From slow to smart – the changing face of remote management technology

Information technology (IT) is going through an interesting evolution as the twin forces of centralisation to the cloud meets the increasingly decentralised device landscape most notable with the rise of smart mobile devices and Internet of Things. IT administrators are now effectively managing more users, devices, applications and networks than at any time previously yet staffing levels are still small in comparison to other business administration functions. This article examines how key remote connectivity technology developments, evolving best practice including security, and automation enable IT administrators to reduce their burdens and enhance the delivery of end-to-end services.

Access and management become smarter

Remote management once meant connecting a dial-up modem to a serial console port on the site's primary server or router. For sites with multiple pieces of critical networked infrastructure, an asynchronous serial terminal server was used to multiplex consoles behind a single port. These solutions were a crude but effective method of establishing point-to-point connections for performing maintenance or remediating a network outage remotely, whenever there was no one qualified close by.

The terminal servers of 20 years ago have evolved into today's out-of-band console servers and remote monitoring and management gateway devices, and they do a lot more than proving remote access to consoles. A new class of device has emerged, known as Smart Out-of-Band (Smart OOB). These devices are management platforms in their own right, integrating troubleshooting tools and capabilities including remote power control – they function as virtual remote hands, aiming to provide the remote operator with the same level of control as if they were physically present. Smart OOB is intended to provide always-available remote access and control of distributed IT, power and network systems – enabling remote setup, ongoing maintenance and disaster recovery of mission-critical infrastructure, even when the network is down.

This new class of solution extends upon traditional out-of-band management to also monitor and log systems health and environmental conditions, proactively detecting faults before they become failures. IT administrators can set automatic triggers for performing tasks and program the Smart OOB out-of-band solutions to monitor the physical environment and devices, and automatically detect and resolve issues.

The switch to cellular

Another big change over the last decade is the choice of out-of-band connection. Although a lot of PSTN lines are still deployed as the "last resort" connection, the most common method especially for remote sites and cabinets is the use of 3G and increasingly 4G/LTE cellular networks.

The reason for the switch to cellular is twofold. Firstly at a technical level, although dial-up speeds are sufficient for multiplexed access to serial console ports, which is enough to fix a remote routing issue, dial-up is frustratingly slow for graphical management sessions using RDP or KVM. The always-on IP and extra bandwidth of a cellular connection also allows for continuous reporting of network infrastructure statistics back to head end monitoring systems. PSTN lines are a technology path that is also being phased out in many countries for new deployment.

DSL is an alternative as an out-of-band connectivity solution but admins need to take care in how it is deployed. In many designs, DSL networks will have the same single points of failure such as trunking into a building or local exchanges that could impact the primary IP network, even when using different carriers. When deploying DSL as the Smart OOB connection method it is worth examining what would happen in the event of different failure issues including physical issues such as damage to cabling.

Cellular has proven popular due to almost total global coverage while the cost of 'data only' plans has dropped along with a growing diversity of carriers. The cost of Smart OOB over cellular can be further minimised with a management device that routes via the site's primary Ethernet network, only bringing up the cellular IP connection when network troubles are detected, or in response to an SMS command from a trusted number.

Using a northbound VPN or reverse SSH tunnel gives you inbound access using a cheap consumer grade SIM without having to pay extra for a public IP.

The cellular landscape is evolving rapidly as faster speeds with little latency emerge with newer LTE-A standards offering deliver tens of megabits per second while still on the horizon 5G promising gigabit connections. Cellular also has the benefit of allowing connectivity to infrastructure that is mobile, for example on vehicles or temporary structures such as kiosks or vending machines. This especially proves useful for locations that are difficult to wire via a traditional fixed link such as construction sites and remote rural areas.

Management and security

Smart OOB devices have also gained more functionality than just simple console access via the serial port. Many of these devices have adopted support for next generation management interfaces, such as USB, and dedicated management LAN Ethernet ports for tight integration with IPMI lights-out-management cards. With continuous infrastructure status monitoring and alerting features, admins get immediate notification by email, SMS or SNMP trap when there is trouble brewing at remote sites. Being directly attached to critical network infrastructure console ports, out-of-band management devices couldn't be better placed to detect the first signs of trouble.

Another key consideration is security, both in the physical and remote access sense. Although IT is increasingly buried within highly protected and centralised data centres, there is still a lot of remote infrastructure that resides out in the field. Best practice says that all equipment should be kept under lock and key with physical access potentially monitored by local sensors such as door open sensors on racks or even CCTV for highly secure infrastructure. At the Smart OOB level, most vendors now support FIPS 140-2 validated encryption and security features such as VPN and remote AAA, to enable secure remote access over public IP networks. However, it is advisable to also ensure that access to Smart OOB is integrated with any Privileged Access Management platforms such as BeyondTrust, CyberArk and Oracle where available.

There is a growing trend towards interoperability with third-party central monitoring and management systems – the Smart OOB management devices act as distributed agents for Nagios, SolarWinds, and other vendor-specific tools, to form the framework of a whole-of-enterprise infrastructure management system.

Automation reduces complexity

This level of integration within operational, management and security frameworks enhances the value of Smart OOB systems which is further supplemented through the use of an advanced automation system often referred to as auto remediation. This auto remediation capability uses a scripting language that uses logic and conditional checks to attempt to ascertain the status of connected devices and in the event of an issue, conduct automatic escalating remedial actions.

This process of automation can include a number of pre-defined scripts for example to check that a device is accepting connections, or that an SNMP status check delivers an acceptable response. However, admins also have the option to build custom automation scripts as Smart OOB platforms support embedded Linux operating systems and GNU bash shell scripts that can be run manually or automatically.

Scripts can be as simple or as complex as the admin chooses and are particularly useful for bespoke applications or non-standard hardware. For example, a custom script could ping a target device and then power cycle the device in event of a ping request failure. The scripts can also take data from connected devices for example environmental sensors or door opening sensors with scripts sounding physical alarms as well as sending email, SMS or IP based alerts to pre-programmed users or to linked network management software platforms. This increased level of overall automation helps IT administrators free up operational resources to focus on value-add applications and problems.

IoT future

Although remote access technologies have evolved dramatically over the last decade, the next few years have just as much potential for further changes. All the talk of the Internet of Things (IoT) from smart-meters to traffic lights is great for the new devices that are designed with built in 3G/4G links. Unfortunately, the vast majority of deployed infrastructure needs to be retrofitted with wireless connectivity to unlock the benefits of IoT. For many applications, Smart OOB over cellular offers a low cost way to reach this goal and the programmable and highly flexible nature of the technology makes it a good fit for both IT equipment and devices within areas such as

healthcare, transportation, building management and utility sector that largely have serial ports for access to the equivalent of a console server.

For the IT admins that may well be looking after an increasingly diverse set of devices attached to the IP network, Smart OOB technologies will become less of a last resort and more of a first port of call when it comes to managing critical infrastructure.