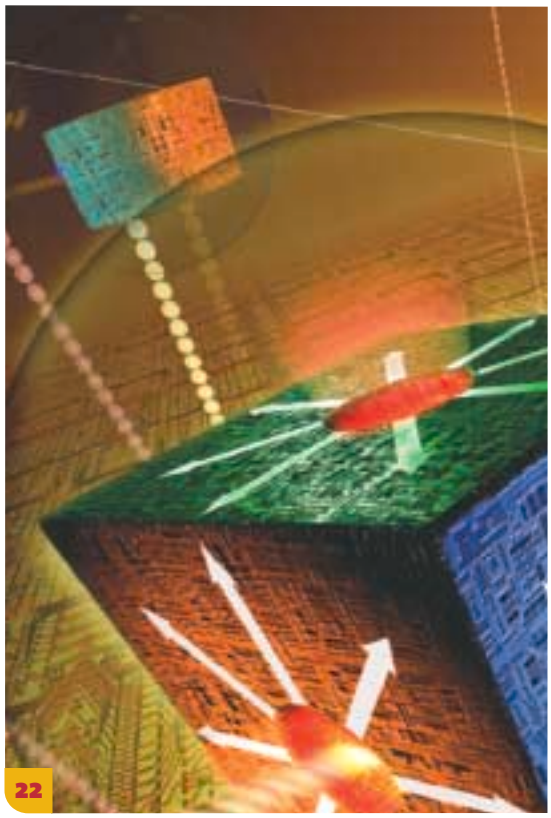
PACKET

CISCO SYSTEMS USERS MAGAZINE

FIRST QUARTER 2003 VOLUME 15 NO. 1



22

68

▼ ON THE COVER

A Good Defense

The extensive, complex, and open communications networks of 2003 require an integrated approach to security spanning the data center, LAN, and WAN. This article explores what it means to have security embedded throughout your network—and how Cisco makes this possible 22

▼ FEATURES

Background Checks

Over the years, Cisco IOS® security features have grown in sophistication as privacy threats have moved inward from the Internet edge to corporate data centers, wireless access points, and user desktops. New and existing features of Cisco IOS Software make an integrated approach to network security a reality for today's networks 27

Layer 2: the Weakest Link

Complete network security is only as strong as your weakest link—and that may well be the data link, or Layer 2. Threats and vulnerabilities to consider at Layer 2 are explored 30

Securing Wireless

Cisco's broad support for numerous Extensible Authentication Protocol types and the IEEE 802.1X standard provides for a centrally managed, standards-based, open wireless network security scheme that addresses the limitations of earlier 802.11 implementations 34

Secure Sleuthing

Lower costs and ready, interactive access to global databases fueled Interpol, the venerable 80-year-old international law enforcement agency, to trade in its private network for a virtual private network (VPN) that leverages the public Internet 37

SPECIAL REPORT

41 BUILDING AN IT BUSINESS CASE THAT WILL SELL—What Business Decision Makers Look for When Evaluating New IT Investments

▼ NETIZENS

Hot Hires

Cisco Networking Academy™ graduates from around the globe talk about how they have parlayed their training and talent into networking careers that provide a foundation for future development 68

PACKET

MPLS Fast Reroute

Korea: Seowon's VPN

Managed Services

TECHNOLOGY

15 MPLS: **Protecting SLAs During MPLS Outages**
A new approach to protecting service-level agreements (SLAs) in networks that run Multiprotocol Label Switching (MPLS) uses Cisco MPLS Fast Reroute connectivity protection and a new Cisco IOS® feature called Tunnel Builder Pro for greater bandwidth protection compared to Automatic Protection Switching.

18 IPv6 ADDRESSING: **IPv6 Time Is Now**
A primer on how IPv6 addresses are constructed and a sampling of the benefits of this next-generation technology.

ENTERPRISE SOLUTIONS

47 **Super Market Strategy**
Korean retailer Seowon is using Cisco virtual private network (VPN) technology, based on the SAFE Blueprint, to carve out an e-business strategy and deliver the foundation for future growth and converged services.

51 **Content Boost**
New Cisco Content Engine network modules combine content networking and edge routing into an integrated branch solution.

SERVICE PROVIDER SOLUTIONS

55 **The Rise of Managed Services**
Enterprises and small and midsized businesses are looking toward IP VPNs, IP telephony, security services, and other IP solutions to support their e-business efforts—and many of them are also turning to managed service providers for help.

62 **Metro Ethernet: More for Less**
Many service providers worldwide are protecting their investments in existing ATM, Frame Relay, and time-division multiplexing (TDM) infrastructures by seamlessly interconnecting them with metro Ethernet services.

SMALL AND MIDSIZED BUSINESSES

65 **Call for VoIP and Data**
Learn how managed services provider CallTower is helping its customers avoid upfront capital costs, ongoing maintenance, and multiple vendors with one integrated IP network service for telephony and data.

PACKET ONLINE EXCLUSIVE

Secure IP Telephony

Many of today's existing security components for data networks can also be used to secure voice in the network distribution layer, including providing security between the data and voice segments. Find out more about the technologies you can use to create secure IP voice networks at cisco.com/go/packet/.

▼ DEPARTMENTS

1 **From the Editor**
Happy Anniversary, *Packet*®!

4 **User Connection**
Latest Cisco e-learning courses ▪ Internet Economy leaders ▪ New Cisco security certification and courseware ▪ Online registration for Cisco products

7 **Tech Tips & Training**
Conquering the CCIE® lab ▪ Reader tips ▪ Storage Networking at-a-Glance tearout

73 **Technically Speaking**
Cisco's Chiara Regale discusses some of the new processes and improvements found in the IEEE 802.1w and 802.1s Spanning-Tree protocols.

75 **New Product Dispatches**
A roundup of what's new from Cisco over the past quarter.

▼ IN EVERY ISSUE

Mail 3
Calendar 4
Acquisitions 6
Networkers 6
Tech Tips 11
Advertiser Index 81
Cache File 82
The 5th Wave 82

CELEBRATING OUR 15TH YEAR IN PRINT

Meet the *Packet* team.

Meet the dedicated staff of professionals who work hard each quarter to make *Packet*® the most informative and useful networking technology magazine in the industry. Back row (left to right): R.J. Smith, production manager, Sunset Custom Publishing; Larissa Linn, production, Sunset; Mark Ryan, production, Sunset; Ellen Sokoloff, diagram illustrator; Bill Littell, print production manager; Kristen Bergman, advertising sales manager; David Ball, editor in chief; Susan Wright, editorial director, Sunset; Norma Tennis, production, Sunset. Front row (left to right): Michelle Gervais, production, Sunset; Sarah Beaver, online editor; Cecelia Glover Taylor, circulation manager; Shannon Thompson, business development director, Sunset; Emily Burch, designer; Jennifer Redovian, managing editor; Susan Borton, senior editor.

Editor's Note: Packet would also like to recognize the many excellent writers with whom we work on a regular basis, including Joanie Wexler, David Barry, Rhonda Raider, Gail Meredith, David Baum, Gene Knauer, Janet Kreiling, Connie Howard, Lee Sustar, and Janice King. Lastly, special thanks to our publisher, Michael Hakkert, who is not only Packet's greatest champion, but our customers' greatest ally, consistently placing editorial quality and reader satisfaction above all else. Thank you, team Packet. Here's to another 15 years. — D.B. ▲▲

Packet magazine

David Ball
EDITOR-IN-CHIEF

Michael Hakkert
PUBLISHER

Jennifer Redovian
MANAGING EDITOR

Susan Borton
SENIOR EDITOR

Sarah Beaver
ONLINE EDITOR

Joanie Wexler
CONTRIBUTING EDITOR

R.J. Smith
Sunset Custom Publishing
PRODUCTION MANAGER

Michele Gervais, Larissa Linn, Mark Ryan, Norma Tennis
Sunset Custom Publishing
PRODUCTION

Emily Burch
DESIGNER

Ellen Sokoloff
DIAGRAM ILLUSTRATOR

Bill Littell
PRINT PRODUCTION MANAGER

Cecelia Glover Taylor
CIRCULATION MANAGER

Fred Gambino
COVER ILLUSTRATION

SPECIAL THANKS TO THE FOLLOWING CONTRIBUTORS: Jessie Burke, Peggy Casey, Sean Convery, Janice King, Julie O'Brien, Stacey Wilkinson

ADVERTISING INFORMATION:

Kristen Bergman, 408 525-2542
kbergman@cisco.com

View *Packet* magazine at cisco.com/go/packet.

PUBLISHER INFORMATION:

Packet magazine (ISSN 1535-2439) is published quarterly by Cisco Systems and distributed free of charge to users of Cisco products. Application to mail at Periodicals Rates pending at San Jose, California, and additional mailing offices.

POSTMASTER: Please send direct address corrections and other correspondence to packet@external.cisco.com or to *Packet* in care of:

Packet Magazine
PO Box 2080
Skokie, Illinois 60076-9324
USA
Phone: 408-526-4000

FROM THE EDITOR

Happy Anniversary, *Packet*!

This year marks *Packet*® magazine's 15th year in print—15 years of keeping readers up to speed with the rapid advancements in internetworking. To celebrate, I'd like to introduce you to the talented people that make up the *Packet* team. I can think of no better issue in which to introduce them than one focused on security, for nothing makes me feel more secure—and able to sleep at night—than this hard-working team of dedicated professionals (see opposite page).

Like the *Packet* team, network security is a necessity, not a luxury. Because it is no longer viewed as an "add on," the trend toward integration—where security features are integrated in the routers and switches that make up the network fabric—will continue (see cover story, page 22). In fact, many of the Cisco routers and switches currently in your network may already boast security features—it's just a matter of turning them on. To learn more about the security capabilities of Cisco routers, read "Background Checks" (page 27). For more on switch security, see "Layer 2: the Weakest Link" (page 30). And of course, no security issue would be complete without the Cisco SAFE Blueprint—a free, pullout poster (after page 34), now in its third year as a *Packet* insert and bigger than ever.

Due to the importance and complexity of network security, there's a growing trend toward managed security services. In "The Rise of Managed Services" (page 55) you'll learn how service providers and their customers are benefiting from a variety of out-tasked services, including security, multiservice virtual private networks (VPNs), and IP telephony.

Whether you outsource or "go it alone," you still need to justify that information technology (IT) expense. "Building an IT Business Case That Will Sell" (page 41) will help you position your next project to management, and offers a look at the technologies that could provide the most promising return on investment.

To satisfy your yearning to learn, we've included some technology pieces on the latest innovations in IPv6 (page 18) and Multiprotocol Label Switching (MPLS) tunneling (page 15). For those on the Cisco certifications track, Networking Learning, Inc.'s Scott Morris shares his study secrets in "Conquering the CCIE® Lab" (page 7). For those not quite ready for the CCIE, check out how some recent Cisco Networking Academy™ graduates from around the world are faring in "Hot Hires" (page 68).

In the "What's New" department, we're adding *cheat sheets* this year—one-page tutorials on key technologies, which are perforated so you can easily tear them out for handy reference. Check out the first in the series, "Storage-Area Networks at a Glance" (page 13). Also, you may have noticed something different at Cisco.com. The Cisco Web site has undergone a major architectural change. Now, *Packet Online* readers can reap the benefit of those changes with advanced functionality, including the ability to search only the *Packet* site for the information you're looking for. There's also a toolbar that will make it easier for you to print articles, or e-mail them to friends and colleagues. Other features include a related links area in addition to the ones included with most *Packet* articles. Visit cisco.com/go/packet and let us know what you think.

David A. Ball
Editor-in-Chief
daball@cisco.com

Mail

Get a GRIP

I would like to know when Cisco Globally Resilient IP (GRIP) will be available, and for which router platform.

—Tiago Luiz Teodoro, EDS Brazil

Following is a response from Tim McSweeney, product marketing manager for Cisco Globally Resilient IP. —Editors

GRIP will be available on several Cisco platforms. The first six GRIP features, including Cisco Nonstop Forwarding and Stateful Switchover, are now available for the Cisco 12000, 10000, and 7500 series routers. A presentation that contains a table listing feature availability by platform (slide 32) is available at cisco.com/warp/public/732/Tech/grip/pres.shtml.

Since that slide was posted in May 2002, several of the features are now available on additional platforms as well. The coverage will increase over time, of course. If you have additional questions, don't hesitate to contact me at timcswee@cisco.com.

Tech Tip Tip

I want to give a warning on one of the tech tips that I saw in *Packet*® [Third Quarter 2002] under Troubleshooting. The tip "debug just a little" is a great tip but I wanted to point out that if you delete the access-list that the debug is linked to before doing a **debug all** the Cisco IOS® Software will do a full **debug ip** packet! This could cause your router to hang if there is a heavy load.

—Shawn Coleman, Equant, New York

How About a Chinese Edition?

I recently read *Packet* for the first time. As a network manager, I was pleased to read your first issue devoted to network management [Third Quarter 2002]. Thank you.

As a Chinese reader, I can learn about the latest Cisco and networking technologies from your magazine. I am especially interested in "Tech Tips & Training." After reading this issue twice, I hurried to Cisco.com to subscribe to *Packet*. I meet with many students who wish to become familiar with Cisco, but they cannot get the right information. Many well-known magazines such as *Science* and *Nature* have Chinese editions, so I believe you could, too, and this would help you develop larger markets and influence more people.

—David Liu, Beijing Army Auto Station, China

We are happy that you find Packet *useful for your job. Someday we hope to have a Chinese edition. In the meantime, you might be interested in a Chinese publication from Cisco called* Networking China *that reports on industry trends and networking solutions important to China, as well as Cisco solutions, programs, events, and customer case studies.* Networking China *also reprints key technical articles from* Packet *that are most relevant to the region. To request a subscription to* Networking China *contact Shang Rong at rshang@cisco.com.—Editors*

Kudos for Tech Tips & Training

Although I enjoy the entire magazine, the "Tech Tips & Training" section is absolutely fantastic. I have been able to apply a lot of it in my own work. Please keep it going. You have a great magazine and I recommend it to all of my students.

—Brent Dillon, CCSI, CCNP, Computer Learning Centers, Utah

We have had an overwhelmingly positive response to the new "Tech Tips & Training" section, especially the reader tips. So rest assured, as long as we keep getting tips from readers, we'll keep printing them.—Editors

Fan Mail

I LOVE *Packet*! Well OK, maybe that's a bit strong, but I enjoy the magazine. Excellent tips inside. *Packet* is welcome in my mailbox, and I religiously reregister my subscription, which leads me to the Web site. I should also throw in my two cents that Cisco.com is, without a doubt, the best Web site out there for support, knowledge base, search tools, information, concepts, and of course, downloadable PowerPoint *Packet* diagrams. I read *Packet* for the snappy diagrams, helpful tips, and layman's language in explaining new technology, which is something I still like to be able to read about without putting on the tech cap.

—Phil Sosaya, Globecast España, Spain

Thank You for the Inspiration

As in the past, with each and every new issue the content you provide in this magazine inspires me to remain in the networking field. All credit goes to your great group that is constantly striving for the GOOD factor to add in this magazine.

—Mani Shankar Pandey, Software Technology Parks of India, India

SEND YOUR COMMENTS TO *PACKET*

We welcome your comments and questions. Reach us through e-mail at **packet-editors@cisco.com**. Be sure to include your name, company affiliation, and e-mail address. Letters may be edited for clarity and length.
Note: The *Packet* editorial staff cannot provide help-desk services.

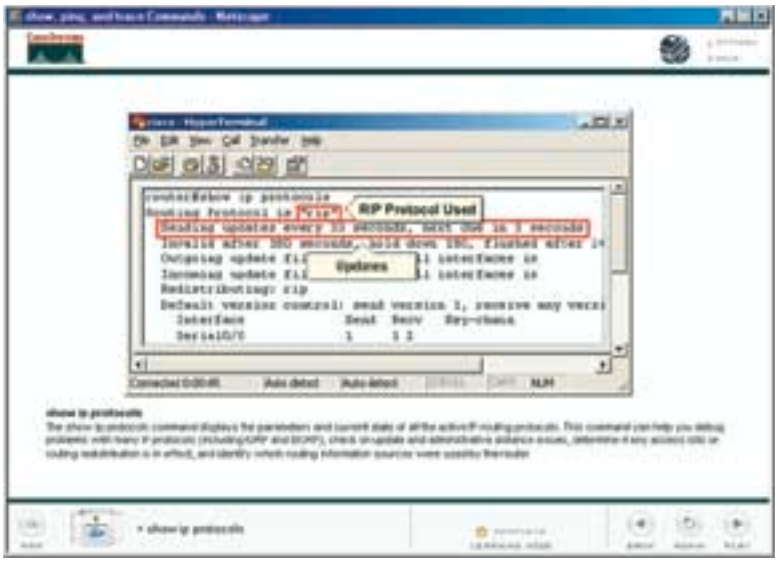
User Connection

Latest Cisco E-Learning Courses

Internet-based courses speed training and certification of networking professionals.

As companies realize that cost-effective online learning is a powerful strategy to build their competitive edge in the knowledge-based economy, the number of certification candidates choosing e-learning courses to prepare for their exams continues to rise. In fact, analysts predict that the corporate e-learning market will reach over US$30 billion by 2005, up from US$2 billion in 2001.

Now the latest Cisco e-learning courses are available from authorized Cisco Learning Partners worldwide. The self-paced courses enable professionals preparing for networking certifications to maximize their knowledge retention, and guarantee results in the shortest period of time. The courses, which are packaged in a more accessible, customized, learner-centric format, are designed to reduce training costs, provide easier access to educational materials, increase opportunities for collaboration, and provide greater accountability.



SELF-PACED MODULES: Hands-on labs ensure in-depth understanding.

Course Offerings and Availability

Updated to reflect technology advancements, product enhancements, and new learning techniques, the online courses use a best-practices approach that takes into account current platforms, technology, and content. Courses include the following components:

- Hands-on emphasis to keep students engaged in learning
- Repeatable labs to help ensure in-depth understanding
- Simulations to provide lab experiences without installing equipment
- Built-in search and reference capabilities to help students get quick answers to questions

The platform-independent courses, which are often blended with other learning solutions such as instructor-led training, mentoring, live labs, and more, include:

- CCNA®: Interconnecting Cisco Network Devices (ICND)
- CCDA®: Designing Cisco Networks (DCN)
- CCNP®, CCDP®, and CCIP™: Building Scalable Cisco Internetworks (BSCI)
- CCNP and CCDP: Building Cisco Multilayer Switched Networks (BCMSN)
- CCNP and CCDP: Building Cisco Remote Access Networks (BCRAN)
- CCNP: Cisco Internetwork Troubleshooting (CIT)

For more information about Cisco e-learning and to see a demonstration, visit cisco.com/go/ciscoelearningcourses. ▲▲

Cisco Worldwide Events

February 10–12	Call Center and CRM Solutions 2003, Las Vegas, Nevada, USA
February 17–18	VoiceCon, Washington DC, USA
February 18–21	GSM World Conference, Cannes, France
March 11–13	Networkers Australia 2003, Brisbane, Australia
March 16–21	Cisco Powered Network Operations Symposium, San Jose, California, USA
March 25–27	OFC 2003, Atlanta, Georgia, USA
April 29–May 1	Networld+Interop, Las Vegas, Nevada, USA

cisco.com/warp/public/688/events.html

Leading in the Internet Economy

Effective leadership may be the single most important reason companies succeed in the Internet economy. The most successful companies have strong, targeted leadership, and these companies are making fundamental changes in how they operate—considering better ways to conduct business and using the Internet to work smarter. Read about the executives, companies, and strategies that exemplify leadership in the Internet economy during challenging economic times. The annual leadership issue of *iQ Magazine,* the Cisco Internet business strategy publication for executives, looks at six industries and how Internet solutions are helping solve long-time challenges. Find it at cisco.com/go/iqleaders2002. ▲▲

New Cisco Security Professional Certification and Courseware

To help meet the heightened demand for knowledgeable network professionals who can design, build, and implement complete end-to-end network security solutions, and to provide a certification career path in the information technology (IT) security market, Cisco has introduced the new Cisco Certified Security Professional (CCSP) certification and three new security designations within the Cisco Qualified Specialists category: the Cisco Firewall Specialist, the Cisco Virtual Private Network (VPN) Specialist, and the Cisco Intrusion Detection System (IDS) Specialist.

SAFE Expertise

The new certifications will enable participants to attain professional-level expertise in designing and implementing secure Cisco networks using VPN, IDS, and firewall technologies. Participants will gain experience using the SAFE Blueprint from Cisco to design integrated security solutions.

Certifications are available to Cisco security professionals, system engineers, Cisco partners, and Cisco network professionals and customers. To become a CCSP or to achieve a focused certification, participants must already hold a valid CCNA® certification and must complete and pass all required exams. The exams test candidates' understanding of how to use and implement the principles in the SAFE white paper, which is available at cisco.com/go/safe. Candidates are tested on their knowledge of how various security devices, such as IOS® routers, PIX® firewalls, VPN concentrators, Cisco IDS sensors, Cisco Host IDS, and the Cisco VPN Client combined create a complete end-to-end security solution. Training to prepare for the security certifications is available through authorized Cisco Learning Partners worldwide.

> "Cisco provides options. If you want to validate your skills in one specific area of security, for example, in firewalling or intrusion detection, you can do that thanks to these specializations."
>
> —IRENE KINOSHITA, CEO, ASCOLTA

"The new Cisco security certifications give professionals the recognition they need to validate their experience in the industry. More importantly, though, Cisco provides options. If you want to validate your skills in one specific area of security, for example, in firewalling or intrusion detection, you can do that thanks to these specializations. But if you are responsible for security across your network, the new CCSP certification validates that you have the right skill set to do just that. The security market is really going to benefit from this," says Irene Kinoshita, chief executive officer (CEO) of Ascolta, a Cisco Learning Solutions Partner.

New Security Courses

The Cisco Networking Academy™ Program is offering two new courses: Fundamentals of Network Security and Fundamentals of Wireless LANs. The courses will be available in mid-2003.

For more information about the new Cisco Certified Security Professional certification, visit cisco.com/go/training or cisco.com/go/securitytrng. ▲▲

Psionic Acquisition Enhances Cisco's IDS Portfolio

CISCO WILL ACQUIRE PSIONIC Software, Inc., of Austin, Texas, a developer of network security software that increases the efficiency of intrusion detection systems (IDS) by reducing false alarms by up to 95 percent. This software will allow Cisco security customers to increase productivity and lower the costs associated with network-based intrusion detection systems (NIDS) by enabling them to focus manpower and attention on legitimate attacks against their networks.

Cisco delivered the security industry's first commercial network IDS in 1995, and the Psionic acquisition underscores Cisco's commitment to continued innovation and leadership in the IDS market. Psionic's intrusion response technology surpasses the alarm consolidation and correlation products on the market today by using patented adaptive scanning techniques to rapidly validate IDS events, escalate legitimate attacks, and remediate costly intrusions. With Psionic's unique technology, only those qualified attacks that have the highest damage potential against vulnerable systems are terminated, ensuring maximum network protection.

The addition of Psionic Software enhances Cisco's existing network security portfolio of virtual private network (VPN) gateways and concentrators, firewalls, IDS, and security management applications.

Psionic's eight employees will join Cisco's VPN and Security Services (VSEC) Business Unit. ▲▲

New Online Registration for Cisco Products

FURTHER STREAMLINING customer processes, Cisco has begun to offer online product registration to its customers. As a convenient alternative to filling out the mail-in registration cards that are included in product shipments, customers can visit cisco.com/go/cpo and register their Cisco products quickly and easily by filling out the Cisco Product Ownership Registration Card. Online registrants can also request a free introductory issue of *Packet*® when filling out the card. ▲▲

Tech Tips & Training

Conquering the CCIE Lab

A Veteran's Advice on Preparing for the Rigors of the CCIE

BY SCOTT MORRIS

THE CCIE® CERTIFICATION from Cisco is one of the most respected certifications in the networking industry. At the time this article was written, there were an estimated 9600 CCIEs (only about 8700 active CCIEs) from countries across the globe.

Every day many more people are working diligently to achieve this certification and take the test in some of the nine CCIE labs around the world. And everyone who works toward this goal likely asks the same question: How do I conquer the CCIE lab?

First and foremost, the answer is study, study, study. Second, nothing replaces hands-on experience with Cisco equipment. Anyone can study networking theory and recite how the Open Shortest Path First (OSPF) Protocol works, but not everyone can put the theory into practice. Worse, if something goes wrong, even fewer people can debug their way through a problem.

Currently, there are three CCIE program tracks: Routing and Switching, Communications and Services, and Security, of which the most popular and common track is Routing and Switching. The one-day, eight-hour exam tests a wide variety of topics. For a look at those topics, visit cisco.com/warp/public/625/ccie/certifications/routing.html.

SCOTT MORRIS, CCIE® No. 4713, Certified Cisco Systems Instructor (CCSI), has been involved in internetworking and integration for more than 15 years. He is currently a triple CCIE in Routing & Switching, ISP/Dial, and Security. As an instructor with Network Learning, Inc., Morris works with a variety of technologies including IP telephony, security, and cable modems. He also teaches the CCIE Routing & Switching Lab preparatory course for CCBootCamp and has authored labs for the course. He can be reached at swm@emanon.com.

Where Do I Start?

You should start preparing for the CCIE lab well before you schedule your lab exam and continue up until you save your last-minute configurations. You *do* remember to save your configurations, don't you?

The CCIE lab requires mastery of the Cisco IOS® Software that comes only from extensive access to routers and switches, so owning a home lab gives you the best access. With a home lab you can maximize your study time and work at your own pace. Renting rack time, particularly for more expensive technologies such as ATM and voice, is an economical method of studying.

What Do I Study?

The short answer is *everything*. Good study habits are essential. Repeat procedures as often as possible, altering scenarios as you go.

When going through various books or the documentation CD, take copious notes. After completing a book or technology section, transpose your notes into a computer document. The seemingly repetitive task of editing and interpreting your handwritten notes keeps details fresh in your mind.

After you have compiled configuration guides for almost all technologies, start working on action scenarios. Whether you devise your own scenarios, mimic real-life networks, or purchase lab scenarios, you can use your study notes. When you transition from the book notes to the scenario configurations, use your notes and further edit them. Keep editing this document as you delve into new books or areas of Cisco.com.

Attend a CCIE lab prep course and purchase CCIE lab scenarios. While these cost money, they can be invaluable to introduce other perspectives on the pertinent technologies. When you attend a prep course, you typically get additional scenarios, books, and notes. Best of all, you work with your peers and have access to an instructor.

Take the lab prep course only after you are familiar with basic and advanced technologies. A lab prep gives you a chance to hone your new skills. You will get the most value out of the course if you use it to "fill in the blanks." Network Learning offers a five-day, intensive bootcamp (www.ccbootcamp.com) that covers many issues and lab scenarios that expose students to problem areas in the CCIE lab. The lab prep course is a 12+ hour-a-day experience, including a full-day lab simulation.

When choosing a prep course, there are several important considerations: the technologies available (ATM, voice, Cisco Catalyst® 3550, for example), the instructor's experience level, and equipment availability. With the CCBootCamp Lab Prep course, every student has their own pod of equipment for the week-long class, plus remote Telnet access to the equipment for nine days following the class. All pods have ATM, voice, and Cisco Catalyst 3550 switches. In the CCIE Security Lab Prep course, Cisco PIX® firewalls are available on every pod as well.

After many hours of studying, transposing, editing, and configuring various scenarios, you may be ready to attempt the CCIE lab. However, tackling the exam also requires mental preparation. Some people perform better at tests than others, and the psychological aspects of the exam are not to be taken lightly.

Continued on page 9

CCIE Lab, Continued from page 7

Checklist for Success

1. When you get your lab guide, avoid the impulse to jump in and start configuring the routers. You are not in a race with anyone but yourself. Read through the exam more than once.
2. Because you have been studying and diligently updating your study notes document with fresh ideas, you should be able to spot issues and potential pitfalls in the lab exam. Use colored pens to diagram the network, connections, network addresses, routing protocols, and anything else of note.
3. Make a checklist of the various exam sections and how many points they are worth. Check off sections as you fully (and correctly) complete them. There is no partial credit within a particular exam section, so if you miss the instruction to name your switch "Bob" instead of "Switch," you have lost points. The small things can kill you.
4. As you configure the lab, assume that, at some point, something won't work right, or something new will come up that you don't remember. Whatever the issue, work logically and try to "think" like a router does. Although Cisco IOS Software is very powerful, routers themselves are not very bright. Often just "putting yourself in the router's shoes" will give you the necessary perspective to fix a problem.
5. Do not spend unnecessary time trying to fix something. If you spend more than 20 to 30 minutes on a problem, it is time to move on. Sometimes changing focus lets you see problems in a much clearer light. Stand up and stretch or get a drink; the only prohibition is making calls to the Cisco Technical Assistance Center (TAC) from the CCIE lab.

Tackling the Exam

The CCIE lab exam occupies a grueling eight hours, and depending on where you take the exam, you may start as early as 7:30 a.m. You come in to the exam with other candidates like yourself—typically quiet, sullen, and trying to remember everything that was in the document that they so carefully edited and added to over the months.

To help you manage stress and use time efficiently, try keeping a running tally of how many points you should have earned at various places within the test. Then if you are running out of time, you can add up how many points you should have and determine how best to earn the remaining points you need. Use this strategy when you encounter problems on an isolated portion of the lab, such as the data-link switching (DLSw) section. If you aren't good at DLSw and you can complete other topics without difficulty, work on those topics. Determine where points are best earned.

What About the Things I Don't Know?

Issues always come up that you may not have anticipated. When I took the lab for the first time in 1999, I was convinced that I was going to pass. My study techniques were great, my own lab scenarios were thorough, and I had practiced just about everything I could imagine, so I thought I was unstoppable.

Needless to say, I ran across something I hadn't thought of. It messed up my entire exam strategy and derailed my confidence, which caused me to fail. Upon returning to work battered and irritated, one of my friends greeted me. "Welcome to the human race," he said. Nobody can know everything there is to know.

If you do not pass the test the first time, try working with just the documentation CD. Get to know the layout of the files, the structure of the technology pages, and where each topic is within the configuration guides. Learn how to navigate without using the search engine. Being a CCIE is not just about what you already know—it's also about your ability to work through the unknown, adapt, and overcome unplanned obstacles.

A Final Word

You can conquer the CCIE lab with motivation, dedication, persistence, and focus.

With good study habits, thorough technology review, and an astute test-taking approach, you can successfully survive the CCIE lab and look forward to the e-mail that comes within a day or two and says, "Congratulations on passing the CCIE lab. Your CCIE number is: _____."

As you are recovering from taking the CCIE lab and becoming reacquainted with your family and friends, keep in mind that the learning is never over. The more you know, the more you realize you don't know.

Best of luck to everyone! ▲▲

FURTHER READING

- Cisco technical documentation: cisco.com/univercd/home/home.htm
- Cisco Career Certification resources: cisco.com/en/US/learning/le3/le11/learning_certification_resources_home.html
- Cisco certification program updates: cisco.com/en/US/learning/le3/learning_recent_article09186a00800d7f66.html

Reade

Packet® would like to thank all of the readers who continue to send in technical tips for this very popular column. While every effort has been made to verify the following technical tips submitted by our readers, *Packet* magazine and Cisco Systems cannot guarantee the accuracy or completeness of these tips, or be held responsible for their use. When trying out these or other tips, it would be wise to remember the best tip of all: Back up your configurations!

