy manageability. Visual alerts can be seen on these graphical views so that topologies having error conditions stand out to the network manager. A single device can belong to multiple topologies thus clearly indicating to the manager how degradation in its performance affects different sets of resource groups.

### Fault Management

At any point of time the complete network can be viewed through the Topology Browser. The status of all the network elements and links are displayed on the network map itself enabling the network administrator to easily identify problem areas and take steps to solve them.

NMS has a sophisticated Fault Management system designed to ensure high network availability and minimize outage. Each device on the network can be assigned thresholds, which define the standards for normal operation. Data pollers strategically positioned at various points of the network continuously monitor these devices on the parameters defined. If any of the parameters exceed a threshold, an alert is generated.

Further for easy usability the Event Viewer, which is a dynamic log of all activities in the network, is linked to the Topology. Thus when viewing a topology the Event Viewer for that topology at the bottom of the screen gives online status of the network. Also, when while in the event viewer, the user can automatically move the specific device in the specific topology by choosing the option on right click. The Event Viewer also provides quick short cuts to Quick Status, Instant Poll, Locating Duplicates, and Ping etc. for access maneuverability. Apart from this, it also offers an option to Detect Links from the associated device, which is useful for plotting and discovering the network.

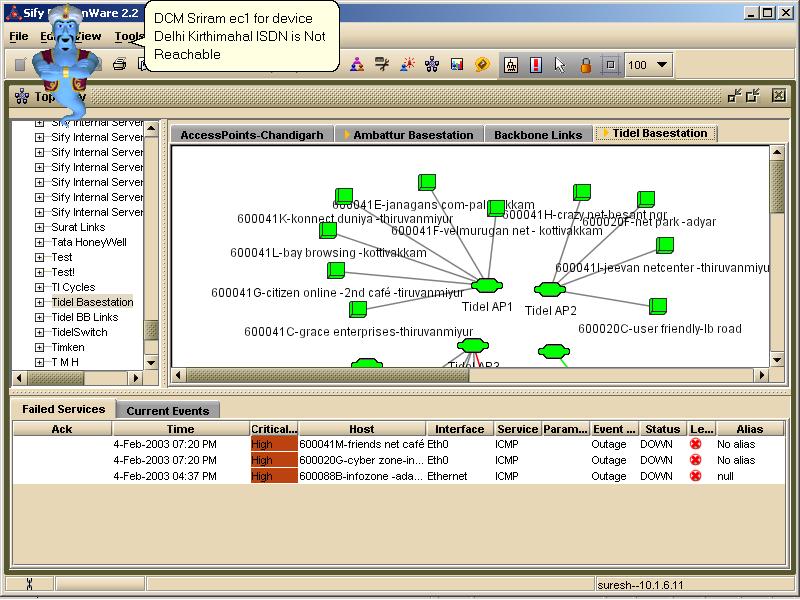
### Trouble Ticketing

All alerts can be automatically recorded in the form of a trouble ticket and the ticket can be assigned to the appropriate team to work on. When an alert is shown in the NMS the monitoring operator can either manually raise a trouble ticket in one click on the monitoring client or the NMS can be configured to raise trouble tickets for each exception reported. The trouble ticket system can be configured to send e-mails to a pre-defined list and also follows an auto-escalation mechanism in case problem resolution time frames exceed pre-set limits.

### SNMP Traps

NMS now supports SNMP traps. SNMP (simple network management protocol) has a facility by which the SNMP agent in the device itself sends across a message to the manager (NMS) whenever some predefined event occurs. This facility helps reduce the polling frequency as the event gets notified the moment it occurs.

Link Up / Down traps are the most useful of all the SNMP traps. Herein the router sends across a trap to the NMS as soon as one the link goes down. As a result, NMS will immediately alert on any link outage.



### Alerts and Escalation

Alerts are graded in terms of seriousness and appropriate action is taken to inform the network administrator of the problem. Alerts are available in different modes viz.

