

PACKET

CISCO SYSTEMS USERS MAGAZINE

FOURTH QUARTER 2004

SERVICES AT WIRE SPEED

Introducing the Cisco
Integrated Services Routers

24



PACKET

CISCO SYSTEMS USERS MAGAZINE

FOURTH QUARTER 2004
VOLUME 16, NO. 4

24



ON THE COVER

Services at Wire Speed

24

Industry analysts explain why it's high time access routing got an architectural makeover and how Cisco heeded the call with the new Cisco Integrated Services Router series.

Security, Services, and Speed...Oh My!

Part 1: The Architecture

29

New Cisco Integrated Services Routers combine speed, security, and services integration to meet growing market demands, redefining "best-in-class" routing.

Security, Services, and Speed...Oh My!

Part 2: The Platforms

32

Customers weigh in on the speed and flexibility of Cisco's three new Integrated Services Router product series.

Bundled Security

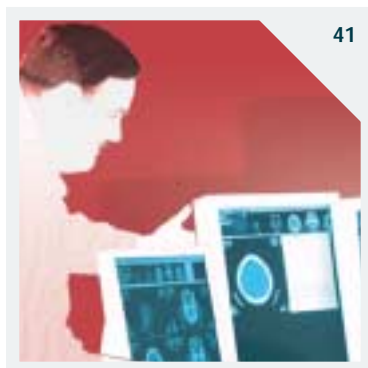
37

How integrated Advanced Encryption Standard and intrusion prevention add layers of defense to the new Cisco Integrated Services Routers.

32



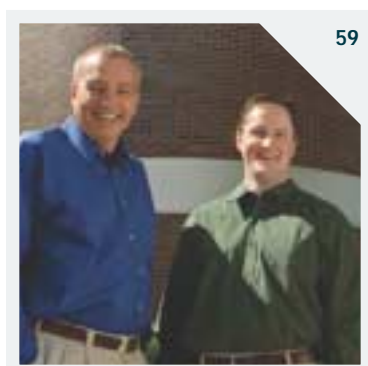
COVER (back to front): Customers Jon Duren, chief technology officer at IdleAire Technologies; Kevin Seim, senior marketing manager at BellSouth; and Chris Fairbanks, principal network architect at ePlus pose with the new Cisco Integrated Services Routers.



41



49



59

TECHNOLOGY

Routing: Transitioning to IPv6 Now 17

IPv6 capabilities to benefit end-to-end communications can be easily tested today.

MPLS VPN: Secure MPLS-Based VPNs 21

Enterprises attracted to the service benefits and potential cost savings of managed virtual private network (VPN) services based on Multiprotocol Label Switching (MPLS) can also enjoy security levels comparable to Frame Relay and ATM technologies.

ENTERPRISE SOLUTIONS

The Wired Hospital 41

An Illinois hospital saves money and lives with a high-speed network.

Around-the-Clock Uptime 45

New Cisco high availability features and services reduce MTTR to seconds.

Good Vibrations 49

The Bonnaroo Music Festival in Tennessee is the site of a massive temporary Wi-Fi network.

SERVICE PROVIDER SOLUTIONS

Head for the Hotspot 51

Guidelines to deploying profitable public wireless LANs.

IPv6 in Broadband 55

Service providers of all types can benefit from the flexibility and new revenue opportunities of IPv6-based broadband.

SMALL AND MIDSIZED BUSINESSES

Go Daddy Grows with IP Communications 59

Hard work, know-how, and a powerful network make Internet domain registrar company Go Daddy a champ.

Big Solutions for Smaller Offices 63

New SMB class products from Cisco provide the modularity, ease of use, and affordability that small and midsize companies need.

IN EVERY ISSUE

Mail	3
Calendar	5
Acquisitions	6
Networkers	20
Tech Tips	11
Advertiser Index	73
Cache File	74
The 5th Wave	74

DEPARTMENTS

From the Editor	1	Technically Speaking	67
Now, What About All These Remotes?		Cisco's Rajiv Kapoor on ITU-T carrier-class standards.	
User Connection	4	New Product Dispatches	68
Cisco Learning Credits • New Cisco		What's new from Cisco over the past quarter.	
Unity Certifications • Certification			
Games • Power Up Your SMB		NetPro Expert	71
Tech Tips & Training	7	Expert advice from Cisco's Josh	
Containing and Mitigating Network		Huston on boosting network	
Attacks • Policing the Infrastructure		security with Cisco Security Agent.	
• Voice over IP at a Glance • Reader Tips			

PACKET MAGAZINE

David Ball
Editor in Chief

Jere King
Publisher

Jennifer Redovian
Managing Editor

Susan Borton
Senior Editor

Kim Austin Peterson
SMB Editor

Karen Dalal
Staff Editor

Joanie Wexler
Contributing Editor

Robert J. Smith
Sunset Custom Publishing
Project Manager

Michelle Gervais, Nicole Mazzei,
Mark Ryan, Norma Tennis
Sunset Custom Publishing
Production

Jeff Brand, Bob Jones
Art Directors

Emily Burch
Designer

Ellen Sokoloff
Diagram Illustrator

Bill Littell
Print Production Manager

Cecelia Glover Taylor
Circulation Director

Valerie Marliac
Promotions Manager

Bart Nagel
Cover Photograph

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

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.

Please send direct address corrections and other correspondence to packet@external.cisco.com.

Aironet, Catalyst, CCDA, CCIE, CCNA, Cisco, Cisco IOS, Cisco Networking Academy, Cisco Press, the Cisco Powered Network logo, the Cisco Systems logo, Cisco Unity, IOS, IQ, Linksys, *Packet*, and PIX are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the USA and certain other countries. All other trademarks mentioned in this publication are the property of their respective owners.

Packet copyright © 2004 by Cisco Systems, Inc. All rights reserved. Printed in the USA.

No part of this publication may be reproduced in any form, or by any means, without prior written permission from Cisco Systems, Inc.

This publication is distributed on an "as-is" basis, without warranty of any kind either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or noninfringement. This publication could contain technical inaccuracies or typographical errors. Later issues may modify or update information provided in this issue. Neither the publisher nor any contributor shall have any liability to any person for any loss or damage caused directly or indirectly by the information contained herein.

This magazine is printed on recycled paper.



10%
TOTAL RECOVERED FIBER

FROM THE EDITOR

Now, What About All These Remotes?

I have a dream—more of a request, really. By way of this letter, I ask the engineers who developed the recently announced Cisco Integrated Services Routers to put their heads together to design the industry's next set-top box. You know—that elusive magic box for couch potatoes that promises to integrate our TVs with the Internet and usher in a new era of on-demand broadband services.

This magic set-top box would be able to download full-length movies in seconds, update my security files, and order my favorite pizza, all while I played poker via a videoconference with four of my friends. It would be so integrated that I could control my TV, stereo, DVD, lights, and microwave oven from the same remote. Its intelligent security features would lock out anyone who even thought of changing the channel to something that didn't adhere to my quality of service settings (any episode of "The Golden Girls," for example). In fact, this thing would be so intelligent, it wouldn't be satisfied with finding and recording my favorite shows; it would send e-mails to Hollywood studios and pitch ideas for movies and TV shows it thinks I might like!

OK. Maybe I *am* dreaming. But the level to which these Cisco engineers raised the bar on access router performance, security, and services integration is impressive, to say the least. To learn more, read our feature articles on the Cisco Integrated Services Routers, starting with "Services at Wire Speed" on page 24.

While I might have to wait a bit longer for my dream set-top box to hit the market, that's not stopping droves of consumers from adopting broadband services. Broadband subscribers worldwide grew from 33 million at the end of 2002 to 97 million at the end of 2003, according to *Ovum Access Forecasts*. And it's expected to reach 140 million by the end of this year. In "IPv6 in Broadband," page 55, Cisco's Salman Asadullah and Adeel Ahmed show how service providers of all types can benefit from the flexibility and revenue-generating opportunities of IPv6-based broadband. Think IPv6 is for the far-flung future? Think again. In "Transitioning to IPv6 Now," page 17, Microsoft's Leigh Huang explains how you can get ready for IPv6 with many of the products you have in your network today.

Lest I leave you with the impression that you need IPv6 to push the limits of the possible, check out "The Wired Hospital" on page 41. The network engineers at Lake Forest Hospital Foundation in Illinois created a single Cisco network that integrates everything from security cameras to X-Ray machines, allowing doctors to monitor patients from home—even change the temperature in a patient's room from a wireless hotspot in a coffee shop—all while saving the hospital money.

There's all this and much, much more in this exciting episode of *Packet*® magazine. Now, if you'll excuse me, I have to find the five remotes I use to turn on my TV.

David A. Ball

David Ball
Editor in Chief
daball@cisco.com



Rob Brodman

MAIL

Which Version of IOS?

I appreciated your Tech Tips & Training article on static and policy routing [Second Quarter 2004], but the article doesn't mention which version of the Cisco IOS® Software is required. It would be nice if you included that information in your articles.

—Jeff Bailey, FundSERV, Inc., Toronto, Ontario, Canada

This feature was introduced in Cisco IOS Software Release 12.3(2)XE and has been available since November 2003. It is also available in the T train beginning with Cisco IOS Software Release 12.3(8)T. Your suggestion is a good one. In the future we will make sure we provide the IOS version in articles.—Editors

When It's Time to Migrate to IPT

"Migrating to IP Telephony?" [Second Quarter 2004] is a great article and could apply to virtually any type of technological migration. It not only emphasizes the importance of up-to-date technical knowledge, but also the value of being versatile and having project management, change management, and team participation skills.

—Amanda Smith, New Horizons Computer Learning Centers of Michigan, Livonia, Michigan, USA

Networkers 2004

Packet® is the kind of publication that brings a real service to the networking community and all of the technical people who work with Cisco products and are trying to learn something new every day. I also want to commend Cisco for the Networkers 2004 convention in New Orleans. I hope to see all of you again next year.

—Rico Valverde, Columbia Association, Inc., Columbia, Maryland, USA



Taking the First Step

Thank you for your tremendous work in the IT sector. I am a regular reader of your magazine and would appreciate a column for people who are still at a lower level of networking knowledge.

—Idehen Rufus Roy, Tripod, Lagos, Nigeria

You may be interested in an excellent new offering from Cisco Press. The "First-Step Series" covers general networking, as well as LAN switching, wireless, and network security. The books are written in clear, easy-to-understand language and are intended for readers with little or no networking experience. For more information, visit ciscopress.com/firststep.—Editors

Mixed Reviews

I recently received the latest issue of *Packet* [Third Quarter 2004] and am quite unhappy with the design changes. *Packet* used to be readable, original, and attractive. The new design is ugly and more difficult to read—some of the print on the cover and the page numbers are too small and faint.

Why do companies so unwisely abandon a popular and familiar design for something worse? Although lack of readability can be easily corrected, the general graphical layout, fonts, etc. that you have introduced in the latest issue are ugly.

—Tomasz Papszun, TP S.A. Lodz, Poland

Congratulations on the new design of *Packet*. It's a great new look. You are always improving yourself, and that says a lot about both you and Cisco. Of course, I'm also impressed with the new CRS-1, especially with the performance you described.

—Miguel Sosa, I.N.S.S.J.P. Pami, Hinojo, Argentina

Helpful Info for Certified Professionals

Congratulations on an excellent and intuitive magazine. I wanted to share some information that I read about on Cisco.com that I think is extremely important to all Cisco certified personnel and would be useful to publish in *Packet*.

Effective October 1, 2004, Cisco certified professionals who pass a CCIE written exam will be able to use that passing score to recertify any associate, specialist, and professional level certifications. The requirement for CCIE level recertification remains unchanged and requires a passing score on any of the 10 available CCIE written exams.

More information on recertification policies is available at cisco.com/go/recertification.

—Ian Whitmore, BT España, Gijón, Spain

For Cisco certification news, check out the "User Connection" section of Packet or visit the Certifications Website at cisco.com/go/certifications. Certification program updates are available at cisco.com/packet/164_2a1.—Editors

Send your comments to Packet

We welcome your comments and questions. Reach us through e-mail at packet-editor@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.

Global Learning Credits Program Simplifies Training

Cisco recently expanded the Cisco Learning Credits Program to countries in Asia Pacific and Latin America, giving nearly all customers worldwide the opportunity to prepay for high-quality training at the same time they purchase Cisco hardware, software, or support services.

“We know that customers who have selected Cisco Learning Credits along with Cisco equipment over the past year have experienced greater satisfaction and productivity with their purchase,” says Dianne Brodie, Learning Credits program manager in Cisco’s Internet Learning Solutions Group.

Customer Benefits

By planning and paying for training at the time they purchase equipment, companies can manage a single purchase order and a single budget, reducing administrative expenses. Businesses can also plan for training to coincide with technology deployments, which is especially important for complex advanced technologies such as security, wireless, and IP telephony.



Program Details

Cisco Learning Solutions Partners, companies authorized to deliver Cisco training courses, help customers identify their training needs and will likely recommend how many Cisco Learning Credits to purchase. Learning Credits come in packs of 10, 100, 500, or 1500, but they can be redeemed according to course needs. One credit is equal to US\$100. Credits can be used toward any form of training.

Geographical Reach

Customers in Mexico, Costa Rica, Puerto Rico, and Panama in Latin America, and in Australia, New Zealand, Singapore, Korea, India, Hong Kong, Taiwan, and Malaysia in Asia Pacific can now access the program, along with customers in the US, Canada, and many countries across Europe, the Middle East, and Africa (EMEA). The program will become available in additional Latin American and Asia Pacific countries over the next year, and in Japan by mid-2005.

For more information about the Cisco Learning Credits Program, visit cisco.com/go/learningcredits. ■

New Cisco Unity Certifications

Field or systems engineers with a valid Microsoft Certified Systems Engineer (MCSE) certification who will be expected to install and troubleshoot Cisco Unity™ Voice Messaging and Cisco Unity Unified Messaging applications are the ideal candidates for the new Cisco Unity Support Specialist certification, according to Dave Bailey, educational product manager for Cisco’s Internet Learning Solutions Group.

“The support specialist is in high demand,” Bailey says. “Companies that use Cisco Unity software and resellers that offer support services for it want their engineers to get trained quickly to install, support, and troubleshoot Cisco Unity and immediately apply their knowledge on the job.”

In addition to holding a valid MCSE with Windows Messaging 2000 or 2003, candidates must successfully pass the Unified Communications System Engineer (UCSE) exam. Recommended training that supports the exam is the UCSE course offered by Cisco Learning Partners.

Design Specialist Certification More Intensive

The requirements and completion time of the support specialist certification are less stringent than those for the Cisco Unity Design Specialist certification (formerly the Unified Communications Design Specialist). Candidates for the design specialist

certification must hold an MCSE and a Cisco CCDA® certification, and also pass the advanced Cisco Unity for Design Networking (CUDN) exam. In addition to the UCSE course, the CUDN course is recommended.

“The design specialist training is very intensive,” Bailey explains. “These individuals will be able to use their knowledge of a company’s current business processes, current network infrastructure components, and other skills to plan, design, and recommend a supportable and sustainable Cisco Unity installation.”

Focused Certifications on the Rise

Both new Cisco Unity specializations are part of the Cisco Qualified Specialist program, which allows professionals to become certified in a particular technology such as IP telephony, network security, or wireless.

According to Bailey, individuals with Cisco IP telephony specializations who complete the Cisco Unity specializations will be able to support or design a Cisco IP communications network that includes Cisco IP phones, Cisco CallManager call-processing software, Cisco Unity software, gateways, gatekeepers, and other Cisco devices.

As companies converge their voice and data networks to one Cisco IP network, they will have a myriad of choices for supporting their networks, says Bailey. "Companies can make sure their own staff obtains the Cisco Qualified Specialist certifications or they can out-task different network functions to qualified Cisco partners—partners with staff engineers who hold these certifications," he explains.

Either way, businesses are adopting advanced technologies such as IP telephony, wireless, and security at increasing rates. Because of the growth in use of these Cisco applications by businesses worldwide, Cisco has granted 60 percent more focused certifications this year than last, according to Cindy Hoffmann, program manager in Cisco's Internet Learning Solutions Group.

Like most Certifications courseware, content for the Cisco Unity training classes is developed by Cisco experts but delivered by Cisco Learning Partners or training companies authorized by Cisco.

Cisco Unity, an integral component of Cisco IP communications systems, delivers unified messaging—e-mail, voice, and fax messages sent to one inbox—plus voice mail with advanced features, to help improve communications, boost productivity, and enhance customer service. The unified messaging and voice-mail components both work in Microsoft Exchange networks, while unified messaging also works in Lotus Domino environments.

For more information, visit cisco.com/packet/163_3b1. ■

CISCO WORLDWIDE EVENTS

December 8–10	Networkers Japan, Tokyo, Japan
December 13–16	Networkers EMEA, Cannes, France
March 8–10, 2005	Networkers Korea, Seoul, Korea
cisco.com/warp/public/688/events.html	

Educational Games for Engineers

Cisco certified professionals can now build a storage area network (SAN) on Mars or protect a network that is under attack when they play the Cisco SAN Rover and Cisco Network Defender games on the Cisco Certifications Community Web portal.

"We wanted to create a fun experience for learning about Cisco's advanced technologies," says Don Field, senior manager of certifications in the Cisco Internet Learning Solutions Group. "There's a competitive aspect to it, and professionals from all over the world are playing and learning together."

Since the games' introduction earlier this year, more than 10,000 site visitors have played. Watch the Web portal for future advanced technology learning games.

Talk Show Panels Answer Viewer Questions Live

The Certifications site also introduced a live talk show earlier this year; each episode focuses on a different topic such as security certifications or IP telephony certifications. According to Field, hundreds of professionals have tuned in live to watch the monthly show and to ask questions of the panel members.

The show's host also shows some of the resources, available on the Certifications site or elsewhere on Cisco.com, that viewers may want to access for more information about the topic.



ROLE PLAY Users build a storage area network for a fictional Mars research station in the latest simulation game focused on Cisco advanced technologies.

The shows are available in video-on-demand format on the Certifications Community site, which also features white papers, bulletin board postings, recertification reminders, and learning materials.

To view and participate in the Cisco Certifications Community, visit cisco.com/go/certcommunity. Access to the portal is available at no charge to Cisco certified individuals who are registered users of Cisco.com. ■

Power Up Your SMB Network

No matter the industry, growing small and medium-sized businesses (SMBs) face similar challenges of simplifying operations, reaching new customers, helping employees work efficiently, and improving profitability. Network technologies can help, but it's not always clear which technologies to adopt.

Power Up Your Small-Medium Business: A Guide to Enabling Network Technologies, a new book written by Cisco technical marketing leader Robyn Aber for Cisco Press®, explains network technologies and their value to business operations in easy-to-understand language.

This valuable resource can help SMB leaders learn about advanced technologies such as IP telephony, wireless, and network security, as well as the benefits of managed network services offered by service providers. The book also describes the questions

SMBs should ask of vendors and advisers as part of determining the best technology investments, and features case studies of how different industries are adopting technology to support their business goals.

Power Up Your Small-Medium Business is part of the Cisco Press Network Business Series, a set of resources that inform IT executives, decision makers, and networking professionals about important technologies and business strategies.

For more information, search for “Power Up” at ciscopress.com. ■

Recently Announced Cisco Acquisitions

Acquired		Employees	Location
Dynamicsoft, Inc.	<p>Developer of Session Initiation Protocol (SIP)-based solutions that allow telecommunications service providers to deliver interactive communications, such as conferencing, voice, and instant messaging, over an Internet Protocol (IP) network.</p> <p>dynamicsoft was founded in 1998. The company's employees will become part of Cisco's Voice Technology Group, and its products will be integrated with Cisco's softswitch technology.</p>	104	104 Parsippany, New Jersey, USA
NetSolve, Inc.	<p>Provider of remote network-management services, including real-time monitoring of IP communications networks, network security software, and network devices.</p> <p>Cisco will extend NetSolve's services and technology to specialized channel partners, or resellers, allowing them to monitor Cisco products in customer networks and proactively resolve problems.</p> <p>The NetSolve team will join Cisco Customer Advocacy. NetSolve was founded in 1987.</p>	292	Austin, Texas, USA
P-Cube, Inc.	<p>Developer of IP service control platforms that can identify subscribers and classify applications. P-Cube's technology allows service providers to control the delivery and accurate billing of content-based services such as voice over IP and video on demand.</p> <p>The team will join Cisco's Routing Technology Group. P-Cube was founded in 1999.</p>	118	Sunnyvale, California, USA

Fortify Your Network

Containing and Mitigating Network Attacks with Cisco IOS Software

By Ramya Venkatraman

The faster an attack or vulnerability is contained and neutralized, the easier it is to minimize the impact on network infrastructure. This requires multiple tools and techniques to manipulate the undesirable traffic at the border routers or the customer edge before it enters the network.

In the last issue of *Packet*®, we outlined the three key areas of network security that should be addressed early on—*threat detection and identification*, *attack containment*, and *mitigation*—and presented various features in Cisco IOS® Software that aid in threat detection and classification (cisco.com/packet/164_4a1). This article discusses attack containment and mitigation and some of the key Cisco IOS features that help enable you to fortify your network against attacks.

First, Secure the Infrastructure

Routers constitute the core components of most networks and, as such, securing the router platform should be the first step toward securing your network. Pay attention to the following areas:

1. Enable secure access methods such as Secure Shell Protocol Version 2 (SSHv2), password encryption, and TACACS+
2. Lock down Simple Network Management Protocol (SNMP) access to a router to a few specified hosts
3. Disable vulnerable global services such as HTTP server, whois, and BOOTP
4. Log at appropriate levels to detect potential attack traffic
5. Authenticate routing updates
6. Secure the forwarding plane by enabling features such as Cisco Express Forwarding (CEF), TCP Intercept, and “black hole” forwarding
7. Secure the control plane by enabling features such as Control Plane Policing and IP Receive ACL (rACL)

Cisco IOS routers support *AutoSecure*, which performs automatic one-touch device lockdown of the router. Introduced in Cisco IOS Software Release 12.3(1), AutoSecure enables accelerated, simplified deployment of security policies and procedures by disabling vulnerable services, such as HTTP server, and enabling secure services, such as SSHv2.

Many non IOS-based software tools are also available to audit router configurations. For example, the freeware utility Router Audit Tool compares existing router configurations to a recommended baseline and suggests ways to increase device security.

Cisco Control Plane Policing

Denial-of-service (DoS) attacks are malicious acts designed to cause failures in a network infrastructure by flooding it with worthless traffic camouflaged as specific types of control packets directed at the router's control plane processor. Distributed DoS (DDoS) attacks multiply the amount of spurious IP traffic, sometimes in magnitude of many gigabytes per second, by involving hundreds of real or spoofed sources. Confronted by this high rate of rogue packets, the route processor must spend an inordinate amount of time processing and discarding the DoS traffic.

Cisco Control Plane Policing provides users with programmable policing functionality on routers that filters, rate limits, and streamlines traffic destined for the control plane. This mitigates attacks targeted at the network infrastructure and maintains packet forwarding and protocol states while the device is under attack. The Cisco Control Plane Policing feature is covered in greater detail on page 12.

Access Control Lists

When an attack has been characterized (its launch location is known), you can apply containment mechanisms such as access control lists (ACLs) to classify and drop the appropriate traffic on the relevant routers. ACLs deployed at network ingress points, including all external-facing connections such as peering connections, customer edge routers, etc., help protect the network from various external threats.

Edge ACLs can be configured to permit routine transit traffic to flow uninterrupted through the network, while also providing the first level of threat containment by denying access to undesirable transit traffic and traffic destined from external sources toward

infrastructure devices. To deploy edge ACLs, you must first define the network infrastructure address space and the authorized protocols that access this space. Network infrastructure space includes all device management addresses including loopback and internal link addresses, and servers and services that are not visible to external sources.

Many DoS attacks rely on flooding core routers with fragmented packets. Using ACLs to filter incoming fragments destined for the core helps prevent attacks that inject fragments by matching Layer 3 permit rules in the transit ACL. Using a deny statement for fragments at the beginning of the ACL denies all non-initial fragments from accessing the router. However, this statement should be configured with caution because certain protocols require fragmentation and, therefore, will be denied access if a deny fragment statement exists in the ACL. Following are three sample deny statements:

```
access-list 101 deny tcp any fragments
access-list 101 deny icmp any fragments
access-list 101 deny udp any fragments
```

IOS Intrusion Prevention System

The *Cisco IOS Intrusion Prevention System (IOS IPS)* feature for Cisco routers provides complete inline intrusion detection and prevention for mitigating security attacks and threats networkwide, both internal and external. Supported in Cisco IOS Software Release 12.0(5)T and higher, IOS IPS watches packet flows and sessions as they traverse the router, and scans each flow to match well-known “signature” patterns of common network threats. Upon detecting spurious activity, IOS IPS can respond with the appropriate steps to isolate the attack and prevent large-scale security breaches.

Cisco intrusion detection system (IDS) sensors identify more than 1000 of the most common security attacks using signatures to detect threat patterns in network traffic. IOS IPS supports 740 (and growing) signatures that can classify attacks based on their severity and complexity, including analyzing both packet header and payload information for suspicious activity. Severe attacks can be further categorized as “Info” or “Attack” signatures. Info signatures detect various information-gathering activities such as port scanning, finger, icmp unreachable, etc. Attack signatures detect malicious activity such as unauthorized access, illegal FTP commands, etc. Complex attacks can be categorized as either “Atomic” or “Compound” signatures; they are triggered by traffic patterns that indicate an attack attempt on a specific host or multiple hosts over an extended period of time with multiple packets.

When packets in a session trigger a known IPS signature, Cisco IOS IPS will take one of three user-configurable actions: automatically discard the

packet, reset the TCP connection and shut down the relevant ports, or trigger an alarm to a central management station alerting the security administrator to manually configure the appropriate actions.

The IPS signatures native in IOS represent a cross section of the most rampant, severe attacks plaguing networks today and are designed to detect a broad range of attack methodologies including DoS attacks, reconnaissance missions, corporate policy violations, and device hijacking attempts. Security administrators have the ability to create custom signatures to address newer threats, modify existing IDS signatures as needed, or even disable certain signatures.

Following is a step-by-step approach to deploying IOS IPS on a Cisco router:

1. Classify signatures as “info signatures” that only trigger an event alarm or “attack signatures” that result in a packet drop and TCP connection reset. This can be done with the **ip audit <info|attack> action [drop|reset|alarm]** command.

2. Create an audit rule that specifies the IDS signatures and associates the rule with an ACL to identify the inline traffic of interest and the policy actions to enforce when individual signature matches are triggered.

```
ip audit name EXAMPLE attack list 101
```

```
access-list 101 deny 172.32.0.0 0.0.255.255 <<<<
This ensures that all packets from 172.32.0.0 sub-
net are not subjected to the IDS audit process.
access-list 101 permit any
```

The **ip audit signature <signature-id> [disable | list acl-number]** command can be used to disable specific IDS signatures or apply ACLs to individual signatures for filtering sources of false alarms.

3. Apply the audit rule to desired interfaces on the router, specifying ingress or egress traffic.

```
interface ethernet0
ip audit EXAMPLE in
```

For ingress policies, IOS IPS audits packets prior to any input ACL processing, which ensures that potential attacks are logged and/or thwarted even if the router has an ACL policy that would drop the packets. For egress policies, IOS IPS processes packets after the packet is acted upon by the input ACL of the



RAMYA VENKATRAMAN is a product manager in Cisco's Security Technology Group. She has worked on numerous QoS and security-related projects, and is a regular speaker at Networkers and a periodic contributor to *Packet*. She can be reached at ramyav@cisco.com.

incoming interface. This action might result in loss of IPS event alarms even though the attack is thwarted.

With all IOS IPS T train routers, including the new Cisco 3800, 2800, and 1800 Series Integrated Services Routers (ISRs), you can select an easy-to-use signature file that contains the most common worm and attack signature patterns. Traffic matching these signatures is automatically configured to be dropped. In addition, *Cisco Router and Security Device Manager (SDM)* provides a Web-based, user-friendly interface to provision these signatures on the router. Cisco SDM simplifies router and security configuration through smart wizards, which help you to quickly and easily deploy, configure, and monitor a Cisco router without requiring command-line interface (CLI) knowledge. SDM IOS IPS support for the ISRs allows a dynamic update of new IPS signatures from Cisco.com on any interface without disrupting basic router operations. With SDM, you can also graphically customize signatures for immediate response to a new worm or virus variant and validate router resources before signature deployment.

QoS-Based Policies

Cisco Network-Based Application Recognition (NBAR) is an intelligent application classification engine within Cisco IOS Software that uses deep, stateful packet inspection to recognize a wide variety of applications and protocols, including Web-based and other difficult-to-classify protocols that use dynamic TCP/UDP port assignments. NBAR looks into the TCP/UDP payload and classifies packets based on payload characteristics such as transaction identifier, message type, or other similar data. NBAR can also detect worms in the packet payload. NBAR plays an important role in threat mitigation because it works with QoS features to block or rate limit network resources to undesirable traffic.

Once a match value unique to the attack is identified, deploying NBAR can be an effective, tactical first step to block malicious worms while you are busy patching the network to establish defenses against the attack. For example, with Code Red, you can use a match on “*.ida” URL in the HTTP GET request. With Blaster, you can look for SQL packets of a specific length. NBAR uses regular expression matching to classify traffic by URL, text, or host fields within a HTTP request. The HTTP subport classification capability in NBAR classifies all Code Red virus packets by locking on HTTP GET requests looking for a file with the “*.ida” extension. Starting with Cisco IOS Software Release 12.3T, Cisco IOS NBAR recognizes nearly 100 different protocols and applications. New application support for NBAR can easily be delivered through a protocol description language module (PDLM). Written by Cisco engineers, PDLMs contain the rules used by NBAR to recognize an application; they can usually be loaded at run time without an IOS upgrade or router reboot.

The *NBAR User-Defined Custom Application Classification* feature gives you the ability to define customized protocols over a range of TCP and UDP ports and inspect the packet payload for a matching signature pattern at a known offset in a specific traffic flow direction. The custom protocol capability in NBAR can be used to classify the SQL Slammer worm, and an associated QoS drop action ensures that the packet is discarded before reaching the server.

The following example shows how NBAR can be used with a QoS policy to mitigate the effects of Code Red virus and the Slammer worm at the network edge.

