PACKET®

CISCO SYSTEMS USERS MAGAZINE

SECOND QUARTER 2004

Cisco Systems

cisco.com/packet

PACKET MAGAZINE

DAVID BALL
EDITOR-IN-CHIEF

JERE KING
PUBLISHER

JENNIFER REDOVIAN
MANAGING EDITOR

SUSAN BORTON
SENIOR EDITOR

JOANIE WEXLER
CONTRIBUTING EDITOR

R.J. SMITH
SUNSET CUSTOM PUBLISHING
PRODUCTION MANAGER

MICHELLE GERVAIS, NICOLE MAZZEI
MARK RYAN, NORMA TENNIS
SUNSET CUSTOM PUBLISHING
PRODUCTION

JEFF BRAND
ART DIRECTOR

EMILY BURCH
DESIGNER

ELLEN SOKOLOFF
DIAGRAM ILLUSTRATOR

BILL LITTELL
PRINT PRODUCTION MANAGER

CECELIA GLOVER TAYLOR
CIRCULATION DIRECTOR

SPENCER TOY
COVER PHOTOGRAPH

SPECIAL THANKS TO THE FOLLOWING CONTRIBUTORS: STEVE ANDERSON, GREG BEACH, KAREN DALAL, GRACE HU-MORLEY, JANICE KING, BRIAN MCDONALD, MARCUS PHIPPS, KARYN SCOTT, BILL STEPHENS, LAURA STIFF

ADVERTISING INFORMATION:
Kristen Bergman, 408-525-2542
kbergman@cisco.com
View *Packet* magazine at cisco.com/packet.

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

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

Packet Magazine
PO Box 2080
Skokie, Illinois 60076-9324
USA
Phone: 847-647-2293

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

What's in a Name?

If the name is ip communications, the answer is *lots*. When I first heard the term used to refer to IP telephony service, I must admit, I didn't like it. I thought it was far too broad and generic. After all, isn't e-mail a form of IP communications? As a matter of fact, it is. And so is IP telephony, and video telephony, and conferencing, and voice mail, and unified messaging.

IP communications, it turns out, is a great way to describe the myriad ways in which we can communicate and collaborate over an IP network. IP communications, as a solution from Cisco, not only encompasses the services noted above; it includes contact centers (or, more precisely, Customer Interaction Networks), voice gateways and applications, security solutions, and network management. These applications and services are not only incremental to your existing network investment, but they go a long way in boosting productivity and driving down total cost of ownership. Because of it, IP communications is *transforming* the way businesses communicate, internally and externally.

And that's what we focus on in this issue of *Packet*® (starting on page 30). We share with you real-life, innovative uses of IP telephony; audio and videoconferencing; unified messaging; and other IP communications solutions in several industries, including transportation, manufacturing, government, and education (page 36). Learn how Cisco's new video telephony solution is helping to break down the cost and usage barriers associated with traditional video telephony and conferencing systems (page 45). We also offer ten top tips to help guide a successful IP telephony implementation—gleaned from Cisco's own IP telephony deployment and lessons learned such as the importance of understanding your users' expectations and requirements (page 48).

Integral to many of these IP communications services and applications is the Cisco IP Phone. In fact, Cisco IP phones are displacing approximately 5000 circuit-based, traditional phones each business day, up from 2000 per business day a year ago. While the productivity gains associated with IP phones' simple adds, moves, and changes are substantial, the real business value is being realized by those companies that integrate their business processes with their new communications infrastructure and tap into exciting applications that make the network work for them.

Many Cisco partners are developing easy-to-use applications based on open standards such as Extensible Markup Language (XML), which demonstrate the power of Cisco IP phones to solve business problems, streamline business communications, and bolster employee productivity and customer satisfaction (see page 41).

As business-wise and increasingly popular as IP-based communications are, they do not diminish the value of communicating face to face—which is exactly how we hope to speak with you at this year's US Networkers conference in New Orleans, Louisiana (July 11 through 16). Come "Meet the Editors" at the *Packet* booth in the World of Solutions. Talk to us about your job, the network challenges you've overcome, and IP communications or other innovative applications or services you've recently deployed. We're especially interested to hear how your company or organization is leveraging network technology to compete or change the rules in your respective industry.

We want to hear from you. Because when it comes to the pages of *Packet*, your voice is our greatest asset.

David A. Ball

Editor-in-Chief
Packet
daball@cisco.com

Mail ✉

Tech Tips Top His List

The First Quarter 2004 issue of *Packet*® was excellent with its coverage of security, IOS®, high availability, etc. I read with particular interest of the AutoSecure feature in Cisco IOS Software Release 12.3 Mainline. But all the information is very helpful to us because we're installing a Cisco infrastructure at our facilities. I am familiar with Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) but was not familiar with Gateway Load Balancing Protocol (GLBP) until now. The article on GLBP written by Rick Williams, "High Availability for Campus Networks," is especially useful to me. I probably will be able to use GLBP for my dual-connected remote sites to do load sharing. I also liked the security best practices section of the article "Proactive Protection." Last year the NetFlow feature on the routers helped me to track down most talking devices and shut them down to prevent Slammer attacks. I also liked the other security articles on wireless and self-defending networks. But most of all, I like your "Tech Tips & Training" section. Please continue to provide technical tips so *Packet* readers can broaden their knowledge and skills.

—Raj Lotwala, New York City Department of Correction, New York, USA

Tracking Down Top Talkers

Affan Basalamah presented a very interesting Reader Tip [First Quarter 2004] on how to track down "top talkers" on a fully meshed network using **alias** commands to speed up the process. While the discussion of aliases is very useful, the tip never addressed the real problem in this situation. Without a network analysis module (NAM) or other tools, how do you find the IP address of the top talker in the first place? I believe this is of far more value in a real-world situation, and is the first step in solving a customer's complaint that "the network is slow."

—Blue Beckham, APS, Phoenix, Arizona, USA

The following is a response by Cisco Technical Support Engineer Phillip Remaker.—Editors

The tip is how to locate the port where an IP address lives once you identify the IP address. We assume you found a suspicious IP address by other means. Using the Cisco Intrusion Detection System (IDS) product line is an excellent way to find devices with anomalous behavior. You can also use NetFlow and NetFlow statistics on routers to find top talkers.

Point of Confusion

In the article "Is It Time to Converge? [Fourth Quarter 2003], I am confused on two points. First, I think adding the TE acronym to MPLS (MPLS-TE) is misleading. Multiprotocol Label Switching (MPLS) was designed for traffic engineering in the first place. It is true that MPLS uses RSVP-TE for the purposes of traffic engineering, but not in every case, because in some situations Lightweight Directory Protocol (LDP) is also used (although using LDP is not a good idea for obvious reasons). I am interested in your comments on this.

Second, the article refers to EXP bits in the shim header, but there are no EXP bits. I think that these are referred to as COS bits instead of EXP bits, which again creates confusion because the EXP bits terminology, though used in the past, is now deprecated.

—Noman Bari, CTTC PVT. Ltd., Karachi, Pakistan

The following is a response by author Santiago Alvarez.—Editors

Regarding the first point, MPLS does not imply traffic engineering. Large MPLS deployments worldwide don't make use of MPLS-TE. Because TE techniques are applied at different levels (for example, TDM, SDH, ATM, etc.), MPLS acts as a qualifier that defines the context under which TE is being discussed. Regarding the second point, my notation is consistent with RFC 3032 (www.faqs.org/rfcs/rfc3032.html) and industrywide use.

CORRECTION

The article "A Winning Game Plan" [First Quarter 2004, page 33] inaccurately stated that storage-area networks are often located offsite. In fact, storage-area networks are typically located in the data center. We apologize for the error. —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.

User Connection

Attend Networkers 365 Days a Year

At Networkers Online, you can experience nearly everything you would if you attended a Cisco Networkers users conference in person, with the exception of the World of Solutions and Customer Appreciation event. Watch and listen to every technical session and keynote address, see Cisco Chief Executive Officer John Chambers demo the hottest technology, and interact with other technical experts—all in the comfort of your home or office.

Networkers Online gives you a few extras, too:

- Monthly live, interactive Webcasts of current topics that meet Networkers' high standards and allow you to ask questions and get answers from Cisco experts during the session
- Direct links to the Cisco Networking Professionals (NetPro) community where you can join other technical experts and discuss today's networking challenges and solutions
- Detailed abstracts and PDF versions of the Networkers presentations, plus white papers and other documents

Credit Toward the Conference

Through July 2004, site content is from the US 2003 Networkers events in Orlando and Los Angeles. If you attended either of those conferences, access the online site today. If you plan to attend Networkers 2004 in New Orleans, you can still subscribe to Networkers Online 2003 for US$150 and receive a $150 credit toward your registration. Early registration for the 2004 conference also gives you immediate access to Networkers Online 2004, where you can complete all your introductory sessions online before the conference. In August, Networkers Online 2004 will offer the entire conference content at no charge to conference attendees.

VIRTUAL EDUCATION: It's easy to learn any time of day—or night—by accessing technical sessions, interactive Webcasts, demos, and discussion forums—all available at Networkers Online.

Equal Opportunity Education

Access to Networkers Online 2004 will be available by subscription in August 2004 to those who who do not attend the conference.

"We wanted to find a way to make the unique experience of Networkers available 12 months a year," says Pat Reardon, manager of Cisco online event marketing. "We also wanted to give industry professionals who are not able to attend Networkers in person an equal opportunity to learn the latest technology that will help their companies and advance their careers."

Subscribe Today

One good reason to subscribe to Networkers Online is to start taking courses now in preparation for the New Orleans conference, according to Reardon. Visit Networkers Online at cisco.com/packet/162_3b1. To learn more about worldwide Networkers users conferences or to register, visit cisco.com/go/networkers. ▲▲

Cisco Worldwide Events

May 10–14	Networld+Interop	Las Vegas, Nevada, USA
June 15–18	Cable-Tec Expo	Orlando, Florida, USA
June 20–24	SUPERCOMM 2004	Chicago, Illinois, USA
July 11–16	Networkers New Orleans	New Orleans, Louisiana, USA
September 5–10	Cisco Powered Network Operations Symposium	Paris, France
October 9–13	USTA Telecom 2004	Las Vegas, Nevada, USA
November 4–6	Networkers China	Beijing, China
November 16–19	Networkers Mexico	Mexico City, Mexico
December 13–16	Networkers EMEA	Cannes, France
March 8–10, 2005	Networkers Korea	Seoul, Korea

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

Cisco Certifications Among Top in Industry

CISCO CAREER CERTIFICATIONS were rated highly for “best supporting materials” and “best specialty certifications,” among other categories, by *Certification Magazine* in its recent lists of leading industry certifications.

Cisco certifications were mentioned first in five of eight categories and were named in an additional category in the magazine’s November 2003 issue.

Certification programs from companies such as Apple Computer, Hewlett Packard, IBM, Microsoft, Novell, Oracle, Red Hat, and Sun Microsystems, as well as various national engineering associations, were included in the article.

To read the *Certification Magazine* article in its entirety, visit www.certmag.com/top10list. To learn more about Cisco Career Certifications, visit cisco.com/certifications. ▲▲

Certification	Category	Category Description
CCIE® Certification and Cisco Associate, Professional, and Specialist certifications	Best Hands-On Programs	Require applicants to demonstrate real-world skills and knowledge.
CCIE Certification	Most Technically Advanced Programs	Consist of extremely high volumes of material or long lists of prerequisites.
Cisco Career Certifications	Best Supporting Materials	Have third-party support or provide superior training materials.
CCNA® Certification	Best Entry-Level Certifications	Represent the first step on the certification ladder.
Cisco Specialist Certifications	Best Specialty Certifications	Allow focused study of narrowly defined topics.
Cisco Career Certifications	Toughest Recertification Requirements	Entail renewal, repeated exams, or continued training.

Source: *Certification Magazine*

Find a Service Provider That Meets Your Needs for Managing VPNs, Security, and More

As businesses incorporate advanced and emerging technology services—such as virtual private networks (VPNs), metro Ethernet, network security, and voice over IP (VoIP)—into their business operations, outsourcing these functions to experts becomes more attractive.

"Companies want to focus on their core competencies, plus the increasing complexity of communications makes network services a great candidate for outsourcing," says Kirt Jorgenson, director of service provider strategic marketing programs at Cisco. "Selecting a provider can be difficult, however, and businesses want some assurances that their providers will meet their business *and* technical needs."

The Cisco Differentiater

The Cisco Powered Network Program—whose service provider members operate networks built end to end with Cisco equipment and meet Cisco support standards—has helped ease the selection process since its inception in 1997. The addition of more stringent technical requirements for program members will soon make this standard even more important to businesses.

"When companies see the Cisco Powered Network mark now, they view it as a sign of superior service," Jorgenson says. He cites a recent survey that showed more than 70 percent of enterprise companies are more likely to purchase a service if it is provided over a network built end to end with Cisco equipment. According to Jorgenson, business leaders know that when the company and its provider use the same vendor's equipment, interoperability problems are less likely to arise, the service will be more reliable, and problems are likely to be resolved more quickly.

Enhanced Technical Requirements

"Technical leaders have been sharing with Cisco their business requirements for outsourcing network services," Jorgenson continues. "It's clear they are more likely to ask a service provider to manage their mission-critical traffic when they know they can count on reliable performance."

Cisco is responding by enhancing the technical requirements within the Cisco Powered Network service designations. For example, in the future, when a service provider brands its IP VPN Multiservice offering with this designation, the provider will have met network performance metrics related to delay and jitter—and will confirm they are maintaining these levels of service as part of annual assessments.

Service Provider Benefits

Service providers will benefit as well when the Cisco Powered Network service designations evolve to better meet their enterprise customers' needs.

"Enhanced requirements will help our carrier partners set themselves even further apart from their competition," observes Jorgenson.

Some of the advanced technology designations available from Cisco include public wireless LAN, metro Ethernet, IP VPN, IP business voice, and managed firewall/intrusion detection systems (IDS).

To find a member of the Cisco Powered Network Program to manage your network services, visit cisco.com/go/cpn. ▲▲

RECENTLY ANNOUNCED CISCO ACQUISITIONS

Acquired	Key Technology	Employees	Location
Riverhead Networks	Security technology that protects against distributed denial-of-service (DDOS) attacks and other threats to enterprise and service provider networks. Riverhead's technology can quickly and accurately mitigate a broad range of known and previously unseen security attacks, and it complements the Cisco Intrusion Detection System (IDS) solution by cleaning malicious packets while allowing legitimate packets to proceed to their destination. Riverhead's business will become part of Cisco's Internet Switching Business Unit.	44	Cupertino, California, USA
Twingo Systems	Desktop security solutions for Secure Sockets Layer (SSL)-based virtual private networks (VPNs). Twingo's technology helps deliver consistent application access to endpoint devices during SSL VPN sessions, and helps eliminate sensitive data on computers after sessions end. Cisco will use Twingo's technology to bring the same quality of endpoint security available with IPSec VPNs to SSL VPN deployments. Twingo's Virtual Secure Desktop software will be integrated into the Cisco VPN 3000 Series Concentrator. Its employees will join the Cisco VPN and Security Business Unit.	4	Mountain View, California, USA

Tech Tips & Training

Static and Policy Routing Enhancements

Common Scenarios and Configurations

BY SHYAN WIGNARAJAH AND ASAD FARUQUI

ONE PROBLEM WITH STATIC routing and policy routing has been the inability for the router to determine the state of the next hop. Routing protocols typically use "hello" mechanisms to determine if a neighbor is alive. However, policy and static routing offer no means to test whether the next hop is reachable. As a result, statically routed or policy routed packets risk being "black holed"—that unfortunate state of being forwarded to a dead neighbor.

Scenario 1: Static Routing

In scenario 1, the remote network has multiple paths to reach the Internet.

The preferred path is via the primary Internet service provider (ISP). The cable-connected ISP provides flat rate service and higher bandwidth than the ISDN-connected ISP (which could bill on a per minute basis). However, if the primary ISP connection should fail, then the secondary ISP would be used.

So how does the CPE router determine when to use the primary ISP and when to use the secondary ISP? The Ethernet interface on the CPE router will remain up as long as it's plugged into the modem. However, there could be a problem with the cable cloud or some other part of the primary ISP's network. In order to detect these problems, the CPE router can't simply rely on the state of its own interface.

You could enable a dynamic routing protocol; however, this isn't always a viable solution, as the ISP may not be willing to run a routing protocol with you. Conversely, some customers may not want to run a routing protocol with their ISP.

Enhancement to Static Routing

An alternative solution is an enhancement to static routing that will enable the CPE router to check the primary ISP's path by forcing test probes out via the interface to the primary ISP. This is achieved with policy routing. If the test probe is successful, the CPE router will install a default route into its routing table to reach the Internet via the primary ISP. If the test probe fails, the CPE will remove the primary default route, and a floating secondary route will be installed to reach the Internet via the secondary ISP.

STATIC ROUTING

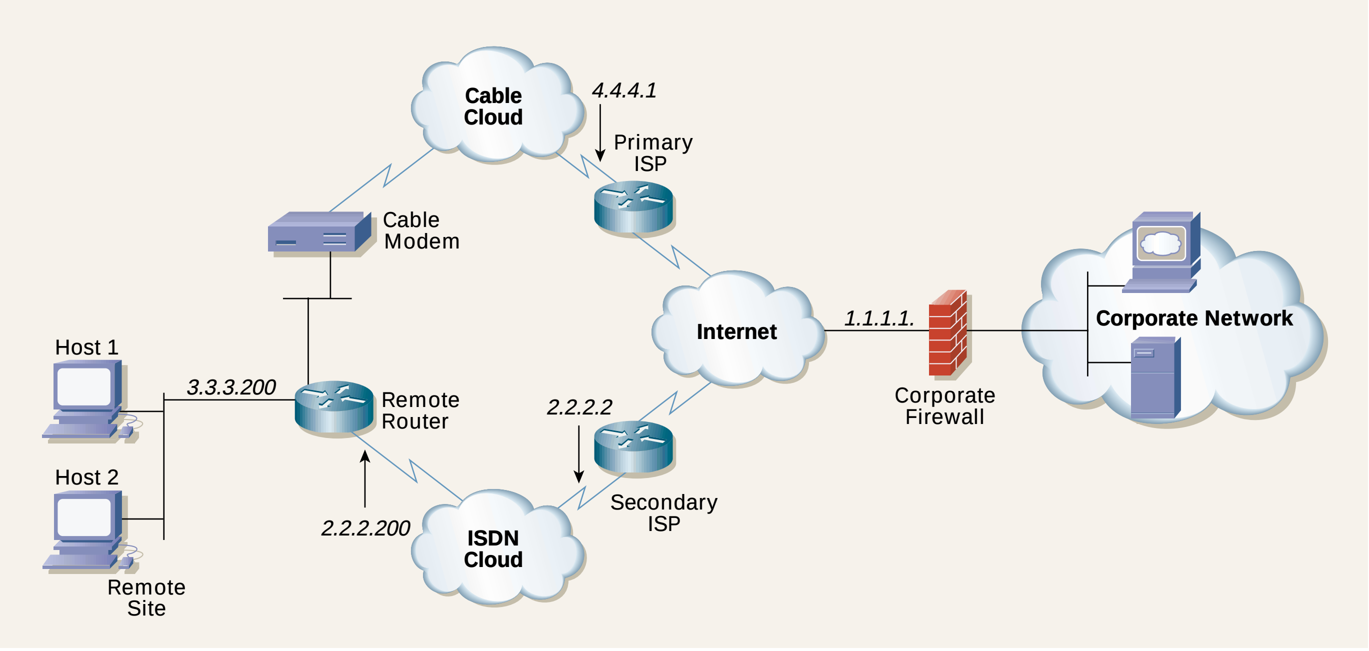


FIGURE 1: In a static routing scenario, the remote network has multiple paths to reach the Internet.

SAA probes are used to test for connectivity. Since the purpose of the probes is to test the primary path, the probes are never sent via the secondary path. If they were, the test might falsely succeed, even though the primary path is not working. To achieve this, local policy routing is used so that the SAA probes are only forwarded out the primary interface. If the primary interface is in a DOWN state, the probes are discarded (forwarded to the null interface).

Tracked objects is a generic mechanism in Cisco IOS® Software used to monitor items of interest, and notify applications if the item changes state. Tracked objects provide a loosely coupled set of building blocks that applications such as static routing or policy routing can use to build on. In this case, a tracked object is created to monitor the state of the SAA probe. Then a static route is configured and associated with the tracked object. Static routing only refers to the tracked object and the tracked object refers to the SAA probe.

If the tracked object is UP (meaning the SAA probe succeeded), the route is installed in the routing table. Traffic to the Internet will go via the primary ISP. If the tracked object is DOWN (meaning the SAA probe failed), then the route is removed from the routing table, and a floating backup route is installed into the routing table that allows traffic to reach the Internet via the secondary ISP.

Instead of the static route directly monitoring the SAA probe, it monitors the probe via the tracked object. This might seem complex from a configuration standpoint, but it's more efficient from a code development standpoint. If ten applications are all interested in monitoring two types of items, each application would have to create new functions to do it (10 applications x 2 items = 20 new functions). Using track objects, the same scenario would require a new function for each of the two tracked objects, and 10 new functions to monitor the tracked objects (10 new functions to monitor the tracked objects + 2 new functions for the tracked objects to monitor the items = 12 new functions).

Sample Configuration #1: Primary link's address is learned via DHCP

The initial configuration of the CPE router is as follows:

```
interface Ethernet0/0
 description primary link
 ip address dhcp

interface Ethernet0/1
 description remote LAN
 ip address 3.3.3.200 255.255.255.0

interface BRI1/0
 description backup link - physical
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type basic-5ess
 ppp multilink
!
interface Dialer1
 description backup link - logical
 ip address 2.2.2.200 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 20
 dialer string 384000
 dialer load-threshold 20 outbound
 dialer-group 1
 ppp multilink

dialer-list 1 protocol ip permit
```

The rest of the configuration is built in the following steps.

Step 1: A "favorite" address is chosen, and an SAA (RTR) probe is configured to ping the favorite address. In this case, the outside address of the corporate firewall is a good choice to ping. For this example, the corporate firewall's public address is 1.1.1.1.

```
rtr 1
type echo protocol ipIcmpEcho 1.1.1.1
-> define rtr probe to ping 1.1.1.1
rtr schedule 1 start-time now life forever
-> probe should run forever
```

Step 2: Policy route the RTR probe's packets so they only go out the primary interface.

```
access-list 101 permit icmp any host 1.1.1.1 echo
-> define ACL to only match rtr probe's packets

ip local policy route-map MY_LOCAL_POLICY
-> define policy routing for router originated packets.

This doesn't affect packets being switched through the router.

route-map MY_LOCAL_POLICY permit 10
 match ip address 101
 -> match only the pings used by tracked objects
 set ip next-hop dynamic dhcp
 -> set the next hop to the gateway learned via dhcp
 set interface null0

-> discard the packet if the dhcp next-hop is unknown.
```

Step 3: Create a tracked object and associate the object with the SAA probe, which was previously configured.

```
track 123 rtr 1 reachability -> creates track object# 123 to
monitor service assurance agent# 1
```

Step 4: Associate the default route via the primary link with the tracked object.

```
interface Ethernet0/0
 description primary link
 ip dhcp client route track 123
 -> dhcp installed default route will be associated with
track object

#123.
 ip address dhcp
 -> enable dhcp on the interface
```

Step 5: Configure a floating static route via the secondary ISP. The administrative distance of the primary route must be lower than the administrative distance of the secondary route.

```
ip dhcp-client default-router distance 1
-> dhcp installed route will have a distance of 1
ip route 0.0.0.0 0.0.0.0 2.2.2.2 254
-> secondary route will have a distance of 254
```

Step 6: Verify proper operation by displaying the routing table and other related items.

```
show ip route -> display the routing table

Gateway of last resort is 4.4.4.1 to network 0.0.0.0
-> gateway of last resort is primary ISP
2.0.0.0/24 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, Dialer1
     3.0.0.0/24 is subnetted, 1 subnets
C       3.3.3.0 is directly connected, Ethernet0/1
     4.0.0.0/24 is subnetted, 1 subnets
C       4.4.4.0 is directly connected, Ethernet0/0
S*   0.0.0.0/0 [1/0] via 4.4.4.1

show ip route track-table -> display routes which are associ-
ated with a tracked object.

ip route 0.0.0.0 0.0.0.0 4.4.4.1 track 123 state is [up]

show track -> display the state of tracked objects and what
clients are tracking them

Track 123
  Response Time Reporter 1 reachability
  Reachability is Up
  -> object is reachable
    5 changes, last change 00:09:07
  Latest operation return code: OK
  Latest RTT (millisecs) 1
  Tracked by:
    STATIC-IP-ROUTING 0
    -> static routing is monitoring this object
```

SHYAN WIGNARAJAH CCIE®, is a software engineer for the Core IP Routing Group at Cisco. He can be reached at dwignara@cisco.com
ASAD FARUQUI CCNP, CCNA, is a software engineer for the Core IP Routing Group at Cisco. He can be reached at afaruqui@cisco.com

```
show route-map -> displays the route-map (which is used by
local policy routing)

route-map MY_LOCAL_POLICY, permit, sequence 10
  Match clauses:
    ip address (access-lists): 101
  Set clauses:
    interface Null0
    ip next-hop dynamic dhcp - current value is 4.4.4.1
    -> dhcp learned next hop
  Policy routing matches: 2265 packets, 144960 bytes
```

If there is a problem reaching 1.1.1.1 via the primary ISP, the tracked object will transition to the DOWN state, the default route will be removed, and the backup path will be used. The above commands will display the following in this situation:

```
show ip route -> display the routing table

Gateway of last resort is 2.2.2.2 to network 0.0.0.0
-> gateway of last resort is secondary ISP

     2.0.0.0/24 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, Dialer1
     3.0.0.0/24 is subnetted, 1 subnets
C       3.3.3.0 is directly connected, Ethernet0/1
     4.0.0.0/24 is subnetted, 1 subnets
C       4.4.4.0 is directly connected, Ethernet0/0
S*   0.0.0.0/0 [254/0] via 2.2.2.2

show ip route track-table -> display routes which are associ-
ated with a tracked object.

 ip route 0.0.0.0 0.0.0.0 4.4.4.1 track 123 state is [down]
 -> object's state is down

show track -> display the state of tracked objects and what
clients are tracking them

Track 123
  Response Time Reporter 1 reachability
  Reachability is Down
  -> object is not reachable
    8 changes, last change 00:04:56
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
```

Sample Configuration #2:
Primary link's address is learned statically configured

This example is similar to the previous one, except there is no DHCP and all the addresses are known in advance. The initial configuration of the CPE router is as follows:

```
interface Ethernet0/0
```

```
 description primary link
 ip address 4.4.4.200 255.0.0.0

interface Ethernet0/1
 description remote LAN
 ip address 3.3.3.200 255.0.0.0

interface BRI1/0
 description backup link - physical
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type basic-5ess
 ppp multilink
!
interface Dialer1
 description backup link - logical
 ip address 2.2.2.200 255.0.0.0
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 20
 dialer string 384000
 dialer load-threshold 20 outbound
 dialer-group 1
 ppp multilink
dialer-list 1 protocol ip permit
```

The rest of the configuration will be built in the following steps.

Step 1: A “favorite” address is chosen, and an SAA (RTR) probe is configured to ping the favorite address. In this case, the outside address of the corporate firewall is a good choice to ping. For this example, the corporate firewall’s public address is 1.1.1.1.

```
rtr 1
  type echo protocol ipIcmpEcho 1.1.1.1
  -> define rtr probe to ping 1.1.1.1
rtr schedule 1 start-time now life forever
  -> probe should run forever
```

Step 2: Policy route the RTR probe’s packets so they only go out the primary interface.

```
access-list 101 permit icmp any host 1.1.1.1 echo
-> define ACL to only match rtr probe’s packets

ip local policy route-map MY_LOCAL_POLICY
-> define policy routing for router packets. This doesn’t
   affect packets being switched through the router.

route-map MY_LOCAL_POLICY permit 10
 match ip address 101
 ->
```

Continued on page 88

The Penalty Box

Cisco QoS features solve bandwidth problems by penalizing network abusers.

MOST UNIVERSITIES TODAY offer LAN and Internet services to their students, faculty, and staff. But high bandwidth usage from the rising recreational use of bandwidth-hogging peer-to-peer applications such as Napster and Gnutella, coupled with an increase in online administrative functions, such as curriculum development and document management, are putting an increasingly heavy technical burden on university networks.

Lehigh University (lehigh.edu), in Bethlehem, Pennsylvania, tackled its bandwidth problem by successfully controlling the Internet usage of its on-campus students through the use of quality of service (QoS) features in Cisco switches and routers. Lehigh recently upgraded its network to 150 Cisco Catalyst® 3550 Series switches in all of its on-campus residences for the QoS features to control its network's usage.

Lehigh uses the per-port rate-limit features of the Catalyst 3550 Series to control 50-Mbit/s Internet bandwidth and 100 Mbit/s of Internet2 bandwidth. If students use excessive amounts of off-campus bandwidth, their ports are rate-limited for off-campus traffic until their usage returns to acceptable levels.

"This is what we call the 'Penalty Box,'"says Mark Miller, lead network engineer at Lehigh. "Basically, students can run whatever applications they want, but not too much of them. It's a fair system, because it only penalizes the users using excessive amounts of bandwidth while letting others run at full speed."

How It Works

Lehigh gathers information from the switches and routers using custom Simple Network Management Protocol (SNMP) programs that are locally written in Perl.

These Perl/SNMP programs constantly track all Address Resolution Protocol (ARP) information from Lehigh's campus Cisco routers, so all IP addresses and the corresponding Ethernet addresses are identified. Other Perl/SNMP programs record and track all the Ethernet address moves and changes from the Cisco Catalyst 3550 Series switches so that the switch port that corresponds to the Ethernet and IP address of each user can be accurately identified.

> "Students can run whatever applications they want, but not too much of them. It's a fair system because it only penalizes the users running excessive bandwidth amounts, while letting others run at full speed."
>
> —MARK MILLER, LEAD NETWORK ENGINEER, LEHIGH UNIVERSITY

NetFlow information from Lehigh's off-campus routers is constantly transferred to a computer running Linux. The NetFlow data is processed hourly using public domain NetFlow processing tools. Off-campus network usage for all campus IP addresses is processed, and the source jack for each flow is identified from the ARP and switch port information. Each jack's usage over the previous 72-hour period is then totaled and jacks that have used more than 2 gigabytes of Internet bandwidth are identified.

These jacks are in violation of the university's usage policy and are added to the Penalty Box. An automated Perl script sets the input and output policy for the switch port corresponding to that jack to rate-limit incoming and outgoing off-campus traffic to 64 Kb. An access list is used so that only off-campus traffic is rate-limited and on-campus traffic can continue at full speed.

The Perl scripts record the port that is rate-limited and the time when the rate-limit was set. When the port's traffic returns to "normal," the rate-limit is removed from the port after a 72-hour penalty delay. "A Web page is also updated so a student can check his or her jack's current status," adds Miller.

Other Perl scripts watch for students who are hard-coding and changing their IP addresses or their Ethernet address (easily done with programs downloaded over the Internet). "We call these users 'cheaters' because they are trying to avoid detection by actively changing their address information. These ports are also rate-limited until this activity stops," says Miller.

Although it might sound complicated, Miller claims the system is relatively simple and very reliable. "It works very well and scales because the limit processing is spread out over all of our Catalyst 3550 switches."

However, even with the penalty box system in place, peer-to-peer traffic can overwhelm off-campus connections at times. This usually occurs when Kazaa is installed and left to run unattended on a PC in an administrative office not currently controlled by the Penalty Box system. When this happens, Lehigh uses Network-Based Application Recognition (NBAR) on its off-campus Cisco 7206 routers to identify and limit the usage of Internet file-sharing applications such as Kazaa and Morpheus. A policy map is used to limit the total of this type of traffic to 5 Mbit/s, allowing it to continue to function but not overwhelm off-campus connections.

Other Switch Features

Lehigh uses several other features of the Cisco Catalyst 3550 Series to control or eliminate common problems on its student network.

Ask your peers and Cisco experts questions or share your own knowledge about QoS in LAN switching and routing at the Cisco Network Professionals Connection "Network Infrastructure" forum: cisco.com/discuss/infrastructure.

Per-port access lists: Each user port has an incoming access list that denies Dynamic Host Control Protocol (DHCP) reply packets. Prior to deploying the Cisco switches, Lehigh had an increasing problem of rogue DHCP servers. According to Miller, the per-port access list feature of the Catalyst 3550 Series has completely eliminated that problem.

Storm control: Each user port is also configured for storm control to limit the rate of broadcast and multicast transmissions. This action limits some types of game playing or possible denial of service (DoS) attacks that can otherwise overwhelm a network.

Port security: Each port is limited in the number of simultaneous Ethernet addresses allowed to control devices such as bridges or wireless access points. This action also reduces security concerns that rely on MAC address flooding.

Management features: Lehigh also uses other features such as Secure Shell (SSH) over a separate management virtual LAN (VLAN), Network Time Protocol (NTP), SNMP, PortFast, and automatic error-disable (errDisable) recovery to make its network as reliable and high performing as possible. “Each switch port is also IEEE 802.1X capable and ready when we are to implement tighter access control into our network,” adds Miller.

◆ ◆ ◆

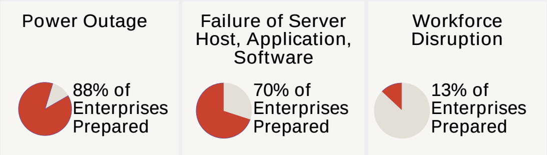
Mark Miller, CCIE® No. 12,409, and lead network engineer at Lehigh University, contributed to this article. He can be reached at mark.miller@lehigh.edu. ▲▲

FURTHER READING

- QoS Scheduling and Queuing on the Cisco Catalyst 3550 Series: cisco.com/packet/162_4b1
- QoS technology information: cisco.com/packet/162_4b2
- Peak Performance with QoS: cisco.com/packet/162_4b3
- LAN Solutions Guide for Higher Education and Universities: cisco.com/packet/162_4b4

Why Should I Care About the Business Ready Teleworker Solution?

A company's ability to continue normal operations in the face of disruption can mean the difference between success and failure. Enterprises that can sustain operations despite unforeseen events have a competitive advantage and, as such, they must provide access to the same information, services, and tools no matter where or when their employees work. Given an uncertain and changing business climate, it is not surprising that 80 percent of enterprises in the US expect to support teleworking employees within the next two years. While many businesses have contingencies for power or server failures, few are prepared for events that block employee access to workplace network resources. *If your employees can't access applications, your business suffers.*



The Cisco Business Ready Teleworker (BRT) solution provides an easy-to-deploy, centrally managed solution that addresses worker requirements for teleworking—while taking into account an enterprise's requirements for reduced operational costs, security, productivity, resilience, and responsiveness.

Key Discussion Points

The four primary considerations for a networked-based teleworker solution are *security, management, authentication,* and *quality of service* (QoS). Any solution that attempts to extend the enterprise network to the teleworker home office must be measured by its ability to deliver these features.

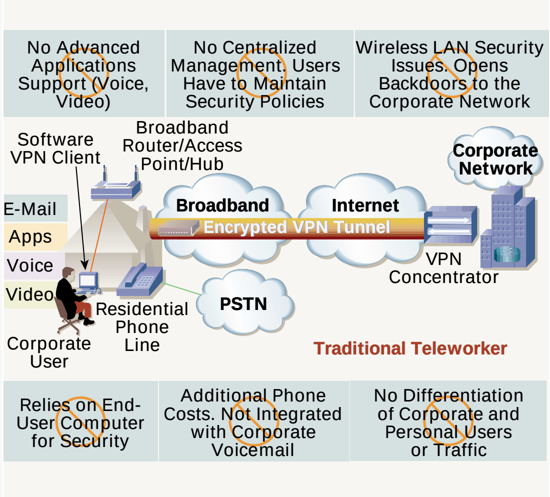
Security	**Management**
• Safeguarding the Corporate Network. • Preventing Unguarded "Back Doors"	• Complexity of Support • Loss of Corporate Control
Authentication	**Quality of Service**
• Who Gets Access to What • Accommodating Personal Use	• Application Availability • Application Behavior

Where Traditional Methods Fall Short

While software VPN clients and "do-it-yourself" hardware-based teleworking options provide teleworker connectivity, they lack QoS for simultaneous delivery of enterprise applications. In addition, security of the system relies heavily on the end user, and IT staff has no way to see, support, or manage the do-it-yourself device.

Reprinted with permission from *Packet*® magazine (Volume 16, No. 2),

BUSINESS READY TELEWORKER
At a Glance
Courtesy of Cisco Enterprise Marketing


No Advanced Applications Support (Voice, Video)

No Centralized Management. Users Have to Maintain Security Policies

Wireless LAN Security Issues. Opens Backdoors to the Corporate Network

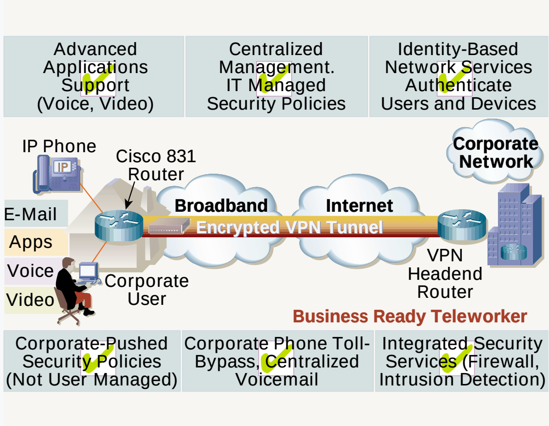
Relies on End-User Computer for Security

Additional Phone Costs. Not Integrated with Corporate Voicemail

No Differentiation of Corporate and Personal Users or Traffic

The Business Ready Teleworker

The Cisco BRT solution differs from other work-at-home or telecommuting scenarios in that it emphasizes providing the same accessibility to applications and services in the home office as those available in the corporate office. With the BRT solution, IT staff can see, support, and manage the teleworker connection using equipment that provides the most comprehensive security and network management available in a teleworking environment running over a standard cable/broadband connection.


