Out-of-Band Management (OOB) involves the use of a dedicated channel for managing network devices. This allows the network operator to establish trust boundaries in accessing the management function to apply it to network resources.

Out of Band Solution for Branch Offices

OOB Secure Solution

Ganeshh Iyer
Overview

**Out-of-Band Management (OOB)** involves the use of a dedicated channel for managing network devices. This allows the network operator to establish trust boundaries in accessing the management function to apply it to network resources. It also can be used to ensure management connectivity (including the ability to determine the status of any network component) independent of the status of other in-band network components.

Implementation of an out-of-band management solution allows a network administrator to have full control over all the elements in wide area networks when in-band and IP based management strategies fail (via out of band connectivity). A comprehensive strategy for out-of-band management is a powerful tool in the arsenal of any administrator who desires a robust remote management strategy.

**CHALLENGE**

Maintaining network availability, while managing cost, is a challenging exercise in any data center environment. When the data center is implemented across buildings and locations, the task takes on a new level of difficulty. There are many tools for managing IT infrastructures remotely but some availability issues require physical access to systems to determine the nature of the outage. When the site is remote, system access has the added cost of travel or the expense of a remote resource. This brief explores management strategies that enable remote diagnosis and repair of IT system issues even when the primary network is down. Enhanced remote management capability helps IT managers exceed their availability goals while reducing costs.
 Secondary management networks (out-of-band) are becoming the standard at most large data centers but it is not always financially feasible to have redundant networks for out-of-band access at remote sites. Historically, a network outage at a remote site was resolved by dispatching a technician. This method was slow and costly. Today, IT managers commonly access and manage remote sites over an analog dial-up modem. However, some sites can be difficult to “wire” with analog lines or the installation could take several months. The cost of provisioning an analog line can also be prohibitive at certain sites.

## OUT-OF-BAND MANAGEMENT SOLUTION

Open gear Console Server variance models to achieve Out Of Band Management for Data centers and branch sites of CUSTOMER Network. Network devices console port will be connected with Open gear devices (RJ45 jack) via Rollover cable.

Below design depicts OOB solution to access the CUSTOMER Data Centers & Branch Sites Network Devices.
A 3G/4G SIM or ADSL Broad Band Connection to remote branch location with min bandwidth connectivity at each site, Open gear boxes are capable to run IPSEC VPN tunnels with Data Center Firewall.

Branch location can have 3G/4G or ADSL Broad Band connection with dynamic public ip address, IPSEC Tunnel will be created dynamically based on traffic initiated from DC for Console Server at Branch Location.

Traffic will be secure over the tunnel and additionally box can act as Firewall for more security.
REMOTE ACCESS MANAGEMENT

Secure access is available through the following local (analog console port) and remote (digital IP and dial-up) options:

- **Mgmt. Port:** Open gear management port should be connected in management segment and should be configured with in-band management IP address via Cat6 straight through cable.
- **2*1 10/100/1000 Ethernet for WAN connection from providers**
- **Console connection:** An administrator can log in either from a local terminal or from a computer with a terminal emulation program that is connected to the console port and can use the CLI utility.
- **SSH & Telnet:** An authorized user can make a Telnet, SSH v1, SSH v2 connection to a target device.
- **Web Manager:** Users and administrators can perform most tasks through the web manager (accessed with HTTP or HTTPS). The web manager runs in Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari on any supported computer that has network access to the console server. The list of supported client browsers and their versions are available in the release notes.

SECURITY

Security profiles determine which network services are enabled on the console server. Administrators can either allow all users to access enabled ports or allow the configuration of group authorizations to restrict access. You can also select a security profile, which defines which services (FTP, ICMP, IPSec and Telnet) are enabled.
AUTHENTICATION

Authentication can be performed locally, with One Time Passwords (OTP), a remote Kerberos, LDAP, NIS, RADIUS, TACACS+ authentication server or a DSView 3 server. The console server also supports remote group authorizations for the LDAP, RADIUS and TACACS+ authentication methods. Fallback mechanisms are also available.

For authentication following are the best possible options:-

1. **Role Based User :**

   This is the primary method for authentication. Below users will be authorized to access the Open Gear device as per their role.

   - **Admin:** Admin will have full privileges (Read-Write) over Open gear device.

   - **Operator:** These users will have limited access over Open gear device. And these users will only be connected to take console of the network devices.

2. **Role Based User : Local Authentication as a fallback method**

   If AAA server goes down, Local user authentication as fallback option to access Open gear device. Local users will be configured as Admin and Operator as mentioned below.

   - **Admin:** Admin will have full privileges (Read-Write) over Open gear device.

   - **Operator:** These users will have limited access (Read-Only) over Open gear device. And these users will only be connected to take console of the device.

3. **Local Password Change Policy**

   To change the passwords, recommended to follow the CUSTOMER password change policy standard.

   If any network associate leaves the organization, his credentials will be disabled immediately and admin password will be changed accordingly.
Out of band management gives direct benefits:

- Secure in-band and out-of-band network remote management
- Streamline installation and configuration with Zero Touch Provisioning
- Eliminates adaptors for Cisco pin-out conversions
- Compliance with data center access and security policies – customizable, multiple access levels
- Integrated power management
- Centralized management
- Automatic event tracking and notification of fault conditions
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>OOB</td>
<td>Out Of Band</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection Systems</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention Systems</td>
</tr>
<tr>
<td>ROI</td>
<td>Return on Investment</td>
</tr>
<tr>
<td>FW</td>
<td>Firewall</td>
</tr>
<tr>
<td>RTR</td>
<td>Routers</td>
</tr>
<tr>
<td>SW</td>
<td>Switches</td>
</tr>
<tr>
<td>CMS</td>
<td>Central Management System</td>
</tr>
</tbody>
</table>