University Provides Unfettered Access with Flexible Network

Mississippi State University
Customer Case Study

Executive Summary

- Customer Name: Mississippi State University
- **Industry:** Higher Education
- **Location:** Mississippi, United States
- **Number of Users:** 24,000

Business Challenge:

- Support free flow of information and ideas
- Protect against viruses and malware in open environment
- Manage rapidly growing wireless user base

Network Solution:

- Cisco Borderless Network powered by Cisco network platforms with integrated security and wireless modules

Business Results:

- Simplify management and segmentation of network security
- Enable flexible, resilient wireless connectivity
- Help ensure secure connectivity for users anywhere, anytime

Mississippi State University uses integrated wireless and security solutions to create borderless academic network.

Business Challenge

Mississippi State University is a leading public research institute, serving nearly 20,000 students and more than 4700 faculty and staff. The university is committed to providing a dynamic academic environment, which increasingly means keeping faculty and students connected to each other and to the larger world over the Internet. Like all modern universities, however, Mississippi State must balance academic freedom with information security.

“Freedom of access is always an issue,” says Gerhard Lehnerer, Manager of Network Services, Mississippi State. “All these viruses and malware are lurking out there, and we have to do everything we can to minimize the spread. But any time you are potentially restricting faculty research or students’ access to information, it’s a tough proposition. There’s always some new technology coming out that we need to support or a new need to collaborate with someone outside the network. There is always a push and pull.”

Some of the biggest challenges that Mississippi State Information Technology Services faces involve managing the massive growth in wireless connectivity.

“Just a few years ago, wireless was considered an optional service, and most users depended on the wired network,” says Todd Hall, Senior Network Analyst, Mississippi State. “Now a lot of our users rely on the wireless network as their primary means of connectivity. On a given day, we support 4000 simultaneous wireless users.”

"We can handle everything right from the Catalyst 6500, and all of our security is managed directly on the backplane. It makes the solution both easier to manage and more cost-effective."

Greg Grimes,
Senior Network Analyst,
Mississippi State University

"Wireless seems to be growing exponentially," adds Greg Grimes, Senior Network Analyst at Mississippi State. "At the beginning of the 2010 school year, we added 1000 new IP addresses to our wireless network. Within two or three weeks, we had less than 100 available, and had to expand again."

In addition to managing the sheer scale of wireless services on campus, controlling wireless security is a constant challenge.

"When people are using physical wall ports, we know where they are," says Lehnerer. "If someone is spreading a virus or engaging in malicious activity, we can find the MAC address and, if necessary, come and find them. With wireless, you could be anywhere. It's much more challenging to manage."

Network Solution

To manage this demanding and constantly evolving environment, Mississippi State uses an end-to-end Cisco® network. Drawing on Cisco Catalyst® switches with integrated security and wireless capabilities, Mississippi State has created a borderless network that allows them to connect anyone (any student, faculty, or guest) to any device or service, anywhere on or off campus, anytime. And, Mississippi State can provide this connectivity securely, reliably, and with excellent performance and manageability. Key to these capabilities is Mississippi State's core network, built on Cisco Catalyst® 6500 Series switches with Firewall Services Modules (FWSM) and Wireless Services Modules (WiSM).

Using the FWSMs, Mississippi State is able to virtualize security services across the campus. The IT team can maintain separate virtual LANs (VLANs) for each department and dormitory, assigning some VLANs to a single physical location, while others, such as IT's own network, extend across multiple buildings or the entire campus. Each VLAN has its own virtual context operating in transparent mode in the FWSM, allowing Mississippi State to maintain virtual firewalls for multiple departments and networks using a single physical device.

To manage the firewall modules and contexts, and simplify the process of controlling policies across the network, Mississippi State uses Cisco Security Manager (CSM).

"CSM gives us the ability to define default rule sets for every firewall context, with the ability to customize policies for individual departments and groups," says Grimes. "The combination of CSM and firewall modules has made it easy to manage each firewall context and our overall security environment."

The WiSM solutions provide comparable flexibility for wireless services, as well as providing an extra layer of redundancy, since a wireless module in one Catalyst 6500 switch can take over management of another platform's connected wireless access points in the event of a failure. Using the WiSMs, as well as Cisco Wireless Control System (WCS), the Mississippi State IT team is able to easily manage and secure the more than 1000 Cisco Aironet® wireless access points that now blanket the campus.

Students, faculty, and other employees connecting to the wireless network all use the same Service Set Identifier (SSID) and a single VLAN. (Guest users connect via a separate, walled-off SSID.) This arrangement allows Mississippi State to add an extra layer of protection to wireless connections using 802.1x port security. The university also blocks unauthorized users by requiring anyone attempting to connect to the university network wirelessly to authenticate with the centralized RADIUS system.

Product List

Routing and Switching

- Cisco Catalyst 6500 Series Switch
- Cisco Catalyst 3750 Series Switch
- Cisco Catalyst 2960 Series Switch

Security and VPN

- Cisco Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series
- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco Security Manager (CSM)

Wireless

- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series
- Cisco Wireless Control System (WCS)
- Cisco Aironet® Wireless Access Points

Business Results

Mississippi State's Cisco network provides the reliability, security, and flexibility to maintain the unfettered flow of information and ideas that is essential for the university. And, with the ability to virtualize many services and consolidate multiple technologies into a single Cisco Catalyst 6500 platform, the university's IT team can efficiently manage and control this dynamic environment.

"Using the firewall modules in transparent mode allows us to eliminate many separate physical security devices that we would otherwise have to maintain," says Grimes. "We can handle everything right from the Catalyst 6500, and all of our security is managed directly on the backplane. It makes the solution both easier to manage and more cost-effective."

"We achieve the same benefits with our wireless services," says Lehnerer. "If we were using an external wireless controller, we would have to manage many separate devices. By using a module on our switch, we don't need any additional rack space, which is a major benefit in some of the older buildings on campus. In addition, since everything is contained in a single chassis with redundant power supplies and fans, all the redundancy we get with our Catalyst 6500 now applies to our wireless and firewall solutions as well."

The integrated security capabilities of Mississippi State's network, and the ability to easily virtualize and segment the network using FWSMs, provide the performance that a thriving academic network requires.

"The ability to use virtual firewall contexts in transparent mode makes it very easy to secure traffic in various VLANs," says Grimes. "In the past, we used ACLs [access control lists] on our switches, which caused performance issues. As soon as we moved to the firewall modules, we saw a significant decrease in CPU utilization."

The Cisco wireless capabilities, powered by the Cisco WiSMs and WCS, allow Mississippi State to provide true borderless mobility and flexibility for users across campus.

"We use WCS to address a broad range of problems in our wireless environment," says Grimes. "We can find signal strength issues, interference issues, authentication, DHCP [Dynamic Host Protocol Configuration]. We're also able to quickly implement consistent configurations across our entire network. The combination of the wireless modules and WCS makes managing our network very easy."

The IT team also uses WCS to detect security threats in the wireless environment, and improve the overall security of the entire network.

"Today, we've mapped our floor plans into WCS for most of our buildings," says Grimes. "We can use it to triangulate the location of rogue access points or even track a device that has been stolen. It's extremely useful."

All of these capabilities are based on the Cisco Borderless Network, and the broad range of Cisco wired, wireless, and security technologies that work hand-in-hand to create a secure, manageable, and highly flexible environment.

For More Information

To find out more about Cisco Borderless Networks, visit www.cisco.com/go/borderless.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.

C36-646476-00 01/11