TATA COMMUNICATIONS

TATA

SMART OUT OF BAND MANAGEMENT

TATA COMMUNICATIONS

Introduction

Out-of-band (OOB) management is a critical component in modern network infrastructure, providing a secure and reliable method for managing network devices and infrastructure independently of the primary network. This whitepaper explores the key aspects to consider when designing an OOB management network and how tata communication's solutions, can address these needs. We will also compare our solution's offerings with other market solutions, such as those from Cisco.

Let's take a standard network design for example, most of the time companies only have a single or a dual ISP connection for network traffic including VPN, web, email, cloud apps, and lots more. In such cases, management information flows through the same interfaces as user data. When management and data share this same plane, you end up using the data plane to access your network equipment. When you manage your equipment using such "In-Band" network, both data and control commands are traveling across the same network route, so your management plane has the same security vulnerabilities as your data plane. And you may find yourself locked out of the management plane because of the outage. While its cheaper to deploy and maintain such solution, its not resilient to attacks and outages and is also sometimes not secure since you mix user traffic with typically less strict access rules and management traffic.

Alternatively, you can run the management traffic via a stand-alone network which only handles management traffic. This is Out-of-band Management (OOB).

OOB gives you an alternate way to connect to your remote equipment such as routers, switches, and servers through the management plane, without directly accessing the device's production IP address in the data plane and independent of the primary ISP connection your company uses.

Below are some of the important key Aspects of designing an Out-of-Band Management network

Network isolation

Ensuring that the OOB management network is completely isolated from the production network is crucial for security and reliability. This isolation prevents any issues on the production network from affecting the management network.

Security

Security is paramount in OOB management to protect sensitive management data and prevent unauthorised access. Since OOB has a separate management plane and is not shared with production data plane, it is also inherently protected against any attacks on production data.

Accessibility

The OOB management network must be accessible even during production network outages or failures. This can be achieved by having separate and redundant access methods such has cellular and DIA/Broadband for OOB network.

Scalability and compatibility

It is necessary to choose OOB solution which can connect to multiple OEM production devices i.e. have maximum number of ports and is compatible with multiple OEM. Choosing an OEM specific OOB solution can cause problems in future digital transformation plans in terms of compatibility.

Storage

It is helpful to have OOB with storage on board, this not only helps with keeping the logs, but also with storing the configuration files, firmware images and patch file so they can be uploaded if any such issue occurs on production devices. Having capability of transferring files over cloud also makes it easier to deploy fixes.

TATA COMMUNICATIONS

How Tata Communications can help

Tata communications recommend a comprehensive suite of smart OOB management solution designed to meet the needs of modern network infrastructures. This solution while take care of the aspect highlighted above, is also complemented with a 4G/5G connectivity and performance SLA driven DIA or broadband connectivity.

To Achieve this, we partner with industry leader opengear and offer solution ranging from fully end-end managed solution with field ops hands and feet support to DIY models.

Below are some of the features of the solution Tata Communications offers and brief on how it handles the key aspect of designing the out of bank network

Lighthouse Service Portal (LSP)

Lighthouse Service Portal (LSP) is a cloud-based service that streamlines the initial provisioning of Open gear appliances into Lighthouse. This is a single pane of glass service portal which provides network professionals with a secure day a 0/1 provisioning experience, eliminating the traditional manual configuration methods, resulting in improved efficiency and productivity and reducing human errors.

Having this separate management portal also takes away the possibility of SPOF which arises from having to use SD-WAN management portal or production network OEM portal for both OOB and production network management. Lighthouse portal can also be deployed across multiple cloud zones/regional data centre to main data localisation for better performance and resiliency.

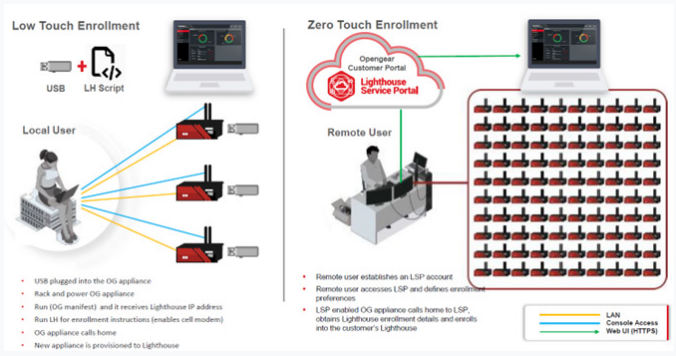


Figure 1 Lighthouse Service Portal Diagram

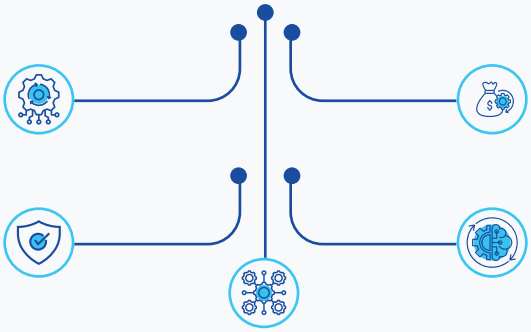
Smart Management Fabric (SMF)

