Console Managers:

The Essential Data Center Component for Maximizing Uptime

Lantronix, Inc.
15353 Barranca Parkway
Irvine, CA 92618
Tel: +1 (949) 453-3990
Fax: +1 (949) 453-3995

Contents

Introduction

In today's fast-paced business world, many organizations would find it impossible to operate without access to their network computers or enterprise-wide systems. As information technology (IT) has become the lifeblood of today's business, the data center has become the heart that drives business-automation systems. The ability to monitor and manage the company network and keep it up and running is pivotal to business.

Now that data centers are more complex and varied, it becomes harder to find technical expertise with the necessary skills and resources to administer such systems. The issue becomes how to expand the capabilities of the data center and its network-management personnel within an organization to better maintain the diverse network infrastructures currently deployed, and how to minimize and possibly avoid network downtime and performance loss.

The stakes are high to maintain availability and performance of the organization's network, regardless of how widely dispersed the network infrastructure is. When the network goes down, so do profits and productivity. And the longer a network remains down, the greater the impact on the company.

Downtime Means Lost Revenue

In 1999, eBay, the nation's leading auction site, went down for 22 hours. This outage led to an estimated $3-to-$5 million of lost revenue for eBay. In addition, shares of eBay were hammered, falling 9-5/8 to 83-1/4. Investors concern was also raised because the outage had a significant impact on the company's third-quarter earnings.

Source: News.com 3/14/2002

To minimize downtime, data centers must maintain 99.999% availability by providing virtual "crash-cart" access to business-critical devices. To achieve this goal, an increasing number of organizations are turning to console managers.

A console manager is a hardware device that provides network administrators with consolidated access to virtually every piece of equipment in the data center using one simple device. It also allows them to deploy a simple and flexible solution for responding to critical situations — all while eliminating costly visits to remote sites. As network infrastructures expand and the challenge of maintaining them becomes increasingly difficult, console managers are becoming a necessary component to any network-management system. This paper examines the vital role that console managers play in keeping businesses operating at peak efficiency, while minimizing downtime, simplifying access, saving time and money, and protecting assets.

The Business Imperative for Maximizing Uptime

A recent study by Infonetics Research revealed that companies experience an average of 501 hours of network downtime every year. This translates into a loss of millions of dollars in annual productivity and revenue, or on an average of approximately 3.6 percent of a company's annual revenue. The study, which is conducted yearly, also revealed that there isn't any one problem area that organizations need to focus on; there's no simple fix. Every decision is critical. Because system failures can result in significant losses, the need to manage the risk of downtime has never been greater.

To manage downtime, today's data centers must:

- Reduce vulnerabilities and single points of failure
- Respond to crises proactively
- Manage users and resources with maximum efficiency
- Tighten security to protect company assets

While these objectives are easy to identify, they are challenging to achieve given the wide range of device types in today's data centers (see Figure 1). These devices can take the form of application servers, email servers, database servers, Web servers, and ecommerce servers — even legacy mini-computers and mainframes. These devices might be equipped with Intel- or RISC-based processors and run operating systems such as Microsoft Windows, Unix, Linux, MacOS, NetWare, AIX, and others. In many cases, the servers rely upon shared storage provided by SANs (storage-area networks) and NAS (network-attached storage) systems.

Communication among servers and client systems requires network devices such as routers, gateways, virtual private networks (VPNs), and firewalls. All of these devices require power, which is often managed by uninterruptible power supply (UPS) devices, surge protectors, and intelligent power strips.

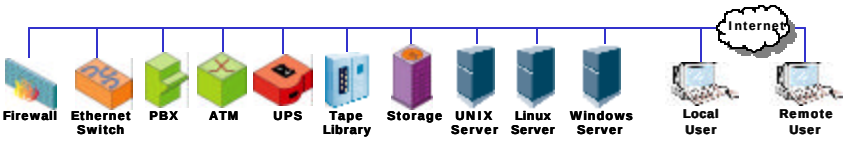


Figure 1. Typical Devices on a Company Network

Given the reliance all these devices have on the network, it is easy to see that when a network collapses (as shown in Figure 2), productivity and profits fall, generating a serious impact on a company's bottom line. Figure 3 shows the financial impact that downtime plays in a variety of business sectors.

Even potential revenue can be affected. For example, if a company's web server can't be found, the customer may go to the competition. The frequency and duration of outages, as well as the average revenue of the company, impact the cost of downtime. And the longer the network is down, the greater the consequences.

