SBC Pacific Bell

Consultant/Vendor

CVSG

Sales Group

Update Special Report

SOLUTIONS FOR SUCCESS & SECURITY

UPDATE - August 2002

Inside

A Taxing Situation

By Tom David

I have found one of the most confusing sections on my telephone bill to be the government-imposed charges for taxes and surcharges. Federal, State and Local entities collect taxes and surcharges have helped to support legislative programs. The details of how and why the monies are collected, I never quite understood. The following explanations may assist you in understanding your bill.

continued on page 10

Vault for Redundant Sonet Ring Readied in San Francisco's Mission Bay Development

The first of two Controlled Environmental Vaults that will provide a fully redundant SONET ring for the 5 million square feet of commercial space planned for Mission Bay is positioned under the supervision of SBC Pacific Bell Engineers Wailin Woo and Paul Lucq. Occupancy will begin later this Summer at the exciting property south of Pacific Bell Park. Mission Bay is a project of Catellus Urban Development Corporation. It also will feature 6,000 residential units and a UCSF technology campus on more than 300 acres. SBC Pacific Bell's Business SmartMoves has a Preferred Marketing Agreement with Catellus.

Chuck Smith is the new President/CEO of SBC Pacific Bell and SBC Nevada Bell. Smith, who joined Pacific Bell in 1967, was most recently President of Network Services.

U.S. Treasury Selects SBC

SBC Global Services will provide the U.S. Department of the Treasury and its bureaus with advanced business telephony solutions--from products to implementation--through a newly awarded blanket purchase agreement. The nationwide award, called the Treasury Telecommunications Solutions Blanket Purchase Agreement, was issued without a value cap and covers a 4 1/2-year term. The agreement is open to all bureaus of the U.S. Treasury, including the Internal Revenue Service, Alcohol Tobacco Firearms, Customs, Secret Service and the U.S. Mint. The US. Treasury will be able to choose from a host of Nortel Networks voice and data equipment and will also have their choice of ADTRAN and Alcatel data networking products, VTEL videoconferencing equipment and Veramark Technologies, Inc. call accounting and facilities management systems. As part of the agreement, SBC will provide network design, implementation and management support and will offer full maintenance for legacy equipment and new products.

"SBC meets all of our requirements for supporting the U.S. Treasury's infrastructure of legacy equipment while providing solutions on a nationwide basis," said Greg Jewell, Treasury Team Leader for the agreement. "We look forward to working with SBC and having access to voice and data solutions that will enable our IT infrastructures to operate efficiently."

July 31st Broadcast

9-11:30am PST

Long Distance & SBC Pacific Bell
Carrie Chikahisa,
Exec. Dir., DSL & LD Marketing

How CV Web Connects You to SBC Pacific Bell
Mark Esfehani, Technical Director

Web Office
Christine Hertzog, Regional Sales Director

ConferenceNOW®
Aaron Eichenlaub, National Sales Manager
1-800-CONFERENCE

SBC News
Kari Watanabe, CVSG Vice President

To find out how you can attend in person or as a streamer, call 1-888-889-6010. Thanks!

VICE PRESIDENT'S CORNER

Letters of Authorization/ Agency Protect You

Kari Watanabe
CVSG Vice President

We're so protective as a society today--with very good reason! You wouldn't want your Social Security Number, Credit Card and other Personal Information available for anyone to see. We strive to protect Personal Information on a corporate level with the Letters of Authorization/ Agency (LOA) process. With LOAs, we're abiding by Federal Regulations to ensure that Personal Information is protected. Since misunderstandings still occur about LOAs, I want to stress the importance of them to each of you. They're the Law, designed to protect you. You can refresh yourself on What's Permissable with LOAs, Requirements for Separate LOAs, What an LOA Must Contain plus much more by reviewing

continued on page 7

How to Reduce the Risk of Fraud

by Randy Wooten

Randy Wooten

Telephone fraud costs an estimated $4 billion each year, according to industry experts. As our communications become more high-tech, criminals find new and even more sophisticated ways to defraud the unsuspecting customer.

While popular belief is that older people are the most frequent targets of scam artists, people of all ages, income, education levels and lifestyles can be taken in by crafty crooks. All customers should be wary, especially business owners.

Evolution of Toll Fraud

Toll Fraud probably began with Collect Call Abuse and Third-Number Billing Abuse.

This type of fraud was not very sophisticated. Over time, more technical methods of committing Toll Fraud emerged. Devices known as "blue boxes," "red boxes," and others were developed that employed known technical attributes of the telephone network. Among other capabilities, these devices could emulate signals or simulate the deposits into pay telephones. Technological improvements have largely defeated these forms of Toll Fraud.

As telephone technology advanced, so did the capability of the *telephone fraudster*. A new breed of "techies" was born with a penchant for penetrating equipment and beating telephone systems. Originally referred to as "Phone Phreaks" or "Phreakers," these individuals were extremely adept at using technology and often characterized themselves as explorers or pioneers. The "Hackers," as they are more commonly referred to today, live for the thrill and challenge of learning to defeat telephone system security.

Today's hackers have been segmented into two groups, the hacker and the "cracker." Hacking activities have traditionally been viewed, by the telephone system owner, as a huge security threat. Some hackers have been hired to test system firewalls and prove in-house telephone system security. Crackers, on the other hand, are considered in a more mercenary light. Often, the cracker will penetrate the telephone system to steal long distance telephone service. If they can, the information is often published and/or sold to persons wishing to conduct an organized call-sell operation. This type of activity has also been linked to organized crime and the drug culture. The ability to "loop" around from telephone system to telephone system (i.e., Voice Mail or PBX) makes it difficult for law enforcement agencies to trace call activity and to determine the originator of the call. Bottom line, you or the owner of your telephone system may be responsible for any toll usage once your system is compromised.

One of the more common forms of Toll Fraud is through a feature found on most PBX systems—Direct Inward System Access (DISA), often referred to as remote access.

Remote access allows employees off premises to dial into your company's PBX and access all user capabilities, including long distance service usage.

Generally, employees use DISA to interact with your company extension or obtain access to less expensive long distance lines, such as tie lines and WATS (Wide Area Telecommunications Service) lines. The feature can be used with local telephone service but is more often used with 800 service.

After dialing the remote access number, employees receive a prompt to enter an access authorization code.

Long Distance thieves try to decipher authorization codes—the shorter and more predictable they are, the easier they can be compromised. If there are no dialing restrictions on a code, thieves can place an unlimited number of long distance telephone calls. Without proper audit trails, unauthorized calls can go unnoticed for months. If you own a PBX you should take the following actions to protect against toll fraud.

Evaluate the Need for Remote Access

The Remote Access Feature is the most vulnerable part of your system and for that reason each user should critically evaluate the necessity of even having remote access capability within its PBX. When making this decision, you should consider alternatives such as the use of Calling Cards, Prepaid Cards, and Remote Access functions with a Virtual Private Network (VPN).

Calling Cards and Prepaid Cards are good alternatives to remote access features because they enhance control over telecommunications expenses and significantly reduce the potential of telecom fraud. While sometimes slightly more expensive than a direct-dialed call, pricing plans have made them more competitive.

Another alternative is to consider replacing Remote Access capability in your PBX with a Virtual Private Network. With a VPN, a public switched network provides capabilities similar to those of a private dedicated network. When your employee places a long distance call, your company PBX recognizes the call as belonging to a VPN.

The PBX transports the call over a dedicated T-1 facility and the call is released to the public switched network at its remote destination. The advantages are enhanced security, monitoring, and call blocking made available by the VPN provider. In some cases, the VPN provider assigns and manages access authorization codes for the customer.

If the Remote Access feature is not used, it should be eliminated or blocked. If the feature is simply left inactive, hackers can penetrate your system and possibly activate it. Be sure to contact your equipment vendor and remove or block the DISA feature.

At a minimum, the system software must be modified and the system administrator capabilities must be protected to prevent remote access hacking.

If you must use Remote Access, then take the following steps to reduce your risks:

1. Use of Security Codes
Most PBXs will accept 10 to 18 digits—use as many as possible. The mathematics are simple. A 7-digit code provides 10 million possible combinations compared with a 4-digit code that provides 10 thousand possible combinations. The greater the number of digits, the greater the protection.

- Do not use telephone extension numbers, employee identification numbers, Social Security numbers, anniversaries, maiden names, or first names for access authorization codes or barrier codes.
- Do not allow employees to determine their own codes.
- Do not use group or department codes.
- Do have all codes randomly generated by the company's system administrator.
- Do assign each employee a separate, distinct code that is neither consecutive nor sequential.

2. Use Multiple Levels of Security
Use a barrier code—an additional code placed in front of the access authorization code—as a second level of protection.

3. Change and Deactivate Access Authorization and Barrier Codes
Change your access authorization codes and barrier codes every 60 to 90 days as a routine administrative function. They should also be changed after any employee leaves the business, including temporary employees and interns. Deactivate any codes that are not being used.

4. Do Not Publish Remote Access Numbers
Never publish remote access telephone numbers. And if possible, use these telephone numbers during normal business hours for other business functions—for example, for telemarketing or other work that dials out of the company.

5. Terminate Access After Second Invalid Barrier Code or Access Authorization Attempt
Do not allow unauthorized callers unlimited attempts at breaking the PBX barrier code or access authorization code. Modify your PBX software to terminate calls after two invalid attempts or transfer the call to a switchboard operator if one is available. An intercept by a live operator will often deter intruders. It also alerts operators of multiple attempts to access the system. These activities should be reported to your company's telecom manager at once.

6. Limit Remote Access During Non-Business Hours
Be sure to restrict or block the remote access capability during non-business hours by using the "time-of-day restriction" feature found in nearly all PBX software. If 24-hour remote access is required, use the "automatic route selection" feature to route all remote access calls to the switchboard operator—which can deter thieves. Plus, regularly revising verbal passwords can identify a caller as a legitimate employee of your business.

7. Limit Your Toll-Free Number
If you use toll-free service for remote access, limit that service to the geographical area your company really needs. If you do business only in the Western United States, don't purchase Eastern access. Another inexpensive defense against toll fraud is to include Call Detail Reports as part of your toll-free service. Then review usage patterns often to watch for signs of fraud. Call Detail Reports include the full 10 digits of the calling number and are provided as a free service. Also most telephones have features that will allow you to receive incoming calls only from selected area codes and/or specific prefixes.

8. Do Not Use Steady-State Dial Tone to Prompt Remote Access
Avoid using a steady-state dial tone as a remote access prompt. Thieves use automatic dialing programs to dial large blocks of telephone numbers. They record those numbers that give a remote access prompt, a modem prompt, or a VMS prompt. Use of a voice recording or silent prompt defeats the automatic dialing program. Most PBXs today can be reconfigured to provide this capability. Request that your vendor do so.

9. Use Ring Delay Option
Most automatic dialing programs automatically disconnect after the second or third ring and move onto another telephone number. Therefore, a ring delay option should be used on remote access lines to deter potential thieves. Usually this option is set for four or five rings before your PBX answers the call.

