

PACKET

CISCO SYSTEMS USERS MAGAZINE

FOURTH QUARTER 2005



BREAKING BUSINESS BOUNDARIES

IP Applications Redefine Business Processes across Industries

30

Wide-Area Wireless LANs

47

New Communications Solutions for Smaller Companies

59

**SPECIAL REPORT:
Application Networking**

41

CISCO SYSTEMS

CISCO.COM/PACKET



Reprinted with permission from *Packet* magazine (Volume 17, No. 4), copyright © 2005 by Cisco Systems, Inc. All rights reserved.

PACKET

CISCO SYSTEMS USERS MAGAZINE

FOURTH QUARTER 2005
VOLUME 17, NO. 4



ON THE COVER

Breaking Business Boundaries

30

IP applications redefine business processes across industries.

Beyond Voice

32

Organizations worldwide capitalizing on quality of service (QoS)-enabled IP networks that they built for IP telephony to deploy new video and Extensible Markup Language (XML) applications.

Next Wave for Wireless

36

Innovative IP-based wireless applications in healthcare, government, and public safety provide inspiration for the enterprise.

SPECIAL REPORT

Application Networking

41

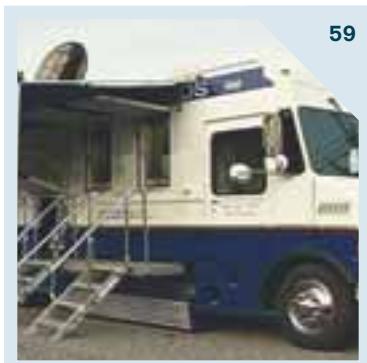
Application networking combines all the traditional benefits of the network—QoS, prioritization, routing, security, etc.—with application load balancing, server offloading, bandwidth and latency management, and application layer security. Find out what Cisco is doing to make application networking a reality.



47



55



59

TECHNOLOGY

VOICE: From Islands to Interconnect

19

Extending the security and reach of voice over IP (VoIP) networks with the Cisco Multiservice IP-to-IP Gateway.

WIRELESS: Extending the Network—to Anything

23

Cisco's radio frequency identification (RFID) solutions bring intelligence to the edge of the network and beyond.

ROUTING: Cell Packing on the Cisco 12000 Router

26

How service providers can improve bandwidth utilization with ATM cell packing capabilities on high-end routers.

ENTERPRISE SOLUTIONS

Wide-Area WLANs

47

Mesh networking architecture enables wireless LANs to move beyond offices, homes, and public hotspots to cover large outdoor areas.

The Changing Network Perimeter

53

Cisco Network Admission Control helps combat proliferating edge devices.

SERVICE PROVIDER SOLUTIONS

Metro Ethernet an Urban Amenity

55

Time Warner Telecom brings Metro Ethernet to 5,500 buildings in 44 major markets across the US—and business customers make the most of it.

SMALL AND MIDSIZED BUSINESSES

Smart, Simple, and Secure

59

Cisco Business Communications Solution offers new products, support, and financing options tailored for small and midsized businesses.

IN EVERY ISSUE

Mail	3
Acquisitions	7
Calendar	5
Networkers	12
Tech Tips	18
Advertiser Index	73
Cache File	74
The 5th Wave	74

DEPARTMENTS

From the Editor

1

IP Spells Innovation

User Connection

5

CCNA Multiplayer Challenge •
NetPro Web Award •
New Certification Exams

Tech Tips & Training

9

IOS IPSec Virtual Interfaces •
Cisco Incident Control System •
Reader Tips

Technically Speaking

63

Cisco's Jim Fenton on e-mail security and accountability.

New Product Dispatches

65

What's new from Cisco over the past quarter.

NetPro Expert

71

Advice from Cisco's Haseeb Niazi on deploying dynamic multipoint VPN solutions.

PACKET MAGAZINE

David Ball
Publisher and Editor in Chief

Jennifer Redovian
Executive Editor

Susan Borton
Managing Editor

Suzanne Jackson
Joanie Wexler
Contributing Editors

Robert J. Smith
Sunset Custom Publishing
Project Manager

Nicole Collins, Amy Mackey,
Mark Ryan
Sunset Custom Publishing
Production

Jeff Brand
Art Director
Emily Burch
Designer
Ellen Sokoloff
Diagram Illustrator
Bill Littell
Print Production Manager
Valerie Marliac
Promotions Manager
Cisco Systems
Cover Photograph

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

Publisher Information:
Packet magazine (ISSN 1535-2439) is
published quarterly by Cisco Systems and
distributed free of charge to users of Cisco
products.

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

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

Packet copyright © 2005 by Cisco Systems, Inc. All rights reserved. Printed in the USA.

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

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

This magazine is printed on recycled paper.

FROM THE EDITOR

IP Spells Innovation

Organizations of all stripes are using their IP networks in innovative new ways, going beyond the typical IT charter of reducing costs and improving productivity. Networks, and the IT people that manage them, are delivering on important business objectives: streamlining processes, enhancing collaboration, improving customer service, even creating new revenue streams.

In this issue of *Packet*, we highlight some of their success stories in areas as diverse as financial services, healthcare, public safety, education, and research. In "Beyond Voice," page 32, find out how IP videoconferencing is being used by one commercial lender to provide big-city service to small-town communities. And in the criminal justice system, the same technology is being used to conduct remote interviews and arraignments, accelerating the judicial process, while reducing the cost and risk of inmate transportation.

In "Next Wave for Wireless," page 36, learn how one hospital has deployed a wireless nurse call application that sends critical patient information in the form of Extensible Markup Language (XML) messages to their Cisco mobile IP phones, or how RF identification (RFID) technology was deployed to quickly locate mobile assets from wheelchairs to dialysis equipment.

You can read about all these applications and more in this issue. However, there is another, highly innovative use of IP networking that Cisco announced to the public as this issue of *Packet* was going to press.

Cisco recently unveiled the Internet Protocol Interoperability and Communications System, or Cisco IPICS. Cisco IPICS is an IP network-based collaboration platform that allows users of two-way radios, often called push-to-talk radios, and other voice devices, such as cell phones and regular telephones, to directly communicate and collaborate.

Today, public agencies and emergency responders have multiple radio systems that don't interoperate because they are based on proprietary technologies. For example, at an incident or disaster site, a police officer using a UHF push-to-talk radio might be unable to talk to a firefighter who is using a VHF radio or a paramedic who is on a Nextel phone.

As we have seen with such recent crises as Hurricane Katrina in the US, or the catastrophic tsunami in Southeast Asia, such lack of interoperability has greatly limited the usefulness of these critical communications tools. Now, with Cisco IPICS, these devices can interoperate and collaborate to help save lives.

Technology is just technology. It's what you do with it that matters. As IT professionals, you are in a unique position to create, discover, or deploy the next application that will propel your organization forward and make a real difference in the way we work, live, play, and learn.

David A. Ball

David Ball
Editor in Chief
daball@cisco.com



Rob Brodman



MAIL

New and Improved Archive

As a regular reader of *Packet* over the years I have seen many requests from your readers for information about various technologies. Many readers are directed to your website for articles in earlier editions of *Packet*. Why don't you catalog all *Packet* articles since the magazine's inception into various groups with different search criteria so that users can simply scroll through and read what they want rather than having to search for them on the site?

—Kartik Subramanian, Infosys Technologies Ltd., India



Thank you for your suggestion. Our new digital edition format (cisco.com/packet/digital), will soon enable readers to search the entire Packet archive using keywords. We are currently digitizing all 2004 and 2005 issues for that purpose. We expect to have the capability to create the sort of catalog you suggest, and we will consider this option in the near future.—Editor

Looking for Bandwidth

Regarding the Reader Tip (Second Quarter 2005) about the missing bandwidth question using the show frame-relay map command, there are at least two other reasons why bandwidth would not show using this command. First, the Local Management Interface (LMI) type is set to ANSI (not Cisco). Second, the circuit was provisioned for a Committed Information Rate (CIR) of zero. My point is that you should probably list all the reasons why that command would not provide the expected output.

—Michael J. Lewellen, Bally Total Fitness, Towson, Maryland, USA

Reader's Web Page for the Penalty Box

About a year ago you published an article about my Penalty Box rate-limiting application (Second Quarter 2004). I continue to get requests for information and have created a Web page with the information and source code: www.lehigh.edu/networksoftware/penaltybox.html.

—Mark Miller, Lehigh University, Bethlehem, Pennsylvania, USA

More on Router Uptime

In the last issue, you printed a letter from a reader about a Cisco 2500 Series Router that had been up for just over four years. At Nederlands Omroepproductie Bedrijf we have a Cisco 3640 router that routes all commercials for Dutch television and has been up for more than five years. Unfortunately, we'll replace this router soon with a PIX 515 Firewall in redundant setup.

A show version:

```
erg_3640#sho ver
Cisco Internetwork Operating System
Software IOS (tm) 3600 Software (C3640-I-M),
Version 12.0(2)XC2, EARLY DEPLOYMENT
RELEASE SOFTWARE (fc1)
TAC:Home:SW:IOS:Specials for info
Copyright (c) 1986-1999 by cisco Systems,
Inc.
Compiled Wed 20-Jan-99 20:11 by rnapier
Image text-base: 0x60008E0, data-base:
0x60664000
```

```
ROM: System Bootstrap, Version
11.1(12)XA, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
1)
ROM: 3600 Software (C3640-I-M), Version
12.0(2)XC2, EARLY DEPLOYMENT RELEASE SOF
TWARE (fc1)
```

erg_3640 uptime is 5 years, 10 weeks, 8 hours, 15 minutes System restarted by power-on at 06:42:27 UTC Thu Jul 20 2000 System image file is "flash:c3640-i-mz.120-2.XC2.bin"

—Marcel Mattheijer, Nederlands Omroepproductie Bedrijf, the Netherlands

I can confirm that Cisco IOS is really the best operating system for uptime. For years we have been using IOS boxes as a reference to monitor the stability of our telecom rooms over the EMEA region. As of today, the best uptime is provided by this box:

————— show version —————

```
Cisco Internetwork Operating System
Software
IOS (tm) 1600 Software (C1600-SY-M),
Version 11.2(13)P1, RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-1998 by cisco Systems,
Inc.
Compiled Fri 17-Apr-98 05:15 by dschwart
Image text-base: 0x02005000, data-base:
0x023D3224
```

```
ROM: System Bootstrap, Version
11.1(12)XA, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
ROM: 1600 Software (C1600-RBOOT-R),
Version 11.1(12)XA, EARLY DEPLOYMENT
RELEASE SOFTWARE (fc1)
```

```
gremicgw1 uptime is 7 years, 17 weeks, 3
days, 6 hours, 58 minutes
System restarted by power-on at 16:37:27
UTC Wed Jun 17 1998
System image file is "flash:c1600-sy-
mz.112-13.P1.bin", booted via flash
Host configuration file is
"template/XXXoscgwX-list199", booted via
tftp from 192.151.16.169
```

We will keep you updated next year. . . .
—Thierry Goyeau, HP Global Managed Network Services, Grenoble, France

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.

CCNA Multiplayer Challenge

A new online game challenges players to compete with their peers as they answer CCNA practice questions. The Cisco Certification Multiplayer Challenge: CCNA is the latest addition to the Cisco Certified Network Associate (CCNA) Prep Center (cisco.com/go/prepcenter). Designed especially for networking professionals pursuing CCNA certification, the game is open to anyone with a Cisco.com login.

"This game is a dynamic, challenging, and fun addition to the CCNA Prep Center," says Don Field, director of certifications at Cisco. "The new game and other training supplements provide CCNA candidates with a growing array of resources to help networking professionals successfully achieve their certification goals."

With hundreds of practice questions in a "first-to-the-buzzer" format, the Certification MultiPlayer Challenge: CCNA enables players to compete one on one, or in teams, and to set up tournaments.

Part of the Cisco Career Certifications program, the CCNA Prep Center offers a wide variety of resources, including practice



CCNA MULTIPLAYER CHALLENGE Learn networking fundamentals by competing against your peers with a new online game available from Cisco's CCNA Prep Center.

questions, labs, simulations, games, tips, expert advice and peer discussion forums for CCNA certification candidates.

For information about the CCNA or other Cisco certifications, visit cisco.com/go/certsupport. ■

Cisco Security Certification Exams

To support the increasing demand for network professionals who can deploy, support, and optimize a cost-effective, self-defending network, Cisco has updated the professional-level CCSP certification, and the Cisco Qualified Specialist security certifications. The new security curriculum provides up-to-date product and application instruction that will help candidates to use firewalls, secure remote access, intrusion prevention, and other key assets to create a converged security platform.

According to Don Field, Cisco's director of certifications, the revamp is a content change only, reflecting the program's shifting security focus and a deemphasis on older technologies in favor of new ones, such as the Cisco Security Agent and the Adaptive Security Appliances line. Cisco has introduced new products and solutions under the Self-Defending Network initiative," says Field.

The titles affected by the change are the Cisco Certified Security Professional (CCSP) and the security-related Cisco Qualified Specialist certifications: Firewall, Intrusion Detection Systems (IDS), and Virtual Private Networking (VPN). Among the old exams for the CCSP, only exam 642-511 CSVPN remains. This exam is now an elective requirement; candidates can choose between it and one of the new exams.

New CCSP exams:

- 642-502 SNRS: Securing Networks with Cisco Routers and Switches
- 642-522 SNPA: Securing Networks with PIX and ASA
- 642-523 IPS: Implementing Cisco Intrusion Prevention Systems
- 642-551 SND: Securing Cisco Network Devices

- 642-513 HIPS: Securing Hosts using Cisco Security Agent (elective requirement; choose between this or CSVPN)

Although exam 642-541 CSI: Cisco SAFE Implementation is no longer a required exam, candidates who want to recertify CCSP can take it or a Cisco CCIE written exam.

The foundation exam for all three Cisco Qualified Specialist certifications is now the 642-551 SND, which replaces 642-501 SECUR: Securing IOS Networks.

The last date for registering for the older exams is December 19, 2005. Candidates will be able to combine the old and new exams for the foreseeable future in order to earn their titles.

For more information about Cisco career certifications, visit cisco.com/packet/174_3c1. For answers to specific questions regarding Cisco certifications, visit cisco.com/go/certsupport. ■

CISCO WORLDWIDE EVENTS

December 4–8, 2005	ITU Telecom World, Hong Kong, China
December 12–15, 2005	Networkers France, Cannes, France
December 19–21, 2005	Networkers China, Beijing, China
February 7–10, 2006	MPLS World Congress, Paris, France
February 13–16, 2006	3GSM World Congress, Barcelona, Spain
March 6–9, 2006	VoiceCon, Orlando, Florida, USA
cisco.com/warp/public/688/events.html	

Cisco Networking Professionals Site Wins Web Award

The Cisco Networking Professionals Connection—an online gathering place to share questions, suggestions, and information about networking solutions products, and technologies with Cisco experts and networking colleagues—has received a Standard of Excellence award in the online community category of the 2005 WebAwards competition. The WebAwards, held annually by the Web Marketing Association, is the premier competition judging website development against the ever-increasing Internet standard. The competition, which evaluates peer sites within 95 industry



categories, provides a forum for recognizing people and organizations that develop some of the most effective websites on the Internet.

With nearly 100,000 users subscribed, the Cisco Networking Professionals Connection (cisco.com/discuss/networking), also known as “NetPro,” averages more than 2,000 postings a week.

To learn more about NetPro, visit cisco.com/discuss/networking. ■

Cisco Acquires Nemo Systems

Cisco has announced the acquisition of privately held Nemo Systems of Los Altos, California. Nemo Systems is the developer of leading-edge network memory technology that will offer enhanced performance on Cisco's core switching platforms and services modules, including the Catalyst 6500 Series Switch and Layer 4–7 services modules.

When incorporated into Cisco's products, the technology will allow customers to scale network systems and line-card bandwidth while reducing the overall cost of high-performance networking systems.

Nemo's six employees will become part of Cisco's Data Center, Switching and Security Technology Group at Cisco. ■

Bypassing GRE

A Guide to Successfully Implementing IOS IPSec Virtual Interfaces

By Muhammad Afaq Khan

Cisco IOS IP Security (IPSec) virtual interfaces (VIs) can be used to deploy static (i.e., site to site) or dynamic VPNs (i.e., Easy VPN or hub and spoke scenarios) that carry IP unicast and multicast traffic—without the need for Generic Routing Encapsulation (GRE). This feature, which was introduced in Cisco IOS Software Release 12.3(14)T, enables IPSec to have its own interface and leverages virtual templates for dynamically creating an interface with IPSec encapsulation. IPSec VI can be used on any router platform running Cisco IOS Software.

Traditionally, IPSec is used to encrypt (ESP) and authenticate (ESP/AH) point-to-point IP traffic in site-to-site and remote access VPN scenarios. The router first encapsulates the packet inside GRE, then encrypts the GRE/IP unicast packet, at a cost of 4 bytes of GRE overhead for each tunneled packet, and operating under the assumption that the remote peer is able to understand GRE (for example, in a multivendor environment). The IPSec virtual tunnel interface (VTI) provides a solution for dealing with these legacy GRE/IPSec implementation issues (see Figure 1).

There are two types of IPSec VIs: static and dynamic. Static VIs provide an alternative to configuring point-to-point IPSec/GRE tunnels. Dynamic VIs provide a method for configuring both point-to-point and point-to-multipoint type scenarios. Both enterprises and service providers can benefit from using IPSec VI.

The following configuration examples can be used to better understand the differences between older GRE/IPSec and IPSec VI configurations.

GRE/IPSec Configuration

7206-VTI-1:

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 7206-VTI-1
!
!
clock timezone PST -8
ip subnet-zero
ip domain name cisco.com
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
  authentication pre
  encryption aes 256
!
crypto ipsec transform-set test esp-aes 256 esp-sha-hmac
!
crypto map test 10 ipsec-isakmp
  set peer 20.1.1.2
  set transform-set test
```

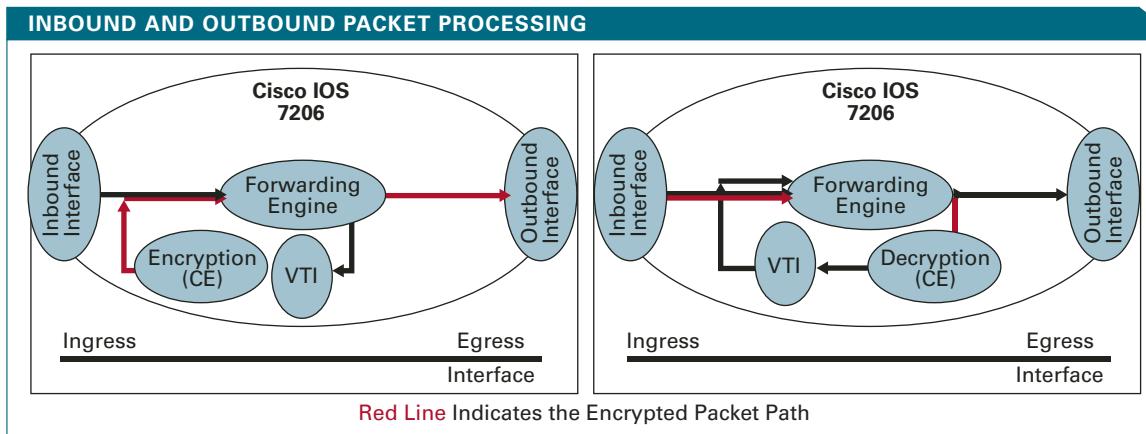


FIGURE 1 With IPSec VI, inbound and outbound packets that need to be encrypted/decrypted are forwarded to VI before they finally exit the router.

```

match address 101
!
!
interface Tunnel0
  ip address 10.10.10.1 255.255.255.252
  ip mtu 1420
  tunnel source Ethernet1/0
  tunnel destination 20.1.1.2
  crypto map test
!
interface Ethernet0/0
  ip address 1.1.1.1 255.255.255.0
!
interface Ethernet1/0
  ip address 20.1.1.1 255.255.255.0
  crypto map test
!
ip classless
no ip http server
!
!
access-list 101 permit gre host 20.1.1.1 host
20.1.1.2
!

Alternative VTI Configuration
7206-VTI-1:
version 12.4

```

```

service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 7206-VTI-1
!
clock timezone PST -8
ip subnet-zero
ip domain name cisco.com
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
  authentication pre-share
  encryption aes 256
  crypto ipsec transform-set test esp-aes 256 esp-
    sha-hmac
crypto ipsec profile vpn
  set transform-set myset
crypto isakmp key cisco address 20.1.1.2
!
interface Tunnel0
  ip address 10.10.10.1 255.255.255.252
  tunnel mode ipsec ipv4
  tunnel source Ethernet1/0

```

```

tunnel destination 20.1.1.2
tunnel protection ipsec profile vpn
!
interface Ethernet0/0
 ip address 1.1.1.1 255.255.255.0
!
interface Ethernet1/0
 ip address 20.1.1.1 255.255.255.0

```

Caveats

Static VIs only support any-to-any (all tunneling) proxy IDs, whereas dynamic VIs also support split tunneling configuration. Unlike GRE/IPSec, static VIs cannot be used to encrypt non-IP traffic.

```

7206-VTI-1#sh cry ips sa
interface: Tunnel0
 Crypto map tag: Tunnel0-head-0, local addr
11.11.11.1
 protected vrf: (none)
 local ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/0/0)
 remote ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/0/0)
 current_peer 11.11.11.2 port 500
 PERMIT, flags={origin_is_acl,}

```

VI with QoS Pre-Classification

When a combination of both voice and data traffic needs to be encrypted, the outbound physical interface from which this traffic departs does not see the actual flows—everything is viewed as a single flow. Cisco IOS crypto implementation provides quality of service (QoS) pre-classification to address this. To enable this feature, the **qos pre-classify** command must be applied on the VI interface. To migrate from a GRE/IPSec implementation that uses pre-classification, apply this command on the VI.

In the example below, a strict priority queue with a guaranteed allowed bandwidth of 50 kbit/s is reserved for traffic that is sent from the source address 10.10.10.10 to the destination address 10.10.10.20, in the range of ports 16384 through 20000 and 53000 through 56000. First, the following commands configure access list 102 to match voice traffic objectives:

```

7206-1(config)# access-list 102 permit udp host
10.10.10.10 host 10.10.10.20 range 16384
20000
7206-1(config)# access-list 102 permit udp host

```



MUHAMMAD AFAQ KHAN, CCIE No. 9070, is a technical marketing engineer in Cisco's Broadband, Edge, and Midrange Routing Business Unit, and previously worked in the Cisco Security/VPN TAC. He also holds CCIEs in routing and switching, security, and service provider tracks. He can be reached at afakhan@cisco.com.

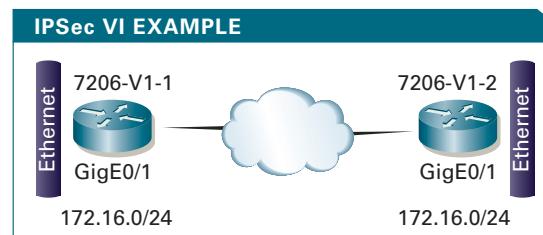


FIGURE 2 IPSec VI solves the issue of overlapping subnets across an IPSec tunnel.

```

10.10.10.10 host 10.10.10.20 range 53000
56000

```

Next, the class map voice is defined, and the policy map called policy1 is created. A strict priority queue for the class voice is reserved, a bandwidth of 20 kbit/s is configured for the class bar, and the default class is configured for Weighted Fair Queuing (WFQ). The service-policy command then attaches the policy map to the fa0/0.

```

7206-1(config)# class-map voice
7206-1(config-cmap)# match access-group 102
7206-1(config)# policy-map policy1
7206-1(config-pmap)# class voice
7206-1(config-pmap-c)# priority 50
7206-1(config-pmap-c)# class bar
7206-1(config-pmap-c)# bandwidth 20
7206-1(config-pmap-c)# class class-default
7206-1(config-pmap-c)# fair-queue
7206-1(config)# interface fa0/0
7206-1(config-if)# service-policy output policy1
!
interface Tunnel0
ip address 10.10.10.1 255.255.255.0
qos pre-classify
tunnel source GigabitEthernet0/1
tunnel destination 11.11.11.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile vpn

```

IPSec VI with NAT/ACL/IOS Firewall

IPSec VI can be used to perform source/destination Network Address Translation (NAT) on the clear-text traffic (for example, scenario with overlapping local LAN networks), where NAT is performed on both sides of clear-text traffic (see Figure 2).