Advanced Applications Support (Voice, Video)

Centralized Management. IT Managed Security Policies

Identity-Based Network Services Authenticate Users and Devices

Corporate-Pushed Security Policies (Not User Managed)

Corporate Phone Toll-Bypass, Centralized Voicemail

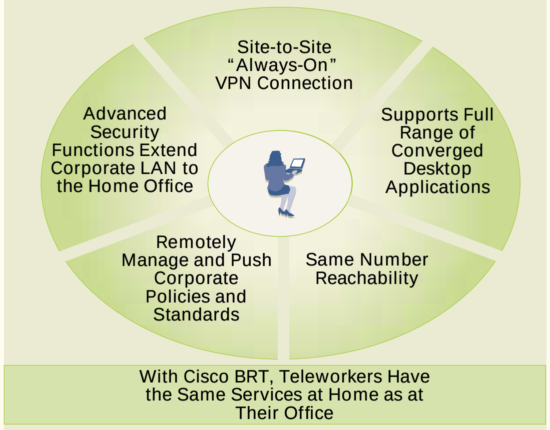
Integrated Security Services (Firewall, Intrusion Detection)

CISCO SYSTEMS

PACKET

The table below compares traditional and BRT teleworking solutions. Only Cisco BRT offers the complete integration of security, manageability, and Cisco QoS that extends all corporate office applications into the home office.

Business Ready Teleworker Makes Full Range of Applications Possible	Occasional Users	Part-Time/Full-Time and Day Extenders
	Unmanaged VPN Client	Enterprise-Class Teleworker
E-Mail	Yes	Yes
Web-Based Applications	Yes	Yes
Mission-Critical Applications	Best Effort	Prioritized
Real-Time Collaboration	Best Effort	Prioritized
Voice Over IP	Best Effort	High Quality
VoD, Cisco, IP/TV®	Unlikely	High Quality
Videoconferencing	Unlikely	High Quality
Remote Configuration and Management	No	Yes
Integrated Security	Basic	Full
Resilience and Availability	No	Yes


Site-to-Site "Always-On" VPN Connection

Supports Full Range of Converged Desktop Applications

Same Number Reachability

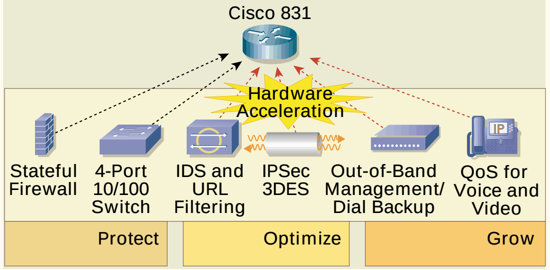
Remotely Manage and Push Corporate Policies and Standards

Advanced Security Functions Extend Corporate LAN to the Home Office

With Cisco BRT, Teleworkers Have the Same Services at Home as at Their Office

Home Office Components

The Cisco 830 Series Router is the backbone of the BRT solution. This Cisco IOS® Software-based access router provides all the features for an always-on, business ready connection in a single, cost-effective platform. Add on an optional IP phone to leverage the benefits of a centralized IP communications system for additional cost savings and productivity.



Reader

Packet® *thanks all of the readers who submitted technical tips this quarter. 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 *Connecting a New Switch to the Network*

When connecting a new switch to your network you can accidentally change your current VLAN database if the new switch has a higher VLAN Trunking Protocol (VTP) revision number. To avoid this, you must clear the VTP revision number on the new switch. The easiest way is to change the VTP domain name to "something_else" and back to "your_VTP_domain" on the new switch. This sets the VTP revision number to 0 and you can connect the switch to the network without any problem. VTP version 3 (just released) has another mechanism for avoiding this problem (see cisco.com/packet/162_4d1).

—Milan Kulík, Aliatel a.s., Prague, Czech Republic

TIP *Adding Comments to Access Lists*

Although I have been to many Cisco classes (including a CCNA® bootcamp) and have been setting up access lists for many years, both on routers and Cisco PIX® firewalls, until recently I had never seen this simple syntax to add a comment to the middle of an access control list (ACL). Instead of using a permit or deny, simply use the *remark* option, for example, access list 1 *remark*. This method works on routers and PIX firewalls. When your file has these comments you can determine exactly what certain sections were originally intended to do, which should make those long ACLs easier to understand in the future.

—Jim Matuska Jr., Nez Perce Tribe Information Systems, Lapwai, Idaho, USA

TIP *Changing the Enable Password on a Remote Router*

While reading a remote configuration tip in the Fourth Quarter 2003 issue of Packet I remembered a tip that I find invaluable for changing the enable password on a remote router. Telnet into the router and log in to enable mode, then Telnet out to another router to Telnet back into the same router again. Change the enable password, exit to global configuration mode, and try to log in to enable mode. If this fails, you can exit from the Telnet session twice until you get back to the same router where you are still in enable mode. This allows you to change the enable password again.

—Phil Burrows, Macquarie Corporate Telecommunications, Sydney, Australia

Editor's Note: This is a good tip, but it is more difficult than it needs to be. A simpler approach is to make two connections from the source machine instead of nesting Telnet sessions.

Maintenance

TIP *Finding Router Interface Information*

I sometimes need to audit a listing of all interfaces on a router or Multiswitch Feature Card (MSFC) for the IP address and description. While there are ways to get either (for example, show ip int brief and sh int desc), I have been looking for a command that enables me to display both types of information at once. To find the exact information that I need quickly, I use the following command:

```
show run | include interface | ip address | description
```

—Robert Yee, CCIE® 11716, J2 Global Communications, Hollywood, California, USA

Editor's Note: For information on the include command and the use of or bars, see the "Alternation" section in the document at cisco.com/packet/162_4d2

Network Management

TIP *Tracking User Logins Using CiscoWorks LMS*

The Campus Manager User Tracking tool in CiscoWorks LAN Management Solution (LMS) allows you to track user names with a login script you place in the Windows Domain Controller:

```
start %WINDIR%\UTLite33.exe -domain %USERDOMAIN% -host
<CW2000-IP-Address>
-port 16236
```

To track user names when users are logged in locally on their Windows workstations, copy the UTLite33.exe file in the Windows directory of your users' PCs and configure their workstations to run this script at startup:

```
start %WINDIR%\UTLite33.exe -domain %USERNAME% -host <CW2000-
IP-Address>
-port 16236
```

The Campus Manager User Tracking report will give you the local user login name and the computer name (username@workstation). This is also an easy way to test the UTLite tool without a domain controller.

—Olivier Muguet, NextiraOne France, Saint Denis, France

Tips

Submit a Tip

Help your fellow IT professionals and show off to your peers by submitting your most ingenious technical tip to packet-editor@cisco.com. Who knows, you may see your name in the next issue of *Packet*. When submitting a tip, please tell us your name, company, city, and country.

Troubleshooting

TIP *Troubleshooting Dial-Peer Configurations*

When troubleshooting dial-peers in a voice over IP (VoIP) environment, you can use the **call simulate** command to simulate calling to a dial-peer's destination pattern (**csim start number**). This command enables you to verify that your dial-peer is configured properly, that there are no hardware problems, and that you are reaching the destination you want (provided that a ringing device is connected to the called port). For example:

```
Router#csim start number <number>

where <number> is the destination pattern of the dial-peer
you are testing.
```

—Jose Gomez, CODETEL, Santiago City, Dominican Republic

TIP *Configuring WAN Links*

When changing or troubleshooting WAN link configuration, you cannot always be certain how remote routers will be affected. Before you make any changes, use the **reload in 60** command. Then if you lose the connection to the remote routers because of a misconfiguration, the router will automatically restore the old configuration after 60 minutes.

—Yang Difei, Nokia Investment Co. Ltd., Beijing, China

Tech Tips

Learn how to use the Cisco TAC Case Collection online support tool. An instructional video on demand (VOD) can help you quickly find solutions to common issues. The Case Collection tool provides support for dial; Frame Relay; IP routing protocols; LAN switching; router and Cisco IOS® Software architecture; network security; voice; and wireless. cisco.com/packet/162_4e1 (requires Cisco.com registration)

Use the Cisco Output Interpreter to get detailed analyses of the output for more than 125 show commands. This VOD explains how to use the Output Interpreter tool to troubleshoot Cisco routers, switches, and Cisco PIX® firewalls running various operating system software, including the Cisco Catalyst® OS, Cisco IOS® Software, Integrated IOS, and PIX OS. cisco.com/packet/162_4e2 (requires Cisco.com registration)

New version of CCIE Security exam available in June 2004. Through written tests and hands-on lab exams, the CCIE® program identifies world-class Cisco experts capable of creating and maintaining highly secure business-ready networks. An updated version of the written Security exam is available beginning June 1, 2004. cisco.com/go/ccie

Explore common causes of slow connectivity in campus switch networks. This technical note addresses the most common issues that may contribute to slow inter-VLAN and intra-VLAN connectivity. Includes classification of common symptoms of slow networks and approaches to problem diagnosis and resolution. cisco.com/packet/162_4e3

Use the Cisco PIX Firewall to handle voice over IP (VoIP) traffic. In this sample configuration, a PIX firewall is configured to allow the traversal of two different VoIP) protocols: H.323, and Session Initiation Protocol (SIP). cisco.com/packet/162_4e4

Find the latest free seminars presented by Cisco experts in cities worldwide. Browse the online Cisco seminar catalog to find free events in your city, as well as streaming media on a variety of topics including security, wireless, IP telephony, and storage solutions. cisco.com/packet/162_4e5

The Promise of PoE

IEEE power standard signals new era for Ethernet.

IEEE 802.3AF, THE WORLD'S FIRST UNIVERSAL power standard, unleashes countless opportunities for organizations to leverage their Ethernet networks in new ways.

Now that a global standard exists for combining Ethernet packets and DC-based power delivery on a common cable, manufacturers of various device types will build 802.3af-compliant power over Ethernet (PoE) support into their products. Surveillance cameras, biomedical equipment, Radio Frequency Identification (RFID) readers, security card readers, and sensor devices are just a sampling of the equipment destined to join Ethernet networks over the next several years.

The basic premise of PoE—also called *inline power*—is fairly well understood. In short, the Ethernet cabling that transports communications packets also supplies the electricity that powers Ethernet-attached devices. This method eliminates one set of cabling to those devices.

PoE is likely to see significant acceptance in the coming years. It is easy to install and manage, it works with existing Ethernet cables, and customers can freely and safely mix legacy and PoE-compatible devices on a network. Managing remote devices is also streamlined with PoE deployments, because once a device is connected to the network, it can be remotely monitored, reconfigured, or reset. And safety is enhanced because power is delivered only to devices that require it. Because no voltage runs on the Ethernet cable until a device that requires the power is connected , the risk of accidental exposure to power on the wire is reduced.

Aside from the simplicity and versatility benefits of Ethernet, customers actually save money by installing and supporting one cabling plant instead of two. An AC power outlet typically costs between US$100 and US$300, and many powered devices, such as video surveillance cameras, will be installed in places where AC power is difficult to deploy. As the number of Ethernet-attached devices grows, eliminating the need for local power for each of hundreds or thousands of end devices significantly reduces deployment costs and greatly simplifies their manageability.

Why Have a Power Standard?

The initial driver for combining Ethernet signals and DC power over a common cable was to support Ethernet-connected IP phones. Shortly thereafter, wireless LANs became popular. By definition, wireless access points often reside in difficult-to-cable locations, such as above ceiling panels, where power outlets are also scarce, so they became especially strong candidates for using PoE.

"It very quickly became clear that power over Ethernet could support a broader range of devices, each with a range of power requirements over the initial innovation that Cisco delivered back in 2000," explains Steven Shalita, senior manager, worldwide product marketing at Cisco. "As a result, PoE was submitted to the IEEE for standardization to allow for broader support for this truly revolutionary technology."

During the standardization process, it became clear that a higher range of power would be required to support the host of new devices that were becoming available. Color telephones were already in development, and people envisioned powering video cameras and other devices over a single Ethernet cable.

When the 802.3af PoE standard was ratified in late 2003, the IEEE body settled on 15.4 Watts as standard output power. This was a significant increase from Cisco's initial implementation, which provided for about 6.5 Watts of power per port. However, it was evident that new devices, such as Cisco dual-radio mode access points, could take advantage of the higher power range made available through the new standard.

Industry's First Gigabit Capability

Cisco, which has offered prestandard PoE for powering IP phones and access points since 2000, recently announced 802.3af-compliant Cisco Catalyst® intelligent switches, line cards, and an IP phone. As a critical requirement for existing customer deployments, all ports on Cisco's new 802.3af-compliant switches also fully support Cisco's prestandard PoE to provide customers with backward compatibility for all existing end devices. Users can plug either a prestandard compatible or 802.3af-compliant PoE device into their Cisco switches, and either will be supported automatically, without preconfiguration.

Along with support for 802.3af, the new Cisco offerings also include the industry's first copper 10/100/1000 gigabit-speed connections with 802.3af-standard power. Gigabit PoE connections are available on the Cisco Catalyst 6500 and 4500 series chassis switches (see Figure 1). Recently, deployments of Gigabit Ethernet to the desktop have increased significantly due to the incremental performance benefits users experience as a result of having higher throughput.

Says Shalita: "It's not necessarily about a single application, but the number of simultaneous applications running on a user's desktop computer. So now customers don't have to choose between high performance or PoE; they can have both along with a future-proof solution that will allow the deployment of higher performance devices without the need to upgrade the LAN port in the future."

New Uses for Ethernet

Many, if not all, network-attached devices require local power for their operation. PoE represents an opportunity not only to provide the connectivity that these devices need, but also to deliver power in a simplified, easy-to-manage environment. IP cameras, point-of-sale terminals, and industrial automation products that take advantage of power delivery have already started to emerge.

But the possibilities don't end there. Imagine being able to charge laptops, integrate security systems, and automate buildings—all over a universal connection: Ethernet. A whole new range of new, easy-to-install devices can be installed wherever an Ethernet cable can be deployed.

Some IP-based 802.3af-capable video cameras are already on the market. While video surveillance networks have been converging onto Ethernet for some time, the advent of PoE will enable simplified deployments and allow for camera placement in locations that were difficult in the past due to the limitations of deploying AC power.

Equipment that is mobile usually communicates to the Ethernet wirelessly, using RFID technology. Tiny RFID tags in mobile devices gather and generate information about the devices in which they are embedded, such as where the device is located at any time. RFID tags communicate to a cabled RFID reader, which collects and displays the information (see "Understanding RFID" on page 83).

IEEE 802.3af-capable RFID readers could connect to an Ethernet switch, enabling a whole new breed of location-tracking information to be transmitted over the corporate Ethernet network.

Exempla Healthcare, a group of hospitals and clinics in Denver, Colorado, for instance, envisions adding both RFID readers and biomedical equipment to its Ethernet network using 802.3af power in its Cisco Catalyst intelligent switches (see sidebar, "Healthcare Facility Sees 802.3af Potential").

Meanwhile, using Cisco PoE has already saved Exempla considerably on its wireless infrastructure costs. Chief Technology Officer Lots Pook estimates that wireless network infrastructure costs alone

FIGURE 1: All new offerings also support Cisco prestandard PoE, so they are backward-compatible with existing Cisco IP phones and wireless access points.

CISCO 802.3AF-COMPLIANT PRODUCTS

Power Source Equipment (PSE)	
Catalyst 6500 Series	■ 10/100/1000, 48-port 802.3af modules (RJ-45) ■ 10/100, 96-port module (RJ-45) with optional 802.3af daughter card ■ 10/100, 48-port 802.3af module (RJ-45 and RJ-21)
Catalyst 4500 Series	■ 10/100/1000, 48-port line card (RJ-45) ■ 10/100, 48-port line card (RJ-45) ■ 10/100, 48-port line card (RJ-21)
Catalyst 3750 Series	■ 10/100, 48-port stackable switch ■ 10/100, 24-port stackable switch
Catalyst 3560 Series	■ 10/100, 48-port fixed-configuration switch ■ 10/100, 24-port fixed-configuration switch
Powered Device (PD)	
7970G IP Phone	Color touchscreen VoIP phone supporting 802.3af and Cisco prestandard PoE

Healthcare Facility Sees 802.3af Potential

Exempla Healthcare in Denver, Colorado, uses Cisco PoE products to power Cisco wireless LAN access points used in a mobile nurse charting application. It also uses Cisco Catalyst intelligent switches to connect and power several hundred Cisco 7960 IP phones.

Exempla's chief technology officer, Lots Pook, anticipates adding intravenous (IV) pumps, digital blood pressure monitors, and fetal heart monitors to the healthcare facility's Ethernet network. Doing so would enable medical staff to remotely monitor the status of a patient's condition and the status of a piece of equipment—as to whether it needs servicing or replenishing, for example—in real time.

In addition, Pook says, he'll likely consider powering RFID readers with his Cisco Catalyst intelligent switches when 802.3af-capable readers become available. Exempla plans to use RFID readers to collect data from beds, wheelchairs, X-ray machines, and other mobile equipment, which will help track the location of this inventory for quick redeployment to other locations when needed.

Among the Exempla facilities are two hospitals in which IT staff use Cisco IP phones powered by Catalyst intelligent switches. A third hospital under construction will use 100 percent voice over IP (VoIP) for telephony, which will require about 1100 handsets that all will use Cisco Catalyst-supplied PoE, says Pook.

dropped 12 percent at one hospital and 22 percent at another, compared with an original budget that called for installing AC power outlets for Cisco wireless access points throughout the facilities.

"With 802.3af available in Cisco equipment, we're now positioned to take advantage of new technologies over the next five to seven years," Pook says.

A Brief Power Tutorial

Historically, there have been different power currents and connectors all over the world. Now 802.3af PoE delivers a universal voltage (48 Volts DC), and plug (RJ-45), simplifying the manufacture and deployment of standards-based devices worldwide.

In an IEEE 802.3af environment, power of up to 15.4 Watts is available at the power source equipment (PSE) or LAN switch port. The powered device (PD) uses this power for its operation. PSE is IEEE terminology for the equipment providing power (such as ports in the Cisco Catalyst intelligent switches). PD refers to the end device or equipment that uses the power (such as IP phones).

Deployments that use PoE require additional consideration for installation and configuration over standard data-only environments. With PoE, power is delivered to attached network devices, and the additional power needs to come from the wall power outlet and through the LAN switch. So in addition to having enough capacity and power to run the switch itself, adequate power must be provided to support the aggregate requirements of the powered devices.

While the 802.3af standard calls for up to 15.4 Watts of power per port, many of the PDs connected to the network will not require the full power levels, so network managers must consider how to manage a budget of available power in the LAN switch. This becomes especially important for large-scale deployments where the amount of power required can quickly add up to thousands of Watts. To address this issue, the IEEE 802.3af standard includes an optional feature called *Power Classification*, to help network implementers better manage the power budget or power allocation available to attached devices.

Power Classification, which is supported in all Cisco Catalyst 802.3af PoE products, is critical because many PDs will not require the full 15.4 Watts of power available with 802.3af PoE. Being able to classify PDs helps to minimize building over capacity in the PSE and ultimately extends the number of PDs supported.

	PSE Output	
Class	**Maximum (Watts)**	**PD Input (Watts)**
0 (default—no classification detected)	15.4	.44 - 12.95
1	4	.44 - 3.84
2	7	3.84 - 6.49
3	15.4	6.49 - 15.4
4	Future Use	Future Use

Although all that power seemingly generates more heat, additional heat in the wiring closet is typically not a significant concern, according to Shalita.

"The bulk of the heat is actually dissipated where consumption of the power takes place, such as at the IP telephone on a person's desk," says Shalita, "so PoE doesn't usually require changes to cooling systems in wiring closets."

Calculate power supply requirements for PoE configurations with the Cisco Power Calculator. The results show output current, output power, and system heat dissipation. For more information, visit http://tools.cisco.com/cpc/launch.jsp (requires Cisco.com login).

For delivering power, the IEEE 802.3af standard allows for using the spare pairs of unused wire typically available with 10/100-Mbit/s connections. However, if unused pairs are not available, such as with 10/100/1000 over copper, which uses all four data pairs, it is possible to deliver (or “float”) power over the same cable pair as Ethernet. The standard specifies that PSE can choose to implement either method of power insertion, while the PD must support both options to maintain interoperability.

Intelligent Power Management

Cisco Catalyst switches offer a range of intelligent power management capabilities that give network managers a high degree of granular control and optimization of power delivery. Intelligent power management allows enterprises to manage their power budgets efficiently. Each switch has an overall power budget or maximum amount of power that it can supply to devices connected to it. This budget is based upon the capacity of the switch’s power supplies and available wall power. A typical chassis LAN switch needs between 400 and 800 Watts to run; to support PoE, however, it could quickly require thousands of Watts of additional power.

While the IEEE power classification feature is important, it is sometimes not granular enough to maximize power allocation for a wide range of power requirements for PDs. Cisco takes the IEEE classification capability a step further by allowing for the identification of the precise power requirements of an attached device. So instead of being identified as one of three classes as defined by 802.3af, a device has the option to precisely identify its power requirements.

To deliver this capability, Cisco Catalyst intelligent switches use the *Cisco Discovery Protocol* to identify devices that connect to the switch. End devices tell the switch how much power they require. If a device’s requirements fall between 802.3af Class 2 and Class 3, requiring 9 Watts of power, for example, the device can request exactly that much. Cisco Discovery Protocol is built into Cisco switch ports and PDs and is also licensed to makers of devices that might connect to a Catalyst switch.

“It is very efficient for a PD to communicate to the switch how much power it actually requires, so that the PSE doesn’t reserve surplus power and unnecessarily drain the available power pool,” observes Shalita.

As deployments of PoE become larger, it will make sense for IT managers to purposely “oversubscribe power,” similar to how bandwidth is managed today, to extend power capacity and the ability to support a higher number of powered devices. For example, when devices such as IP phones are sitting idle on the desktop, they might require just 3 Watts instead of 6, which is needed for ringing or speaker-phone use. So network administrators can assume that only a certain number of devices would be in use at any given time and account for that when managing the available power budget.

In addition, IT managers can predefine power limits. For example, they could configure switches such that a particular port or set of ports is not allowed to support high-power devices. Cisco PSEs can also override the IEEE classification—so that no matter what is plugged into a given port, the port can have a maximum amount of predefined power it is allowed to deliver, thereby preventing unexpected power consumption from unexpected devices being connected to the network.

Finally, Cisco Catalyst switches can prioritize power delivery on ports. Network managers can configure certain ports to always receive power, for example, in the case of an event during which a switch runs out of power and starts shutting down devices to conserve power. Rather than completely shutting down or randomly removing port from ports, Cisco PSEs enable network managers to specify which devices should remain powered.

Cisco is unique in its support for IEEE 802.3af across its family of Catalyst intelligent switches, which includes modular, stackable, and fixed-configuration devices. PoE-enabled products from Cisco are also all part of a unified product portfolio with full intelligent switching functionality, allowing customers to take advantage of all of the intelligence they are accustomed to in Cisco switches, plus added PoE functionality.

The architectural design of Cisco Catalyst PoE-enabled products is unique in enabling high-density customer deployments of up to 48 ports using fixed and stackable products and up to hundreds of devices in a single chassis deployment. In addition to the ability of the chassis to support a high density of powered devices, Cisco introduced a new 96-port 10/100 module for the Catalyst 6500 Series that enables even higher densities per slot. ▲▲

FURTHER READING

- **Cisco Power over Ethernet: cisco.com/go/poe**
- **Power over Ethernet Business Case: cisco.com/packet/162_5a1**
- **IEEE 802.3af resources: ieee802.org/3/af/**

A Case for VPLS

Virtual Private LAN Service is emerging as an alternative multipoint Ethernet technology.

BY SANTIAGO ALVAREZ

ETHERNET IS THE TECHNOLOGY OF choice for LANs due to its relative low cost and simplicity compared to alternative technologies. Ethernet has also gained recent popularity as a metropolitan-area network (MAN) technology, taking advantage of the large fiber deployments in metro areas. Now, *Virtual Private LAN Service (VPLS)* helps extend the reach of Ethernet further to enable it as a WAN technology. Other technologies also enable Ethernet across the WAN—for example, Ethernet over Multiprotocol Label Switching (MPLS), Ethernet over SONET/SDH, Ethernet bridging over ATM, and ATM LAN Emulation (LANE)—however, they only provide point-to-point connectivity; their mass deployment is limited by high levels of complexity, or they require dedicated network architectures that do not facilitate network convergence.

The enterprise WAN is experiencing significant changes, which are driving the development of VPLS technology. Frame Relay and ATM have prevailed for many years as the technologies of choice for packet networks, and enterprises have commonly designed their WAN connectivity with hub-and-spoke or partial-mesh topologies. These designs have been the result of how applications make use of the network infrastructure along with the price characteristics and point-to-point nature of Frame Relay and ATM. A new generation of enterprise applications has created the need for an enterprise WAN architecture that can offer more flexible topologies and higher bandwidth capacity. Recently, service providers have resorted to private IP offerings based on MPLS Layer 3 virtual private network (VPN) to respond to these new requirements. Meanwhile, VPLS has been proposed by the industry as an additional alternative to implement high-bandwidth multipoint services across the WAN based on Ethernet.

What Is VPLS?

A VPN technology, VPLS enables Ethernet multipoint services over a packet-switched network infrastructure. VPN users get an emulated LAN segment that offers a Layer 2 broadcast domain. End users perceive the service as a virtual private Ethernet switch that forwards frames to their respective destination within the VPN. Figure 1 shows the logical view of a VPLS connecting three sites. Each customer edge (CE) device requires a single connection to the network to get full connectivity to the remaining sites. A multipoint technology allows a user to reach multiple destinations through a single physical or logical connection, which requires the network to make a forwarding decision based on the destination of the packet. Within the context of VPLS, this means that the network makes a forwarding decision based on the destination MAC address of the Ethernet frame. From the end customer's perspective, a multipoint service is attractive because fewer connections are required to get full connectivity between multiple points. An equivalent level of connectivity based on a point-to-point technology requires a much larger number of connections or the use of suboptimal packet forwarding.

LOGICAL VIEW OF A VPLS

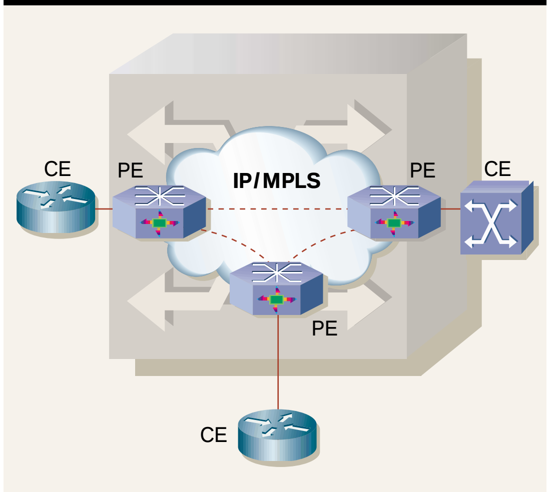


FIGURE 1: Each CE device requires a single connection to the network to get full connectivity to the PE devices and remaining sites.

VPLS Technology Components

In its simplest form, a VPLS consists of a collection of sites connected to a number of provider edge (PE) devices implementing the emulated LAN service. A *virtual switching instance (VSI)* is used at each PE to implement the forwarding decisions of each VPLS. The PE devices make the forwarding decisions between sites and encapsulate the Ethernet frames across a packet-switched network using an Ethernet virtual circuit (VC) or pseudo-wire. PEs use a full mesh of Ethernet VCs to forward the Ethernet frames

VPLS COMPONENTS

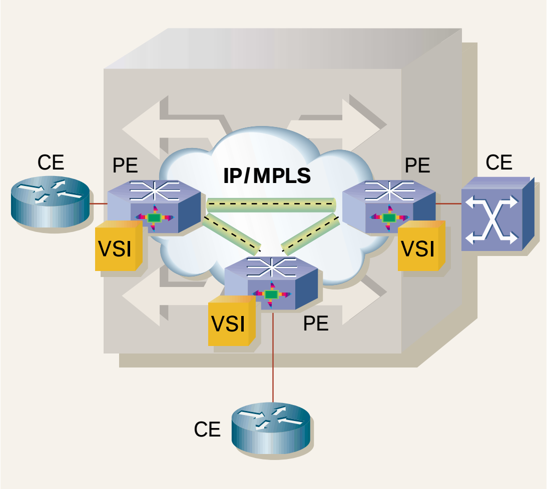


FIGURE 2: In this VPLS that connects three sites, a VSI is used at each PE to implement the forwarding decisions of each VPLS. The PEs use a full mesh of Ethernet VCs to forward the Ethernet frames between PEs.

between PEs. VPLS relies on the same encapsulation defined for point-to-point Ethernet over MPLS. The frame preamble and frame check sequence (FCS) are removed, and the remaining payload is encapsulated with a control word, a VC label, and an Interior Gateway Protocol (IGP) or transport label. VPLS has been initially specified and implemented over an MPLS transport. Figure 2 shows the components of a VPLS that connects three sites.

PEs automatically populate the VSI with the forwarding information required to switch frames within the VPLS. PEs acquire this information using the standard MAC address learning and aging functions used in Ethernet switching. The VSI forwarding information is updated with the MAC addresses learned from physical ports and from the virtual circuits. These functions imply that all broadcast, multicast, and destination unknown MAC addresses are flooded over all ports and VCs associated with a VSI. PEs use split-horizon forwarding on the VCs to form a loop-free topology. In this way, the full mesh of VCs provides direct connectivity between the PEs in a VPLS, and there is no need to use more resource-intensive protocols to generate a loop-free topology (for example, Spanning Tree Protocol, or STP).

There are two functional components in VPLS that involve signaling: *PE discovery* and *VC setup*. Cisco VPLS currently relies on manual configuration of PE associations within a VPLS. However, the architecture can be easily enhanced to support several discovery protocols, including Border Gateway Protocol (BGP), RADIUS, Label Distribution Protocol (LDP), and Domain Name System (DNS). The VC setup uses the same LDP signaling mechanism defined for point-to-point services. Using a directed LDP session, each PE advertises a VC label mapping that is used as part of the label stack imposed on the Ethernet frames by the ingress PE during packet forwarding.

Cisco VPLS does not require the exchange of reachability (MAC addresses) information via a signaling protocol. This information is learned from the data plane using standard address learning, aging, and filtering mechanisms defined for Ethernet bridging. However, the LDP signaling used for setting up and tearing down the VCs can be used to indicate to a remote PE that some or all MAC addresses learned over a VC need to be withdrawn from the VSI. This mechanism provides a convergence optimization over the normal address aging that would eventually flush the invalid addresses.

Even though most VPLS sites are expected to connect via Ethernet, they might connect using other Layer 2 technologies (for example, ATM, Frame Relay, or Point-to-Point Protocol). Those sites connecting with non-Ethernet links exchange packets with the PE using a bridged encapsulation. The configuration requirements on the CE device are similar to the requirements for Ethernet interworking in point-to-point Layer 2 services.

VPLS Scalability Characteristics

VPLS is not the first industry attempt to provide multipoint Ethernet services. Previously, ATM was used to transport Ethernet across the enterprise WAN. One approach was to implement bridging over ATM VCs connecting Ethernet switches, and a second approach used ATM LANE. These alternatives failed to gain popularity due to excessive complexity and limited scalability.

In the case of VPLS, packet replication and the amount of address information are the two main scaling concerns for the PE device. When packets need to be flooded (because of broadcast, multicast, or destination unknown unicast address), the ingress PE needs to perform packet replication. As the number of PEs in a VPLS increases, the number of packet copies that need to be generated also increases.

Depending on the hardware architecture, packet replication can have an important impact on processing and memory resources. In addition, the number of MAC addresses that may be learned from the data plane might grow rapidly if a large number of hosts connects to the VPLS—a situation that can be alleviated by avoiding large flat network domains in the VPLS.

SANTIAGO ALVAREZ

SPENCER TOY

SANTIAGO ALVAREZ, CCIE® No. 3621, joined Cisco in 1997 as a member in the Technical Assistance Center. A technical marketing engineer in Cisco's Internet Technologies Division since 2000, Alvarez focuses on MPLS and QoS technologies. He has been a regular speaker at Networkers and a periodic contributor to *Packet*. He can be reached at saalvare@cisco.com.

A hierarchical model can be used to improve the scalability characteristics of VPLS. *Hierarchical VPLS (H-VPLS)* reduces signaling overhead and packet replication requirements for the PE. Two types of PE devices are defined in this model: *user-facing PE (u-PE)* and *network PE (n-PE)*. CE devices connect to u-PEs directly and aggregate VPLS traffic before it reaches the n-PE where the VPLS forwarding takes place based on the VSI. In this hierarchical model, u-PEs are expected to support Layer 2 switching functionality and perform normal bridging functions. Cisco VPLS uses IEEE 802.1Q tunneling, a double 802.1Q or Q-in-Q encapsulation, to aggregate traffic between u-PE and n-PE. The Q-in-Q trunk becomes an access port to a VPLS instance on an n-PE. Figure 3 shows the H-VPLS architecture.

The H-VPLS model allows service providers to interconnect dispersed Metro Ethernet domains to extend the geographical coverage of the Ethernet service. Moreover, H-VPLS helps scale Metro Ethernet services beyond their 4000 subscriber limit (imposed by the VLAN address space). Conversely, having an Ethernet access network contributes to the scalability of VPLS by distributing packet replication and reducing signaling requirements. Metro Ethernet and VPLS are complementary technologies that enable more sophisticated Ethernet service offerings.

Cisco IOS MPLS Virtual Private LAN Service

Cisco IOS® MPLS VPLS encompasses the Ethernet, MPLS, and management components needed to implement an end-to-end strategy, and is based on the IETF Internet-Draft draft-ietf-pppvpn-vpls-ldp, which has industry-wide support. Cisco's first implementation of VPLS was on the Cisco 7600 Series Router, a product widely deployed in Metro Ethernet architectures by service providers worldwide. Cisco has also introduced support for VPLS in Cisco IP Solution Center (ISC) 3.1 (in addition to MPLS VPN, Any Transport over MPLS, quality of service, and point-to-point Ethernet VPN). Cisco ISC is a provisioning and management tool designed to provide management automation and intelligence while helping to increase productivity of network operators. These components, along with Cisco's portfolio of Metro Ethernet equipment, provide a complete solution for Ethernet services.

In addition, Cisco VPLS is part of the service portfolio that can be offered over a converged network using Cisco MPLS. One of the benefits that service providers seek when deploying MPLS is the ability to offer multiple services over a single network infrastructure. Due to the inherent nature of MPLS, the core devices do not need to be aware of the service associated with packets that travel through the network. As such, the core devices switch traffic in a service-agnostic manner. Only PE devices have to implement the signaling and encapsulation specifics of VPLS. PE devices do not have to be dedicated to one service or another (for example, MPLS VPN, VPLS, Frame Relay, or ATM).

◆ ◆ ◆

The popularity of Ethernet and the flexibility of VPLS as a multipoint service make it an attractive option for some enterprises. VPLS is being considered by many service providers as part of their complete service portfolio using an MPLS infrastructure. While not the industry's first attempt to provide a multipoint Ethernet service over a WAN, Cisco VPLS strives to improve on previous solutions. But VPLS is still a new technology, and there are areas that need work (for example, Ethernet OAM and Ethernet LMI) and areas that could also benefit from deployment experience. Time will tell how popular services based on VPLS become among service providers and enterprises. ▲▲

HIERARCHICAL VPLS ARCHITECTURE

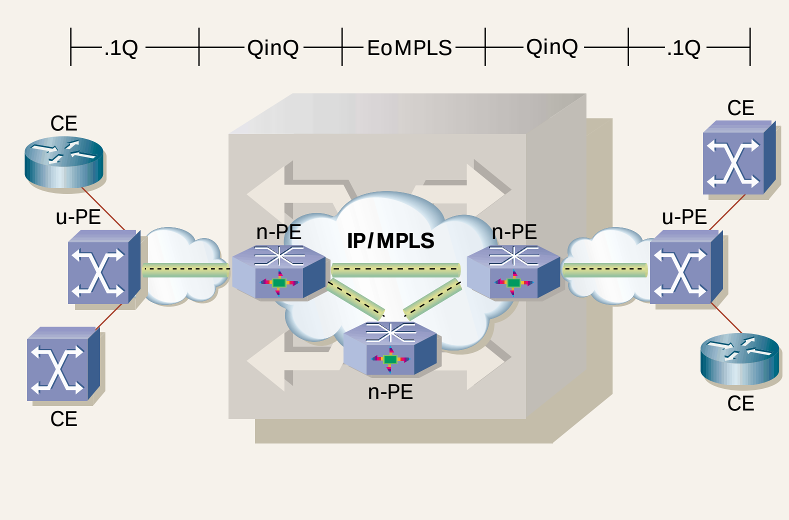


FIGURE 3: In the H-VPLS model, Cisco VPLS uses IEEE 802.1Q tunneling, a double 802.1Q or Q-in-Q encapsulation, to aggregate traffic between the u-PE and n-PE. The Q-in-Q trunk becomes an access port to a VPLS instance on an n-PE.

FURTHER READING

- **Cisco IOS MPLS VPLS Statement of Direction: cisco.com/packet/162_5b1**
- **Cisco IOS MPLS VPLS Application Note: cisco.com/packet/162_5b2**
- **Moving Beyond Traditional VPNs, Q&A with Cisco's Ali Sajassi: cisco.com/packet/162_5b3**
- **Cisco ISC Layer 2 VPN and VPLS concepts: cisco.com/packet/162_5b4**
- **Cisco ISC Layer 2 VPN management: cisco.com/packet/162_5b5**

Discover more about VPN technologies from Cisco experts and your peers at the Cisco Networking Professionals Connection "Virtual Private Networks" forum: cisco.com/discuss/vpn.