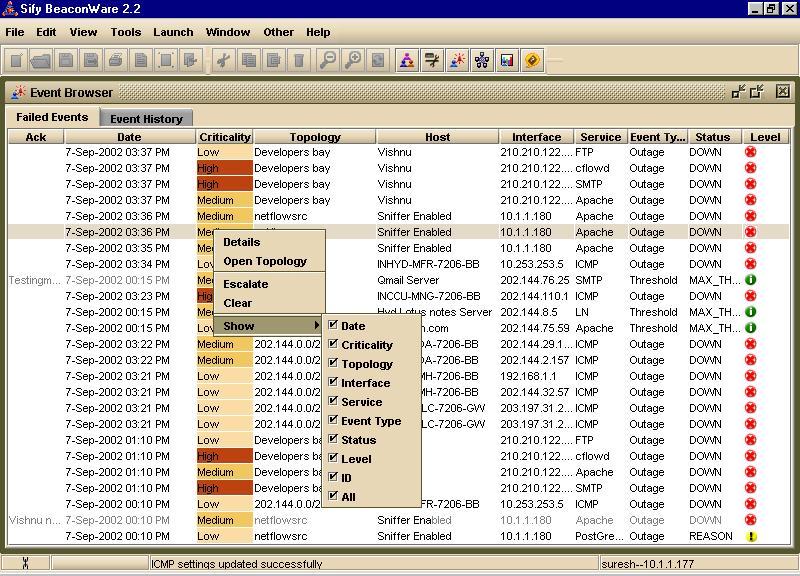
* Message Popup
* Text-to-Speech voice alerter
* Playing a voice file
* SMS or E-mail

In case, the problem is serious and not resolved within a specified time frame, NMS will intelligently escalate the alert to the next level in the escalation hierarchy using email and SMS. Escalation charts can be setup for each network device or service indicating the escalation hierarchy. The escalation hierarchy is completely customizable - different escalation charts can be specified for different types of alerts –for intimating an outage or threshold exception for each device or application. NMS also monitors the connection of Poller(s) and intimates the same to the user.

NMS offers the option of creating, using and assigning multiple Escalation Charts and assigning them to network devices or services as required. Further the charts offer the flexibility to incorporate the days of week with time when the escalation is to be disabled along with facility to mute escalations on specific days (like public holidays) of the year.

### Event Viewer

An Event Viewer is provided for viewing the detailed events logged. Alert details, severity of problem and the current status is displayed in the event browser along with details of different information that the system records dynamically.



Events can be filtered based on the seriousness of the event - so that only the events relevant to the user are displayed. For each event about an outage or a threshold violation, there is a corresponding event generated when the normalcy is achieved. The user has the option of viewing only the failed devices at that particular point of time. A drill down facility is supported where users can always find out more about an event by double clicking on it.

Users can now directly do the following from the Event Viewer:

* Escalate
* Open Topology containing a specific device
* Create trouble tickets
* Manage view of event viewer
* Acknowledge an event, which will carry the user’s name (login name) and time of acknowledgement, which is useful in multi-user environment

By default the Event Viewer has two tabs:

* Current Events: It shows events as they occur which includes threshold exceptions and outages
* Failed Services: It shows the events linked to outages, as they are more critical than other events

### Performance Management

NMS helps you to improve performance of your network by presenting real time and historic information about your network. The performance metrics measured can be used as elements of service level reporting. NMS aids capacity planning too - network devices and links that are approaching peak capacity utilization will be indicated in the reports enabling you to add capacity before problems arise. Performance reports enable proactive troubleshooting of your network by helping you isolate faulty devices.

NMS helps you monitor performances across any of the parameters that are supported by the SNMP agents of the device. In a typical deployment the relevant parameters are identified from the list (made available by the vendors) and these are then enabled with lower and upper thresholds defined.