```

7206-VTI-1:
crypto isakmp policy 1
authentication pre-share
encryption aes 256
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set myset esp-aes 256 esp-
sha-hmac
!
crypto ipsec profile vpn
 set transform-set myset
!

```

```

!
interface Tunnel0
  ip address 10.10.10.1 255.255.255.0
  ip nat outside
  tunnel source GigabitEthernet0/1
  tunnel destination 11.11.11.2
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile vpn

interface GigabitEthernet0/3
  ip address 172.16. 255.255.255.0
  load-interval 30
  duplex auto
  speed auto
  media-type rj45
  no negotiation auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 11.11.11.2
!
no ip http server
no ip http secure-server
!
ip nat inside source static 172.16.1.0 172.17.1.0

```

Due to VI, there is better control over pre/post encryption traffic filtering; any pre-encryption or post-decryption traffic can be filtered by applying an

in/out ACL on the VI. ESP/IKE traffic is filtered by applying ACL(s) on the physical interface(s) where traffic is entering/exiting the router. To enable host-A to communicate with host-B across the VPN tunnel, and assuming that proxy IDs are “permit ip any any,” define an ACL to permit only host-to-host traffic.

```

interface Tunnel0
  ip address 10.10.10.1 255.255.255.0
  ip access-group 109 in
  ip nat outside
  ip inspect myins out

tunnel source GigabitEthernet0/1
tunnel destination 11.11.11.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile vpn

access-list 109 permit ip host 172.18.1.1 host
172.17.1.1

```

Any combination of NAT, ACL, and Context-Based Access Control (CBAC) will follow the standard order of IOS ingress/egress feature processing. In general, VI is used to implement features on clear-text traffic (pre-encryption), and the actual outbound physical interface(s) for all post-encryption features.

Dynamic VI Configuration

Dynamic VI can be used to create on-the-fly VI instances to support remote access Easy VPN or hub and spoke configuration. With dynamic VI, Easy VPN tunnels can carry routing protocols and multicast traffic while still providing all the inherent benefits of Easy VPN. Following is a real-world Easy VPN example.

Hub Router:

```
username afakhan@cisco passwd cisco123
aaa new-model
aaa session-id common
aaa authentication login users local
aaa authorization network users local
!
crypto isakmp client configuration group mygroup
key cisco
dns 10.10.10.1
wins 10.10.10.2
pool mypool
!
crypto isakmp profile cisco-ezvpn
match identity group mygroup
client authentication list users
isakmp authorization list users
client configuration address respond
virtual-template 1
!
crypto ipsec transform-set myset esp-aes 256 esp-
sha-hmac
!
crypto ipsec profile VTI-profile
set transform-set myset
!
interface Loopback0
ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet2/0
description Egress Interface
ip address 192.1.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
description Dynamic VI
ip unnumbered Loopback0
tunnel mode ipsec ipv4
tunnel protection ipsec profile VTI-profile
!
ip local pool mypool 172.16.1.1 172.16.1.10
ip route 0.0.0.0 0.0.0.0 192.1.1.2
```

Spoke routers can have regular static VIs. Several scenarios can be configured if a gradual migration to IPSec VI is planned. For example:

Static VI on one peer, and static crypto map on the other. Requires code/configuration update only on one peer; cannot run routing protocol.

Static VI on both peers. Requires code/configuration update on both routers; an alternative to IPSec/GRE

configuration. Routing protocols, multicast traffic, and so on, can be run.

Dynamic VI on hub, and static crypto map on spokes. Requires a code/configuration update on one router; cannot run routing protocols.

Dynamic VI on hub, and static VI on spokes. Requires a code upgrade and configuration on both peers alternative; provides support for routing protocols, multicast, and eliminates the need for RRI on the hub compared with the traditional Easy VPN scenario.

IPSec VI. Can also be used as a workaround for having multiple wildcard (all 0's) pre-shared keys on a single router. This is particularly useful when service providers use network-based VPNs.

IPSec VI Troubleshooting (Show and Debug)

```
7206-1#sh int tun0
Tunne10 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 1.1.1.1/24
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
    reliability 255/255, txload 1/255, rxload
  1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 11.11.11.1 (GigabitEthernet0/1),
  destination 11.11.11.2
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPsec (profile "vpn")
  .....
7206-1#sh cry session
crypto session current status

  interface: Tunne10
  session status: UP-ACTIVE
  peer: 11.11.11.2 port 500
  IKE SA: local 11.11.11.1/500 remote 11.11.11.2/500
  Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0
  0.0.0.0/0.0.0.0
  Active SAs: 2, origin: crypto map
```

For real-time debugging purposes, all crypto-related debugs can be used. ■

FURTHER READING

- IPSec VTI Product Features
cisco.com/packet/174_4a1
- Configuring a VTI with IPSec Deployment Guide
cisco.com/packet/174_4a2

Raising the Bar on Network Protection

Incident Control System uses Trend Micro's expertise to turn Cisco devices into rapid-response incursion mitigation points.

Cisco and antivirus vendor Trend Micro have teamed up to significantly increase the industry's level of protection against network threats and improve mitigation response time and effectiveness among IT personnel. The fruit of their collaboration is the Cisco Incident Control System (ICS). Using Trend Micro's global, always-on threat monitoring and response capabilities, ICS works with existing Cisco network devices to rapidly distribute worm and virus immunization capabilities throughout the network—effectively turning the Cisco devices into incursion mitigation points within minutes after an outbreak is detected.

The heart of ICS is the Cisco ICS server, the administrative and delivery center that enables IT to deploy rapid-response mitigation policies to a large variety of Cisco devices worldwide. The ICS solution includes the Cisco ICS server software, mitigation devices, and annual subscription licenses to outbreak prevention information and countermeasures. Mitigation devices are the Cisco products within the network that will receive outbreak prevention policies provided by ICS and act as enforcement points against the incursion and propagation of an outbreak. Administrators purchase a copy of the Cisco ICS software and the desired number of Cisco ICS licenses; each license must then be associated with the appropriate mitigation devices in their network. There are three types of ICS licenses:

Access control list (ACL) licenses apply to Cisco routers and switches running standard Cisco IOS Software images.

Intrusion prevention system (IPS) low-end licenses apply to low-end Cisco IPS devices, including Cisco 900, 1700, 1800, 2600XM, and 3700 series routers; IPS 4215 sensors; ASA 5500 Series adaptive security appliances with SSM-AIP-10 modules; and IPS-capable IOS routers running IOS Software security images.

IPS high-end licenses apply to midrange and high-end Cisco IPS devices, including 3800 Series routers; 7200 Series routers; many IPS 4200 Series sensors; IDSM2 blades for Cisco Catalyst 6500 Series switches; ASA 5500 Series appliances with SSM-AIP-20 modules; and IPS-capable IOS routers running IOS Software security images.

Trend Micro's TrendLabs monitors the Internet and other sources of information around the globe for new outbreaks, relying on elaborate processes that

include threat analysis; rapid-response and permanent signature development; visual, functional, and false alarm testing; and uploading of patterns to the company's ActiveUpdate (AU) servers. When a new outbreak of malicious software is detected, professionals at TrendLabs immediately begin analyzing, classifying, and identifying the threat. Typically within 15 minutes of detecting the outbreak, TrendLabs creates an *outbreak prevention policy (OPP)*, a temporary measure to prevent the malicious software from entering or spreading in the network. The OPP is placed on the AU servers and available for download by the Cisco ICS server as part of an *outbreak management task (OMT)*.

The Cisco ICS server constantly polls AU servers for OMTs and, upon spotting one, it will create the task in the Cisco ICS server, alert the administrator, download the OPP, and translate it into an *outbreak prevention access control list (OPACL)*, and if configured to do so automatically, deploy the OPACL to appropriate Cisco mitigation devices. If the server isn't configured for automatic deployment, administrators can inspect the OPACL and make any desired changes before manually deploying it. After the OPP is released, TrendLabs creates an *outbreak prevention signature (OPSig)* that uniquely identifies the threat from all other types of traffic and places the OPSig on AU servers within 90 minutes of the outbreak detection. The Cisco ICS server downloads the OPSig and deploys it to IPS-capable Cisco mitigation devices, replacing the previously installed OPACL.

To help lessen the risk of internal infection, the Cisco ICS server has the ability to log and track hosts generating OPSig-triggering traffic—information that is leveraged by Trend Micro's Damage Cleanup Service (DCS). If DCS servers are registered with the Cisco ICS server, the service will automatically and remotely clean infected Microsoft Windows machines that have been identified by Cisco ICS as internal sources of infection. ■

FURTHER READING

- Cisco ICS Technical Overview
cisco.com/packet/174_4b1
- Cisco Outbreak Prevention Solutions
cisco.com/packet/174_4b2

Reader Tips

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

Configuration

TIP Cutting and Pasting config via Hyperterminal

If you cut and paste your config onto an IOS-based switch using Hyperterminal, it breaks down about midway. This occurs because Hyperterminal sends the text too quickly for the switch, particularly if a command returns a message, such as portfast. To avoid this, in Hyperterminal, select File – Properties; click the Settings tab, click the ASCII button, and add a character delay of 5 milliseconds. You should now be able to cut and paste your config successfully.

—Suhail Kulasi, Ashurst, London, England

TIP Using Frame Relay End-to-End Keepalives

When implementing a Frame Relay point-to-point network you are often required to have a backup solution in place. Most backup methods are triggered by either a routing protocol failure or an interface going down. When using the interface method, problems can arise if the Frame Relay provider is using multiple switches between the two endpoints. A point-to-point interface on one end might be brought down due to a link failure, but might remain up on the other end. This might cause the backup solution to not work. Frame Relay end-to-end keepalives (EEK) can resolve issues such as these. For example:

```
Hostname R5
!
interface Serial0/0.54 point-to-point
ip address 163.1.54.5 255.255.255.0
frame-relay interface-dlci 504
class EEK
!
map-class frame-relay EEK
frame-relay end-to-end keepalive mode request
!

Hostname R4
!
interface Serial0/0.54 point-to-point
ip address 163.1.54.4 255.255.255.0
```

```
frame-relay interface-dlci 405
class EEK
!
!
map-class frame-relay EEK
frame-relay end-to-end keepalive mode reply
!
```

To verify that this is working:

```
R5#show frame-relay pvc 504
```

```
PVC Statistics for interface Serial0/0 (Frame Relay
DTE)
```

```
DLCI = 504, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE
(EEK UP), INTERFACE = Serial0/0.54
```

```
input pkts 5161          output pkts 6022
in bytes 56771
out bytes 331070         dropped pkts 0
in pkts dropped 0
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0          in BECN pkts 0
out FECN pkts 0
out BECN pkts 0          in DE pkts 0
out DE pkts 0
out bcast pkts 860       out bcast bytes 294936
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 14:19:49, last time pvc status
changed 13:45:49
!
```

—Mike Griffin, Robert Half International Inc., Pleasanton, California, USA

Editor's Note: For more information about Frame Relay keepalives, refer to the Cisco documentation at cisco.com/packet/174_4d1.

TIP Migrating M1 and Other Server Services from Old to New IP Addresses

Since it is not possible to put a secondary IP address on a Cisco PIX Ethernet interface, how do you migrate from one network to another, with servers in DMZ with public IP addresses and without Network Address Translation (NAT)? For example, suppose that your LAN IP addresses are M1IPADDR for the M1 server and PIXIPADDR for the M1 server's

gateway. The new IP address (secondary) for M1 needs to be M1NEWIP in a different IP network, but with the old IP gateway. (You cannot change the PIX address.) In your Cisco PIX, enter:

```
nat (dmz) 0 0.0.0.0 0.0.0.0 0  
static (dmz,outside) M1NEWIP M1NEWIP netmask  
255.255.255.255 0 0  
route dmz M1NEWIP 255.255.255.255 M1IPADDR 1
```

In this way, you can use the new M1NEWIP without changing the PIXIPADDR. Therefore, you can migrate M1 (and other) server services from old to new IP addresses and then change the PIXIPADDR for the new network.

—Gianrico Fichera, ITESYS, Catania, Italy

Troubleshooting

TIP Avoiding VoIP Call Issues

Many customers experience this problem: When they dial a destination number and hear a tone, it takes from 10 to 15 seconds for both parties to hear each other. This occurs because the RTP channel (voice path) comes up after the source router receives a connect message from the destination router. (Both

routers are communicating using H.245 signaling, which is similar to Q.931 of ISDN.) The connect message is sent after the called person picks up the phone. The solution for this problem is to use the following command in the global configuration:

```
RouterA(config)#voice rtp send-receive
```

When this command is enabled, the voice path will cut through (establish) in both backward and forward directions before a connect message is received from the destination switch. This command affects all VoIP calls when it is enabled.

—Ahmed Baher, Equant, Cairo, Egypt

SUBMIT A TIP

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

Tech Tips

Managing the File System on a VPN 3000 Concentrator.

Learn about several options to manage the file system on a Cisco VPN 3000 Series Concentrator. This TAC solution document discusses the most efficient way to synchronize the configuration on two VPN 3000 Concentrator devices when configuring redundancy between them.

cisco.com/packet/174_4e1

Understanding EAP Certificate Types. This TAC solution document describes certificate types, formats, and requirements associated with the various forms of Extensible Authentication Protocol (EAP).

cisco.com/packet/174_4e2

Using GRE Keepalives. Generic Routing Encapsulation (GRE) tunnel keepalives are not supported with the tunnel protection **ipsec profile** command. This document discusses this issue and describes the one situation where these features work together. cisco.com/packet/174_4e3

Identifying High CPU Utilization Causes on Cisco Catalyst

6500/6000 Series Switches. Get help determining the causes of high CPU utilization on Cisco Catalyst 6500/6000 series switches. This document clarifies differences between Cisco routers and switches, and describes use of the CPU on the switches and how to interpret **show processes cpu** command output.

cisco.com/packet/174_4e4

Provisioning Timing on the Cisco ONS 15454 using Cisco Transport Controller.

This document describes how Cisco Transport Controller provides two methods for provisioning timing and modifying the settings. At the node level, configure timing from the Provisioning/Timing tab. Here, provision different timing modes and references for the entire node. Alternatively, at each optical port, change the default Synchronous Status Message (SSM) settings. cisco.com/packet/174_4e5

From Islands to Interconnect

Extending the Security and Reach of VoIP Networks

By Lori Gadzala

With deployments growing worldwide, the next voice-over-IP (VoIP) opportunity becomes interconnecting these islands of IP securely and efficiently. Today, enterprises are happily saving money and enjoying the features of their voice and video IP phones as they call within their organizations. Outside their organizations, however, calls to other VoIP networks are being converted to PSTN signals and back again, typically through media gateways installed back to back in the service provider's network. Currently, the PSTN is used as the lowest common denominator for services, and any IP features embedded in the calls, such as video or special dialing instructions, are lost. Conversions also introduce additional latency and can degrade voice quality, because the IP call goes through two unnecessary codec conversions. From the service provider's perspective, these conversions are an inefficient use of network resources. Yet there are a few issues to address before allowing native VoIP connections across administrative domains.

The first issue is security. Both service providers and enterprises want to keep their IP addresses, and indeed their entire network topology, private. Revealing their network and its IP addresses to the rest of the world increases the risk of potential security breaches, ranging from worms and viruses to theft of information and distributed denial-of-service (DDoS) attacks.

The next issue is interworking. For example, because a range of VoIP protocol options exists, calls placed using H.323 and G.711 codecs might need to be converted to Session Initiation Protocol (SIP) signaling and G.729 codecs.

For billing, management, and maintenance purposes, service providers must define proper points of demarcation between themselves, their peering networks, and their enterprise customers.

Session Border Controllers to the Rescue

Session Border Controllers (SBCs) are relatively new devices that connect IP voice and video networks securely, cost effectively, and efficiently. An SBC resides at the edge of an enterprise or service provider network, acting as both the source and destination for call signaling and media. Incoming or outgoing call signaling is terminated at the SBC and then reoriginated using the IP address of the SBC. The media is also terminated and reoriginated, providing complete privacy for the endpoint or network that generates the call.

SBCs must interoperate with many different network elements—voice gateways, IP phones, and call control servers—in many different application environments. A full-featured SBC supports advanced enterprise voice and video services, as well as simpler toll bypass and VoIP transit applications. From its humble

beginnings in 2003, the worldwide SBC market is projected to grow to US\$400 million in 2007 and US\$1 billion in 2008.

In October 2005, Cisco released the latest version of its SBC: the Cisco Multiservice IP-to-IP Gateway. Designed to meet enterprise and service provider SBC needs, the Cisco Multiservice IP-to-IP Gateway is an integrated application within the Cisco IOS Software. The Multiservice IP-to-IP Gateway runs on the Cisco Integrated Services Routers—on the Cisco 2800 and 3800 series for integrated voice, video, and data services—and on the Cisco 2600 XM, 3700, 7200VXR, and 7301 routing and gateway platforms.

The Cisco Multiservice IP-to-IP Gateway supports a range of SBC functions. It terminates and reoriginate call signaling, protecting the IP address of the source and destination parties and hiding network topology information. It supports a complete suite of media interworking, including DTMF, fax, modem, and voice transcoding. It provides a network-to-network interface or demarcation point, producing call detail records (CDR) for use in billing applications. It can also manage bandwidth using Resource Reservation Protocol (RSVP) and codec filtering, and provide quality of service (QoS) marking using type of service (ToS) and Differentiated Services Code Point (DSCP). It interoperates with H.323 gatekeepers, SIP proxies, and Cisco CallManager.

Transitioning from H.323 to SIP

Previous versions of the Multiservice IP-to-IP Gateway supported H.323-to-H.323 signaling and H.323-to-SIP signaling. Now, the Multiservice IP-to-IP Gateway also supports SIP-to-SIP signaling.

Cisco has demonstrated market leadership with VoIP in the enterprise, and service providers are transitioning TDM [time-division multiplexing] to IP, says Jennifer Blatnik, a product manager in the Access Routing Business Unit at Cisco.

"With the continued acceleration of IP communications deployments and market acceptance of SIP, service providers are beginning to transition their H.323 installed bases to SIP," says Blatnik. "The Cisco Multiservice IP-to-IP Gateway will allow these service providers to phase in SIP while interworking with their existing H.323 deployments using the same hardware."

These service providers can also prepare to repurpose their H.323 gateways for SIP-to-SIP interconnects, explains Blatnik. And because the Multiservice IP-to-IP Gateway is a Cisco IOS

Software load, it also uses a familiar user interface and configuration commands.

Cisco actively participates in the evolving SIP standards. Most recently, in SIPIT 17, a SIP interoperability testing event in Stockholm, Sweden, Cisco validated its IOS implementation of SIP standards such as RFC 3261 along with dozens of other companies worldwide. Vendor interoperability is an important element of any SBC, because it must communicate with SIP proxies, SIP user agents, and SIP phones.

Enterprise and Service Provider Environments

The Cisco Multiservice IP-to-IP Gateway interconnects VoIP and video networks within enterprises, between enterprises, between enterprises and service providers, and between service providers. The Multiservice IP-to-IP Gateway is already being used by service provider, enterprise, and small and midsized business (SMB) customers in both H.323 and H.323-to-SIP voice and video networks.

Enterprises deploy the Multiservice IP-to-IP Gateway for different reasons. Some need its security or interworking capabilities to communicate with the outside world, while others use its QoS features for better internal communication. For example, a department of the US government uses the Multiservice IP-to-IP Gateway to improve the quality of its internal, encrypted H.323 conversations and videoconferences. Even with dedicated lines between all

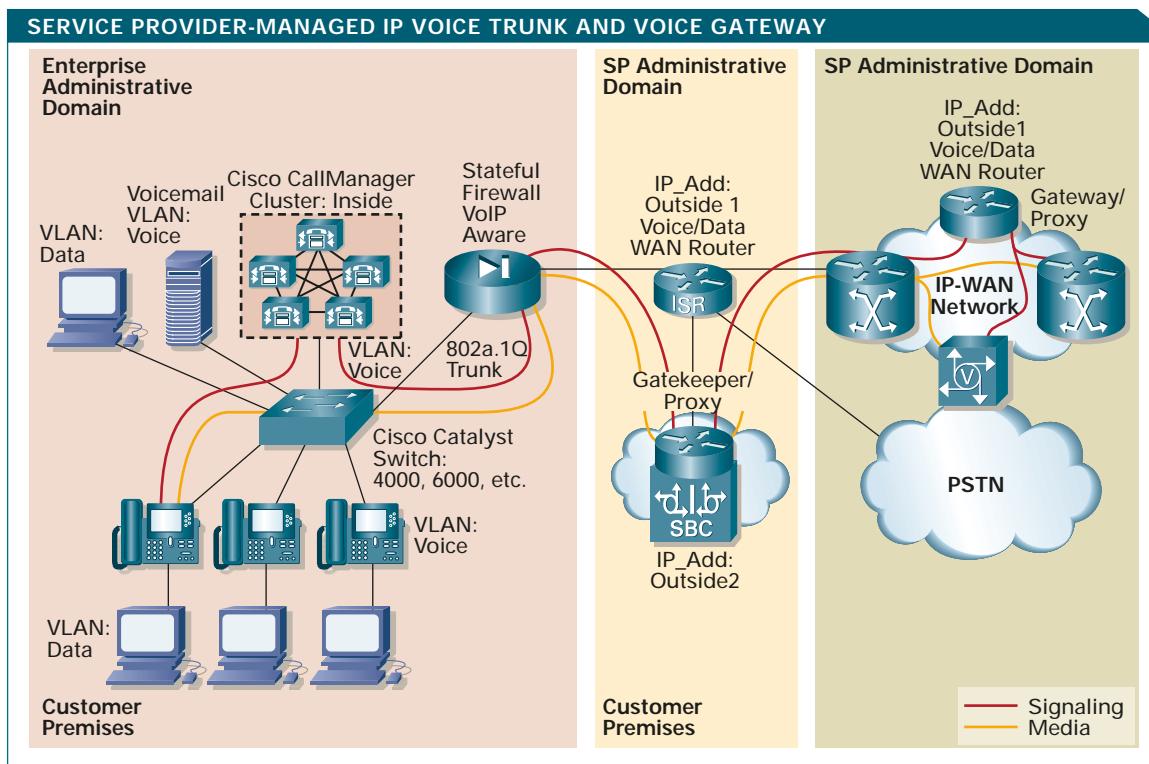
its locations, employees were often frustrated with their voice and video calls breaking up at unpredictable times. Now, using RSVP, the Multiservice IP-to-IP Gateway reserves an appropriate level of bandwidth throughout the network before a call is completed. Quality is consistent for the duration of the entire call.

Service providers also use the Multiservice IP-to-IP Gateway in several different ways. Service providers with existing VoIP service offerings replace their back-to-back media gateways with a more efficient, less latency-inducing Multiservice IP-to-IP Gateway. They deploy it as part of a managed VoIP service for their SMB customers, or they insert it between other peered service provider networks. In either case, the Multiservice IP-to-IP Gateway acts as a network demarcation point, providing signaling and media interworking, and collecting billing information.

Service Provider Peering Example

iBasis is one of the many service providers using the Multiservice IP-to-IP Gateway. A leading carrier of international long distance telephone calls and provider of retail prepaid calling cards in the US, iBasis has points of presence (POPs) and service-level agreements (SLAs) with Internet service providers (ISPs) in 120 countries worldwide. With the aim of reducing its capital expenses, iBasis began installing Multiservice IP-to-IP Gateways several years ago to replace its back-to-back time-division multiplexing (TDM) gateways.

FIGURE 1 Service providers can install the Cisco Multiservice IP-to-IP Gateway on the customer premises and offer a managed IP voice trunk and voice gateway services to enterprises.



Sample Configuration of a Multiservice IP-to-IP Gateway

	COMMAND OR ACTION	PURPOSE
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Router(config)# voice service voip	Enters VoIP voice-service configuration mode.
Step 4	allow-connections from-type to-type Example: Router(config-voi-serv)# allow-connections h323 to h323 Router(config-voi-serv)# allow-connections h323 to sip Router(config-voi-serv)# allow-connections sip to sip	Allows connections between specific types of end points in an IP-to-IP Gateway. Arguments are as follows: <i>from-type</i> —Type of connection. Valid values: h323 and sip. <i>to-type</i> —Type of connection. Valid values: h323 and sip.
Step 5	exit Example: Router(config-voi-serv)# exit	Exits the current mode.

The return on investment was immediate, with the Multiservice IP-to-IP Gateway paying for itself in a matter of months, says Ajay Joseph, vice president of Network Architecture and Engineering for iBasis. The company was able to stop using TDM B2B [back-to-back] gateways and related PSTN circuits entirely, meeting its goal of reducing capital expenses. "Not only did we save money, we also improved our voice quality," explains Joseph. "Now we are a 100 percent IP network."

One of the reasons iBasis chose Cisco was its routing functionality. "The Multiservice IP-to-IP Gateway acts as a tandem point in our Assured Quality Routing network," says Joseph. iBasis' proprietary Assured Quality Routing performs real-time monitoring and dynamically reroutes traffic to alternative routes if key thresholds of network performance are exceeded.

Managed Voice Service Example

Figure 1, page 20, illustrates two administrative domains. The service provider offers a managed IP voice trunk and voice gateway service to the enterprise network on the left. The service provider has

installed a Cisco Multiservice IP-to-IP Gateway on the customer premises, and manages the transport of calls to and from enterprises that use Cisco Call-Manager. Billing records are generated on the Multiservice IP-to-IP Gateway. Service providers offering bundled voice, video, and data services can choose to install the Cisco Multiservice IP-to-IP Gateway on the Cisco Integrated Services Router that provides the data and WAN connectivity. Supporting these three functions on one hardware platform greatly simplifies setup, configuration, and maintenance on the customer premises.

Prepaid Calling Service Example

Another example of a Multiservice IP-to-IP Gateway deployment is a prepaid calling service. iBasis offers customers a prepaid calling service that runs across Cisco Multiservice IP-to-IP Gateways. Incoming PSTN calls using iBasis calling cards are terminated by local ISPs on media gateways and passed off to the iBasis network using the Multiservice IP-to-IP Gateway. The Multiservice IP-to-IP Gateway supports Toolkit Command Language (TCL), prompting callers for their usernames and passwords via an interactive voice response (IVR) script. Depending on the service being offered, service providers can also use the authentication, authorization, and accounting (AAA) capabilities of the Multiservice IP-to-IP Gateway to authenticate their users.

Enterprise Deployment Environment

Enterprises installing the Gateway also have several options. They can deploy it on a standalone Cisco router platform, such as a Cisco 3800 Series Integrated

Talk About It

Want to share your expertise on voice technology with your peers? Get answers to your questions from Cisco experts? Join a Networking Professionals Connection discussion at cisco.com/discuss/voicegeneral.

Services Router. They can also deploy it on the same router as their Cisco Gatekeeper, minimizing configuration and maintenance (see online figure at cisco.com/packet/174_5a1). Once the Multiservice IP-to-IP Gateway registers with the Cisco Gatekeeper, all calls to the Gatekeeper send call setup information directly to the Multiservice IP-to-IP Gateway's IP address. All signaling messages are terminated and reoriginated on the Multiservice IP-to-IP Gateway. The enterprise advertises only two IP addresses: *Outside2*, the address of the Multiservice IP-to-IP Gateway, and *Outside1*, the address of the voice/data/WAN router.

In this deployment, IP and video phones are on one virtual LAN (VLAN), and computers and laptops are on another. Each VLAN has defined different QoS policies using the IEEE 802.1Q standard. The IP-to-IP Gateway also supports RSVP Call Admission Control (CAC) for voice and video H.323 or SIP calls. RSVP CAC and QoS define bandwidth, jitter, and burst requirements, and are useful for real-time traffic such as videoconferencing.

According to Richard Wheeler, president of Wheeler Network Design, RSVP support was the key reason his client chose Cisco. "Cisco was the only vendor

able to proxy their voice, video, and other multimedia services using RSVP," explains Wheeler.

The Cisco Multiservice IP-to-IP Gateway enables secure, rich-media communications across both enterprise and service provider boundaries. By creating IP-based interconnects and eliminating PSTN connectivity, both enterprises and service providers can secure their voice and video over IP networks, reduce their communications costs, and improve their voice quality. ■

FURTHER READING

- Cisco IP-to-IP Multiservice Gateway technical documentation
cisco.com/packet/174_5a1
- Cisco voice technologies
cisco.com/packet/174_5a2
- Cisco Integrated Services Routers
cisco.com/packet/174_5a3
- Session Initiation Protocol (SIP) RFC 3261
www.faqs.org/rfcs/rfc3261.html

Extending the Network—to Anything

Cisco's RFID solutions bring intelligence to the edge of the network and beyond.

By Janet Kreiling

IP networking has brought a huge burst in productivity. But until recently those increases in productivity necessarily stopped at the computers, PDAs, mobile phones, and similar devices that link to the network at its edge. Of course, the network extends to wherever people take these devices—but only that far. Now, however, networking is poised to overtake those limits.

Radio frequency identification (RFID) and sensor tags are beginning to take the network to anywhere a need exists: a case of milk on a truck, a pallet of VCRs, a drug that can't be exposed to high temperatures, a patient in an assisted living facility, or even a child. "If a farmer wants to locate cattle easily," says Ed Jimenez, marketing manager for RFID at Cisco, "even a steer, given an 802.11 RFID tag, could someday have an IP address."

RFID devices can identify things such as that case of milk, and in combination with sensors, can tell what temperature, shocks, pressure or other conditions an object has been exposed to; they can locate items; and they can get all of that information onto the Internet.

To help companies and other organizations employ RFID technology effectively, Cisco has introduced an RFID solution for each of the two basic types of RFID tags. Cisco's Application-Oriented Networking (AON) for RFID solution initially works with *passive tags*, the inexpensive ones used on cases of milk and most other products. (For more on application networking, see the special report, page 41.) These tags don't do anything except let themselves be read. In contrast, Cisco's Wireless Location Solution works with *active tags*, which contain batteries; their locations can be deduced so the items to which they are attached can be found.

In addition, Cisco offers the expertise to help companies develop cost-effective and useful RFID implementations, and a "vendor ecosystem" of technology development partners that enables makers of RFID tags and readers to make sure their products are compatible with Cisco networks and RFID solutions.

"Cisco is getting involved with RFID technology because it is the future of the network; RFID potentially

allows anything to become part of the network. That's definitely Cisco territory," says Jimenez.

Moreover, Cisco's AON solution for RFID achieves another important step: installing intelligence at the network edge so it becomes a place where some business decisions can be made—a strategy that can improve productivity and save costs. "This is a whole new way of looking at the network," says Chris Wiborg, a solution product manager in Cisco's Application-Oriented Networking Business Unit. "For many people, when they understand what intelligence at the edge can do, it's an 'Aha!' moment."

Cisco AON for RFID Solution

Most tags are passive, affixed to pallets or cases so their identification can be obtained by readers. The readers can generate continuous streams of data; servers then interpret it and create reports or orders for action. This scenario has a couple of problems. If you have many, many tags and readers, your network may feel the strain—a large distribution center may have a daily in-and-out of a half-million cases of goods. Sending raw data back to a server for interpretation takes time, especially if a human must weigh in for a decision.

"If you are loading a truck with TVs and you mistakenly load a case of VCRs, you don't want to wait for an exception notice from a system in the data center, based on the VCR case tag. In the time that alert takes to get back to you, the truck might leave with the wrong goods," Wiborg says.

Moreover, you cannot always put servers close to where tags are deployed. Sometimes the environmental conditions are not friendly to server hardware; sometimes there are just too many locations for a company to absorb the capital and maintenance costs. As RFID tags come into wide use, these problems can hinder their potential.

At its most basic, the AON for RFID solution understands RFID messages and events, so it helps integrate RFID data into enterprise applications while lowering the overall cost of an RFID infrastructure.

But this solution can also promote RFID technology up to its full potential: adding many more information sources to business decision-making in a managed way

to enhance productivity, particularly throughout the supply chain. Two examples:

1. The manager of a grocery store wants to be sure that a case of milk has been refrigerated properly all along its route. But how? An RFID tag on the case is automatically correlated by Cisco AON with temperature data from a sensor on the delivery truck, indicating whether the temperature has exceeded specifications at any time. If it has, the case stays on the truck because Cisco AON raises the alarm.
2. Before: A case of a soft drink arrives at a store's loading dock. Notification of the store manager, the department manager, and the financial department requires data entry into three different applications. After: All three, along with the vendor and supplier, are notified electronically, automatically, and instantly.

The RFID tag—and the item to which it is affixed—has become part of the network. And an action is taken or a decision made at the edge of the network, using intelligence in a Cisco AON module located on a blade in the nearest Cisco Integrated Services Router.

These examples are based on Cisco AON's ability to filter, secure, correlate, and integrate data from RFID tags. In the first example, tag readers register the case or pallet of the product as it comes in through the loading dock, and send the information on to the Cisco AON blade. Cisco AON, which interacts with all reader types, has already been configured to control when a given reader should read—say a few seconds out of every minute—so as to log every case or pallet but not overload the system with multiple readings of the same tag.

The Cisco AON module filters out any remaining duplicates, aggregates readings as instructed by an application such as a warehouse management system (WMS) to create an application-level event, and then sends the event to specified destinations while generating a notification event as instructed. If the event is an exception to the parameters the Cisco AON module has been given, the module can make a decision, at the network edge, such as notifying warehouse personnel to refuse acceptance of the too-warm milk.

As Roland Saville, a technical leader in Enterprise Systems Engineering at Cisco, explains, the information on the tag is encoded in a 64- or 96-bit message as specified by the Electronic Product Code (EPC) Global Network Architecture. The code includes the type of product, the manufacturer's name, and the serial or lot number. Filtering and aggregation, as well as reader management, are performed by RFTagAware middleware written by Cisco partner ConnecTerra. Cisco has added features such as reader management, message routing, authentication, security, and others.

The EPC framework also extends to a higher level, called the EPC Information Services (EPCIS) layer, whose role includes interpreting data. The intelligence required at this level might be built into a data center-based WMS or enterprise resource planning (ERP) system that gives Cisco AON instructions as to what specific RFID information or events it is interested in receiving. This level of intelligence can also be built into the Cisco AON module—for example, in a “bladelet” that reads EPC values and correlates them with temperature sensors, as with the case of milk. A bladelet is a bit of special-purpose code programmed into the Cisco AON module.

Multilingual

The Cisco AON speaks many protocols, including different versions of Extensible Markup Language (XML). So after the Cisco AON blade has filtered and aggregated the data, it can translate the data into XML or the message format required by any application. Once given instructions, it can then send information anywhere within the company's various enterprise software systems or to specific individuals or departments.

Using its protocol vocabularies, Cisco AON can understand the context and contents of a message, so it can apply policies and priorities. It can distinguish among point-of-sale (POS), RFID tag, customer relationship management (CRM), WMS, and e-mail messages, for example, and appropriately mark traffic for prioritization across the WAN. If so instructed, Cisco AON can thereby prevent tag data from interfering with POS transaction data traveling over the LAN or WAN. It can also route and prioritize messages according to content.

Saville explains, “Say a store runs out of chairs that are on sale and orders more. It can identify the needed order quickly by the EPC tag coding. Cisco AON can then notify the store manager immediately by sending a high-priority message that the new order has arrived at the distribution center.”

Cisco Wireless Location

Cisco also has a solution for active RFID tags, which are generally used differently from passive tags. The trick with active tags is figuring out where they, and the items they are attached to, are. An example:

Before: A truckload of DVD players, game consoles, and other goods has arrived at the warehouse, but where's the forklift? The goods register as being in the warehouse, but can't be found for customers. After: the RFID-tagged forklift is found immediately and begins unloading the truck. Goods located are goods that can be sold.

Cisco's wireless location solution uses a patented “fingerprinting” technology to locate items with active tags to within a few meters anywhere inside a

hospital, warehouse, or other building. Just as warehouse managers and nurses have become immediately reachable through mobile phone networks, now equipment or people can also be found instantly. The solution can incorporate both PanGo and Aeroscout tags for Wi-Fi devices.

RF fingerprinting is done by a triangulation scheme in which readings of power levels throughout a building and within individual rooms, taken from several nearby wireless access points for each location, are programmed into the Cisco Wireless Location Appliance database. "Cisco is the only manufacturer that has both the location technology and the access points, so customers can get the benefits of dynamic power adjustments to optimize coverage without disrupting the ability to locate devices that depend on the RF fingerprinting," says Saville.

The Cisco Wireless Location Solution can also locate rogue access points, and through its Simple Object Access Protocol/XML application programming interface, can be linked to a variety of enterprise applications or an AON console in the data center. The system can locate any IEEE 802.11-compliant device, as well as RFID tags, and can also filter and aggregate data if needed.

Pieces of the Solutions

The Cisco AON for RFID solution consists of the Cisco AON Module, which can be installed as a blade in any of the Cisco 3800, 3700, 2800, and 2600 series routers and the Cisco Catalyst 6500 Series Switch, along with the Cisco AON Management Console and the Cisco AON Development Studio. The latter is a Windows-based tool with which developers can configure the handling of messages, bladelets for functions such as security, priority, and custom functions. Cisco technology partners Intermec and ThingMagic readers have been tested and approved as compatible with AON for RFID.

The Cisco Wireless Location Solution employs the Cisco Wireless Location Appliance, the industry's first location solution that simultaneously tracks thousands of devices within the WLAN infrastructure. Simple to deploy, it enables easy tracking of high-value items—not only those with active RFID tags, but also Wi-Fi-enabled laptops and rogue access points.

Services to Support the Solutions

Cisco has developed an extensive support program for both solutions. "Because extending the network with passive or active RFID devices is new, many companies need more help than usual in an IT installation for using the application most effectively and ensuring that their network is primed for it," says Mike Crane, senior director of Advanced Services at Cisco.

Cisco can support all three phases of installing an RFID application: assessing network readiness, developing and running a pilot, and production-scale implementation. In the readiness assessment phase, Cisco looks at such critical areas in the network as physical connectivity and QoS configuration, and performs an RFID Data Flow Assessment. "By looking at these areas we can proactively identify potential RFID issues in the network," Crane says. "We can also ensure that RFID traffic behaves as a 'good network citizen', and minimizes impact to the other applications that use network resources."

During pilot planning, the Cisco support team can recommend and implement proven use cases that address specific business objectives.

The "Internet of Things"

As RFID becomes a networked application, its communications change from serial to IP; proprietary technology changes to open; separate networks yield to converged ones; and high costs drop to affordable—all good results. But perhaps the most important change is that all kinds of things can potentially be networked: products, drugs, pets, people, currency, livestock, shipping containers, food.

"The result will be lower operating and capital costs, a more flexible, agile network, improved productivity, and optimized business processes," says Kevin Raack, an enterprise marketing manager at Cisco.

"Cisco's is the only RFID solution that is embedded in the network," Wiborg adds. "It leverages the network an enterprise already has in place to provide functions such as filtering, quality of service, authentication, routing, security, and many others so the RFID application itself works smoothly and effectively."

As one customer pointed out, "RFID will be the differentiator between the haves and have-nots."

The *network* is the source of competitive advantage. ■

FURTHER READING

- *Packet* article on RFID technology
cisco.com/packet/174_5c1
- *Packet* article on Cisco AON
cisco.com/packet/174_5c2
- Cisco RFID website
cisco.com/go/fid
- Cisco AON website
cisco.com/go/aon
- Cisco Integrated Services Routers poster
cisco.com/packet/174_5c3

Cell Packing on the Cisco 12000 Series Router

ATM cell-packing technology enables service providers to improve bandwidth utilization.

By Javed Asghar, Syed Nawaz, and Muhammad Waris Sagheer

Cell packing (also referred to as *cell concatenation*) is a mechanism in which multiple cell-relay Asynchronous Transfer Mode (ATM) cells are encapsulated in an IP/MPLS packet. It allows service providers to overcome bandwidth inefficiencies inherent in cell relay transport.

Cell Relay Bandwidth Inefficiency

Cell relay causes inefficient use of packet-switched network (PSN) bandwidth for the following reasons.

Cell relay reduces packet-per-second (PPS) efficiency by switching every cell relay packet. For example, if six ATM cells are transported the core switches six packets and six PPS bandwidth is consumed. However, if six ATM cells are packed into a single packet using cell packing, then the core switches one packet and one PPS bandwidth is consumed. Service providers can use cell packing to save PPS bandwidth in the core.

Cell relay also causes inefficient bandwidth utilization. For example, assume that a service provider

wants to transport a stream of cell-relay ATM cells over a Multiprotocol Label Switching (MPLS) core that consists of packet-over-SONET (POS) interfaces. On the ingress provider edge, the 52 bytes of ATM cell (without 1-byte header error checksum [HEC]) is prepended with 4 bytes of control word, 4 bytes of virtual circuit label, 4 bytes of tunnel label, and 4 bytes of Cisco High-Level Data Link Control (HDLC) Layer 2 header. The total overhead is 16 bytes for every 52 bytes of ATM cell. The resultant packet size on the POS fiber equals 68 bytes (that is, 52 bytes of ATM cell + 16 bytes of overhead). In this case, the bandwidth inefficiency of cell relay is approximately 23.52 percent (52/68 percent).

When cell packing is used in the preceding scenario, and assuming that you pack six cells into a single MPLS packet, the total overhead is still 16 bytes but payload is 312 bytes, which improves bandwidth efficiency by approximately 4.87 percent. Therefore, service providers can use cell packing to improve bandwidth utilization to 18.65 percent (23.52-4.87 percent).

Cell packing is supported on Cisco 12000, 7500, and 7200 series routers, but this article focuses primarily on implementations on Cisco 12000 Series routers with 4-Port IP Services Engine (ISE) ATM-over-SONET OC-12/STM-4 and 4-Port ISE ATM-over-SONET OC-3/STM-1 line cards.

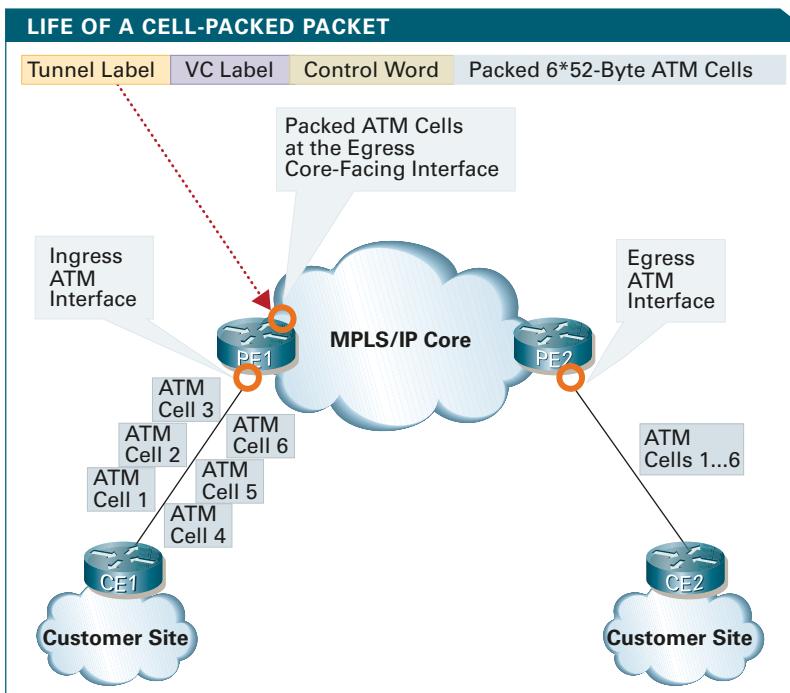
The table on page 27 lists Cisco 12000 cell-packing feature support.

Cell-Packing Parameters

Cell-packing has two parameters: *Minimum Number of Cell Packing (MNCP) size* (also known as cell-pack size) and *Maximum Cell Packing Timer (MCPT) timeout*.

During provisioning of cell-packing connections, you must configure the MNCP size and MCPT timeout values. This information is programmed in ingress and egress hardware cell-packing field programmable gate array (FPGA).

SAVING BANDWIDTH
ATM cells are packed in an MPLS network, improving PSN efficiency.



Ranges are as follows:

- MNCP size range is 2 to 28 ATM cells
- MCPT value range is 2-4095 microseconds (μ s) (IOS-configurable range)
- MCPT hardware programming range is 50 μ s to 25ms (MCPT timeout granularity is in 50 μ s increments)

Maximum MNCP size is 28 ATM cells because Ethernet MTU is 1500 bytes; otherwise cell-packed MPLS packets greater than 28 packed ATM cells will be dropped on Ethernet interfaces. Although the Cisco IOS Software command-line interface (CLI) enables you to configure MCPT values 2-4095 μ s, the hardware programmable range is actually 50 μ s-25ms in 50 μ s increments.

During the label advertisement and binding period, PE1 and PE2 exchange the MNCP size by setting the LDP Interface Parameters field. When the MNCP of PE2 is received on PE1, it is stored in the predefined VC/VP/port database on PE1 and vice versa. Any change of MNCP on either of the provider edges triggers label withdrawal and re-establishment of the emulated virtual circuit on both ends, and the old value is replaced by the new one.

If cell packing is not supported on PE1, (that is, MNCP equals 1) PE2 should send a single cell per MPLS packet, but can receive packed cells if cell packing is enabled on PE2.

The MCPT is locally significant and its range is usually determined by the ATM link speed OC-3 or OC-12. When the MCPT timer expires, the packed cells are immediately sent out in an MPLS packet even if the packing is not completed; that is, the number of cells in the packet does not reach the MNCP.

Life of a Cell-Packed Packet in an MPLS Network

Figure 1, page 26, illustrates ATM cells being packed in an MPLS network.

On the ingress provider edge, the ATM cells arrive at the ATM port for segmentation and reassembly (SAR) chip processing. The SAR chip classifies each ATM cell as an AAL0, AAL5, or OAM cell. For valid AAL0 cells the SAR chip strips 1 byte of HEC from the ATM cell header and forwards the resultant 52-byte ATM cell to the cell-packing FPGA. The cell-packing FPGA packs cells based on MNCP and MCPT-configured parameters.

Incoming ATM cells are queued up to the configured number of cell-pack size before the MCPT timeout to form one cell pack. Then the FPGA generates the control word, encodes the T flag to 0 to specify AAL0 ATM cell type, and generates a sequence number for each cell-pack packet. The remaining fields are set to 0.

The FPGA prepends the control word (CW) to the cell-packed packet and forwards the packet to the hardware-forwarding ASIC. (CW is optional during pseudowire setup. If both PEs negotiate to support CW it will be used; otherwise it is not inserted.)

Cisco 12000 Series Router Cell-Packing Support

Cisco 12000 line cards	4-Port IP Services Engine (ISE) ATM over SONET OC-12/STM-4 4-Port ISE ATM over SONET OC-3/STM-1
Cisco 12000 chassis	All
Software	Cisco IOS Software Release 12.(27)S1 and later
Cell-packing transport modes	Virtual Circuit Connection Mode Virtual Path Connection Mode Port Connection Mode
Operation, Administration, and Maintenance (OAM)	Segment loopback and fault management on F4 and F5 Fault management on F4 and F5
Quality of service	Cell loss priority (CLP) classification Experimental (EXP) marking ATM Forum Traffic Management 4.0 and 4.1 per virtual circuit policing, queuing, and shaping Policing action-based cell packing Weighted Random Early Detection (WRED) and Modified Deficit Round Robin (MDRR) Egress dual CLP threshold queue limit
Switching types	Pseudowire Local switching

The hardware-forwarding ASIC imposes the VC and Tunnel labels and then forwards the packet to the core-facing MPLS link. The core-facing MPLS link prepends Layer 2 headers to the MPLS packet and places the MPLS packet on the fiber.

In the MPLS core the packet will consist of one pack of ATM cells + CW + VC label + IGP label + Layer 2 header. The Tunnel label will be disposed of on the penultimate hop. The packet sent to the egress provider edge consists of one pack of ATM cells + CW + VC label + Layer 2 header.

On the egress provider edge, the core-facing MPLS link extracts the packet from the fiber, removes the Layer 2 header, and forwards the packet to the edge-facing line card. The hardware-forwarding ASIC on the edge-facing line card disposes the VC label and forwards the resultant packet to the egress cell-packing FPGA.

The egress cell-packing FPGA strips off the control word and uses its FIFO buffer to unpack the ATM cell-packed packet to 52-byte ATM cells. The 52-byte ATM cells are then forwarded to the SAR chip.

The egress SAR chip receives the 52-byte ATM cells from the FPGA and adds a 1-byte HEC to the ATM cell header to make a 53-byte ATM cell. The ATM cells are transmitted out of the wire on the egress ATM permanent virtual circuit.

Cell-Packing Configuration and Verification

Following are three examples of cell-packing configuration: VC Mode, VP Mode, and Port Mode. Cell-packing verification is also shown.

In Example 1 (see also figure on page 26), PE1 and PE2 are configured with cell-packing VC mode, MNCP is six cells, MCPT is 100 µs, and traffic is bidirectional at OC-3 line rate.

Example 1: Cell-Packing VC Mode Configuration

```
PE1#sh running-config interface ATM 5/0
Building configuration...
Current configuration: 286 bytes
!
interface ATM5/0
  atm mcpt-timers 50 100 200
```

JAVED ASGHAR is a software engineer who specializes in Advanced MPLS Technologies for the Gigabit Switching and Router platform in the Routing Technologies Group at Cisco. He can be reached at jasghar@cisco.com.

SYED NATIF NAWAZ, CCIE No. 8825, is a software development manager for the Gigabit Switching and Router platform in the Routing Technologies Group at Cisco. He can be reached at sawaz@cisco.com.

MUHAMMAD WARIS SAGHEER is a software engineer who specializes in Advanced MPLS Technologies for the Gigabit Switching and Router platform in the Routing Technologies Group at Cisco. He can be reached at waris@cisco.com.

```
pvc 0/32 12transport
cell-packing 6 mcpt-timer 2
encapsulation aal0
xconnect 203.203.203.203 1 encapsulation mpls
!
end
PE2#sh running-config interface ATM 2/2
Building configuration...