1. Create custom protocol to identify all SQL traffic:

```
ip nbar port-map custom-01 udp 1434
```
2. Create QoS class-map to identify SQL packets 404 bytes long and Code Red virus packets:

```
class-map match-all slammer_worm
match protocol custom-01
match packet length min 404 max 404
class-map code_red
match protocol http url “*.ida”
```
3. Use QoS drop action to discard the matching packets at the ingress interface:

```
policy-map mitigate_worms
class slammer_worm
drop
class code_red
drop
```

Depending on the type of attack, service providers can use a variety of approaches instead of simply dropping traffic. For instance, they can identify traffic using Layer 3 access-list and rate-limit using class-based policing. This approach limits the bandwidth consumed by identified traffic to a certain threshold.

♦ ♦ ♦

Security policy enforcement is most effective when it is an inherent component of the fundamental network design. The diligent application of various Cisco IOS Software features and capabilities will ensure that IOS helps protect your business and defend your network with pervasive, easy-to-manage, integrated security. ■

FURTHER READING

- Cisco IOS IPS
cisco.com/packet/164_4a2
- NBAR
cisco.com/packet/164_4a3
- Infrastructure security
cisco.com/go/autosecure
- Cisco Router and SDM
cisco.com/go/sdm
- Cisco Integrated Services Routers
cisco.com/go/isr

Reader Tips

Packet® thanks all of the readers who have submitted technical tips. Each quarter we receive many more tips than we have space to include. While every effort has been made to verify the following reader tips, *Packet* magazine and Cisco Systems cannot guarantee their accuracy or completeness, or be held responsible for their use.

Configuration

TIP Using Privilege Mode Commands in Global Configuration Mode

Here's a handy tip when using the **show**, **ping**, and **telnet** commands. Instead of switching back and forth between global configuration mode and privilege mode to use these commands, you can remain in global configuration mode and type the **do** command with the original syntax.

For example:

```
Router(config)#do show running-config
or
Router(config)#do show interface e0
or
Router(config)#do PING 10.0.0.1
```

—Bharat Kumar Raney, Document World Pakistan (Pvt) Ltd., Karachi, Pakistan

Editor's note: This is a good tip about a great, little known feature.

TIP Optimizing Port Configuration

Using the **set port host** command on the Cisco Catalyst® 6500 Series is a useful way to optimize a switch port for host connection. Using the *all* option works magic in turning on or off the right mix for optimum network connection for all end hosts (desktops, Windows workstations, etc.). When each switch port has a single host connected to it, you can use this command instead of manually setting the correct features for every port. This command sets channel mode to off, enables spanning-tree PortFast, sets the trunk mode to off, and disables the 802.1q tunnel feature. Note that this command is not for connecting hubs, concentrators, switches, and bridges because spanning-tree PortFast is enabled and can cause temporary spanning-tree loops.

```
cisco6509> (enable) set port host all
```

You should enable spanning-tree PortFast start only on ports connected to a single host.

The **clear port host** command sets channel mode to auto, disables spanning-tree PortFast, and sets the trunk mode to auto:

```
clear port host <all | mod/port>
```

—Aamer Kaleem, CCIE® No. 11443, UBS AG, Chicago, Illinois, USA

Editor's note: This tip is Catalyst specific. The equivalent command in the Cisco IOS® Software is **macro apply cisco-desktop**.

TIP Binding IP Addresses to MAC Addresses

I needed to set the IP addresses on several devices that were connected to the network but had not been configured. I knew the first four digits of the Organizationally Unique Identifier (OUI), so for locations that had switches I used the following command to learn the MAC addresses:

```
sh mac address-table | include xxxx (xxxx = first
four digits of the OUI)
```

In config t, using the MAC address above, I bound the IP to the MAC:

```
arp xx.xx.xx.xx yyyy.yyyy.yyyy.yyyy arpa
(x = IP y = MAC)
```

I then was able to Telnet to the device and complete the network configuration.

For sites that did not have switches, I turned on Address Resolution Protocol (ARP) debugging in the router (the sites had fewer other devices and low traffic): **debug arp**. I cleared the arp table: **clear arp**.

Then I watched for the device to appear in the router log (referring to the first four digits of the MAC address).

I turned off debug: **no debug all**.

In config t, using the MAC address found in the log, the IP binding was done:

```
arp xx.xx.xx.xx yyyy.yyyy.yyyy.yyyy arpa
(x = IP y = MAC)
```

—Tim Wietlispach, Wietlispach Consulting Corporation, San Antonio, Texas, USA

Troubleshooting

TIP Testing Remote Authentication of Users on Wireless Networks

One of the greatest challenges in supporting a large wireless network is testing authentication from a remote access point. Asking a user to retry a login multiple times can be time consuming and frustrating. To solve this problem, you can use the **test aaa group** command to test both RADIUS and TACACS authentication using a user ID and password combination from the access point:

```
AP#test aaa group ?
  radius    Test list of all Radius hosts
  tacacs+   Test list of all Tacacs+ hosts
```

While this isn't exactly like a connecting user, it can verify a critical piece of the login. Here are some examples using the command.

```
AP#test aaa group radius <domain>\<userid>
<goodpassword> new
Trying to authenticate with Servergroup radius
User successfully authenticated

AP#test aaa group radius <domain>\<userid>
```

```
<badpassword> new
Trying to authenticate with Servergroup radius
User rejected
```

—Kevin Miller, HMI Network Services, Zeeland, Michigan, USA

Editor's note: This is a good tip that plays to the "divide and conquer" model of troubleshooting.

TIP Locating IP Addresses

In the First Quarter 2004 issue, you published a technical tip on locating IP addresses in a switched network. I use a perl script (geocities.com/milicsasa/Tools/l2trace) that does something similar, Layer 2/Layer 3 trace, graphically, but on a much larger scale.

—Sasa Milic, CCIE No. 8635, Belgrade, Yugoslavia

SUBMIT A TIP

Help your fellow IT professionals by submitting your most ingenious technical tip to packet-editor@cisco.com. When submitting a tip, please tell us your name, company, city, and country. Tips may be edited for clarity and length.

Tech Tips

Test the latest Cisco technical support tools and services.

Become a tester of Cisco technical support tools and services before their general release. As a tester, your feedback greatly influences future tool features and interfaces. Sign up as a tester or renew your registration information. cisco.com/packet/164_4e1 (requires Cisco.com registration)

Troubleshoot V.110 call connections on Cisco access servers. Get help with V.110 problems on Cisco AS5000 Series access servers with Cisco IOS® Software Release 12.0(5T) and above and Cisco 3600 Series routers with Cisco IOS Software Release 12.1(5)T and above. cisco.com/packet/164_4e2

Configure Cisco MGCP IP phones. This document provides a sample configuration for Cisco Media Gateway Control Protocol (MGCP) IP phones controlled by a Cisco BTS 10200 Softswitch. The configuration is suitable for basic call handling and lab environments. cisco.com/packet/164_4e5

Configure port monitoring on a Cisco Catalyst 2900 or 3550

Series Switch. This TAC solution document describes how to configure Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) on Cisco Catalyst® 2900 or 3550 series switches, and provides several configuration examples. cisco.com/packet/164_4e3

Detect and clear hung TCP connections using SNMP.

Learn how to use Simple Network Management Protocol (SNMP) to detect and clear hung TCP connections on a Cisco IOS Software device. This document also provides information about the SNMP objects that you use for this purpose. cisco.com/packet/164_4e4

Obtain a compatibility matrix for Cisco ONS 15454 SDH Multiservice Provisioning Platform hardware and software.

This table shows software and hardware compatibility for Cisco ONS 15454 SDH systems configured with XC-VXL-2.5G cards for releases 3.3, 3.4, 4.0, 4.1, and 4.6. cisco.com/packet/164_4e6

Policing the Infrastructure

New IOS Control Plane Policing feature protects the route processor.

By Michael Keohane

Denial of service (DoS) attacks made world news in 2000 when popular Websites such as eBay, Yahoo, and CNN were rendered inaccessible by hackers. The stakes were high—the Yankee Group estimated DoS attack-related losses approached US\$1.2 billion that year. While these attacks were devastating, they were relatively unsophisticated. By contrast, today's distributed DoS attacks (DDoS) use worms, viruses, and zombies to cripple network resources and are increasing in complexity, sophistication, and speed. Hackers can quickly amass an army of "zombie" remotely controlled computers by scanning the Internet for unprotected systems, a method that was used in the Code Red virus on July 19, 2001, infecting more than 250,000 systems in less than nine hours. Research organization Computer Economics estimated the associated costs of the Code Red attack reached an astronomical US\$2.5 billion.

Today an entire company's revenue can be dependent on its network being operational and accessible, a phenomenon that has created a target too tempting for some to resist. In October 2002 hackers used a relatively primitive Internet Control Message Protocol (ICMP) request flood to attack the Internet's 13 root Domain Name System (DNS) servers. While this attempt failed, it served as a "wake-up call" that, rather than just attacking individual Websites, the infrastructure of the Internet could be targeted. If the network infrastructure of a corporation, region, or country is indeed the focus of attacks, then it is likely that the routers and switches that provide the connectivity are also vulnerable to such attacks.

Recently introduced in Cisco IOS® Software Release 12.2(18)S, *Control Plane Policing (CoPP)*, builds on the existing rACL feature (receive access control list) to offer a new paradigm for protecting the control plane of Cisco IOS routers and switches against the increasing threat of reconnaissance and DoS attacks.

Operational Planes

Routers have three operational planes: the *data plane*, the *management plane (MP)*, and the *control plane (CP)* (see figure on page 13). The data plane handles customer data packets arriving on the device's interface modules. The packets are meant to be sent through the router as quickly as possible to the next-hop destination. The MP is involved with the configuration and monitoring of the router through the Cisco IOS Software command-line interface (CLI) or remotely

through a network management station. The CP includes network protocols, such as routing, signaling, and link management protocols, which are used to establish the forwarding paths required by the data plane. All packets arrive on the same input interfaces regardless of which operational plane they are destined.

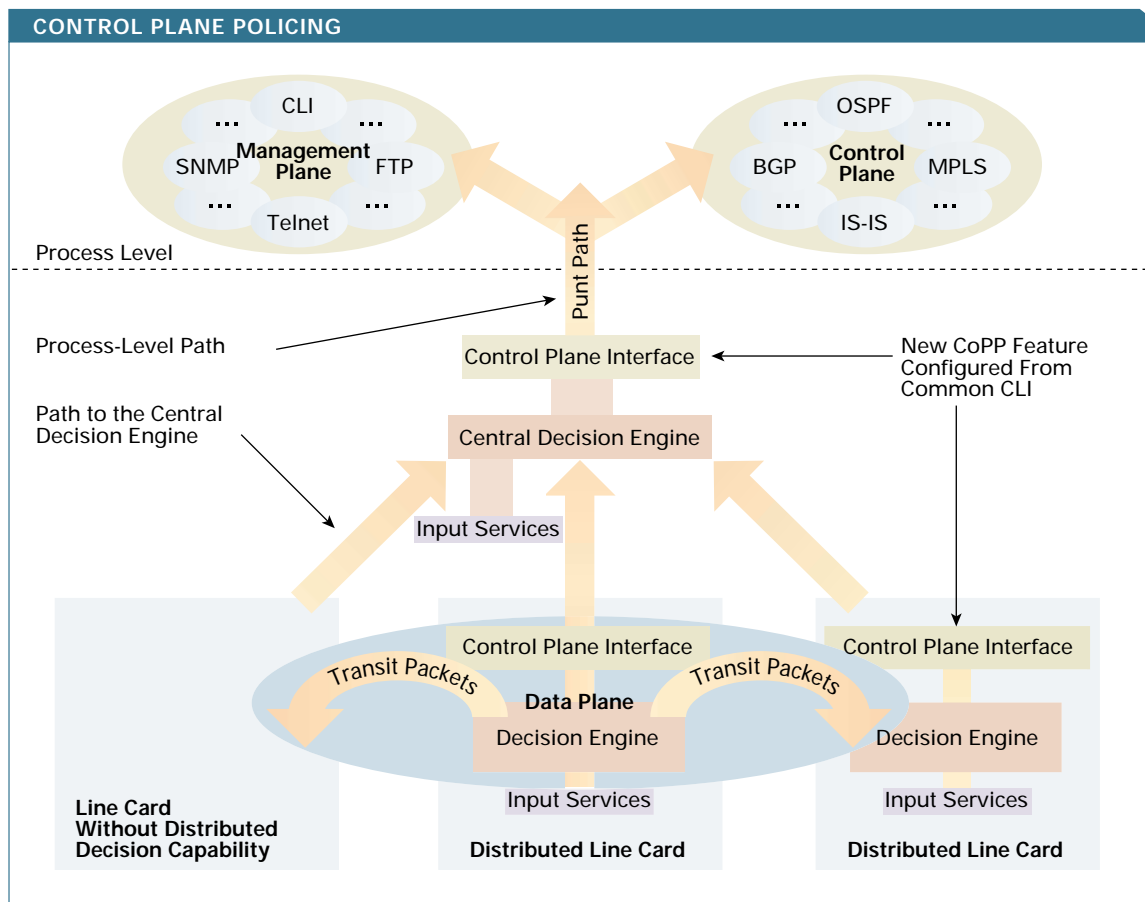
Traditionally, both the MP and CP run at *process level* on the route processor (RP). Process level is used for functions that are CPU intensive and need to be performed out of the data switching path. The path to process level from the data plane is referred to as the *punt path*, a term that derives from the image of "kicking" a packet out of the data plane to be handled by the router itself. In the figure, the data plane is shown processing transit packets which pass through the box at high speed. This can be done in a distributed manner, as shown in the figure, or through the central switch engine. Those packets destined for processes in the MP or CP arrive on the same interface but must travel the slower punt path to process level.

Today, DDoS attacks predominately seek to interrupt the MP and CP processes in order to cause the greatest service disruption. For example, a DDoS attack might attempt to prevent the routing protocols between two routers (running in the CP) from communicating with each other. Each device believes its routes are lost and begins the CPU-consumptive task of finding new data forwarding paths. In the meantime, customer traffic is "black holed" while new paths are computed. If an attack is successful at the network core, the effect is even more devastating as the loss of route convergence is amplified back toward the edge devices, potentially causing a larger and more far-reaching network outage.

Routers under attack can experience long periods of high CPU, RP resource exhaustion (for example, packet buffers and process memory), and indiscriminate packet drops as the punt path becomes overwhelmed. Indiscriminate drops can lead to the loss of Layer 2 keepalives and Layer 3 routing updates. When these are prevented from reaching the device, the links and routes represented on those links can be



MICHAEL KEOHANE is a technical leader in the Routing Technologies Group at Cisco and has been a developer for the Cisco 7500 and 7600 series router platforms for eight years. He is co-author of a patent pending on control plane policing and can be reached at mkeohane@cisco.com.



PUNT PATH With Control Plane Policing, attacks are absorbed at the control plane interfaces before affecting applications and protocols running at process level.

lost. Network administrators attempting to analyze an attack can also be prevented from accessing the device if they connect over a link under a bandwidth attack. Even if the administrator is directly attached to the router's console, the persistent high CPU makes analysis difficult as console response slows to a crawl.

With today's routers this problem is even more significant. Data plane speeds are increasing as forwarding functions are moved into ASICs that are capable of very high aggregate bandwidth. However, the control plane traditionally exists at process level running at relatively slower speeds. For example, the ASICs on the Supervisor 720 module in the chassis of a Cisco Catalyst® 6500 Series Switch or Cisco 7600 Series Router can run up to 30 million packets per second (Mpps) centrally and can be distributed to line cards that are capable of moving data at 48 Mpps per module. In contrast, the R7K CPU used as the RP runs at 600 MHz, providing 500–600 thousand packets per second (Kpps) at interrupt level (packets transiting through the box but handled in software), decreasing to approximately 20 Kpps for those packets that are punted to process level. Routers and switches were designed to move very high data rates through the system, but not necessarily to process punted packets at these rates.

Protecting the Control and Management Planes

Several features of the Cisco IOS Software help manage this issue. Authentication and encrypted protocols, as well as trusted hosts, can help protect data integrity at the management and control planes. ACLs, unicast Reverse Path Forwarding (uRPF), and policers that condition traffic to a specified rate also help limit the data that can be punted to the RP. However, limiting traffic in this way has inherent problems.

Consider the example of a customer with a large configuration. This customer can develop classes and policies to filter traffic destined to the RP from the data plane. The customer must then apply or merge the policy maps to every interface on the system because data destined for the control plane could arrive on any interface. But most customers do not want to incur this management overhead. Because the policies are applied to all data on the interface, whether transit or destined for the router, switching performance can be affected as a result of the policy. More importantly, the aggregate throughput of all interfaces could still conceivably overwhelm the RP. Assume that the customer in this example is hit by a DDoS attack. It has applied policies on all interfaces that limit RP-destined traffic to 500 Kpps for a given traffic type. Because the policy is 500 Kpps per

interface, if four interfaces are under attack, the aggregate attack on the RP CPU would be 2 Mpps. This cumulative rate might be enough to begin affecting the performance of the MP and CP at process level. Finally, certain types of traffic cannot be defined by a class for filtering. Examples include packets with IP options bit set or certain Layer 2 control traffic. These could slip under the radar toward process level, denying services on the router.

New Control Plane Policing Feature

The CoPP feature handles traffic destined to RP process level in an innovative way by treating traffic that is punted out of the data plane as though it is arriving on a distinct interface module: the *control plane interface*. To the router, the interface appears to be like any other interface on the system, and as such can be configured to accept a policy that applies to all traffic destined to the RP. When packets are punted, the control plane interface must accept them before the RP does. With this model, one can establish a centralized control plane policy that is completely independent from the other interfaces on the system and that represents the aggregate of all RP-destined traffic. The policy is developed using the familiar Modular QoS (MQC) CLI and applied globally to the control plane interface as an input or output policy. The policy determines the acceptable levels of traffic defined in each class by the network administrators. Because the control plane interface operates outside the data plane, transit switching performance is not affected and existing interface configurations are preserved.

Logically, you can envision a DoS attack coming in on a high-speed interface, such as a 10 Gigabit Ethernet, and consuming all of the aggregate bandwidth permitted for all interfaces by the control plane policer. While the control plane interface will handle the attack properly, interfaces not under attack might find their traffic policed indiscriminately as the available CoPP bandwidth is consumed. For this reason, CoPP can also be distributed to intelligent line cards. When distributed CoPP is used, each line card enforces the control plane service policy locally for RP destined traffic. Permitted traffic is then combined at the central aggregate control plane interface where it is subjected to further conditioning. Referring back to the figure, the complete model can now be fully understood. Packets destined for the punt path on the RP are policed in a manner determined by the network administrator policies. Attacks, malicious or unintentional, will be absorbed at the control plane interfaces before affecting applications and protocols running at process level.

Configuring CoPP and Understanding Packet Flow

The following is a simplified configuration example for CoPP on a router. In this example, the administrator has configured four classes of service: *critical*, *important*, *normal*, and *default*.

CoPP Configuration Example

```
access-list 120 remark CPP ACL for critical traffic
! allow BGP from known peer to BGP TCP Port
access-list 120 permit tcp host 47.1.1.1
  host 10.9.9.9 eq bgp
! allow full telnet access from specific host,
access-list 120 permit tcp host 10.86.183.3
  any eq telnet

access-list 121 remark CPP important traffic
! permit return traffic from TACACS host
access-list 121 permit tcp host 1.1.1.1
  host 10.9.9.9 established
! ssh access to the router from a subnet
access-list 121 permit tcp 10.0.0.0 0.0.0.255
  host 10.9.9.9 eq 22
! police the rest of the 10.86.183.xx subnet
access-list 121 permit tcp 10.86.183.0 0.0.0.255
  any eq telnet

access-list 122 remark CPP normal traffic
! permit router originated traceroute
access-list 122 permit icmp any any ttl-exceeded
access-list 122 permit icmp any any port-unreachable
! allow pings to router
access-list 122 permit icmp any any echo

access-list 123 remark rest of the IP traffic for CPP
access-list 123 permit ip any any

R1(config)#class-map cpp-critical
R1(config-cmap)# match access-group 120
R1(config-cmap)#class-map cpp-important
R1(config-cmap)# match access-group 121
R1(config-cmap)#class-map cpp-normal
R1(config-cmap)# match access-group 122
R1(config-cmap)#class-map cpp-all-other-ip-traffic
R1(config-cmap)# match access-group 123

R1(config-cmap)#policy-map cpp
R1(config-cmap)#!No policing is done on the critical
traffic
R1(config-pmap)# class cpp-critical
R1(config-pmap)#class cpp-important
R1(config-pmap-c)# police 125000 1500 1500
conform-action
    transmit exceed-action drop
R1(config-pmap)#class cpp-normal
R1(config-pmap-c)#police 64000 1500 1500
conform-action
    transmit exceed-action drop
R1(config-pmap)#class cpp-all-other-ip-traffic
R1(config-pmap-c)#police 32000 1500 1500
conform-action
    transmit exceed-action drop

R1(config)#control-plane
R1(config-cp)#service-policy input cpp
```

Continued on page 73

Voice over IP

At a Glance

Compressing Voice

A key issue with VoIP is bandwidth conservation. Because the routing information in VoIP packets can more than double the size of the packet, it is important to compress the voice data as much as possible. There are three levels, or orders, of compression. The first order is to simply not transmit what can't be heard. A typical conversation is mostly silent (hard to believe, but true). These silent parts of speech are not transmitted. The second order of compression is to get the most out of the digital conversion of the analog signal. While the analog signal has an infinite number of states, the digital representation must be a series of 1's and 0's and will be limited by the number of bits used. More bits means more levels (a good thing) and more bandwidth required (a bad thing). For example, an 8-bit digital signal could represent 256 levels. Any instantaneous measurement taken in the A/D process will be represented by one of these levels. This is referred to as quantization. By stacking more levels at low amplitudes (rather than having them evenly spaced out), you can use fewer bits to get the same quality you would achieve by using a greater number of levels (without consuming additional bandwidth).



The third order of compression is to not send the actual voice data. Speech signals can be modeled using pitch and tone. There are wide variances of tone and pitch data, but these can be stored in lookup tables. Modern computing techniques and impressive statistical modeling enable the table location (or vectors) of the pitch and tone data to be sent across the network. On the receiving end, the vectors are applied to the tables, and the sound is recreated.

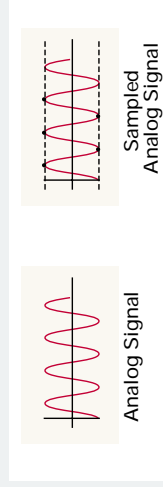
Comfort Noise

The digital signals used in VoIP are usually much "cleaner" than the analog signals used in circuit-switched telephony. With analog, any amplification of the signal also amplifies noise, resulting in static that can be heard in the background during a call. With digital, noise can be cleared away for a much more pure sound. This might seem advantageous but can actually cause problems. On analog calls, slight background noise indicates a good connection. Most phone users are accustomed to this noise, and the absence of the static can cause people to wonder if the connection is still live (hello?). Thus, digital systems inject static—called comfort noise—on the receiving end to let users know that there is still a good connection.

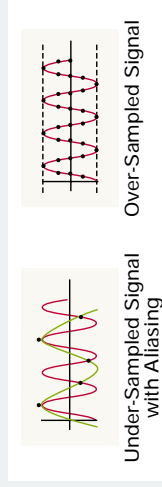
—Jim Doherty, Cisco Product & Technology Marketing

Analog Voice to Digital Conversion

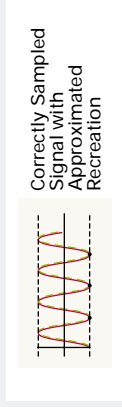
Analog signals are composed of continuously variable waveforms with an infinite number of states, and therefore can theoretically be replicated exactly. For digital telephony (including VoIP), the original signal must be converted to a digital stream (or series of packets) on the transmitter and recreated on the receiving end. Analog to digital conversion is accomplished by sampling: taking instantaneous measurements of an analog signal. If enough samples are taken, the original analog signal can be replicated by "connecting the dots" of the instantaneous measurements.



To correctly replicate the original signal, the proper ratio of samples must be taken. If too few samples are taken, more than one signal (frequency) can connect the dots. This is called aliasing. Too many samples, however, is not always better. Over-sampling can improve the accuracy of the replicated signal, but will eventually consume too many resources (CPU, bandwidth) without commensurate benefits.



The ideal sampling rate for any signal is twice that of the signal's highest frequency. So, a signal with a frequency of 2 cycles per second can be accurately recreated by digitally sampling it at 4 samples per second. This is called the Nyquist Rate, named after the AT&T engineer who discovered it. The Nyquist theorem states that any analog signal can be digitally recreated by sampling it at twice that of the highest frequency contained in the original signal. Typically, signals are sampled at just over the Nyquist Rate.



Why Should I Care About Voice over IP?

Before voice over IP (VoIP), separate networks were required to carry circuit-switched voice traffic and packet-switched data traffic. The two networks actually operated on the same types of wires, but the physical network infrastructure was optimized for circuit-switched voice traffic. Why? Because voice traffic existed first and accounted for the vast majority of the traffic.

Over the past 20 years, however, the volume of packet-switched data traffic has increased exponentially. Several industry studies estimate that data traffic has already exceeded voice traffic and will be substantially greater by 2005.

Because bandwidth is a limited and expensive resource, there is continuous pressure for companies to use it more efficiently. One of the best ways to accomplish this efficiency is by converging the voice and data networks. Convergence also reduces training and operational costs because there is only one network to maintain. And because the primary network is now packet (data) based, it is more practical to modify voice signals to traverse data networks than vice versa.

What Issues Need to Be Addressed?

Analog voice signals must be converted into digital packets. All sounds (including speech) are analog waves composed of one or more frequencies.



For VoIP networks, these analog signals must be converted into digital packets before they are transported over the IP network. Once transported, the signals are recreated into soundwaves for our listening pleasure.

Packets must be transported in real time. VoIP sound quality is based on the network's ability to deliver packets with a very high success rate (99 percent or better) and minimal delay (less than 150 msec end to end). There are well-established standards for quality. While some people using VoIP might be willing to tolerate lower quality sound in exchange for free long distance, when it comes to business applications, VoIP quality must rival that of circuit-switched telephony.

Transitioning to IPv6 Now

IPv6 to benefit end-to-end communications can be easily tested today.

By Leigh Huang

Of all the benefits that IPv6 promises for next-generation networking—autoconfiguration, limitless addresses, mobility—its ability to recreate end-to-end communications will be among its greatest contributions. By re-enabling direct peer-to-peer communications, IPv6 will be the catalyst for a new generation of shared-experience applications—virtual concerts, video meetings, online video classes, and real-time gaming—using voice, video, and presence-based technology that far transcend today's early-stage applications.

Contrary to perceptions in the market, IPv6 is not a distant technology, but is now widely available as embedded feature sets in a range of networking products and recent operating system releases. IPv6 stacks are supported in Microsoft operating systems such as Windows Server 2003, Windows XP Service Pack (SP1) and SP2, Windows CE, and PocketPC 2003. Transition mechanisms such as Intrasite Automatic Tunnel Addressing Protocol (ISAT-AP), Teredo, and 6to4 tunneling provide simple approaches to edge deployment of IPv6 without costly infrastructure upgrades.

IPv6 was facing a typical dilemma: if no mass market existed, developers were hesitant to adopt, hindering the availability of a “killer” application. But IPv6 is gaining momentum worldwide, and enterprises and service providers can easily begin to explore and gain experience with IPv6 through minor infrastructure changes. Developers can begin to write applications that are also IPv6 compliant at minimal extra cost and effort, providing them with a key advantage in an early, but soon to be huge, market.

The Promise of End-to-End

One of the key issues hindering the growth of rich streaming and real-time collaborative applications is the lack of true end-to-end connectivity. Today's Internet is based on the IPv4 protocol that has not been substantially changed since RFC 791 was published in 1981. Network Address Translators (NATs) have evolved as a makeshift measure to extend the life of the IPv4 public address space. NATs have enabled enterprises, service providers, homes, and Wi-Fi hotspots to hide inside private addresses and share a single public IP address to the outside world.

While NATs provide a useful function by extending the limited range of IPv4 addresses, NATs pose significant problems in an increasingly collaborative and mobile world. NATs break end-to-end connectivity by inserting translation devices that manipulate the data, thereby blocking direct peer-to-peer communications between two devices. While workarounds are available, they increase the complexity of both the development and deployment phases of the project. Finding ways to “traverse” NATs requires developers to divert key resources to address this non-core func-



Greg Mabry

tion during the development cycle. Additionally, many applications and services address the NAT situation by deploying servers in the network. This is an expensive overhead that many smaller organizations cannot afford. The problems created by broken end-to-end connectivity ultimately limit availability of solutions to all customers.

A Transparent Internet

Beyond the difficulties developers face with NAT workarounds, network administrators must deploy gateways and servers to circumvent the problem. This has led to situations like the AOL MegaPOPs that are proxying millions of people behind gateway devices. All of this activity must be tracked, and it consumes significant bandwidth.

IPv6 eliminates the need for address translation because it restores the network connectivity through its rich IP addressing scheme. This means that each device can have its own IP address, and media streams can be sent directly from peer to peer without going through a translation device. IPv6, therefore, brings back the capability of end-to-end control of communications, making networking applications simpler as the network again becomes transparent.

In addition to enabling peer-to-peer communications and resolving IPv4 address limits, IPv6 presents an opportunity to create a protocol with new and improved features. A simplified header architecture and protocol operation translates into reduced

Cisco and Microsoft Interoperate with Mobile IPv6

Mobile IPv6 is a technical specification designed to address mobile connectivity in IPv6. Its standardization has been handled by the Mobile IPv6 Working Group (MIPv6 WG) in the IETF, and the latest version of Mobile IPv6 is RFC 3775. To date, both Cisco and Microsoft have implemented this to enable market exploration and functional interoperability.

Three elements are specified in Mobile IPv6: the *mobile node* that conducts communication while in transit, the *home agent* that temporarily responds to communication requests on behalf of mobile nodes, and the *correspondent node* that communicates with mobile nodes. Cisco will include support for the home agent on routers running Cisco IOS Software Release 12.3T. The Cisco MIPv6 home agent is interoperable with Microsoft mobile nodes running Windows XP SP1, Windows CE, and PocketPC 2003.

operational expenses. Built-in mobility and security features mean easier and, therefore, more ubiquitous, applications and services that are lacking in IPv4-based networks.

