



## Secure Remote Access for IT Infrastructure Management: Cyclades ACS Advanced Console Server

### Executive Summary

New technologies have replaced mainframes and minicomputers located in a single data center with a distributed infrastructure of servers, private branch exchanges (PBXs), and network equipment. These developments have reduced space requirements and cost, and increased scalability and flexibility in today's computing environment.

At the same time, however, the configuration and management of the information technology (IT) infrastructure is now more complex, creating new challenges for a company's IT staff. Chief among these challenges is maintaining server and network availability in a widely dispersed infrastructure. Without remote IT infrastructure management, unplanned network and server downtime could lead to regulatory non-compliance, lost customers, and lost revenue.

Managing today's dispersed computing infrastructure requires access to any device on a network at any time from any place in the world. Because all servers and many non-computing devices already include a serial port, gaining remote access to those serial ports provides a cost-effective way to manage all of a company's servers and network-attached devices. Through a device's serial port, an IT administrator can monitor and manage the device whether or not the network itself is functioning. This capability saves travel time and cost, and reduces unplanned downtime, maintaining network operation and improving company productivity.

Avocent's Cyclades ACS Advanced Console Server offers the most feature-rich set of capabilities in modern console servers. The ACS console server provides the scalability, reliability, and security a company requires to control and manage servers and other networked devices.

# Secure Remote Access for IT Infrastructure Management

## Introduction

Over the past decade, corporate information technology (IT) departments have replaced large mainframes and minicomputers with smaller, less costly, and more scalable servers. This transition offers substantial benefits. In the past, increasing an organization's computing power meant replacing a large computer with an even larger one – a process that was both expensive and time-consuming.

The switch to clustered computing (also called server farms) reduced both the expense and the disruption of adding more computing resources. Mainframes offered high availability and reliability, but at a premium price. Servers offer equally reliable and available computing resources using less expensive hardware – and because servers are incrementally scalable, adding more computing power leverages previous IT investments.

As IT departments adopted cluster computing practices, managing the widely dispersed servers became a significant issue. Monitoring and managing remotely located servers usually relies on an on-site IT staff member, a third-party service contract, or a willing, but untrained, employee. The first two are costly, and the third compromises IT access and security policies.

This white paper explores the issues facing the IT staff as it attempts to manage the dispersed and growing IT infrastructure. As more servers and more support equipment connecting these servers enter the corporate computing environment, the demand for high-quality, platform-independent infrastructure management tools also increases. Effectively managing centralized or remote servers, networking equipment, and other IT assets will remain a critical aspect of IT infrastructure management.

## Identifying And Meeting Infrastructure Management Challenges

Managing today's IT infrastructure requires an approach that maintains virtually continuous business operation, provides high levels of security, and reduces operating cost and complexity while increasing IT staff productivity (see Figure 1).

