Sify Managed LAN Services Proposal

Submitted To: <Customer Name>

Sify Technologies Ltd.

Contents

[Document History 3](#_Toc168591317)

[Sign-Off 3](#_Toc168591318)

[Document Title 3](#_Toc168591319)

[Preparation 3](#_Toc168591320)

[Release 3](#_Toc168591321)

[Distribution List 3](#_Toc168591322)

[Statement of Confidentiality 3](#_Toc168591323)

[Executive Summary 4](#_Toc168591324)

[About <CUSTOMER NAME> 4](#_Toc168591325)

[About Sify Technologies Ltd. 4](#_Toc168591326)

[Business Units 4](#_Toc168591327)

[Managed Network Services Portfolio 5](#_Toc168591328)

[Scale of Operations 5](#_Toc168591329)

[What does Sify bring to the table? 5](#_Toc168591330)

[Sify Managed LAN Services (MLAN) 7](#_Toc168591331)

[Sify’s Experience in Deploying Enterprise LAN & WiFi 8](#_Toc168591332)

[Service Objectives 10](#_Toc168591333)

[Service Overview 11](#_Toc168591334)

[Service Components 11](#_Toc168591335)

[Access Points 12](#_Toc168591336)

[PoE Switch 13](#_Toc168591337)

[Security Appliance 13](#_Toc168591338)

[Authentication Infrastructure 14](#_Toc168591339)

[Service Tiers 14](#_Toc168591340)

[Service Deliverables 15](#_Toc168591341)

[Service Implementation 16](#_Toc168591342)

[Service Assurance 16](#_Toc168591343)

[Service Level Agreements 18](#_Toc168591344)

[Network SLA 18](#_Toc168591345)

[Delivery SLA 18](#_Toc168591346)

[Operation SLA 18](#_Toc168591347)

[Change Management 18](#_Toc168591348)

[Service Request 19](#_Toc168591349)

[SLA Exceptions and Exclusions 19](#_Toc168591350)

[Service Level Conditions 19](#_Toc168591351)

[Site Uptime SLA – Service Credits 19](#_Toc168591352)

[Site Uptime SLA - Penalty Exclusion 20](#_Toc168591353)

[Severity Level Definitions 20](#_Toc168591354)

[Ownership of Managed Devices post contract period 21](#_Toc168591355)

[Faulty Managed Devices Caused by Customer Site Conditions 21](#_Toc168591356)

[Addition of New Sites, Managed Devices Post Contract Period 22](#_Toc168591357)

[RMA Process 22](#_Toc168591358)

[Device Warranties 22](#_Toc168591359)

[Sify Service Portal: AakaashTM 22](#_Toc168591360)

[<Customer Name>’s Requirement 24](#_Toc168591361)

[Requirement Understanding 25](#_Toc168591362)

[Proposed Solution 26](#_Toc168591363)

[Solution Components 26](#_Toc168591364)

[Detailed Solution 27](#_Toc168591365)

[Commercial Proposal 28](#_Toc168591366)

[Reviews 30](#_Toc168591367)

[Information Security Policy 31](#_Toc168591368)

[Standard Terms & Conditions 32](#_Toc168591369)

[General T&Cs 32](#_Toc168591370)

[Payment Terms 33](#_Toc168591371)

# 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** | Sify Managed LAN Services Proposal |
| **Document Name** | <CUSTOMER NAME> - LAN Transformation Approach v1.0.pdf |

## Preparation

|  |  |  |
| --- | --- | --- |
| **Action** | **Name** | **Date** |
| **Prepared By** | Solution Architect | June 2024 |
| **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 |  | 🗹 |  |
| Sify Technologies Limited |  | All | 🗹 | 🗹 |  |
| Sify Technologies Limited |  | All | 🗹 | 🗹 |  |