Next-Generation Transport

SCTP is becoming the transport protocol of choice for real-time, message-oriented applications.

BY HELEN M. ROBISON, RANDALL R. STEWART, AND KEN A. MORNEAULT

IN OCTOBER 2000, STREAM CONTROL Transmission Protocol (SCTP) was standardized by the International Engineering Task Force (IETF) standards body as RFC 2960. Like Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), SCTP is a transport protocol for sending data from one point to another over the Internet (IP) (see Figure 1).

Authored by the IETF Signaling Transport (sigtran) working group, SCTP was primarily designed to provide a transport mechanism for message-oriented applications such as telephony signaling messages (for example, PSTN Signaling System 7 [SS7] and ISDN) over IP. However, by building upon lessons learned from TCP, SCTP is a feature-rich, general-purpose transport protocol that can be used anywhere TCP is used, with several notable advantages.

Best of Both Worlds

Both stream oriented and datagram oriented, SCTP is a blend of TCP and UDP—and more. The decisive differences between SCTP and TCP are *multihoming* (two or more links to the same endpoint) and multiple streams within a single connection, which are called an *association*. While in TCP a stream refers to a sequence of bytes; in SCTP a stream represents a sequence of messages.

SCTP's built-in features include congestion avoidance and resistance to flooding and masquerade attacks. It has several protocol extensions including partially reliable data delivery. SCTP also provides a heartbeat mechanism and tunable timing controls so that applications can customize the efficiency of failure detection and retransmission.

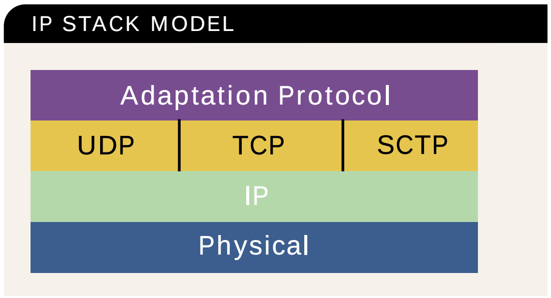


FIGURE 1: Like TCP and UDP, SCTP is a data transport protocol used in IP.

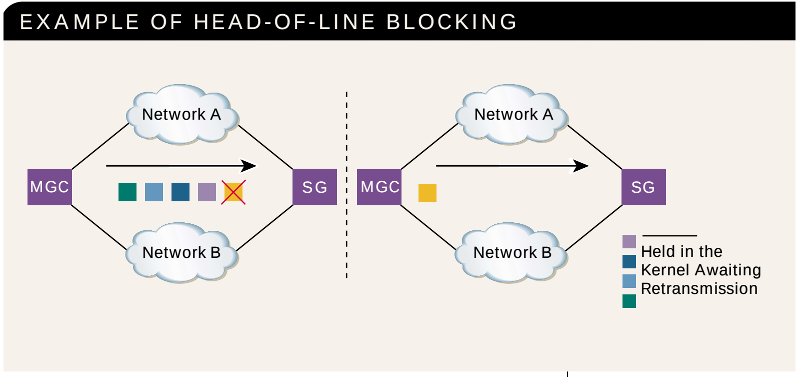


FIGURE 2: TCP is susceptible to HoLB, which can cause unnecessary delay.

Next-Generation Reliable Transport

Why was a new protocol needed for next-generation transport? TCP (IETF RFC 793), developed more than 20 years ago, does an excellent job of providing reliable transport for applications that are relatively insensitive to delay. TCP provides reliable data delivery through acknowledgement mechanisms and strict order of transmission delivery. However, some newer applications require reliable transport without sequence maintenance while others require only partial ordering of data. TCP is susceptible to head-of-line blocking (HoLB) which can add unnecessary delay to these types of applications (see Figure 2).

In the left portion of Figure 2, the first message in the queue has been dropped because of congestion, etc. In the right portion of Figure 2, all messages except the first one have been received and must wait in the receive queue for retransmission of the first message.

As shown in Figure 2, HoLB can occur when multiple independent messages all share one transmit or receive queue. With HoLB, a message must wait until all messages ahead of it are received before being sent to the application. Also, TCP has no built-in support for multihoming, and applications might have stringent reliability requirements that require no single point of failure in the network.

SCTP ASSOCIATION WITH TWO STREAMS

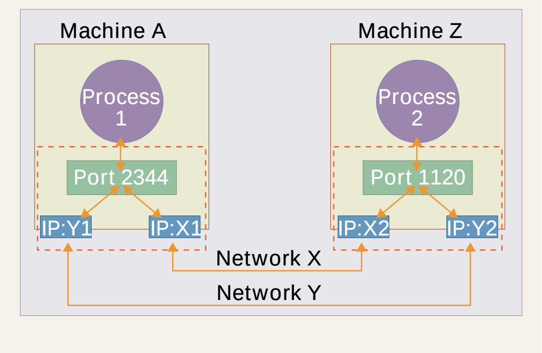


FIGURE 3: In an SCTP association between two multihomed endpoints, the transport address is the port number plus the IP address(es).

SCTP Association

Figure 3 shows an example of an SCTP association between two multihomed endpoints: machines A and Z. The transport address for each endpoint is the port number plus the IP address(es). Each endpoint lists its IP addresses, as well as its port number, as part of association initialization. Therefore, the sender or receiver of the SCTP packets has a list of transport addresses that share the same SCTP port number.

In the example in Figure 3, if Network X failed, the association would remain active and the machines would be able to continue sending data over Network Y. On each retransmission attempt over Network X, SCTP selects one or more alternate path so that endpoints A and Z can continue to transmit data over Network Y while Network X remains in a failed state.

Until a destination is actually marked down (typically after five retransmissions), the primary link is used and retransmissions travel across alternate links. Because SCTP provides a built-in heartbeat mechanism and application-tunable timers (for example, the retransmission timer), delay before failover can be tightly controlled. Furthermore, because selective acknowledgement (SACK) is built into the protocol, SCTP need only acknowledge the highest level of transmission sequence number (TSN) that is complete, along with the gaps. Dropped packets only need to be retransmitted, rather than the entire group of packets since the last acknowledgement.

Data Ordering

While 32-bit TSNs are used for reliability, SCTP uses streams and stream sequence numbers for ordering of data. In SCTP, a stream is a unidirectional flow of messages. Each SCTP association can have multiple streams; at association initialization, endpoints list the number of outbound streams desired and the maximum inbound streams they can support, resulting in maximum inbound streams (MIS) and a requested number of outbound streams (OS) for the association.

Whenever a message is sent between endpoints, it is placed in a stream. If complete ordering of messages is required, then messages can only be sent in a single stream. However, if partial ordering of messages (for example, signaling messages for different voice calls or a set of graphics to be downloaded from an HTML Web page) can be tolerated then messages can be sent over multiple streams. The stream number and the stream sequence number control the message ordering within a stream and across multiple streams. Thus, using multiple streams can avoid HoLB.

SCTP Sublayers

Figure 4 summarizes the functionality of SCTP sublayers. In SCTP, the user initiates a request for association initialization and shutdown. During initialization, a signed cookie is exchanged to provide protection against security attacks.

For sublayer 1, sequenced delivery within streams, the user specifies the number of streams to be supported by the association at association startup. For sublayer 2, user data fragmentation, SCTP supports fragmentation and reassembly of user messages to ensure that the SCTP packet passed to the lower layer conforms to the path MTU.

In sublayer 3, acknowledgement and congestion avoidance, SCTP assigns a TSN to each user data message (fragmented or unfragmented). The receiving end acknowledges all TSNs received, even if there are gaps in the sequence. In sublayer 4, chunk bundling, the SCTP packet delivered to the lower layer consists of a common header followed by one or more chunks.

FURTHER READING

- **Cisco IOS® Software implementation of SCTP, release 2: cisco.com/packet/162_5c1**
- **SCTP Website: sctp.org**
- **Stream Control Transmission Protocol: A Reference, by Randall Stewart and Qiaobing Xie (Addison-Wesley Publishing): www.awprofessional.com/bookstore/product.asp?isbn=0201721864&redir=1**
- **SCTP Implementors' e-mail list: sctp-impl@external.cisco.com (visit sctp.org to subscribe)**
- **IETF Signaling Transport (sigtran) Website, including SCTP RFC 2960: ietf.org/html.charters/sigtran-charter.html**

With sublayer 5, packet validation, a mandatory verification tag field and a 32-bit checksum field are included in the SCTP common header. And for sublayer 6, path management, the SCTP path-management function chooses the destination transport address for each outgoing SCTP packet based upon the application's instructions and the currently perceived reachability status of the eligible destination set. However, not all of these SCTP sublayers are required in a specific implementation.

A typical implementation includes sublayers for the following:

1: Sequenced delivery—in a stream or the ability to bypass

2: User data fragmentation—large messages can be cut into pieces

3: Acknowledgements and congestion control—very important in IP

4: Multimessage (chunk) bundling—messages can be chunked together into a packet but each message retains its boundary

5: Packet validation

6: Path management

SCTP Enhancements

Two extensions that enhance the original features and functionality of the SCTP transport protocol were created after the initial IETF RFC 2960 was approved. The *Add-IP* extension allows for dynamic addition or deletion of IP addresses to an existing SCTP association. An endpoint can also request that a particular local address (to it) be made the peer's primary address.

The *PR-SCTP* extension allows optional choice of partial reliable or unreliable data delivery—for example, an application might require reliable delivery of control messages, while data messages require only partial reliability delivery (that is, if the data message has not been acknowledged within a certain time period, skip past it). This feature allows an endpoint to "skip" a message. Messages within a stream can be fully reliable or partially reliable based on application sending options.

Currently, SCTP is used in an increasing variety of ways. Several groups are now studying or have adopted SCTP for transport, including IETF sigtran for signaling transport over IP (IUA/SUA/M3UA); IETF megaco for media gateway control; and AAA for authentication and authorization. The IETF ipfix working group will use SCTP and its PR-SCTP extension; ITU Study Group 16 will use it for H.248; and ITU Study Group 11 will use SCTP for Bearer Independent Call Control (BICC), Multiprotocol Label Switching (MPLS), and Label Distribution Protocol (LDP).

There is also considerable interest in using SCTP for Session Initiation Protocol (SIP) and MPEG because SCTP supports partial reliability and multimedia. Look forward to seeing many more implementations and applications of the SCTP next-generation transport protocol coming soon. ▲▲

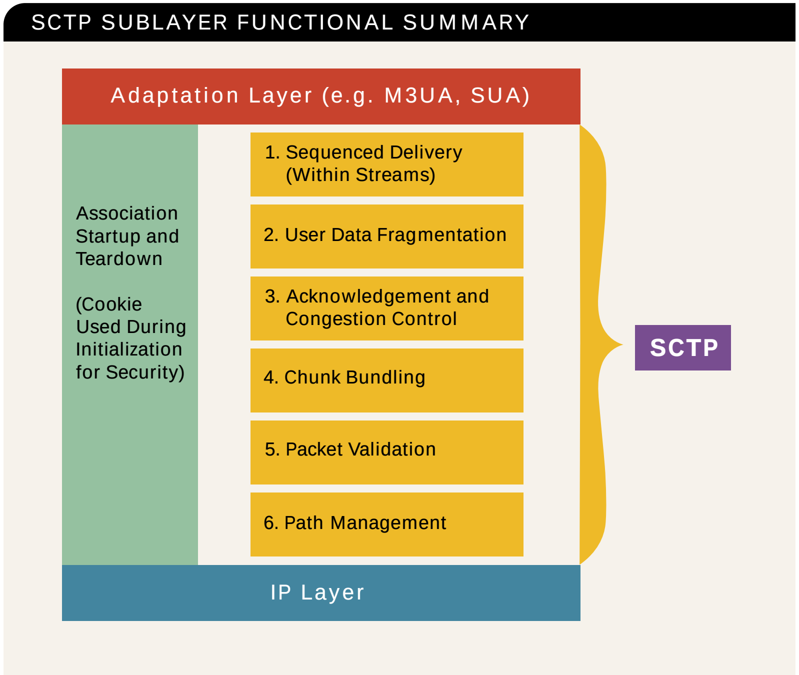

SCTP SUBLAYER FUNCTIONAL SUMMARY
Adaptation Layer (e.g. M3UA, SUA)
Association Startup and Teardown
(Cookie Used During Initialization for Security)
1. Sequenced Delivery (Within Streams)
2. User Data Fragmentation
3. Acknowledgement and Congestion Control
4. Chunk Bundling
5. Packet Validation
6. Path Management
SCTP
IP Layer

FIGURE 4: SCTP is particularly efficient for real-time message transport, including built-in features for security, selective retransmission, and timely path failure detection.

HELEN ROBISON is a senior voice technical marketing engineer in Service Provider Solution Engineering at Cisco. An engineering graduate of Stanford University, she has worked in service provider voice protocols and technologies for 17 years, including 9 at Cisco. She can be reached at hrobison@cisco.com.

RANDALL STEWART, IP transport technologies senior software engineer at Cisco and primary author of SCTP, can be reached at rrs@cisco.com.

KEN MORNEAULT, technical leader for voice architecture at Cisco, is a primary author of the sigtran IUA, M2UA, and M3UA adaptation layer protocols. He can be reached at kmorneau@cisco.com.

IP CALL TO ACTION

BY GAIL MEREDITH OTTESON

TO ACHIEVE SUCCESS in life and in business, people need to understand one another. Everyone has wrestled with misunderstandings and differing interpretations. There is no way around it: interpersonal communication is challenging, and the globalization of business makes it more so. As project teams become more geographically dispersed, they need technologies that facilitate effective collaboration. These technologies should break down distance barriers, overcoming traditional limitations with new ways to share information and enhance discussions, ultimately leading to better decisions and business growth. That's why businesses need IP communications.

IP communications encompasses IP telephony, video telephony, unified messaging and voice mail, IP video- and audioconferencing, customer contact solutions, voice gateways and applications, security solutions, and network management. It exemplifies the systemic approach inherent in intelligent networking. "Where the network has always provided connectivity, now it also solves business problems," says Rob Redford, vice president of Product and Technology Marketing at Cisco. "With intelligent networking, the network, applications, and other components interact in a systemic way—the right function finds the right place in the system. This systemic approach is less complex, application-aware, and secure."

ENABLING ANYTIME, ANYWHERE BUSINESS COMMUNICATIONS

Industry analysts and vendors alike agree that network convergence using IP technologies is inevitable, yet conversions occur only when there is a strong business case for them. According to META Group research, the business case for IP communications must prove operational cost savings, end user productivity gains, capital expenditure savings over private branch exchange (PBX) replacement, and a competitive advantage through new capabilities. According to findings from "Enterprise Convergence 2003: Issues and Trends, a META Group Multi-Client Study" (January 2004), some businesses wait for current PBX contracts to expire. Others deploy it in new facilities or branch offices. Still others—especially small and midsized businesses—will only converge as IP Centrex services become available from service providers.

What Enterprises Want

A technology solution proves itself with a "killer" application—the thing that no one can live without. This application differs widely with IP communications depending on the nature of the business, according to Elizabeth Ussher, vice president of technology research at META Group. "The killer app is what is most useful to the customer, and that varies by vertical market and even by department," she says. For example, a human resources professional might use video telephony to help manage personnel issues, while a customer support desk might need flexible automatic call distribution (ACD) capabilities, and sales people might need access to their e-mail via the telephone. Fortunately, the horizontal nature of IP communications allows deployment of not one but many killer applications, such as enterprise-wide employee communications deployed on IP phones, integrated access to data from enterprise business applications such as customer relationship management (CRM) or workforce management solutions, or Extensible Markup Language(XML)-based applications customized for a specific department or use in a vertical-market segment (for more on XML-based applications, see "Calling on Innovation," page 41).

META Group research indicates that the number one application driving network convergence is conferencing. Other popular drivers are IP phone-based productivity applications such as integrated directories or local transit schedules, remote user access to mission-critical applications, user mobility, and networked voice mail. META Group's January 2004 multi-client study shows that these applications should come from a technology leader that reduces risks associated with convergence, provides high-quality service, reacts to changing customer needs, and helps enterprises target and address their own customers more effectively.

"The enterprises that most successfully adopt IP communications are those with a solution-oriented corporate culture," says Ussher. "But first they have to converge their data and telephony groups." The converged staff should cross-train so that data people acquire telephony skills, and telecom people learn IP. And despite dire predictions several years ago, network convergence does not equal job loss. "I've never seen a client fire any telecom staff after converging their voice and data networks. Voice people are not going away," observes Ussher. "In fact, as they increase their skill sets, they command higher compensation."

Cisco has been a leader in the drive toward network convergence, starting with its 1998 acquisition of Selsius Systems and its IP telephony system. The recent acquisition of Latitude brings critical Web and audioconferencing technology to the Cisco portfolio. And the latest innovation, Cisco VT Advantage, adds video telephony to the mix.

Video Telephony

The first video telephone was introduced at the World's Fair in 1964. "It was an interesting concept, many years ahead of its time," says Rick Moran, vice president of Product Technology Marketing for IP Communications at Cisco. Video telephony has had a hopeful and stormy history, because vendors were unable to solve critical problems of economics, bandwidth, and ease of use. "I believe our implementation is different, because it is cheaper, it is part of the phone call, and it doesn't require any special gear. You are really off to the races," says Moran.

Traditional videoconferencing and corporate television have been cost-prohibitive for widespread business use. Cisco's solution is an extension of an existing IP communications infrastructure, and the video telephony component itself is attractively priced, making it economically available to more users.

Traditional video bandwidth, like traditional videoconferencing, is expensive, which limits deployment of in-house television networks and videoconferencing systems. Ethernet is far less expensive than television coax or leased lines, and the cost continues to drop. Enterprises can afford to install enough bandwidth to reach every user. For branch offices and teleworkers, the cost of broadband services has put video telephony within reach. Picture quality does not suffer. Video compression techniques assure smooth, natural motion over broadband links.

Also, traditional videoconferencing gear is notoriously difficult to use, often requiring dedicated staff to operate it. Cisco's new video telephony solution—Cisco VT Advantage—integrates a Cisco IP Phone with an associated PC to deliver a rich-media video telephony experience. Once the requisite Cisco CallManager functionality is in place, users simply plug the Cisco VT Camera into their computers, install a small PC application, and obtain permission from the Cisco CallManager administrator to transmit video over the network. When a call is placed, the IP phone automatically detects another video-enabled phone at the other end and makes the video option available. "If you don't want video, you can suppress it," says Moran. "You have a 'bad hair day' button." (For more on Cisco's video telephony solution, see "The Video Advantage," page 45.)

With the economic and technology issues of video telephony solved, do enterprises really need it? "It has serious business benefits," says Moran. "We have had a lot of discussion about the impact of video telephony on corporate culture. Will it replace face-to-face meetings? Absolutely not. Is it a great augmentation to voice? Absolutely. It changes the tenor of a conversation and builds bonds between people. If you're looking at the person you're talking to, you have to give the conversation your undivided attention. You can't be composing e-mail or playing solitaire. Body cues help you guess how people are responding to your messages, and you can modify your delivery."

Corporate users spend about half their time in conference calls, and the Cisco video telephony solution supports multipoint conferencing capabilities for any combination of video-enabled and voice-only users. Video automatically switches to the speaker during conferences. Users require minimal training, because conferencing is transparently embedded into the Cisco IP communications infrastructure and is available on a scheduled or ad-hoc basis through the telephone interface. All of Cisco's IP communications solutions offer productivity, mobility, and resilience features designed to enhance communications among employees, customers, vendors, and partners. Cisco's IP communications portfolio includes enhancements that tie the network and applications into systems that solve customer problems. The most notable enhancements tighten communications security and improve user productivity. They include Cisco CallManager version 4.0, Cisco Security Agent for IP Communications, and Cisco MeetingPlace 8106 Rich-Media Conferencing Server.

Cisco CallManager Version 4.0

Among its many enhancements and new features, Cisco CallManager 4.0 enables video telephony and enhances voice security. It provides secure connectivity with media encryption (initially supported in the Cisco IP Phone 7970G with future extension to other end-station platforms) and signaling encryption. When media encryption is active, the IP phone displays a small icon to confirm secure call status.

The 128-bit Advanced Encryption Standard (AES) media encryption is implemented via the Secure Real Time Protocol (SRTP), a standards-based extension to the protocol that transmits voice in IP telephony environments. Because the latency introduced by SRTP is so small, "adding encryption has no detectable impact on call quality—users can't tell the difference," says Roger Farnsworth, senior manager in the Product and Technology Marketing Organization at Cisco.

Placing an encrypted call is easy and secure with new trust and identity management features. Where some vendor phones require manual encryption authentication that can be spoofed, Cisco

CallManager 4.0 and many Cisco IP phones now include support for an X.509 version 3 digital certificate, which embeds the encryption key to automate the call encryption process. The solution also supports third-party certificate authorities, protecting existing investments. "With the trust afforded by digital certificates, you have absolute certainty that you're talking to the correct person," says Farnsworth. "So encryption is not only cool, it becomes useful." What's more, encryption and secure key exchange enables the software images in the IP phones to be signed and verified using the Message Digest 5 (MD5) Secure Hashing Algorithm (SHA), certifying the legitimacy of the image. On top of that, when in secure mode, the signaling used in the IP telephony system can be encrypted through the use of Transport Layer Security (TLS), or Secure Sockets Layer (SSL) version 3.0, thereby preventing man-in-the-middle attacks from compromising system integrity.

Cisco Security Agent

Cisco CallManager 4.0 provides improved threat defense with an embedded version of Cisco Security Agent for IP Communications included at no additional cost, which contributes to the vision of the Cisco Self-Defending Network by adding anomaly-based intrusion protection and policy control to the IP communications infrastructure. (For more on the Self-Defending Network, see *Packet*® First Quarter 2004, cisco.com/packet/162_6a1.) Cisco Security Agent is now also included with such Cisco IP communications applications as Cisco Unity™ and IP Contact Center.

Cisco MeetingPlace 8106

The new Cisco MeetingPlace 8106 conferencing system integrates secure multimedia conferencing with enterprise groupware applications. Conferencing capabilities support both ad-hoc and scheduled voice, video, and Web conferencing. It enhances user productivity through integration with existing applications such as Microsoft Outlook and IBM Lotus Notes. It can also interact with Microsoft NetMeeting, Lotus Sametime, or an intuitive Cisco MeetingPlace Web conferencing application for sharing presentations, applications, or desktops. Participants can "upgrade" a conference in progress to include another person or show everyone a document.

"Cisco is redefining voice as another application on the network," says Moran. "As an application, voice should seamlessly integrate with other applications and pass information back and forth." This integration is intuitive and requires minimal user training. For example, a user can book a Cisco MeetingPlace conference through the Cisco IP Phone, and then find it later on the Outlook calendar on the PC desktop. Conversely, she can book a conference through Outlook and it automatically communicates with Cisco MeetingPlace to reserve the conference. Later, she can look up the reservation using the IP phone interface, and then initiate the call.

More IP Communications Solutions

The Cisco IP communications solution also includes voice gateways, unified messaging, IP-based contact centers, and management tools. Most Cisco switches and routers can become a voice gateway with the addition of a module or software, allowing ubiquitous deployment of IP communications systems throughout enterprise campuses, full-service branch offices, and teleworker locations. Specialized gateways provide protocol translation between legacy audio and video equipment and the primary IP communications infrastructure.

While unified messaging has been available for more than a decade, customer adoption has been slow. "The challenge was that it was difficult to implement. That's not true any more," says Moran. Enhancements to Cisco Unity unified messaging simplify deployment and management. More enterprises are using the integration functions of Cisco Unity to support convenient message retrieval by increasingly mobile workforces. For example, people can now connect their laptop to a public network such as an airport lounge or coffee shop, establish a VPN connection to their corporate network, and download both e-mail and voice-mail messages.

Cisco offers IP-based contact center functionality through its Customer Interaction Network architecture, which includes Cisco IP Contact Center (IPCC) Enterprise Edition, Cisco IPCC Express Edition for companies that need an entry-level or midmarket contact center solution, and Cisco Internet Service Node (ISN), which offers Web-based interactive voice response (IVR), queuing, and IP switching services. While META Group notes that IP-based contact centers are not as important to enterprise IP communications strategies today as they were two years ago, Ussher suggests that IP-based systems are more cost-effective and flexible than their traditional counterparts, particularly for installations up to 75 agents.

For management, the CiscoWorks product line includes comprehensive network management tools that cover the full management lifecycle, from planning and design through implementation/deployment, operations, and maintenance (for more on managing IP communications networks, see page 42).

Building Understanding

IP communications offers tremendous potential for easing the logistical barriers of time zones and geographic dispersion between companies and their branch offices, teleworkers, customers, partners, and vendors. For example, it can enhance collaboration between design teams in the US and Europe, manufacturing in Asia, and sales and distribution centers worldwide. It simplifies the process of connecting with your customers, while enhancing the value of your interactions with rich-media sharing and video telephony. With such enormous potential for increasing productivity and sales through effective collaboration, can you afford to wait? ▲▲

FURTHER READING

- **Cisco IP Communications: cisco.com/go/ipc**
- **Cisco CallManager 4.0: cisco.com/packet/162_6a2**
- **Cisco VT Advantage: cisco.com/packet/162_6a3**
- **Cisco MeetingPlace: cisco.com/go/meetingplace**
- **Cisco IP Communications security: cisco.com/go/ipcsecurity**

IP COMMUNICATIONS IS TRANSFORMING BUSINESS AS USUAL IN MANY INDUSTRIES.

LICENSE TO COMMUNICATE

BY RHONDA RAIDER

WASN'T THAT AIR CANADA ticket counter a Lufthansa ticket counter earlier in the day? It could be so if you're at Toronto Pearson International Airport in Canada. Until last year, Pearson assigned each airline its own counters, with phones dedicated to the airline's own extension and speed-dial numbers. Now the Greater Toronto Airports Authority (GTAA) management can assign any airline to any unused counter: agents personalize the Cisco IP phones and PCs at the counter in just a few minutes, with a single sign-on. "The inability to shift unused counters to another airline has long been a problem for the airline industry, creating the potential for wasted resources," says Thomas Tisch, the airport's general manager of electronic systems and technology. "Now, with Cisco CallManager and its Extension Mobility feature, we have far more flexibility and can use our space more efficiently."

CORBIS.COM; PHONE: SPENCER TOY

IP Network as "Communications License"

Pearson's application is a prime example of innovative uses of IP telephony across the spectrum of industries, including transportation, manufacturing, government, education, insurance, healthcare, and financial services. "In any industry, IP communications is changing the way people work to make them more productive," says Alex Hadden-Boyd, director of marketing for IP communications in the Product and Technology Marketing Organization at Cisco. "Just as a driver's license gives you permission to drive any number of cars, an IP network gives you a license to communicate using any device—phone, PC, fax, or videoconferencing terminal from any location."

Transportation: "Virtual Gate" Application

The "virtual gate" application at Pearson International Airport runs over the GTAA's optical backbone network, based on the Cisco 7600 Series Router, and was introduced in 2003 to replace 82 separate data, telephony, and video networks. "Agents in our new terminal can customize both the PC and Cisco IP Phone 7960G's at the gate with a single sign-on," explains Ian Grant, manager of electronic systems for the GTAA. The first agent to arrive logs on to the airline's Common Use Passenger Processing System (CUPPS), which runs on a PC. The airport uses the Cisco CallManager application programming interface (API) to instruct CUPPS to alert Cisco CallManager when the airline identity changes, at which time Cisco CallManager automatically pushes the new airline's profile to the Cisco IP phones at the gate. The profile includes the phone number as well as the airline's speed-dial numbers. "Those features make the Cisco IP Phone behave like the phones the agents are accustomed to, which eliminated our airlines' training concerns," says Grant. "Then we took advantage of unique features of Cisco IP communications solutions to add even more value."

For instance, to make the directory more relevant for airline employees, the GTAA divided it into two branches: one with numbers important to "above the wing" employees such as airline agents, and another for "below the wing" employees such as baggage handlers and maintenance staff. And the airport also wrote another Extensible Markup Language (XML) application for the airport's Resource Management Group that lets employees receive calls pertaining to a particular function, such as baggage, simply by logging onto that screen on their Cisco IP phones. "IP telephony has created new application possibilities that weren't possible with standard phones," says Grant. "Cisco CallManager and Cisco IP phones enable the airline industry to take advantage of a common format, XML, to cut costs and to improve service for our passengers."

Manufacturing: Rapid Response to Change

The ability within IP telephony to quickly set up new phones solved a different business need for Ingersoll-Rand, a leading manufacturer of solutions for security and safety, climate control, and industrial solutions and infrastructure. In late 2003, the company sold a division in Torrington, Connecticut, and needed a quick, cost-effective way to set up a telephony network for the 30 executives who remained behind—with no local IT staff. The company didn't have the luxury of waiting weeks to order and deploy a small PBX and order phone service. Instead, Ingersoll-Rand had a fully functional IP telephony service just days later, by setting up the office as a satellite off of an existing, centralized Cisco CallManager call-processing cluster in the company's Huntersville, North Carolina office. Besides PCs and printers, the only new hardware needed to bring up a fully functional new office was a Cisco 3745 Router and Cisco IP Phone 7960G's. "All routing, switching, and voice and data connections to the IP network and PSTN [public switched telephone network] terminate in that one little router," says Damon Cahill, manager of infrastructure strategy at Ingersoll-Rand.

Employees in the satellite office have access to all features enjoyed by their corporate counterparts, over the WAN. Should the WAN link fail, telephony service continues without interruption, thanks to the Survivable Remote Site Telephony (SRST) feature, a standard feature of Cisco IOS® Software that, when enabled, automatically begins routing calls over the public PSTN. "Centralized call processing means we need less hardware at local sites and less administrative burden, which translates to lower costs," Cahill notes.

Ingersoll-Rand plans to use the same centralized call-processing model for its other smaller sales offices. "The business case for centralized call processing with SRST is very compelling for offices with 100 or fewer users, and we can cost-justify it for certain larger sites, as well," says Cahill. "It's simple: the cost of a Cisco router and Cisco IP phones is far less than that of a PBX."

Unified Messaging Boosts Productivity

The Cisco CallManager cluster at Ingersoll-Rand's Huntersville office also provides Cisco Unity™ unified messaging, which lets employees retrieve both voice mail and e-mail from their IBM Lotus Notes groupware e-mail inbox. "Before I leave for the airport, I replicate my inbox locally so that I can compose responses when I'm on the plane," says Cahill. "Next time I connect to the network I send them out. Now, with Cisco Unity, I can listen to and compose responses to voice-mail messages as well, with my laptop and headset."

Hadden-Boyd of Cisco has a similar approach to productivity during airport layovers, but uses a cell phone instead of a PC. "If I'm in the airport and have ten minutes before my flight, I don't necessarily have time to find an Internet connection to check e-mail from my PC. With Cisco Unity unified messaging, I can call on my cell phone and listen to both voice mail and e-mail using text-to-speech translation."

Unified messaging improves productivity during Ingersoll-Rand's meetings, as well. Come break time, participants use their laptops on the Ingersoll-Rand wireless network to retrieve and respond to e-mail and voice-mail messages. "In this case, people like the fact that they don't have to listen to every voice mail in order, as they would on their phones," says Cahill. "They see all the callers' names or numbers in their inbox and can jump directly to the most urgent."

In addition to unified messaging, the Cisco CallManager cluster at the Ingersoll-Rand Huntersville office supports a 25 to 30-person contact center whose agents field questions about employees' pensions and benefits. "Cisco IPCC Express Edition software provides us more capabilities than we had on our small PBX system, like recording conversations, allowing supervisors to enter a call midstream, and historical reporting," says Cahill. "And we no longer have to pay someone $250 an hour to add a queue, for instance. Now we can make the change ourselves, using the simple interface. In the manufacturing industry, where it's fairly frequent that we would add or divest ourselves of a company, the ability to make changes easily is very valuable."

Measuring the Cost Savings

Organizations in all industries are likely to cite cost savings as a chief benefit of IP communications, and Ingersoll-Rand has the metrics to prove it. For conference calls, the company traditionally has used a managed service. In the Huntersville facility, where executive meetings might have 100-plus participants, the bill amounted to US$15,000 a month. Now, the company has eliminated the need for that service with Cisco Conference Connection software, which integrates with Cisco CallManager to provide audioconferencing. Total monthly costs have plummeted to US$4000 for infrastructure. "Employees like being able to go into a Web interface to schedule their own calls instead of calling the carrier," says Cahill. People join the conference call by dialing a four-digit extension, or by scrolling down on their Cisco IP phones to see the call and then pressing the Join button. Callers from outside the network can join over the PSTN.

Ingersoll-Rand determined that the Cisco IP communications system will slash equipment costs by 38 percent, maintenance costs by 18 percent, and conference call costs by 70 percent. Factoring in the one-time installation charges, the company estimates it will save US$1.17 million over five years.

Information Services: Combined Audio and Data Conferencing Cuts Costs

LexisNexis Group, the global legal publishing arm of Reed Elsevier, the Anglo-Dutch world-leading publisher and information provider, uses a large-scale Cisco conferencing solution, Cisco MeetingPlace, both to cut costs and to safeguard its proprietary data presentations. Until 2002, the company had used two different service providers for external audio and data conferencing. "We were paying US$1.29 million a year," says Jeff Sira, manager of conference services. "As long as we were billed per minute, we knew the costs would grow each year."

The company not only wanted to slash its audio and data conferencing costs, but also wanted to address a key security concern regarding intellectual property. "Our data presentations deal with strategic issues such as acquisitions, confidential communications with major shareholders, and R&D that we wouldn't want our competition to be aware of," says Sira. "It bothered us to upload this type of asset to someone else's server and then just take their word that it was deleted when the meeting ended."

LexisNexis Group found the answer in Cisco MeetingPlace, which it uses to handle both audio and data conferencing. "It's been extremely cost-effective," says Sira. "We expected to see ROI [return on investment] in 18 months; instead, Cisco MeetingPlace paid for itself in just 7 months, because our conferencing calling volume increased. And because we own MeetingPlace, it won't cost us more to conduct more conferences as the business grows." The company began with 360 seats, recently added another 240, and expects to add another 240 by the end of 2004.

Government: Low-Cost Application Delivery

Located 20 miles northwest of Washington, DC, the Town of Herndon, Virginia took up IP telephony for one reason, and now appreciates it most for an entirely different one. "We adopted IP telephony for scalability and to reduce our phone bills," says Bill Ashton, the town's director of IT. "We succeeded: we're already saving 30 percent every month and expect that to rise to 50 percent when we add the police department to the system. But the more remarkable gain is that we're using IP telephony as a low-cost platform to deliver applications."

For instance, the town has begun pushing AMBER alerts, about missing or abducted children, to its employees' Cisco IP Phone 7900 Series, using the PhoneTop AMBER Alerts system from Cisco Premier Certified Partner AAC Inc.

"When we see an AMBER alert for a child within a 50-mile radius, we push it to all Cisco IP phones using XML," says Ashton. A distinctive ring tone sounds, and then employees have the option to press soft keys on their phones to see more information, including suspect and victim pictures, on the phone display. "With the PhoneTop AMBER Alerts application, we suddenly have six times the number of eyes looking for abductees than we have police officers alone," notes Ashton.

The Town of Herndon is also planning to deploy AAC's PhoneTop EAS Alert Service to push other critical information to employees' Cisco IP phones. "If we receive any kind of emergency message from the county into our database—tornado watch, heightened terrorist alert, major accident on a heavily trafficked highway—we can immediately route it to municipal employees who need to see it," says Ashton.

The benefit potential of IP telephony during disasters hit home when Hurricane Isabelle struck in 2003. Local government offices were closed, but the Town of Herndon nonetheless had to call in certain employees to deal with problems with the water system. Ashton plans to install Cisco IP SoftPhones on key employees' home PCs so that they can work from home during hazardous conditions, which will help to ensure their safety and alleviate traffic on the roadways.

"If you give me enough money and time, I can deliver any application you want me to," Ashton continues. "But if you want to save money and time, the Cisco IP Phone is a superior delivery platform. It's low cost, always on, and I already have a phone everywhere in the organization. I have fine control over the applications because I subscribe employees to the service, which runs in the background. To have that level of control if I delivered an application to the computer, I'd have to deal with operating system concerns, and buy and install backend software. This way, everything I need is native to Cisco CallManager."

Education: Facilitating Communication

The benefits of IP communications extend beyond cost and productivity. In education, IP telephony is changing the way teachers, students, and parents communicate. The impact is especially noticeable at Washington School for the Deaf (WSD) in Vancouver, Washington. Since WSD transitioned from a traditional telephone system to Cisco IP communications with NXi Telephony Services (NTS) text-messaging software from NXi Communications, all WSD employees—hearing and deaf—have enjoyed equal access to communications services.

When WSD relied on a traditional telephone system, a teacher who was deaf and needed to talk to a hearing person by phone either needed to use a relay service or ask another staff member to call the parent and then interpret using American Sign Language. “Apart from the obvious privacy and independence issues, this system increased WSD’s phone bills because the relay service charged more for long-distance calls than the school would pay if the caller had dialed directly using the low-cost, state-controlled access network,” says Lorana Myers, supply officer at WSD.

Now WSD staff and faculty, both deaf and hearing, can make and receive calls independently using either their Cisco IP phones or NTS client software on their PC or laptop. “One of our deaf teachers used to e-mail me if she had questions during her prep time,” says Myers. “Sometimes we barely had enough time to resolve the issue before class started—and that’s if I received and opened her e-mails immediately. Now she uses her NTS client software to call me and we can converse in real time, resolving questions much more quickly. With our Cisco IP communications solution we can now do all the things that hearing people take for granted.”