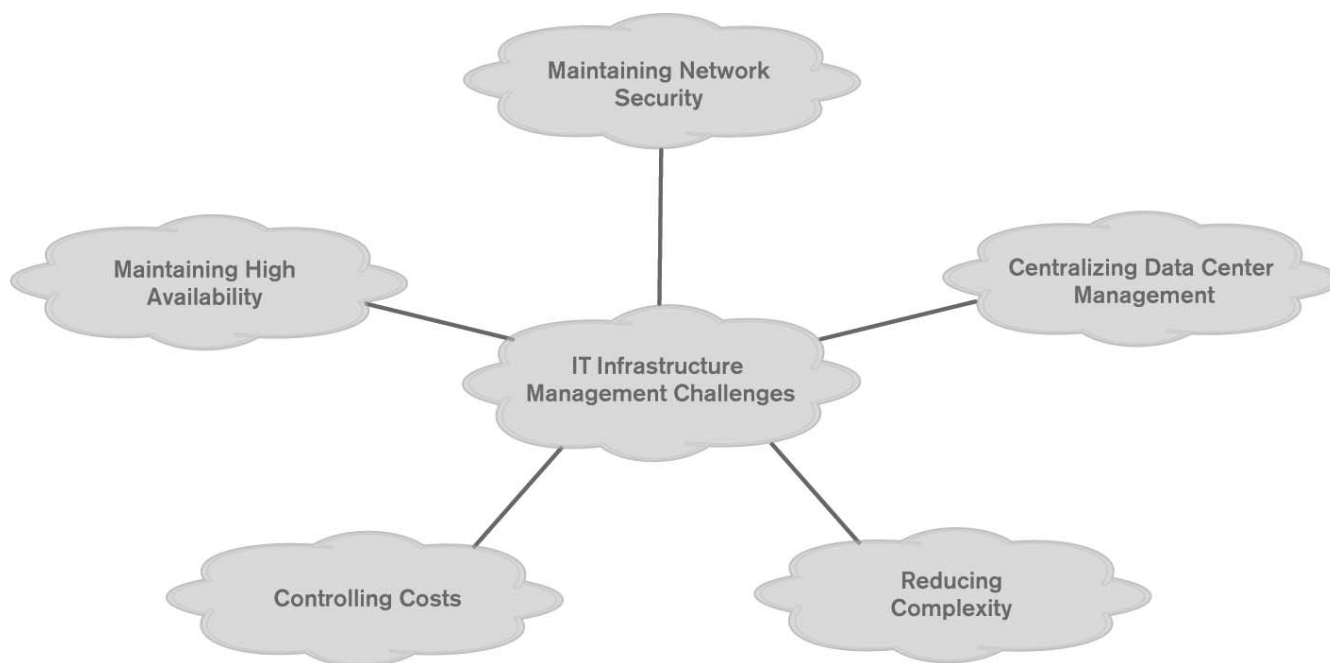


Figure 1. Challenges to Managing the IT Infrastructure

Each of these challenges presents IT administrators with unique issues, many of which involve ensuring secure and immediate access to the IT infrastructure.

An effective way to achieve this access is through a console server, which connects the serial console ports of many managed devices to a single appliance. An IT administrator can access any managed device's console from any location at any time, even when the production network is unavailable. State-of-the-art console servers offer the following features:

- Scalability – The ability to manage several servers in high-density racks is beneficial.
- Port density – A console server should use a minimum amount of space in a rack to manage all the equipment in that rack.
- Reliability – All connectors are located on the same side of the console server; the unit must be rack-mountable; and the unit should require minimum cabling and offer a high level of integration.
- Power supply – The console server's power supply needs to be integrated into the device.
- Compatibility – The console server needs to be compatible with all of the IT organization's servers and network equipment.
- Security – Comprehensive support for IT security policies, including multilevel user access control and logging capability, is critical.
- Audit capability – The console server needs to log all its activities in order to maintain security and regulatory auditing compliance
- Hardware flexibility – Support for out-of-band management, the ability to connect to more than one LAN, and integration with service processors and intelligent power distribution units (IPDUs) is useful.
- Software flexibility – Upgradability helps to take advantage of emerging technologies.
- Cost and service – The console server vendor should be committed to a product roadmap in IT infrastructure services.

#### Maintaining high availability

Widely dispersed computing resources create an environment that relies on component peak performance for a maximum amount of time. Infrastructure problems, including environmental factors, hardware and operating system errors, power failures, and natural disasters, comprise 20 percent of all unplanned data center downtime (see Figure 2).

