



Remote Server Management for Data Center Professionals

by Barry Nance, Network Testing Labs

Raritan Computer Europe.
July 2004

Copyright and Trademark Information

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without express prior written consent of Raritan Computer, Inc.

© Copyright 2004 Raritan Computer, Inc., CommandCenter™, Dominion™ and the Raritan company logo are trademarks or registered trademarks of Raritan Computer, Inc. All rights reserved. Java® is a registered trademark of Sun Microsystems, Inc. Internet Explorer® is a registered trademark of Microsoft Corporation. Netscape® and Netscape Navigator® are registered trademarks of Netscape Communication Corporation. RC4® is a registered trademark of RSA Corporation. Other trademarks or registered trademarks are the property of their respective holders.



Table of Contents

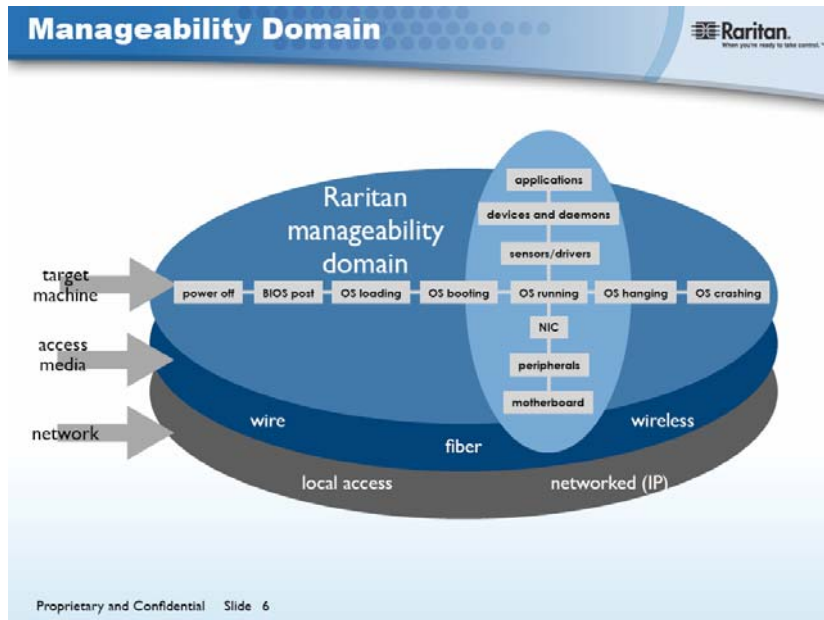
1.	Introduction	1
2.	Who Needs KVM Access?	3
2.1.	At the Rack.....	3
2.2.	Across the Hall.....	3
2.3.	Remote Data Center Access.....	3
2.4.	Remote Office Access	4
3.	KVM-over-IP Technologies	6
3.1.	Bandwidth Constraints	6
3.2.	Security.....	7
4.	Server Access Issues and Challenges.....	8
4.1.	Performance	8
4.2.	Security.....	8
4.3.	Flexibility	9
4.4.	Ease of Use and Installation	9
4.5.	Costs.....	9
5.	Conclusion	10
6.	About the Author	11
7.	About Network Testing Labs.....	12
8.	Raritan Computer – Profile	13
8.1.	About Raritan Computer	13

1. Introduction

Today's distributed, complex IT infrastructures -- made up of heterogeneous servers, routers, switches and other devices -- are challenging environments to control and manage. IT departments are charged with maintaining operations performance throughout the enterprise -- from headquarters' data centers to remote offices -- in order to support business initiatives, while keeping costs down.

The financial consequence of IT Infrastructure downtime on companies can be severe in terms of lost business, loss of user/customer confidence, labor costs incurred to fix the problem, overhead fixed asset costs associated with technology upgrades and repairs and punitive costs imposed by contracts (Service Level Agreements) with internal or external clients. Depending on the industry, the cost of IT down time can range from hundreds to millions of dollars per hour.