Current configuration : 307 bytes
!
interface ATM2/2
  atm mcpt-timers 50 100 200
  pvc 0/32 12transport
  cell-packing 6 mcpt-timer 2
  encapsulation aal0
  xconnect 201.201.201.201 1 encapsulation mpls
end
```

Sample Cell-Packing VP Mode Configuration

In Example 2, PE1 is configured with Cell Packing VP mode and PE2 configuration is symmetric. MNCP is six cells and MCPT is 100 µs.

Example 2

```
PE1#sh running-config interface ATM 5/0
Building configuration...
Current configuration : 263 bytes
!
interface ATM5/0
  atm mcpt-timers 50 100 200      << Three independent timers in microseconds
  atm pvp 1 12transport           << MNCP 6 and MCPT 100 microseconds
  cell-packing 6 mcpt-timer 2
  xconnect 203.203.203.203 1
  encapsulation mpls
end
```

Sample Cell-Packing Port Mode Configuration

In Example 3, PE1 is configured with Cell-Packing Port mode and PE2 configuration is symmetric. MNCP is six cells and MCPT is 100 µs.

Example 3

```
PE1#sh running-config interface ATM 5/0
Building configuration...
Current configuration : 238 bytes
!
interface ATM5/0
  atm mcpt-timers 50 100 200
  cell-packing 6 mcpt-timer 2
  xconnect 203.203.203.203 1 encapsulation mpls
end
```

Verification of Cell-Packing in Example 1:

```
PE1#sh atm cell-packing
average          average
circuit          local nbr of cells    peer
nbr of cells     MCPT
type            MNCP   rcvd in one pkt  MNCP
                sent in one pkt  (µs)
```

ATM5/0	vc	0/32	6	6
6	6		100	
 PE2#sh atm cell-packing				
average average				
circuit	local	nbr of cells	peer	
nbr of cells	MNCP			
type	MNCP	rcvd in one pkt	MNCP	
sent in one pkt	(μs)			
ATM2/2	vc	0/32	6	6
6	6		100	

Summary of **show atm cell-packing** output:

- Circuit type shows that cell-packing is VC mode.
- Local MNCP shows that the local configured MNCP value is 6.
- Peer MNCP shows that the peers configured MNCP value is 6.
- MCPT (μs) shows the local configured MCPT timeout window.
- Average number of cells received in one packet shows the six cells received in one cell pack from the peer.
- Average number of cells received in one packet shows the six cells sent in one cell pack to the peer.

Cell-Packing Deployment Considerations

When planning to deploy cell-packing you must consider MCPT and MNCP values based on network traffic patterns and service-level agreements (SLAs). Additional latency and jitter is induced during cell-packing that can be controlled by selecting optimal MCPT and MNCP values.

Assuming ideal conditions, the following is the required theoretical MCPT timeout value for MNCP size 2 and 28 cells, respectively. This example assumes that ingress traffic is at line rate on the Engine 3 ATM OC-3 or OC-12 interfaces. You can use Formula 1 as a tool for your cell-packing network design.

Formula 1:

$$\text{Theoretical_MCPT } (\mu\text{s}) = \frac{\text{MNCP_Size (cells)}}{\text{Ingress_traffic_Rate (cells/s)}}$$

Case 1:

- MNCP size = 2 cells
- OC-3 line rate ingress traffic rate = 353208 cps
- Using Formula 1, the theoretical MCPT = 5.662μs

Case 2:

- MNCP size = 28 cells
- OC-3 line rate ingress traffic rate = 353208 cps
- Using Formula 1, the theoretical MCPT = 79.27μs

Case 3:

- MNCP size = 2 cells
- OC-12 line rate ingress traffic rate = 1412832 cps
- Using Formula 1, the theoretical MCPT = 1.416μs

Case 4:

- MNCP size = 28 cells

- OC-12 line rate ingress traffic rate = 1412832 cps
- Using Formula 1, the theoretical MCPT = 19.82μs

The preceding computed MCPT values are theoretical, but in your network design calculation you will need to factor in the hardware programmable range 50μs -25ms in 50μs increments. During cell-packing provisioning the MCPT should budget for the Cell Transfer Delay (CTD) contributed by ATM switching, network propagation delay, queuing and scheduling delay, and latency or jitter at congestion points.

The preceding calculation demonstrates that cell packing improves bandwidth utilization. However, when packing more cells, each cell being packed must wait until all cells are received for packing or the MCPT expires, whichever occurs first. This introduces additional CTD (latency) and Cell Delay Variation (CDV, or jitter).

The Cisco IOS Software provides flexible knobs to control such tradeoffs by allowing users to configure a range of MCNP and MCPT values, which permits optimization of the CTD and CDV to meet tight SLA requirements.

For real-time traffic ATM service categories (where UNI negotiates CTD, CLR, and CDV) such as CBR and VBR-RT, use minimal packing (two to five cells) to optimize induced CTD and CDV from cell packing on SLAs.

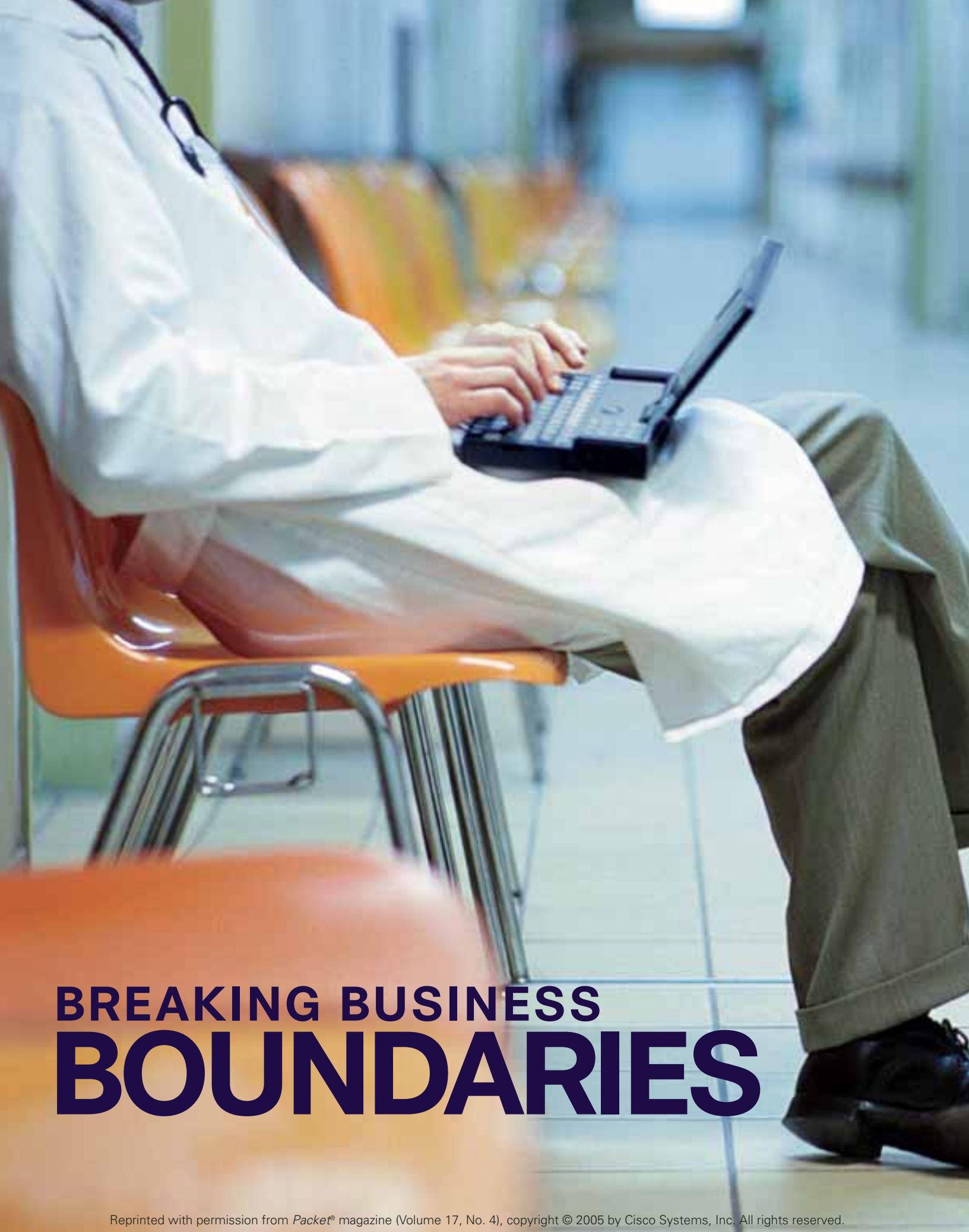
For non-real-time traffic ATM service categories (where UNI QoS negotiation is not required), such as VBR-NRT and UBR, you can pack more cells (10 or more), within SLA boundaries.



In conclusion, cell-packing improves PSN efficiency by concatenating ATM cells. It provides flexible knobs such as MNCP and MCPT to optimize induced CTD and CDV. ■

FURTHER READING

- Cisco IOS Software Release 12.0(30)S 12000, 7500, and 7200 Series AToM
cisco.com/packet/174_5d2
- Cisco IOS Software Release 12.0(30)S 12000, 7500, and 7200 Series Layer 2 QoS
cisco.com/packet/174_5d3
- PWE3 ATM Transparent Cell Transport Service
[ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-ietf-pwe3-cell-transport-04.txt](http://ftp.rfc-editor.org/in-notes/internet-drafts/draft-ietf-pwe3-cell-transport-04.txt)
- Encapsulation Methods for Transport of AToM Networks
[draft-ietf-pwe3-atm-encap-09.txt](http://cisco.com/packet/174_5d4)

A photograph showing a person from the side and slightly from behind. They are wearing a white lab coat over a dark shirt and dark trousers. A stethoscope hangs around their neck. They are seated at a light-colored wooden table, looking down at a black laptop computer. Their hands are on the keyboard. In the background, there are other chairs and what appears to be a hallway or a room with other people.

BREAKING BUSINESS BOUNDARIES



IP APPLICATIONS REDEFINE BUSINESS PROCESSES ACROSS INDUSTRIES

W H E T H E R D E P L O Y I N G I N N O V A T I V E video or Extensible Markup Language (XML) applications to bolster decision-making through collaboration or tapping into their wireless LANs to deliver critical information to the right place at the right time, organizations everywhere are yielding these and other business benefits of running IP applications on their networks.

Success stories of process improvements, enhanced collaboration, improved customer service, productivity gains, and cost savings abound in industries as diverse as healthcare, financial services, government, public safety, and education. Several of these successes are described in "Beyond Voice" (page 32) and "Next Wave for Wireless" (page 36). Regardless of the industry, network administrators of all stripes can tailor the IP-based video, XML, and wireless applications featured on the following pages to support their own business goals.

BEYOND VIDEO



VIDEO AND XML
IP-BASED
APPLICATIONS
TRANSFORM
BUSINESS
PROCESSES—
AND THE
BUSINESSES
THEMSELVES.

BY RHONDA RAIDER



NOT LONG AGO, IP COMMUNICATIONS WAS

synonymous with IP telephony, and organizations adopted it primarily to save money on phone bills and network support. The ensuing process efficiencies from technologies such as unified messaging and advanced call routing often came as unexpected, or side, benefits of rolling out IP telephony.

Jump ahead. Today, IP communications encompasses so much more than IP telephony, and organizations around the world are capitalizing on their quality of service (QoS)-enabled IP networks that they built for IP telephony to deploy innovative new video and Extensible Markup Language (XML) applications. This time around, the explicit purpose is to transform business processes to achieve goals such as differentiating service levels, improving public safety, and enabling better decision-making through collaboration. Success stories of process improvements abound in industries as diverse as financial services, government, public safety, schools, and scientific research consortiums.

Customer Service on Par with Large Counterparts: MagnetBank

Consider MagnetBank, a commercial lender with headquarters in Salt Lake City, Utah. Serving markets in the southeastern US with offices in Atlanta, Raleigh, and Orlando, MagnetBank fills a unique market niche by providing the full range of loans offered by large financial institutions together with the responsive, highly personalized service delivered by community banks.

"Some markets are not large enough to justify a full loan production office with four to eight relationship managers," says Christopher Worel, president and chief operating officer at MagnetBank.

"Using technology, we can provide remote support for a single banker,

enabling them to deliver the same level of client services as a larger branch office," adds Worel.

The bank's infrastructure is based on Cisco 2800 Series Integrated Services Routers, Cisco Catalyst switches, Cisco PIX 500 Series security appliances, Cisco CallManager and Cisco Unity software, and Cisco 7900 Series IP phones.

MagnetBank depends on Cisco voice and video solutions to consolidate all of its communications on a single, manageable network for increased employee collaboration and productivity, and to provide the exceptional customer service its business model is based on. Video-conferencing plays an important role in keeping MagnetBank's customers and employees connected.

"Videoconferencing enables our clients to feel closer to their banks and their bankers," says Worel. "If a client would like to meet me or another executive, the relationship manager can set up a video-conference. It makes the relationship with the bank and senior officers much more tangible."

In-house videoconferencing saves the bank significant dollars as well, reducing travel expenses and the cost of third-party video services. This year MagnetBank conducted its first videoconference board meeting, which included board members from Atlanta and Salt Lake City. Previously, to hold a board meeting, MagnetBank had to rent a videoconferencing system from a local vendor, according to Lindsay Jones, chief financial officer at MagnetBank.

"We were paying almost US\$1,500 to hold a board meeting," says Jones. "When you consider the expense of 12 board meetings a year, the network solution pays for itself quickly. And we can exercise more control by having our own system."

"IP communications provides more than cost savings to MagnetBank," Jones adds. "We're delivering what many banks have lost, which is the personal relationship."

Bring the Courtroom to Defendant: Criminal Justice Applications

Although they grapple with different business challenges than financial institutions, criminal justice agencies around the world capitalize on the same Cisco IP communications solutions. Video, in particular, transforms criminal justice processes for greater effectiveness and safety, according to Morgan Wright, Cisco's global industry solutions manager for public safety.

"Remote video arraignments eliminate travel time, reduce security personnel requirements, decrease transportation costs, and accelerate the justice process," says Wright. "Remote video depositions and hearings reduce or eliminate travel time and expenses for witnesses and increase scheduling efficiency. And virtual proceedings, based on voice and video, bring the courtroom to judges and their staffs when last-minute negotiations require judicial action or approval, or when the judge doesn't need to appear in person."

For the Bernalillo County Metropolitan Court in Albuquerque, New Mexico, IP communications avoids the time and expense of securely transporting inmates and related parties to the court for arraignments and bonding. Instead, intake officers at the court use a Cisco videoconferencing solution to gather demographic, charge, criminal history, and community ties information to determine if a person is eligible for release on his or her own recognizance.

The ability to conduct remote interviews and arraignments accelerates the judicial process, frees staff for other tasks, and reduces the costs of inmate transport vehicles and extra security.

Inmate medical care has received a boost from Cisco videoconferencing solutions both at the Virginia Department of Corrections and the Isle of Man, an independent self-governing dependent territory of the British Crown. Nursing personnel accompany the inmate to an on-site area and conduct an examination that's captured through an IP-based video camera. An off-site physician views the video in real time, asking questions if necessary to provide a diagnosis.

"The telemedicine solution improves the safety and security of corrections personnel as well as the surrounding community by minimizing the need for prisoner transportation," says Wright. "At the same time, it reduces costs such as multiple personnel for transport, vehicle and fuel expense, overtime, and physician contracts."

Greater Situational Awareness for First Responders: Humberside Police

While MagnetBank and the criminal justice agencies use video for one-to-one interactions, a growing number of public safety agencies take advantage of the technology to increase situational awareness of incidents such as fires or traffic accidents.

Case in point: Humberside Police, which serves a resident population of 900,000 on England's eastern coast. One of the most successful police forces in the UK, Humberside Police uses a Cisco IP/TV solution to transmit live video footage of

major incidents captured from a helicopter to the ten or so largest police stations across the jurisdiction. Personnel can view the images over the departmental intranet, giving them the context to make decisions with the best outcome.

"The Cisco IP/TV solution provides us with brilliant additional information," says Mike Foster, data network systems and security supervisor for Humberside Police. "Decision-makers can actually see what's happening on the ground."

A Less Expensive Cable TV Broadcast: City of Monterey

Citizens can see what's happening in City Council chambers, thanks to another innovative use of Cisco IP communications by the City of Monterey, California. The city records its council meetings for live broadcast over a local cable TV channel.

"Most cities build a dedicated analog video network for this purpose, but we engineered our IP network from the start with video in mind," says Fred Cohn, assistant city manager.

The video is captured with an analog camera, passes through a codec for transmission over the Cisco IP network in digital format, and then finally arrives at the community media center where it is translated to an analog signal that can be broadcast over the cable TV network. Council meetings are also streamed live from servers at the community media center and are also stored there for later video-on-demand service, says Cohn.

"By sending the video streams over our Cisco IP network, we avoided the extraordinary expense—more than US\$450,000—of developing a separate analog network," says Cohn.

Sharing Lab Space Across the Globe: Lawrence Berkeley National Laboratory

Not surprisingly, the global scientific community has embraced the potential of IP communications to overcome an inherent challenge of global science. To wit: geographically dispersed researchers can accomplish far more through collaboration, but generally cannot meet face to face because of time and money constraints.

IS IT A PHONE OR A PC?



More kudos for creativity go to the organizations that deliver XML applications via the built-in display screens of their employees' Cisco IP phones. Employees can access data when they need it—which is often while they are talking to someone else on the phone—and in some cases employers save the cost of deploying an extra PC.

In the UK, the Blackpool Local Education Authority provides Cisco IP phones in classrooms, which teachers use with an XML application to record pupil attendance. This application relieves administrators of the time-consuming chore of manually entering attendance information from paper logs. In another creative use of the network and IP phones, administrators communicate efficiently with teachers in every classroom by sending instant bulletins as text messages that appear on the Cisco IP phone screens, or as announcements played over the IP phone speakers.

The Arizona State Department of Commerce developed another XML application, called TravelWeb, which improves service levels to callers. The agency's employees travel often to help cities, counties, town boards, etc., throughout Arizona plan and develop their communities and improve their infrastructure for constituents, as well as to make presentations to businesses considering relocating to the state. Employees enter their travel schedules into a Web-based application, and any other employee can retrieve that schedule from their Cisco IP Phone, using TravelWeb.

"A business considering establishing itself in Arizona might call the front desk and ask to talk to the person who gave a presentation to their group on a particular date," says Eric Mayer, IT manager for the Arizona Department of Commerce. "From the IP phone, the receptionist can enter the date and see a list of all people who were traveling that day, and where they went. This level of service gives businesses a flavor of what they can look forward to by moving to the state."

For the Energy Sciences Network (ESnet) located at Lawrence Berkeley National Laboratory in California, a Cisco IP communications solution enables scientists from around the world to collaborate by conducting conferences that integrate voice, video, and Web conferencing.

Behind some of the world's most important scientific projects—the Human Genome, fusion energy research, nanotechnology and research on climate change—ESnet is a high-speed network serving thousands of scientists and collaborators conducting research for the US Department of Energy's Office of Science at more than 1,000 locations worldwide.

"The ability to share information with other scientists, 'see' their lab setups, control their instrumentation, and view results via the Web makes it much easier for scientists to collaborate," says Clint Wadsworth, ESnet collaboration specialist. "They don't have to physically travel to each others' labs, which usually isn't in the budget."

Using the Cisco MeetingPlace solution, ESnet scientists can set up ad hoc meetings combining voice, video, and Web resources in a single step, or pre-schedule meetings through Web, Microsoft Outlook, or Lotus Notes calendars. They dial in from any video endpoint or telephone, and use Cisco MeetingPlace to share visual aids as they would in face-to-face

meetings—to show presentations, share applications running on their computers, and jointly develop plans and reports.

An example: To study the structure and properties of various materials, researchers at the labs and at the University of Wisconsin use Cisco MeetingPlace to collaborate using Berkeley Lab's Advanced Light Source, the world's brightest source of soft X-ray light. They simultaneously conduct voice conversations, view video of the equipment and its output, and use the Web conferencing capability to view, monitor, and take turns interacting with the Advanced Light Source.

"With Cisco MeetingPlace, ESnet users can feel as though they've walked through another scientist's shop or workroom, whether it's in Albuquerque or Tokyo," says Wadsworth. "A scientist engaged in smashing or fusing atoms might not want to take time out to worry about scanning and digital formats. Video is the answer."

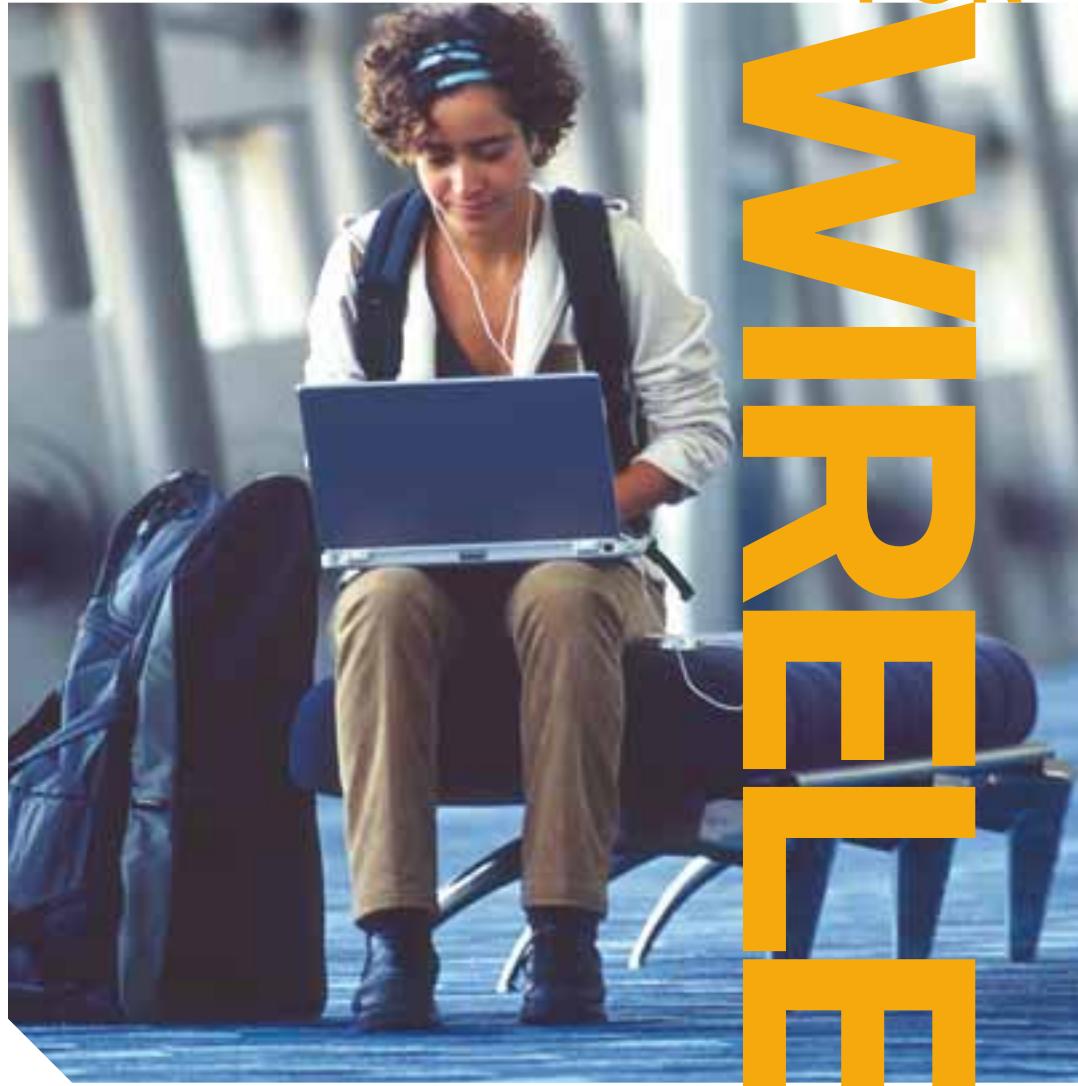
"Our job at ESnet is to support scientific research," notes Wadsworth. "By providing a single means of collaboration with voice, video, and data, the Cisco MeetingPlace solution serves a valuable role in our mission." ■

FURTHER READING

- Cisco IP Communications Applications Central cisco.com/packet/174_6c1

NEXT WAVE FOR

WIRELESS



INNOVATIVE
APPLICATIONS
IN HEALTHCARE,
GOVERNMENT,
AND PUBLIC
SAFETY PROVIDE
INSPIRATION FOR
THE ENTERPRISE.

BY RHONDA RAIDER

VISIT THE HOSPITAL, call the fire department, or request a building permit, and it's more and more likely you might interact with wireless technology. No longer simply a means of Internet connectivity, wireless LANs (WLANs) are irrevocably transforming business processes for greater effectiveness by delivering the "right information to the right place at the right time."

Healthcare, government, and public safety organizations occupy the vanguard of wireless innovation. It's no surprise, because in these industries the stakes for delivering information where and when needed can be life itself. IT groups in all industries can tailor the IP-based wireless applications being used in healthcare and the public sector to support their own business goals.

XML Messaging to Wireless IP Phones: Boston Medical Center

Hospitals are prime candidates for wireless applications. Not only are clinicians mobile, but so are their "customers"—and even their equipment. "Wireless applications help to increase clinician productivity, patient safety, and patient satisfaction, and to reduce costs," says Kent Gray, healthcare solutions process lead at Cisco.

Consider Boston Medical Center, a private, not-for-profit, 547-bed academic medical center. With its old nurse call system, nurses did not always hear overhead pages, which also disturbed patients. And the person sending the page had no way of knowing whether the nurse had heard it, which led to repeated pages and phone calls.

Boston Medical Center improved this process using a wireless nurse call application. Now when patients ring their nurse call buttons to request assistance, the requests are still captured by the hospital's previous Rauland-Borg Nurse Call system. What happens next is new: The nurse call system delivers the requests to an event notification gateway that captures the bed number and type of request, formats the information in an Extensible Markup Language (XML) message, and sends it over the Cisco WLAN directly to the appropriate nurse's Cisco Wireless IP Phone 7920. The nurse can instantly confirm receipt of the message by pressing a soft key on the Cisco IP Phone. Productivity increases for both the nurse and message sender, and patient care improves because nurses receive the message the first time and the XML message contains more information about the patient's needs.

"We chose Cisco for the original campus-wide wired and wireless infrastructure to provide the foundation for adding new services without having to rebuild the network from scratch," says Darrin Dworkin, chief technology officer at Boston Medical Center. "The new nurse call solution is just the beginning, since we can securely integrate other clinical systems and monitoring devices."

This wireless nurse call application is part of the new Cisco Clinical Connection Suite, which also includes applications for patient monitoring, location-based services, and collaborative care. The patient monitoring solution consolidates rules-based alerts from several monitoring devices into a Cisco wireless phone; the on-phone screen displays both text and waveform patient information. With location-based services, users can log in from any PC, where a campus map pinpoints the actual location of misplaced equipment such as wheelchairs and IV pumps. And the collaborative care solution uses audio and videoconferencing technologies to interconnect teams on demand.

Asset Tracking with RFID: Bronson Healthcare Group

When used with active RF identification (RFID) technology or Wi-Fi tags, a Cisco wireless infrastructure helps hospitals more efficiently track assets ranging from wheelchairs to intravenous pumps and dialysis equipment. "The average hospital buys 30 percent more wheelchairs than it needs because they're hard to

find," says Gray. "And at [US]\$1,000 to \$1,500 a piece, that's a very large, preventable capital expense."

At Bronson Healthcare Group in Kalamazoo, Michigan, greeters and orderlies previously had to devote part of each day to looking for wheelchairs, and twice-weekly e-mail "wheelchair alerts" were sent to all 4,000 employees. "We quantified the problem and found that it was costing the hospital thousands of dollars each month if we added up the employee time spent searching and e-mailing, not including the costs relating to lost and vandalized assets," says Nancy Radcliff, registered nurse and director of customer service at Bronson.

Bronson found its solution in a Cisco Unified Wireless Network based on Cisco Aironet lightweight access points, Cisco WLAN controllers, the Cisco Wireless Control System (WCS), a Cisco 2700 Series Wireless Location Appliance, and third-party locator monitor software. In June 2005, Bronson put location tags on 25 percent of its wheelchairs and embarked on a pilot. Now any clinician who needs a wheelchair simply calls a greeter's station and asks for the nearest chair. "A quick glance at the [WCS interface] screen shows exactly where the tagged wheelchairs are located on a map of the site," says Radcliff. "Patients wait no more than a few minutes for a wheelchair, and we save money every month by eliminating searches."

RFID-based asset tracking also increases the productivity of the biomedical engineers who maintain sophisticated medical equipment. Much of the labor costs associated with some equipment calibrations, repairs, and upgrades stem from time spent locating the assets.

THE TECHNOLOGY BEHIND BOSTON MEDICAL CENTER WIRELESS MESSAGING

Before introducing its XML messaging application, Boston Medical Center had already deployed Cisco Catalyst 6509 switches in its network core. To ensure high availability and support a new computer-based physician order-entry (CPOE) system, the hospital IT group upgraded the switches with Cisco Catalyst 6500 Series Supervisor Engine 720 modules. The network core connects 22 campus building and is split, with dual redundant Cisco Catalyst 6509 switches connected by 1 Gigabit Ethernet trunks or 2-Gbit/s EtherChannel links, for high-bandwidth traffic such as radiology images.

The Cisco Catalyst switches support Power over Ethernet (PoE), which is used to supply power to the hospital's Cisco Aironet access points. In 2003, the hospital's IT team extended the wireless network directly to the bedside, enabling staff to bring new applications directly into a patient's room.

CREATIVE WIRELESS APPLICATIONS AT OVERLAKE HOSPITAL MEDICAL CENTER

All-Digital Emergency Information System

In the Overlake Emergency Department, nurses and physicians use portable devices to chart progress notes, look up labs and radiology, and even to show patients their radiology films, bypassing the need to set up light boxes to display them.



Mobile X-Ray

Mobile, wireless-enabled X-ray units transmit images over the WLAN directly to the picture archiving and communication system (PACS). "Wireless X-ray devices can save critical minutes in diagnoses because they eliminate time spent finding a network connection in the patient's room, and then afterwards wheeling the cart back to the radiology docking station," says Overlake Chief Information Officer Kent Hargrave.

Free High-Speed Wireless Access for Patients and Family

Because the Cisco WLAN infrastructure is already in place for business applications, Overlake also uses it to provide free high-speed wireless access to its patients and their visitors. "We've created a VLAN for public access behind our firewall, using the built-in security features of Cisco Aironet access points and the Cisco Unified Wireless Network infrastructure," says Hargrave. Patients who are well enough can do a little work, and new fathers can send digital images from their laptops.

"By enabling us to provide care closer to the bedside, our Cisco wireless infrastructure has increased staff efficiencies and improved patient satisfaction," Hargrave notes.

Bedside Registration: Overlake Hospital Medical Center

Overlake Hospital Medical Center in Bellevue, Washington, also capitalizes on its Cisco WLAN to improve patient care as well as clinician productivity. For example, patients no longer need to wait in the Emergency Room or lobby to be registered because it's the only place the database can be accessed. Instead, a roaming registration person brings a wireless tablet to the patient's bedside after the patient has received critical care. "With our Cisco WLAN, we can 'bring the registration to the room,'" says Kent Hargrave, chief information officer at Overlake. Recently the hospital upgraded to the Cisco Unified Wireless Network using Cisco Aironet lightweight access points, which maintain WLAN connectivity even when the registration person exits one zone and enters another.

Overlake nurses use wireless IP phones to check the status of lab orders or to call radiology, eliminating the time they previously spent returning to the nurse's station to use the phone. And when physicians call back to return a nurse's message, they can reach the nurse directly instead of calling a central location where someone has to find the nurse—another time savings.

Hospital personnel who conduct short conversations, either one-to-one or one-to-many, use voice-over-IP (VoIP) badges instead of wireless IP phones. These users include radiology staff, the lead staff member of each modality, pathologists, and registration staff for the Emergency Department. "Previously, when a patient needed an X-ray we would have to page the radiology transport staff, who left what they were doing to find a phone and call back," explains Hargrave. "Now caregivers can make one call to reach the entire transport staff at the same time, and the one who is closest and available can respond to the need. Wireless VoIP helps us improve patient satisfaction by providing transport more quickly."

Online Permit Processes: City of Cleveland

Perhaps you are lucky enough to live in a "connected community," where government takes advantage of advanced network technologies to increase service effectiveness, improve public safety, fuel economic development, and improve educational excellence. One such place is Cleveland, Ohio, where the city government forged a novel partnership with Case Western University to deploy a citywide wireless infrastructure. The same Cisco wireless infrastructure that professors and students use for research and communication also supports OneCleveland, a nonprofit group of community organizations that provides community-based broadband networking services. Its users include educational, governmental, research, arts, cultural, and healthcare organizations in greater Cleveland. Subscribing organizations connect their networks to the OneCleveland network via Cisco coarse wavelength-division multiplexing devices.

Among several applications, the City of Cleveland uses the OneCleveland WLAN to create, issue, and track permits. City inspectors no longer need to spend time driving to the office to file paperwork. Instead, they drive up to one of the conveniently located Wi-Fi hotspots throughout the city and use their laptops to upload completed permit and inspection forms, reschedule inspections, and download new assignments. The city has improved its service effectiveness without increasing headcount because inspectors can spend more time productively in the field.

Stimulating Economic Development: Fredericton, Canada

The City of Fredericton, the capital of the province of New Brunswick, Canada, has parlayed its Cisco WLAN into a competitive advantage for attracting technology companies, a primary contributor to economic growth. "We want to give our business community and professionals the best possible tools and promote Fredericton as an innovative, business-friendly city," explains Maurice Gallant, chief information officer for the city.

After building a fiber-optic network in 2000, Fredericton built a not-for-profit, community-wide, high-speed IEEE 802.11g Wi-Fi network in 2003 to offer residents and businesses free or steeply discounted Internet access. The result of this effort, "Fred-eZone," comprises more than 200 Cisco Aironet Series access points that form a single, near-contiguous hotspot covering almost half the city. Institution, government, and business customers contract for certain amounts of network bandwidth. Because these users seldom consume their maximum allotment, the City of Fredericton's IT group makes the unused surplus available to the public Wi-Fi network.

Fredericton's IT staff is testing VoIP services over the wireless network using Cisco CallManager voice management software, so that mobile city workers will be able to make calls using special IP-enabled PDAs anywhere within the city's hotspot range. Fredericton hopes to see net savings of up to CA\$80,000 per year on telephone, cell phone, and land mobile radio (LMR) transmission expenses. "As a municipality, we already provide infrastructure such as roads, sidewalks, and water distribution systems. We're just adding connectivity to the list," says Don Fitzgerald, executive director of Fredericton's economic development department.

Desktop Offices in the Field: Renton Police Department

For Renton, Washington, a citywide IP standards-based wireless network improves situational awareness for police officers and enables them to spend more time on patrol. The impetus for the WLAN arrived when the agency deployed an advanced record management system at a cost of more than US\$1 million. Unfortunately, the department's radio network was too slow for downloading information such as mug shots and outstanding warrants. Lack of access to this information compromised the safety of officers, who had no way of knowing that a suspect they pulled over for a traffic violation had a history of violence, for example. What's more, officers had to return to the station daily to submit reports, manage their e-mail, fill out timecards, and track down information—hours siphoned from their time on patrol.

THE TECHNOLOGY BEHIND FREDERICTON'S FRED-eZONE

The City of Fredericton's wireless infrastructure spans almost 30 square kilometers (11.5 square miles). And yet the city's IT department can manage it with existing staff levels thanks to the remote management and monitoring capabilities of the Cisco Wireless LAN Solution Engine (WLSE).

Cisco Aironet autonomous access points at the network edge are aggregated on assigned virtual LANs (VLANs) using Cisco Catalyst 2940 switches that connect back to a Layer 3 Cisco Catalyst 3750 Switch, the community network core router. Ultimately, all traffic destined for the Internet is routed through a Cisco 2821 Integrated Services Router that functions as the network Internet gateway.

THE TECHNOLOGY BEHIND THE CITY OF RENTON WLAN



The City of Renton's IT staff installed 32 outdoor access points and 32 indoor access points in and on city buildings and water towers. A Cisco Catalyst 6500 Series Switch manages multiple wired and wireless devices such as laptops, handsets, PDAs, printers, and Web cameras. A bidirectional 1-watt amplifier boosts PDA and laptop antenna signal strength. With full repeater capability, first responders can work online away from their vehicles at distances up to 100 yards outdoors in line of sight, depending on topology, or up to 200 feet inside buildings.

In addition, citizens and businesses can take advantage of the wireless network for Internet connectivity. To shield police and other sensitive communications from the public, the City of Renton IT group uses the multiple VLAN and Service Set Identifier (SSID) features of the Cisco WLAN infrastructure.

To make the case for a Cisco wireless infrastructure to the Renton City Council, Police Chief Garry Anderson and the IT staff staged a live demonstration comparing the time required to download a mug shot using an IEEE 802.11b wireless device and an 800-MHz radio device. The 800-MHz radio device took several minutes, including four or five attempts and repeated timeouts. The wireless device took five seconds in its first attempt.

The City Council heeded the point, and today 30 City of Renton police vehicles function as "roving wireless networks," equipped with mobile access radios. The WLAN is anchored by a Cisco Aironet 1300 Series Access Point/Bridge that supports 54 Mbit/s bandwidth. Safety and productivity applications include online access to mug shots, warrants, stolen property reports; crime bulletins, incident logs, which replace handwritten reports; access to US Federal Bureau of Investigation (FBI) and Washington State Patrol resources; and online timecard reporting. Soon after deployment, a Renton police officer tracked down and arrested a suspect after downloading a mug shot from the police records management system from his squad car and then linking to a public Internet site to find the suspect's address using a phone number.

Says Ron Hansen, network systems supervisor for the City of Renton, "Every day we find that people are discovering new ways to use our system that we never thought of, and that's very satisfying." ■

FURTHER READING

- Cisco Unified Wireless Network Overview
cisco.com/packet/174_6d1
- Wireless/Mobility Solutions for Large Enterprises
cisco.com/packet/174_6d2

Application Networking

Integrating applications and optimizing their performance will increasingly become the network's job.

SPECIAL REPORT

By Janet Kreiling



As their applications proliferate, enterprises wrestle with the growing level of complexity in their application infrastructures and the corresponding lack of IT control. Because the applications they've accumulated were never designed to actively communicate with each other, application integration (the ability to make independently designed application systems work together) presents a formidable challenge. Meanwhile, the business success of these organizations increasingly depends not only on their ability to use the applications cooperatively to meet common goals but also to sharpen their competitive edge.

Research firm Gartner estimates that a typical Global 2000 organization has 100 or more applications and spends 30 to 40 percent of its IT budget on application integration and related resources. No doubt, enterprises need applications. And more than ever before, these same organizations that are becoming more globalized and geographically distributed need to get these applications into the hands of their users. And they need efficiency in integrating applications across their organizations—efficiency that simply can no longer be achieved with their traditional application infrastructures.

So, here is something to think about: Instead of bringing in heavy-duty application integration programmers, adding more server blades, or heaping bandwidth on your WAN, let your network handle the application networking functions such as application delivery,

acceleration, and security. Your existing network already provides essential packet-based network services such as quality of service (QoS), perimeter and session-level security, IP Security (IPSec) encryption, and high-throughput routing and switching fabrics. A network equipped with the proper technology and products for application integration and delivery will significantly extend the network to create a pervasive fabric for collaboration between applications, to optimize the performance of those applications and maximize use of the infrastructure for application delivery.

To this end, Cisco has developed application networking strategies for both the data center and the branch office, bringing together the concepts of application delivery and application integration and allowing deployment on routers and switches or other network appliances.

Together, these application networking components optimize the performance of applications stored in the data center and used by branches and remote users; place intelligence in routers that give them the ability to "make business decisions" right at the network edge; reduce application bandwidth usage and roundtrips over the WAN; offload server infrastructure to enable faster response time from servers; perform other tasks that make business processes more productive and cost effective.

Cisco's application networking system is ready to work with enterprise software applications from many vendors, including IBM, Oracle, PeopleSoft, SAP, and Siebel, among others.

Application Networking in the Data Center

One reason application networking is so attractive is that it supports a sweeping trend in enterprise data operations: the bringing together of most or all corporate databases and applications into one data center, rather than having them dispersed in siloed centers. Organizations are consolidating their data operations in one place to combine databases and give employees easier access to all company data and applications. If a financial institution puts its

customer relationship management (CRM), transaction processing, and marketing systems into one place, for example, tasks such as identifying the 10 or 20 percent of customers who will be most profitable become much simpler, and employees in all locations can access all systems and data.