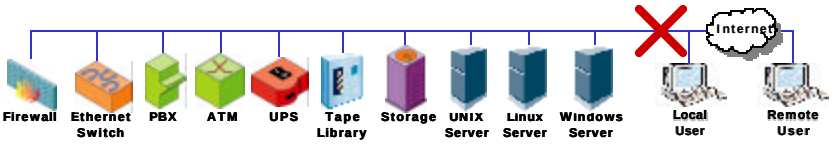
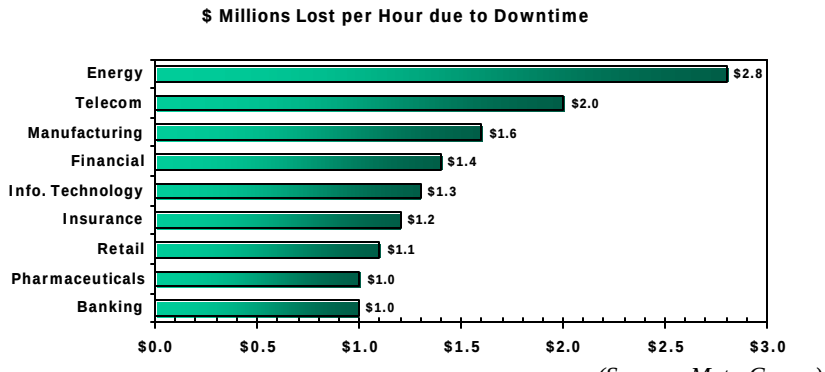


Figure 2. Network Failure Prevents Access to Resources



(Source: Meta Group)

Figure 3. The Cost of Downtime

The costs of failure can reach well beyond lost customers. In some cases, it can mean life and death. Take, for example, hospital settings, where network devices send and receive vital patient information. If the network or one or more devices on it becomes impaired or goes down, patient lives can hang in the balance until the problem is resolved.

The Console Manager Solution

A console manager enables the user to access and control all the equipment in the data center through one central terminal. Users can manage the equipment any time, from any place, either locally through the company network or remotely through the Internet or dial-up connections. To connect to the serial ports on data center devices, a console manager contains multiple RS-232 serial lines. It also has an Ethernet port for connecting to the network, and may include a dial-up modem port for emergency remote access (see Figure 4).

