

Challenger in Gartner MQ for Managed Hybrid Cloud Hosting APAC 2017

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

Leadership Award for Network Transformation 2019



**CIO Choice Awards**

Data Center Transformation Services 2018

Network Transformation Services 2018

*Submitted to:*

**Customer Name**

**Managed Wi-Fi Services Proposal**

The Economic Times Iconic Brands 2020 Hybrid & Multi Cloud

**Date**



Table of Contents

[2. Document History 4](#_Toc150361535)

[2.1 Sign-Off 4](#_Toc150361536)

[2.2 Document Title 4](#_Toc150361537)

[2.3 Preparation 4](#_Toc150361538)

[2.4 Release 4](#_Toc150361539)

[2.5 Distribution List 4](#_Toc150361540)

[2.6 Statement of Confidentiality 4](#_Toc150361541)

[3. Executive Summary 5](#_Toc150361542)

[3.1 About <CUSTOMER NAME> 5](#_Toc150361543)

[3.2 About Sify Technologies Ltd. 6](#_Toc150361544)

[3.2.1 Business Units 6](#_Toc150361545)

[3.2.2 Differentiators 8](#_Toc150361546)

[3.2.3 Network Capabilities 9](#_Toc150361547)

[3.2.4 Scale of Operations 12](#_Toc150361548)

[3.2.5 What does Sify bring to the table? 12](#_Toc150361549)

[4. Sify’s Experience in Deploying Enterprise WiFi 14](#_Toc150361550)

[5. Sify Managed Wi-Fi Service Description 16](#_Toc150361551)

[5.1.1 Service Overview 16](#_Toc150361552)

[5.1.2 Capabilities 16](#_Toc150361553)

[5.1.3 Service Components 18](#_Toc150361554)

[5.1.4 Sify Managed WiFi Deliverables 18](#_Toc150361555)

[5.1.5 Sify Managed WiFi Tiers 19](#_Toc150361556)

[6. <Customer Name>’s Requirement 20](#_Toc150361557)

[7. Requirement Understanding 21](#_Toc150361558)

[8. Proposed Solution 22](#_Toc150361559)

[8.1.1 Solution Components 22](#_Toc150361560)

[8.1.2 Detailed Solution 23](#_Toc150361561)

[9. Service Levels 24](#_Toc150361562)

[9.1.1 Network SLA 24](#_Toc150361563)

[9.1.2 Management SLA 24](#_Toc150361564)

[10. Reviews 25](#_Toc150361565)

[11. Commercial Proposal 26](#_Toc150361566)

[12. Terms & Conditions 27](#_Toc150361567)

# 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 WiFi Implementation |
| **Document Name** | <CUSTOMER NAME> - WiFi Implementation 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>

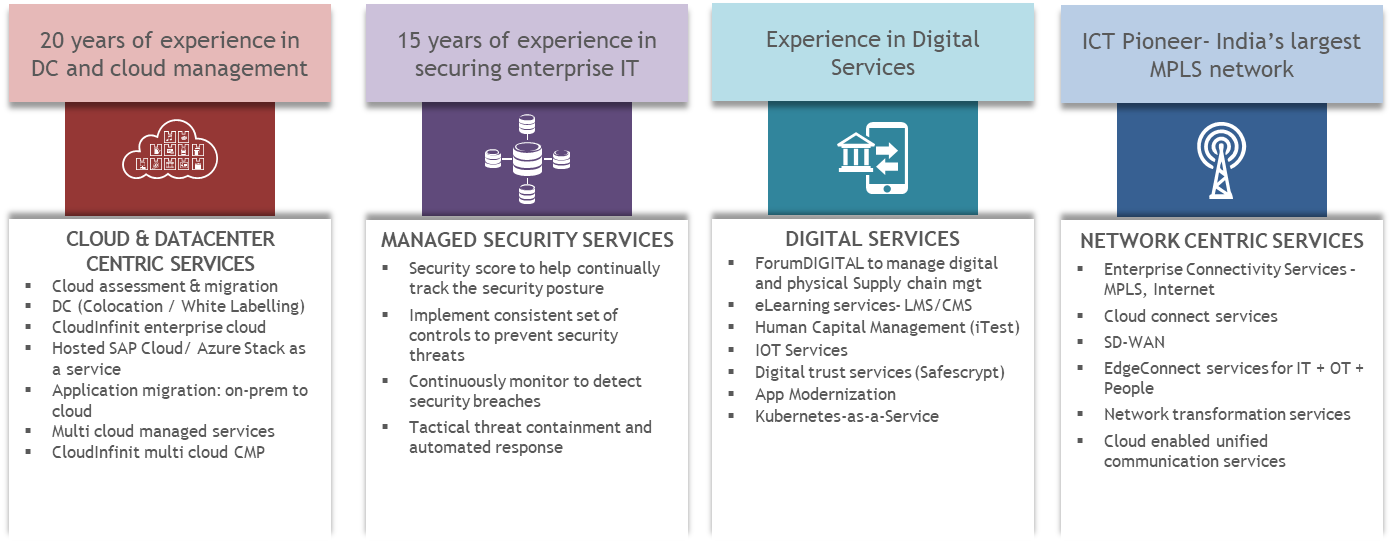
## About Sify Technologies Ltd.