Administration

TIP If you need to recover the password on a Cisco LocalDirector, the Cisco TAC Web site has an excellent guide (Cisco.com login required): cisco.com/warp/customer/474/pswdrec_localdir.shtml

Note that if you use an MS-DOS emulator (NT, Windows 2000, etc.), you will get the following error message when attempting to rawrite the *unlock3000.bin* file:

```
unlock3000.bin: No such file or
directory
```

When you use the **directory** command, it is clear that the *unlock3000.bin* file is available:

```
26/09/2002 07:53 92,160 unlock3001.bin
```

Your "get out of jail free" card for this is the excellent program RawWrite for Windows, by John Newbigin, which can be found at uranus.it.swin.edu.au/~jn/linux/. This will enable you to rawrite on a Windows machine.

— Doug Legge, Berkeley Homes PLC, Cobham, United Kingdom

TIP A good tip when upgrading RAM memory in Cisco 2600 Series routers: If the router does not recognize the extra memory you just inserted, try inserting the least capacity memory card in slot 0 and then the other one in slot 1. It usually works.

— Eduardo Kenji Matsuoka, Citibank, Sao Paolo, Brazil

TIP The Cisco IOS Software image residing in the router's Flash memory does not usually use all the available space. This extra space can be used to store almost any type of data. For example, you may want to have a backup copy of your configuration while testing another configuration. The following command lets you save your running config to your Flash memory:

```
copy running-config flash:Conf120102
```

Confirm this using the **dir** command. This saved configuration can always become running-config by reversing the filenames in the above command. Do not erase the Flash while running the **copy** command.

— Syed R. Ahmad, WorldCom ETC Inc.

MPLS VPN

TIP When deploying a virtual private network (VPN) service in a Multiprotocol Label Switching (MPLS) network, it is more secure to use an unnumbered loopback address instead of an ordinary address to connect a provider edge (PE) router interface to a VPN customer edge (CE) router. This way, the PE router cannot Telnet or ping its VRF interface or VPN CE router. Also, the CPN CE router cannot ping or Telnet the PE router.

— Mohammad Reza, ITRC, Tehran, Iran

Router Configuration

TIP If you are running Open Shortest Path First (OSPF) with static routes and you use the **distribute-list** command to control the advertisement of these routes, always use the **clear ip ospf redist** command if you make a change to the distribute list. If you do not, the routing tables will not reflect the change. We run Cisco IOS Software Release 12.0(7)XK2 on our Cisco 2600 routers and the IP OSPF priority does not appear to have any effect when the DR fails or recovers. So if this situation occurs, we use the **clear ip ospf proc** command on the current DR rather than reloading it.

— Kevan Lee, Schumbergersema, Enfield, England

TIP If you experience problems with ISDN setup and connection, it may be due to the telephone company's legacy switches, which send a bearer capability of 56K. This results in a mismatch on the receiving end because the Cisco IOS Software defaults to and expects 64K bearer capability.

In our case, the ISDN backup was able to establish itself if we administratively brought down either end of the serial interfaces. However, if we were to physically pull the T1 or ping the receiving BRI, it would generally fail, and the receiving-end bri interface would essentially flap.

After running a **debug isdn** q931, just before physically pulling the T1, the output showed a bearer capability mismatch with the error *"ISDN not end-to-end. May have inband info".*

By specifying the speed of the calling end on the receiving BRI interface,we overcame this issue:

```
dialer map ip 10.1.1.2 name New
Chester speed 56 0155512120
```

We also could have used **isdn not-end-to-end** command on the receiving interface.

— A.G. Teslicko, Amscan, Inc., Chester, New York

Switch Configuration

TIP Configuring individual interfaces with the same parameters on a Cisco Catalyst switch can be tiresome and time consuming. However, you can use the interface range configuration mode to simultaneously configure multiple interfaces with the same-configuration parameters. When you enter the interface range configuration mode, all command parameters you enter are attributed to all interfaces within that range until you exit interface range configuration mode. Beginning in privileged EXEC mode,

follow these steps to configure a range of interfaces with the same parameters:

configure terminal to enter global configuration mode.

interface range port-range

Enter interface configuration mode and enter the range of interfaces (virtual LANs or physical ports) to be configured. Each comma-separated port range must consist of the same port type. You do not need to enter spaces before or after the comma. When you define a range, the space between the first port and the hyphen is required. You can use the normal configuration commands to apply the configuration parameters to all interfaces in the range.

end to return to privileged EXEC mode.

copy running-config startup-config (Optional) to save your entries in the configuration file.

Sample configuration:

```
Switch#configure terminal

Switch(config)#interface range
fa0/1 -48

Switch(config-interface-range)
#description test

Switch(config-interface-range)#exit

Switch(config)#exit

Switch#copy run start

Switch#show run
```

— Venkatesan Natarajan, Network Solutions, Ltd., Maduri Maldives

Trouble-Shooting

TIP When using debug commands that increase CPU load, disable console logging using the Cisco IOS global configuration command **no logging console** and enable buffered logging with the IOS global configuration command **logging buffered**. Then execute the command from a virtual

Tech Tips

Find out about changes to the Cisco TAC Web site. The TAC Web site has been redesigned to provide simpler navigation and faster access to Cisco online technical support resources. Check the Hardware , Software , and Technology support modules for all the technical content on the site.
cisco.com/public/news_training/whats_hot.shtml

Check out best practices for the Cisco Catalyst® switches. This document discusses how to implement Catalyst 4000, 5000, and 6000 Series switches in your network and covers configurations and commands for the Catalyst Operating System (CatOS) General Deployment software version 5.5(7) or later. Includes some design considerations.
cisco.com/en/US/products/hw/switches/ps663/products_tech_note09186a00800947l3.shtml

Maximize security on the Cisco PIX® Firewall. Find out how packets are passed from and to higher security interfaces from lower security interfaces using the **nat, global, static,** and **conduit** commands or the **access-list** and **access-group** commands in PIX software versions 5.0 and later. This document explains the differences between these commands and how to configure port redirection in PIX software version 6.0 and the outside Network Address Translation (NAT) feature added in PIX software version 6.2.
cisco.com/warp/public/707/28.html#intro

Analyze and troubleshoot router crashes. This document provides practical information, examples, and customized analysis of system devices with tips on how to handle crashes.
cisco.com/warp/public/122/crashes_router_troubleshooting.shtml

Troubleshoot the Spanning-Tree Protocol. This document provides recommendations for implementing a safe network as it pertains to bridging. It covers reasons that can cause the Spanning-Tree Protocol to fail, as well as what information to look for to identify the source of a problem and what kind of design minimizes spanning-tree risks.
cisco.com/warp/public/473/16.html

Upgrade software for the Cisco PIX Firewall. This document provides instructions for upgrading your PIX software on the following hardware: PIX Classic, 10000, 501, 506, 515, 520, 525, and 535. It covers PIX software versions 4.4, 5.0, 5.1, 5.2, 5.3, 6.0, 6.1, and 6.2.
cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a00800094a5d.shtml

Use the debug command to troubleshoot IPSec configuration issues. This document explains common debug commands for troubleshooting IP Security (IPSec) issues on both the Cisco IOS® Software and the Cisco PIX Firewall after an attempt to configure IPSec.
cisco.com/en/US/tech/tk648/tk367/technologies_tech_note09186a00800949c5.shtml#intro

Configure VLAN Trunk Protocol. This document provides background and configuration information on VLAN Trunk Protocol (VTP), a proprietary Cisco protocol that is available on most of the Cisco Catalyst Family products.that can help you reduce administration in a switched network.
cisco.com/warp/public/473/21.html

For more Tech Tips from the Cisco Technical Assistance Center (TAC) Web site, visit cisco.com/public/support/tac/.

terminal session and view the output in that session. If the session is unresponsive, you can use the console to disable the debug because the console has higher priority than the virtual terminal session. Review the debug output in the log buffer using the IOS EXEC command **show log**. If syslogging is enabled, you can also view the output in the log file on the syslog server.

— *Jude M. Velasquez, CPKelco Philippines Inc., Cebu City, Philippines*

TIP Using a UNIX or Lynx machine and need to send a show tech or log to the Cisco TAC? Try using the **tee** command after the **pipe** (|) command. This creates a file that records all key strokes and output. An example is Telnet ***Router-name*** **| hold**. When you're ready, just attach the file named "hold" to the e-mail instead of doing a copy and paste. Because passwords are not echoed back to the screen, they do not appear in the file. This also works well when you are trying to find something specific in large ARP tables or routing tables.

— *Carlo Calabrese, State of Oregon, Salem, Oregon*

TIP An effective way to detect "suspicious" ports in a large campus switched network is with the **show diag link-flap** command, which is available on Cisco IOS Software-based switches.

— *Milan Kulik, Aliatel, a.s. Praha, Czech Republic*

Tunneling

TIP Whenever a Generic Routing Encapsulation (GRE) tunnel is formed, the tunnel interface shows status UP in **show interface tunnel<no>,** but actually the tunnel is not active. You need to manually do a "no shutdown" in the tunnel interface. One can also view the tunnel status in **show interface summary** or **show ip interface brief**.

—*Amarnath Gutta, Data Access (I) Ltd., Mumbai, India*

Submit a Tip

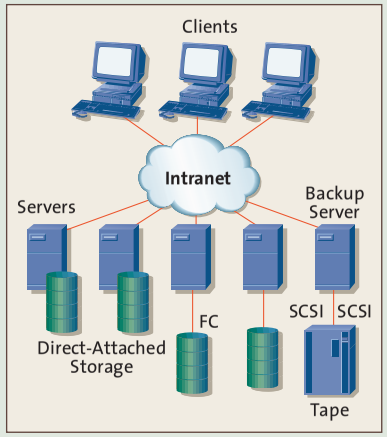
Help your fellow IT professionals *and* show off to your peers by submitting your most ingenious technical tip to packet-editors@cisco.com. Who knows, you may see your name in the next issue of *Packet*.

Storage Networking

At a Glance

Why Should I Care About Storage Networking?

Most companies use online storage to house business-related information. As more information from business functions such as sales, inventory, payroll, engineering, marketing, and human resources is stored online, the efficient acceptance, management, and retrieval of this information becomes more critical to the success of the business.



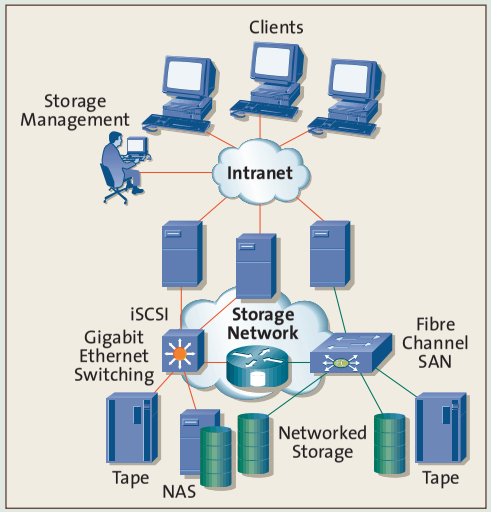
What Are the Problems to Be Solved?
For many years, information was stored in server-centric architectures. As businesses grew and had greater storage needs, additional servers were added when and where they were needed.

However, this direct-attached storage (DAS) approach is limited in its ability to scale as it is expensive to manage and uses resources inefficiently. Servers are added where needed (in each department, for example), and each is associated with a specific CPU. Additionally, standard activities such as backing up data and adding capacity are difficult and inefficient.

What Is Storage Networking?

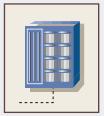
To overcome the drawbacks of server-centric storage, a network-centric model called "storage networking" has been developed. Storage networking is the software and hardware that enable storage to be consolidated, shared, accessed, replicated, and managed over a shared network infrastructure.

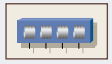
To understand how storage networking works you must understand the different storage methods and technologies.



Traditional Server-Centric Storage Methods

Redundant Array of Inexpensive Disks (RAID) is a fault-tolerant grouping of two or more disks that a server views as a single disk volume. It is a self-contained, manageable unit of storage.



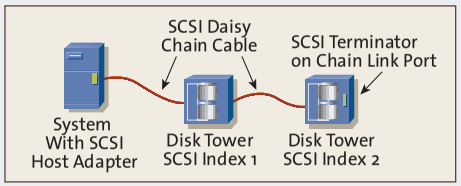


Just a Bunch of Disks (JBOD) is a simple, efficient method for raw storage. Each drive is independently attached to an I/O channel.

This method has limited scalability because it requires separate servers to manage multiple volumes of disks. Drives share common power supplies and physical chassis.

Storage Networking Technologies

Small Computer Systems Interface (SCSI)
SCSI is a parallel bus interface port used to connect peripheral devices such as RAID, tape devices, and servers. SCSI is a low-cost method of directly connecting devices but is limited with regard to scalability and distance.



Fibre Channel

A Fibre Channel is both a physical connection and a Layer 2 protocol used by storage-area networks (SANs). Fibre Channel is the most common method of transporting SCSI commands and data between servers.

Fibre Channel capabilities have kept up well with companies' ever increasing need for bandwidth. Using Fibre Channel, application servers can access data on a SAN without impacting the company IP network.

Internet Small Computer Systems Interface (iSCSI)

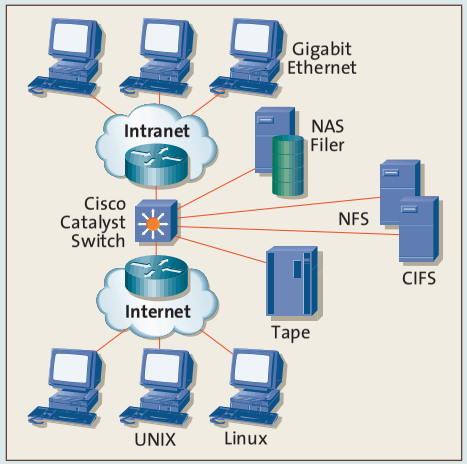
iSCSI is a method of encapsulating SCSI data and command frames into IP packets enabling universal access to storage devices and SANs over standard TCP/IP networks.

Cisco Systems

PACKET

Storage Retrieval Methods

The two main methods for retrieving stored data are block retrieval and file retrieval. A block refers to the largest amount of data that can be accessed in a single operation. Blocks are the most elemental units of storage. SANs access blocks directly.

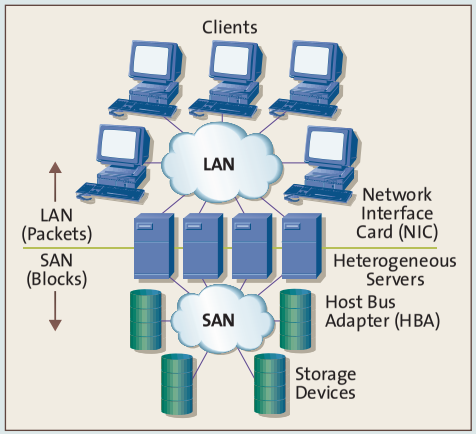


A file is comprised of several blocks. In network-attached storage (NAS) systems, the server organizes blocks into files.

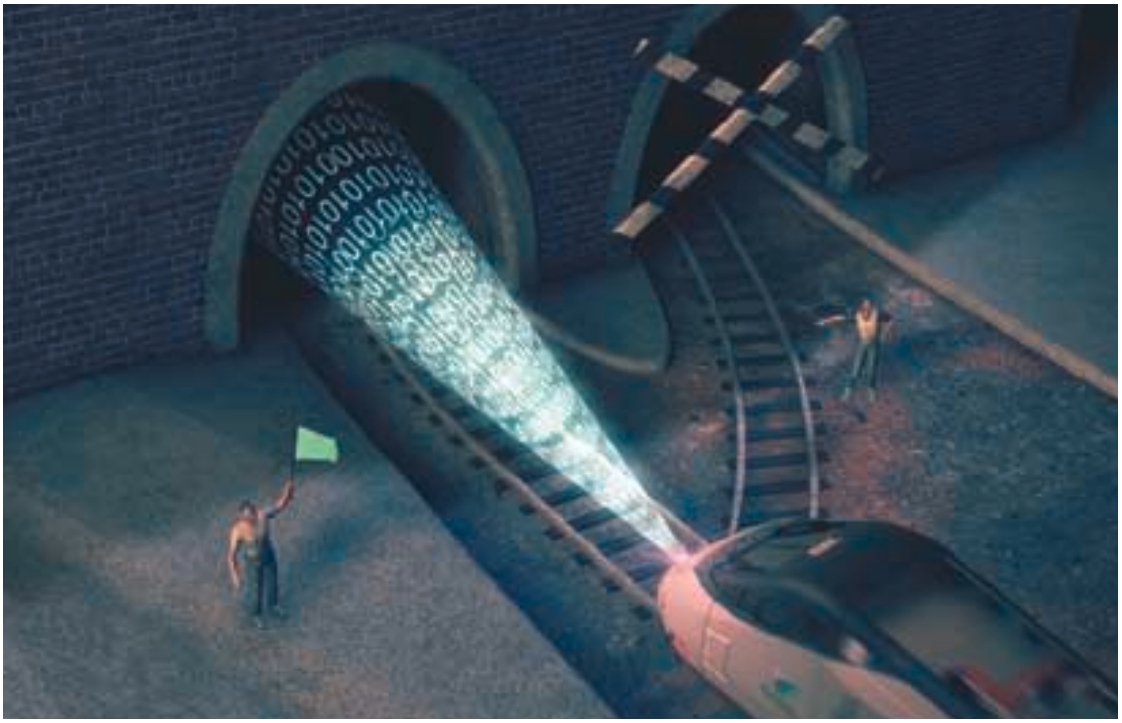
Storage Networks

NAS: NAS uses specialized file servers to connect storage devices to a network. NAS is well suited for collecting, storing, retrieving, and sharing data over IP networks. NAS also supports multiple operating systems and file system and protocols. NAS is optimized for file-based access to shared storage over an IP network.

SAN: A SAN is an independent network designed specifically for connecting storage devices. SANs are optimized for the efficient collection, storage, and retrieval of raw block data. Most SANs use Fibre Channel interconnections and require a media converter to connect to an IP network.



Technology



RANDY LYHUS

Protecting SLAs During MPLS Outages

How to Ensure Equivalent Bandwidth Availability for Primary and Backup Tunnels **BY SANTIAGO ALVAREZ**

At a minimum, a high-availability network service platform requires redundant routers, a mesh of dual-homed circuits, and routing protocols that redirect traffic around failed network elements. This setup maintains Layer 2 and Layer 3 network connectivity during a router or circuit outage, in that existing network sessions will remain live and new ones will not be blocked.

However, to fully preserve quality-of-service (QoS) guarantees for low-latency traffic, such as voice, traffic rerouting must happen quickly enough so as not to degrade application performance. In addition, the same amount of bandwidth that was allotted to traffic on its primary path must be available on a backup path. Otherwise, traffic failing over to an alternate route could encounter congestion while the secondary path tem-

porarily carries an extra load. Delay and packet loss are likely to increase during periods of congestion, and this could lead to service-level agreement (SLA) violations.

Automatic Protection Switching (APS) is the most prominent method today for making sure that the required amount of backup bandwidth is available to network traffic. APS is implemented at the physical layer in SONET/SDH networks, and it protects networks against failed circuits using SONET/SDH's dual, counter-rotating ring configuration. When a traffic flow hits a failed circuit, such as a fiber cut, it loops back in the opposite direction, segmenting off the failed link. When it changes direction, traffic fails over to a fully redundant backup circuit. SONET/SDH APS restoration times are fast, on the order of 50 milliseconds.

There is also a newer approach to protecting SLAs in networks that run Multiprotocol Label Switching (MPLS). This approach, called *bandwidth protection*, combines the MPLS Fast Re-Route (FRR) functionality in Cisco IOS® Software with an offline client/server application called Cisco Tunnel Builder Pro. When implemented in an MPLS traffic engineering (TE) network, these features offer two main advantages over APS: the ability to quickly reroute around failed nodes in addition to failed circuits, and a greater degree of scalability with lower associated capital and circuit expenses.

COMPARATIVE ATTRIBUTES OF FAULT-RECOVERY TECHNOLOGIES

	Cisco Fast Reroute with Bandwidth Protection (Tunnel Builder Pro)	Cisco Fast Reroute Without Bandwidth Protection	SONET/SDH Automatic Protection Switching
Ability to Recover in Milliseconds	Yes	Yes	Yes
Protection Against Failed Links	Yes	Yes	Yes
Protection Against Failed Nodes	Yes	Yes	No
Efficient Use of Bandwidth	Yes	Yes	No
Bandwidth Guarantees	Yes	No	Yes (Against Link Failures Only)

FIGURE 1: MPLS TE networks using bandwidth protection and backup tunnel calculation can fully protect SLAs.

SAMPLE RESULTS: TUNNEL BUILDER PRO VERSUS CSPF*

Algorithm	Protected	Proved Impossible	No Solution Found
CSPF	54	12	86
Tunnel Builder Pro	134	17	1

*Single network backbone with 152 router-protection scenarios

FIGURE 2: Testing of Tunnel Builder Pro and CSPF and algorithms for finding backup MPLS routes resulted in a far higher success rate for Tunnel Builder Pro.

Comparison of Bandwidth Protection Approaches

The enhanced scalability and cost savings of implementing MPLS bandwidth protection result from configuring the MPLS TE network to use *many-to-one,* or *N:1,* protection and sharing backup bandwidth. In this configuration, *N* represents some number of primary MPLS *Label Switch Paths (LSPs),* or tunnels, and *1* represents a single backup MPLS tunnel. The backup is configured with an amount of bandwidth equal to the aggregate capacity of the primary bandwidth. The sharing of backup bandwidth is viable because multiple simultaneous failures are rare. One backup pool of bandwidth can protect several independent element failures. In other words, backup bandwidth can be reused.

The shared backup bandwidth pool concept contrasts with APS, which is a *1:1* protection scheme and requires full redundancy of all components. For example, APS divides the available bandwidth in a SONET/SDH ring in half; 50 percent is dedicated to live traffic, and the other half is "on call" for use during an outage. This approach is very reliable, but not as cost effective or resource-efficient as one that enables backup bandwidth sharing, because the standby capacity is not used most of the time. Also, APS requires external multiplexers or additional line cards and router ports to support the standby circuits, which constitute added capital expenses.

Computing Backup Tunnels

Cisco developed MPLS Tunnel Builder Pro with PARC Technologies to create a tool that provides bandwidth protection by computing the optimal placement and size of backup tunnels. The backup tunnel-generation algorithm in Cisco MPLS Tunnel Builder Pro collects input about the MPLS TE network topology from a *seed router*—any router in the MPLS TE network. It uses this information to compute the amount of bandwidth to be protected and the amount of bandwidth to be used for protection on each link. The computation takes into account how backup bandwidth can be shared among backup tunnels using common links.

There are three key advantages to this approach. First, the network can be protected before any primary tunnels have been created. Backup tunnels are computed to protect a maximum amount of aggregate bandwidth. So, any tunnels created within the protected bandwidth pool are

automatically bandwidth-protected. This is an important advantage, especially in dynamic environments where primary tunnels are created and torn down frequently.

Second, the sharing of backup bandwidth makes it possible to achieve a greater level of protection in the network with lower bandwidth requirements, resulting in significant cost savings. Third, the placement of backup tunnels takes into account the bandwidth requirements of other backup tunnels activated by the same failure, so the level of protection is optimized.

An alternative algorithm to compute backup tunnel placement is Constraint-Based Shortest Path First (CSPF), which is used to compute the primary tunnels in MPLS networks. CSPF is an adequate algorithm for computing primary tunnels, but provides suboptimal results for computing backup tunnels requiring bandwidth protection. CSPF cannot take into account the bandwidth requirements of other tunnels activated on neighboring nodes during a single failure, yielding a lower amount of protection for the network (Figure 2).

After backup tunnels have been computed and proposed by Cisco MPLS Tunnel Builder Pro, the network operator can use the tool to visualize the possible tunnels and have them configured automatically on the different network nodes. It is not always possible to protect all elements on the network due to network topology characteristics and bandwidth definitions. When protection is not possible, the network operator has the option of introducing changes to the network topology, modifying the bandwidth pool definitions, or using MPLS TE attributes to force primary tunnels requiring protection to avoid those elements.

Primary tunnels that will use protection are signaled explicitly during setup. The level of protection that the primary tunnel will experience depends on the actual backup tunnels configured on its path. The amount of protection is a design consideration that depends on the traffic requiring bandwidth protection, the probability of failure on nodes or links, and cost.

Cisco IOS Software Release 12.0(22)S and a Cisco MPLS Tunnel Builder Pro server and application are required to implement bandwidth protection. Without the use of Cisco MPLS Tunnel Builder Pro, it is possible to provide connectivity protection relying exclusively on the MPLS FRR capabilities in Cisco IOS; however, the implementation of bandwidth protection enabling enhanced SLAs is not possible with FRR alone. Cisco MPLS Tunnel Builder Pro solves the *NP Complete* challenge of computing backup tunnels for bandwidth protection. For example, without this algorithm, computing a full backup solution for a 16-router network would require up to 663,000 years, assuming that 2 seconds are needed to compute a backup tunnel solution for each node failure.

SANTIAGO ALVAREZ is a technical marketing engineer in the Internet Technologies Division at Cisco. He can be reached at saalvare@cisco.com.

MPLS FAST REROUTE WITH BANDWIDTH PROTECTION

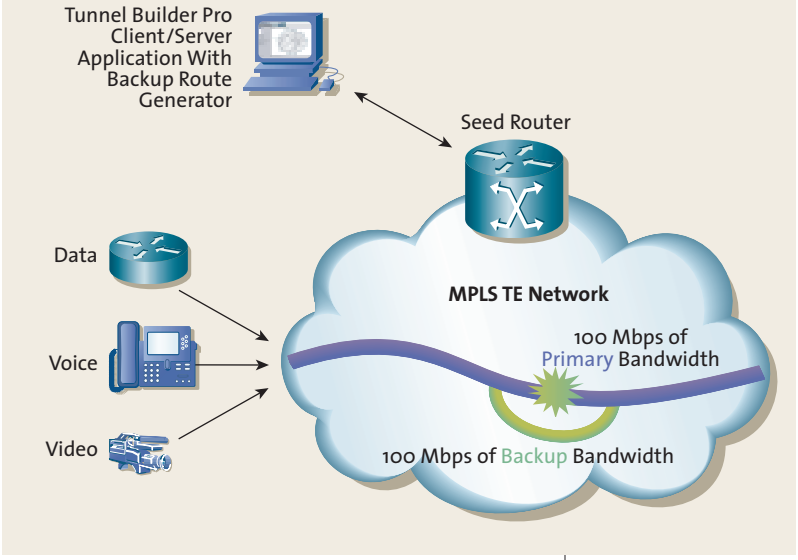


FIGURE 3: To fully protect QoS during rerouting, Tunnel Builder Pro ensures that backup bandwidth is as plentiful as primary bandwidth. It learns the network topology, computes the amount of available backup bandwidth, and generates properly sized alternate route options for each MPLS TE tunnel.

In summary, Cisco MPLS Tunnel Builder Pro:

- Configures and manages MPLS TE nodes, links, and tunnels
- Determines what parts of a network are not protected by backup tunnels and creates detailed reports
- Provides the ability to define bandwidth protection levels by specifying over- or under-booking levels in the event of failures
- Recommends backup tunnels with sufficient bandwidth

When combined with Cisco FRR in an MPLS TE network, these capabilities enable network operators to build highly available network service-delivery platforms that not only maintain session connectivity during the failure of a network circuit or node, but also protect QoS by ensuring that the necessary amount of backup bandwidth is available to rerouted primary traffic. ▲▲

FURTHER READING

- **Tunnel Builder Pro Release Notes:** cisco.com/en/US/products/sw/netmgtsw/ps4731/prod_release_note09186a00800f683e.html
- **MPLS TE FRR with RSVP Hellos Support:** cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00800a869a.html

IPv6 Time Is Now

A Primer on How IPv6 Addresses Are Constructed and the Benefits of this Next-Generation Technology

BY RAJ GULANI

The current Internet address protocol has a potential of about 4 billion public 32-bit addresses. Shortages, so far caused primarily by allocation, have already forced many Internet users to make do with Network Address Translation (NAT) or private addresses piggybacking on public ones. What's more, the number of 32-bit addresses, governed by IP Version 4 (IPv4), is already shortchanging some areas of the world, particularly the Far East. It will be wholly inadequate after devices needing Internet connectivity are placed in mobile phones, personal digital assistants (PDAs), vehicles, appliances, and an as-yet unimaginable list of other devices.

The solution to the shortage of addresses that has been adopted by IP standards bodies around the world is a new address format of 128 bits, part of a protocol known as Internet Protocol Version 6 (IPv6). The 128-bit length was chosen because it creates an optimum number of addresses in a header of workable size. And it will expand the number of public addresses to 340,232,366,920,938,463,374,607,431,768,211,456, or 3.4×10^{38}.

Work has been underway for a decade, and IPv6 addressing and IPv6 networks are now realities. A number of academic and government networks already carry IPv6 traffic shifting from the experimental IPv6 backbone (also known as 6Bone networks) to production dual-purpose IPv4 and IPv6 networks now under construction. Cisco has been involved in IPv6 development since its inception. In addition to being a founding member of the IPv6 Forum and co-chair of the Internet Engineering Task Force (IETF) IPv6 and Transition (NGTrans) Working Group for several years, Cisco runs a well-known 6Bone router that helps up to 70 other companies make their first IPv6 steps, and acts as an IPv6 to IPv4 relay for individual users or small companies. And its implementation of the protocol on Cisco IOS® platforms was one of the industry's first official IPv6 support in a broad product portfolio.

The same registries that now allocate IPv4 addresses—the Asia Pacific Network Information Center (APNIC) for Asia, the American Registry for Internet Numbers (ARIN) for the Americas, and the Reseaux IP Europeens-Network Coordination Center (RIPE-NCC) for Europe and the Middle East—will allocate IPv6 addresses to Internet service providers (ISPs) and National Research Networks (NRN), who will continue to assign them to end users.

This article explores the five major areas of change brought about by IPv6:

- Enhanced address space
- Header format simplification
- Enhanced routing protocol support
- Security and mandated IP Security (IPSec) support
- Enhanced support for Mobile IP

Enhanced Address Space

The 128 bits in the IPv6 address space are broken down into eight groups of 16 bits, each of which can be represented in text as a hexadecimal value. The text address then reads x:x:x:x:x:x:x:x, where each "x" represents a given hexadecimal value. Typical addresses would be written as 2031:0000:130F:0000:0000:09C0:876A:130B.

Because of the methods used for allocating addresses, IPv6 may contain long strings of zeros. It is acceptable to substitute a pair of colons "::" anywhere in the address to represent and thus compress two or more 16-bit groups of zeros in a string. The above address would then be written: 2031:0000:130F::09C0:876A:130B. As a computer expands the "::" with 0 to get 128 bits, an address may not contain more than one set of paired colons, as it won't be possible to determine how many zeros in each segment.

RAJ GULANI

RAJ GULANI, CCIE®, is a manager of technology marketing at Cisco. He has presented at Networkers and various other technical forums. With a Bachelor's Degree in Engineering (Electronics) from Bombay University, India, Gulani's networking career spans more than eight years. In 1997, he started his career at Cisco in Customer Advocacy as a Technical Assistance Center (TAC) engineer focusing on WAN and broadband technologies, and moved on to lead network design engineer in the Advanced Network Services Group. He can be reached at rgulani@cisco.com.