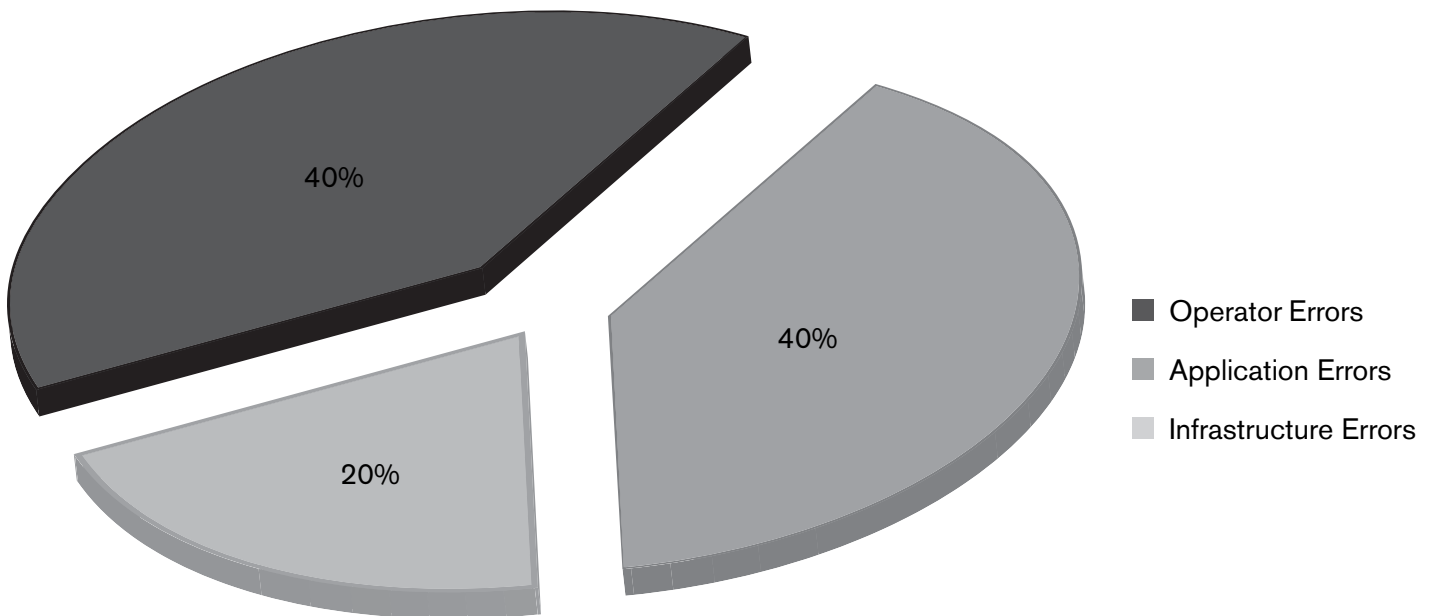


Figure 2. Causes of Unplanned Data Center Downtime

Unplanned downtime causes a variety of problems: lost revenue; lower customer satisfaction and, potentially, lost customers; and breaches of service level agreements that can result in penalty payments, which further reduces revenue.

# Secure Remote Access for IT Infrastructure Management

When the network is operating properly, local or remote access is available through the network (in-band) and standard programs such as SSH and encrypted Web browser sessions. However, if a server or a network router has failed, IT administrators need access to the failed device through an out-of-band mechanism that connects to the device's serial port and provides low-level control such as hardware self-tests or power cycling (see Figure 3).