"The biggest issue we're seeing from our customers is application response time, especially for the large global, extended enterprise," says Janey Hoe, director of marketing in Cisco's Application Delivery Business Unit. "As they expand their operations globally, latency between the data center and an application user located halfway around the world significantly diminishes the performance of an application."

Compression alone does not solve this latency problem. Cisco's application networking strategy, Hoe says, "uses a combination of techniques for accelerating the response time of applications and optimizing their performance by better utilizing the server, minimizing the amount of data and roundtrips that must traverse the WAN, and improving the flow of content in the data center and out to the branch and remote users."

Chief among the application networking products in the data center:

- The new Cisco AVS 3100 Series Application Velocity System optimizes application performance
- The Cisco Content Services Switch (CSS) and Content Switching Module (CSM) for the Catalyst 6500 balance Web-based requests across servers or systems such as the AVS
- The Cisco Catalyst 6500 Series Application-Oriented Networking (AON) Module integrates applications and forwards messages among them
- The Cisco Catalyst 6500 Series Switch, an integrated services platform for high-performance service blades such as the Firewall Services Module in addition to the CSM, SSLM, and AON modules, among others

Cisco AVS: Speeding Up Performance

Based in part on technology developed by Fine-Ground Networks, Inc., which was acquired by Cisco in June 2005, the Cisco AVS minimizes the bandwidth usage and number of requests to an application from a user and responses from it, alleviating traffic on the WAN and thus response times. As Nat Kausik, director of engineering in Cisco's Application Delivery Business Unit, explains, "We based our design

goal on the premise that every page view should require only one network roundtrip between the user and the application."

Take the example of a user requesting a single page, say a customer record, from an application. He or she sends a brief request via the browser. But transmitting the page back in its entirety creates one or more lengthy messages and often as many as 100 separate request/response streams to render the full Web page. Here's where the Cisco AVS does its magic.

"Given that the user has previously requested that record page, as is almost always the case, the template, page layout, and other encapsulation factors remain the same. Only the customer data change," says Kausik. "The AVS subtracts the old page from the new one and transmits only the changes. This patented technique is called delta, or differential, encoding. If the whole page normally takes 50 kilobytes to send, and the changes only two, delta encoding has created an improvement of 96 percent."

In addition, the Cisco AVS uses byte compression, which "further reduces the number of bytes sent by half, perhaps down to an amount that can fit into one packet," adds Kausik. "Then, through dynamic HTML or Javascript, the browser is instructed to take the previous copy of the screen, make the changes, and display the new one. That's one type of optimization."

The other type, called flash forwarding, suppresses the embedded object requests that follow on from the initial user query. "When the application gets the request, it usually gives the browser a 'container page' with perhaps 20 embedded objects that refer to other locations in the application or a corporate database," explains Kausik. "When the browser gets a container page, it understands that it must fetch all 20 objects to deliver a meaningful screen of data, so the user's one request has spawned 20 more. But the user doesn't need to have all these objects retrieved again; he or she already has the basic page. With each request creating one network exchange and one network latency, the composite latency can delay the response to the user and cut down on application performance within the data center. AVS steps in and suppresses the requests for embedded objects so there is only one network transmission—the reply to the user."

In addition, the Cisco AVS can aggregate requests by the individual user, further cutting down on network roundtrips. And, Kausik notes, it can be used with practically any Web-based application. Cisco has

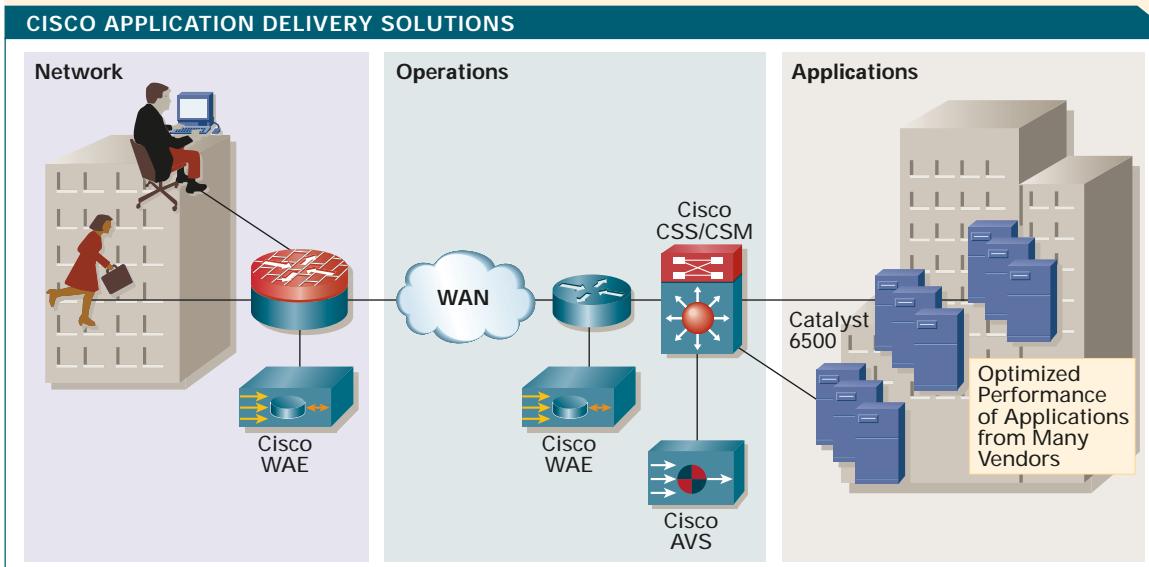


FIGURE 1 The Cisco WAE in the branch office and its counterpart in the data center, along with the Cisco AVS and CSS or CSM, all work together to optimize the performance of applications from many vendors.

templates for many standard applications, and a developer's kit enables enterprises to build custom templates as well.

The Cisco AVS also contains a firewall that provides security for SSL-encrypted packets typical in enterprise applications, which are not read by standard firewalls. Additionally, it monitors performance of an application for an individual user: how much time for the server to respond, how much time on the network, and how much time for the browser to render the page on the user's PC. "This enables network personnel to know even if an individual PC is slowing down, perhaps because it's been infected with spyware," says Kausik.

Cisco CSS and CSM: Enterprise-Class Load Balancing

The Cisco AVS can be scaled by grouping as many as needed for a given application, their activities coordinated by a Cisco CSS 11500 Series or the Cisco CSM for the Cisco Catalyst 6500 Series Switch or Cisco 7600 Series Router. "The CSS and the CSM both understand Web requests. So, if you need two or 200 servers to handle your application, they can spread requests across the servers so no one of them gets overloaded," Kausik points out.

The CSS and CSM perform load balancing by examining the contents of messages so as to forward them to specific machines according to policies that meet the needs of the application or device. For example, they can combine policies for load balancing, persistence (requests are directed to the same server until a session is finished), server failure (what to do if the server fails in mid-transaction), content (a server

farm might be divided into static and dynamic sections), and specific devices (requests from wireless devices might go to a certain set of servers). A policy might state that persistence is most important, even if a request is slowed down waiting for its particular server; another might provide that in case of server failure in mid-session, a certain number of milliseconds may elapse before looking for another server in hopes of saving persistence.

The Cisco CSS and CSM can offload SSL operations, which draw on CPU capacity intensively, from servers, freeing them to focus on applications processing. These products also perform health checks, to ensure that messages are actually being delivered to the correct servers.

The Cisco CSS can achieve a throughput of up to 6 Gbit/s with help from configurable modules; the CSM offers 4 Gbit/s of throughput in a single module, and multiple modules can be configured in a single Catalyst 6500 chassis to scale the performance further. Installed in a Catalyst 6500 Series Switch, the CSM interoperates with Cisco IOS Software features in the switch, including industry-leading Layer 2 through Layer 3 capabilities, integrated firewall, intrusion detection, and VPN.

Cisco Catalyst 6500 Series switches are also crucial components of the data center, as they host modules containing several data center products and coordinate their work with network functions such as QoS and security.

Cisco AON Module: Integrating Applications

The AON module acts as a “universal translator” for all types of enterprise applications. The module’s basic task in the data center is to translate the protocol or language of one application into the protocol or language spoken by virtually any other application. AON speaks many protocols and languages, including HTTP, HTTPS, Websphere Java Messaging Service, SSL, Public Key Cryptography Standards (PKCS), Triple Data Encryption Standard (3DES), Java Database Connectivity, Oracle 9I, Lightweight Directory Access Protocol (LDAP), XML, Simple Object Access Protocol (SOAP), Financial Information Exchange (FIX), and many others. It can also apply policies and priorities to messages.

AON uses innovative technology to read application-to-application messages flowing through the network such as purchase orders, investment transactions, or shipment approvals, translates them, for example, from SSL to PKCS or from XML to FIX and LDAP, and then routes the translations to the one or more applications that need them.

This ability to link applications has become crucial in environments where any single enterprise application touches many others. As Peter Linkin, manager of product marketing in the AON Business Unit at Cisco, explains, “When you purchase a book online, for instance, hitting the ‘Buy’ button sets off a number of backend processes. The transaction goes through SSL to the data center, and into ERP, financial, warehouse management, and other applications, all as you are getting instant confirmation of your purchase. The AON system can read a purchase order from SAP and send it to an Oracle database. It simplifies mundane but vital jobs such as shipping the product and getting paid.”

Application Networking at the Edge

The primary application networking task at the network edge is improving performance—cutting the time between user request and application response. According to Baruch Deutsch, director of product marketing in the Application Delivery Business Unit at Cisco, “With the HTTP Web protocol, or even the more verbose CIFS protocol for file access, one page or file from an application might use from several kilobytes to one or more megabytes. We put a tracer on the requests and responses involved in sending a

Thwarting Application Abuse

Network- and Internet-based applications are transforming business models and opening them up to outsourcing, offshoring, and other practices that require communications links around a region, country, or the world. Moreover, enterprises are expanding their use of advanced technologies such as IP-based wireless and voice over IP. Overall, these conditions create a multitude of interesting opportunities to misuse, misappropriate, or just plain steal data.

Part of the problem, according to Dave Zwickl, security technology manager in the Products and Technology Marketing Group at Cisco, is that mission-critical data that used to remain in relative safety behind

corporate firewalls is now quite available practically anywhere. Techniques such as port-hopping permit malefactors to scan for open ports in a firewall intelligently, finding perhaps the one for Internet browsing; then they might tunnel through to gain unfettered access to corporate data. “These intrusions occur at the application level, and lower levels of security can’t detect them,” Zwickl says. “Of course, there are also threats from the inside—employees who negligently or intentionally open holes in the network.”

Traditional protections—firewalls, antivirus software, and intrusion detection—no longer provide adequate protection. What’s needed is a network-wide, end-to-end approach that involves all layers and all components of the network and the applications

that run on it; Zwickl points out that the Cisco Self-Defending Network was designed to provide just such a comprehensive approach to application security.

Application delivery and network products in the data center, such as AVS, provide integrated application-level inspection and security to quickly identify and prevent application-layer threats and data theft. These products work in conjunction with other Cisco Self-Defending Network solutions to provide an end-to-end approach to application security.

To learn more about Cisco Self-Defending Network application abuse prevention solutions, see cisco.com/go/appabuse.

1-MB Word file across a WAN, and measured over 1,400 messages between the server and the user. Multiply that by a network latency from 20 to 200 ms and you get a significant delay."

Enterprise applications aren't the only bandwidth hogs. Streaming media rich in content—video, audio, animation, voiceover—are often sent to remote locations where the WAN links are thin, as are software and patches to be installed on local PCs.

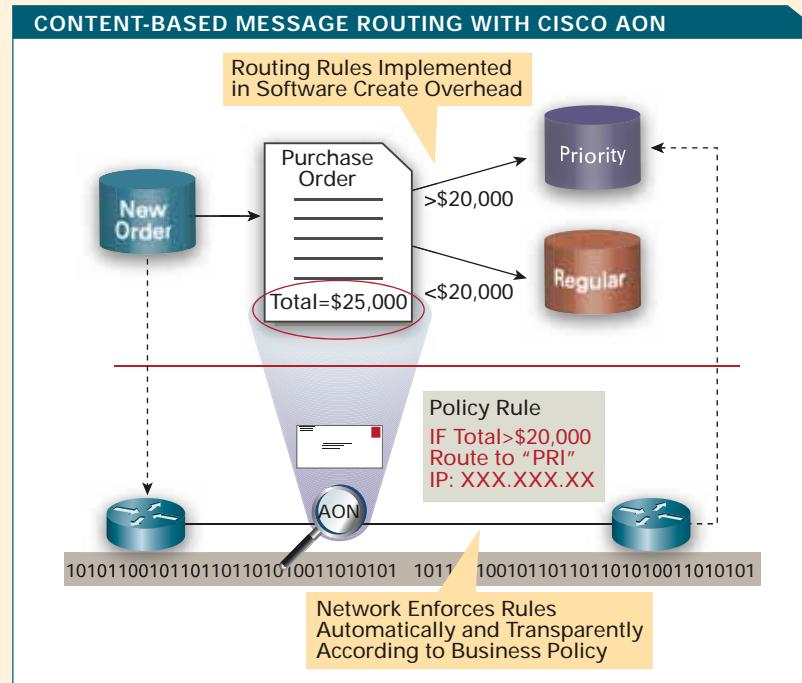
Chief among the application networking products in the branch:

- The new Cisco WAE-511 and WAE-611 Wide-Area Application Engine (WAE), which cache application data locally
- The Cisco 2600, 2800, 3700, and 3800 series Integrated Services Router AON modules, which work with the central AON system to filter and aggregate information before it goes to the data center and also can be programmed to make decisions

The Cisco WAE-511 and WAE-611 can run either Cisco Application and Content Networking System (ACNS) or Wide Area File Services (WAFS) software. ACNS and WAFS software enable remote users to use an application more efficiently by locally storing stable content that is frequently used but infrequently changed, and by minimizing the amount of information that must traverse the WAN. "We've found that well over 90 percent of requests can be handled locally," says Deutsch.

ACNS was designed for Web and video services such as enterprise applications, POS video displays, e-learning applications, virus scanning, and content filtering. The software works with HTTP and Real-Time Streaming Protocol (RTSP) and their variants. WAFS was designed for file and print services such as file access and distribution, and works with standard-file system protocols Common Internet File System (CIFS) with Windows and Network File System (NFS) with UNIX. Both ACNS and WAFS contain adapters that help their respective protocols minimize bandwidth usage.

In addition to caching stable content, the Cisco WAE can ensure that messages traversing the WAN are as small as possible. It compresses data for transport, pipelines multiple messages together, and performs content filtering such as virus scanning and authentication, authorization, and accounting (AAA). One



model, the Cisco WAE-7326, is installed in the data center to decode compressed or pipelined messages and provide an interface to the centralized storage.

The Cisco WAE-511 and WAE-611 complement the Cisco AVS, notes Deutsch. "They come into play lower in the protocol stack, dealing with transport protocols, whereas the Cisco AVS deals with protocols used by specific applications and, more importantly, can deal with dynamic data." The Cisco AVS works to expedite request handling and minimize network latency within the data center. Much of what it transmits can then be cached in the Cisco WAE to further minimize messages from the branch to the data center. In internal testing on a specific internal portal application, the Cisco AVS cut the response time to users by more than 50 percent, and Cisco WAE reduced that even further by as much as 90 percent.

Deutsch also points out the importance of the Cisco Integrated Services Router in enhancing application performance. "The two systems cooperate with regard to policies and security, for example," he says. "In addition, the router can be configured to send certain messages to the WAE, and ensure that the cache receives only the data it should have."

FIGURE 2 In the data center, Cisco AON technology translates the various languages and protocols used by most major enterprise applications. It also interprets content so that it can receive a purchase order from one application and route it according to policies to one or more others.

The Cisco AON module in the branch puts intelligent decision-making at the network edge. It can intercept and analyze traffic in various message formats and protocols and bridge between them, provide security, and validate messages, creating a transparent interface between trading partners and, in effect, a good business-to-business gateway. It can manage remote devices that send messages to the Cisco Integrated Services Router in the branch. It can also filter messages from multiple sources that come into the branch router for duplicates or by other criteria, aggregate them, make decisions according to instructions, and transmit selected messages to a sister AON module deployed in the data center.

It All Comes Back to the Network

With its increasingly strong security safeguards, high availability, speed, pervasiveness, and scalability, the network provides a logical placement for certain application, message, and integration functions.

Application networking combines all the traditional benefits of the network—QoS, prioritization, routing, security, AAA, etc.—with application load balancing, server offloading, bandwidth and latency management, and application layer security. The result? Application integration and delivery at the business transaction and application-to-application message transaction levels. And this is just what enterprises need to handle application proliferation efficiently and competitively across their organizations. ■

FURTHER READING

- Cisco Application-Oriented Networking
cisco.com/go/aon

Wide-Area WLANs

Mesh network architecture enables wireless LANs to move beyond offices, homes, and public hotspots.

By Gene Knauer

The popularity of Wi-Fi technology and explosive growth of Wi-Fi clients is inspiring US cities to explore providing truly ubiquitous outdoor wireless access to citizens and municipal employees when they venture beyond wired and conventional wireless LAN (WLAN) networks.

With the continuing improvements and extensions to the Wi-Fi standard and the development of wireless routing technology, the cost of provisioning and providing unlicensed Wi-Fi access over large outdoor areas has become feasible. The cost of providing a wired connection to each individual Wi-Fi hotspot is prohibitively expensive when deploying a high density of outdoor access points.

Enter the mesh wireless network architecture. In a mesh network, wireless access points discover each other and interconnect automatically (see Figure 1, page 50). Together they select the optimal route to the connected network within the mesh of access points. This architecture provides resiliency to interference and helps ensure high network capacity.

With the introduction of the Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Point, which complements the unified wireless network products, Cisco is among the first companies to offer an end-to-end outdoor and indoor Wi-Fi access solution. Two separate radios in the outdoor Aironet 1500 Series Access Point provide 2.4-GHz 802.11b/g network access and 5-GHz 802.11a backhaul. Based on the Lightweight Access Point Protocol (LWAPP), the Cisco Aironet 1500 Series operates over Layer 2 or Layer 3, extending the same Cisco WLAN architecture that is popular indoors to the outdoors, and bringing seamless integration and roaming to Wi-Fi devices. The solution supports IEEE 802.11a and 802.11b/g, and with a software upgrade supports the 4.9-GHz public safety band, so different types of users can use the same WLAN for many different purposes.

Coverage, Cost, and Management Efficiencies

"In a mesh network, you don't need a directly connected network presence everywhere; each access point is just responsible for communicating with the



Thomas Oliver

WIRELESS OUTDOORS Cisco 1500 Series access points are mounted on street lights or traffic signal poles and connected to their power sources.

next closest hop," says Fred Archibald, network manager at the University of California at Berkeley Department of Electrical Engineering and Computer Sciences. Archibald was the first customer to test the Cisco "thin access point" mesh solution in his department, which extends coverage to 20 percent of the UC Berkeley campus.

"We think this is a much more feasible way of delivering networking over a large area. Once you install the access points, you don't have to touch them. You can make changes centrally and push them out to the access points through the controller," says Archibald.

An intelligent wireless routing algorithm based on the Cisco patent-pending Adaptive Wireless Path Protocol (AWPP) enables each Cisco 1500 Series Access Point to collectively form a dynamic mesh network with the other access points in the WLAN. This intelligence enables an access point that encounters environmental interference to switch access communications to an alternate channel, dynamically optimize traffic routes

Continued on page 50

Wireless Mesh, Continued from page 47

as traffic levels change, and self-heal from an outage. The availability of AWPP, combined with the availability of 80 to 500 MHz of unlicensed bandwidth around most of the world is enabling the deployment of outdoor broadband wireless access worldwide.

The Cisco outdoor wireless mesh architecture uses Cisco WLAN controllers, which come embedded with Radio Resource Management (RRM) algorithms to detect and adapt to changes in the air space in real time, creating a self-configuring, self-optimizing, self-correcting WLAN environment. Cisco Wireless Control System (WCS) software provides a common network management platform to manage both the indoor and outdoor Wi-Fi network.

The WCS network management system provides an easy-to-use graphical interface that lets a network administrator configure and reconfigure access points and push out security policies and radio frequency parameters. A dashboard shows what is happening on the WLAN, from traffic statistics to information about individual clients accessing services.

Cities Go Wireless

Another early adopter of mesh outdoor WLANs is the city of Dayton, Ohio. Beginning in December 2004, local Internet service provider (ISP) HarborLink LLC and the city decided to begin testing an outdoor WLAN based on the forerunner of the Cisco 1500 Series technology.

"We installed about 20 access points on street lights, traffic signals, a cell tower, and buildings within a few square miles," says HarborLink president Rick Tangeman. HarborLink had already installed hotspots for several Dayton restaurants and proposed the same model to the city, owning and operating the network in exchange for making the service available to the public and city agencies. "Once we saw that the cost of entry with mesh WLAN technology could be relatively low and that such a network could be reliable, didn't require a lot of maintenance, and could be centrally managed, we were able to convince the city to test it," says Tangeman.

The Cisco 1500 Series access points are mounted on street lights or traffic signal poles and connected to their power sources (see photo, page 47). Some access points are directly connected to the network by an Ethernet cable, and these are typically installed on rooftops and use a power injector to provide Power over Ethernet (PoE).

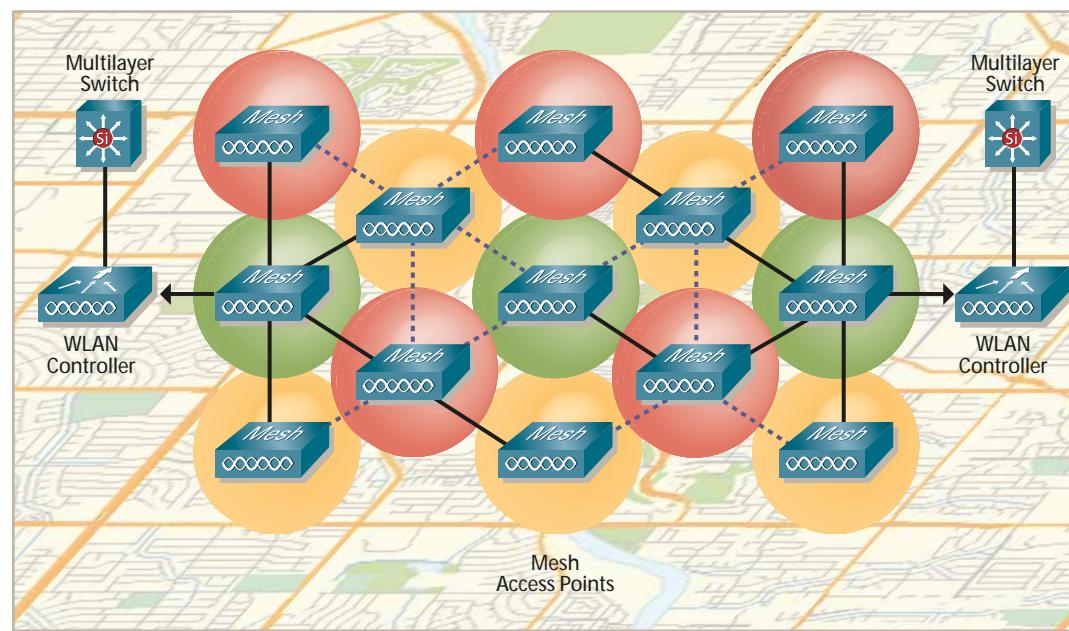
Talk About It

Want to share your expertise on wireless LANs with your peers? Get answers to your questions from Cisco experts? Join a Networking Professionals Connection discussion at cisco.com/discuss/wlangeneral.

MESH ARCHITECTURE

Cisco Aironet 1500 Series access points form a mesh using the Cisco Adaptive Wireless Path Protocol, with centralized management by Cisco wireless LAN controllers.

WIRELESS MESH NETWORKING



The city of Lebanon in Oregon's Willamette Valley, was also attracted to the features of the Cisco Wireless Mesh Networking solution. Lebanon was considering a mobile network for police and public works when a local ISP approached them about providing an outdoor WLAN for both city employees and the general public.

"We stumbled across the wireless mesh technology for indoor WLANs in a trade magazine and wanted to find out if it could be used outdoors," recalls Dusston Denver, general manager of Oregon ISP and systems integrator for Valnet & Design Systems. "We were interested in the self-healing features because when you're on a public frequency in a city, interference from cell phones, video cameras, buildings, and other obstacles can cause dropped or impaired signals. The indoor WLAN turned out to be just what we were looking for in an outdoor solution."

Valnet deployed four access points in April 2005, and 22 were in place by July, covering 40 percent of Lebanon's 10-square-mile metropolitan area, with access speeds of between 256 Kbit/s and 1.5 Mbit/s, depending upon a client's distance from an access point. Without officially announcing the network, Lebanon had an average of 50 regular users by the end of the summer. Half of these users exceeded the 10 free hours a month that Valnet offers and were paying for the service.

"We expect that when we're fully deployed, we'll have 50 to 60 access points and 200 to 300 paying subscribers," says Denver.

The city of Dayton wireless network is free for unlimited use, which is partly underwritten by the *Dayton Daily News*, whose splash page appears when users first log on and includes local news and advertising. Rick Tangeman of HarborLink anticipates eventually collapsing other municipal networks into the WLAN for greater cost efficiency for the city and added revenue for HarborLink. The public access to the network would be carefully partitioned, maintaining privacy and security for city and public users.

Cisco Outdoor WLAN Differentiators

There are different architectures for wireless mesh solutions and some confusion about how many radios are necessary in each access point. Some access points contain a single radio for backhaul and access. Others provide multiple backhaul radios. In a mesh network, Cisco has determined that for greater scalability and stability two radios are optimal, one for backhaul and one for access.

The Cisco Wireless Mesh Networking solution also owes its efficiency to intelligent wireless routing features based on the Cisco Adaptive Wireless Path Protocol, which is an extension of Cisco LWAPP used in indoor enterprise WLANs. These features include the ability of each access point to find the fastest and most efficient path back to the wireless gateway, location-based services, and intrusion detection capabilities.

Promising Signals from Early Adopters

The first wave of customers using the Cisco Wireless Mesh Networking Solution has been very pleased with the results.

"I think this is a feasible way to deliver networking over a large area," says UC Berkeley's Archibald.

Students seem equally pleased by the outdoor WLAN, content to sit on campus lawns and in plazas, even squinting in the sun to access services on their laptops. Berkeley has successfully tested soft phone applications such as Skype and Archibald intends to see what quality of service parameters will be necessary in the outdoor WLAN to support video.

Municipal WLANs

Large and small cities across the US are now considering the feasibility of offering outdoor municipal WLANs to support mobile employees including police, fire fighters, public works, and parks and recreation departments. Hospitals, schools, hotels, and many other organizations see the benefits in expanding Internet access beyond hot spots, to enable employees, students, customers, and visitors to remain connected to network services.

This year, the US Congress introduced legislation to allow municipalities to offer high-speed Internet access. Senator John McCain, a co-sponsor of the bill, noted that the US has dropped from tenth in the world for high-speed Internet penetration in 2004 to 16th in 2005. Regulatory and competitive hurdles with incumbent carriers are now being sorted out, but with mesh WLAN architectures and products and technologies from Cisco, the solutions are here. ■

FURTHER READING

- Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Point
cisco.com/packet/174_7b1
- Cisco Wireless Products
cisco.com/packet/174_7b2
- Understanding the Lightweight Access Point Protocol
cisco.com/packet/173_7b3

The Changing Network Perimeter

Cisco NAC2 helps combat proliferating edge devices.

By David Barry

Despite years of security technology development and millions of dollars spent on deployment, viruses, worms, spyware, and other forms of malware remain the number one issue facing organizations today, according to the 2005 CSI/FBI Security Report published by the Computer Security Institute and the US Federal Bureau of Investigation (FBI).

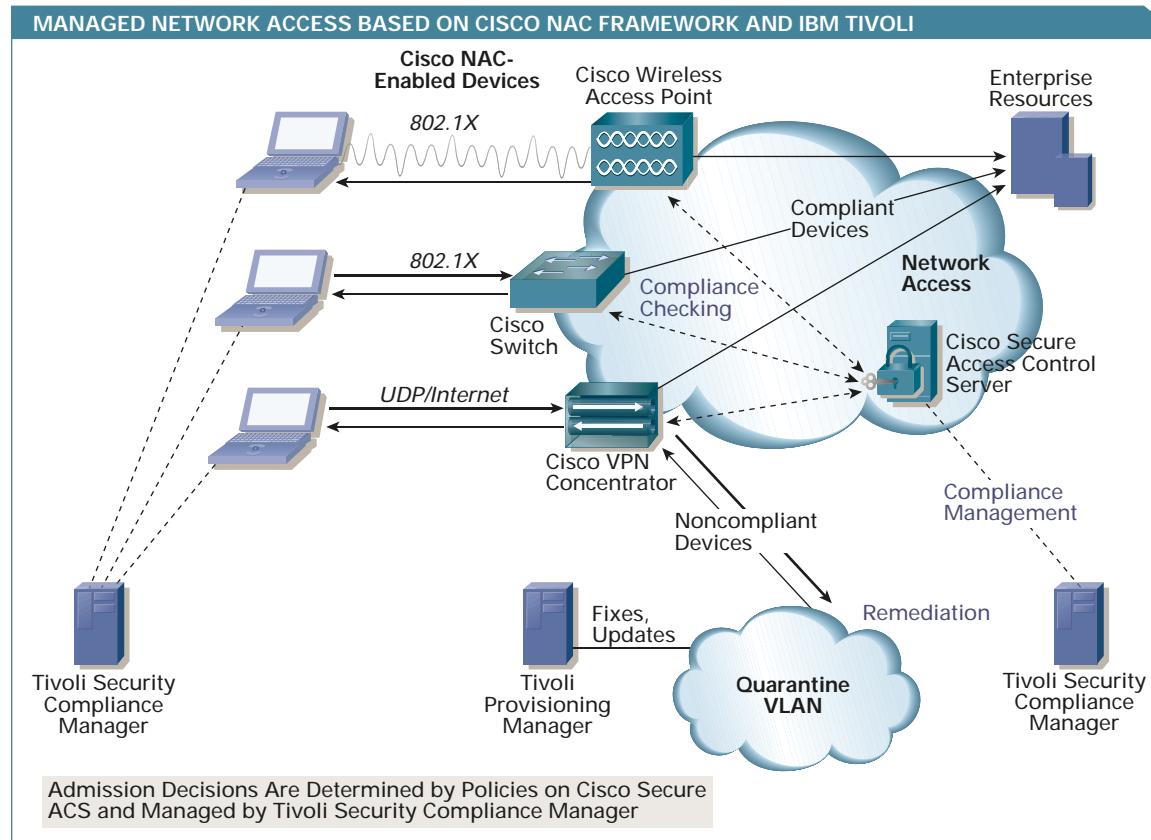
Online viruses and worms have evolved in their intelligence and are now able to proliferate by mutating around blocks, making attacks increasingly dangerous. Of equal concern is the changing nature of the network and, in particular, the location of the perimeter or edge—the place where it was once believed the virus or worm could be stopped.

"The concept of the perimeter is disappearing," says Bob Glechauf, chief technology officer in the Security Technology Group at Cisco. "It's now all about edges. Companies no longer have purely private

networks; all are shades of private and public networks—except perhaps a military network. Clients are edges, whether it's a Bluetooth phone, a PC remotely connecting to the network, or a Windows laptop—they're passing packets. And this increasing number of edges presents myriad new ways for trouble to reach the network."

What's the Health of the Device?

While most organizations use identity management and authentication, authorization, and accounting (AAA) to authenticate users and authorize network privileges, they have had virtually no way to authenticate the security profile of a user's endpoint device. Without an accurate way to assess the "health" of a device, even the most trustworthy user can inadvertently expose everyone else on the network to significant risks posed by either an infected device, or by one that is not properly protected against infection.



"An employee could be at an airport hot spot or a local coffee shop and inadvertently download a virus while browsing the Internet," says Russell Rice, director of marketing in the Security Technology Group at Cisco. "Or an employee could mistakenly turn off a laptop's antivirus software and then bring that laptop into the enterprise. Companies need a way to check the security profiles of devices."

Cisco began to address these challenges two years ago with its Network Admission Control (NAC) initiative. NAC is a set of technologies and solutions that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. Customers implementing NAC can restrict network access to compliant and trusted endpoint devices (PCs, servers, and PDAs, for example) and can control the access of noncompliant or unmanaged devices.

Initially, NAC was only available on Cisco routers, including Cisco Integrated Services Routers, modular access routers, multiservice access routers, 7200 Series routers, and VPN concentrators. NAC, therefore, could be extended to remote branches or remote device access, but deployment on corporate LANs and wireless access points was limited.

Now Cisco's NAC2, adds Cisco Catalyst switches and wireless solutions, making NAC available on the enterprise LAN, where it is badly needed, according to Rice.

"When Cisco first introduced NAC, the main concept was how to reduce the risk of bringing viruses or worms into the network," says Rice. "That is still the major goal but NAC has now evolved. With NAC2, we're helping enterprises to answer the question 'As an enterprise, how do we ensure that we enforce and audit our corporate access and business policies by ensuring that only the right people and assets connect to our managed network, while reducing the risk that these assets might cause harm?'"

The NAC vendor program, an ecosystem of partners with more than 60 participants, now includes vendors with solutions for assessing unmanaged and agentless assets. This includes products from Altiris, Symantec, and Qualys. They join vendors already in the program, including leading antivirus, remediation, and client security providers such as Altiris, BigFix, Computer Associates, IBM, McAfee, and Trend Micro.

Cisco takes two approaches to the challenges of NAC: an appliance-based approach and one based

Continued on page 73

Metro Ethernet an Urban Amenity

Time Warner Telecom brings Metro Ethernet to more than 5,700 buildings in 44 major US markets—and business customers make the most of it.



Cisco Systems

By Janet Kreiling

At one time, San Francisco's Barbary Coast welcomed roustabouts and pirates. Today it courts more civilized inhabitants, including lawyers, financiers, architects, realtors, and other business tenants leasing space in the Embarcadero Center, a waterfront property consisting of five multistory towers. The property spans five blocks with more than 3.9 million square feet of office space, retail shops, restaurants, and other amenities.

Now, there's one more amenity at the Embarcadero Center: Metro Ethernet bandwidth and services provided by Time Warner Telecom, a Cisco Powered Network provider. Earlier this year, Time Warner Telecom finished extending its San Francisco fiber network to each of the five Embarcadero Center towers and is now delivering Metro Ethernet services to the business tenants.

"Telecommunications are important to prospective tenants," says Danny Murtagh, director of engineering at Boston Properties, LP, the Embarcadero Center's owner. "They are very interested in the bandwidth and service providers available. And they're now comfortable they can get fiber to their spaces."

Boston Properties, adds Murtagh, wanted to give its tenants an alternative to the incumbent. "We were looking for a stable, viable company that could offer packages from regular phone service all the way to high broadband."

Time Warner Telecom offers up to 1 Gbit/s to individual offices in the center. "We can deliver any combination of bandwidth and services a tenant wants—from voice over IP to 10 to 100 Mbit/s to 1 Gigabyte, and any combination of voice, video, and data."

Continued on page 57

Metro Ethernet, Continued from page 55

according to John Reese, vice president and general manager at Time Warner Telecom. "For instance, if a legal firm wants video to conduct depositions, we can supply the transport capacity."

The company is signing contracts with tenants as their existing contracts expire. Time Warner Telecom's nationwide network is one of the factors that weigh favorably in the tenants' decision-making. "We have over 20,000 route miles of fiber connecting 44 major markets in the US," says Reese. "One financial customer at Embarcadero, for example, has an extended Native LAN [Time Warner Telecom's name for its inter-city Metro Ethernet service] of 10-Mbit/s links from its San Francisco office to other locations in the Midwest. We give them LAN speeds throughout their network." Another tenant is using Native LAN (NLAN) connections of 40 Mbit/s.

"Our ultimate goal is linking businesses to businesses. A high-speed Native LAN helps companies open or expand operations in other parts of the country," Reese adds. "The Ethernet port is becoming ubiquitous. All business functions are migrating to the PC—applications, voice, video, data, graphics—and everything are converging. As this occurs, we're able to deliver the bandwidth and flexibility of service offerings that people need."

Of particular importance to Murtagh at Boston Properties is the amount and use of riser space throughout the Embarcadero Center. Helping to ease his concerns, when Time Warner Telecom readies a building for Metro Ethernet, it serves multiple tenants with narrow-diameter 24- to 72-fiber cables it installs in the building, instead of running one fat cable with fewer fibers for each new customer.

Metro Ethernet Services Coast to Coast

In addition to the Embarcadero Center, Time Warner Telecom currently delivers Metro Ethernet services directly to more than 5,700 properties across the US. The aforementioned 20,000-plus route miles Time Warner Telecom owns and operates add up to approximately 1 million fiber miles. Cisco optical networking solutions are a key component in those networks.

"We extend our networks when good opportunities are available to us," says Mike Rouleau, senior vice president of marketing and business development at Time Warner Telecom. "Call these success-based extensions—in each instance, we had customers asking us for service."

Time Warner Telecom has developed a very robust fiber facilities network over the years, according to

Rouleau. "Seventy percent of our revenue is due to carrying 100 percent of our traffic on our own network. Having our own facilities also makes us a lot more flexible than we could be if we depended on local-exchange carriers for some of our route miles. After the mergers of SBC/AT&T and Verizon/MCI, no other non-incumbent carrier has as many buildings directly connected to a fiber network than we do."

Since 1997, Rouleau says, "We've been focused on building a network, delivering solutions, and supporting those solutions with a good customer experience. I think that's played out well. We've also been able to diversify our revenue mix more. Just in the last two years, for example, the amount of revenue we derive from enterprises has grown from 46 percent to 55 percent."

In building out its network, the company has steadily added new Metro Ethernet services over the past two years. The first of these, all with speeds from 10 Mbit/s to 1 Gbit/s, were CD-NLAN, a customer-managed Native LAN; Switched NLAN, a Time Warner Telecom-managed service with switching capabilities; and SONET NLAN, a premium service for mission-critical communications.

These local Metro Ethernet services from Time Warner Telecom are based end to end on Cisco gear, including the Cisco ONS 15327 SONET Multiservice Provisioning Platform (MSPP), Cisco 7600 Series routers, and Cisco Catalyst 6500 and 3550 Series switches.

Time Warner Telecom's Metro Ethernet services are especially attractive to healthcare, financial, education, and government enterprises—"any company that needs to send a lot of data from one place to another," says Rouleau. "Ethernet is very efficient, more so than Frame Relay or ATM."

Metro Ethernet Services in Healthcare

Radiology Ltd., based in Tucson, Arizona, uses 100-Mbit/s links to connect its four locations across the city and to route X-rays, computerized axial tomography and positron emission tomography scans, and ultrasound and magnetic resonance imaging to area hospitals and consulting physicians. It even reaches doctors at home over T1 links.

In addition to helping Radiology Ltd. implement its network using fiber and T1 lines, Time Warner Telecom provides the company managed Internet and Native LAN services.

"The 100-Mbit/s pipes allowed us to cut the time to deliver imaging interpretations to physicians by 60 percent," according to Eric Nied, director of IT at Radiology Ltd. "Scalability was important," Nied adds,

"because we have a very low tolerance for data flow disruptions. Native LAN allows us to add bandwidth on the fly to meet growing demands, and because new radiological imaging instruments create much larger imaging data sets, we'll be able to deploy cutting-edge technology without fear of being limited by bandwidth considerations."

"Radiology Ltd. is a Cisco shop, and they're pleased that we have a Cisco Powered Network," Rouleau says. "We use the same basic platforms, so our network links easily into theirs."

With three data centers and three healthcare facilities in the Milwaukee, Wisconsin area, ProHealth Care recently contracted with Time Warner Telecom for 12 Gigabit Ethernet Native LAN circuits to link its facilities point to point. The company's staff needs to move radiology and cardiology images between sites, and the Gigabit Ethernet links deliver sub-millisecond performance.

Getting rid of noticeable latency was one of the company's goals. Another was eliminating ATM gear, says Bill Bailey, ProHealth Care's enterprise architect. "Most everyone on our staff has Ethernet protocol experience compared to a couple who understood ATM. That change alone has taken a large administrative burden off our shoulders," he says.

Metro Ethernet Services in City Government