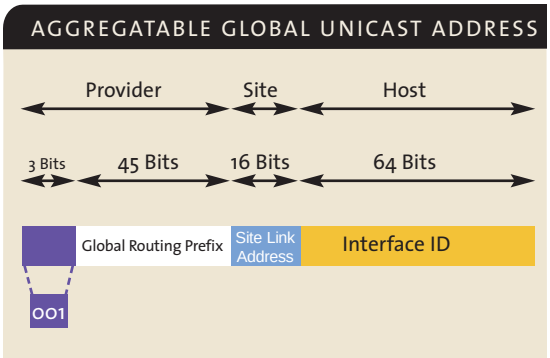
ROB BRODMAN

An alternative form (nearly deprecated) for the address is x:x:x:x:x:x:d:d:d:d, in which the "x's" are hexadecimal values of the six higher-order 16-bit pieces and the "d's" represent the decimal values of the four lower-order 8-bit pieces. The latter portion is the standard IPv4 address, and this form would be used when configuring automatic IPv6 tunnels through an IPv4 network. This particular format has shown some operational challenges, so its use is discouraged.

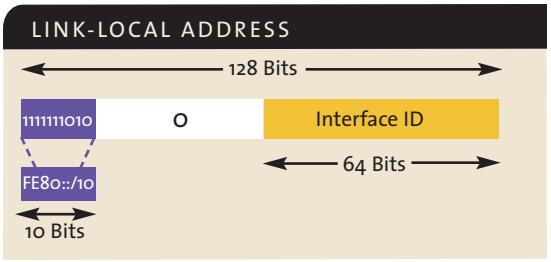
An IPv6 address typically has two major 64-bit parts: the *network prefix*, which contains the registry, provider, subscriber ID, and subnet, and occupies the higher order groups of bits; and the *interface ID*, which occupies the lower ones. Bits within these groupings are allocated according to the specific requirements of various types of addresses. An IPv6 address prefix is represented as ipv6-address/prefix-length, similar to IPv4 address prefixes written in IPv4 Classless Interdomain Routing (CIDR).

There are three major types of addresses: *unicast*, *anycast*, and *multicast*. Addresses are assigned to interfaces. A unicast address governs one-to-one transmission. It identifies a single interface and is the equivalent of an IPv4 unicast address. A transmission is delivered only to that address. There are, however, several types of unicast addresses, including the global, link-local, and site-local.

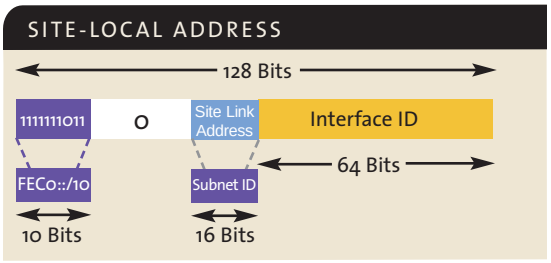
The *global unicast address* is the equivalent of the IPv4 global unicast address, used on links that are aggregated upwards though an organization and eventually to the ISP. The structure of this type of address enables policies that allow aggregation of routing prefixes so as to limit the number of entries in the global routing table. The address consists of a 48-bit routing prefix managed by the provider and a 16-bit subnet ID managed by the local site.



A *link-local unicast address* is used to communicate among nodes on a local link, in the neighbor discovery protocol, and in the stateless autoconfiguration process. It can be automatically configured on any interface by using the link-local prefix FE80::/10(1111 1110 10) and the interface identifier in the IEEE EUI-64 format (an EUI-64 may be derived from an EUI-48).

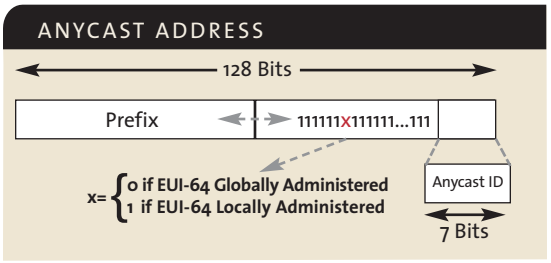


A *site-local unicast address* is similar to a private address in IPv4 format (for example, 172.16.0.0/12). Because the prefix is not propagated between routing domains, this restricts communication to a specific domain.



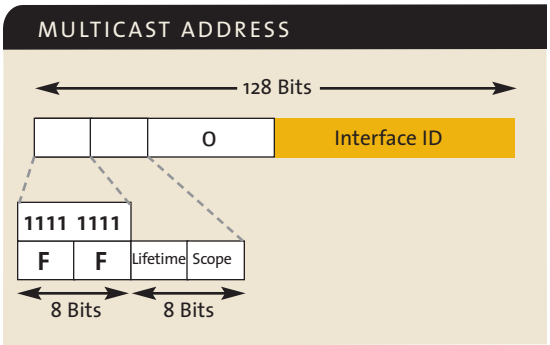
The unicast address 0:0:0:0:0:0:0:1 or ::1 is the loopback address, which should never be assigned to any interface. It performs the same function as in IPv4—identifying a transmission sent by a node back to itself.

An *anycast address* directs one-to-any transmission. Examples are the use of anycast addresses to reach a DNS server or a 6to4 Relay or Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) routers (see next page for more on 6to4 and ISATAP).



An IPv4-mapped IPv6 address is used to identify an IPv4-only node to an IPv6 node. The 16 bits of zeros before the IPv4 decimal representation in the address should be replaced with four F's. An IPv4-mapped address should never be used as an "Src" or "Dst" on the wire.

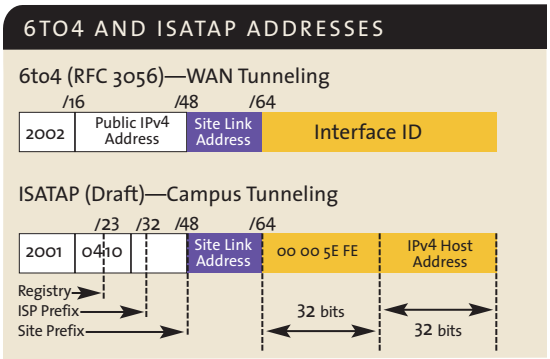
A *multicast address* governs one-to-many transmission. The address subsumes a set of interfaces, usually



belonging to different nodes, and orders delivery of the packet to all of them. IPv6 does not include any broadcast addresses, their function being taken over by the multicast address.

6to4 and ISATAP Addresses

To ease the IPv6 integration on the campus and WAN, the IETF NGTrans Working Group has been working on several tunneling mechanisms that can be set when native IPv6 or dual-stack are not a solution. Automatic IPv6 over IPv4 tunnels require that an IPv4 address be extracted from the IPv6 address to establish a tunnel on request. This approach leads to a particular IPv6 unicast address called *6to4* (RFC 3056) on the WAN and *ISATAP* (draft-ietf-ngtrans-isatap) on campus.



Simplified Header Format

An IPv4 header contains at least 12 different fields: version, header length, type of service, total length, identification, flags, fragment offset, time to live, protocol, header checksum, source address, destination address, and possible options. The simpler IPv6 header has only eight: version, traffic class, flow label, payload length, next header, hop limit, source address, and destination address. They are used as follows:

- The field specifies 6 for IPv6.
- The traffic class identifies differentiated services.
- The flow label tags packets with a specific flow that differentiates packets at the network layer.
- The payload length indicates the length of the data portion of the packet.
- The "next header" field determines the type of information following this packet—perhaps a TCP or UDP packet or extension header.
- The hop limit specifies the maximum number of routers the packet can pass through before being considered invalid.
- The "source address" and "destination address" contain the appropriate IPv6 128-bit addresses.

Neighbor discovery provisions are built on top of Internet Control Message Protocol for IPv6 (ICMPv6) and are a combination of IPv4 protocols. They enable router discovery, parameters discovery, address autoconfiguration, next-hop determination, neighbor unreachability detection, and other functions, as well as determine the link-layer address of a neighbor on the same link, and identification and tracking of neighboring routers.

Stateless autoconfiguration (see Figure 1) is a key feature of IPv6.

Enhanced Routing Protocol Support

IPv6 headers have been designed to be as compatible as possible with current standards and protocols. For example:

- They use the same "longest-prefix match" routing as IPv4 CIDR.
- The changes to existing IPv4 routing protocols for

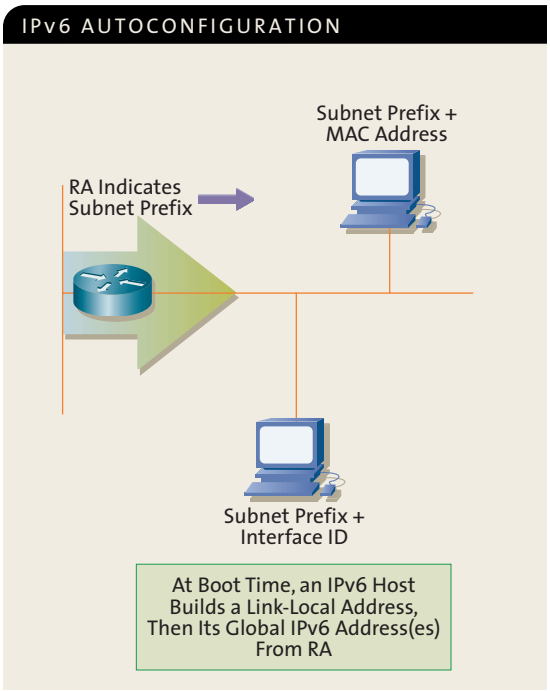


FIGURE 1: With IPv6 stateless autoconfiguration, the host autonomously configures its own link-local address. Booting nodes request router addresses (RAs) to help in configuring the interfaces.

handling longer addresses are done through new IETF documents.

- Use of Routing Information Protocol (RIP) is achieved with RIPng similar to RIPv2 on IPv4.
- A new version of Open Shortest Path First (OSPF)—OSPFv3—is defined for IPv6.
- IPv6 address family in now in Intermediate System to Intermediate System (IS-IS) and Multiprotocol Border Gateway Protocol v4 (MP-BGP4).
- Headers with anycast destination addresses can be used to route packets through particular regions for provider selection and performance, compliance with policies, among other reasons.

Mandated IPSec, Enhanced Support for Mobile IP

Compliance with the IPSec standard is mandatory in IPv6, not optional as in IPv4, and is part of the IPv6 protocol suite. Network administrators could enable IPSec in every node, if desired, potentially making networks more secure, but IPv6 does not specify how the key can be distributed. IPv6 provides security header extensions that make it easy to implement encryption, authentication, and virtual private networks (VPNs). The security extensions help to prevent hacking and ensure data integrity. Nevertheless, when a centralized security mechanism (for example, firewalls) is preferred, there is no definition—yet—on how to make both IPSec and firewalls coexist on the network.

IPv6 also offers other features that facilitate mobility. Mobility is essentially built in, and any node can support it as needed, in contrast to IPv4, in which mobility must be specifically provided for.

IPv6 packets addressed to the home address of a mobile node are transparently and automatically routed to its care-of address because both addresses are bound and cached together. On Mobile IPv4, a correspondent node can't talk directly with a mobile node; it has to go through the home agent. But a mobile node can talk directly with a correspondent node. This is called triangular routing. On Mobile IPv6 (see Figure 2), a correspondent node can talk directly with a mobile node after a binding update process.

◆ ◆ ◆

Growth in mobile and fixed applications that require Internet-connected devices is just one factor putting a strain on the current IPv4 32-bit address pool. The time for IPv6 has come, and IT professionals need to begin familiarizing themselves now with IPv6 addresses and their benefits. ▲▲

ENHANCED SUPPORT FOR MOBILITY WITH IPv6

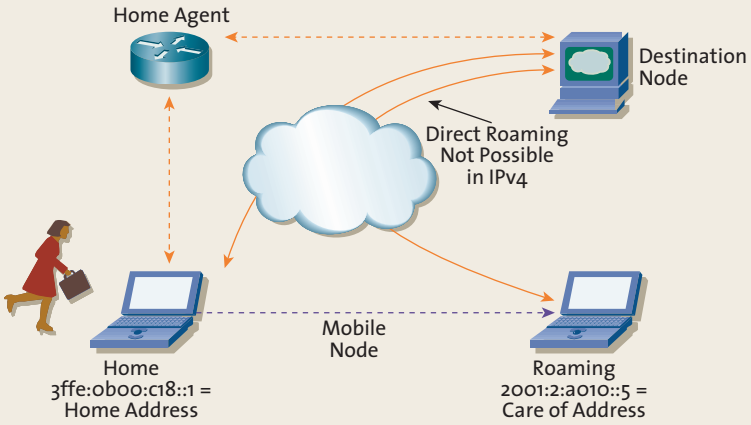


FIGURE 2: With IPv6, use of the routing header for Mobile IP enables the service to avoid "triangle routing," making the service much more efficient than in IPv4.

The IPv4 to IPv6 Transition

A number of techniques have been identified and developed to make the transition from IPv4 to IPv6. They fall into three categories:

- *Dual-stack techniques,* which allow both protocols to coexist in the same devices and networks
- *Tunneling techniques,* to avoid order dependencies when upgrading hosts, routers, or regions
- *Translation techniques,* to allow IPv6-only devices to communicate with IPv4-only devices

These three techniques, which probably will be used in various combinations, also lay the foundation for IPv6 deployment scenarios. To view a dual-stack IPv4/IPv6 campus and ISP deployment scenario, go to cisco.com/go/packet/dual-stack at *Packet Online*.

FURTHER READING

- **Cisco IPv6:** cisco.com/ipv6
- **IPv6 Forum:** ipv6forum.org
- **IPv6 Information Page:** ipv6.org
- **IETF IPv6 Working Group:** ietf.org/html.charters/ipv6-charter.html

A GOOD DEFENSE

Today's open, complex networks require an integrated approach to security.

THE COMMUNICATIONS NETWORKS OF 2003 ARE MORE EXTENSIVE, complex, and open than most of us would have imagined a decade ago. As such, implementing security safeguards just at the traditional network perimeter—the Internet edge—is no longer a sufficient strategy. Security must be embedded throughout the network.

Most network operators today realize that outsiders do not represent the only security threat to an organization. Also, there are now more points of entry into corporate networks to tempt unauthorized users. For example, wireless access points have created an additional network edge, which, if not secured, can be penetrated by anyone chancing by with a wireless network interface card (NIC). In addition, teleworkers and traveling users are using the public Internet for ubiquitous and cost-effective remote-access connections. So security strategies must account for the fact that most remote-access traffic now traverses an untrusted, open network to and from the corporate data center.

Finally, security attacks can affect network uptime. With the increasing reliance on the IP network for voice calls, including emergency service dialing such as wireless Enhanced 911 (E911) in the US, defending the network against any denial of network service is mission-critical.

"Not only can all network devices be a potential target of attack, they can also be a source of attack," points out Stephen Collen, director of security at Cisco. "Organizations must create an intelligent, self-defending network that can identify attacks as they occur, send alerts as appropriate, and then automatically respond, without user intervention."

To this end, network operators evaluate where to *embed* security technologies to safeguard their networks. A comprehensive set of security solutions from Cisco defines and enforces user access privileges through policy-setting and identity management; filters and scans packets for malicious code; protects network traffic from interception and tampering; secures network devices and servers; and safeguards management traffic.

After organizations have decided where to embed these security capabilities, they must choose whether that secured network segment should take advantage of *integrated security* deployed within a network connectivity device (such as a router or switch) or in a purpose-built security appliance (such as a firewall).

Corporate networks provide user access to certain resources to enhance productivity and provide a competitive advantage. Simply closing off access to these resources as a security approach, then, largely defeats their purpose. To maximize network returns, organizations delicately balance the benefits of user access with their risk of exposure and the financial impact of a potential breach. This approach first requires conducting a security posture assessment (a profile of the users, devices, and security currently within the network) and creating a security policy that grants levels of access. After these steps are done, it is time to pinpoint the network devices that require protection. For example, laptops of users who telework or travel would likely be target devices for IP virtual private network (VPN) encryption software, personal firewalls, and antivirus software. And corporate wireless LAN (WLAN) access points and client devices should be enabled with secure, intelligent security services that support enterprise-class authentication and encryption features.

Similarly, remote branch offices will embed firewalls and intrusion detection capabilities between their LAN and Internet access connections. Intrusion detection and firewalls should also be placed in the data center to protect core switches and hosts. These capabilities can be implemented in a variety of different devices and form factors. This is where "integrated security" choices enter the picture.

Integrated security bundles multiple security services into a single device. As traffic passes through the device, it is scanned, analyzed, and compared against an organization's security policy. Based on the policy, the device will decide to forward, partition, encrypt, or reject each packet.

These security services can be integrated into network connectivity devices—routers and switches—in the form of Cisco IOS® Software or as high-performance security modules, or blades. Alternatively, they can reside in specialized security appliances, such as PIX® firewalls, which can perform a single security function or combine several.

Let's take a look at strategies for embedding network security.

Securing wireless access points. Wireless access points distributed throughout the organization are a point of network entry. This is one reason that Cisco Aironet® Series access points—IEEE

FRED GAMBINO

802.11a and 802.11b WLAN radio infrastructure devices—feature the Cisco Wireless Security Suite now available in IOS Software. Enterprises can extend Cisco's standard security features, including virtual LANs (VLANs), to these intelligent access points.

"Segregating wireless users onto VLANs with limited, associated access rights is an important component to managing user access," says Ron Seide, Cisco wireless LAN product line manager. This is particularly the case as companies begin offering wireless Internet access to guests with wireless-enabled laptops, Seide notes.

In addition, Cisco offers the Cisco Wireless Security Suite, an IEEE 802.1X-based enterprise-class security solution that supports a choice of Extensible Authentication Protocol (EAP) authentication types and a prestandard version of Temporal Key Integrity Protocol (TKIP). EAP helps guard against wireless-initiated denial-of-service attacks by providing support for mutual authentication of the user and the RADIUS server. "This support prevents unauthorized users from accessing the network and unauthorized users from unknowingly associating with rogue access points," explains Cisco Product Manager Pejman Roshan.

TKIP, currently in development at the IEEE, adds additional encryption features to 802.11 security with per-packet keying, broadcast key rotation, and message integrity checks. Together, these capabilities make sessions nearly impossible to hack. The Cisco Wireless Security Suite is covered in greater detail on page 34, "Securing Wireless."

LAN-based privacy. VLANs can also partition user group traffic on the wired LAN using IEEE 802.1Q technology in Cisco IOS Software. Sometimes additional privacy is also required. For example, top management will likely want to prevent employees from seeing certain sensitive communication—such as the details of an imminent merger or acquisition.

In such cases, organizations can encrypt LAN sessions using IP Security (IPSec) technology, suggests Kevin Flynn, senior manager of security marketing at Cisco. "Because IPSec encrypts both the data payload and the header, internal employees cannot see the data or who is engaged in a session," Flynn explains.

Security Stats

The network is increasingly both a *target* and a *source* of attack. Consider the following:

- A recent study by Riptech, a real-time information protection company, says network security breaches rose 28 percent during the first half of 2002, compared to the last half of 2001.
- A 2002 US Federal Bureau of Investigation (FBI) report reveals that 85 percent of businesses have detected computer security breaches within the last 12 months.
- In a 2001 survey, the FBI found that 91 percent of respondents reported insider network abuse.

"Hardening" the data center. The data center, of course, is a primary area for reinforced security. *Intrusion protection* of both networks and hosts is important in this portion of the network for shielding core switches and enterprise hosts, including intranet/Internet Web server, from malicious attacks.

A network intrusion detection system (IDS), such as the Cisco 4200 IDS Series, monitors traffic flows for known malicious *signatures.* After one is detected, the IDS protects against an attack by automatically telling the next-hop router to block connections from that source. Host-based IDS software, such as the Cisco IDS Host Sensor, guards against users gaining access to ports on the host that they are not supposed to have.

Hosts and switches should also be protected on the front end with *stateful firewall* appliances. These firewalls inspect and compare each packet's attributes against a defined security policy, then treat them accordingly. The Cisco PIX Firewall combines these functions with IDS and VPN capabilities. To further enhance security services, Cisco CSS 11500 Series content services switches and Catalyst content switching modules can be used to provide high availability and increased scalability through intelligent load balancing of traffic across security devices in the data center.

Secure WAN connectivity. Protecting the integrity of connections from remote locations is another fundamental consideration. Depending on the size and situation of the remote user, managers can implement different solutions.

Larger regional sites might connect by services that inherently offer a strong degree of privacy because they are confined to a single service provider's network and to specific routes through the network. These could include Multiprotocol Label Switching (MPLS) VPN, Frame Relay, and leased-line services. Encryption may or may not be necessary on top of these services. Branch offices of any size also can be securely connected over the Internet via IPSec VPN technology. The encrypted connectivity can occur on Cisco routers or Catalyst® 6500 Series switches. PIX firewalls can also provide encryption for site-to-site VPN implementations.

IPSec VPNs allow organizations to protect their networks, offer new services such as voice, and reduce costs. For example, using Dynamic Multipoint VPN (DMVPN)—new in Cisco IOS Software Release 12.3(13)T—reduces configuration complexities, reduces latency, and improves scalability for large and small IPSec VPNs. For more on DMVPN and other recently announced Cisco IOS Software features, see "Background Checks," page 27.

Traveling users, teleworkers, and small-office sites can connect to the data center via an IPSec VPN connection over the public Internet—where encryption is a must. IPSec capabilities can be implemented in IP VPN client software or access routers

with hardware encryption for small-office and branch-office applications.

At the headend, the Cisco VPN 3000 Series Concentrator and 7000 Series Router can terminate several different types of remote tunnels, including IPSec sessions. It supports high-performance encryption/decryption in hardware, and authenticates and authorizes remote users.

Multiple Safeguards and Form Factors

No technology can single-handedly enforce an organization's security policies, says Russell Rice, manager of technical marketing for security technology at Cisco. Rice advises using a combination of identity-based access control firewalling, IPSec-based VPN, VLAN, and IDS technologies. In other words, developing what Cisco's Collen calls a "defense in depth" strategy, with multiple overlapping layers of countermeasures.

These capabilities can be deployed in form factors that are appropriate for the network segment, required performance and functionality level, and budget at hand. With the option to deploy integrated or specialized security capabilities, organizations gain flexibility, from a cost and floor-space standpoint, to better penetrate their environments with security technology.

"Integrating security technologies into routers and switches facilitates internal security, because it enables organizations to leverage existing infrastructure components," observes Mark Bouchard, senior program director of global network strategies at the META Group, a networking research firm.

Integrated switch and router blades. Several security modules are now available for Cisco switches and routers. For example, a blade supporting *Secure Sockets Layer (SSL),* the de facto encryption/decryption security standard for browser-based e-commerce transactions, is available for Cisco Catalyst 6500 Series data center switches, as well as Cisco's dedicated CSS 11500 Series content services switches.

The Cisco Firewall Services Module also provides the full performance of a standalone Cisco PIX Firewall in a blade for the Catalyst 6500—an industry first for embedding stateful firewall filtering into a switch, says Rice.

On the router side, the Cisco 7600 Series Router supports the same SSL and firewall blades. Built on Cisco IOS Software, Cisco routers accommodate multicast and multiprotocol traffic, as well as routing across VPNs, to deliver flexible solutions for the most diverse VPN environments. The Cisco 831, 837, 1700, 2600, 3600, 3700, and 7000 series all offer hardware acceleration options that provide up to 10 times the performance over software-only solutions by offloading encryption processing from the router CPU. These router-based solutions provide industry-standard encryption (IPSec), application-aware quality of service (QoS), and robust perimeter security options. In addition, with Cisco IOS Software Release 12.2(13)T, Cisco supports the Advanced Encryption Standard (AES) with IPSec in addition to Data Encryption Standard (DES) and Triple DES (3DES).

Software integration. Using the breadth of networking and security features in IOS Software, the branch-office router has evolved from basic multiprotocol routing to a device now used to deliver advanced services and applications. "As customers deploy end-user applications in the branch office, the router becomes a point of integration for network applications such as security, data, and voice," says Adrian Amelse, director for engineering access router security at Cisco. "Our goal is to offer a flexible, modular solution where customers can turn on selected security services that make the most sense given their application in the network. Cisco routers and switches provide industry-leading investment protection by enabling customers to take advantage of new capabilities via hundreds of field-upgradable modules and/or Cisco IOS Software updates."

Such investment protection can come from products Cisco customers already have, notes Amelse, such as Cisco 1700, 2600, 3600, 3700, and 7000 series routers and Catalyst switches.

Security appliances. These purpose-built systems incorporate one or more security functions. Good examples include the Cisco PIX firewall, which supports an integrated VPN (encryption) module, as well as VPN and intrusion protection software, the Cisco 4200 Series of intrusion protection systems, and the Cisco SCA 11000 Series of appliance-based SSL optimizers, which deliver the same benefits of Cisco's switch-integrated SSL blades.

The Cisco PIX firewall product family spans the entire security appliance spectrum, from desktop firewalls for teleworkers and small offices to carrier-class, gigabit-speed firewalls for large enterprise and service provider environments. Cisco PIX firewalls support up to 500,000 simultaneous connections and deliver nearly 1.7 Gbits/s aggregate throughput, says Collen.

"An exciting new class of appliance," adds Collen, "is the Cisco Catalyst 6503 and 6506. These security solutions are prepopulated with either VPN or firewall modules. They offer high performance, are aggressively priced, and have upgrade potential—for additional security modules or network connectivity options."

Which form factor an organization chooses depends on priorities for cost, performance, and real estate (floor space). For example, if a Catalyst switch has free slots sitting idle, this could boost the return on an organization's investment to deploy security blades and make full use of the switch. However, if the Catalyst switch slots are filled, it could prove more economical to install a specialized security appliance or to run the capabilities in Cisco IOS Software.

Identity-based networking. Guarding against unauthorized access to the network and its servers requires users to first be identified based on parameters such as username, IP address, and MAC address. Cisco IOS Software supports 16 levels of user and administrator privileges for granular policy enforcement.

For identity-based networking, the Cisco Secure Access Control Server (ACS) offers

Continued on page 81

FURTHER READING

- **Cisco IOS security and other IOS technologies: cisco.com/warp/public/732/Tech/**
- **Cisco routers: cisco.com/en/US/products/hw/routers**

Integrated Security, Continued from page 25

centralized authentication, authorization, and accounting (AAA) from a Web-based, graphical interface, and distributes those controls across the network. The ACS can interact with a server-based user directory using the Lightweight Directory Access Protocol (LDAP) to carry out the policy definition function. Network-wide, switches, routers, and other network devices enforce those policies.

A user connecting to the network via a Cisco switch or wireless access point might use the IEEE 802.1X protocol. Each user device connected to a switch port or access point is authenticated to an AAA server, such as ACS, before gaining access to any services. Following authentication, a VLAN assignment is sent back to the device via the Remote Access Dial-In User Service (RADIUS) protocol with specific associated access privileges, to the switch or access point for the user. The access profile follows the user anywhere around the corporate IP network. The ACS provides mapping of user to VLAN, while the switch or access point acts as a security policy enforcement point.

Securing the management framework. The management infrastructure itself is a potential point of sabotage that must be secured. For enterprises, the CiscoWorks VPN/Security Management Solution (VMS)—a CiscoWorks management module—can securely configure thousands of local and remote devices, such as routers, PIX firewalls, and intrusion protection systems.

The Auto Update Server (AUS) within CiscoWorks VMS devices allows local, remote, and dynamically addressed devices to periodically pull down the most current security configurations or updates to the Cisco PIX operating system. This function eliminates the need for manual updates of each remote device.

For service providers, the IP Solution Center (ISC), formerly called the VPN Solution Center, is a UNIX-based multidevice manager. "ISC uses Secure Shell, a remote-access router configuration method, to encrypt all traffic, including passwords, between a remote console and a network router," explains Mike Loukola, IOS IPSec product manager at Cisco. The Cisco Hosting Solution Engine is a turnkey, hardware-based solution for e-business operations in Cisco *Powered* Network data centers.

◆ ◆ ◆

It's clear that the open nature of network environments has increased the need for comprehensive security spanning the data center, LAN, and WAN. Fortunately, a rich, multilayer set of security capabilities is available to protect the new, multifaceted communications network in strategic, embedded locations. From there, organizations can deploy security in the integrated form factor that makes sense in each particular network segment. ▲▲

Special ROI Report, Continued from page 45

Good security can enhance operations—making it feasible, for example, to move critical functions onto an IP network or to move data from discrete silos to a consolidated database, thus making applications more widely available.

Platon lists five specific areas where investments may be attractive: secure connections; extending perimeter or firewall control; security monitoring (protection from intrusions); identification, authentication, and authorization; and management of security services.

Secure connections are most easily obtained and extended to all workers through the use of an enterprise virtual private network (VPN), Platon says, particularly an IP VPN. With Layer 3 provisions such as IP Security (IPSec), the firewall goes where the worker goes. This business case can be quantified: the cost of the VPN versus the cost of the leased facilities it replaces. Of course, adds Platon, any enterprise that's ever had a major security breach—and most have—needs no persuasion. Without security, there's no business.

◆ ◆ ◆

The ideas in this special report should help you get started on evaluating projects and building successful business cases. However, Kisch says, "Every company's evolution will be unique depending on the technology it has, its business needs and strategic goals, and the size of its budget." The project you develop must fit your organization and no other. ▲▲

Cisco IOS Software is hard at work behind the scenes providing multilayer network protection.

BACKGROUND CHECKS

FOR A LONG TIME, CISCO IOS® SOFTWARE HAS QUIETLY BEEN SECURING THE perimeter of corporate and service provider networks with access control, inline firewall filtering, and intrusion detection. Over the years, Cisco IOS security features have grown in sophistication as privacy threats have moved inward from the Internet edge to corporate data centers, wireless access points, and user desktops.

Cisco IOS Software takes an integrated approach to network security on many levels. First, it combines the capabilities of multiple specialized security appliances—such as IP Security (IPSec) virtual private network (VPN), inline firewalls, and intrusion protection systems—into a single device, which also conveniently serves as a high-performance router or switch for forwarding packets.

"Integrating multiple security and network service features into one device eases management complexity and lowers the total cost of ownership," says Mark Denny, manager of IP services and security at Cisco.

The total-cost-of-ownership (TCO) benefit comes from reducing the capital equipment and associated configuration and management required to perform multiple network functions, and the savings in annual support and software updates (included with Cisco SMARTnet™). After organizations choose where to strategically embed security in their networks, they can implement the technologies right in the connectivity devices in those network segments simply by configuring them in software, Denny explains.

In addition to routers and switches, Cisco Aironet® 1100 Series wireless LAN access points—the radio-based, Layer 2 hubs that provide wireless user access to the corporate network—now also support Cisco IOS Software and many IOS features. Because they are a point of entry into the corporate network, wireless access points feature the award-winning Cisco Wireless Security Suite on all Cisco Aironet products (see "Securing Wireless," page 34). These products also feature virtual LAN (VLAN) support to segregate over-the-air communication, mutual authentication for access control, quality of service (QoS) for end-to-end traffic prioritization, and other capabilities.

Security integration within Cisco routers and switches doesn't stop with all-in-one bundling. "Cisco IOS security consistently cuts across the network control, data, and management planes in Cisco platforms and integrates with other IP services such as QoS, voice over IP, Multicast, and routing protocols," says Anand Nuggihalli, marketing programs manager in the Internet Technologies Division at Cisco.

Greater Than Sum of the Parts

The advantage in deploying a Cisco IOS Software-based security implementation is that Cisco can integrate security and VPN with the rich set of IP and network services within IOS, to offer a variety of security and secured solutions that are easier and less costly to manage.