As part of Lighthouse platform solution comes with the feature of Smart Management Fabric (SMF). SMF is the foundation for a modern management network. It is a network overlay that Open gear devices create, allowing out-of-band and resilient access to the IT infrastructure. It comes with below features

Key features:

Always-on OOB management:
SMF ensures Net Admins can access and manage their network even when the production network is down.

Resilient and secure:
The fabric maintains secure communication channels, and since it operates independently of the production network, it improves network reliability.



Cost efficiency:
By providing remote access and automation, it reduces the need for on-site technicians and minimises downtime.

Automated failover:
SMF detects failures and automatically reroutes management traffic via alternate paths (cellular/secondary WAN).

Centralised management:
SMF integrates with Lighthouse, enabling centralised control over distributed infrastructure, which is crucial for scaling.

Connected Resource Gateway (CRG)

As part of Lighthouse enhance, our solution is bundled with the feature of connected resource gateway. CRG is a proxy that allows clientless access to Web GUIs of connected virtual and physical network resources making access and management of these resources easier.

It also improves security by providing precise and granular RBAC based permissions and attributes (tags). CRG extends the Open gear solution beyond just console and management port access, making it possible for users to interact directly with the Web GUI of and network infrastructure devices. CRG gives Web GUI access to any/all network equipment. Net Admins can open multiple browser tabs and click back and forth between GUIs to resolve the issue quickly.

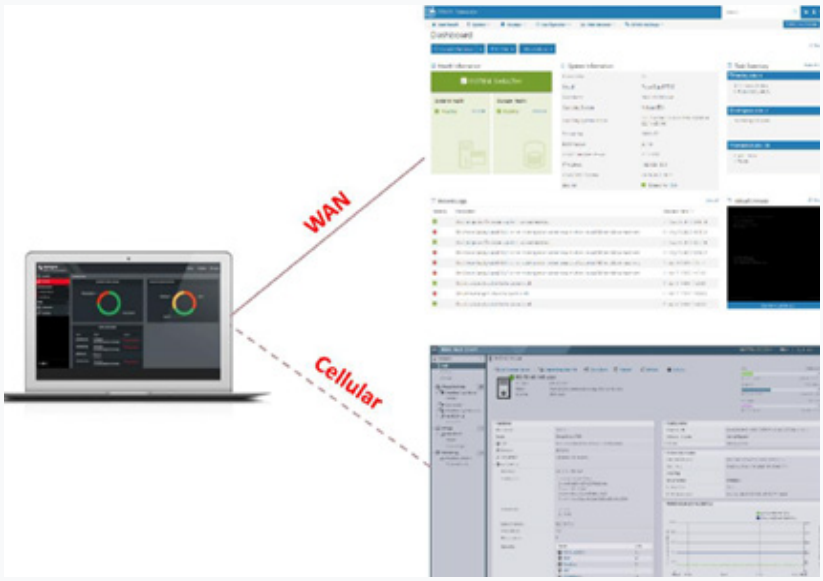


Figure 2 Connected Resource Gateway -Diagram

Leveraging these key features and many other, below is how tata communications handle all the key aspects of out of band management network

Network isolation

Solution deploys separate network and management plane for OOB to connect and communicate to production device. Customer also have an option having multiple WAN link such has 5G and DIA/broadband for resiliency.

Security

Opengear Smart OOB supports the industry's most stringent security, encryption and AAA requirements ensuring that management policies are continually and safely enforced. Our solution includes below features.

