LANTRONIX®

The ABCs of KVMs:

How Remote KVM™ Switches Put You in Control of Your Data Center

Lantronix, Inc.
15353 Barranca Parkway
Irvine, CA 92618
Tel: +1 (800) 422-7055
Fax: +1 (949) 450-7232
www.lantronix.com

Contents

Introduction

While the goal of today's technology is to accomplish more with less, the reality is that information technology (IT) equipment in today's modern data centers is growing at unprecedented rates. This proliferation calls for a cost-effective solution that can provide centralized control of IT devices in the data center, without adding to the clutter. That solution is the KVM switch. KVM is short for **k**eyboard, **v**ideo and **m**ouse. This simple device consolidates data center management by enabling a single keyboard, video monitor and mouse set to control the GUI on multiple servers.

With a remote KVM switch installed at the data center, IT operators can sit at a single workstation anywhere in the world and have secure access and control of many servers in multiple locations across the globe. For this reason, server management with remote KVM switches is becoming the cornerstone of most data centers today.

This paper describes the evolution of remote KVM switches and the benefits they bring to modern data centers and outlines the key features to look for when shopping for a remote KVM switch.

The Evolution of KVM Switches

Before remote KVM switches, computer servers in the data center were managed by multiple redundant I/O devices. Traditional KVM switches, forerunners to today's remote KVM switches, reduced clutter in the data center by allowing multiple servers to be controlled using a single remote KVM switch.

Traditional KVM switches connect directly to the keyboard, video and mouse ports on the server, and require operators to have physical access to the console. This arrangement provides operators in the data center with powerful BIOS-level access to target devices. In this way, a single KVM switch can be used to access and control an entire room or rack full of servers.

Looking Closely at Remote Management

Data centers are expanding to keep up with the increasing amount of data in today's rapidly growing information infrastructure. It is not uncommon to find data centers spread across floors in a building, dispersed among buildings in the same city, or located in various facilities around the world. To keep up with this rapid expansion, IT managers are upgrading from the traditional KVM switches to Remote KVM managers which enable secure anytime, anywhere access and management via the Internet.

Remote KVM switches provide data centers with unsurpassed scalability and flexibility. Unlike traditional KVM switches, which require operator to have physical access to the console, remote KVM switches transmit KVM information over standard TCP/IP connections. This approach leverages a company's existing network infrastructure by enabling operators to control servers and other distributed IT assets remotely over local-area networks (LANs) and wide-area networks (WANs) using a single computer located anywhere in the world.

The benefits of IP connectivity within LAN and WAN environments are well known.

- IP networks are scalable. New devices can be dynamically added by just assigning a new IP address.
- IP networks offer substantial flexibility. Almost any device or platform can be accommodated within an IP network. These devices can easily be reconfigured according to changing business needs or other requirements with minimal impact on other nodes.
- The technical requirements of IP networks are well understood.

Despite these advantages, IP networks can create complex management issues. The primary one is security. The same openness that makes IP networks scalable and flexible also creates the potential for intruders to gain access to the network. Security guidelines to observe when selecting a remote KVM switch are discussed later in this paper.

Benefits of Using Remote KVM Switches

Remote KVM switches deliver the benefits of:

- **Global, anytime access**
  Provides access to servers and other connected devices from anywhere in the world using the ubiquitous IP network, the Internet, and a web browser.
- **Space conservation**
  Remote KVM switches eliminate the need for connecting a keyboard, video monitor, and mouse to each server. Combined with a small form factor, KVMs reduce the amount of equipment that must be packed into the data center.
- **Reduced costs**
  Remote KVM switches eliminate the need for connecting a keyboard, video monitor, and mouse to each server. This not only lowers hardware costs and power consumption, but also reduces the heat generated from multiple monitors and lowers air conditioning costs.
- **Reduced downtime**
  Remote KVM switches reduce downtime by providing easy access and control to any connected server.
- **Improved business continuity**
  Some Remote KVM switches also allow out-of-band access to a company's servers. Because these remote KVM switches are not forced to rely on a corporate backbone or network, they allow IT operators to access, control, and manage company servers even if the network is down.
- **Hardware platform and operating system independence**
  Remote KVM switches work in heterogeneous server environments, providing access to multiple platforms within one switching system. Because they are not dependent on hardware or operating systems of specific manufacturers, remote KVM switches work in corporate IT environments that have servers that are from different manufacturers and run on different operating systems.
- **Scalability**
  New systems and devices can be added as easily as assigning a new IP address.

Global Access is Critical

"Global access to multiple servers is proving to be a key success factor for many companies. The benefits in terms of decreased server downtime and distributed IT control are clear."