In sophisticated distributed IT environments, software solutions, such as IBM's Tivoli®, Computer Associates' UnicenterTNG® and HP Open View™, monitor for the functionality of devices on a network. They are designed primarily to discover faults and to alert network administrators. However, their device management functionality is limited to what can be accomplished when accessing the target device via the network interface card (NIC) (See Figure 1) and when the devices operating system (OS) is healthy. If the network is down, or the device OS has hung or crashed, restoration of service still depends on dispatching IT technicians to diagnose the problem and take corrective action.



For remote office management, some companies use software utilities like Carbon Copy®, Windows® Terminal Services and PCAnywhere™. Like the more sophisticated data center software solutions mentioned above, these low cost solutions also have limited access and control capabilities, and also depend on a healthy operating system on the target device. In addition, some software solutions only work with certain servers and devices, requiring the purchase of multiple remote control products. The result is an environment with multiple logins, different user interfaces and other obstacles to managing a server closet. While this may be acceptable for remote office application administration, it falls far short of what's needed for OS and server administration. BIOS-level control or console-level control is critical in bringing up a down server, because users can still control a computer via the KVM ports, even when the operating system is not functional.

This is where hardware-based KVM (keyboard/video/mouse) and serial console management tools are so productive. They help IT professionals restore service and fix device-related problems without ever having to come into direct physical contact with the actual devices.

With the right KVM technologies and tools, data center operators can work more productively whether inside or outside the data center. They can troubleshoot, configure, maintain and, even reboot, IT equipment – just as if they were physically present at the rack, even if (and especially when) the server or the network is down. In addition to being able to handle problems far more adeptly, KVM solutions enable a greater level of preventive maintenance. They also save valuable data center and remote office space by eliminating multiple keyboards, monitors and mice, as well as cable.

Some KVM solutions operate independent of the network – or out of band -- and route keyboard, video and mouse signals along a dedicated cable from servers to the KVM switch. These analog KVM solutions are ideal for managing servers from up to 1,000 feet from the data center.

For extended remote access, digital KVM -- or KVM-over-IP -- solutions are ideal because they use IP-based networks to extend the managerial reach of data center operators. Prior to being routed over a TCP/IP IP network, analog keyboard, video and mouse presses are converted into digital signals. Systems administrators can use the Internet to log in from anywhere and immediately implement a fix. Server administrators no longer have to travel to remote sites or to headquarters in off hours in order to answer alarms and fix faults.

Not only does remote-access KVM enable IT staffs to be more responsive and productive, it also enables companies to leverage their IT resources better. Virtual IT teams, for example, can be assembled for specific projects or to solve specific problems, regardless of geographic location.

Not all remote KVM solutions are equal. This paper identifies and explores the issues an IT manager should consider in order to select the right KVM solution. It explores the type of access that data center staff need – whether they work at the rack, across the hall or around the world.

2. Who Needs KVM Access?

To a large extent, the KVM products in use in the company determine the effectiveness, productivity and efficiency of the data center staff. No matter how near or far a data center operator is from the servers, the operator needs responsive, reliable, secure and easy-to-use server access in order to configure, change or fix any server problem in the shortest possible time. Typically in enterprises administrators need 3 modes of responsive, reliable access to servers.

2.1. At the Rack

Some people need “at the rack” access to multiple servers because they are operators whose work includes inserting CD-ROM disks, changing tape cartridges, setting up new servers and, once in a while, replacing failed power supplies, network adapters or hard disk drives.

Data center operations, configuration and repair personnel – who work inside the data center – typically interact with individual servers through a simple, direct-connect analog KVM switch. All the KVM cables from the servers in a pool or subgroup connect directly to a KVM switch, which in turn has a physical keyboard, monitor and mouse attached. For multiple concurrent user access, some KVM switches offer connections for up to 16 user stations and some manufacturers support even more concurrent users when multiple switches are cascaded or stacked.