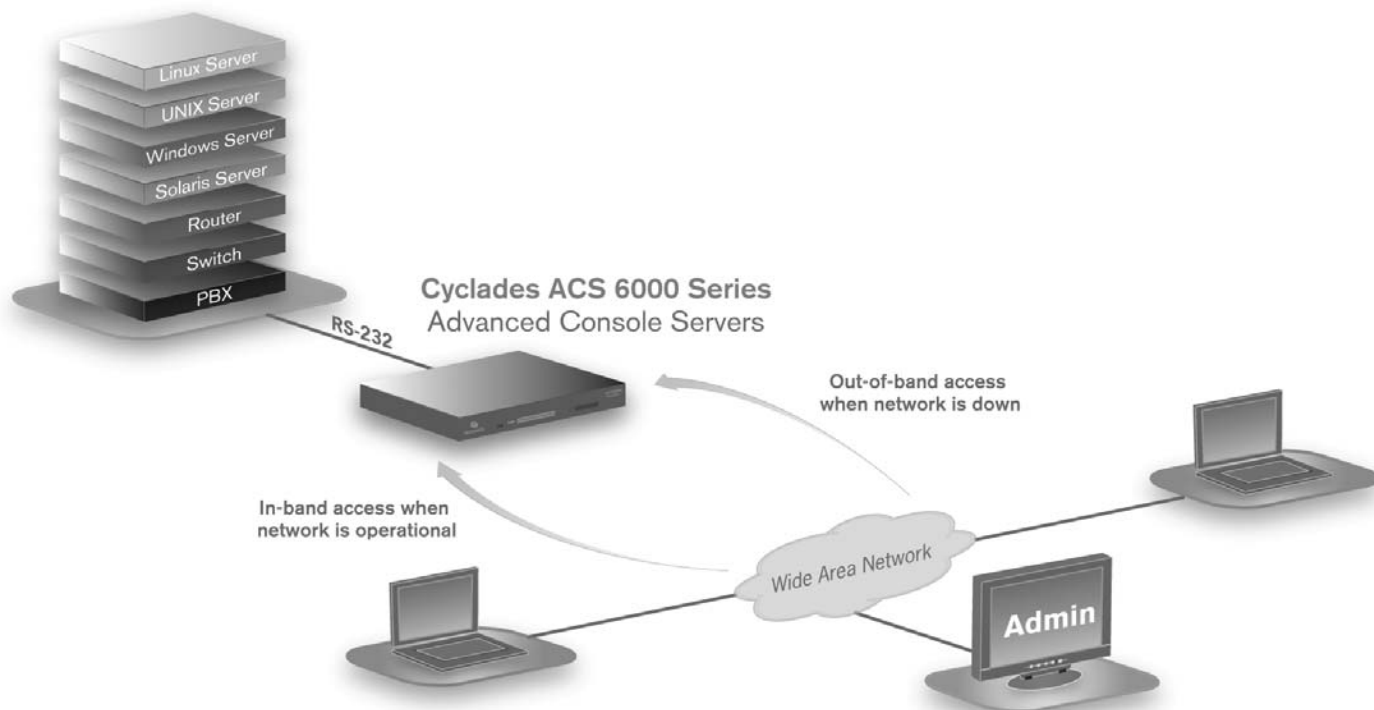


Figure 3. In-band and Out-of-band Administrative Access

## Maintaining network security

Widely dispersed computing resources often create a serious challenge to maintaining network security. Established access policies become more troublesome to enforce (e.g., when a non-IT employee reboots a server). Likewise, talking an employee through the steps to change BIOS settings involves employee access to administrative passwords, which violates established authentication, authorization, and auditing policies. In the event of an IT audit, these practices increase company vulnerability to charges of security policy violation and non-compliance with regulatory requirements.

Out-of-band access strengthens IT security policies by supporting features such as encryption of console traffic, authentication protocols including token-based authentication, and IP packet filtering, among others. Role-based access limits access to only those administrators with responsibility for maintaining specific servers. A console server also needs to support session management and maintain local and remote event logs, access logs, and data logs.

Effective physical security (e.g., keeping servers in a locked room) is rarely possible at remote locations that do not employ full-time IT staff. Access to a server's serial console from anywhere strengthens server security and enhances IT policies governing the confidentiality of corporate data.

### **Centralizing data center management**

Today's data center environment includes both a heterogeneous mix of servers and geographically dispersed servers and other devices such as uninterruptible power supplies and PBX phone systems. The IT staff needs to be able to manage this diverse environment from any location at any time of day or night, without regard to hardware type, operating system, or network status.

A console server needs to support all popular server operating systems and hardware features, such as a service processor and its Intelligent Platform Management Interface (IPMI). In addition, because many network-connected devices include only a serial console interface, a console server needs to be able to aggregate operating information from these devices. Uninterruptible power supplies, network routers and switches, telephony systems, and environmental control systems are examples of non-computing devices that can be controlled through a console server.

### **Controlling Costs**

Without remote access to a device's serial port, IT administrators are unable to securely communicate with an inoperative server unless they travel to the site. IT administrator travel incurs costs. A far larger cost is incurred if server availability is critical to the company's business. Productivity losses throughout the company further increase the negative effects of unplanned downtime. Space requirements also increase without remote access to the device's serial port.

When servers and other network equipment are functioning properly, in-band access to the devices and systems management applications normally suffice to monitor and manage the IT infrastructure. A serial console server directly addresses infrastructure hardware failures using secure out-of-band access to the failed device, even when the network is not functioning. The out-of-band capability enables IT administrators to communicate with a failed device without having to be physically present at the site where the device is located. Quicker access to failed devices reduces unplanned downtime on the production network and enhances a company's ability to maintain or even improve its revenue stream.