For example, IPSec with Generic Routing Encapsulation (GRE) enables secured routing and multicast deployments; Dynamic Host Control Protocol (DHCP) together with Address Resolution Protocol (ARP) makes it more difficult for hackers to hijack a live session. To view a table of "Recently Added

FRED GAMBINO

Cisco IOS Security Features," visit *Packet Online* at cisco.com/go/packet/iossecurity.

Three of the recently announced Cisco IOS features—Dynamic Multipoint VPN (DMVPN), Low-Latency Queuing (LLQ) with IPSec, and IPSec Stateful Failover—all combine to reduce latency and jitter across VPN networks. Additionally, resilience improves, and most of the deployment is automated, reducing the burden on operations staff.

Dynamic Multipoint VPN. New in Cisco IOS Software Release 12.3(13)T, the DMVPN feature allows users to better scale large and small IPSec VPNs by combining GRE tunnels, IPSec encryption, and Next Hop Resolution Protocol (NHRP). DMVPN makes deployment of meshed VPNs easier by automating provisioning of connections between spoke sites and dynamically setting up connections based on network traffic patterns.

DMVPN is excellent for reducing latency and jitter for spoke-to-spoke calls, as it offloads these communications from the hub site. Using multipoint GRE, this new IOS feature also supports multicast voice and video traffic.

QoS preclassification and LLQ with IPSec. Running real-time voice (and video) over an encrypted link can be tricky. This is because, by definition, encryption disguises the data packets and addresses, including QoS markings. To overcome this challenge, two Cisco software capabilities—QoS preclassification and LLQ—work with IPSec to make sure voice gets top priority across an encrypted session.

Packet preclassification takes place first to prevent Differentiated Services Code Point (DSCP) and IP Precedence priority markings from being concealed. QoS markings are applied at the outbound interface in the transmitting router before encryption. The markings are then copied to the new outside IPSec tunnel header before transmission.

The preclassification feature first became available in Cisco IOS Software Release 12.1(5)T and is now available on most Cisco IOS VPN routers running Cisco IOS Software Release 12.2(8)T. Alone, it generally provides sufficient IPSec QoS for VoIP. However, to cover all bases, IPSec has also recently become LLQ-aware. The Cisco LLQ is a priority queue, or "fast lane," within Cisco routers that is dedicated to voice traffic.

"LLQ-aware IPSec avoids voice delays caused by congestion where encryption/decryption takes place," explains Mika Loukola, IOS IPSec product manager at Cisco. "Without IPSec's ability to recognize high-priority [real-time] traffic, congestion within one of the IPSec routers could prevent high-priority packets from receiving preferential treatment across internal router queues."

IPSec Stateful Failover. This feature provides fast, scalable network resilience for VPN sessions between two IPSec endpoints. It ensures that VPN sessions continue without disruption during a connectivity loss to the primary central site VPN router.

IPSec Stateful Failover uses Hot Standby Router Protocol (HSRP) to maintain state information for IPSec sessions between active and backup routers. Maintaining state of IPSec sessions enables subsecond failover times and session failover, and is transparent to remote VPN routers.

Control Plane Security

The control plane in a router or switch is the process responsible for signaling, storing, and updating routing information, and setting up forwarding paths. Cisco IOS Software contains several features for securing these functions. For example, routing protocols, such as Border Gateway Protocol (BGP) and Intermediate System-to-Intermediate System (IS-IS), are protected with the Message Digest Algorithm 5 (MD5) to verify that any information received from a peer was indeed originated by that peer.

Other control-plane security relates to the secure setup and configuration of VPNs. For example, IPSec leverages the Internet Key Exchange (IKE) to securely create encrypted tunnels. IKE, in Cisco IOS Software Release 11.3(3)T and higher, eliminates the need to manually specify all the IPSec security parameters in peer routers. It also allows encryption keys to change during IPSec sessions and performs dynamic authentication of peers.

Data Plane Security

To protect the privacy of data, Cisco IOS Software integrates packet filtering according to corporate security policies, monitoring of traffic flows for malicious code, and traffic segregation using tunneling.

Inline firewall filtering. The integrated Cisco IOS Firewall Feature Set inspects many components of each IP packet and tracks each connection on all the firewall interfaces to make sure they are valid. It can examine the contents of the packet up through the application layer, then take action on the packet according to firewall rules associated with that application.

For example, by inspecting a TCP/IP packet and determining whether a TCP handshake is being conducted in the proper sequence, the firewall could ward off an attack whereby someone deliberately sends startup handshakes to simulate thousands of users attempting to launch a TCP session. Such an attack would cause TCP control blocks to crash.

Intrusion protection. This feature protects against network attacks from malevolent sources by looking for known malicious *signatures*—a set of byte codes in a packet. Once detected, the software automatically tells the next-hop router to reject further connections from that source.

Cisco software recognizes 101 signatures, 42 of which were recently added in Cisco IOS Software Release 12.2(13)YJ. Intrusion protection comes bundled with the Cisco IOS firewall and is available in Cisco IOS Software Release 12.0(5)T and higher.

Tunneling. Cisco IOS Software supports a variety of tunneling capabilities for use across the public Internet. GRE encapsulates a wide variety of protocol packet types inside IP tunnels to create a virtual point-to-point link between remote Cisco routers. GRE and a related capability, Layer 2 Tunneling Protocol (L2TP), do not provide encryption, though L2TP does require user authentication. Instead, these schemes create a cut-through tunnel

across the public Internet, with no forwarding decisions having to be made at router hops. GRE and L2TP sites avoid Network Address Translation (NAT), so they get a packet-processing boost at the network edge.

For routers, GRE is generally used with IPSec so that multicast routing protocols can go through the IPSec tunnel. A recent addition to IPSec and IKE is the new Advanced Encryption Standard (AES) encryption cipher, which comes in three flavors: AES-128, AES-192, and AES-256. With Software Release 12.2(13)T, Cisco IOS supports AES in addition to Data Encryption Standard (DES) and Triple DES (3DES) ciphers. IPSec is highly recommended for traffic sent over the public Internet.

To maximize investments in WAN edge routers and access circuits, it is possible to use *split tunneling*. In this configuration, IPSec tunnel forwards only the VPN traffic securely over a common access link from a branch office, and clear-text Internet traffic is forwarded directly to the Internet.

Split tunneling avoids the extra hops and latency incurred in branch offices when traffic flows through a central site. However, advises Loukola, when deploying split tunneling, it is very important to use firewalling and intrusion detection at the edge. "Otherwise, intruders from the Internet might be able to penetrate the branch site and, via the branch, get to the headquarters location," he points out.

Where traffic segregation is required on the LAN, *IEEE 802.1Q VLANs*—tunnels that run at Ethernet's Layer 2—can be created using Cisco IOS Software. This capability runs in Cisco routers, switches, and wireless LAN access points. IPSec can also run in tandem with VLANs to encrypt traffic over Ethernet LANs to protect highly confidential communications within the company.

A Cisco enhancement to IEEE 802.1Q, called *802.1Q tunneling*, is available to service providers that want to offer high-speed Layer 2 LAN extension services in metro and wide-area networks. "Cisco 802.1Q Tunneling adds an extra 802.1Q tag to customer traffic in the switch at the edge of the service provider's network," explains Chiara Regale, technical marketing engineer in the Metro Ethernet Group at Cisco. "This tag segregates all customers' VLANs by giving each a unique VLAN ID number in the service provider network."

Did You Know?

Stateful inline firewall and intrusion protection capabilities built into Cisco IOS Software require simply that you activate them to protect your organization. These IOS features perform the following:

- Stateful application-based filtering
- Per-user policy to define access control
- Dynamic per-user authentication and authorization
- Inspection of a wide range of supported applications and protocols
- Block malicious Java applet attacks, Internet Control Message Protocol packets, SIP, H.323v2, N2H2 and Websense URL filtering, etc.
- Authenticate peer routers to ensure they receive reliable routing information from trusted sources
- Recognize 101 intrusion detection signatures and provide interception and response
- Severity: 40 info signatures, 61 attack signatures
- Complexity: 74 atomic signatures, 27 compound signatures
- Send real-time alerts of denial-of-service (DoS) attacks or other predefined conditions, configurable on a per-application, per-feature basis

Management Plane Security

A multifaceted set of capabilities falls into this software security category, including identity and authentication management. For example, authentication, authorization, and accounting (AAA) schemes such as Remote Access Dial-In User Service (RADIUS) and TACACs+ are supported, and Cisco IOS Software supports 16 levels of user privileges for granular access control. Networks can configure which commands are available within the 16 privilege levels, authenticate access on a user-by-user basis, and authorize even on a command-by-command basis, says Denny.

From a management perspective, Secure Shell (SSH), a remote-access router configuration method introduced in Cisco IOS Software Release 12.0(5)S, encrypts all traffic, including passwords, between a remote console and a network router across a Telnet session. Because SSH sends no traffic in the clear, network administrators can conduct remote access sessions that casual observers will not be able to view. CiscoWorks VPN/Security Management Solution (VMS), for example, uses SSH to securely configure VPN tunnels on many routers, even across public networks. ▲▲

FURTHER READING

- **Configuring IPSec security:** cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7b1.html
- **Cisco IOS security:** cisco.com/warp/public/732/Tech/security

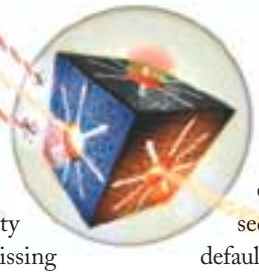
Security Considerations at the Data Link Layer

LAYER 2

The Weakest Link

WHAT'S SIGNIFICANT ABOUT LAYER 2? AS THE DATA LINK LAYER IN THE OSI model, it's one of seven layers designed to work together but with autonomy. It sits above the physical layer, but below the network and transport layers. Its independence enables interoperability and interconnectivity, but from a security perspective, creates a challenge because a compromise at one layer isn't always known by the other layers. If the initial attack comes in at Layer 2, the rest of your network can be compromised in an instant. Network security is only as strong as your weakest link—and that may well be the data link layer.

By
CONNIE HOWARD



Who's Minding Layer 2?

Another consideration is perspective. Often, network operations have one agenda, security another, and both end up missing Layer 2.

Administrators in network operations use virtual LANs (VLANs) all the time, many of which route in and out of the same switch. When a security administrator approaches a network administrator to ask for a new segment, the network administrator creates a VLAN and assigns the security administrator an address space. The security side doesn't know it's using a VLAN—why would security care about what the network administrator does with the switch? The security administrator often doesn't even look at Layer 2, focusing instead on Layer 3 and above.

This difference in perspective even shows itself in networking equipment. Firewalls are in a secure state when they arrive. By default, until modified, they do not allow communication when first turned on. Switches and routers, on the other hand, are designed to enable communication—they are accommodating. While their very function—open communications—can create inherent insecurities in the network, switches and routers have many security features built in. However, these features and capabilities are not enabled unless network administrators turn them on, and often, these features aren't used, or worse, are unknown (see "Did You Know?" on page 32).

The 2002 Computer Crime and Security survey conducted by the Computer Security

FRED GAMBINO

Institute and US Federal Bureau of Investigation shows a shift in the way networks are attacked (gocsi.com). In 1996, the greatest number of attacks came from internal systems, with smaller numbers coming from remote dial-in and Internet scans. By 2002, the number and types of attacks had changed. Today, more than 70 percent of all attacks are external scanning attacks, with 30 percent coming from internal systems. Even though the percentage of internal-system attacks has declined, the sheer volume of external attacks, such as viruses, is to some extent displacing them. Internal attacks are still great in number, and the damage they cause is potentially greater than the damage inflicted by external attacks.

While it's beyond the scope of this article to describe all of the attack signatures that threaten Layer 2, we can address two of the most problematic attacks, MAC flooding attacks and VLAN hopping, and ways to mitigate their effects. Both can give you a better understanding of the problems faced at Layer 2.

MAC Flooding Attacks

Content Addressable Memory (CAM) tables store the MAC addresses available on physical ports along with their associated VLAN parameters-they're the Layer 2 equivalent of routing tables. The CAM table keeps track of machine network locations and knows which port future traffic travels over because it saw previous communication there. The MAC flooding attack tries to make switches act more like hubs by flooding the CAM table. The space within the CAM table is limited and, therefore, vulnerable to an overflow of traffic.

A MAC flooding attack looks like traffic from thousands of computers moving into one port, but it's actually coming from one station spoofing the MAC address of thousands of bogus hosts. Macof, a popular tool for launching this type of attack, can generate 155,000 MAC entries on a switch per minute. The switch sees this traffic and thinks that the MAC address from the packet the attacker sent is a valid port, and will add an entry. The goal is to flood the switch with traffic by filling the CAM table with false entries. Once flooded, the switch will broadcast traffic without a CAM entry out on its local VLAN, allowing the attacker to see traffic he wouldn't ordinarily see. Flooding is easy, even with big tables and high-end switches.

There are ways to mitigate MAC flooding attacks. The primary method is configuring port security on the switch. Port security allows administrators to specify the number of PCs that can be connected to any single switch port. If that number is exceeded, the port can be configured to shut down or block the MAC addresses that exceed the specified limit. Because of the performance impact involved in keeping track of the extra MAC addresses, the recommended best practice is to shut down the port that exceeds the limit.

Port security offers additional features beyond those needed to stop MAC flooding attacks. To learn more about how port security works and how it's configured, see cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_4/config/sec_port.htm.

VLAN Security and VLAN Hopping Attacks

Growing misinformation regarding VLAN security, compounded by fear and uncertainty that VLANs can be compromised, led Cisco to contract with @stake, an organization of internationally recognized network and application security experts, to determine the feasibility of executing successful VLAN attacks on Cisco Catalyst® switches. The @stake research found that there is no way to execute these attacks unless a misconfiguration exists on the switch. In these cases, misconfigurations are due mostly to the aforementioned open-communications design of a switch, rather than operator error. Hence, VLAN security is made more problematic because the default configuration of a switch makes it vulnerable to attacks such as *basic VLAN hopping* and *double encapsulated VLAN hopping* (described below). For more information on VLAN security and attacks, see the August 2002 research report from @stake: cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf.

VLAN hopping attacks are designed to allow attackers to bypass a Layer 3 device when communicating from one VLAN to another. The attack works by taking advantage of an incorrectly configured trunk port. Trunk ports have access to all VLANs by

Cisco Catalyst 6500 Series Security Modules

Preparing for threats and tightening VLANs at Layer 2 is important, but there are other things you can do to protect your networked assets, especially when you deploy any of the Cisco Catalyst® 6500 Series switches.

Cisco has raised the bar for Layer 2 security by integrating a suite of advanced security modules to complement existing software security offerings, including a Firewall Services Module (FWSM), Secure Socket Layer (SSL) Module, IP Security Virtual Private Network (IPSec VPN) Services Module, and Network Analysis Module (NAM).

Along with the existing Intrusion Detection System Module (IDSM), these modules enable you to deploy integrated security on the switch without the need to purchase, install, and manage separate security appliances. Deploying one or more of these modules hardens the switch, while increasing performance and manageability and driving down the total cost of network ownership.

For more information on the Cisco Catalyst 6500 security modules, visit cisco.com/en/US/products/hw/modules/ps2706/prod_models_home.html.

default. They are used to route traffic for multiple VLANs across the same physical link, generally between switches. The data moving across these links can be encapsulated with IEEE 802.1Q or Inter-Switch Link (ISL).

Dynamic Trunking Protocol (DTP) automates ISL/802.1Q trunk configurations and operates between switches. It synchronizes the trunking mode on link ends and prevents the need for management intervention on either switch. Administrators can configure the DTP state on an ISL/1Q trunking port to *On*, *Off*, *Desirable*, *Auto*, or *Non-Negotiate*. Here's how those states work:

- *On:* "I want to be a trunk and I don't care what you think!" State used when the other switch does not understand DTP.
- *Off:* "I don't want to be a trunk and I don't care what you think!" State used when the configured port is not intended to be a trunk port.
- *Desirable:* "I'm willing to become a VLAN trunk; are you interested?" State used when the switch is interested in being a trunk.
- *Auto:* "I'm willing to go with whatever you want!" This is the default on many switches.
- *Non-Negotiate:* "I want to trunk, and this is what kind of trunk I will be!" State used when an administrator wants a specific type of trunk ISL or .1Q.

The key thing to remember about DTP is the default mode on most switches is *Auto*.

Basic VLAN hopping attack. The attack occurs when an attacker fools the switch into thinking he is a switch that needs trunking. This attack requires a "trunking-favorable" setting, such as *Auto*, to succeed. Now, the attacker is a member of all the trunked VLANs on the switch and can send and receive traffic on those VLANs.

The best way to prevent a basic VLAN hopping attack is to turn off trunking on all ports except the ones that specifically require it.

Double encapsulated VLAN hopping attack. The double encapsulated VLAN hopping attack takes advantage of the way the hardware on most switches operates.

Did You Know?

Did you know that many of the Cisco products you've deployed at Layer 2 already have security features built in, including port security, private VLANs, and ACLs?

Here's what each of these features does.

- **Port security** allows administrators to specify the number of PCs that can be connected to any single switch port.
- **Private VLANs** provide security and isolation between ports on a switch, which are members of the same VLAN. This feature ensures that users can communicate only with their default gateway, not with one another. Private VLANs are useful in DMZ environments.
- **STP root guard/BPDU guard** mitigate spanning-tree attacks by shutting down ports that would cause the Layer 2 topology to change.
- **SSH support** provides a secure, remote connection to a Layer 2 or a Layer 3 device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This feature has both an SSH server and an SSH integrated client.
- **VMPS (VLAN Membership Policy Server)** enables specific MAC addresses to be bound to specific VLANs, allowing in-campus mobile users to always have the same network security permissions.
- **IEEE 802.1X authentication** secures the network by having users authenticate against a central database before any form of network connectivity is allowed. In contrast, most internal networks are accessible by just plugging into an internal Ethernet connection.
- **Wire-rate ACLs** allow access control lists to be processed without incurring a performance penalty. This feature enables ACLs to be deployed in situations where they might not normally be deployed.

CISCO CATALYST SWITCH FEATURE SUPPORT

	Cat 2900 XL	Cat 3500 XL	Cat 2950	Cat 3550	Cat 29xx G	CatOS 4000	CatOS 6000	IOS 4000	IOS 6000
Port Security	X	X	X	X	X	X	X		
Private VLANs	X	X	X	X		X	X	X	X
STP BPDU Guard			X	X		X	X	X	X
STP Root Guard	X	X	X	X	X	X	X	X	X
SSH Support					X	X	X		
VMPS Client	X	X	X	X	X	X	X	X	X
VMPS Server					X	X	X		
802.1X Auth			X	X	X	X	X		
Wire-Rate ACLs			X	X		X	X	X	X

Best Practices for Layer 2 Networks

In addition to MAC flooding and VLAN hopping attacks, there are several others, such as spanning-tree, Address Resolution Protocol (ARP) spoofing, and Dynamic Host Control Protocol (DHCP) attacks, that can invade Layer 2. Details of these attacks and their mitigation best practices can be found in a recent Blackhat.com presentation given by Sean Convery, security researcher in Cisco's Critical Infrastructure Assurance Group. For a copy of the presentation, see www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf. Among these best practices are the following:

- *Restrict* management access to the switch so that parties on nontrusted networks cannot exploit management interfaces and protocols such as Simple Network Management Protocol (SNMP).
- *Prevent* denial-of-service attacks and other exploitation by locking down spanning-tree and other dynamic protocols.
- *Use* Cisco IOS® hardware ACLs, where available, to block undesirable traffic.
- *Use* a dedicated VLAN ID for all trunk ports.
- *Shut* down unused ports in the VLAN.
- *Use* port security mechanisms to limit the number of allowed MAC addresses, providing protection against a MAC flooding attack.
- *Avoid* using VLAN 1, where possible, for trunk and user ports.
- *Avoid* using cleartext management protocols on a hostile network.

For additional information about VLAN security, visit cisco.com/go/safe. You'll find SAFE: A Security Blueprint for Enterprise Networks. (Also, see the SAFE poster inserted after page 34 in this issue of *Packet*®.)

Most switches today perform only one level of IEEE 802.1Q decapsulation. This allows an attacker, in specific situations, to embed a hidden .1Q tag inside the frame, allowing the frame to go to a VLAN that the outer .1Q tag did not specify. An important characteristic of the double encapsulated VLAN hopping attack is that it works even if trunk ports are set to *OFF*.

Thwarting this type of attack isn't as easy as stopping basic VLAN hopping attacks. The best approach is to make sure that the native VLAN of the trunk ports is different than the native VLAN of the user ports. For more on stopping double encapsulated VLAN hopping attacks, see the Blackhat.com presentation link in the sidebar, "Best Practices for Layer 2 Networks."

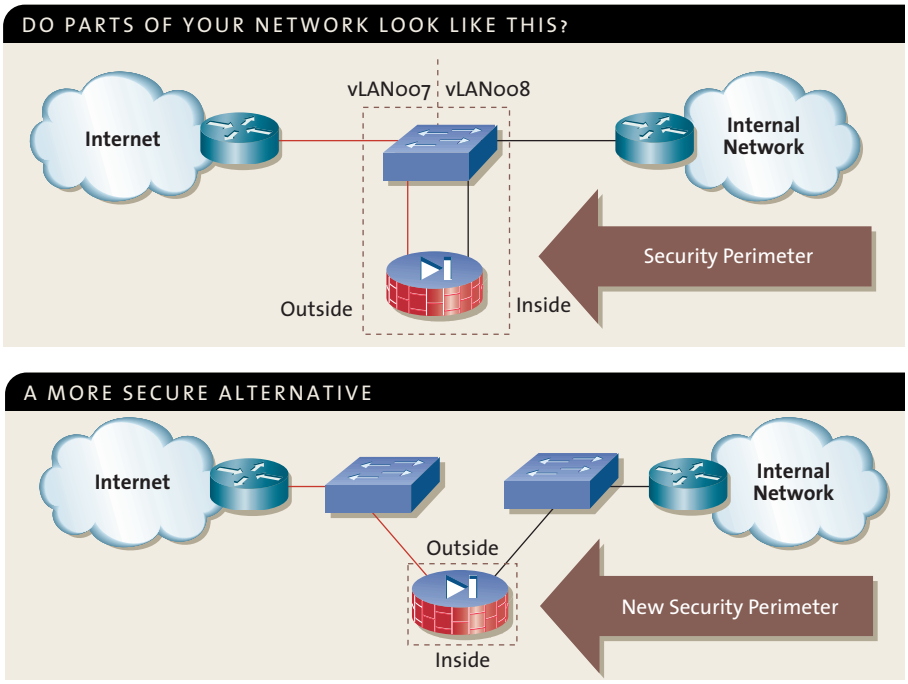


FIGURE 1: Instead of implementing VLANs that must be monitored closely, consider installing two switches with no VLAN. If either switch is compromised, the intruder still hasn't crossed the firewall.

Switch Management and Access Control

Recently, some Internet edge designs have used a single switch to control both the trusted and untrusted portions of the network (see Figure 1, top). In this design, multiple VLANs are used to differentiate trusted and untrusted traffic. As the @stake study found, if properly configured, VLANs can be used to segment traffic in this way. Unfortunately, using multiple security layers on a single switch increases the configuration complexity and likelihood of operator error. In addition, if the switch is ever compromised, an attacker can completely bypass the firewall, establishing a direct connection between the Internet and the internal network.

The important thing to remember is that the security perimeter of your network includes the switch as well as the firewall. And because in most networks, the security team doesn't control the switch, this can be problematic. An alternative design uses multiple switches without the need for VLANs (see Figure 1, bottom). In this case, if a single switch is compromised, the security of the entire network isn't bypassed. ▲▲

Cisco brings rich features of the Cisco Wireless Security Suite to IOS Software.

SECURING WIRELESS

CREATING NETWORK SECURITY FEATURES THAT ANTICIPATE AND thwart malicious attacks from inside and outside networks is a major focus at Cisco. The Cisco Blueprint for security, which is built on Cisco AVVID (Architecture for Voice, Video and Integrated Data) technology, provides a design strategy that emphasizes embedded security features at all network layers (see SAFE pullout after page 34). Cisco is keeping a step ahead of security threats by bringing powerful Cisco IOS® Software security protocols to key layers and elements of multiservice networks.

Cisco Aironet® 1100 Series access points, with their full complement of Cisco Wireless Security Suite features, now support IOS Software. Cisco Aironet 1200 Series access points with support for IOS Software will begin shipping in the first calendar quarter of this year.

The Cisco Wireless Security Suite supports IEEE 802.1X authentication and numerous Extensible Authentication Protocol (EAP) types, including EAP Cisco Wireless (LEAP); EAP-Transport Layer Security (EAP-TLS) and types that operate over EAP-TLS, such as Protected EAP (PEAP), EAP-Tunneled TLS (EAP-TTLS), and EAP-Subscriber Identity Module (EAP-SIM). The suite also supports a prestandard version of Temporal Key Integrity Protocol (TKIP).

Safeguarding WLANs

As wireless networks have proliferated, so has the concern over keeping them secure. Because all Wi-Fi-certified wireless LAN (WLAN) products ship with security turned off, enterprises need to be diligent about turning on WLAN security features. Open-access WLANs, while acceptable for public wireless hot spots, such as coffee shops, airports, and college campuses, are not suitable for business environments. Enterprise WLANs need strong security policies that protect the company from rogue access points, intruders, unauthorized users, and unauthorized viewing of transmitted data. Two security options are available for securing WLANs: (1) IEEE 802.1X for authentication and key management, plus Wired Equivalent Privacy (WEP) with TKIP enhancements for encryption; and (2) IPSec VPN.

"Both of the security options we've made available to customers—802.1X with TKIP and IPSec VPN—consist of three major components: authentication, encryption, and data integrity," says Sri Sundaralingam, technical marketing engineer in the Wireless Networking Business Unit at Cisco. "IEEE 802.1X provides user authentication, and TKIP provides encryption and data integrity. With IPSec-based VPN, IPSec provides data confidentiality and data integrity, and extensions to IPSec allow for user authentication and authorization to occur as part of the IPSec process."

IEEE 802.1X provides WLANs with strong, mutual authentication between a client and authentication server. It also provides dynamic per-user, per-session encryption keys, removing the administrative burden and security issues surrounding static encryption keys.

"With standard WEP, if somebody leaves the company, you have to change the static WEP key," explains Sundaralingam. "But even without employee turnover, these static WEP keys are common to all users on the WLAN. Each client's network interface card has the key to the network. There is no mechanism to centrally manage keys and control user access into the WLAN. That's why you need 802.1X—to facilitate user authentication and to generate a per-user/per-session dynamic encryption key."

TKIP provides enhancements to 128-bit encryption. One such enhancement is *per-packet key hashing,* where the encryption key is changed on each packet. This feature helps combat a common WLAN hacking tool called "AirSnort," which takes advantage of a weakness in WEP encryption when static WEP keys are not changed during a session.

Another important new security advance with TKIP is *Message Integrity Check (MIC).* With MIC, a digital signature is included with every frame sent, neutralizing the "man-in-the-middle" attack by hackers who can capture a wireless packet, modify it, and resend it.

"The digital signature is automatically calculated and incorporated into the 802.11 payload portion of each frame in Layer 2 and sent to be encrypted," explains Sundaralingam. "Per-packet keying is used to encrypt each packet before it is sent to the access point or WLAN station."

A third feature of TKIP allows network managers to rotate not just unicast keys but also the broadcast WEP keys used on access points to encrypt broadcasts and multicasts.

Cisco Wireless Security Suite

The Cisco Wireless Security Suite for the Cisco Aironet Series provides support for all IEEE 802.1X authentication types and prestandard TKIP. The Cisco Wireless Security Suite enables the use of Remote Access Dial-In User Service (RADIUS) for centralized authentication and accounting records. Either the client or the access point can initiate authentication. In both cases, the client responds with a user name. The access point encapsulates the response in a RADIUS access request message and forwards it to the RADIUS server, such as a Cisco Secure Access Control Server (ACS). The challenge and response process then begins—initiated by either the client or the RADIUS server.

After the challenges are met and success messages are sent between the client and RADIUS server, both the client and RADIUS server simultaneously derive the unicast key. The RADIUS server forwards its unicast key for the specific client to the access point. In this way, IEEE 802.1X mutual authentication validates both the client and RADIUS server (ACS), and by default confirms the validity of the access point. At this stage, the broadcast key is encrypted with the client's unicast key and sent to the client, along with the key length specifying 40-bit or 128-bit WEP key.

With the Cisco Wireless Security Suite, now a component of Cisco IOS Software, access points and client devices authenticate each other, traffic is encrypted, and a higher degree of data integrity is maintained.

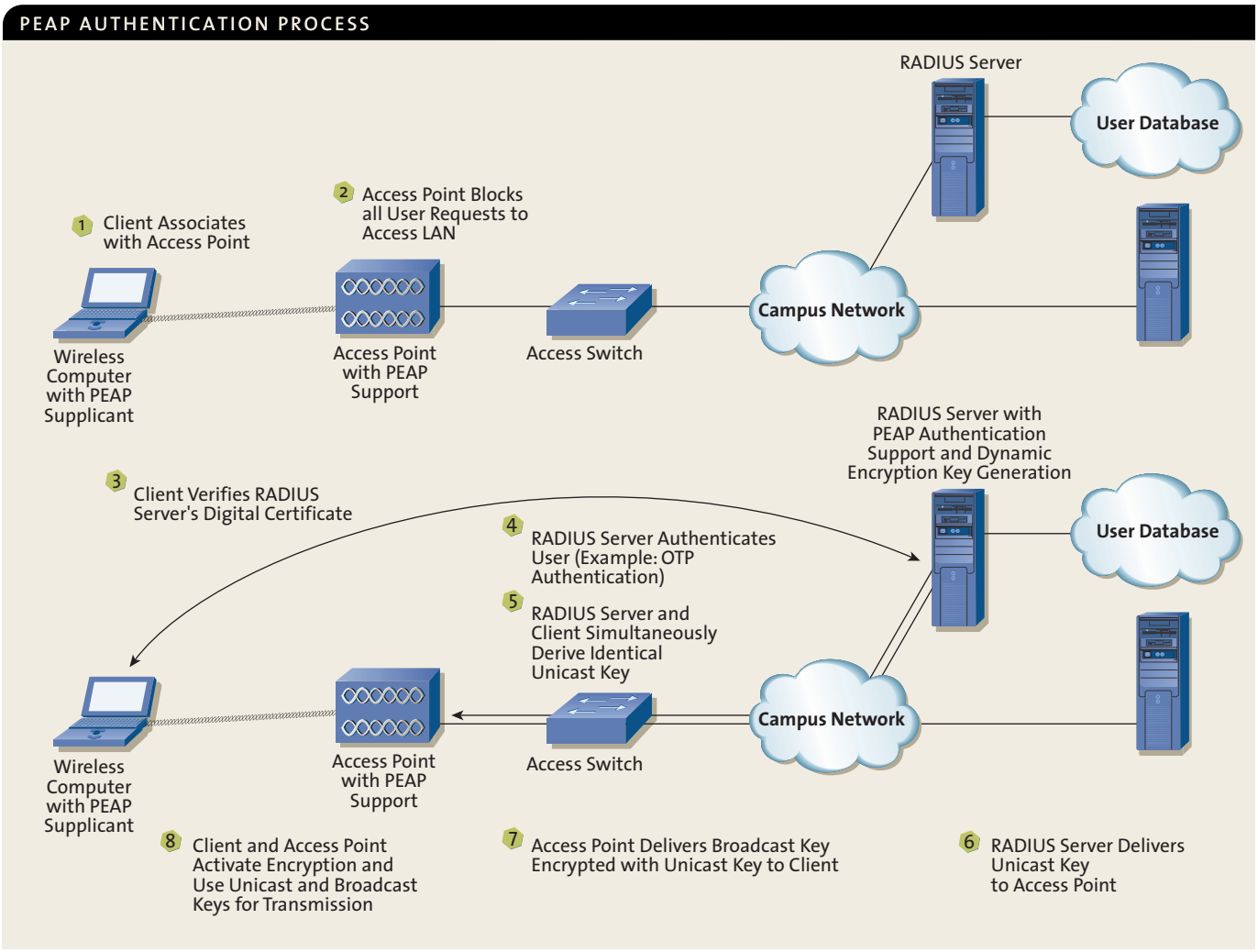
IPSec VPN

An alternative to 802.1X with TKIP is IPSec VPN. IPSec is a framework of open standards for ensuring secure, private communications over IP networks. It includes encapsulating security payload (ESP) protocol that provides data confidentiality and protection by completely encapsulating data. The authentication header (AH) protocol can be used either alone or with ESP to provide packet authentication. And Internet Key Exchange (IKE) protocol is used to establish a shared security policy and authenticated keys for services that require keys. Before IPSec traffic can be passed, each router, firewall, or host must be able to verify the identity of its peer.