Gaining Momentum

As with any major technology change, the transition to IPv6 will occur over time. But 2004 has seen a spike in the interest in and deployment of IPv6. In June 2003, the US Department of Defense (DoD) announced a five-year procurement plan stipulating that all future purchases of networking hardware and software would need to be IPv6-capable, or must plan to be before the end of 2007. This doesn't mean that the products need to fully implement IPv6 today, only that they have the necessary IPv6 protocol stacks and ASIC-accelerated hardware to enable the US DoD to successfully deploy IPv6 on the projected turn-on date in 2008.

Cisco and Microsoft are fully committed to supporting these deployment efforts by delivering a complete set of IPv6 solutions to the market and by collaborating with standards bodies such as IETF and other international forums in this area. Both companies are also actively working with US government organizations such as the National IPv6 Task Force, directed by the Secretary of Commerce under the auspices of The President's National Strategy to Secure Cyberspace, to examine the issues around the deployment of IPv6 in the US. Microsoft and Cisco will also work with other industry players.

The electronic consumer industry is also leading the IPv6 effort as demonstrated by Sony Corporation, whose executive vice president, Mario Tokoro, recently stated "All Sony products will be IPv6-enabled in 2005."

Making the Transition

While IPv6 mass adoption is a few years off, organizations can start today to take small steps and gain familiarity with IPv6. This process has been simplified through the following transition technologies that most equipment manufacturers have built into their products:

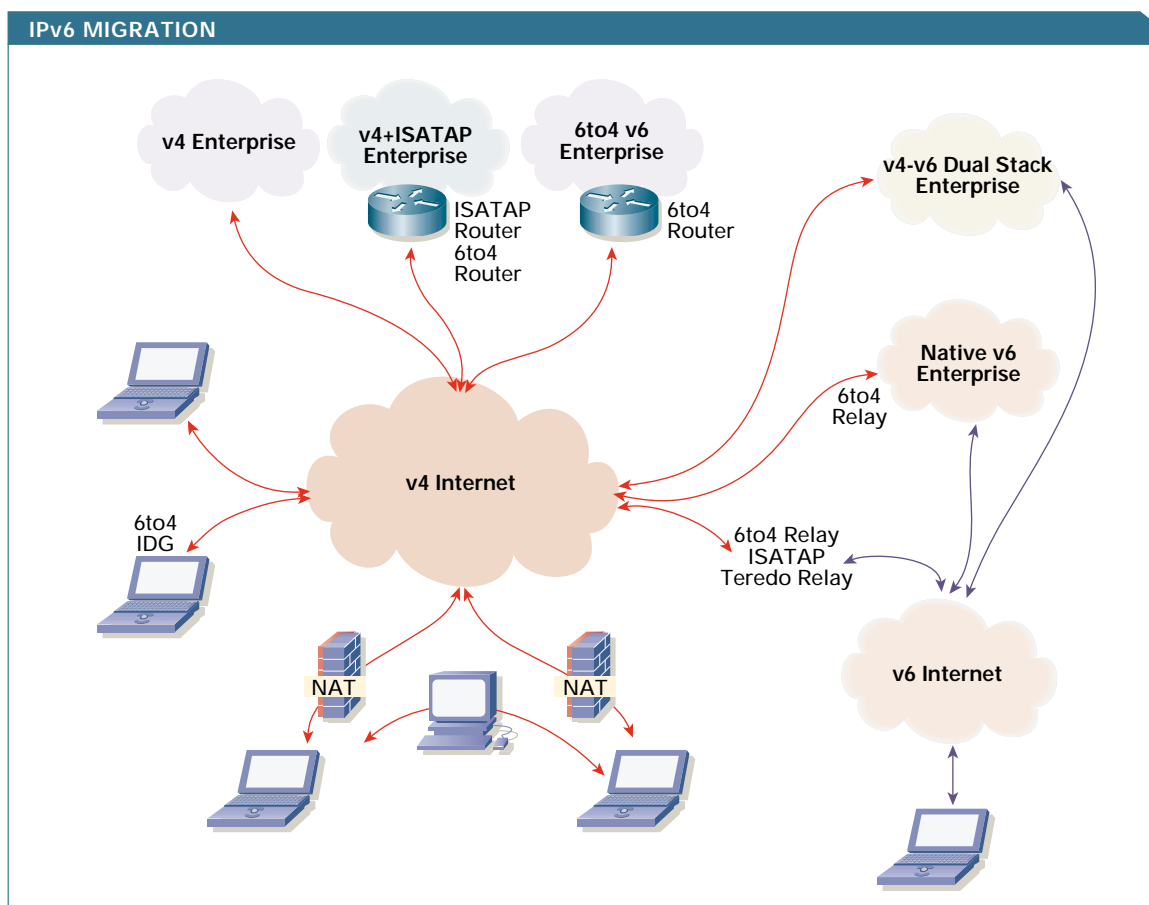
- 6to4 for PCs and access routers that have at least one public IPv4 address. 6to4 is typically configured by enterprises and allows tunneling of IPv6 traffic across the open Internet. 6to4 is included with Windows Server 2003, Windows XP SP1 and XP SP2, and Cisco IOS® Software releases.
- Teredo for PCs and devices that have private IP addresses, especially in the home. Teredo is a NAT traversal technology that provides tunneling between two hosts when one is behind an IPv4 NAT, and is also used on the open Internet. Microsoft includes Teredo support in The Advanced Networking Pack, a free add-on for Windows XP SP1, and is integrated into Windows XP SP2.
- ISATAP is an enterprise solution for campus networks which tunnels IPv6 packets across an intranet, enabling a smooth deployment of IPv6 devices even when the Layer 3 infrastructure is not yet fully IPv6-ready. Windows .NET server 2003, XP SP1 and XP SP2, and Cisco IOS releases include ISATAP and are fully interoperable.

To enable connectivity across the IPv6 Internet for the above users, many service providers have already deployed 6to4 relays and routers, and Teredo servers and relays into their networks. Deploying transition technologies is an inexpensive and fast way to gain operating experience with IPv6 and enable IPv6 applications with minimal disturbance to the existing network.

For example, a service provider only needs to deploy a Teredo server somewhere on the network to allow consumers who are behind NATs in their homes to begin using IPv6 applications. One example of an IPv6 application is 3Degrees (threedegrees.com), a



LEIGH HUANG is an IPv6 Program Manager in Windows Networking and Device Technologies at Microsoft. She holds an MSEE from MIT, and a BSCS from the University of Washington.



V4/V6 COEXISTENCE STRATEGY Many transition technologies are now included in vendor's products to enable the migration to IPv6, including ISATAP, Teredo and 6to4. Simple migration can actually begin today at the network edge without requiring costly infrastructure upgrades.

peer-to-peer, collaborative, and file-sharing application. When the 3Degrees application is downloaded to an IPv6-capable Windows XP machine, the application automatically turns on the Windows IPv6 capability—in essence, the machine becomes an island of IPv6. If somebody else also runs the 3Degrees application, these two users can begin to share music files or photos or set up a social group with other 3Degrees users. The main advantage is that the machines are talking peer-to-peer using the unique features of IPv6 to allow real-time control of music sharing between users. And best of all, these users are doing this without requiring any infrastructure upgrade by their service providers.

ISATAP is targeted for enterprise campuses. Hosts running Windows 2003 Server, Windows XP SP1, or XP SP2 with ISATAP can directly communicate using IPv6 even though the overall campus infrastructure is still based on IPv4. Packets from these hosts can then reach the external IPv6 Internet through a Cisco IOS router configured with ISATAP on a tunnel interface.

One of the goals of the Microsoft corporate network is to be an IT showcase for IPv6 deployment. All

users have access to IPv6 connectivity. The majority receives IPv6 connectivity through ISATAP servers, while some buildings have routers with dual stack IPv4 and IPv6 capabilities. Microsoft's IT organization is working with industry leaders, such as Cisco, to continue to pilot, deploy, and expand enterprise IPv6 operations.

With these transition technologies, the network does not need to change in order to begin deploying IPv6 applications. In effect, there is not a mutual dependency between network upgrade and application development.

Beyond these transition technologies are more extensive upgrades to the network infrastructure that will come in the near future, including dual stack and native IPv6. Dual IPv4/IPv6 stacks work well with legacy systems and will enable a gradual infrastructure upgrade through normal product life-cycle upgrades.

Native IPv6 offers the highest network capability and end-user benefit, and will provide the most sustainable network over the long term. Though it will require significant upgrades, careful planning will enable a strategic transition of the network and its applications to a viable, long-term infrastructure.

IPv6 stacks are included today in the following Cisco core routers: CRS-1, 12000, and 7600 series, and Layer 3 switches, including the Catalyst 6500, 4500, and 3750 series. Learn more at cisco.com/packet/164_5a2.

Developer's Perspective

The ease with which users can begin to use IPv6 applications based on transitional technologies mentioned earlier means a market is ready for early developers. As the peer-to-peer model is restored on the Internet, and applications are able to address and identify each device individually, along with the autoconfiguration and mobility features, many new opportunities will become available. Markets such as gaming, mobility, and telematics are only a handful of these potential new opportunities. Telematics, which is the use of a wireless network to support the collection and dissemination of data, will see tremendous growth.

Already, Matsushita Electric Works in Japan is making plans to intelligently control buildings and homes with IPv6. According to Junji Nomura, member of the board and director of new business development at Matsushita, "Toward 2005, Matsushita is developing a new business around device control systems through the network, based on open standards and IPv6. It will be oriented to homes and buildings that have equipment and devices needing ongoing service." In this scenario, customers will plug their IP-addressable refrigerators, washing machines, and other appliances into the network and the service will become available. According to

Nomura, this need to address all of these individual devices is why the service will require IPv6.

This scenario suggests that IPv6 will be initially deployed at the edges of the network and will gradually migrate inward toward the core. The combination of deploying transition technologies and migrating applications to be IPv6-capable is the key to getting started. This can be done easily and inexpensively today.

At a minimum, developers should begin by creating IPvX-agnostic applications. As the market and the infrastructure evolve, applications will move into the enterprise space. For those developers wanting to compete in international markets, IPv6 will be a critical capability. ■

FURTHER READING

- Cisco IPv6 Website
cisco.com/ipv6
- Microsoft IPv6 Website
microsoft.com/ipv6
- IPv6 Transition Technologies white paper
cisco.com/packet/164_5a1
- IPv6 Style: For people who learn, build, and use IPv6
www.ipv6style.jp/en/index.shtml

**TAKE YOUR NETWORK,
YOUR COMPANY AND
YOUR CAREER TO
THE NEXT LEVEL.**



NETWORKERS

"The ability to interact with Cisco technical staff who develop equipment, protocols and applications is unprecedented in our area."

—Rafaela Delgado, Banco de Crédito, Bogotá

BEIJING, CHINA
November 4–5, 2004

TOKYO, JAPAN
December 8–10, 2004

CANNES, FRANCE
December 18–19, 2004

SEOUL, KOREA
March 8–10, 2005

LAS VEGAS, NEVADA
June 19–24, 2005

GOLD COAST, AUSTRALIA
September 18–22, 2005

Learn more at www.cisco.com/go/networkers

Secure MPLS-Based VPNs

MPLS-based VPNs provide comparable security to Frame Relay and ATM.

By Michael Behringer and Stephen Wong

Enterprises attracted to the service benefits and potential cost savings of managed virtual private network (VPN) services based on Multiprotocol Label Switching (MPLS) can also enjoy security levels comparable to Frame Relay and ATM technologies. Proper design and deployment of the provider MPLS network—as recommended by Cisco and implemented by Cisco Powered Network service providers—makes common attacks such as denial of service (DoS) and spoofing either difficult or impossible to perpetrate.

There are several commonly held—and false—beliefs about the security of MPLS technology. Chief among them is the perception that IP-based MPLS is intrinsically insecure. In fact, MPLS augments native IP-based networks with a broad spectrum of route separation, data separation, packet filtering, and network concealment mechanisms to enhance security.

Another common misunderstanding is that service provider customers can intrude into each other's VPNs. This is impossible, because MPLS VPNs are completely isolated from each other. A third misperception is that MPLS VPNs are susceptible to outside DoS attacks. Again, not true. Pure MPLS VPN networks are fully secured. MPLS cores that also provide Internet access are completely safe from DoS attacks if the provider edge router only provides VPN access.

An additional common concern is that even a provider edge router used exclusively for VPN services is susceptible to DoS attacks. While theoretically

true, this concern is unfounded in practice, because it is easy to identify and disconnect any offenders.

No Address Changes

A managed VPN service should not require major changes to an enterprise's internal network, desktops, or servers. Most enterprises use a private IP addressing plan. For cost and security reasons, they want to retain the plan when they migrate to the shared network environment of a managed IP VPN service. MPLS allows distinct VPNs to use the same address spaces (RFC 1918). It enforces routing separation by adding a 64-bit route distinguisher to each IPv4 route, so that even a shared address appears unique within the MPLS core. Every VPN customer and the MPLS core itself can use the entire IPv4 address range completely independently.

Routing and Data Separation

MPLS achieves routing separation in two ways. One way is to assign each VPN to a Virtual Routing and Forwarding (VRF) instance. Each VRF on the provider edge router is populated with routes from a unique VPN, either through statically configured routes or through routing protocols that run between the provider edge and customer edge routers. Another way is to add unique VPN identifiers, such as a route distinguisher, to multiprotocol Border Gateway Protocol (BGP). Multiprotocol BGP exchanges VPN routes between associated provider edge routers, which keep routing information in VPN-specific VRFs. Routing across an MPLS network remains separate for each VPN.

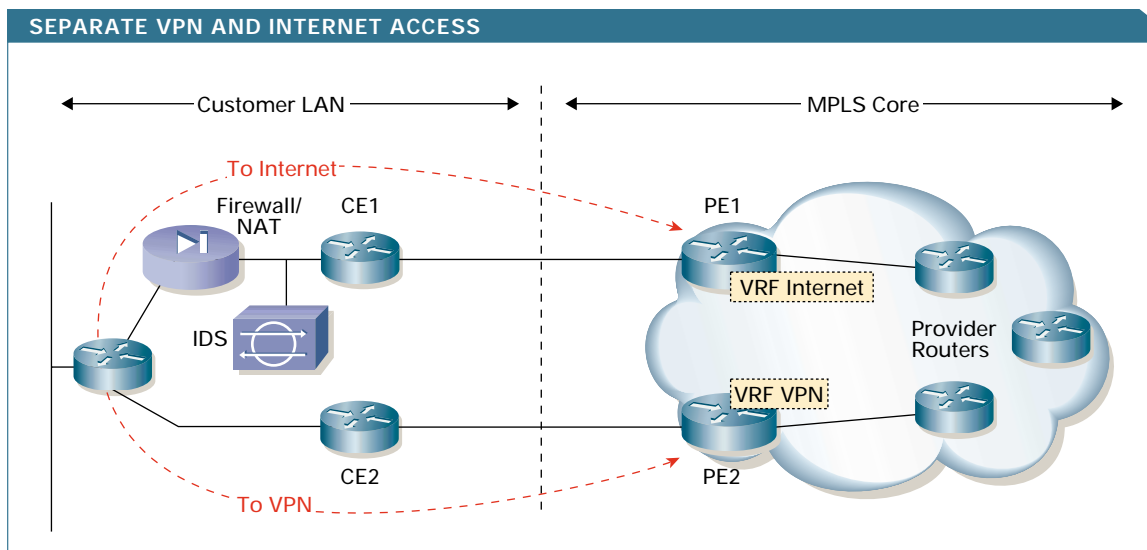
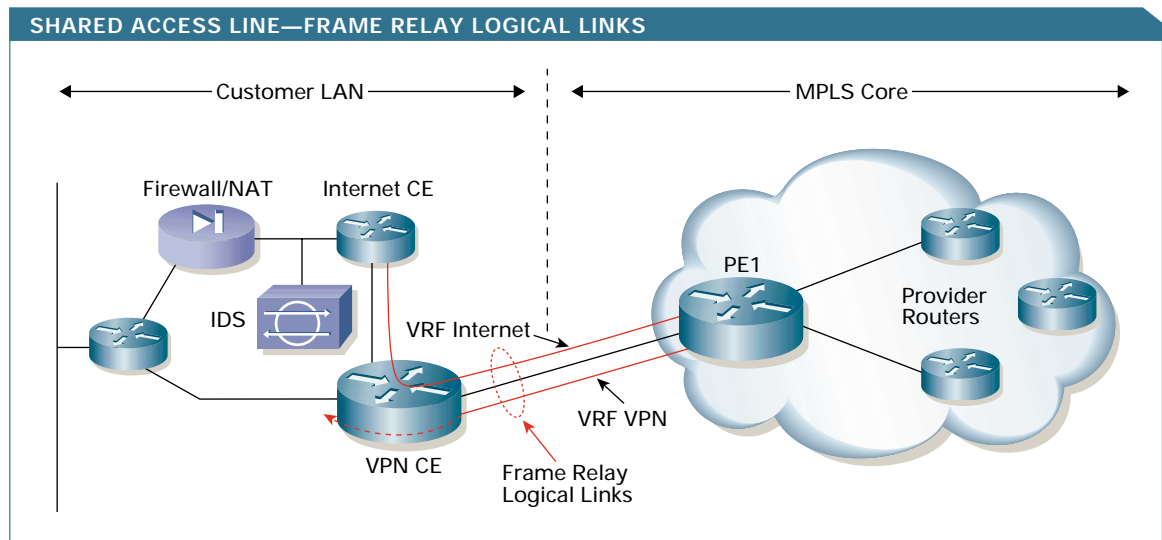


FIGURE 1 For maximum security against DoS attacks in the VPN, enterprises can provision separate VPN and Internet access connections to the provider edge, mimicking Frame Relay or ATM provisioning.

FIGURE 2 Enterprises can control costs and separate VPN and Internet access services with multiple Frame Relay logical links over a single link between customer and provider edges.



MPLS VPNs perform data separation at Layer 3 through separate IP VPN forwarding tables. Forwarding within the service provider core is based on labels. MPLS sets up label-switched paths (LSPs) that begin and terminate at provider edge routers. A packet can enter a VPN only through a provider edge router interface associated with that VPN, and the interface determines which forwarding table the router uses. This separation of address plans, routes, and data provides MPLS VPNs with the same level of security as Frame Relay or ATM VPNs.

Concealing the Core

Hiding the MPLS core network from the outside world renders it much more difficult to attack. MPLS conceals the network core by both filtering packets and not revealing network information beyond its own borders. Packet filtering prevents exposure of any information about the VPN customer's internal network or the MPLS core to the outside. Because only the provider edge routers contain VPN-specific information, it is unnecessary to reveal internal network topology information. Rather, the service provider only needs to reveal the address of the provider edge router, which is required by dynamic routing protocols between the provider edge and customer edge.

In cases of dynamic route provisioning, when customer VPNs must advertise their routes to the MPLS network, there is no compromise to network security, because the core only learns network routes, not specific hosts. An MPLS VPN environment thwarts attackers because the provider network does not reveal addressing information to third parties or the Internet. In a VPN service with shared Internet access, the service provider can announce routes using Network Address Translation (NAT). This approach reveals the same amount of information to the Internet as a typical Internet access service does.

Resisting Attacks

Service providers filter packets and hide addresses to prevent their routers from being reachable. Access control lists (ACLs) confine access only to routing protocol ports from the customer edge router. Outside hackers might attempt to penetrate the MPLS core and use it to attack Layer 3 VPNs through a direct attack on a provider edge router, or by attacking MPLS signaling mechanisms. Proper router configuration can prevent both of these assaults.

Element addresses are hidden from the outside, but internal hackers may resort to guessing them. MPLS address separation mechanisms treat incoming packets as belonging to the address space of a VPN customer, so it is impossible to reach a core router by guessing its address, because it is logically invisible.

Through routing configuration, service providers can prevent direct attacks on the known peer interface of the provider edge router. Static routing is the most secure approach. In this case, provider edge routers drop dynamic route requests. A static route points to either the IP address of the provider edge router or to an interface of the customer edge router. When the route points to an interface, the customer edge router does not need to know any IP addresses in the core network, not even the address of the provider edge router.

Dynamically routed links between customer and provider edge routers are vulnerable, because each customer edge router needs to know the router ID or

Read "Analysis of MPLS-Based IP VPN Security: Comparison to Traditional L2VPNs such as Frame Relay and ATM and Deployment Guidelines" at cisco.com/packet/164_5b1.

MICHAEL BEHRINGER, a senior consulting engineer at Cisco, based in Nice, focuses on service provider security issues, such as MPLS security and DoS attack prevention. He is an active member of the IETF and can be reached at mbehring@cisco.com.

STEPHEN WONG has 20-plus years in the service provider and networking industry. At Cisco, he has held several positions in service provider marketing, covering MPLS, IPSec, Layer 2, and Layer 3 VPN services. He can be reached at stepwong@cisco.com.

peer IP address of the provider edge router. Cisco recommends several ways to fortify this connection:

- If possible, use BGP between the customer and provider edge routers, because it offers the most advanced security capabilities for this application. To add stability, BGP has multiple countermeasures, such as prefix filtering and dampening.
- Use ACLs to limit access only to the port(s) of the routing protocol, and only from the customer edge router.
- Configure Message Digest Five (MD-5) authentication for routing protocols to prevent spoofing.
- Configure a maximum number of routes accepted per VFR.

Spoofing Impossible, Encrypted Communications

Spoofing attacks are an attempt to change routing information or gain access to authentication sequences, then use this information to attain unauthorized access. While a VPN customer can perform IP source address spoofing in an MPLS environment, the strict separation between VPNs and between VPNs and the core makes it impossible to use this mechanism to attack other VPNs or the core. Likewise, label spoofing is useless—provider edge routers automatically drop labeled packets received from a customer source.

Enterprises have the option to send encrypted traffic through a properly configured MPLS core, enabling regulatory compliance and enhancing data security. Encryption operates between customer edge routers. MPLS and IP Security (IPSec) encryption work well in combination, but proprietary or application-level encryption schemes are also compatible if packet payload is transparent to the service provider network.

Provisioning Options

Enterprises can exercise tradeoffs between security and cost when provisioning a connection between their network and the provider edge. In all cases, the provider maintains full control over VPN separation. The provider edge treats the customer edge as untrusted and only accepts pure IP packets from the customer edge. In most deployments, service providers offer both VPN and Internet access services over the same core, and security is acceptable when the service provider takes appropriate security measures as recommended by Cisco. In most MPLS VPN deployments, VPN services are offered with the option for Internet access over the same core. With Frame Relay and ATM cores, in contrast, providing both services requires two separate infrastructures, which increases costs.

The most secure, and most expensive, provisioning scenario is complete separation between VPN and Internet access for a single site, much like a Frame Relay or ATM model (Figure 1, page 21). The customer buys two edge routers and two WAN access lines, and these

enter the provider network on separate edge routers. This scenario insulates the VPN network from any DoS attack over the Internet connection.

Another deployment scenario converges VPN and Internet access services at the provider edge. The customer buys two edge routers and two access lines, but they feed into separate VRF interfaces on the same provider edge router. This scenario is less expensive than complete separation, but offers comparable protection against DoS attacks on the VPN.

In another provisioning option, enterprises can use a single access line for both services to reduce WAN line costs. This option is less resistant to DoS attack because the infrastructure supporting both services is shared; however, the risk is more theoretical than practical, because the service provider can control access with correct configuration of both customer edge and provider edge routers. A typical single-line scenario uses a single Frame Relay access line with dual logical links and separate subinterfaces on both the customer and provider edge routers (Figure 2). Internet traffic is switched to the Internet customer edge router. The customer edge VPN router maintains separation of VPN traffic via the VPN logical interface and never sees Internet traffic as it is switched to the Internet customer edge router.

Ask Your Service Provider

Enterprises can evaluate the security qualifications of a service provider's MPLS VPN offering by asking them the following questions:

Are Internet and VPN access provided over the same core network? While a VPN-only service is most secure, a shared core network is usually secure enough for most enterprises.

Do you offer separate provider edge routers for Internet and VPN services? A converged provider edge router presents a slightly higher risk of exposure to DoS attacks. Hackers cannot breach VPN separation whether the provider edge router is shared or separate from Internet access services.

How do you secure the core? A Cisco Powered Network provider follows Cisco security best practices for securing an MPLS network, making its VPN service as secure as it would be over Frame Relay or ATM. ■

FURTHER READING

- TechTalk: "Understanding MPLS VPN Security"
cisco.com/packet/164_5b2
- Engineering Report MPLS VPN by Miercom for Cisco
cisco.com/packet/164_5b3
- IETF Internet-Draft "Analysis of the Security of BGP/MPLS IP VPNs"
cisco.com/packet/164_5b4

SERVICES AT WIRE SPEED

ACCESS ROUTING GETS AN ARCHITECTURAL MAKEOVER.

DISTRIBUTED enterprises have begun seeking a greater degree of network-technology integration in their branch sites. The main reason is that organizations continue to splinter into numerous, far-flung locations that use virtual private network (VPN) connections to access data and, increasingly, voice applications and resources. This trend toward the “extended” enterprise has IT and upper management keenly focused on optimizing and future-proofing branch-office network configurations, which now represent a significant chunk of network total cost of ownership (TCO). And technology integration can be a boon to lowering TCO.



Reliance on the network for basic business survival (see Figure 1) has also swung the spotlight around to the issue of network performance and security at branch sites. No longer is it just the revered data center and headquarters LAN that require world-class security, optimum availability, and wire-speed throughput. Now, branches and remote offices—especially those expected to generate revenue—are being elevated to equal status in terms of network performance expectations.

Specifically, the following circumstances are among the drivers behind network technology reassessment and, in many cases, technology integration:

- Security concerns associated with broadband Internet connections have escalated such that each site needs multiple types of protection. Among them: encryption, firewall filtering, antivirus protection, and intrusion detection/prevention.
- Most enterprises have either deployed voice over IP (VoIP) or have put it on their roadmaps. Eventually, they will want to extend the capability to all remote sites, allowing for consistent IP PBX features, converged VoIP/data applications, and telco savings.
- Convergence of multiple application types on a single WAN access link has spurred greater use of network analysis and traffic management tools—available in Cisco IOS® Software, for example—to ensure strong quality of service (QoS) for each application.

To perform all of these and other network-related tasks, it is often not practical, affordable, or manageable to install multiple standalone appliances at every site.

“Most enterprises have a limited number of IT staff to manage large numbers of branch offices,” observes Joel Conover, principal analyst of enterprise infrastructure at Current Analysis, a networking research firm and consultancy in Sterling, Virginia. “Setups must be kept as simple as possible in terms of managing configurations and limiting the number of devices that might fail.”

For example, he says, management, budget, and configuration requirements usually dictate that enterprise customers don’t want a stack of security appliances at every office.

Still, enterprises have typically deployed some number of separate devices in these sites, because once the access router assumed a certain number of tasks, network performance suffered. An organization would need to decide whether to invest in multiple pieces of equipment at a particular location—and the staff to manage them—or to bundle all the network services required into router software and interface cards, but sacrifice some throughput.

Security at Full Throttle

As enterprises increase the number of VPN connections at remote sites, it has grown imperative for them to gain the ability to combine the benefits of streamlined, router-based configurations with wire-speed performance, regardless of which network services are activated. Performance-wise, encryption acceleration and voice processing loads have traditionally been the most burdensome for the router to handle.

Enter the newly launched WAN access routers in Cisco’s Integrated Services Router series. The architecture of these devices relieves users from having to

choose between throughput and the capital (CapEx) and operational (OpEx) efficiencies of an all-in-one platform.

Specifically, the Integrated Services Architecture of the Cisco 1800, 2800, and 3800 Series (see article, “Security, Services, and Speed . . . Oh My!” on page 29) offloads encryption acceleration and, optionally, analog and digital voice processing, directly onto the access router’s motherboard. These processing improvements, general CPU and memory enhancements, and faster interfaces enable the router to continue forwarding packets at wire speed no matter how many additional network services run concurrently.

With this architectural development, Cisco believes it is the first company to embed both security and voice into a single routing configuration without relinquishing any performance.

The routers also support the option of bundling in Layer 2 Ethernet switching for further consolidation of equipment, complete with IEEE 802.3af-standard power-over-Ethernet (PoE) support. This further simplifies network configuration at smaller sites, thereby helping enterprises and small businesses reduce both CapEx and OpEx.

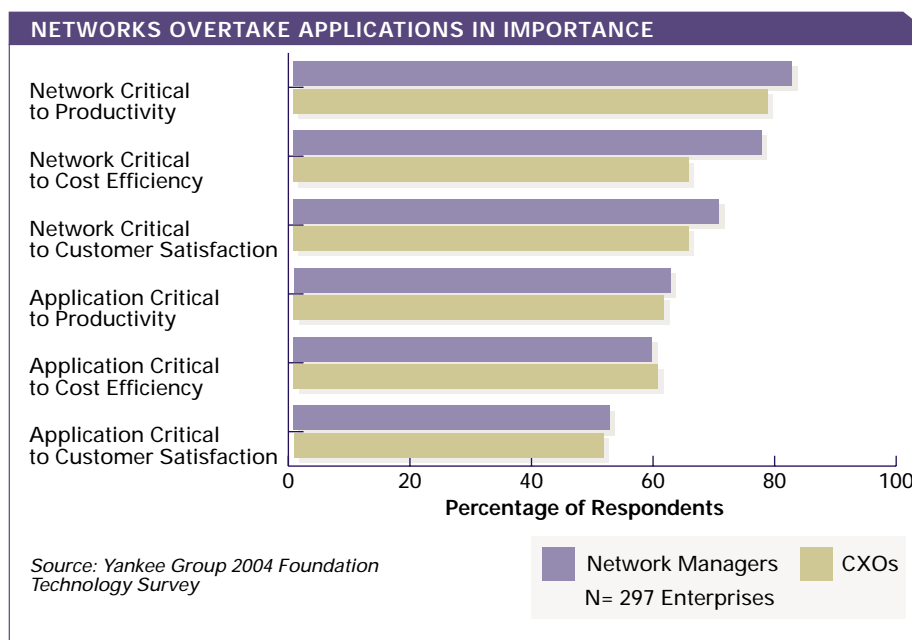


FIGURE 1 Network managers and CXOs alike now rate the network as more critical to productivity, cost reduction, and customer satisfaction than applications.