## 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>

< Content about the Customer>

## About Sify Technologies Ltd.

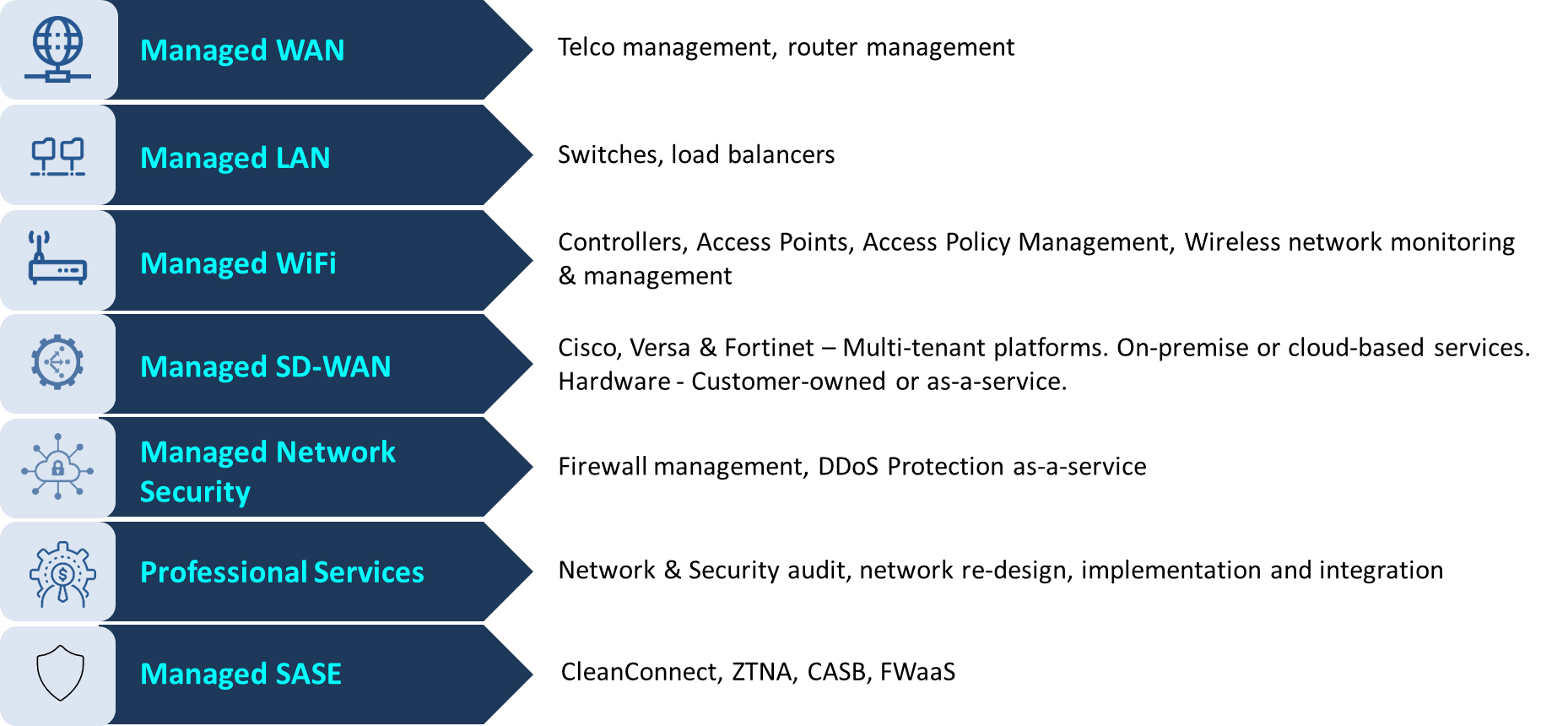
A Fortune 500 India company, Sify Technologies is India’s most comprehensive ICT service & solution provider. Sify being Digital at Core in our solutions portfolio, Sify is focused on the changing ICT requirements of the emerging Digital economy and the resultant demands from large, mid and small-sized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

