The Distributed Enterprise:

Remote Access and Management of IT Infrastructure

A White Paper from Raritan

Overview

While the proliferation of branch and remote offices is a positive sign of company growth, it can be a challenge for IT staffers. Besides managing data centers, IT teams take on the additional responsibility of managing and repairing branch office assets like routers, switches, firewalls, WAN optimizers and servers. Employees who work in these remote locations typically do not have the IT skills to trouble-shoot problems. To overcome this challenge, many IT staffers use remote access software to diagnose and repair branch office problems. However, these tools are only useful if the OS and network are functioning. If the network or OS is down, an on-site employee might be asked to go to the server closet and address the problem. If that doesn't work, then additional costs in travel, time, and lost business might be incurred.

This paper addresses the added value (in terms of uptime and security) of out-of-band access and control tools for branch offices.

Challenges in the Branch Office

It's estimated, by the Internet Research Group, that in the United States alone there are more than 1.5 million branch offices with direct communications back to headquarters. And this does not take into account kiosks, ATMs and other self-service transaction locations.

While branch offices broaden the reach of businesses, they also broaden the burden of IT managers who are responsible for the installation, monitoring and mainte-nance of technology assets in these various locations. These assets can include networking devices, such as routers, switches, WAN optimizers and firewalls. They can also include distributed application and storage servers for transactions and e-mail.

The challenges associated with managing remote offices break down into the following categories:

Control and Complexity

Branch office networks can have an array of hetero-gonous components in terms of devices and manufactur-ers. The increasing complexity of these networks brings an increased concern about failures and how to fix them. Also, with hundreds, or potentially thousands, of IT assets spread out across the globe, the need for a centralized dashboard to manage these devices becomes critical.

Security

Many branch offices, especially retail locations and banks, contain sensitive customer information and/or credit card data that can be vulnerable to intrusion without the proper safeguards. The proliferation of Wi-Fi in branch offices adds yet another layer to this security concern.

Limited Budgets and Resources

Typically, remote offices do not have their own dedicated IT staff. In this common scenario, it is incumbent on the HQ-based IT administrators to diagnose and correct networking and server problems. Sometimes, this involves traveling to the location to troubleshoot, which can increase the Mean Time to Repair (MTTR) as well as increase costs from travel expenses. Another option is to hire a service provider to do a "truck roll" to the location, which can also be costly. If the problem is critical and must be corrected immediately, then travel might not be an option. Remote access tools become an ideal way to log in and correct IT issues at branch offices and remote locations. Most remote access solutions are segmented into in-band and out-of-band categories.

In-Band Access Options

Remote Management Software

This type of solution enables IT administrators to access the desktop and applications running on target servers. A significant limitation of remote management software is that it requires that the target OS is available. If the operating system is frozen or crashes, then the server cannot be accessed. In addition, these software solutions are dependent on a connection to the target server's network interface card. If the network is unavailable, then this also becomes a roadblock to repairing the problem.

Table 1 illustrates the gap betweek remote access software and out-of-band options like KVM-over-IP

Terminal Emulation Protocols

Telnet and its encrypted counterpart SSH are used to access and configure devices with serial ports: routers, switches, firewalls, power distribution units and servers. Like remote management software, this access method is only as effective as its network connection.

If there is a problem with the WAN, then an IT professional might be required to go to the remote location to make the repairs. In addition, these maintenance interfaces can make branch offices more vulnerable to network intrusion since hackers could use these same interfaces to steal data and plant viruses.

The Gap Betweek Remote Access Software and Out-Of-Band Options Like Kvm-Over-IP

	In-Band	Out-of-Band
Tasks	**Remote Access Software**	**KVM-over-IP**
Remote access to servers	Yes	Yes
BIOS-level access	No	Yes
Modem access if network is unavailable	No	Yes
User profiles, port-level permissions	No	Yes
Support for multiple users, concurrent sessions	No	Yes
Warm rebooting	Yes	Yes
Cold rebooting	No	Yes*
Logging	No	Yes

*When used with remote power management   Table 1

The Security Advantages of an Out-Of-Band Alternative Like A Secure Console Server