And, by adding extra wiggle room with memory, processing power, and the embedded voice processing and acceleration option, the design future-proofs the platform for converged applications. So enterprises can bank on having their access routers in place for at least four to six years, says Mike Volpi, senior vice president and general manager of Cisco's Routing Technology Group.

Not having to swap out equipment reduces TCO in several ways, according to a July 2004 report published by The Yankee Group, a networking consultancy in Boston, Massachusetts, entitled, "Looking Ahead When Making Network Foundation Purchases Leads to the Right Choices."

Among the ways a longer product lifecycle reduces TCO is by lowering network downtime due to product changes, by decreasing CapEx, and by requiring staff skills to be upgraded less frequently, the report says.

"Cisco Integrated Services Routers provide five times the service density, seven times the performance, and four times the memory of the previous generation of routers, ensuring that customers will have the capacity they need as their businesses grow," Volpi says.

Overhaul Overdue

The access routing industry has been due for an architectural overhaul of this nature, according to Jeff Wilson, principal analyst at Infonetics Research in San Jose, California. "Routers have had plenty of features, but turning them all on meant that the router would stop working," he says.

"The question has been how to integrate everything and make sure the routers perform adequately. With the Integrated Services Routers, now we can have firewall appliance-strength [performance] for security, for example, in access routers," Wilson says.

A recent study by Infonetics revealed that enterprises are driven to invest in emerging router technology to increase security and decrease downtime. In addition, more than three-fourths (77 percent) of the enterprises surveyed already used some degree of integrated security. Users require more integrated security services at the WAN edge these days largely due to the influx of viruses, malicious code, and end users picking up infections on their laptops. Cisco Integrated Services Routers bundle not only IP Security (IPSec) VPN tunneling with Advanced Encryption Standard (AES)—the latest US National Institute of Standards and Technology standard for encryption—as well as with Triple Data Encryption Standard (3DES) and DES encryption, but Network Admission Control (antivirus protection), inline dynamic intrusion prevention, and high-performance stateful firewall filtering (see article, "Bundled Security," page 37). Dynamic Multipoint VPNs, for meshed IPSec networking, are also supported at wire speed.

"Branch offices are most susceptible to security issues," says Current Analysis' Conover. "Broadband Internet connections at home, and fast wide-area connections in the branch, make it simple for highly disruptive malicious code to get into the corporate network in a hurry, unlike the old days when branches had meager 64-Kbit/s leased or dialup lines."

The Voice Factor

Containing security risks is one reason to install a more intelligent router, Conover says. Voice is another.

"Cisco is the only vendor driving voice through a branch-office router today," says Conover. "It's a key differentiator that will give Cisco a 12- to 18-month advantage over the competition."

The advantage, he says, is that high-performance voice support in WAN access routers helps future-proof customer investments. "Cisco's solution positions voice in the branch-office router as a replacement

strategy for legacy TDM-based PBXs, which are increasingly proving more expensive to maintain," Conover says.

Voice services are embedded inside the router in new optional onboard and field-upgradable packet voice/fax DSP modules (PVDMs), to provide maximum deployment flexibility, while offering higher densities for stations, trunks, and conferencing. Call processing is based on Cisco CallManager Express, part of Cisco IOS® Software. Larger companies may choose to run call processing centrally with CallManager and use Survivable Remote Site Telephony (SRST) in the branch for uptime and reliability in the event of a WAN failure.

Extending CallManager-like features to the branch also helps customers eventually presence-enable their enterprises. "Presence" refers to real-time communication on a VoIP network that allows users to be contacted via their choice of device or application regardless of their whereabouts.

Presence applications such as instant messaging and short message service will enable employees to find and interact with others when needed and reduce communications costs, Conover observes. They should also boost productivity by decreasing time spent dealing with voice mail and e-mail, and scheduling conference calls.

Planning Ahead

The trend toward the "extended enterprise" shows no signs of abating. As such, branch and remote sites must be on par, from a network capability perspective, with their headquarters brethren. Given that the days of flush CapEx and OpEx budgets are behind us indefinitely, it is prudent to streamline configurations at numerous dispersed locations and make them as consistent as possible to ease manageability, so long as security, performance, and uptime are not compromised.

These enterprise goals are why a new generation of access routing architecture was in order, and how the resulting Cisco Integrated Services Routers series came about. The economics, performance, and future-proof nature of this milestone development should change the face of branch-office routing for several years to come. ■

SECURITY, SERVICES, AND SPEED... OH MY!

PART 1: THE ARCHITECTURE

By Janet Kreiling

IN SEPTEMBER, Cisco introduced a new line of next-generation access routers. Designed from the ground up to support the growing needs of enterprise branch offices, and small and midsize businesses (SMBs), the new Cisco 1800, 2800 and 3800 series Integrated Services Routers combine IP communications, virtual private network (VPN), firewall, intrusion prevention/detection, and many other services, all in one high-performing platform. This high degree of integration and unique design—encryption is offloaded from the CPU to separate silicon to speed up processing—allow multiple services of the customer's choosing to run concurrently, while still leaving plenty of room for growth. Even with the WAN link oversubscribed, one tester reports the CPU ran at only 74 percent of capacity. (See "Passing with Flying Colors" sidebar on page 34.)

Services at Wire Speed

To help define market needs for this new generation of routers, Cisco surveyed over 300 branch and SMB customers. "We asked customers what they wanted and we built it," says Mike Stallone, product line manager at Cisco. More than half wanted services and capabilities integrated into the routers, rather than having to deploy separate appliances. Highest on the list were security features: firewall, VPN setup, intrusion prevention/detection, and antivirus software, in that order. Next came IP telephony, followed by compression, content filtering, caching, quality of service (QoS), streaming, and multicasting.

Heirs apparent to the Cisco 1700, 2600, and 3700 series, all three lines in the Integrated Services Router series boast what Stallone refers to as "encryption at wire speed." Encryption and decryption are offloaded from the central processor onto application-specific integrated circuits (ASICs) in the Cisco 2800 and 3800 series, and onto a field-programmable gate array (FPGA) in the Cisco 1800 Series—and thus from software to hardware. Since encryption/decryption chews through processing power, this significantly improves CPU throughput and makes it possible for users to deploy a previously unheard-of number of concurrent services.



Chris Fairbanks, principal network architect at ePlus, and Cisco 3825 Router customer. See story, page 32.

**NEW CISCO INTEGRATED SERVICES ROUTERS
OFFER SECURE, WIRE-SPEED DELIVERY OF CONCURRENT
DATA, VOICE AND VIDEO SERVICES.**

As one measure of encryption performance, the new Cisco 1841 Router can support up to 800 VPN tunnels; the Cisco 2800, up to 1500; and the Cisco 3845, up to 2500 VPN tunnels.

According to Mike Wood, Cisco Integrated Services Routers voice product line manager, the ASIC and FPGA also contain a switch that can direct streams of voice traffic to various components on the motherboard, or to modules plugged into slots in the router. This specialized silicon also enables direct memory access between optional digital signal processors (DSPs) and on-board memory, further offloading the CPU.

Future-Proof Integration

While their performance is impressive, services integration is the next-generation routers' defining characteristic. The Cisco 1800 and 2800 series, which run Cisco IOS® Software Release 12.3(8)T, and the Cisco 3800 Series, which runs IOS Release 12.3(11)T, bring together many security features on the motherboard, such as Network Admission Control (NAC) for antivirus protection, and intrusion prevention.

The Cisco 2800 and 3800 series can also function as voice messaging-enabled small PBXs or key systems with Cisco CallManager Express (an IOS application) and Cisco Unity Express. These new routers are the first to integrate DSP slots directly inside the router. The DSP slots are activated using innovative packet voice/fax DSP modules (PVDMS) that also provide conferencing, transcoding and secure voice features.

Further integration is achieved by adding a variety of other modules that expand their capabilities: advanced integration modules (AIMs), network modules or enhanced network modules (NMEs), and high-speed WAN interface cards (HWICs). The Cisco 2821 and 2851 routers also have dedicated slots for extension voice modules (EVMs), which deliver analog and BRI voice connectivity without sacrificing a network module slot. EVMs also function in any NME slot on the 3800 Series. The routers also have integrated Fast Ethernet and/or Gigabit Ethernet ports, as well as USB ports.

"Customer demands are growing all the time," says Brian Ryder, product line manager and Integrated Services Router architect. "Initially many of them wanted just security and IP voice. Now they want more security—intrusion prevention, encrypted VPNs, Network Admission Control—and also software distribution, messaging, local content caching, and others. The number and variety of these slots enable customers to have essentially all the services they want."

Ryder also points out that "each feature intelligently knows about the others, whereas in an appliance environment, they may not. For example, without this level of integration, the functionality that sets up VPNs may not know about the QoS, so it may not perform the needed preclassification of packets. You can do things with an integrated platform you could never do with a group of appliances."

Network awareness is a capability that David Willis, senior analyst with the Stamford, Connecticut-based META Group, sees not only as useful, but essential. "Cisco Integrated Services Routers possess the intelligence to be aware of and optimize operations for specific applications," says Willis. "They can recognize if an application requires a certain QoS priority, for example, and apply the technologies to ensure it receives fair access to the network. If it's desirable, they can apply compression to the traffic for a given application."

Integrated for Security

Number one on most survey respondent's list, security in the new line of routers is focused on four key areas: *secure connectivity*, *threat defense*, *trust and identity*, and *protection of network infrastructure*.

Secure connectivity is delivered through VPN tunneling and encryption; dynamic multipoint VPNs (DMVPNs); Easy VPNs; voice, video, and data VPNs (V³PNs); and multi-VPN Routing and Forwarding (multi-VRF) capabilities.



DMVPNs are a particularly interesting capability, Willis says. "They change the way users think about VPNs. Historically, if they were built over the Internet, management was time-consuming and cumbersome. Larger enterprises tended to use private solutions such as MPLS or frame relay networks. But DMVPNs raise the bar for Internet VPNs. They're set up and taken down automatically, which makes using the Internet feasible for much larger sites, saving costs."

Threat defense is provided by the Cisco IOS Software security feature sets, which include the Cisco IOS firewall, the new transparent firewall, intrusion prevention, antivirus defense via NAC, URL filtering, and content security. The IOS firewall is a stateful inspection program that includes denial of service protection; enhanced awareness of applications, traffic, and users; advanced protocol inspection for voice, video and other applications; and per-user, interface or sub-interface security policies. The transparent firewall enables the Integrated Services Routers to provide Layer 3 protection for Layer 2 connectivity.

They are also the first routers in the industry to offer inline intrusion prevention. As part of Cisco IOS Software, the Intrusion Prevention System (IPS) is an inline, deep-packet inspection service that stops intruders before they get into the access network. Leveraging technology from Cisco's Intrusion Detection System Sensor appliances, IPS offers a very wide range of signatures against common viruses and worms, and permits users to choose those most appropriate for the equipment and operating systems they're using.

To further enhance inbound security, users may want to install Cisco's Intrusion Prevention System and/or the content engine network module for content security. The latter also includes destination URL filtering. As Stallone says, "security really has two parts: security to protect incoming signals, and privacy to protect what information goes out."

Trust and identity are confirmed through IOS features such as NAC for antivirus defense, and authentication, authorization, and accounting (AAA), and also by removable credentials. NAC enables a branch or SMB to ensure that every endpoint—

even a mobile unit or home office—conforms to prescribed security policies.

“The feature is valuable because the network itself becomes more host- and user-aware,” Willis says. “That will reassure many companies that now feel that if they open up a pipe, they lose control of who and what goes over it.”

AAA allows administrators to establish and maintain access control dynamically on a per-line or per-user basis. USB ports, integrated into the Cisco 1800, 2800 and 3800 series, can be configured to work with an optional USB token for secure configuration distribution and off-platform storage of VPN credentials. With this separation, the administrator can ship the router and token separately for greater security. (USB capabilities will be available in the first quarter of 2005.)

Individual network devices and the network overall are further protected through features such as Network-based Application Recognition (NBAR), Secure Shell Version 2 (SSHv2), Simple Network Management Protocol version 3 (SNMPv3), and role-based Command-line Interface.

Protection of network infrastructure is accomplished with the Cisco Router and Security Device Manager (SDM), an intuitive, Web-based management tool for Cisco IOS Software-based routers. While Version 1.0 has been available for about a year in certain router packages, Ranjan Goel, product manager at Cisco, points out that now “SDM is going mainstream, and version 2.0 will ship on all of the Integrated Services Routers.”

Configuring security has become complex, Goel says, with “lots of interrelationships, such as between security settings on the LAN and the WAN, or Network Address Translation and the firewall.” Moreover, the administrator must “execute security across the network end to end.” With SDM, administrators can configure routing, switching, QoS, and other services easily, and also monitor network performance.

SDM makes use of all of the “know-how” acquired by Cisco’s Technical Assistance Center (TAC) in the form of smart wizards that significantly reduce configuration errors. “If an error is made, a wizard will flag it and suggest corrective action,” Goel says. In addition, one click dispatches a security audit wizard to check that all of TAC’s detailed recommendations on securing routers have been followed—a task that previously could have taken hours.

For more on the integrated security features and functionality of the Cisco Integrated Services Routers, see “Bundled Security” on page 37.

Integrated for Multiple Services

Each module or card slot on the router can be used for more than one purpose, so the user can mix and match to get just the right combination of services. For example, a network module or enhanced network module can be used to provide voice messaging and auto attendant with Cisco Unity Express, throughput up to 1.2 Gbit/s on a Cisco 3800 Series, URL filtering, power over Ethernet, higher density for analog voice calls using the extension voice module (EVM), and other functions. Advanced integration modules (AIMs) can also be used to deliver voice messaging and

auto attendant (via Cisco Unity Express), a VPN accelerator, additional security features, additional encryption, signal compression, ATM segmentation and reassembly, and other capabilities.

Into the high-speed WAN interface card (HWIC) slots, the user can slide HWIC cards, which transmit wire speed connectivity, or other WAN interface cards (WICs) that operate at lower speeds—WICs from earlier router models can be reused as well, providing backward compatibility. The HWIC slots can also accept Voice Interface Cards (VICs) for PRI, PSTN, voice over frame relay, voice over ATM, and voice over IP, as well as power over Ethernet. The packet voice/fax DSP modules (PVDMM) can support voice, fax, video, conferencing, and transcoding. Ethernet ports support Fast Ethernet LANs at 10 or 100 Mbps on the smaller systems, and Fast or Gigabit Ethernet LANs on the larger systems. The dedicated EVM slot in the 2821 and 2851 routers can accept modules that significantly increase the number of analog phones and analog/BRI voice trunks supported.

Given the variety of module and card slots, network managers can deploy a wide array of services tailored to the specific needs of each branch or SMB. For example, a Cisco 2821 customer might use the system’s EVM module to support more voice lines, saving the network module slot to boost throughput or add video streaming. The PVDMM slots would handle IP voice termination, and the built-in AIM slots could be used for VPN acceleration, compression, or voice messaging and auto attendant via Cisco Unity Express.

A user of the top-of-the-line Cisco 3845 Router has the highest services density and flexibility. The router’s four network module slots can be used for a variety of services, such as Ethernet switching with Power over Ethernet, voice messaging—up to 100 mailboxes—along with auto attendant, content caching, and network analysis. Dual 802.3af power supplies provide redundant chassis and inline power.

Users of the Cisco 1841 can choose from more than 30 WICs for data connectivity—perhaps choosing to support T1 data with one HWIC slot, and a slower link to a Frame Relay network with the other. The AIM slot provides the power of VPN acceleration.

All told, Cisco offers more than 90 different modules and cards that fit into various slots, according to Jennifer Lin, product line manager at Cisco. This flexibility greatly expands the potential applications of the new routers, while still offering ease of management, lower costs, and faster deployment. Many of the network modules have embedded processors and hard drives that permit them to run largely independent of the router’s CPU, further off-loading work, yet they can be managed through the same interface. “Customers have the flexibility of using intuitive Web browser-based management tools or CLI [command-line interface], whichever suits their needs,” explains Lin.

Being able to run different multiple WAN interfaces is a big deal, Ryder points out. “We’re offering one chassis that customers can standardize on, knowing that it’s flexible enough to deal with pretty much any WAN environment that comes along.” Even legacy systems back to DECnet and Token Ring are supported. ■



Kevin Seim, Senior Marketing Manager, BellSouth

SECURITY,
SERVICES,
AND SPEED...
OH MY!

PART 2: THE PLATFORMS

"THIS IS WHAT WE WOULD HAVE BUILT," SAYS ONE BETA CUSTOMER OF THE CISCO INTEGRATED SERVICES ROUTER. HERE'S WHAT THE REST HAD TO SAY.

By Janet Kreiling

WHERE the rubber meets the road is not just in branch offices and small to mid-sized businesses (SMBs)—where the business meets its customers (see Part 1, page 29). It is also when a product goes into actual service. Each of the platforms in the new Cisco Integrated Services Router series has been extensively beta tested, in both production environments at customer sites and by independent consultants. Says one user: "If we could have designed a router ourselves, this is what we would have built."

The Cisco 1800 Series

Kevin Seim, senior marketing manager at BellSouth, has been beta testing the new Cisco 1841 Integrated Services Router as potential customer premises equipment (CPE). He has no reservations about recommending the Cisco 1841 or the Cisco 2800 Series, which BellSouth has also tested. "They perform as promised," says Seim, who has run a full complement of services on both routers. "We're still not maxed out. There's plenty of room for growth."

The Cisco 1841 Router, Seim says, can support a variety of transport solutions including Ethernet, Frame Relay, ISDN PRI, and T1, which his company markets as BellSouth Megalink. Seim sees it as a "great platform for business enablement, especially for security and future growth." The router fits into his plans because it helps BellSouth to offer "all solutions, along with a suite of professional services and a wide variety of robust transport options that can work seamlessly with the router."

Customers, Seim points out, "are asking for flexible platforms. They don't want to be pigeon-holed with systems that are only good for certain functions." The Cisco 1841 Router is designed for offices that need secure, high-speed data services but plan to continue using traditional circuit-switched voice. Fitting easily on a desktop (it can also be wall-mounted), the Cisco 1841 offers a more than fivefold performance improvement over the Cisco 1700 Series routers. Among its specific features is integrated accelerated encryption hardware, enabled by an optional Cisco IOS® Software security image.

A virtual private network (VPN) encryption acceleration module can be added via its advanced integration modules (AIM) slot to boost encryption performance by a factor of two, and support up to 800 simultaneous VPN tunnels. The router can also host a wide range of WAN interface cards (WICs) and high-speed WAN interface cards (HWIC). Cisco IOS Software provides a complete suite of transport protocols and quality of service (QoS). “All told, the Cisco 1841 Router is an ideal system that integrates into one box all types of services,” says Mike Stallone, product line manager at Cisco. “All the functionality a small branch office or SMB needs, and it’s easy to maintain and manage. It’s the industry’s most robust and adaptable security solution available to SMBs and branch offices.”

The Cisco 2800 Series

Seim had equal success testing the Cisco 2800 Series: processing power to spare, lots of room for growth, excellent security. This series also fits into BellSouth’s Full Service Office solution for branch offices and SMBs. “The 2800 router is the platform for enabling the full-service office, because you can turn on services like IP telephony and advanced security,” says Seim. “And we’ve got services that will help you decide whether these solutions are right for you.”

Seim plans to include the Cisco Integrated Services Routers in BellSouth’s “soft bundling” program, which creates custom solutions by helping a customer determine whether a specific CPE or service is right for it. For example, BellSouth’s “IPT Snapshot” service simulates voice traffic on the customer’s existing data network to see if it can support high-quality telephony. “If so, we can download [Cisco] CallManager Express onto the router, either the 2800 or 3800 series,” explains Seim. “Using a proxy server and guide to an initial set of security services, we can also demonstrate advanced security services so as to create a comprehensive security profile.”

And, Seim adds, “I would finish this off to the customer by saying, ‘We’re not done yet. You’ve got plenty of room for future growth. These routers present a journey for the customer, not a destination. Customers will take these routers with them as their business grows.’”

IdleAire Technologies, which offers electrical, heating, ventilation, and air conditioning (HVAC), video, phone, and Internet service to truckers at truck stops and travel centers, has been beta testing the Cisco 2811, emulating the replacement of two current routers. The idea is to let truckers shut off their trucks overnight to save oil and cut pollution. According to Jon Duren, chief technology officer at IdleAire, “If every trucker did so it would save eighteen percent of the country’s oil reserves.”

Like the truckers who run their engines for ventilation (since truck stops often aren’t safe enough to leave the vehicle windows open), Duren says IdleAire’s particular communications concern is security. Its network incorporates several LANs at each site that have differing security requirements, for example, credit card transactions and first-run movies—both must be secure—and public Internet access, which need not be. Among the features he’s using are Network Address Translation (NAT) on the public access system; QoS so voice comes through clean and clear; and Network-Based Application Recognition (NBAR), to categorize services such as file transfers as lowest priority.

Security features include those that are available on the Cisco 1841 Router, plus an optional accelerated encryption

module that increases performance to the level of 2500 VPN tunnels. In addition, the Cisco 2800 Series supports V³PN for voice and video transmission with QoS enforcement over VPNs. The series also offers Dynamic Multipoint VPN (DMVPN) and Easy VPN for enabling more scalable and manageable VPN networks. The higher-end models can support more than six T1s/E1s running multiple services concurrently.

“Cisco has combined some products to reduce the number of pieces of equipment we will have to buy in the future, and has given us room to grow,” says Duren. “Even though we’re only running a T1 out to the site, the ability to support multiple LANs—enhancing the speed and throughput to support some LAN routing—is really a big plus. We’re doing quite a bit of heavy video; the ability to implement some protection among the LANs and still interconnect them efficiently is pretty valuable.”

The Cisco 2800 Series, which includes the 2801, 2811, 2821, and 2851 routers, also adds voice to data. Customers can use Cisco CallManager Express (CME) in IOS to provide IP voice services. Cisco CME provides calling services similar to a key system or small PBX, but as part of the data stream, so customers can deploy a converged voice and data network from

INTEGRATED SERVICES ROUTERS FEATURE COMPARISON

	1800 SERIES	2800 SERIES	3800 SERIES
WIRE SPEED	One T1/E1/xDSL	Multiple T1/E1/xDSL	T3/E3
HWIC SLOTS	2	2-4	4
AIM SLOTS	1	2	2
DSP SLOTS	NA	2 or 3	4
MAX. SRST IP PHONES	NA	96	720
NME SLOTS	NA	0 or 1	2 or 4
EVM SLOTS	NA	0 or 1	NMEs support EVMs
BUILT-IN FE/GE PORTS	2 FE	2 FE or 2 GE	2 GE
BUILT-IN USB PORTS	1	1 or 2	2
FORM FACTOR	Desktop	1 or 2 RUs	2 or 3 RUs
802.3af + POWER	No	Yes	Yes
DEFAULT DRAM	128 MB	128 or 256 MB	256 MB
MAXIMUM DRAM	384 MB	384 MB or 256 MB	1 GB
DEFAULT FLASH	32 MB	64 MB	64 MB
MAXIMUM FLASH	128 MB	128 MB or 256 MB	256 MB
SECURITY	Choice of eight IOS Software images that include voice and security features such as the IOS firewall, IPS support, IPSec, DES, 3DES, AES, VPNs, DMVPNs, NAC, Secure Shell (SSH) protocol version 2.0, and Simple Network Management Protocol (SNMP). Note: Cisco 1841 does not support voice features.		

a single platform. Cisco Unity Express can be added through the AIM or Enhanced Network Module (NME) slot for voice mail and auto attendant service. As part of the Cisco 2800 Series bundled voice offering, users also get Survivable Remote Site Telephony (SRST), so local calling can proceed even when the WAN link is down, or connectivity to a centralized Cisco CallManager is lost.

The dual AIM slots on the Cisco 2800 Series enable the user to install any two capabilities such as hardware-accelerated security, ATM segmentation and reassembly, compression, and voice mail/auto attendant. The NME slot can be used to boost throughput up to 1.2 Gbit/s. The Enhanced Voice Module (EVM) slot

provides support for up to 24 simultaneous analog voice/fax sessions without consuming an NME slot.

The integrated digital signal processor (DSP) slots enable feature-rich integrated IP telephony. They support analog and digital voice terminations, conferencing, transcoding, and secure Real-time Transport Protocol (RTP), while freeing up NME or AIM slots for other applications. They help enable packet voice technologies such as voice over IP (VoIP) protocol H.323, Media Gateway Control Protocol (MGCP), Session Initiation Protocol (SIP), voice over Frame Relay, and voice over ATM. These DSPs also deliver advanced echo cancellation, de-jitter buffering, and packetization.

The Cisco 3800 Series

ePlus, a US-wide firm based in Herndon, Virginia, helps businesses reduce the costs of purchases and purchasing, often through Web-based enterprise applications. It has been beta testing a Cisco 3825 Router in its Sunnyvale, California, branch office, linked back to a corporate data center in Ashburn, Virginia. Chris Fairbanks, principal network architect at ePlus, says the Integrated Services Router is actually in "full-blown production—we've migrated all our voice and WAN services over to it. We've also turned up content networking and IDS [intrusion detection system] services on the box."

PASSING "WITH FLYING COLORS"

Cisco Integrated Services Routers have been tested by two independent consultants, Mier Communications, based in Cranbury, New Jersey, and Current Analysis, based in Sterling, Virginia.

According to Ed Mier, president of Mier Communications (Miercom), "Our tests prove the Cisco 3845 Router simultaneously sustains full T3 WAN rates for multiple applications. Its embedded crypto processor handles both 128 AES and IPSec VPNs with ease, concurrently delivering firewall, intrusion prevention, QoS, and data routing at maximum WAN-link speeds. Additionally, an impressive 72 streams of voice traffic, including transcoding, voice mail, auto-attendant, fax, and Survivable Remote Site Telephony were handled with no performance degradation in the Cisco 3845."

Miercom reports that "an extraordinary mix of concurrent traffic streams was generated to exercise services running on the 3845, as well as QoS processing . . . With the full load of traffic mixes and streams running, the testers then manually established three real conference calls with four phones each, including VoIP and PSTN/analog stations; sent analog

faxes; placed secure RTP branch-to-headquarters calls; interacted with the auto-attendant; and placed and retrieved voice mail. These confirmed proper working of the services with high traffic loads."

In addition, the report says that "Miercom proudly attests to this system's performance, in particular:

- The Cisco 3845's ability to load a full T3 IP-WAN link [with AES/IPSec VPN encryption].
- Concurrent provision of key high-level network services to a busy branch office, including firewall/NAT, IPS, even content control (Web caching), VoIP and analog telephony services, while under heavy transport load.
- Assurance of quality voice service while under heavy data load, and smooth survivable failover to PSTN."
- Miercom reports similarly satisfactory performance for the Cisco 2851, Cisco 2811, and Cisco 1841 routers, which were also tested.

Current Analysis tested the Cisco 2821 router to validate claims of wire-speed performance of up to four T1s, according to Joel Conover, senior analyst. The load, says the Current Analysis report, "included basic and extended access control lists, stateful firewall inspection, IDS, point-to-point IPSec VPNs, GRE,

traffic classification via Layer 4 packet attributes, queuing for quality of service, H.323 call termination and VoIP toll bypass, and operating as a fully functional IP telephony key system using Cisco CallManager Express."

Not satisfied just with running the full load Cisco said the router could carry, Current Analysis tested it further by oversubscribing to the extent of seven analog calls, four VoIP calls, and music-on-hold and all services enabled. CPU utilization under those circumstances was only 74 percent.

"We pretty much tried to beat the router to death," Conover says. Each service, he points out, "was added individually and verified before another was added, and then we went back and tested everything together." He is confident that "if you're an enterprise, you don't have to worry about the router failing if you add another service."

There is, Conover adds, "nothing else available with this performance in this price range." And, he says, "Integration of encryption as it exists on this router is essential if you intend to use the CPU for other services."

Results? "It's been working great. We're seeing a five-fold improvement in performance. This is everything we need in one box. We're using DMVPNs with digital certificates, voice, fax, SRST, IDS, the firewall, NAT, and other features. We just don't have the personnel to deal with software upgrades and day-to-day maintenance on multiple boxes. Also, the content caching really speeds up applications for our employees." Fairbanks likes the Advanced Encryption Standard (AES) capability: "It's stronger and lighter than 3DES, although that doesn't matter on this router because it's so powerful." (See "Bundled Security," page 37, for more on AES.)

Fairbanks and his staff are considering putting a pair of Cisco 3845 routers into headquarters, both operating at T3 speed, and Cisco 2821 routers in five other offices. He's interested in more local caching, both for applications and software upgrades, and content networking to manage access to external sites.



The Cisco 3825 and 3845 routers include all of the capabilities and features of the 2800 Series, including the full complement of integrated security features, and more. They too can achieve up to 2500 simultaneous VPN tunnels. Cisco Call-Manager Express on the 3800 Series routers can support up to 240 phones, and Cisco Unity Express can support up to 100 mailboxes. An EVM module for local and long-distance calling can add up to 48 foreign exchange station, 24 foreign exchange office, or 16 BRI ports.

In particular, the Cisco 3800 Series provides many features to enhance availability. According to Jennifer Lin, product line manager at Cisco, "Modules can be swapped out while the router is operating, saving on downtime for routine maintenance and upgrading capabilities on the Cisco 3845 Router, even the motherboard can be hot-swapped. Redundant power supplies are available, and IOS Software Warm Reboot shortens bootup time."

As networks evolve, Lin adds, the router platform must be able to "carry customers through the next transition. For example, as people move to MPLS from Frame Relay, the router must accommodate the change. Yet users still need their legacy systems. The router must be very flexible, scalable, and diverse."

♦ ♦ ♦

A leading US retailer summed up the benefits of the Cisco Integrated Services Routers when commenting on one it had beta tested: "The Cisco 2800 Series Router will become the 'communications hub' of our new stores and regional offices. We'll be able to deploy a single converged solution that's easier to manage, lowers our operating costs, and leverages the infrastructure already in place."

And this is just the beginning. ■

FURTHER READING

- Cisco Integrated Services Routers
cisco.com/go/isr

BUNDLED SECURITY

INTEGRATED AES, INTRUSION PREVENTION ADD LAYERS OF DEFENSE.