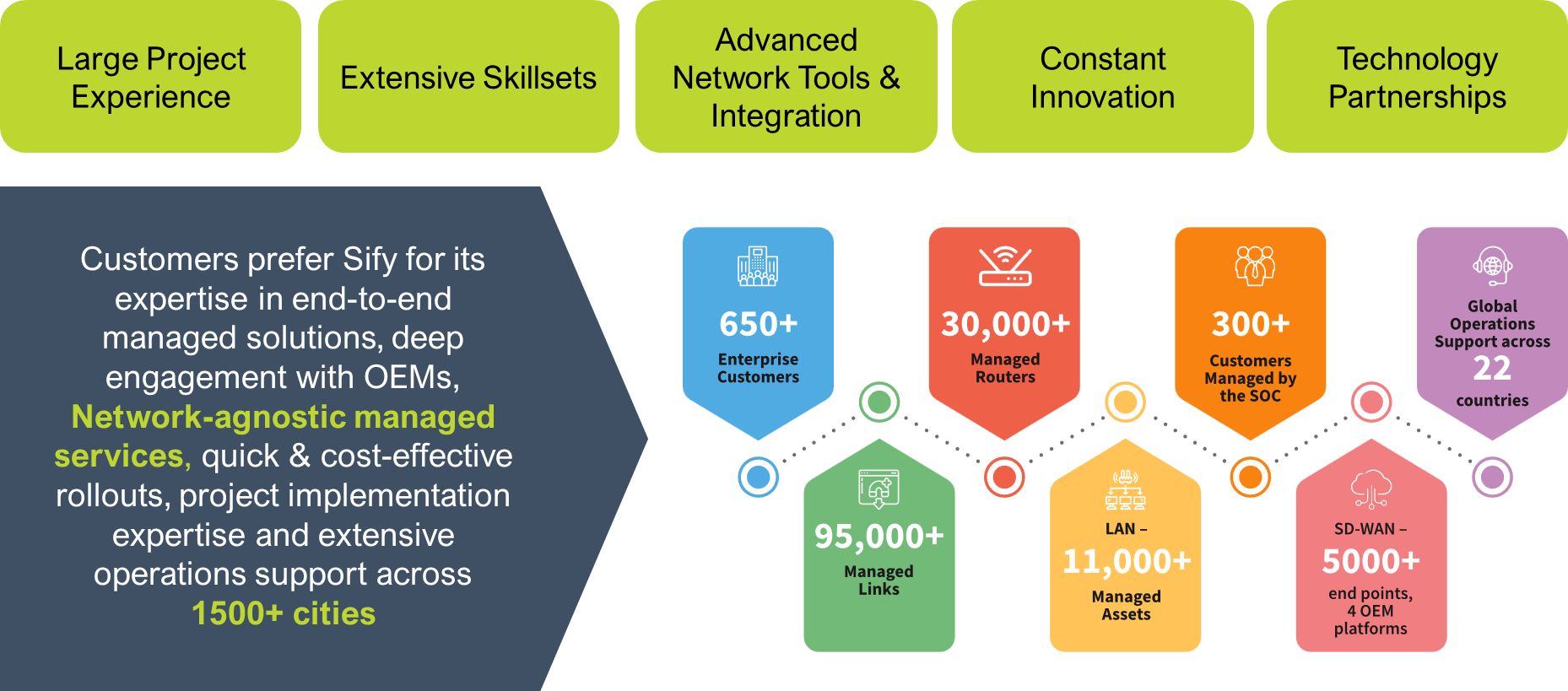
## Business Units



## 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 LAN Services (MLAN)

This Service Descriptor Document outlines the specifications of Sify’s Managed WiFi service on the Aruba & Meraki platforms. The aim behind this document is to describe the features & specifications of the Sify Managed WiFi product which will cater to customers who need a highly scalable, cloud-managed wi-fi service which is tightly integrated with the Aruba/ Cisco ecosystems.