10. Restrict Individual Calling Capability
Assign restriction levels in your PBX based upon your employees' business needs. Few individuals need access to international long distance service. Most employees need access only to specific regions or specific states. Use alternate restriction levels on each access authorization code to restrict long distance calling during nonbusiness hours. If your PBX does not provide for this capability, you can use Centrex for your outgoing trunks. These trunks can then be equipped with features such as Toll Restriction and Network Class of Service Restrictions.

11. Toll-Restrict Outside Trunks and Station Lines
We strongly recommend that you restrict international calls and calls to the Caribbean, unless you routinely do business there.

With most PBXs, you can restrict all International Calls—and restrict calls to selected area codes. There are still two potential risks, however: (1) The PBX software might fail to implement the program change for any number of reasons; (2) An intruder or a dishonest staff member or technician could reverse the restriction. So be sure to test these restrictions often.

Take special care when restricting calls to the Caribbean, the destination for a high proportion of all fraudulent calls. Note that some locations within the area code, such as Puerto Rico, are not considered international. So simply blocking international calls is insufficient. Be sure to block Caribbean area codes specifically. In addition, restrict 10-1-XXX casual calling during nonbusiness hours. And if possible, restrict tandem trunk and outbound toll-free access during nonbusiness hours.

continued on page 6

Getting Value For Your Information Security Dollar

by Jerry Hinek, CISSP

Introduction

Jerry Hinek, CISSP
Corporate Information Security, SBC Services

Information Security is neither a panacea nor a product you can buy off the shelf. It's a process of business decisions, written policies and procedures, education and enforcement. How much to spend on security is a business decision. You have to weigh the cost of security against the risks of security vulnerabilities. Too little security may cost less in the short run, but your information assets are more vulnerable and the risk of loss in the long run is greater. Too much security means that you're probably not getting the best return for your security dollar investment. You may be spending more to protect an asset than it's replacement or recovery would cost — money that might be better used in other parts of your business. The information security policy is the expression of these business decisions; it will guide employees to make the best decisions when protecting corporate information.

Value Information Assets

Information is valuable, but it is not all equally valuable. A well-run business should not guard all its information with the same level of security. Your business may invest money to develop analyses of publicly available information. Those analyses may inform the development of the business plan and should be protected. The source information may not be worth guarding. Your business has to determine which information is worth the cost of security and how much security to provide. There are several factors to consider when deciding the value of information.

Competitive Value

A lot of information has competitive value. If a competing business or a potential competitor gained access to your information it might avoid the cost of developing or obtaining this information on its own. A competitor could use your information to steal your customers, or negotiate better deals with your suppliers. If your competitive information is compromised it can lose its value to you, your business could be harmed without your realizing it. You could still have all that information safely in a database or a file cabinet but your competition has become stronger at your expense.

Replacement Value

Information might become lost to your business. A disk drive crash or a malicious hacker could delete important files. Businesses have gone into bankruptcy because files destroyed by a disgruntled former employee were critical to day-to-day operations. If your business can't run without certain information then you should protect it like money. Even if you can survive the loss, you still have to think about the risks and how much to spend to mitigate those risks.

Legal Value

Corporations are required to keep certain financial information secret until it is released to the public. Early disclosure of this information could lead to insider trading that affects the stock price and could lead to fines, civil penalties or

News You Can Use

1-800-CONFERENCE® IS NOW PROUD TO INTRODUCE CONFERENCENOW® - An On-Demand Audio and Web Conferencing Service

ConferenceNOW, a 24x7 reservation-less audio conferencing service, now allows for reservation-less web conferencing capabilities. ConferenceNOW offers the convenience of delivering presentations via the web and conducting on-line meetings with 20 participants or less 24 hours a day, 7 days a week through one registration process. The presenter and participants can simply share presentations, spreadsheets, documents and web co-browsing while an audio conference is conducted.

ConferenceNOW, reservation-less audio and web conferencing is ideal for:

- Companies looking to improve their Disaster Recovery communications
- Training, product development and other project teams where ad hoc meetings occur frequently
- Organizations that have the need to share visual information during an audio call
- Executives who want the ease and efficiency of having their "own" conference bridge

1-800-CONFERENCE provides a complete set of global collaboration services – Audio, Video and Web Conferencing plus Web Streaming solutions. Video Conferencing equipment is also available.

In addition, 1-800-CONFERENCE is proud to sponsor and offer the streaming service for the SBC Pacific Bell CVSG streaming broadcast on July 31, 2002. Please contact 1-888-889-6010 for registration information.

For general information, please contact 1-800-CONFERENCE at 1-800-266-3373 or www.1800conference.com. Register for ConferenceNOW at: http://www.meetme.net/sbc/conferencenow/index.htm.

Long Distance Service, when applicable, is provided by certificated carriers through Conference Plus, Inc., and will be itemized separately on your bill. 1-800-CONFERENCE® and ConferenceNOW® are registered trademarks of Ameritech Corporation. The SBC logo is a trademark of SBC Communications Inc. Service provided by Ameritech Communications, Inc. (a subsidiary of SBC Communications Inc.) and Conference Plus, Inc.

-- Toni Warbyla, Associate Director, 1-800-CONFERENCE.

litigation for the corporation as well as criminal penalties for persons involved. Failure to do due diligence can be costly.

Time Value

The value of information can change. In a fast paced and competitive world a lot of information is only valuable if it's accessible and accurate when it's needed and loses its value if it's not available. It can seem expensive to spend money on system reliability but the cost to your business if critical information is unavailable can reflect right on the bottom line.

Information Classification

One of the first things to do is to develop a schema of information categories and guidelines so employees can know the relative value of information and how to safeguard it. Two obvious categories would be public information and most sensitive information. Those are the extremes in value; the majority of the business's information will be placed in an in-between category. Having one or two additional categories for the information between the extremes will give employees a schema that's easy enough to work with and robust enough to stimulate cost-effective information security. On the other hand, having too many categories adds complexity and cost and makes the system difficult to use. The classification categories and guidelines must be published to all people authorized to see and manage the company's information.

Write a Policy

Policy as Part of the Business Plan

Information Security will only succeed if it's able to support the business plan or to enable cost cutting. Management must create an information security policy that provides benefit to the company, both enabling the business plan to succeed and safeguarding the company's information assets. Employees trying to perform a task tend to see security as an obstacle to success. With management creating and endorsing the information security policy employees can understand that security is important to the well-being of the company.

The Information Security Policy

The company should both write and publish the information security policy. The policy should require employees to protect the company's information assets and state penalties for non-compliance. This policy is strategic rather than tactical. It should not bind the company to particular security solutions or to specific technologies. Those decisions can be made and re-evaluated periodically by organizations that write standards and guidelines to support the policy. For example the policy might require strong authentication to gain access to the most sensitive information, but it would not specify the mechanisms or forms of that authentication. The policy should be written so that it does not have to change regularly and it should be signed by the CEO or a high level officer or manager who reports to the CEO.

What Employees Must Do

A policy will mean nothing if employees don't execute it. The employees who have access to the company's information are the ones who have to protect that information. The policy must clearly define responsibilities and penalties for non-compliance.

What Systems Must Do

The company's information systems must also protect the company's information. The policy should require computers and networks to have adequate security mechanisms to protect the confidentiality, availability and integrity of company information.

What Management Must Do

Management is not the last or least important element in the policy. Management not only creates the policy, but must support it. The company's leadership must consider information security as part of the cost of doing business and as a mechanism that supports the development of new and more efficient ways to do business. The policy must make clear the commitment of management to information security.

Conclusion

A successful information security policy will integrate information security into the business plan as seamlessly as possible. A successful policy is based on sound valuation of information assets and appropriate resource allocation to safeguard them. It's difficult to quantify the success of information security. If information security works there's often nothing to show, but when it breaks down the need for better security is all too apparent. The benefits will only be seen in the continuing success of the company.

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

SBC Executive News

John Atterbury, Group President, is named Group President-Strategic Processes, responsible for improving and standardizing all strategic processes to take cost out of the business. He reports to **Ed Whitacre**, SBC Chairman and CEO. Reporting to Atterbury is **Jim Shelley**, Senior Vice President-Government Relations, who has been named Senior Vice President-Strategic Process Improvement.

Forrest Miller, President and CEO of SBC Southwestern Bell, is named President and CEO for Southwestern Bell, SBC SNET and SBC Telecom. He reports to **Stan Sigman**, Group President and Chief Operating Officer. Reporting to Miller are **Bill Blaze**, President and CEO of SBC SNET and **Tim Harden**, President of SBC Telecom. Miller, Blase and Harden are former Pacific Bell executives.

Denita Willoughby, Assistant Vice President, Business Solutions Team, has accepted the position of Regional Vice President--Healthcare. She reports to **Bob Campbell**, Sales Vice President-G.E.M.

Thom Matson, Sales Vice President, Valued Accounts, assumes leadership and responsibility for the Business Solutions Team. He reports to **Bob Ferguson**, President-BCS.

continued from page 3

For domestic long distance service, program your PBX to block calls to area codes where you do not do business. In addition, area codes or prefixes that result in charges, such as 900, 950, 976, and 700 should be blocked. And consider blocking, as appropriate, 10-1-XXX, "0+," "0–," and "00-" may be used to alternately bill calls like calling card or collect, since these may be used to circumvent other restrictions you have put in place.

In some cities, the capacity of the 976 exchange has been exceeded, and additional "976 look-a-like" exchanges are being used. Be sure to block these exchanges, too, because they play a primary role in pager toll fraud. In this form of fraud, thieves set up an information service with surcharge and leave the number on the pagers of your unsuspecting employees. Because 976 look-a-like numbers are not generally recognized as toll calls, the employees return the call—and your company is charged.

12. Evaluate the Need for Using the Call Forwarding Feature From Your PBX

Determine whether you really need to forward calls to your answering service during nonbusiness hours. Thieves can take advantage of this service and gain access to the long distance network.

13. Use Effective System Audit Trails

Effective audit trails that monitor PBX access and usage offer the first indicators that a PBX is experiencing toll fraud activity. By monitoring PBX traffic with Station Message Detail Recording (SMDR), Call Detail Reports from the toll-free service provider, and/or trunk activity reports generated by your PBX daily, PBX system administrators can help curtail toll fraud. System administrators should watch for:

- Multiple short-duration incoming calls and long-duration outgoing calls.
- PBX activity at off-peak hours such as evenings and weekends.
- International long distance calls.
- Multiple failed attempts to access your PBX or multiple calls to unusual locations.
- Unusual increases in toll-free line usage.
- High volume of calls from a particular number or geographic area.

Of all the system audit trail capabilities, the most responsive is online PBX call detail reporting on a near real-time basis. This approach allows employees to react immediately to any attempt to decipher codes or to unusual calling activity that normally indicates toll fraud. (This 24-hour-a-day, 7-day-a-week approach naturally involves a higher commitment of money and manpower.)

Another weapon for system administrators is the verification and validation of telephone bills. As bills are received they should be broken down and disbursed to the applicable divisions, branches, and work centers for management to review and verify. Calls that cannot be verified as business oriented can be returned to the PBX system administrator and subjected to a company investigation to determine the source of the call.