Source: IDC

- **Standardization**
  Because remote KVM is based on TCP/IP, IT staffs are already familiar with the underlying technology and equipment requirements.
- **Cabling**
  Many new Remote KVM switches use Category 5 cables, which help reduce clutter and save on cable costs, but require special adapters. Other solutions use standard KVM cables.

How Remote KVM Switches Work

Remote KVM switches use standard TCP/IP protocols to transmit digital signals for managing the keyboard, video and mouse outputs of servers. Operators control servers from any location using a standard web browser. This arrangement gives operators total access to the servers, just as if they were setting in front of them.

IP-enabled KVM switches take advantage of the TCP/IP infrastructure already in place:

1. Analog signals from a keyboard, monitor, and mouse are captured.
2. The signals are converted into digital packets.
3. The signals are digitized and the packets are compressed and securely transmitted across your existing infrastructure using TCP/IP connections.

Factors to Consider in a Remote KVM Switch

The following sections describe key factors to consider when selecting a remote KVM switch.

Simplicity

A Remote KVM solution should require no special hardware, client software or special adapters.

Scalability

Your network will grow and change over the coming weeks, months, and years. As the number of users, servers, and network devices increase, your remote KVM switching system must be able to expand with your business. For these reasons, look for a reliable, manageable, and scalable remote KVM switch that can grow with you and accommodate a large number of simultaneous users, without requiring internal architecture restructuring. If a traditional KVM is installed, look for a remote KVM that has cascading capability. This feature will allow you to re-use your current infrastructure.

Access Methods

Determine whether you prefer to access your data center devices using TCP/IP connections or using direct connections. If you decide on an IP-enabled remote KVM switch, choose one based on your infrastructure to avoid special design

considerations. Some remote KVM switches also allow for direct local access in addition to remote access.

Access-Level Rights

If more than one operator will be controlling multiple target devices at one time, select a remote KVM switch that supports access levels. Access levels let you assign port permissions by user and/or group. For example, you can configure an administrator to have access to more devices than an entry-level operator. If multiple users may need simultaneous access, look for switches which support more than one remote user.

Modem Access

If you select a remote KVM switch, consider what you would do if the network is down. For this reason, select a remote KVM switch with modem dial-up capabilities, if necessary. That way, if the network goes down, you can dial in to the remote KVM switch and control the target servers.

Target Devices

Different remote KVM switches can accommodate different types of target devices. Therefore, look for a remote KVM switch that supports the devices you intend to control. If you intend to control servers only, for example, do not select a remote KVM switch that supports both servers and serial devices. If, on the other hand, you have, or will have, serial devices such as remote power controllers that need to be managed along with servers, select a remote KVM switch that also has serial interfaces.

It is also important to ascertain the number of devices that will be controlled. If you expect to add devices to your data center, select a remote KVM switch that has more ports than you need at the present time to accommodate future growth.

Graphical Interface

Choose remote KVM switches that have an intuitive graphical user interface (GUI), so you do not have to retrain your staff after each upgrade or reconfiguration. A standard Windows® application, for example, should provide a familiar interface for busy IT staff that needs to quickly access and control any network device. Avoid choosing a remote KVM switch that calls for installation of client software and acquire one that only requires a web browser.

Browser / Telnet Compatibility

Although remote KVM switches do not require software to be installed on the managed computers, they work with software to manage target devices (even a web browser and Telnet are considered software). If you are considering the purchase of a remote KVM switch, be sure it is compatible with standard web browsers like Internet Explorer and Netscape® Navigator. Avoid remote KVM solutions that require their own proprietary software, especially when licenses are purchased separately.

Security and Authentication

No company can afford to have its data or customer information fall into the wrong hands. Because security threats come in so many forms, and because it's never wise to rely on a single point-of-protection when guarding against these threats, the remote KVM switch must have:

- Effective controls to prevent unauthorized access by internal users, as well as
- Safeguards to prevent critical systems from dangers that can result from human error.

The following list summarizes essential security features to look for in a remote KVM switch.

- **Key exchange**
  Additional security can be achieved through a key exchange between the remote KVM switch and client-access software. Best-practice security requires that a time limit be put on this exchange.
- **Encryption**
  Encryption of data transmissions eliminates the chance that critical systems might be compromised by the interception of legitimate KVM sessions. The level of encryption that can be used depends on the ability of the operating system, device, and/or browser involved. Best KVM security practices should include 128-bit SSL encryption and 3DES encryption, which encrypts, decrypts and re-encrypts packetized KVM data with separate keys to prevent "snooping"of sensitive management information. HTTPS should also be considered when selecting a remote KVM. HTTPS encrypts the session data using either a version of the SSL (Secure Socket Layer) protocol or the TLS (Transport Layer Security) protocol, thus ensuring reasonable protection from eavesdroppers.
- **Auditing**
  Auditing mechanisms are also critical to the maintenance of KVM security. Security managers should have access to logs of all KVM activity. These logs should provide appropriate native reporting and be exportable into popular reporting applications, so that anomalies and trends can be detected as soon as possible. In particular, security managers should continually monitor events such as failed authentications and attempts to gain access beyond authorized permissions. Regular audits should also be performed with other security best practices.
- **Privacy Features**
  Choose remote KVM switches that support features such as stealth and turtle modes. Stealth mode is designed to only allow those users who know both the IP address and web server port number to access the remote KVM switch and keep outsiders out. Turtle mode enables the remote KVM switch to shut down when it feels that its security may be under attack. For example, if more than five password failures are detected in a certain timeframe, the remote KVM switch shuts down and disconnects itself from the network.

