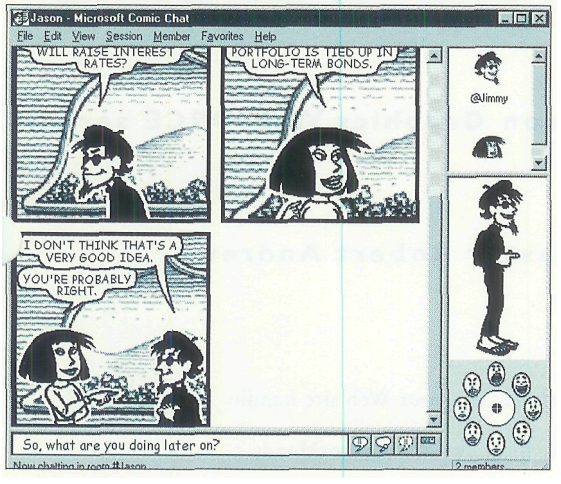
transform a static Web site into a "personalized one-to-one relationship with customers and partners," according to Microsoft literature.

For example, Normandy technology will allow users to custom-tailor their Web pages to suit their interests. By answering a series of questions upon first accessing a site, users can receive "personalized" news threads. This is due to the server's support for content personalization, as Microsoft calls it, which lets the software retain information about each user, and deliver that user's sought-after active content automatically. This process is refined over time, based on user queries, after the initial user profile is established.

While this is nothing new to many Usenet and other news service users, Microsoft hopes it will become much more widely available with the release of Normandy to general-purpose business users.

"One of the most interesting things we've found from customers is that many users are interested in the threaded forums and chat rooms available on CompuServe and America Online," says Michael Ahern, product manager for Internet platforms and tools at Microsoft. "That capability, if you look at the entire Internet today, is very small. This announcement means that many more people will have access to that kind of communication."



Microsoft's Chat Server, part of the Normandy line, enables real-time, one-to-one, one-to-many and many-to-many conversations among users.

The release of the first Normandy servers for general business users coincides with Microsoft President and Chief Executive Officer Bill Gates' keynote speech at October's UNIX Expo in New York. There, Gates outlined the company's plans to make Windows NT the server of choice for the corporate Internet and intranet, and, indeed, spent the bulk of his hour-long speech convincing show attendees that the company is addressing scalability and performance issues in the server software. That, he said, coupled with low-cost, high-performance PC hardware, will provide an Internet platform that can compete with today's workstations.

Of course, he compared prices and relative performance with arch-enemy Sun Microsystems Inc.'s more expensive boxes and got a few jibes in to further remind us of the two companies' ongoing jousting.

Analysts say they view the initial availability of the Normandy line as a logical extension of Microsoft's presence among commercial on-line server providers, where it had been supplying Internet server software to the likes of America Online Inc. and CompuServe, in addition to providing its own on-line service, Microsoft Network.

"They essentially said that the bottom line is we've got the technology so let's make it more widely available," says Ted Julian, Internet research manager at International Data Corp., Framingham, MA. "Initially, they targeted Internet service providers and on-line services, and then when they looked closely at the various components, such as mail, chat and news, they said, 'aren't these things everyone would want?' Companies that would be interested in these servers could really be any size."

If there is one big question mark regarding the Normandy server line, it is the suitability of Windows NT as the Internet server of the future for corporations. While this may seem a foregone conclusion given Microsoft's hegemony over the business world, the company can't retain that grip, no matter how iron-clad, if its products don't deliver the goods.

Says IDC's Julian: "As far as Windows NT goes as an Internet server, they've still got to prove themselves. That goes for reliability and scalability, and use for mission-critical applications. We hear about people raising warning flags about scalability, even if you only have 10 to 20 users on it."

He also adds, however, that NT is a relative newcomer on the corporate scene and scalability "doesn't just sprout when operating environments are born." Bugs will occur and, over time, will be addressed and the software improved. In at least this area, Julian says, UNIX has the advantage of years of maturation and refinement.

And the truth of the matter is, many corporate users don't want to learn UNIX, despite its prowess as a network operating environment. They'd rather choose the path of least resistance and stick with Microsoft, despite the lumps and bumps of its still immature NT server and operating environment.—*jsw*

Phone Network Headed for Disaster?

Dial-up Internet service providers may be jeopardizing the nation's public switched telephone network (PSTN), according to a study issued this summer by Bell Communications Research, or Bellcore.