IPSec VPN uses the services defined within IPSec to ensure confidentiality, integrity, and authenticity of data communications across public networks, such as the Internet. IPSec VPN secures WLANs by overlaying IPSec on top of cleartext 802.11 wireless traffic. Confidentiality is achieved through encryption

Join the Security Discussion

Ask your peers and Cisco experts questions, provide advice, or participate in "Tech Talk" and "Ask the Expert" events at *Cisco Networking Professionals Connection*: cisco.com/discuss/security.



PEAP IN SECURITY: Based on an Internet Engineering Task Force (IETF) Internet-Draft, PEAP is an EAP authentication type that provides mutual authentication of the client and RADIUS server via the access point.

using a variant of the Data Encryption Standard (DES) called Triple DES (3DES), which encrypts the data three times with up to three different keys. A recent addition to IPSec and IKE is the Advanced Encryption Standard (AES) encryption cipher (AES-128, AES-192, and AES-256). With Release 12.2(13)T, Cisco IOS Software now supports AES in addition to DES and 3DES ciphers.

Another major security option for the WLAN, beyond authentication, encryption, and data integrity, is *group-level differentiation*. Groups can by organized by user type (project or team) or application type.

Added Protection with Wireless VLANs

Cisco Aironet access points support up to 16 virtual LANs (VLANs) through 802.1Q trunking to a switch. Because WLAN clients are not VLAN-aware, the access point maps VLANs to Service Set Identifiers (SSIDs). Both static SSID-to-VLAN and dynamic RADIUS-based VLAN assignment are supported.

Traditionally, when there is one wire, there is one network with no differentiation. Now, separate groups within a company can be trunked via the access point to the same switch and differentiated. Also, a dedicated VLAN can be created to securely manage the access point, which avoids combining management and user traffic over the same segment. For example, a department store employee taking inventory with a wireless device might have access to some network resources via a wireless VLAN, whereas an executive using a laptop in a store office might have access to an additional set of resources via another wireless VLAN. As the users roam, their connections are forwarded via VLAN trunking to Layer 2 switches. At Layer 3, routers enforce each group's access privileges using access control lists.

◆ ◆ ◆

Cisco's support for numerous EAP types and the 802.1X standard provides a centrally managed, open wireless network security scheme that addresses the limitations of earlier IEEE 802.11 WEP implementations. The WLAN security options discussed here—802.1X with TKIP and IPSec VPN—along with security best practices for WLAN deployments, are covered in the SAFE Blueprint (cisco.com/go/safe). ▲▲

BUILDING An IT BUSINESS CASE that will SELL

By JANET KREILING

What Business Decision Makers Look for When Evaluating New IT Investments

THE RETURN-ON-INVESTMENT (ROI) numbers touted by analysts and vendors for various information technology (IT) projects can be tantalizing: paybacks in 16 months; productivity increases worth more than US$6 million a year; total cost of network ownership down 25 percent; administrative costs down almost 80 percent.

The business advantages inherent in new technology are equally intriguing: integrated customer care centers; disaster-resistant IP communications; e-learning; secure access for teleworkers and mobile workers; unified messaging. The list goes on.

IT staffs see great potential in new technology. However, many senior managers and financial decision makers feel they have been burned once too often by IT promises left unfulfilled. Moreover, IT now accounts for almost half of all capital spending, and IT projects must compete not only against each other, but also against proposals to add research and development (R&D) funds, manufacturing capacity, or staff. And most senior managers are not IT people; they find new plants and R&D more comfortable propositions. Furthermore, many chief information officers (CIOs) have been admonished not to approve radical new ventures, but to build on what they have.

So, how do you sell that great new IT project?

What Business Leaders Want

"Financial decision makers are looking for technology investments that generate both hard cost savings as well as strategic business benefits," says Mike Kisch, marketing manager at Cisco. "Given the state of the global economy, they're placing more emphasis on investments that will save money. Yet they still recognize the need to prepare for the future."

While computing cost savings can be relatively straightforward, measuring strategic value is tougher. But it is crucial. According to Forrester Research, almost 70 percent of businesses expect their IT networks to be a source of competitive advantage.

Increasingly, Kisch points out, "decision makers are using ROI analyses to decide whether or not to approve a project and to make sure they're making the best use of their capital investment dollars." To reinforce its importance, he cites a recent study by *Darwin Magazine*, which found that more than 80 percent of organizations now require some form of ROI analysis.

Kisch and his colleagues have worked with more than 1500 customers in evaluating the ROI expected from a variety of Cisco technologies, and in the process, they have heard a good deal about what makes a successful business case for a new IT project. Among the considerations to keep in mind:

- Infrastructure investments need to pay back in less than 18 to 24 months.
- If a business case is built on "soft" business benefits—those without clearly defined cost savings—the CIO will discount its projected impact by 25 to 50 percent.
- An ROI analysis needs to be based on internal data, not industry averages or other companies' numbers.
- The proposal must identify ways to get more from less by leveraging existing technology investments.
- CIOs are increasingly competing with other business managers for scarce resources. Therefore, technology business cases must be rock solid.

How to Build the Business Case

What makes a winning business case? Kisch lists five components.

1

1. It must clearly state the value proposition of the solution and focus on the primary cost-benefit drivers.

Do you expect to save money on toll charges? Leased line charges? Support costs? Maintenance? How much are you paying now? How much will the new installation cost, and over what period of time?

"Those numbers must describe your own IT infrastructure," Kisch says. "No other company is like yours. Nobody else has equipment leases running out when you do; nobody else has the same transport network, number of users, locations and operations, support staff, strategic goals." Often, he adds, IT departments don't fully present the core value proposition of their proposed project. When they come to build the business case, they struggle to frame the pertinent costs and benefits effectively.

Benefits that can't be quantified (soft benefits) must still be outlined as part of the value proposition. Will the installation improve customer relationship management (CRM)? How? What additional capabilities will it offer? What new applications will it support? Delve into your corporate library or database. If you're a bank or merchandiser, for instance, check out analyst reports on CRM in the financial services or retailing industries.

2

2. The analysis should be broken into manageable pieces, or the proposal can seem overwhelming.

Instead of building an ROI analysis that includes every site within the enterprise, identify key segments that are rep-

What Are Your Terms?

ROI (return on investment)—compares the net benefits of a project versus its total costs over the analysis period, expressed as a percentage. ROI is used to determine if an IT investment can pay off the same or better than other investments the company might make. Traditionally, the ROI calculates how much return is generated or results from increased profit or cost savings.

TCO (total cost of ownership)—an accounting of all the costs associated with procuring, deploying, and owning an IT system. Unlike ROI, which compares benefits against cost, TCO is an average annual cost figure over a given time period without regard to the benefit of owning or using the asset.

Payback period (breakeven point)—the length of time required to recover the cost of an investment. Calculated as payback period=cost of project/annual cash inflow, it is the exact point at which benefits exceed costs, generating positive cash flow from the project investment.

resentative of the whole. For example, many large organizations group their sites by size or common characteristics such as being a new facility or needing a network upgrade. Then they identify several representative sites within each segment, perform the ROI analysis, and project the results across the whole enterprise. "Look for compelling events such as a PBX coming off lease, a greenfield facility, or a planned network upgrade," Kisch advises. Plan into the future, perhaps over three to five years, with extensions of the project taking place on a timetable that makes sense for both company and project, and that ties in with corporate goals.

At the same time, be careful not to "suboptimize" your ROI calculations by fragmenting the analysis to individual sites. For example, by running your analysis branch office by branch office, you may find it difficult to justify the cost of IP telephony. However, by taking a holistic view of the network—and realizing that you can deliver voice services to multiple branch offices from a single clustered Cisco CallManager implementation in a single data center—a different picture of quicker payback and higher ROI emerges.

3. It should be based upon a solid financial model using fundamental financial principles that properly allocates the costs and benefits over the term of the project.

Often organizations do an excellent job of collecting the necessary cost and benefit data, but are challenged by the finance department when they run the numbers through a financial model. Make sure the model you use is grounded in sound financial and accounting principles and has been blessed by financial experts. Cisco has developed a well-researched, proven Web-based ROI calculator, the Cisco Network Investment Calculator (see sidebar, page 45) for many applications such as IP telephony, unified messaging, contact centers, and storage-area networking that creates estimates from your company's own data.

4. It should contain a sensitivity analysis—multiple "what-if" scenarios to determine the range of potential outcomes.

"This point is especially important for financial managers who have been burned when projects didn't yield promised benefits, often because technology was deployed without people looking at factors crucial to success," Kisch says. "You need to outline possible variants, such as delays in deployment and deviations in costs and benefits, so senior managers know exactly what they're buying into." Moreover, he adds, "acknowledging that there is a range of potential outcomes for any potential IT project is a great way to build credibility with financial managers."

5. The business case should provide for pre- and post-deployment analyses, so executives are assured you are monitoring effectiveness.

Plan to run the numbers again after deployment to see how well you've met your goals, and adjust multiyear plans as needed. Identifying how and when you intend to validate your results will help build credibility. While ROI analysis can be a headache, it's crucial that organizations track the success of IT investments compared to the initial business case. Doing so helps them improve their project approval and implementation process.

PROJECTS WITH POTENTIAL

IP Communications

Perhaps the project that offers the most potential to enhance business operations and cut costs is IP communications—transporting voice calls and services over your data network. Indeed, a recent Phillips InfoTech survey found that 44 percent of enterprises have already begun migrating to IP telephony, and 12 percent of all voice lines shipped in 2002 were IP station lines.

The cost savings are definitely there: The industry consensus is that a phone and PC sharing one Ethernet drop saves US$150 per drop. Based on anecdotal reports from Cisco customers, the productivity of network support staff goes up by 10 to 40 percent, freeing people to do more value-added work. And then there are the substantial savings in interlocation toll charges, as well as savings from managing the consolidated infrastructure centrally.

In a case study that involved moving from a 1000-line Centrex environment to IP telephony, the projected payback was 22 months, and network support staff productivity increased by 25 percent. Interoffice calling charges went down by US$25,000 a year; adds, moves, and changes costs by $30,000. For a new 650-phone facility at Cray, Inc. of Seattle, Washington, the payback was nine months, including 33 percent lower network administration costs, 25 percent lower networking equipment costs, and 35 percent lower interoffice phone charges. These two examples were modeled for specific customers with the Cisco Network Investment Calculator.

Beyond cost savings, the business advantages of a converged voice and data network are legion: integrated IP contact center, unified messaging, videoconferencing, distance learning, multicast video streaming, teleworking, e-business, and more. According to a survey conducted by the Radicati Group in 1998, unified messaging alone has freed up 25 to 40 minutes per employee per day, yielding commensurate productivity increases. Compare the cost of Cisco's Conference Connection audioconferencing to the subscription service you may be using now. Videoconferencing versus travel? For many meetings, there's no contest, and easily quantifiable savings.

Cisco IP communications enterprise-class solutions include IP telephony, unified communications, IP video/audioconferencing, IP video broadcasting, contact center, and third-party applications that leverage a single network infrastructure enabled by Cisco AVVID (Architecture for Voice, Video and Integrated Data). Cisco AVVID includes gateways to the public switched network, Catalyst® switches, routers, call processing platforms, media convergence

servers, call managers, and other systems that comprise a complete solution for any enterprise's scale and budget.

Mobility

Add wireless communications to converged voice and data over IP and you have a winning combination that helps improve productivity, lower operations costs, and maximize profitability. Together, these essential enabling technologies expand the productivity zone of workers who are too often away from their wired desktop connections—and whose ability to make decisions, collaborate effectively at meetings, and even close deals is impeded by that disconnect. Today's mature mobility solutions, and their decreasing capital costs, let companies extend connectivity to employees roaming in buildings and around campuses, working from home, or traveling almost anywhere in the world. Mobile access has been shown to add one to two hours a day of productivity per worker, while enabling users to respond to customers, partners, and colleagues more quickly.

Adding wireless to a campus LAN typically costs US$300 to US$500 per person. It can connect workers to network resources an additional 1.75 hours per day, according to a wireless LAN (WLAN) benefits study conducted by NOP World. At an annual salary of US$64,000, the added connectivity translates to as much as US$7,000 a year of potential greater productivity per employee. "In addition to enhancing communications, mobility allows organizations to better utilize existing investments in laptops, applications, and their network," Kisch points out.

In other words, the cost of installing a wireless access-point infrastructure and laptop connections, when divided up among the number of users, is only US$1 to $2 per person per day. For about the price of a cup of coffee or a soda, users can have a wireless extension cord to their companies' highly tuned, valuable corporate networks.

Switching

When building a business case for a converged LAN, companies should make sure that the switches they put into their access, distribution, and core layers are scalable enough that they can integrate voice, video, and higher-bandwidth applications in the future, says Vanessa Vogel, Cisco product manager. That will produce savings on overhead and capital costs for future services—and that's where customers will see significant returns on their investment."

Standardizing on Cisco Catalyst equipment, she adds, allows customers to extend Cisco IOS® Software and thus similar security and operational provisions across all switches, limiting the training and configuration costs associated with multivendor environments. Standardizing on switch architecture end to end in the network—on the Catalyst 6500 Series, for example—lowers total cost of ownership (TCO). Modules can be added to render them capable of Layer 2 through Layer 7 integration. Other modules can upgrade these switches to provide higher availability, security (including intrusion detection and virtual private networks), load balancing, and packet acceleration. This seamless integration can reduce training, maintenance, and overhead costs, while the additional functionality can further enhance ROI.

Moreover, Vogel points out, the Catalyst 6500 Series supports IP communications, "because the architecture for voice over IP is embedded in these systems' architecture." They integrate voice, video, and data in a converged network, and deliver the quality of service (QoS) people expect for voice and other higher-bandwidth applications without additional equipment.

Routing

Your WAN can also offer up savings, whether it extends over multiple branches in the same city, across the country, or around the world. For example, according to Bev Gallagher, business development manager in the Multiservice Customer Edge Business Unit at Cisco, the advanced routing, packetizing, and compression technologies in Cisco multiservice routers cut the operational expenses of backhauling voice and data traffic from regional hubs over your WAN.

Many branch offices, particularly those of retail banks and chain stores, support multiple, separate lines to handle different systems: ATM machines, point-of-sale terminals, video surveillance, and telephone service, in addition to "traditional" data networking access. By converging these separate systems onto a single, multiservice data network connection, these organizations can save a tremendous amount of money. The increased bandwidth and intelligent services of a converged network will allow them to deliver enhanced applications and services to employees and customers, further increasing ROI.

Here's an example of how multiservice routers can squeeze more bandwidth out of your WAN's transport capacity. Take a T1 line with twenty-four 64-Kbit/s channels. With integrated voice and data service, some channels can be devoted to voice, but when voice traffic trails off—in the wee hours, for instance—the router can cram them with file dumps. Also, compression algorithms can squeeze up to five voice calls onto just one 64-Kbit/s channel. "These technologies reduce the number of access lines needed, thus cutting toll charges and local and long-distance facility costs," Gallagher says.

They also make it possible, she points out, "to centralize resources such as call managers, voice-mail servers, business applications, customer databases, and employee directories, reducing capital costs and making them more readily available to users across the network." Centralized assets also allow WAN managers to take advantage of capabilities such as time-of-day routing, routing around traffic congestion, and load balancing that further improve availability and ROI.

Moreover, Cisco routers expand the services available to WAN users. Located at the network edge, they provide the infrastructure to support a host of multiservice voice, data, and video applications, and allow the customer to manage, migrate, and maintain these applications efficiently. A multiservice WAN that can support all protocols—IP, ATM, Frame Relay, Multiprotocol Label Switching (MPLS)—is where things really get exciting. It enables the enterprise to make available all business applications that will save money and allow the company to do its business more effectively.

The vehicles of choice are Cisco 2600XM and 3700 series branch routers,

Hard, Reliable Numbers on ROI

The Cisco Network Investment Calculator is a Web-based tool designed to help customers understand the specific financial implications of deploying Cisco solutions. It includes modules for IP telephony, unified messaging, audioconferencing, storage networking, computer-telephony integration, intelligent contact management, and intelligent call distribution.

Says Mike Kisch, marketing manager at Cisco, "We provide the financial model and help you understand how it works. Then you populate it with your own numbers, so the ROI results apply specifically to your company."

Customers view the ROI calculators provided by most vendors with a healthy degree of skepticism, Kisch says. To address this concern, the Cisco calculator's methodology is transparent, so financial decision makers can see clearly how the expected ROI was derived. Also, its methodology has been validated by financial experts and the analyst community as conforming to established financial principles, so "it will hold up under the scrutiny of your chief financial officer."

The Cisco Network Investment Calculator is a thorough tool that enables organizations to input multiple sets of assumptions for customized ROI forecasts. Your Cisco account representative can provide you with more information and help walk you through the process.

which offer very high LAN/WAN connectivity, resiliency, security, scalability, and QoS. The access router becomes the single point of integration for network applications such as security, voice, and content, enabling customers to extend e-learning, customer care, e-commerce, and collaboration applications to the branch securely and reliably.

Storage-Area Networks

Data storage requirements grow dramatically as enterprises adopt Internet business solutions. Most have historically used direct-attached storage (DAS), with storage systems linked to a specific server. But increasingly, says Sandhya Venkatachalam, product manager at Andiamo Systems, which was recently acquired by Cisco, enterprises are seeking more efficient topologies that scale their storage more efficiently, and are adopting storage-area networks (SANs) in which some or all servers are networked to storage subsystems. The benefits are clear: centralized management, and, importantly, a robust business continuance strategy. According to SearchStorage.Com, SANs help prevent interruption of mission-critical applications and the recovery of full functionality as quickly as possible if disaster strikes.

Specific cost savings from SANs lead to a high ROI. A report by McKinsey-Merrill estimates that SANs can increase disk utilization to 75 and 80 percent, compared to the 50 percent typical of DAS, resulting in a deferment or even elimination of excess disk purchases. In addition, SANs enable storage administrators to manage, on average, two to ten times as many terabytes of storage as they can with DAS systems. This can decrease the budget for administration from 47 percent of total storage costs to 10 percent. Moreover, SANs permit centralized tape backup, which can reduce backup expenses and reduce overall backup time.

Perhaps the best business benefit of all: SANs' record for data availability is 99.999 percent. If you're a brokerage firm, a minute of downtime typically results in US$6.5 million of lost business; if you're a catalog sales company, US$0.09 million.

But, of course, all SANs are not equal. Venkatachalam points out that Cisco's new MDS 9000 Family of multilayer directors and fabric switches offers advanced intelligence and scalability that yield industry-leading reductions in TCO. The Cisco 9500 Series offers the highest scalability—up to 256 ports per chassis—and the highest performance—1 terabit per second of system bandwidth—of any SAN platform on the market. Moreover, the Cisco MDS 9000 Family offers innovative, intelligent network services such as virtual SANs (VSANs), in which one physical entity is partitioned into smaller entities to increase security, availability, and manageability, while still maintaining benefits such as disk capacity reduction.

In addition, the Cisco MDS 9000 Family integrates on one platform with a unified management interface all relevant storage protocols, including Fibre Channel, iSCSI, FCIP, and, in the future, FICON, further boosting their cost benefits.

Security

"Security has changed from an IT issue to a business issue," says Jeff Platon, senior director of marketing for network security at Cisco. "It's now looked on as an enabler, an investment rather than just a cash outlay."

Continued on page 81

Enterprise SOLUTIONS

Super Market Strategy

Korean retailer Seowon uses VPN technology to transform its business and maintain an edge.

THE KOREAN DISTRIBUTION MARKET IS becoming ever more competitive with the expansion of large domestic discount stores and multinationals, such as Tesco, out of the Seoul metropolitan area into smaller city markets.

To combat this trend, supermarket giant Seowon, a progressive retailer with more than 1000 stores across southwestern Korea, has embarked on a strategy of entering into new markets, typically in smaller cities, where its larger competitors cannot follow. Seowon is also introducing a new e-business strategy. Mindful of the importance of security, its information technology (IT) department is revamping its existing network infrastructure to provide the company with the security and performance it needs to grow its business. To accomplish this, Seowon has adopted a Cisco virtual private network (VPN) solution, based on the SAFE Blueprint for security from Cisco.

NEW MARKET ENTRY: Seowon is rapidly opening up new outlets in smaller southeastern Korean cities.

Competitive Pressure

Founded in 1980, Seowon is one of the fastest growing distribution companies in Korea, with more than 10 outlets in southwestern Korea. Its network comprises 40 major supermarkets and 1000 additional smaller supermarkets. With a turnover of US$480 million in 2002, its business grew 23 percent compared to the prior year. However, competition from both local and foreign players has been steady and mounting, and Seowon became convinced that it needed to change its business model to maintain its leading position.

The company introduced an e-business strategy, which necessitated a careful look at security, and at the same time began to focus on reducing operational costs and improving employee efficiency. According to Kim Sang Soo, IT director for Seowon, "Our business is changing at lightning speed. First, we are expanding our network of stores from our traditional locations in cities to the suburban areas. Second, we are looking at how we can transform ourselves into an e-business. For our business to enjoy success in the future, we needed to invest in the latest technology solutions available, for example, virtual private networks."

Changing Requirements

For many years, Seowon depended on traditional Frame Relay for its WAN infrastructure to link up the supermarkets across the 10 cities in which the retailer operates. But it was ill equipped to deliver the availability, reliability, and scalability new business requirements demanded. Cost was also an issue because it was very expensive to deploy dedicated leased lines to connect all Seowon's branches.

The situation was exacerbated by the introduction of a new image-based point-of-sale (POS) system, which almost brought the Seowon network to a standstill. While the head office was connected at 128 Kbit/s, the stores in outlying areas were connected at only 56 Kbit/s, because the cost of 128-Kbit/s connections was prohibitive. To upgrade the current network to an acceptable level would have cost more than Seowon was willing to invest at the time.

> "The Cisco VPN solution, along with the SAFE Blueprint, has provided us with a secure foundation for migrating to a cost-effective converged network and a platform for future growth."
>
> —KIM SANG SOO, IT DIRECTOR, SEOWON

Because 40 percent of all its sales transactions were paid for by credit card, connectivity and the availability of skilled personnel support, especially in the suburbs, was fast becoming a business-stopping issue.

A Solution with Security Built In

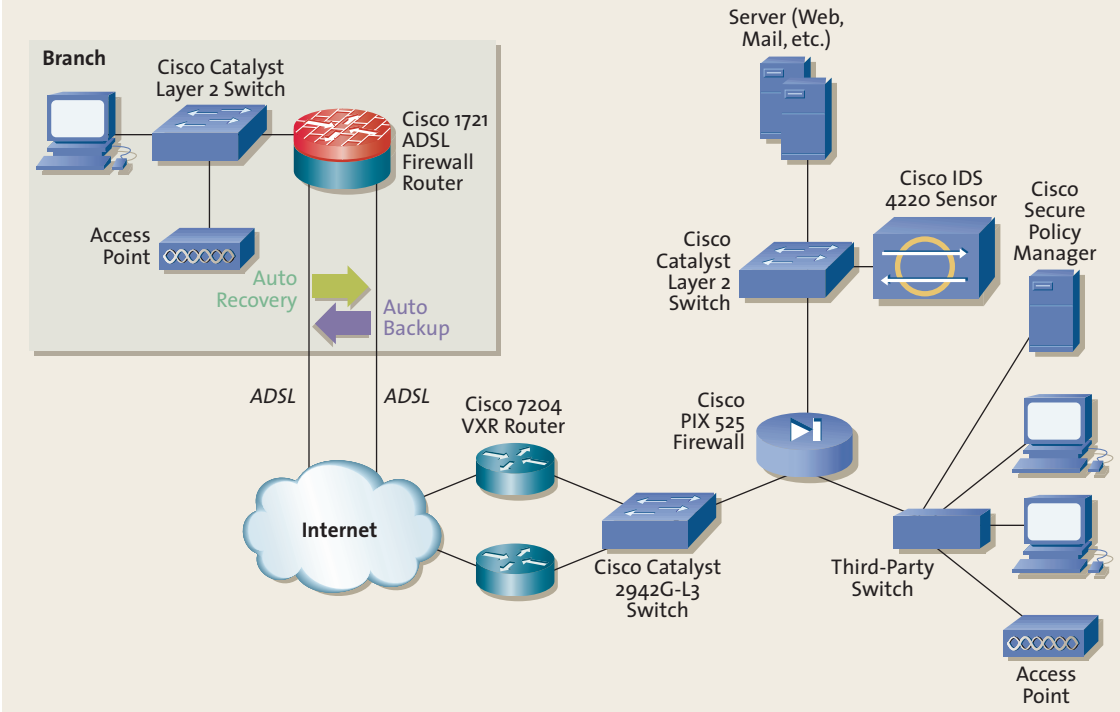
Seowon wanted an integrated network solution with security built in from the start. Instead of a simple VPN solution, Cisco came up with a router-based VPN for greater flexibility and scalability.

"We were very impressed with the Cisco VPN proposal, which is based on the Cisco SAFE Blueprint for security. Because it is modular in nature, we were able to select the functions and features we wanted, have the peace of mind that they would work well together, and at the same time, retain the option of adding others in the future if necessary," says Kim.

"The Cisco VPN solution can scale to support our future branch expansion plans and provides redundant branch connectivity. The network performance has been excellent, which is exactly what we needed to support the e-business applications at our head office, as well as our branch offices."

An initial network security design was based on the SAFE Internet Access Module, and the SAFE VPN

SEOWON VPN SOLUTION



MODULAR SOLUTION: The Seowon router-based VPN solution provides redundancy and scalability for future growth.

and Remote Access Modules. To put as many walls between would-be attackers and Seowon's business-critical systems, a multilayered defense was adopted using Cisco PIX® Firewall products and the Cisco Intrusion Detection System (IDS).

Ensuring Business Continuance

Implementation of Seowon's VPN solution began in February 2002. Says Kim, "The implementation went very smoothly and was complete in two months. Because of the modular structure of SAFE, we didn't need to design the entire security architecture from the ground up. An onsite Cisco security expert provided knowledge transfer to enhance the capabilities of our IT team."

PROGRESSIVE GROWTH: IT Director Kim Sang Soo oversees integrated security at expanding supermarket giant Seowon.

To ensure that Seowon's business stays online around the clock, dual asymmetric DSL (ADSL) links were implemented to provide proper load balancing and redundancy to all the company's branches.

The Seowon IT team was thrilled with the performance of the Cisco PIX Firewall and Cisco IDS. The integrated hardware and software of the PIX firewall—the highest performance, enterprise-class firewall product line within the Cisco firewall family—delivered the high security Seowon's management demanded without negatively impacting network performance.

In addition, the Cisco IDS has provided a comprehensive, pervasive security solution for combating unauthorized intrusions and malicious Internet worms, along with bandwidth and e-business application attacks. It has helped reduce the cost of advanced intrusion protection with network-integrated and hardware-based solutions.

Strong Results

During tough times, few companies are willing to invest in new technology unless the return on investment (ROI) is fast and tangible. In Seowon's case, the ROI on the VPN project satisfied both criteria in a record two months time.

Not only was security much better than before, Seowon found that it was able to recoup its 260 million Won (US$221,000) investment in setting up the VPN very quickly. Careful ROI studies conducted by the Seowon IT department indicated that the VPN would save them 16 million Won (US$13,600) a month, which meant that they would get back their entire investment in just a year and four months. For new stores, it would cost a minimal 68,000 Won (US$57) to set up a new line. To top it off, the Cisco VPN solution came with a two-year warranty so the cost of maintenance was negligible.

The VPN also made possible the introduction of a new network management system with real-time network monitoring. Thanks to the increased network speed and adoption of remote control server, 60 percent of PC problems encountered by Seowon's employees can now be fixed remotely, resulting in even further cost savings.

Web-Enabled for the Future

The future looks bright for Seowon because the VPN will form the basis of a new Web-based information system environment for the company.

"It is certain that the Web-based IT environment will be the dominant IT system for companies in the near future. The VPN not only migrated our network to a Web-based environment, but also took care of the security problem, and has enabled Seowon to go Web-based in a speedier manner," says Kim.

Seowon plans to evolve its network security design to adopt more SAFE modules, including mobile access with VPN clients and the construction of a secure campus network. Plans are also underway to move from its current enterprise resource planning (ERP) applications to a supply-chain management environment in 2004.▲▲

Content Boost

New Content Engine network modules combine content networking and edge routing into an integrated branch solution.

BY DAVID BAUM

Delivering rich media like streaming video, audio, animation, and graphics files across a national or global network can exact a heavy toll on the underlying network infrastructure. And as rich media becomes more common within enterprise networks, many companies are turning to enterprise content delivery networks (ECDNs) to minimize wide-area bandwidth usage and streamline network performance. Cisco pioneered the industry's first content-routing technology, the Web Cache Communication Protocol (WCCP), along with network appliances, called *cache engines,* to store frequently accessed content at the edge of regional networks. Now, newly introduced Content Engine network modules from Cisco extend these ECDN capabilities to Cisco 2600, 3600, and 3700 series access routers, providing the industry's first and only router-integrated solution for enterprise caching and content delivery services (see figure on page 53).

"Enterprises continue to accelerate the extension of productivity-enhancing networked applications to branch and remote offices. The addition of integrated content delivery services builds on the available security, IP telephony, and QoS [quality-of-service] suites to enable new levels of integration and intelligence in the access router," according to Dave Frampton, senior director of product management for the Multiservice Customer Edge Business Unit at Cisco. "Leveraging the modularity of Cisco's access routers to incorporate content services makes for a compelling integrated solution for the emerging full-service branch or remote office. This solution's improved security, manageability, and infrastructure efficiency make it an excellent value proposition for customers seeking good return on investment."

"The integration of content networking into branch office routing enhances the user experience while reducing cost of ownership," adds Jennifer Lin, product manager at Cisco. "We're making it easier for customers to rapidly deliver strategic applications to branch personnel including e-learning, corporate communications, content acceleration, employee Internet access control, file distribution, and streaming media—all through Cisco's modular access routers.

Content Networking 101

Content delivery networks combine routing intelligence with content-aware technology to streamline the distribution of all kinds of content. By caching content locally at the network edge, these solutions lower propagation delays and latency while improving overall response time. Ideal for rich content, such as large graphics files and streaming video, ECDNs also optimize the delivery of static content like HTML code and Web page text.