### **Reducing Complexity**

The variety of servers and other devices in a typical corporate environment complicate detection of hardware failures and initiation of correct recovery features. Each device may support a different serial port connector, and there is no standard for the pin assignments on the commonly used RJ-45 serial connector. Add to this the different types and lengths of serial cables, and the complexity of merely gaining access to serial ports often requires significant investments of IT staff time and budget.

Simpler cabling and connectors increase the infrastructure management value of a console server. Standard CAT5 cables and RJ-45 connectors, coupled with configurable cabling pin-outs, add flexibility and eliminate the need for specialized adapters to connect to the console server.

### **Increasing staff productivity**

Automating as many routine, repetitive administrative tasks as possible contributes significantly to a more productive IT staff. Locating and creating an inventory of all IT assets, particularly at remote locations, consumes many hours of staff time that could be more productively used on other, more strategic tasks. Staff hiring and training also becomes more difficult, time-consuming, and expensive in a heterogeneous and dispersed environment in which each server and device relies on a different user interface.

A serial console that automates discovery of any serially connected device saves configuration and installation time, and reduces the chance of human error. In the same vein, a consistent user interface simplifies configuration of a large number of servers and other devices that could be dispersed among many locations. And a consistent, simple, Web-based interface reduces hiring and training costs.

# Secure Remote Access for IT Infrastructure Management

## The Cyclades® ACS Advanced Console Server Solution

Avocent's Cyclades ACS advanced console servers provide IT and network operations center staff with the ability to perform secure, remote and out-of-band data center management of IT infrastructure from anywhere in the world. It also offers an Enhanced Security Framework that provides current security profiles and enough flexibility for IT administrators to create custom security profiles that comply with existing network security policies. Figure 4 illustrates a typical production network infrastructure including an ACS console server.