NETWORKING and security technology have grown inextricably linked. Organizations now rely on computer networks for everyday operations and often for their very survival. With that level of dependence, the cost of data theft and any network downtime caused by malicious code and denial-of-service (DoS) attacks looms large. In fact, it is estimated that a cyber crime occurs in the US every 20 seconds, accounting for US\$141 million in corporate losses last year, according to the "2004 Computer Crime and Security Survey," conducted by the Computer Security Institute (CSI) in conjunction with the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad.

"So it is imperative to integrate several types of security technologies right into the network to foil various kinds of attacks before they can do any damage," says Charles Goldberg, product line manager for IOS security in Cisco's Security Technology Group.

The explosion of cyber crime in general and data theft in particular is one reason the industry is moving to a stronger form of packet encryption, known as the Advanced Encryption Standard (AES). In July 2004, for example, the US National Institute of Standards and Technology (NIST)

determined that the strength of the Data Encryption Standard (DES), also known as Federal Information Processing Standard (FIPS) 46-3, is no longer sufficient to protect government information.

NIST proposed withdrawing FIPS 46-3 except for use as a component of the Triple Data Encryption Algorithm (TDEA). Rather, NIST now recommends AES, also known as FIPS-97, which is a stronger and faster form of cryptography. NIST is influential throughout the world, and other countries often follow FIPS standards.

Similarly, the Internet Engineering Task Force (IETF) IP Security (IPSec) Working Group is moving toward standardizing AES as the default IPSec Encapsulating Security Payload (ESP) cipher. Early adopters, most notably highly sensitive organizations such as government and financial institutions, have already started migrating to AES.

Cisco's recently launched Integrated Services Routers are branch-office access devices that bundle virtual private network (VPN) tunneling with on-board AES, Triple DES, and DES encryption acceleration processing (see article, "Security, Services, and Speed . . . Oh My!" on page 29), helping organizations with a phased approach to this migration while boosting performance to remain at wire speed. All three of these encryption mechanisms can be used with IPSec VPNs.

These branch- and small-office access routers bundle a number of security capabilities right into on-board processors and Cisco IOS® Software, enabling integrated network security with no network performance compromise. In addition to embedded encryption, for example, another new security capability has been integrated into Cisco access routers to thwart downtime caused by malicious code entering the network: inline intrusion prevention (IPS).



Jon Duren, Chief Technology Officer at IdleAire Technologies, and Cisco 2800 Series Router customer. See story, page 32.

This article will look closely at the role of improved encryption and IPS in the layered approach to network defense.

Cryptography Evolution

Hardware-based support of AES in routers is currently unique in the industry to the Cisco Integrated Services Routers. These routers, which includes the Cisco 1800, 2800, and 3800 Series, supports any combination of AES, Triple DES (3DES), and DES encryption acceleration on their motherboards. The routers ship encryption-ready in combination with the appropriate image of Cisco IOS Software.

The multimode encryption positions enterprises for the future, maximizing their Integrated Services Router investment by enabling them to eventually move to AES, whether that happens in one, five, or seven years.

Cisco headend devices, including the Cisco 7200 and 7300 Series routers with VPN Acceleration Modules (VAM), VPN Concentrator, and PIX® Firewall, support all three encryption modes. As a result, enterprises are free to continue



running whichever algorithm is already installed in the Integrated Services Routers in their various branch locations, then upgrade remote-site “spokes” to AES as they see fit, says Kevin Sullivan, security product manager in Cisco’s Routing Technology Group.

Cisco has delivered AES in IOS Software images starting with Software Release 12.2(13)T. Cisco routers support both DES/3DES and AES running concurrently.

“If a bank wants to migrate from DES to AES, for example, it can convert four branches to AES in October, another four in December, and so forth, in phases,” explains Sullivan. “As the organization is ready, AES is already both hardware- and software-enabled at the remote site. Cisco changed the licensing in IOS to provide [DES/3DES and AES] in the same image for no extra charge to ease migration.”

How and Why to Migrate

AES brings stronger cryptography and generally faster encryption/decryption to the table, particularly for larger payload packets. Like DES, AES is a block-cipher encryption mechanism. Block ciphers divide data (and encryption keys) into blocks. A hacker must run rounds of operation on each block, break the key on that block, then chain that calculation to the next block and do it again. DES supports an 8-bit block cipher with a 56-bit encryption key length, while AES supports 128-, 192- and 256-bit block cipher lengths and encryption key sizes.

Block ciphers make an attack laborious and difficult, in effect, by requiring multiple attacks, one on each block. Triple DES performs DES three times on each block. However, DES-based encryption has been around for 25 years, so there is now enough understanding about the algorithm that it could potentially be cracked with brute force. In fact, it already has, in a 1998 contest designed to do just that! (See *New York Times* article at cisco.com/packet/164_6d1.)

Block ciphers differ from stream-cipher algorithms (such as RC4, for example). Stream ciphers generate a key stream that is the same length as the data stream. So 200 bytes of data would generate 200 bytes of a key stream, which is a fairly simple mathematical operation. Hackers can more easily use brute force to attack and break a stream cipher.

In addition to user data, Cisco routers enable enterprises to encrypt Simple Network Management Protocol Version 3 (SNMPv3) messages with 3DES and DES (AES support will be added soon).

SNMP appears on The SANS Institute’s “Top 20” list of Internet security vulnerabilities. The SANS Institute is a 15-year-old cooperative research and education organization for information security training and certification based in Bethesda, Maryland.

The SNMP management protocol is commonly used to remotely monitor and configure TCP/IP devices such as printers, routers, switches, and wireless access points and bridges. It consists of different types of messages between SNMP management stations and software agents in network elements. These exchanges have

OTHER ROUTER-INTEGRATED SECURITY FEATURES

- **Stateful firewall.** Routers can be configured to filter on a per-application basis with performance throughput on par with the Cisco PIX® Firewall. Network administrators can configure the firewall to permit legitimate traffic to enter the LAN only while a session is active. The Cisco IOS Firewall also supports the Transparent Firewall, available in Cisco IOS Software Release 12.3(7)T and above, which enables the insertion of a new firewall without renumbering the network.
- **Cisco Network Admission Control (NAC).** A NAC-enabled Cisco router automatically checks that antivirus settings on client devices attempting to connect to the internal network are current before granting access. When a noncompliant device is detected, NAC may take one of several actions, depending on the enterprise’s policy.
- **Dynamic Multipoint VPN (DMVPN).** DMVPN enables fully meshed, secure connectivity with zero-touch IPsec provisioning. By creating on-demand site-to-site IPsec tunnels, DMVPN minimizes the number of hops and encrypt/decrypts, reducing bandwidth usage and maximizing performance.
- **Voice, Video VPN (V³PN).** Cisco routers combine QoS and IPsec over remote access IP VPN links, enabling the convergence of voice, video, and data across a secure IPsec without performance compromise.

INTEGRATED VERSUS DEDICATED

Some enterprises have philosophical and organizational reasons for letting “routers route” and installing dedicated appliances to perform specialized tasks. For those who worry about too many personnel touching router configurations as a router takes on additional tasks and possibly endangering a router’s inherent ability to forward packets, the Cisco Integrated Services Router series supports a feature called the “Role-Based CLI.”

This feature divides access to router functions among different administrator roles so, for example, the network security administrator has access to security configurations only, not to routing tables. This division of labor should reduce configuration errors and protect the integrity of separate routing and security functions by keeping administrative domains separate.

significant exploitable vulnerabilities, particularly in SNMP Versions 1 and 2, which do not encrypt messages and use a default public “community string” as their only authentication mechanism, which many users don’t bother to change.

“Having access to a read/write SNMP MIB is as good as having a system compromised,” says Joshua Wright, deputy director of training at The SANS Institute, and author of the book, *Securing Cisco Routers: Step-by-Step*. “[Once they have access], attackers could change configuration files to do whatever they want. There are instructions on how to do that on the Cisco Website.”

The institute recommends running SNMPv3, which allows SNMP messages to be encrypted and includes authentication and authorization to mitigate these risks. As DES is now deemed by NIST insufficient protection going forward, the IETF is writing AES into SNMPv3 standards for further protection.

“AES in general is a better performer than DES, making it easier to maintain router stability,” says Wright. “It will also bring a throughput benefit to SNMP, where performance is even a bigger issue.”

However, he notes that 3DES will probably satisfy many enterprises’ security needs for some time and does not expect an immediate, mass migration to AES because of the recent NIST decisions.

“Having AES on routers is a good future-proofing benefit, though,” Wright says. “Organizations can deploy it, should we find that 3DES is indeed becoming a problem.”

Protection for Telephony

AES also plays a role in securing IP telephony in Cisco’s new Integrated Services Routers. The first level of defense is to provide access control to the voice domain. The next level, supported in the new routers on digital voice processors and Cisco IOS Software Release 12.3(10)T, leverages the IETF-standard Secure Real-time Transport Protocol (SRTP)—initially developed by

Cisco—which encrypts voice conversations using AES. This renders conversations unintelligible to internal or external hackers who have penetrated and gained access to the voice domain.

“In this way, the Cisco 2800 and 3800 series routers support and secure Cisco CallManager Express IP PBX features,” Sullivan explains.

SRTP encrypts only the payload of a voice packet without adding additional encryption headers. Because of this, an SRTP-encrypted voice packet is almost indistinguishable from an RTP voice packet, allowing quality-of-service (QoS) features and compressed RTP to be supported without any additional packet manipulation. Voice encryption keys are generated per call, ensuring a higher level of security protection. SRTP also validates the identity of gateways or IP phones encrypting the calls.

Battling Malicious Code

Bundled into the Cisco Integrated Services Router series is the ability to dynamically load and enable any or all of the 740 signatures supported by the Cisco IDS Sensor appliance platforms in real time. The Cisco IOS Dynamic Intrusion Prevention System (IPS) gives users the ability to modify an existing signature or create a new signature to address newly discovered threats.

Because Cisco IOS IPS operates inline, each signature can be configured to send an alarm, drop the packet, or reset the connection. This enables the router to respond immediately to security threats.

An additional capability allows network administrators who want maximum intrusion prevention to select an easy-to-use signature file that contains “most-likely” worm and attack signatures. When Cisco routers match these “high confidence”-rated worm and attack signatures to live traffic, that traffic is automatically dropped.

The Cisco Router and Security Device Manager (SDM), which ships with every Integrated Services Router loaded into flash memory, provides an intuitive user interface to provision these signatures. SDM allows the dynamic upload of new signatures from the Cisco.com Web site without requiring a change in software image, and configures the router appropriately for these signatures.

“No longer must network managers reload an entire IOS software image to get new signatures,” points out Bruce Johnson, security marketing manager in Cisco’s Products and Technology Marketing Organization. “Rather, now they can dynamically load and unload them.” ■

FURTHER READING

- Integrated Services Routers Security Features
cisco.com/packet/164_6d2
- FIPS-140-2: Security Requirements for Cryptographic Modules
cisco.com/packet/164_6d3
- IETF RFC 3711: the Secure Real-time Transport Protocol
cisco.com/packet/164_6d4
- The SANS Institute’s “Twenty Most Critical Internet Security Vulnerabilities”
sans.org/top20/

The Wired Hospital

Illinois hospital saves money—and lives—with a high-speed network.



John McFaul/Bernstein & Andriulli, Inc.

By Rhonda Raider

When Dr. Ahmed Farag joined Lake Forest Hospital Foundation (LFHF) of Lake Forest, Illinois, in 2000, he and his fellow radiologists had to manually hang diagnostic films in front of viewers. Given that the average computer tomography (CT) scan generates more than 300 images, this process could delay emergency diagnosis and treatment. “The problems with managing films also included lost images, high warehouse space rental costs, and long delays while the technician developed the film and confirmed the image was usable,” says Kerry Rosenbarger, technical coordinator for the hospital’s imaging system. “And for two or more physicians in different locations to confer about an image, they would each need their own copy.”

Today the hospital captures and stores patient images digitally, on a Picture Archive Communication System (PACS) that doctors access over a high-speed network that spans all campus and buildings in the foundation. “When I’m in the hospital, diagnostic images come up like lightning and I can see them within seconds,” says Farag. And when he’s at home on call, he can access the same images in JPEG format via the virtual private network (VPN), receiving the average CT chest exam ordered by the emergency room (ER) in just five minutes. “In the old days, I had

to get dressed, drive to the hospital to look at the films, and then drive back home,” he says. “The ability to receive images at home accelerates our workflow, increases physicians’ efficiency, and lets us read many more exams in the same amount of time.”

Faster diagnosis translates to faster treatment. According to Rosenbarger, the average time needed for a preliminary image reading has dropped from one hour to 15 minutes, and a full image processing has been halved from the industry standard of 48 hours to 24 hours. “We’re not just saving money, we’re saving lives,” he says.

Birth of a Network

PACS is but one of many healthcare innovations that LFHF has introduced since deploying a foundation-wide Cisco network. LFHF comprises two main campuses and 10 remote sites in a 20-mile radius. In 1999, the hospital’s IT group built its first network, with an ATM backbone based on Cisco Catalyst® 5500 Series switches. “Ethernet connectivity was becoming a standard feature of medical and office devices alike, and we decided to capitalize on that trend by building a single network that would

carry all device traffic,” says Stephen Morenzoni, network engineer.

In 2001, LFHF extended network access to locations outside the foundation by deploying a VPN based on a Cisco VPN 3015 Concentrator. “Now hospital employees can access network applications from any location—either on premises or off,” says Jay Manfred, also a network engineer, and Morenzoni’s colleague. For instance, a facilities engineer can reset the temperature in a patient’s room from a wireless hotspot at a coffee shop, or a doctor can view and manipulate images from home in the middle of the night.

Then, in early 2003, the LFHF upgraded its backbone from ATM to Gigabit Ethernet to take advantage of the greater throughput capacity and speed. Two Cisco Catalyst 6500 Series switches comprise the core, and a combination of Catalyst 4500 Series and Catalyst 3500 PWR XL Series switches support the campuses and remote sites, which are interconnected using an OC-12 SONET ring. Four T3 lines provide connectivity to the Grayslake campus.

The network already supports more than two dozen types of devices as diverse as security cameras, building management systems, time clocks, blood gas analyzers, and multiple imaging modalities, including CT, interventional radiography, X-Ray, magnetic resonance (MR), ultrasound, and others. “The network doesn’t notice any difference, whether it’s carrying a mundane print job or a fetal echocardiogram that will help a physician decide whether to transfer a newborn for surgery,” says Manfred, “so if a device has an Ethernet port, we just plug it in and give it an IP address. The healthcare and business application possibilities have become endless.”

For instance, in January 2004, LFHF opened a Women’s Center that offers a new digital mammography service. Now, rather than waiting for images to be developed and physical copies delivered, doctors in any location of the foundation can view the digital images as soon as they are captured. “We have a radiologist on site, for our patients’ comfort level, but it’s not really necessary because any doctor on the network, in any location, can read images in real time,” says Morenzoni.

Centralized Patient Monitoring: Increased Nurse Productivity

The network also enables physicians and doctors to monitor more patients, more effectively. Consider the fetal monitoring system. This system used to be a standalone serial network. It is now Ethernet based and uses the hospital’s Cisco enterprise network. “This takes a huge load off the nurses—so much so that if the system ever went down, IT would need to warn the department so they could staff up,” says Manfred. And because nurses can monitor all patients from a centralized console at the nursing

station, the staff ratio has been reduced, an especially salient benefit given the nursing shortage. “Without the centralized monitoring system, one nurse is needed for every patient in labor,” says Morenzoni. “With the centralized monitoring system, nurses are not only able to monitor more patients, but, because they do not have to be continually present at the mom’s bedside, they can be much more efficient in carrying out their other responsibilities.”

Additionally, because the monitoring system is on the enterprise network, LFHF can make this system available to doctors and their staff over the Internet. Before the hospital had its network, nurses called the doctor to report that a patient was in labor, and the doctor would generally ask the nurse to monitor progress and call when the labor had reached a certain threshold. Now doctors can monitor patient progress themselves, using the Web, from the office, home, or any other place with Internet access.

Hospital staff credit network-based patient monitoring with making them more effective at their jobs. “Physicians are suddenly much more in control,” says Manfred. “In the old days, a labor room nurse who was unsure of a patient’s progress had to call the doctor in. If the patient wasn’t ready, the doctor lost an hour or more when he or she could have been seeing other patients. Now the doctor can view the monitoring strip directly—from another part of the hospital, from home, even from the physician sleeping area of the hospital.”

Telemedicine: Fetal Echocardiography

The high-speed Gigabit Ethernet network is a boon to telemedicine, enabling hospital physicians to collaborate with their peers in other locations. “With our network, a physician at LFHF can confer with another in Washington D.C. and another in Israel, while each looks at the same image,” says Rosenbarger.

The same benefit extends to real-time monitoring data. Suppose a newborn child is suspected to have a heart abnormality that requires surgery shortly after birth. This kind of testing is done by fetal echocardiologists, a very specialized subfield with only a handful of practitioners in the Chicago area. LFHF has the specialists to perform the tests, but not to interpret the tests. So in the past, the tiny patient would be transferred to a hospital in Chicago while the mother, recovering from childbirth, had to remain behind. Now LFHF technicians can conduct the tests on the hospital premises and share the results over the network in real time with a fetal echocardiologist at a Chicago-area hospital, through a DSL videoconferencing link. Remote echocardiogram interpretation has worked so well that LFHF has extended its use to outpatients who are elementary school-age children, sparing the need for families to travel to Chicago for the test.

Enhanced Staff Communication: Wireless IP Telephony

The hospital is further extending the value of its network with voice over IP (VoIP). Doctors and nurses in one LFHF location have begun using wireless phones from SpectraLink, which connect to the network using Cisco Aironet® 1200 Series access points. The 120 doctors and nurses who have the phones can call each other conveniently using 4-digit dialing, thanks to two Cisco CallManager servers that provide centralized call processing. A Cisco 2600 Series Voice Gateway Router provides connectivity to the PSTN. Certain users have Cisco Unity™ voice messaging on their wireless phones so that if they happen to be on the phone when called, they can swap calls or receive the incoming call in voice mail. And the built-in quality-of-service (QoS) features in the Cisco IOS® Software ensure that the network delivers business-class voice.

"In the old days, if I called the doctor's office and the doctor was unavailable, we might play phone tag for awhile," says Manfred. "With wireless IP telephony, we can reach each other immediately by paging each

other. The win is especially huge for the ER and maternity departments, which are traditionally short-staffed in most hospitals."

ROI Through Radiology

At the outset, the IT group at LFHF couldn't accurately predict ROI. "Our primary goal is quality of care," says Morenzoni. "We knew the network would save us money and be much more efficient, but we didn't know by how much." Now the cost savings are accruing like cells in a culture. "Before we deployed PACS across the foundation, we spent [US\$]2 million a year for 68,000 procedures in 11 modalities," says Morenzoni. "Last year we performed 130,000 procedures in 30 modalities, and despite the increase spent \$600,000 less, for a savings of 30 percent."

The savings from PACS extend to storage, as well. Before deploying PACS on the network, LFHF spent US\$18,000 a month on warehouse space to store

Behind the Scenes of a Wired Hospital

LFHF's first network success story involved the pharmacy. The hospital wanted to install a pharmacy distribution system that would receive prescription orders from the clinical system and then dispense medications to nurses from dispensers strategically distributed throughout the campus. "The technological challenge of building a separate LAN for the application was overwhelming because we would need it to span so many buildings and locations," says Manfred. "The foundation-wide network made the plan feasible, because the network already connected every location where we would want to install a dispenser, now or in the future."

Simplified Moves

Like other hospitals, LFHF undergoes nearly constant construction, so temporary and permanent departmental moves are common. For IT, moves have been transformed from a major infrastructure challenge involving moving equipment and recabling to a simple matter of reconnecting Ethernet adapters. "Our only concern regarding moves is whether the local data closet has adequate capacity," says Manfred. "In terms of access to applications, location has become irrelevant."

Expanded Pool of Medical Transcriptionists

Medical records transcription typically poses numerous

challenges for hospitals, such as the difficulty of finding skilled medical transcriptionists who live nearby, because many in the field prefer to work from home. Since LFHF deployed a network-based dictation system, doctors and other staff store their dictation on the network as .wav files, which transcriptionists can access over the network from home, using the VPN. "Now we have a larger pool of skilled transcriptionists to hire, because where they live doesn't matter," says Manfred. "We've hired people who live more than 100 miles away."

Security Cameras

The hospital has deployed a mix of analog and digital video recorders that capture images from key locations. Security personnel can view real-time and archived images from anywhere in the foundation—or even from home, using the VPN.

Enhanced Support from Vendors

An unexpected benefit of the centralized network is better support—both from the hospital IS group to its internal clients, and from application vendors. "I can access people's desktops to help them, and vendors can securely get into our network when needed," says Morenzoni. "For IT, this is a fantastic benefit. Our customer satisfaction rate has gone through the roof."

films that were 18 months or older. That expense disappeared as of August 2004, when LFHF completed its transition to a digital image archive.

Another source of cost savings is that LFHF no longer needs to pay for application-specific LANs when it deploys a new application. Recently, that slashed \$110,000 from the cost of a cardiac heart monitoring system for the ER and \$78,000 from the cost of a digital video recorder security system. "If any of our hospital departments wants to add an application to the network, we can do it without purchasing any additional hardware," says Manfred.

Consistent Processes Across All Locations

Yet a final source of savings is process efficiencies—a key business driver for LFHF. In the past, each medical office building functioned as an independent island, with access usually limited to the applications in the building. As a result, staff that transferred to different locations had to be trained on the new location's processes, such as patient check-in. Now that every building has access to the same applications, all campuses and offices can follow the same processes, greatly simplifying training and transfers. And in some cases the patient experience has improved, as well. For instance, the Sports Medicine office in Vernon Hills, Gurnee, and the Lake Forest Hospital now share the same patient database, something they

couldn't do before. "Before, if a patient was seen by a therapist in one office and then the therapist transferred to another office, the patient had to re-register in the new office," says Morenzoni. "Now we have a complete view of the patient from any office."

A Steady Heartbeat

The LFHF core network has remained continuously available since it was deployed in 2003. That kind of reliability enables the hospital to count on it for new services. "Our network has changed our business model," says Morenzoni. "The hospital's senior business leaders have been able to factor in the fees for outpatient procedures that we can perform from any location in the county." He notes, as well, that the network helps the hospital comply with requirements of the US Health Insurance Portability and Accountability Act (HIPAA). "With one centralized network, we're able to more easily monitor who is logging in to what applications, and when. Rather than managing 40 networks, we're managing one. Coming down our fiber is an incredible medley of information: from fetal monitoring systems, PACS, radiology, computers, printers, and even security cameras. From our network statistics, we see that its potential has barely been touched. In years to come, we can plug in many, many more devices and applications with no appreciable difference in performance." ■

Around-the-Clock Uptime

New Cisco high availability features and services help reduce MTTR to seconds.

The “R” in MTTR stands for repair. Now you can say that it means *recovery*. Your customers do not care whether you have repaired a hardware or software glitch—they want their service running again, whether they are trying to bank by phone, buy a music download, or order a truckload of filters. With customer service, e-business, and internal operations depending increasingly on intranet and Internet applications, your network needs to be up *all the time*.

Today, 24-hour network availability is achievable. With new Cisco initiatives in system design and network monitoring, a failing interface card, router table error, cable cut, or application problem can be detected and identified almost instantly and a workaround can be put in place. Often problems can be fixed within seconds: a redundant interface card, power supply, or supervisor engine might be switched into service; traffic can be rerouted around a bad link. Other times, while the problem can't be fixed quickly, the network can provide continuous service by reconverging around an outage.

Two Cisco IOS® Software features now available on Cisco Catalyst® 6500 and 4500 series switches and the Cisco 7600 Series Router, along with advanced network management and services, help to keep your network online even when problems arise. *Generic Online Diagnostics (GOLD)* provides enhanced fault detection for the Catalyst 6500 and 4500 series switches and Cisco 7600 Series routers. *Non-Stop Forwarding (NSF) with Stateful Switchover (SSO) for the Catalyst 6500 Series* and *SSO for the Catalyst 4500 Series* ensure service continuity. The *Cisco Network Connectivity Center (NCC)* automatically identifies root causes in real time and makes clear their impact on the network. *Network Availability Improvement Service (NAIS)* assesses network operations and helps identify gaps in operational processes and tools. Each contributes significantly to around-the-clock network operation.

Following is a look at these new high availability features and services by some of the Cisco people involved in their development and release.

GOLD

By **Danny Khoo**, Manager, Software Development, Internet Systems Business Unit



A crucial question in maintaining a highly available network is, “What triggers a switchover?” The answer depends largely on how the fault is detected—by manual or semi-manual troubleshooting after customers have lost service, or auto-

matically, even proactively. This also affects the length of a service outage. Unless troubleshooting is automatic and proactive, a fault will likely cause an outage and negatively affect service. Manual troubleshooting can take an hour or more. GOLD finds problems proactively and often before they affect service. If service has already been affected, GOLD can minimize downtime by identifying the problem and triggering a switchover within one to two minutes, sometimes within a few seconds. Designed to provide a common diagnostic framework for Cisco equipment running Cisco IOS Software, GOLD is debuting on the Catalyst 6500 and 4500 series switches and Cisco 7600 Series Router.

GOLD tests hardware and software with bootup and runtime diagnostics. During bootup of a supervisor or a module, such as a service or interface card, GOLD checks several functions before allowing the component to become active, so faulty ones never come online. You can choose the range of tests, from minimal to exhaustive. Runtime diagnostics include nondisruptive monitoring tests that run in the background at selected intervals to pick up developing problems—unstable supervisors or modules will be switched out of service—and disruptive ones, which can be initiated on demand or scheduled as regular maintenance. In the Cisco Catalyst 6500 Switch and Cisco 7600 Router, GOLD proactively checks proper functionality of the data and control path. In the Catalyst 4500, GOLD offers full troubleshooting capabilities; comprehensive background checking is being developed.

If it finds during background monitoring that given control and data paths are inconsistent or faulty or that a hardware unit is malfunctioning, GOLD automatically triggers a switchover before loss of service. In the Catalyst 6500 Series switches and Cisco 7600 Series routers, it also regularly monitors the standby supervisor, making sure it is ready to take over if needed. Hardware and software checks detect problems such as bad components and connectors, faulty

memory, and inconsistent lookups. In the Catalyst 6500 and Cisco 7600, GOLD can also differentiate between hardware and software problems, and those that are long term or transient. For example, as it monitors the communications channel between the active and standby route processors, it can distinguish between a blockage caused by heavy traffic and one caused by locked-up hardware. When GOLD and NSF/SSO are employed, networks designed with Catalyst 6500 Series switches and Cisco 7600 Series routers can achieve availability of close to 100 percent. For more on GOLD, see cisco.com/packet/164_7b1.

NSF and SSO

By Aurelie Fonteny, Technical Marketing Engineer,
Internet Systems Business Unit



SSO keeps voice over IP (VoIP) services up during supervisor switchover in a Layer 2 network. NSF with SSO offers seamless supervisor switchover in a Layer 3 network with *zero packet loss*. Both active and standby supervisors are synchronized at all times with NSF and SSO. Supervisor switchover time is typically zero to three seconds. NSF and SSO on Cisco Catalyst modular switches dramatically increase operational efficiency by eliminating service disruptions, minimizing network downtime, and reducing troubleshooting costs. NSF with SSO is available on the Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers for hitless Layer 3 switchover. SSO is available on the Catalyst 6500 and 4500 series switches for hitless Layer 2 switchover.

Because a network infrastructure is only as available as its weakest link, SSO is well suited for the Layer 2 access network where end stations are connected to a single modular switch. NSF with SSO is especially valuable at critical network edge locations where you want to avoid Layer 3 disruption or in data centers where the loss of a supervisor can affect Layer 4–7 services availability.

Previously available only on larger systems, both features represent an evolution from Route Processor Redundancy (RPR) and RPR+. SSO and NSF with SSO are stateful at Layer 2 and Layer 3, respectively. NSF with SSO also provides continuity for multicast traffic. In addition, SSO ensures continuity of some Layer 4 functions such as quality of service (QoS) and access control lists (ACLs). NSF with SSO is available in Cisco IOS Software Release 12.2(18)SXD on the Catalyst 6500 Series. SSO is available in Release 12.2(20)EWA on the Catalyst 4500 Series.

The active and standby supervisors in Catalyst 6500 and 4500 switches run “hot,” so the standby is always ready to take over. Upon supervisor failure detection, which might be detected by GOLD or

other means, SSO ensures transparent switchover for Layer 2 functions and protocols such as Spanning Tree Protocol, virtual LAN trunking, and Power over Ethernet. SSO also provides the actual synchronization between the supervisors, handling runtime data synchronization as well as startup configuration, startup variables, running configuration, and hardware table synchronization.

With NSF, the Catalyst 6500 Series Switch and Cisco 7600 Series Router continue to forward packets along known routes based on the most recent forwarding information base (FIB) data while the new supervisor is taking over, even though networking arrangements with other routers have been lost. NSF maintains a separation between the data and control planes for Layer 3 operations during switchover; the data plane continues forwarding packets based on the pre-switchover FIB data, while the control plane builds a new routing protocol database and new peering arrangements with neighbor switches. For the latter task, it relies on *NSF-aware* neighbors. A switch equipped with NSF, able to perform the packet forwarding during switchover, is *NSF-capable*. An NSF-capable switch implements IETF graceful restart routing protocols extensions to signal to its peers that it is recovering from a failure. A switch that is NSF-aware understands these extensions and can relay routing information to help a neighboring NSF-capable switch build its new database. Upon receiving a graceful restart notification from its neighbors, an NSF-aware switch maintains its peering arrangements with the restarting router and doesn't need to reconverge. An NSF-capable router is also NSF-aware. A Catalyst 6500 Series Switch supports NSF capability and NSF awareness; a Catalyst 4500 Series Switch supports NSF awareness.

Because Cisco Catalyst switches are in many critical parts of the enterprise network, it is especially important that they are available virtually all of the time. NSF and SSO, along with GOLD, help ensure that they are. For more on NSF and SSO, see cisco.com/packet/164_7b2. For independently conducted high availability testing results on the Catalyst 6500 and 4500 series switches, see cisco.com/packet/164_7b3 and cisco.com/packet/164_7b4, respectively.