Indian businesses are increasingly embracing digital transformation & the Cloud to enhance efficiency and competitiveness. Managed service providers (MSPs) play a crucial role in assisting organizations in this journey by offering services such as cloud computing, cybersecurity, data analytics, and IoT solutions.

The managed WiFi market has been experiencing significant growth due to the proliferation of wireless devices, the rise of IoT (Internet of Things), and the increasing dependence on WiFi in various industries. Several technology and telecommunication companies offer managed WiFi based products, including Cisco Systems, Networks (a Hewlett Packard Enterprise company and others.

Some of the most important trends deciding the success of these players are Security features, including encryption, threat detection, and user authentication, are critical components of managed network services, addressing the growing concern of cyber threats. Many managed WiFi services are offered through cloud-based platforms, providing scalability, ease of management, and remote accessibility. Solutions with advanced analytics and reporting capabilities are gaining popularity as businesses seek to understand and optimize their WiFi networks.

Sify has a well-established practice around Managed Wi-Fi services. As a leading player in the Network Managed Services space, we offer a Service based Managed Wi-Fi model with End-to-End ownership which is highly scalable & resilient. We also have extensive experience with pan India delivery & support of Wi-Fi solutions. Some of the well-known names onboarded on our Wi-Fi platform are - The Tata Steel Group, Britannia, Siemens, ICICI & Bajaj Finance along with a host of other well-known brands in the Indian market. Today, we centrally manage over 2500 access points for our customers.

Sify’s Managed WiFi brings networking infrastructure near to the end-user providing an on-demand WiFi experience without any hassles, while providing centralized management of your local wireless network. We provide an efficient policy management platform to effortlessly onboard new devices, grant varying access levels, keep networks secure, and safely connect business & personal devices to the network. Our team of expert engineers enable seamless implementation of the latest technologies. With Sify’s fully managed wireless network, we expect to provide <Customer Name> an unprecedented level of visibility & control over their entire network.

## Sify’s Experience in Deploying Enterprise LAN & WiFi

Sify has extensive experience in delivering high-quality LAN & Wi-Fi solutions for our customers in the following industries –

* Steel & Mining
* FMCG
* IT & ITES
* Manufacturing
* Private BFSI
* Public BFSI
* Retail

While enabling digital transformation for the world’s second largest geographically diversified steel producer, Sify was tasked to achieve the following two objectives –

* To establish a NOC integrating IT, OT assets to enable insights into the network across DC, Cloud and end users.
* Build and operate a private network across all Campuses.

Key pain points of this customer were –

* **Design:** Poorly designed & conceived AP positioning resulted in blackspots in many areas.
* **Configuration:** Role based policy enforcement for different profiles of users not available.
* **Visibility:** No online visibility into the ongoing activity of the Wi-Fi Users.
* **Reporting:** Granular reporting on Wi-Fi usage was not available.
* **Scalability:** Rapid addition of WLAN nodes not possible.
* **Management:** Complete end-to-end WLAN management from a central console not possible.
* **Authentication:** Multiple authentication modes at the same time were not available.
* **Guest Access:** No Controlled Internet access to guest users with OTP based authentication.
* **User experience:** Poor end user experience resulted in Wi-Fi not being the preferred network.
* **SLA:** There was no accountability & SLA on the Wi-Fi provider.

Sify designed a solution involving specialized skillsets and processes across NOC setup & managed services which outclassed the traditional IT outsourcing model deployed by the incumbent. We also integrated our Managed Wi-Fi platform with the customer’s Access & Identity Management System (AIMS), which ensured an integrated Platform for all IT, OT assets, as well as Wearable Safety devices across their workforce.

Thus, Sify was able to generate the below value additions for this customer –

* The WiFi NOC has enabled network orchestration and analytics for the customer across his IT & OT assets and people, which in turn has resulted in better efficiency & control.
* Sify’s private network has enabled large scale sensorization of plant operations leading to better efficiencies and significant cost savings.