Despite Station Message Detail Recording (SMDR) and call accounting systems, many PBXs are not equipped to detect irregular activities. There are a number of PC or mainframe-based call accounting system software packages available. The cost can range from a few hundred dollars to over a hundred thousand dollars. These systems can decode SMDR data and produce reports on incoming and outgoing traffic, and show such information as date, time, origin, and termination of the call.

Larger users have the option of using a service bureau. Service bureaus electronically retrieve data from the company's PBX system and produce reports. They can consolidate traffic from switches at several different locations. Some service bureaus provide services aimed at identifying fraud, and provide exception reports that highlight abuse and suspicious activity. In addition, they will work with the users, carriers, and law enforcement agencies to document incidents for possible prosecution.

14. Educate Your Employees About Remote Access Fraud

Employees who have access codes should learn that:

- Codes are confidential business information.
- Codes should not be written down on anything that may be discarded, lost, or seen by an unauthorized person.
- Codes must not be shared with other people, even if the other person is an employee of the company.
- Codes should be stored in a secure location or database.
- Codes should be protected from observation when the employee is using payphones at airports, hotels, bus stations, or similar locations.

Toll Fraud Indicators

Toll fraud indicators are complex and contradictory at times. They can be broken down into two distinct categories: operational and statistical. The mere presence of one toll fraud indicator is not conclusive evidence of theft. Abnormal activity is often easy to explain. For example, a huge spike in outbound traffic may be triggered by an internal telemarketing campaign, or may result from a relatively simple anomaly. It should, however, serve as a catalyst for an immediate investigation.

Operational PBX Toll Fraud Indicators

Operational indicators involve situations which your staff and customers encounter that suggest a potential problem.

- Staff difficulties in obtaining open long distance lines or local access lines.
- Customer complaints that your lines are busy, particularly 800 lines.
- Operator complaints about frequent hang-ups or of callers requesting outbound or long distance service, particularly international calls.
- Operator complaints or comments that calls are frequently from individuals with foreign accents or poor English.
- Indications that lines are being used by strangers to converse in a foreign language.
- Attempts by outsiders to obtain sensitive information regarding the telecommunications system or calls from individuals posing as employees when they clearly are not.
- Any sign that the outgoing or inbound system is clogged or overloaded.
- A significant increase in the frequency of wrong number hang-ups.
- Any calls from inside or outside claiming to be from important personnel and requesting operator assistance to dial international calls.

Statistical Indicators of Potential PBX Toll Fraud

Statistical toll fraud indicators are revealed through PBX call accounting systems, voice mail administration reports, and trunk activity reports. Careful attention, preferably daily, should be given to the following statistical indicators of potential

CPE toll fraud activity on a near real-time basis, through the implementation of a system that contains an automatic alarm algorithm.

- Any sudden increase in toll-free service usage that cannot be easily explained (e.g., an advertising campaign or other marketing promotion, or a seasonal variation).
- A sudden and significant increase in short-duration calls or frequent short-duration calls to a specific number.
- The appearance of high-volume, long-duration incoming calls, particularly when associated with a similar increase in outbound long distance service.
- Any significant increase in incoming or outbound calls during nonbusiness hours.
- A significant increase in calls from or a sudden and unexplained increase in calling volume to a particular country, geographic area, or exchange (particularly countries or area codes where the user does not normally engage in any business).
- Simultaneous multiple usage of an individual access authorization code in your PBX.
- A sudden increase in multiple failed attempts to use access authorization codes, barrier codes, and personal identification numbers.
- Unusual tandem trunk-initiated incoming and outgoing calls through your PBX.
- Any unusual activity connected with known toll fraud regions.
- Invalid attempts to enter administration port, which can occur through the dial-in capability or through an in-facility terminal.

Although there is no foolproof prevention method for toll fraud, the above steps will significantly reduce your risks.

(Randy is Area Manager for Core Network Operations at SBC Pacific Bell. His grandfather, father, mother, brother, aunt & uncle have all worked for the SBC family.)

NEWS FOR SMALL BUSINESS CUSTOMERS

On 7/29/02, pending CPUC approval, SBC Pacific Bell will be introducing a new offering designed to meet the needs of its Small Business customers, both new and existing. **Business Solutions** (sm) provides additional discounts on the basic products small business customers rely on to keep their businesses running smoothly: **Custom Calling Services** and **Wire Pro**. A Centrex version of Business Solutions is also available.

Business Solutions requires a 12 month commitment to maintain the minimum services on their SBC Pacific Bell account, which include 2 access lines (minimum), 2 Wire Pro plans, and 1 Custom Calling Package.

Business Solutions has built-in flexibility by allowing customers to choose which of the 3 Custom Calling packages available for business is best suited for them. The packages are:

- **The WORKS**, which provides Caller ID and 10 or more Custom Calling services desired by the customer.
- **CCS Power Pack**, the mid-sized package anchored around Caller ID and at least 5 additional CCS features.
- A new, 4 feature package called **Business Essentials**, containing Call Forwarding, Call Waiting, Three-Way Calling, and Remote Access to Call Forwarding…just the basic services most businesses find critical to have.

Also, customers with additional lines have the option to add Wire Pro plans to these lines at a discounted price.

Several options have been designed to enhance the Business Solutions base package for customers with additional telecommunications needs. They include exclusive discounts on selected CPE, SBC Pacific Bell Voice Mail, Cingular Wireless discounts, SBC Pacific Bell DSL Internet Service and SBC Yahoo! Dial-Up Service, and on SBC Pacific Bell's new Local Usage Blocks of Time (pending CPUC approval).

Savings will depend on the specific options chosen, and range from 3% on the base package to 30% on specific bolt-on products. SBC Pacific Bell is continuously looking for ways to meet the unique needs of the small business customer, and Business Solutions allows for the customization for different environments and applications, while driving discounts the customer will really appreciate.

--Lori Dickey, SBC Product Management

continued from page 1

the April Issue of Update (page 16) on pacbell.com/Products_Services/CSG. If you still have questions, please call us on 1-800-552-5299. Thanks.

Security

With the importance of Security, we have some informative pieces on **Getting Value for Your Information Security Dollar, Reassessing Your Vulnerabilities** and a **Special Update Report on How To Reduce The Risk of Fraud**. Speaking of Security, we've been providing it to our customers for more than 120 years and we'll always be here for you. *Can you say that about any other telecom company? After they sell you a product are they available to you? Will they be around for you tomorrow?*

Are You Getting the Best Deal?

Other companies are calling, making offers to give you cheaper prices, better service... but to really find out if you're getting the best deal, you need to ask several questions:

Do you get monthly documentation to prove your savings? Will the service be as reliable as SBC Pacific Bell? If you have a power failure, what happens to your calls? Our Central Offices have backup generators so even when the power goes out, customers have dial tone and crucial services, like Message Center.

July 31st SBC Pacific Bell Broadcast

Be sure and sign up to see our July 31st Broadcast from 9-11:30am PST. It will feature *Long Distance*, *How CV Web Connects You to SBC Pacific Bell*, *Web Office*, *ConferenceNOW*® and the latest SBC news plus much more, The Latest Company News, Web Office plus lots more. Please call 1-888-889-6010 for reservation and further information.

Our goal continues to be to assist you in Working Faster, Smarter and More Efficiently by utilizing our many resources. Your Success is Our Mission.

Thanks for reading and participating.

Kari

Kari Watanabe

SBC Pacific Bell Consultant/Vendor Sales Group Vice President
415-542-4516
kw6875@sbc.com

10 Gigabit Ethernet:

The New Network Workhorse

by Paul Bedell


SBC's Paul Bedell

Though Gigabit Ethernet was just introduced in 1998, some customers are already clamoring for faster technologies. The average IT shop probably isn't feeling the squeeze on its 1-Gbps backbone yet, but vendors are preparing for the next level of speed and performance. 10 Gigabit Ethernet is well beyond the concept stage, and while there might not be a need for 10 billion bits per second of capacity today, it would behoove enterprises to build their network infrastructures to support this technology in the near future.

Many IT shops only recently migrated to Gigabit Ethernet technology in their network backbones, and the idea of yet another technology migration may seem daunting. Although some experts predict that network spending will drop sharply well into 2003, the evolution of technology and applications will drive the need for more bandwidth, especially in the network core.

The traffic load on a network is directly proportional to the amount and type of systems attached. As enterprises continue to deploy Gigabit Ethernet uplinks toward the network's edge (the users), the demand for more bandwidth at the core will inevitably increase.

Why 10 Gigabit Ethernet ?

Why all the fuss about 10 Gigabit Ethernet (10GigE)? Because Gigabit Ethernet (GigE) has done so well. Because Ethernet, at all speeds, has a proven track record. As the dominant LAN protocol, Ethernet is well understood with very few integration problems and no special Customer Premises Equipment (CPE) requirements. Ethernet prices per port are declining 30 percent annually, making it an incredibly cost-effective technology. 10 GigE can be used with or without SONET or ATM, dropping infrastructure prices even further, which minimizes network complexity. And it's by far the most easily provisioned technology around, capable today of bandwidth-on-demand delivery in 1Mbit/sec increments. The reason Ethernet technology has not only survived but thrived is the ease with which new technologies have been able to gain more bandwidth from the same infrastructure. Ethernet has done it again, multiplying its capacity tenfold.

One way to gauge just how excited we should get over 10GigE is to look at the projected size of the market. At the higher end, Lantern Communications claims that the metro market for 10 GigE will hit $2 billion by 2004. According to the Gartner Group, 10GigE service should be available in 100 cities by 2003, as opposed to the roughly 30 or so cities where it was available in late 2001. 10 GigE revenue and port shipments are expected to grow from $440M and 25,000 ports in 2002 to $3B and 450,000 ports in 2004.

Pricing will be key to market acceptance and adoption depends heavily on whether customers can get fiber to their buildings, as 10 GigE will only operate over glass.

KEY: Currently, only about 10 percent of buildings in the United States have direct access to optical fiber facilities. It can be very expensive to construct fiber "laterals" to buildings, and this issue might raise prices in the long run. What multi-tenant unit (MTU) customers are willing to spend on Internet access is also a key issue.

So what makes it a worthwhile technology?

1. It will scale enterprise and service provider LAN backbones. In other words, it provides the means to easily migrate to the next highest speed in the Ethernet technology hierarchy (10, 100, 1000, 10,000 Mbps).
2. Similar to GigE, it allows for extending Ethernet to both the MAN and the WAN, providing transparent data connectivity between LAN, MAN and WAN.
3. 10 GigE makes use of the Ethernet installed base – a base of more than 300 million Ethernet ports worldwide.
4. It will support all traffic types – data, voice and video-over-IP.
5. It is faster, simpler and more cost-effective than other alternatives. It's the best in total cost of ownership when compared to other protocols and technologies.

Another major driver for 10 Gigabit Ethernet in the enterprise is the proliferation and widespread adoption of gigabit Ethernet over copper in the wiring closet. Wiring desktops for gigabit Ethernet may seem like overkill, but soon desktop systems will have integrated 10/100/1000Base-T ("LAN-on-motherboard") network interface cards (NICs). Apple Computer's G4 tower computers now come with integrated 1000BaseT interfaces as "standard". And though the average desktop user may not need 1,000 Mbps all day, he or she will benefit significantly from decreased wait times on large file transfers when they're required. This use will create very bursty traffic patterns on wiring-closet uplinks, ultimately increasing backbone network load. It's not unrealistic to believe that gigabit Ethernet will be a common technology at many desktops by 2004.

