SBC Pacific Bell

Consultant/Vendor

CVSG

Sales Group

UPDATE - November 2002

SBC Employees Called To Active Duty; Many Are Still Serving Today

More than 250 SBC employees were called to active military service after 9-11-01. They served in a variety of duties and locations--overseas near the violence of War in Operation Enduring Freedom and across the U.S. providing Homeland Security. About 140 SBC employees remain on active duty today. We at SBC are proud of their extraordinary service and Thank Them for defending our freedom both here and abroad. SBC employees have served in the military for over 100 years. (Your CVSG Editor and Data Administrator were in the Army Reserve.) Here's the cover of our 1918 magazine honoring employees fighting overseas in World War I. AT SBC, we're here to serve our country & our customers. Always have. Always will.

Inside

AN UPDATE SPECIAL REPORT - *PERSPECTIVES*

"What's the Most Important Issue Facing the Telecom Industry Today?"

CUSTOMER FOCUS

George Cisler
Principal
G Services

For almost a century the sole provider of telecom services was the Bell System. No one questioned the strength, viability or longevity of regulated utilities.

The corner stone of the industrialized world depended on the presence of the monopoly companies to provide unparalleled services. Recently, several dozen service providers in the marketplace have disappeared on little or no notice, leaving customers stranded without critical

continued on page 3

CONVERGENCE

Peter Bologna
President
World Communications Group

con·ver·gence noun
1. **con·ver·gence** or **con·ver·gen·cy -- coming together**: a coming together from different directions, especially a uniting or merging of groups or tendencies that were originally opposed or very different.

Will voice and data "Convergence" change the face of Telephony, as we know it today? Probably… But what will this altered landscape look like? If you surveyed an appropriate number of industry experts,

continued on page 3

INDUSTRY CREDIBILITY

Jacque Mercier
Principal
Eagle Soar Communications

In my opinion, Industry credibility is at an all time low. Restoring that credibility and thus customer loyalty is the most important issue today.

Because of the ever increasing number of economically challenged telecom providers (like WorldCom), business's are fearful of being faced with business interruptions, being auctioned off to a new telecom company or disconnected. Our company has queried a number of our

continued on page 3

FUNCTIONALITY

Rob Lee
Principal
Results From Technology

Looking at the big picture, it is always easier to see the big opportunities. But the big opportunities are not always where the real prize lies. Just as the computer industry suffers through the throws of dealing with a mature market, so must the telecommunications industry. In this case, it is not a maturity of technology, but of functionality.

Easily justified technology upgrades exist in a corporate environment, but what is truly at stake is the ability for these same jumps to occur in the home/soho market. Here lies

continued on page 3

VICE PRESIDENT'S CORNER

LONG DISTANCE, SECURITY & MUCH MORE!

Kari Watanabe
CVSG Vice President

Long Distance News as we were going to press: SBC has asked the Federal Communications Commission for permission to offer long distance service in California, the country's largest long distance market. The FCC filing follows an endorsement by the California Public Utilities Commission of SBC's application. "California consumers are one step away from enjoying the benefits of full competition," said William Daley, President of SBC Communications Inc. "California's local telecom markets are more open and more competitive than any other state at the time of its Federal long distance application." Daley said FCC statistics show that 85 percent of California zip codes have competitors offering local phone service, while 46 percent of zip codes have four or more competitors. Companies authorized to provide local phone service have soared from 132 in 1998 to 364 as of First Quarter 2002. Total lines served by competitors have grown to 3.7 million, nearly seven-fold since 1998. The Telecommunications Research and Action Center estimates consumers could realize savings of about $800 million

continued on page 7

REMAKE THE BASIC BUSINESS MODELS

Mark Fei
Principal
Fei Communications Group

When ***Update's*** editor called and asked me to comment on this question, I briefly contemplated the usual list of causes given for our industry's current downturn. The over-exuberant investment of the late 90s; the overbuilding of long-haul fiber facilities; the bursting of the "bubble"; the failure of the Telecom Act of 1996. But all these explanations, to the extent that they're even correct (and some are not), only represent a superficial look at what's going on.

continued on page 3

Jerry Hinek, CISSP

The Role of Digital Signatures in Electronic Commerce

Jerry Hinek
CISSP
Corporate Information Security, SBC Services

Introduction

Businesses conduct business on the Internet. That's not news anymore. There are business to business (B2B) and business to consumer (B2C) transactions. When business is conducted over the Internet it is called E-Commerce. Trust is an issue in all transactions and businesses have learned to accept a certain amount of loss as the cost of doing business. Civil litigation or criminal law can enforce contracts on paper and even contracts made by handshake.

Enforcing a contract made in E-Commerce may be more difficult. One party to the transaction may deny having placed an order or having received an order. Anyone can bring up an Internet order form and put in anyone's name on the screen. There's no binding signature. There's no handshake. There's no eye contact. How can both sides trust the transaction?

With most B2C E-commerce the business will accept your credit card for your ID. So long as the business gets paid the business is satisfied. Of course you may not be happy if someone else has discovered your credit card number and used it to place that order. And what if you did place the order but the order was intercepted without reaching the business you were ordering from? How can these risks be mitigated? How can electronic contracts be enforced?

You may have heard of digital signatures. A digital signature is not simply typing your name into a text box on an on-screen order form. As I said, anyone could have typed in that name. A digital signature is a specific use of encryption technology, not for keeping secrets but for authenticating parties in a communication or transaction, parties who may even be strangers.

Encryption Background

I'll assume that everyone knows that encryption can be used to conceal the meaning of a message. You have to have a special "key" to reveal the meaning. Broadly speaking there are two types of encryption: The first uses the same key (secret key) both to encrypt the message and to decrypt the message. For the key to be a secret, the two parties to a confidential message must be able to agree to a key in some way that keeps the key secret from everyone else.

The other kind of encryption uses two keys, known as a key-pair. Either key may be used to encrypt the message. Only the other key of the key-pair will be able to decrypt the message. What is special here is that one key can actually be published for the whole world to see. This is called a public key. The key not published is called a private key. You can still encrypt a message using either the public key or the private key.

If you encrypt a message with a public key you get confidentiality. Only the holder of the private key will be able to read the message. If you encrypt a message with your private key anyone with access to the related public key can read the message, but only you could have encrypted it. Only you have the private key. You have created a digital signature.

Digital Signatures

A digital signature is simply using a private key of a key-pair to encrypt or sign a message or transaction.

The Role of Digital Signatures in Electronic Commerce

To Create:	Secret Message	Digital Signatures
Encrypt With	recipient's public key	sender's private key
Can Be Sent By	anyone	sender only
Decrypt With	recipient's private key	sender's public key
Can Be Read By	recipient only	anyone
Security Services	confidentiality integrity	authentication non-repudiation integrity

Table 1 - Uses of Encryption

It may seem like a big leap to reach that conclusion, but let's look at how that happens. Software and applications that generate key pairs do so in a way that only one person has the private key. The software or the server controls access to the private key, demanding a password or passphrase in order to see or use the private key. The public key may be left on your computer as a text file or stored in a public key database. The database would be available for anyone to read, but there would be access controls to prevent unauthorized updates.

If you keep your password or passphrase a secret then only you will be able to use your private key. If you encrypt a message with your private key, anyone can read the message because anyone can read your public key. But if anyone else encrypts a message, your public key will not be able to decrypt it. Any message that someone can decrypt with your public key is tied to you alone.

E-mail and Digital Signatures

Security people often attach digital signatures to E-mail. An awful lot of security alerts are hoaxes. One way to know that a security alert is real and not a hoax is for the message to be signed digitally by a trusted person or entity. Usually the message itself is not encrypted, but an encrypted signature is attached to the message. Companies and organizations that sign security alerts normally post their public keys on their web sites for anyone to download and use. So long as the web site is secure and hackers can't modify the public key then the signatures can be assumed to be valid.

Smart Cards and Digital Signatures

I mentioned credit cards in the Introduction. The next wave of plastic cards a lot of people expect to see might be "Smart Cards". Smart cards carry a little chip embedded in the plastic. The circuitry is visible. On the chip someone can store your digital signature, a signature created with your private key.

Some businesses already embed this smart card technology into their Employee ID Badges. The badge has a picture. The card is inserted into a card reader that verifies your identity and may perform some authorization checks to see whether or not you're allowed to enter a room or to read a file. The cards themselves are an attractive use for digital signatures.

Of course smart cards require smart card readers and that's an additional expense. It takes time for technology to get off the ground.

Combating Identity Theft with Digital Signatures

One reason identity theft is a growth industry in the modern world is that businesses are unwilling to pay for the security and privacy of their customers. As smart cards with digital signatures become common in the USA identity theft should diminish because authentication will be stronger. As consumers become more educated about smart cards and about the problems of identity theft they will probably demand that business implement these measures. It could become a competitive advantage.

How Secure is All This?

You never really know how effective your security is until you find out that someone has broken it. If someone breaks it and leaves no clues or you don't discover the clues, then you still don't know. Using digital signatures involves careful planning. Encryption technology has many links that can be tested for weaknesses. How securely you store the keys, how randomly you can generate the keys, how long are the keys and how trusting are you with strangers are all things that someone might use to break your security. You will always have to remain vigilant.

When investigating encryption products or digital signatures, deal with reputable companies that have been in business for some time and that use non-proprietary, public domain encryption algorithms. Then ask a lot of questions about how well they protect encryption keys. You need to know that only the owner of a private key can ever have access to it and that no one can break into or make changes in a public key repository.

Jerry is a Senior Business Security Manager for SBC Services. He earned an MBA in Information Management & is a Certified Information Systems Security Professional.

CUSTOMER FOCUS *by George Cisler - continued from page 1*

services, disrupting their operations. Such actions have shaken customer confidence. The once 'bigger is better' concept is no longer necessarily true. Questionable credibility of published statements leave customers with skepticism over their chosen providers.

With the increase in dependency on communications facilities, on what is now a global scale for virtually any size business, service providers have more opportunities than ever before to grow their client base. Saddled with older and ever decreasing valued technologies and infrastructures, and with price-war competition from all angles, even the largest of companies are franticly searching for ways to decrease operating expenditures while maintaining an acceptable grade of service. To the amazement of virtually everyone the corporate scandals, having hit our industry first, may have drawn our attention away from the core business, **service**. There is too much emphasis on stock price and monetary valuation and not enough focus on real customer, product, and service values. We can achieve sustained growth through a customer centric model (i.e. Cisco), even during a downturn in an entire market sector.

Prudent organizations investigate all aspects of critical service providers. This affords a quality telecommunication consultancy with more in depth customer interaction and involvement at multiple levels. This environment offers greater opportunities for consultants to fill the void for acceptable customer satisfaction than most current day service providers can afford.

G Services is a communications consulting & engineering firm offering services worldwide and specializing in Voice-Over-IP, remote office connectivity, video/audio broadcast services and Northern Telecom M-1 PABX system engineering, installation and programming services. George Cisler: www.gservices.info

INDUSTRY CREDIBILITY *by Jacque Mercier - continued from page 1*

current clients, and many were found not to have a real inventory or audit of their telecom services, and would experience a real disaster if they were forced to make a quick change. This lack of critical audit information is now being added to our "Disaster Recovery Program" that is used for our clients.

Recently, we had to resurrect the voice and data services for a client who was the victim of a failed telecom provider. Our client was not given a notice or a chance to prepare to change to another carrier, when their carrier went out of business.

In the process of working to restore service to my client, we discovered that they did not have a real inventory of their telecom services, copies of their correlating contracts or accounting practices in place that cross-referenced the services with their billings. Recently, I personally conducted a telecom audit for a school district that is preparing to change telecom providers and in the process it was discovered that the contracted Centranet rates were not being honored on the billings. The long distance plan rates were not being honored and the excessive billing charges amounted to over $350,000.00 over 36 months. On behalf of the district we obtained $56,000.00 in combined refunds and credits from the LEC and have filed for refunds from the long distance carrier as well. A contributing factor to my client's problems was the failure of the LEC account manager to concern himself with the client's services or advise the client. This lack of attention severely undermined the relationship.

Jacque Mercier is Principal at Eagle Soar Communications, experts in designing serve based voice applications and Unified Communications in the public sector, entertainment industry and commercial development. The firm's current project involves designing a master technology plan for 9 cities in Riverside County. Jacque Mercier: eaglesoar@earthlink.net

CONVERGENCE *by Peter Bologna - continued from page 1*

I'm sure that you would get as many different opinions -- and descriptions-- as there are flavors of a well known frozen dessert.

About twenty-five years ago, at the beginning of the digital age, we began to hear the hype and promise of the merging of voice and data. However, very few saw the need or had the courage to experiment with the combining of these two, seemingly very dissimilar technologies. The telecommunications people and the data communications folks were very content on doing their own thing, in their own way.

Now, a quarter of a century later the promise is revived and this time it looks as if it's for real. However, does that mean because we can converge, we should? Maybe, maybe not… As always -- the age old doctrines should prevail. We must be very careful not to introduce new technology for technology's sake.

Make sure the application fits, there is a good business case, and the costs are justified.

Peter Bologna is President of World Communications Group. He has more than 35 years of Telecom planning & management experience as Director of Administration with an international airline; Manager of Telecom for a large county government and as a Telecom Consultant. Peter, who teaches at Golden Gate University, can be reached at pbologna@worldcommgroup.net

FUNCTIONALITY *by Rob Lee - continued from page 1*

the rub. The home/soho market is the money loser and the core reason why regulatory controls persist, to protect the tiny consumer and make communications accessible and affordable to all. It is also where the greatest opportunity exists.

Access lines are dropping as technology extends itself. In the foreseeable future a single access point will carry all voice, data and video in a digital format. Yes, you've heard that before, but now is the time to make good on that promise. The victor will be the company that migrates the masses to this digital vision; and how hard could this really be? A simple black box at the POE to convert traditional services into digital transmissions would do it. Is anyone really up to the challenge to create it?

To the leader will go not only salvation from declining line revenues, but real increases in efficiencies and payback for existing technology investments, plus (re)captured customer loyalties. If the traditional telecommunications companies don't address this, perhaps the cable companies and possibly the wireless folks will take the lead.