> “IF YOU GIVE ME ENOUGH MONEY AND TIME, I CAN DELIVER ANY APPLICATION YOU WANT ME TO. BUT IF YOU WANT TO SAVE MONEY AND TIME, THE CISCO IP PHONE IS A SUPERIOR DELIVERY PLATFORM. IT’S LOW COST, ALWAYS ON, AND I ALREADY HAVE A PHONE EVERYWHERE IN THE ORGANIZATION.“
>
> BILL ASHTON, DIRECTOR OF IT, TOWN OF HERNDON, VIRGINIA

Two redundant Cisco CallManager servers form the core of the solution, providing telephony services throughout the school’s 12-building campus fiber network. One Cisco CallManager server includes Cisco IPCC Express Edition software, which provides automatic call distribution (ACD) of calls from hearing and nonhearing callers. People who call the school’s main number are given a voice prompt to press 1 to continue. “Callers who don’t press 1 are presumed deaf and are automatically transferred to the NTS server,” Myers explains.

Both the Cisco IP Phone and NTS client provide visual indicators not only for dial tone, but also for ringing, hold, call termination, message waiting, and the like. A strobe light connected to the Cisco ATA 186 Analog Telephone Adapter provides another indication of incoming calls. The dial-tone indicator enables deaf employees to use the two-stage dialing required to access the low-cost, state-controlled access network.

Remarkably, WSD now provides equal access to voice mail, as well. A Cisco Unity server residing on a Cisco MCS 7835 platform can handle voice-mail sessions for both hearing and deaf users. When a hearing person calls a deaf person’s extension, the system issues a voice prompt that the person called does not accept voice messages, and offers the caller the option to either insert the telephone handset into the teletypewriter (TTY) coupler to leave a text message or be routed to a hearing operator, who takes a TTY message. Either way, the message is delivered to the deaf user’s NTS client software on the desktop. “With Unity and NTS, parents and others without TTY devices for the first time have the ability to leave messages for deaf staff and faculty,” says Myers.

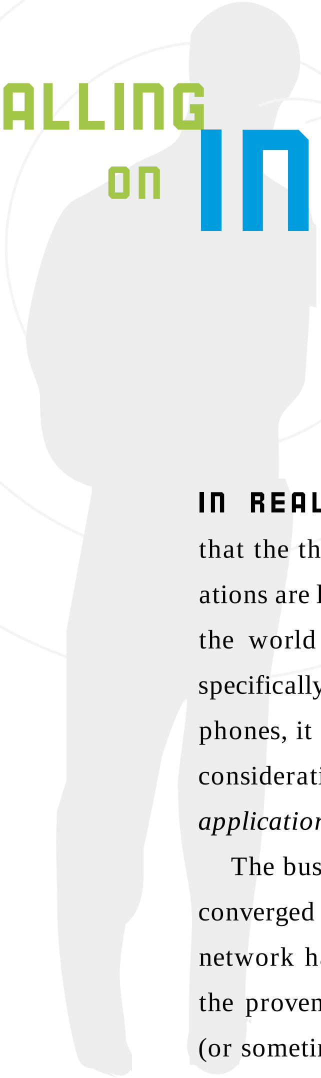
Freedom to Innovate

“Before we built our Cisco IP communications network, I was in the business of saying ‘no’ to requests for telecommunications service changes, because they were too costly and time-consuming,” says Ashton, from the Town of Herndon. “Now I’m in the business of saying ‘yes.’” Case in point: the town is engaged in an ongoing debate about extending rail service to Dulles International Airport. The train would roll just outside the town limits, so at one point the town became a focal point for the media, and Ashton needed a media center for the major news services—and in a hurry. “Six months ago I would have declined,” he says. “But with the Extension Mobility feature in Cisco CallManager, I just grabbed a few phones from stock, plugged them into a conference room, and added the newscasters and their phone numbers to the system. Within 20 minutes we had our media center.”

Communications is the lifeblood of many industries and, like Ashton, IT people are waxing creative with new, IP-based solutions for improving productivity. For instance, when Cisco recently had a power outage, the company broadcast instructions on how to leave the building to employees’ Cisco IP phones, which remained on because they drew inline power from Cisco routers.

“IP is the universal translator that integrates voice, video, and data,” according to Hadden-Boyd. “The end user has the freedom to choose what media they want, and what device they want to use to receive it. Hearing about some of these applications, people might ask, ‘Weren’t they possible ten years ago?’ The answer is yes. The difference is that today, technologies like IP and XML have made it so much easier. Something that used to be either impossible or incredibly complicated, like walking down the hall talking on a Cisco Wireless IP Phone 7920 and then switching to a Cisco IP Phone 7970G, with color touch-screen, when you arrive in your office, or adding video to a call midstream with Cisco VT Advantage software, can now be done with the press of a button. What once was very difficult is now casual and ad hoc.” ▲▲

XML APPLICATIONS DEMONSTRATE THE POWER OF IP PHONES TO STREAMLINE BUSINESS PROCESSES AND BOLSTER PRODUCTIVITY.



CALLING ON INNOVATION

BY JENNIFER REDOVIAN

IN REAL ESTATE, it is oft-stated that the three most important considerations are location, location, location. In the world of IP communications, and specifically as it pertains to Cisco IP phones, it can be said that the three top considerations today are *applications, applications, applications.*

The business value of a converged voice and data network has grown beyond the proven 20 to 50 percent (or sometimes greater) savings companies yield by eliminating leased-line charges and lowering maintenance fees and management costs. The value proposition now taps directly into a company's existing investments in IP communications and the customizable, easy-to-use nature of IP phones to enable innovative, business-enhancing applications. Viewed as a strategic business asset, these applications marry communications with business processes to boost employee productivity, drive new efficiencies and revenue, and enhance customer service and satisfaction.

"In addition to the total-cost-of-ownership benefits of running a converged network, IP telephony has the ability to transform business processes and deliver improved user productivity and satisfaction," according to Zeus Kerravala, vice president of enterprise infrastructure at the Yankee Group. "The applications running on an IP phone over a converged network will transform enterprise communications from a static, delayed communications environment to one that is more real time and proactive. . . . The IP telephony applications will make convergence more of a business decision rather than one focused primarily on technology."

Just ask Maurice Ficklin, director of technical services at the University of Arkansas, Pine Bluff. For more than two years, Ficklin has managed approximately 2000 Cisco IP phones and Cisco CallManager clusters in each of four cores at the university campus with "no complaints, no problems," he notes. Slowly but surely, however, Ficklin moved toward a more technologically self-sufficient IP network, offering phone, data, and wireless services to students and faculty, including using Cisco IP phones to conduct surveys and enable other productivity-boosting applications. "Of course, the return on investment is very important to us, but we look far beyond that now," says Ficklin. "We have gone from *paying* for something [the IP phones, for example] to *receiving cost recovery* on something."

A 2003 survey conducted by Sage Research offers further evidence of the benefits of IP communications. One hundred organizations that have deployed IP communications reported the following:

- Faster moves, adds, and changes—respondents report an average saving of 1.5 hours per move
- Easier-to-use features on IP phones—average saving of 5.5 hours per week for each IT employee involved in phone support
- Less "telephone tag" among employees—average saving of 3.9 hours per week (or 25 days a year) per employee
- Improved remote worker productivity—average benefit of 4.3 hours per week (or 28 days a year) for each remote worker

MANAGING YOUR IP COMMUNICATIONS NETWORK

To successfully administer, maintain, and plan for the present and future of an IP communications network, network managers must fully understand their voice and data traffic and how it can affect the behavior of corporate networks. Establishing a process to evaluate, document, and monitor this important operational resource is imperative. The CiscoWorks product line includes comprehensive network management tools that cover the full management lifecycle, from planning and design through implementation/deployment, operations, and maintenance. They are designed to improve productivity and lower total cost of ownership (TCO) through automation, integration, and simplification.

CiscoWorks software includes tools to centrally manage critical network characteristics such as availability, resilience, responsiveness, and security. Among these tools are CiscoWorks IP Telephony Environment Monitor (ITEM), CiscoWorks QoS Policy Manager, and the Cisco Catalyst® 6500 Series Network Analysis Module. The Cisco CallManager user interface also simplifies the most common subscriber and telephony configuration tasks by adding software and Web-based applications.

CiscoWorks ITEM, through the WAN Performance Utility (WPU), is used for both the planning phases as well as routine operations phases of managing your IP communications network. CiscoWorks ITEM uses Service Assurance Agent (SAA) functionality of Cisco IOS® Software to measure latency and jitter between key points in a network that deploys Cisco IP telephony. WPU is used to help assess IP telephony readiness of Cisco-based IP networks. It also provides real-time health and fault monitoring of converged IP networks, and the ability for operations and administrative staff to monitor and manage telephony resources to capture and record performance and capacity management data. Powerful tools, such as CiscoWorks IP Phone Help Desk Utility, enable operations and help-desk staff to respond to customer issues efficiently and maintain surveillance on the introduction and movement of IP phones in their environment.

Another important application in the CiscoWorks ITEM suite—CiscoWorks IP Telephony Monitor 2.0—features a user interface with a Web-based operations screen that gives you real-time network status and alerts of actual and suspected problems in the underlying IP network and IP telephony implementation. This Alerts and Activities Display (AAD) can be customized to show all or selected elements in the managed space.

Call control is also critical in managing your IP communications network. Management applications help to assess the aggregate number and distribution of calls, identify peak hours, and monitor analog FXO/FXS connections and PRI channel activity. This data can be used to assess best and worst performance and to support trend analysis and forecasting. Platform metrics such as CPU utilization and memory allocation can also be tracked.

Another IP communications management application, CiscoWorks IP Phone Information Utility, can assist with system maintenance, monitoring, and reporting by providing real-time fault analysis and management, including fault history and information about all the phones on the network, their operational status, and implementation details. Utilities such as CiscoWorks ITEM Gateway Statistics Utility collect key performance and behavior statistics about the gateways and trunks to ensure systemwide health and device availability.

To learn more about managing your IP communications network, see cisco.com/packet/162_6c2.

Open Standards, Easy-to-Deploy Apps

Cisco IP phone applications are based on open industry standards such as Extensible Markup Language (XML), Telephony Applications Programming Interface (TAPI), and Java-based TAPI (JTAPI), which provide the ability for software developers to create telephony applications. Because developers write to the intuitive, point-and-click, browser-based interface, there's no need for IT personnel and other end users to know anything about the lower layers.

Enterprises can take data from their back-office business applications and deliver select information to the LED screens of their Cisco IP phones. Softkeys on the phones are used to access and display data from the XML applications—extending real-time business information, services, and enhanced images to every corner of an organization, even in settings where PCs are typically inaccessible to employees such as warehouses, factory floors, and sterile lab environments.

XML support is available on the Cisco IP Phone 7905G and 7912G monochrome displays for text-based applications; the Cisco IP Phone 7940G and 7960G with monochrome displays for both text-based and graphics-based applications; the new Cisco IP Phone 7970G model that features high-resolution, 234-pixel color graphics on the phone display along with touch-screen access to features and applications; and the Cisco IP Communicator (Softphone). For Cisco IP Phones 7940G and 7960G, Cisco CallManager Version 3.1 or higher is required for XML support. Cisco IP Phones 7905G, 7912G, and 7970G require Cisco CallManager Version 3.3 or higher. CallManager upgrades are available free; to download, visit the Cisco Software Center: cisco.com/packet/162_6c1 (Cisco.com login is required for full access to the software downloads).

To date, the most prevalent Cisco IP Phone applications have been developed for use in information-laden vertical-market industries, notably in education, retail, hospitality, and government. Among the many applications being deployed are administrative and attendance solutions for school districts and universities; inventory tracking and lookups for retail branches; concierge, restaurant listings/reservations, and other guest-service applications for hotels; emergency notification and audio streaming systems for government and public-safety personnel; and time-clock applications for use on manufacturing floors, and in hospitals, bank branch offices, and other work environments with large numbers of hourly-wage employees.

Likewise, enterprise applications readily available on desktop PCs—e-mail and unified messaging, corporate directories, conference-room booking, and expense reporting, for example—can be provided on IP phones. In this way, the phone serves as an always-on communications and information vehicle for business, critical, and time-sensitive communication with employees—anytime and anywhere they are. No doubt, the simplification of menu-driven information access improves efficiency and expedites day-to-day business processes.

Another benefit of Cisco IP phones: they are managed like PCs. Deploying new applications and services to the phone sets is as easy as distributing software and automating installation on a remote PC. Upgrading business applications, enhancing telephony services, and extending phone-based transactions can be accomplished smoothly and rapidly (see the sidebar, "Managing Your IP Communications Network," page 42).

IP Phone Productivity Applications

Many of the XML-based, off-the-shelf productivity applications are being developed by, and can be purchased from, Cisco partners for easy customization to suit a company's business requirements. What's more, these applications are already proving their worth in both measurable productivity gains and cost savings, results that were demonstrated with enthusiasm at the Cisco Innovation Through Convergence (ITC) Expo last September.

More than 70 Cisco AVVID (Architecture for Voice, Video and Integrated Data) IP communications and wireless technology partners showcased their integrated voice and data software applications for IP phones. An independent panel of judges from the CIPTUG selected 13 application developers that demonstrated the most compelling benefits in categories such as "Employee Productivity," "Return on Investment and Innovation in a Vertical Market," "Cost Controls and Reductions," and "Best Innovative Single Idea," among others.

The PhoneTop K-12 application from AAC Inc., for example, won for customer satisfaction and best innovative use of technology in education and government. PhoneTop K-12 (see Figure 1) lets grade-school and high-school teachers use their Cisco IP phones to perform tedious, otherwise-manual administrative tasks such as taking daily attendance and managing student hall passes.

AAC's application is helping Frederick County Public Schools in Virginia streamline communications between its 20 networked facilities, and reduce costs by eliminating the 20-plus different existing phone systems (offered by half a dozen vendors) and centralizing telephone processes into a single, easy-to-manage voice and data IP communications structure.

In the government arena, AAC is applying its PhoneTop AMBER Alert Services software to help find missing children in and around the Town of Herndon, Virginia. For more on this and other IP communications applications being deployed in vertical markets, see "License to Communicate," page 36.

Chosen best in the category of "Cost Controls and Reductions" was Aptigen Designer from EDCi, a horizontal application that allows anyone to create IP telephony prototype solutions quickly and easily—no XML coding skills required. "Ninety percent of Cisco CallManager deployments don't have applications deployed to them," says Aptigen Vice

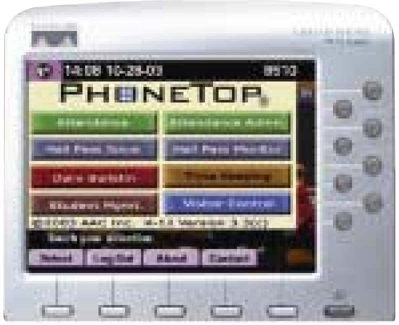


FIGURE 1: AAC's PhoneTop K-12 application gives teachers the flexibility to perform routine, otherwise paper-based processes on their IP phones—freeing them up to devote more time to students in the classroom.

NET IMPACT 2004: FROM CONNECTIVITY TO PRODUCTIVITY

A newly released study by Momentum Research looks at the effects of integrating Internet applications, networking technologies, and business processes on the public sector in Europe. The study—called *Net Impact 2004: From Connectivity to Productivity*—asked nearly 1400 IT and business decision makers in eight European countries what technologies, applications, and processes they had implemented to accelerate e-government or e-health. The survey found that organizations were between three and seven times more productive than their peers if they invested in network functionality beyond the minimum required to support their applications (for example, deploying layered security or sophisticated traffic management tools), changed their business processes before deploying a new application aimed at increasing efficiency, and automated business processes with Internet applications and integrated those processes with other service functions. Interestingly, but not surprisingly, a desire to accelerate operations and improve citizen satisfaction ranked significantly higher than cutting costs as the top goals among respondents for improving productivity.

Net Impact 2004 is the fourth in a series of research projects sponsored by Cisco to evaluate the impact of Internet technologies on organizations and productivity. For more on the Net Impact research, see netimpactstudy.com.

President Nick Tseffos. Aptigen Designer is helping to change that.

With this application, you can design, demonstrate, and deploy the full value of IP phone technology *immediately*, emphasizes Tseffos. Instead of merely talking through the productivity benefits of an IP phone application, you can use Aptigen Designer's Windows-based interface and drag-and-drop environment to create a custom application, publish it to a phone emulator to check your work, and instantly deploy it to the enterprise, thus increasing your ROI and reducing development time to production.

Named best in the “Return on Investment/ Vertical Market” category was Vytek’s *Extend*Time application. A complete time and attendance solution targeted at a broad range of industries, *Extend*Time replaces traditional time clocks, and automates time data collection, auditing, and reporting via IP phones. With a unique employee ID number and password, workers can “clock in” and “clock out” using any Cisco IP Phone in their organization. They can also receive messages, view scheduled work hours and accrued benefits such as vacation or sick days, and locate company-wide resources using the *Extend*Time directory (see Figure 2).

Flexible, Instant Communications

The flexibility and advanced capabilities of IP phones offer the opportunity for software developers to use text, graphics, audio, alerts and now, with the Cisco IP Phone 7970G, color to deliver a rich user experience. Many of these users, for example, are benefiting from an application developed by Twisted Pair Solutions called WAVE (Wide Area Voice Environment). Chosen for “Best Innovative Single Idea” at ITC Expo 2003, WAVE allows integration between IP-based networks and other systems such as IP telephony and mobile radio environments—enabling you to create new, scalable group communications consisting of audio, video, and data content.

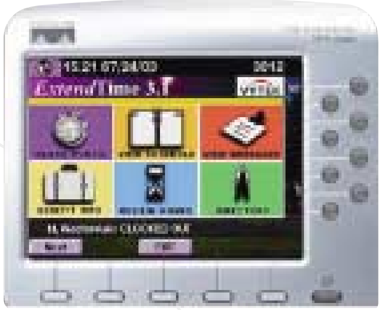


FIGURE 2: *Extend*Time 3.1, developed by Vytek, replaces traditional time clocks, automating time data collection, audits, and reporting via Cisco IP phones.

WAVE not only leverages your existing IP network but brings together communications among previously disparate groups. A firefighter and a police officer, for instance, with their different VHF and UHF radio communications, can now instantly talk to each other while their streams of audio are carried over an IP infrastructure.

As Twisted Pair Solutions and many other software developers are demonstrating, IP communications solutions can be considered strategic business assets that are transforming how organizations communicate—internally and externally. Productivity gains result not simply from adding applications to your network, but by integrating business processes with communications to tap into your network and the technology that will make those *applications work for you*.

◆ ◆ ◆

To learn more about the applications showcased at ITC Expo 2003, and for general information on developing and deploying XML applications and IP phone services, visit Cisco IP Communications Applications Central (AppsCentral) at cisco.com/go/apps. ▲▲

FURTHER READING

- **“Thinking Outside the Talk Box,” *Packet*® Third Quarter 2002: cisco.com/packet/162_6c3**
- **Cisco IP communications: cisco.com/packet/162_6c4**
- **Cisco ITC Expo 2003 Video: cisco.com/packet/162_6c5**
- **CIPTUG: ciptug.org**

THE VIDEO Advantage

EXPANDED IP COMMUNICATIONS PORTFOLIO ENABLES RICH-MEDIA CALLS AND CONFERENCES.

BY DAVID BAUM

STUDIES HAVE SHOWN that at least 60 percent of human communication is nonverbal—conveyed by hand motions, facial expressions, and body language—so a video image that enhances an audio conversation is a tremendous asset. Until recently, however, video telephony and conferencing systems have been expensive and difficult to use. The networks used were not architected for video, so the quality was poor and the pictures were grainy and jerky. Despite the lofty promises of converged IP networks that could seamlessly transmit voice, video, and data, only about 2 percent of today's meeting rooms are equipped with videoconferencing equipment, much of that still running over ISDN, and video is almost nonexistent on the desktop.

That's changing fast with the introduction of Cisco CallManager Version 4.0. This mature, IP-based business communications system is the heart of Cisco's video telephony (VT) solution. Along with the new desktop product called Cisco VT Advantage, Cisco CallManager 4.0 adds video telephony functionality to Cisco IP phones. Cisco's video telephony solution enables real-time, person-to-person video sessions to be transparently added to telephone calls and conferences. Video telephony is now simply a phone call.

Instead of working as a standalone system with separate endpoints, administrative systems, and dial plans, Cisco's new VT solution uses the same IP network that carries a company's data and voice communications, enabling real-time videoconferencing and collaboration for an incremental cost of less than US$200 per seat. Cisco CallManager, enabled by Cisco AVVID (Architecture for Voice, Video and Integrated Data), is the software-based call-processing component of the video telephony solution.

"We have finally delivered on the promise of the second 'V' in AVVID," explains Hank Lambert, director of product marketing for Enterprise Call Control at Cisco. "In the past, Cisco AVVID customers could send H.323 video over the IP backbone, but the video applications were never closely coupled with IP telephony."

Cisco VT Advantage

Cisco VT Advantage application software coupled with a Cisco Universal Serial Bus (USB) camera allows a PC co-located with a Cisco IP Phone to add video to phone calls without requiring any extra button-pushing or mouse-clicking. When registered to Cisco CallManager, the Cisco VT Advantage-enabled IP phone has the features and functionality of an IP videophone. With Cisco VT Advantage, call features such as call forward, transfer, conference, hold, and mute are now available with video—and are easily initiated through the Cisco IP Phone.

"By connecting a computer with a Cisco IP Phone and equipping it with a small camera, the PC monitor can work as the phone's video screen," explains John Restrick, software development manager for Cisco CallManager. "Although Cisco VT Advantage harnesses the display power of desktop computers, all calling functionality runs through the phone. The broadcast-quality video images can run at speeds of up to 30 frames per second in a window about one-fourth the size of a typical computer screen."

Restrick believes Cisco's forward-looking transition from time-division multiplexing (TDM) to IP-based PBX systems makes it easy for customers to adopt Cisco CallManager and related video telephony technology. They don't need separate networks for voice and video, and IP phones can be used as endpoints for both types of calls. This makes it very simple to deploy and use the technology. "With Cisco VT Advantage, users have all the functionality of the PBX system," he says. "They can put a call on hold, transfer the call, or press a conference button to initiate a group meeting."

Cisco VT Advantage works with Cisco's midrange and high-end IP phones, including the 7940G, 7960G, and 7970G Cisco IP phones. Video endpoints are configurable from 128 Kbit/s for low-resolution video, to 4.5 Mbit/s for broadcast-quality displays. Two-GHz Pentium processors are required to enjoy maximum resolution video, and 1-GHz Pentium processors are suggested for all video applications.

Cisco CallManager 4.0

Cisco CallManager 4.0 also provides video telephony functionality to IP-based H.323 video endpoints from Cisco AVVID partners, allowing customers to preserve and enhance their expensive videoconferencing equipment without requiring a complete upgrade to existing video equipment. Calls can be made to and from endpoints, regardless if they are audio or video calls. This increases call completion rates, thus increasing productivity.

Calls can also be made to executive desktop and conference room video systems from TANDBERG; the systems are specifically enhanced for use with Cisco CallManager 4.0 and employ a user interface that is the same as a Cisco IP Phone, including hold, transfer, conference, and directory services buttons.

Cisco CallManager version 4.0 also works with Cisco IP videoconferencing solutions such as the Cisco IP/VC 3500 Series, enabling multiple users to be connected into videoconferences simply by pressing the conference button on their phones.

"It's much more convenient now than ever before," says Lambert. "There's no need to preschedule through a reservations center or Website—as you had to do in the past. You just dial the phone and use the conference button to add more people."

Technology Convergence

Evolving technologies have converged to make Cisco's video telephony solution possible: the advent of centralized configuration, management, and call control for scalability and ease of management; unified voice and video dial plans for ease of use; merging voice, data, and video equipment and applications on a single network; and the descending cost of network bandwidth.

Additionally, Cisco recently introduced the Cisco MeetingPlace 8106 Rich-Media Conferencing Solution, an IP-based meeting environment that provides organizations with easy access to secure, integrated, rich-media meetings that combine voice, Web, and instant messaging capabilities. Because MeetingPlace runs "on network," behind the corporate firewall, meeting content is secure. Cisco MeetingPlace also allows users to participate in and control audio and Web conferences through their Cisco IP phones, traditional phones, or network connected desktop PCs. Cisco IP Phone users can easily view schedules, set up audio conferences, attend real-time meetings using soft keys on their phone display screens—even initiate a meeting through the corporate instant messaging client.

Video Revolution

Many corporate networks already have the fundamental infrastructure in place to enable easy-to-use, easy-to-manage, broadcast-quality video to the desktop. Cisco features the latest technology and advancements available with true IP communications today. Enterprises can now take full advantage of their IP networks to deliver enterprise-class business communications that extends voice and video to every user in their organization.

It is a dynamic solution that is designed to grow with new system capabilities. For customers that already have Cisco CallManager, it's a simple upgrade to get started. If they also have Cisco IP/VC video products, they can upgrade not only the call manager, but also the IP/VC Multipoint Conference Unit (MCU), to provide an even tighter coupling of the video infrastructure. Cisco has sold more than two and a half million IP phones to date—most of them with Cisco CallManager solutions—creating a ready market for the new video telephony technology.

"It is a technology whose time has come," emphasizes Lambert. "Many Cisco customers have the necessary bandwidth for video telephony on their local-area networks, and some customers have the infrastructure to transmit video over metropolitan and wide-area networks as well. Typically, you will want Gigabit Ethernet or better for the backbone."

Organizations that have already deployed redundant data centers and have invested heavily in their network infrastructure are immediate candidates for Cisco's video telephony technology. "We're seeing a lot of interest from customers in financial services, telecommunications, healthcare, education, and some sectors of the manufacturing industry," adds Lambert (for more information, see "License to Communicate" on page 36).

Extending the Promise of IP

Cisco CallManager 4.0 scales to support thousands of phones at multiple locations and offers a full set of business telephony features and a complete IP-based applications portfolio including unified messaging, unified communications, IP contact centers, and advanced conferencing services. Small businesses with fewer than 100 users can use Cisco CallManager Express to obtain some of the same benefits.

Running on the Cisco Media Convergence Server (MCS) platform, Cisco CallManager software delivers enterprise telephony features and capabilities to many types of packet telephony network devices. This includes not only IP phones, but also media-processing devices, voice over IP (VoIP) gateways, and multimedia applications.

According to Alex Hadden-Boyd, director of marketing for IP communications in the Product and Technology Marketing Organization at Cisco, VT Advantage is just one aspect of Cisco's complete strategy for IP communications. "If you think of IP as a universal translator," says Hadden-Boyd, "the various devices and applications on the network are starting to merge. PCs, PDAs, pagers, wireless phones, desk phones, and video endpoints are coming together. Users want to integrate not just the devices themselves, but also the desktop applications that run on them. Audioconferencing, videoconferencing, video telephony, Web conferencing—they can all be tied together through IP."

Enhanced Security, Migration, and Interoperability

Important enhancements in Cisco CallManager 4.0 improve security and interoperability. "CallManager 4.0 has many security features that help users verify the identity of the devices and servers with which they communicate, and ensure data integrity," says Restrick, "and with the Cisco IP Phone 7970G, they can also ensure privacy through encryption."

Additionally, Cisco has added digital certificates into each IP phone. When a phone is first connected, it goes through an authentication process. After that, when calls are placed, the setup is authenticated and audio data is encrypted. Cisco CallManager 4.0 also features an intrusion detection system (IDS), firewall, and audit logging through the inclusion of the new Cisco Security Agent, a key component of Cisco's overall security strategy. Cisco Security Agent provides proactive and adaptive threat protection for Cisco IP phones, servers, and desktop computing systems. It brings together multiple levels of security functionality by combining host intrusion prevention, authentication to Cisco IP phones, distributed firewalls, malicious mobile code protection, operating system integrity assurance, and audit log consolidation—all within a single agent package. Cisco CallManager 4.0 customers, as well as Cisco Unity™ unified messaging and Cisco IP Contact Center customers, receive all of these additional levels of safety and protection for their converged networks at no extra cost.

Restrick spearheaded the development of video in Cisco CallManager 4.0 and coordinated the development of conference bridges, PSTN gateways, and Cisco CallManager integration with a wide range of video endpoint solutions. He says Cisco CallManager has native support for Q.SIG and Session Initiation Protocol (SIP) signaling, enabling the Cisco IP communications system to interoperate with new and old PBX systems. SIP is an IP telephony signaling protocol used by a wide range of hardware and software, including the Cisco MeetingPlace conferencing server. Q.SIG is the worldwide signaling standard for PBX systems.

Support for SIP allows Cisco CallManager 4.0 to interoperate with a variety of current and future communications systems, including Cisco MeetingPlace, the Cisco BTS 10200 Softswitch, and a variety of SIP proxy servers. These additions, combined with H.323 voice and video interoperability, make it easy for customers to integrate Cisco IP communications systems with existing voice and video communications equipment.

Freedom to Roam

Hadden-Boyd sums up the advantage of these expanded IP communications capabilities in a single word: freedom.

"I no longer have to worry about how I'm going to communicate at any particular time," she says. "I have a lot of freedom over what medium I use, and when I'm going to use it. It doesn't matter if I'm at home, at the office, or at a hotel in New York. My phone number is associated with whatever communications device I'm using, and Cisco CallManager knows how to deliver a message to me—any time, anywhere—based on the preferences I specify. With IP, users choose what works best for them."

As Hadden-Boyd points out, when Cisco AVVID was introduced in 1999, the advantage was at the network layer. "The primary focus was on transport and its associated cost savings—the cost and productivity advantages of running voice and data over a converged intelligent infrastructure," she explains. "Now that convergence is moving to the application level."

Both the Cisco VT Advantage and the Cisco MeetingPlace solutions deliver on Cisco's promise of a rich-media communications experience. "This is much more than just video to the desktop," Restrick concludes. "We're introducing a cohesive system for video communication. We have integrated access to the PSTN and provided simple-to-use conferencing and support for legacy systems—all with the scalability and manageability you expect from your phone system." ▲▲

TOP TEN TIPS

FOR GUIDING
A SUCCESSFUL
IP TELEPHONY
IMPLEMENTATION.

MIGRATING TO IP TELEPHONY?

BY
STEPHANIE
L. CARHEE

OFTEN WHEN AN ORGANIZATION considers change that will impact every employee—such as an enterprise-wide IP telephony implementation—the process tends to focus on hardware, software, and getting the technology up to speed as quickly as possible. However, a company's infrastructure is composed not just of hardware and software, but also of people. The successful conversion to IP telephony does not rest solely on viability or reliability. It requires a careful combination of the right products, people, processes, tools, services, best practices, and methodologies—all working in concert.

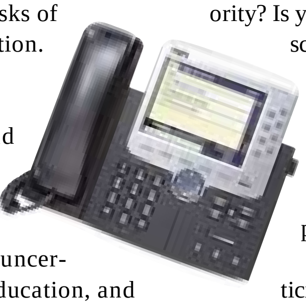
While the needs of every enterprise are different, some things are universal. Planning, communication, teamwork, and understanding your users' requirements are as important as technical expertise. With this key objective in mind, I have compiled the following top ten tips for project managing an enterprise-wide IP telephony implementation. They are not meant to tell you how to technically architect your network, but to share best practices gleaned from Cisco's own experience as well as customer engagements with phased migrations to a converged voice and data network. If your company is in the planning stages of an IP communications implementation, read on.

Tip 1. Build a Cross-Functional "Tiger" Team

The greatest up-front contributor to a successful, large technology migration is building a cross-functional team that not only has the requisite skills and technical expertise but represents users in every area in the organization impacted by the implementation. This team is responsible for ensuring rapid delivery of the migration that optimizes company investments. At Cisco, we called this group the "Tiger Team."

Key members of the team include an executive program sponsor and steering committee composed of organizational stakeholders; a project Tiger Team lead; technology experts; security specialists; and subject matter experts in the areas of design and engineering, support, finance, and project management. When global or multinational theaters are involved, include team leads for each theater who will represent the needs of that location and user community.

After skill sets are identified and all representatives chosen, this well-represented team should start off the implementation by clearly defining the objectives and overall goals of the project, and identifying the tasks necessary to achieve those goals. Also begin defining the change management process, at-risk factors, and problem escalation challenges, which will minimize the risks of integrating an enterprise-wide IP telephony solution.



Tip 2. Get Your Users On Board

Resistance to change is normal and should always be anticipated. Managing user expectations will be paramount to making the process run as smooth as possible. One key way to achieve this is to take away the mystery and uncertainty among the individuals affected through education, and open, honest, and frequent communication with the stakeholders. Create a plan that gives you the ability to be flexible and proactive. Anticipate the glitches and constantly improve the process along the way, tailoring it to the specific needs of the stakeholders and the users they represent.

In addition to managing users' expectations, an IP telephony implementation typically will require significant business adjustments, staff training and education, and some redesigned business processes and fundamental shifts within the organization. All of these changes must be identified early and continually managed, and change initiatives coordinated and integrated in a timely fashion.

Your change management plan should be created only after change impacts have been identified and organizational change readiness has been assessed. Consider first the impact change will have on employees—paying close attention to details and being considerate of the timetable (ensuring that the implementation cutover doesn't take place during your company's fiscal-quarter close or other critical event, for example). And *do it right the first time* so that when users experience the change, the effect is minimal and expectations are met.

Managing change involves four important components: Sponsorship, Resistance, Cultural Alignment/Communications and Skills. All team members should strive to understand the process in which change occurs, and incorporate the following recommendations into an effective organizational change plan:

- Know the tools and methods that can be used to analyze and manage change
- Plan and implement proactive change management principles
- Understand the nature and impact of change in the program environment
- Manage the negative implications of change
- Realign expectations
- Build commitment
- Drive cultural acceptance

Tip 3. Do Your Homework

Corporate culture is often defined as "the way we do things around here." Culture builds a common language and brings people together, enabling them to work toward a shared goal. Understanding and working with your organization's culture is critical to successfully implementing new technology on a large scale. Does your company encourage risk taking? Is change incorporated often, and does the company embrace it? How has change been introduced and institutionalized in the past? Was the process successful or fraught with problems? Is new technology welcomed or resisted? Do employees solve problems in a team environment? Is communication a top priority? Is yours a virtual company with telecommuters or employees scattered across the globe? What have previous technology deployments taught you about how users prefer to be trained? All of these factors are part of your organizational culture and can influence your ability to integrate a new solution. Take the time to know your users. Do your homework, capitalize on what has worked in the past, and learn from the mistakes of others.

Equally important, it's essential that you have the participation and cooperation of all Tiger Team members from the outset. A planning workshop will help you to educate and rally cooperation among the team, as well as ensure that the initiative stays true to the business requirements of your organization and meets implementation objectives. The team should work together to plan project deliverables, address solution capabilities, define hardware, software, and security requirements, assign third-party implementation services, identify the project critical path and milestones, and outline the migration strategy. There is plenty of ground that should be covered, and you can use the "IP Telephony Migration Questionnaire" on page 51 to get your project team thinking and collaborating together.

Tip 4. Ensure That User Requirements Drive Design Requirements

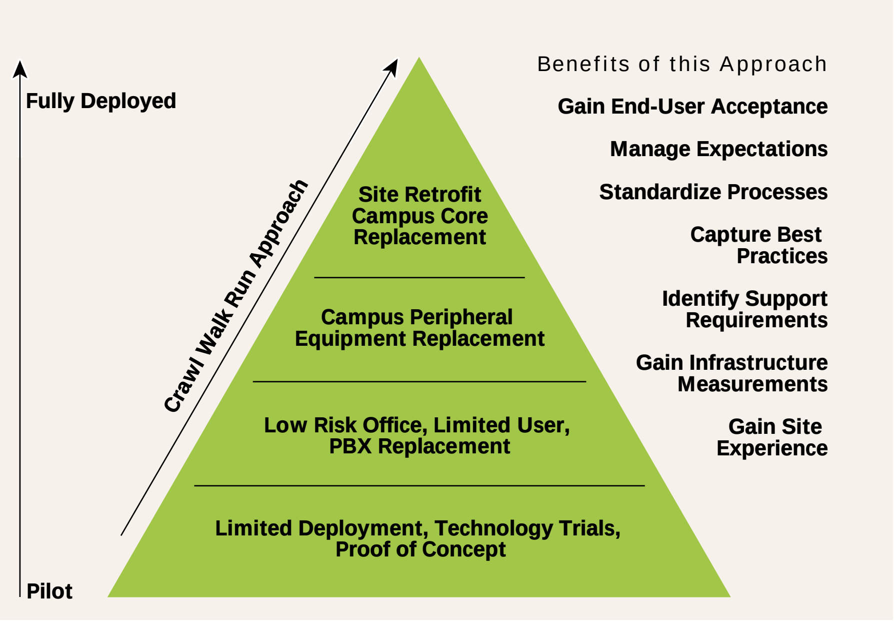
Consider developing a "Voice of the Client" program that consists of client-targeted surveys and focus groups to benchmark and track user-preferred services, products, solutions, and features. Use the survey as a tool to identify critical phone features, validate key business needs, gauge risk tolerance and user discomfort, and identify key functionalities that are paramount to your business. You can also use the survey as an opportunity to incorporate features of the new IP telephony system and to help determine the priority of which features should be enabled.

Survey results provide the design and engineering team with a "report card" that validates their concept of the new design.

Missing key design elements are a critical mistake that can be avoided by listening to your users, conducting traffic analysis, performing a network audit and readiness assessment, understanding how the technology will impact your current infrastructure, and familiarizing yourself with the new technology.

And, as daunting and overwhelming as all this may sound, remember that IP telephony is simply a new application running on your current network, not an entirely new network. Therefore, knowing how your users use the system today, aligning their goals with the design requirements, and setting the right expectations will go a long way in making sure that you design your network right the first time.

MIGRATION IMPLEMENTATION APPROACH


Fully Deployed
Pilot
Crawl Walk Run Approach
Site Retrofit Campus Core Replacement
Campus Peripheral Equipment Replacement
Low Risk Office, Limited User, PBX Replacement
Limited Deployment, Technology Trials, Proof of Concept
Benefits of this Approach
Gain End-User Acceptance
Manage Expectations
Standardize Processes
Capture Best Practices
Identify Support Requirements
Gain Infrastructure Measurements
Gain Site Experience

AT YOUR PACE: Adopting a Crawl/Walk/Run approach will help you manage user expectations, identify critical support and infrastructure requirements, build on your knowledge gained, and overall minimize the risk of your technology implementation.