The local KVM devices might connect via coaxial or Unshielded Twisted Pair (UTP) Category 5 cables. These Cat5 cables offer superior bandwidth within a local area, up to about 1,000 feet.

Some manufacturers’ KVM switches can be daisy-chained or cascaded to handle a large numbers of servers. Other solutions, specifically digital KVM solutions can scale to thousands of servers by just adding switches to the network, each switch with it’s own IP address.

2.2. Across the Hall

A different group of IT employees – consisting of capacity planners, troubleshooters and network engineers, who might be across the hall or somewhere within a campus – also need to operate servers, but these employees don’t need to be at the rack.

This group needs KVM connections that carry signals over greater distances than ordinary coaxial KVM cables can carry. An adjacent room/floor computer operator needs KVM switch equipment that makes it seem like he or she is right next to the server. While UTP Cat5 is appropriate for campus locations within 1,000 feet of the servers, fiber-optic cable is a good solution for distances up to about six miles. KVM-over-IP connections are also a good alternative.

2.3. Remote Data Center Access

Still other people, including centrally located, high-level operations center managers, require remote access to servers. These employees may be located at headquarters or in another state or country.

These operators need KVM connections that operate over a network – WAN, VPN or the Internet. Using an IP network to access and manage servers in a remote data center is termed KVM-over-IP. Data center operations people get a special, convenient capability in KVM-over-IP but – depending on the KVM vendor – KVM-over-IP presents tradeoffs in bandwidth utilization and responsiveness.

Addressing these tradeoffs means making sure the vendor's KVM over IP tools provide a level of encryption, compression and bandwidth control to meet current and future security and performance requirements.

2.4. Remote Office Access

In addition to needing remote access to servers in the data centers, IT staffers are often also responsible for managing servers and networking equipment located in remote offices and branch offices. This remote office equipment can consist of a wide variety of devices including:

- KVM controlled servers including: Windows, Linux and Solaris servers
- Serial console controlled devices including: routers/switches, firewalls, network appliances, HVAC controls, security systems, telecom controllers and headless servers (UNIX, Linux, Solaris)

Usually, employees located at these remote sites do not have IT expertise and therefore do not have the skill set to troubleshoot and manage the infrastructure. In some cases, data center staffers use software solutions to address remote infrastructure maintenance. However, software solutions only work if the network is up and, in the case of servers, if the server OS is healthy. When the network is down, or when the server OS has crashed, on-site employees are often asked to "go to the server closet and press the reset button," and then if the router or server does not come back up, a truck has to roll.

For these situations, the ideal solution is an "all-in-one" box that contains both KVM ports and serial console ports, and is available in port densities that make it cost effective for remote office use. For example, 4 KVM ports and 4 serial ports. It is important that you choose a device that also has a built-in modem, because if the network edge device at the remote location is a router, and the router goes down, the only way to get to the router to bring it back up without rolling a truck, is to dial-in, through the modem, to the "all-in-one" box and access the router through the serial console port.

The following chart summarizes KVM connectivity options for the three IT groups. It's important to select the best solution for each situation. KVM solutions that use Cat 5, coaxial and fiber-cable connections address security and bandwidth issues, but have limitations in distance. IP, of course, provides the greatest distance, but there may be some slight delay in the keyboard and mouse signals. There are also hybrid solutions that combine analog and digital KVM switching technologies.

Location	Distance to servers	Typical cabling
Data Center	Local/direct access up to ?? feet	Coaxial
Data Center	Local/direct access up to 1,000 feet	UTP Cat 5
Campus	up to 1,000 feet	UTP Cat 5
	up to 6 miles	Fiber optic cable
Remote Branch Office	Any	Wide Area Network (WAN) (T1, Frame Relay, etc.) Dial-up
From the operator's home	Any	DSL, cable modem, dial-up

The various manufacturers have implemented KVM technologies with varying degrees of success regarding responsiveness, bandwidth utilization, security, scalability and other factors. Some vendors of server-access equipment and technologies offer products that focus on the needs of one of the three groups and then, inappropriately, promote using the same "solution" for the other groups.