Rob Lee is principal of Results From Technology! His main areas of focus include, Internet and e-commerce site development, remote access, VPN and branch office networks. Rob, who does complete technology strategy development, is author of "The ISDN Consultant: A Stress Free Guide to High Speed Communications." He can be reached at rob@roblee.com

REMAKE THE BASIC BUSINESS MODELS
by Mark Fei - continued from page 1

The most important issue facing the telecommunications industry today--and the one that will spell the demise of numerous players if they don't come to grips with it--is the need to completely remake the basic business models that form its underpinnings.

The telecommunications industry has been built, for well over a century now, on a set of basic business assumptions. A complete discussion of this would occupy a considerable set of books, but in essence it has boiled down to this: telecommunications capacity (switching and bandwidth) is complex, expensive and

continued on page 4

Cassandra Jessie-Johnson

DSL DATA SOLUTIONS

SBC Yahoo! and Speed Tiers…

Cassandra Jessie-Johnson

September 13, 2002 was a significant date for SBC. It marked the launch of SBC Yahoo! DSL and Speed Tiers. These two product enhancements have allowed us to mainstream broadband to offer more bandwidth and price choices to your customers. SBC Yahoo! DSL is an information service provided by SBC Internet Services that combines DSL transport with Internet access, and customized and enhanced content, services and applications from Yahoo! Inc., to provide the customer with high-speed broadband access to the World Wide Web.

With Speed Tiers, we now offer the following products:

Product Name	Speed (downstream x upstream)	Loop Length	Rack Rate
SBC Yahoo! DSL Basic Package	Up to 384Kbps x 128Kbps	16K	$42.95/mo
SBC Yahoo! DSL Standard Plus Package	384Kbps - 1.5Mbps x 128Kbps	12K	$49.95/mo
SBC Yahoo! DSL Standard Plus - S Package	384Kbps - 1.5Mbps x 128Kbps	12K	$64.95/mo
SBC Yahoo! DSL Deluxe Package	768Kbps - 1.5Mbps x 256Kbps	9K	$59.95/mo
SBC Yahoo! DSL Deluxe Package - S Package	768Kbps - 1.5Mbps x 256Kbps	9K	$79.95/mo
SBC Yahoo! DSL Expect Plus - S Package	1.5Mbps - 1.5Mbps x 384Kbps	7.5K	$159.95/mo

The availability of the new speeds is contingent upon the distance or loop length from the customer's premise to the Central Office. If the SBC Yahoo! DSL service is served by a Remote Terminal (RT), the loop length limitation does not apply. The guaranteed speed is the minimum speed in the speed range selected. Actual throughput speeds will vary due to Internet congestion and other factors associated with the Network or the customers' computer.

All SBC Internet customers can now benefit from SBC Yahoo! Dial or SBC Yahoo! DSL service. Customers can E-mail from home or from the Web, instant message, organize with their calendar and contact list, personalize their home page and create their own Web page, secure their PC and control online time. The core service features are:

- Customized browser with integrated instant messenger and Launchcast radio
- SBC Yahoo! Mail Account with @sbcglobal.net for new customers (25 MB)
- 10 Additional SBC Yahoo! sub-accounts, each with separate e-mail addresses (10 MB each)
- SBC Yahoo! Photos and Briefcase (Dial=60MB, DSL=110MB)
- Three free SBC Yahoo! Classified listings per life of membership
- Three free SBC Yahoo! Auctions listings per life of membership
- Parental Control Software
- Zone Alarm Firewall Software
- Access to all of the SBC Yahoo! content and features, including Finance, News, Movies, Sports, Games and Music.

Customers who would like to take a tour of the SBC Yahoo! product can be referred to http://yahoo.sbc.com/.

Also available…

DSL over Centrex is now available! SBC Yahoo! DSL can now be provisioned on Centrex lines. There are some limitations - DSL over Centrex cannot be provisioned from a Remote Terminal (RT). It can only be provisioned from a CO DSLAM. But don't let that stop your customers! This product enhancement provides customers with a high-speed data connection to the Internet or to their host server at their main office location. This is another quality, high-speed Internet access option for your customers. With DSL over Centrex, a customer will only have usage charges on the Centrex portion. Plus, there is even more good news - promotions from SBC Internet Service apply to DSL over Centrex. So call your Unique Services Center South Consultant Queue today at 1-866-234-4DSL (4375)!

We've got promotions…

SBC Yahoo! DSL takes what's good about the Internet and makes it great. We have incredible new offers in the marketplace allowing your customers to experience SBC Yahoo! DSL at promotional rates. Bundles, discounts on CPE, monthly rates as low as $29.95/month and waivers of processing fees are continuing throughout the quarter. Be on the look out for direct mail drops. Listen for radio ads announcing an offer in your neighborhood!

Delivering the difference…

With over 1.7 million DSL Internet subscribers, SBC remains on the cutting edge, with continued rapid deployment of DSL technology. At the end of August 2002, we had 1,780 Remote Terminals (RTs) with over 10,205 Distribution Areas (DAs) ready for service, in ASI West, SBC Pacific Bell and SBC Nevada Bell. For more information, to qualify your customers for SBC Yahoo! DSL Internet Service, as well as to order the service for your clients, contact the Unique Services Center South Consultant Queue at 1-866-234-4DSL (4375).

Cassandra is Associate Director-Data Solutions, SBC Pacific & Nevada Bell

REMAKE THE BASIC BUSINESS MODELS

by Mark Fei - continued from page 3

scarce. Large companies with substantial capital (e.g., "phone companies") can afford to make the necessary investments to build the capacity and then generate profitable revenue streams by selling access to their network. That's it. It doesn't matter if you're looking at voice services or data services; switched or dedicated, the basic business model is the same.

Well, guess what? We've all learned in the last several years that the premises of the above model are simply invalid. Is some of the technology complex? Sure, but not insurmountably so. And as for expensive and scarce, nothing could be further from the truth today. The price of telecommunications technology and bandwidth has plummeted at an astonishing rate that makes even Moore's Law look slow. As a consequence of that, the resources have become abundant. There is nothing "value-added" about switching or bandwidth. They are both commodities. There are still some important issues to be dealt with in this regard; perhaps most pressing is the need for widely available high bandwidth in the last mile. But, this is a short term problem that will go away through the ongoing application of both technology and competition.

The fact that a resource becomes a commodity doesn't mean that it becomes any less pervasive. Once upon a time, electricity was scarce and expensive--several dollars per kilowatt hour--and today is plentiful and cheap--a few pennies per kilowatt hour. Is electricity more or less important to the functioning of our society today? The same thing has happened with transistors. Today transistors have a negligible cost and are used by the millions in everything from TVs to PCs to electric toothbrushes. This exact phenomenon is underway with telecommunications commodities.

Bandwidth is not precious but it is important. It is in new, freely imaginative applications of bandwidth, unfettered by concerns about cost, that the new telecommunications industry will thrive. Successful participants will not follow this inevitable trend; they will lead it.

Mark Fei, founder of Fei Communications Group, LLC, has been training CEOs and other leaders in the Telecom World for nearly 20 years. He has been a great strategic resource, particularly for service providers and his opinions and expertise have helped many compete in an increasingly commodity-driven market. Mark can be reached at www.fei-comm-group.com

"Get your point across in less than 30 seconds"

- Update Tip for Success

Terry Young, Healy & Co

Wireless Broadband: WLANS – The New Local Competition

Global public and industry interest in Wireless LANs (WLANs) has exploded in the past year. Companies are deploying WiFi, (Wireless Fidelity) as it is often called, in offices and factories as replacements for wired LANs or to provide untethered access to the corporate network. Universities and hospitals are also deploying WLAN for access to internal resources as well as the Internet. WLAN service providers or WISP (Wireless Internet Service Providers) have launched fee-based services in public venues such as coffee shops, hotels, and airports. WLANs are also being installed by consumers to create in-home networks, and by community groups and individuals in public spaces to provide free Internet access.

WLANs are broadband access for public "hot spots". WLAN provides "cordless" access to the Internet / IP network within a limited range of an access point tethered to a DSL or T1 connection.

Indeed, Nicholas Negroponte of the MIT Media Lab recently proclaimed to the Financial Times; "WiFi will turn the telecommunications industry on its head." He predicts that WiFi will be provided as freely as the original Internet was provided to university – a fertile ground where a whole new grassroots level of communicating will evolve. This would be a world were "public networks" become a collection of user-provided access points instead of huge carrier-provided infrastructures.

DEFINITION OF WIRELESS LAN

A wireless local area network (WLAN) is a data communication system implemented as an extension to, or as an alternative for, a wired Ethernet LAN within a building or campus. Private WLANs are being deployed for in-home, institutional (e.g. universities and hospitals), and single-company use, typically as a replacement for a wired LAN. WLAN service providers and public operators are deploying public WLANs in high-traffic "hot spots" (i.e. hotels, airports, convention centers, and cafés) to allow high-speed Internet access. For example, Wayport and Boingo, two public WLAN service providers, have over 250 hot spot locations in California alone.

Public WLAN is intended for users "on-the-go", meaning that while WLAN could be used in different "hot spots"; but unlike a mobile phone, public WLAN requires the user to be stationary while accessing services. A comparison of private and public wireless LAN characteristics is presented in Table 1. Unlike private WLANs, public WLAN services must also address billing, ease-of-use, and more stringent security, privacy, and traffic management issues.

Table 1. A comparison of private and public wireless LAN characteristics.

Characteristics	Private WLAN	Public WLAN
Location	Homes, businesses and factories	"Hot spots": hotels, airports, cafés, public spaces
Operated by	Individual businesses and individuals	WLAN Service Providers and public operators
User base	Desktop and non-desktop employees, individuals	Individuals
Purpose	Replacement for wired LAN and/or access to company network; also provides an "instant" LAN	Medium to high bit rate access to Internet and/or company VPN
Security & Privacy	Medium but adequate	Medium but being improved

Source: Telecompetition, Inc. and the UMTS Forum, May 2002

WLAN is simply a wireless access mechanism for reaching an Ethernet LAN, the wired Internet, or corporate/institutional intranet/extranet. As such, the WLAN user has nomadic access to all the information and IP-based rich media services currently available on the wired Internet.

WLAN TECHNOLOGY AND KEY ATTRIBUTES

The emerging de facto standards for WLANs are 802.11b and 802.11a, but there are other contenders that could be used in the same market sector. The following describes some possible wireless access technologies, including: 802.11b, 802.11a, 802.11g, and Bluetooth.

IEEE 802.11b (Wireless Fidelity – WiFi): Operating in the license-exempt 2.4 GHz band, the IEEE 802.11b standard currently dominates the WLAN space. Using Direct Sequence Spread Spectrum (DSSS) techniques it delivers more throughput (up to a theoretical 11 Mbps) and greater range than the alternative of Frequency Hopping Spread Spectrum (FHSS) used in Bluetooth. Interference concerns regarding the use of 802.11b and Bluetooth in the same physical space exist. Efforts are currently underway to minimize the interference potential.

The key attributes of WiFi, the de facto WLAN standard, are: license-exempt spectrum, high-speed, and wide availability.

IEEE 802.11a (WiFi5): Using Orthogonal Frequency Division Multiplexing (OFDM) instead of spread spectrum techniques, the 11a standard is intended to operate in the 5 GHz spectrum band. With the potential to deliver up to a theoretical 54 Mbps, the use of OFDM also improves the ability of radio devices to operate in a complex environment where multipath fading will be commonplace. Several vendors are shipping 802.11a-compatible devices.

IEEE 802.11g: The draft IEEE 802.11g specification is generating interest in the WLAN community. 802.11g, an extension of the 802.11b standard and also operating in the 2.4 GHz band, uses the same OFDM modulation scheme as 802.11a to provide a theoretical maximum data rate of 54 Mbps. Though the higher-speed advantages of 802.11g over 802.11b are obvious, numerous engineering and standards-ratification issues remain to be resolved before 802.11g is formally adopted as a standard and compatible products become commercially available (most likely late 2003 or 2004).

Bluetooth: Bluetooth is a global computing specification for short-range communications between computers, handsets, PDAs, printers, and other devices. It uses the licensed-exempt 2.4 GHz band and currently has a maximum range of approximately 10 meters. Efforts are underway to increase the range to 100 meters.

Key Attributes of WiFi (802.11b)

Numerous attributes have contributed to the market interest and deployment of public 802.11b (WiFi) WLANs:

- Use of easily available (license-exempt) spectrum
- Wide availability of WiFi-compatible products
- Economies of scale and declining component costs
- Technology of choice for private WLANs (office and home)
- Growing need for untethered access to the Internet or corporate systems and information
- High data rate access to the Internet, in areas where high data rate access has not been previously economical
- The appearance of community grassroots initiatives to provide free access to the Internet via WLAN in public spaces

continued from page 5

WiFi, though the dominant WLAN technology, faces several key constraints to widespread deployment as a public network access technology:

- Shared spectrum: WiFi shares the license-exempt 2.4 GHz spectrums with other devices, including household appliances (e.g. microwave ovens and garage door openers) and Bluetooth devices.
- Lack of consistent operational regulations for WiFi and other WLAN technologies between countries: For example, some countries do not allow public access applications and other restrict the amount of the bandwidth that can be utilized.
- Deployment and scaling difficulties: The coverage area of a WiFi access point depends on a number of environmental factors, including: the distance and configuration of nearby walls, the material content of the walls, and the proximity of reflective surfaces. In a situation where the users are expected to be stationary, WiFi network planning is relatively simple (single cell approach). However, if users are expected to re-locate/move from the coverage area of one access point to that of another, WiFi network planning becomes more difficult (cellular approach).
- Security and privacy constraints: Researchers have shown that holes in Wired Equivalent Privacy (WEP), the encryption technique used by WiFi, can be exploited by hackers to uncover the encryption key used to encrypt WiFi traffic. The 802.11b protocol does not provide true end-to-end security. However, proponents feel the level of privacy is comparable to that experienced on wired Ethernet LANs. Currently, WLAN access providers and third-party developers are working on methods to enhance WiFi security and privacy capabilities.
- As with most wireless systems, advertised data rates are generally not attainable: The characteristics of the physical surroundings, Ethernet collision-avoidance schemes, quality of WiFi network design, and the number of simultaneous users, all contribute to actual shared user data rates to below the nominal 11 Mbps. A similar situation exists for wired Ethernet LAN. The actual total data throughput is about 6 Mbps over a short range and degrades over distance, number of users and location of users within the coverage.