Gigabit Ethernet aggregation is occurring in three places in these large networks:

1. In building basements, aggregating Gig links that come down the risers from wiring closets.
2. In storage area networks (SANs)
3. At server farms

At these aggregation points, 10 GigE should be a clear winner. Today, the only option high-bandwidth users have is to trunk multiple 1 GigE ports together between two switches using multi-link trunking (MLT) to create a backbone of 2 Gbps or higher. This technique is useful for higher capacity, and as a means to provide failover for network redundancy. But there are downsides to trunking. For one thing, it uses up valuable Ethernet switch ports. But the second and bigger problem is that it may not always deliver the capacity users expect. According to sources at Spirient, some tests have shown that because of the way the control plane and data plane interact in trunking scenarios, on some Ethernet switches there is hardly any additional bandwidth gleaned when using MLT.

KEY: It's estimated that Ethernet in the wide area may be one-fifth the cost of SONET, and one-tenth the cost of ATM. Ethernet is also rightfully viewed as being media "agnostic", since it interfaces transparently with various transmission media including copper cable, wireless systems, and several types of fiber.

10 GigE Standards Development

The 802.3ae Committee was formed in January 2000 at the recommendation of an IEEE study group to develop a standard for 10 gigabit Ethernet. Unlike Ethernet standards of the past, the 10 Gb standard will no longer support shared media access. It is highly unlikely that any significant work will be done on copper standards for 10 Gbe in the near term. The 10 Gbe standard should be ratified in 2002, although pre-standard products started appearing on the market from nearly all existing providers of high-speed layer 2/3 switching products during late 2001. The equipment manufacturers are not passively waiting on a standard because several vendors expect to announce 10 gigabit Ethernet products, in advance of the standards ratification expected in 2002. Of course, each of these vendors hope that their products will reflect (one of) the standards, and they promise that they will conform once those standard interfaces are defined. It is expected that as the standard nears completion, prices will reflect

the typical incremental costs of previous versions of Ethernet (i.e. 10BaseT; 100BaseT). In December, 2001, multi-mode 10 GbE ports cost approximately $30,000 to $60,000, and single-mode pricing should be in the $15,000 to $20,000 range. Prices will drop by at least 50 percent during the first year (2002-2003), followed up by the historically proven Ethernet price decreases of 30% year over year.

The 10 Gigabit Ethernet standard is going to be significantly more complex than the previous Ethernet standards. When 100Base-TX technology was introduced in 1993, vendors were able to leverage the FDDI physical interface (copper) to facilitate development of the standard. When gigabit Ethernet was introduced in 1998, vendors leveraged the optical and electronic interfaces developed for Fibre Channel. But with 10 Gigabit Ethernet, there is no comparable technology to leverage. To develop a 10-gigabit physical layer, vendors have to develop a layer capable of transporting 10 billion bits of information per second !

The IEEE 802.3ae 10 Gigabit Ethernet Task Force has outlined several key objectives that should be of interest to IT managers. The most important is that 10 Gigabit Ethernet will remain an Ethernet technology. n other words, it will preserve the 802.3 Ethernet frame format, minimum and maximum frame size, and MAC (Media Access Control) client service interface. Like the GigE standard, the 10 Gigabit Ethernet standard will be a full-duplex-only standard. Like the GigE 802.3z standard, CSMA/CD will not be a part of the 10 Gigabit Ethernet standard either. The gigabit Ethernet standard included support for a special half duplex repeater-based implementation called a buffered distributor. However, this technology never made it into widespread deployment. So 10 Gigabit Ethernet will not include a half-duplex option. This decision not only solves the problem of network "diameter" (switched networks have no inherent distance limits other than cabling limitations), but it will significantly simplify the standard. Half duplex was once implemented for cost reasons: it was cheaper than full duplex. But given that most of the cost of gigabit and 10-gigabit interfaces is in the optics, half-duplex connections no longer make sense. They aren't and won't be available.

Supplementing the work of the 802.3ae Task Force are the efforts of the 10 gigabit Ethernet Alliance (10 GEA), an industry consortium of about 100 equipment vendors working to promote the acceptance and success of 10 gigabit Ethernet. The group is not the same as the IEEE 802.3ae standards committee, which is working on a set of proposed standards for 10 gigabit Ethernet.

Two Flavors

The 10 GigE standard will define two physical layers ("PHYs"): the "LAN PHY" and the "WAN PHY". 10 gigabit Ethernet is being designed to support not only enterprise backbone networks (LAN PHY), but wide-area and long-haul networking applications as well (WAN PHY).

The LAN PHY standard will represent the typical LAN interfaces used today, operating at a 10-Gbps data rate. The WAN PHY standard is designed to operate at a data rate compatible with the payload rate of OC-192c and SDH VC-4-64c (9.58 Gbps).

The WAN PHY standard will be a SONET OC–192 compatible stream, which is therefore clocked at 9.953 Gbps. The disadvantage is that it is not a pure 10 times 100 megabit Ethernet. There may also be disadvantages of cost—SONET is not the least expensive transport method. The advantages, however, are that it would be guaranteed to interoperate with all OC–192 SONET devices, including the networks of all of the major telephone companies, and all of the OC–192 compatible DWDM systems. And the reality is that 9.953 Gbps is close enough to 10.000 that no real applications are likely to notice the difference anyway.

Ethernet transport has not yet taken off in the long-haul network, but this is expected to change as 10 gigabit Ethernet interfaces become available. Some of these interfaces are expected to operate at SONET OC–192 speeds, and at the distances required for long-haul networks. The distance limitations are not a serious concern, because most long-haul networks use dense wavelength division multiplexing (DWDM) systems to combine multiple circuits over a single fiber, each on its own wavelength, and these DWDM systems provide the long-haul capability themselves.

KEY: Unlike SONET networks, 10 Gigabit Ethernet over SONET will remain asynchronous. This will enable 10 gigabit to run over SONET networks, but the switches and routers that terminate 10 GigE links will not need the complex and expensive stratum clocks that native SONET interfaces require.

Getting Ready For 10 GigE

Whether a business or carrier is interested in 10 Gigabit Ethernet now, or planning for the future, several concerns must be addressed. If planning to retrofit a building or a campus, the challenge lies in adapting the infrastructure to support the new data rates. FDDI-grade cabling will support a maximum distance of just 300 meters. For many campus environments, this means that multimode fiber will no longer be suitable for backbone networking. Single-mode LAN installations will be available for ~ 6-24 mile configurations, with the potential for 48-miles or more as laser technology continues to improve. If the campus does not have sufficient single-mode fiber to replace existing multimode runs, upgrade now if planning to run Gigabit Ethernet campus-wide. When developing new campuses and when buildings are under construction, it's necessary to provision a sufficient amount of single-mode fiber to support the new requirements of 10 Gigabit Ethernet. Single-mode fiber was once an expensive option compared to multimode installations, but network managers should consider single mode not only for intra-building links but for vertical risers as well, to plan for the future. "Futureproofing" buildings is the critical objective when designing and implementing structured cabling systems these days.

KEY: 10 Gigabit Ethernet is expected to cost three to five times more than today's GigE (1000Base-X) interfaces when it's available. Early modules from Extreme Networks and Foundry Networks cost $40,000 or more, but a $10,000 to $15,000 initial price range is more likely by the time the standard is ratified in 2002.

The good news is that many existing vendor architectures, including Foundry's BigIron, Extreme's Black Diamond and Cisco's Catalyst 6500, will support 10-gigabit Ethernet modules in their current form. Although these architectures were only marginally designed for 10 GigE, they can still use the technology to significantly improve data rates over 1-Gbps Ethernet, thereby protecting existing investments. Cisco Systems and other vendors already offer 24-port 10/100/1000Base-T gigabit-over-copper modules for around $375 per port. In 1995, 10/100 Fast Ethernet interfaces cost about the same

Gigabit Ethernet versus 10 Gigabit Ethernet

The table below shows the basic functional and standards-based differences between gigabit Ethernet and its cousin, 10GigE, which will be standardized this year.

Attribute	GigE	10 GigE
Physical Media	Single and Multimode fiber and Wide Wave Division multiplexing (802.3z), twisted pair copper (802.3ab)	Single and Multimode fiber
Media Access Control	Full and Half Duplex	Full duplex only
Physical Media Dependent	850 nm; 1300 nm, 1550 nm WWDM	850 nm, 1310 nm and 1550 nm
Accommodates OC-192 TDM and WDM	No	Yes
Packet Size	Variable 64-1514bytes,	64-1518 bytes

Source: 10 Gigabit Ethernet Alliance (www.10gea.org) and the Yankee Group

continued on page 15

continued from page 1

Federal Excise Tax

Under the Internal Revenue Code, Federal Excise Tax is applied to telephone service.

It applies a monthly percentage to:

- Monthly service charges
- Zone Usage Measurement (ZUM) charges
- Local Toll charges
- IEC charges
- California Billing Surcharge
- State Regulatory Fee
- California Relay and Communications Devices Fund surcharge
- Universal Lifeline Telephone Service surcharge
- California High Cost Fund - A surcharge
- California High Cost Fund - B surcharge
- California Teleconnect Fund surcharge
- Universal Service Fund Surcredit
- End User Common Line (EUCL) charge
- Non-regulated Inside Wire per-visit repair charge

The effective rate as of 1/1/83 is 3.0%.

State 911 Tax

This tax was established to provide funds to public agencies that operate emergency 911 services. It applies monthly percentage to:

- Monthly service charges
- All calls made within California
- ZUM charges
- California Billing Surcharge
- State Regulatory Fee
- California Relay and Communications Devices Fund surcharge
- Universal Lifeline Telephone Service surcharge
- California High Cost Fund - A surcharge
- California High Cost Fund - B surcharge
- California Teleconnect Fund surcharge
- Universal Service Fund Surcredit

The effective rate as of 11/1/94 is 0.72%.

Local Taxes

Local governments may choose whether or not to impose a Telephone Utility User's Tax (a.k.a. City or Local Tax) and at what rate. Various local ordinances provide that certain telephone services are taxable and others are not and certain customers are exempt from all or part of telephone services provided. Generally, the local tax applies to:

- Monthly service charges
- Message unit/Zone Usage Measurement (ZUM) charges
- Intrastate toll
- California Billing Surcharge
- State Regulatory Fee (CPUC Surcharge)
- End User Common Line (EUCL) charge (only if local tax is applied to interstate and international charges)
- CA Relay Services and Communications Devices Fund Surcharge (formerly known as Deaf and Disabled Surcharge)
- Charges for interstate and international calls when not exempted by local ordinance

Fed. Universal Service Fund

All telecommunications companies are required to contribute to the Federal Universal Service Fund (FUSF). This Fund, established in January 1998, supports the telecommunications needs of low-income households, consumers living in high-cost areas, schools (K-12), libraries and rural hospitals. The fund was established in the Telecommunications Act of 1996 and was created by assessing both intrastate and interstate revenues of providers of interstate telecommunications services.