	In-Band		Out-of-Band
Tasks	**Telnet**	**SSH**	**Secure Console Server**
Secure Appliance	No	No	Yes
Modem access if network is unavailable	No	No	Yes
Encryption	No	Yes	Yes
Customize TCP Ports	No	No	Yes
Strong Password	No	No	Yes
Password Retry Lockout	No	No	Yes
SYSLOG	Yes	Yes	Yes
Keystroke Logging	No	No	Yes
Security Login Banner	No	No	Yes

Table 2

Out of Band Options

Secure Console Servers

The common denominator of most branch office IT deployments is network connectivity, which typically requires a router, switch and firewall. If these components fail in a remote location, then business can suffer. Most networking equipment have serial interfaces and, as mentioned above, in-band tools like SSH and Telnet are common methods of accessing and maintaining the gear. Unfortunately, if there is a problem with the network then these access tools might be useless.

Secure Console Servers (SCSs) provide remote access to serially-managed servers and other serial devices via SSH/Telnet and Web browser. One advantage of SCSs is that they provide one point of access and control to serially-managed servers, WAN equipment, networking gear and power control devices. Another advantage is that they can provide modem access if the WAN is unavailable, which can prevent a trip to the remote location and speed repair time.

"Once we made a mistake, causing our firewall to lock up, so we couldn't connect through the network. We ended up having to send someone to the site, console into the server and restart it. If we had the Dominion® SX at that time, it would have taken five minutes to fix. I think that was the incident that made it mandatory for us to add Raritan's secure serial console server solution to our IT infrastructure."

- KEVIN BYRNE
Network Operations Engineer,
Charter Communications

Consider the following when selecting a console server:

Rights and Authentication
- Local Accounts
- Port-level access
- Strong Passwords
- Support for Active Directory, LDAP, RADIUS, TACACS+

Console Features
- Logging
- SNMP traps
- Solaris key trapping
- Shared access

Management Features
- E-mail alerts
- SNMP support

Access Methods
- SSH
- Telnet
- Web interface
- Dial-in option

Facilities Management
- Dual power
- Power management
- CAT5 cabling

KVM-Over-IP

KVM switches provide the ability to access and control servers that have a Keyboard/Video/Mouse interface. They simulate the experience of being inside the data center and accessing the server directly.

KVM-over-IP switches provide the same experience, but over a secure IP connection. One significant advantage of this is the ability to access servers from anywhere, which makes it ideal for accessing and controlling servers in remote offices. Whether IT administrators are at their HQ location or at home at 2 a.m. in a snowstorm, they will have access to their branch office assets.

What's more, KVM-over-IP switches provide both in-band and out-of-band access. In other words, the IT staff can access and control their servers either at the OS/application level or at the BIOS level if the OS is unresponsive. For extra peace of mind, KVM-over-IP switches with integrated modems provide an alternate access method in the event of a network failure.

Additional value-added features like Virtual Media enable IT staffers to transfer files from their desktop, CR-ROM or USB stick to servers across the globe. This is an ideal tool for upgrades and patches that need to be installed at numerous remote locations.

The KVM-over-IP Buyers' Guide lists the following considerations when selecting a switch:

True Anytime/Anywhere Resource Access
- Multiplatform support
- Browser/desktop compatibility
- IP and modem access
- No-cost, downloadable client
- Non-blocked access via local ports
- Full remote power control
- Virtual Media access

Appliance-Based Solutions
- Ease of implementation
- Size and port density
- Reliability and uptime

Level of Security and Performance
- Minimized vulnerability
- External and internal access controls
- Syslog support
- Data encryption
- Strong password support

Intelligent Power Distribution Units

There are times when cold rebooting is required as a last-resort method to fix a problem. While switched Power Distribution Units (PDUs) are typically associated with remote power cycling, some PDUs are equipped with intelligence to provide additional monitoring capabilities. In a branch office, where IT equipment is typically relegated to a closet or small room, it is important to be notified when environmental factors and power utilization exceed user-defined thresholds. For example, electrical closets in small offices often suffer from poor ventilation and cooling and may have only one electrical circuit that is shared with other equipment. Monitoring the closet temperature and IT equipment current draw can prevent a network outage or equipment damage.