IMPACT ON SBC

As with any new network technology, there are opportunities and challenges. With WiFi, every access point in every hot spot will need to be connected to a high speed wired Internet connection. This holds opportunity for both T1 and DSL service from SBC.

The challenge comes from the fact that WiFi will also directly compete with other retail, broadband access services including both DSL and cellular. Some home workers and SOHOs, for example, could opt to take their laptop to their local coffee shop "hot spot" for free access rather than pay for a DSL connection at home. DSL cannibalization impacts the SBC local exchange companies and Cingular, the cellular operator. Certainly one solution is for SBC to offer WiFi services. Concern for WLAN replacement of 3G services has already prompted some mobile operators to consider adding WLAN into their product portfolio. Indeed, if Nicholas Negroponte's vision were realized, WiFi would ultimately replace all network operators!

FUTURE ARTICLES

Look for future articles on WLAN players, pricing, target market and revenue potential or contact Terry Young at Healy & Co for further information tyoung@healy-co.com.

FAA Turns to SBC

The Federal Aviation Administration has turned to a consortium of companies, including SBC, for help in modernizing its crucial telecom infrastructure. SBC will join forces with Harris Corp., to do the work under the terms of a 15-year multi-billion contract to upgrade operations at more than 5,000 facilities nationwide. The project is designed to enhance network security, cut operating costs and improve the quality and reliability of the FAA's telecom services. Under terms of the contract, SBC will work with Cisco Systems, Raytheon and others to merge four data and communications systems into one integrated network.

Cingular Takes "Rollover" Nationwide

Cingular Wireless announced the launch of "Rollover"--the wireless plan that lets customers keep their unused monthly minutes. Customers who have leftover package minutes in one month will have them "rolled over" into the next month for up to 12 months. Market research conducted for Cingular shows consumers believe "Rollover" provides value and personal control because customers no longer feel they are wasting money on unused minutes. For further information, contact your liaison manager.

Beware: Telemarketing Fraud & Slamming on the Rise 370%

In the past few months, SBC Pacific Bell has received a significant increase in calls from customers seeking assistance with alleged incidents of deceptive sales and marketing practices and slamming by other carriers.

Customers have told SBC that "Pacific Bell is going out of business" or that "Pacific Bell has been merged or bought" so they "need to change carriers." These types of calls are up 370% compared with January. The alleged comments are untrue. SBC Pacific Bell remains a vital part of the SBC family.

Tips to Prevent Deceptive Sales & Marketing Practices and Slamming

-- **Be Direct.** Be suspicious of anyone calling and claiming to be a local telephone or long distance company employee. If you're in doubt about the caller being an SBC rep, hang up and call your local SBC Pacific Bell Business Office (the number's on your bill or in the phone directory).

-- **Ask Questions First.** When receiving a call with an offer to switch your phone service to a new provider, be sure to ask questions that will help clearly identify the company, what it offers, price of the service and how you can contact a service rep.

-- **Carefully Read Your Phone Bill.** Be sure you understand charges listed on the bill and have chosen to do business with the provider billing for those charges.

-- **Be Suspicious of Alleged Changes in Your Service.** Some SBC Pacific Bell customers have reported receiving calls or mailings from other companies alleging that they bill or provide services on behalf of SBC--a tactic used to slam customers.

SBC Pacific Bell customers can report such fraud & slamming calls by phoning 1-800-310-2355 and business customers, 1-800-750-2355.

News Flash
S.S.3
SBC Sells 3Com!
Stay tuned. More to come...

"Listen"

-Update Tip for Success

ASTRALcom Internet Solutions and SBC Pacific Bell Provide Web Site Success

SBC e-Services provides customers with robust and scalable web hosting services: shared or virtual web hosting; basic dedicated web hosting; and complex/managed hosting on high powered servers housed in highly secure and redundant data centers in Irvine, CA and Dallas, TX. These services were recently profiled in our April 2002 ***Update***. Articles have also appeared in ***Update*** describing our Irvine Data Center and the benefits of web hosting from SBC Pacific Bell. What we haven't discussed has been the content customer's place on their web site and how that is developed.

SBC Pacific Bell works with ASTRALcom Internet Solutions, an independent business and an SBC Pacific Bell Authorized Sales Agent, to help customers develop their web content and design. With over 30 combined years of Internet experience, ASTRALcom provides total solutions for Business-to-Business, Business-to-Consumer and Government-to-Consumer entities.

Together, SBC and ASTRALcom deliver complete digital business services, strategies and solutions:

- Secure website and application hosting
- Fast, reliable Internet connectivity
- Award-winning website design and development
- Superior and friendly customer service

Here are two customer testimonials showing the value of this teaming:

Digital Solution Business Case Examples That Work

Texas Greenhouse Company

"Our plans to increase our business on the web started with SBC. We wanted to be sure that our site would perform under high-traffic circumstances. SBC is a leader in website hosting and we knew they could handle our site. SBC recommended their web development partner ASTRALcom Internet Solutions for the content development and design services we needed. After having ASTRALcom do an initial redesign, some navigational changes and some search engine work, our company has been able to triple our website traffic and double our web-based business."

Tom Benua, Texas Greenhouse Company

David Martin and Son Roofing, Inc.

"All of the hard work that goes into a productive website is critical in today's commerce driven society. Our vision was to create an online strategy to help support our growth and enhance our customer service. Choosing SBC was the first step in ensuring the security and stability of our online business model. ASTRALcom worked with us from the ground up on establishing an effective and successful web presence that we can maintain. Now, after each project, we snap a digital photo of our completed work and then upload it to the website easily and quickly. It's not only a portfolio of our work, it's also a way to showcase our clients."

Walt Sorenson, David Martin & Son Roofing, Inc.

To learn more about ASTRALcom go to their website at www.astralcom.com or call 800-536-6637.

SBC webhosting.com (http://www.sbchost.com/home.shtml) contains information on a comprehensive range of services designed by SBC. We can provide a reliable and secure hosting solution that will grow with the needs of your client's business. Below is an overview of these services.

SBC provides Shared Web Hosting allowing multiple customers to utilize the same server. Shared Web Hosting is designed for small businesses who wish to outsource web hosting and operate on a small budget.

Medium to large customers whose sites have a large number of images, plan to offer any type of e-commerce or who intend to attract large volumes of traffic will use Dedicated Web Hosting by SBC. These companies have their own "dedicated" server, not shared with anyone else. Although more expensive than Shared Hosting, it provides more space, security and bandwidth.

Customers looking for an unparalleled level of system management and support choose Advanced Web Hosting from SBC. Our entire Advanced Hosting line is fully monitored and includes reports and predictive analysis that is accessible online. Our technical staff leverages their extensive experience in designing customer solutions and an individual team lead is assigned to oversee the customer's implementation. Completing the package, we back our solutions with ironclad SLAs including 99.99% availability.

If you're apprehensive about leaving your hosting in the hands of another company, but don't have funds to physically maintain a server and direct Internet connection, a co-located server is the next best thing. With co-located servers, SBC will connect your hardware to the Internet at our Internet Data Centers (IDC) in Irvine, CA or Dallas, TX. We provide physical space in the IDC to house your server in a secure environment and provide technical support.

For more detailed information on SBC hosting solutions please see our web site at:

http://www.sbchost.com/home.shtml or call your Liaison Manager at 800-552-5299.

Tom David
Liaison Manager, td1898@sbc.com

LONG DISTANCE, SECURITY & MUCH MORE!

a year, once California's long distance market is fully open. Typically, as soon as state regulators permit long-distance competition, prices drop and customers immediately receive the benefits of more choices. Not only is there increased competition in long distance but competition in local service takes off as well. SBC currently offers long distance as well as local service in Connecticut, Texas, Missouri, Oklahoma, Kansas and Arkansas.... **Security**: Be sure and read "The Nation's Strategy to Secure Cyberspace" (p. 19) courtesy of Paul Eaton of Booz Allen Hamilton, "Understanding IP Security" (p.15) by Nehemiah Chriss and "The Role of Digital Signatures in Electronic Commerce" (p.2)by Jerry Hinek. **Special Reports**: "The Hidden Power of Voice Mail" (p. 10) by Chris Horne of Pinnacle Bay Group; "Pre-Call Preparation for Video Conferencing" (p. 13) by the SBC Executive Briefing Center's John Bianchi, "Wireless Broadband: WLANS" (p. 5) by Terry Young of Healy & Co., "Resilient Packet Ring" (p. 8) by SBC's Paul Bedell and a Special Healthcare Report (p.16) by Jagdish Kohli, Ph.D., and "Data With David" (p.11) plus lots more, including a new feature - "Perspectives" - that shows what some consultants think on important issues. Our goal is to continually evolve ***Update*** to bring you a variety of valuable ideas and solutions that will assist in maximizing your efficiency and success. Read on & enjoy. **Thanks**,

Kari

Kari Watanabe
CVSG Vice President
415-542-4516
kw6875@sbc.com

SBC Playing Critical Role In Combating Cyberterrorism

SBC is providing ongoing consulting expertise to support San Antonio's "Operation Dark Screen." The first step in the project was a recent secret simulated attack to test the effectiveness of local government, military and business in preparing, detecting and responding to an attack of information warfare. SBC worked with the University of Texas's Center for Infrastructure Assurance and Security to identify problem areas and make recommendations for improvement. A followup event is being planned for next year. SBC's services and equipment are involved in the information systems of every participating group. SBC also will be helping other cities and organizations in their efforts to counteract cyberterrorism. SBC works closely to help ensure the integrity of organization's networks at every stage-- from network design to implementation to ongoing managed security services. We provide network security for some of the largest companies in the world as well as the most critical government agencies.

A story on the need to secure Cyberspace can be found on P. 19

SBC's Paul Bedell

Ringing In 2003 …

Will RPR Be The Silver Bullet For Data Transport?

Paul Bedell

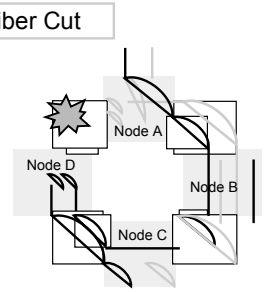
Resilient Packet Ring (RPR) is an emerging standard focused on facilitating native Ethernet deployments outside LANs into MAN and WAN topologies where Ethernet traditionally had not been deployed until 1999. RPR strives to create a standard for WAN Ethernet transport that improves service reliability, lowers deployment costs and facilitates provisioning while at the same time adopting Ethernet for ring topologies. Not exclusively designed for Ethernet transmissions, RPR attempts to combine the simplicity, granularity and high performance of IP packet transmissions with the network protection and survivability of SONET-style optical rings. This isn't to say Ethernet won't work well with RPR, just to note that it wasn't designed specifically with Ethernet in mind, but rather "packet transport" in a generic sense.

RPR is a new Layer 2 media access control (MAC) protocol that combines features of SONET, ATM (statistical muxing), and Gigabit Ethernet (simplicity and popularity). As the name indicates, RPR is designed to work in ring topologies, and will provide sub-50ms restoration times critical for delay-sensitive (voice) traffic. It will also streamline routing decisions by assuming a ring topology is in place. As a result, routing logic can be simplified to one of three choices: add, drop, and "pass-through". RPR devices are essentially packet add-drop multiplexers.

RPR will effectively double the capacity of each metro ring, a big plus for service providers who lease their fiber infrastructures. RPR is striving to create a set of standards so that Ethernet can be delivered in its native form without being encapsulated into SONET payloads. It will enable service providers to maximize bandwidth efficiency. For example, not having to provision a SONET OC-48 circuit (of 2.5 Gbps capacity) to transport a 1 Gbps Ethernet signal. RPR should also help carriers facilitate provisioning by not having to deploy a separate, additional layer of SONET rings. RPR standards should make multi-vendor interoperability easier, which should lead to lower system prices in the long run and help stimulate demand.

As with SONET, packet rings are configured with a working and spare protection ring. Nodes adjacent to each end of a fault can use the "ring wrap" technique to route packets in the opposite direction over the "protect" ring. Protection switching occurs in less than 50 ms. RPR is also being designed to support up to 100-200 nodes on one ring, which compares very favorably with the maximum of 16 nodes for a SONET ring if all nodes are TDM, and 32 if all nodes are IP. Figure1 illustrates how the ring wrap process works.

Some equipment vendors already offer proprietary solutions for "reliable" Ethernet delivery in a WAN environment, but the success of these solutions has been limited. Other equipment vendors also support pre-standard resilient packet ring (RPR) technology. This includes vendors such as Cisco Systems, Lantern Communications, Luminous Networks, Nortel Networks or Riverstone Networks.



Traffic incoming to node D is ring wrapped. It is looped around and sent back in the other direction to node C. This is also known as digital wrapping.

Figure 1: Ring Wrapping in RPR

RPR's objective is to get network restoration time down to 50 milliseconds - the same as SONET. It's easier to implement a fast and robust link-failure recovery mechanism in a ring topology than in a mesh topology. This is because in a ring the alternate route is always known. The IEEE 802.17 committee does not view RPR as solely Ethernet-based, and indeed there is no intent to have an IEEE 802.3 device directly connected to an 802.17 interface.

While RPR should enable carriers to offer reliable Ethernet service delivery, some major obstacles still exist. Obviously, the most significant impediment is finalizing the parameters of the standard, which is expected in 2003. Another issue that could limit RPR deployments is adoption by service providers. To date, most deployments of proprietary versions of RPR-like solutions have occurred in IP-centric networks, not SONET-based networks.