A Fortune 500 India company, Sify Technologies is India’s most comprehensive ICT service & solution provider. With Cloud at the core of 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.

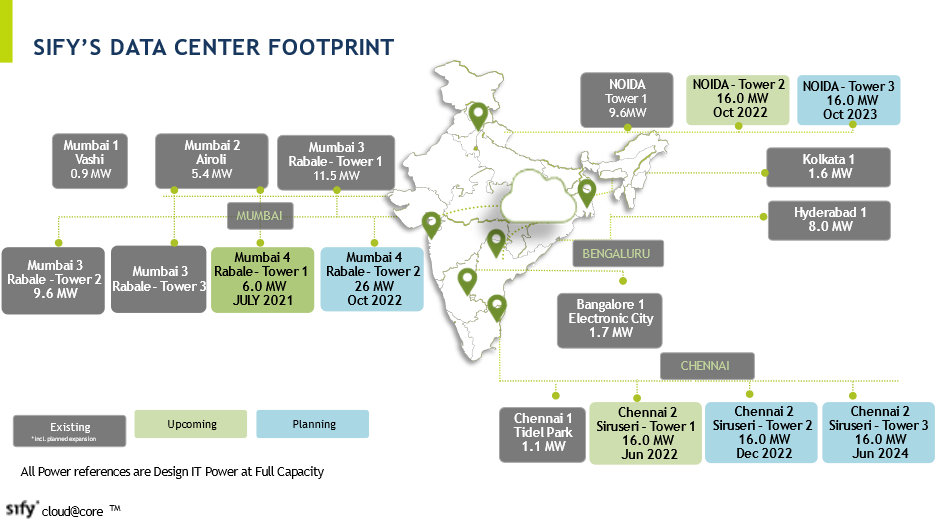
Sify has a well-established practice around Managed Wi-Fi services. As a leading player in the Network Managed Services space, we offer a Service based Managed Wi-Fi model with End-to-End ownership which is highly scalable & resilient. We also have extensive experience with pan India delivery & support 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.