When selecting a remote power management solution, take into consideration the following capabilities:

- Remote serial and TCP/IP access to outlet-level switching
- User-configurable, outlet-level delays for power sequencing
- Unit-level and outlet-level power monitoring and utilization information
- User-defined thresholds
- Alerts via SNMP, e-mail and syslog when thresholds are exceeded
- Up to 256-bit AES encryption and strong password support
- Advanced authentication and authorization options including outlet-level permissions and LDAP/S, RADIUS and Active Directory®
- Support for HTTP, HTTPS, IPMI, SMASH-CLP, SSH, Telnet and SNMP

Centralized Management

Having tens, hundreds or over a thousand locations to manage can be a daunting task. Even with KVM-over-IP, secure console servers, Embedded Service Processors (iLO, DRAC, RSA) and intelligent PDUs to address remote troubleshooting challenges, the need to track all

of these heterogeneous assets in a consolidated view is essential. Consider a centralized management solution that can support a wide breadth of devices, as well as advanced security and authorization capabilities.
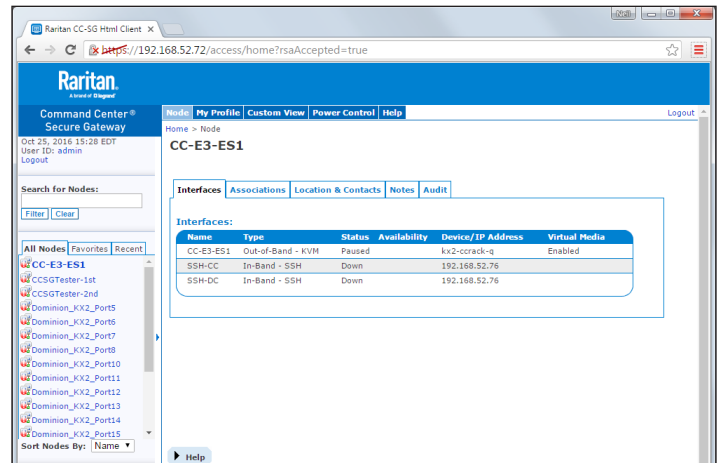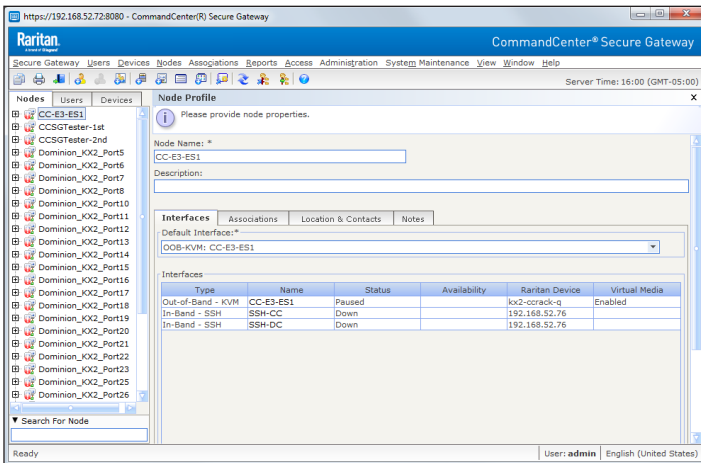
Sample screens of CommandCenter® Secure Gateway, which provides centralized access and management of IT devices.

Conclusion

While there is no substitute for having an IT professional in each branch office location to keep things running, this is a luxury that few businesses can afford. The next best solution is to have the right tools that extend the reach of HQ-based IT staff to the remote locations. While some tools are currently available for what seems like little or no cost, there is indeed a cost in terms of sacrificing availability and security. This can result in unforeseen travel expenses and downtime, which is what remote access solutions are meant to avoid. The gaps left by in-band access tools can best be filled with out-of-band solutions.

For additional information on how Raritan can help you manage and maintain your remote office networks, please visit **Raritan.com/branch-office-management**

About Raritan

Raritan, a brand of Legrand, is a trusted provider of rack power distribution units, branch circuit monitors, transfer switches, environmental sensors, KVM-over-IP switches, serial console servers, and A/V solutions for data centers and IT professionals. Established in 1985 and based in Somerset, N.J., Raritan has offices worldwide serving customers in 76 countries. In more than 50,000 locations, Raritan's award-winning hardware solutions help small, midsize, enterprise, and colocation data centers to increase efficiency, improve reliability, and raise productivity. And provide IT departments with secure, reliable remote access tools needed to manage mission-critical environments. For more information, visit us at Raritan.com.