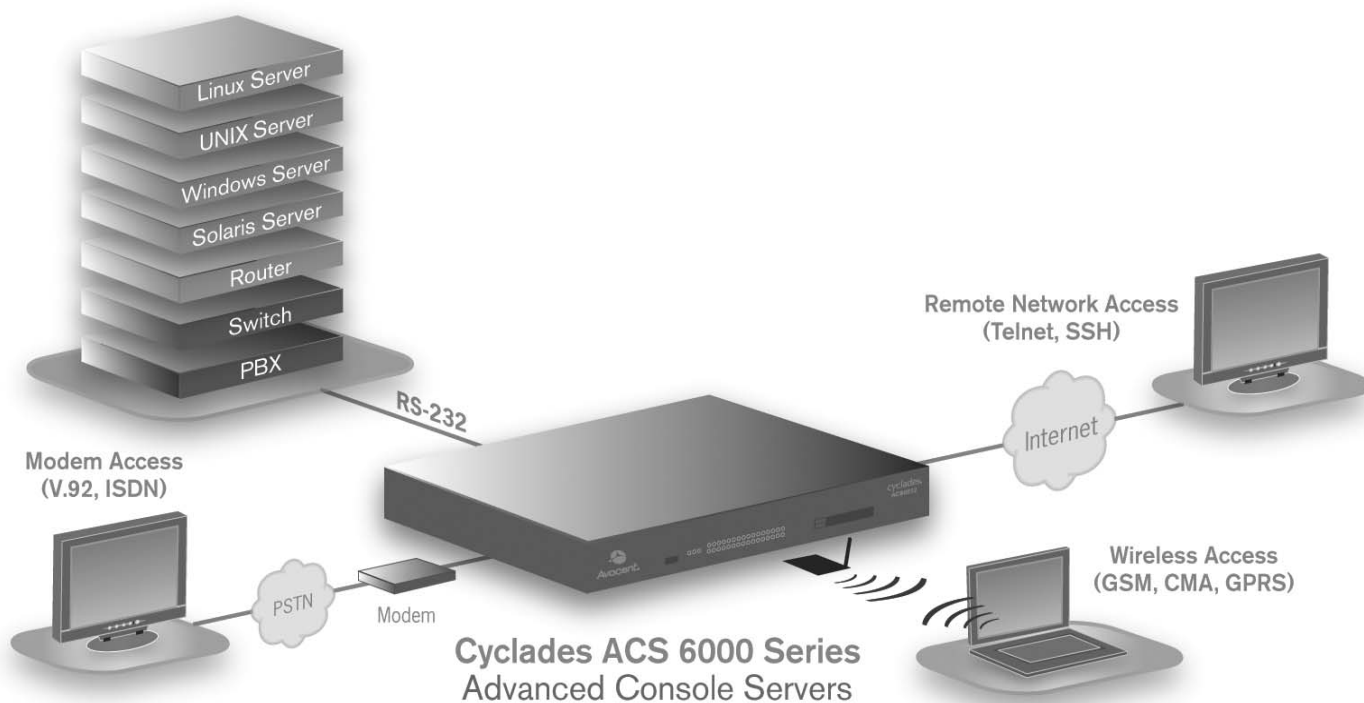


Figure 4. The Cyclades ACS Console Server in the Data Center Infrastructure

### Maximizing Network Availability

Perhaps the single most important objective of today's IT staff is to ensure that data is available to customers, suppliers, and company employees without interruption. Unplanned server or network downtime undermines that objective and causes productivity losses and reduced revenue to every one of the company's partners.

To ensure that a company's data and its network are always available, the Cyclades ACS console server provides both in-band and out-of-band remote access to servers and other serially connected networked devices. IT access to the console server is available from any location at any time, providing the IT administrator with low-level control of network attached hardware. This control includes hardware self-test, BIOS access, power cycling, and remote rebooting.

### Protecting Network Security

The Cyclades ACS console server integrates with a company's existing security structure and supports enterprise security policies. It supports strong user authentication using two-factor authentication with RSA SecurID and device authentication using certificates and a host key. The ACS console server is compatible with virtually all authentication servers, including RADIUS, LDAP, Active Directory, TACACS+, Kerberos, and NIS protocols. Supported authorization methods include local access control lists or server-based group authorization through Active Directory, LDAP, TACACS+, or RADIUS. The ACS console server also supports role-based authorization, and maintains both remote and local data and event logs and audit trails. It supports data encryption and secure out-of-band dial-up access through a V.92 or ISDN modem.

### Centralizing Data Center Management

The Cyclades ACS console server provides both in-band and out-of-band remote access to connected serial devices. In-band access is available through single or dual Ethernet ports, which support up to 1 Gbit/second transmission speeds and secure Telnet and SSH access to serial devices. A PC card slot (16- or 32-bit) supplies wireless remote access. Out-of-band access is available through either a built-in modem or a customer-supplied V.92 or ISDN modem.

The ACS console server easily configures and manages large data centers using a browser-based interface. Tight integration with Avocent DSView 3 software provides an effective method to configure and manage servers using a consistent, simple interface (see Figure 5). The ACS console server also integrates power management from a single interface for any third-party power supply vendor.