While these content delivery and caching tasks can be effectively handled by standalone network appliances such as the Cisco Content Engine 500 Series, the Content Engine network modules provide an integrated solution that fits conveniently into a single slot on the Cisco 2600, 3600, and 3700 series multiservice access routers. A dedicated processor within the module runs Application and Content Networking System (ACNS) software to optimize delivery of e-business applications and content from the network edge.

As with Cisco's other ECDN solutions, the Content Engine network modules use Cisco IOS® Software-supported WCCP for redirecting users' content requests, as well as HTTP routing. With WCCP, the router transparently redirects specified traffic to the Content Engine module, reducing WAN bandwidth usage and improving the delivery of HTTP and streaming content to users. And because WCCP offers advanced transparency for redirection, customers don't have to make any changes to the existing network architecture, client browsers, or servers. The new Content Engine modules running the latest Cisco ACNS software are available on Cisco IOS Software Releases 12.2(11)YT and 12.2(13)T.

Customers can choose the network module with one of three field-replaceable expansion modules: a 20-gigabyte hard drive, a 40-gigabyte hard drive, or a SCSI connector to accommodate an external disk array. All three options enable customers to rapidly deliver strategic ECDN applications to branch personnel with minimal additional network management. The Content Engine network modules can be configured and managed from the Cisco IOS Software command-line interface (CLI). However, a flexible management interface allows the

Content Engine network modules to be configured and managed from the Cisco Content Distribution Manager for advanced content services, as well as standards-based management platforms such as CiscoWorks.

Users can deploy a mixture of Content Engine modules and existing appliances in their networks, because modules are fully interoperable with other Content Engine appliances within the ECDN.

Customers can take a "stepped" approach to deploying the new ECDN solutions, starting small and then scaling to higher capacity and availability. Small to medium branch offices might start with a simple service, such as transparent caching, and then add e-learning and other advanced services over time. "These modules extend infrastructure investments in Cisco branch routers without degrading router performance," Lin emphasizes. "They are simple, cost effective, and straightforward to deploy. The integrated design allows customers to enhance their networks as they grow—without creating additional levels of management complexity."

Escalating Appeal

Cisco foresees strong industry demand for the new ECDN solutions, as evidenced by a survey conducted by its Internet Business Solutions group. Completed by more than 520 IT decision makers in the Americas, Europe, the Middle East, and Africa, the survey revealed content delivery as one of the top three planned networking investments.

SBC Communications Inc. (sbc.com), one of the world's leading data, voice, and Internet service providers, is actively testing the Content Engine network module on a Cisco 2611 edge router in its Indianapolis, Indiana lab. According to Jim Runnels, senior network manager at SBC, the company plans to use the solution to optimize caching and Windows Media streaming capabilities as it ramps up its e-learning initiatives. "We experience improvements in access performance by placing rich content closer to users," Runnels says. "We also boost content availability, because content is replicated and distributed across the network in multiple locations, thereby avoiding single-site or single-server failures."

Runnels and his team currently use Cisco Content Engine 500 systems to cache rich content at the edge of SBC's regional networks. Because the service provider also depends on Cisco 1600, 2600, and 3600 series edge routers, Runnels can foresee a need for the Content Engine network modules in the future. During the testing, he found the network modules were easy to manage using tools such as CiscoWorks network management software. "We like the interface—it has a similar look and feel to a router, and we can manage it using familiar IOS commands," says Runnels. "Having the content engine in the same cabinet as the router means fewer network devices and fewer power cords—it's a cleaner, simpler design to install and manage."

Customers can also extend their existing SmartNet™ service agreements to simply the purchase of the new modules. "It's often easier to justify adding a module to a router than it is to get approval for a standalone content delivery device," Runnels points out.

A Rich Multitude of Uses

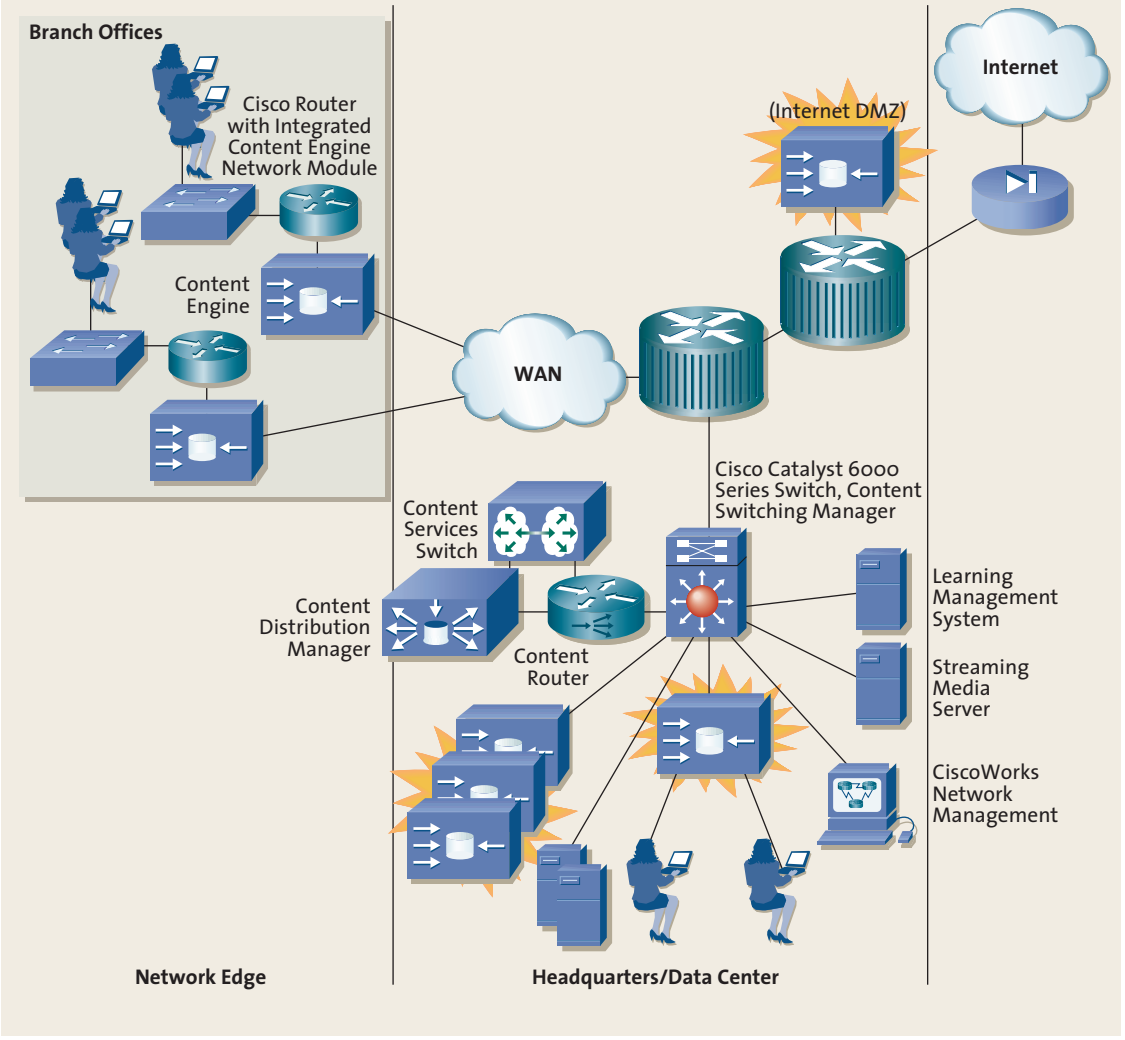
Cisco Content Engine network modules have many uses. The most basic one is called *content acceleration,* in which an organization caches frequently requested content at the edge of the network so users don't have to download large files over a WAN link. For example, each network zone might have its own cache of rich content.

Content filtering can be used to block objectionable content such as gambling, adult entertainment, and shopping, further freeing up WAN bandwidth. This serves to increase security, boost employee productivity, and reduce potential legal liability to the organization.

File distribution entails more efficient distribution of bandwidth-intensive content such as software executables, PDF files, PowerPoint files, CAD/CAM drawings, and other graphics. With a CDN solution, this type of rich content can be positioned at the network edge to boost access speeds.

Streaming media enables an organization to deliver high-quality video over the IP network. The new network modules offer full support for key streaming technologies such as MPEG, Windows Media, RealNetworks, and QuickTime. Streaming media is popular for executive communications and e-learning, both live and on demand, as SBC Communications has proven with its video-on-demand content.

CISCO CONTENT NETWORKING SOLUTION



RICH MEDIA: Integrating content networking capability into branch routing platforms enables key content services such as advanced transparent caching; live and on-demand streaming media; large file and software distribution; and content filtering and user authentication.

Proven Platform Integration

While standalone Content Engine appliances are attached to the network through an external Fast Ethernet connection, communication between Cisco IOS Software and ACNS software is handled internally when the module is plugged into the router.

Cisco IOS Software runs on the router and provides "hooks" into the network software module, which runs ACNS. The solution is integrated from a management standpoint, but if anything happens to the Content Engine, it will not affect the availability or integrity of the router. By offering integrated content delivery and branch office routing, Cisco reduces the complexity of value-added ECDN services, while optimizing WAN bandwidth and reducing operational costs.

Having an integrated ECDN architecture simplifies deployment exercises, reduces management complexity, and lowers operational cost. Most users will see a rapid payback by minimizing the need to purchase additional WAN bandwidth and enabling new applications that take advantage of existing platforms. ▲▲

FURTHER READING

- **Content delivery networking solutions for small, medium, and large enterprises: cisco.com/en/US/netsol/ns110/ns49/ns50/networking_solutions_packages_list.html**
- **Networking solutions for small and midsized businesses: cisco.com/en/US/netsol/networking_solutions_small_medium-sized_businesses.html**

The Rise of Managed Services

Enterprise and SMB interest grows for outsourced IP VPN, IP telephony, and security services.

BY DAVID BARRY

PETER HOEY

As the North American economy slowly recovers, businesses are expressing a keen interest in further development of their e-business initiatives. According to a February 2002 Nielsen and IDC study of more than 521 information technology (IT) decision makers worldwide, more than 60 percent indicated that they plan to implement e-business solutions over the next 24 months, including workforce optimization, customer care/e-commerce, and corporate communications.

Many organizations are looking to adopt IP solutions in support of these efforts—IP virtual private networks (VPNs), security, and IP telephony ranking among the most desirable solutions by nearly half of all organizations in the study. The reasons cited were to drive down operating costs, increase functionality, and improve quality.

The IP VPN market, for example, which is the most established of the three, has had robust growth and will continue in the future, according to Steve Harris, senior analyst at IDC. Harris says that the total US IP VPN services market (including equipment rental, but not equipment sales) will grow from US$6.2 billion in 2002 to US$14.7 billion in 2006, a compound annual growth rate (CAGR) of 22 percent.

Of that market, the majority of companies—about 74 percent—are currently managing their IP Security (IPSec) customer premises equipment (CPE) in house by either upgrading a Cisco edge router with Cisco IOS® Software or using a firewall. This compares with 12.3 percent who are outsourcing the management of the CPE device and approximately 11 percent using a combination of both. However, many companies that are do-it-yourselfers are finding that self-managing VPNs has its limitations: For example, the company may need to maintain modem banks for remote-access users and build virtual circuits between sites—the complexity of each can substantially escalate as network use grows. Also, as e-commerce and e-business grows and more users have access to company networks, security no longer means a simple point-product solution. It demands a much more cohesive security policy and ongoing 24x7 monitoring and management that many companies are ill equipped to handle.

"A recent Gartner study found that 97 percent of cyber attacks exploited known security flaws for which a patch was *already known*," says Mark Bornstein, manager of service provider marketing for VPN and security solutions at Cisco. "That statistic says a lot because it indicates how formidable the challenge is. A company might decide to go ahead and make the capital

What's driving the move to managed services? Find out at cisco.com/go/packet/1518A.

investment to buy the security equipment, commit the resources to developing a detailed security policy, and test all of the point products and different testing methodologies. But if it slips in its continuous monitoring of firewall logs, intrusion detection logs, and problem tracking, and doesn't stay abreast of the latest threats, viruses, and patches that are available, all that effort and expense is for naught when an attack occurs."

> "Today, security is no longer an IT issue; it has become a business issue with high visibility at the board of directors level."
>
> —JOHN DEBACCO, DIRECTOR OF SEGMENT BUSINESS MANAGEMENT, IBM BUSINESS CONTINUITY AND RECOVERY SERVICES

Opportunity for Service Providers

In the coming years, the managed services opportunity for service providers is projected to be substantial. Gartner estimates that the total managed services market for the United States alone will grow from US$15.3 billion in 2002 to US$31.5 billion in 2006, a CAGR of 22.4 percent. And unlike before, when enterprises wanted to outsource their entire network operations, the new trend is to *out-task* only those portions of the network they do not have resources to handle.

"Out-tasking is turning over only a part of the network," says Peter Wells, director of field operations for the ILEC Group at Cisco. "The trend we see is that enterprises are focusing on their core competencies and out-tasking certain parts of their network management to fit their needs."

"This is a great opportunity for service providers to move up the value chain," Wells continues. "Managed services is about managing more than the pipe. It's also about managing the end point of the pipe—the CPE—which creates more stickiness with the customer, reduces churn, and opens the door for more professional services and higher-margin services."

Bell Canada, Canada's largest telco company, built a Multiprotocol Label Switching (MPLS) network three years ago and has offered both MPLS-based VPNs and IPSec VPNs, and has recently introduced a managed IP telephony service. "Our customers look to us for out-tasking services," says Hugh Pilkington, senior team leader, managed solutions at Bell Canada. "We take over the burden of implementing and managing IP VPNs or IP telephony. Not only do we do an assessment of their environment to be sure it's capable, but we help upgrade the environment. We do all the project management, all the testing once it's up and running, and we do proactive monitoring, call management, and performance management. This allows our customers to reassign IT staff to higher-value work such as developing important new applications, rather than managing the network."

Outlook for the Future

As profit margins on transport continue to plummet, managed services will play an ever more important role in service provider viability and profitability. According to a recent report from Gartner, "Going forward, transport bandwidth will only be as valuable as the enabling bundles of value-added services and applications that will increasingly require managed data services for efficient operation. These services and the value-added services they enable will provide the vast majority of economic margin for service providers in the future. Going forward, infrastructures cannot be viewed as only a pipe, which taps a small portion of the potential service and revenue."

THE SERVICES

Though each is in a different phase of its life cycle, IP VPNs, IP telephony, and security are promising areas for managed services in the coming years.

IP VPNs: the Enabler

While a large percentage of companies handle their own VPN management, this is expected to change in the coming years as VPN management becomes more complex and scalability becomes a larger issue. For many enterprises, managing VPNs requires a large capital outlay for equipment and ongoing commitment of human resources.

From a total-cost-of-ownership (TCO) perspective, out-tasking is advantageous because many companies can share the costs of one infrastructure, according to Wells.

"The service provider has already built out the network so it's cheaper if many enterprises or SMBs [small and midsized businesses] share it rather than build their own," explains Wells, "much like the efficiency gained from one common highway. Also, service providers can deliver a more reliable service because they've been building networks for many years and they do it 24x7."

The idea of convergence is slowly gaining currency as companies see the economic and productivity advantages of running their voice, video, and data over one network. IP VPNs lay the groundwork for that convergence by

providing a more robust WAN environment that is secure, cost-effective, and more flexible than leased lines or Frame Relay. Also, with the increasing maturity of service provider infrastructures, and as enterprises and SMBs gain confidence that service providers can deliver the levels of service they require, the growing trend will be toward using managed services.

This fact is particularly true for customers and service providers that have an MPLS network. One of the major advantages of a VPN based on MPLS is that the enterprise needs only one private connection into the service provider's network to carry voice, corporate data, and Internet traffic. With a single T1 line, for example, users can set up an employee intranet, a voice-over-IP (VoIP) network, a public Internet link, or even a partner extranet. This unification translates to significant cost savings as customers reduce the number of connections and customer premises devices.

Another key value from the service provider perspective is that an MPLS network allows easy addition of new managed applications that deliver greater value to customers while adding service revenue. Belgacom, Belgium's largest service provider, deployed an MPLS network in 2000. While the company has provided MPLS VPN site-to-site services to many corporations, its customers continued to manage their own remote access VPNs based on IPSec—but this was cumbersome and time consuming.

"Our customers wanted us to handle their remote needs for their mobile workers or teleworkers who couldn't access the corporate VPN," says Frederic Matagne, growth marketing programs line manager at Belgacom. "They were doing it themselves—managing the modem banks, procuring the circuits, installing the IPSec software on the ADSL [asymmetric DSL] routers—and it was a resource drain.

"When Cisco introduced Cisco Remote Access to MPLS VPN, we were able to go to our customers and say 'let us manage all of your teleworking and mobile workers and we'll bring them into the company VPN on our network.' Now, over an ADSL access connection, we bring the user into our MPLS cloud where they become part of the corporate VPN. This brings in new revenue while allowing us to further serve our customers and establish a stronger partnership," says Matagne.

The power of an IP VPN for service providers is that it acts as a foundation service for other advanced managed offerings, such as voice and storage. As basic IP connectivity becomes a commodity, service providers that can successfully differentiate themselves with high-margin, managed IP-based services will gain a competitive advantage. Cisco designed its multiservice VPN solutions to enable service providers to quickly offer basic IP transport and VPN services, and then take advantage of their packet-based architecture to add other value-added services over time. The ultimate effect is increased average revenue per user and increased customer loyalty.

Planning Tool for VPN Payback

Cisco has developed a new tool called the Cisco VPN Solution Payback Calculator that helps service providers determine the financial payback on a VPN investment. The graphical tool helps the service provider build a business case for deploying a Cisco VPN solution.

The user simply selects from the options available—Cisco VPN platforms used, market assumptions, monthly recurring revenues and expenses, one-time operating and capital expenses—and the calculator determines the payback period of the investment.

"More and more service providers are being asked to justify their investments in technology against profit to be gained," says Joan Zhu, business analyst from the service provider business modeling team at Cisco. "This tool is one of many ways Cisco is partnering with service providers as they develop future business models and look to deploy new services."

To obtain a copy of the Cisco VPN Solution Payback Tool, e-mail VPNPaybackTool@cisco.com.

IP Telephony: the Rise of the IP PBX

Once companies have migrated to IP VPNs, the foundation is in place to build multiservice VPNs and deliver other services including voice and video.

An area that is showing great promise for managed services is the IP PBX, an IP replacement for the traditional legacy PBX. Service providers have long provided legacy PBX platforms and support to enterprises. As the market shifts away from legacy time-division multiplexing (TDM), providing managed IP telephony services for customers deploying IP PBXs presents a natural opportunity for these providers.

"There is a strong precedent set in the TDM world for customers outsourcing the ongoing maintenance and management to a service provider," says Brian Walsh, solutions manager in Cisco Voice Systems Marketing. "They need a partner for operational support and it provides a big annuity for providers. Customers are looking for this same type of support in the IP world."

The move toward IP PBX solutions is unmistakable. According to Walsh, at the 2000 VoiceCon show all the legacy providers announced that they would not

Why would an enterprise with its own IT staff hand over management of critical network functions and technologies to a service provider? "Helping Hands" in the January/February 2003 issue of *iQ Magazine,* the Cisco publication for senior business decision makers, explores the managed services landscape, business drivers, and bottom-line benefits. To read the article or send it to your business management, visit cisco.com/go/iqmagazine/managedservices.

Find out how the Cisco *Powered* Network Program can help you define, deploy, and market new managed services at cisco.com/go/packet/1518A.

build next-generation TDM PBX platforms. Research from Allied Business Intelligence, Inc., a New York-based market researcher that specializes in emerging technologies, shows that in 2003, the value of shipments of IP PBX equipment will, for the first time, surpass the revenues generated by legacy PBXs. By 2007, manufacturers of new IP-based systems will boast revenue five times greater than that of legacy equipment in that year, the research firm adds.

The Cisco managed IP telephony solution is deployed at the customer site, where the customer environment is upgraded with Cisco CallManager (the Cisco IP PBX platform), IP phones, and quality-of-service (QoS)-enabled LAN switches and routers to support voice and video. Additionally, a gateway is provided for failover to the public switched telephone network (PSTN). The service provider sells, deploys, and provides ongoing management for the customer's IP telephony environment. The service provider can either lease or resell the CPE device to the enterprise. Management services are offered individually or in tiered bundles and are typically priced on a monthly per-user basis.

Now is an excellent time for service providers to offer managed IP telephony services, according to a recent Gartner report, *Professional Service Needs for Emerging Enterprise Networks,* by Mike Harris and Eric Goodness. According to the report, "Overall, IP telephony requires much more external assistance throughout the life cycle, including planning, deployment, and support services, than other technologies such as VPNs and WLANs [wireless LANs]. The complexity of call servers, unified messaging services, and collaboration tools outweighs the improved simplicity of plug-and-play moves, adds, and changes when it comes to relying on external providers. This is a prime opportunity for services companies to deliver comprehensive IP telephony services to enterprises that are entering the planning and evaluation stages."

This year, many of the world's largest service providers have announced managed IP telephony services, including Bell Canada, Bell South, Cable & Wireless, China Unicom, Equant, Sprint, and Verizon.

In October 2002, Sprint announced Sprint Internet Protocol (IP) Telephony Services, which provides a vehicle for customers to IP-enable their business and transition to IP-based voice services. Sprint IP Telephony Services are a combination of Sprint management, monitoring, and maintenance services for IP-based voice services, and related CPE, presented as an integrated network management service. At the heart of the service, Sprint IP Telephony Services is enabled by Cisco AVVID (Architecture for Voice, Video and Integrated Data) with Sprint Managed Network Services and transport via the Sprint 100 percent native IP network.

Sprint also offers a multiservice VPN that not only voice-enables the customer network, but also provides a private dial plan. The private dial plan ensures that IP voice calls among a company's branches are sent across the private VPN WAN rather than traverse the PSTN, which would be costly. Sprint will sell the multiservice VPN and IP telephony solutions together to provide both the VPN that is voice enabled for transport and the IP telephony call processing based on Cisco CallManager.

At Equant, offering IP telephony is a natural outgrowth of its experience managing its customers' IP LAN environments and offering IP VPNs. In February 2002, Equant announced its managed IP telephony service, which extends Equant's multiservice MPLS VPN capabilities onto corporate LANs. The offering is built on Cisco CallManager IP PBXs, Cisco Unity™ unified messaging, Cisco IP Contact Center, Cisco Catalyst® LAN switches, and Cisco multiservice WAN access routers.

"We offer a fully managed service that is aimed at customers who don't want to be hands on; they expect the IP phone on their desk to work," says Richard White, product manager for Managed LAN IP Telephony at Equant. "They don't have the technical staff to support this. We've taken our existing practice around enterprise monitoring that we've been doing for years, that is, our ability to drill into our customer's LAN environment and offer fault management on their switches and routers. We took that capability and modified it so we can offer it for IP telephony."

"We also offer a first in the industry in that we've achieved full interoperability between a network-based gatekeeper and Cisco CallManager, and this allows us to support both legacy PBXs as well as IP PBXs in the customers' network," continues White. "Also, with our MPLS-based multiservice VPN that we deliver over a customer Cisco AVVID foundation, we install and manage the customers' CPE devices and provide five classes of service [CoS]: two very high-priority COSs for voice and video each, and three for data, prioritized for mission-critical or best-effort traffic."

The newest technology for IP telephony from Cisco that is still in its early stages is called hosted IP telephony, which will allow service providers to host the call-processing function in their network and offer these services across multiple customers.

Managed Security: Strength in Numbers

When BHP, one of the world's largest and most diver-

sified natural resources companies, based in Houston, Texas, noted some unusual activity on its network, it asked its provider of security services, IBM, to look into it. IBM gathered data from the Cisco 4200 Series Intrusion Detection Sensor at BHP's site and, after entering the data into IBM's Zurich Correlation Engine that correlated the data with suspicious activity on other customer networks and industry alerts, determined that an attack was about to occur.

"IBM called it a 'slow attack,' which meant it didn't come up on the radar screen right away," says Jim Kates, US lead for information security at BHP. "This gave them time to alert us and tell us what to do about it, which was only possible because IBM was able to co-relate what was happening on our network with data from other networks. If we hadn't had this service, we might not have known until after the attack had been publicized or had happened."

BHP and IBM's success in thwarting this attack is an excellent example of the value of managed security services. As the challenge and complexity of securing a network grows, many enterprises and SMBs are looking to service providers and managed service security providers to provide them with reliable, comprehensive services. An entire gamut of new concerns, from the growing importance of e-business to greater exposure due to increased Internet and remote access use, to rapidly changing technology and continuously morphing hacker capabilities, have changed the playing field for security services.

"Today, security is no longer an IT issue; it has become a business issue with high visibility at the board of directors level," says John DeBacco, director of segment business management for IBM Business Continuity and Recovery Services. "Point products aren't sufficient in this new environment. Companies come to IBM because they're looking for a comprehensive security service. Sometimes they're not completely aware of where their exposure is. We offer a total end-to-end security solution, from assessment to security policy creation to incident management, vulnerability testing, intrusion detection, firewall services, and virus scanning."

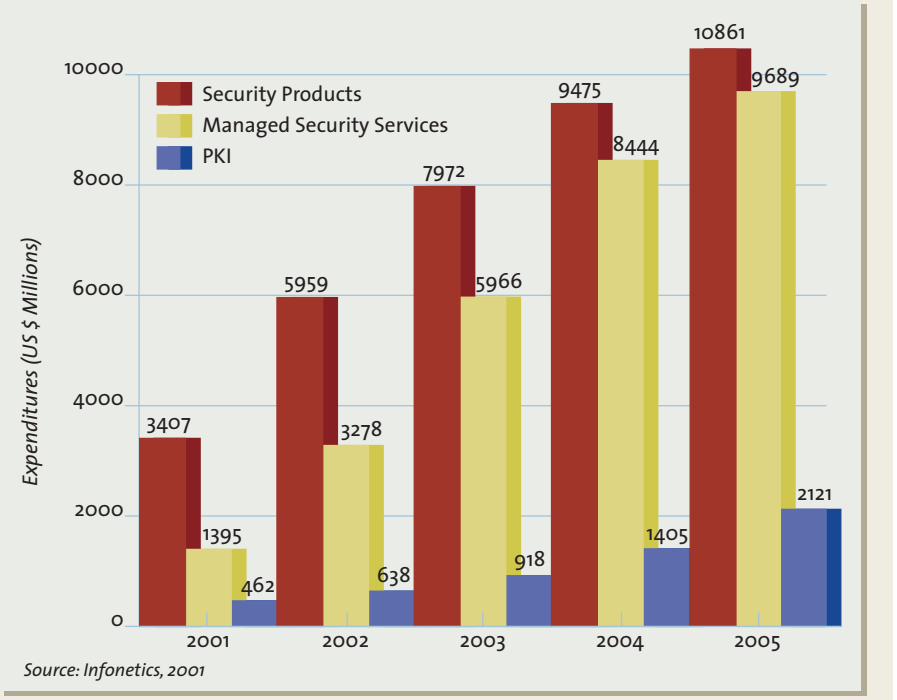
Cisco provides several security solutions that enable service providers to offer managed security services to their customers. These include VPN solutions, firewalls, intrusion detection systems, access control servers, secure scanners, security consulting services, security training, and a full suite of security management tools. (See the security feature articles in this issue of *Packet*®, starting on page 22.)

As part of its managed security services, IBM uses Cisco PIX® firewalls and the Cisco 4200 intrusion detection sensors, and monitors customer sites that are located anywhere in the world. According to John Suehr, segment executive, managed security services at IBM, the quality of Cisco's security solutions has been instrumental in IBM's ability to offer the best service to its customers.

"We love Cisco because nobody has done a better job of providing the full range of CVE [common vulnerability and exposures] values right in the signatures that are part of the sensors of the Cisco 4200 intrusion detection software," says Suehr. "This allows us to match intrusion detection with our vulnerability testing. Because of Cisco, we've been able to co-relate our two services like we did with BHP and make determinations that a customer might not be able to do by itself."

"Cisco's value to us goes beyond the quality of the products," continues Suehr. "We have the highest level of maintenance available from Cisco—a four-hour maintenance service globally—which is outstanding. Our customers are Cisco customers and they expect the best. And we can offer it because of Cisco and there are very few companies that can offer that reach." ▲▲

WORLDWIDE SECURITY SERVICES EXPENDITURES 2001-2005



Source: Infonetics, 2001

SECURE FUTURE: As the world races to build secure internetworks, the security industry will see marked growth, especially in the area of managed security services.

Metro Ethernet: More for Less

Service providers worldwide see Ethernet as a sustainable alternative access technology.

BY DAVID BARRY

Tens of thousands of businesses and residences in Italy are currently enjoying a revolutionary 10-Mbit/s connection to the Internet thanks to metro Ethernet. But the technology is enabling much more than high bandwidth. Customers can receive a wide range of broadcast TV channels, videos on demand, and unlimited voice service anywhere in Italy—all at a cheaper price than they were paying for more basic voice services and slower access speeds.

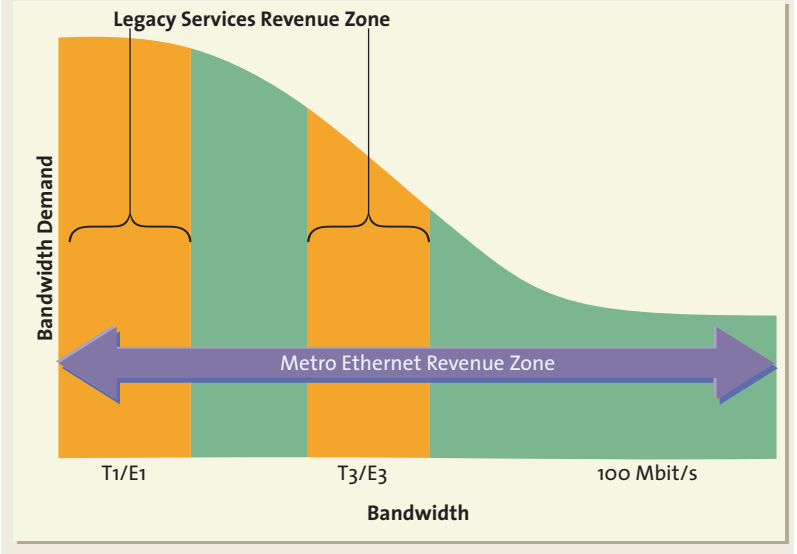
In short, metro Ethernet is allowing savvy service providers, such as FastWeb in Italy, to deliver faster and richer services for a cheaper price than offered by traditional providers.

FastWeb (www.fastweb.it), a subsidiary of e.Biscom (Milan's Nuovo Mercato: EBI) that was founded only three years ago, has had striking success in Italy and is rapidly gaining new customers, having already reached operational profit break-even ahead of schedule in just over two years of commercial operations. With only 76,700 customers at the end of March 2002, that number skyrocketed to more than 130,000 subscribers by the end of the third calendar quarter of 2002 and is projected to reach a combined figure of nearly one-quarter million subscribers in its Italian and German operations by the end of the year.

"The marketing proposition was 'sign with us and you will have more for the same price,' " says Alberto Trondoli, chief technology officer at FastWeb. "A family can get voice service, 10 Mbit/s Internet access, hundreds of videos on demand, and multichannel television from us for less than the price that they are paying their traditional service provider for basic voice and slower data access speeds."