The Federal Communications Commission (FCC) determines on a quarterly basis a contribution factor that is based on the ratio of total projected quarterly costs of the "universal service support mechanisms" to total end-user interstate and international telecom revenues. The calculation of the FUSF Flat Rate End User Charge takes all interstate and international revenue less special access end user revenues.
The result is then multiplied by the contribution factor released by the FCC (currently 7.2805% for 2Q02) and then multiplied by four. The result is then divided by the annualized amount of Presubscribed Interexchange Carrier Charge (PICC) lines (minus resold and lifeline counts) for the period of three months prior to the obligation period. Needless to say it's not a simple calculation. Conversely the special access end user USF obligation is recovered through a percentage surcharge factor applied to the end user billed special access charges.

Primary residential and single line business, including multi-line business customers are assessed one USF charge per line. PRI ISDN customers are assess five (5) times the business USF charge. Centrex customers are assessed one-ninth (1/9) of the business USF charge on all lines.
A special access USF factor is assessed monthly to end user billed special access recurring charges.

Charges for Network Access for Interstate Calling

The Federal Communications Commission's (FCC) Order on Access Reform, effective January 1, 1998, was designed to realign the recovery of costs for access service more closely to the cost using entity(s).

There are three rate elements included under this umbrella:

<u>End User Common Line Charge (EUCL)</u>
This allows Pacific Bell (and all other Local Exchange Carriers) compensation for the cost to maintain the local loop connecting the customer to the local switching office via wire, poles and conduits. These costs were originally subsidized by long distance revenue prior to Divestiture in 1984. The effective rate as of 8/11/01 is $4.40 for business lines and changes annually and sometimes more frequently.

<u>Presubscribed Interexchange Carrier Charge - PICC</u>
This was a monthly per line recurring charge assessed on customers who have not selected a Primary Long Distance Provider. It was also billed to a Long Distance Provider when a customer selected and subscribed to their service. However, SBC Pacific Bell ceased to charge the PICC on 7/1/99 for BRI ISDN, PRI ISDN, Centrex, Multi Line Business Lines and SuperTrunk. It is charged today ONLY for a single business line where there is only one account billed to that name in the state of California. The effective rate as of 4/1/99 is $0.87.

Digital Line Port Charge

This is a monthly charge applied only to ISDN customers. Effective 07/01/98 the cost is $0.97 per line for a Basic Rate Interface (BRI) and $32.80 per Primary Rate Interface (PRI).

Federal taxes apply to these charges and local tax applies only if a local tax is applied to interstate and international charges State taxes do not apply.

California Billing Surcharge (Rate Surcharge)

The rate surcharge was established to collect revenue for the CPUC ordered changes to SBC Pacific Bell's revenue requirements until such time as individual rates for products and services are adjusted. It applies a monthly percentage to all recurring and nonrecurring rates and charges for service or equipment provided under our tariffs. The surcharge has different rates for IntraLATA exchange service, IntraLATA toll and IntraState access (products contained in CPUC 175T).

The effective rate as of 1/1/02 is: -1.7200% for exchange service, -1.7220% for toll service and –1.7260% for access service.

California High Cost Fund-A (CHCF-A)

The fund was adopted to provide financial support to small and mid-size Local Exchange Carriers (LECs) of which there are over 20 in California. It subsidizes basic exchange rates for small and mid-size LECs and was originally imposed against Interexchange Carriers via an increment to the carrier common line rate. Effective 1/1/95, it was imposed against same billing base as California Relay and Universal Lifeline Telephone Service surcharges (described below).

It applies a monthly percentage to each subscriber's intrastate services.

- Regulated and Non-regulated charges
- Includes recurring and nonrecurring rates and charges
- Toll charges
- California Billing Surcharge
- Universal Service Fund Surcredit
- Interexchange Carrier's portion of bill carries surcharge portion covering intrastate service and calls carried by carrier

The effective rate as of 1/1/02 is: 0.30%

California High Cost Fund-B (CHCF-B)

This surcharge is collected to fund "Carriers Of Last Resort" for a portion of its cost of providing service to residential customers in high cost (rural and suburban) areas. The subsidy allows basic service rates to remain low for primary lines and ensures basic service providers will have an incentive to continue to serve high cost areas. It's mandated by the CPUC as part of introducing competition within local exchange companies' service territories. All telecommunications carriers within California are required to bill the CHCF-B surcharge that funds the California Universal Service Fund (CUSF). This is a statewide fund established to assess and reimburse "Carriers Of Last Resort" and the CPUC is administrator of the California Universal Service Fund (CUSF)

It applies a monthly percentage to the same billing base as the California High Cost Fund-A (CHCF-A)

The effective rate as of 11/1/01 is: 1.47%

California Relay Services and Communications Devices Fund

The CPUC order states each certified deaf or severely impaired subscriber or user will be furnished a telecommunications device and a signal unit at no charge in addition to basic exchange service.

The cost of providing such minimum basic equipment is funded by this surcharge on all telephone customers' bills in the state. Prior to 7/1/94, it was known as the Communication Devices Funds for Deaf and Disabled.

It applies a monthly percentage to each end user's intrastate services:

- Includes recurring and nonrecurring rates and charges
- Toll charges
- California Billing Surcharge
- Universal Service Fund Surcredit
- Interexchange Carrier's portion of bill carries surcharge portion covering intrastate service and calls carried by carrier
- Nevada accounts which are located in California.

The effective rate as of 12/1/01 is: 0.480%

California Teleconnect Fund Surcharge

This surcharge is collected to fund discount of service provided to qualifying schools, libraries, municipal and county owned hospitals and qualifying community based organizations. It is mandated by the CPUC as part of introducing competition within local exchange companies' service territories. All telecommunications carriers within California are required to bill appropriate surcharge. It is part of the California Universal Service Fund (CUSF) administered by the CPUC. Discounted Advanced Services is SBC Pacific Bell Telephone Company's name for services offered under California Teleconnect Fund.

It applies a monthly percentage to each end-user's intrastate services as the CHCF-A previously discussed.

The effective rate as of 11/1/01 is: 0.30%

Equal Access Recovery Charge

Equal Access Cost Recovery Charge (EARC), mandated by the California Public Utilities Commission, was a three year cost recovery surcharge for expenses associated with the conversion of IntraLATA Presubscription (ILP) in Pacific Bell territory. This charge began on 8/3/99 and stopped on 8/3/02. EARC applied to all originating local toll call minutes of use.

Local Number Portability

The Federal Telecommunications Act of 1996 required local telephone companies to initiate measures that permit customers to retain their local telephone numbers should they change their local telephone service provider while remaining at the same location. This capability is commonly called "number portability". The Federal Communications Commission (FCC) has allowed that the costs associated to provide "number portability" be recovered through a customer service charge. This service charge will be a monthly charge per line*. This service charge will:

- be labeled "Number Portability Svc Charge"
- begin February 1, 1999 and end on January 31, 2004

continued on page 19

DSL DATA NEWS

Do You Yahoo? We do!

by Cassandra Jessie-Johnson

Cassandra Jessie-Johnson

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.

By late October 2002, all SBC Internet customers (including Prodigy) will be transitioned to the SBC Yahoo! Dial or SBC Yahoo! DSL service. 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! Classifieds 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 can enjoy additional premium bundles by choosing features from different categories. Additional discounts are available for *Entertainment, Professional/Finance, and Life Management/Family features*.

Our current customers will continue to receive the Prodigy portal until the new co-branded SBC Yahoo! service is available. Once it is, customers will be alerted via e-mail, portal postings and letters. The first communication was sent to our existing Dial customers in May, alerting them of an upcoming client kit (which included a CD, welcome letter and instructions) and encouraging them to immediately load the CD to take advantage of our great new features. A DSL CD will also be sent to existing DSL customers in late August. Customers need only to pop in the CD to install the software. Within minutes, they'll begin enjoying the SBC Yahoo! Experience. 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

If customers would like to take a tour of the SBC Yahoo! product, you can refer them to http://yahoo.sbc.com/.

What Else is New?

SBC Pacific Bell Internet Services has reduced the price of the **Home Networking/Office Gateway** product. This solution allows multiple users per home or small business to share a single DSL Internet connection. Customers can use their existing phone wires to connect up to 10 DSL-compatible PCs simultaneously to one DSL Internet access connection, and share printers, scanners and other devices in the home or small office. Home Networking/Office Gateway is offered with or without a built-in DSL modem, and customers have the option to choose between standard or wireless gateways. Prices have been discounted between $25 and $150, depending on equipment selected.

Centrex/DSL is coming soon! Centrex/Plexar DSL is the provisioning of DSL data over the same pair of wires that provides the analog circuit switched voice capabilities of Centrex/Plexar. It will provide customers with a high-speed data connection to the Internet or to their host server at their main office location. The competitive alternative today is Centrex/Plexar ISDN. Centrex/Plexar DSL will be another quality, high-speed Internet access option for your customers. With Centrex/DSL, a customer will only have usage charges on the Centrex portion.

Want a Promotion?

We are still sizzling with The Get Up To Speed 2002 campaign. The three favorites from last year - Get Up To Speed II, Low Speed Enhanced DSL with discounted router, and Speedracer (High speed) are back by popular demand. We've also expanded the area codes for the targeted offers. Discounts on CPE, monthly rates, and processing fees are continuing throughout the campaign. Be on the look out for direct mail drops. Listen for radio ads announcing an offer in your specific area code!

Got DSL?

With over 1.6 million DSL Internet subscribers, SBC is infinitely dedicated and committed to remaining on the cutting edge, with continued rapid deployment of DSL technology. We answer to the customer! At the end of May 2002, we had nearly 1613 Remote Terminals (RTs) with over 9,265 Distribution Areas (DAs) ready for service, in ASI West and SBC Pacific Bell. For more information, to qualify your customers for DSL Internet Service, as well as to order DSL Internet service for your clients, contact the Emerging Products Center Consultant Queue at 1-866-234-4DSL (4375).

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

EchoStar & SBC

EchoStar's DISH Network digital satellite TV offerings will be combined with SBC's DSL Internet Service under a marketing alliance to provide customers with a convenient and competitively priced alternative to cable. Consumers who take advantage of the service bundles will receive credits of up to $10 on monthly service charges later this year. Stay Tuned for further details.

DATA WITH DAVID

Virtual Private Network Growth is Significant

by Tom David


Tom David

Recall the days when customers would connect private lines between company sites to exchange data information. Circuits would be costly because they were distance sensitive and networks often difficult to manage due to size and complexity. As networks evolved over time companies migrated to packet, frame and cell based transport technologies that were more efficient and less costly. In the past decade the Internet has provided new transport options that has spurred the growth of Virtual Private Networks (VPN).

A Virtual Private Network is a private data network that makes use of the public Internet or a service provider's IP network. A VPN can be contrasted with a network of owned or leased lines that can only be used by one company. The idea behind a VPN is to give companies the same capabilities of a private network at a much lower cost by using the shared public infrastructure. VPNs enable business customers to experience the same security, quality of service, reliability, and manageability as they do in their private network.