Implementation of RPR by carriers with a large installed base of SONET equipment could prove challenging. Telco product marketing groups need to develop a solid business case that underscores the importance of deploying metro Ethernet products that have an RPR-based infrastructure as their foundations. Even if this means slowly building these networks in parallel to legacy (SONET) networks, in the long run it's still a logical and cost-effective path to a future revenue stream that's certain to only grow. The only question is how fast these newer optical Ethernet services will grow. The key aspect of an effort like this is to show – in the business case – that RPR-based Ethernet platforms are more cost-effective than other options such as next generation SONET.

KEY: Most service providers have two distinct transport operations groups: (SONET) network engineers and IP/Ethernet network engineers, each having separate capex budgets. RPR deployments would require coordination between the two groups, potentially complicating deployments. Sharing a common operating software for the platform could also complicate deployments, management and billing. In the RBOC world, these groups are actually separated into distinct operational and legal entities via regulatory edicts (Telecom Act of 1996).

RPR Objectives

Current objectives for RPR include using Ethernet framing in SONET-style rings. The goal of RPR is simple: to define a high-performance, high-availability optical transport method suitable for ring-based carrier networks in metro service areas. The RPR standard attempts to define a new media-access controller (MAC) to run both Ethernet and SONET on fiber-optic rings, which are the prevalent topologies in metropolitan networks. RPR aims to parcel bandwidth more efficiently than SONET and to provide resiliency that's not inherent to Ethernet.

KEY: The (4) primarily goals of the RPR Working Group are restoration, resiliency, scalability, and QoS.

As reported by the RPR Alliance, the following objectives comprise a high-level outline of the architecture that the Alliance is currently promoting – the features that will make RPR "SONET-like":

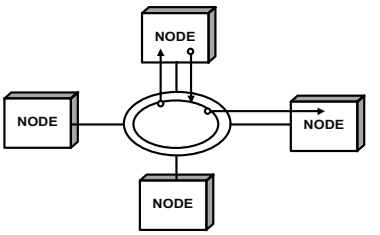
Dual Counter-Rotating Ring Topology. In dual ring topologies, SONET uses only one ring to carry live traffic; the other ring is reserved as a backup. No production traffic is routed across this backup ring, which is a tremendous waste of fiber facilities. To increase fiber utilization, RPR will send traffic over both rings (in opposite directions, of course) during normal operation.

A fully distributed access method without a master node: An RPR ring will continue operating despite the loss of any node.

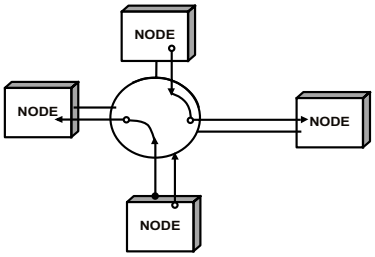
Protection switching in less than 50 milliseconds. In the event of a fiber break or node failure, RPR will restore service at least as fast as SONET.

Destination stripping of unicast traffic. Unicast traffic is communication between a single sender and a single receiver. In some older packet ring architectures, the source node removes unicast packets after they come all the way around the ring. With RPR technology, destination nodes remove their unicast packets, freeing downstream bandwidth for re-use by other flows. Together with packet multiplexing and counter-rotating rings, destination stripping will more than double RPR's total throughput compared to SONET. See **Figure 2** below for a high-level illustration of the difference between source stripping and destination stripping.

Figure 2: The Functional Difference Between Source Stripping and Destination Stripping



SOURCE STRIPPING



DESTINATION STRIPPING

Source: Business Communications Review, September 2001 "RPR: Building a Better Ethernet"

Support For Multi-Cast Traffic. Multicast traffic is communication between a single sender and multiple receivers. Multicast packets will travel once around the ring to reach every node. By contrast, mesh networks must replicate multicast packets in order to reach all destinations.

Support For Up To 10 Gbps: RPR will be fast enough to carry Gigabit and 10 Gigabit Ethernet traffic, but will also support lower data rates.

Support For SONET/SDH (physical layer), GigE and 10 GigE (LAN PHY). Support for existing physical layer standards as well as Ethernet up to 10 GigE will allow RPR products to use widely available equipment components.

Layer One and Payload Agnosticism. To be truly universal, the new RPR MAC standard will be completely independent of the physical layer transport, and will not interfere with customer payloads.

Plug and Play Support: New nodes may join the ring without manual configuration – a form of auto discovery. This will be one of the best advantages of RPR, and compared to SONET provisioning requirements, it will save weeks or months of provisioning time that's normally required when turning up or upgrading a SONET network.

Managed Objects. By defining managed objects, the RPR standard will facilitate OSS integration.

Support For Services That Require Bounded Delay and Jitter, and Guaranteed Bandwidth. RPR will deliver TDM-like QOS. But the RPR Alliance needs to be very careful with this concept. RPR moves too far from Ethernet in trying to support TDM, it won't be able to use commodity chipsets, and it may pose more direct competition to SONET than some suppliers would like.

Dynamic Weighted Bandwidth Distribution. RPR will allocate bandwidth to competing traffic flows on demand, offering a form of statistical multiplexing. This makes RPR very similar to ATM.

Support For Multiple Service Types. RPR will adapt to future requirements.

Vendor Interoperability. RPR equipment from different vendors will interoperate on the same ring, because RPR will be an open standard.

In summary, RPR's primarily mission is to make optical rings more efficient for packet traffic, but the standardization effort has attracted some developers who want to see it do more, especially in the realm of QOS and traffic control. Other factions maintain that Layer 3 mechanisms such as DiffServ and MPLS can be used to provide these functions, which makes sense.

RPR interoperates with SONET and DWDM, making it suitable for deployment in existing metropolitan optical networks. It can be used to improve packet-handling capabilities of existing SONET core networks without affecting TDM traffic handling functions. RPR also supports multiple classes of service.

RPR Controversies

Some metro area Ethernet developers are opposed to the new MAC concept which RPR will offer. A Vice-President from one equipment supplier is quoted as saying that "RPR is as similar to Ethernet as token ring is to Ethernet: that is, they're not similar at all. Ethernet is standard, understood, and based on cheap components that scale fast. RPR will need different components, a different operational support system (OSS), and so on".

Atrica is one vendor that's taking a different approach with its family of optical Ethernet switches. It uses a 10 Gbps Ethernet MAC over WDM wavelengths, and relies on existing standards to make up for Ethernet's shortcomings. For example, DiffServ and 802.1p will let switches manage traffic priorities, while MPLS provides fast recovery from outages.

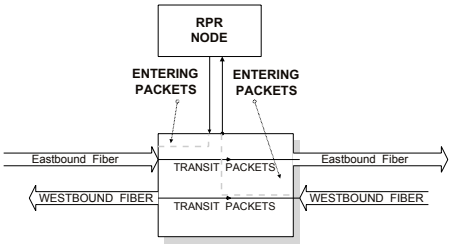
The engineers at Appian Communications aren't entirely opposed to an RPR MAC, but they are also concerned about its complexity. They believe that matters like "fairness and QOS' should be handled by existing standards outside of RPR. They believe if the objectives of the RPR working group aren't kept simple, nothing will get accomplished. Good point.

By contrast, Cisco doesn't share Appian's or Atrica's concerns. In fact, it already has a new proprietary MAC layer, the Spatial Reuse Protocol (SRP), that meets many of the RPR objectives. (SRP is part of Cisco's Dynamic Packet Transport (DPT) product line, which has been shipping since late 1999, largely to cable modem service operators. Cisco submitted SRP to the IETF in 1999 as informational RFC 2892, and participates in both the IEEE RPR working group (802.17) and the RPR Alliance).

Packet Priority

One of the controversies that the RPR Alliance has been wrestling with is the relationship between packets entering the RPR ring and those already on the ring. Should packets in transit take precedence over entering packets, or should all packets compete equally for bandwidth at every hop? With Cisco's SRP, transit packets take precedence over entering packets, so there's no packet loss on the ring itself. This is different from how Ethernet switches operate. Ordinary Ethernet switches, which lack a "cut through" path for transit traffic, exhibit varying packet loss throughout the network as traffic congests at each node. See Figure 3 below.

Figure 3: Graphic Depiction of Transit and Entering Packets In RPR Rings



KEY: If the 802.17 working group decides against transit cut-through, then RPR will lose a potential advantage over ordinary Ethernet switching.

RPR and TDM: Keep It Simple Folks

Another controversial topic is the relationship between RPR and TDM. This controversy involves the definition and scope of RPR, and the migration path from a SONET network to an RPR network.

There are two camps:

- One camp sees RPR as a SONET ADM replacement,
- The other camp sees RPR as simply a high-performance packet MAC.

The rationale of the SONET replacement camp (camp #1) echoes every convergence vendor's slideware: voice is still a big revenue producer, so RPR has to handle voice efficiently. In contrast, the keep-it-simple camp (camp #2) argues that TDM support will be RPR's undoing. A common refrain from camp # 2 is that if RPR tries to do everything, it won't do enough TDM for the TDM camp, and it won't do enough packet for the packet group. They don't want to kill RPR by overloading the working group with a list of objectives that have a huge, varied mix.

Appian Communications offers a hybrid solution to this controversy, a compromise of sorts. Its Optical Service Activation Platform (OSAP) dedicates some channels on a SONET ring to packet traffic and leaves other channels for ordinary TDM traffic. This allows OSAPs to share fiber rings with conventional SONET ADMs.

KEY: Equipment vendors are likely to ignore any standard that requires massive re-engineering of their product lines to support TDM, since today, carriers are mostly content with running their voice circuits over SONET.

Networking history is littered with at least three now-defunct packet ring standards: FDDI, DQDB (802.6) and Token Ring (802.4). To avoid membership in this unfortunate club, the 802.17 Working Group should stick to its main objective: efficient, robust, ring-based metro area data transport. Likewise, if technical complexity makes RPR too expensive, some other flavor of optical Ethernet will capture the market. If the working group tries to be all things to all carriers and equipment makers, standards-based RPR products will never make it past the interoperability demos, and the group will have failed.

The Competing RPR Proposals

In September 2001, two proposed standards competed for acceptance within the RPR Working Group. Cisco's implementation was based on a data switching architecture where resilient packet ring (RPR) is viewed as a feature of a router or a switch. This coalition's approach was to build products to provide optimized SONET circuits to service providers that allow any kind of traffic, including IP, to be carried over a ring.

The Gandalf Proposal

Named for the wizard in J.R.R. Tolkien's *The Lord of the Rings*, the Gandalf proposal was incompatible with Cisco's Spatial Reuse Protocol (SRP) and would require entirely new silicon, erasing any head-start advantage Cisco would have had with SRP. Cisco conceded on this issue, hoping to get the RPR standard back on track by eliminating the arguments over SRP. Cisco drafted Gandalf with 12 other companies, and realized that SRP wasn't going to become the 802.17 standard because at least 26 % of the vendors would never vote for SRP. The following companies also jumped onto the Cisco bandwagon: Riverstone Networks and several semiconductor companies such as Mindspeed Technologies, Broadcom, and Applied Micro Circuits. Startup Corrigent Systems also jumped on board with support for all or some of Cisco's proposal.

The Alladin Proposal

Startups, including Luminous and Lantern Communications, formed a coalition to block Cisco's effort, recruiting heavyweight Nortel to anchor their faction. The Aladdin camp preferred the steering method, where every node is notified of a line break and the packets are forwarded away from the break. Gandalf included some provision for steering, but was primarily geared toward wrapping. The Aladdin camp would preferred to have steering emphasized, and some members preferred to leave out wrapping altogether because it requires implementation at the silicon level. The Cisco camp believed it came up with the preferable option since its proposal would support both methods of protection switching.

Riverstone Networks' concern was that their customers were already asking for RPR. If the draft of the standard wasn't completed on time, the technology could lose credibility and customers would solve the problem using other technology.

The political controversy centered around the fact that Cisco's proposal was based on SRP, a solution that is already shipping on several different versions of Cisco switches and routers with over 13,000 ports deployed. The resentment from camp # 2 lies in the fact that some companies were worried that if Cisco pushed through its proposal with few changes, it would dominate the market and leave many of the smaller players behind.

Both sides remain optimistic that a single resilient packet ring (RPR) standard can be ratified in 2003 as originally planned. Part of the reason for the optimism is that the Gandalf and Aladdin proposals include some large concessions by both sides. Gandalf and Aladdin presented incompatible approaches, which forced the membership to choose one proposal or the other. The probable outcome will include elements from both Gandalf and Aladdin.

As the 802.17 working group mulls these kinds of debates, simulations will become key tools. One highlight of the January, 2002 meeting was simulations of the competing proposals. This gave the attendees a more concrete view of the differences and an assurance that the algorithms in question would work in line with the standard's goals.

Once the initial draft is completed, the rest is relatively easy. The draft will at least allow equipment manufacturers to build boxes that they know will conform to RPR, even though the final details aren't yet hammered out. This is evident in the standards development of 10 gigabit Ethernet, where silicon and systems were shipped in small quantities since late 2001 even though the formal (IEEE 802.3ae) standard wasn't complete until June, 2002.

Nortel Networks, Cisco and Luminous are among the companies with pre-standard RPR technology actually installed in live production networks. Many equipment vendors are already shipping pre-standard RPR gear. Vendors building RPR-based OEPPs include Luminous Networks and Lantern Communications. Nortel Networks also has an RPR approach through its OPTera Packet Edge System (the OPTera Metro 3500).

The RPR Compromise: The Darwin Proposal

The competing Gandalf and Alladin camps in the RPR standards group crafted a compromise proposal - just in time for the group's meeting in late January, 2002. The IEEE-802.17 Working Group appeared to be split 50-50 between the two camps, leaving neither side with the 75 percent "supermajority" needed for ratification. This was the case for months, as Cisco's original proposal stood head-to-head against the competition.

The compromise, the so-called "Darwin" proposal, has been posted on the Web page of the IEEE 802.17 Working Group. Darwin attempts to bridge the gaps between the competing Gandalf and Aladdin proposals for RPR that were presented at the 802.17 meeting in November, 2001. While it won't necessarily become the 802.17 standard, Darwin presents the compromise that RPR participants felt was inevitable once the Gandalf-Aladdin split formed in 2001.