Tip 5. Crawl First, Walk Proudly, and Run Aggressively

Your implementation strategy should allow you to progressively go faster as your experience levels become more efficient (see figure). You don't want to go too fast or, conversely, too slow. The number of employees, complexity of user requirements, size of the campus, and how widely all are dispersed will, of course, affect your migration strategy. Like most organizations, you are not dealing with a static environment. There will always be employees changing locations, getting hired or leaving, or exercising their mobility working on the road, at home, in the field, and places other than their office desktop. To accommodate this ever-changing environment, develop a migration strategy that takes into account all of the variables that can change, alter, or otherwise affect implementation of your new converged voice and data network.

Make sure no one falls through the cracks by dividing your migration into user- and/or site-defined categories. Your categories might be, for example, new employees; existing employees who are moving to a new location; buildings coming online (greenfields); retrofit of existing buildings; merger- and acquisition-related facilities; or buildings with upcoming PBX lease renewals.

And, as noted, don't forget to take the time to learn from your mistakes, obtain feedback, build proven processes, and create standards for the entire team to adhere to. Minimize your migration risk by starting in the lab, developing your proof of concept, and allowing time for training and practice. Follow that success with implementation in a non-critical field office. Then, apply what you've learned and start to build momentum by moving more aggressively with a campus-wide implementation.

Tip 6. Follow the 80/20 Rule for Implementation

When it comes to actual implementation, the success of your IP telephony migration will depend on several considerations: proper planning, creating consistent standards, identifying at-risk factors, having a ready backup/backout plan, customer service, doing the prep work up front, applying best practices, paying attention to detail, and automating as much of the process as possible. Of all these important factors, planning weighs most heavily. In fact, a winning formula for migration success consists of 80 percent preparation and 20 percent installation. Quite simply, if you focus on your plan first, the implementation will go a lot smoother.

The fruit of managing several implementations, Cisco's "IP Telephony Steps to Success Engagement Guide" is a knowledge management portal designed to help Cisco IP telephony partners in creating their own implementation plans (cisco.com/go/stepstosuccess, Cisco.com login required). Following is a condensed version of the high-level steps that should be considered when beginning and completing the implementation phase:

Step 1. Facilitate Implementation Planning
Step 2. Hold Implementation Planning Meeting
Step 3. Define Project Monitoring and Control
Step 4. Develop Status Reporting Structure
Step 5. Begin Site Preparation
Step 6. Conduct Install and Configure
Step 7. Manage Test and Acceptance
Step 8. Deliver Knowledge Handoff
Step 9. Ensure Customer Acceptance
Step 10. Complete Closeout

A comprehensive depiction of the key implementation steps, the "Road to IP Telephony" mini poster, is available to download free at ciscopress.com/1587200880.

Tip 7. Ensure a Successful Day 2 Handoff

A successful Day 2 handoff requires a well thought out support plan (Day 2 is defined as the time period immediately following cutover of your new IP telephony solution). Four critical components are required to enable efficient operation and responsive support of your converged network: the support team, support processes, support services, and support tools.

Support Team. The primary goal of support is to have all issues resolved quickly and effectively. You need the right mix of people in place at the right time to resolve the entire spectrum of issues that can arise in a converged network environment. To streamline this process, consider creating a cost-effective, three-tiered internal structure to resolve issues based on the type of problems that arise matched to the skill set required to resolve them. Escalation is based on severity and complexity of the issue. Easy-to-solve or repetitive issues, such as IP phone resets and user access passwords, are handled by Tier 1. Tier 2 tackles more complex problems such as software issues, LAN support, and data problems. And Tier 3 requires the involvement of individuals responsible for the design and engineering of the IP telephony solution.

Support Process. Resist the temptation to completely reinvent your support model with each new application, a mistake often made during large-scale technology implementations. While the converged support model requires collaboration among multiple groups who are likely unaccustomed to working together, you should still consider and take advantage of much of your existing support processes.

Support Services. Many companies do not have the resources required to adequately plan, design, implement, operate, and optimize (PDIOO) a converged communications environment. When making the investment in an IP-based network, organizations need to look closely at their ability to provide all the required services and support parameters. Key elements for implementing, supporting, and optimizing IP-based communications consist of end-to-end PDIOO capabilities, expert internal and external resources, cutting-edge management tools, knowledge management and transfer, and global coverage.

Support Tools. Attentive management and monitoring of your new network will help to catch and resolve many problems before they become visible to users. With the right support tools, the network can maintain the highest level of reliability and stability, providing increased performance

IP TELEPHONY MIGRATION QUESTIONNAIRE

Use the following questionnaire in your team planning workshop to jump start migration strategy discussions and identify key areas that need to be addressed in your converged network implementation. This abbreviated list is excerpted from the upcoming Cisco Press book, *The Road to IP Telephony: How Cisco Systems Migrated from PBX to IP Telephony.*

PLANNING

How will you determine if your current network is ready for convergence?

What specific hardware, software, and infrastructure changes are needed?

What is your company’s security policy? Determine how the new network will adhere to this policy.

What experience, tools, and methodologies are required to take advantage of converged technologies?

How will IT staff learn to manage the converged IP network? Who will manage it?

How will the new technology impact end users?

Who are the stakeholders companywide? Which groups absolutely require zero failure rate?

Have you assembled a ”Tiger Team” and outlined their core requirements for the design? Is there a chart of roles and responsibilties?

Has an IP telephony assessment been conducted?

Have all leased PBX equipment and lease expirations been identified?

What are the risk factors? Is there a governance model to address and manage the risk factors?

What is your content management plan? Are there naming convention standards?

Are local site managers included in the planning discussions?

Is there a plan in place to minimize customer impact?

DESIGN

What core functionality is required by key stakeholders/business units?

Who are the high-risk users for whom failure is not an option? Have solutions or workarounds been established?

Have you defined the ”must-have” functionality for the network design? Are there any unusual considerations the design should address?

Are the implementation and support teams part of the design strategy? (They should be.)

Will the design requirements meet users’ expectations? Has a survey been conducted?

Did you compare the PBX dump with your new design? Are there gaps?

Have you identified all the existing applications that will integrate with the new IP telephony solution?

IMPLEMENTATION

Who is the champion/sponsor of the migration? Are reasons for the conversion clearly articulated?

Is your company’s culture factored into the migration plan?

What are the users’ expectations? How will users be trained?

Have you identified a migration plan for critical phone users?

Is there a site escalation path if something goes wrong during cutover? Are there backout procedures?

What is your selection process for the pilot site? Have acceptance criteria been identified?

OPERATION

Have you created customer service standards for all deployment members?

How will you capture lessons learned and ensure that other sites benefit?

Will you require spares at each site? Is there a resource for allocating phones in a pinch?

What monitoring and troubleshooting tools will you need to manage the new network?

Has a PBX decommission plan been identified? Will the port reduction be monitored to ensure lower costs?

Do you have a policy for managing analog line disconnects?

Do you have a solid change management process in place?

Do you have a system for capturing FAQs to be used for the support team?

and availability. The five key functional areas of the network must be managed to ensure the highest levels of availability: fault, configuration, accounting, performance, and security management.

Tip 8. Keep Your New Network Clean

Most large enterprises have hundreds of lines and circuits that, through the years, have either been forgotten about or are simply unused. While this tip isn't meant to cover all the technical considerations required to "clean out" your network, it's an important reminder to view your IP telephony implementation as an opportunity to clean out your network to start anew, as well as clean, groom, and prepare the IP infrastructure. So, when the implementation team begins the conversion to IP telephony, remove as many unused lines off the PBX as possible, and only convert those lines that were proven as valid. Conduct a final cleanup at the end of the conversion to ensure that the implementation team has ample time to carefully review and trace all unidentified analog lines and circuits. Take steps to verify that business-critical lines aren't removed, and make it a point to only migrate what you use, not what you have, so that you can help to keep the network clean.

Tip 9. Plan for PBX Lease Returns

At the time of implementation, you might have equipment that is leased, which meant that your IP telephony implementation schedule was largely dictated by the PBX lease return dates. To ensure that the massive effort of returning large quantities of leased equipment is organized and that items are returned on schedule, the team leader responsible for the retrofit cleanup should enter all PBX leases into a spreadsheet and develop a project plan to keep the returns on track. Carefully match the equipment list on the original lease agreement to the inventory being returned, create a box-level inventory list, and get a signed receiving list from the vendor.

In addition to managing the return of all leased equipment, there is also the process of removing all ancillary solutions and systems that are tied to the main PBX. The process of completely decommissioning your main PBX will take longer than you expect; therefore, assemble a project team to address the removal of all applications still running on it.

Tip 10. Look Back, Move Forward, and Prepare for the Future

Whether an IP telephony implementation involves 200 phones or 20,000 phones, careful and comprehensive planning, communication, teamwork, and knowing where the "gotchas" are hiding will divert problems before they even arise.

STEPHANIE L. CARHEE

STEPHANIE L. CARHEE is a senior project manager with Cisco's IP Communications Services Marketing team and author of *The Road to IP Telephony: How Cisco Systems Migrated from PBX to IP Telephony*. Prior to her current role, Carhee was an IT project manager for voice services in the Strategic Program Management group, and was team lead for Cisco's migration to IP telephony, the largest deployment of its kind in the industry to date. She can be reached at scarhee@cisco.com.

TAKE A PAGE FROM THIS BOOK

The Road to IP Telephony: How Cisco Systems Migrated from PBX to IP Telephony (ISBN: 1-58720-088-0), from Cisco Press, provides a roadmap for your IP telephony migration that includes deployment, installation, management, and troubleshooting guidance from Cisco experts. Written by Stephanie Carhee, the book's focus is not on technology but on the planning and business processes associated with a large IP telephony implementation. Included are more than 200 best practices and lessons learned from Cisco that every IP implementation team lead should know.

The Road to IP Telephony will be available in June 2004. For more information, visit ciscopress.com/1587200880.

OK, you've almost arrived. You can see your destination and it is a fully converged voice and data network with all users migrated to IP telephony. Before celebrating, however, there are still a few important items that require your attention. You still need to be ready to address how to prepare your network for the future.

Change management will be the toughest process to maintain once your new network is in place, but not because of routine changes or software upgrades. Maintaining a strict, yet manageable and scalable, process will be key to your success. Not only will your methods and procedures require a solid execution plan, but so will the standards by which you communicate the plan. Eliminate as many unknowns as possible by documenting your procedures, capture and incorporate lessons learned, and optimize your change management process. Make the commitment to continually support your new, dynamic network by reevaluating contingency plans often, conducting ongoing audits of network performance, incorporating new features through software upgrades, and reexamining the contract services that protect, monitor, and support your network.

To prepare for the future, you must embrace being prepared for new IP telephony applications. As applications become available, a system must be in place to analyze the technology for applicability, test it for feasibility, provide an adoption position, and ensure that all teams are involved, in agreement, and ready to reap the benefits that will come from rolling out another new IP communications application.

◆ ◆ ◆

The author wishes to thank Debbie Hart for contributing to this article. ▲▲

Switching to Layer 3

New network opens doors to advanced technologies at Duke University Medical Center.

BY GRANT ELLIS

THE CAMPUS OF DUKE University Medical Center (DUMC) in Durham, North Carolina, is a world of its own—home to one of the foremost hospitals in the US, a clinic that treats 700,000 patients a year, a highly regarded medical school, and research facilities that attract more than US$400 million in grants. The Medical Center (mc.duke.edu) serves as the hub for a regional network of health services, called the Duke University Health System, that includes clinics, care providers, two community hospitals, home health, and hospice. This is a growing healthcare system with specialized communications needs.

HUB OF ACTIVITY: Duke University Medical Center is home to one of the foremost hospitals in the US.

DUMC originally created its Common Services Network (CSN) to provide communications services to the hospital campus and the medical center buildings. The CSN was a 100-Mbit/s fiber distributed data interface (FDDI) ring consisting of 22 hubs with 10-Mbit/s Ethernet shared interfaces. Each interface served as an uplink to a local closet with multiple hubs.

“We had what I would call one big LAN,” says DUMC Associate Chief Information Officer Rafael Rodriguez. “It was a flat network, where all traffic was seen by everyone, and any malfunction or misconfiguration could affect the whole operation.”

Growth and Changing Technologies

Rapid growth steadily magnified the shortcomings of this unrouted network. In addition, two community hospitals, as well as off-campus clinics, needed to be added to the CSN. By 2000, there were 35,000 nodes on the network. Faculty, physicians, and researchers became frustrated with the network’s inability to transfer high-quality digital medical images in a useful time frame. New network-based technologies were available to help DUMC carry out its educational, research, and patient care missions, but the network lacked the bandwidth to accommodate them. And reliability had become a major issue.

“At any given time, there were 10,000 MAC addresses registered on this network,” says Tim Bell, a DUMC systems analyst. “Needless to say, it was barely running. If any little thing went wrong, the network went down and everybody had to go back and figure out how to restart processes.”

Adding to the high cost of management was the large number of protocols the CSN dealt with. In addition to TCP/IP, network users were working with IPX, AppleTalk, SNA, DECnet, and others. Also, there were two Class B IP addresses under the Duke domain, but addresses were allocated to them more or less randomly. All these factors made it a necessity for DUMC to migrate to a more effective networking technology.

Making the Choice

"We sat down with our senior leadership to evaluate our infrastructure," says DUMC Director of Networking Nhan Vo. "We invited leading network technology companies to talk to us. In the end, we chose Cisco."

Cisco was selected because a successful partnership already existed between Cisco and Duke on the academic side, where Rodriguez had worked prior to assuming system and networking responsibilities for the Medical Center. DUMC's academic campus had already moved to a segmented network using Cisco routing technology. Although the academic and health networks called for different topologies—the academic network was necessarily more open and accessible than the health network system, which functioned more as an intranet with greater security requirements—Duke saw advantages in standardizing on Cisco as the primary networking vendor.

"As we considered who we should partner with, we looked at Cisco's reputation in the networking environment," says Rodriguez. "They also had a facility not far away in RTP [Research Triangle Park] and had approached us about forming a strategic relationship."

> "We're using more automated network management tools that help us to be proactive as well as to react quickly to events. So with basically the same staff, we're able to accommodate a growth in users and increase the availability and reliability of the network."
>
> —RAFAEL RODRIGUEZ, CHIEF INFORMATION OFFICER, DUKE UNIVERSITY MEDICAL CENTER

Continues Rodriguez, "We developed an excellent relationship with Cisco all the way from the executive level to the account rep. We had biweekly meetings with the account executive management at which we discussed where we wanted to go and the benefits that went along with the choices we could make. That relationship has continued to flourish."

Six-Month Planning Cycle

With Cisco established as the vendor of choice, a collaborative team that included Enterprise Communication Infrastructure (ECI), the Duke University Health System (DUHS) information group; Cisco network engineers; and other vendors was formed.

"We felt we needed to move to a routed, segmented network," says Rodriguez, "and we wanted to think through the other issues that faced us, including security zones, patient and financial confidentiality, and HIPAA [Health Insurance Portability and Accountability Act] compliance."

Vo and his colleagues built a Cisco technology-based switched network that would fill all current needs and scale to meet any future challenges. In 2001, Bell was commissioned to develop the detailed network design for implementation. After six months of planning and design, Duke was ready to begin migration to the routed Layer 3 Duke Health Enterprise Network—a high-density, high-performance WAN that could scale reliably and cost-effectively to deal with growth and emerging technologies.

The first phase of the implementation began in March 2000. ECI installed the first four Cisco Catalyst® 6509 gigabit switches as the new backbone, using the CSN's existing fiber-optic cables. This new throughput core increased the backplane transmission rate from 800 megabits to 32 gigabits and instantly eliminated the convergence and scalability problems of the old Layer 2 network.

Moonlight Migration

The second phase of migration was the segmenting and readdressing of the network—a daunting task. "My first thought was, 'Wow, what am I doing?'" says Rodriguez. "And I wasn't even doing the hard part. I was thinking about the staff. I'm glad they're such dedicated people."

ECI designated each of the 400 closets as a separate virtual LAN (VLAN) to give workgroups of up to 200 users 10/100 Mbit/s per outlet and a gigabit uplink to the core. TCP/IP is the only transport protocol on the network. All other legacy protocols were eliminated. Dynamic Host Configuration Protocol (DHCP) provides client mobility across the network and reduces the labor cost of IP address management.

The migration was completed in just 56 weeks, with some 64,000 IP addresses deployed in more than 200 IP routed segments.

The new network, now known as the Duke Health Enterprise Network, includes a LAN, a WAN, and an extended WAN. The LAN, which comprises multiple Cisco Catalyst 6513 switches, connects Duke Hospital North, on-campus clinics, and more than 40 research buildings on the campus. Each of the Catalyst 6513 switches is equipped with a Supervisor Engine 720 module that incorporates ASIC-based Cisco Express

Forwarding technology, which supports up to 720 gigabits of throughput on the passive fabric backplane and forwards more than 400 million packets per second.

The WAN provides gigabit bandwidth to nine campus buildings in the Durham area and the two Duke community hospitals. The extended WAN provides access over T1 and T3 links to more than 80 remote clinics throughout the state. It can scale cost-effectively to accommodate a large number of additional connections.

Instant Gratification

The obvious immediate benefit of the migration, apart from faster downloads, was sheer dependability of service.

"We now have a significantly more reliable, more secure network," says Rodriguez. "And when issues do occur, they're isolated to specific sections of the network so we can quickly pinpoint them. We're using more automated network management tools that help us to be proactive as well as to react quickly to events. So with basically the same staff, we're able to accommodate a growth in users and increase the availability and reliability of the network."

There are no premigration statistics available to quantify the difference the new technology has made in network performance, but Vo sees a dramatic change. "How do you quantify user satisfaction? It used to be that anytime a user went to the Internet to download a lot of images, you could see the progress of the download, and hear people complaining about its impact. Now all users have their own Gigabit Ethernet access. They can download all day long without having a negative affect on anyone."

Continues Vo: "We used to have a 20,000 broadcast domain; now we've segmented out to 400 VLANs, and each has fewer than 200 devices. We used to have 10-Mbit/s share up to the local closet for the user; now we have Gigabit Ethernet. We used to have 10-Mbit/s Layer 2; now we have gigabit Layer 3."

Bell measures the new network's reliability by the way calls to the help desk have changed. "When somebody expects something to work all the time, it's a reliable service," he says. "Before the migration, they wouldn't call in unless the network was pretty much dead for a couple of hours. Now when there's a tiny blip people will call and say, 'What's wrong? What happened to the network?'"

DUHS is now installing equipment that will give the network the redundancy it needs to protect key processes, including access to patient records. The redundancy already includes multiple paths across the WAN. Soon it will include redundant Cisco Catalyst 6509 switches at the core, a redundant distribution layer, and increased Layer 3 firewalling protection. The design incorporates the full range of Cisco's resiliency and redundancy features, including Per-VLAN Rapid Spanning Tree Protocol (PVST), Hot Standby Router Protocol (HSRP), and routing failover techniques, as well as Cisco SAFE blueprint design guidelines.

Enabling New Technologies

DUHS's new level of network service has opened the door to a host of advancements that were not supportable with the old technology. Many network-based projects have now been funded and are moving ahead on the strength of faster, more reliable network service. Technology vendors had been patiently waiting for the migration to offer products that were network-limited. One example is a recent major upgrade of compute systems. Another is access to high-quality digitized medical images such as MRIs, sonograms, and CT scans with their supporting patient records. Images are available not only to radiologists and others on the network, but also to referring physicians, who can access them securely with a Web browser from any location over a VPN.

"The migration enabled the movement of images to happen," says Bell. "Before, people could only move very small images that were for the most part unusable. After the migration they could pretty much move images that met the specifications the physicians require for their duties."

Other new applications enabled by the migration are now coming online. DUHS is piloting wireless technology from Vocera that enables instant voice over IP (VoIP) communication across the network. A physician wearing a Vocera Communications Badge at a patient's bedside will be able to speak the name of a colleague and be instantly connected, accelerating diagnosis and treatment and reducing the patient's hospital stay. This is part of Duke Hospital's expansion of its wireless network to give faculty and staff greater mobility while raising the level of patient care.

"Electronic information technology is enabling us to correlate activity from genomic research to clinical studies to highly personalized patient care," says Rodriguez. "It is producing patient care that is more proactive." ▲▲

FURTHER READING

- **"Putting the IP in Hippocrates" [*Packet*® Third Quarter 2003]: cisco.com/packet/162_7b1**
- **"Deployment Diary" [*Packet*® First Quarter 2004]: cisco.com/packet/162_7b2**
- **Cisco SAFE: cisco.com/go/safe**
- **Cisco Catalyst 6500 Series: cisco.com/packet/162_7b3**

Are You Business Ready?

Protect, optimize, and grow your business through system networking. BY GAIL MEREDITH OTTESON

A NETWORK DOES MORE THAN CONNECT users with applications—it's the foundation for applications and technologies that enhance productivity—the hundreds of processes that facilitate business relationships; track manufacturing, inventory and financials; assure product quality; and increase customer satisfaction. In a typical enterprise, the network encompasses a data center, campus, branch offices, WAN and mobile workers and teleworkers. This highly distributed infrastructure should support secure business communications and processes, empowering users to attain optimal productivity and organizations to accelerate business growth.

Is Your Network *Business Ready*?

"Networks should no longer be viewed merely as a means of connectivity," says Pierre-Paul Allard, vice president, Worldwide Enterprise Marketing at Cisco. By taking a systems-level view and adding intelligent capabilities to the network, organizations can implement resilient networks that allow their business to quickly adapt to changing requirements, rapidly and securely enable new and emerging applications, and streamline processes through improved access to information and communications."

By shifting their focus from individual boxes to an integrated systems approach, IT managers can make their networks more "business ready." This means taking a planned, architectural approach instead of backend, point product integration.

However, enterprises often purchase networking gear based on "speeds and feeds" or price, trusting that standards compliance can assure interoperability. "But standards don't define how systems work," says Glen Fisher, business development manager in the Enterprise Solutions Marketing group at Cisco. "Standards are a foundation, but you really address bigger issues with an architectural approach. It gives you the most value from your IT investment. That is why it is important to work with a vendor that can design, test, and implement a complete solution, not just make pieces of one."

Enterprises with point-product networks have to spend more time performing systems integration. They must also train staff on more platforms, and spend more time troubleshooting and planning. Add to this the cost of multiple sets of spare parts and the complexity of multiple management systems, and the result is an expensive network with limited flexibility, which slows efforts to adapt the network to changing business conditions.

"The decision to use Cisco for our enterprise architecture was based on technology, future vision, and support services for the entire end-to-end network," says Lots Pook, chief technical officer at Exempla Healthcare. "Cisco offered critical technology for Exempla's immediate needs and its long-term goal of securely delivering accurate patient information to caregivers, regardless of location. The Cisco sales and support staff worked closely with Exempla to understand those requirements and determine how Cisco products could best meet Exempla's long-term needs. We were impressed with the way the Cisco team sat down with us, rolled up their sleeves, and helped us design and architect the business ready solutions that we have today."

A business ready systems strategy best supports business agility because it offers consistency, advanced intelligence, and service integration throughout the entire enterprise, allowing users to be more productive and respond faster to market opportunities. Enterprises that are business ready use the network to *protect*, *optimize*, and *grow* their business.

Protect the Organization

A Business Ready systems strategy uses many means to protect systems and information, such as scanning endpoints to verify their identity and antivirus software status before allowing them access to enterprise resources. Defense-in-depth security measures, such as intrusion detection and prevention systems and firewalls, protect resources. The network can secure business communications with data/voice encryption. A Business Ready strategy also supports regulations such as those under the Health Insurance Portability and Accountability Act (HIPAA) in the US, which requires that medical records transmitted through a network remain private. The network assists regulatory compliance with technologies such as virtual private networks (VPNs). The network can also increase business resilience through highly redundant platforms and software features that provide transparent failover to mirrored or backup systems.

Optimize Productivity

Business ready enterprises can increase worker productivity through improved network access and better performance, wherever workers are. "But productivity is not about access speeds—it is about accessing applications and information and being able to act on them when and where you need to," says Fisher. The network can also support collaboration among geographically dispersed workforces. Cisco IP communications solutions, such as the new Cisco MeetingPlace 8106 Rich-Media Conferencing Server and Cisco Video Telephony Advantage for IP phones, improve information exchange, fostering greater collaboration among distributed project teams (see "The Video Advantage," page 36). On the backend, integrated equipment provides economies of scale for end-to-end management of Cisco networks, improving operational efficiencies and reducing complexity for IT staff, optimizing their own productivity. This is a critical benefit, because analysts estimate that up to 70 percent of IT staff time can be devoted toward maintaining IT infrastructure. Reducing this cost releases time and funds for new IT initiatives that create value.

Grow the Business

The final test of business readiness is how well the network and other IT systems interact to support business strategies, increase business effectiveness, improve customer relationships, and accelerate business responsiveness, which all contribute to revenues. Perhaps the most striking example of using the Cisco Business Ready strategy to grow the business is in the data center.

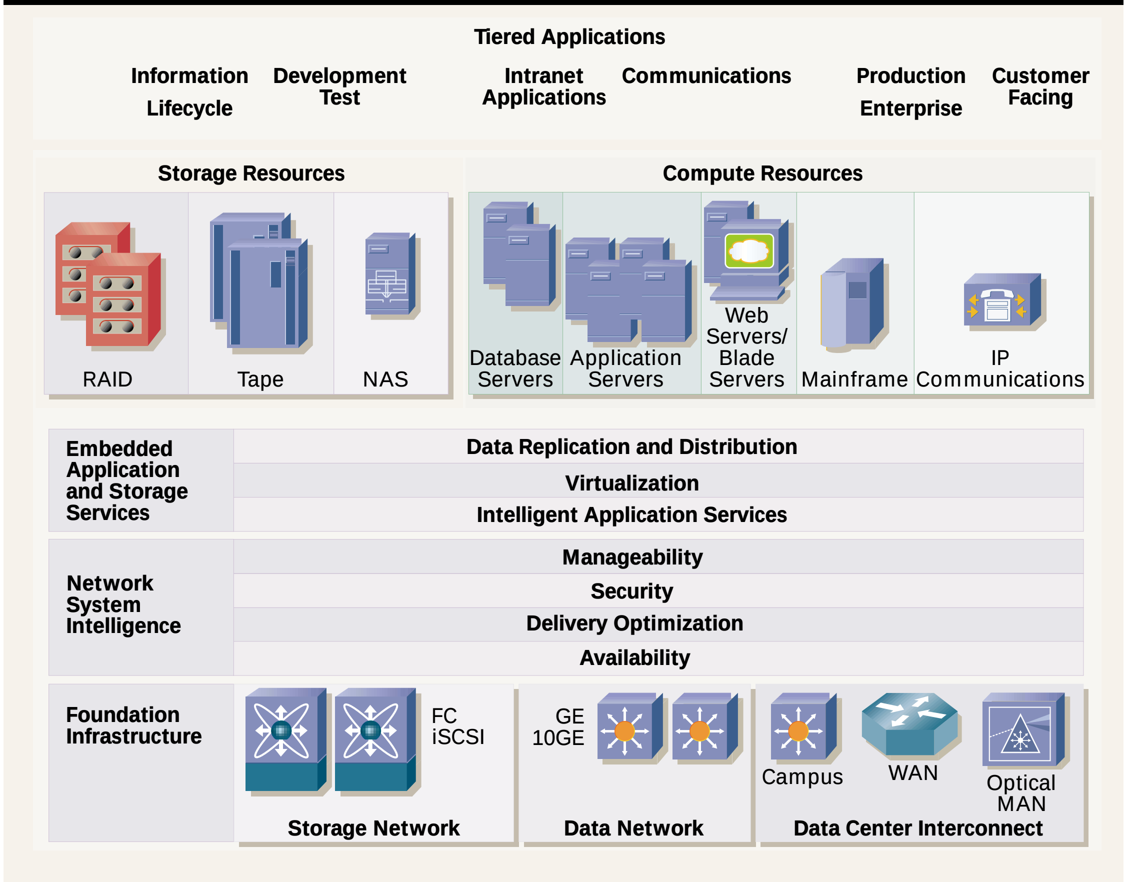
Cisco Business Ready Data Center

As the nerve center of IT, the data center houses critical applications that make business operate. However, during the rapid growth of the 1990s, data center managers focused more on time to deployment than on protection and optimization, and the typical result was complex, disparate infrastructures with limited flexibility and operational inefficiencies. Multiple isolated application environments, each with separate servers, storage, and networks, were optimized for the particular requirements of each application, yet were difficult to manage and slow to change.

Today's trend toward data center consolidation to reduce total cost of ownership (TCO) calls for close collaboration between data center and network managers to develop a network architecture with intelligence that enables rapid, secure, and reliable deployment of resources and applications.

"Successful data center consolidation begins with an

BUSINESS READY DATA CENTER ARCHITECTURE



READY AND ABLE: The Cisco Business Ready Data Center consolidates network resources and provides end-to-end intelligent services, thereby enabling enterprises to protect, optimize, and grow their business.

architectural approach to the network," says Jonathan Gilad, solutions marketing manager for Data Center Networking at Cisco. "Data center managers can tie everything to a common network infrastructure that is much easier to manage, and can integrate intelligent services, such as security and application optimization, to protect and enhance each application environment."

The Business Ready Data Center lets enterprises transform their data centers into secure, optimized, agile environments that closely align resources with today's business goals and readily adapt to future trends such as on-demand computing and service-oriented systems. This initiative provides comprehensive solutions, architectural vision, roadmaps, partnerships, advanced services, and support. It includes reference architectures, proven best practices, and configuration templates. Easily upgradable, modular products let enterprises quickly embrace new technologies and integrate intelligence into the network. Management tools facilitate end-to-end service deployment with automated configuration templates and greater device and traffic visibility.

The Cisco Business Ready Data Center architecture has three tiers:

- **Foundation infrastructure** includes the intelligent IP network infrastructure, intelligent storage networking, and data center interconnect
- **Network system intelligence** includes security, delivery optimization, manageability, and availability
- **Embedded application and storage services** include data replication, virtualization, and intelligent application services

Data Center Foundation Infrastructure

Data and storage networks interconnect and provide access to data center resources. The intelligent, switched IP data network is comprised of Cisco Catalyst® switches, which offer the rich feature sets of Cisco IOS® Software in a range of modular and fixed-port platforms. For optimal value, Cisco recommends the Catalyst 6500 Series Switch, which features high-density 1-Gigabit and 10-Gigabit Ethernet, intelligent services modules, and virtualization capabilities for scalable, secure and reliable application deployment. The modular platform supports incremental upgrades for flexibility and growth, and is easier to deploy and manage than multiple switches and appliances.

In the storage network, Cisco offers the MDS 9000 Series Multilayer Switch, which supports a range of storage protocols (such as Fibre Channel, FICON, and iSCSI) and advanced security and virtualization features. These switches enable scalable storage-area networks (SANs) that can be shared by multiple application, server, and storage resources.

Between data centers, Cisco multiservice metro optical and WAN solutions offer cost-effective, high-capacity infrastructures that support business continuance through applications such asynchronous and synchronous replication.

Network System Intelligence

"Data center managers can realize the true value of the Cisco approach when they consistently integrate intelligent services across the foundation infrastructure," says Gilad. Available as software features and as integrated service modules for Cisco Catalyst 6500 and Cisco MDS 9000 Series platforms, these services include security, delivery optimization, manageability, and availability, enabling service levels not possible with independent appliances. For example, service modules enable interaction between the load-balancing function of the Cisco Content Switching Module (CSM) and the security features of the Firewall Services Module (FWSM), illustrating Cisco's vision of intelligent networking and providing system-level solutions to customer problems (see the sidebar, "The Role of Intelligent Networking," page 60).

Embedded Application and Storage Services

The Cisco Business Ready Data Center embeds application and storage services for close interaction of the network with attached resources. The network can centrally host third-party partner applications such as data replication and storage virtualization, and enable future intelligent application services.

Data replication services in the storage network support mirroring and snapshot applications. The Cisco MDS 9500 platform supports two application modules that support copy and volume management services for specific storage vendor systems.

The trend toward virtualization supports the emergence of technologies such as blade servers, on-demand computing, and n-tier server architectures. Virtualization allocates physical devices into logical resources according to business need, allowing management flexibility to align storage, compute, and network infrastructure with application needs. To this end, Cisco Catalyst switches support virtual LANs (VLANs), firewall virtualization, and load balancing, and Cisco MDS 9000 Series switches feature virtual SANs (VSANs) and embedded storage virtualization.

Intelligent application services facilitate application communications, simplify application deployment, and enhance application performance and security. They will be made available as part of Cisco's ongoing effort to optimize emerging application architectures.

Achieving Business Continuance

The data center network is central to the business continuance strategy. Data center interconnect solutions such as SAN extension over metro optical networks are critical for achieving Recovery Point Objective (RPO) and Recovery Time Objective

(RTO) metrics. Equally important is the Recovery Access Objective (RAO), which defines the time required to reconnect users to a recovered application, regardless of where it is recovered. Without RAO, achieving application RPO and RTO has limited practical value. Therefore, business continuance managers should provide alternative connectivity measures such as VPN services and Global Site Selector Services that connect users to secondary data center resources in case of disruption.

Beyond the Data Center

Being business ready is a horizontal strategy, according to Allard. "It ties together the horizontal technologies—security, IP communications, network management, network-based provisioning, and user mobility—throughout the campus, branch office, data center, mobile workforce, and teleworker environments. This systems-level, end-to-end perspective drives the protection, optimization, and growth potential for our customers."

"When you ask enterprises whether they are business ready, they'll probably say yes, but that is today," says Gene Arantowicz, manager in Enterprise Solutions Marketing at Cisco. "As requirements change, Cisco is adding value by increasing our network intelligence over time. The Business Ready strategy gives our customers a business-oriented approach to networking that helps them respond more quickly and effectively to new opportunities and threats. This reduces their total cost of ownership and improves their ability to do business." ▲▲

The Role of Intelligent Networking

The role of the network is evolving. Organizations of all kinds are facing the challenges of new and daily threats from hackers and viruses, increasing scalability of infrastructure, the need to integrate new technology that may add complexity, and the escalating costs of systems integration. These burdens are quickly sapping the ability to respond to changing business conditions or new opportunities. Organizations the world over must find ways to increase the agility needed to respond to and capitalize on change, while simultaneously decreasing ever-escalating costs.

Solving these increasingly complex problems will require more sophisticated systems and tools that deliver greater capability with less complexity. The network plays a crucial role—it is the foundation that touches every element of the infrastructure, from end users to middleware, services, applications, and servers. Adding key capabilities, or *intelligence*, to the network, will enable applications and services to operate more effectively. Intelligent networking increases the capability and adaptability of your infrastructure. If the network is aware of the goals and objectives of your applications and services, it can make more informed decisions regarding the handling and processing of those applications. This intelligence lays a strong foundation upon which to implement business process re-engineering and optimization in order to become more agile and responsive.

There are three key elements in Cisco's intelligent networking strategy: adding network *intelligence*, providing a *systems-level* approach to integration, and delivering *policies* that help streamline costs.

- Enabling ***intelligence*** inside the network allows the network to better understand the mechanics of applications and services and to actively participate in their effective operation.
- The delivery of integrated ***systems*** reduces the complexity of this added capability as well as reducing operational costs and total cost of ownership.
- ***Policy*** mechanisms allow each organization or business to adapt this intelligence to its unique set of requirements based on their business rules

Cisco's vision of intelligent networking provides a foundation for building a network infrastructure that helps meet the customer's strategic and continually changing business objectives. To help customers to begin leveraging intelligent networking today, Cisco has defined a "Business Ready" initiative for each of the four key areas of the enterprise network: data center, campus, branch, and teleworker. These system blueprints demonstrate how Cisco routing and switching technologies, along with our advanced technologies (security, wireless, IP communications, optical, and storage) work together to deliver intelligence throughout the network, enabling customers to protect, optimize, and grow their businesses.

FURTHER READING

- **Cisco Business Ready Architectures: cisco.com/go/businessready**

DMVPN Extends Business Ready Teleworker

Cisco IOS DMVPN reinforces teleworker initiative with unmatched end-to-end security, connectivity, deployment, and management.

BY PLAMEN NEDELTCHEV, GAUTAM AGGARWAL, HELDER ANTUNES, AND DAVID IACOBACCI

THE EXISTING MYRIAD OF IP-BASED virtual private network (VPN) solutions allows enterprises to provide secure home access to corporate resources for three main categories of users: "road warriors" (workers who travel extensively), "day extenders" (employees who access their corporate network from home after regular business hours), and full-time telecommuters. Every Cisco VPN solution can be successfully used as a single solution in each of these categories; however, client- or Web-based VPN solutions target mainly the needs of road warriors, while Cisco site-to-site IOS® VPN solutions address the needs of day extenders and small/ remote and branch offices. The latest Cisco IOS VPN solution reinforces the Business Ready Teleworker initiative. It extends and improves end-to-end connectivity, end-to-end deployment models, and end-to-end management. This VPN innovation also provides enterprise-class connectivity; enterprise-quality voice, video, data, and multicast; and unprecedented, layered IOS security features within a Cisco routing protocols framework. In its full evolution, the end-to-end solution will encompass secure, interoperable networks including data, voice-over-IP (VoIP), and wireless LAN (WLAN) networks for enterprises and Internet service providers (ISPs).

From a features standpoint, this new extension divides into four major components: end-to-end layered security, IOS-based end-to-end connectivity, end-to-end deployment, and end-to-end management (see table, page 62). An end-to-end model can significantly reduce operational, support, and management costs, which in general represent 80 percent of total cost of ownership (TCO), according to Sage Research.

