Market Central®

www.secureswitch.com

500 Business Center Drive Pittsburgh, PA 15205 USA
412.494.2800 CAGE 1BGJ7

APPLICATION NOTES
SwitchMaster® R5000 Series & R6000 Series Switching Systems

SwitchMaster® R5000 Series & R6000 Series Switching Systems are Layer 1 Switches are used to add access control, network backup and fail-over switching and other capabilities to data networks. This paper presents some typical applications. Applications diagrams shown below apply to the R5000 Series as well as to the R6000 Series that is shown. R1000 Series switching systems are not expandable but support most applications shown within the limits of the number and ports (10/100 Base-T Ethernet and Gigabit fiber optics). Please note that the R1000 Series systems do not support Gigabit, wire-based Ethernet as do the R5000 Series and R6000 Series systems.

A Layer 1 switch is a device that operates at layer 1 in the OSI model. The device transmits electrical or optical signals. It does not concern itself with bits, bytes, or protocols. Each switch has a 'common' port (referred to as C) that is latched to its associated A or B port. A SwitchMaster chassis will usually contain multiple switch modules.

There are several features of these switches that make them attractive. First, the port settings are software controllable, making it a simple matter to toggle a connected device from the A to the B position remotely. This also allows for automation to control individual settings. It's a significant boost for building a reliable network. Second, the switches support any number of connection types: RJ45, DB9, AC power and multi-mode fiber with various connector types. Third, and most important for a resilient design, the switches transmit signals even if the box is 'down'. That is, you can disconnect the AC to the switch, or even remove the management module, and the switch will continue to let signals pass. The switches use relays or micro-miniature mirrors that are physically latched into position. Once a position is set, it stays

set. Thus, even though it might look like you are introducing a single point of failure, the switch is nearly as reliable as the cables attached to it.

Consider a call center where IP phones and user workstations are connected to a data closet. It may be desirable to provide some resilience in case the layer2 switch in the data closet goes down, However, you may not want to dual-attach every call center device; that's too expensive and also impractical if there are IP phones. Until now, the only option was a chassis-based Layer 2 switch with dual power supplies and dual supervisors. That option is expensive and still leaves an exposure: if the blade in the chassis fails, workstations and IP phones still become unavailable.

Putting a Layer 1 switch in the mix is a better solution. Place the Layer1 switch between the Workstation/IP phone and the Layer 2 switch in the closet. Replace the expensive, mostly-redundant, chassis with separate inexpensive standalone Layer2 switches. Management access to the Layer1 switch is via a normal Ethernet port on the secondary Layer2 closet switch.

When using the Layer1 switch, the Layer2 switches in the closets do not have to be of the dual-supervisor and dual-power-supply flavor. This makes for a more cost effective solution and it provides a simple solution to the problem of a failed chassis blade. As discussed earlier, the hardware 'latching' of the A/B position keeps electrical signals moving, even if the Layer1 switch is down; there is no need to worry about a failure in the Layer1 switch.

Another application provides a backup optical link for OC1/OC3 communications that permits the communications provider to test the backup line remotely for integrity before switching to it. A specially-configured fiber optic switch card provides this function, adding effective backup to a critical communications path. The backup optical link can be tested continuously for rapid switch-over in the event of a failure of the primary link.

Access to networks that contain confidential information has become a critical issue to those who generate and manage intellectual property. Chemical formulations, unique manufacturing processes and classified government information are examples of data that must be protected from unauthorized access. SwitchMaster systems provide a simple and effective way of controlling access to confidential information.

Providers of network service are usually required to supply network connections continuously. SwitchMaster switching systems make it a simple task to switch all users from a main network to a backup network locally or remotely under the control of a single network administrator. Software upgrades and network maintenance will not interrupt user activity when SwitchMaster systems are included at the edges of networks where users are connected.

Examples of the types of applications presented above are shown in the following slides. Please note that SwitchMaster R5000 Series systems will support the same applications for which the R6000 Series has been shown here. R5000 Series systems are one-half the height of R6000 Series systems and are preferred where rack space is limited.