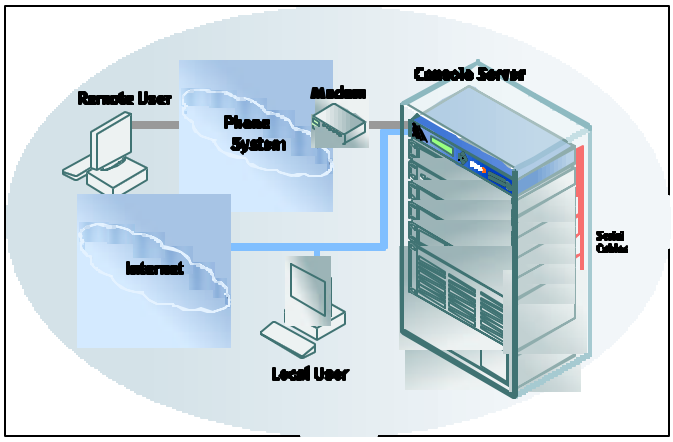


Figure 4. Sample Configuration Using a Console Manager

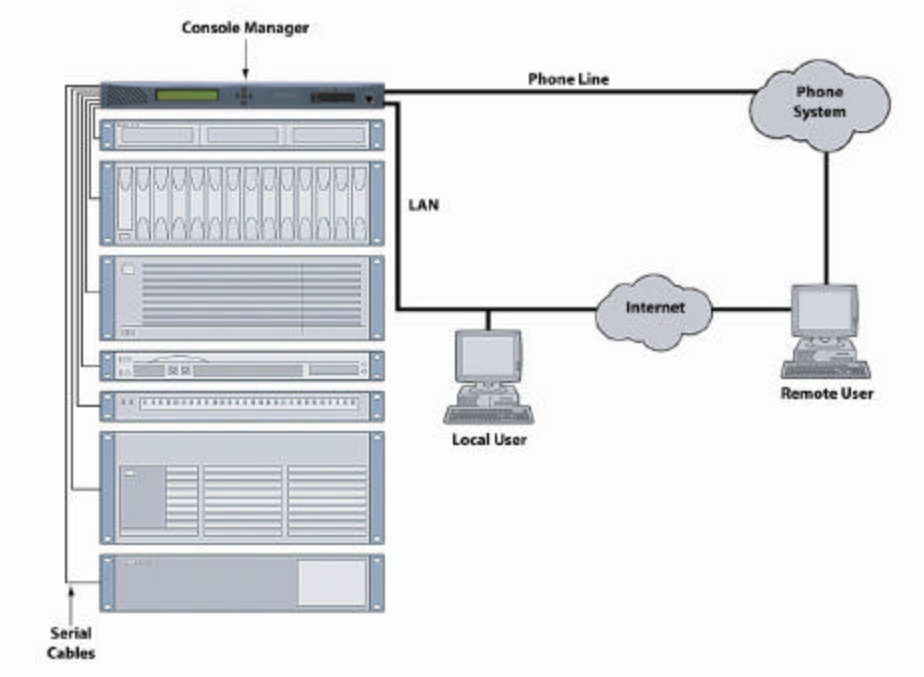


Figure 5. Example of Connecting a Console Manager

Console Manager Features and Benefits

The following list summarizes key features and benefits of console managers.

Issue	Feature	Benefit
Response Time	Console managers provide an immediate, no-maintenance way to access IT equipment from any location, even when the network is down.	Instant on-demand device access slashes response time, improves efficiency, maximizes uptime, and improves your bottom line.
Simplified 365/24/7 Access	Equipment can be accessed securely and remotely after hours, on weekends, or during holidays.	Problems can be fixed now, without having to arrange for technician visits or off-hour access.
Protects Assets	Console managers come with security features that protect IT infrastructure and its resources.	The network and its assets are protected against hackers and other unauthorized individuals.
Frees Space in Data Centers	A single console server can manage multiple devices, freeing valuable data center space.	Equipment costs and monthly service fees are lowered and the number of cables in the data center is reduced, making for a cleaner data center with more room to expand
Boosts IT Staff Productivity	Console managers reduce the number of individual devices that the IT staff has to learn about or manage on a per-device basis.	IT staff operations are streamlined and IT training costs are lowered.

Alternatives to Console Managers

The following sections describe two alternatives to console managers: software management tools and the Simple Management Network Protocol (SNMP).

Stacking Up Console Managers against Software Management Tools

Up to now, we have described console managers as hardware solutions. Software management tools are also available that try to mimic the functions of console managers. Generally speaking, console managers are easier to install, have fewer dependencies, and offer a lower total cost of ownership (TCO) and a higher return on investment (ROI) than software management tools.

Software management tools are also finicky. They might only run on certain operating systems, demand that certain patches or other software be pre-installed or not installed, and consume vast amounts of precious hard drive space.

Software management tools can also be more expensive than console managers, especially when it comes to licensing agreements. Software vendors typically charge according to the number of servers on which their software management tools run. This can become very pricy for enterprises that need to install software management tools on multiple computers in various locations.

TCO and ROI include the initial cost of installation, plus the administration and support costs over a product's lifetime, product downtime, and restoration service. With console managers, network downtime and TCO are minimized, improving the company's ROI.

Can't SNMP Be Used in Place of a Console Manager?

SNMP provides status and performance of network devices through their Ethernet connections. However, if the network goes down or the operating system is locked up, servers and other network devices will not respond through the Ethernet port.

Moreover, some devices in the network, such as the UPS, do not have an Ethernet connection. The console port provides the only way to gain control of these devices. It is where fundamental corrections to the device can be made. As a result, SNMP is more of a complement to, rather than a replacement for, console managers.

Factors to Consider in a Console Manager

The following sections describe key factors to consider when selecting a console manager.

Protecting the Network

The need to protect the network and its assets and resources has never been greater. Therefore, a console manager must walk a fine line between allowing quick and easy access to legitimate users, while denying access to hackers and other unauthorized individuals.

To walk this balancing act, console managers with security features such as local- and server based authentication, authorization, and encryption are important to an organization. In particular, look for console managers that support SSH, which provides strong authentication and secure communications.

The console manager you choose should also have full support to Internet, local-area network (LAN), and dialup connectivity. Avoid products that lack the security or Internet connectivity required by today's networks.

Maximizing Port Usage

Port densities for console managers vary widely. If you expect the number of managed devices in your data center to increase, or even if you don't, it is best to choose a console manager with more ports than you currently need to prepare for the inevitable future expansion. If space in your data center is at a premium, you may want to look for "stackable" console managers that can form a single "virtual" solution.