The Headend and Remote Sites

At the ***headend,*** the solution incorporates Cisco IP Solution Center (ISC), Intelligence Engine 2100 (IE2100) Series Cisco Networking Services (CNS) engine, IOS-based Public Key Infrastructure authentication, authorization, and accounting (PKI-AAA) integration, a security management gateway, and numerous security data gateways. The headend fully controls the remote site based on an enhanced set of CNS agents running on the remote routers.

At the ***remote site,*** the solution incorporates a low-end router (typically Cisco 830 Series for home users) or midrange router (Cisco 1700, 2600, or 3600 series for branch users), and easy-to-deploy IOS security features such as antitheft protection, configuration integrity protection, and a variety of authentication mechanisms including Auth-Proxy-AAA and port IEEE 802.1X-AAA. Based on configurable policies at the headend, the remote site can be enhanced with features such as Cisco Network Admission Control (NAC), Network-Based Application Recognition (NBAR), and intrusion detection system (IDS).

To facilitate end-to-end interoperability, a great deal of automation is designed into the solution (see table, IOS End-to-End Management, page 62).

End-to-End Connectivity

Dynamic Multipoint VPN (DMVPN) is a key factor in achieving the end-to-end connectivity model, essentially incorporating Cisco routing protocols framework into IP Security (IPSec) VPN framework, which converts the secure peer-to-peer VPN into a secure end-to-end VPN. As a technology, DMVPN comprises IPSec, Next Hop Resolution Protocol (NHRP), and multipoint Generic Routing Encapsulation (mGRE).

From a design perspective, DMVPN offers unmatched flexibility, allowing dynamic hub-to-spoke, virtual partial-mesh architectures, and in its extreme virtual full-mesh architectures (note that large full-mesh architectures can be expensive and difficult to manage in time-division multiplexing and Frame Relay environments). From a deployment perspective, DMVPN simplifies the burden of headend management and thus reduces TCO.

Automated End-to-End Deployment

In general, enterprises and ISPs apply the following basic deployment models:

- In-house model—IT team configures the router and sends it to the branch or home user; the most cost-

For an overview of the components that make up the Cisco Business Ready Teleworker solution, see "Business Ready Teleworker At a Glance," page 15.

END-TO-END VPN AT A GLANCE

IOS End-to-End Layered Security

Device and User Authentication and Antitheft Protection

- Secure RSA Lock Key
- Secure ARP-Proxy
- Auth-Proxy-AAA
- IEEE 802.1X-AAA

IOS-Based PKI

- Certificate Server (CA and RA Modes)
- PKI-AAA Integration
- Auto-Enrollment
- Multiple Trust Points

Underlying Security Features

- IPSec (3DES or AES)
- Stateful Firewall
- NBAR and IDS

IOS End-to-End Connectivity

DMVPN

- Failover/Load Balancing
- Dynamic Routing
- Full-Mesh and Partial-Mesh Topologies
- Hub-to-Spoke and Spoke-to-Spoke Tunnels; Permanent and On-Demand Tunnels
- mGRE, IPSec, NHRP; Transport and Tunnel Modes
- Multiple DMVPN Clouds per Headend Router; Resilience

Full Support of IP Applications

- Data
- VoIP
- QoS
- Wi-Fi
- Multicast
- Video

IOS End-to-End Deployment

Configuration Automation IP Solution Center

Cisco CNS 2100 Series Intelligence Engine

- CNS Configuration Engine
- CNS Notification Engine
- CNS Image Management Engine

Automated Zero Touch Deployment

- Bootstrap Configuration and PKI Certificates (EzSDD)
- Dynamic Addressing

Automated Policy Deployment, Redeployment, and Audit

- DMVPN/IPSec
- Firewall
- QoS
- NAT
- NBAR and IDS

IOS End-to-End Management

Ongoing Management IP Solution Center

Cisco IE2100-Based CNS Notification Engine

- CNS Configuration Engine
- CNS Notification Engine
- CNS Image Management Engine

EMAN Framework Integration

- Automated User Service Application and Entitlement
- Automated Configuration/Preconfiguration and Audit
- Automated Image Management
- Automated Control, Monitoring, and Security Management
- Interactive/Automated Decision Making and Service Termination
- Antivirus, Antiworm, and DoS Protection (per Identification)
- Automated Event Log Management
- Automated Notification of the Support Teams

LOW TCO, BIG BENEFITS: An end-to-end, highly automated approach enables enterprises to maintain low TCO even when increasing and enhancing the feature set of the solution.

ineffective model. Works relatively well for small and midsized businesses or deployments.

- Outsource/out-task model—Some large enterprises prefer to outsource to one big customer with global presence, who performs the initial task of configuration and logistics, while the enterprise ensures the provisioning. This model adds to the cost of both the acquisition of assets and deployment management.
- Out-of-house model—Some large enterprises or ISPs can use their own staging facilities for initial or complete CPE configuration. The CPE is shipped to the end user /administrator; adds an additional cost to the acquisition of the assets. Sometimes the cost can be significant compared to the purchase price.
- Touchless or ZTD model—Requires presence of at least one user with necessary credentials (AAA account in the corporate AAA server); most frugal model; no extra cost associated.

Of course, these models can vary significantly, and their comprehensive details and cost analyses are beyond the scope of this article. Suffice to say that Business Ready Teleworker supports all common deployment scenarios; however, maintaining the lowest TCO requires the no-cost-associated model to be applied. As noted, in the ZTD model, the remote site can be automatically deployed/decommissioned/redeployed. ZTD is based on a new Cisco IOS Software feature called *Easy Secure Device Deployment (EzSDD)*. While very simple for end users, ZTD is not quite as simple on the backend. Therefore, ZTD is a "virtually simple," fast process that requires all the components of the system work in sync and all scenarios be anticipated and automated.

Let's assume the common case. A home user has subscribed for cable ISP service, and the ISP has provided a cable modem for him. The user can connect his PC to the cable modem, obtain his IP address via Dynamic Host Control Protocol (DHCP), and connect to the Internet. In the most general case, the user can use Security Device Manager (SDM) to configure his router with Point-to-Point Protocol over Ethernet (PPPoE) or Static IP and connect to the Internet. Meanwhile, the home user applies for VPN service from his company, obtains approval, and orders a new Cisco 830 Series Router. After he receives the router at his home office, he connects the router to his cable modem, obtains an IP address from the router (typically 10.10.10.0/24 range), and gets connected to the Internet.

PLAMEN NEDELTCHEV, Ph.D, network engineer with the Intelligent Network Solutions team at Cisco, is author of *Troubleshooting Remote Access Networks*, Cisco Press. He can be reached at pnedeltc@cisco.com.

GAUTAM AGGARWAL, CCIE® No. 4714, is a manager of software development in the Internet Technologies Division at Cisco, specializing in VPN and network security. He can be reached at gaggarwa@cisco.com.

HELDER ANTUNES is a senior development manager in the Internet Technologies Division at Cisco, specializing in network security. He can be reached at helder@cisco.com.

DAVID IACOBACCI is a network engineer with the Intelligent Network Solutions team at Cisco, specializing in VPN and home networking. He can be reached at diacobac@cisco.com.

To be deployed as a VPN user with his company, there are three easy-to-understand steps (from the end user's perspective):

Step one (welcome)—User launches a browser and types in the browser's address filed: http://10.10.10.1/ezsdd/welcome.

Step two (introduction)—User prompted to type a URL in the Web page, https://www.join-mycompany.com/ezsdd/intro, and to press "Next."

Step three (complete)—User prompted for user name and one-time-password ("OTP," this is provided to the user by the IT group or integrator). After a while, his browser will announce "Complete" state and prompt him to release/renew his PC's IP address.

At the headend, this "virtually simple" process (as expected) is a little more complicated and includes a preparation and an action phase. In the preparation phase, while the user is waiting for his router to arrive, the ISC will be configured and all policies will be in "Wait_to_deploy" (Pause) state. In the action phase, the user (Introducer) interacts with CPE (Petitioner), which establishes Trusted Transitive Introduction (TTI) relationship with a CERT router (Registrar). Registrar acts as a proxy for the user authentication. After successful authentication, it intercepts the login_name and requests a general, customized initial bootstrap configuration from ISC, which is pasted into Petitioner's (CPE's) running configuration. The CNS agent is activated. A CNS "connect" event is sent to CNS Engine, which forwards the "connect" message to ISC. All waiting policies are sent to the CPE over the management tunnel. The last Service Request (policy) will complete the process, which on average lasts about 200 seconds.

Automated End-to-End Management

The first and foremost objective of Business Ready Teleworker is managing security. For this solution, based on a broad set of application programming interfaces (APIs) and Simple Object Access Protocol/Extensible Markup Language (SOAP/XML), every new deployment can be integrated into the existing enterprise or ISP infrastructure and interact with AAA, Domain Name System (DNS), and DHCP services. The remote site is fully controlled and managed, and the security policies can be applied, changed, and audited. Therefore, many of the traditional headend functions such as antivirus/antiworm protections and anti-DoS attacks can be managed at the remote site (if identified), effectively increasing the availability of the headend site and corporate network.

In Cisco's global IT deployment, the headend is integrated into the Cisco IT framework. With an in-house management tool suite created by Cisco IT, EMAN incorporates the built-in intelligence of the system using a variety of available APIs and interacts with Cisco ISC and IE2100-based CNS engines. EMAN brings additional features such as monitoring and performance trending, thresholds-based alerts and notifications, as well as image management. In its ultimate functionality, management covers the whole spectrum of information services: monitoring, analyzing, and decision making.

Cisco ISC introduces and supports the notion of fully managed service (FMS). If any configuration changes are scheduled and performed from ISC/EMAN, FMS will accept and register the change. If the change is originated from a non-ISC/EMAN source, FMS triggers a set of functions to audit the CPE's configuration and notifies the supporting teams about configuration/policy change, security violation, connect/disconnect events, and the like. Furthermore, if a policy violation is identified or virus/worm attack or DoS is discovered, the EMAN will trigger an automated/interactive process to prevent the violation.

Non-Cisco customers can plug in additional logic to adjust the system to the way they typically operate or to their management system. The EMAN experience and scripts and available APIs would allow every enterprise or ISP to apply their own set of policies or procedures to control and manage the security risks in their environments.

Unmatched Integration

Cisco's extension to the Business Ready Teleworker solution offers a level of networking and security integration unmatched in the industry to date. Virtual simplicity, maximum automation of management, design flexibility, and scalability are key factors in large-scale (global) deployment and management, and in achieving these factors, this Business Ready Teleworker solution effectively allows low TCO to be maintained.

Cisco's own global deployment includes architectural and design solutions that enable enterprise home, enterprise branch, and ISP deployment models, and provide enterprise-class connectivity, and enterprise-quality voice, video, data, and multicast. The real potential exists for other enterprises to incorporate or integrate the whole solution, or a subset of it, into their existing network environment.

◆ ◆ ◆

The authors express their appreciation to the following Cisco people, who contributed to this article: Mike Sullenberger, Max Pritikin, Henry White, Jennifer Redovian, Dalia Geller, Hom Bahmanyar, Ajith Thrivikramannair, and Pedro Leonardo. ▲▲

FURTHER READING

- **Business Ready Teleworker portal: cisco.com/go/teleworker**
- **DMVPN white paper: cisco.com/packet/162_7c1**

Service Provider SOLUTIONS

Building a Service-Driven Metro Network

A service-first approach in metro and long-haul networks leads to greater customer satisfaction and service provider revenues.

BY JANET KREILING

CYBELLE

BUILD IT AND THEY WILL COME" HAS never been an effective marketing strategy. Too often, it really means "Build it and hope they will come." Far better to build it *so* they will come. The road to revenues in the future is paved with a concrete understanding of what services customers actually want and where.

Consider some specific end-user needs: A financial enterprise's foremost requirement is a 50-ms failover time. A small business wants cheap bandwidth and can accept a slower recovery time—even up to 10 seconds. A residential customer wants a "triple play" of voice, video, and high-speed Internet access.

What's the best way to deliver these services? To meet the 50-ms failover time, the best choice might be a SONET/SDH optical ring. For bandwidth with longer recovery times, you might use native Ethernet, delivered by local Ethernet switches and transported over a Layer 2 or Layer 3 link; oversubscribing capacity and using statistical multiplexing can keep costs down. And the residential customer might be well served by hybrid fiber-coax or by all fiber.

After you've defined the needs of your specific customers and the technologies that can satisfy them, you can begin thinking about where your current network has those capabilities and where you need to adapt, augment, or expand it. But, emphasizes Frank Brockners, a technologist at Cisco, "Every choice must be driven by specific business requirements such as user needs and new profitable service offerings."

The service-driven network must be considered as a whole—a substantive change from the past, Brockners adds. Typically, service providers have deployed technologies, not services: building an ATM network, a Frame Relay network or two, or a SONET/SDH time-division multiplexed (TDM) network. Personnel have been organized in silos around the technologies. Technical and sales experts on ATM don't necessarily talk to the experts on Frame Relay or IP. Too often customers have had to deal with specialists in one technology or another and haven't always gotten the solution that best suited their needs.

The reality that revenues from traditional services constrained in their flexibility are declining and service providers must find a new business model is a major impetus to change. Like any change, adopting a service-driven model opens up opportunities with big potential benefits.

- **Benefit 1:** New services can generate significant revenues from higher network layers as well as Layers 2 and 3.
- **Benefit 2:** Service providers can bundle packages of services to achieve real competitive differentiation based on something more than pricing. Bundling will become more common and flexible as providers

move away from the traditional revenue model wherein pricing is based on time and distance to new ones based on bandwidth, services, content, and customer experience.

Start with Services and SLAs

This is not a time to think narrowly. You'll want to offer some services that neither customers nor service providers have even thought of yet, so the network must be capacious and capable well into the future.

Consider the services you can offer now or very soon. Already, many customer want Layer 2 or Layer 3 virtual private networking (VPN) services to connect their headquarters with remote offices. As communications become more integral to every aspect of an enterprise, business customers want the triple play of voice, video, and data, usually all IP-based. They're also moving on to Web hosting, network storage, intrusion detection, surveillance, disaster recovery, hosted IP telephony, and others. Residential customers want voice, video, and broadband Internet access, and they are also finding other services attractive, such as VCR on demand, pay per view, gaming, VoIP, instant messaging, sending photos, and others.

Ethernet is central to delivering this wide range of services for two reasons: It's an efficient protocol that works well with other transport and service technologies, and it provides for a very wide range of bandwidth capabilities. "All these services can be delivered over a flexible Ethernet User Network Interface [UNI]," says Wesley Mukai, product manager for metro Ethernet at Cisco. "The Ethernet UNI can scale bandwidth easily from a few kbit/s to 10 Gbit/s depending on the end user's service requirements—a granularity that is not possible with other formats. And it can be delivered through a wide variety of technology options—Layer 1, 2, or 3 transport format—SONET/SDH, ATM or Frame Relay, or IP/MPLS."

By offering an Ethernet UNI, the service provider tailors its edge network to what its customers are already using—even, to a surprising extent, in the residential market. Many enterprise customers already rely internally on the high bandwidth and QoS provisions possible with Ethernet—with an Ethernet UNI, traffic retains these characteristics as it enters the service provider's network. Ethernet and IP go together: IP traffic is easily encapsulated in Ethernet packets, retaining the IP priority and QoS information.

"Most people still think of Ethernet as an enterprise technology," Mukai points out, "but it's for service providers, too." Carrier-class Ethernet switches, routers, and other network components are now available that

Ethernet Equal Access Networks

Some 40 European cities are already building or planning Equal Access Networks (EANs) for broadband services based on Ethernet, according to Gloria Formenti, Cisco's metro Ethernet solution manager for Europe, the Middle East, and Africa. EANs embody a new concept in communications delivery: an independent urban network built, owned, and operated by a private company, community, or other organization.

"Multiple service and content providers have access to the network to deliver services to multiple market segments, and enterprise, small business, and residential customers pick and choose the services they want from among them," Formenti says. Both service and content providers and customers have broad access, and if the network is owned by a communications service provider, it might deliver its own services as well as leasing capacity to others. Providers can use a combination of pricing formulas, such as flat-rate, per-byte, per-application, or on-demand to create a wide range of attractive packages to appeal to different customers and market segments.

As an example of an EAN, Formenti cites the one built by MKB Fastighets AB, a real estate company owned by the City of Malmo, Sweden. The company wanted its own network to offer tenants in its 20,000 apartments a variety of voice, video, and data services from different providers over the 10 Mbit/s provided to each unit. Tenants can self-provision the services they choose, in any combination. MKB Fastighets AB also uses the network to handle online booking of apartments, communications with tenants, and fire, burglar, and safety alarms.

FastWeb, a service provider in Milan, Italy, and Bredband, a Swedish company, have experienced dramatic growth in their EANs. FastWeb has added more than 180,000 subscribers in the past 18 months, and Bredband has added some 270,000.

All three networks employ Cisco Catalyst 6500 Series switches in the core linked by fiber to Catalyst 2950 Series switches in the access network.

"EANs are becoming central to the economies of urban economies—appropriate for communities of as few as 10,000 end users," Formenti adds. And she points out that the shorthand for these networks is ETTx—Ethernet to the anything.

enable service providers to carry Ethernet not just in the metro network, but also across the core, if desired.

Consider service-level agreements (SLAs), too. They alone will dictate much of how you design your network, determining where certain levels of bandwidth and QoS must be available. For example, one customer's SLA can specify availability (three nines on certain services, five nines on others?), delay or jitter (50 ms? 20? 100?), data delivery rate (99.99 percent? 99.999 percent?), sequence preservation (yes, no, varies with different types of traffic?), and bandwidth (committed and peak rates?).

The requirements for availability, for example, help you plan where certain features, redundancy, and resiliency of equipment and software—and security—must be provided. For example, features such as MPLS Fast Reroute, Rapid Spanning Tree, subnetwork connection protection, and others can all improve availability. Sequence preservation will invoke QoS mechanisms and transport choices. QoS, incidentally, benefits the provider as well as the end user: It increases the transport capacity of the network. By using intelligent packet processing with QoS, service providers can oversubscribe their networks to make better use of their existing interfaces and bandwidth. Other SLA specifications determine where in the network other capabilities must be available.

Architecture and Technologies

Essentially, Brockners says, "a flexible network will need to expose all layers to service delivery. In addition, a layered approach will allow for scalability and SLA control at each of the layers in the network, which is far more scalable and flexible than just delivering everything across one layer." As providers build service-driven metro networks, they can use all three layers for service delivery and scalability, rather than a single layer. Of course, the metro network architecture depends in part on the installed base—what's in the ground and what it's connected to.

When you know what capabilities you need where, the next step is mapping products and technologies to the different network roles and the complete development of the network. A comprehensive, service-driven network solution employs multiple technology and product options. A single device or several devices might fulfill each role in the network, depending on the service and SLA requirements, the network architecture, and the technologies that have been deployed.

For example, Mukai says, at the network edge service providers might deploy fixed or modular switches such as Cisco Catalyst® 3750 Metro Series switches, Catalyst 6500 or 4500 series switches, or the Cisco 7200 Series VPN Router. The Catalyst 4500 Series is a cost-effective and modular option; it can serve a mix of residential and business customers. In addition, it can support single-fiber connections to the business or home; along with the Catalyst 6500 Series, it can deliver fast failover times for those customers that need them. The Catalyst 3750 Metro Series, which is installed on the customer's premises, can tunnel traffic using MPLS. Mukai points out that it also offers advanced QoS with hierarchical queuing, in which packets can be prioritized according to three policy levels—at the physical, logical, or class level—for a very high degree of granularity in traffic management.

Larger systems can be employed at the edge as well as in aggregation or core networks. The Cisco Catalyst 6500 Series Switch and 7600 Series Router provide an edge gateway to 10-Gbit/s transport, as well as a high degree of scalability. "These systems enable the provider to control flows with traffic engineering at the network edge and deliver advanced QoS—and it can be a transition point between Layer 2 and MPLS networks," Mukai says.

Optical equipment also plays a role on the metro edge—for example, the Cisco ONS 15302 and 15305 multiservice customer access platforms deliver support for TDM and Ethernet services in compact form. Their plug-in slots accommodate a variety of services, helping the provider deliver precisely those needed on given transport routes.

In the aggregation layer, which can include hybrid fiber-coax access networks, the provider might choose mid- to large-scale switches and routers, along with somewhat larger optical networking systems. The network core calls for high-speed, high-performance routers with excellent QoS capabilities and an integrated core and edge feature set, such as the 7600 Series Router, and perhaps the ONS 15454 and ONS 15600 optical platforms.

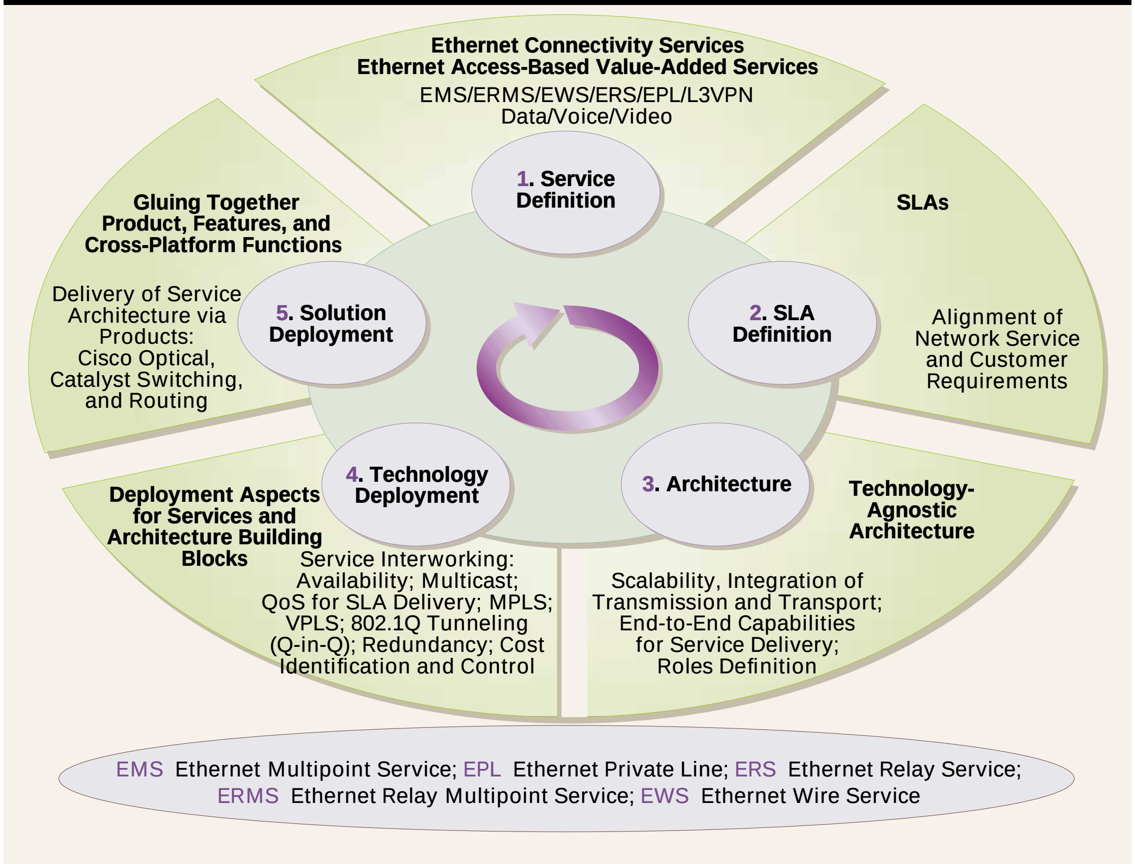
Using Ethernet in the edge network permits delivery of all of the types of connectivity end users now employ. Cisco's Ethernet Private Line Service (EPL) provides dedicated point-to-point connections. Ethernet Wire Service (EWS) provides point-to-point connections over a shared infrastructure. Ethernet Relay Service (ERS) provides point-to-multipoint links. Ethernet Multipoint Service (EMS) provides multipoint-to-multipoint connections and can carry Layer 3 services. Ethernet Relay Multipoint Service (ERMS) provides any-to-any connectivity and supports service multiplexing. Ethernet Private Ring (EPR) is a multipoint service using Layer 1 transport technology (see figure).

FURTHER READING

- **Toward a Service-Driven Metro Network—A Service Provider Guide for Enabling Metro Business Services: cisco.com/packet/162_8a1**
- **Managed Metro Ethernet Services: cisco.com/packet/162_8a2**

An Ethernet network is enabling SureWest Broadband to offer voice, video, and Internet connections to customers. Find out more at cisco.com/packet/162_8a3.

SERVICE-DRIVEN METRO NETWORK


Ethernet Connectivity Services
Ethernet Access-Based Value-Added Services
EMS/ERMS/EWS/ERS/EPL/L3VPN
Data/Voice/Video
1. Service Definition
SLAs
2. SLA Definition
Alignment of Network Service and Customer Requirements
3. Architecture
Technology-Agnostic Architecture
Scalability, Integration of Transmission and Transport; End-to-End Capabilities for Service Delivery; Roles Definition
4. Technology Deployment
Deployment Aspects for Services and Architecture Building Blocks
Service Interworking: Availability; Multicast; QoS for SLA Delivery; MPLS; VPLS; 802.1Q Tunneling (Q-in-Q); Redundancy; Cost Identification and Control
5. Solution Deployment
Gluing Together Product, Features, and Cross-Platform Functions
Delivery of Service Architecture via Products: Cisco Optical, Catalyst Switching, and Routing
EMS Ethernet Multipoint Service; EPL Ethernet Private Line; ERS Ethernet Relay Service;
ERMS Ethernet Relay Multipoint Service; EWS Ethernet Wire Service

NEW PARADIGM: In the new service-driven business model, the traditional transport-driven approach is being replaced by one that is business driven. Services and solutions can incorporate multiple technologies and network layers to satisfy specific, individual customer needs.

"These services all interwork," Brockners says, "so any combination can be employed in different parts of the network to achieve optimal communications."

Beyond the Ethernet Island

After the metro architecture has been defined, service providers can begin thinking about how to interconnect islands of metro Ethernet. Enough experience has now been logged with MPLS and virtual private LAN service (VPLS) for wide-area networks so that providers can begin to make decisions about their ability to deliver specific services.

Brockners explains that using pure Layer 2 control protocols between metro Ethernet islands is not feasible because Layer 2 requires Spanning Tree Protocol, which does not scale to span wide areas. But Layer 2 transport technologies can still be used in the core through VPLS, which supplies high-bandwidth, multipoint-to-multipoint Layer 2 connectivity across an IP/MPLS network. More than 45 Cisco customers worldwide are now evaluating VPLS architectures for Layer 2 multipoint services.

According to Santiago Alvarez, technical marketing engineer at Cisco, VPLS improves the scalability and reliability of traditional switched Ethernet networks, simplifies their provisioning for both the customer and the service provider, and takes advantage of the outstanding price/performance ratio of Gigabit and 10 Gigabit Ethernet.

MPLS is another effective means of inter-metro area transport. Service providers can connect any Layer 2 transport over a single IP/MPLS converged infrastructure, with the advantages of resiliency, policy control, and service flexibility. And Cisco's MPLS now incorporates bandwidth-assured Layer 2 services with tight guarantees for packet loss, latency, and jitter to meet very precise SLAs.

Brockners offers this perspective on a service-driven network: "Look at the difference between what you can do with your landline phone and what you can do with your mobile. We're looking at that magnitude of change." For example, he points out, "Mobile operators offer different services and service bundles along with a wide variety of pricing options and pricing. The differences in offerings allow providers to differentiate themselves from others, and the healthy competition drives further diversity."

Most service providers, he adds, "are going to need to scale up their networks in the next few years. The time is now to take a step back, assess customer needs, and build a metro network that will meet service needs now and in the future." ▲▲

Make Your Mark with MPLS

Embedded OAM tools help monitor MPLS networks and services—fostering new value-added offerings.

MANY SERVICE PROVIDERS ARE REALizing operational efficiencies and cost savings by backhauling multiple types of network traffic over a common Multiprotocol Label Switching (MPLS) backbone. MPLS technology brings virtual circuit-like characteristics to IP networks, giving network operators greater control over network performance. In addition to using integrated MPLS backbone networks for efficient transport, most service providers would like to offer value-added services off their MPLS platforms to generate greater revenues. Such offerings require the ability to guarantee bandwidth to certain traffic, such as voice over IP (VoIP) and IP virtual private networks (VPNs), with assurances similar to Frame Relay and ATM committed information rates (CIRs), and the capability to closely monitor MPLS networks and their services to keep such traffic-sensitive offerings as VoIP running smoothly.

Offering premium services across a converged MPLS network requires a multiple-service management view of the network, says Ripin Checker, product manager in Cisco's Internet Technologies Division. "Several legacy revenue-generating subscriber services—Frame Relay, ATM, leased lines, and, increasingly, Ethernet transparent LAN services—are starting to ride the MPLS backbone," Checker says. Subscribers accustomed to these services' characteristics and guarantees would like those attributes preserved, regardless of the WAN infrastructure their provider runs.

To successfully enforce service-level agreements (SLAs) for premium and legacy services, service providers require the ability to verify connectivity and quickly find and troubleshoot failed paths and measure IP SLAs for each service and customer. Automation and proactive connectivity testing is essential and helps to reduce time to repair and operational costs. This requires cohesive management of all MPLS networks and the subscriber services associated with them.

The Cisco suite of standards-based MPLS management tools and technologies enables service providers to increase the overall reliability, availability, and serviceability of MPLS networks and services. Simplified provisioning and automated troubleshooting lower the total cost of ownership (TCO) and boost productivity. Cisco offers an integrated suite for network and service management that provides an end-to-end, flexible, intelligent solution for business agility.

Cisco recently significantly enhanced its MPLS Management portfolio to include Cisco IOS® *MPLS Embedded Management* tools and new versions of *Cisco Info Center VPN Policy Manager* and *Cisco CNS NetFlow Collection Engine* (see sidebar, "Effectively Correlate Service Assurance Information," page 71, for more on Cisco Info Center and Cisco CNS NetFlow Collection Engine).

MPLS Embedded Management

With important MPLS operation, administration, and management (OAM) requirements folded in, MPLS Embedded Management brings the robust set of OAM tools to MPLS environments that have long been available for Frame Relay/ATM WAN backbones. Integrated in Cisco IOS Software Release 12.0(27)S, MPLS Embedded Management features such as LSP Ping, LSP Traceroute, Virtual Circuit Connection Verification, and AutoTunnel Traffic Engineering (TE) and AutoMesh TE consolidate the operations support systems (OSSs) that handle fault, configuration, accounting, performance, and security (FCAPS) management functions across the different service types (see Figure 1, page 70).

Cisco MPLS Embedded Management capabilities are based on emerging Internet Engineering Task Force (IETF) draft standards for MPLS OAM. They enable service providers to guarantee service levels across MPLS-based IP VPNs, regardless of the subscriber interface connecting customers to the WAN service. For example, the availability of *MPLS MIBs* (management information bases), accessible by third-party management systems via the industry-standard Simple Network Management Protocol (SNMP), stitch together the various service views needed to quickly troubleshoot a converged MPLS network.

The traditional Cisco command-line interface (CLI) can also be used to access MIB information, and Cisco is working on making a programmable Web-based Extensible Markup Language (XML) management interface available, says Checker. In addition, the ability to automate the MPLS OAM tools via Cisco Service Assurance Agent (SAA), for example, will help service providers in automating critical fault isolation and detection mechanisms in MPLS networks.

LSP Ping and LSP Traceroute

These tools provide diagnostics and troubleshooting for MPLS Label Switch Paths (LSPs). *LSP Ping* helps to detect fault, and *LSP Traceroute* helps in isolating the fault. Analogous to the Internet Control Message Protocol (ICMP) ping function in native IP networks, an "MPLS echo request" message is sent over an MPLS LSP from an originating provider edge (PE) router to a target PE router. If the MPLS data plane is up and running, the target PE router will send back an "MPLS echo reply." If there is no reply, it can be assumed that there is a fault somewhere along the LSP.

At that point, the originating PE router automatically performs a traceroute for hop-by-hop fault localization and LSP path tracing. It sends an MPLS ping to each of the interim routers, one at a time, on the LSP. When the originating PE router fails to receive a reply from one of the routers along the way, it can deduce that the problem lies on that particular hop. For a graphic depiction of the role LSP Ping and Traceroute play in troubleshooting MPLS LSPs, see cisco.com/packet/162_8b1.

OAM for Layer 2 Tunneled Traffic

It is not only necessary to automate end-to-end fault detection for Layer 3 MPLS traffic. Layer 2 traffic tunneled through MPLS using Cisco Any Transport over MPLS (AToM) technologies—as specified by the IETF Pseudo Wire Emulation Edge to Edge (PWE3) working group—requires the same level of management. In an AToM deployment, edge routers encapsulate incoming native Layer 2 traffic in MPLS labels and tunnel it through the MPLS backbone via virtual connections called *pseudo-wires*. An MPLS LSP Ping is sufficient to monitor the PE-PE tunnel, but not the individual customers' virtual circuits inside of that tunnel.

So the newly embedded *Virtual Circuit Connection Verification (VCCV)* tool creates an in-band control channel between two PE devices. The channel is used to identify the connectivity verification packets from Layer 2 payloads. VCCV enables troubleshooting and diagnostics on the Layer 2 tunnel in aggregate, as well as on each customer circuit within the tunnel.

Automating TE Tunnel Setup

Cisco MPLS Embedded Management has also automated the process of building a mesh of MPLS TE tunnels between MPLS PEs. The Cisco *AutoTunnel TE* tool automates the configuration of primary and backup tunnels, as well as full or partial meshes of logical TE tunnels over the physical infrastructure. *AutoMesh TE* can be used to "automatically self-configure a mesh of TE tunnels between PEs similar to a manual mesh of ATM virtual circuits between ATM edges," says Checker. For example, network operators can use a combination of

MPLS MANAGEMENT ARCHITECTURE

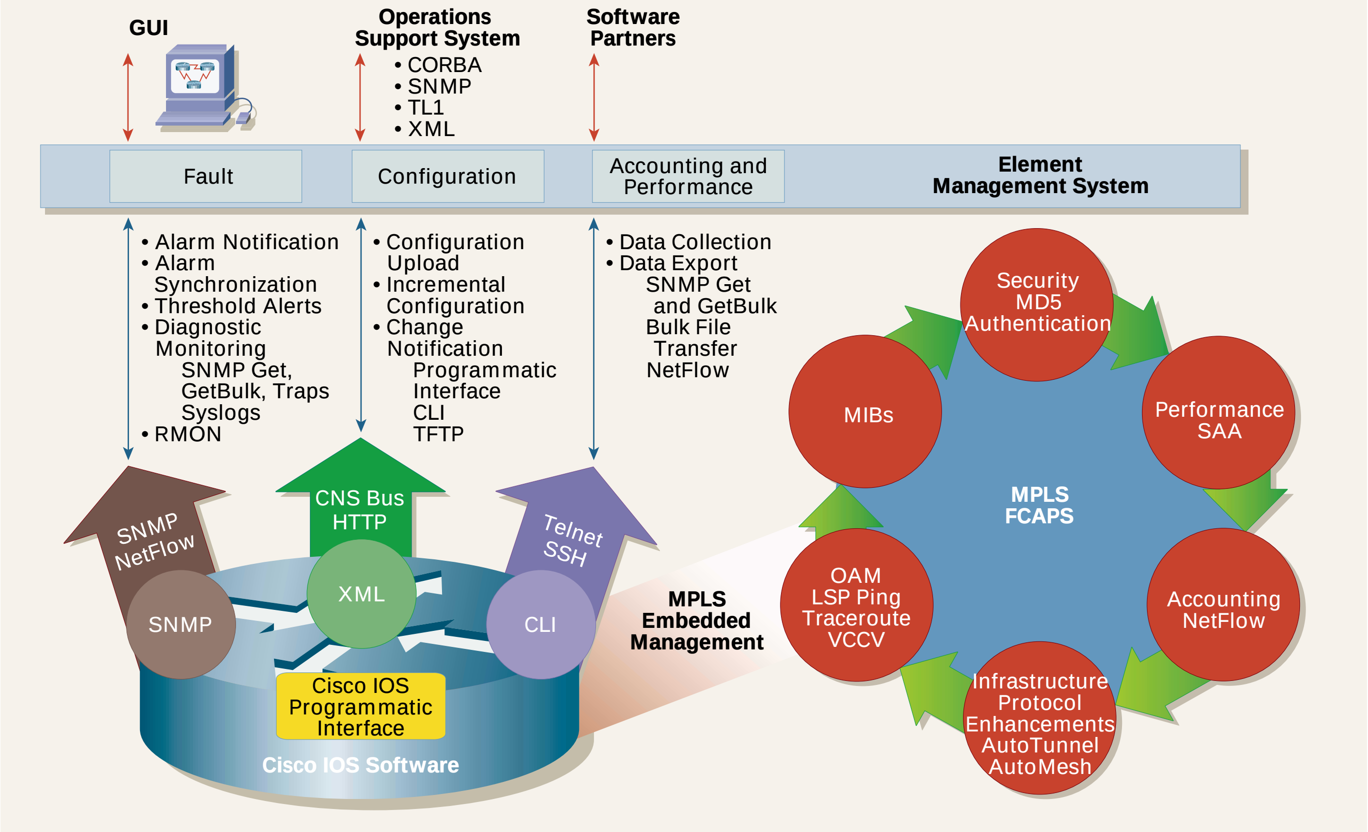


FIGURE 1: MPLS Embedded Management FCAPS features and important OAM tools are now available in Cisco IOS Software Release 12.0(27)S.

Effectively Correlate Service Assurance Information

Cisco recently updated key network management applications to automate the correlation of event and provisioning information in MPLS networks. Cisco Info Center VPN Policy Manager 3.1 and Cisco CNS NetFlow Collection Engine 5.0 help network operators improve their mean time to resolution (MTTR) more quickly on a per-customer basis, automate escalations to maintain SLAs, and provide flexible, scalable access to critical NetFlow data.