Cisco NCC

By Joe Zhao, Product Manager, Network Management
Technology Group



A network problem usually announces its presence by triggering dozens or even hundreds of alarms from all over. So how can you tell which one is the root cause of the problem and which are only symptoms? And which IT group(s) should resolve it? While every group gets alarms, not every group always has the same picture of the IT infrastructure. The Cisco Network Connectivity Center, or NCC, identifies the root causes of problems in real

time, no matter where they occur in the network—often before they affect service. You don't have to spend hours checking out alarms and trouble tickets when troubleshooting a failure. NCC also analyzes the impact of the outage on your business, so you can prioritize repairs to maximize service delivery. Using patented technology, Cisco NCC presents a single data representation of the network to all groups involved with network operations. Detailed maps display exactly what is in the network, including where the components are located, their interdependencies, and real-time status. Cisco NCC's true effectiveness comes from a powerful root cause analysis engine that builds a complete end-to-end model of all the network's interdependencies and develops alarm and symptom signatures for failures. When a failure occurs, Cisco NCC matches the alarm pattern to signatures in its database to diagnose the root cause. This instantaneous and automated analysis enables you to correct the problem as soon as physically possible.

At the network level, Cisco NCC analyzes relationships in different technology domains, from individual ports and cards to IP networks, routing protocols, and Multiprotocol Label Switching (MPLS). It cross-correlates events and shows their impact across domains. Cisco NCC can also pinpoint the root cause of an application problem, be it caused by a network failure, in the application itself, or in related systems or applications. Moreover, it is a model that can grow with your network.

Cisco NCC translates hundreds of confusing alarms into specific problems and impacts. It reduces costs by automating root cause and impact analysis, and maximizes network availability by proactively identifying problems before they affect your business. Customers have reported up to 80 percent improvement in MTTR with Cisco NCC, and up to tenfold reduction in trouble tickets. For more on Cisco NCC, see cisco.com/packet/164_7b5.

NAIS

By **Dave Knuth**, Senior Manager, Customer Advocacy
Advanced Services



When was your last major outage? Do you know what caused it, how it impacted your user communities, and what the business costs were? Did you lose a customer as a result? What percent of network changes does your staff manage successfully?

Do you have the right NMS tools and instrumentation to effectively manage your environment? Can you predict and prevent an outage before it occurs? Even if your network was in superb condition when it was installed or last upgraded, without careful, continuous management of day-to-day operations it will suffer "network entropy." Over time it will lose its designed resilience and stability due to ill-conceived or poorly executed changes.

Cisco's NAIS team offers what might be called "Day 2" services including network resilience assessments, NMS architecture and instrumentation analysis, and gap resolution services. NAIS performs detailed assessments of how areas such as availability, performance, security, changes, and configurations are managed within the network environment. We use as benchmarks practices that Cisco has created and observed in companies in several industries, such as financial services, healthcare, manufacturing, and carrier environments, as well as practices recommended by the Information Technology Infrastructure Library (ITIL) and found in the ISO Fault, Configuration, Accounting, Performance, and Security (FCAPS) management framework. To resolve gaps found between these practices and leading practices, the NAIS team works with customers to implement their desired changes based on the recommendations. NAIS also works extensively with customers to provide the necessary network architecture and platform changes to achieve targeted availability goals.

Two examples demonstrate the depth and value of the NAIS assessments and interventions. When a large international financial services firm asked us to perform a detailed resilience assessment of its US network, one area we looked at was change management. We examined change controller and review meetings, the change control system, risk level and validation requirements, emergency change procedures, change metrics, and consistency in change management. NAIS concluded that the company was using best practices in three of these six areas. In the others, we suggested that the company modify its change control system to ensure that certain types of configuration changes actually occurred and were documented correctly; that it develop or adopt change metrics; and that management continue to emphasize the importance of consistent change management processes. We also recommended alterations in change planning and validation, such as formalizing network management requirements during planning and identifying performance and scalability requirements. These modifications resulted in significantly improved network availability, increased customer satisfaction, cost reductions, and improved time to market.

For a financial services customer, NAIS found gaps in capacity and performance management, fault exception reporting, configuration and software lifecycle management, and certification and testing procedures. Recommendations included establishing a clear definition of availability, adding more metrics and a cross-functional process to review the effectiveness of network management tools, redefining the software lifecycle process, and enhancing lab testing procedures. This customer reported year-on-year results including a 60 percent drop in problems from software defects, a 10 percent decrease in operating expenses, and a 24 percent decline in outages ranked service-affecting. For more on NAIS, see cisco.com/packet/164_7b6. ■

Good Vibrations

Cisco deploys massive Wi-Fi network for Bonnaroo Music Festival.

By David Baum

"How many times must a man look up before he can see the sky?"

These memorable lyrics by Bob Dylan more than likely occurred to Cisco's Andy Hettinger, a cable marketing manager, as he scanned the gathering clouds above rural Tennessee the day before the Bonnaroo Music Festival was about to begin. Hettinger and colleagues had been working around the clock to create a wireless network for the festival, helping to set the stage for some of the biggest artists in the music business. Would adverse weather affect the radio signals?

Music Milestone

With a coverage area of more than five square miles, the network represented the largest temporary Wi-Fi deployment in US history. Network solutions from Cisco and Linksys were deployed with a high-speed transport infrastructure from Cisco Powered Network provider Charter Communications to supply high-speed connectivity to hundreds of musicians, along with production personnel, administrative workers, and festival-goers.

"All ticketing was handled electronically, and administrators had unlimited network access for business activities such as shipping and receiving and cutting paychecks," says Jeff Steinberg, service acceleration manager at Cisco, who worked with Hettinger on the event. "Wireless access was also provided for the organizers and VIP campground residents. Everybody was extremely pleased with the results."

Named by *Rolling Stone* magazine as one of the top 50 milestones in music history, more than 130,000 people attended the four-day music festival, which was held on a 650-acre farm on the outskirts of Nashville.

Workers began with a patch of unimproved farmland and constructed what amounted to a small city, with temporary administrative offices, six sound stages, general stores, concession stands, camp sites, parking facilities, and all the services necessary to allow tens of thousands of fans to enjoy more than 80 bands including Trey Anastasio, The Dead, Bob Dylan, Dave Matthews, Patti Smith, Wilco, and dozens of others.



SEA OF FANS The Bonnaroo Music Festival drew more than 130,000 rock music fans this year.

Getting in Gear

Co-promoted by A.C. Entertainment of Knoxville, Tennessee, and Superfly Productions of New Orleans, Bonnaroo has spun off concert CDs and DVDs, along with an Internet radio broadcast.

For Cisco and Charter, the six-month project involved planning, design, construction, setup, and teardown of all network facilities—and a fair amount of related IT gear. In addition to the network itself, Cisco and Charter supplied the infrastructure for an Internet Village where festival attendees could share music, burn CDs, access the Internet, and read e-mail.

One month before the event, systems engineers John Kerrigan and Mike McCullough of Cisco conducted a site survey to scope out the physical terrain, determine where to place utility poles, and assess what kinds of equipment they would need. In addition to careful placement of wireless "hotspots," they decided to supplement the wireless transport facilities with Cisco Long-Reach Ethernet where a thick line of trees bisected one section of the farm. While wireless transmissions normally penetrate trees, Kerrigan was concerned that, in the event of rain, water on the leaves would cause interference by reflecting the radio signals in random ways.

You can relive the Bonnaroo music experience at livebonnaroo.com, the festival's online outlet, where downloadable recordings of live performances are available.



FIELD WORK Andy Hettinger and Jeff Steinberg of Cisco hard at work building Bonnaroo's wireless LAN from their "virtual office" on Tennessee farmland.

The Infrastructure

Event organizer Superfly Productions supplied power through diesel generators located near each pole, while Cisco created enclosures for the wireless equipment, which included Cisco Aironet® 1200 Series access points and Cisco Aironet 350 Series wireless bridges. The access points were connected to the Internet using dual cable modems and a Cisco uBR7246VXR cable modem termination system (CMTS).

The Cisco Aironet 1200 Series Access Point is commonly used to create secure wireless LANs. Its modular design allows single or dual radio configurations for up to 54-Mbit/s connectivity in both the 2.4 and 5 GHz bands. The technology is compliant with the IEEE 802.11a, 802.11b, and 802.11g standards. The Cisco Aironet 350 Series Wireless Bridge enables high-speed long-range outdoor links and is ideal for harsh environments.

Thanks to this innovative infrastructure, anyone at the festival who had 802.11b-enabled adapters in their laptop computers and personal digital assistants (PDAs) could easily communicate over the airwaves at 11 Mbit/s. Attendees could stay connected with friends and family at the VIP camping area, in the Centeroo village, and in an Internet café, where 40 laptop PCs were available to check e-mail, download music, and access the Internet. Festival organizers also created a music-sharing village where attendees could burn CDs from a huge library of music supplied by the artists.

"Cisco Aironet 1200 Series Access Points gave users high-speed wireless performance," says McCullough. "Many users were astounded by the speed, which was generally in excess of 3 megabits per second."

Design Considerations

The Cisco engineers carefully laid out the network to avoid interference from one wireless area, or cell, to another. "When you lay out the wireless access points, typically you design them with overlapping coverage areas, much like the concentric circles in the

Olympic logo," McCullough explains. "However, you must be careful not to assign the same channel IDs to overlapping cells or the devices will interfere with each other, reducing the available bandwidth to clients who use those particular cells."

According to McCullough, the sound mixers consumed the most bandwidth, as they recorded and mixed music from each act onto 8 terabytes of local storage, then streamed the final cuts to offsite servers. Next year, says Hettinger, the team hopes to enable live streaming of audio and video to local servers for immediate sharing and download.

"The wireless network and associated applications were a great success," says Joel Patten, director of business development at Charter Communications. "The general consensus from my team is that we would definitely like to partner with Cisco and do the event again in 2005."

Confronting Challenges

Because there were few precedents for this type of installation, a large part of the challenge was to predict how much bandwidth Cisco and Charter would need. "Soon after the festival began, we realized that we had underestimated the Internet throughput requirements, both internally and externally, as well as the number of available clients," says McCullough. "We had to tune the network as needed to accommodate burgeoning usage."

The team also faced challenges delivering wireless connectivity to 25 aluminum trailers set up for musicians and crew, because radio waves don't permeate metallic substances. They solved the problem by placing antennas in front of windows and doors, which were generally constructed of glass and wood. In cases where wireless signals coming through windows were too weak, or the PCs did not have the proper access cards, they supplemented the endpoints with Linksys® routers, which support wireless communication with the Cisco Aironet access points on the poles. Other challenges involved occasional power surges from generators and competing wireless signals in the area. Because of the overlapping coverage supplied by adjacent cells, neither issue caused significant disruptions.

Continued on page 70

FURTHER READING

- Cisco Aironet 1200 Series
cisco.com/packet/164_7c1
- Cisco Aironet 350 Series
cisco.com/packet/164_7c2
- Cisco 7200 Series Router
cisco.com/packet/164_7c3
- Cisco CMTS
cisco.com/packet/164_7c4

Head for the Hotspot

How Service Providers Can Deploy Profitable Public Wireless Networks

By Sherelle Farrington

Wireless networking: it's everywhere users want to be.

That's the goal of service providers deploying public wireless networks (PWLANS) worldwide. Based on the IEEE 802.11 standard, these networks offer ubiquitous access to online services such as the World Wide Web, e-mail, virtual private networking (VPN) connections to corporate networks, music, ring tones, and movies.

Today, road warriors use PWLANs in airport and railway terminals and lounges, hotel rooms, convention centers, bookstores, and coffee shops. With an estimated 100,000-plus wireless hotspots scheduled for installation by the end of 2004, wireless service providers are well on their way toward mass-market scale. Deployments already underway are mobilizing wireless networking, extending service to airplanes, trains, and automobiles.

Where Is the Money?

In the past, public access was viewed as a novelty service with a questionable business model and was primarily pursued by niche operators targeting hotels or airports. However, as more hotspots are deployed, and especially as more users adopt wireless, public access is becoming a widely accepted service offering that can play multiple roles for a service provider. Three distinct strategies are emerging for capturing positive return on investment (ROI) from PWLAN deployments.

The first model is simply having a profitable PWLAN standalone service offering. Taking a look at available results and market data, primary factors for having a profitable hotspot business include the following:

Capturing attractive locations—Airports and hotels appear to have the strongest usage rates and are key sites for most successful operators.

Creating a critical mass of hotspots—Outside of airports and hotels, most PWLAN business models depend on subscription services, which can be sold only if a service is widely available in convenient locations. Many other operators are assembling a larger service footprint through roaming arrangements.

Effective pricing—Many operators have priced PWLAN access as a premium service that costs up to US\$25 to US\$30 per day for

use. While this price might be acceptable to high-level road warriors, it is a barrier to most users. The most successful operators offer competitive hourly and daily rates as well as monthly subscription prices as low as US\$10 to US\$20 per month.

As PWLAN usage and customer awareness grow, it has become more attractive to service providers seeking to differentiate their core fixed or wireless services. The second model for achieving PWLAN ROI is to bundle it with an existing service to increase ARPU or reduce churn. Service providers worldwide, such as Portugal Telecom, Comcast, and Singtel, have pursued this strategy. Most recently, SBC announced that it will offer PWLAN access to current DSL subscribers at its 3500 hotspots (growing to 20,000 by 2006) for only US\$1.99 per month.

Finally, perhaps the greatest potential ROI for PWLAN is to integrate it with other technologies to provide a seamless mobile data service. Swisscom has deployed an integrated PWLAN/General Packet Radio Service (GPRS)/Universal Mobile Telecommunications System (UMTS) service that provides ubiquitous connectivity for its subscribers. Customers are always connected through the best available wireless connection, and they pay based on usage. In this model, customer sessions are maintained across the different wireless networks through mobile IP, and customers do not need to know which access network they are using or do anything to be connected. In addition to offering complete ease of use, this service also offers the strongest possible wireless security through 802.1X/EAP authentication and encryption.

Architectures

To achieve mass-market scale, wireless service providers need to deploy flexible infrastructures that support many services today and are adaptable to services under development. On the network, this translates to a flexible architecture that users find easy to access and use. It accepts connections from any client device, requiring no particular client software or configuration. These PWLAN infrastructures are scalable to thousands of centrally managed, geographically dispersed sites.

The carrier-class PWLAN architecture enables deployment of many small hotspots such as coffee shops and bookstores, and large hotspots such as airports and convention centers (see figure on page 53). (This discussion ignores the single-site PWLAN, which as an independently owned and managed network can only offer wireless Internet access.) All hotspots have centralized management for configuration, troubleshooting, and inventory accounting. Large hotspots with dozens of access points require engineering that is similar to a standard enterprise deployment, such as a site survey and radio tuning between access points.

NETWORKERS 2004

This article is based on a session presented at the Cisco Networkers 2004 users conference. To learn more about Networkers, visit cisco.com/networkers.

Whether large or small, all hotspots deliver many services over a single infrastructure. A typical site has both wireless and wired network access—the first for customers and roaming employees, the second for transactions from desktop systems. A robust design uses multiple wireless virtual LANs (VLANs) to separate user groups and provider control traffic, requiring quality of service (QoS) mechanisms and compliance with IEEE 802.1Q. Support for tunneling technologies based on IP Security (IPSec) or Generic Routing Encapsulation (GRE) enables session privacy. Economies of scale enable large sites to deliver high-bandwidth services such as online movies and support devices such as wired and wireless IP phones, video phones, and dual-mode Global System for Mobile Communications (GSM)/802.11 phones.

Cisco PWLAN Components

The end-to-end Cisco PWLAN solution includes components at the hotspot and central data center. The hotspot includes access points such as the Cisco Aironet® 1100, 1200, or 1300 series, which connect into a Cisco Access Zone Router (AZR) for WAN or Internet backhaul to the data center. Cisco IOS® Software in a Cisco AZR has PWLAN-specific feature enhancements such as IP spoofing protection, Layer 2 user detection and session termination, switch port-based location identification, and client static IP support. Standard router features required for a PWLAN deployment include WAN connectivity, IETF 802.1Q VLANs, dynamic address assignment, QoS mechanisms, and policy-based routing. Traffic separation with VLANs and QoS is especially useful in a large site, where many vendors may use the same network in addition to the general public. In an airport, for example, the user base might include baggage handlers, food service vendors, ground traffic controllers, and others.

In the data center (or local distribution point in a large site), the Cisco Mobile Exchange solution manages user access, service delivery, management, security, and billing. It includes the Cisco Service Selection Gateway (SSG), which works with the Cisco Subscriber Edge Service Manager (SESM) to provide subscriber and service management. They authenticate users, present the branded portal, collect and forward billing information, and track activities for billing, security, and management purposes. As a flexible RADIUS server, the Cisco Access Registrar provides authentication, authorization, and accounting services, supporting many authentication types, including different Extensible Authentication Protocol (EAP) types.



SHERELLE FARRINGTON is a technical marketing engineer for Cisco service provider solutions. As the former lead for the Cisco Public WLAN solution, she worked with customers worldwide to define, develop, and deploy large-scale Cisco PWLAN networks. She can be reached at sherelle@cisco.com.

Some countries require PWLAN providers to support equal-access, neutral-host networks. The provider must offer connectivity to other provider networks and services from the public hotspot. A network with local access control can route users, based on their selection, to multiple service providers.

The User Experience

The essential user experience should perform the following steps in a manner that is intuitive to users:

1. User connects to the WLAN and opens Web browser.
2. User is automatically directed to a login screen—the branded portal.
3. Without login, user can access free services from the portal.
4. Users log in to access premium services such as e-mail or corporate VPN.
5. Billing commences when user accesses premium services.

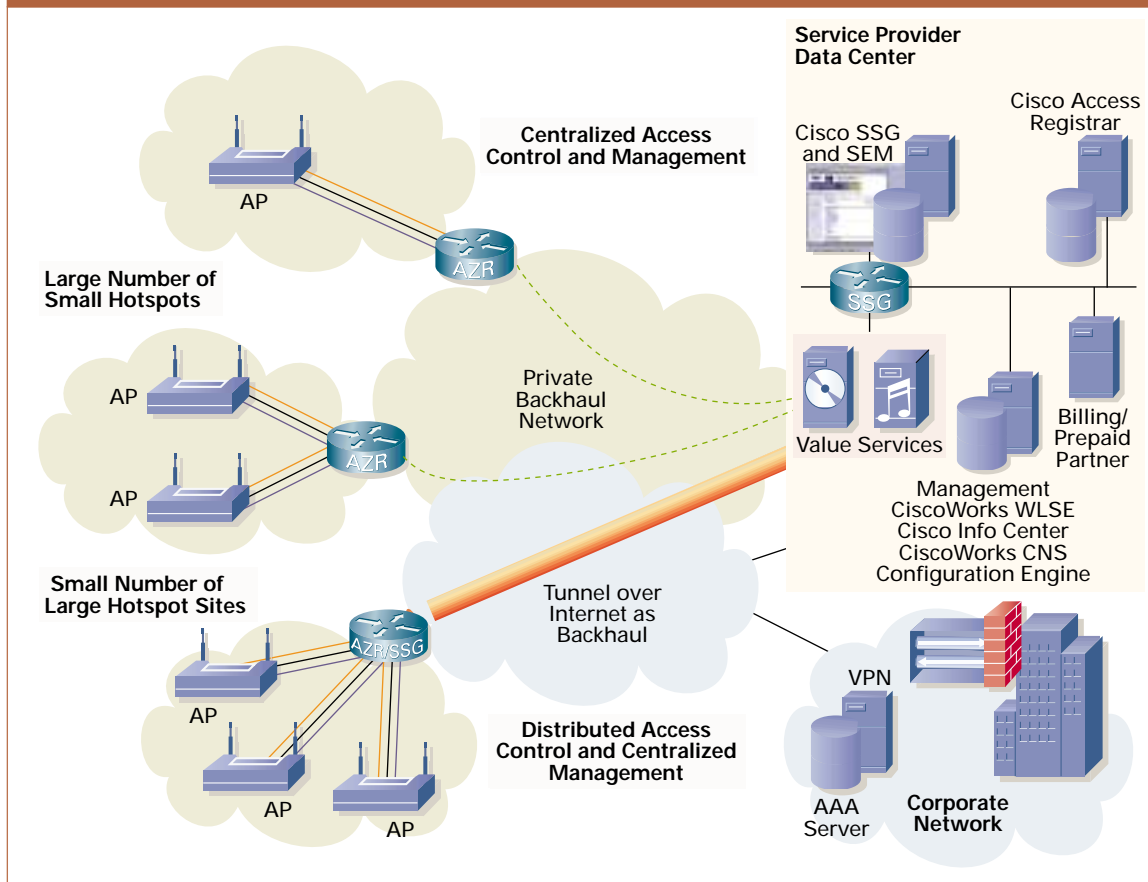
A well-designed PWLAN supports ease of use in several ways. Easy connectivity through open, no-WEP, wireless access points, which broadcast Service Set Identifiers (SSIDs) associated with the public VLAN. Client devices see the network and can connect without entering SSIDs.

To accommodate many possible client configurations, network devices must be plug and play. Clients with static IP, static Network Address Translation (NAT), and Web proxy setting can connect without configuration changes. The service provider configures NAT at the AZR to support static IP clients. Private DNS services allow providers to spoof addresses to redirect users to a local DNS server, then define per-service DNS settings in service profiles based on the assigned IP address range.

Web proxy settings redirect users to both authenticated and unauthenticated local Web proxies. Service providers must lock down access to authenticated Web proxy services and ports to prevent people from using them for unpaid access. To avoid detailed login instructions, the Cisco SSG automatically redirects users to the Web interface or portal and requests a username and password or offers new users the ability to sign up for a new service.

The PWLAN uses client IP addresses to locate users and present them with the correct branded portal and services. A single site is generally identified through a particular range of IP addresses; in large sites with many access points, the Cisco AZR can be used to identify the user location down to the individual access point, using switch-port based location identification

TYPICAL CISCO PROVIDER ARCHITECTURE



MANY SERVICES, ONE NETWORK A profitable PWLAN business model begins with a centrally managed network architecture that delivers many fee-based services to thousands of hotspots.

via Dynamic Host Control Protocol (DHCP) Option 82. This location awareness is an important feature of PWLANs, enabling the cobranding of services within large sites, such as airports, and with large chain customers, such as hotels and coffee shops. The Cisco SESM knows from the IP address which portal to present to the user.

When users close up and leave without logging out, the Layer 2 user detection and session termination feature in the Cisco AZR closes the session. This terminates time-based billing and protects the user from session hijacking.

Most importantly, the service provider must support a range of pre- or post-payment options on a one-time or subscription basis and accept both vouchers and credit or debit cards. Because PWLAN is a nascent market, the most common payment type today is prepaid by credit/debit card or voucher, which authorizes a specific amount of time on the network. As the market matures, subscribers are migrating toward subscription-based billing similar to a utility or phone service.

Security

As an open network, a PWLAN presents security risks to the service provider infrastructure and users. Securing a public network differs from securing an enterprise network. Enterprises exercise control over the type and configuration of devices and users it allows onto the network, whereas an open PWLAN must be agnostic to client devices to encourage widespread use. Providers want everyone on the WLAN, but users must pay for anything they do once connected.

Today, security on an open PWLAN addresses four user threats:

- **User authentication**—because the portal is a Web page, the standard solution today uses HTTP over Secure Sockets Layer (HTTPS/SSL) encryption.
- **Air link sniffing**—easy to do because there is no air link encryption, service providers can offer fee-based VPN services to users that do not have a corporate VPN.
- **Local direct peer attack**—these are easy to block using the Publicly Secure Packet Forwarding (PSPF) feature on Cisco Aironet access points and the Policy-Based Routing (PBR) feature on the Cisco AZR.

- Session hijacking—is tempting because hackers love to get free services by piggybacking onto someone's paid session. The provider can mitigate hijacking, which uses spoofed IP addresses by locking the MAC address of a valid user to the IP address, as well as terminating sessions when users forget to log off. This solution is not bulletproof—hackers can spoof MAC addresses to gain entry, but providers are working to solve this problem by starting to offer authentication based on the IEEE 802.1X standard.

Security Enhancements

Preventing mischief on an open PWLAN presents challenges, but service providers are working to deploy enterprise security technologies for public use. One hurdle is user authentication. Usernames and passwords are relatively easy to crack, and users can forget their passwords. One-time passwords (OTPs) are expensive and require user training. IPSec authentication transmits MAC addresses in the clear prior to tunnel setup. Rogue access points, especially next to smaller sites, can be a problem, so users need assurance that they're logging into and providing billing information on a legitimate network.

Emulating enterprises, service providers are working to solve these problems with IEEE 802.1X authentication and some flavor of EAP, and the Cisco PWLAN solution includes these technologies. Based on RFC 2284, 802.1X/EAP generates dynamic, per-session encryption keys in a manner that protects data from sniffing. Encryption also protects against session hijacking. Mutual authentication between users and the network mitigates login into rogue networks. Wi-Fi Protected Access (WPA), a subset of the IEEE 802.11i draft standard, combines 802.1X, EAP, Temporal Key Integrity Protocol (TKIP), and Message Integrity Check (MIC).

However, both 802.1X and EAP require client software. To achieve mass-market scale, providers cannot require specific client configurations. The obvious solution is to incorporate 802.1X and EAP into device operating systems. Windows XP includes these technologies today, but it may be years to complete a migration across all operating systems and platforms. Another challenge is that many types of EAP exist, and the lack of an immediately apparent industry standard creates concern about interoperability as users roam.

Network Management

Network uptime equals revenue. Efficient, centralized network management is essential to protecting revenues, controlling operating costs, and solving problems quickly. Cisco offers management solutions that can automate provisioning, monitor network and wireless behavior, and centrally administer equipment in thousands of hotspot locations. For device management, CiscoWorks LAN Management Solution (LMS) includes tools for configuration, backup, and inventory management. The Cisco CNS Configuration

Engine enables zero-touch configuration of the Cisco AZRs by automatically pushing the appropriate configuration to a Cisco AZR across the network when it is installed at the hotspot location. Similarly, the Cisco Wireless LAN Solution Engine (WLSE), part of the Cisco SWAN solution, automatically configures and manages authenticated Cisco Aironet access points when they log into the network from remote sites. It also supports full radio management capabilities, including the ability to map hotspot wireless coverage and detect radio interference from neighboring access points or noisy appliances.

On the Horizon

Wireless networking technologies are mature enough to introduce to the mass market, and vendors are fine-tuning service delivery issues such as worldwide, cross-provider roaming. For example, a corporate road warrior might want to log into the corporate VPN through a convention center PWLAN operated by a different service provider. The solution must be completely transparent to the user. The technology exists to connect the user to her home network, but billing agreements are required. Clearing and settlement providers can assure the visited provider that it will be paid and the home provider that the bill is correct. Portions of this system are not yet standardized, such as chargeable user identity and location identification, and the large number of providers today limit mass-market proliferation of roaming capabilities.

Another area under deployment is seamless roaming across different access technologies and provider networks, including mobile data networks based on 3G. Mobile IP technologies pioneered by Cisco offer standards-based solutions for seamless roaming.

A third area of interest is voice over 802.11. Some vendors have introduced dual-mode phones, which operate on both GSM and 802.11 wireless infrastructures. Dual-mode phones can help PWLAN customers save toll charges. For example, security personnel at an airport might use the 802.11 network for voice communications, with a fallback to the GSM network when they are out of range or off site.

Last, some providers are deploying 802.11 gear outdoors, enabling ubiquitous access from sidewalk cafes and public outdoor venues such as parks and amphitheaters. Cisco supports this effort with Metropolitan Mobile Network solutions, which provide local government and transit agencies with a secure broadband city-wide network that enables new applications by extending services from the wired infrastructure to the wireless IP network. These solutions offer new ways for public sector agencies to accelerate communications and service delivery to employees and citizens. ■

IPv6 in Broadband

Service providers of all types can benefit from the flexibility and new revenue opportunities of IPv6-based broadband.

By Salman Asadullah and Adeel Ahmed

The number of broadband subscribers worldwide grew from 33 million at the end of 2002 to 97 million at the end of 2003, reports *Ovum Access Forecasts*, and is expected to reach 140 million by the end of this year. Studies show that these broadband consumers, with their high-speed, “always-on” connections, spend more time online, are generally willing to spend more money on communication services (such as music) and high-value offerings, and are more likely to set up home networks and expand their network capabilities incrementally with applications such as wireless and home surveillance and even advanced services such as voice over IP (VoIP) and real-time video on demand.

The exponential growth of broadband worldwide and the online proclivities of these end users provide one of the best opportunities for service providers of all types to increase their revenues and profitability. They are looking for ways to evolve their current network architecture to meet the needs of Internet-ready appliances and new applications, as well as provide new services to their customers. And Internet Protocol version 6 (IPv6) is designed to help service providers meet these challenges. IPv6 gives every user multiple global addresses that can be used for a wide variety of devices including cell phones, personal digital assistants (PDAs), and IP-enabled vehicles.

The life of the current IPv4 protocol is extended by applying techniques such as Network Address Translation (NAT) and temporary address allocations, but the manipulation of data payload by intermediate devices has challenged the paradigm of peer-to-peer communication, end-to-end security, and quality of service (QoS). In contrast, enhancements in IPv6 overcome these limitations while quadrupling available 32-bit IPv4 address space to 128 bits (RFC 3513). IPv6 addresses the need for always-on environments to be reachable without using IP address conversion, pooling, and temporary allocation techniques. IPv6 has the capability to enhance end-to-end security, mobile communications, QoS, and ease system management burdens.

IPv6-Based Services in Practice

To capitalize on these benefits, many service providers are aggressively evaluating the capabilities of IPv6 in the broadband arena. Some countries, in fact, have already moved from the test and evaluation stage of IPv6 to actual customer deployments. Not surpris-

ingly, these are the same countries that lead the world in consumer broadband access—namely, South Korea, Japan, and China, which along with a few other countries are looking toward moving IPv6 to full production in 2005. Some of the ISPs providing broadband IPv6 services are SpaceNet in Germany (www.space.net), Nerim in France (www.nerim.com), XS4ALL in The Netherlands (www.xs4all.nl), Dolphins in Switzerland (www.dolphins.ch/ipv6), and NTT East in Japan (www.ntt-east.co.jp).