Some of the sub-projects executed by Sify for the same customer are –

**Group Managed Hospital**

* Providing complete High Availability Wi-Fi Network coverage of hospital building infrastructure.
* Managing Access and Authentication of different user sets - VIPs, Doctors and Employees and Guests.
* Providing predictable and secure network infra to enable personalized healthcare experiences from edge to cloud.
* Sify is helping improve patient and staff experiences while improving operational outcomes.
* We enabled rapid and seamless client onboarding and proactive monitoring and support of the Wi-Fi Network.

**The IOT Project**

* Managed Wi-Fi to enable connectivity for the IoT devices and VIP & other corporate internet users implemented at multiple customer locations.
* The installed IoT sensors emits data signals at short intervals that need to be transmitted to Customer’s Cloud
* The Customer’s floor locations required Access Points equipped to function at extreme environments.
* The data from the sensors need to be transferred to the IoT developer & NMS for monitoring and reporting.

Volumetrics to indicate the scale of this project –

Graphical user interface, application

Description automatically generated

# Service Objectives

Chief service objectives of the Managed LAN product are –

|  |  |
| --- | --- |
| **Objectives** | **Description** |
| Reliability and Performance | Ensure a stable and high-performing WiFi network to support uninterrupted operations and enhance user experience. |
| Scalability | Accommodate the growing number of devices and users on the network, providing flexibility for business expansion. |
| Security | Implement robust security measures, including encryption and intrusion detection, to protect against cyber threats. |
| Centralized Management | Facilitate easy monitoring and control of the network through a centralized management system for efficient operations. |
| Cost Efficiency | Provide a cost-effective solution by reducing the need for on-site IT staff and optimizing resource utilization. |
| Quality of Service (QoS) | Prioritize critical applications and services to ensure consistent and reliable performance, especially for real-time applications. |
| Guest Access Management | Offer secure and controlled guest WiFi access with features such as authentication, time limits, and bandwidth restrictions. |
| Analytics and Reporting | Provide tools for gathering insights into user behavior, network performance, and other metrics to inform decision-making. |
| Compliance Requirements | Address industry-specific regulatory compliance requirements related to data protection and privacy on the WiFi network. |
| Remote Management | Enable remote management and troubleshooting to efficiently address issues and implement changes across multiple locations. |

# Service Overview

Sify’s Wi-Fi 6 ready platform promises high performance, low latency, and advanced security even in crowded areas.

Key elements of our Managed WiFi solution are –

* Cloud-based Centralized Authentication Infrastructure
* Cloud-based Centralized WLAN Monitoring Console
* Captive Portal for Guest Management
* Access Points at Customer sites

# Service Components

WLAN as a service consists of the following components:

* **Access Point:** deployed in every customer site with capabilities supporting WIFI6.
* **Switches**: deployed in every customer site with capabilities supporting PoE+.
* **Security Appliance**: deployed in customer place with firewall and tunnel capability.
* **Meraki Dashboard**: Applications hosted in public cloud for network device management and monitoring.
* **AAA Server**: A centralized system that authenticates, authorizes, and tracks user access to network resources.
* **Transport Networks**: Provides last mile network connectivity to CE’s that establishes connection towards Control & Management plane communication and data plane Communication.
* **Service Management Portal:** a single pane of glass for complete service lifecycle management.

## Access Points

Access Points are placed at every customer premise. Access Points provide a secure WLAN service to the users and devices, including various types (Corporate, Guest, Contractor, Headless devices). Based on the type of network authentication and encryption is applied. Various model available based on the environment type the Access Point models will vary. Access Points are delivered as part of Sify’s managed WLAN services and will be configured and managed by Sify MWIFI. Access Points create overlay secure tunnels between Cloud Dashboard using transport links.