### Comprehensive Reporting

Reports are presented in an easy to understand graphical format with the ability to customize the report based on date interval, type of graph (bar, area, line), legends, colors, and information to be plotted. Report customizations can be stored and retrieved for future use. NMS's flexible reporting system provides real time and historic information useful for network monitoring and management. Detailed availability reports are provided to help monitor your service level agreement fulfillment. To enable planning for future network growth, detailed outage reports are provided. The report system enables network managers to comprehensively monitor network devices on an hourly, daily, monthly or even yearly basis on the following parameters:

* CPU Utilization
* Memory Utilization
* Traffic In
* Traffic Out
* Errors In
* Errors Out
* Response Time

NMS Report system provides detailed network link reports including availability reports, performance reports and traffic reports. This would help the user understand the utilization of bandwidth across the network.

Some of the special reports (apart from standard value vs. time plots) are:

* Top N Reports (which gives the top “N” number of devices which are of a particular state or profile where N is defined by the user)
* Location Specific Reports giving reports for specific locations
* Topology wise reports for reports on specified topologies
* Reports with filters for Business Hours (which would then discount parameter values for off-office hours)
* Reports with filter for specific device type in topology, location

NMS also offers service-monitoring reports. Availability and response time reports are provided for FTP, HTTP, DNS, LDAP, IMAP, POP3, SMTP and generic TCP services. It is also has the inbuilt intelligence to monitor the following database servers with ease: Oracle, PostgreSQL, SQL Server, MySQL, and DB2.

The report engine is also linked to a Reports Newsletter Engine which enables users to set pre-defined reports to be e-mailed at pre-defined times (e.g. every Monday morning). The reports also provide an option to export data in standard format to integrate with third party products or to get raw data on the network performance. The reports are web based; hence they can be viewed from any machine in the network

### SLA tracker

This module enables to configure and track SLA adherence of devices. Any violation will be reported and reports will be generated in a graphical and tabular format

### Administration

Multiple levels of users can be setup based on roles they play. Hence access can be restricted based on the responsibilities of the person. As a result the personnel who are responsible for say the Chennai part of the network can see events / alerts and performance graphs along with the status of only the Chennai network devices.

The entire setup, use and administration of NMS is GUI based with simple menu driven functions. NMS has a backup facility in-built into the system enabling the Network Administrator to easily backup the crucial information about network performance that NMS collects.

### SNMP support

NMS can monitor any device or application that is SNMP enabled

* Support for snmpget, snmpset, snmpwalk, snmpbulkget, snmpbulkwalk, snmptraps and snmptable
* Support for stable SNMP v1, v2c & v3
* Extensive library of MIB’s maintained at backend to support a vast number of devices.
* Support for updating MIB library with new MIBs

### Port monitoring

Sify NMS can monitor and report availability and performance of any TCP port. This is a good feature where a customized application listening on a TCP port can be monitored. Reports on the port response time will also be available.

### Secure

All data that is transferred from the Poller to the station for processing is 3 DES encrypted. This feature is of great use when the NMS polling device has been deployed at the customer site and the station is installed at Sify

### Data Persistence

In the event of a network cut between the Poller and the station, then all polled data is persisted at the Poller end and then sent to the station when the connectivity is back on again

### Simple

Sify NMS comes as a single package. You do not need to install separate packages and plug-ins for any additional monitoring requirements. The entire Sify NMS is highly configurable with no extra licensing requirements, provides ease of administration.

### Scalability

Resource utilization intensive data collection process can be spread across multiple machines located anywhere on the reachable network. This not only lends to scalability but also contributes to failover and load balancing. Strategic positioning of these data collection engines also lends to multiple views of the network performance and end-to-end connectivity issues.

### Monitoring Parameters

Sify NMS can monitor the following parameters

Mandatory

* ICMP Latency
* ICMP Packet loss
* SNMP Cisco Link Reliability
* SNMP Interface Input Errors
* SNMP Interface output Errors
* SNMP Interface Output Traffic - Threshold can be configured
* SNMP Interface Input Traffic - Threshold can be configured

Optional

* SNMP Cisco Used Memory Pool - Threshold can be configured
* SNMP Cisco Free Memory Pool - Threshold can be configured
* SNMP CPU 1-minute Average Utilization - Threshold can be configured
* SNMP CPU 5-minute Average Utilization - Threshold can be configured
* SNMP Cisco-TempInlet
* SNMP Cisco-TempOutlet

## Sify’s Service Portal: Aakash

### Aakash: An Overview

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 Service desk and a reporting functionality to Customer and its users.