The VPN Policy Manager, for example, integrates the fault-event collection capabilities of Cisco Info Center with Cisco IP Solution Center, an element-level provisioning application for Layer 2 and Layer 3 VPNs. With this combined view, network operations center (NOC) personnel can immediately see which customers' VPNs are affected by network faults, performance thresholds, configuration changes, or other events. This capability substantially improves SLA management and automates escalation procedures.

“Before, critical alerts would be displayed [in Cisco Info Center],” explains John Gaudin, product manager in Cisco's Network Management Technology group. “Someone would note the IP address, node name, and other information about the affected devices. Then, that person would look up which, if any, customer VPNs are affected in Cisco IP Solution Center.”

Now, Gaudin says, events reported to the Cisco Info Center are automatically passed through the VPN Policy Manager, which queries the Cisco IP Solution Center real time and displays the affected customer VPNs. Network operators can quickly prioritize and act based on customer SLAs. The Cisco Info Center desktop includes drop-down menus to easily launch Cisco MPLS Embedded Management tools for faster fault resolution.

In addition, the Cisco Info Center integrates with the Cisco CNS NetFlow Collection Engine 5.0. A new Web-based interface allows NOC personnel to define which combinations of packet fields they would like to see aggregated into reports about traffic flows.

“This helps network operators better understand the traffic profiles on their networks,” explains Ken Ross, manager of product partner marketing in Cisco's Network Management Technology group. With flexible, scalable access to NetFlow data, operators can better understand traffic patterns, which in turn, aids in capacity planning and performance monitoring. The application works with both IP and MPLS networks.

AutoMesh TE along with Differentiated Services (DiffServ)-TE to automatically add a mesh of TE tunnels between the newly added VoIP PE gateway and the rest of the PE VoIP gateways in the network—thus surpassing ATM in not only guaranteeing traffic in the network but in automatically discovering and configuring PEs.

Accounting and SLA Measurement Tools

Cisco NetFlow and SAA, two network-management features in Cisco IOS Software originally designed for native IP networks, have also gained “MPLS awareness.” Combined, NetFlow and SAA performance metrics provide a complete view of how a network is behaving, both historically and in real time. The NetFlow accounting feature provides highly granular traffic statistics for Cisco router-based networks on a per-flow basis. A “flow” is a unidirectional set of packets that all arrive at a router on the same subinterface and have the following additional variables in common: source and destination IP addresses, Layer 4 protocol, TCP/UDP source and destination ports, and IP type of service (ToS) byte.

Continued on page 89

FURTHER READING

- **Cisco IOS MPLS Embedded Management Q&A: cisco.com/packet/162_8b2**
- **MPLS-Aware NetFlow: cisco.com/go/netflow**
- **Cisco IOS SAA: cisco.com/packet/162_8b3**
- **Cisco IOS MPLS: cisco.com/packet/162_8b4**
- **IETF MPLS OAM Requirements Internet-Draft: ietf.org/internet-drafts/draft-ietf-mpls-oam-requirements-02.txt**
- **Detecting MPLS data plane failures Internet-Draft: ietf.org/internet-drafts/draft-ietf-mpls-lsp-ping-05.txt**
- **IETF Pseudowire VCCV Internet-Draft: ietf.org/internet-drafts/draft-ietf-pwe3-vccv-02.txt**

High-End Innovation

The Changing High-End Routing Landscape . . . Where It's Headed

BY DAVID BARRY

FROM ITS MODEST BEGINNINGS AT Stanford University in 1984 when Cisco founders Len Bosack and Sandy Lerner devised a new method to exchange e-mail between two incompatible computer systems, Cisco has continued to be the innovation leader of the networking market. The multiprotocol router that evolved from their exchange of e-mail went on to completely redefine the then nascent "internetworking" industry and set the stage for the coming Internet boom.

As Cisco has grown along with the enormous changes in networking and the Internet, it has continued to lead in delivering networking innovations, especially in its high-end routing platforms. These platforms, combined with the industry-proven, ubiquitous Cisco IOS® Software have helped service providers respond to overwhelming market changes as the worlds of telco and data networking merged. Voice and time-division multiplexing (TDM) networks gave way to Frame Relay and ATM, which in turn gave way to optical and IP networking and then to IP/Multiprotocol Label Switching (IP/MPLS). Today, those innovations continue with the recent announcements of enhancements to the best-in-class Cisco 12000 and 7600 series router product lines.

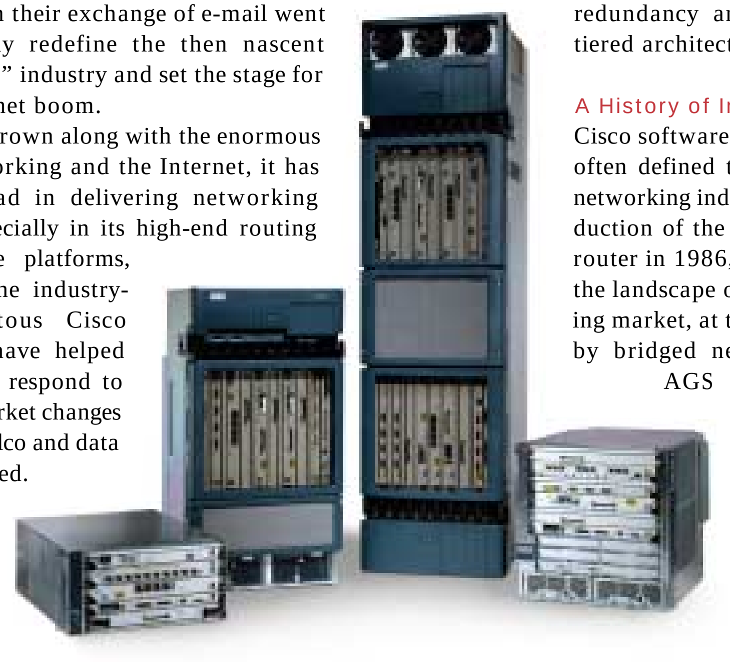


FIGURE 1: Recent enhancements to the Cisco 12000 Series routers deliver 40 Gbit/s of capacity per slot—doubling the world's largest IP/MPLS core networks without a forklift upgrade.

Looking ahead, service providers face equally dramatic challenges as they seek to transform their infrastructures for the next networking evolution.

"Innovations, especially in the network core, have always defined Cisco as the networking market leader and will continue to do so in the future," says John Doyle, director of marketing for Core and Edge products at Cisco. "The new challenges our service provider customers face will be to dramatically decrease capital and operational burdens of managing multiple overlay networks by moving to a converged architecture. This movement will also allow them to deliver innovative, profitable services faster and more efficiently. Most important, they will need to simplify their IP/MPLS networks through POP [point of presence] consolidation and flattening, to eliminate costly redundancy and overly complex tiered architectures."

A History of Innovation

Cisco software and hardware have often defined the direction of the networking industry. With its introduction of the AGS multiprotocol router in 1986, Cisco transformed the landscape of the internetworking market, at that time dominated by bridged networks. With the AGS router companies could, for the first time, build larger, more reliable networks without concerns about issues such as broadcast storms and suboptimal logical topology.

By 1994, Cisco showed its strength in software with the introduction of IP Multicast technologies that would enable massively scalable, efficient distribution of data, voice, and video streams to hundreds, thousands, and even millions of users.

The Cisco 7500 Series Router, introduced in 1995, again moved the industry into a new phase, playing a key role at the foundation of the Internet. In 2000, *Network Computing* magazine named the Cisco 7500 Series the third most important product of the decade to shape the networking industry. The first two products were the NCSA Mosaic Web browser and Novell Netware 3.x.

Technology innovations for the Cisco 7500 Series included a new distributed architecture and switching engine that pioneered the use of shared port adapters via Versatile Interface Processor (VIP) cards. The Cisco 7500 Series was the first multigigabit backplane router from Cisco. The distributed architecture allowed service providers to begin scaling their networks by taking the processing load off the main CPU and distributing it to line cards with their own processing capabilities. Another first on the Cisco 7500: it had a packet-over-SONET (POS) interface—a revolution in simplifying how Internet and IP traffic are carried over long distances.

The new, market-changing products from Cisco began enabling service providers to rearchitect their networks—from multiple, disparate networks built largely on circuits and the PSTN to networks built around packets. Over time, the concept of the network as a service-delivery platform began to emerge. Rather than merely deliver pipes, the new packet network would provide a single point of control, offer a ubiquity of implementations, provide end-to-end services, and bring dramatic cost advantages.

Cisco 12000 and the Shift to IP/MPLS

As bandwidth demand continued to escalate on the Internet, service providers looked not only for more performance from their core routers, but also for the ability to rise above commodity pricing by delivering more *intelligent* services. In 1997, Cisco delivered the 12000 Series, the first router built specifically for service providers and carrier customers seeking to meet the extraordinary demands of scaling the Internet backbone and IP networks. The Cisco 12000 Series offered the first completely distributed, modular router with the ability to seamlessly scale—more than 100 times the original capacity to date—without being taken out of the network and replaced by an entirely new appliance.

The Cisco 12000 Series helped usher in the era of MPLS, an Internet Engineering Task Force (IETF) industry standard that was based on the Cisco innovation "Tag Switching," which combined the scalability and control of Layer 3 routing with the performance and traffic management of Layer 2 switching techniques. Using a system of labels (tags) to associate data with destination and quality of service (QoS), and employing Layer 3 and Layer 3 techniques, enables high-performance services, packet- or cell-based infrastructures, and end-to-end service definitions and QoS.

By combining the intelligence of IP routing with the performance of switching through label-switched paths, MPLS allowed service providers to perform traffic engineering in their network backbones, and enabled scalable virtual private networks (VPNs) and end-to-end QoS. This gave providers the ability to deliver highly scalable, differentiating end-to-end IP services with simpler configuration, management, and provisioning for both themselves and their subscribers.

Innovative Investment Protection

Cisco recently introduced significant enhancements to the Cisco 12000 Series that reveal another unique perspective on Cisco innovation—protecting the investments of its customers. The Cisco 12800 Series delivers 40 Gbit/s of capacity per slot and doubles the capacity of the world's largest IP/MPLS core networks.

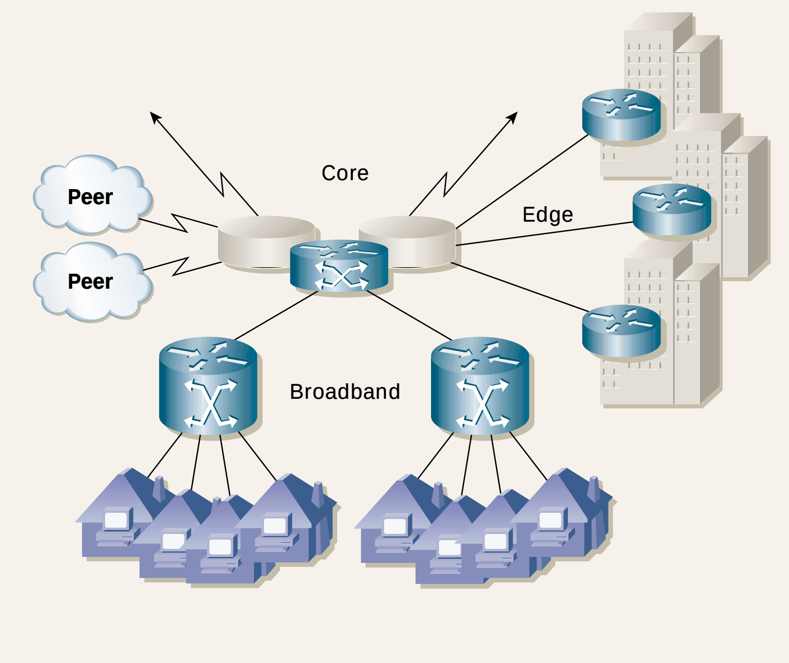
"What's really significant here is that our longtime customers who have Cisco 12016, 12416, and 12410 routers can install the new switch fabric cards in these platforms in the field—immediately doubling the capacity of their existing networks without complete equipment upgrades or changes to their power or cooling infrastructures. Customers also can use all of their Cisco 12000 Series line cards in 40-Gbit/s-per slot Cisco 12800 Series routers," says Mike Volpi, senior vice president and general manager in Cisco's Routing Technology group.

Cisco also introduced new 2-port OC-192 POS and 8-port OC-48 POS line cards that add architectural flexibility to the Cisco 12000 Series and allow these platforms to migrate to the edge in an IP/MPLS network. These 50 million-pps line cards deliver wire-speed performance with a rich set of IP/MPLS features including *Nonstop Forwarding (NSF)* and *Stateful Switchover (SSO)*, extending access control list (ACL) support for more than 32,000 entries and enhanced scalability for VPN and multicast applications.

Another example of investment protection and further strengthening edge MPLS services, Cisco

FIGURE 2: The greatly simplified POP will consist of one or a few core routers with interfaces and features for core, peering, and edge services. Each slot on this carrier-class router will generate revenue because it will no longer be needed to provide connections with aggregation or peering routers.

THE CONSOLIDATED POP



recently introduced a new route processor, the Supervisor Engine 720-3BXC for the Cisco 7600 Series. This supervisor engine enhances the role of Cisco 7600 as an edge device: as a label edge router for pure MPLS-based networks and as a provider edge device for MPLS VPN networks. The numerous interface speeds and media types available on the Cisco 7600 enable the aggregation of various types of transport traffic across an MPLS-based Layer 3 core.

New Demand for Edge Services Drives Further Innovation in High-End Routing

While service provider networks are scaling to handle continued bandwidth growth and new demand for edge services on IP/MPLS networks, most service provider networks still comprise many disparate networks: Layer 2 Frame Relay and ATM; the PSTN; optical networks; mobile networks; and others. And while this patchwork of networks is meeting customer demands, it is no longer the most efficient method for service providers to operate.

"We see several pressing factors hindering service provider profitability," says Doyle. "First, voice revenues are in decline and data services are becoming commoditized due to a maturing marketplace and flat-rate, bandwidth-based revenue models. Also, legacy circuit networks based on TDM, Frame Relay, and ATM are offering little revenue growth potential because they can't deliver innovative or unique new services. Most challenging is that they require individual management, monitoring, and provisioning systems, which contributes to high OPEX [operating expenses] and slow service delivery."

To become more profitable in the changing market and landscape, service providers are looking for ways to decrease the capital and operational burdens imposed by maintaining and managing multiple overlay networks, while continuing to support their existing service offerings for the foreseeable future. They must also be able to deliver innovative, differentiating, and profitable new services to a broad market while avoiding commoditization. And they must simplify their IP/MPLS network infrastructures using highly available routing systems to eliminate costly redundancy and overly complex tiered architectures.

To achieve these goals, service providers are focusing on convergence—the consolidation of legacy Frame Relay, ATM, and voice traffic onto a common IP/MPLS packet network. This will enable them to reduce the capital and operational expenses of operating multiple overlay networks. It will also improve manageability—only one network with vastly fewer networking elements will need to be managed, monitored, and provisioned. It will improve service flexibility and reach that will be provided by IP/MPLS ubiquity. And it will deliver economies of scale by leveraging investments in one technology instead of many.

Look at Telecom Italia, for example. Eighty percent of Telecom Italia's voice traffic and 50 percent of its international European voice calls now run over a converged IP/MPLS network. With its voice over IP/MPLS network—the largest VoIP network in Europe—Telecom Italia is saving two-thirds of its transit operating expenses and providing better service to its customers.

The road to a simplified, next-generation network requires that POP architectures be flattened and consolidated, says Doyle. POPs will begin to flatten as the aggregation layer is eliminated. Instead of many routers deployed for aggregation and peering, these functions will merge into a much larger, more capable core router with interfaces and features for core, peering, and edge services. Therefore, each POP will consist of few or even one much larger, capable router. These POPs will easily scale into the tens of terabits. Multiservice edge features will enable new services and will support consolidation of overlay networks.

The full realization of this vision will occur with the fully consolidated POP (see Figure 2, page 73). Here, adding capacity will be nondisruptive and can be done in-service; core routers will offer a multidecade lifespan. Because slots will no longer be needed for connectivity to aggregation or peering routers, all slots on these core routers will generate revenue. POPs will scale easily to tens of Terabits.

◆ ◆ ◆

Cisco's commitment to innovation and to helping service providers meet their technical challenges forges on—and will continue to help redefine the next generation of service provider networks. ▲▲

FURTHER READING

- **Cisco 12000 Series Router: cisco.com/packet/162_8c1**
- **Cisco 7600 Series Router: cisco.com/packet/162_8c2**

Law Firms Partner with Technology

The legal industry is making progressive moves toward converged voice and data networks.

BY JOANNA HOLMES

IT'S SURVIVAL OF THE FITTEST IN THE LEGAL industry, where leaders are coming to recognize that a law firm's network can be a strategic business asset. Accordingly, several top US firms have "right-sized" their networks, creating powerful, intelligent information systems that allow for application-enabled network solutions, including integrated voice, video, mobility, and Web application optimization. These firms are making mission-critical applications such as unified messaging, time tracking, and corporate databases more accessible to their attorneys. They're also adopting new horizontal business applications, such as IP communications, security, videoconferencing, and network-enabled collaborative tools, which have driven tremendous improvements in their overall business by increasing productivity, collaboration, and customer satisfaction, while lowering operational expenses.

JOHN MCFAUL

Changes Afoot in Business Climate

The last decade has seen a major reshaping across the legal industry's landscape. Ongoing industry consolidation and increased competition for top clients are among the changes that leave law firms struggling to stay competitive. The client profile is changing, too: Clients demand new services and more immediate access to attorneys and information.

In parallel with these changes, some firms place increasing emphasis on high-value work, such as mergers and acquisitions, while others are moving from time-based billing models to a commoditization of services into fixed-price products. These new models force law firms to maximize efficiencies and explore new ways of streamlining business operations.

"Some very dramatic changes are in play that have not been seen since the opening of the Old World trade routes," says Mark Chandler, Cisco's vice president of legal services and general counsel. "In part as a result of technological advances, business productivity has increased exponentially. The legal industry is not exempt. The Internet and new networking technologies can be instrumental in helping law firms stay competitive. The Internet is driving both law firms and legal departments to be gateways to information, rather than gatekeepers."

That's why, in the traditionally technology-shy world of the legal industry, many forward-looking firms are now moving their business to integrated voice and data networks. Such investments can help lower their costs and increase both their productivity and their responsiveness to clients. They also enable open internal team communication, client collaboration, and improved responsiveness to clients—three mission-critical success factors.

The Empowered Law Firm

Supporting more than 70 percent of the top law firms in the US, Cisco offers a "right-sized" suite of network solutions for the legal sector, including application-enabling voice, security, and wireless network services. In 2003, Cisco unveiled its vision for the "Empowered Law Firm" at LegalTech Chicago. "As a basis for that vision, we partnered with Gartner research analysts to conduct custom research with business and technical decision makers to find out their needs," says Rod Kay, director of marketing for Cisco professional services. "We're confident, based on the positive response, that our Empowered Law Firm solutions hits the mark."

The Empowered Law Firm targets several key solution sets geared to create workplaces that are:

- Collaborative
- Connected
- Streamlined
- Responsive
- Protected

Efficiency and Improved Collaboration

Law firms increasingly recognize that innovative, networked applications can help them differentiate themselves from competitors by delivering superior client service. A converged Cisco network paves the way for a collaborative workplace where legal organizations can improve overall efficiency and enable staff to be more productive, responsive, and client-focused. Using the network for processes such as knowledge and document management; time management and billing; client collaboration; and e-discovery and research, applications can boost productivity, lower costs, and strengthen client relationships.

Support for these advanced applications calls for a network infrastructure that provides performance and ease of use for employees and clients. One way that law firms can boost efficiencies and collaboration is through IP telephony. Cisco IP communications solutions and products like Cisco call-processing software and Cisco Unity™ Unified Messaging can introduce voice capabilities that save time and increase attorneys' ability to respond rapidly to clients.

At the Los Angeles-based law firm of Alschuler Grossman Stein & Kahan LLP, IS Director Ali Shahidi recently led a migration to a converged, Cisco-based voice and data infrastructure when the company of 260 employees moved to new offices. The Cisco solution's ease of use has been a catalyst for enhanced productivity throughout the firm. For example, Shahidi says, "Attorneys can listen to their e-mail on the telephone, or, with Cisco Unity, they can get all their voice mail in a unified mailbox. They can even forward voice messages that originated internally to an external client, via e-mail." Previously, Shahidi explains, those same voice messages would have been transcribed by a member of support staff and sent as memos—a far slower and more labor-intensive process.

Network Resilience

More than ever, law firms rely on networks to serve clients effectively. In the connected workplace, the network infrastructure must be highly resilient, minimizing unplanned downtime and providing unstoppable support for critical applications.

Among those law firms most attentive to network resilience are those who experienced firsthand the events of September 11, 2001. One year after those attacks, the 381-employee firm of Thacher, Proffitt & Wood, formerly located in Tower Two of the World Trade Center, rebuilt its offices in downtown Manhattan. The calamity afforded TPW an opportunity to completely rebuild, and they opted for a network core based on Cisco products, replacing their PBX-based telephony system with a Cisco-based IP communications system.

"Everything we do now is redundant, because of 9/11," says Dierk Eckart, TPW's IT director. To ensure that no outage interferes with vital communications, TPW uses redundant Cisco CallManager and Unity servers in its New York and New Jersey offices. "It would have been entirely cost-prohibitive to do that with a traditional phone system, or even a hybrid system, and achieve the level of redundancy that we've established with a few redundant Cisco CallManager instances," Eckart notes.

Like TPW, New York-based Hahn & Hessen took advantage of its corporate relocation to upgrade its network. The 70-year-old firm of 100 employees moved from the Empire State Building to a more upscale midtown Manhattan address, and in the process installed an end-to-end Cisco network encompassing voice and data communications.

"Our clients are very sophisticated financial institutions, and they're at the leading edge of technology," says John Amato, Hahn and Hessen attorney and member of the firm's management and IT committees. Like any business, though, Hahn & Hessen couldn't risk downtime or network outages.

The IP communications component of the new network is one that Hahn & Hessen reviewed particularly carefully before approving the decision. "IP-based voice technology was still maturing in 2002, and not many law firms were going that route back then," says Nicholas Lucenko, Jr., IT manager for Hahn and Hessen.

Ultimately, the solution's rich capabilities were what sold them. "We've actually increased our core phone system resiliency by 500 percent," Lucenko comments.

Mobile and Responsive

Attorneys are under escalating pressure to be responsive around the clock, both inside and outside the office. They travel to client sites, working from hotels, airports, or home. To respond to clients and colleagues quickly and maximize productivity, legal professionals need a responsive, protected workplace that provides secure, real-time access to case information and communication tools, wherever they are.

Virtual private networks (VPNs) are an increasingly vital tool in this network landscape, because they afford not only reliable connectivity, but also a high level of security. Likewise, Cisco products such as the Cisco PIX® 501 Firewall enable legal staff to work securely from home or in small, remote offices.

At Hahn & Hessen, Nicholas Lucenko plans an initiative to give attorneys broadband access in their homes, improving productivity and adding more billable hours to the work week. His vision calls for direct VPN access into the firm's network, with not only soft phones, but even hard phones (handsets) in attorneys' home offices. "For example," Lucenko says, "using a Cisco 501 PIX Firewall, we could tunnel from a partner's home office directly into our network through a VPN. The connection would be up 24x7 at the home office, and the partner would use a handset phone to make calls that are routed through our system and billed to clients. And the calls would be billed to the firm at better rates than if the call was placed on the attorney's home phone."

Lucenko sees firsthand how his firm's Cisco IP communications deployment has enabled new degrees of mobility—and responsiveness to clients—among attorneys. Lucenko recalls two partners at Hahn and Hessen whom he describes as "not really technically savvy." But, he observes, "Every morning on their commute, they're listening to their e-mail through their voice mail." The text-to-speech feature of Cisco Unity Unified Messaging converts text to a user-friendly wave format, so these partners can listen and respond to messages long before they reach the office.

The Hidden ROI

Law firms that invest in the advanced capabilities of Cisco networks are often surprised by many fringe benefits that bolster the firms' bottom lines.

The Pearl Law Group in San Francisco, named in 2002 as one of *Inc.* Magazine's fastest-growing US companies, created a streamlined workplace by deploying a sophisticated Cisco network infrastructure to support its service-based business model. A small company of 32 employees, PLG built a client-facing extranet that enables the firm to fast-track business processes through an Amazon.com-like self-service model for clients. But what PLG CEO and co-founder Julie Pearl didn't expect was how the network technology would draw some attractive clients, not to mention a strong talent pool from all over North America.

"Our ROI is most measurable in terms of new clients," says Pearl. "We recently received a call from a large biotech firm; they found us on the Web. Their in-house counsel felt that attorneys with a strong Web presence would also be technologically savvy. Reading on our site that we're promoting the technology we're using brought them to us."

"Possibly the strongest case for investing in technology is something you can't see—the clients you're not getting today," Pearl concludes.

Law firms that fail to address to address the challenges and business opportunities in today's turbulent legal marketplace are unlikely to thrive in the coming decades. The winners will be those firms that can reengineer their operations to dynamically connect people, expertise, and resources across multiple offices—regardless of geographic location—into highly responsive virtual organizations. In realizing this goal, law firms will reduce costs and develop high-value, flexible, cost-effective support capabilities. ▲▲

Streamlined Operations for IT Staff

While law firms are coming to recognize the network as a strategic business element, many firms have limited technical resources. They need networks that provide robust administration and troubleshooting tools, yet are easy to deploy, manage, and maintain.

Replacing a PBX phone system with the rich voice capabilities of a Cisco network is one way law firms can streamline their network administration. For Thacher, Profitt & Wood, that simplification started from day one. "When we moved into our new building," says TPW's Dierck Eckart, "we didn't even run wiring for phones—just data jack wiring."

At AGSK, "very easy" is how Ali Shahidi describes his firm's Cisco IP telephony network administration. "If someone has already done some PBX setup, they can easily adjust and use the IP telephony system," he says. "But better still is that IP telephony administration is much closer to network administration, so the administrative resources you need would be the same resources you need for your data network."

Shahidi recalls the labor-intensive process of managing moves, adds and changes in the days when AGSK used a PBX for its voice network. These days, the firm's network administration is a centralized process that relies on the flexible Cisco IOS® Software.

Smooth Sailing

A robust network helps SMBs navigate choppy waters.

BY JAMES A. MARTIN

This article is excerpted from iQ Magazine. *Newly refocused, iQ addresses the challenges faced by small and midsized businesses (SMBs) and explores how technology can help them succeed and grow. For the full article, along with a wealth of other content to help SMB executives improve their bottom line and work smarter, see the Second Quarter 2004 edition of* iQ Magazine *at cisco.com/go/iqmagazine. —Editors*

For many SMBs trying to sail to success in an increasingly networked economy, the waters have grown choppy. Computer viruses, worms, spyware, and hacker attacks are now a daily threat to network security, and SMBs that lack the IT resources of larger enterprises can be particularly vulnerable. Moreover, many SMBs face new government regulations that place even higher demands on securing digital assets. And unpredictable events, such as power outages resulting from severe weather, natural disasters, or strains on an aging electrical infrastructure, affect all businesses, whether it's a small restaurant in Toledo, Ohio, or a large bank in New York City. SMBs must put systems in place to recover rapidly from these events to keep their businesses running smoothly.

Meanwhile, many of these SMBs are still competing with large corporations equipped with sophisticated, global network infrastructures, as well as trying to satisfy the operational demands of their enterprise customers. Wal-Mart Stores, for instance, only works with SMB suppliers or partners who can electronically interact with them for invoicing, shipping and receiving, and other business-to-business transactions.

"To compete in an increasingly networked economy, SMBs must understand the relevance of a robust network architecture and how it can apply to their particular business," says Kneko Burney, chief market strategist for customer and service provider markets for research firm In-Stat/MDR. "A strong network can help small companies grow bigger and help them save time, which is their most precious asset. SMBs simply don't have enough time to do all the things they need to do."

Fortunately, many networking-hardware components, applications, and other products and services today are designed specifically for SMBs to address the new business environment. "These products aren't simply scaled-down versions of enterprise products," notes Andy Bose, chief executive officer of research firm AMI-Partners, Inc. (see sidebar, "New Solutions Just for SMBs," page 79).

Indeed, many SMBs are already realizing that a robust network isn't out of reach. A Gartner study estimates that overall IT spending by SMBs from 2003 to 2004 will increase by 5 percent. Among organizations with 5 to 99 employees, 36 percent say they will increase spending; likewise, 44 percent of organizations with 100 to 499 employees, and 36 percent of organizations with 500 to 999 employees say they will make increases. Networking/telecommunications was the highest-ranked IT spending priority among organizations with 500 to 999 employees and a close second in the other two SMB categories.

Securing the Network

To determine the network solutions that best suit their needs, SMBs must first assess their current and potential business challenges and determine how a robust network can help overcome them. For instance, in this era of rampant computer viruses and other threats, security is often an SMB's No. 1 network concern. Security is particularly essential to organizations that have highly confidential data, such as healthcare and financial institutions.

Often, it's necessary to secure parts of a network from internal users as well as from potential outside intruders. Rocket Software, a software development company with 210 employees, maintains multiple levels of security throughout its Cisco IP network to prevent engineers working on one proprietary project from accessing information related to another proprietary project, says Troy Heindel, Rocket's chief information officer. "We have significant confidentiality agreements with the large companies we design software for," he explains. "Segmenting our network with multiple levels of security enables us to satisfy our customers' needs."

Being Fast on Your Feet

Agility and resilience—the abilities to be flexible and responsive to changing conditions even in adverse situations—are vital to any business. Change can come suddenly in the form of unexpected events mentioned earlier. Change can also be positive, such as the need to quickly add new employees to meet growing customer demand. Ether way, a robust network architecture and the applications that run on it can provide SMBs with high reliability, backup, and redundancy as well as scalability and flexibility.

Out of Rocket's 210 employees, 60 engineers developing mainframe software work remotely and collaboratively from far-flung locations, such as China, Denmark, and Russia. "Without a flexible, robust network," Heindel says, "that wouldn't be possible."

Leveling the Playing Field

A robust, secure network can help SMBs better compete with larger companies, and an advanced network infrastructure can also help SMBs meet the demands of their enterprise customers. Rocket has built a Web-based application that allows Rocket engineers to collaborate online with its large corporate customers, says Heindel.

The application breaks down the barriers that existed between internal and external users in different companies and across varying time zones. The customers require that level of online collaboration, Heindel adds, and without a strong network foundation, Rocket could not offer it.

It's About Time

To be sure, some SMBs may question the return on investment (ROI) a sophisticated network infrastructure can deliver, or the relevancy of such a network to their business. But to be a player in the global, networked economy, the question SMBs should be asking themselves about an advanced network shouldn't be, "Why?" but "When?"

"Though the payback is certainly there, it's not all about ROI," says Rocket Software's Heindel. A networked economy "is where the world is going, and you'll be left behind if you don't seriously look at how an expanded network applies to your business."

Put another way, a sophisticated network can help SMBs navigate through choppy seas, adeptly dodge bigger boats, and have the time to relax when, at last, they reach calmer waters. ▲▲

FURTHER READING

- **Cisco SMB Class products and services: cisco.com/packet/162_9b1**

New Solutions Just for SMBs

Kevin Outcalt, senior director of commercial marketing for the Worldwide Commercial Market segment at Cisco, explains the elements and benefits of the recently unveiled SMB Class solutions.

iQ: What is SMB Class?

Outcalt: SMB Class provides SMBs with a suite of easy-to-use network solutions designed specifically to help them meet their top business challenges, such as productivity, security, customer satisfaction, profitability, and business agility. With the help of our channel partners, we can now deliver complete network solutions that are appropriately sized for each customer, rather than offering a one-size-fits-all package or a scaled-down version of a larger network solution.

iQ: What are the elements of SMB Class?

Outcalt: SMB Class solutions include service and support; training; financing; and applications. For example, we've priced our service and support solution, SMARTnet®, to provide SMBs with a better value. SMBs often have only one or two people on staff performing all IT functions, so SMB Class solutions offer a wide variety of e-learning resources that provide a much deeper technical understanding. SMB Class also offers a quick and easy application process for financing, fast turnaround, and aggressive pricing on a variety of lease options on such solutions as IP telephony. And we have developed appropriately sized applications that increase an SMB's ability to collaborate, such as Cisco Unity™ Express unified messaging solution and Cisco IP Contact Center. We've also partnered with Microsoft to promote its Microsoft CRM application with our IP communications platform to help SMBs more effectively respond to their customers.

iQ: What is the value of SMB Class?

Outcalt: We listened to the SMB market, and now we're delivering to SMBs what they need: a complete end-to-end network solution. Along with that, SMB Class provides world-class local support, intelligent networking services across the infrastructure, security, and scalability. And most of all, SMB Class provides businesses with peace of mind, because they know that all the pieces of their network fit together.

By GENE KNAUER

Though many predicted its demise with the growth of Internet banking, the bank and credit union branch office has not gone the way of the dinosaur. Far from it. Today, the branch is the epicenter of a major transformation as separate point-to-point networks with limited services give way to converged data, voice, and video networks running over IP. Cisco is focusing an array of products and technologies to meet the needs of branch environments. Financial institutions in particular have been quick to embrace branch transformation.

"Bank and credit union customers want to be able to use all of the different channels of communication—the branch, the Internet, ATMs [automated teller machines], and contact centers," says Jim Bright, industry marketing manager at Cisco. "Sometimes you can solve things face to face that you can't solve otherwise. With a big deposit or transaction, many people want to come to the branch to do that. But the branch customer is more sophisticated now; they want to know about their accounts and find out about other products. And institutions see the opportunity to migrate off of older, less efficient networks and computing platforms and to become more efficient and competitive."

Many financial institutions have already warmed to the idea of lower total cost of ownership from converged IP data, voice, and video networks in their branches. The benefits in higher reliability and easier management of vertically integrated networks are clear. They are enabling higher employee productivity, better customer service, and better security with network applications such as IP telephony; IP public branch exchanges (PBXs); video applications for staff and branch customers; IP-enabled ATMs and kiosks; IP video surveillance systems; and wireless LANs. Branches are beginning to view their networks as platforms for doing business better, more efficiently, and more profitably.

Cascade Bank Converges Voice Networks

Serving the greater Seattle, Washington, area, Cascade Bank was one of the first institutions of its kind to offer online banking. Yet when the bank looked at enhancing efficiency in the branches, Robert Gamboa, senior vice president of information services, saw 14 branches, each with its own phone system and varying system capabilities from branch to branch. Customers calling one branch phone number couldn't be transferred to bank personnel in another branch. Although Cascade had some Off-Premises Extension (OPX) lines that could conference the customer to the right person, these lines were limited in capacity and features. At Cascade's home office, the phone system was also "failing."

Working with a local Cisco partner, NEC BNS, Cascade chose Cisco AVVID (Architecture for Voice, Video and Integrated Data) to consolidate T1 lines under one service provider cloud and build an integrated voice and data network. By converging to a voice over IP (VoIP) phone system and using Cisco CallManager call-processing software for call routing and Cisco Unity™ Unified Messaging for voice mail, employee productivity, cost savings, and customer satisfaction have all increased dramatically.

"We've reduced overall network costs by 25 percent," says Gamboa. "By using the AVVID toll bypass feature, we have seen a significant decrease in our long-distance bill, because many calls are between branches."

According to Gamboa, the bandwidth available for data was doubled when the bank eliminated all of the separate network interfaces, which provided the additional capacity for voice applications.

"By introducing an IP contact center, we no longer have stopped, dropped, or lost calls," says Gamboa, "and the functionality increase is considerable. We can now route calls right to any handset within our operations, help desk, and information services departments. We're clearly seeing improved service and response times." Using the unified messaging capability of Cisco Unity, bank employees can view voice mail in their e-mail inboxes.

First Albany Capital—Reducing Costs, Increasing Reliability of Hoot 'N Holler Network

Independent investment bank and asset management firm First Albany Companies, Inc., based in Albany, New York, has used an always-on Hoot 'N Holler network for high-level customer service. Hoot 'N Holler networks are specialized audioconference networks commonly used in the brokerage industry. Brokerage firms can spend millions in monthly leased-line charges to pay for dedicated circuit-switched Hoot 'N Holler long-distance connections. The application provides an open channel for audio-conferencing between traders

JOHN RITTER

in different locations, especially during a morning call. During the rest of the day, the channel is open for instant communication of stock-related information and customer orders.

"It was expensive, and because it was an analog system it required individual drops to each remote office, so it was costly," says Chat Herrgott, First Albany chief technology officer.

The system was also vulnerable to failure; if any of the leased lines or analog connections went down, that office lost its connection with the Hoot 'N Holler service. The cost for creating redundant connections to each office was prohibitively expensive.

First Albany Capital chose to replace its old solution with Cisco Hoot 'N Holler over IP (HHoIP), deployed on the organization's existing Cisco-based WAN. Cisco 2621XM routers were upgraded with NM-2V voice modules and voice interface cards. Two Cisco 2621 routers connect each office with dual Cisco 7507 routers in each of three main offices in Albany, NewYork City, and Boston.

"We use two service providers for even greater redundancy," says David Hughes, manager of network and server infrastructure at First Albany, who estimates that uptime on the WAN is close to 99.999 percent.