“Private” network

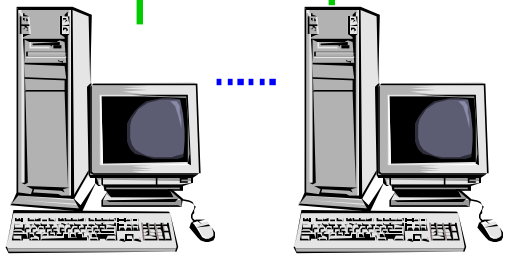
“Public” network

A

B

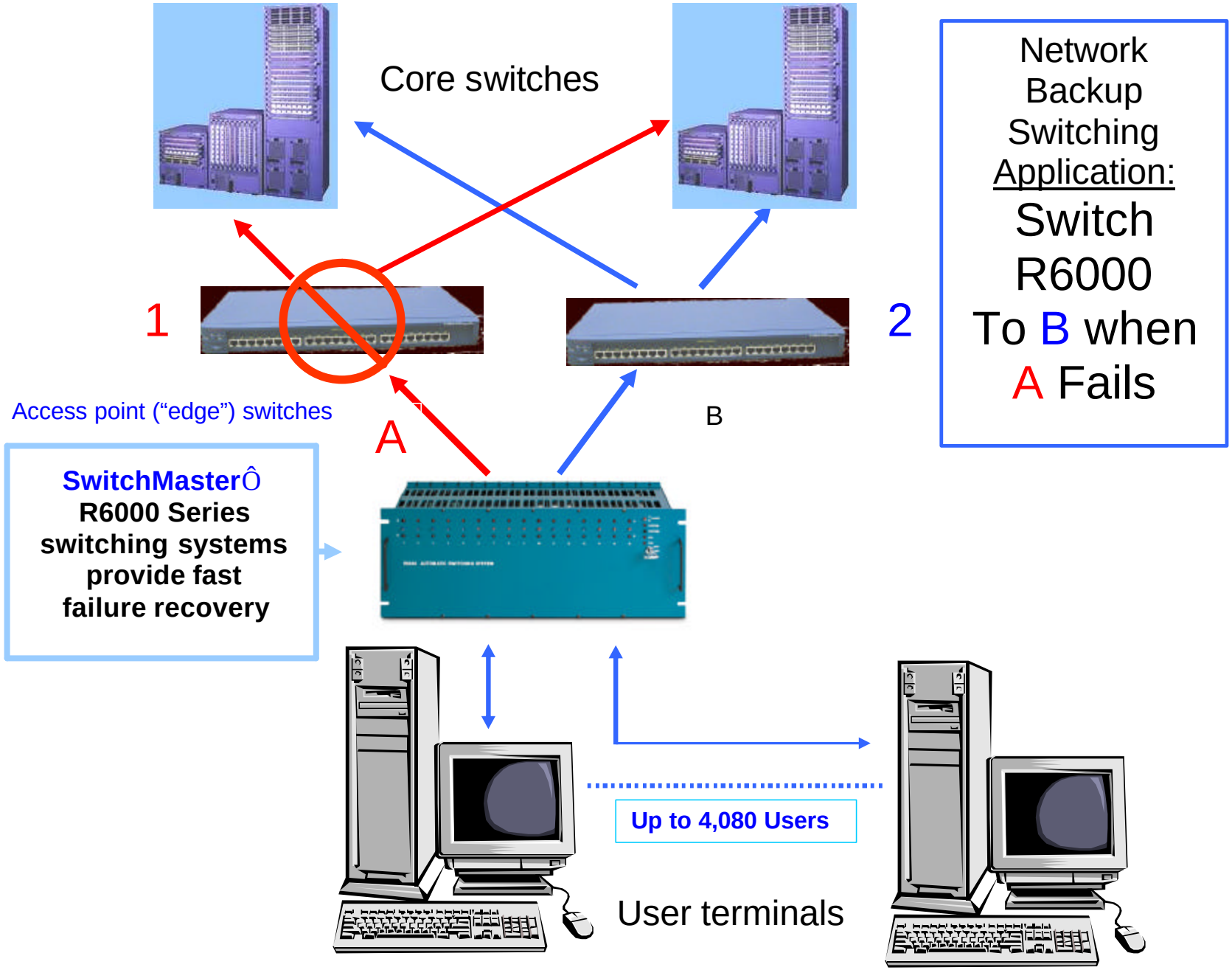
SwitchMaster™
R6000 Series
switching systems
implement remote
access control

Shut off access to the Private network based on time of day, virus detection, hacker alert...



User terminals

Network Access Control Application

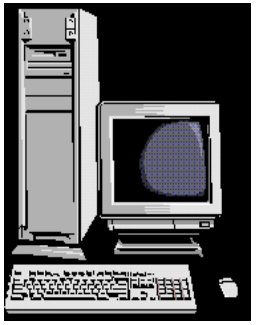


Network Backup Switching Application

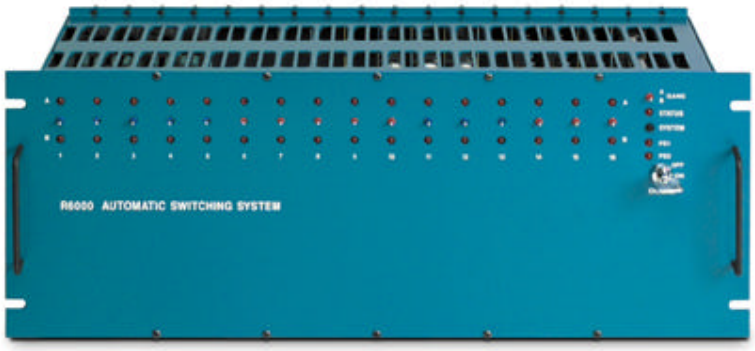
Market Central, Inc. 500 Business Center Drive Pittsburgh, PA 15205 412.494.2800 www.secureswitch.com CAGE Code 1BGJ7