NTT East, for example, launched a commercial dual-stack (devices capable of forwarding both IPv4 and IPv6 packets) unicast service option earlier this year for its ADSL and fiber to the home (FTTH) subscribers. The company is charging an additional 300 yen (about US\$3.00) monthly for this service. The subscribers are dual-stack capable with IPv4 and IPv6 addresses, and the IPv6 addresses are dedicated (/64 per user) and used when needed.

Some ISPs currently providing IPv4-based multicast and VoIP services are also evaluating the benefits of IPv6. Their multicast services mostly consist of video (a movie, for example) and audio (Karaoke, for example) streams. Users sign up with a content provider that is multicasting several channels of video and audio, and after authentication, these subscribers join their multicast group of interest to start receiving the streams. This service is akin to cable television offerings in which cable customers sign up and pay for single events or programs (pay per view) or packages of programs. With IPv4, there is generally a single device directly attached to the customer premises equipment (CPE) that receives the multicast stream. In moving to IPv6, ISPs should expect to serve multiple devices attached behind a single CPE.

ADSL, FTTH, cable, and wireless are the main broadband access technologies currently deployed. The rest of this article will focus on some key components of IPv6 broadband networks, how IPv6 differs from IPv4, and specifically how IPv6 is deployed using ADSL, FTTH, and cable broadband access technologies. For a comprehensive overview of IPv6 addressing schemes and various network deployment scenarios including broadband, see *The ABCs of IP version 6*, at cisco.com/packet/164_8b1. For detailed IPv6 broadband deployment scenarios, see IETF working draft, “ISP IPv6 Deployment Scenarios in Broadband Access Networks,” at cisco.com/packet/164_8b2.

IP Address Allocations

IPv4 primarily relies on Dynamic Host Control Protocol (DHCP) for address assignment to clients. In IPv4, clients typically receive a single IP address from the DHCPv4 server, or the address is statically configured. In IPv6, a single client can have multiple addresses assigned to it. IPv6-enabled CPE might receive a /48 or /64 prefix from the service provider, depending on the provider's policy and the customer's requirements. If the CPE has multiple networks connected to its interfaces, it can receive a /48 prefix from the provider and use it to assign a /64 prefix to each of its interfaces. Hosts connected to these interfaces can automatically configure themselves using the /64 prefix. There are four ways to append an interface ID (last 64 bits of the IPv6 address) to make it a complete 128-bit IPv6 address: EUI-64 format, manual configuration, random generation (RFC 3041), and DHCPv6. IPv6 primarily uses *stateless autoconfiguration* or *DHCPv6* to automatically assign addresses.

Stateless autoconfiguration (RFC 2462) enables basic configuration of the IPv6 interfaces in the absence of a DHCPv6 server. Stateless autoconfiguration relies on the information in the router advertisement (RA) messages to configure the interface. The /64 prefix included in the RA is used as the prefix for the interface address. For Ethernet, the remaining 64 bits are obtained from the interface ID in EUI-64 format. Thus, an IPv6 node can autoconfigure itself with a globally unique IPv6 address by appending its link-layer address-based interface ID built in EUI-64 format to the /64 prefix. Randomly generating an interface ID, as described in RFC 3041, is part of stateless autoconfiguration and used to address some security concerns.

Using DHCPv6 (RFC 3315), IPv6 also supports stateful configuration of IP addresses to nodes. Clients can send a Solicit message to the All_DHCP_Relay_Agents_and_Servers address and request IP address assignment and other configuration options from the DHCPv6 server. Called *stateless DHCPv6* (RFC 3736), this option is used to deliver information such as Domain Name System (DNS) (RFC 3646) or Session Initiation Protocol (SIP) server addresses. The client-server message exchange can consist of either two or four messages.

Because CPEs might receive a /48 or /64 prefix, a technique called *DHCPv6 prefix delegation* (RFC 3633) can be used by delegating routers to assign variable-length prefixes to requesting routers or CPEs. Requesting routers use DHCP options to request prefix(es) from the delegating router via a unique identifier.

IP Address Renumbering

When the service provider for a network changes, all the node's IP addresses must be renumbered. IPv6

simplifies renumbering by configuring the routers to send out the RA with added prefix information, a current prefix with a shorter lifespan and the new prefix with a normal lifespan. The RA will include only the new prefix (RFC 2461) when the current, shorter-lifespan prefix expires. Renumbering also requires changes to the DNS entries and the introduction of new IPv6 DNS records. Renumbering an entire physical site also requires that all the routers be renumbered. Stateless autoconfiguration does not address the issue of finding the DNS server for DNS resolution—stateless DHCP does—or registering the computer in the DNS space. IPv6 introduces new DNS record types for IPv6 addresses that are supported in the DNS name-to-address and address-to-name lookup processes. These include the *AAAA* (or *quad*) *record*, which maps a host name to an IPv6 address; the *pointer (PTR) record* used in IP address-to-host name lookup; and *DNAME* and *binary labels records*, which make renumbering easy for inverse mapping (IP address to host name).

Embedded Security

While IPv4 has several mechanisms to provide security on network devices, IPv6 has *built-in capability for providing data protection through IP Security (IPSec)*. IPv6 provides security extension headers, making it easier to implement encryption and authentication. IPv6 uses IPSec to provide end-to-end security services such as access control, confidentiality, and data integrity. But as with IPv4, security is a more complex issue than just configuring IPSec, and a full set of integrated security features is required to protect a network. The following security features can be configured to protect an IPv6 network:

- **Access control lists (ACLs)** for traffic filtering based on source and destination addresses, and filtering of traffic based on a combination of IPv6 option headers and optional, upper-layer protocol information for finer granularity of control
- **Stateful filtering or firewalling** to control the IPv6 traffic. Cisco IOS® Firewall for IPv6, in Cisco IOS Software Release 12.3(7)T and higher, performs up to Layer 4 inspection including IP fragment inspection of IPv6 packets.
- **Unicast Reverse Path Forwarding (uRPF)** to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router.

SALMAN ASADULLAH, CCIE®, a technical leader in Cisco's Customer Assurance Group, has been designing and troubleshooting large-scale IP and multiservice networks for more than eight years. He represents Cisco in worldwide industry panel discussions and technical conferences, and can be reached at sasad@cisco.com.

ADEEL AHMED, CCIE, is a network consulting engineer in Cisco's Service Provider Broadband Group. He has worked with major worldwide cable MSOs in designing and troubleshooting cable networks, and has written several white papers and design guides. He can be reached at adahmed@cisco.com.

■ **Authentication, authorization, and accounting (AAA)** along with RADIUS is typically used in DSL and FTTH networks for users connecting to the service provider's network. The current Cisco IOS Software implementation of IPv6 on RADIUS uses Cisco Vendor Specific Attributes (VSA) with specified AAA user attributes. In Cisco IOS Software Release 12.3T and higher, support for the AAA user attributes is provided as defined in RFC 3162. Currently, the RADIUS transport is IPv4, not IPv6.

IPv6 in ADSL and FTTH Access Networks

Customer link encapsulations such as *Point-to-Point Protocol over ATM (PPPoA)*, *PPP over Ethernet (PPPoE)*, and *Routed Bridge Encapsulation (RBE)* can leverage the IPv6 extensions to the AAA function. ADSL supports all three encapsulation techniques, while FTTH supports PPPoE and RBE. PPP over ATM adaptation Layer 5 (AAL5), as described in RFC 2364, is created between the CPE and access concentrator. The IPv6 traffic originated by the user's PC flows over Ethernet to the CPE; it is then encapsulated over PPP to flow between the CPE and the access concentrator. The CPE is Layer 3 and IPv6 aware.

PPPoE (RFC 2516) is used to transmit IPv6 traffic between the user's PC/CPE and the access concentrator over PPP. If the PC is acting as a PPPoE client, the CPE bridges all traffic received from the PC to the access concentrator. In this case, the CPE is Layer 3 as well as IPv6 unaware. If the CPE is acting as a PPPoE client, it needs to form a PPPoE session with the access concentrator and send the IPv6 traffic over it. The CPE needs to be Layer 3 and IPv6 aware in this case. Additionally, the IPv6 traffic can be natively forwarded to the service provider with no additional PPP-like encapsulations. If the CPE is already bridging the IPv4 traffic (RFC 1483), it can forward the IPv6 traffic at Layer 2 as well. There is no need for an upgrade or a change in the CPE configurations, which is a major deployment benefit. The provider edge (PE) router has to be upgraded to dual stack, and the IPv6 RBE feature has to be configured on the CPE-facing interfaces to enable the PE router to route the IPv6 traffic while continuing to bridge IPv4 traffic. In this case, the PE communicates directly with the hosts behind the CPE, where CPE is IPv6-agnostic.

Note: Throughout this discussion, the term PE refers to the access router located in the broadband provider's network, and CPE refers to the router located in the customer's network.

If the CPE is Layer 3 aware, a prefix is set between CPE and PE, where the traffic is natively routed between them. The CPE and PE are upgraded to dual-stack routers. In this scenario, when the CPE

needs to service multiple subnets, it can acquire a /48 prefix via DHCP-PD from the PE. Once CPE acquires /48 prefix, it segments it to /64s and assigns them to its interfaces.

If customer access is offered via PPPoE for both IPv6 and IPv4, the IPv4 and IPv6 addresses are negotiated with PPP at Layer 2 (IPCP for IPv4 and IPv6CP for IPv6). On the other hand, if the user stays with PPPoE for IPv4 and routes IPv6 using RBE encapsulation, then the IPv6 addresses are negotiated by DHCP or neighbor discovery (ND) using RA at Layer 3. Using RBE makes IPv6 deployable on any data-link layer.

There are two main ADSL/FTTH deployment models: *ISP operated* or *wholesale*.

ADSL/FTTH Access ISP Operated Architecture

In an ISP-operated architecture, the PE (Network Access Server, or NAS) owned by the broadband service provider assigns the IPv4 address to the CPE device. This is done by either DHCPv4 using AAA and RADIUS, or statically. The IPv4 traffic is sent from the CPE to the PE using the aforementioned encapsulation techniques. For a diagram of an ISP-operated architecture with the NAS function, see cisco.com/packet/164_8b3.

When deploying IPv6 in this framework, the same encapsulation techniques are used and the same behavior is achieved by the PE (NAS) assigning the IPv6 address to the CPE device. Assigning the IPv6 address is done either by using stateless autoconfiguration, DHCPv6 using AAA and RADIUS, or statically. Depending on the agreement between the broadband provider and the user, the IPv6 address assignment could have a prefix length from /48 to /64. The PE and CPE are upgraded to dual-stack routers to support both IPv4 and IPv6. The only scenario when the CPE is not upgraded to a dual-stack router is when the PC behind the CPE is running a PPPoE client, where IPv6 address will be assigned to the PC from the PE router and CPE would act as a bridge.

ADSL/FTTH Access Wholesale Architecture

In a wholesale environment, currently IPv4 traffic is sent from the CPE to the PE (Layer 2 Tunneling Protocol access concentrator, or LAC) using the aforementioned encapsulation techniques. The LAC initiates an L2TP tunnel to the L2TP network server (LNS) router, which assigns an IPv4 address to the CPE or device initiating the PPP session using DHCPv4 with AAA and RADIUS, or statically. Once the L2TP tunnel comes up, all traffic is forwarded to the LNS router over the L2TP tunnel. For a diagram of a typical wholesale architecture with LAC and LNS functions, see cisco.com/packet/164_8b4.

While deploying IPv6 in the wholesale model, the CPE and PE (LAC) are upgraded to dual-stack routers to support both IPv4 and IPv6. The only

scenario when CPE is not upgraded to a dual-stack router is the same as in the ISP-operated model. The PE (LAC) initiates a L2TP tunnel to the LNS router to forward traffic received from the CPE. The LNS assigns IPv6 addresses to the devices (routers, PCs, etc.) located behind the CPE using stateless autoconfiguration, DHCPv6 using AAA and RADIUS, or statically. The CPE might receive a prefix of /48 to /64 depending on the broadband provider's policy and user's requirements. In this case, the LNS router is also upgraded to dual-stack to support both IPv4 and IPv6.

IPv6 in Cable Networks

Currently native IPv6 is not supported over cable networks because of asymmetric communication that creates issues with ND. The existing IPv4 cable architecture heavily depends on DHCPv4, and changes will need to be made to the DOCSIS specification to support native IPv6 over cable. At this time, IPv6 can be tunneled over an IPv4 cable network. The current IPv6 architecture for cable networks includes two components that must be provisioned: the cable modem and the CPE. The CPE might be a device, such as a computer, or an embedded system that uses a single IPv6 address, or it might be a gateway device that connects one or more customer networks to the link to the Multiple Service Offering (MSO) network. The cable modem and CPE are provisioned separately.

In a bridged CMTS environment, to keep the IPv6 transition smooth and reduce operational complexity, the CMTS and cable modem continue to be the bridging devices. In addition to bridging IPv4 traffic, the CMTS and cable modem need to bridge IPv6 unicast and multicast traffic as well.

In a routed CMTS environment, a dual-stacked CMTS is needed. The CMTS might need to tunnel IPv6 traffic over the existing IPv4 infrastructure until service providers can enable native IPv6 on their cable networks.

IP Addressing Allocation in Cable Networks

The cable modem still uses an IPv4 address on the cable interface connected to the link to the MSO network for management functionality. During the initialization phase, it obtains its IPv4 address using DHCPv4 and downloads a DOCSIS configuration file identified by the DHCPv4 server. The CPE needs to obtain an IPv6 address for the interface connected to the MSO network. In addition, if the CPE is a gateway device, it will obtain a network prefix for addresses assignment within the customer network. The CPE uses either stateless autoconfiguration or DHCPv6 to obtain an IPv6 address.

The CPE uses DHCPv6 to obtain an IPv6 address in the same way as DHCPv4 is used today. The DHCPv6 messages exchanged between the CPE and the DHCPv6 server are forwarded by the CM. DHCPv6 gives the MSO explicit control of the

address used by the CPE for accounting, traffic management, and assigning a separate prefix for use by CPEs at each customer location.

In the case of stateless autoconfiguration, the CPE listens for the RA from the edge router (access router). The RA carries the prefix assigned to that particular downstream interface. Upon receipt of an RA, the CPE constructs its address by combining the prefix in the RA (/64) and a unique identifier EUI64 (e.g., its MAC address). All CPEs attached to a particular interface will receive the same prefix and hence will be in the same subnet, where MSO will have no control of the addresses used by the individual CPEs.

If the CPE acts as a gateway device, it will use DHCPv6 prefix delegation (PD) to obtain a prefix to assign addresses to devices attached to the customer network. For a diagram of a typical IPv6 cable deployment, see cisco.com/packet/164_8b5.

QoS and Security in IPv6 Cable Networks

The QoS mechanisms on the cable modem termination system (CMTS) and cable modem must be IPv6 capable. This includes support for IPv6 classifiers, so that data traffic to and from CPE devices can be classified appropriately into different service flows and be given the appropriate priority. Appropriate classification criteria would need to be implemented for unicast and multicast traffic. Security in DOCSIS 1.1 and 2.0 environments is provided using Baseline Privacy Interface Plus (BPI+). The only portion of the specification that depends on IP addresses is encrypted multicast. Semantically, multicast encryption would work the same way in an IPv6 environment as in the IPv4 environment. However, appropriate enhancements are needed to support encrypted IPv6 multicast.

♦ ♦ ♦

The flexibility of IPv6 is helping service providers offer new broadband services as well as enhance current offerings with a strong focus on servicing endpoints. With plenty of addresses to accommodate the world's population for decades as well as a slew of devices, IPv6 is significantly expanding the possibilities for service providers of all types.

The authors wish to thank Ciprian Popoviciu and Patrick Grossetete for contributing to this article. ■

FURTHER READING

- White paper: IPv6 Access Services
cisco.com/packet/164_8b6
- Cisco IOS releases for IPv6 features
cisco.com/packet/164_8b7
- Internet-Draft: ISP IPv6 Deployment Scenarios in Broadband Access Networks
cisco.com/packet/164_8b8
- e-Nations IPv6-related links
cisco.com/packet/164_8b9

Go Daddy Grows with IP Communications

Hard work, smarts, and a powerful network make Go Daddy a champ.



Tom Garczynski

GROWING STRONG IN ARIZONA Go Daddy's Mark Wachtmann, vice president of Information Technology, and Greg Schwimer, director of Network Engineering and Telecommunications, have helped the company become an industry leader by creating a strong network infrastructure based on Cisco technology.

By Fred Sandsmark

The business of helping people and companies establish an online presence is a rough-and-tumble proposition. Competition abounds, and price competition is fierce. Although the company is just seven years old, Scottsdale, Arizona-based Go Daddy has emerged as a contender and was recently rated No. 8 on the Inc. 500 list of fastest-growing privately held companies in the United States; it is also the fastest-growing IT company on the list.

Best known as a domain-name registrar—it registers a new domain name every 7.4 seconds—Go Daddy registered more than 1.5 million domains in 2003—more than any other registrar, according to independent industry watcher Name Intelligence. It leads the pack in customer satisfaction. Go Daddy also offers Web hosting, e-mail, Secure Sockets Layer (SSL) certificates, and an online shopping cart directly to customers online and through a network of 11,000 resellers. It hosts sites for 300,000 customers and processes 5 million to 8 million e-mail messages per day.

How does Go Daddy do it? A staff of more than 500 people, over 300 of whom are customer-service agents, brings together a combination of hard work, serious smarts, and a powerful, flexible network infrastructure that Greg Schwimer, the company's

director of Network Engineering and Telecommunications, calls the Go Daddy Backbone Network.

The Go Daddy Backbone Network consists of the company's optical metropolitan-area network (MAN), connecting three sites in the Scottsdale area, plus a WAN connection to an office in Iowa. The backbone extends to the network's edge, where it peers via Border Gateway Protocol (BGP) at multigigabit rates to multiple Internet service providers (ISPs). "We use those providers not only to get as close to the end customer as possible, but also for redundancy," explains Schwimer.

For security reasons, Schwimer won't discuss those connections in detail. "Let's just say that there's a reason we have multigigabit connections to the Internet," he says. "We need it." The company's bandwidth requirements doubled in the first nine months of 2004.

"We treat the whole backbone like a carrier-class network," Schwimer says. "We've implemented MPLS [Multiprotocol Label Switching] VPN [virtual private networking] and traffic engineering, which gives us flexibility and the ability to virtualize a lot of services over the network. It's saved us a bundle of money because we can use existing circuits for multiple

purposes without buying additional services or circuits for back-end connectivity.” (Go online to cisco.com/packet/164_9a1 to see a network diagram of the Go Daddy Backbone Network.)

Go Daddy uses a combination of open-source products and proprietary tools it has developed to monitor and manage its entire infrastructure. “Monitoring extends beyond the network,” says Mark Wachtmann, Go Daddy’s vice president of Information Technology. “Sometimes issues in one part of our infrastructure alert us to a potential issue in the network. And many times our monitors in the network alert us to issues going on in other places in the infrastructure.”

Bandwidth on the backbone has increased dramatically over the last few years, going from a single T1 connection between sites to multiple T1s, to DS3 and OC-3, and finally to an optical MAN owned and operated by Go Daddy, which should address the company’s long-term growth needs. “We’re constantly adding new services, whether it’s new servers or new applications on existing servers,” Schwimer says. “That requires input and change from my team on a daily basis.”

The backbone handles office-to-office connectivity in addition to customer-facing services. All of the company’s business applications are, of course, Web-based.

Browser-based applications help keep Go Daddy competitive. The staff works long hours and is constantly on the move. Some staffers use handheld Palm Treos for e-mail (a service they also offer to their customers). “Everybody’s a home user at some point,” Schwimer says, “so everybody has remote access by VPN. They provide their own equipment at home and we provide them with a VPN client.” This allows employees to connect to the network and its services reliably and securely wherever there is an Internet connection.

Making the Call

In August 2004, the company implemented Cisco IP communications for its full staff and Cisco IP Call Center (IPCC) to the services it runs on the Go Daddy Backbone Network.

Wachtmann cites three reasons for the move to IP communications. “One, it was a question of growth. We have more than 300 people in our call center handling massive numbers of calls every day, both inbound and outbound,” he says. “Two, we needed additional features—such as preview and predictive dialing—that would make our employees and customer-service representatives more productive. And three, we wanted to use this same system in multiple locations and tie it all together.”

Tying it together saves Go Daddy money. “It gives us opportunities to scale all of our telecom through our Scottsdale office, which gives us more leverage with vendors, lower long-distance prices, fewer

trunk circuits, and more aggregation of trunks,” Wachtmann says.

Planning for IP communications took several months—time that Go Daddy considers well spent. The company looked hard at its growth plans over the coming 12, 36, and 60 months. “We did a lot of iterations,” Wachtmann continues. “But when we put the request for proposals out, we had decided that IP telephony was the direction we needed to go.”

The company also specified that the phone system had to work with its existing Cisco gear. “We started upgrading the infrastructure in our offices a year ago. When we did our Cisco IPCC implementation there wasn’t a huge core upgrade associated with it,” Wachtmann says. “We had been planning for inline power before we purchased the phone system.”

As for the additional cost to build a phone-capable network, Schwimer says “the incremental cost was so small that it didn’t make sense not to do it. We elected to spend that extra money to future-proof ourselves.”

The phone system handles more than 50,000 calls per week, but network operations didn’t change dramatically. “We operate the network the same way we did previously,” Schwimer says. “We monitor it the same way. On a day-to-day basis, it’s really no different.”

Go Daddy implemented its IP communications system very quickly. “From the signing of the contract to going live took 60 days,” says Wachtmann. “That’s to roll out a redundant, 500-node Cisco IPCC phone system with a call center, scripting, prompting, advertising, messaging, and more. All equipment on site, configured, and full cutover.”

Go Daddy accomplished this feat by carefully creating the proposal, managing the implementation process, and vetting its implementer. “We had telephony experience on staff, and we worked very closely with our contact center team,” Schwimer explains. “They were able to provide quite a bit of information as to their specific requirements. We had a detailed list of what we were looking for, which ultimately helped us make the decision to implement what we did. And it helped us manage the actual implementation by making sure that everything was mapped to our requirements.”

Wachtmann feels that choosing a good implementation partner was a factor in Go Daddy’s successful IP communications rollout. “The service provider you choose is a key decision,” he says. Go Daddy evaluated several before selecting NEC Unified Solutions. “We talked to other companies and checked references,” he says. “I can’t stress enough the importance of making sure that you get the best implementation services team that you can.”

IP Centrex

Although more than 50 percent of midsize and large enterprises are expected to implement IP telephony in the next 12 months, smaller businesses can also benefit from increased productivity facilitated by a converged network for voice and data applications.

BT, for example, initially targeted its IP telephony offering at larger companies but developed an even lower-cost solution for smaller organizations when one of its longstanding customers, vehicle-rental company Northgate PLC, turned to the U.K.-based carrier for help. Similarly, Italian service provider FastWeb offers an integrated package of voice, data, and Internet access services for a range of small and medium customer types.

Both BT and FastWeb use Cisco CallManager Express, a business-class software module for Cisco IOS® routers that offers popular IP PBX features for up to 120 Cisco IP phones or traditional analog phones.

"For customers who see full-blown IP communications solutions as being too expensive, Cisco CallManager Express is a way they can put their toe in the water with a minimal investment," says Cuan Middleton of BT Convergent Solutions.

SMBs get increased benefits when they host Cisco CallManager Express on a router on their own premises and augment it with the Cisco BTS 10200 Softswitch in the service provider's data center. The Softswitch extends customers' capabilities by providing additional network-based services, such as routing on-net calls between distributed sites, managing private customer dial plans, and serving as a central point for connecting to the PSTN for off-net calls. —Sam Masud

"We had already done numerous IPCC deployments in the Phoenix-Scottsdale area," explains R. Vijayasarithi, account manager with integrator NEC Unified Solutions, the networking subsidiary of the Japanese electronics giant. "NEC Unified Solutions traditionally is a voice company, and we have cross-trained data and voice engineers who have had more than 20 years of call-center applications expertise."

Do-It-Yourself Attitude

NEC Unified Solutions' involvement ended when the system went live. "We needed additional resources

to get through the implementation," Wachtmann says. "But one key deliverable was that, once the phone switch was in, they walk away from the engagement. We're more than prepared to manage our own phone switch."

"We also did a lot of mentoring," says Vijayasarithi. "Making Go Daddy self-sufficient was a very important part of the engagement, so we had them work in our labs for about three weeks. We built call flows, then had their engineers build the call flows on their own. We also trained almost 400 people."

That sort of self-sufficiency typifies how Go Daddy runs its network and its business. The company doesn't outsource or offshore jobs. It builds its own infrastructure-management tools and its own business-intelligence and enterprise resource planning (ERP) software (all Web-based, of course).

"The benefit of doing things yourself is that it creates ownership internally," explains Schwimer. "You really need to understand how the business operates in order to effectively implement a network or a service on the network. I don't think anybody from outside would be able to do that at the level we need it."

Go Daddy also rigorously defines the processes that support its tools. "You can have all the tools in the world, but without the proper processes behind them, they're ineffective," says Schwimer.

As its IP communications implementation demonstrates, rigorous, refined processes underlie all technology decisions at Go Daddy. An information security group that's separate from the general IT staff reviews all equipment, and thorough, early analysis is routine. "It's a discipline that we've had to drill into ourselves," says Schwimer. "If you don't put in the early analysis, you might pay for it on the back end. It's always a tension we have, and we struggle with it: Move quickly, but make the right move."

Go Daddy does that by investing in the right equipment. "It comes down to buying flexibility and scalability," says Wachtmann. "That's a discussion we have all the time: Will this solution be flexible enough for Go Daddy, and will it scale at the rate we need it to?"

"We've invested heavily in Cisco gear because the network is an area where we cannot fail," he concludes. ■

FURTHER READING

- Introduction to Cisco MPLS VPN Technology
cisco.com/packet/164_9a2
- MPLS VPN documentation
cisco.com/packet/164_9a3
- NEC Unified Solutions
www.necunifiedsolutions.com

Big Solutions for Smaller Offices

New SMB Class networking products are designed specifically to provide the modularity, ease of use, and affordability that SMBs need.

By Gene Knauer

Small and midsize businesses (SMBs) today want it all—and they deserve it. They want the cost benefits and competitive advantages from data, voice, video, mobile, and other services and applications running on their IP networks. They want high availability, security to protect against attacks, and virtual private networks (VPNs) for secure external access. They want solutions to be affordable to buy and maintain. And with smaller staffs responsible for their networks, SMBs are looking for equipment that doesn't require an advanced engineering degree or extensive study to operate.

Shopping for it all can be a challenging experience. Multiple hardware and software components from hundreds of vendors exist in each solution category. Getting all of the pieces to work together, managing and maintaining technologies in converged IP networks, and adapting quickly as new priorities arise are tasks that can keep SMB information managers awake at night.

The Cisco SMB Class portfolio of networking solutions emphasizes a network foundation with the security, availability, and quality of service (QoS) designed specifically for smaller organizations. Until recently, these types of solutions were often available only for larger enterprises, which meant smaller companies had to adapt solutions for their use or come up with something on their own.

The Cisco 1800, 2800, and 3800 series of integrated services routers (ISRs) represent a new architecture designed to fit the needs of SMBs. The ISRs are complemented by the Cisco Catalyst® 4503 Switch, which has been made more modular and expandable, and has more user-friendly security and network management tools. Cisco has designed these products with greater modularity and flexibility, added simpler and more powerful management features, and scaled pricing.

"The Cisco ISRs, the Catalyst 4503, and free management tools together deliver features and functions that you would otherwise have to buy in many separate appliances for a lot more money," says Kevin DeCato, marketing manager in Cisco Commercial Solutions. "These products emphasize ease of use and affordability while delivering the technologies to offer converged, multiservice networking at wire speed and the security, high availability, and management that any serious business requires."



JUST FOR THE SMB CLASS The new Catalyst 4503 Switch has been made more modular with user-friendly security and network management tools to better fit the needs of small and midsize businesses.

Modular and Expandable Routers

Unlike many other products, the new Cisco ISRs embed security, voice, video, and network analysis services inside the router as a single, resilient system. To address the changing priorities of SMBs and give companies flexibility, more interfaces are available for each router than ever before. For example, the ISRs include special slots that can accommodate digital signal processors (DSPs) for voice to free up the network module slots for other IP services.

An array of modules are available to SMBs, including content engines, Cisco Unity™ Express voice messaging, Layer 2 switching with Power over Ethernet (PoE), and more. Hardware encryption is now performed on the ISRs, so a separate AIM module is not necessary—but larger environments can opt to add the additional module for even higher performance.

"We think the new chassis for the ISRs will revolutionize customer premises equipment," says Brian Ryder, product line manager for the Cisco 2800 Series routers. "Our intent is to encourage adoption of new IP services by making the routers more easily deployable and scalable."

Previously, running multiple services over a T1 line could cause strain on the routers from all of the added components for each new service. With the ISRs, which are designed to run multiple services,

Continued on page 65

SMB Networks, Continued from page 63

security and voice are built into the motherboard of the chassis so it doesn't require separate cards for voice and VPN, which would take up slots on the router. IP telephony can scale from 2 to 88 lines. WAN interface slots on the ISRs have also been increased from two to four.

A Switch Businesses Can Grow Into

"SMBs are rolling out more advanced applications such as IP telephony. They're converging their networks, which means they need all of the elements of larger networks, but with ease of use and affordability," says Dave Dhillon, product marketing manager for the Cisco Catalyst 4500 Series switches.

"We've made the Catalyst 4503 Switch more affordable and scalable by adding a SMB-sized Supervisor II-Plus-TS, which features 20 built-in 10/100/1000 PoE and Small Form-Factor Pluggable (SFP) ports that increase the scalability of the Catalyst 4503 to 116 ports," Dhillon adds. "Also, new line cards give SMBs the option of scaling their networks by increments of 6, 24, or 48 ports as their organizations grow."

Another feature allows the Catalyst 4503 to utilize a standard office 15-amp power plug instead of a 20-amp plug when enabling the 12 PoE Ethernet ports on the Supervisor to simplify connectivity to wireless access points, IP phones, IP-based surveillance cameras, and other devices.

The modular architecture of the Catalyst 4500 Series offers easier PoE management, centralized configuration, troubleshooting, and control. In addition, modularity offers businesses an easy upgrade path to new modules and services, as well as redundant power, fans, and hot-swappable components, easing serviceability and delivering higher availability.