Below are the access point types based on the environments type –

* Indoor Access Points
* Rugged Access Point
* Outdoor Access Point
* Hospitality Access Point

Key features of Sify’s cloud Managed Access Points –

* **Cloud Management​:** All Meraki devices can be centrally managed through the Meraki Dashboard, thus MRs can be configured, monitored, and troubleshot from any location with internet access​.
* **Zero-touch Deployment​:** All Meraki devices can be deployed with minimal manual configuration. Once connected to the network, they automatically pull configurations from the cloud, streamlining the deployment process​.
* **Intelligent Radio Assignment​:** Support intelligent radio assignment, which optimizes the allocation of 2.4 GHz and 5 GHz frequencies based on real-time usage and interference conditions​.
* **Mesh Networking​:** Support mesh networking, allowing MRs to wirelessly extend the network coverage without the need for additional cabling​.
* **Auto RF Management​:** The Auto RF feature continuously monitors the radio environment and adjusts settings dynamically to optimize performance​.
* **Integrated Security Features:** MRs include built-in security features such as WPA3 encryption, stateful firewall, integrated Layer 7 application visibility, and content filtering.
* **Scalability:** Meraki solutions are designed to scale easily, whether deploying a small network for a single location or managing large, distributed networks with thousands of access points.
* **Location Analytics:** MRs can provide location analytics, allowing ability to gather insights on visitor behaviour, track foot traffic, and analyse user engagement within a physical space.
* **Firmware Updates:** Firmware updates are automatically managed through the cloud, ensuring that devices are always running the latest and most secure software.
* **Application Visibility & Control:** MRs offer Layer 7 visibility, allowing administrators to see which applications are being used on the network for policy enforcement and network optimization.

## PoE Switch

MWLAN Switches is primarily POE switches used for powering on Access points where the access point count is more than 2 in a single location. Customer requires wired authentication for their end devices connecting to the network via LAN these switches can act as NAS/NAD device like WiFi Access points.

These switches ensure that connectivity, L2 Switching and L3 Routing, security, Stacking and smart network management complement each other so that all these devices can securely connect.

Key features of Meraki’s MS series of PoE Switches –

* **Network Visibility and Monitoring​:** The Meraki Dashboard provides comprehensive visibility into the network, including real-time monitoring, traffic analysis, and historical data. This allows administrators to quickly identify and address network issues.​
* **Power over Ethernet (PoE) Support​:** Many Meraki switches support Power over Ethernet (PoE) and PoE+ to power devices such as IP phones, cameras, and access points directly through the Ethernet cable, eliminating the need for separate power sources.​
* **Stacking and Virtual Stacking​:** Meraki switches support physical stacking, allowing multiple switches to be interconnected and managed as a single logical unit. Virtual stacking is also supported, enabling the management of multiple switches as a single entity, even if they are not physically stacked.​
* **Smart Link Aggregation​:** Meraki switches support link aggregation, allowing multiple physical links to be combined into a single logical link. This enhances redundancy and increases available bandwidth between switches and connected devices.​

## Security Appliance

Security Appliance offer centralized network engineering, IP services, security and policy controls, and app-aware platforms. In addition to network control, they can be deployed as branch gateways, VPN concentrators, WIPS/WIDS and stateful network firewalls with integrated content filtering. Security Appliance are available as both Hardware models as well as VM based.

In Sify Deployments Security Appliance are normally preferred tunnel mode SSID security appliance is required.

Security Appliance will be deployed in campus or branch location and Access points will be configured in tunnel or bridge mode from Customer side back to Security Appliance. In tunnel mode all the traffic from the Access point (control plane + data plane) will reach the Security Appliance. In bridge mode only the control plane and data traffic will be routed locally.

## Authentication Infrastructure

Sify’s Managed WiFi services provide robust network access control with granular role-based policies for authentication, authorization, continuous monitoring, and enforcement. Its highly interoperable features enable robust network access control. This is achieved through the Clear Pass Policy Manager (CPPM) on the Aruba platform & via the Identity Service Engine (ISE) on the Meraki platform.

The advanced endpoint posture assessments on both platforms can automatically remediate or quarantine endpoints that violate corporate security and compliance policies.