Sify Aakaash Portal is also 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 reporting. 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 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 customer.

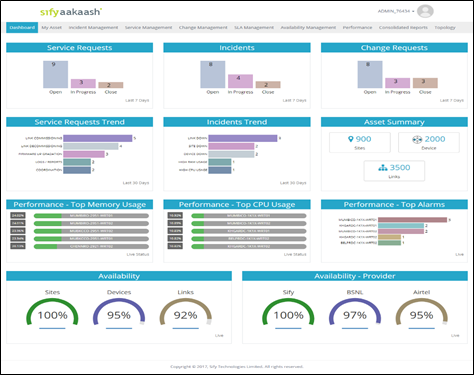
* Admin Account
  + User Management – This module to onboard and manage site accounts with required features and reports.
  + SLA Management (Monthly SLA Reporting)
  + Service management (Incident / Service / Change Requests)
  + Performance Reporting
  + Topology
  + Dashboards
  + Asset Management
* User Operator Account
  + Performance Reporting
    - Reports pertaining only to that particular 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

### Aakaash: Service Screens

Unified Dashboard View

Aakaash Portal dashboard provides snapshot of the services, network health and trouble ticket status and trends. Following key KPI’s are presented in the dashboard:

* Service Requests
* Incidents
* Change Requests
* Service Requests Trend
* Incidents Trend
* Assets Summary
* Performance – Top Memory Usage
* Performance – Top CPU Usage
* Performance – Top Alarms
* Availability – Device based
* Availability – Provider based



SLA Management Reports

Fortis will have complete view of Site wise and Link SLA reporting as shown in the below screenshots.

This module provides last 3 months SLA trend for each site and per device:

A screenshot of a social media post

Description generated with very high confidence

SLA Reports in Tabular format: Reports can be exported through excel and PDF formats:

A screenshot of a computer

Description generated with very high confidence

Incident Management

Incident management section shows the complete list of incidents with status information

A screenshot of a computer

Description generated with very high confidence

Customer can report incident from this module, and they can track the incident till the closure.

A screenshot of a social media post

Description generated with very high confidence

Service Request

Customer can raise service requests for link commissioning / de-commissioning, upgradations etc… and will have the complete visibility of service status for each request.

A screenshot of a social media post

Description generated with very high confidence

Asset Management

This module provides complete network (physical & logical) inventory for the customer.

A screenshot of a computer

Description generated with very high confidence

Device Asset Summary view:

This module shows summary of no of sites, devices, and links along with site wise incident information.

A screenshot of a social media post

Description generated with very high confidence

Availability Management:

This module provides site availability and link provider availability with Uptime and Downtime bifurcation.

A screenshot of a social media post

Description generated with very high confidence

User Operator Account:

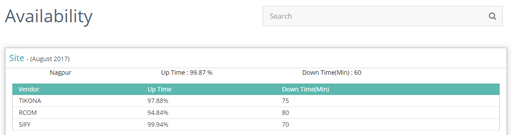
Site-Wise Device & Link Asset:

This module shows site wise Device and Link asset information along with live status A screenshot of a social media post

Description generated with very high confidence

Availability Management

This module provides site availability and link provider availability with Uptime and Downtime bifurcation.



Performance Management

This module provides following network performance metrics in graphical view.

* Device Health
* CPU
* Memory
* Interface Statistics
* Bandwidth Utilization
* Errors
* Network Performance
* Latency
* Packet loss
* Jitter

A screenshot of a social media post

Description generated with very high confidence

# 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 >>>>>>>>>>>>>>**

# Terms & Conditions

* All pricing provided is 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 the customer will incur hardware charges for replacement of faulty hardware (OTC). Customer must provide UPS Power and earthing for the WiFi 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, 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 will result in associated change of commercials.
* Any changes to the Solution design and configuration will result in a design change along with the revised commercials.
* The provisioning/commissioning of any unmanaged or managed network security services (apart from anything included within Solution) is considered out of scope.
* All payments 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.