Reporting and Event Logging

Find out whether the remote KVM switch provides detailed reporting and event logging. For example, does the remote KVM switch provide you with the activity log from any hour of the day so that you can track users and events in the system? Check whether information such as failed authentication attempts, channel blocked, and insufficient access rights are collected and stored from all devices in the network and

available to be exported into a compatible format (such as .CSV or .XLS format) for integrated reporting.

Leveraging Your Current KVM Switch

If you have a traditional analog KVM switch, look for a remote KVM switch that lets you integrate your current KVM investment. This typically is done by connecting one of the consoles on your current KVM switch to a port on the new remote switch. Select a remote KVM switch that is compatible with your other equipment and will allow it to be cascaded. Such features allow you to take advantage of remote access features without having to replace existing infrastructure.

The Lantronix Advantage

Once the decision has been made to acquire a remote KVM switch, the next question is deciding which vendor offers the best solution? This paper has presented points to consider when evaluating competing KVM solutions, including operational features, ease of implementation and ease of use, scalability, security, and overall value.

It is equally important to choose a KVM vendor with a proven track record of technical advancement and innovation. After all, if a server fails, business can come to a halt in a matter of seconds.

As the industry leader in network and connectivity innovation and advancement, Lantronix offers its new SecureLinx™ SLK Remote KVM™ solutions. SecureLinx SLK empowers users to access and manage servers from anywhere over the Internet, greatly enhancing the value of the KVM solution. With unsurpassed access to the GUI on critical servers, SecureLinx SLK is operating system and platform-independent. It requires only a Java-enabled browser, so no additional software is needed to control servers from a remote location. The 16-port SLK also offers dial-up capability for access and control – even when the network is down – so users can immediately respond to equipment issues to minimize downtime.

SecureLinx SLK includes advanced security features such as stealth mode to protect servers from security threats and turtle mode to deny access when multiple bad login attempts are detected.

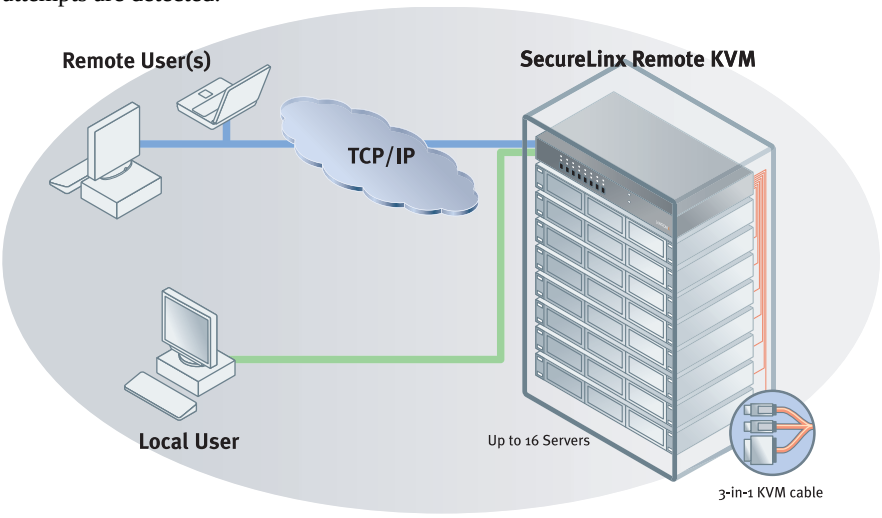

Figure 1. Sample SecureLinx KVM Configuration

SecureLinx SLK Remote KVM leverages the existing IP network and fit seamlessly into your data center's multilayered security model. This makes setup easy — just assign an IP address, set the network configuration, connect the SLK to the server, and configure it either locally or remotely. With no software to install, SecureLinx SLK does not impact server performance and seamlessly supports multiple operating systems.

SecureLinx SLK Remote KVM uses hardware encoding of KVM outputs to transfer them over a standard TCP/IP network. SecureLinx SLK Remote KVM leverages the existing IP network and fit seamlessly into your data center's multilayered security model. It supports SSL to ensure that network resources are secure and protected.