Make sure the KVM vendor can provide an integrated, platform-neutral solution that any authorized person from any of the three work groups can use anytime, from anywhere. Keep in mind that fixing IT problems often entails more than having server access; an IT troubleshooter may very well need access to serial (RS-232) devices, such as routers, switches and headless Sun servers. Furthermore, if there are several remote locations, a solution is needed that makes it simple and easy for data center staff to access devices in far-flung sites. The ideal KVM system also provides a single, consistent view of all the data centers' and remote offices' equipment and provides features, such as an intuitive user interface and single sign-on.

In addition, the KVM tools should scale well, support multiple simultaneous users, work with multiple platforms, have flexible access options and be backward compatible with any existing KVM gear.

3. KVM-over-IP Technologies

The technology for sharing monitors, keyboards and mice among myriad servers and devices has come a long way over the past few years. From rudimentary A/B switches to analog KVM boxes with limited -functionality to unprecedented access-and-control analog and digital KVM enterprise-class systems, KVM technology is now a critical part of an enterprise's overall IT management strategy.

A data center operator using KVM-over-IP might be many miles from the server, but he or she can start or stop software, reconfigure the server's software settings and reboot the server – as if being physically in front of the server. The operator can even access BIOS-level computer configuration data.

KVM-over-IP technology turns a network-connected client computer into a server console. The technology encodes keypresses, mouse movements and mouse clicks into TCP/IP packets the client sends to the server and it similarly encodes the server's video signals into TCP/IP packets the server sends to the client. Each vendor has an upper limit on the video resolution it supports, so making sure a vendor's products will work with the server resolutions that operators now use or will use in the future is critical. Most KVM vendors support a maximum video resolution of 1280 x 1024, with a refresh rate of 60 Hz. Rarely, but significantly, will a vendor support even higher resolutions.

3.1. Bandwidth Constraints

The KVM-over-IP client, ie. the user station, whether a PC or notebook computer or wireless device, typically links to an IP network via a moderate-speed DSL or cable modem connection or perhaps a relatively slow-speed dial-up connection. The number of concurrent users will also affect KVM-over-IP's bandwidth utilization.

Unfortunately, the remote operator may very well experience sluggish responses from the server because of bandwidth limitations between the client and the server. Waiting for a keypress to show up on the remotely connected server screen or waiting for a mouse cursor to catch up to the operator's mouse movements is annoying and unproductive. Moreover, if the KVM tool isn't properly designed, multiple concurrent operators accessing a bank of servers can slow each other down.

A very important factor is the volume of data the KVM client and server exchange over the network, especially for a high-resolution server screen – KVM-over-IP video signals can consume significant network bandwidth. Furthermore, if the KVM-over-IP software isn't designed well, multiple operators working over the same network connections can use up available bandwidth and slow the network to a crawl.

KVM vendors use two technologies to reduce the network bandwidth required to transmit large volumes of video data. First, a KVM system keeps track of what is already showing on the operator's screen and only sends changed data, called deltas, over the network. Sending just deltas to the client, rather than always sending entire screens, dramatically reduces bandwidth utilization. Note that some KVM vendors have better quality algorithms for determining the deltas and thus use the network more frugally. Lastly, a KVM system compresses the deltas before transmitting them. Because some vendors have more efficient compression algorithms, the size of the resulting compressed delta varies widely across vendors.

Also note that selectively and intelligently controlling video parameters, such as the amount of color information the KVM system transmits, affects bandwidth utilization. In some implementations, a KVM system will actually allow operators to “tune” the system’s transmission of video data. For example, the operator can choose to reduce the color depth and view a screen with fewer colors in order to improve KVM system performance and responsiveness for slower connections.