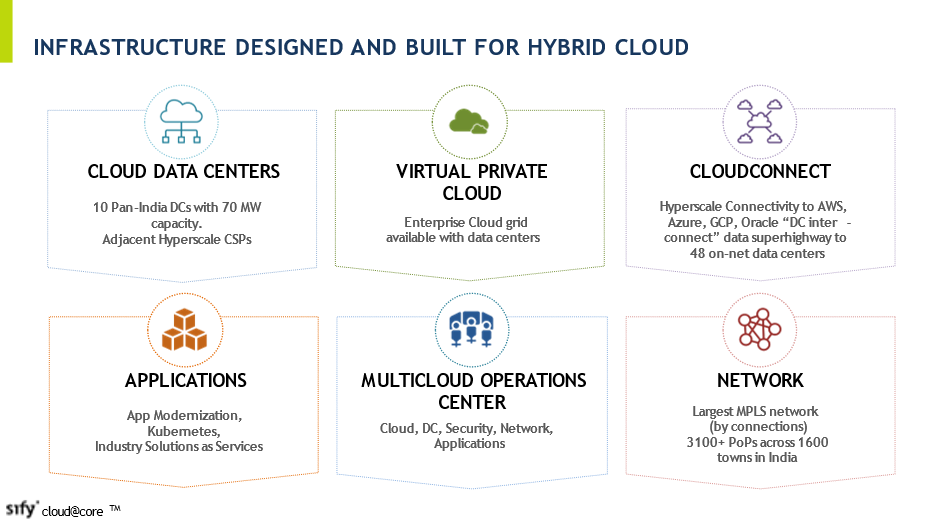
### Business Units



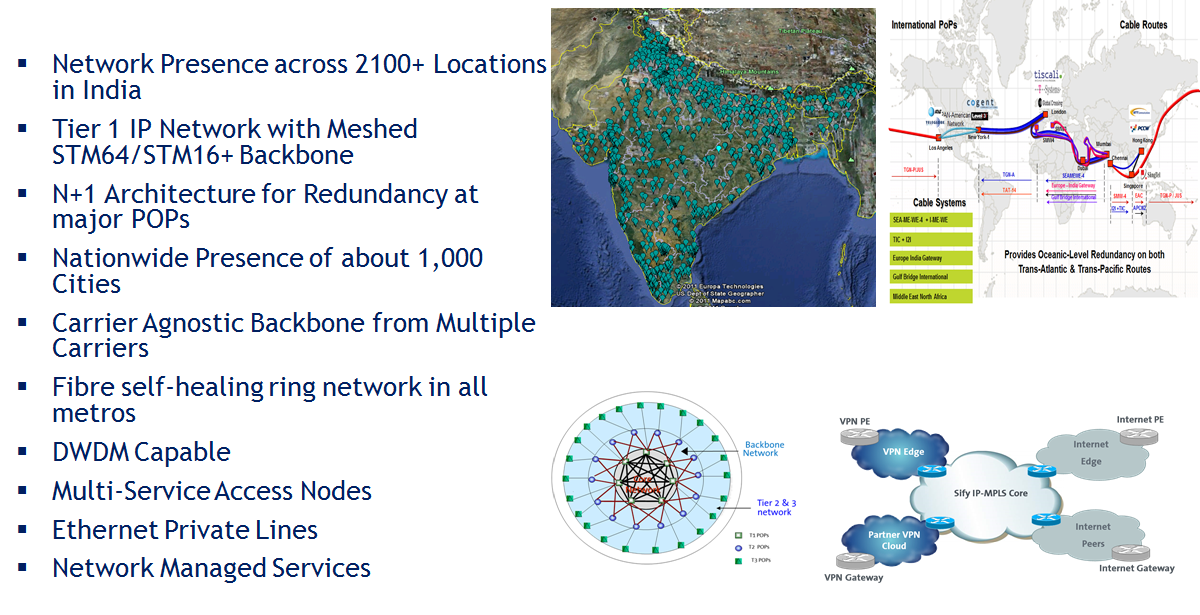
#### Sify’s Data Center Footprint



#### 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 by 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

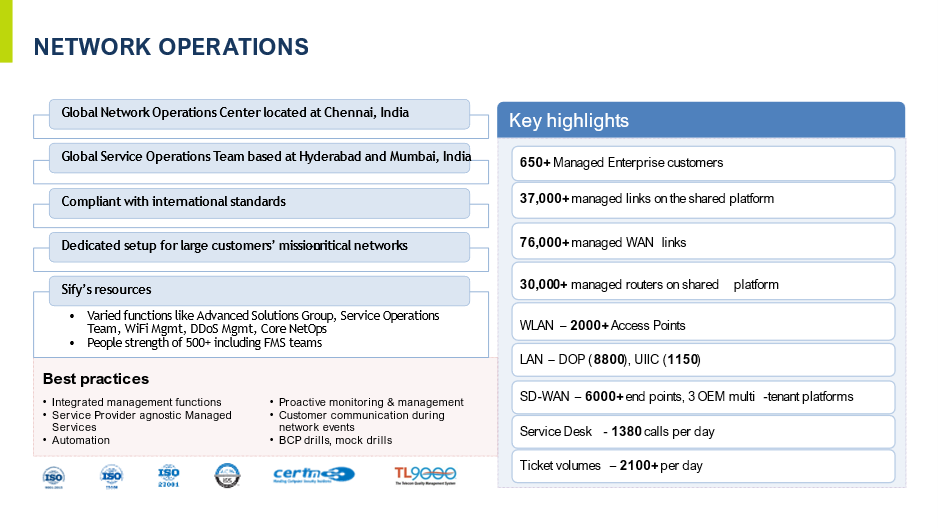
This engagement has the executive leadership commitment being led by the CEO.

### 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 |  |
| 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>.

# Sify’s Experience in Deploying Enterprise WiFi

Sify has extensive experience in delivering high-quality 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 –