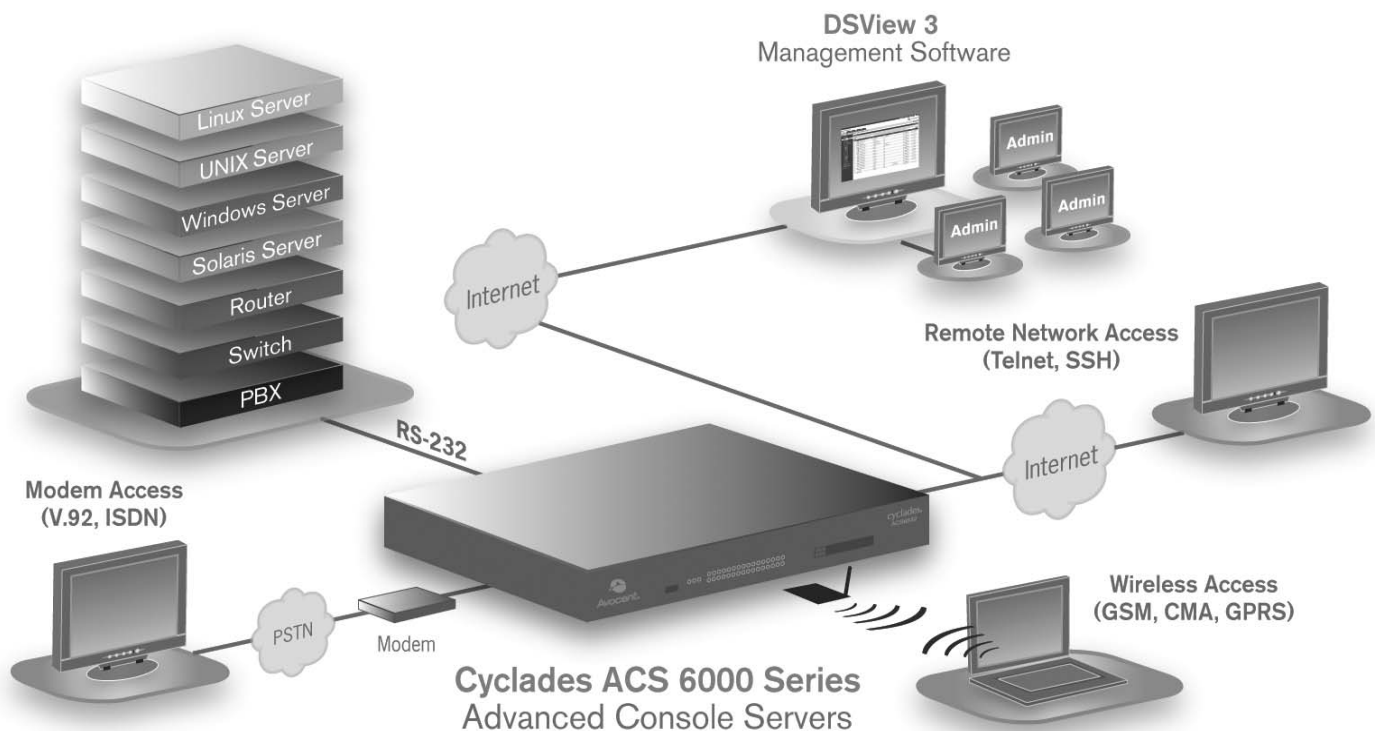


Figure 5. Integrating DSView 3 in the Data Center Infrastructure

### Controlling Operational Costs

Remote access to all devices connected to the ACS console server virtually eliminates the need for IT staff to travel to remote sites in order to manage and maintain servers and other network equipment. Not only does this save travel costs, but remote access also reduces recovery time for unplanned downtime, which helps a company meet its revenue goals.

### Providing Easier IT Management

By using a simple, secure Web-based interface, the Cyclades ACS console server enables an IT administrator to configure and manage any networked device with a serial port. This includes servers, routers, switches, and some non-computing devices such as power supplies, HVAC controls, and building alarms.

The ACS console server also simplifies cabling requirements. Standard CAT5 cabling terminated with inexpensive RJ-45 connectors supply the needed connections to the console server. Because RJ-45 pin-outs differ from one manufacturer to another, the ACS console server provides a software-configurable pin-out feature to simplify serial connections between a device and the console server.

## Enhancing IT Staff Productivity

The auto-discovery mechanism of the ACS console server saves significant amounts of IT time at the time of initial installation and configuration. Auto-discovery detects the names of connected devices and updates the network configuration automatically, reducing the possibility of data entry errors and further helping to maximize uptime. The auto-discovery feature also detects servers that have been re-located, which allows the IT staff to avoid time-consuming and error-prone re-configuration.

The ACS console server's consistent Web-based interface also simplifies hiring and training requirements, and enables the IT staff to configure and manage large numbers of servers and other devices.

## Conclusion

The Cyclades ACS Advanced Console Server provides secure remote access to serial consoles for servers and other devices, including power supplies, telephony equipment, and network routers and switches. Out-of-band capability enables secure console access from anywhere at any time regardless of network availability, reducing downtime and virtually eliminating travel to remote sites. The Cyclades ACS console server solution includes integrated power management and centralized management to support network security, administration, maintenance, and upgrades. The ACS console server reduces operational costs, automates device discovery, and simplifies cabling and pin-out requirements.

## About Avocent Corporation

Avocent (NASDAQ:AVCT) delivers IT operations and infrastructure management solutions for enterprises worldwide, helping customers to reduce costs and simplify complex IT environments via integrated, centralized in-band and out-of-band hardware and software.

Through LANDesk®, Avocent also is a leading provider of systems, security, and process management solutions. Find more information at [www.avocent.com](http://www.avocent.com).