In addition, some solutions can be programmed to automatically restrict the amount of bandwidth available to users, so that more critical applications are not constrained. A truly ideal KVM solution that’s bandwidth-aware allows the tuning of bandwidth utilization on a user-by-user basis. For some network-intensive organizations, using a second, separate network just for KVM access can alleviate bandwidth issues.

3.2. Security

The best KVM solution should offer data security and authentication through a data encryption scheme, such as Secure Sockets Layer (SSL) and it should not require major firewall configuration changes. In the best of all possible worlds, the KVM-over-IP tool would require the opening of only a single port on the firewall. The ability for a KVM-over-IP solution to work across a Virtual Private Network (VPN) is also a big plus.

For security, some vendors employ a 128-bit encryption standard, which can also affect bandwidth utilization and overall performance. Encryption should be used in both the SSL communications and in the data stream transmitted between remote clients and servers. In addition, some vendors only encrypt the keyboard and mouse signals, leaving the video un-encrypted, which is not as secure as systems where the keyboard, mouse and video are encrypted.

To control access to vital Active Directory structures and other critical administrative data, the KVM-over-IP product should work with all industry-standard security protocols, including Windows NT authentication (NTLM), Lightweight Directory Access Protocol (LDAP), Radius, Active Directory and TACACS+. Security support should be built into the KVM-over-IP product and not require the purchase and configure of a separate server computer just for KVM-over-IP authentication. Because the KVM solution needs to always be available in order to resolve problems that may arise in a data center, it must be a self-contained solution -- completely independent from any external servers in order to operate. If a data center came under attack from a malicious worm or virus, for example, the KVM solution should not rely on the same Windows servers in order to operate. The KVM solution’s own authentication should be activated if an Active Directory server becomes unavailable.

4. Server Access Issues and Challenges

A data center operator trying to quickly fix a problem needs a KVM system that's responsive and unobtrusive. The following is a comprehensive list of the issues and challenges to be considered when evaluating and selecting KVM products. To make the job easier, the considerations are grouped into categories – **performance, security, flexibility, ease of use and costs.**

4.1. Performance

Performance/mouse synchronization – How long is the lag time between the server operator's actions and the visual feedback in the monitor?

Bandwidth utilization – Will performance degrade in different network environments, dial-up, DSL, WAN, IP? Can the administrator or user throttle the bandwidth? Does it hog bandwidth on the data center network? Does it provide configurable video compression technology?

Client software responsiveness – Is the client component for server access well-designed? If it downloads a Java applet into the Web browser, does it take a long time to transfer? Once downloaded, does the applet keep up with the operator or is it sluggish? For non-browser-based clients, is the software highly proprietary? Does it have unusual or restrictive PC or OS system requirements?

Blocked versus non-blocked access – Are there enough client paths to each rack so that multiple users can always access the server(s) that they need to manage?

Disaster recovery – Can the tool help data center staff members quickly recover from major catastrophes, such as a pervasive network failure? Does the solution provide a single sign-on or do operators have to wade through multiple logons to get to the devices they need to access?

Maximum video resolution – Does the KVM tool support the high-video resolutions required?

Network backup – What server access alternatives exist, such as back-up modem access, if the network fails?

Self contained – Is the KVM solution self contained so it will always be available when data servers go down?

4.2. Security

Server and network security – Does the tool satisfy the company's need to keep server and operator interactions authentic and confidential?

Protocol support – Does the KVM system work with industry standard security protocols?

Authentication – Is security and authentication built into the box or does the KVM product need a centrally located authentication server? If it needs an external server for authentication, what happens when the WAN goes down? How do operators authenticate themselves from a remote location?

4.3. Flexibility

Scalability – Can the remote-access KVM solution scale as the company grows? Does it allow multiple concurrent users access to a server pool? Does it limit concurrent access to just two or four people?

Migration to new technologies – Is the solution likely to work with new advances in KVM?

Platform independence – Does it support the management of a heterogeneous computing environment?