Time Warner Telecom serves both the City of Boise and its school district with Metro Ethernet. City Hall is served by 10 Mbit/s for high-speed Internet access. The Boise school district is getting 20-Mbit/s, with plenty of room for higher speeds of more than 100 Mbit/s into the district's service center. The district's 52 schools tie into the service center over the district's own existing fiber network; overall, Internet access capacity among the school district is quadrupled.

"The City of Boise solution delivers significant cost savings, improves the city's network efficiency, and enables them to upgrade their WAN without investing in any new hardware," says Rouleau.

Metro Ethernet Services in Hospitality

Outback Steakhouse, Inc., based in Tampa, Florida, has also reported significant returns on the Metro Ethernet link between its corporate offices and its data center in Tampa. The company's substantial expansion—more than 1,000 restaurants across the US—necessitated a 100-Mbit/s link, and the prospects of future growth made scaling to 1 Gbit/s an attractive possibility.

Time Warner Telecom brought redundant fiber into Outback's headquarters and deployed a Cisco Catalyst

6509 Switch and a Catalyst 3550 Switch, which connect to a Cisco 7609 Router in Time Warner Telecom's central office via a SONET backbone and the 100-MB Native LAN service. This metro SONET backbone ensures high availability with 50-ms recovery times using redundant fiber paths and systems. This helps ensure near 100 percent availability for Outback's business-critical operations at headquarters and across the chain's locations.

The Cisco 7609 Router in Time Warner Telecom's central office delivers Outback operations data traffic to a Cisco ONS 15327 SONET MSPP, owned by Time Warner Telecom and collocated in a Qwest Cyber Center. Once the traffic enters the Cisco ONS 15327 in the Cyber Center, it must be converted to OC-3 (155 Mbit/s) to run over the Qwest infrastructure for long-distance transmission. Traffic is then reconverted at the destination city back to Ethernet for delivery over Time Warner Telecom's metro network via its Ethernet Native LAN service.

In addition to yielding Outback high availability chainwide, greater bandwidth, and the scalability needed during its period of fast growth, employees at each restaurant location now have access to timely data anytime, anywhere (something they didn't have previously).

Metro Ethernet a Cornerstone of IP NGN

These are just a few of the uses for Metro Ethernet that Time Warner Telecom's customers are benefiting from. They begin to demonstrate why Metro Ethernet is a key technology on which to build an IP next-generation network (IP NGN). The infrastructure supports very high bandwidth, scales easily, and accommodates the convergence of voice, video, data, wireless, and just about any other type of communication. It also supports a rich set of features that providers can use to create their signature services, as Time Warner Telecom has.

The future to be built on Metro Ethernet holds many opportunities for service providers and abundant efficiencies for end users—as those business tenants in San Francisco's Embarcadero Center are finding out. ■

FURTHER READING

- Cisco Metro Ethernet Solutions
cisco.com/go/metro
- Cisco Optical Networking Solutions
cisco.com/go/optical

Smart, Simple, and Secure

Cisco Business Communications Solution offers new products, support, and financing options tailored for SMBs.

By Joanna Holmes

It's time to even the playing field. For too long, tight budgets and limited staff—the hallmarks of the small and midsized business (SMB) sector—have placed sophisticated network technology out of reach. That limitation weakens SMBs' ability to compete with bigger companies (armed with larger IT budgets). Cisco has set out to balance this inequity with a raft of new products, services, and financing options that will allow SMBs to refocus their energies away from IT and on to more important things—like growth.

Although Cisco entered the SMB market in the early 1990s, this story really begins in April 2004, when Chief Executive Officer John Chambers announced a two-year, US\$2 billion investment and rollout of 30 new products for SMB customers. Pivotal to that commitment is a shift in Cisco's product development strategy. Rather than provide "pared down" versions of enterprise products, Cisco pledges to create SMB products from the ground up, factoring in the unique needs of smaller businesses.

Fast forward to September 2005, when Cisco announces the Cisco Business Communications Solution—a tailored family of products, services, support, and financing options. This smart, simple, and secure solution helps SMBs control costs, improve operations, and gain a sustainable competitive advantage.

"Since John Chambers' announcement in 2004, we've already delivered more than 40 new purpose-built products," says Julie O'Brien, senior manager of IP communications in Cisco's Product and Technology Marketing Organization. "The Cisco Business Communications Solution underscores our commitment to SMBs," she says. "For small and midsized businesses, this solution delivers a product portfolio that's tailored for their needs, but also the complete package they need for success. That includes financing programs, service and support, and the channel to help them with successful implementations."

Purpose-Built for SMBs

According to Don Proctor, senior vice president of Cisco's Voice Technology Group, "Many smaller companies that use Cisco products have provided feedback on how to improve our products to better meet their needs." Their message is clear, he says: They recognize the quality of Cisco technology, but they need products specifically crafted for their businesses. "One thing we often heard from smaller businesses is they just don't have the staff to set up a complete converged communications system, which encompasses a secure data network with voice communications."

In response, Cisco has created complete product packages that substantially ease deployment costs and complexities. These packages are



BANK ON WHEELS Peoples Federal Credit Union uses the Cisco Business Communications Solution within its unique mobile bank, which reaches underserved communities in West Virginia.

as close to off-the-shelf communications systems as you can get, says Proctor. "With this new suite of products and services we put the missing pieces in place, including financing and channel partner support, so both installation and management can be simple and fast."

New SMB-Tailored Products

A cornerstone of the Cisco Business Communications Solution is the new SMB-class Cisco Catalyst Express 500 Series switching family, which is designed specifically to help smaller businesses deploy converged networks. These wire-speed, Layer 2-managed Fast Ethernet and Gigabit Ethernet switches provide a security-enabled network foundation that is optimized for data, wireless, and voice. "The Catalyst Express is neither a scaled-down enterprise switch nor a rudimentary model that lacks advanced capabilities or scalability," says Maciej Kranz, senior director of marketing in the Desktop Switching Business Unit at Cisco. "This product offers the exact capabilities smaller businesses need to securely run voice, data, and video over their IP LANs."

Solutions for Small Businesses

The Cisco Business Communications Solution for companies with 20 to 250 employees is based on the Cisco Catalyst Express 500 Switch and the IP Communications Express Solution. The Catalyst Express 500 switches deliver smart, simple, secure Layer 2 switching capability that is optimized for data, wireless, and voice. The solution also features new versions of Cisco CallManager Express with "meet me" conferencing support and Cisco Unity Express with new Basic Automatic Call Distribution (ACD) integration and remote management support—all within the Cisco Integrated Services Router. Customers can use the Cisco Network Assistant 3.0

application to enable advanced technologies, such as wireless LANs, quality of service (QoS), and IP communications. Cisco Network Assistant replaces the traditional command-line interface (CLI) with an easy-to-use GUI and pulldown menu to make configurations simple and fast, even for those with minimal technical experience.

Together, these solutions deliver affordable, converged data and voice services. Available immediately, they are free upgrades for customers with Cisco SMARTnet support contracts. Complementing the products are the recently introduced Cisco SMB Support Assistant service offering and Cisco Capital financing programs tailored specifically for SMBs.

Products for the Midmarket

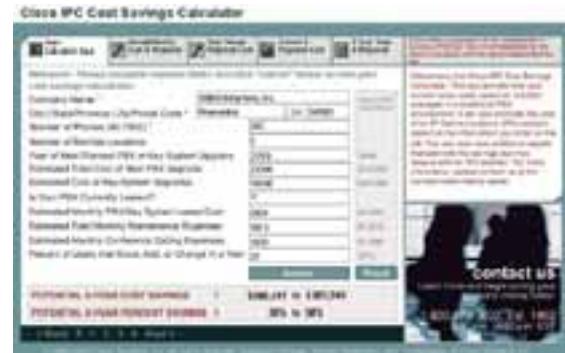
For companies with 250 to 1,000 employees, the Cisco Business Communications Solution is based on Cisco CallManager and features a host of new IP communications applications such as Cisco MeetingPlace Express, Cisco Unity Connection, Cisco IPCC Express, and Cisco Mobile Connect.

"We're introducing an enhanced voice-mail product, Unity Connection, for medium-sized businesses," says Proctor. "It incorporates speech recognition and several advanced features. We've also developed a midmarket conferencing and collaboration offering, Cisco MeetingPlace Express, which helps our smaller customers collaborate globally."

And for ease of configuration and management, Cisco is introducing the Cisco Voice Provisioning Tool, CiscoWorks IP Communications Operations Manager, and CiscoWorks IP Communications Service Monitor, which will dramatically reduce provisioning time while improving system monitoring.

For both small and midmarket users, Cisco has introduced new telephony endpoints, including the Cisco IP Phone 7941G, 7961G, and 7985G models. These phones provide a platform for innovative applications such as XML and video.

A new family of fixed-configuration switches has joined the Cisco midmarket switching portfolio. The Cisco Catalyst 2960 features embedded Cisco ASIC technology to offer advanced security, services and higher performance. These new switches provide desktop Fast



CALCULATE THE DIFFERENCE The IPC Cost-Savings Calculator tool enables organizations to estimate the costs and savings of Cisco IP communications solutions.

Ethernet and Gigabit Ethernet connectivity with integrated security, advanced QoS, and resilience.

Success Stories

For many businesses in the commercial sector, the Cisco Business Communications Solution provides the impetus to converge voice and data networks into a single infrastructure. Brian Sims, vice president and network engineer for Cisco channel partner Advanced Technical Solutions, LLC, recently completed several such projects. Among them is City National Bank of West Virginia, a midsized business with 72 branches in West Virginia, Kentucky, and Ohio. In the last two years City National has opened new branches while also growing through a series of multibranch acquisitions.

This bank has built its brand on personalized, responsive customer service, but its rapid expansion made maintaining that standard a genuine challenge. "City National was struggling with manageability and scalability," says Sims. "When they tied in all their new and acquired branches, they had a hodgepodge of systems and only one voice-capable engineer on staff."

Maintenance costs soared as City National found itself maintaining several network infrastructures, including outdated phone systems that could not be managed remotely. The bank's one telephony technician was spending countless hours traveling to each branch to perform what were often simple administrative network tasks.

To support its new branches and provide customers and staff with a full array of banking services, City National Bank sought a network solution that could accommodate both voice and data applications.

"The Cisco Business Communications Solution gave City National a single infrastructure that reduced their costs," says Sims. "With Cisco SMARTnet support, they have only one management cost on the equipment. And they have much greater flexibility now—they can remotely access their devices and generally support their users much better than they could previously."

Moreover, adds Sims, this solution tackled a common challenge—productivity. "As in many of these IP

Cisco SMB Select Partner Program

Resellers can learn more about the unique business and technology requirements of SMBs and the Cisco portfolio of marketing and sales resources at cisco.com/go/smbselect.

telephony deployments we're doing," he notes, "productivity has been crucial for City National." By streamlining network tasks, City National can reduce operational expenditures and increase its overall productivity.

Productivity has also been a key factor for LeTourneau University in Longview, Texas, another organization that recently deployed the Cisco Business Communications Solution to converge its voice and data networks. "The relative challenge between administering the [PBX] system and administering our new system is night and day," says Ken Johnson, the university's manager of network services.

LeTourneau had used a PBX-based phone system, which supported the university's 600 employees and its widely dispersed facilities, including six satellite locations. In setting out to upgrade its network, LeTourneau had three business goals: to reduce or eliminate copper cabling costs, replace its aging, inefficient phone system, and manage growth while expanding services—all within its existing IT budget.

The post-installation productivity gains Johnson's team saw were impressive. Cisco Network Assistant management software on Cisco Catalyst switches simplifies administration tasks for LeTourneau's local and remote switches, routers, and wireless access points. That means IT staff can support a fast-growing student population without increasing headcount, because everyone on staff can perform voice and data administration.

The Cisco CallManager system is another great time-saver for Johnson's team. "Moves, adds, and changes happen in minutes rather than hours, using the Cisco CallManager administrative interface," he says.

Productivity gains extended to LeTourneau staff and faculty. "Cisco IP phones give our users greater freedom of movement and help them be more productive," Johnson observes. The university faculty and staff members tell him they enjoy the ability to access both voicemail and e-mail through a computer or IP phone, as well as the ability to set up instant voice conferences.

"When we put in the IP phones, we expected there would be some concerns among users about their complexity," says Johnson. But soon after their deployment, his team was pleasantly surprised. "When users did embrace the technology, it was more than we expected." In fact, he says, his one regret is not rolling out IP phones to all his users at once. "Our users who aren't on the IP phones get frustrated that they don't have all the features the other users have," he says. "The best advice we could have had is just dive into it, because the system works so well, and it integrates so well with other systems."

Security Simplified

Security is a crucial component of any communications system for smaller businesses. "These businesses have

the same concerns as bigger businesses, but they don't have the staff and resources to counter all the sophisticated types of attacks that can happen these days," explains Kathy Hill, senior vice president of Cisco's Ethernet and Wireless Technology Group. "The key is to provide a class of protection similar to what we've created for larger business networks, but make it easier for smaller businesses to install and manage."

Products such as Cisco Integrated Services Routers and the Catalyst Express 500 support layered security for smaller businesses. But more importantly, says Hill, Cisco has created intelligent applications, such as the Cisco Network Assistant, that do the technical background work—what functions to turn on or off, depending on security needs. "Instead of having to program each security function through a text-based, command-line interface, our customers just click on a toggle that looks like a volume control to choose a security level from high to low," Hill says. "The application then activates various network security controls accordingly. Very simple, very quick—the network does the configuration, but the customer controls the parameters."

A Holistic Solution

"While the business objectives of SMB customers may vary, they each require increased protection for their business assets, 24-hour uptime, reduced operating costs, higher productivity and better responsiveness to customers," says Mika Krammer, SMB research vice president for Gartner. "Savvy SMB customers realize that products alone won't address their needs. Rather, they need a holistic solution that will allow them to focus on running their business, instead of having to systems-integrate their own products, services, and financing."

With the comprehensive Cisco Business Communications Solution, those savvy SMB and midmarket businesses can now arm themselves with the technology they need to compete with larger companies, at last becoming world-class players in the global market. ■

FURTHER READING

- Cisco Business Communications Solution
cisco.com/packet/174_9a1
- News@Cisco Q&A on Cisco Communications Solutions for Small Businesses
cisco.com/packet/174_9a2
- CRN interview with Cisco CEO John Chambers on Small Business Strategy
cisco.com/packet/174_9a3
- Network Computing article on Cisco SMB offerings
cisco.com/packet/174_9a4
- Network World article, "Cisco Targets SMBs with Convergence"
cisco.com/packet/174_9a5
- eWeek.com article, "Cisco Takes IP Networking to SMBs"
cisco.com/packet/174_9a6

Restoring Trust in E-Mail

By Jim Fenton

Those of us who have been Internet users for several years remember a time when e-mail messages were nearly uniformly valuable—either a message from a friend or associate, or part of a discussion on a topic of personal or professional interest. Today, however, those messages are only a trickle within a larger flood of e-mail that brings unwanted advertising, viruses, and worms, or fraudulent messages such as phishing. For many, e-mail has gone from a productivity enabler to a burden.

A couple of years ago several Cisco engineers, led by Dave Rossetti, Cisco's vice president of Strategic Software Technology, began discussing how we could contribute to making e-mail a more effective, productive medium again. We concluded that the best approach is to improve the *accountability* for e-mail—to strengthen the trust among recipients that the messages they receive are actually coming from the alleged senders.

The biggest challenge in doing anything to the e-mail system lies in the wide variety of ways that e-mail is used. Many of the good ideas we initially had for improving e-mail accountability would interfere with one or more common applications. Take, for example, the popular send-this-article-to-a friend feature found on many Websites. To send such a message, the Website spoofs the sender's address. This behavior is also used for online invitations and greeting cards and by services including mail forwarding and mailing lists, all of which can present problems depending on how the accountability is enforced.

In our discussions about improving accountability, we also wanted to support use cases such as the outsourcing of business functions, which might require that a third party be granted permission to send mail on a client's behalf.

While others in the industry proposed techniques such as analysis of the IP address from which a given message is received, Cisco focused on the flexibility afforded by applying cryptographic signatures. Cryptographic signatures have been around for some time, but these signatures have a different meaning. Rather than coming from the message author, these signatures would come from the domain that "owns" the sender's e-mail address, signifying that the sender had permission to use that address.



JIM FENTON, a Distinguished Engineer in Cisco's Security Technology Group, is responsible for defining new router-based security features and architectures in addition to his role in e-mail authentication. He can be reached at fenton@cisco.com.

Ubiquitous message signatures present new challenges, as well. The signer of a message would not know, in general, whether the recipient or the domain is "signature aware" and can interpret these signatures properly. We therefore had to make sure that message signatures would be as invisible as possible to non signature-aware recipients. Fortunately, there is considerable flexibility in adding new fields to the e-mail message header that can convey the signature and associated data, while remaining invisible to most users.

Our discussions led to Cisco's message authentication proposal, Identified Internet Mail, which was recently merged with a very similar proposal from Yahoo! called DomainKeys. The resulting specification, *DomainKeys Identified Mail* or DKIM (dkim.org), has been submitted to the IETF for possible standardization. Several DKIM implementations exist now, and we are gaining experience on how DKIM would be used on a large scale. Message signing and verification, while an important step, is just one part of the task to improve e-mail usability.

In a few cases, it might be possible to automatically dispose of messages that violate policies published by the sender regarding their use of signatures. But in many cases, the message recipient will need to understand how to interpret the results of message authentication, which means the recipient should understand both how the authentication status of a message is displayed and what it means. Furthermore, senders of unwanted e-mail will probably sign their messages as well; accountable messages might still be unwanted.

Accreditation and reputation mechanisms, operating much like better business and credit bureaus, respectively, will inevitably be created to help users determine whether messages from a given (authenticated) e-mail address are worth opening.

Users' current experiences with e-mail are negatively affecting not only their productivity but their perception of the Internet as a whole. As the worldwide leader in networking for the Internet, Cisco feels a responsibility to help protect the usability of the Net. To that end, we will continue to apply our experience in protocols and hardware and software technology to not only help restore trust in and bring accountability to e-mail, but to promote the Internet's long-term usability as a productivity enabler. ■

SPOTLIGHT ON:

New Application Networking Products

Two new Cisco application networking solutions for data center and branch deployment help organizations optimize application performance, ease infrastructure consolidation, and improve end-user productivity.



The Cisco AVS 3100 Series Application Velocity System (AVS), which includes the Cisco AVS 3120 and AVS 3180 appliances, accelerates, monitors, and secures Web-based application delivery to all remote users across the extended enterprise without requiring changes to clients or servers. Deployed in the data center, Cisco AVS accelerates and optimizes any HTML or Extensible Markup Language (XML)-based application over HTTP or HTTPS—resulting in user response time improvements of as much as 500 percent, bandwidth requirement decreases of as much as 80 percent, and reduction in server processing cycles by as much as 80 percent.

cisco.com/go/avs

The Cisco WAE 500 Series Wide Area Application Engine (WAE), pictured here, gives branch offices high-performance access to applications, data, and content across the WAN. At a branch office or remote campus, the Cisco WAE serves as a storage and content distribution device. When running Cisco Wide Area File Services (WAFS) software, the Cisco WAE replaces file and print servers while providing fast read and write access to data center files. When running Cisco Application and Content Networking System (ACNS) software, the Cisco WAE optimizes delivery of Web content to the network edge for enhanced access speed and availability. Models include the Cisco WAE-511, WAE-611, and WAE-7326. The Cisco WAE is also offered as a network module for Cisco Integrated Services Routers. cisco.com/go/wae

For more on these new Cisco application networking products, see the *Packet* Special Report, "Application Networking," page 41.

Edge Routing, Access, and Aggregation

Cisco 3800 Series Integrated Services Routers: ATM OC-3 Network Module

The ATM OC-3 network module for Cisco 3800 Series Integrated Services Routers provides a single port for high-speed ATM WAN access in remote branch offices. The module supports the ATM Forum standard for ATM Adaptation Layer 5 (AALS) with a variety of quality of service (QoS) traffic classes. The network module increases flexibility by supporting Cisco Small Form-Factor Pluggables (SFP) that are also supported on other Cisco products. A single ATM OC-3 network module is recommended for the Cisco 3825 Integrated Services Router; a maximum of two modules are recommended for the Cisco 3845 Integrated Services Router.

cisco.com/packet/174_npd1

Switching

Cisco Catalyst 2960 Series Switch

The Cisco Catalyst 2960 Series intelligent Ethernet switches provide Fast Ethernet and Gigabit Ethernet desktop connectivity in a fixed-configuration, standalone LAN switch. The series includes models with dual-purpose (copper or fiber) uplinks for Gigabit Ethernet and a 24-port Gigabit Ethernet switch for desktop connectivity. The Cisco Catalyst 2960 Series software offers integrated security, advanced QoS, and resilience features. Models are suitable for medium-sized businesses and branch offices, providing 24 or 48 ports of 10/100 Fast Ethernet or up to 24 ports of 10/100/1000 Gigabit Ethernet for LAN connections.

cisco.com/go/catalyst2960

Continued on page 67

NEW PRODUCT DISPATCHES

New Products, Continued from page 65

Cisco Catalyst Express 500 Series Switch

Designed for organizations with up to 250 employees, the Cisco Catalyst Express 500 Series switches offer non-blocking, wire-speed Fast Ethernet and Gigabit Ethernet for data, voice, and wireless traffic. Currently available models provide up to 24 ports of 10/100 Fast Ethernet for connecting PCs, wireless access points, and IP phones as well as two 10/100/1000BASE-T Gigabit Ethernet ports for uplink or server connectivity. These switches also include advanced security features, GUI-based management, and Cisco Smartports technology that presets a Cisco-recommended switch configuration. Selected models provide Power over Ethernet (PoE) ports, and one model is designed for switch aggregation with up to 12 Gigabit Ethernet ports. The new Cisco Catalyst Express 500 Series is covered in greater detail on page 59.

cisco.com/go/catalystexpress500

Cisco Catalyst 4500 Series Switch: New Supervisor Engine and Switching Module

The Cisco Catalyst 4500 Supervisor Engine II-Plus-10GE rounds out the Catalyst 4500 Supervisor portfolio with 10-Gigabit capability in an enhanced Layer 2 Supervisor Engine. The Supervisor Engine II-Plus-10GE is equipped with Gigabit (SFP) and line rate 10-Gigabit (X2) ports on the supervisor, allowing for 10-Gigabit future-proofing and easy, cost-efficient migration to 10 Gigabit. Compatible with the widely deployed Cisco Catalyst 4503, 4506, and 4507R chassis and with existing Catalyst 4500 Series line cards, the Supervisor Engine is ideal for enterprises and medium-sized businesses that require secure, high-performance connectivity with maximum uptime in the LAN access layer, and is also suited for DSLAM aggregation in Metro Ethernet environments. The Cisco Catalyst 4500 Series 48-port, nonblocking, 100BASE-X line card gives users the ability to mix and match SFP optics. One to 48 100BASE-X SFP optics can be populated on a single line card.

Supervisor Engine:
cisco.com/packet/174_npd2
Switching module:
cisco.com/packet/174_npd3

Security and VPNs

Cisco Clean Access Commercial Solution

The Cisco Clean Access Commercial software provides comprehensive security policy enforcement and remediation specifically designed for businesses with 250 to 750 users. The Cisco Clean Access product family delivers features such as posture assessment and remediation support for Cisco switching, routing, and wireless solutions. Cisco Clean Access Commercial software automatically detects, isolates, and cleans infected or vulnerable devices that attempt to access the network. It identifies whether the devices are compliant with security policies and repairs vulnerabilities before permitting network access. For more on new Cisco products designed for small and midsized businesses, see page 59.

cisco.com/packet/174_npd4

Cisco Security MARS Version 4.1

The Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) appliances provide capabilities for monitoring, managing, and mitigating security threats. Cisco Security MARS version 4.1 offers distributed threat mitigation capabilities for a coordinated response to security threats from multiple network and security elements. The version 4.1 software also supports monitoring of additional Cisco devices and added features such as Network Admission Control (NAC), a new incident reporting and correlation capability, and integration with several third-party security products. Cisco NAC is covered in greater detail on page 53.

cisco.com/packet/174_npd5

Wireless

Cisco 3200 Series Wireless and Mobile Routers: New Wireless Interface Card and Cisco Rugged Enclosure Option

The Cisco 4.9 GHz Wireless Mobile Interface Card (WMIC) for Cisco 3200 Series wireless and mobile routers provides integrated wireless WAN or LAN capabilities in the licensed 4.9-GHz frequency band for public safety agencies in the US. The WMIC has a ruggedized, compact PC/104-Plus form factor and is designed to withstand a wide range of

environmental conditions. The 4.9 GHz WMIC can be configured as an access point, bridge, or workgroup bridge. As part of the Cisco 3200 Series, the 4.9 GHz WMIC is deployed in moving vehicles and used for creating outdoor wireless mesh networks for public safety and homeland security agencies. The Cisco 3200 Series Rugged Enclosure option provides the Cisco 3200 Series Router and WMICs with a completely sealed enclosure for both in-vehicle and outdoor deployments worldwide. Using passive conduction cooling, the Rugged Enclosure innovative design improves reliability in harsh environments and has been tested to withstand extreme variations in temperature, altitude, shock, vibration, and moisture.

WMIC: cisco.com/packet/174_npd6

Cisco 3200 Rugged Enclosure:
cisco.com/packet/174_npd7

Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Point

The Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Point forms a dynamic mesh for outdoor wireless networks. With dual-band support for IEEE 802.11a and 802.11b/g standards, the Cisco Aironet 1500 Series employs patent-pending Adaptive Wireless Path Protocol to provide robust, self-healing, self-configuring mesh wireless access to any Wi-Fi compliant client. The Cisco Aironet 1500 Series operates with Cisco Wireless LAN Controllers and Cisco Wireless Control System (WCS) software. Sixteen broadcast service set identifiers (BSSIDs) create multiple virtual wireless LANs, allowing network segmentation for different user types—such as police, fire, municipal services, or public access—over a single access point. The Cisco Aironet 1500 Series is covered in greater detail on page 47.

cisco.com/go/wirelessmesh

Cisco Aironet 1240AG Series Access Point

The Cisco Aironet 1240AG Series IEEE 802.11a/b/g Access Point is designed for challenging wireless environments such as factories, warehouses, and large retail organizations. A rugged metal case, extended operating temperature, and external antenna versatility provide flexible range and installation options. Available in either a lightweight or autonomous version, the Cisco Aironet 1240AG Series supports local power and 802.3af Power over Ethernet (PoE) and can be configured as an access point, repeater, or bridge. The dual-band Cisco Aironet 1240AG Series delivers data rates up to 108 Mbit/s in the 5-GHz and 2.4-GHz bands, and supports 12 non-overlapping channels under US Federal Communications Commission standards.

cisco.com/packet/174_npd8

Cisco 4400 Series Wireless LAN Controller

The new Cisco 4400 Series Wireless LAN Controller supports up to 100 access points with complete, system-level resilience. The Cisco 4402 provides two Gigabit Ethernet ports and supports up to 50 lightweight access points. The Cisco 4404 includes four Gigabit Ethernet ports and supports up to 100 access points. These models include expansion slots for adding specialized features such as virtual private network (VPN) termination and advanced security. Ideal for large-scale deployments, both models include embedded software for adaptive, real-time RF management and support an optional redundant power supply. The Cisco 4400 Series Wireless LAN Controller is covered in greater detail on page 47.

cisco.com/packet/174_npd9

Voice and Video

Cisco MobilityManager

Cisco MobilityManager makes Cisco Mobile Connect services available to Cisco CallManager users who want single-number reach. Users can redirect incoming IP calls to up to four different client devices, including their desktop IP phone and cellular phone. All voice mails for the user are stored and managed in a single Cisco Unity voice mail box. An integrated suite of mobility application services includes Web-based utilities for system administration and configuring user profiles. Cisco MobilityManager is installed on the Cisco 7800 Series Media Convergence Server (MCS) appliances and integrates with Cisco CallManager.

cisco.com/packet/174_npd10

Cisco 7900 Series IP Phone: New Models and Features

The Cisco IP Phone 7985G is a desktop video phone that includes a camera, LCD screen, speaker, keypad, and handset. The phone supports features such as call forward, transfer, conference, and hold. The Cisco IP Phone 7961G is an enhanced manager IP phone with six programmable line/feature buttons and four interactive soft keys. The Cisco IP Phone 7961G and Cisco IP Phone 7941G include higher resolution, 4-bit grayscale displays, enabling improved text and graphics display and a host of innovative, productivity-driven applications. Both the Cisco 7961G and 7941G IP Phones offer IEEE 802.3af Power over Ethernet (PoE) as a powering option. The Cisco Wireless IP Phone 7920 version 2.0 firmware delivers enhancements such as Extensible Markup Language (XML) applications, faster roaming, increased security, extension mobility, and support for Cisco IP Contact Center (IPCC) and Cisco IPCC Express systems.

cisco.com/packet/174_npd11 □



Cisco Unity Connection

Cisco Unity Connection combines integrated messaging, speech recognition, and call routing rules into an easy-to-manage system. Designed for deployment at a midsized company headquarters or centralized in one of several branch offices, Cisco Unity Connection supports up to 1,500 users. Features include voice mail with speech-enabled browsing and dialing, integrated voice and e-mail messages for Web access, and user-defined rules for call transfer.

cisco.com/packet/174_npd12

Cisco Voice Provisioning Tool

The Cisco Voice Provisioning Tool (VPT) provides a unified set of provisioning interfaces and services to simplify the initial setup and ongoing administration of Cisco CallManager and Cisco Unity systems. The Cisco VPT combines the most common user attributes from multiple Cisco CallManager and Cisco Unity servers to simplify common administrative tasks such as moves, adds, and changes with a single console, common commands, and user templates.

cisco.com/packet/174_npd13

Cisco MeetingPlace Express

Cisco MeetingPlace Express is an integrated voice and Web conferencing software solution, designed for midsized organizations to deploy on their internal networks, and is installed on a single server. As many as 120 concurrent users can participate in conferences managed by a single system. Cisco MeetingPlace Express helps enable highly productive virtual meetings by integrating meeting management capabilities directly into Web and Cisco IP Phone interfaces. Support for industry-standard protocols—H.323 and Session Initiation Protocol (SIP)—facilitates connectivity with a range of telephony systems, including Cisco CallManager and Cisco CallManager Express. For more on new Cisco products designed for small and midsized businesses, see page 59.

cisco.com/go/meetingplaceexpress

Networked Home

Linksys Wireless-G Broadband Router with SRX200

The Linksys Wireless-G Broadband Router with SRX200 combines MIMO (Multiple Input, Multiple Output) technology with two Wireless-G compatible radios and antennas for improved speed and range expansion (SRX). The WRT54GX2 yields significantly higher performance when used with the Linksys WPC54GX Wireless-G Notebook Adapter or the Linksys WMP54GX Wireless-G PCI Adapter. Linksys SRX200 devices are Wi-Fi certified and designed to be backward compatible with IEEE 802.11b (Wireless-B), 802.11g (Wireless-G), and other Linksys SRX products.

cisco.com/packet/174_npd14

ABOUT NEW PRODUCT DISPATCHES

Keeping up with Cisco's myriad new products can be a challenge. To help readers stay informed, *Packet* magazine's "New Product Dispatches" provide snapshots of the latest products released by Cisco between August and October 2005. For real-time announcements of the most recently released products, see newsroom.cisco.com/dlls/.

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/.

Linksys Wireless-G Travel Router with SpeedBooster

The high-speed, mobile Linksys Wireless-G Travel Router with SpeedBooster (WTR54GS) enables users to easily set up a wireless network in a hotel room or through a public hotspot such as an airport. The router includes a built-in power supply, wireless signal antenna, a WAN port for a cable or DSL connection, and an Ethernet port for connecting a wired device or computer. Users simply plug the router directly into the wall and establish either a wired or wireless connection to the available Internet access service.

cisco.com/packet/174_npd15

Deploying DMVPN Solutions

The Networking Professionals Connection is an online gathering place for Cisco experts and networking colleagues. Following are excerpts from a recent Ask the Expert forum, “Deploying Dynamic Multipoint VPN (DMVPN) Solutions,” moderated by Cisco’s Haseeb Niazi. To view the full discussion, visit cisco.com/packet/174_10a1. To join other live online discussions, visit cisco.com/discuss/networking.

Q: Are dynamic VPNs supported on firewalls as well as routers? Do the firewalls support compression? We use Generic Routing Encapsulation (GRE) on the router and IP Security (IPSec) on the PIX hub and spoke. Would multipoint GRE (mGRE) and Next Hop Resolution Protocol (NHRP) work in my design?

A: Currently, DMVPN is only supported on IOS. The PIX and VPN 3000 Series Concentrator do not support mGRE (or GRE). If your environment is a mix of IOS and PIX, DMVPN cannot be used. If you have a large number of routers and your hub is an IOS device, you can deploy DMVPN on routers and continue running IPSec between the PIX and IOS headend. PIX does support dynamic VPNs to terminate EzVPN hardware and software clients—although that is not the same as DMVPN.

Q: Are packets compressed before they are encapsulated and encrypted? How effective is the compression? Is it similar to point-to-point compression?

A: Compression is done before encryption and is actually performed by creating an additional set of security associations (SAs). The compression is less effective than some other techniques but is better than trying to compress the encrypted packets.

Q: I am about to deploy a DMVPN solution but I have not been able to send the amount of traffic that will simulate the real world. Can tunnel interfaces handle over 45 Mbit/s of traffic? I see the following output on the tunnel interface. Does this suggest a maximum data rate of 8 Mbit/s?