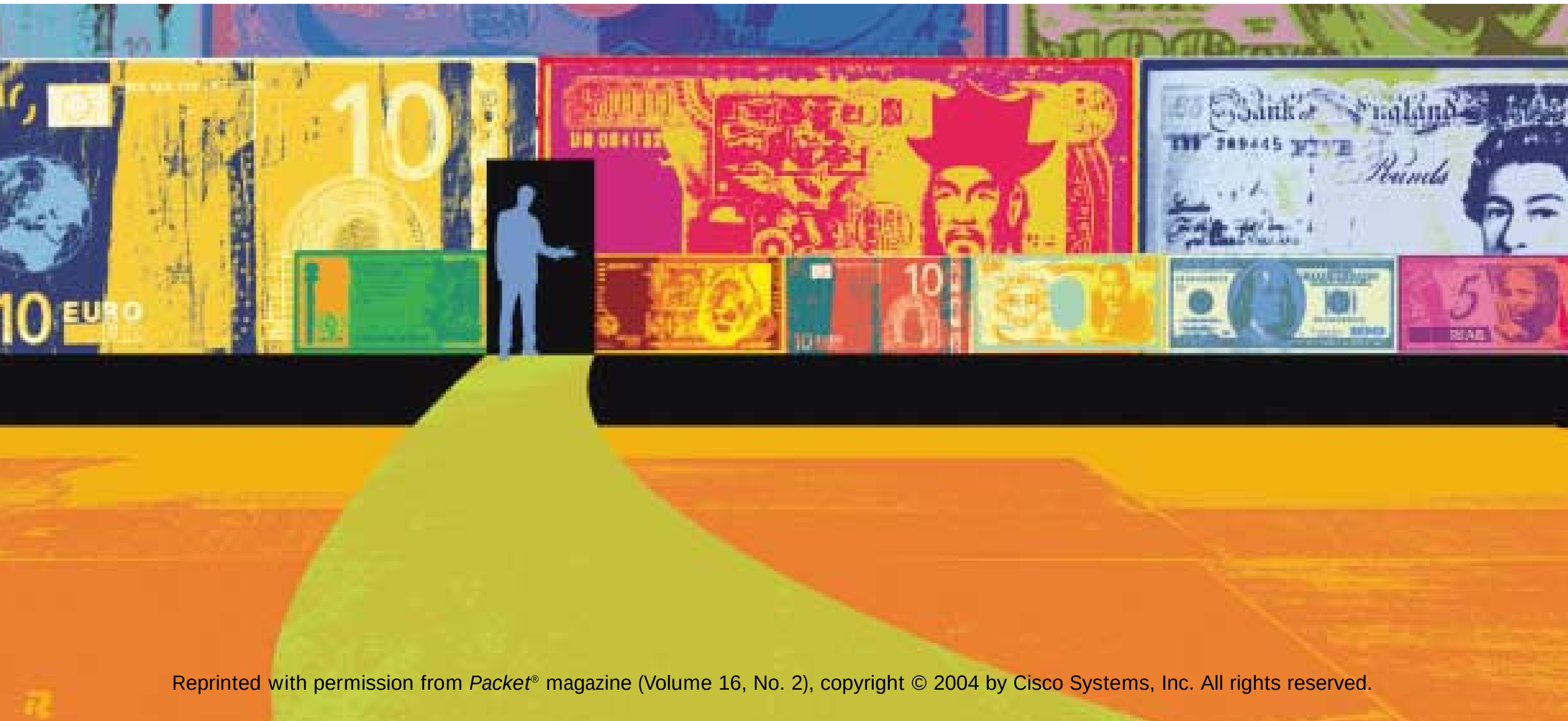
Future plans include expanding access to the HHoIP solution beyond end terminals to desktop PCs, home offices, and, if First Albany implements VoIP, to IP phones.

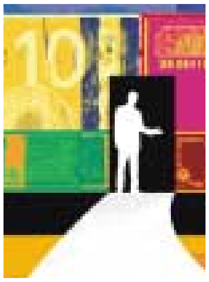
Municipal Credit Union of New York—Branch Video Programming for Entertainment and Profit

The Municipal Credit Union of New York serves 350,000 members and manages US$1.1 billion in assets. With 10 branches, the organization has a lot of customer foot traffic each week. Chief Technology Officer Barry Grant concentrated first on expediting the waiting time in branches by

Branching Out

Financial institutions transform the way they do business with the Cisco "Branch of the Future."





installing ATMs and kiosks for self-service but realized that for certain transactions, customers would always wait in line to see tellers.

Already running IP telephony, the credit union decided to implement a video content delivery network solution that would give customers standing in line daily news feeds interspersed with commercials on Municipal Credit Union products and services.

The credit union chose the Cisco Application and Content Networking System (ACNS) solution to deliver rich streaming video content to branch offices using the IP network already in place. A Cisco Content Distribution Manager (CDM) is used to manage and distribute content to the Cisco Content Engines deployed at the branch offices, allowing the Municipal Credit Union to quickly and easily update its play lists without worrying about shipping videotapes to the branches. A Cisco Content Engine 507AV pushes promotional and informational content to monitors in the branches.

The content delivery network can also be used to conduct e-learning for branch employees and broadcasts from headquarters. Content engines can cache video overnight during off-peak hours and have it available in the morning.

The Municipal Credit Union is moving next to creation of IP contact centers using the existing Cisco WAN, which will allow any employee—even those based in home offices—to function as call-center support personnel. Virtual private networks (VPNs) using Cisco features in Cisco IOS® Software will connect employees securely outside of the credit union's firewall.

Other Branch of the Future Initiatives

A VoIP project using Cisco solutions on a newly converged data and voice network at South Trust Bank in Birmingham, Alabama, is expected to save US$1 million annually on conference calling alone. This institution, with more than 700 offices, also gained a dependable disaster recovery failover solution, replacing nonredundant legacy phone systems.

A converged Cisco IP data and voice network is in place at American Savings Bank, which has 68 branches throughput Hawaii. The Cisco solution uses the SAFE Blueprint for security and VPNs. Cisco PIX® 500 Series firewalls deliver Stateful Inspection Firewalling, protocol and application inspection, intrusion protection, and specialized security for voice and multimedia services.

"Cisco VPN products give our remote office and mobile workers secure access to the network," says American Savings Bank Chief Information Officer Craig Lee. "This is a great benefit to employees on call around the clock, those working from home after hours, and our sales force on the road."

Two hub sites have two Cisco 7200 Series routers that provide data encryption and quality of service (QoS), and are connected to Cisco Catalyst® 6006 distribution switches. Branch offices use Cisco 3660 and 3640 series multiservice routers for VPN connections to T1 lines. Cisco Catalyst 3524 XL switches connect the network to Cisco 7960 Series IP phones and desktop PCs.

Data and voice packets are protected by IP Security (IPSec) and Triple Data Encryption Standard (3DES) features in Cisco IOS Software. Cisco CallManager software extends enterprise telephony features to branch phones and supports unified messaging, multimedia conferencing, and collaborative contact center solutions.

"A week after we activated our Cisco VoIP system, we moved 70 employees to our new corporate headquarters," says Lee. "We literally unplugged the Cisco IP phones from their old locations, moved to the new offices, plugged them in, and everything worked."

New Trends in the Full Service Branch

"Increased government regulations have made Cisco's self-defending network (see "The Self-Defending Network" in the First Quarter 2004 issue of *Packet*®) features and the Cisco SAFE blueprint for security of major interest to financial institutions," says Rune Olslund, Cisco's industry solution manager for small to midsized financial services companies. "We are helping our customers to implement branch solutions that pass audits from regulators. That includes full solutions for business continuity in case of catastrophic failures, network access control, and intrusion detection."

A new US government initiative, the Check Clearing for the 21st Century Act—Check 21—which will become effective later this year, will allow the use of check images in place of original checks to greatly expedite check processing. The 38 billion checks written in the US each year can lead to many bottlenecks for financial institutions. With Check 21, banks, credit unions, retailers, and others can transmit the image of the check for clearance.

"The savings from faster processing, compared with handling paper checks, will drive institutions to implement the infrastructure to process checks on the network," believes Olslund. "Putting systems in place to allow businesses to verify funds availability immediately and verify signature authenticity will provide greater operational efficiency and cut down on fraud. Cisco's full service branch network technologies provide the platform to make it happen."

Meanwhile, savings from converged networks, higher productivity, and better customer service from newly implemented network solutions are key drivers of full service at the branch among Cisco customers.

"We're giving our customers not just an optimized network platform but a better, adaptable platform for doing business with measurable benefits from day one," says Jim Bright of Cisco. ▲▲

FURTHER READING

- **Cisco Branch of the Future: cisco.com/go/bank**
- **Cisco Full Service Branch transformation: cisco.com/packet/162_10a1**
- **Article on the Cisco Full Service Branch: cisco.com/packet/162_10a2**
- **Article on Cisco and IBM Alliance for Branch Transformation: cisco.com/packet/162_10a3**
- **Check Clearing for the 21st Century Act (Check 21): federalreserve.gov/paymentsystems/truncation/default.htm**

JOHN RITTER

Understanding RFID

BY ROB REDFORD

Chances are that you're already familiar with RFID, or Radio Frequency Identification. Essentially, RFID is an "electronic bar code," and RFID tags are used to wirelessly identify inventory or products. Do you have an employee badge that you place *near* a card reader, rather than swiping it through the reader? An E-ZPass tag on your windshield for automatic toll deduction? These are examples of RFID.

Combined with a network, RFID promises to realize its full potential and fundamentally change the way businesses manufacture, distribute, and sell products, as well as the way consumers buy and use them.

How RFID Works

RFID tags exploit the basic properties of electromagnetic (EM) fields to power a small radio frequency (RF) transmitter. An antenna collects the EM radiation and the resulting energy is used to transmit a unique ID code. Currently, this code can be up to 128 bits, which is far more information than can be encoded in a bar code. So significantly more information can be associated with an item—color, place of purchase, model, size, expiration date, etc. The tags are also unique to the unit, unlike a bar code that only identifies a whole category.

The advantages of this wireless approach are that units can be tracked individually, line-of-sight access to the item is not required to sense it, and multiple tags can be read simultaneously. Imagine an auto manufacturer that can determine every car part by serial number simply by scanning it, or an overnight delivery service that can locate every package in its system any time. Finally, consider the consumer implications: truly enabling the "store of the future," where you place items in your shopping cart and bypass the checkout line because the RFID scanners detected all of your purchases and charged your credit card (see "A Trip to the Future Store," Fourth Quarter 2003 issue of *Packet*® at cisco.com/packet/162_11a1).

Why Is RFID Hot?

RFID technology has existed for years, so why is it now such a hot topic? The cost of tags has been steadily declining, from a few cents today to a fraction of a cent in the near future as volume increases. The "tipping point" is about one-half cent US. At this low cost, it is economically feasible to build an RFID tag into every product or package. Furthermore, carbon ink can now be used to "print" the antenna, increasing flexibility and making the tags more reliable. A recent study by Venture Development Corporation projects a 37 percent compound annual growth rate (CAGR) for RFID by 2005.

While RFID is a "wireless" technology, it differs from IEEE 802.11 Wi-Fi data networking technology. But it's the combination of RFID with network technology that's creating excitement. Because RFID is just an identification mechanism, networks have to connect data from the RFID readers and transmit this information to the application or database. To enable an entire supply chain, networks at different locations must be connected and tied into a central tracking application.

RFID-ready networks based on new, open standards such as Electronic Product Code (ePC), ePC Information Systems (eIS), and Physical Markup Language (PML) will significantly reduce infrastructure costs and enable much greater scalability than today's proprietary reader/server implementations. The benefit for businesses is real-time collection of end-to-end supply-chain data, creating an opportunity for radical business process optimization. Consider the business implications of knowing where each unit of your entire inventory is any time or knowing exactly which items on your display shelf will expire in a week. With detailed information readily available over the network, businesses can implement revolutionary inventory, distribution, and retail processes.

RFID can benefit a wide range of businesses. For example, a healthcare worker could instantly locate the nearest emergency medical equipment. This requires an interconnected network throughout the entire supply chain at each stage of the business process, as well as with suppliers and partners. This network must also possess the right enabling technologies such as quality of service (QoS), security, and management. Networking the readers could be accomplished with power over Ethernet (PoE), a standard that is quickly taking hold in the process automation industry (for more on PoE, see page 19), or fixed or mobile RFID readers that use 802.11 Wi-Fi connectivity.

The implications for consumers are equally significant. One example: With RFID readers in your kitchen, your computer could give you a list of recipes you can make with the items you have available. The possibilities are endless.

All of the elements are in place for RFID technology to take off in the near future: the declining cost of RFID tags, open industry standards, and enabling technologies such as PoE and 802.11 Wi-Fi. ▲▲

ROB REDFORD

ROB REDFORD is vice president of Product and Technology Marketing at Cisco. A frequent presenter at conferences, he has published many technical and business papers and articles and is a member of the editorial advisory board of *Telecommunications Magazine*. He can be reached at rredford@cisco.com.

New Product Dispatches

Cisco IOS Software

Cisco IOS MPLS Virtual Private LAN Service

Cisco IOS® Multiprotocol Label Switching (MPLS) Virtual Private LAN Service (VPLS) technology connects a large number of geographically-dispersed sites into a single LAN infrastructure. Network resilience is increased with innovative services such as MPLS Fast Reroute for Any Transport over MPLS (AToM) circuits, quality of service (QoS) guarantees using Differentiated Services (DiffServ), and better bandwidth utilization with MPLS Traffic Engineering. VPLS technologies emulate the traditional Layer 2 infrastructure enabling a smooth mitigation to an IP/MPLS network. VPLS technology is covered in greater detail on page 23.

cisco.com/packet/162_npd8

Edge Routing, Access, and Aggregation

Cisco 7600 Series Routers and Cisco Catalyst 6500 Series Switches: New Gigabit Ethernet Module

The 48-port Mixed-Media Gigabit Ethernet Module for Cisco Catalyst® 6500 Series switches and Cisco 7600 Series routers offers service providers increased flexibility and scalability in high-performance metro networks. The module provides 48 small form-factor pluggable (SFP) optics to address a mix of media types and distances. Features supported by the module include 40-Gbit/s switch fabric connections for 48 Gigabit Ethernet ports; 9K Jumbo Frame-size support, and upgrade to Distributed Forwarding capability with daughter card options.

cisco.com/go/catalyst6500

Cisco 2600, 3660, and 3700 Series Routers: Network Analysis Module

The new network analysis module (NM-NAM) for selected Cisco 2600, 3660, and 3700 series routers provides multiservice traffic monitoring in enterprise branch offices for troubleshooting, capacity planning, and managing network-based services. An embedded, Web-based traffic analyzer supports real-time and historical monitoring of LAN and WAN traffic as well as network services such as quality of service (QoS) and voice over IP (VoIP). The NM-NAM optimizes performance with two monitoring interfaces (one internal and one external) and a single processor architecture that supports processing with dedicated 256-MB RAM.

cisco.com/go/nam

Switching

Cisco Catalyst 4500 Series Switches: New Chassis, Supervisor Engine, and Power over Ethernet Line Cards

New hardware choices expand deployment options for enterprise or metro Ethernet customers using Cisco Catalyst® 4500 Series switches. The 10-slot Catalyst 4510R chassis offers scalability up to 336 ports of 10/100/1000 Ethernet as well as two dedicated Supervisor Engine slots for redundancy. The Supervisor Engine V, available for all Catalyst 4500 Series chassis, offers capacity of 96 Gbit/s for scalable, nonblocking Layer 2/3/4 switching with enhanced hardware-based features such as broadcast and multicast suppression and Q-in-Q encapsulation. Three new Cisco Catalyst 4500 Series Power over Ethernet (PoE) line cards provide 48V DC power at 15.4 watts per port over standard Category 5 unshielded twisted-pair (UTP) cable up to 100 meters. The cards provide 48-port 10/100 Ethernet (RJ-45 or RJ-21 options) or a 48-port 10/100/1000 Gigabit Ethernet (RJ-45) option with support for IEEE 802.3af and the Cisco prestandard PoE implementation.

cisco.com/go/catalyst4500

Cisco Catalyst 6500 Series Switches: New Modules and Integrated Services

The Cisco Catalyst 6500 Series offers two new high density modules, a set of Power over Ethernet (PoE) modules, Supervisor Forwarding Engine and 10 Gigabit Ethernet XENPAKs, and integrated services software. **High Density Modules**—A 96-port 10/100 Ethernet module delivers industry-leading 10/100 port density for flexible deployments in compact form factors in the wiring closet, and a 48-port Gigabit Ethernet mixed media module for high density, high-performance Gigabit aggregation in the distribution, core, and data center. **PoE Offerings**—A 48-port 10/100 IEEE 802.3af PoE module, available in RJ-45 or RJ-21 connectors, and 48-port 10/100/1000 802.3af PoE modules for both value and premium wiring closet applications have been added to the Catalyst 6500 Series. In addition, 802.3af PoE daughter card upgrades are available for the 10/100 and 10/100/1000 Ethernet modules for maximum investment protection when migrating to converged networks. **Supervisor Forwarding Engine and 10 Gigabit Ethernet XENPAKs**—With an enhanced field-upgradable Policy Feature Card (PFC3BXL), the Supervisor Engine 720 delivers enhanced security and scalability to the network, and enables deployment of scalable, secure, manageable switch-integrated services throughout the network. New 10 Gigabit Ethernet XENPAK options for the 10 Gigabit Ethernet modules provide multimode fiber and copper XENPAK support for 10 Gigabit Ethernet deployment in enterprise and data center networks. **Integrated**

Services Software—Software enhancements to the Content Switching Module, Secure Sockets Layer (SSL) Services Module, IP Security (IPSec) VPN Services Module, and Network Analysis Module 1 and 2 provide additional security defense, application awareness, and visibility of network traffic.

cisco.com/go/catalyst6500

Cisco Catalyst 3560 Series Switches

The new Cisco Catalyst 3560 Series offers fixed-configuration, multilayer switches that deliver IEEE 802.3af Power over Ethernet (PoE), Layer 2/3/4 intelligent services, and advanced Layer 3 routing with integrated security and QoS. Two models are available now, providing the standard or enhanced multilayer software image (SMI or EMI) with either 24 or 48 ports for 10/100 Ethernet connections and two or four SFP ports. Cisco Catalyst 3560 Series switches are ideal for use in small enterprises and branch offices to connect IP phones, wireless access points, video surveillance systems, and building management devices. IEEE 802.3af PoE and Cisco Catalyst switches are covered in greater detail on page 19.

cisco.com/go/catalyst3560

Cisco Catalyst 3750 Metro Series Switches

The new Cisco Catalyst 3750 Metro Series is a unique line of fixed-configuration, customer-located switches that bring greater intelligence for metro Ethernet access. The switches are ideal for service providers offering differentiated metro services with greater bandwidth and service-level agreement (SLA) flexibility. The switches support hierarchical quality of service (QoS) and traffic shaping, intelligent IEEE 802.1Q tunneling, virtual LAN (VLAN) translation, Multiprotocol Label Switching (MPLS), and Ethernet over MPLS. The Cisco Catalyst 3750 Metro Series is a single rack unit with redundant AC or DC power, 24 ports of 10/100 Ethernet, two small form-factor pluggable (SFP) ports for Gigabit Ethernet access, and two SFP-based Enhanced Services uplink ports. With flexible software options, the Cisco Catalyst 3750 Metro Series provides a cost-effective path for meeting current and future service requirements.

cisco.com/packet/162_npd1

Cisco Catalyst 3750 Series Switches: New Power over Ethernet and 10 Gigabit Ethernet Models

New models in the Cisco Catalyst 3750 Series of enterprise switches support IEEE 802.3af Power over Ethernet (PoE). The Catalyst 3750-48PS provides 48-port 10/100 Ethernet and four SFP ports; the Catalyst 3750-24PS provides 24-port 10/100 Ethernet and two SFP ports. IEEE 802.3af PoE and Cisco Catalyst switches are covered in greater detail on page 19. Ideal for wiring-closet deployments or server aggregation in a small data center, the new Cisco Catalyst 3750G-16TD provides 16 copper ports for 10/100/1000 Ethernet with a single 10 Gigabit Ethernet uplink. Each model occupies a single rack unit and supports installation with Cisco StackWise™.

cisco.com/go/catalyst3750

Wireless

Cisco Aironet Family: New Client Adapters

New Cisco Aironet® IEEE 802.11a/b/g Wireless CardBus and PCI Adapters provide seamless connectivity to any compliant network as well as Cisco Aironet 1100 and Aironet 1200 Series access points. Both adapters are Wi-Fi compliant, support 54-Mbit/s communications in the 2.4-GHz and 5-GHz bands, and provide an intuitive user interface for easy configuration, monitoring, and management. The CardBus client adapter is ideal for laptops and tablet PCs; the low-profile PCI client adapter is ideal for slim desktop and point-of-sale devices.

cisco.com/go/aironet

Cisco Persistent Storage Device

The Cisco Persistent Storage Device (PSD) extends storage on a Cisco Content Services Gateway (CSG) card to assure capture of billing data for mobile services. If a service provider's billing system is unavailable, the Cisco CSG will redirect call detail records (CDRs) to the Cisco PSD for storage and later transmission. With 37 GB of onboard storage space, the Cisco PSD can save up to 264 million CDRs from up to three Cisco CSGs. The Cisco PSD is implemented as a single services module card on Cisco Catalyst® 6500 Series switches or Cisco 7600 Series routers.

cisco.com/go/mobile

Network Management

Cisco Transport Manager Version 4.6

Cisco Transport Manager delivers intelligent element management software for the Cisco ONS family of optical networking products. Major new features available in Cisco Transport Manager Version 4.6 include automatic subnetwork grouping, integrated Multiservice Transport Platform (MSTP) and dense wavelength-division multiplexing (DWDM) management, and link-layer network model.

cisco.com/packet/162_npd2

Cisco Mobile Wireless Center Version 2.0

Cisco Mobile Wireless Center (MWC) software gives service providers an intelligent network management system for Cisco Mobile Exchange and other Cisco products in mobile wireless networks based on 2.5-GHz, 2.75-GHz, and 3-GHz technologies. Cisco MWC Version 2.0 provides device configuration and network services provisioning, fault mediation, and performance mediation for Cisco service selection gateways, content services gateways, Packet Data Serving Node and Home Agent, and Gateway General Packet Radio Service (GPRS) Support Node on the Cisco Catalyst® 6500/Cisco 7600 Multiprocessor WAN Application Module and on Cisco 7200 Series routers.

cisco.com/go/mwc

Enhanced Management Tools for MPLS Networks

An enhanced suite of Cisco software tools eases management of Multiprotocol Label Switching (MPLS) networks. Embedded MPLS management capabilities in the Cisco IOS® Software encompass unique Cisco technologies—Label Switched Path (LSP) Ping/Traceroute, Virtual Circuit Connectivity Verification (VCCV), AutoTunnel/AutoMesh Traffic Engineering, and Cisco Auto Service Assurance Agent (SAA)—which make it easier to deploy, operate, and monitor MPLS enhanced services. These enhancements are compatible with new MPLS features in three Cisco network management products. Cisco Info Center VPN Policy Manager Version 3.1 offers faster correlation of MPLS network events and supports the MPLS troubleshooting tools in Cisco IOS Software. Enhancements in Cisco CNS NetFlow Collection Engine Version 5.0 include a MPLS VPN provider-edge-to-provider edge (PE-PE) module for collecting traffic data. The new Cisco CNS Performance Engine Version 2.1 captures LSP Ping and Traceroute results in MPLS networks and supports PE-to-PE aggregation of NetFlow MPLS VPN usage. These new IOS MPLS management tools are covered in greater detail on page 69.

cisco.com/go/mplsmanagement

CiscoView Device Manager for Cisco Catalyst 6500 Series

A new embedded device manager, CiscoView Device Manager (CVDM) provides Web-based, graphical user interface (GUI) for easy configuration and management of Cisco Catalyst 6500 and integrated services modules. CVDM further simplifies deployment and manageability of flexible, integrated services network designs.

cisco.com/packet/162_npd3

Voice and Video

Cisco Internet Service Node 2.1

Cisco Internet Service Node (ISN) 2.1 software provides Web-based IVR, queuing, and IP switching services on both IP and traditional telephony networks to support speech-enabled, customer self-service applications. The ISN Voice Browser handles speech interaction with the caller, based on media files and controls defined by the ISN Application Server. Other supported capabilities include call queuing and agent-initiated or outpulse call transfers. Cisco ISN 2.1 integrates with Cisco ICM Enterprise Edition, Cisco ICM Hosted Edition, Cisco IPCC Enterprise Edition, and Cisco IPCC Hosted Edition.

cisco.com/packet/162_npd7

Cisco 2600XM, 2691, and 3700 Series Routers: IP Communications Modules

Three new IP Communications High-Density Digital Voice/Fax Network Modules (NM-HDV2, NM-HDV2-1T1/E1, and NM-HDV2-2T1/E1) support high-density digital voice traffic, analog voice traffic, WAN connectivity, and conferencing and transcoding capabilities for Cisco 2600XM, Cisco 2691, and Cisco 3700 series multiservice access routers. Designed for both enterprise and service provider applications, the modules directly connect PSTN, traditional telephony equipment, and WAN to the router for toll bypass or IP communications capabilities offered by Cisco CallManager with Survivable Remote Site Telephony (SRST) or Cisco CallManager Express. The modules have a single voice interface card (VIC) or voice/WAN interface card (VWIC) slot, four digital signal processing slots, and offer options for one or two built-in T1/E1 ports.

cisco.com/packet/162_npd5

Cisco Video Telephony Advantage Release 1.0

The new Cisco Video Telephony (VT) Advantage Release 1.0 software allows real-time, person-to-person video sessions to be added transparently to telephone calls. With Cisco VT Advantage and Cisco CallManager 4.0, users can create an instant, face-to-face video call with access to the familiar hold, transfer, and conference features of their Cisco IP phone. Enabled by integrating the Cisco VT Advantage software with any Cisco IP phone, a PC, and a USB video camera—the Cisco VT Camera—this solution allows enterprises to deliver IP telephony and IP video telephony to every employee using a unified dial plan and a common directory, over a single infrastructure through Cisco CallManager. The features and benefits of Cisco VT Advantage are covered in greater detail on page 45.

cisco.com/packet/162_npd4

Cisco IPCC Hosted Edition, Cisco IPCC Enterprise Edition 6.0, and Cisco IPCC Express Edition 3.5

New Cisco IP contact center (IPCC) software editions offer expanded capabilities for customer contact centers. The new Cisco IPCC Hosted Edition software enables service providers to offer managed customer contact services. Installed on servers located in a central office or customer data center, Cisco IPCC Hosted Edition supports applications such as virtual call center, intelligent call routing, and network-based automatic call distribution (ACD) and interactive voice response (IVR) functionality. Cisco IPCC Enterprise Edition 6.0 software offers new features such as Java-based computer-telephony integration (CTI) capabilities and a redesigned agent desktop with enhanced redundancy for large contact centers. Cisco IPCC Express Edition 3.5 software provides a unified implementation of ACD, IVR, and CTI capabilities in a single-server platform that is scalable up to 200 agents.

cisco.com/go/ipcc

Cisco CallManager Version 4.0

A new version of Cisco CallManager introduces a videoconferencing capability,

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 January and April 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/index.shtml.

security enhancements, and new options for private branch exchange (PBX) interoperability. The Cisco Video Telephony (VT) Advantage software enables a user to activate an instant, face-to-face video session while on a telephone call by integrating any Cisco IP Phone, a PC, and a Cisco universal serial bus (USB) video camera. Security enhancements in Cisco CallManager 4.0 include industry-standard digital certificates to confirm the identity of network devices, standards-based encryption for end-to-end privacy of voice calls, and integration of Cisco Security Agent (CSA) to provide proactive and adaptive threat protection for Cisco IP phones, servers, and desktop computing systems. CSA brings together multiple levels of security by combining host intrusion prevention, authentication to Cisco IP phones, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation. Also in Cisco CallManager 4.0, enhanced interoperability with PBX systems is delivered by native support for Q.SIG and Session Initiation Protocol (SIP) signaling. These new CallManager 4.0 features are covered in greater detail on page 45.

cisco.com/go/ipcommunications

Cisco uMG9820 QAM Gateway and uMG9850 QAM Module

A new series of digital video quadrature amplitude modulation (QAM) products help cable operators deliver video-on-demand services with lower costs and greater flexibility. The Cisco uMG9820 QAM Gateway and the Cisco uMG9850 QAM Module serve as gateways between an IP-based Gigabit Ethernet transport network and a hybrid fiber-coaxial (HFC) cable network carrying MPEG-2 signals. The standalone uMG9820 is a QAM-only platform optimized for smaller deployments, supporting up to 24 QAM channels in a single-rack-unit chassis. The uMG9850 is installed in a Cisco Catalyst® 4500 Series chassis for deployments with up to 120 QAM channels, or a mix of switching and QAM architectures.

cisco.com/packet/162_npd6

Cisco MeetingPlace 8106 Rich-Media Conferencing Server

The Cisco MeetingPlace 8106 Rich-Media Conferencing Server allows users to participate in and control secure audio and Web conferences through a Cisco IP phone, traditional telephone, or PC. Cisco MeetingPlace 8106 operates on carrier-grade hardware and advanced system software that is connected to a PBX, IP telephony system, or the public switched telephone network (PSTN). Suitable as an enterprise conferencing solution, or a managed or hosted offering from a service provider, Cisco MeetingPlace 8106 supports deployments up to 480 IP ports within a single system; scalability is enabled by connecting to distributed servers over the network. Cisco MeetingPlace is covered in greater detail on page 45.

cisco.com/go/meetingplace

Policy Routing, Continued from page 12

```
match only the pings used by tracked objects
 set ip next-hop 4.4.4.1
 ->  set the next hop to be the primary ISP's router
 set interface null0
 -> discard the packet if it wasn't forwarded to 4.4.4.1
```

Step 3: Create a tracked object and associate the object with the SAA probe, which was previously configured.

```
track 123 rtr 1 reachability
-> creates track object# 123 to monitor service assurance
   agent# 1
```

Step 4: Associate the default route via the primary link with the tracked object.

```
 ip route 0.0.0.0 0.0.0.0 4.4.4.1 track 123
-> default route via primary ISP will be associated with
   track object #123.
   Since the distance isn't specified, the distance has a
   value of one.
```

Step 5: Configure a floating static route via the secondary ISP. The administrative distance of the primary route must be lower than the administrative distance of the secondary route.

```
ip route 0.0.0.0 0.0.0.0 2.2.2.2 254
-> secondary route will have a distance of 254
```

Step 6: Verify proper operation by displaying the routing table and other related items as in the previous scenario.

More Scenarios and Configurations Online!

This is just a sample of the ways in which you can configure your network to determine when to use the primary or secondary ISP. For more scenarios with sample configurations, including injecting routes into routing protocols based on reachability of hosts, non-ICMP test of server reachability, server running a given application, and Policy Routing, visit Packet Online at cisco.com/packet/162_4a1. ▲▲

FURTHER READING

- **Policy-based Routing Support for Multiple Tracking Options:**
  cisco.com/packet/162_4a2
- **Reliable Static Routing Backup Using Object Tracking:**
  cisco.com/packet/162_4a3

MPLS Management, Continued from page 71

Cisco SAA is complementary to NetFlow. It measures latency, jitter, and packet-loss metrics between two endpoints to verify each customer's service levels and generate statistical network trending information. Measurements can be made end to end—between customer VPN locations—or across the service provider backbone between either two MPLS PE routers or two "shadow" routers. Shadow routers connect to edge routers to offload SAA processing so as not to impede forwarding performance. SAA is also essential for connectivity testing and proactive verification of MPLS networks, and can be used to notify the network management system (NMS) of threshold violations for performance or connectivity; path operations can be used to isolate problem areas in the MPLS core. With NetFlow and SAA running in an MPLS network, operators can guarantee customer network service levels and monitor per-customer SLAs in real time. By gathering flow-by-flow accounting data using MPLS-Aware NetFlow, they can also create services that support usage-based billing and service-class differentiation.

MPLS-Aware NetFlow. MPLS-Aware NetFlow captures MPLS traffic that contains IP and non-IP packets. Network operators activate MPLS-Aware NetFlow inside an MPLS cloud on a subset of core backbone routers. These routers export MPLS-Aware NetFlow data to an external NetFlow collector for further processing and analysis. This mechanism provides a way to get accounting and capacity-planning data via an MPLS label. For example, network operators can discover which points of presence (POPs) are forwarding traffic and measure traffic volumes forwarded by each POP.

MPLS-Aware NetFlow uses the Cisco NetFlow Version 9 export format. The IETF has chosen NetFlow Version 9 as a standard template for the Internet Protocol Information Export (IPFIX) of router-based flow information to data-collection devices and network management systems.

MPLS-Aware SAA. An SAA feature called a *responder* can be placed on any Cisco router, including customer equipment, to gather real-time service-level measurements on a per-customer basis from the POP to the edge router, POP to POP, or CE to CE. For example, service providers could offer a special managed service that enables customers running SAA on their customer premises equipment (CPE) to validate their own SLAs. SAA data also can be compiled into monthly customer performance reports.

In addition to Layer 3 MPLS networks, network operators can use MPLS-Aware NetFlow and MPLS-Aware SAA to gather accounting information and to monitor Layer 2 VPNs built on AToM technology.

◆ ◆ ◆

This article puts forth a basic introduction to the new Cisco tools that network managers can use to preserve the integrity of their existing revenue-generating services while also offering premium Layer 2 and IP services off of a common MPLS network platform. For more details on these capabilities, refer to the links in the "Further Reading" box, page 71. ▲▲

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)	www.apc.com	4
BellSouth Business	www.bellsouth.com/business	OBC
Boson Software	www.boson.com/NetSim	A
Cisco Press	www.ciscopress.com	B
Cisco Systems	www.cisco.com/securitynow	34/35
eiQ Networks	www.eiqnetworks.com	14
GL Communications	www.gl.com/packet	87
NIKSUN	www.niksun.com/packet	18
OPNET Technologies	www.opnet.com	64
Panduit	www.panduit.com/vip05	IBC
RedSiren	www.redsiren.com/packet.htm	26
SMARTS	www.smarts.com	56
Solsoft	www.solsoft.com/packet	8
The Siemon Company	www.siemon.com/go/10Gip/pa	88
WANDL	www.wandl.com	12
Websense	www.websense.com	F

Cache File

SNIPPETS OF WISDOM FROM OUT ON THE NET

Deskbar Searches and Wireless Top Internet Trends

The growth of mobility, wireless connectivity, and voice over IP are among the top Internet trends for 2004, according to the Web Talk Guys (webtalkguys.com/10604.shtml). High on the trends list is the decline of desktop Web browsers as a way to obtain content, making room instead for deskbar-enabled direct Web searches (such as Google Deskbar). It's projected that the biggest growth in wireless connectivity will be among mice and keyboards, as these all go wireless and their cost drops.

VIRUS NAMING ETIQUETTE

Ever since "Brain," the first computer virus, was created in 1986, the antivirus researcher who discovers a new worm or virus is generally given the honor of naming it, according to *Wired News*. A name is expected to have some relation to the capabilities or concept behind the virus, and researchers are loosely bound by a few other conventions. For example, viruses are not supposed to be named after businesses or brand-name products. Using the name of a famous person is also frowned on, and no matter how peeved a virus researcher is feeling, obscene or offensive names are forbidden.

Net Lingo

Sheepdip—The process of checking physical media, such as CD-ROMs, for viruses before they are used in a computer. Typically, a computer that sheepdips is used only for that process and is isolated from other computers and the network. Comes from the practice of dipping sheep in chemical solutions to clean their wool of fleas and lice (webopedia.com).

CYBER QUOTE

"Man IS STILL THE most extraordinary computer OF ALL."

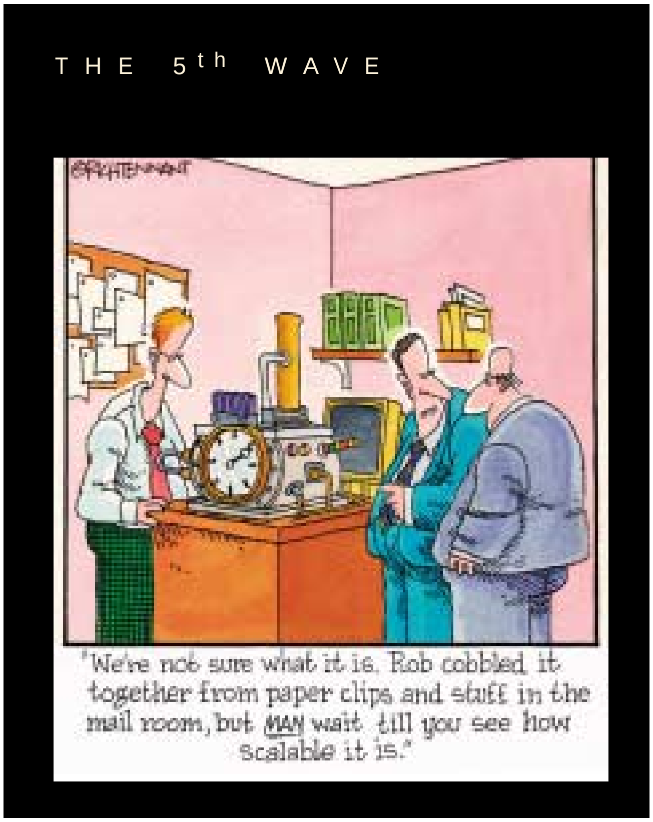
—John F. Kennedy,
35th US President

WANT TO BE A WEBMASTER?

Check out this article: "Becoming a Webmaster: One Man's Journey" at clickfire.com/viewpoints/articles/webmaster_become.php. From the correct spelling of Webmaster, to where to look for a job, to the right skills needed to succeed, this article lays it out.

Higher ROI for Aligning IT and Biz Strategies

Businesses that align their IT and business strategies are significantly more likely to achieve a high return on IT investment, according to a recent survey of senior financial officers conducted by Computer Sciences Corporation (csc.com) and Financial Executives International (fei.org). The sixth annual Technology Issues for Financial Executives survey, which looked at the IT trends most critical for chief financial officers and other senior finance executives, also found that only 10 percent of companies achieve a high rate of ROI for IT projects. Among those companies with a business-aligned IT plan, however, the percentage more than doubles to 24 percent.


THE 5th WAVE
RICHTENNANT
"We're not sure what it is. Rob cobbled it together from paper clips and stuff in the mail room, but MAN wait till you see how scalable it is."

©*The 5th Wave, www.the5thwave.com*