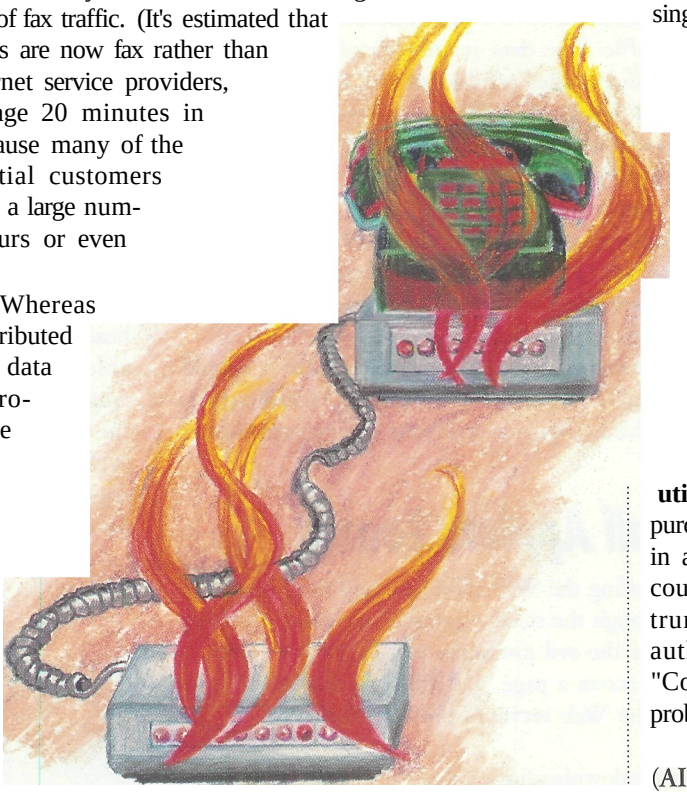
The report, "Impacts of Internet Traffic on LEC Networks and Switching Systems," by Amir Atai and James Gordon, says that telephone calls to Internet service providers are fundamentally different than the kinds of telephone calls the system has been used for until now. As a result, the report concludes, this traffic is "challenging the engineering, forecasting, planning and operational procedures established by the former Bell System over the past 80 years."

That could spell disaster for the nation's phone system, according to Atai and Gordon. If telephone companies are not able to properly plan for the network's expansion, the demands placed on the phone system by people

trying to access the Internet could result in busy circuits, call disruptions and even the loss of dial tone in some areas. Already, the researchers say, many of the regional Bell operating companies (RBOCs) have reported problems as a result of Internet use.

The report's authors say Internet access threatens the nation's phone network because it is fundamentally different from the typical voice traffic that the network was engineered to carry:

• **Call Durations.** The telephone network was engineered for calls that average three minutes in length. Indeed, the average length of calls has been steadily dropping over recent years, thanks to answering machines and the increase of fax traffic. (It's estimated that half of all international calls are now fax rather than voice.) Calls to local Internet service providers, on the other hand, average 20 minutes in length. Furthermore, because many of the calls come from residential customers who have free local service, a large number of calls last many hours or even many days.



• **Calling Patterns.** Whereas normal voice calls are distributed throughout the network, data calls to on-line service providers tend to concentrate telephone traffic from an entire metropolitan area into a single telephone exchange. That can quickly saturate all of the trunks that reach into the exchange. As a result, callers trying to reach other homes or businesses via the exchange may get busy signals, because the trunk lines reaching into that particular central office are all busy.

Industry insiders who have seen the report say it is really part of a long-standing campaign by the RBOCs to convince the Federal Communications Commission to eliminate a special exemption from access fees to the nation's telephone network. These fees are paid by long-distance providers and other companies that wish to interconnect their networks with the nation's public switched telephone networks. Access fees range from 2 to 5 cents per minute and are "typically 40% to 45% of the cost of a long-distance call," says Kevin Werbach, an Internet specialist at the FCC.

"We believe the access charges that the local exchange companies are charging are really exorbitant. They are way above cost, and they need to be brought down," says Mike Miller, a spokesman for AT&T, which recently got into the Internet service provider business itself. "We think that when the local exchanges bring down the access charges to a more reasonable level, something approaching costs, then that is the time to look at bringing the access fees for the data circuits into line with the other charges."

Besides, says Miller, "on-line services are a long way from being the only calls that result in long holding times. Teenagers talking to their friends result in long holding times. Conference calls result in long holding times. Lengthy faxes, possibly the kind you sent me on Friday, result in long holding times."

But there is a big difference between teenagers talking on the telephone and teenagers chatting with each other over an on-line service like America Online, says Atai. In the first case, the teenagers' telephone calls both originate and terminate over a large geographical area. In the second case, the phone calls originate throughout an entire region but all terminate in a single exchange.

Bellcore also denies the charge that its research is politically motivated. The company says it has simply identified a problem that needs to be solved if the nation is to continue to have a reliable telephone service.

Indeed, the Atai/Gordon report identifies seven different solutions to the problem-several of which could benefit companies that directly compete with the RBOCs:

1. **Managed Trunking Solution.** ISPs could simply continue to purchase telephone lines that terminate in a switch, and telephone companies could ensure that there is sufficient trunk access to those switches. The authors do not like this solution. "Congestion is likely to be a chronic problem on ISP lines," the authors state.

