

University Protects Fair Network Access for Students and Staff

Indiana State University chooses a carrier-class solution to control peer-to-peer traffic and optimize bandwidth.

| EXECUTIVE SUMMARY |
|--|
| <p>Indiana State University</p> <ul style="list-style-type: none"> • Education • Terre Haute, Indiana • 10,679 <p>BUSINESS CHALLENGE</p> <ul style="list-style-type: none"> • Control peer-to-peer traffic on the university's network • Scale bandwidth and protocol management capabilities to manage a 1-GB Internet connection • Simplify bandwidth management for thousands of active users, applications, and endpoint devices |
| <p>NETWORK SOLUTION</p> <ul style="list-style-type: none"> • Cisco Campus Secure for Higher Education Networks, including the Cisco SCE 1010 Series Service Control Engine for comprehensive bandwidth management and Cisco Clean Access for secure student network access. |
| <p>BUSINESS RESULTS</p> <ul style="list-style-type: none"> • Automated bandwidth control to help ensure fair bandwidth access for users and to enforce policies • Avoided cost of having to purchase additional bandwidth to make up for bandwidth consumed by peer-to-peer traffic • Reduced burden on IT resources Enable company and key executives to maintain and benefit from established working relationship. |

Business Challenge

Indiana State University (ISU) was founded as a teachers college in 1865. Today, students choose from more than 100 degree programs and are supported by extensive technology resources. Three thousand students live on campus and access the public Internet from their residence hall rooms using a broadband connection.

Like all universities, ISU must manage bandwidth carefully, so that students, faculty, and administrators can use secure, highly available applications while maintaining an open, flexible learning environment. However, the growing volume of bandwidth-intensive, peer-to-peer (P2P) traffic and gaming applications posed a significant bandwidth management challenge. P2P applications frequently tunneled into regular browsing protocols, making it difficult to manage without denying Internet access altogether. Many campus users did not realize that using a P2P application to download files from the Internet also allowed external users to access files from ISU users' systems. ISU

maintained an 88-MB connection to the public Internet, and external P2P application users would take advantage of the high bandwidth to upload files from ISU users' computers—consuming up to 30 MB of Indiana State University's costly bandwidth without anyone knowing and without ISU users receiving any benefit. Canny external users had also learned how to bypass the university's existing packet-shaping bandwidth management solution to avoid detection.

This situation would be further complicated when ISU was joined to the Indiana I-Light network early in 2007—the Indiana higher education network which in addition to providing inter-institutional connectivity, provides a 1-GB connection to Internet2. ISU will connect at 1-GB, which exceeded the existing packet-shaping solution's interface and throughput capacity. The new I-Light connection also required a comprehensive firewall solution.

With thousands of active users, endpoint devices, and applications, ISU needed a better way to better control network traffic and preserve fair access to bandwidth without further straining the resources of its IT staff.

Network Solution

Gerald Oliver, along with his team of dedicated network engineering staff, searched for a bandwidth management solution that could meet the university's requirements. Unfortunately, the school's bandwidth and management requirements exceeded the capabilities of the enterprise solutions previously identified, and Indiana State University's small IT team did not have the time or resources to develop a solution internally. Instead, ISU turned to Cisco® and tried a new approach to solving the problem.

Cisco suggested the Cisco SCE 1000 Series Service Control Engine, a network element originally designed for carrier-grade deployments. The Cisco SCE 1000 provides high-capacity stateful application and session-based classification and control of application-level IP traffic, on a per-subscriber basis. It would give ISU the ability to optimize bandwidth while identifying and managing application traffic flows over the existing broadband cable infrastructure. In addition, the Cisco SCE 1000 enables Oliver's team to control content-based services in real time for any given user or group of users—all with carrier-grade high performance.

ISU set the bandwidth management policies, allowing students to have 10 GB of bandwidth per day for FTP downloads and Web browsing. P2P traffic is assigned a lower priority than other traffic types. When the Cisco SCE 1000 detects P2P protocols, it limits maximum allowable bandwidth for that user. If students exceed 10 GB per day, they are rated down to 20 MB during the day. During the evenings, student network traffic has access to almost all available bandwidth.