4.4. Ease of Use and Installation

Breadth of product line – Does the product come in a variety of user and port configurations to maximize non-blocked access? Does it require buying IP access for every port?

Ease of administration – To what extent, if any, does the KVM tool intrude on the server operator's daily tasks?

Span of control – Does the tool integrate with serial console and power control devices? Does it have a single sign-on for cascaded switches?

Setup and configuration – Is it easy to set up and maintain? Does it require additional software or equipment? If a switch loses power, does it remember the server names when it comes back up? If operations people move a server and re-connect it elsewhere on the network, does the KVM product recognize the server in its new location?

4.5. Costs

Hidden Costs – Does it require a dedicated authentication or systems management server, or is everything included in the switch itself?

Budget and resource constraints – What are the KVM tool's positive or negative dollar value effects on data center expenses, productivity and computing environment utilization?

Investment protection – To what extent does a new KVM tool require changing any part of the computing environment -- including existing KVM devices -- to suit the new tool? Will it work with legacy KVM systems or does it mandate the replacement of perfectly good hardware just to accommodate a KVM upgrade?

Software – Does it require additional software – client and/or server?

Total Cost of Ownership – What is the KVM tool's overall cost to the organization, taking every aspect of data center operation into consideration?

5. Conclusion

Remote-access KVM is a simple, but powerful idea. It enables entire data centers and branch offices to be managed from wherever the IT resources reside in order to simplify IT management, reduce costs and improve operations performance.

The right KVM decision will give IT staff members responsive, secure, flexible, easy-to-use and cost-effective access for managing your enterprise's IT equipment.

Raritan Computer offers analog and digital KVM solutions -- and a combination of both -- so that IT organizations can have the highest performing solutions to meet their specific IT infrastructures. Factors such as proximity to the rack, number of servers and devices, and the number of users should be considered in determining the best Raritan solution.

6. About the Author

Barry Nance is a networking expert, magazine columnist, book author and application architect. He has 29 years experience with IT technologies, methodologies and products. Over the past dozen years, working on behalf of Network Testing Labs, he has evaluated thousands of hardware and software products for Computerworld, BYTE Magazine, Government Computer News, PC Magazine, Network Computing, Network World and many other publications. He's authored thousands of magazine articles and three popular books: Introduction to Networking (4th Edition), Network Programming in C and Client/Server LAN Programming.

He's also designed successful e-commerce Web-based applications, created database and network benchmark tools, written a variety of network diagnostic software utilities and developed a number of special-purpose networking protocols.

His e-mail address is barryn@erols.com.

7. About Network Testing Labs

Network Testing Labs performs independent technology research and product evaluations. Its network laboratory connects myriads of types of computers and virtually every kind of network device in an ever-changing variety of ways. Its authors are networking experts who write clearly and plainly about complex technologies and products.

Network Testing Labs' experts have written hardware and software product reviews, state-of-the-art analyses, feature articles, in-depth technology workshops, cover stories, buyer's guides and in-depth technology outlooks. Our experts have spoken on a number of topics at PC Expo and other venues. In addition, they've created industry standard network benchmark software, database benchmark software and network diagnostic utilities.

8. Raritan Computer – Profile

8.1. About Raritan Computer

Raritan Computer Inc. is a leading supplier of IT infrastructure management solutions for secure access, monitoring, and management of servers and other IT devices in data centers and remote offices. Raritan's products are used to control and manage millions of servers at more than 50,000 data centers, computer test labs, and other sites around the world. From the small business to the enterprise, Raritan's complete line of compatible and scalable digital and analog KVM, serial console, and remote connectivity products offers IT professionals the most reliable, flexible, and secure solutions to manage IT equipment, while improving operational productivity. Founded in 1985, Raritan has experienced 19 consecutive years of profitable growth and technical innovation. Raritan has 25 offices and is distributed in 76 countries. More information on the company is available at www.raritan.com.