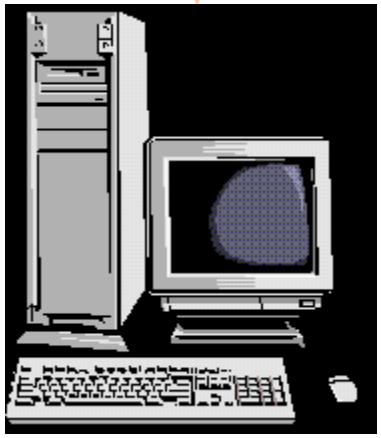
Manage trade secrets securely.
Control access and connections remotely via RS232, SNMP or World Wide Web, or locally under key-locked supervision.

Remotely located supervisor



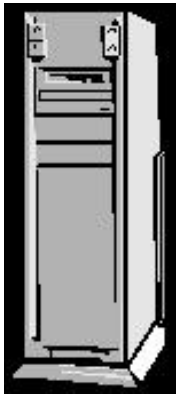
Cable, fiber RS232 or Coax (others optional)





Controlled user group

SwitchMaster Ô R6000 Series Switching System

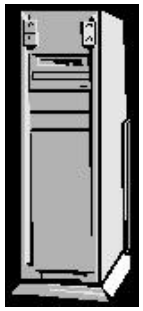


Trade Secrets & other intellectual property

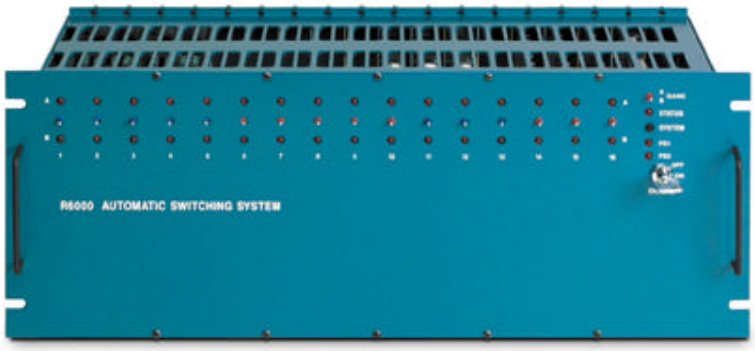
Market Central, Inc. 500 Business Center Drive Pittsburgh, PA 15205 412.494.2800 www.secureswitch.com CAGE Code 1BGJ7

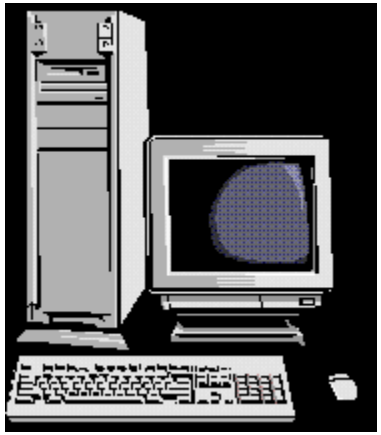
Switch connections from the main network to the backup network during maintenance or failure of the main network

Main Network Servers



Gigabit wire or fiber Ethernet, RS232 or Coax

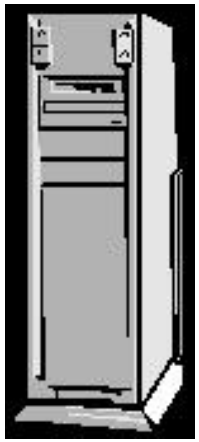




User groups of up to 4,080 users

SwitchMaster Ô R6000 Series Switching System

Backup Network Servers



Facilitate testing of the idle fiber optic connection by the central office

Central Office Primary Fiber Optic Connection

Central Office Secondary Fiber Optic Connection

A

B

SwitchMaster™ R6000 Series switching system with fiber optic loopback capability

The idle “OCX” connection can be loop tested for integrity before switching by the Central Office via SwitchMaster’s all-optical, full duplex fiber optic switch

OC1/OC3 Fiber Optic Backup Application