BANDWIDTH TO ORDER: With metro Ethernet, business customers are free to increase bandwidth quickly and cost effectively, in 1-Mbit/s increments or less, thus expanding revenue opportunities for service providers.

METRO ETHERNET—EXPANDING THE REVENUE ZONE



The Beauty of Ethernet

Ethernet is changing the face of metro environments, from Asia to Europe to the US, and creating radical new sales opportunities for service providers in both residential and business markets. "The beauty of Ethernet is that you can run fiber to a multidwelling unit and then potentially get access to all the customers in that building with one truck roll," says Bernard Lamy, metro Ethernet product marketing manager for Cisco in Europe, the Middle East, and Africa (EMEA). "Once a service provider has brought fiber into a switch in a building basement, it can use a variety of Ethernet-based access technologies, such as fiber, copper, or wireless, to connect customers at 10 Mbit/s in the *last yard*."

For businesses, metro Ethernet uses the ubiquitous Ethernet customer interface, thus taking advantage of the prevalence of enterprise Ethernet installations. This well-known LAN technology can be used on a standalone basis or to access existing network services such as the Internet or Frame Relay and ATM networks. It can be provisioned on SONET/SDH, wavelength-division multiplexing (WDM), native fiber, or across Dynamic Packet Transport (DPT) networks.

As a control plane, metro Ethernet can use Multiprotocol Label Switching (MPLS), Layer 2 Tunneling Protocol version 3 (L2TPv3), IP, and IEEE 802.1Q tunneling. A standard method of tunneling one set of virtual LAN (VLAN) tags inside another, 802.1Q tunneling enables compatibility between a service provider's network and an enterprise customer in situations where both use different VLAN implementations.

Ethernet offers powerful benefits over traditional transport services such as private lines, Frame Relay, or ATM. Metro Ethernet is much more flexible than Frame Relay or ATM. For example, business customers can increase bandwidth in 1-Mbit/s increments or less, from 10 Mbit/s all the way up to 1 Gbit/s across the same physical port. With Frame Relay or ATM, customers can make changes only in huge increments, from T1/E1 to T3/E3 to OC-3/STM-1—bandwidth that they may not need. Metro Ethernet allows service providers to target a wider variety of customers with services that are tailored and priced right for each individual account.

In addition, upgrading ATM or Frame Relay bandwidth entails installing a new physical port for each speed, which requires the service provider to send technicians to each customer for the upgrade. This is time consuming, and provisioning can often take up to 90 days. Ethernet bandwidth, in contrast, can be upgraded remotely, using Cisco IOS® Software, in a matter of minutes. This alternative not only reduces service provider operating costs, but it also means quicker time to billing and revenue.

Metro Ethernet Networks Are Worldwide

While SONET/SDH is still the primary form of transport, many service providers worldwide are embracing metro Ethernet as an efficient, economical and potentially profitable transport alternative. Ethernet to the MxU (multidwelling and multitenant units), also referred to as ETTx, offers a rapid return on investment for providing innovative broadband services to consumers and to small or medium business customers.

FastWeb, which operates in Milan, Rome, Genoa, Turin, Bologna, and Naples, installed Cisco 12000 Series Internet routers in the network core, and uses Cisco Catalyst® 6000 Series switches for optical connections to what can best be described as "miniPOPs." These POPs are in residential areas and serve nearby buildings directly. FastWeb lays fiber-optic rings from the miniPOP to Cisco Catalyst 3524 and 2950 switches—one switch in the basement of each building. Fiber is then run inside the building to each apartment.

FastWeb provides a Home Access Gateway in each residence for broadband connections. Analog phones can be connected directly into the gateway, which immediately converts the traffic to voice over IP (VoIP), where it is then transferred as packets across the network. An IP phone can also be plugged into the gateway. As packetized data, the voice traffic consumes a fraction of the bandwidth required for a 64-Kbit/s analog call.

Cisco Enhances Metro Ethernet Switching Portfolio

Cisco recently introduced several important metro Ethernet switching enhancements:

- **Improved redundancy/resilience of Cisco Catalyst 4500 Series switches**
  Combining 1+1 redundancy of supervisor cards and power supplies with a redundant switching fabric helps provide a highly available platform for metro aggregation and high-density access.
- **New IP Multicast features**
  Enhancements to IP Multicast are important to cope with serving video to the large number of subscribers in the metro. Enhancements include improved video security in Cisco IOS® Software via Internet Group Management Protocol (IGMP) filtering for increased privacy of IP Multicast and unicast video streams.
- **Cost-effective Layer 3 VPN services**
  New high-performance IP routing enhancements to the Catalyst 3550 Series switches allow service providers to deliver cost-effective Layer 3 VPN services for businesses. Enhancements such as Border Gateway Protocol (BGP) and Multi-VRF-CE make it possible to serve multiple VPN customers securely from a single switch in building basements via shared fiber runs.
- **New Ethernet-to-ATM Layer 2 service interworking capabilities**
  Available on the Cisco 7600 Series Router and the Catalyst 6500 Series Switch, the new features enable these platforms to aggregate traditional WAN connectivity services while offering new Ethernet connectivity in the same platform.

The Home Access Gateway also provides a wide range of channels of broadcast TV through Cisco IP multicast. Video on demand is provided over the same connection through unicast. FastWeb has already signed deals for content with major US film studios such as Universal Studios, Fox Home Entertainment (formerly Twentieth Century Fox), and Dreamworks to create an enormous video library. Subscribers select a movie via the onscreen Electronic Program Guide, and can stop the movie, rewind, or fast forward just like they would with a video or DVD—except there is no need to return the movie to a store. FastWeb customers can also log on to the FastWeb portal from any Web browser to record a TV program for later playback, thanks to the VideoRec service.

"A family can get voice service, 10 Mbit/s Internet access, hundreds of videos on demand, and multichannel television from us for less than the price that they are paying their traditional service provider for basic voice and slower data access speeds."

—ALBERTO TRONDOLI,
CHIEF TECHNOLOGY OFFICER, FASTWEB

MANs and MDUs

Enterprise Networks in Korea (formerly GNG Networks) is building an optical metropolitan-area network (MAN) along the subway networks of six major Korean cities, including Seoul, and plans to offer metro Ethernet to businesses. Enterprise Networks is using Cisco 15454 optical platforms with four-port gigabit carrier-class Ethernet cards running across dense wavelength-division multiplexing (DWDM) metro networks. Cisco Catalyst 6506 and 6509 Series switches will be located in the POPs and will connect to Catalyst 3500 and 3550 Series switches in nearby businesses to deliver high-bandwidth IP virtual private networks (IP VPNs) and IP-based storage over low-cost Ethernet.

In Sweden, B2 Bredband AB (B2), one of Sweden's leading service providers, has built a metro Ethernet network and is targeting residential multidwelling units (MDUs). B2 has leased capacity for its core IP network and MAN from local transportation suppliers to power 36 city POPs, and is using Cisco's ETTx solution to reach residential buildings. After a building is lit, B2 only needs to provide subscribers with a network card, connection cable, and a self-installation program to begin service. Each subscriber gets a two-way, 10-Mbit/s Internet connection for around US$30 per month. B2's competitors provide 512 Kbit/s (or roughly 0.5 Mbit/s) over DSL or cable for a monthly charge also of about US$30. Users are delighted with the service, according to a survey conducted by Sweden's *Internet World* magazine, which reported that 83 percent of respondents said they were either satisfied or very satisfied with the service. Users cited high speed and reliability, low installation and monthly fees, and lack of need for a modem as critical success factors.

Metro Ethernet Coexists with Traditional WAN Services

Metro Ethernet switching can also be combined with other traditional WAN services for customers who may still rely on Frame Relay or ATM services. For example, many customers have branch and regional offices that are well-served by time-division multiplexing (TDM), Frame Relay, or ATM service at T1/E1 speeds or less, but face bandwidth constraints in WAN connections to their headquarters. And it can be expensive and time consuming to upgrade those headquarters links from T1/E1 to T3/E3, or from T3/E3 to OC-3/ STM-1.

Any Transport over Multiprotocol Label Switching (AToM) is the Cisco solution for transporting Layer 2 packets over an IP/Multiprotocol Label Switching (IP/MPLS) backbone. AToM enables enterprise customers to upgrade their corporate WAN router to an Ethernet connection while still maintaining their investment in ATM or Frame Relay at the branch office. In addition, this solution allows service providers to offer enhanced bandwidth services while still maintaining their investments in existing WAN technologies.

Such enhancements mean that service providers can protect their investments in existing ATM, Frame Relay, and TDM infrastructures—and revenues—by seamlessly interconnecting them with metro Ethernet services. By using the same network equipment platform for metro Ethernet and traditional services, service providers can achieve greater efficiencies in equipment management, provisioning, and service assurance. ▲▲

Small AND Midsized BUSINESSES

Call for VoIP and Data

CallTower customers avoid upfront capital costs, ongoing maintenance, and multiple vendors with one integrated IP network service for telephony and data.

BY GENE KNAUER

San Francisco-based managed services provider CallTower (calltower.com) is attracting a growing clientele of small to midsized businesses (SMBs) with its integrated IP telephony and data services, which offer clear cost benefits, painless scalability, and an array of features that help promote mobility and efficiency. A Cisco *Powered* Network, CallTower is working cooperatively with Cisco to demonstrate that the hosted IP telephony model offers real advantages over the choice of an in-house, proprietary private branch exchange (PBX) and separate data network.

Managed IP Telephony/Data Services Catch On

A few years ago, small to midsized companies had few options in setting up their phone systems. They could choose a proprietary PBX that integrated call processing and voice mail and sign up for local and long-distance plans with carriers. Then they had to train their own dedicated support personnel to manage the PBX and phones. But today, managed service providers like CallTower bring the feature-rich, cost-effective option of IP telephony to every desk and mobile IP device within a company. Prospective CallTower customers are asked to compare an integrated single network service to buying and managing a PBX in-house, maintaining a separate data network, and maintaining relationships with up to 10 separate vendors for telephony, voice mail, e-mail, Internet access, paging, and other applications.

"For our 25-person company, it didn't make sense to make a [US] $20,000 to $30,000 investment in phone equipment and take on the level of technical support required if we brought it all in-house," says Pam Galligan, director of technology and infrastructure at Alpha Omega Pain Medicine, a specialized medical practice on the San Francisco Peninsula. Originally started on the Stanford University campus by professors and staff at the medical school, the company began searching for a communications solution before moving to new offices off campus.

"Typically, we approach companies that are experiencing an impending event such as moving offices because they are growing or shrinking," says CallTower director of sales Bob Barnes. "It's an opportunity for them to reevaluate their communications infrastructure."

Barnes and his team evaluate a prospect's call logs, long-distance service, and Internet services to determine the total current cost of these features. Also considered are the costs in-house to maintain voice and data infrastructures. CallTower can then confidently demonstrate not only upfront savings on capital costs—if newer or larger systems must be purchased to support growing numbers of employees—but monthly savings from reduced maintenance costs and toll charges.

Multiple Advantages for SMBs

When semiconductor manufacturer Bermai outgrew its first office in Palo Alto, California—where six phone lines inadequately served 20 people—vice president of finance and administration Harvard Sung needed to

find a better infrastructure for both the new location and the company's other site in Minnetonka, Minnesota.

"In Palo Alto, the phone infrastructure is a challenge because the buildings are very old," says Sung. "The wiring is faulty. Getting phone engineers in to do the work was going to be very expensive and we were limited by how many phone lines we could install."

Yet the company originally planned to go ahead and buy and maintain a traditional phone system. Sung and his colleagues paid a visit to the Cisco Executive Briefing Center (EBC) in San Jose and discovered how an integrated IP telephony and data network could provide huge benefits. Choosing a provider such as CallTower further eliminated prohibitive upfront capital equipment costs and ongoing training and manpower requirements.

For a list of managed services providers that have earned the Cisco *Powered* Network designation, visit cisco.com/warp/public/779/servpro/cpn/.

"There are no long-distance charges anymore," says Sung. "And because we're on the same network as our Minnesota office, we can use four-digit extensions from anywhere. Employees who travel frequently between the facilities use the unified messaging service, which lets them check their voice mail and faxes through their e-mail inboxes."

CallTower customers on the move also like the "Find-Me-Follow-Me" feature, a Cisco CallManager service that attempts to track down called individuals by systematically dialing the telephone numbers in their user profile if the first number called is unanswered.

"Many of our staff are highly mobile," says Pam Galligan of Alpha Omega. "Doctors can open their laptops and see all of their voice, e-mail, and fax messages in their Microsoft Outlook inboxes. And they can get important calls routed right to their cell phones via the Find-Me-Follow-Me feature."

"The convenience of creating a sense of a virtual environment for our five offices in California and Washington State is a great benefit," says Ken Zimmerman, chief financial officer at Arcadian Management Services, headquartered in Oakland, California. The company provides nurses, administrators, and back-office functions for Individual Provider Association (IPA) medical groups. "The ability to expand with the system as we grow, without having to buy new equipment or change systems, is another big plus."

"The convenience of creating a sense of a virtual environment for our five offices in California and Washington State is a great benefit. The ability to expand with the system as we grow, without having to buy new equipment or change systems, is a big plus."

—KEN ZIMMERMAN, CHIEF FINANCIAL OFFICER, ARCADIAN MANAGEMENT SERVICES

Arcadian first tested the CallTower service at the corporate headquarters in Oakland and another office in Tacoma, Washington. At the time, the company had separate phone systems for each office. Calls couldn't be transferred to other Arcadian offices. And staff in the field had to rely on separate cellular, pager, and fax connections.

"Most of us are not using the most sophisticated features for mobile users, but we are very pleased with the ease of use of the IP phones," says Zimmerman. "They give each one of our 83 users personalized, dedicated features and generally speed up communications within the company. Using a single vendor for everything has also greatly simplified things administratively."

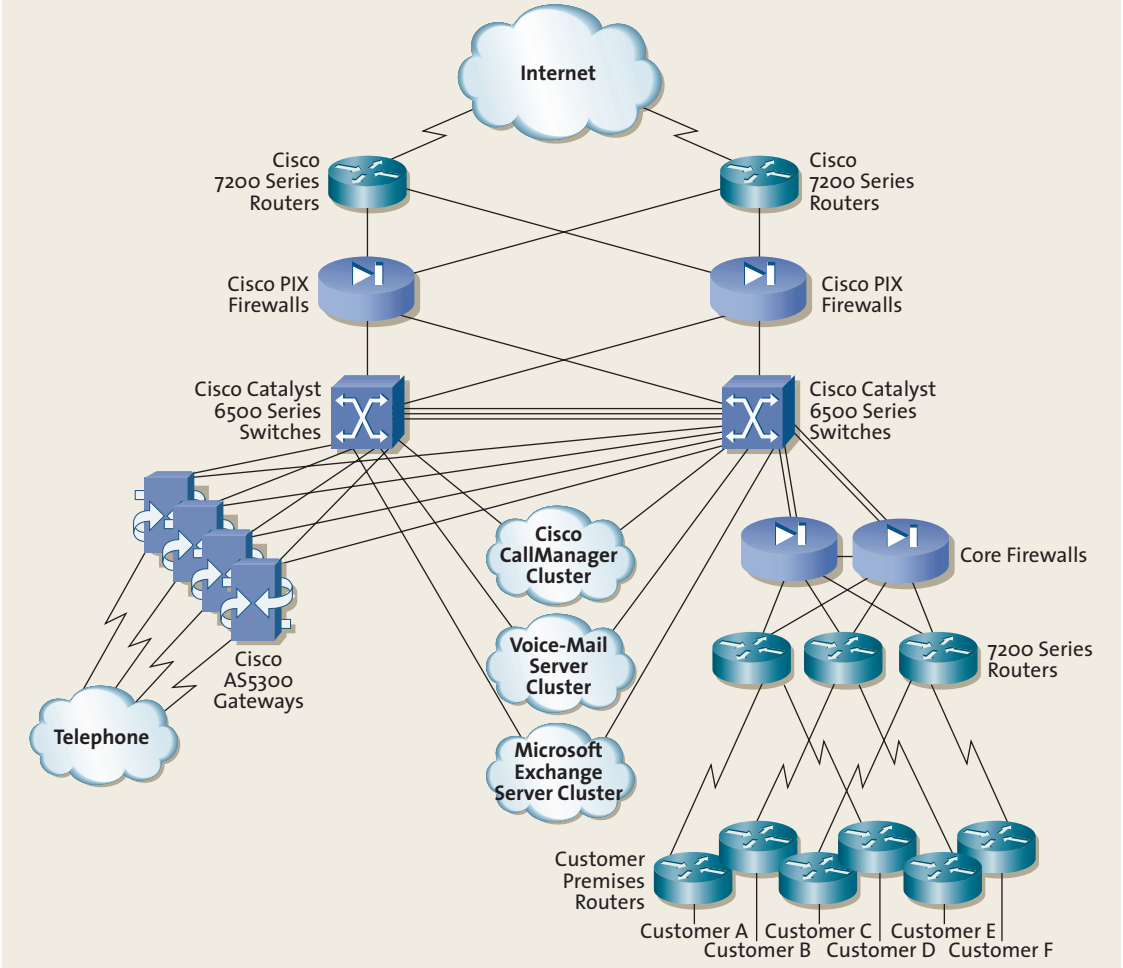
Cisco AVVID Infrastructure

Each CallTower customer site has a T1 line or multiple T1s, one or more Cisco 2600 Series routers providing IP telephony, Cisco Catalyst® 3534 or 4006 Series switches with inline power for data traffic, and a Cisco 7960 IP Phone for each user. As a Cisco *Powered* Network provider, CallTower has a 100 percent Cisco infrastructure. IP telephony, messaging, and networking services are integrated and securely managed on the same network through the power of Multiprotocol Label Switching (MPLS) technology. CallTower provides services for local and long-distance calling, Internet access, and data services over a WAN to its customers through a mix of local, regional, national, and international telecommunications partners.

Cisco CallManager is the software-based call-processing component of the Cisco IP telephony solution, which is part of Cisco AVVID (Architecture for Voice, Video and Integrated Data).

The software extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. It also offers unified messaging and integration of other features through standard application programming interfaces (APIs). The Microsoft Exchange server is used to

CALLTOWER DATA CENTER



ALL CISCO NETWORK: CallTower's infrastructure comprises Cisco Catalyst 6500 Series core switches, Cisco AS5300 gateways to the public switched telephone networks (PSTN), Cisco PIX® firewalls for security, and Cisco load balancers behind Cisco 7200 Series routers that connect the customer sites to the Internet.

manage customer e-mail traffic, multiuser calendaring, and task management applications.

Customers sign up for the CallTower service much as they would with a cellular provider, based on a number of minutes of calling for the US per seat per month. Minutes not used by one caller are averaged into the entire company's usage for the month. Any overages for the entire aggregate of users are billed separately, as are call tariffs on international calls. Domestic long-distance charges are a thing of the past.

The company delivers a T1 from one of its partner providers within a few weeks. Then the customer premises routers and phones are preconfigured and can be installed within a day. Once turned on, each IP phone can be moved to any office on the network and plugged in without any reconfiguration necessary.

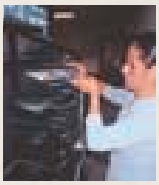
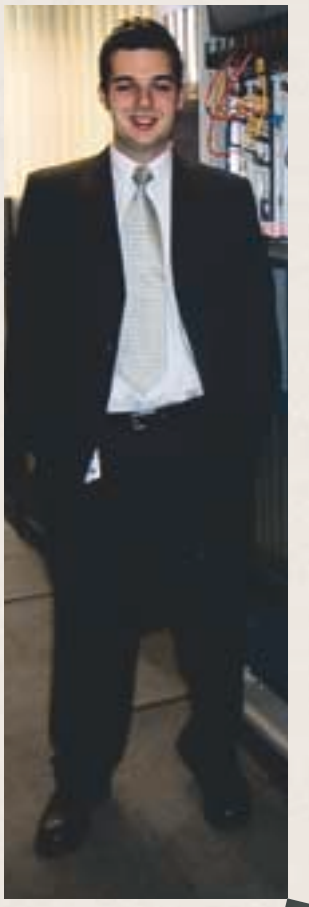
"We know we'll be moving again in 2003," says Bermai's Harvard Sung, "and we'll be able to pick these routers and phones up, set up a new T1, and go. We have 40 staff and we could easily double that without any problem with CallTower." ▲▲

FURTHER READING

- **SMB networking solutions: cisco.com/en/US/netsol/networking_solutions_small_medium-sized_businesses.html**
- **Cisco benchmarking tool: compare your company's technology adoption with other SMBs: cisco.com/warp/public/779/smbiz/resource_net/tools/benchmark/**
- **Cisco Executive Briefing Center (EBC): cisco.com/en/US/about/ac156/about_cisco_executive_briefing_center.html**

Most Likely to Succeed

CLASS of 2003



Clockwise from top left:
Christian Caramida, Romania;
Norma Carrillo Rangel, Mexico;
David Weinberg, Australia;
Aingara Paramakuru, Canada
Khor Kean Hock, Singapore;
Patricia McCormick, Canada;
Ahmed Zohdi, UK.

Below: Beth Murora, Rwanda

THE INTERNET AND EDUCATION ARE becoming the great equalizers among people and countries, eliminating barriers of socioeconomic status. The Cisco Networking Academy™ Program is providing students worldwide with the Internet technology skills essential in a global economy. Now in 149 countries, the program is offered in more than 10,150 academies and has produced more than 296,000 graduates. These men and women, and their employers, credit the training they received through the Cisco Networking Academy Program with benefiting their careers, their companies, and even their countries' economic prospects.

Hot HIRES

Cisco Networking Academy graduates launch careers around the globe.

By **RHONDA RAIDER**

Launching Careers

In Romania, the Cisco Networking Academy Program has become a vital component of the nation's technology resurgence. In 1997, a 17-year-old Romanian student, Cristian Caramida, entered the Networking Academy program at his high school. Now he's regarded as one of the select few top networking engineers in his country, and has earned CCNA®, CCNP®, and CCIE® certifications from Cisco.

Caramida especially appreciated the hands-on nature of the Academy program—a hefty 40 percent of the curriculum. "You learn how to cable a router and how to enter commands—skills you can use straight away," he says. For his first major employer, a large Internet service provider (ISP) in Bucharest, Caramida installed the first ATM/asymmetric DSL (ADSL) network in Eastern Europe. After that, he spent a period with Yellow Pages, the online telephone directory, gaining networking experience from an enterprise perspective. Next, he moved back into the ISP world, this time with a satellite provider. In 2001, Caramida joined his current employer, KPNQwest. As an IP network operation center specialist, he maintains the network, and works in sales support, helping propose solutions for customers. Recently, Caramida developed a new service management application that collects metrics from networking equipment and organizes it into customer-focused management information. According to Caramida's boss, KPNQwest country manager Marius Panait, "Cristian built this application from start to finish, which required detailed knowledge of both Cisco networking and UNIX. When we looked at his qualifications, the Cisco accreditations told us that he had the solid knowledge to back up his experience and proved that he takes the subject seriously."

Theory and Practice

In Melbourne, Australia, David Weinberg, age 25, parlayed his Cisco Networking Academy training into a coveted network designer position with telecommunications giant Telstra. As an undergraduate, Weinberg studied biomedical engineering. Realizing his true interest was networking, he returned to Swinburne University in Melbourne and earned a Master of Science Degree in Network Systems. "The major reason I chose Swinburne University was that its curriculum included the Cisco Networking Academy Program," he says. "It teaches not only the

theory of networking but also provides hands-on experience through weekly labs. After completing the program, I felt competent working with routers and switches in a work environment."

Weinberg is often asked to contribute to the network designs of his peers, largely because of the knowledge he gained from the program, including advanced routing concepts such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF), switching concepts such as IEEE 802.1Q and Inter-Switch Link (ISL), and security concepts such as access lists, lock and key, and reflective access control lists (ACLs). "David's CCNP skills have greatly contributed to making him a valuable member of the professional design team," says Hans Chhabra, IT team manager at Telstra. "When it comes to selecting networking products for our customers, you need an in-depth understanding of various products and interface capabilities. David possesses that understanding. I consider a CCNA a prerequisite for anyone starting work on my team."

Weinberg plans to pursue his CCIE certification. "I am finding that the detail provided in the Cisco Networking Academy Program has prepared me to pick up new concepts quickly," he says.

Rebuilding an Economy

Cisco's Least Developed Countries (LDC) initiative has brought the Networking Academy program to 32 of the world's 49 LDCs. Among the beneficiaries are Beth Murora and her country, Rwanda. Murora attended the Cisco Networking Academy Program in Addis Ababa, Ethiopia, nearly 1000 miles away from her home. She was 27 at the time, a program officer with the National Rwandan Ministry of Women's Affairs—and six months pregnant with twins. Even so, when Murora was offered a full residential scholarship for a Networking Academy program pilot project sponsored by Cisco, the United Nations Economic Commission for Africa (UNECA), and the World Bank's Information for Development Program (InfoDev), she heeded the call. "I could not pass up this opportunity, which would help me to help other women in Rwanda to develop technical skills and become employed," she says. Murora is applying her training to establish an Information Communication Technology (ICT) department in her ministry, which will promote IT to every government organization and present it as a career option for women. Women currently represent 70 percent of Rwanda's population. Now Murora is meeting with community leaders to explain the value of ICT in meeting their needs. The next phase will be to implement LANs for these organizations, and every LAN will represent new jobs. "The women of Rwanda must be able to earn a living and support their children," says Murora. "I intend to use the knowledge gained through the Cisco Networking Academy to help raise women out of poverty with the technical training to run organizations and develop businesses."

> "By supplementing technical skills with skills such as problem-solving and teamwork, the Networking Academy curriculum provides its students with competencies, skills, and personal qualities needed to succeed in the high-performance workplace."
>
> —JULIE KAMINKOW, EDUCATION MARKET ANALYST, CISCO

Career Enrichment

For Patricia McCormick of Nova Scotia, Canada, the Cisco Networking Academy she attended at Nova Scotia Community College last year added a new dimension to her existing job as a librarian for Eastern Counties Regional Library. McCormick already had 14 years of job experience, a Bachelor of Science Degree in Mathematics, and a Master of Library and Information Science Degree—but the field had changed.

"There still exists the stereotypical view of libraries as warehouses of books, where women in sensible shoes peer over horn-rimmed glasses," she says. "But in reality, Internet access, online catalogs, and electronic databases have become key components to library services. As a result, there is a high-demand for librarians with training in information technology. It was this realization that led me to the Cisco Networking Academy. The labs were excellent at providing hands-on experience in wiring, configuring routers and switches, and troubleshooting networking problems."

According to McCormick's employer, Dave Cumby, acting chief executive officer of the Eastern Counties Regional Library, "Even in the three months since Patricia has joined us on a one-year Systems Librarian contract, she has demonstrated excellent training and a high-level expertise with TCP/IP as well as other Ethernet protocols such as SPX/IPX [Novell Sequence Packet Exchange/Internetwork Packet Exchange] and DLC [Data Link Control]. Credit goes to her Nova Scotia Community College and Cisco Networking Academy courses."

Hands-On Curriculum

The hands-on emphasis of the Cisco Networking Academy curriculum garners widespread praise from both graduates and their employers. Aingara Paramakuru of Toronto, Canada, credits the program's practical focus with helping him obtain a help-desk internship at Maple Leaf Sports & Entertainment Ltd. "Not only was I able to gain the theoretical knowledge from the CCNA curriculum, I was also able to apply that knowledge through the practical labs," he says. Using the advanced equipment in the Networking Academy labs, Paramakuru was even able to perform labs outside of the

scope of the CCNA program, such as WAN emulation using the ADTRAN Atlas 550. Paramakuru's employer put him to work immediately. "In a short time, Aingara has brought exceptional value to our organization through his contributions to our helpdesk and networking operations," says David Huang, IT manager for Maple Leaf Sports and Entertainment. Among Paramakuru's achievements is configuring a redundant WAN (point-to-point serial and 56K Frame Relay links) connection on a Cisco router. "I was the only one qualified to configure the device, having previously configured Frame Relay in a back-to-back router configuration (Frame Relay emulation) as well as through a Frame Relay switch," he says. "My previous applications of Frame Relay concepts allowed me to configure the device quickly and ensure optimal functionality."

New Career Paths

Some graduates of the Cisco Networking Academy have used the program to transition to networking from other fields. Take Khor Kean Hock of Singapore. At 38, he was dissatisfied with his job as coordinator for a shipping company. He decided to pursue his dream of working in technology by enrolling in the Cisco Networking Academy Program through Singapore's National Trade Union Congress (NTUC). To accommodate his full-time job, Khor attended classes three nights a week and spent the other nights studying for the CCNA exam, which he passed on the first try. His efforts paid off when he secured a job as a network engineer with a Singapore computer company, where his main responsibility was network troubleshooting for his company's clients. In October 2002, Khor joined the IT department of Pan Pacific Hotels and Resorts as corporate systems manager. In his new position he's charged with maintaining a high-quality IT environment for all users in the corporate offices and recommending software and hardware for corporate offices and hotels. In his first month he had already switched over his employer's domain name and set up a main server. "Many people are familiar with networks, but fewer people know how to configure routers," says Khor. "This skill makes me valuable." Adds his employer, Rex Demanser, "We are very reliant on Khor's expertise. He is extremely patient when teaching our team how to maximize our IT resources and has provided invaluable advice in ensuring that our systems are operational and secure." Continues Demanser, "Khor will be involved in helping us integrate our data from a variety of systems within Pan Pacific. This will ensure that we have consolidated information and data across the counties in which we operate."

Like Khor, Ahmed Zohdi of London, UK, enrolled in the Networking Academy program to make a radical career change—in his case, from catering to technology. Zohdi studied at the Academy at Westminster Kingsway College in London. Logging on from home while he continued working in the restaurant business full time, Zohdi managed to complete both semesters of the course in just six months. Upon graduation he landed a network engineer position with the Bank of America. According to his manager at Bank of America, Simon Legg, "When I tested Ahmed's networking knowledge, he passed with flying colors. My test is designed to sort out the people who've just passed an exam from those who've worked with the products and really understand them. Ahmed was definitely in the second category."

Student Becomes Teacher

Across the globe from Zohdi, in Mexico, Norma Carrillo Rangel attended the Cisco Networking Academy at University of Tamaulipas, Tampico campus, when she was 21. Upon graduation, she was offered a position at the university as the project leader for the Excellence Center, where her responsibilities include providing networking support and proposing designs for the center's structured cabling system. For the latter project, she relied on the training she received in the Fundamentals of Voice and Cabling course offered by Panduit Latinoamerica as part of the Cisco Networking Academy Program. Rangel's chief accomplishments to date include participating in the reconstruction of the University's LAN and construction of the Cisco Networking Academy laboratory. She's come full circle, now teaching the CCNA course at the Academy.

Evolving Curriculum

To ensure its graduates continue to meet the needs of industry, Cisco has expanded the Networking Academy program to include optional, partner-sponsored courses by IT industry leaders in the Fundamentals of UNIX, sponsored by Sun Microsystems; the Fundamentals of Web Design, sponsored by Adobe Systems; the Fundamentals of Voice and Data Cabling, sponsored by Panduit; and IT Essentials sponsored by Hewlett-Packard. All courses are delivered through the Cisco Networking Academy Program.