The demand for VPN services to meet the increasing business need for secure, transparent and scalable data transport continues to grow. The Yankee Group predicts that VPNs will be used by 70 percent of all companies for up to 90 percent of their data communication needs by 2003, in place of private line and alternative data communication services. It's been estimated that the US VPN market will reach approximately $10 billion by 2005, with a compounded average annual growth rate of over 60 percent, according to market research firm IDC.

The attraction to VPNs and what is spurring this phenomenal growth is that it provides an inexpensive means of extending corporate communications and operations. It provides an inexpensive means of extending corporate network access to mobile workers, replacing expensive leased lines for site-to-site connections, and securely communicating with customers and business partners.

Software-based VPN

SBC is responding to this demand by offering the next-generation, subscription-based managed VPN service that simplifies the deployment and administration of secure access to business-critical network resources for remote users such a mobile employees, telecommuters, business partners and customers. Announced in May at Networld + Interop in Las Vegas, SBC introduced in June 2002 a software-based VPN (S/VPN) solution that uses a management platform in the SBC network to connect remote user branch locations with secure VPN tunnels.

The software-based VPN consists of three software components – the *S/VPN Gateway*, the *S/VPN Manager* and the *S/VPN Client*.

The *S/VPN Gateway* is a software package that is placed on a customer's existing Windows NT/2000 server. It is responsible for integration of members from inside the private enterprise intranets. The gateway may reside on any Windows NT/2000 server or workstation on the corporate LAN that is behind a firewall. The gateway is significantly less computation-intensive than traditional VPN gateways and allows for the seamless overlay of VPN service on top of an existing IP network infrastructure.

The *S/VPN Manager* is a web-based application that manages all aspect of the VPN. Clients, gateways and VPNs are created on the Manager. VPN encryption and authentication policies are set and controlled on the Manager via an easy to use web-based interface. The *S/VPN Manager* controls client access levels and performance and auditing may be viewed on the Manager.

The *S/VPN Manager* features include:

- Single Socket Layer (SSL) Security
- Instantaneous addition, deletion and suspension of clients, gateways and VPNs
- Centralized client software distribution
- Forceful deactivation of users from active sessions
- Dynamic policy control
- VPN traffic logs
- Dynamic traffic usage reports by VPN or client
- Dynamic billing logs
- Dynamic manager
- Configure alert settings and views of alert logs

The *S/VPN Client* is a combination of downloadable application software and network drivers that allow external hosts to access the corporate LAN by connecting securely to the gateway. The client software intercepts and encrypts packets destined for the corporate LAN, which are then forwarded to the gateway or another S/VPN client for decryption.

In addition to allowing remote access to the corporate LAN via the gateway, the client allows for direct connections to other clients without involving the corporate LAN. Thus peer-to-peer VPNs may be created if allowed by the VPN administrator.

The *S/VPN Client* software resides on the desktop of internal hosts, the desktop/laptop of remote users, and the desktops of remote offices. The Client software provides a simple GUI interface for clients via a dialup, wireless or network connection to the local VPN server. With *S/VPN Client* software, remote users can access corporate resources quickly and easily over the Internet.

The *S/VPN Client* common specifications include:

- IPSec Security (Internet Protocol Security-a standard for remote user access)
- IKE authentication and key management (Internet Key Exchange for pre-shared keys)
- Network address translation (NAT) (translates network names to IP addresses)
- DES (56-bit) and 3DES (168-bit) (widely used method for data encryption)

- MD5 and SHA-1 data integrity authentication
- DSA/RSA public keys
- Split tunnel access (simultaneous VPN and Internet access)
- Multiple simultaneous tunnel support
- Automatic version checking and software updates
- 24x7x365 monitoring
- Shows a list of authorized gateways and clients the user can access
- Zero-configuration (dynamic configuration via Internet at every login)
- File browser for accessed client
- Virtual adapter (DHCP configured from gateway)
- Supports all IP protocols
- View user's digital certificate
- Change user password

The following mimimum requirements are necessary to run the client software:

- Pentium or higher, Pentium II or higher is strongly recommended
- Windows 98, 98SE, NT4 or 2000
- 32MB RAM minimum, 64MB recommended
- 5MB free hard disk storage
- Internet connection

Customer Benefits from Software-based VPN

The S/VPN application allows the customers' end user to have the same TCP/IP experience as they would have on the corporate LAN including:

- Print to a printer
- Log onto a Windows Domain
- Access internal email server

Some additional benefits from using this software-based VPN solution include:

- *Rapid deployment without CPE*
  Users may access their corporate network from remote locations as if they were in the office. This product can deployed instantly without installing CPE. Industry-standard security algorithms and network protocols are implemented efficiently in the software to support high bandwidth throughput for all remote access neeeds.
- *Zero-administration client and gateway software*
  Downloading and installing the client software is simple. The software is downloaded in minutes together with a digital certificate used to authenticate the user.
- *Policies are centrally configured & managed via the browser by simple self-service*
  The customer's S/VPN administrators maintain complete control of policies and network settings without having to install or manage policy servers or public key infrastructure. They can also respond to a rapidly changing environment and remove or add users on-demand.
- *Instant activation/deactivation from anywhere*
  Software-based VPN can be set-up and deployed within minutes. Service deployment requires zero client configurations, minimal administration, and no extensive networking or security knowledge. A simple web-based interface guides the administrator through set up and maintenance.
- *Standards based security (IPSec, IKE, RSA)*
  The software-based VPN service utilizes industry-standard security including IPSec, PKI, IKE, CA and 3DES. Connections are securely authenticated with passwords and public key cryptography, the policy database authorizes access to network resources, and network links are encrypted point-to-point.

Service Activation and Setup

The SBC S/VPN administrator sets up the customers VPN to support the required number of gateways and the universe of remote access users. Once this is setup the customer's S/VPN administrator controls the remote user signup process. This administrator will assign a user name and password to allow remote users access to the software-based VPN web-based interface. This information exchange is secured by SSL encryption.

The client setup is done through the *S/VPN Manager* where the administrator sets up clients (users) by entering their names and e-mail addresses. Batch is also an alternative for a large number of clients. An e-mail is automatically sent to each user, containing a secure link to the client download page. This simple download takes minutes and does not require any user configuration. The administrator may also choose to install the software manually.

The Gateway setup is done through the *S/VPN Manager* and the administrator defines the gateway's IP address and then installs the gateway software on a PC in the corporate network. As the gateway uses DHCP to assign internal IP addresses for remote clients, a range of IP addresses must also be assigned. Should the customer not wish to do this SBC professional services can be engaged for an additional cost to install and integrate the gateways for the customer.

Pricing

The monthly per user fee varies depending upon the number of users and the term of the agreement. The month-to-month pricing varies from $23 to $25 per user. The range for a one year term is from $20 to $22 per user and for a two year term from $18 to $20 per user, again depending upon total quantity of users. The set-up fee of $50 and the $250 Gateway per LAN segment fee is waived with a one or two year agreement.

Summary

Software-based VPN is a subscription-based managed VPN service that enables corporations to extend secure access to network resources for remote users, customers and business partners. Its unique advantages are instant deployment, easy administration, the highest levels of security, and tremendous cost savings to corporations.

It delivers a revolutionary solution to meet the needs not served by SBC's traditional hardware-based VPN products or services. Software-based VPN make it easy for SBC customers to create and maintain an infrastructure that extends secure Internet-based access to business-critical resources.

(Tom David is a Consultant Liaison Manager at SBC Pacific Bell. His email is td1898@msg.sbc.com)

"No brain is stronger than its weakest Think."

T. Masson

continued from page 9

10 GigE Applications

10 GigE will change the way enterprises use their networks. It will also change the face of MANs and WANs. With LAN PHYs and SONET-compatible WAN PHYs, Ethernet will take on a whole new role in the MAN. The applications for 10 GigE range from the obvious expansion of LAN backbones, to MAN and WAN services. In the LAN, 10 GbE will be used primarily as a switch-to-switch link in large backbone networks, running through vertical risers in collapsed backbone LANs. It will also play a smaller role as an aggregator between workgroup switches where GigE is justified at the desktop.

10GbE will not be found in end systems/servers until I/O technology migrates, or improves to the point of a higher-capacity architecture such as InfiniBand.

InfiniBand is an architecture (and specification) for data flow between processors and I/O devices that promises greater bandwidth and almost unlimited expandability in tomorrow's computer systems. Between 2002 and 2004, InfiniBand is expected to gradually replace the existing Peripheral Component Interconnect (PCI) shared-bus approach used in most of today's personal computers and servers. Offering of up to 2.5 gigabytes per second and support for up to 64,000 addressable devices, the architecture also promises increased reliability, better sharing of data between clustered processors, and built-in security. InfiniBand is the result of the merging of two competing designs:: Future I/O, developed by Compaq, IBM, and Hewlett-Packard; and Next Generation I/O, developed by Intel, Microsoft, and Sun Microsystems. For a short time before the group came up with a new name, InfiniBand was called System I/O.

KEY: Like migration to GigE, enterprises running very large campus backbones must ensure that their switch platforms have the necessary backplane and buffering capacity to adequately support 10 GbE links.

Other LAN-oriented applications for 10 GigE will be for "server-less" buildings; server backup; and disaster recovery.

The more interesting applications for 10 GbE are for new WAN services. The 10 GbE standard is being defined with two separate physical interfaces: One interface running at exactly 10 Gbps (LAN PHY), the other at 9.952 Gbps (OC-192; WAN PHY) to allow Ethernet to map directly to the WAN SONET and DWDM infrastructures. These options will allow two types of Ethernet-based carrier services. The first will be MAN services running at native Ethernet speeds, constructed with a mesh of high-speed Layer3 switches. The second offering will be WAN-based, with rate adaptation to OC-192 speeds. By using SONET framing and existing DWDM capabilities, the distance limitations of standard Ethernet links will be eliminated.

These offerings will dramatically shift the price/performance curve of WAN services. New Ethernet-based services are already offering a 2.5 times to 25 times increase in price-to-performance. As of 2002, Ethernet-based services offer up to 100 times improvement over traditional WAN offerings.

The early adopters will likely be major metro multi-tenant units (MTUs). The lack of availability of voice services related to 10 GigE may eventually inhibit market growth also.

KEY: 10 GigE won't replace SONET by 2008, but SONET's decline may begin by that time. Some estimates place pure Ethernet services at 30 percent or more of the metro market infrastructure by 2005.

QoS In 10 GigE Networks

Once QoS issues are resolved, 10 GigE possibilities could include what Lantern Communications calls "new economically sound applications," meaning those apps that are too expensive or unpredictable to really grab today's business users. If 10GigE really does open up the local loop, the first killer-app contenders would likely be the perennially threatened video applications category, led by videoconferencing. There's also some talk of 10GigE private line services for international business traffic as an alternative to OC-192, but that's even further down the road.

However, the vendor community has an answer to the QoS and protection dilemma: Resilient Packet Ring (RPR) technology, a layer-2 protocol being designed to bring SONET-type capabilities to the data world. Led by Nortel, Cisco, Luminous Networks, Dynarc and Lantern Communications, the RPR standard is a work in progress, and not due for finalization until 2003.