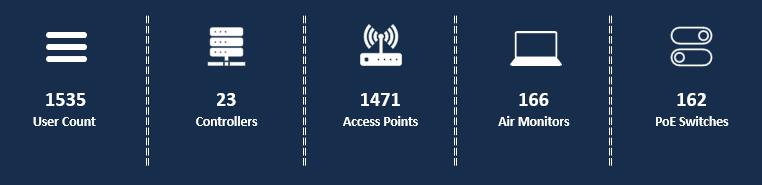
**Group Managed Hospital**

* 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 –



# Sify Managed Wi-Fi Service Description

### 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 Name> sites

### Capabilities

Sify’s Managed WiFi brings the following capabilities to the table –

* Role-based network access enforcement for multi-vendor wireless, wired and VPN networks.
* Posture checks for endpoint compliance.
* User profiling and Device Profiling
* Health-check capabilities to ensure compliance and network safeguards before devices connect.
* Supports multiple authentication/authorization sources (AD, LDAP, SQL dB).
* Self-service device onboarding with built-in certificate authority (CA) for BYOD.
* Supports NAC and MDM integration for mobile device assessments.
* Comprehensive integration with the OEM Security Exchange Program.
* End user device monitoring with NOC services.
* User Access can be tracked for monitoring and troubleshooting.
* Availability of intuitive policy configuration templates and visibility troubleshooting tools.

Authentication Infrastructure –

Aruba Clear Pass Policy Manager (CPPM) provides 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.

Its OnGuard Advanced endpoint posture assessments can automatically remediate or quarantine endpoints that violate corporate security and compliance policies.

Key features of ClearPass Policy Manager are –

* AI-Powered Visibility
  + ClearPass Policy Manager has built in device discovery and profiling features that can be complemented with AI-powered ClearPass Device Insight or Aruba Central Client Insights.
* Robust Authentication
  + ClearPass authenticates the user or device identity against a wide variety of identity sources such as Microsoft AD, LDAP, ODBC-compliant SQL database, token servers, and internal databases.
* Secure Authorization
  + ClearPass provides authorization based on a user’s role, device type and role, authentication method, UEM attributes, device health, traffic patterns, location, and time of day.
* Reliable Policy Enforcement
  + When a security compromise is detected ClearPass can be signaled to take a response action from a wide range of security, network, and IT sources.
* Powerful Integrations
  + ClearPass is a vendor agnostic solution and seamlessly integrates with more than 140 security-based partner solutions to provide robust authorization and enforcement.
* SSO Support
  + Single sign-on (SSO) support works with identity management tools to improve user experience of SAML 2.0-based applications.

Centralized Visibility & Management

Aruba AirWave is a powerful and easy-to-use network operations system that not only manages wired and wireless infrastructure from Aruba, but also provides granular visibility into devices, users, and applications on the network. With unprecedented insight and centralized control to effectively manage global enterprise infrastructures, AirWave lets IT organizations proactively optimize network performance, strengthen wireless security, and improve the end-user experience.

Through a centralized and intuitive user interface, AirWave provides real-time monitoring, proactive alerts, historical reporting, and fast, efficient troubleshooting. Dedicated dashboard views quickly help view potential RF coverage issues, unified communications, and collaboration (UCC) traffic, application performance and network services health.

Key features of Aruba Airwave are –

* Proactive Monitoring
  + With the Aruba Clarity module, AirWave proactively monitors critical non-RF metrics — the time it takes for a mobile device to associate with a Wi-Fi radio, authenticate to a RADIUS server, gather an IP address through DHCP, or resolve names for DNS services. With custom alerts and simulated client testing, Clarity lets IT take proactive action against future performance problems.
* Application-Level Visibility
  + With Aruba AppRF, AirWave provides deep visibility into performance and usage of mobile and web apps. Reputation reports allow you to quickly act against high-risk sites and control Wi-Fi usage by app category. User role, device type and location specific insights let you make quick decisions to protect business critical apps.
* WiFi Coverage Visibility
  + AirWave uses VisualRF to allow for time-lapse mining of Wi-Fi coverage – enabling wireless network engineers to record and replay 24 hours of RF heat mapping. VisualRF also power’s location specific, visual analytics on mobile and web app usage, mobile device performance, mobile UC voice and video quality, and more.
* Simplified Management of Networks
  + AirWave gives granular visibility across the entire access infrastructure and manage multiple generations of wired and wireless networks from just about any vendor – from controllerless to controller-managed and from legacy Wi-Fi to the latest 802.11ac WLANs.

### Service Components

WLAN as a service consist of following below 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.
* NMS Dashboard – Applications hosted in public cloud for network device management and monitoring.
* 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.

### Sify Managed WiFi 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 | * This is covered as separate section – Section 7 service engagement model |
| 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. |

### Sify Managed WiFi 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 |

# <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 DESCRIPTION OF SIFY’S UNDERSTANDING OF THE CUSTOMER’S REQUIREMENT**

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

# Service Levels

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

The following commitments will be applicable for the proposed solution:

Uptime: > 99.50%

### Management SLA

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

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 effected (does not include hardware replacements) |
| Change Resolution | Severity 1 – 4 hours  Severity 2 – 8 hours  Severity 3 – 48 hours |

# 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 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.