Darwin forged compromises in the areas of protection and bandwidth management. Darwin would make steering a mandatory part of the RPR standard, with wrapping available as an option. This gives neither faction what it wants, which is usually the case in compromise situations. Gandalf makes wrapping mandatory with steering as an option. Conversely, Aladdin makes steering mandatory but left out wrapping entirely.

On the bandwidth management front, the Darwin proposal assigns unused bandwidth to subscriber connections in a "provisioned unfairness scheme," giving a larger share of bandwidth to users who paid more for connectivity. The alternative was to distribute the spare bandwidth evenly among all users, as Ethernet does.

The Darwin concept appears to be satisfactory to both camps. A compromise such as Darwin was considered inevitable by most RPR participants, especially since Gandalf and Aladdin already represented softened versions of the opposing stances. While the RPR tussle is admittedly dramatic, IEEE veterans say the contentious nature of RPR standard development is business as usual for a standard-setting process.

Vendors promote RPR technology as bridging the worlds of SONET and Ethernet and bringing the best features of both technologies to carriers. RPR marries Ethernet's ability to efficiently handle IP data traffic with SONET's sub-50ms protection and the ability to handle voice traffic. By mirroring key SONET features, RPR vendors hope to sell their Ethernet products for both data and voice applications. However, the downside of the RPR approach is that re-creating SONET functionality adds significant cost to the equipment, making it significantly more expensive than enterprise Ethernet solutions. For example, recreating SONET's strict timing would require a Stratum clock in every central office and these clocks cost $50,000-$100,000 apiece.

The Yankee Group believes that by the end of 2003, all of the major Ethernet switch vendors addressing the carrier market will embrace RPR as a method for offering SONET-like restoration and deterministic QoS to IP networks.

Market acceptance of RPR techniques for handling bread-and-butter circuit services will be slow because RPR equipment vendors will need to extensively prove to incumbent service providers that their approach is a viable alternative to SONET. But RPR will gain traction with future greenfield players who want to offer Ethernet data services with some level of reliable support for voice traffic. Thus in the near term, pure RPR products will command a share of greenfield dollars for optical Ethernet infrastructure but few dollars from incumbent carriers. This will only change if and when RPR proves itself useful for transport of all types of traffic. Incumbents may then see the value of RPR and slowly deploy it in their networks.

RPR development is one of the biggest network technology developments underway in the early 21st century. It's the technology that could have the most impact on cementing GigE's place in enterprise and carrier metro networks for many years to come.

Paul is a Product Manager, Business Marketing, Optical Data Networks, SBC. He teaches at DePaul University and can be contacted at paul.a.bedell@msg.ameritech.com.
The opinions expressed in this article are not necessarily those of SBC.

This article is an excerpt from his upcoming book, "Gigabit Ethernet For Metro Area Networks", to be published by McGraw-Hill in November, 2002. It will be available at Amazon.com; Borders; Barnes and Nobles and other major bookstores.

"Call-in-One"

Integrated Voice Mail Introduced

SBC recently announced a new integrated voice mail service with Cingular Wireless in California designed to serve consumers using both wireless and wireline phone services with a single way to stay connected. Plans call for the service to be introduced in SBC's Southwestern Bell and Ameritech regions over the next several months.

"Call-in-One" service enables customers using both an SBC Pacific Bell business or residential phone and Cingular services to access and retrieve their messages by combining messages from both phones on a single voice mail box. For a nominal monthly charge, they also can choose to be notified via pager when messages arrive in their "Call-in-One" mailbox. This new service follows a recent partnership between SBC & Cingular to offer customers the option to add discounted wireless service from Cingular with a single bill from SBC. Contact your Liaison Manager to learn more about this exciting offer.

DATA WITH DAVID


Tom David

January's *Data with David* featured an article on how a new SBC Pacific Bell optical product, point-to-point Multi-Service Optical Network, would be introduced to meet customers' increased bandwidth requirements. The California Public Utilities Commission (CPUC) approved this new service in May 2002 that allows for optical point-to-point transport between dedicated customer locations. As an enhancement to this service we plan to introduce a ring topology in 2003 that will be offered across SBC's 13-state region based upon regulatory approval in each state.

As a refresher, Multi-Service Optical Networks use Dense Wavelength Division Multiplexing (DWDM) capable of transmitting data at speeds of up to 2.488 Gbp/s on an optical wavelength. What's significant is that a single fiber may carry up to 32 optical signals and this results in tremendous data carrying capability. Ultimately, a MON system can carry up to 80 Gbps protected or 160 Gbps unprotected. Additionally, SBC's MON solution supports over a dozen different protocols and this allows customers to take full advantage of high-bandwidth services without expensive protocol conversion.

MON Ring Service

SBC's Multi-service Optical Network (MON) Ring service will offer a high-end migration path to high-speed IntraLATA bandwidth that is bit-rate and protocol independent. This service is designed for corporate enterprise customers who use multiple protocols (e.g., ESCON, SONET, Gigabit Ethernet) and have more than two locations requiring connectivity.

In today's operating environment, most large enterprise customers use several data interfaces that are being transported over a variety of networks. SBC's MON Ring will allow customers to combine their multiple data signals so they may be transported over one network. It affords these customers the ability to maintain a simpler, more efficient network that simplifies adding circuits in the future by pre-defining future circuit types on currently installed shelves. This offers scalability and flexibility by allowing customers to add pre-defined circuits, e.g., SONET up to OC48, Gigabit Ethernet, Fast Ethernet, Fibre Channel, ECSON, FICON, or D1 Video.

SBC's MON Ring will be offered in two configurations. Customers can purchase a MON Ring with growth up to 16 wavelengths or up to 32 wavelengths. Two types of nodes are available: central office and customer premise site. Customer data interfaces are offered as universal ports. These are capable of supporting a variety of speeds up to OC192 or 10 Gbp/s Ethernet with WAN-PHY.

Data Services Supported by MON Ring

The MON Ring wavelengths can be lit to carry the following data services to each port on the node of the ring:

- Dedicated SONET (155 Mbp/s to 2.488 Gbp/s and 10 Gbp/s OC192): A custom synchronous optical network that connects multiple customer designated locations at OC-3/3c, OC-12/12c, OC48/48c and OC-192 rate levels
- Gigabit Ethernet (1250 Mbp/s): A data transmission at the rate of 1 Gbp/s
- Fast Ethernet (125 Mbp/s): A version of Ethernet, which allows data transmission rates of 100 Mbp/s. Also called 100BaseFX.
- 10-Gigabit Ethernet with WAN-PHY interfaces. This service is a 10 Gigabit Ethernet service with a WAN-PHY only interface.
- FIBRE Channel (1062 Mbp/s): Allows for Storage Area Networks (SANs) to rationalize storage architecture. SANs offload storage requirements from local area networks onto a separate storage network and will allow storage devices of varying types to coexist on the same network. (See April 2002 ***Update*** for more information on SBC's SAN solutions). FIBRE channel is a new industry standard that will displace ESCON/FICON.
- ESCON (200 Mbp/s): Enterprise Systems Connection. A duplex optical connection used for computer-to-computer data exchange. ESCON is the most common communications protocol used by mainframes networked with other mainframes and storage devices. Virtually all mainframe architectures, including the market dominant IBM-compatible System 390 platform, utilize ESCON protocol (200 Mbp/s) for connectivity among host processors and storage devices.
- FICON (1.062 Mbp/s): A higher-speed evolution of ESCON, enabling 1 Gbp/s connectivity among mainframes, storage devices and peripherals. 1 FICON = 8 ESCON.
- D1 Video (270 Mbp/s): Uncompressed digital video
- ETR (up to 16 Mbps): External Time Reference/Control Link Oscillator (Sysplex Timer) provides timing synchronization to all elements of the network.
- ISC (1.0625 Gbps): Inter-System Coupling. It is high-speed, fiber-optic, control link in a Parallel Sysplex Environment.

LAN PHY vs. WAN PHY

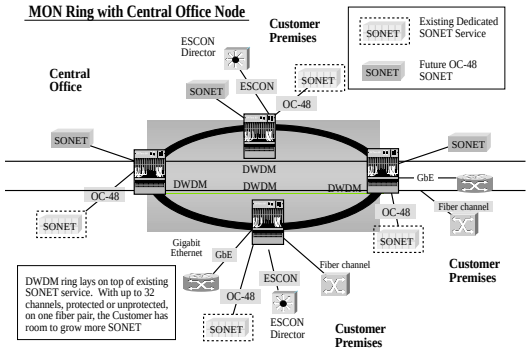
The 802.3ae standard defines two OSI Layer 1 (Physical) specifications: a LAN PHY and a WAN PHY. The LAN PHY was primarily adopted to support legacy and dark fiber, whereas the WAN PHY was adopted to support the installed SONET/SDH infrastructure. Both are being adopted to enable unification of the LAN, MAN, and WAN (Source: Nortel Networks, January 2001). The 10 Gigabit Ethernet LAN PHY is intended to support existing Gigabit Ethernet applications at ten times the bandwidth with the most cost-effective solution. SBC plans to offer a 10-Gigabit Ethernet point-to-point service with a LAN-PHY interface in the future. Over time, it is expected that the LAN PHY may be used in pure optical switching environments extending over all WAN distances. However, for compatibility with the existing WAN network, the 10 Gigabit Ethernet WAN PHY supports connections to existing and future installations of SONET/SDH circuit-switched telephony access equipment. The WAN PHY differs from the LAN PHY by including a simplified SONET/SDH framer in the WAN Interface Sublayer. The WAN PHY is described as "SONET friendly" although it is not fully compliant to all of the SONET standards. Some SONET features are to be implemented: the OC-192 link speed, the use of SONET framing, and some overhead processing. The more costly attributes of SONET, TDM support, performance requirements, and management requirements, will not be integrated. Partial compliance was desired to enable low-cost WAN PHY implementations.

Performance and Protection

MON Ring architecture increases network survivability by protecting at the optical layer. Customers may choose which wavelengths need to be protected and which should run unprotected. Some compatible customer payloads, with built-in protocol that facilitates protection switching, can be provisioned on two unprotected connections. For example, the SONET layer would provide protection for SONET traffic. For payloads without built-in protection switching capabilities, such as Gigabit Ethernet, ESCON, and Fibre Channel, the customer can choose to enhance the quality of service by enabling protection switching on the MON Ring. The MON Ring offers internal end to end performance monitoring by SBC. All traffic is monitored in terms of alarms, and only SONET traffic will be monitored for performance. SBC would provide 24 X 7 monitoring and performance management for the MON Ring.

continued from page 10

Below is a diagram showing how the MON Ring could be configured with a Central Office (CO) node. The MON Ring could also substitute an optical amplifier in lieu of the CO node.



Summary

Customers that need high transmission speeds, increased bandwidth capacity, in-service network changes, equipment and network redundancy, and protocol and bit-rate independence can use Multi-service Optical Networking to meet their needs. High-end customer applications for this service include data center mirroring, mainframe to mainframe connectivity, data center disaster recovery and Storage Area Networks. Service today is offered through point-to-point MON and in 2003 offered in a ring architecture that will afford greater flexibility and route survivability.

-- Tom David, Liaison Manager
td1898@sbc.com

Web Watch

By Paul Bedell

Here's a cool site for all you cool cats out there: Marshall Brain's www.howstuffworks.com.

This awesome web site has tutorials on - you guessed it - how stuff works. For all you curious people, or just those who like to learn how things work, this is the web version of the little kid who liked to take things apart "just to see what's inside". (Naturally, most times the darn kid couldn't figure out how to put the thing back together again).

On the left side of the home page is a listing of "supercategories" such as "Science and Technology", "Money", "Toys and Games", "Engines", "Transportation", "Cool Stuff", "Electronics", "Body and Health", etc. You get the idea. Like any web site, these supercategories have their own subsets of categories and menu items so you can drill down to the information or topic you'd like to learn about. The site even offers books on "how stuff works".

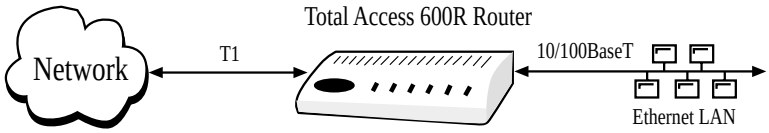
There's even a free newsletter you can subscribe to from this site. There's a "Top 40" listing, a suggestion box, "daily stuff", "what's new" and of course Forums.

You may not become the next Henry Ford or Steve Jobs by reading this site, but hey, ya never know…. Surf, and enjoy !!

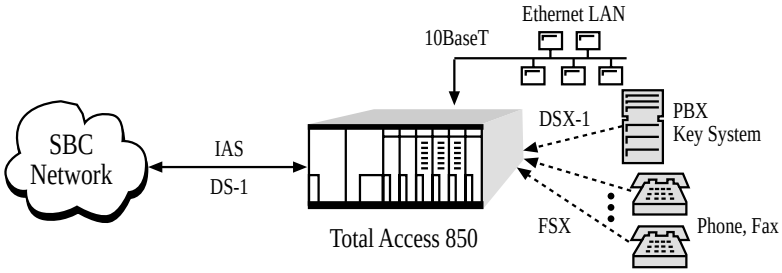
SBC Business Marketing Announces New Access Routing and Integrated Access Packages Featuring ADTRAN Total Access CPE

Now SBC T1 customers can choose new WAN access solutions for data and integrated data and voice applications. These new choices are:

T1 Access Router Package, for pure data applications



Integrated Access Service, for combining voice, data, internet access and long distance over a single T1



Both packages feature ADTRAN Total Access equipment and are fully supported by SBC PremierSERV ensuring world class, single point of contact service from SBC DataComm.

The equipment packages that compliment SBC T1 services have been aggressively priced and bring new, lower price points to the T1 access market making SBC solutions more competitive and more affordable than ever before.

More information about these T1 packages and SBC PremierSERV is available from your Liason Manager.

511 in Bay Area

SBC Pacific Bell announces the availability of 511 in the San Francisco Bay Area. Callers dialing the 511 number will reach the Metropolitan Transportation Commission (MTC) system that will provide Traffic and Transportation related information.