```
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
```

A: This bandwidth does not represent the actual amount of traffic a router (tunnel interface) can handle. The bandwidth measurements are used in routing protocol calculations. The amount of encrypted traffic a router can handle actually depends on platform, encryption card, and packet size. For example, if you are deploying a Cisco 7200 with VAM2 or VAM2+, it can handle 250-Mbit/s bidirectional throughput with a 1,400-byte packet size.

Q: We have deployed several DMVPN networks of different scales with Cisco 7206, 3745, and 1712 routers as the headend;

and Cisco 2691, 1712, and 831 routers as spokes. Does Cisco have any real-world data on the most stable software releases for both hub and spokes when deploying DMVPNs?

A: Cisco recommends 12.3(8)T8, 12.3(14)T2, or 12.3(15), and we are currently trying to qualify 12.4(3). I've had success with 12.3(11)T6, although there have been reports of memory leaks at some customer sites.

Q: Cisco does not support multiple mGRE tunnels using the same tunnel source. Is there a workaround?

A: Cisco implemented a methodology to share the IPSec protection between multiple tunnels using the same tunnel source (but different tunnel keys). Use the keyword “shared.”

```
tunnel protection ipsec profile <name> shared
```

Although the command is in the 12.3(11)T and 12.3(14)T code and works in certain environments, there are some issues with the implementation. Refer to CSCed68627 Bug Details in the Bug Toolkit.

Q: We have a hub-and-spoke scenario and want to encrypt data packets only. We do not want to encrypt voice packets over the GRE tunnel to the same location. How do we use DMVPN for this? Can we selectively send some traffic encrypted and some not?

A: Unlike crypto maps wherein you can use access control lists (ACLs) to define interesting traffic, traffic going through GRE tunnels is controlled via routing. After a packet gets encapsulated into a GRE packet, IOS encrypts it. In your scenario, you can have two tunnels on the hubs and spokes. On the hub, source the tunnels from two different public addresses. Apply tunnel protection to one and not the other. Route data and voice traffic accordingly. You can also segregate all traffic using VPN Routing and Forwarding (VRF). Have one VRF for voice and one for data. Again, use two tunnels—each can be part of a different VRF. Route the data traffic in one VRF and voice in the other. You will have segregated routing tables.

Do you have a question about deploying DMVPNs? Ask the NetPro Expert. Send your question to packet-netpro@cisco.com, with the subject line “Dynamic Multipoint VPNs.” ■



HASEEB NIAZI is a solutions engineer at Cisco with more than five years of experience in network-based security services. He currently focuses on testing scaling and performance of these services on a large scale, and assists service providers and major enterprises with their deployments. He can be reached at hniazi@cisco.com.

on an architectural framework—also called the NAC Framework.

Cisco Clean Access is an appliance that provides rapid NAC deployment with self-contained endpoint assessment, policy management, and remediation services, including patching and updates from Microsoft and leading antivirus vendors. More than 350 customers have deployed Cisco Clean Access, and it now enforces more than 2.5 million end users. In the largest deployment, Cisco Clean Access enforces 63,000 users. Arizona State University found that after it deployed Cisco Clean Access, “the number of security incidents fell from 6,000 a year to fewer than 50,” according to a university spokesperson.

The NAC Framework solution is an enterprise-wide approach that combines NAC-aware network devices, services, and central policy management with solutions from leading antivirus, security, and management vendors to provide granular admission control management. It is the best option for long-term, enterprise-wide deployments.

The NAC Framework comprises four components:

- **Endpoint security software.** To extend the NAC Framework to endpoints, companies install the Cisco Trust Agent software that includes open application programming interfaces (APIs) and which enable existing security software on the endpoints such as antivirus, antispyware, or personal firewalls to interact with NAC.
- **Network access devices** that enforce admission control policy include routers, switches, wireless access points, and security appliances. These devices demand host credentials and relay this information to policy servers where NAC decisions are made.
- **Policy server** evaluates the endpoint security information relayed from network devices and determines the appropriate access policy to apply. Cisco Secure Access Control Server (ACS), an AAA RADIUS server, is the foundation of the policy server system.
- **Management system.** Cisco management solutions will provision the appropriate

Cisco NAC elements and provide monitoring and reporting operational tools. Cisco Secure Monitoring Analysis and Response System (CS-MARS) has been enhanced so it can provide centralized help-desk and troubleshooting support for the NAC system, as can CiscoWorks Security Information Manager Solution (CiscoWorks SIMS).

IBM Tivoli software is one of the many security applications that have been integrated with the Cisco NAC Framework. Figure 1, page 53, shows NAC operating with IBM's Tivoli identity management and remediation system. The Tivoli Security Compliance Manager enables enterprises to define policy for devices that connect to the network. This policy information is relayed to Cisco Secure ACS, where network admission decisions are

determined. Cisco Trust Agent runs on each of the end devices and state information is relayed to the Cisco network device, an access point, a Cisco switch, and a Cisco VPN concentrator using three different techniques—over wireless, over 802.1X, or using User Datagram Protocol (UDP) over the Internet. Compliance checking is immediately carried out with Cisco ACS. If the device is compliant, it is given direct access to the enterprise network. If it is found to be out of compliance, Cisco ACS directs the end device to a quarantine LAN. On this restricted VLAN the Tivoli Security Compliance manager agent can open a session with the Tivoli Provisioning Manager to remediate the device. Once the remediation is complete, the Cisco network allows the device access to the secure production environment. ■



PACKET ADVERTISER INDEX

ADVERTISER	URL	PAGE
ADC - The Broadband Company	www.adc.com/truenet	D
ADTRAN	www.adtran.com/info/wanemulation	2
Aladdin Knowledge Systems	www.aladdin.com/Cisco	IFC
American Power Conversion (APC)	http://promo.apc.com (key code f757x)	4
BellSouth Business	www.bellsouth.com/business/nobrainer	OBC
Boson Software	www.boson.com	A
Cisco Marketplace	www.cisco.com/go/marketplace/packet	16
Cisco Press	www.ciscopress.com	B
Cisco Systems Networkers	www.cisco.com/networkers/wos	12
Citrix	www.citrix.com/cisco	72
eIQ Networks	www.eiqnetworks.com/cisco	10
Empirix	www.empirix.com/cisco	6
Extraxi	www.extraxi.com/packet	7
Funk Software	www.funk.com/csco	22
GL Communications	www.gl.com	46
Interstar	www.faxserver.com	70
Ipcelerate	www.ipcelerate.com	64 / 68
Network General	www.networkgeneral.com/cisco4	66
New Edge Networks	www.newedgenetworks.com/distribution/reseller	40
OPNET Technologies	www.opnet.com	56
Panduit	www.panduit.com/dp33	IBC
SBC	www.sbc.com/ipt	F
Solsoft	www.solsoft.com/packet	8
Sprint Communications	www.spirentcom.com/go/securitytest	54
Statseeker	www.statseeker.com	62
SurfControl	www.surfcontrol.com/go/blended	14
Trend Micro	www.trendmicro.com/cisco	48 / 49
Websense	www.cdw.com/remote/websense	52

CACHE FILE

Snippets of Wisdom from Out on the Net

CYBER QUOTE

"Home computers are being called upon to perform many new functions, including the consumption of homework formerly eaten by the dog."

—Doug Larson, Cartoonist

Working Group Casts a Line on Phishing Scams

The Anti-Phishing Working Group (antiphishing.org) received 13,776 reports of phishing scams in August 2005 and, in the same month, 84 brands were hijacked by phishing campaigns. Financial services continues to be the most targeted industry sector with nearly 85 percent of all attacks. Phishing is a form of online identity theft that aims to steal consumers' personal identity data and financial account credentials.

Click Clack

Researchers at the University of California, Berkeley, have found a way to turn the typing on a computer keyboard into a startlingly accurate transcript of what is being typed. The technique works because the sound of someone striking an "a" key is different from the sound of striking the "t." Once the different tones were identified, techniques from a field of research called statistical learning theory were applied to map the tones into similar categories and arrive at early guesses at what the text might be. A number of spelling and grammar correction tools were applied to this text to refine those guesses (computerworld.com, September 2005).

UK Shows Fastest Gain in Active Home Web Use

The active at-home Internet audience for the 10 countries tracked by Nielsen//NetRatings increased an overall 0.5 percent from November 2004 to February 2005. This modest growth is somewhat slower than the 1.5 percent growth measured for the same countries from August to November 2004. Among the leading gainers, the UK showed the fastest rise, increasing 11.3 percent from November to February. Continuing a recent trend, Spain added almost 500,000 home users in the same period. Australia was the third-fastest growing country, adding approximately 276,000 users, a 3.1 percent increase.

Net Lingo

Egosurfing—Looking to see how many places on the Web your name appears (whatismyname.com).

Mobile Web Users Access E-Mail, Weather Most

Mobile Web users still approach the Internet as a utilitarian tool for vital information, rather than as a platform for entertainment. The Mobile Internet Report published by Telephia identifies e-mail, weather, and maps among the most accessed site categories by mobile users. E-mail is the number one use of the Internet on a mobile device, and the second is access to weather Websites. Of the 191 million US wireless users, 4.8 percent access e-mail on their devices, and 3.9 percent access weather sites. The Mobile Internet Report was compiled with data from June 2005, and includes more than 1,200 panelists who responded to questions regarding their mobile Internet usage and demographics.

THE 5TH WAVE



"Daddy and I are going to give you all the love.com, care.com and opportunities.com that we possibly can."

©The 5th Wave, www.the5thwave.com