Seamless Integration

The console manager should fit in seamlessly with your data center's existing rack and cable setup. Features to look for include console managers that have:

Look For Console Managers that Have:	Avoid Console Managers with:
Built-in RJ45 connectors. RJ45 ports are industry-standard interfaces for connecting devices to Ethernet networks. The standard cabling pin assignments of these connectors let you use normal cables to connect devices.	Proprietary interfaces.
LED status indicators. The indicators should show the status of the console manager and the devices it is managing.	No LED status indicators or indicators placed at locations that make viewing difficult.
Their own power supply. For improved availability and added reliability during critical times, look for console managers with integrated dual redundant AC/DC power supplies; if one power supply fails, the backup supply takes over operation with no interruption in service.	Fans or other moving parts that can be noisy or dangerous.

Proactive Alerts

Murphy's Law dictates that devices fail at inconvenient times. In many cases, the needed administrator is not in the office when the failure occurs. Because prevention is impossible and intervention is critical, it is important to choose a console manager that works proactively by monitoring the status of network components and alerting network technicians via console and/or e-mail when a network device or the network itself is down. This feature provides instant notification of key events, empowering network managers to gain information about what business processes are affected by network events and assign the right priority to fixing the problem.

Simple Web-Based Interface

A console manager can have all of the state-of-the-art features one could ask. Without an intuitive user interface to access these features, however, users may be reluctant or unable to access critical features, leaving their network unprotected. Therefore, be sure the console manager provides an intuitive, point-and-click graphical user interface (GUI). Users who prefer typing to clicking may opt for a console manager with a command-line interface (CLI). The GUI and CLI should be sufficiently intuitive to allow users to get the console manager up and running in a matter of minutes, without having to learn another interface or possess a Computer Science degree.

SNMP Compatibility

Administrators often become aware of failed systems through user complaints. By the time complaints occur, however, business has already been impacted. It would be a wonderful world if administrators could respond to system failures before they impact the user community.

SNMP traps are tools that enable administrators to take proactive measures. Console managers that include an SNMP agent allow SNMP managers to view standard management information base (MIB) variables, such as MIB-2. For the most part, these variables provide status and statistical usage information.

Support and Equipment Cost

Two factors often overlooked are technical support and service contracts. Industry analysts estimate that 85% of the cost of owning a hardware device is related to equipment support (*source: http://www.syo.com/about/iosyo.PDF*). Because many vendors allocate their primary resources to marketing and sales, they may not have the budget or the in-house expertise to provide a fully staffed support department. Therefore, it is well-advised to select a console manager from a company that has a well-trained support staff and offers service contracts to enhance the cost-effectiveness of its products.

Miscellaneous Features

Other features to consider in a console manager include:

- Telnet capabilities to a serial port.
- Multiple-port addressing methods.
- Message-logging capabilities.
- Full RS-232 signaling support, along with the ability to generate intentional break signals without sending unintentional breaks.

Lantronix's Console Manager Solutions

Designed for a wide range of businesses including retail, industrial, hospitality, finance, and medical sectors, Lantronix's best-in-the-industry products empower our customers to gain a competitive advantage as they build their business and maximize network profitability. In addition, the savings in IT efficiency, user productivity, and revenue achieved with Lantronix console management products empower companies to realize a speedy ROI.

SecureLinx Family of Secure Console Servers

SecureLinx products from Lantronix allow IT professionals to monitor, manage, and troubleshoot nearly any device in the data-center rack — including Linux, Unix, or Windows® 2003 servers, routers, switches, PBXs and other telecom equipment, UPS devices, and even building-access equipment. Devices can be managed from any location, at any time — even when servers or networks are down. Access to the SecureLinx SLC is accomplished via secure Telnet or SSH, without requiring users to purchase and learn additional software. This means faster response rates which translate into reduced costs and less downtime.

With a common GUI and CLI that are simple to set up and use, SecureLinx products enable easy, secure administration and management — from BIOS settings to application software — all from a single location. In-band access is provided through dual Ethernet connections for both public and management networks, along with out-of-band access using a dial-up modem.

SecureLinx SLC models support from 8 to 48 serial ports, with single or dual AC or dual DC power supply options. Other key features include email notifications when unexpected console activity occurs and SNMP support, dual Ethernet ports and two PC Card slots.

A top priority for the data center manager is to protect IT resources. The SecureLinx SLC provides integrated security features to help safely manage and access those assets. SSL and SSH support provide encryption of data. The SecureLinx SLC also supports remote authentication for integration with other systems already in place in the data center. With additional security features that vary by model, SecureLinx SLC models can support authentication using usernames and passwords, modem dial-back, PAP/CHAP, RADIUS, Kerberos, SecurID, and SSH v2. Some models also offer LDAP, NIS, port-based user permissions, and a built-in firewall to minimize the visibility of the SCS device to network port scanning by rejecting or denying connection attempts. For even greater protection, SecureLinx SLC includes firewall features to reject connection attempts or block ports.