511 is an abbreviated dialing code that was nationally reserved by the FCC in July, 2000. Since that time, SBC Pacific Bell has been developing this service and is pleased to inform the public that 511 is available in the nine-county Bay Area. Through a partnership with MTC, callers dialing the 511 abbreviated dialing code will be able to access traffic and transportation information. In October, MTC plans to announce significant improvements to the existing service. In anticipation of this announcement, and to facilitate access to the service, please notify your customers as soon as possible.

At this time the call is free to the calling party. To make this service accessible from a PBX, Dialing Plan Key System, or changes of Centrex station dialing restrictions, customers will need to reprogram their systems to accept the 511 dialing code to access this valuable service.

Implementation of the dialing code will be by local and/or state transportation agencies. Once implemented, each agency is responsible for advertising the availability of this service as well as the information provided to the general public. If a call to 511 is placed in a geographic area where 511 has not been implemented, the caller will be routed to a vacant code message.

If you have questions or need more information about 511, please contact your Liaison Manager at 800-552-5299.

-- Lowayne Shieh, Liaison Manager
ls1869@sbc.com

John Bianchi, SBC Executive Briefing Centers

Pre-Call Preparation

The Second Element in Successful Videoconferencing


John Bianchi

A videoconferencing system can be an incredibly valuable and effective tool. It can reduce expenses while increasing productivity. It can open new markets and retain current customers.

On the other hand, it can sit in the closet, rolled out every once-in-a-while to be used as a $30,000 VCR/TV combo. What's going to make the difference? A track record of success. New users must have a positive, effective, successful experience on their first several calls or they lose trust in the technology. It can take a long time to win them back. *As a telecommunications consultant, you can help ensure such positive, effective experiences for your new users.*

And there are a great many new users. Why? Price.

Videoconferencing was once the stuff of cartoons like the Jetsons and Dick Tracy. In the real world, until the mid '90s, only the heads of large corporations or government agencies could afford the low-to-mid-6-figure price tag that went along with every video room.

By the mid '90s, though it was still possible to spend much more, high-quality room systems had reached the $40K-to-$80K range. Naturally, new markets opened up within this new level of affordability. Distance learning in particular, in both the corporate and academic worlds, really took hold during this period.

The next video/value revolution took place in 1998. Pleasanton, California-based Polycom Inc. brought room-system quality videoconferencing down to the $10K-$20K with their ViewStation product line. Other makers soon followed suit.

As the prices have fallen, the technology has matured. Video systems are cheaper, and also smaller, more reliable and easier to use. The result is more users getting their first look.

So, how do we ensure that the first call – every call – is a success? Ninety percent of the battle can be won by focusing on three basic elements:

- Choosing the right technology
- Pre-call preparation, planning and testing
- Effective during-the-call techniques

In this column, we will focus on the second element: Pre-Call Preparation.

Videoconferencing works only if it makes the 'meeting' as effective as it would have been had the participants met face-to-face.

Keeping that goal in mind, we are aiming to replicate the face-to-face, all-in-one-place experience. Problems with the Video system obviously detract from if not derail that goal. Pre-call prep greatly lessens the chances of such show-stopping problems.

Here is a brief Pre-Call Prep Checklist for a point-to-point (2 locations) call:

Pre-Call Prep Checklist:

- Trade information between the "technical" contacts at each end.
  - Name of primary and back-up contacts.
  - Telephone numbers at their desks.
  - Wireless numbers (Cellular, PCS)
  - Telephone number of voice line in video room.
- Reserve the room and video system.
  - The desired time of the call plus (at least) a half-hour before and after. Plus…
  - Test call one week prior to the meeting.
  - Test call the day before the meeting (consider this a sleep aid!)
- Video system information
  - Dial-in number
  - System Make and Model.
  - Connection speed (128K? 336K? 384K? etc.)
  - Back-up system? Get same info if available.
- Set up your own room and system
  - Save pre-set camera positions. Make a chart for the participants.
  - Position microphone(s)
  - Peripheral equipment
  - Document camera
  - Computer/Scan Converter
  - VCR
- Make your test calls.
- Practice

Now, a little more detail on the checklist:

Technical Contact

Throughout the testing process, and even more so when problems arise during the meeting, it's a great comfort to have contact with a technical person at the other end, especially if that person has a phone within reach of the video unit. That way, you can talk each other through troubleshooting with minimal awareness on the part of the meeting's participants. Try to get both a primary and secondary contact.

If you're lucky, the far-end contact will have much experience with the system. However, even a willing neophyte is better than no contact at all. If things go wrong, get on the phone! It can be confusing and frustrating trying to solve a problem when you don't know what's happening at the far end.

Reserve the Room

With the growing popularity of roll-about systems, it's important to reserve both the video unit and the room it will be in.

You will want to reserve the day of the meeting as well as the test calls.

The meeting day reservation should include a half hour or more before the scheduled meeting start – more time if this is not a frequently made connection with a proven track record. Also, add time at the end in case the meeting runs long.

Once the successful connection is made, leave it up! Many videoconferences have bombed because of connection problems even though multiple test calls went fine.

As for test calls, you will sleep better if you make a successful test call the day before the meeting. Finally, if this is a first-time connection, make a test call at the earliest opportunity. Wouldn't you rather have a week or two to resolve a network problem than, say, 24 hours?

Video System Information

The minimum information required here is the "phone" number you will dial to connect your video system to the far end. Even if they will be calling you, have this information handy. Sometimes, problems can be solved just by changing the caller to the callee.

For example, an unresolved network problem at one site limits outgoing calls to 56KBPS per channel, so a six-channel call gives us a total bandwidth of 336KBPS. Incoming calls can be received at 64K, or 384K total. The result is better motion handling, improved sound – a better user experience.

Speaking of connection speed, the latest technologies have all but eliminated the need to pre-negotiate the speed of the call. Newer systems can often adjust to each other when they do the "handshake" at the beginning of the call. Also, 384K is the de facto standard as it seems provide the best value in terms of quality and cost. Still, it's almost automatic to confirm the connection speed at the time the reservations are made.

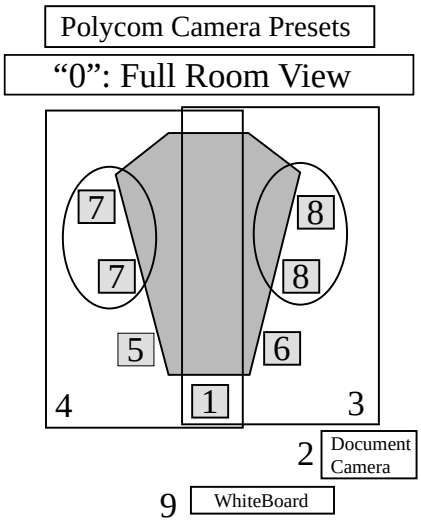
Get all the same information on any available back-up system. Include that system in your tests, if possible.

Room and System Set up

High-end video rooms will have much of their set up already done. Roll-about systems, however, mean that any room can be a video room. That means more set up considerations for every call. In this column, we'll assume that bigger issues such as system placement and lighting have already been addressed and we will focus on the per-call issues.

First, the microphone: If there is just one mic, plug it in and place it at least six to eight feet in front of the video system and as centrally located among the meetings participants as possible. If there are two or more mics, position them similarly, perhaps placing one closer to any "main" presenter.

Most room systems have the ability to memorize pre-set camera positions. Use of these presets is one of the most effective strategies for a successful videoconference. To promote their use, program your presets, then make a diagram of the room indicating the view of each preset. Here's one such diagram:



And here's a good rule-of-thumb on presets, specifically those that focus on just one person (like Preset #1 in the diagram.). Make like a scarecrow and put your arms straight out from your shoulders. The edges of the screen frame should cut between your wrists and your elbows. Any closer than that can be unnerving while any farther loses some of the face-to-face feel that we hope to get by using videoconferencing.

Next, test any peripheral equipment that may be used on the call. This may include a document camera, computer, VCR of…ahem…other device. Switch to each of these sources to be sure they are in working order.

Special note on computers: Some video systems may allow direct connection of the computer to the system via a monitor cable. Many, however, require a "scan converter" which takes the signal from the computer, which is designed to go to a computer monitor, and converts it to the lower resolution signal used by TVs, VCRs, etc. This is a common point of failure and problems, so be sure and test it.

And finally: practice! Many say that fear of public speaking is second only to fear of death. Fear of gadgets and technology has to make the top 10 or 20. Add use of high-tech gadgets to public speaking and you've got a pretty challenging situation. If at all possible, set up practice time for your presenters. Even one dress rehearsal can iron out many wrinkles and make the real thing more effective.

In one extraordinary instance, SBC Pacific Bell V.P. of Network Operations Norbert Rivera was to do a presentation to a major SoCal Newspaper. He came in early to practice and found that there was a five-to-ten second delay between his click of the mouse and when the slide in his presentation advanced. Knowing this, he clicked to advance to the next slide about one sentence before he was done speaking on the previous one. His presentation was flawless!

Again, this was extraordinary. Far more experienced presenters have been guilty of the pause-click-wait-speak method. Perhaps that's because, as experienced videoconferencers, they didn't think it necessary to practice. We can all learn from Mr. Rivera's fine example of how much more effective any meeting, and especially a videoconference can be with a little rehearsal.

In summary, applying these pre-call preparation steps can help avoid videoconferencing catastrophes and help ensure a positive user experience. By sharing this information with our clients, even before they buy a videoconferencing system, we establish ourselves as valued consultants and resources to be called on again as new applications arise.

John Bianchi, Briefing Center Manager in Sacramento, has worked 23 years at SBC Pacific Bell.

SBC Pacific Bell Executive Briefing Centers

SBC Pacific Bell Executive Briefing Centers:

- Sacramento, 2700 Watt Ave., Room 2092 John Bianchi, Manager
- San Francisco, 370 Third St., Room 100 Kevin Hurley, Manager
- San Ramon, 2600 Camino Ramon, Room 1CN70 Jay Ainworth
- Santa Clara, 1700 Space Park Drive, Room 200A Cam Ireland
- Los Angeles, 1010 Wilshire Blvd., Room 100, Rex Moyer
- Anaheim, 200 Center St. Promenade, Room 100, Jeff Weddle
- San Diego, 101 W. Broadway, Room 800, Gail Cadman

Contact your Liaison Manager for further information.

Spotting A Customer Need Speech Enabled Call Routing & Speech-Dial Directories

1. **Overloaded Operator Stations?** Check to see what percentage of calls coming in are internal in nature. To date, industry averages suggest the number is about 35% or higher. A packaged speech telephony application will divert these calls away from live operators and reduce or avoid incremental live call handling costs.
2. **Looking for cost reductions without compromising customer service levels?** Front end speech enabled call routing will transfer calls successfully while allowing callers to use their voice to control the call, 24 hours a day.
3. **Implementing a dial plan change?** Speech Dialed directors will eliminate the resource cost inherent in re-training the user population of the new dial plan.
4. **Adding Port capacity to an existing auto-attendant/voice mail system?** If any of the existing ports are used to support an auto-attendant application, research a packaged speech telephony solution. You may end up recommending a similar costing solution that delivers a much higher return.
5. **Triaging Calls into a Contact Center through Touch-Tone or live operators?** A packaging speeching telephony application can triage calls to the skills-based agent groups or to an IVR application through a voice user interface, all at costs that produce rapid ROI models and improved customer service levels

-- Larry Lisser
VP, Marketing & Sales, LocusDialog

SBC is an authorized distributor of the LocusDialog STS (Speech Telephony Systems)

DMV FRAUD HOTLINE

California Department of Motor Vehicle Driver License/Identification Fraud Hotline
To report identity theft of your DL/ID information, call toll free: 1-866-658-5758 or email DLFraud@dmv.ca.gov

Understanding IP Security

By Nehemiah Chriss, Security Engineer
Booz Allen Hamilton

Introduction

This article presents a practical view of Internet Protocol Security (IPSec), a protocol suite which protects data at the network layer. As the TCP/IP network layer provides 'end-to-end' connectivity, IPSec provides 'end-to-end' security in the following respects:

Confidentiality – IPSec provides mechanisms to ensure that data is exchanged in secret and the intended recipient is the only party that will be able to view data contents.

Integrity – IPSec is designed to detect tampering of data in transit between communicating parties.

Authentication – Using IPSec, the sending and receiving parties trust each other and the identity of both parties is known to the other.

Why IPSec

Shortcomings in the Internet Protocol Layer

IPSec addresses age old security challenges including:

Eavesdropping – active monitoring (man in the middle), passive monitoring (traffic sniffing).

Impersonation – the attacker masquerades as an end host and fields authentication and/or accepts data on its behalf (more commonly known as spoofing).

Message Delivery – replaying of recorded network packets against the authenticating end host allows the attacker to impersonate the client without having knowledge of the proper credentials.

Message Modification – extension of active monitoring. The attacker can modify messages in transit to their advantage.

These attacks are all possible due to the general lack of integrity inherent in TCP/IP. TCP/IP packets can be trivially forged, rewritten, or monitored. These shortcomings are due to the original primary focus of design for interconnectivity across the Internet: reliable transport, not security.

Throughout the life span of the Internet, the need for integrated security features has increased proportionately to increasing threats, resulting in the development of a number of protocol suites to ensure the security of data traveling over distrusted mediums. These include Secure Socket Layer (SSL) and Secure Shell (SSH), among others. Success, or wide-spread adoption of these protocols, is dependent on the flexibility of their implementations. Generally, SSL, SSH, and IPSec all do the same thing: protect data in transit and ensure confidential delivery, but IPSec allows for a more seamless and flexible integration because it is implemented at the lower layers.

How IPSec Works

IPSec Components

The IPSec protocol suite is in fact two separate protocols, employed alternately in combination or independent of each other depending on implementation requirements. In either case, the two protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP), take the form of additional headers and trailers in a common TCP/IP (or UDP/IP) packet.

AH provides a TCP/IP packet with data integrity, data source authentication, and protection against replay attacks. These features are effective for preventing the tampering of data in transit from the originating host to the receiving host. These features are not effective for keeping data confidential - the packet is sent in the clear and observable by any active or passive intermediary.