Key features of the MWiFi authentication infrastructure are –

* AI-Powered Visibility
* Robust Authentication
* Secure Authorization
* Reliable Policy Enforcement
* Powerful Integrations
* SSO Support

# Service Tiers

|  |  |  |  |
| --- | --- | --- | --- |
| **Tier** | **Basic** | **Enterprise** | **Industrial** |
| Feature | Guest Access | Guest Access | Guest Access |
| AD Integration | AD Integration / BYOD |
| BYOD | Policy Enforcement / Advance Security |
| Policy Enforcement | Custom Web Pages |
| Custom Web Pages | Outdoor APs |
| Advance Security | Location Based Services |

# Service Deliverables

|  |  |
| --- | --- |
| **Deliverable** | **Description** |
| Monitoring & Reporting | 24x7 pro-active monitoring of network and Devices related metrics and reporting on Aruba dashboard and metric specific dashboard.  Ability to view real-time and historic reporting in Aruba Dashboard and Sify Aakaash. |
| Configuration management | Management data is replicated across independent same-region data centers in real time. The same data is also replicated in automatic nightly archival backups hosted by in-region third-party cloud storage services.  Configuration audit for compliance |
| Incident management | Ticketing – customers can use Sify Aakaash as single portal for managing incidents.  MWIFI prepares RCA for incidents raised by customers and on-request.  Fault and performance management – this would be based on logs, events and data retrieved from Aruba Dashboard and central components |
| Change management | MWIFI manages all changes to be executed in customer WLAN networks – MACD based on requests from customer and proactively.  Changes are carried out on Aruba dashboard and Central components.  Customer would be providing approval for every change based on detailed POA prepared by MWIFI |
| Inventory management | Managing inventory of customer devices within the scope of managed Wireless services – network wide and site wide  Managing logical resource of customer network – WLAN networks, IP address (WLAN, LAN, WAN), VLAN, customer site contact information details etc. |
| Vendor management | MWIFI co-ordinates with Aruba vendors to work on issues related to managed Wireless services |
| Provider governance | MWIFI owns the complete transport provider lifecycle management. This includes identifying transport providers in each customer site, engaging with provider for ordering till circuit turn up, connecting transport links to Security appliance, Router or Firewall, coordinating with transport providers for any issues |
| Implementation and transition services | Implementation & transition services will be the responsibility of Sify’s delivery teams unless this scope is outsourced to a 3rd party in exceptional cases. |
| SLA reporting | Sify MWIFI is the single owner for all enterprise network connectivity of managed Wireless services. Sify Aakaash is the common portal for managing end to end SLA between Aruba Components which includes Access Point, Switches, and Security Appliance. |

# Service Implementation

Sify will follow a transition plan to ensure a systematic and effective deployment of the managed WiFi service, minimizing disruptions, optimizing performance for end-users & ensuring a smooth migration of services. The plan will be adjusted based on the specific needs and scale of the project.

Toll Gate Reviews

Transition Metrics

Transition Reporting

Transition Governance will ensure below aspects of service migration are correctly followed –

* Project Management
* Relationship Management
* Partner Management
* Risk Management
* Human Resource
* Contract Management
* Knowledge Management
* Tools / Best Practices
* Quality Management

**Transition Workflow:**

A diagram of a project management

Description automatically generated

# Service Assurance

The managed Wi-Fi product must deliver reliable, efficient, and secure internet connectivity for users across various scenarios and locations. The below given performance metrics will be monitored –

|  |
| --- |
| **Performance Metrics** |
| Network Availability/Uptime |
| Throughput |
| Latency |
| Packet Loss |
| Jitter |
| Coverage Area |
| Signal Strength |
| Capacity |
| Load Balancing Efficiency |
| Client Roaming Performance |
| Client Connection Time |
| Guest Access Performance |
| Device Onboarding Time |
| Security Effectiveness |
| Bandwidth Utilization |
| Incident Response Time |
| Firmware Update Success Rate |
| User Satisfaction Scores |