Best of all, SecureLinx SLC provides a comprehensive suite of features that allows quick setup and deployment, with typical "box-to-operation" times of less than 10 minutes. A front panel LCD with keypad, "Quick Setup" Web interface, and a CLI setup script are all available, as well as more detailed Web-based setup screens and CLIs for the advanced user. The comprehensive online help system includes context-sensitive information during configuration and operation.

ActiveLinx™ Family of Secure Console Servers

Lantronix also offers the ActiveLinx™ family of Secure Console Servers (SCS). These SCS solutions connect to the console or serial port on your IT equipment providing the ability to globally manage hubs, switches, routers, servers, UPS systems, PBX systems, storage-networking equipment, and telecom switches.

With a wide variety of models to choose from, ActiveLinx SCS solutions can manage up to 48 IT devices. All ActiveLinx models support in-band management for managing equipment over the network from any location via Telnet or SSH, as well as out-of-band management with dial-in access through a modem connection.

ActiveLinx SCS devices ensure the integrity of your equipment and dat a by supporting a variety of security capabilities, including usernames and passwords, modem dial-back, PAP/CHAP, RADIUS, Kerberos, SecurID, and SSH v2, LDAP, NIS, port-based user permissions, and a built-in firewall.

All ActiveLinx SCS models provide an intuitive, point-and-click Web-based graphical interface that makes configuration a snap. A CLI is also provided for configuration via a serial port or Telnet. Some models also provide a front-panel keypad and display for configuring network settings and other related parameters.

Terminal Servers

Lantronix also offers a line of Terminal Servers that provides remote management of networking equipment and servers. Used as multi-port device servers, these versatile products can network-enable up to 32 serial devices in a convenient rack-mount or desktop form factor.

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 over 2 million devices and 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
- A variety of service and warranty options

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 platitudes 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.

Pulling It All Together

With a wide range of equipment to manage, administrators are challenged to find the ideal console manager for their data-center devices. This paper has focused largely on console managers. However, it is important to realize that virtual crash cart access required to make your data center totally manageable may need to extend to remote KVM and power-management products.

Fortunately, Lantronix's SecureLinx product family includes a full range of solutions that deliver real value to today's data centers. For more information about Lantronix's complete line of console management solutions, please visit the Lantronix Web site at www.lantronix.com to see which products offer the performance and application needs to meet your data center requirements.

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.
Authorization	The process of granting or denying access to a network resource. Most computer security systems are based on a 2-step process. The first stage is authentication (described above). The second stage is authorization, which allows the user access to various resources based on the user's identity.

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.
Hypertext Transfer Protocol Secure) (HTTPS)	The secure version of HTTP, the communication protocol of the World Wide Web. Instead of using plaint-text socket communication, HTTPS encrypts the session data using either a version of the Secure Socket Layer (SSL) protocol or the Transport Layer Security (TLS) protocol to protect against eavesdroppers and "man-in-the-middle" attacks.
Kerberos	A secure method designed to enable two parties to exchange private information across an otherwise open network. It works by assigning a unique key, called a ticket, to each user that logs on to the network. The ticket is then embedded in messages to identify the sender of the message
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 user's 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.
Point-to-Point Protocol (PPP)	A way to connect a computer to the Internet. PPP is more stable than the older SLIP protocol and provides error checking features. Working in the data link layer of the OSI model, PPP sends the computer's TCP/IP packets to a server that puts them onto the Internet.

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.
RJ-45	Short for Registered Jack-45, an eight-wire connector used commonly to connect computers onto local-area networks, especially Ethernets. RJ-45 connectors look similar to the ubiquitous RJ-11 connectors used for connecting telephone equipment, but are somewhat wider.
Serial Line Internet Protocol (SLIP)	A protocol for connecting to the Internet via a dial-up connection. Developed in the 80s, SLIP was designed for simple communication over serial lines. SLIP can be used on RS-232 serial ports and supports asynchronous links.
Simple Network Management Protocol (SNMP)	A set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.
SSH v1	SSH v1 is based on the V1.5 protocol and 1.3.7 F-Secure code base. It is incompatible with SSH v2, but can coexist on an SSH-capable console manager.
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.
Storage Area Network (SAN)	A high-speed subnetwork of shared storage devices. A SAN's architecture works in a way that makes all storage devices available to all servers on a LAN or WAN. As more storage devices are added to a SAN, they too will be accessible from any server in the larger network. In this case, the server merely acts as a pathway between the end user and the stored data.
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.