ESP also provides data integrity, data source authentication, protection against replay attacks as well as confidentiality. The payload of an ESP packet is encrypted using one of several predefined cipher transforms common in most modern security applications (DES, 3DES, AES, Blowfish, etc).

Given these two components of IPSec, one might wonder, "why the inclusion of two separate subordinate protocols with overlapping benefits." AH and ESP exist as two separate protocols primarily based on order of events. The protocols were originally designed by separate teams to solve similar security risks in the IP protocol suite. In simplified terms, use of both protocols is common and provides more robust security.

Security Associations

In a common network environment, a majority of the network traffic does not require end-to-end security. However, some traffic contains sensitive data that requires strong transport encryption and sender/receiver authentication. The Security Association (SA) is used to specify to the end system or security gateway when it needs to apply IPSec protocols and how to apply those protocols to outgoing or incoming traffic. Simply, an SA "consists of all the information needed to characterize and exchange protected communications."[1]

The SA functions not unlike the guest list at a popular establishment. There are those that are on a list (IPSec traffic) and receive some special form of treatment (secure connection), and there are common patrons (regular TCP/IP traffic) who wait in line to be allowed in as normal.

The SA is a granular identifier for these sensitive traffic flows and includes the use of a shared authentication key. To address issues associated with keying procedures, special protocols have been designed specifically for automated key generation and negotiation between IPSec-capable systems. These protocols have the capacity to establish SAs on the fly, given proper guidelines (policy).

Protocol Semantics

IPSec can be implemented on end systems (e.g., hosts) or on security gateways (e.g., routers or firewalls). As an extension of TCP/IP, IPSec protocol semantics largely involve the same transactions involved in IP protocol. An enabled IPSec device adds the proper AH or ESP protocol headers in accordance with a pre-defined SA. For the purposes of this article, protocol semantics can be separated in two categories which generally define the entities participating in the IPSec connection:

Transport Mode (Host to Host): Transport mode is typically used when end-to-end secure communication between two hosts is desired. When system A wants to communicate with system B privately, an SA is set up such that each host individually encrypts the payload of the upper layer protocols (i.e., TCP/UDP headers and payload), leaving the IP headers intact so that they can be appropriately routed across the Internet.

Tunnel Mode (Network to Network): Tunnel mode is typically used when end-to-end secure communication is required between two networks. Here, an SA is set up between two respective security gateways, qualified as any IP level gateway, router or firewall, such that hosts on subnets behind their respective gateways can communicate with their counterparts over an encrypted virtual tunnel. This to say, encryption does not originate on the hosts themselves (they send data in the clear and are functionally unaware of the encrypted link), but instead occurs only between the security gateways. At this level, the security gateways have encapsulated the entire original IP packet within another IP packet and an IPSec header is inserted between the outer and inner IP headers.

Conclusion

Because of its ability to establish secure remote access, currently Virtual Private Networks (VPN) are the most popular uses for IPSec. While IPSec was designed as a method of addressing security shortcomings of TCP/IP, its use on the end user level is gaining popularity for securing a variety of user application protocols. In addition to its primary base of router and firewall products, IPSec functions are being integrated more and more into consumer grade operating platforms. These platforms include common UNIX systems (Solaris, HP-UX, AIX) as well as the desktop (MacOS X, Windows 2000. For now though, IPSec provides the strongest network layer security solution, at least until the wide standardization and adoption of Internet Protocol version 6, a more security conscious overhaul of Internet Protocol version 4.

1 Frankel, Sheila. Demystifying the IPSec Puzzle. Artech House, Inc., 2001.

Jagdish Kohli, Ph.D.

Health Information Services

A sound mind in a physically sound body has been advocated as a healthy state of any human being. "Our health is in our own hands" signifies the importance of individual responsibility in managing ones own health. Because of the complexity of modern day living, it has become increasing difficult to discharge this individual responsibility without assistance from family, friends and healthcare professionals.

Jagdish Kohli

Many healthcare consumers continue to receive more education and an enhanced level of awareness from many sources of information. Recent developments in Web based sources of information easily provide instant answers to many questions that were extremely difficult a few years ago. With the development of Web, there has been an explosion of health-related available information and also misinformation. The sheer volume and the questionable quality of some information sources have caused chaos for many healthcare consumers and professionals alike.

In this article we explore the following aspects of evolving health information services:

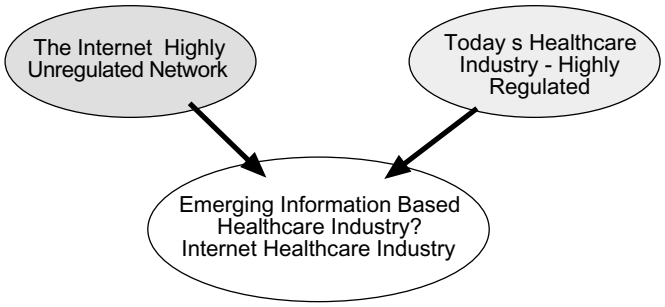
- Emerging Healthcare Industry
- Preventive Health Information Services
- Corrective Health Information Services
- Future Implications

Emerging Healthcare Industry

Many healthcare consumers continue to receive more education and an enhanced level of awareness from many sources of information. Recent developments in Web-based sources of information easily provide instant answers to many questions that was extremely difficult a few years ago. With the development of Web, there has been an explosion of health-related available information and also misinformation. The sheer volume and the questionable quality of some information sources have caused chaos for many healthcare consumers and professionals alike.

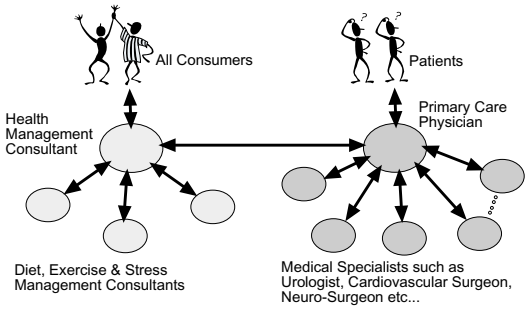
The Internet is a highly unregulated network and provides healthcare information with ease-of-access. Whereas the current healthcare industry is heavily regulated and there is a high degree of bureaucracy for even to get access to one's own personal healthcare records. The Internet is a powerful force and will bring unprecedented changes in the delivery of future healthcare services. Major healthcare stakeholders have recognized this paradigm shift and a beginning has been made towards a new "Internet healthcare industry". This merging of the Internet with current healthcare industry will continue in the coming years. The diagram below captures this major paradigm shift in the healthcare industry.

Paradigm Shift in Healthcare Industry

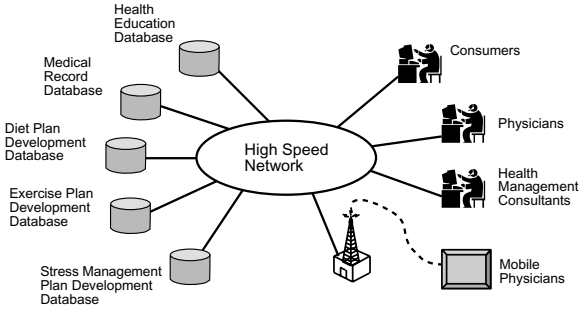


Preventive healthcare services need to be provided to all members of the society using interactive networking technologies. The availability of interactive technologies will also require a change in the structure of healthcare system. A consumer centric model for the delivery of information technology-based services as shown below.

A Consumer Centric Model for Healthcare Delivery



Under this arrangement, each consumer will have access to a health management consultant to stay healthy and access to a primary care physician during disease management. The health management consultant and physician will work closely with the consumer and other sub-specialists and bring the best care to the consumer. A high-speed communication network will provide the needed information to consumers, physicians, health management consultants, educators, nurses, administrators, researchers and pharmacists. A configuration of such a network is shown below. Wireless networking technologies will be important to access all online resources for people on the go.



A High Speed Health Information Network

Preventive Health Information Services

A family of preventive health information services can be designed using the power of the Internet. These services can be personalized based on individual needs by using adaptive artificial intelligent technologies. With some assistance from a health management consultant, this can become a very valuable and cost-effective resource to keep masses of people healthy.

The body of knowledge generated by alternative medicine research group should be used to train a new breed of healthcare professionals.

Table 1 (p. 17) lists a number of potential health information services along with implications for the healthcare providers. The role of information technology is also included in providing these services.

Table 1: Preventative Health Information Services

Service	Provider Implications	Information Technology Basis
Health Information Data Service	All healthcare providers need to provide basic online information to its members	Healthcare providers need to build or outsource secure preventative health information data repositories
Meal Plan Development Service	Healthcare providers and/or supermarkets need to provide an interactive database for creating personalized daily/weekly meal plans	This service will need an interactive online data repository with member profiles
Exercise Plan Development Service	Healthcare providers need to provide an interactive database for creating personalized and daily/weekly exercise plans	This service will need an interactive online data repository with member profiles
Alternative Medicine Information Service	Healthcare providers need to provide synthesized alternative medicine information to all its members	This service will need an online alternative medicine data repository
Health Education Service	Healthcare providers need to capture all current health education information for consumers and healthcare consultants	This service will need an online medical information repository

Corrective Health Information Services

A number of health information services can be provided for people with disease using the information technology. Such an approach will involve patients in the recovery process and fully use all relevant supporting technology resources. Even patients with similar disease diagnosis such as breast cancer can form their own support group to share information. The Internet chat service can be used to keep these and other similar groups together during the recovery process. Examples of a number of corrective health information services are given in Table 2.

Table 2: Corrective Health Information Services

Service	Provider Implications	Information Technology Basis
Clinical Patient Record Data Service	All healthcare providers need to provide basic online information to its members	Healthcare providers need to build or outsource secure clinical health information data repositories
Disease Management Data Service	Healthcare providers need to provide an interactive database to physicians for creating personalized medication exercise and meal plans	This service will need an interactive online data repository with member profiles
Online Prescription Service	Healthcare providers need to provide a service to physicians to use personal computers for writing drug prescriptions	This service will need an email access to the customer selected pharmacy
New Drugs and Treatment Service	Healthcare providers need to provide the information to all affected physicians	This service will need an online new medicine and treatment data repository
Medical Education Service	Healthcare providers need to capture all medical education for physicians and heathcare consultants	This service will need an online medical information repository

Future Implications

The information technology is well positioned to transform the current healthcare industry in the coming years and decades. Examples of some of ways the healthcare would be delivered include:

- Computer aided diagnosis and treatment
- Cradle to grave medical information based treatment
- Adaptive artificial intelligence based meal and exercise personalized plans
- Holistic mind & body healing
- Virtual doctor home visits
- Personal health management consultant

The Internet and general advertising media will also become a source of lot of healthcare misinformation. Many con artists will craft schemes and do false advertisement on unproved medications or treatments. Many will make quick bucks and get out while some will be caught of fraudulent schemes and punished accordingly to the law. An informed healthcare consumer is the best defense for not being cheated while the new healthcare industry matures.

Over the past centuries, average life expectancy has been improving and this will impact the delivery of healthcare for older citizens in the coming years. A historical perspective of increasing life expectancy is captured in Table 3. During the last 150 years, average life expectancy has almost doubled.

Table 3: Average Life Expectancy

Date	Years
Prehistoric Times	20
Roman Empire 0 A.D.	30
1870 (USA)	40
1915	50
1930	60
1955	70
1992	75.8
1997	76
2000 (Estimated)	80

Healthcare has reached well over a trillion-dollar industry in US alone. In 2000 America spent $131.9 Billion on prescription drugs. A major part of this occurred in the elderly population. With the increased expected average life expectancy, we must get prepared to spend much more on medicines just to keep our elderly healthy. To adopt good dietary intake, exercise and stress management habits during early years of life is extremely important for all people in order to reduce health management expenses during later years of life.

Our mind & body health is the most valuable wealth we posses. Let's manage this life's precious resource wisely!

Jagdish Kohli has worked on a number of information technology projects during the past 20 years. He can be reached at jagdish_kohli@yahoo.com His contributions in the area of remote medical imaging, medical data repository and medical communications are published in reputable publications.

The Hidden Power of Voice Mail

By Chris Horne, Project Manager
Pinnacle Bay Resource Group, Inc.

In my many years in the Telecom Industry, I have seen dramatic technology changes. I believe one the most significant was the introduction of voice mail. Sadly, in many businesses, this powerful technology is not being used to its fullest potential. Most voice mail systems were installed many years ago. While employees were given one-time, basic training on features and functions, and perhaps received a user guide, no recurring or follow up training has been provided.

In the years since then, no one has instructed the staff on how to properly and effectively use the real power of voice mail—the lesser-known features such as reply, copy, playback controls and group messaging. New employees are required to figure out how to use the phone and voice mail features on their own, through trial and error (mostly error!), or at best, through a 5-minute "training" session by a co-worker who doesn't really understand the system either. The company's voice mail policy and voice mail etiquette may never be discussed at all.

Eventually, no one on staff knows or understands the many time-saving features and capabilities of the voice mail system. Instead, this powerful business tool has become a source of aggravation to employees and customers alike. With minimal effort and investment that aggravation can be quickly transformed into more productive employees and happier customers.

For starters, if your system is more than a few years old, conduct a thorough training session for all staff. Include training on the lesser-known or advanced features and be sure to include recommended greetings and any company policy. Annually thereafter, conduct refresher classes for all employees on voice mail, phones and any other technology that is not being used to its fullest extent.

When new employees come on board, consider providing individual training as part of their orientation program. This can be done in a variety of ways, such as using training videos provided by your telecom equipment vendor, using your own properly trained personnel or hiring a qualified telecommunications trainer.

Three major benefits of voice mail training or re-training are: 1. Increased productivity of your employees, 2. Re-enforcement of the company's policy regarding voice mail etiquette, 3. The opportunity to better serve your customers.

Giving each voice mail user an understanding of how the features work, and how those features can be applied in their business, leads to improved productivity and increased morale. Happier, well-trained employees help improve customer satisfaction and retention.

Some of the more productive features of voice mail that should be addressed during a training session are:

How to "rewind" a message. Employees will often replay all or part of a message several times to attain all the information it contains. By using the "rewind" or "fast forward" feature, your employees will ease their frustration by hearing only what they need. The "pause" allows time to take notes.