With a nod to a changing workplace, the program also now includes essential "soft skills" identified by the US Department of Labor Secretary's Commission on Achieving Necessary Skills (SCANS). Says Julie Kaminkow, education market analyst at Cisco, "By supplementing technical skills with skills such as problem-solving and teamwork, the Cisco Networking Academy curriculum provides its students with competencies, skills, and personal qualities needed to succeed in the high-performance workplace." ▲▲

FURTHER READING

- **Cisco Networking Academy Program: cisco.netacad.net**

Technically Speaking

New IEEE 802.1w/1s Protocols

BY CHIARA REGALE

A robust, reliable network needs to transfer traffic efficiently, providing redundancy and recovering quickly from faults. In a Layer 3 environment, routing protocols can track redundant routes to the destination, quickly identify a secondary path if the primary path fails, and load share the traffic across multiple paths. In a Layer 2 network, routing protocols are not available. To address this problem, the IEEE developed the 802.1D Spanning-Tree Protocol (STP), which is responsible for building a loop-free logical forwarding topology from a meshed physical topology, while providing connectivity to all nodes. If a link fails, the algorithm typically recovers within 50 seconds [convergence time = (2 x Forward_Delay) + Max_Age], greatly exceeding stringent network availability requirements. Cisco has enhanced and accelerated the convergence time of the original IEEE 802.1D specifications with features such as Portfast, Uplinkfast, and Backbonefast. But these mechanisms are proprietary and need additional configuration.

The IEEE and Cisco have approached Spanning Tree and virtual LAN (VLAN) interaction differently. The IEEE proposal specifies a single, loop-free topology shared by all the VLANs, while Cisco Per VLAN Spanning Tree+ (PVST+) builds a different logical topology for each VLAN. The IEEE protocol is scalable from a computational overhead standpoint, but the traffic for different VLANs is not balanced across redundant links. Cisco PVST+ allows load balancing by having different forwarding links per VLAN, but it is less scalable (CPU time is required to process bridge protocol data units, or BPDUs, for each VLAN). Cisco overcame this limitation with *Multi-Instance Spanning-Tree Protocol (MISTP),* which couples a single spanning tree with a set of VLANs. To address convergence and scalability limitations, the IEEE developed two new standards: *Rapid Spanning-Tree Protocol (RSTP),* defined in IEEE 802.1w, and *Multiple Spanning Trees (MST),* defined in IEEE 802.1s. RSTP achieves faster convergence by relying on an active bridge-to-bridge handshake mechanism instead of depending on timers specified by the root bridge as in 802.1D. After a port receives the agreement in reply of a proposal sent earlier, it immediately transitions into forwarding. This handshake propagates quickly toward the edge of the network and restores connectivity after a topology change.

Other new concepts in RSTP include clear difference between port states and port roles, new BPDU format (to encode the role and state of port originating BPDUs for handling the proposal/agreement mechanism), port fast aging of the protocol information, BPDUs originated every "hello time" by each bridge, and rapid transition of a port into forwarding state without reliance on any timer configuration. RSTP maintains most of 802.1D parameters and terminology and can interoperate with legacy STPs. However, the inherent fast convergence benefits of 802.1D are lost when interacting with legacy bridges.

MST, inspired by Cisco MISTP, improves RSTP scalability by aggregating a number of VLAN-based spanning trees into distinct instances, and by running only one (rapid) spanning tree per instance. To determine the VLAN-instance association, 802.1s introduces the concept of MST regions. Each switch running MST has a single MST configuration identified by an alphanumeric configuration name, a configuration revision number, and a 4096-element table that associates each of the 4096 VLANs potentially supported to a given instance. To be part of a common MST region, a group of switches must share the same configuration attributes. Switches that differ in one or more of these attributes are part of different regions. To ensure consistent VLAN-instance mapping, the protocol has to identify the boundaries of the regions. Thus, the region characteristics are included in BPDUs. The switches must know whether they are in the same region as a neighbor, and so a digest of the VLANs-instance mapping table is sent with the revision number and the name. After a switch receives a BPDU, it extracts the digest and compares it with its own digest. If the digests differ, the port on which the BPDU was received is at the boundary of a region.

IEEE 802.1s also introduces *Internal Spanning Tree (IST)* and *MST Instances (MSTIs).* IST is an RSTP instance that extends the 802.1D single spanning tree inside the MST region. MSTIs are RSTP instances that exist only inside a region and run RSTP by default. Unlike IST, MSTIs never interact or send BPDUs outside a region. MST interoperates with legacy and PVST+ switches. More information on RSTP and MST can be found at cisco.com/warp/public/473/146.pdf and cisco.com/warp/public/473/147.pdf. ▲▲

ROB BRODMAN

CHIARA REGALE

CHIARA REGALE is a technical marketing engineer in the Metro Ethernet Group at Cisco. She focuses on design and validation of solutions in the Metro Ethernet arena. After earning a Master of Science Degree in Telecommunications Engineering from Politecnico of Turin, Italy, Regale joined Cisco's Catalyst® 6000 Spanning-Tree Protocol development team, where she designed and implemented features to improve Spanning-Tree performance. She can be reached at chiarar@cisco.com.

New Product Dispatches

Edge Routing, Access, and Aggregation

Cisco 10000 Series Internet Router: New Line Cards and Enhanced ATM Interface Module

Two new line cards and a carrier card increase the modularity and deployment options for Cisco 10000 Series Internet routers. The carrier card holds one or two half-height line cards with online insertion and removal (OIR) support. The Fast Ethernet half-height line card, which uses only a half-slot of the chassis, provides eight 100-Mbit/s Ethernet ports. The single-port Gigabit Ethernet half-height line card doubles the platform Gigabit Ethernet density and enables uplink redundancy in a single slot. For ATM networks, the Cisco 10000 Series Eight-Port DS3/E3 ATM Interface Module delivers traffic shaping per virtual circuit and per virtual path, as well as support for IP layer traffic shaping on Parallel Express Forwarding (PXF) network processors.

cisco.com/go/10000

Cisco 7200 Series Router: NPE-G1 Network Processing Engine

The new NPE-G1 Network Processing Engine increases processing power on the Cisco 7200 Series Router to 1 million pps, more than double the performance of the Cisco 7200 Series NPE-400. This performance improvement further enables enterprises and service providers to deploy a wide range of network applications with multiple services. The NPE-G1 also adds high-speed LAN connectivity with three built-in Gigabit Ethernet/Fast Ethernet ports, doubles scalability by supporting up to 1 GB of dynamic memory, and reduces system cost by eliminating the need for an I/O controller.

cisco.com/en/US/products/hw/routers/ps341/products_data_sheet09186a00800c6bd6.html

Cisco 7000 Family Internet Routers: Enhanced ATM Port Adapter

An enhanced ATM port adapter is now available for Cisco 7200, 7400, 7500, and 7600 series routers using the FlexWAN module. This adapter enables service providers to offer broadband aggregation for up to 8000 subscribers on a single ATM interface. The single-port, single-wide ATM port adapter supports advanced traffic management per virtual circuit and dynamic bandwidth selection with a range of WAN media interfaces from DS0 to OC-3.

cisco.com/en/US/products/hw/routers/ps341/products_data_sheet09186a008010190a.html

Cisco 3700, 3600, and 2600 Series Routers: New Network Modules and Advanced Integration Module

Three new network modules and a new advanced integration module (AIM) extend the versatility of selected models in Cisco's broad families of access routers. The Content Engine network modules provide integrated content delivery, supporting intelligent caching, streaming, and content filtering and helping enterprises optimize WAN bandwidth utilization. (For a related article, see "Content Boost," page 51.) The Gigabit Ethernet Network Module offers high-speed, copper- or fiber-based connectivity to enable new applications, provide greater capacity for routing and bridging among virtual LANs (VLANs), and provide connectivity for branch offices to metropolitan-area networks. The Packet-Over-T3/E3 Network Module switches between T3 and E3 with a single Cisco IOS® command, simplifying global deployment. The Cisco NM-AIC-64 Network Module provides remote alarm monitoring and control for elements in service providers' operations support networks, and can be applied in enterprise applications to provide security and system monitoring. Two new AIMs extend Cisco's virtual private network (VPN) network support to include the new Advanced Encryption Standard (AES), and provide 5 to 10 times the performance of previous modules.

NM-AIC-64: cisco.com/en/US/products/hw/modules/ps2797/products_data_sheet09186a008010fd25.html
VPN Modules: cisco.com/en/US/products/hw/routers/ps259/products_data_sheet09186a0080088750.html
Content Engine: cisco.com/en/US/products/hw/modules/ps2797/products_data_sheet09186a008010fb9f.html

Cisco 3631-CO Modular Access Platform

The Cisco 3631-CO Modular Access Platform optimizes operations support for service providers and is compliant with central office standards. The Cisco 3631-CO Router provides flexible, modular connectivity to legacy X.25, asynchronous, and synchronous devices as well as Ethernet devices. Using only two rack

units, the Cisco 3631-CO is equipped with two network module slots, two WAN interface card slots, a built-in AIM slot, an integrated autosensing 10/100 Mbit/s Ethernet port, external AUX and console ports, and the option of AC or DC power.
cisco.com/en/US/products/hw/routers/ps274/ps277

Cisco 830 Series Secure Broadband Routers

The Cisco 830 Series secure broadband routers connect small remote offices and teleworkers to the Internet and corporate networks. These routers provide new, higher-performance integrated firewall and VPN services, advanced quality-of-service (QoS) features, easy deployment, and remote management. Two models are available now: the Cisco 831 Dual Ethernet Router provides an Ethernet WAN port for connecting an external DSL or cable modem. The Cisco 837 ADSL Router provides an integrated asymmetric DSL (ADSL) WAN port. Both models also offer a four-port 10/100 Ethernet LAN switch.
cisco.com/go/800

Cisco SOHO 90 Series Secure Broadband Routers

Two models in the Cisco SOHO 90 Series of secure broadband routers deliver the integrated security features of Cisco IOS® Software to small offices. These features include firewall protection for secure Internet connectivity and encryption for VPNs. The Cisco SOHO 91 Dual Ethernet Router provides an Ethernet WAN port for use with an external DSL or cable modem. The Cisco SOHO 97 ADSL Router delivers an integrated ADSL WAN port. Both models also offer a four-port 10/100 Ethernet LAN switch.
cisco.com/go/soho90

Switching

Cisco Catalyst 6500 Series Switch: New Three-Slot Chassis, 48-Port 10/100 Module, Firewall/VPN Security Systems, Secure Content Bundle

The new, value-priced, three-slot Cisco Catalyst® 6503 chassis is ideal for low-density wiring closet deployments, secure data centers, remote access, e-commerce, and converged network solutions. It uses the same supervisor modules and line cards from the Catalyst 6500 Series switches, for maximum investment protection and broader 6500 deployment options in the wiring closet, distribution, core, data center, and WAN edge. The new Catalyst 6500 Series 48-port 10/100 Ethernet module, in RJ-45 and RJ-21 interfaces, is inline power-ready and field upgradable for deploying converged multiservice networks, with the addition of the Cisco Inline Power voice feature card, and field upgradable to support the IEEE 802.3af inline power standard. Additionally, two new Catalyst 6503 and 6506 Firewall Security Systems offer up to 5 GB of firewall throughput, flexible I/O options, and multiservices that can be integrated in the remaining slots. Available in three- or six-slot chassis, the new VPN systems provide up to 1.9-Gbit/s IP Security (IPSec) throughoutput, and enable flexible, high-performance connectivity in campus and WAN edge VPN deployments. The secure content bundle includes content switching and Secure Sockets Layer (SSL) modules for secure e-commerce.
cisco.com/go/catalyst6500

Cisco Catalyst 3550-24 PWR Switch

The stackable, multilayer Cisco Catalyst 3550-24 PWR Switch offers 24 ports of 10/100 Ethernet with two Gigabit Interface Converter (GBIC) ports that provide integrated inline power to Cisco IP phones and wireless access points. The new switch provides up to 15.4 watts per port of -48-volt DC power on every 10/100 port for maximum device support. Inline power enables centralized power provisioning, which eases deployment and reduces ownership costs. This inline power switch is compatible with the Cisco RPS 675 Redundant Power System and uninterruptible power supply (UPS) systems to maximize switch availability.
cisco.com/go/catalyst3550

Security and VPNs

Cisco Secure Access Control Server Version 3.1

A highly scalable, high-performance access control server (ACS), the Cisco Secure ACS operates as a centralized Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) server. Cisco Secure ACS controls the authentication, authorization, and accounting (AAA) of users and administrators accessing corporate resources through the network. Among the new features of ACS 3.1 are support for IEEE 802.1X Protected Extensible Authentication Protocol (PEAP) for wireless LANs, Secure Sockets Layer (SSL) support for administrative access via the Web GUI, and password change enhancements that allow control over whether administrators can change passwords during Telnet sessions hosted by TACACS+ AAA clients. Cisco Secure ACS 3.1 integrates with Cisco securing management tools, including the new CiscoWorks VPN/Security Management Solution (VMS), Version 2.1.
cisco.com/go/acs

Optical

Cisco ONS 15600 Multiservice Switching Platform

The Cisco ONS 15600 Multiservice Switching Platform delivers multiple network elements in a single platform for deployment in a carrier's point of presence (POP) or large central office. This platform encompasses SONET/SDH multiplexers and digital cross-connect network elements used in metro core and edge networks. Delivering traffic scalability up to 960 Gbit/s in a single rack, the Cisco ONS 15600 complements the market-leading Cisco ONS 15454 Multiservice Provisioning Platform by leveraging that product's proven architecture and operating software.
cisco.com/en/US/products/hw/optical/ps4533

Content Networking

Cisco GSS 4480 Global Site Selector

The Cisco GSS 4480 Global Site Selector hardware platform performs real-time load balancing among data centers distributed globally. The product supports a choice of eight load-balancing algorithms to meet diverse enterprise requirements for traffic management, backup, and disaster recovery. Compatible with other Cisco content networking products, the Cisco GSS 4480 scales to support hundreds of data centers or Cisco content load-balancing products for servers.
cisco.com/go/gss

Cisco Content Switching Module Version 3.1

The Cisco Content Switching Module (CSM) software integrates content switching and load-balancing functionality into Cisco Catalyst® 6500 Series switches and Cisco 7600 Series Internet routers. New features in Version 3.1 provide additional options for managing loads on primary and backup servers, including global server load balancing for disaster recovery. Also included are a resource usage display, a full Simple Network Management Protocol (SNMP) Management Information Base (MIB), and an Extensible Markup Language (XML) application programming interface (API) for module configuration.
cisco.com/go/csm

Wireless

Cisco Aironet 1100 Series Access Point

The Cisco Aironet® 1100 Series Access Point provides secure connectivity for wireless LANs in enterprises. The first access point based on Cisco IOS® Software, the Cisco Aironet 1100 Series also leverages Cisco wireless security technology to protect data privacy. These Wi-Fi-certified access points provide a single, upgradable IEEE 802.11b radio, integrated diversity dipole antennas, and an innovative mounting system for easy installation in a variety of locations and orientations. For a related article on the Cisco Wireless Security Suite, see "Securing Wireless," page 34.
cisco.com/en/US/products/hw/wireless/ps4570

Cisco 3200 Series Mobile Access Router

The new Cisco 3200 Series Mobile Access Router creates networks of communication devices in moving vehicles such as airplanes, ships, tanks, and trains. The product supports always-on connectivity and seamless mobility for data, voice, and video communications via the Mobile IP feature in Cisco IOS Software. The Cisco 3200 Series Mobile Access Router offers a compact, rugged design for use in harsh environments and accommodates any type of standard wireless connection. Inclusion of Cisco wireless software in the Cisco 3200 Series enables advanced IP services and security features such as firewall protection and encrypted virtual private networks (VPNs).
cisco.com/go/3200

Network Management

Cisco 12000/10720 Internet Router Manager Version 3.0

The Cisco 12000 Series Internet Router Manager product has been expanded to include full support of the Cisco 10720 Internet Router and is now called the Cisco 12000/10720 Internet Router Manager. Consolidation eases deployment and manageability by having multiple device types in a single product for consistent look-and-feel features. Version 3.0 supports additional Cisco 12000 Series line cards for OC-3, OC-48, OC-192, and Gigabit Ethernet connectivity as well as Cisco IOS® Software features for Resource Manager Essentials (RME) and customized Cisco IOS command templates. This new version also includes the November 2002 Cisco Element Management System (EMS) upgrade, which delivers fault prefiltering, improved bidirectional operations support system (OSS) interfaces, and Cisco IE2100 integration with the Internet OSS.
cisco.com/en/US/products/sw/netmgtsw/ps156

Cisco 7600 Internet Router Manager Version 3.0

Previously part of the Cisco 6500/7600 Manager, the Cisco 7600 Internet Router Manager is now a standalone product. Version 3.0 adds support for up to 4000 virtual LANs (VLANs), private VLANs, IEEE 802.1Q tunneling (QinQ), QinQ network views (network-wide view of outer 802.1Q tag across managed nodes), and summary dialog (alarm/fault, performance, configuration tools in a single summary screen). This added functionality improves troubleshooting and diagnosing network and node problems quickly and efficiently. New cards supported in this version include 1 and 2xOC-48 packet over SONET (POS), 8xT1-IMA port adapter, 1xChOC-48/T3, 1xChOC-12/T3, 7609 Vortex chassis, and 2xOC-48. Version 3.0 also includes the November 2002 Cisco EMS upgrade, which delivers RME integration for improved IOS management and configuration and fault prefiltering to increase NOC productivity. OSS integration is also easier with improved bidirectional OSS interfaces and Cisco IE2100 integration with the Internet OSS.
cisco.com/go/oss

Cisco Info Center Version 3.5

The Cisco Info Center provides network fault and performance monitoring, trouble isolation, and real-time service-level management for large networks. This set of software applications is typically deployed in a service provider's network operations center. Version 3.5 delivers many improvements in failover capabilities, display parameters for filtered events, and configuration of network monitoring tools. This version also supports PCs connected to dual servers, a high-performance Oracle gateway, and new versions of selected server and PC operating systems.
cisco.com/en/US/products/sw/netmgtsw/ps996

Cisco Catalyst Switch Manager Version 3.0

The Cisco Catalyst Switch Manager (CSM)

provides consistent element management for Catalyst 2950, 3550, 4000, and 6500 series switches, meeting the requirements of service providers. Version 3.0 adds support for up to 4000 VLANs, private VLANs, IEEE 802.1Q tunneling, QinQ network views (network-wide view of outer 802.1Q tag across managed nodes), and summary dialog (alarm/fault, performance, configuration tools in a single summary screen). This added functionality improves troubleshooting and diagnosing network and node problems quickly and efficiently. New cards supported in this version include 1 and 2xOC-48 POS, 8xT1-IMA port adapter, 1xChOC-48/T3, 1xChOC-12/T3, and 2xOC-48. This new version also includes the November 2002 Cisco EMS upgrade.

cisco.com/en/US/products/sw/netmgtsw/ps837/products_data_sheet09186a0080113704.html

Cisco Packet Telephony Center Monitoring and Troubleshooting Software

The Cisco Packet Telephony Center Monitoring and Troubleshooting (PTC-MT) Software delivers an analysis tool to help service providers quickly deploy, monitor, and troubleshoot voice-over-IP (VoIP) services on a data network. Cisco PTC-MT correlates Signaling System 7 (SS7) signaling control protocols to equivalent packet protocols based on a unique identifier for each call. Other features include automatic call-leg correlation for end-to-end call tracing; real-time discovery and monitoring of signaling traffic; non-intrusive monitoring of network performance; and real-time statistical reports on key performance parameters.

cisco.com/en/US/products/sw/netmgtsw/ps4883

CiscoWorks VPN/Security Management Solution Version 2.1

CiscoWorks VPN/Security Management Solution (VMS) combines Web-based tools for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network and host-based intrusion detection systems. Version 2.1 delivers many new features that enable centralized management, a unified security monitoring console, and automated configuration of security and VPN devices. Additional tools in this version enhance security controls, reporting of VPN activity, and integration with other Cisco and third-party management tools.

cisco.com/go/vms

Cisco CNS Subscriber Edge Services Manager Version 3.1.7

Cisco CNS Subscriber Edge Services Manager (SESM) software enables service providers to create and manage a branded Web portal to offer revenue-generating services such as IP VPN, differentiated bandwidth, and streaming multimedia. The product encompasses an extensible set of applications for providing on-demand services and service management. New features in Version 3.1.7 support an API for dynamic host-key mapping; user control of configuration in the personal firewall provisioning feature; and the ability for a service provider to brand a particular Web portal page based on location attributes.

cisco.com/en/US/products/sw/netmgtsw/ps2180

Cisco WAN Access Performance Management System

The Cisco WAN Access Performance Management System (WAPMS) enables rapid rollout of managed services by providing advanced, real-time and historical performance information that service providers can use for cost-effective operational support of the managed network. Providers can also use this information to generate revenue, as it helps their enterprise customers validate network performance with intuitive reporting and measurable service-level agreements. The Cisco WAPMS allows organizations to cost effectively add WAN performance management to remote locations without having to use remote hardware monitoring probes.

cisco.com/en/US/products/sw/netmgtsw/ps4884

Voice and Video

Cisco IP Phone 7905G

The Cisco IP Phone 7905G provides a core set of business features in a cost-effective, basic IP phone. The phone is suited for use in small and home offices and in places where single-line phones are typically installed, such as cafeterias, break rooms, lobbies, and manufacturing floors. The Cisco IP Phone 7905G provides inline power and four interactive soft keys that guide a user through call features via the phone's graphical display.

cisco.com/en/US/products/hw/phones/ps379/prod_models_home.html

Cisco IP/VC 3511 Multipoint Control Unit Cisco IP/VC 3521 and Cisco IP/VC 3526 Videoconferencing Gateways

The Cisco IP/VC 3511 Multipoint Control Unit (MCU) connects three or more H.323 videoconference endpoints in a single, multi-participant meeting. H.320 endpoints can also participate in the conference via a Cisco IP/VC videoconferencing gateway. The Cisco IP/VC 3521 BRI and Cisco IP/VC 3526 PRI gateways connect H.323 videoconferencing systems on IP networks to ISDN networks, which enables connectivity with H.320-based endpoints. The H.323 and H.320 connectivity supports worldwide reach and existing ISDN equipment. Both gateways support calls at rates from 128 Kbit/s to 1.5 Mbit/s.

cisco.com/en/US/products/hw/video/ps1870/prod_models_home.html

Cisco Conference Connection

The Cisco Conference Connection software gives enterprises an IP-based audioconferencing solution that integrates with the Cisco CallManager and Cisco IP phones. The product is compatible with both IP networks and the public switched telephone network (PSTN). A Cisco Conference Connection system can scale from 20 to 100 ports for a single audio conference. The product offers a Web-based interface for scheduling, a full set of conferencing features, and simple administration.

cisco.com/en/US/products/sw/voicesw/ps752

Cisco Unity Version 4.0

Cisco Unity™ is the premier unified communications solution for enterprises. Version 4.0 delivers powerful unified messaging tools (for example, e-mail, voice, and fax messages sent to one inbox) for Lotus Domino and Microsoft Exchange environments. For Microsoft Exchange, this version also supports additional intelligent voice messaging options, and failover and message interoperability for migration from traditional voice mail systems. Features common to both environments include support for Session Initiation Protocol (SIP), numerous user features for message handling, notification, fault-tolerant system tools, and dual-switch integration for seamless migration to Cisco end-to-end IP communications.

cisco.com/en/US/products/sw/voicesw/ps2237

Cisco Media Convergence Server 7845-1400

The Cisco Media Convergence Server (MCS) 7845-1400 is a high-availability server platform for large enterprises that support a large number of IP phones. As a Cisco CallManager server, each MCS 7845-1400 can handle up to 7500 IP phones. To support additional phones, multiple MCS 7845-1400 servers can be configured into a Cisco CallManager cluster. Remote sites can be interconnected with a standards-based H.323 interface and an H.323 gatekeeper.

cisco.com/en/US/products/hw/voiceapp/ps378

Cisco ICM Software CTI Driver for Siebel 7

The Cisco ICM Software CTI Driver for Siebel 7 provides a pre-integration for the Cisco Intelligent Contact Management (ICM) software and the Siebel Call Center application. The integrated solution, also featured with Cisco IP Contact Center, allows agents to control call functions such as answer, hold, transfer, and conference directly from the Siebel desktop application. Additional features supported by the computer-telephony integration (CTI) driver include routing decisions made based on Siebel customer profiles, data-rich Siebel screen pops, and carrier-class fault tolerance and system reliability.

cisco.com/warp/public/cc/pd/cucxsw/icm/prodlit/seibl_ds.pdf

Cisco IOS Software

New IPSec VPN and Inline Stateful Firewall and Intrusion Detection Features

Cisco IOS® Software uniquely embeds security throughout the network and integrates key security functions such as IP Security (IPSec) virtual private networks (VPNs), inline stateful firewalling, and intrusion detection along with other IP services. New security capabilities in Cisco IOS Software include Dynamic Multipoint VPN, Low Latency Queuing (LLQ), IPSec Network Address Translation (NAT) Transparency, IPSec Stateful Failover, and Advanced Encryption Standard (AES) support, Certificate Auto-enrollment, and Internet Key Exchange (IKE) support for Public Key Infrastructure (PKI) Multi-key Pair. New inline stateful firewall and intrusion detection features include support for N2H2 Websense URL filtering, Session Initiation Protocol (SIP) inspection, and 42 new intrusion detection signatures. Cisco IOS security is covered in greater detail on page 27.

cisco.com/warp/public/732/Tech/security

Cisco MPLS Tunnel Builder Pro: MPLS Bandwidth Protection Solution

Cisco MPLS Tunnel Builder Pro is a Web-based application that simplifies visualization, configuration, and management of Multiprotocol Label Switching (MPLS) tunnels in a network that uses MPLS Traffic Engineering (TE). In contrast to command-line interfaces, Cisco MPLS Tunnel Builder Pro provides an integrated, graphical interface for monitoring and configuring individual nodes and links within an end-to-end topology. This management tool also integrates configuration of Cisco MPLS TE features such as Autoroute, AutoBandwidth, Differentiated Services (DiffServ)-aware TE, and Fast Re-Reroute (FRR). It uses a sophisticated hybrid optimization algorithm to provide MPLS bandwidth protection, which ensures that FRR backup tunnels have adequate backup bandwidth during failure conditions. MPLS bandwidth protection is a cost-effective alternative to SONET/SDH protection or can complement SONET/SDH protection. Cisco MPLS Tunnel Builder Pro is covered in greater detail on page 15.

cisco.com/warp/public/732/Tech/mpls/tb

Cisco Conferencing and Transcoding for Voice Gateway Routers

The Cisco Conferencing and Transcoding for Voice Gateway Routers feature provides audioconference and transcode capability for Cisco IOS voice gateways using the NM-HDV and NM-HDV-FARM modules on Cisco 2600, 3600, 3700, and VG200 series products. Delivered within Cisco IOS Software, this feature operates in conjunction with Cisco CallManager. Cost savings are realized with the location of conference resources in the branch to reduce WAN utilization and the use of transcode services to reduce bandwidth needs.

cisco.com/en/US/products/sw/voicesw/ps4952

ABOUT NEW PRODUCT DISPATCHES

Keeping up with Cisco's myriad new products can be a challenge. To help readers stay informed, *Packet*® magazine's "New Product Dispatches" provide snapshots of the latest products released by Cisco between October 2002 and January 2003. For real-time announcements of the most recently released products, see "Product News" at newsroom.cisco.com.

Cache File

SNIPPETS OF WISDOM FROM OUT ON THE NET

IT Spending to Rise in 2003

After suffering its largest decline ever in 2002, the information technology (IT) industry will grow by more than 5 percent in 2003, according to worldwide research firm IDC (idc.com). Although the IT industry worldwide shrunk by 2.3 percent this year, compared to average annual growth of 12 percent during the past 20 years, IDC expects to see spending on IT and communications increase at a rate of 5.8 percent in 2003.

2002: Year of the Klez

The Klez worm was the most prolific virus in 2002, followed by the Bugbear worm and Badtrans, reports Sophos, a corporate anti-virus protection provider based in the UK (sophos.com). Nine of the culprits on Sophos's top ten list for 2002 are mass-mailing Windows 32 viruses, with the exception of ElKern, which is dropped by Klez. As of early December, the Sophos customer support team had detected 7189 new viruses, worms, and Trojan horses for the year. What about 2003? Sophos believes that virus writers will persist in distributing Windows 32 viruses as they have the most widespread impact. For more targeted attacks, a rise is expected in Backdoor Trojans, which open up holes in operating systems for hackers to implant remote access tools, or RATs.

ARE YOU A *NERD* OR A *GEEK*?

In a story posted on Geek.com, author Tom Ziegler expounds on the origins, nuances, and evolution of these two terms. To find out which moniker rings true for you, visit geek.com/features/name/index.htm.

CYBER QUOTE

"The INTERNET is like A GIANT JELLYFISH. You can't STEP ON IT. You can't GO AROUND IT. You've got to GET THROUGH IT."

—John Evans, Author

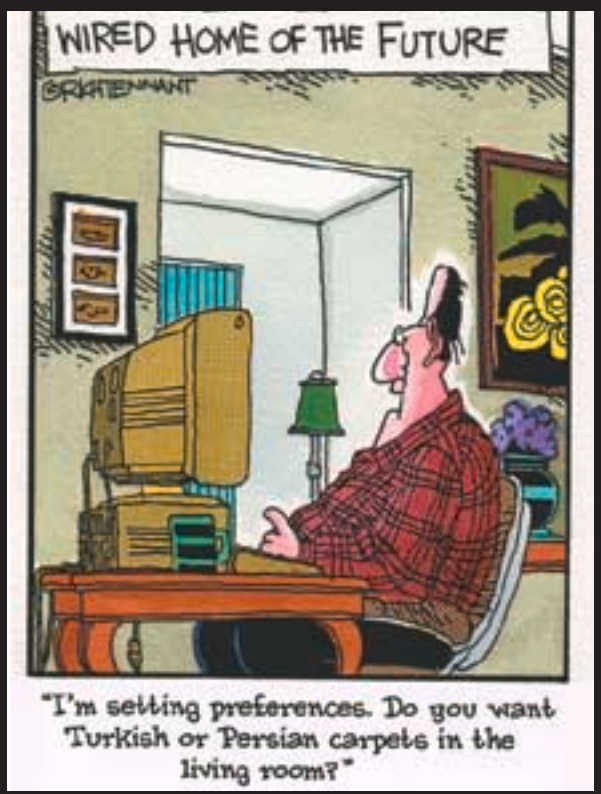
SWEET SCENT OF CELLULAR

Electronic Aromas, a company based in Inverness, Scotland, is developing technology that will deliver aromas to cell phones. The system won't actually be able to transmit scents, but will use a molecule-packed component that is inserted into the back of the mobile handset. The component is stimulated each time there's an incoming call from specific numbers, which triggers odors previously stored in the handset. Future plans call for delivering aromatherapy products via phone.

Signs of the Times—and Pickled Herring?

In the English language, as well as the language of e-mail transmissions, the symbol @ is referred to as the "at sign." However, other countries have different names for the symbol, and many of them associate it with either food or animals. For instance, in South Africa, the symbol is called *aapstert*, meaning "monkey's tail." In the Czech Republic, it's called *zavinac*, meaning "rollmop" or "pickled herring." And in Greece, it's referred to as *papaki*, or "little duck." To find out more about the history and colorful meanings of the @ sign, visit Webopedia at webopedia.com/DidYouKnow/Internet/2002/HistoryofAtSign.asp.

THE 5TH WAVE



©*The 5th Wave*, www.the5thwave.com