Aside from lack of robust standards and compliant chipsets for vendor gear, the two biggest threats to a speedy rollout of 10 GigE are ultimately:

1. The lack of compelling service applications to drive return on investments (ROI), which directly impacts
2. The cost of deploying fiber to unconnected buildings.

Beyond 10 Gigabits

Like the growth of 10-Megabit Ethernet led to the need for 100-Megabit Fast Ethernet, and just as the growth of Fast Ethernet led to the need for Gigabit Ethernet, the growth of Gigabit Ethernet is now driving the market to 10 gigabit Ethernet. This trend is not likely to stop anytime soon. Servers—whether Web servers, file servers, e-commerce servers, or others—must obviously have exponentially greater bandwidth than the customers they serve, otherwise, those customers would feel frustrated with inadequate performance. A prime example is Web servers. If the average Web browser is using a 56k modem, a server connected to a T1 circuit can simultaneously handle approximately 30 customers. But the broadband movement has already started – albeit slower than expected - and millions of consumers are now accessing the Internet from DSL and cable networks. These consumers access the Internet at speeds up to 10-Megabit Ethernet (typical connectivity for a cable-modem service), and for them, a service provider limited to a T1 circuit is already unacceptably slow. This requirement to always be faster than the customer by a factor of the number of projected "simultaneous accesses" drives the need for DS-3 (45 megabits) or even greater speeds today, and will drive the need for Fast Ethernet and Gigabit Ethernet tomorrow.

Many carriers-SBC among them-are already offering gigabit Ethernet services today. Some may limit their customers to a few megabits per second, but the links are still gigabit-capable.

KEY: Engineers are already dreaming of the next step, and arguing over what speed it will be. 40-gigabit speeds (SONET OC–768) have already been demonstrated, so that is possibly Ethernet's next target. However, the Ethernet "purists" insist that the only logical next step is to move the decimal point one more time—to 100 gigabits per second.

The limits on optical Ethernet bandwidth may just be the limits of fiber-optic bandwidth— perhaps 25 Terabits per second for the available spectrum on today's fiber, which is still well beyond the capabilities of today's lasers and electronics. Still, extrapolating from current trends gets us to that level in only 5 or 10 years (Moore's Law).

Paul is Product Manager, Business Marketing, Optical Data Networks, SBC. He teaches at DePaul University and can be contacted on paul.a.bedell@msg.sbc.com. *This article is an excerpt from his upcoming book,* ***"Gigabit Ethernet For Metro Area Networks"****, to be published by McGraw-Hill in Autumn, 2002. It will be available on Amazon.com, and at major bookstores.*

Speech Recognition

A Proven, Practical Technology

by Aki Sigle


Aki Sigle

A recent report by independent market analyst Datamonitor Technologies was clear: "Speech recognition allows businesses to take advantage of the ubiquity of the telephone […] and the increasing penetration of mobile devices, thus enabling them to improve customer service, generate new revenue and reduce costs. There are already numerous examples of implementations that have delivered high returns on investment and companies that don't seriously consider the opportunities that speech recognition offers them will miss out."[1]

Why? The following scenario (using a ficticious company) gives a compelling reason.

Company greeting: *"Welcome to the West Coast Product Support Hotline for Computerz 'R Us. If you already know the extension number of the agent responsible for your selected product, please dial it now. For product information please press 1; for technical problems relating to a previously purchased product press 2; for information on current promotions press 3; for the name of the nearest retail outlet press 4 or stay on the line, your call is valuable to us, an agent ..."*

Caller presses 1.

Company greeting: *"For information on hardware press 1 now, for software press 2, for peripherals and accessories press 3, for an update on our current modem promotion campaign press 4. To speak to an operator press 0 or stay on the line."*

Caller impatiently presses 4.

Company greeting: *"To receive information on the retail outlets participating in our modem promotion campaign, please press the first four letters of the name of your state."*

Caller (fuming) pounds out C A L l on the keypad.

Company greeting: *"Please press the first three letters of the name of your city followed by the number sign. To speak to an operator press 0, or stay on the line."*

Caller (gnashing teeth) presses 0.

Company greeting: *"All our operators are currently busy. Please stay on the…"*

Caller (livid): "?!@*#%X!" *and hangs up.*

Wanting to ensure that the customers' first (and frequently lasting) impression of a company is positive (i.e. beneficial to the company), corporate managers and telephony system administrators are increasingly turning to speech recognition technology.

Often referred to simply as "speech", it is an effective self-service-model technology that delivers high quality, readily accessible customer service, reduces the "DTMF-dread" that the conversation above points to, and can thus increase customer loyalty and retention. Plus, with operator costs accounting for a significant portion of any telephony investment (especially so in the burgeoning customer contact center environment), speech solutions that limit the need for operator intervention can control costs directly and significantly.

The above analysts' opinion simply recognizes that speech has gone way beyond its past reputation for being difficult to implement, unreliable and unproven. Thus more and more callers experience the following exchange:

Company greeting: *Welcome to the West Coast Product Support Hotline for Computerz 'R Us. To receive assistance, just say the name of the service you want. Your options are "Product Information", "Technical Assistance", "Retail Outlets", or if you're calling for the modem upgrade promotion, say "Modem Promotion".*

Caller: *Modem Promotion.*

Company greeting: *Please say the name of your state.*

Caller 3: *California*

Company greeting: *What city?*

Caller: *Sacramento*

Company greeting: *A list of our retail outlets and their contact information in Sacramento follows. At anytime you may simply say "Place an order" and you'll be connected to our order-taking agent.*

Caller: *Place an order.*

Company Agent: *Good afternoon, welcome to the Computerz 'R Us order desk. How can I help you?*

Answering the Call with Speech Telephony

The preceding exchange is typical of a speech-enabled call routing application; a caller simply says the name of a person, a service or a department, and the call is quickly transferred.

Such a speech application (a) quickly gets callers through to a human being without them spending time on keystrokes, especially with inquiries involving high branching factors (i.e. the caller at some point is faced with a long list of choices); (b) reduces the demands on agents for handling routine queries; (c) lowers the number of IVR ports needed in call centers to field incoming calls; (d) is normally implemented much more rapidly than IVR applications. That these benefits produce a rapid and significant return on Investment cannot be overemphasized enough.

The speech application prevents callers from either disconnecting or getting lost in a Gordian knot of touch-tone options. Even with a complex directory menu, a judiciously designed Voice User Interface (the speech telephony system's prompts and messages) can quickly guide the caller to where they want to go, using simple spoken commands.

Speech Recognition also efficiently combines with automatic response for static information retrieval and access to supply data. In such cases, analysts estimate that as much as 85 percent of routine contact center requests can be handled without agent intervention. Speech recognition thus gives the customer an important measure of control in accessing information 24 hours a day, seven days a week.

In the example above, the caller who wants to hear the list of retail outlets would be provided with detailed information such as:

Contact center: *The Computerz 'R Us outlet in Sacramento, California is at 0000 Johnston Ave. E., 10 blocks North of the intersection with Lincoln*

Boulevard. Opening hours are 9:00 A.M to 6:00 P.M weekdays and 9:30 A.M. to 5:30 P.M. on Saturdays. Telephone 916-xxx-xxxx. E-mail address is sales@computerz.com. If you wish to place an order please call during business hours and simply say "Place an order" to be connected to our order-taking agent.

Enhanced Customer Service

The ultimate goal of a front-end speech telephony solution is to have operators/agents working as efficiently and productively as possible with important clients. Speech applications can leverage the information supplied by telephone switches to rapidly route customers to the correct agents. For example, Computerz 'R Us also has a technical support hotline that receives calls nationally with callers using two main telephone numbers, one for PC Support, the other for Mac Support. A caller dialing 1 800 MAC HELP from a California location would experience the following exchange:

Caller 1IS for MAC Support

Contact center greeting: *Welcome to the California MAC Support Hotline for Computers 'R Us. Please name the product you need help with, such as, printer, keyboard, software, or missing pieces.*

Caller: *Software.*

Contact center: *Please name the software you need help with, such as QuarkXPress, Photoshop, or say 'General Help.'*

Caller: *Photoshop.*

Contact center: *Thank you. Transferring your call to a Photoshop support specialist.*

According to the CLID, DNIS and the caller's spoken choices, the caller received a location- and platform-specific greeting, a platform-specific software menu, and was routed to the right agent. When integrated with multimodal, multi-channel response systems to identify customers requiring more customized treatment, the speech telephony system can play a critical role in allowing agents to devote time to the most important requests.

Efficient Internal Auto-Attendant Capabilities

The same speech telephony solution (front-ending for contact center calls) can also do cost-effective double duty in providing highly efficient internal enterprise communications tools.

A speech telephony solution is ideal for offloading routine, time consuming employee calls from enterprises' operators; such calls have been estimated to represent 35 percent or more of all calls received by operators. Mobile workers can access telephony resources (such as conference calling and personal directories) with simple voice commands, from anywhere and using any telephone device. Speech eliminates having to memorize extension numbers; callers just specify a name in order for their call to be transferred.

By expanding employees' self-directed communication capabilities, speech solutions can not only give an important boost to workforce productivity, it also plays an important role in optimizing telephony infrastructure use from an internal communication perspective.

Telephony Integration

State-of-the-art speech telephony applications integrate seamlessly with digital and analog switches, IP networks and in Centrex service environments, easily supporting large call volumes. The speech telephony system can front IVR systems (but does not replace them); sends calls to the correct ACD queue where such a functionality is present; and supports call reporting tools and call accounting and call management systems allied with the enterprise telephony infrastructure.

Summary

With a much more powerful and user-friendly interface than traditional DTMF-based systems, speech telephony solutions increasingly occupy an integral part of enterprises' and contact centers' customer response options and internal telephony solutions. Keeping, as always, close tabs on the pulse of state-of-the-art telephony solutions, SBC Pacific Bell offers speech telephony applications from LocusDialog, the leading manufacturer of multi-lingual speech-enabled call-routing solutions (LocusDialogSTS™) for organizations of all sizes.

In the most recent past, financial services and airline contact centers have been the first to use speech telephony applications on a large scale. Benefits have included not only a reduction in caller waiting time, but also in significant cuts in 800 toll costs and the transferal of many call center employees and operators to crucial sales initiatives and customer service tasks. And in the vital area of user-friendliness, most such call center speech telephony applications consistently report a 50 percent decline in opt-outs to the operator (compared to DTMF implementations). That's a performance metric that no telecom manager can afford to disregard!

There are currently more than 600 LocusDialogSTS systems deployed in call centers and in other vertical market sectors such as healthcare, education and government. Given the established distribution/integration skills of SBC and LocusDialog, telecommunications consultants can be assured of being able to provide their clients with a best-of-breed speech telephony product.

The increasing demand for speech applications clearly has important ramifications for both application providers and telecom consultants. We need no further confirmation of this than from telecom analysts the Kelsey Group, which estimates "worldwide revenues from core speech technologies-automated speech recognition (ASR), text-to-speech (TTS), natural language understanding (NLU), embedded speech and attendant infrastructure hardware and software-will grow from $505 million in 2001 to more than $2 billion in 2006. The firm predicts this growth in core speech technologies will trigger a multiplier effect, driving voice-activated and enhanced telephony services revenues to $27 billion by 2006.