- Hardware level security with TPM 2.0 enabled.
- One secure network port tunnel all management traffic through default-deny SSH bastion tunnels
- FIPS 140-2 validated encryption
- Two-factor authentication using RSA and SecureID
- Complete user policy integration with off-load authentication to Radius, TACACS+ or LDAP Active Directory server
- Open VPN and IP-sec enterprise-grade PKI VPN remote access through default-deny SSH bastion tunnels
- Every device comes with a private SSL Certificate that encrypts communications between it and the browser
- Lighthouse supports the independent, concurrent use of both SAML and AAA authentication. SAML authentication is independent of, and does not interact with, other authentication methods.
- All Opengear products can perform two-factor authentication via remote AAA servers, such as RADIUS

Scalability and compatibility

Opengear nodes work with all the Major OEMs in the market, hence providing a future safe solution. These devices also have 24 serial port and 24 Port Switch which means you can have consol access to multiple devices by deploying just one (or two for resiliency) OOB device in data centre. The solution also has capability of being integrated with customer's internal tool via API.

Storage

While we have device with storage up to 64 Gb storage which is also expandable using external hard drive, and with the capability of service portal and reliable network connectivity, it has ability to deploy the patches/firmware remotely as well.

Customer can also use lighthouse instance's storage in cloud/on-prem orchestration platform to store configuration and firmware files.

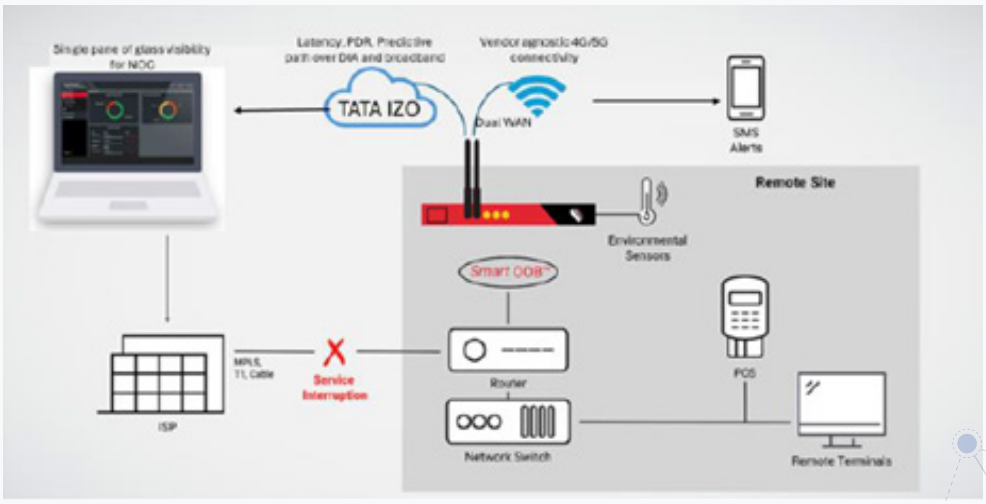


Figure 3 TATA Communications smart out of band solution

TATA COMMUNICATIONS

Tata Communications' value add

Tata communications with its help of extensive global coverage, footprint and partner ecosystem can not only deliver a reliable network connectivity but can also help customers in Deployment (Day 1) and Management (Day 2), below are some of the value-add tata communications can bring

Hands and feet support:

TATA Communications can provide field engineer support for Day1/Day2 activities across the globe which will negate the need of having to send resources from head offices, saving time and cost and result in reduce carbon emission because of reduced travel.

Warehousing:

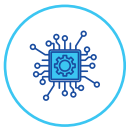
TATA Communication can store hardware at open/bonded warehouses to be shipped to location in case of RMA/IMAC saving on valuable time.

Day 2 support:

Our Day 2 support includes, 24x7 Monitoring and Alerts, assurance of Resilience and Redundant network setup, Proactive 24x7 Support.

Single hand to shake:

We can offer network, management, monitoring and break-fix service being a single hand to shake for the network related problems.



Focus on sustainability and operational efficiency:

In alignment with our commitment to responsible innovation, our Smart OOB solutions reduce the need for on-site technician dispatches, eliminate the carbon footprint from frequent site travel, and extend hardware lifecycle through remote patching and automation.

Network connectivity:

With TATA Communication's network presence in 150+ countries with industry leading SLA, allow customer to deal with just a single service provider for its network connectivity. TATA Communication is also a licensed SIM provider globally, we provider a vendor agnostic SIM which can connect to multiple mobile operators in a country allowing a exceptional reach in hard-to-reach areas.

Conclusion

Out-of-band management is essential for maintaining network resilience and ensuring continuous access to critical infrastructure. TATA communication's solutions offer Smart OOB including a service portal, providing a robust, secure, and cost-effective options for managing network devices. Compared to other solutions, we offer purpose-built solution, greater flexibility, centralised yet separate management from production network, and better integration with other OEM and a cost competitiveness with diverse network environments.

CONTACT US