The Cisco SCE 1000 complemented ISU's existing Cisco Clean Access implementation, part of its Cisco Campus Secure for Higher Education solution. Cisco Campus Secure for Higher Education Networks provides a suite of powerful solutions that enable ISU to effectively secure and optimize its network campus while supporting a complex, open academic environment. In addition to delivering high visibility into network activity, the solution helps ISU effectively manage traffic and protect against known and unknown security threats.

“We rely on our network to help meet the needs of researchers and students, so downtime is not acceptable. The Cisco SCE 1000 Series has delivered carrier-class reliability since the first day. We installed it, turned it on, and it has remained up ever since.”

—Gerald Oliver, Assistant Director of Engineering Services

All student computers must have the Cisco Clean Access Agent installed, and each must pass Cisco Clean Access requirements for user authentication, vulnerability assessment, and remediation before gaining full access to the ISU network. ISU has implemented limited filtering features, such as virus blocking, to prevent students from consuming excessive campus bandwidth while enabling access to the public Internet. ISU also deployed redundant Cisco Firewall Services Modules in its Cisco Catalyst® switches, to meet the firewall requirement for its I-Light network connection.

Business Results

“We rely on our network to meet the instruction and research needs of our faculty and students, so downtime is not acceptable,” says Oliver. “The Cisco SCE 1000 Series has delivered carrier-class reliability since the first day. We installed it, turned it on, and it has remained up ever since.”

| PRODUCT LIST |
|--|
| Routing and Switching <ul style="list-style-type: none"> • Cisco Catalyst Switches |
| Network Management <ul style="list-style-type: none"> • Cisco SCE 1010 Service Control Engine |
| Security and VPN <ul style="list-style-type: none"> • Content Networking • URL filtering; virus blocking; Authentication, Authorization, and Accounting |
| Wireless <ul style="list-style-type: none"> • Cisco Structured Wireless-aware Network |

The Cisco SCE 1000 is also easy to support. A service configuration editor allows ISU to easily create configurations and deploy them to the control engine. This offers high operational flexibility while requiring minimal network bandwidth. A quota management feature enables ISU Network Engineering staff to allocate a defined amount of bandwidth to users on a per-hour or per-day basis. If usage exceeds the amount allowed, the engine automatically reduces the amount of bandwidth

available down to a predetermined amount. Each 24 hours, the engine automatically resets the defined quota.

“When we began using the Cisco SCE 1000, we allowed students 10 GB per day,” says Oliver. “We quickly identified several users who were using 20 to 30 GB per day. Using the Cisco SCE, we could automatically reduce their bandwidth to 100 MB when they exceeded the daily limit, which quickly stopped the bandwidth abuse.” Today students in our residence halls have access to a portion of the total bandwidth during the day; during the evening, when the network is not as heavily used for instruction, research, and administrative activities, students in residence halls have access to significantly more bandwidth.

ISU Network Engineering staff also identified users who used protocols that successfully bypassed the previous bandwidth control solution and used a very large portion of ISU’s bandwidth for outgoing P2P traffic. When the Cisco SCE 1000 was deployed, those users could no longer use those applications, which almost doubled ISU’s available outgoing bandwidth and improved connection performance for all users. As a result, ISU avoided having to purchase additional bandwidth to support its own distance learning applications and Website, which were being affected by the high P2P traffic volumes.

Now ISU can easily manage bandwidth over its 1GB connection to the I-Light network to support high-performance computing requirements, such as a remote sensing project and high-definition video research. In addition, Cisco Clean Access has greatly reduced the amount of user support required from the university to manage viruses and minimize security threats.

Next Steps

The next step for Oliver and his team of network engineers is to begin maximizing the Cisco SCE 1000’s statistical data and reporting capabilities. However, the solution has already greatly improved the university’s ability to manage bandwidth.

“The Cisco SCE 1000 just runs,” says Oliver. “If users really begin exceeding bandwidth quotas or external users begin consuming our bandwidth, we can simply push a button. It takes care of our most important network asset—bandwidth.”

For More Information

To find out more about Cisco solutions for education, visit www.cisco.com/go/3750-E.



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0701R)