How to "reply" and "copy" a message. Reply and Copy features enable users to reply to messages (from same-system users) without the need to call them on the phone. The reply can go to more than one person. Forwarding messages to additional people enables the user to be more productive and reduce the likelihood of errors from misinterpretation of messages. Many people think only e-mail offers these features, but in reality voice mail has offered this convenience long before e-mail was the ubiquitous tool it now is.

How to "Tag" a message. "Tagging" a message is a feature only a few know about. Those that do, may only use the "urgent" option. However, there are other tags that can be very useful. These include "future delivery", used sometimes as a tool to remind yourself of important dates or meetings, "receipt notification", where you are notified when a message that you sent was received or opened, and "private delivery", which denies the recipient the ability to forward the message to other voice mail users.

So far, we've focused on the features of voice mail. Now, let's talk about user "programming" issues. One training tool that is common to most voice mail systems is something referred to as "the navigation map". This is a chart showing which buttons to push to access all the features of the system. It is intended to be a quick reference guide for employees. I like to make a joke in my training classes by referring to this chart as a "litany of convolution". An experienced trainer will point out the items on the navigation map that the user needs to follow for first time set-up of a new mailbox or re-programming an individual voice mailbox. Other items to be highlighted include changing the default password to a secure one, scripting and recording greetings and setting up and use of group distribution lists.

If the company does not have a policy regarding voice mail etiquette, consider getting one. Use of professional greetings that are consistent throughout the organization is a good place to start. Giving examples of acceptable greetings in the training session is advisable. Some companies require greetings to be updated daily and include alternate numbers, such as cell phones or pagers where the employee can be reached if a matter is urgent. Callers like voice mail when they get a timely callback and hate it when they don't. Many companies mandate that calls must be returned within a certain timeframe. Above all, we should not hide behind voice mail; the caller's first choice is to speak with someone directly. So policy might say, "If you're available, answer your phone when it rings."

The proper and effective use of voice mail reaps benefits in increased productivity and employee satisfaction, but also leads to improved relationships with customers, which is ultimately reflected in the bottom line. With knowledge comes power, so get ready to unleash the power of your voice mail system, and see immediate improvements in employee morale and customer satisfaction.

Chris Horne is a Project Manager for Pinnacle Bay Resource Group, Inc., a vendor-independent telecommunications project management and consulting firm based in Sacramento. She assists the State of California and SBC Pacific Bell with numerous call processing, telephone and voice mail issues. Horne can be reached at info@pbrg.com The opinions expressed are not necessarily those of SBC Pacific Bell.

SBC Executives Certify Company Reports

On August 12, 2002, SBC filed with the Securities and Exchange Commission sworn statements by Chairman and Chief Executive Officer Ed Whitacre and Senior Executive Vice President and Chief Financial Officer Randall Stephenson attesting the SBC's most recent periodic reports filed with the Securities and Exchange Commission contain no untrue statements or omissions of material facts.

These certifications were filed pursuant to the Security and Exchange Commission's Order No 4-460, issued June 27, 2002, which requires the principal executive officers and principal financial officers of publicly traded companies with revenues during their last fiscal year of greater than $1.2 billion to sign and file these statements no later than August 14, 2002.

"Enthusiasm's Contagious. Spread it!"

-Update Tip for Success

National Strategy to Secure Cyberspace

A conference on "The National Strategy to Secure Cyberspace" recently took place at Stanford University. Participating were representatives from the President of the United States, the directors of both the FBI & Secret Service, and Business Leaders from such companies as Booz Allen Hamilton. Here is a summary from the conference. We will have more in our next issue of ***Update****.*

The first ever National Strategy to Secure Cyberspace responds to one of the most challenging aspects of the Information Age: securing shared systems. Because, cyberspace is not owned or operated by one person, group or entity, securing is a collective responsibility. In response to this unique challenge, the President's Critical Infrastructure Protection Board has created an interactive strategy that identifies 24 strategic goals and offers more than 80 recommendations on how America can make cyberspace more secure. The strategy is a road map to ensure the protection of information systems of critical infrastructures and the physical assets that support such systems. It supplements both the Homeland Security Strategy and the National Security Strategy and is designed to empower all Americans to secure their portions of cyberspace.

The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of information technology infrastructures. Our cyberspace security protection program must involve continuous efforts to secure information systems. Cybersecurity enables the economy, national security, and critical infrastructures. Protection of these information systems is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services.

A system originally designed to share unclassified research, the Internet is at the core of the information infrastructure we depend upon. Today, that same Internet connects into millions of computer networks, which, in turn, make most essential services work. While it has grown enormously and globally, it has also grown increasingly insecure. People in almost every country on the globe can access a network that is ultimately connected to networks that run critical functions in the United States, including transportation, aviation, utilities, banking and finance, etc.

Cyber attacks on U.S. information networks occur regularly and can have serious consequences, disrupting critical operations, causing loss of revenue and intellectual property, or loss of life. It is the policy of the United States to protect against disruptions of information systems for critical infrastructures. We must ensure that any disruptions of cyberspace are infrequent, of minimal duration, are manageable, and cause the least amount of damage. The implementation of this policy depends upon a voluntary public-private partnership, involving corporate and non governmental organizations. This strategy is the result of cooperation of thousands of people including those in the private sector, state and local governments, and supporting programs in corporate and academic organizations. To create this strategic roadmap, the owners of each major component of cyberspace have been developing their own plans for securing their portions of cyberspace. The overall strategic goal of the strategy is to empower all Americans to secure their portions of cyberspace. For this to be accomplished, each person and each organization must do their part. Some of those plans are already developed. Others will be added over time. Together they will reflect a national partnership between private sectors, government, and individuals to vigorously secure, maintain, and update the security of cyberspace.

In order to make this strategy easier to use, it is broken into five audience levels:

Level 1: Home User and Small Business
Level 2: Large Enterprises
Level 3: Sector, including Government, private industry, and higher education
Level 4: Nation issues and efforts
Level 5: Global issues

Empowerment will be accomplished through six major tools:

1. Awareness and information
2. Technology and tools
3. Training and education
4. Roles and partnerships
5. Federal leadership
6. Coordination and crisis management

In each section, the reader will find some or all of these themes reflected in two ways. First, the introduction to each section lays out strategic goals for that audience or level of strategy. Second, each section will highlight ongoing programs, recommendations, and topics for discussion that will serve to develop the strategic goals. These strategic goals include:

- **Home User/Small Business:** The strategic goal is to empower the home user and small business person to protect their cyberspace and prevent it from being used to attack others. Home users and small business collectively own/operate a vast amount of computing in America. These users face threats from the cyberspace and the insecurity of their systems put cyberspace at risk. The plan calls on home users and small business to recognize their role in protecting cyberspace and it also asks Internet service providers, vendors and retailers to consider how to make security computer systems easier.
- **Large Enterprises:** The strategic goal is to encourage and empower large enterprises to establish secure systems. The plan calls on industry to consider developing "best practices" for secure out-of-the-box shipping of software and asks the software industry to find ways to help users implement and install software in a secure fashion.
- **Federal Government:** The strategic goal is to significantly improve the security of Federal information and information technology. The plan highlights numerous recommendations that will improve the IT security of the federal government including: increasing accountability, expanding the use of automated security tools, explore the use of common access cards in the federal agencies, reduce the risk of wireless local area networks to Federal information systems.
- **Information Integration and Information Technology for Homeland Security**:
  - Create collaborative partnerships with State and local government and the private sector.
  - Ensure adoption of leading-edge information technologies as offensive weapons in the prevention and detection of terrorism.
  - Drive national and international information integration and information delivery standards.
  - Develop innovative service delivery models and business models that enable government to use information held outside the government arena.
- **State and Local Governments:** The strategic cybersecurity goals include achieving and maintaining the ability to protect critical information infrastructures from natural events and intentional acts that would significantly diminish State and local governments' capacity to maintain order and deliver essential public services. The White House Plan encourages States and Local governments to (1) participate in information sharing for cybersecurity, and (2) consider the benefits of scholarships for service as a means of attracting more IT security experts.
- **Institutions of Higher Education (IHE):** The strategic goals for universities, four-year colleges, community colleges in the United States is to adopt and implement a level of information system and network security to protect sensitive information, and to prevent its systems from being used for attacks on others.
- The overall strategic goal in implementing the **national priorities** is establishing foundations for securing cyberspace, including securing shared systems, fostering a reinforcing economic and social framework, and developing national plans and policy.
  - **Mechanisms of the Internet:** The strategic goal is to foster the development of secure and robust mechanisms that will enable the Internet to support the nation's needs now and in the future.
  - **Digital Control Systems/Supervisory Control and Data Acquisition (DCS/SCADA) Systems:** These systems facilitate the remote operation and management of energy, communications, transportation, water, and manufacturing and many other systems. The plan calls public-private effort to identify the most critical DCS systems and develop ways to

protect them by 2004. The strategic goal is to empower users to protect their cyberspace and prevent it from being used to disrupt the nation's critical infrastructure.

- **National Cyberspace R & D Agenda:** The strategic goal is to coordinate the development of technologies to counter threats, reduce vulnerabilities, and first a reliant, secure cyberspace for the future.
- **Highly Secure and Trustworthy Computing:** The strategic goal is to ensure that future components of the cyber infrastructure are built to be inherently secure and dependable for their users.
- **Securing Emerging Systems:** The strategic goal is to address vulnerabilities that emerging technologies are introducing in cyberspace and determine how to eliminate, mitigate or manage the potential risk of these vulnerabilities. Protocols, routers and switches are all highlighted as critical components that need to evolve and mature to ensure cyber space is secure for the future.
- **Vulnerability Remediation:** The strategic goal is to significantly improve the speed, coverage and effectiveness of remediation in the near term by improving tools, and practices, and in the longer term by reducing vulnerabilities at the source.
- **Awareness:** The strategic goal is to stimulate actions to secure cyberspace by creating an understanding at all audience levels of both cybersecurity issues and solutions.
- **Training and Education:** The strategic goals are: (1) develop and sustain well-trained highly skilled, domestic corps of information technology (IT) security professionals sufficient for the nation's growing needs, and (2) establish and maintain in the general population a basic proficiency in cybersecurity and cyber ethics.
- **Certification:** The strategic goal is to develop a national standard for certification of information technology security professionals that could ensure consistent and competent assessment and maintenance of IT systems and networks.
- **Information Sharing:** The strategic goal is to increase the voluntary sharing of information about cybersecurity between public and private sector entities, as well as among private sector entities.
- **Cybercrime:** The strategic goal is to prevent, deter, and significantly reduce cyber attacks by ensuring the identification of actual or attempted perpetrators followed by an appropriate government response, which in the case of cybercrime includes swift apprehension, appropriate sever punishment.
- **Market Forces:** The strategic goal is to stimulate and leverage market forces to promote and increase cybersecurity.
- **Privacy and Civil Liberties:** The strategic goal is to achieve security in cyberspace without infringing on individual privacy and civil liberties.
- **Analysis and Warning:** The strategic goal is to detect incidents at their earliest inception, to respond to them efficiently, and to the extent possible, predict them in advance. The plan calls for major ISP's, manufactures and experts in the private industry to consider creating a cyberspace network operations center (Cyber NOC). This center would be owned and operated by the private sector and would provide an important focal point for identifying and Internet attacks.
- **Continuity of Operations, Reconstitution and Recovery:** The strategic goal is to provide for a national plan for continuity of operations, recovery and reconstitution of services during a widespread outage of information technology systems in one or more sectors.
- **National Security:** The strategic goal is to improve our national security posture in cyberspace to limit the ability of adversaries to pressure the United States and quickly remove threats once identified.
- **Interdependencies and Physical Security:** The strategic goal is to mitigate the potential negative effects that the disruption of one infrastructure might have on another.
- **Global:** The strategic goals is to work with the international community to ensure the integrity of the global information networks that support critical U.S. economic and national security infrastructure.

The Federal Government will help facilitate the evolution of these discussions so that they become recommendations. Recommendations will, in turn, become ongoing programs once they gain the necessary support and approval. It is important to remember that the strategy is a "living" document on the web, updated as threats, vulnerabilities, and technologies change. It will include "hotlinks" to government and private sector sites offering more information on cyber security.

The Federal Government alone cannot secure cyberspace. Everyone must be responsible for the piece of cyberspace which they own or operate. This strategy is designed to provide tools and remove roadblocks so that we can all do our duty to secure parts of cyberspace and, thereby, protect our economy and national security.

Thank you for reading Update

SBC PACIFIC BELL CONSULTANT/VENDOR SALES GROUP

Toll-Free Hotline 1-(800) 552-5299
(For any other number, toll charges may apply.)

Vendor/Consultant Service Center – **1-800-773-3318**

Kari Watanabe	CVSG Vice President (415) 542-4516 e-mail: kw6875@sbc.com
Tom David	Liaison Manager (949) 855-5055 Fax: (949) 348-2941 e-mail: td1898@sbc.com 27402 Camino Capistrano Room 211, Laguna Niguel 92677 Helps Consultants and Vendors in the following area codes: 619, 714, 760, 858, 909, 949
Bree Ma	Liaison Manager (415) 542-1071 Fax: (415) 542-2648 e-mail: bm1254@sbc.com 370 Third Street, Room 711 San Francisco 94107 Helps Consultants and Vendors in the following area codes: 209, 408, 415, 510, 530, 559, 650,707, 831, 916, 925
Craig MacDonald	Editor/Communications/Seminars/Conferences (714) 284-2370 Fax: (714) 563-1736 e-mail: cm9816@sbc.com 200 Center Street Promenade, Room 100 Anaheim 92805
Lowayne Shieh	Liaison Manager (626) 576-3045 Fax (626) 576-5081 e-mail: ls1869@sbc.com 500 E. Main Street, Room 540 Alhambra 91801 Helps Consultants and Vendors in the following area codes: 213, 310, 323, 562, 626, 661, 805, 818
Eric Aguirre	Data Administrator e-mail: ea3515@sbc.com
Lonnie West	Graphic Designer, SBC Pacific Bell Graphic Arts e-mail: aw1497@sbc.com