If you already have a traditional analog KVM switch, you can attach it to a SecureLinx SLK server port for anytime, anywhere access to an expanded number of servers, without disrupting existing hardware.

Lantronix understands that the more servers an operator can monitor and manage remotely, the less time that operator is tied up crossing the floor, heading down the hall, or visiting a remote location. For this reason, SecureLinx SLK Remote KVM is available in three convenient models, as shown below

Table 1. SecureLinx SLK Remote KVM Models

Model	Features
SLK1	• Single KVM port • Up to 10 user profiles • Two serial ports (one DB9 female, one eight pin mini-DIN) • Ideal for remote-enabling analog KVM switches
SLK8	• Eight KVM ports • Up to 10 user profiles • Monitors up to eight video outputs simultaneously • Two serial port ports (one DB9 female, one eight pin mini-DIN) • Perfect for managing multiple servers or analog remote KVM switches
SLK16	• 16 KVM ports • Up to six independent remote (digital) sessions to all channels (non-blocking) • Up to 32 user profiles • Monitors up to 16 video outputs simultaneously • Out-of-band dial-up access through external serial modem • Three ports (two DB9 female, one DB9 male) • Suited for larger installations with more users

Lantronix Networking Expertise and Service Quality

Lantronix products are known all over the world by their quality and reliability. To date, Lantronix has delivered network connections to millions of devices and more than 20,000 customers — and those numbers continue to grow. As the networked world evolves, we are well-positioned to be a major factor in networking as we help our customers increase uptime of their systems, manage billions of dollars of equipment, and connect virtually any electronic product to a network or the Internet.

At the same time, we believe that service quality is often of no less importance for the user than performance of the product. It is due to this reason that Lantronix provides warranty and contract services for our products. When you purchase Lantronix products, you get even something more: high-quality service. And this means:

- Technical support assistance (see below)
- A flexible system of service contracts

Technical Support Factor

At Lantronix, we know that when a vendor touts “unparalleled technical support,” it has to mean something. The industry is competitive, and it's not good enough to offer vague promises and the same promises everyone else is making. For this reason, Lantronix maintains a staff of highly skilled networking specialists who possess in-depth knowledge of serial and network connectivity.

Support ranges from basic configuration and troubleshooting to guidance in creating custom web pages and using configurable I/O pins to read or set triggers for unique signal indicators. Technical support is available to customers at no additional charge via phone, email, and the web. Real-time phone support is available for US domestic clients from 6:00 am to 5:30 pm PST via our toll-free support phone number.

Lantronix also provides an online knowledge base, video-configuration tutorials, chat support, and “live assist” — a virtual onsite systems engineer that allows secure, shared control of your personal computer.

Glossary

The following table identifies the technical terms used in this paper.

Authentication	The process of identifying an individual, usually based on a username and password. Authentication ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.
Challenge-Handshake Authentication Protocol (CHAP)	A standards-based security protocol commonly used to verify remote access logons by mobile and remote users. The CHAP protocol validates users or systems with a challenge that requires an appropriate response. If the user supplies proper credentials, the logon is validated and a network connection is established. The most important feature of CHAP is that passwords are never sent over the line.
Lightweight Directory Access Protocol (LDAP)	A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.
Network Attached Storage (NAS)	A server that is dedicated to file sharing. NAS allows more hard disk storage space to be added to a network that already utilizes servers without shutting them down for maintenance and upgrades. With a NAS device, storage is not an integral part of the server. Instead, the server handles all of the processing of data but a NAS device delivers the data to the user. A NAS device does not need to be located within the server but can exist anywhere in a LAN and can be made up of multiple networked NAS devices.
Packet filtering	Controlling access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP addresses of the source and destination. Packet filtering is one technique, among many, for implementing security firewalls.
Password Authentication Protocol (PAP)	The most basic form of authentication, where a users name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. The Basic Authentication feature built into the HTTP protocol uses PAP. The main weakness of PAP is that both the username and password are transmitted "in the clear" – that is, in an unencrypted form.
Remote Authentication Dial-In User Service (RADIUS)	An authentication and accounting system. When you access a RADIUS-protected system, you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the system.

SSH v2	SSH v2 is based on the V2 protocol and the F-Secure 3.1.0 code base. SSH v2 is generally regarded to be more secure than SSH v1. It is incompatible with SSH v1, but can coexist on an SSH-capable console manager.
Secure Sockets Layer (SSL)	A protocol for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL.
Telnet	A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects it to a server on the network. You can then enter commands through the Telnet program, which are executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you log into a server by entering a valid username and password.
3DES	A mode of the DES encryption algorithm that encrypts data three times. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key).