Way to Grow

Designed to help companies invest in new technology and equipment, the Routing Migration Program provides incentives for companies that want to upgrade from the Cisco 1600, 1700, 2500, 2600 classic, and 3600, and 3700 series multiservice access routers to the new Cisco 1800, 2800, and 3800 series ISRs. Under this program, customers can trade in their older Cisco routers for credit toward newer or higher-end routing platforms.

For more information, go to cisco.com/packet/164_9b1.

Start Small, Grow Easily

The Linksys® to Cisco Trade-Up Program provides both new and existing Linksys customers with a migration path to Cisco routing, switching, and wireless solutions, while offering up to 100 percent investment protection on their existing small-business Linksys products. Linksys customers that have outgrown the capacity and features of their Linksys equipment can trade up to Cisco solutions and receive a cash rebate for their relevant small-business Linksys equipment.

For more information, go to cisco.com/packet/164_9b2.

"The Catalyst 4500 Series was engineered based on the security, availability, and converged network features in Cisco enterprise switching products and then right-sized and competitively priced for the mushrooming needs of SMB networks," says Dhillon.

Free, GUI-Driven Tools

Today SMBs represent a broad spectrum of different kinds of businesses, some very small and often without dedicated network staff or a depth of technical expertise. It's important then, that networking products be made easy to use.

Cisco Network Assistant is now available and supports the Cisco Catalyst 4500 Series switches as well as fixed-configuration Cisco Catalyst switches. The free Cisco Network Assistant has an easy GUI for centralized network management that users can use instead of the more complex command-line interface. Cisco Network Assistant automatically identifies supported Cisco devices running in a network, and provides status on each device.

Cisco Network Assistant lets users launch other device managers, including the Cisco Router and Security Device Manager (SDM), an intuitive, Web-based tool that comes preinstalled on all ISRs and also supports earlier generations of Cisco access routers.

Designed for SMB customers and Cisco channel partners, Cisco SDM is unique due to its built-in application intelligence and integrated Cisco Technical Assistance Center (TAC) knowledge base to reduce configuration errors and assist in troubleshooting network issues.

Another user-friendly tool, the Catalyst device manager, is a lightweight, embedded, HTML-based application that replaces Cisco Cluster Management Suite (CMS) as the device manager for Catalyst switches with fixed configurations. Typically used when configuring a single Catalyst switch, this tool provides an



The Fourth Quarter issue of *iQ* features articles about the financial-services and manufacturing industries as well as profiles of companies using the Web to grow their businesses in innovative ways.

You'll also find articles to help you with marketing, partner relationship management, financing technology investments, and other information that helps bring your organization's business needs and technology strategy together.

Find the articles online at cisco.com/go/iq. Find ways to make your businesses work smarter with insights, strategies, and news for decision makers. Subscribe today to get *iQ Magazine*, a free quarterly publication from Cisco for small and midsized businesses. cisco.com/go/iqmagazine/subscribe/packet.

easy way to perform IOS® Software upgrades and leverages Cisco Smartports technology to quickly implement advanced features.

Calculating Long-Term Value

With the rapid pace of network expansion among SMBs, the initial purchase price of network

infrastructure often drives purchasing decisions, while associated costs and long-term investment are not fully understood. However, incremental labor costs to integrate different equipment effectively, training for solutions from different vendors, and costs for downtime due to troubleshooting problems between multiple vendors can quickly add up.

The degree of flexibility and scalability of products can also drive value up or down as the size and priorities of companies evolve.

Cisco has developed an integrated services approach to routing and switching for SMBs to minimize training requirements, troubleshooting, downtime, and outside professional services. Customers benefit from the long list of IP services possible with the same Cisco end-to-end infrastructure. Companies looking for WAN connectivity and VPNs today can leverage the same investment to add IP telephony or multicast video features tomorrow. ■

FURTHER READING

- Cisco Network Foundation for SMBs
cisco.com/packet/164_9b3
- Cisco Network Assistant
cisco.com/go/networkassistant

Wielding Influence in the ITU-T

By Rajiv Kapoor

Cisco's influence is growing quickly in The International Telecommunications Union—Telecom Sector, or ITU-T (itu.int/itu-t)—the standards body that specifies the technologies and standards most important to large telecommunications companies and service providers. With its long history and involvement with other standards bodies devoted to IP networking technology and the Internet—IEEE and IETF—Cisco is in a unique position to help forge agreement across standards bodies as traditional IP technology and telephony merge.

Earlier this year, the ITU-T approved two Cisco-developed standards proposals: Q.NSS.1 (Q.1980.1) Narrowband Signaling Syntax (NSS), and Time-Division Multiplexing (TDM) over MPLS encapsulation (Y.1413). Both standards were driven substantially by involvement of Cisco's Carrier Standards and Architecture Group.

Standards Innovation

NSS, formerly called Generic Transparency Descriptor (GTD), is one of several significant standards efforts in the area of voice call control. NSS is a text-based syntax that enables the many ISDN User Part (ISUP) parameters to be transparently transmitted through IP networks. In particular, it is used to transmit ISUP parameters—the call control part of the Signaling System 7 (SS7) protocol—within Session Initiation Protocol (SIP) and H.323 networks.

By transmitting these parameters within SIP and H.323, NSS reduces data redundancy and data synchronization problems. This helps the interworking between the PSTN and SIP or H.323 networks, helping to speed the migration of voice to IP. With standardization, service providers will be more likely to deploy NSS; service providers Singtel and British Telecom are already using NSS as part of the Cisco PGW 2200 Softswitch and other Cisco IOS® Software platforms.

GTD was invented inside Cisco and is an example of innovation that Cisco is now bringing into service provider standards organizations once dominated by Cisco competitors.

MPLS Standards

Proposals from Cisco on TDM over MPLS interworking were approved to be standardized at the ITU-T Study Group 13 meetings. In the past few years, the IETF has endeavored to make progress on TDM encapsulation over IP/MPLS. In May 2003, with a strong push by Cisco, the ITU-T began working on TDM over MPLS encapsulation and completed Recommendation Y.1413 in less than eight months. This development aligned the work done in both the IETF and the ITU-T—a positive step for

the industry facilitated by Cisco's long involvement with the IETF and its new status in the ITU-T.

With TDM over MPLS, carriers have a method to offer private-line TDM services such as T1/E1, T3/E3, and V.35 over a common MPLS network infrastructure. To support emulation of TDM traffic, it is necessary to emulate the circuit characteristics of a TDM network.

TDM over MPLS is based on an earlier Cisco technology, Any Transport over MPLS (AToM), which is based on the IETF draft-martini encapsulation, so named for Cisco engineer Luca Martini, who authored the draft. AToM is generically used to encapsulate many protocols such as ATM, Frame Relay, and TDM inside MPLS frames when these networks are at the edge and use MPLS backbone infrastructures for transport. AToM is also the basis for Cisco's solution for transporting TDM traffic over an IP or MPLS backbone.

In accordance with the principle of minimum intervention by the backbone MPLS network, the method uses encapsulation of raw TDM data into MPLS packets. The encapsulated data can come in two formats:

- **Unstructured TDM.** TDM that consists of raw bit streams of data that disregard any structure that may exist in the TDM bit stream such as T1 or E1 framing described in G.704. This method makes all bits available for payload. This is suitable for applications that do not require discrimination between timeslots or intervention in TDM signaling.
- **Structured TDM.** In this method, data is included in one or more levels of structure, including frames, channelization, and multi-frames. This ensures that packets consist of entire TDM structures and can also be used to carry TDM signaling.

Products that support the TDM over MPLS standard include the Cisco PGW 2200 Softswitch, the BTS 10200 Softswitch, and other Cisco IOS gateways. ■



RAJIV KAPOOR, technical marketing manager, leads Cisco's Carrier Standards and Architecture Group. He is a 15-year veteran of AT&T Bell Labs and was one of the primary designers of the Frame Relay data transport protocol. He can be reached at kapoorr@cisco.com.

SPOTLIGHT ON:

Cisco MDS 9000 Family for SANs: New Products for Secure SAN Extension

The Cisco MDS 9000 Family of Multilayer Directors and Fabric Switches provides intelligent network services such as virtual storage area networks (VSANs), multi-protocol support, and integrated management to



lower the total cost of ownership for storage networking. Multiprotocol support includes Fibre Channel, Small Computer System Interface over IP (iSCSI), Fibre Channel over IP (FCIP), and Fiber Connectivity (FICON). Several new hardware and software additions to the Cisco MDS 9000 SAN Switch family make transporting storage traffic over metro and WANs (or SAN extension) faster and more secure and cost effective—ideal for business continuance, disaster recovery, and remote tape backup applications.

The modular Cisco MDS 9216i Multilayer Fabric Switch integrates 14 Fibre Channel ports and two Gigabit Ethernet ports, which can be configured to support either FCIP for long-distance SAN extension or iSCSI for cost-effective SAN expansion. Additionally, the Cisco MDS 9216i offers an expansion slot capable of supporting any of the Cisco MDS 9000 modules.

The Cisco MDS 9000 Family 14/2-port Multiprotocol Services Module is designed for use in any MDS 9000 modular chassis, including the MDS 9500 Series directors and MDS 9200 Series fabric switches. It combines 14 Fibre Channel and two IP ports in a single form factor for optimized SAN extension.

Cisco MDS SAN-OS 2.0, the most recent software version, improves business continuance with innovations such as tape acceleration and hardware-based compression for improved long-distance SAN extension, and hardware-based IP Security (IPSec) encryption for comprehensive, standards-based security.

cisco.com/go/mds

Edge Routing, Access, and Aggregation

Cisco 3800, Cisco 2800, and Cisco 1800 Series Integrated Services Routers and New WICs

The Cisco 3800, 2800, and 1800 Series Integrated Services Routers offer concurrent security, voice, and routing services at wire speed for enterprise branch offices and small to mid-sized businesses. All models include on-board VPN encryption and acceleration; feature-rich Cisco IOS® Software for security services such as integrated VPN, stateful firewall with Network Address Translation (NAT), Cisco IOS inline Intrusion Prevention System (IPS); the Cisco Router and Security Device Manager (SDM); and more. The Cisco 3800 and 2800 series routers also offer optional voice gateway, call processing, voice mail and auto attendant, transcoding, conferencing, and secure voice features. The Cisco 3800 Series provides dual Gigabit Ethernet ports for converged networks, and the Cisco 2800 Series supports dual Fast Ethernet or Gigabit Ethernet ports. The Cisco 1841 Router supports secure data connectivity at Fast Ethernet speeds. Three WAN interface cards (WICs) are also introduced with these routers. The single-port Cisco Gigabit Ethernet High-Speed WIC (for Cisco 3800 and 2800 series routers) accelerates applications such as Metro Ethernet access, inter-VLAN routing, and high-speed connectivity to LAN switches. The Cisco 4-port and 9-port 10/100 EtherSwitch High-Speed WICs integrate switching and routing and support Power over Ethernet. The new Cisco Integrated Services Routers are covered in greater detail beginning on page 24.

cisco.com/go/isr

Cisco uBR10012 Universal Broadband Router: New Performance Routing Engine

The Cisco Performance Routing Engine (PRE-2) for the Cisco uBR10012 Universal Broadband Router offers high performance, scalability, and availability for delivering advanced data, voice over IP (VoIP), and video services over cable networks. The engine's forwarding perform-

ance of 6.2 million pps and Cisco Parallel Express Forwarding (PXF) features serve up to 64,000 subscribers in a single Cisco uBR10012 chassis. The Cisco PRE-2 also offers memory capacity of 1024 MB and supports full-rate OC-48 network links. cisco.com/packet/164_npd1

Switching

Cisco Catalyst 4948 Switch

The new Cisco Catalyst® 4948 Switch offers 48 ports of wire-speed 10/100/1000BASE-T Ethernet with four alternative wired ports that can accommodate optional 1000BASE-X Small Form-Factor Pluggable (SFP) optics. Supporting Layers 2 through 4, the switch is designed for aggregation of servers and workstations with low latency, high performance, and reliability. Numerous security features help to protect the connected servers from network attacks. The fixed-configuration Cisco Catalyst 4948 Switch occupies a single rack unit and provides optional internal AC or DC 1+1 power supplies that are hot-swappable as well as a hot-swappable fan tray with redundant fans. cisco.com/packet/164_npd8

Cisco Catalyst 4503 Switch: New Supervisor Engine and Line Cards

Exclusive to the Cisco Catalyst 4503 Switch chassis, the Catalyst 4500 Series Supervisor Engine II-Plus-TS is a 64-Gbit/s, 48 million-pps, Layer 2 through 4 switching engine that provides 12 ports of 10/100/1000 802.3af Power over Ethernet (PoE) and eight SFP ports. These wire-speed ports increase switch capacity for connecting LAN users and servers in mid-sized businesses. Also available are four new line cards with a 6-port 10/100/1000 PoE or SFP configuration, and 24-port cards in 10/100 Ethernet, 10/100 PoE, or 10/100/1000 PoE configurations. The Supervisor Engine II-Plus-TS and line cards also include features, such as self-defending security, comparable to those in high-end switch platforms. For more on these and other recently launched Cisco SMB-Class products and services, see page 63. cisco.com/go/catalyst4500

Security and VPNs

Cisco IOS Intrusion Prevention System for Cisco Routers

The Cisco IOS® Intrusion Prevention System (IPS) integrates intrusion detection and prevention capabilities into a wide range of Cisco edge and access routers. Cisco IOS IPS offers inline inspection deep into packets to identify and block attack traffic based on

signature matches. A security administrator can configure threat response actions, such as sending an alarm, dropping the packet, or resetting the connection. In addition, Cisco IOS IPS offers the ability to load and enable selected intrusion detection system (IDS) signatures in the same manner as Cisco IDS sensors, supports more than 700 attack signatures to choose from, and allows administrators to add or modify signatures using the new Cisco Router and Security Device Manager (SDM). SDM (see “Network Management” below) allows dynamic updates of the latest signature packages from Cisco.com. For scalable deployment of IPS across branch-office routers, a centralized HTTPS or TFTP server can be used to load signature files. Cisco IOS IPS is covered in greater detail on page 8.

cisco.com/packet/164_npd2

Cisco VPN Client Version 4.6

Cisco VPN Client Version 4.6 delivers new features to simplify the user's experience when accessing an enterprise VPN. With the automatic update feature, the VPN Client automatically downloads and installs new software or administrator-defined profiles for Windows 2000 and Windows XP users. The browser proxy configuration feature allows the user's browser proxy settings to be configured transparently based on information defined on the Cisco VPN Concentrator. Cisco VPN Client Version 4.6 also complies with Section 508 of the US Rehabilitation Act, ensuring that the software is accessible to people with disabilities. Version 4.6 now offers support for mutual group authentication, providing the ability to replace static preshared keys with a central site certificate. The certificate is used to validate the connection between the VPN Client and the VPN central site device, providing security against potential man-in-the-middle (MITM) attacks.

cisco.com/go/vpnclient

Network Management

Cisco Router and Security Device Manager Version 2.0

Cisco Router and Security Device Manager (SDM) Version 2.0, a Web-based device management tool, simplifies router and security configuration for most Cisco edge and access routers. Version 2.0 offers a completely redesigned user interface with smart wizards to guide configuration tasks. New security features include the Cisco IOS® Intrusion Prevention System (IPS), Easy VPN Server, VPN troubleshooting, Public Key Infrastructure (PKI), Secure

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 August and October 2004. For real-time announcements of the most recently released products, see "News Archive, News Releases by Date" at newsroom.cisco.com/dlls/index.shtml.

ABOUT SOFTWARE: For the latest updates, versions, and releases of all Cisco software products—from IOS to management to wireless—registered Cisco.com users can visit the Software Center at cisco.com/kobayashi/sw-center.

Shell Version 2.0 (SSHv2), and role-based user access. SDM Version 2.0 also supports enhanced router management with features such as real-time application traffic monitoring, WAN troubleshooting, integrated services dashboard, and quality of service (QoS) policies. For more on the Cisco SDM and IOS IPS, see "Fortify Your Network," page 7.

cisco.com/go/sdm

Cisco Network Assistant Version 1.0

Cisco Network Assistant is a PC-based application for managing LANs with up to 250 users in small and mid-sized businesses. Cisco Network Assistant offers centralized management of Cisco Catalyst® switches, routers, and wireless access points typically used in small and mid-sized businesses. A GUI enables users to monitor, configure, and manage a wide array of switch functions as well as start device managers for Cisco routers (SDM) and Cisco Aironet® wireless access points. The Smartports feature automatically implements Cisco best practices for device and port configuration to ensure consistency and reliability in functions for security, availability, and QoS on managed devices. Cisco Network Assistant is available as a free download (see link below) to registered Cisco.com users.

cisco.com/go/networkassistant

Networked Home

Linksys Home VoIP Products >

Three new Linksys® products enable users to access a service provider's voice over IP (VoIP) service over a cable or DSL broadband connection. The Linksys Phone Adapter with 2 Phone Ports (PAP2) turns an Internet connection into a high-quality phone line for placing and receiving calls. The adapter is equipped with two standard phone ports (RJ-11) and one Ethernet port (RJ-45). Each phone port operates independently, with separate phone service and phone numbers. The Wireless-G Router with 2 Phone Ports (WRT54GP2) and a wired Broadband Router with 2 Phone Ports (RT31P2) integrate phone adapter functionality to share the broadband connection between Internet access and phone calls. Both routers provide a three-port switch for connecting Ethernet devices and two phone ports.

Phone Adapter: cisco.com/packet/164_npd3
Broadband Router: cisco.com/packet/164_npd4

Wireless-G Router: cisco.com/packet/164_npd5



Linksys High-Gain Antennas

New high-gain antennas increase the range of a Linksys home wireless network, enabling users to gain wireless access in multiple rooms. The dual Linksys TNC Connector Antennas attach to a Linksys wireless broadband router or access point to increase the effective strength of outgoing Wi-Fi signals and improve the receive sensitivity for incoming signals. The single SMA connector antenna increases the effective signal range for Linksys single-antenna wireless adapters, bridges, and routers. Also available are new stands for mounting antennas on a wall or ceiling.

cisco.com/packet/164_npd6

Cisco IOS Software

Cisco IOS Software for Cable

Cisco IOS® Software for Cable bridges hybrid fiber-coaxial (HFC) and IP domains to enhance the performance and scalability of a Cisco cable modem termination system (CMTS). This software helps cable operators deliver differentiated services such as voice over IP (VoIP), managed virtual private network (VPN), and video transport. Cisco IOS Software for Cable includes features for bandwidth management through load balancing on the Cisco uBR10012 and Cisco uBR7246VXR Universal Broadband Routers. Advanced subscriber traffic management features enable administrators to monitor, analyze, and respond in real time to network usage. MAC domain configuration or virtual interfaces associate different combinations of upstreams to downstreams using the Cisco uBR7246VXR Broadband Processing Engines.

cisco.com/packet/164_npd7

Wi-Fi Network, Continued from page 50

McCullough says the project was an unmitigated success, although they learned a great deal about how to improve the network the next time around. His advice to network engineers constructing similar networks: "Know your physical environment before you get started, and be prepared to supplement wireless transport with other transmission methods. Also, make sure the company supplying the power agrees to routine maintenance and to constantly check the fuel levels. You need continuous power if you want to avoid interruptions in your service."

Looking Ahead

Hettinger believes the hands-on experience gained in wireless technology was extremely valuable to both Cisco and Charter, particularly as Wi-Fi installations become increasingly popular. Researchers at In-Stat/MDR, in Scottsdale, Arizona, expect the number of Wi-Fi hotspots

worldwide to increase from 31,455 in 2003 to 113,555 in 2006, while Gartner predicts that 70 million users will frequent public hotspots by 2007. Hotspots based on Cisco equipment are already located in about 30 countries. These include installations in Starbucks coffee houses, Asian Internet cafes, Fairmont and Starwood hotel chains, airports, European rail stations, and mixed communities of businesses and residences.

Next year, says Hettinger, Cisco and Charter hope to provide greater capacity to support live video and audio transmissions in Bonnaroo's Internet Village. Plans under consideration include using Ethernet more freely to supplement the wireless hubs and enabling more Internet bandwidth, perhaps with a DS3 circuit. They will also consider VoIP services so festival-goers can make phone calls as well as access the Internet using Charter's reliable IP-based communications services.

♦ ♦ ♦
Establishing a network presence at Bonnaroo was an immense task, and many Cisco personnel volunteered their time to make the vision a reality. In addition to the people mentioned in this article, Cisco engineers Kevin Troutman and Paul Lee assisted with the project, and special thanks go to Steve Hoch and Kathy Devine from Mobility Segment Marketing, and Mike Wagner from Linksys Marketing. ■

Boosting Network Security Using Cisco Security Agent

The *Networking Professionals Connection* is an online gathering place to share questions, suggestions, and information about networking solutions, products, and technologies with Cisco experts and networking colleagues. Following are excerpts from a recent *Ask the Expert* forum, "Increasing Network Security Using Cisco Security Agent," moderated by Cisco's Josh Huston. To view the full discussion, visit cisco.com/packet/164_10a1. To view an index of forum topics or to join in on other live online discussions, visit cisco.com/discuss/networking.

Q: *How can we use Cisco Security Agent (CSA) to configure safe browser zones? We have a lot of downloads on our intranet, but CSA treats the browser the same no matter what. I would like to be able to configure URLs in an application class for the browser. That way we could add an app class exception to the "processes executing downloaded content" app class and not have to make individual exceptions based on a filename. I know you can do this with trusted zones in the browser but I'd like to find a way to do it with CSA.*

A: You could create a rule that would add this Web browser process to a dynamic application class when it communicates with certain hosts. This rule would be configured via IP address and could be automatically aged out of that dynamic class after a specified time period.

Q: *I want to protect my servers from threats that can originate from inside as well as outside the network. I have a Cisco PIX® 515E Firewall and Integrated Services Adapter (ISA) protecting the network. I want to protect the servers using CSA. Would I also require antivirus on the servers?*

A: CSA is a host-based intrusion protection system (HIPS), so it does not specifically require other hardware or software components to function. We advocate a defense-in-depth approach, so antivirus does have added value, specifically with cleaning systems that are already infected.

Cisco has a white paper on securing network endpoints without signatures, which can help you to understand where CSA fits compared to these other technologies: cisco.com/packet/164_10a2.

Q: *The CSA starter pack includes VMS Basic, the management console, one server agent, and ten desktop agents. It says that you can add agents to this bundle. Are there any restrictions on the number of agents or any limitations in comparison to buying the components separately?*

A: Once you have the VMS server installed, then you can add more agents without a problem. You might see information linking VMS to the number of supported devices, but this is just for hardware

devices. The CSA licensing is handled per agent, so VMS Basic will work fine. A VMS server with CSA management console (MC) can handle up to 10,000 agents in the current 4.0 release.

Q: *How well do CSA and CiscoWorks VPN/Security Management Solution Management Center (VMS/MC) work in a distributed environment? When rolling this out across the WAN, can I pull down the kits and deploy them to each machine that is using the same profile/policy without pulling them down separately for each machine?*

A: How well CSA and VMS/MC work in a distributed environment is highly dependent on your polling interval and amount of agents across your WAN link. Each poll is small (2K), and once your environment is tuned, the event and policy updates should be infrequent. Because the policy and agent kit updates are the largest items, we will be transferring these over HTTP starting in CSA release 4.5. This method will allow you to cache them at the remote site after the first agent in the group downloaded the update. Your agent kits can be distributed directly, so you don't have to download those from the MC each time.

Q: *I'm curious to know how a client protected by CSA would have responded to receiving an e-mail with the new Mydoom variant if no other protection mechanisms have been installed? I understand and value the concept of defense in depth, but let's assume that there is no other protection and the user unwittingly activates the attachment.*

A: The Mydoom variant would have a new signature compared to the original virus, but the behavior is very similar. CSA with default policies protects against this virus through the following layers of defense: creating the startup registry key; reading from a .WAB file and a .DBX file (e-mail address lists); establishing Simple Mail Transfer Protocol (SMTP) connections; executing downloaded code; creating system files.

Do you have a question about how to increase network security using Cisco Security Agent? Ask the NetPro Expert. Send your question to packet-netpro@cisco.com, with the subject line "Cisco Security Agent." ■



JOSH HUSTON is a technical marketing engineer in Cisco's VPN and Security Business Unit. Formerly an engineer in the Cisco Technical Assistance Center supporting IP contact center products, Huston's current specialty is Cisco Security Agent. He can be reached at johuston@cisco.com.

The matching criteria of the classes are determined by the corresponding ACLs. A “permit” in the ACL indicates that matching traffic *will be* policed if a policing action is configured for that class on the control plane. A “deny” in the ACL indicates that matching traffic *should not* be policed in that class. In the example, ACL 120 is used for the important traffic class where a Telnet session, presumably from an administrative host and sourced from 10.86.183.3, is allowed full access to the RP’s control and management planes. All other hosts on the subnet will be subject to the class policer in ACL 121 while remaining Telnet sessions fall into the default class. The policy is applied using the new control-plane global CLI command.

From the submenus, an administrator can set up a central aggregate control plane policer as shown in the example. If line cards are capable of distributed CoPP, then a keyword can be used to reference the control plane interface on the line card itself. Refer to the Cisco configuration guide at cisco.com/packet/164_4c1 for more specific information on the syntax of the CoPP CLI.

When a packet arrives on an interface it first enforces any service policies configured on the interface, and then a Layer 2 or Layer 3 switching decision is performed. The information retrieved indicates if the packet needs to be punted to the RP or is destined out another interface port. RP packets are directed as input to the control plane interface; all other transit packets are unaffected. The control plane interface performs the necessary packet classification and policing as specified in the input service policy. A packet can be accepted, dropped, or marked as a result of the policer action in the policy.

While the input policies on the control plane interface are an intuitive need, output policies can also be used for those packets originated by the router itself. This feature puts the router in “Silent Mode.” Silent Mode prevents the router from sending a system message when a packet is discarded by CoPP. An example would be a packet destined for a port not currently being listened to by the router, which may occur when reconnaissance probes are received. An output policy on the control plane interface is performed on RP-originated packets prior to any specific interface output policies.

♦ ♦ ♦

CoPP represents a strong step forward in securing the potentially vulnerable router control and management planes, and its extensibility lays the foundation for the development of new IOS features and enhancements in the future as the need for stronger security tools arises. ■

FURTHER READING

- “Locking Down IOS” (*Packet*® First Quarter 2004)
cisco.com/packet/164_4b2
- White paper: “Deploying Control Plane Policing”
cisco.com/packet/164_4b3
- Cisco IOS Software Release 12.2S Feature Guide
cisco.com/packet/164_4b4
- Cisco IOS security information
cisco.com/go/iossecurity



PACKET ADVERTISER INDEX

ADVERTISER	URL	PAGE
ADC - The Broadband Company	www.adc.com/performance	D
AdTran	www.adtran.com/info/wanemulation	2
Aladdin Knowledge Systems	www.eAladdin.com/Cisco	IFC
American Power Conversion (APC)	http://promo.apc.com	F
BellSouth Business	www.bellsouth.com/business/metroethernet	OBC
Boson Software	www.boson.com	A
Cisco Press	www.ciscopress.com	B
eiQ Networks	www.eiqnetworks.com	35
GL Communications	www.gl.com/packet	66
NetScout	www.netscout.com/netflow	40
NIKSUN	www.niksun.com/packet	16
NIKSUN	www.niksun.com/pro	44
OPNET Technologies	www.opnet.com	48
Panduit	www.panduit.com/pp03	IBC
Pulver.com	www.von.com	72
RedSiren	www.redsiren.com/IPC	64
SMARTS	www.smarts.com	62
Solsoft	www.solsoft.com/packet	36
Websense	www.websense.com	28

CACHE FILE

Snippets of Wisdom from Out on the Net

CYBER QUOTE

**"Diamonds are forever.
E-mail comes close."**

—June Kronholz
Correspondent, *The Wall Street Journal*

Internet Is 35 and Only Getting Faster

As the Internet turned 35 in early September, computer scientists claimed a new record for how fast data can be transmitted over computer networks, announcing they had sent the equivalent of a fat DVD movie file from Switzerland to California in a few seconds. Teams of scientists from the California Institute of Technology (Caltech) and CERN, the European particle physics lab in Switzerland, dispatched 859 gigabytes of data in less than 17 minutes across 16,000 kilometers of computer networks—at roughly 6.63 Gbit/s. Thirty-five years ago on September 2, scientists at the University of California Los Angeles linked two computers with a 15-foot cable and tested a new way of swapping data that led to the Internet.

Hit Spam at the Source

CNET News.com reports upcoming antispam technology standards that promise to hit spammers where it hurts the most—their wallets. At issue is the ability to authenticate the original source of e-mail messages, a major hole in the current system that allows spammers to easily forge return addresses. The IETF will fast-track a submission from Microsoft known as "Sender ID." The group reviewed submissions for signature-based authentication from Cisco and Yahoo and recommended the authors combine and resubmit those proposals together.

Net Lingo

Banner blindness—The tendency of people to ignore banner ads on Websites. Contrary to the prevailing marketing philosophy that the larger an item on a Web page, the greater its perceived visual importance and likelihood of attracting attention, researchers found that users had more difficulty finding information when it was located in a banner ad (whatis.com).

Record Growth Spurt for DSL

After three consecutive record-breaking calendar quarters, global DSL subscriptions are entering a high growth phase. According to the DSL Forum, the first quarter of 2004 brought 9.5 million new lines worldwide, nearly doubling the same period in 2003, and bringing the total to 73.4 million DSL subscribers. China topped the global DSL ranking, adding another 2.9 million subscribers in the first quarter of 2004, bringing its total slightly under 14 million. Japan and the US ranked second and third, respectively. While South Korea ranked fourth in terms of subscriber numbers, it was first in achieving 20 percent DSL penetration of phone lines—registering 28.3 percent penetration per 100 lines in the first quarter of 2004.

From Afghanistan to Zimbabwe . . .

ClickZ Stats has compiled its annual list of global online populations. Arranged alphabetically, the findings for each country include overall population, Internet users, active users, and ISPs. Find this online data and more under "Geographics" at clickz.com/stats.

THE 5TH WAVE



"It's another deep space probe from earth, seeking contact from extraterrestrials. I wish they'd just include an e-mail address."

©The 5th Wave, www.the5thwave.com