**Sify’s On-Call Support Teams:**

|  |  |
| --- | --- |
| **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 and Sify management.  During the project, the Project Manager is the first line interface between customer and Sify Management. The Project Manager will therefore act diligently and honestly in all such dealings and will encourage and 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 customers.  Provide remote hands & feet support to NOC.  Initial troubleshooting of the network issues.  Report generation based on customer 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 and Sify during the project. The Account Manager will also be responsible for ensuring any commercial change arises due to a change in scope to be taken up with customer. Actively participates in review process. |

# Service Level Agreements

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

## Network SLA

Uptime: > 99.50%

## Delivery SLA

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

## Operation SLA

**Incident Management**

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

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

## Change Management

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

## 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**

## 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

## 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 Devices post contract period

* All Sify owned managed devices 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 devices 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 devices 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 Devices 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 Devices 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 Devices 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 Sify Managed LAN Services 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 devices are procured with minimum 1 year of warranty. Any project specific procurements are done with warranty scope as per project.
* Faulty devices 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.

# <Customer Name>’s Requirement

**<<<<<<<<<<<<<<**

**INCLUDE DETAILED DESCRIPTION OF THE CUSTOMER’S REQUIREMENT**

**>>>>>>>>>>>>>>**

# Requirement Understanding

**<<<<<<<<<<<<<<**

**INCLUDE DETAILED DESCRIPTION OF SIFY’S UNDERSTANDING OF THE CUSTOMER’S REQUIREMENT**

**>>>>>>>>>>>>>>**

# Proposed Solution

## Solution Components

Our proposed solution includes the below components. These are subject to change as further discovery is made of <Customer Name> network landscape –

|  |  |  |  |
| --- | --- | --- | --- |
| **Solution Components** | **#** | **Line Items** | **Description** |
| Active Components | 1 | Wireless AP | The AP is the gateway for the users to wirelessly access internet / intranet from their end devices (Laptops/Tablets/Smartphones/Handhelds). |
| 2 | 12 Port PoE Switches | PoE switch powers up the APs and allows data flow between the APs. |
| 3 | Licenses | Airwave, Enterprise & ClearPass Licenses |
| 4 | Aggregation Switches | Aggregation Switch aggregates traffic from multiple PoE switches deployed in an area and provides a single uplink to the TSL LAN access switch. |
| Passive Components | 5 | Console Cables | Console Cables for Access Points |
| 6 | Passive Cabling | UTP cabling for connecting the APs with the PoE switches. |
| Sify Services | 7 | Managed Services | 24x7x365 monitoring & management services from Sify NOC |
| 8 | Web Development | Web Development for captive portal |
| 9 | True BusinessID | SSL Certificate |
| 10 | Installation | Installation & Setup |
| 11 | VM | VM Instance for CPPM |

Support will be required from <Customer Name> as below:

* Suggestions required from <Customer Name> for user authentication mechanism.
* Integration with existing infrastructure devices.
* Access permission to sites for deployment of network elements.
* UPS-power, earthing, collocation space & cooling for network elements.
* Provisioning of WAN links for end use access.
* Provide details for captive portal to be configured in Wi-Fi setup.
* Provide details of internet access policy for Wi-Fi setup.
* Application testing & security.
* Providing internet access for the WiFi network.
* Managing the performance of the internet connectivity if not provided by Sify.
* Providing permission for inter-floor & Inter-building Passive Cabling,
* AD – integration support.
* VLAN for each SSID & Management VLAN should be allowed in <Customer Name> LAN.
* <Customer Name> to provide power point and access switch within 80m from Sify Access Points.

## Detailed Solution

**<<<<<<<<<<<<<<**

**INCLUDE DETAILED SOLUTION AS PER SIFY’S UNDERSTANDING OF THE CUSTOMER’S REQUIREMENT**

**>>>>>>>>>>>>>>**

# Commercial Proposal

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

# 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.

# 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 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 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 WiFi 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 WiFi 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.

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