1.Quoted online in "Speech Technology Magazine e-blast," May 2002

This article is by Aki Sigle, SBC Pacific Bell Regional Product Manager, V-CPE & VoIP Solutions, in collaboration with Ormsby Ford, Communications and Marketing Editor, LocusDialog, and Stéphane Couture, Marketing Director, LocusDialog.

"Know the true value of time--snatch, seize and enjoy every moment of it!"

Lord Chesterfield

Interdependencies

Reassess your Vulnerabilities

by Heather Dobbins

- 43% of companies never reopen after a disaster. An additional 29% close within two years.
- 68% of businesses that lose their computers for more than seven days never reopen.
- Within two weeks of the loss of computer support, 75% of those organizations affected reach critical or total loss of business functions.

Heather Dobbins
Booz Allen Hamilton

Source: Gartner Study 1998

Undoubtedly you have been inundated with security statistics urging that you protect your networks and safeguard your information. Maybe security has been tacked on to your job description. Organizations often address security by increasing the responsibilities of their system administrators. Be cognizant of the threats, and plug the holes. Write security plans, and install intrusion detection systems. Such reactive behavior is increasingly ineffective in an economy so reliant on information technology and telecommunications and so interconnected with itself and the world. The statistics above are more sobering than most. Now question whether you would allow another entity to position your organization against such odds.

Interdependencies

As an organization, how many other businesses or other outside players do you rely on to operate? Do you have business alliances, partners, suppliers? Do you rely on electricity, telecommunications, and transportation to achieve your business mission? Rhetorical questions, but consider that Ford Motor Company, in the three days following the September 11 events, lost $30 million because suppliers could not cross the US/Canadian border to deliver parts. Reliance on other organizations increases risks—risks affecting operations, hence profit, and risks to your security posture.

Security risks associated with interdependencies arguably were best realized in the aftermath of September 11th . Ralph Shrader, chairman and chief executive officer of Booz Allen Hamilton and Mike McConnell, vice president with Booz Allen and former director of the National Security Agency, best describe the inherent risk of interconnectivity:

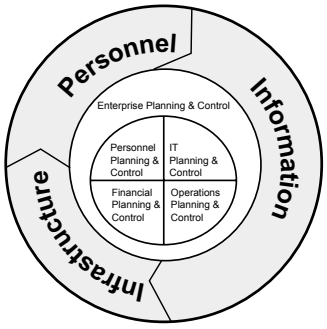
Bound intimately to the globalization of communications, finance, trade, and corporate activity, as well as to the deregulation and privatization of supporting infrastructures, interdependence risk is the potential for ostensibly small events—a trader covering derivatives trades, a rogue computer hacker, a fire in a supplier's factory—to spiral rapidly into a company threatening crisis.1

What to do about all those Interdependencies?

Integrate Security with Strategy

Protecting an organization from such a spiral involves tying the organization's business strategy to its security strategy. Through integration, security becomes integral to enterprise planning and control, operations planning and control, financial planning and control, personnel planning and control, and information technology (IT) systems planning and control.

Once security is embedded throughout an organization, potential threats can be



more thoroughly assessed and a richer risk management plan developed.

Reassess Vulnerabilities

Vulnerabilities can impact business operations in a number of ways:

- Increased liabilities
- Loss of operations
- Customer loss
- Damage to brand
- Loss of life
- Cost of recovery

Embedding security within an organization's operations means reassessing security vulnerabilities. With security integrated with all aspects of an enterprise (financial, personnel, operations, IT), the scope of vulnerabilities widens. In this model, vulnerabilities are not limited to potential network incidents. Assessing possible vulnerabilities becomes a bit more complex. Weak security policy is a vulnerability. An untested contingency plan is a vulnerability. Relationships with an electric provider and financial institutions are potential vulnerabilities. All your interdependencies with other companies and infrastructures become potential vulnerabilities. Input from upper management, those responsible for operations, personnel, IT, finance, and enterprise strategy is required to get an accurate view of potential threats—somewhat of a departure from the security engineer sitting down with the systems administrators to assess vulnerabilities.

Once vulnerabilities are identified, there are steps organizations can take to protect themselves.

- Identify the organization's critical assets and associated infrastructure dependencies necessary to fulfill the organization's most critical functions. Determining and even prioritizing critical functions allows a more focused approach to assessing and managing risk.
- Conduct a risk assessment taking into account the new vulnerabilities and develop an integrated risk management program. This risk management program is the foundation for a strong security posture.

Other best practices include[2]:

- Position a security office high within the company's organization and provide the authority and resources to develop and enforce an adequate security program.
- Reassess the company's disaster recovery plan in light of potential new threats to the new business security model.
- Understand the risk/reward payoff for security options and sequence the rollout of a new security program to address the worst risks first.
- Review and update, review and update, review and update.

Share Information

A final best practice is to develop working partnerships with other industry members, and local, state and federal government entities. The United States relies heavily on Internet communications and commerce. As a result, our infrastructures are increasingly interconnected, interdependent, complex, and vulnerable. Remember the train wreck in a Baltimore tunnel last year? Networks in Seattle and Los Angeles slowed as a result. For a few days, adventurers in Michigan were not able to make campground reservations by phone. Think of the effects of 9/11.

Strengthening partnerships, public-private, public-public, and private-private is key to furthering understanding and securing our interdependencies and vulnerabilities as a nation. The government has been examining interdependencies, especially among the nation's critical infrastructures3 for years. Industries have developed information sharing and analysis centers (ISACs). The government's Critical Infrastructure Assurance Office (CIAO) facilitates an industry Partnership for Critical Information Security (PCIS). The Government is working to update its first National Plan for Information Systems Protection. The private sector is working to contribute its plan by industry. Daily news is saturated with homeland security issues-the pros and cons of creating a cabinet-level agency, of creating security standards. We all know the story. We've been inundated with statistics. Now let's pull it together. What better way to address interdependent vulnerabilities than through an integrated security program—strategy and security. Just remember to include input from all "senior management."

Heather is a member of Booz Allen Hamilton's Information Technology Team. Based in San Francisco, she has worked with numerous government agencies and industry groups to promote awareness and implement security programs and policies.

1 Ralph W. Shrader and Mike McConnell, "Security and Strategy in the Age of Discontinuity," strategy+business, First Quarter 2002.

2 Best practices are derived from Shrader & McConnell, "Security and Strategy."

3 Including transportation, electric power, oil and gas, telecommunications and information technology, finance networks and institutions, water, emergency services, and government services.

continued from page 11

- not apply to Lifeline accounts
- Is a flat monthly charge (not based on usage)
- Is billed on a per line basis
- Applies to all lines capable of dialing out on the local network, therefore capable of reaching a "ported" number

The Service Charge may be applied in ratio format to certain products, e.g., Centrex, PRI ISDN, PBX trunks. The effective rate as of July 7, 1999 is $.34 per line.

State Regulatory Fee

Formerly known as the CPUC Surcharge, the California Public Utilities Commission Reimbursement Fee was established by State Legislature in 1983 and is paid by the utilities to fund regulation by the CPUC.

It applies a monthly percentage to:

- Monthly service
- Nonrecurring charges
- California Billing Surcharge
- Universal Service Fund Surcredit
- Intrastate calls
- Intrastate directory assistance

The effective rate as of 7/16/96 is 0.11%.

Universal Lifeline Telephone Service Surcharge

Imposed by the CPUC to help subsidize the Gwen Moore Fund for Universal Lifeline Telephone Service, it is billed to all customers, Business and Residence.

It applies a monthly percentage to each subscriber's intrastate services.

- Includes recurring and nonrecurring rates and charges
- Toll charges
- California Billing Surcharge
- Universal Service Fund Surcredit
- Interexchange Carrier's portion of bill carries surcharge portion covering intrastate service and calls carried by carrier

The effective rate as of 7/1/01 is: 1.45%

Universal Service Fund Surcredit

This fund was established to refund revenue until such time as individual rates for products and services are adjusted. It applies a monthly percentage to all regulated charges for:

- Recurring and nonrecurring rates
- Service or equipment provided under Pacific Bell's tariffs
- Applies to resellers for local competition

The temporary effective rebate rate from 2/1/02 to 4/30/02 had been 29.143% and as of 5/1/02 is zero percent.

With over a dozen different types of taxes and surcharges on your SBC Pacific Bell bill imposed by regulators and government entities, you now have a resource to turn to when someone asks you why they pay these charges.

(Tom is a Liaison Manager with a Masters Degree in Business Administration. He's also a Scoutmaster. We think he should receive a Special Merit Badge (SMB) for trying to explain this "taxing effort.")

BusinessWeek has recognized SBC as the highest ranked Telecom Company in its annual InfoTech 100 List.

"The Zest of Life is made up largely of anticipation. We get more enjoyment in striving for than in having the things we want."

C.E. Curry

Upcoming Feature

Health Information Services, a Jagdish Kohli SPECIAL REPORT, will appear in our next issue.

Challenges & Solutions

Challenges

Do you or your clients:

--Spend too much on local usage and local toll usage?

--Have separate vendors for different services?

--Have Telecom coordinators who spend hours figuring the true costs of your service?

--Have Discount Calling Plans but a few months after you sign, the rates increase?

--Have multiple locations, each with separate charges?

Solutions

SBC Pacific Bell CompleteLink may be just the solution for you! It helps you save on your whole calling package. By letting us be your single telecom provider, you get quality, reliability and rewards. You can tailor your package to suit the size and scope of your business and it grows with your business and advances with new technologies. You select an annual spending level and we discount your rates.

First, you receive low flat rates on all your local calls, intraLATA toll calls, Custom 8 toll free and calling cards calls*. Then we give you a total volume discount on those toll calls, plus discounts on other eligible products/services. In conjunction with your total-volume discount, you can:

-- Group your telecom services to save on the overall package.

-- Combine spending across multiple accounts in Northern and Southern California.

-- Group up to 250 accounts.

-- Choose higher volume and longer contract terms to save more.

-- Get easy-to-read SBC Pacific Bell billing that includes precise savings statements every month.

And, **SBC Pacific Bell CompleteLink** requires no special equipment.

Further Benefits:

-- Options for 1, 3 or 5-year contracts. The higher your Minimum Annual Revenue Committment and the longer the contract, the greater the discount.

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

-- Multi-year contracts allow you to take advantage of the greatest discounts. If you wanted to add special services like ISDN or ADTS-E lines, you may save enough with CompleteLink to add these services.

-- Reliance on a $30 billion telecom company with diverse resources, technology solutions and customer service.

There are so many more benefits of **CompleteLink**, let us tell you all about them. Contact your Liaison Managers (1-800-552-5299) for all the details.

--Kathi Peterson
Associate Director
SBC Pacific Bell

* SBC Pacific Bell FCC Interstate/IntraLATA calls do not qualify for CompleteLink discounts. SBC reserves the right to bill the customer the tariffed, standard rates for these calls, including the ability to adjust billing or back bill to reflect the proper rate.

SBC Pacific Bell President Chuck Smith with CVSG Team

"It's not how much we do but how much love we put in the doing."

Mother Teresa

Thank you for reading Update