2. **Automatic Identified Number (AIN) Routing/Numbering Solution.** Telephone companies could program their switches to recognize the telephone numbers of popular ISPs and automatically route those calls to a special switching system that has sufficient capacity to handle data calls, "or route them out of the PSTN entirely and use a packet network to concentrate the data transport for transport to the ISP."

3. **Modem Pool in Central Office/ Post-Switch Adjunct.** Instead of having the ISPs operate their own modems, they could be operated for the ISPs by the RBOCs themselves. "This implementation may provide a more attractive interface for the ISPs–maintenance of large modem pools is an acknowledged problem." The report further notes that this solution would allow ISPs to cover a wide geographical area at comparatively low cost.

4. **Packet Mode ISDN.** Telephone companies could speed deployment of ISDN, a digital system. Normally, people accessing the Internet over ISDN do so using one of ISDN's circuit-switched channels. But ISDN also has provisions for packet-switched data. This could be used for a low-speed, full-time connection to the Internet. One barrier to this approach, though, is that few ISPs are currently equipped to handle packet-mode ISDN.

5. **Pre-Switch Adjunct.** Telephone companies could place modems directly on customer telephone lines in the telephone company central office. Data calls could be intercepted before they reach the public switch and handed off to an appropriate data network.

6. **Asymmetric Digital Subscriber Line.** ADSL is a new technology for carrying both voice and very high-speed data traffic. The data is intercepted from the subscriber's line before it reaches the switch and handed off directly to a data network.

7. **Cable Modems.** Customers could forsake the telephone network entirely and get their Internet traffic from cable modems. "The public switched telephone network was not designed for this application," says Atai.

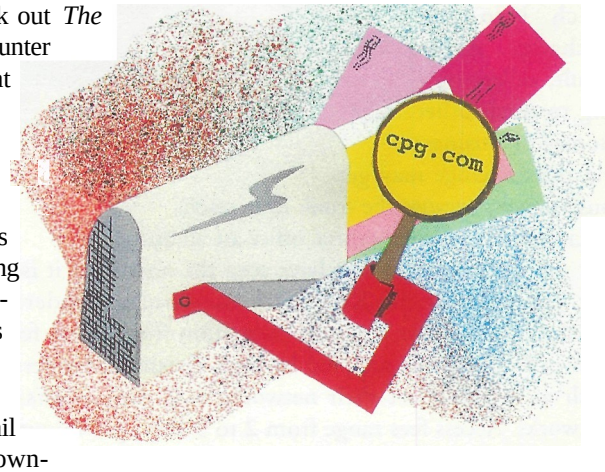
Atai thinks that as the number of Internet users grows and they want faster access to the network, there will be an economic incentive to develop very efficient, high-speed, low-cost ways of providing bandwidth to users. But that future system probably won't resemble today's Internet service providers, running large modem banks and receiving telephone calls from all over a wide metropolitan area.

"In general, engineering of packet networks is lagging behind where it should be," says Gordon. "Most of this stuff is still done in terms of switched virtual circuits rather than true packet technology. I think that it is a matter of the [telephone] industry improving its expertise."–*slg*

Threat of Hostile Email Applets Looms

For many users, part of the allure of surfing the Web is the anonymity of it all. On the Web, no nosey librarians peer through the stacks, trying to see who's browsing the Marquis de Sade section, or give you the evil eye when you check out *The Communist Manifesto.* On the Web, you access a page, and while a counter might register that *someone* was there, the Web server is blind to that persons identity. Right?

Not necessarily. That is, not if you are downloading Java applets. It would in fact be very easy–not to mention legal–for a Java applet that you downloaded to obtain your user name and IP address without you knowing it. This happens when the downloaded applet, which is now running locally on your machine, "phones home" to its originating host and connects to the SMTP port (port 25). Once that SMTP connection has been established, the applet-without your consent-has access to your IP address and, depending on how your sendmail is configured, your user name as well.



CPG

The upshot of this Java feature is the potential for hostile email applets. So, what is a hostile applet? "Any applet which, when downloaded, attempts to monopolize or exploit your system's resources in an inappropriate manner," says Mark LaDue, assistant professor of mathematics at Georgia Tech University in Atlanta.

Professor LaDue has written several hostile applets, which he has published on his Web page (http://www.math.gatech.edu/~mladue). In particular, he uses the SMTP port loophole to write applets that forge email and gather email addresses. Also, you can witness an email forging applet at work by accessing Jim Buzbee's page, http://www.nyx.net/~jbuzbee/mail.html (Buzbee is a group software engineer at Lockheed Martin Corp.).

Of course, the issue of whether or not these hostile applets constitute security breeches is still being hotly debated. When asked about the so-called hostile email applets, Marianne Mueller, security analyst at JavaSoft, says she "does not regard this as a security problem." The jury is still out on how private email addresses are, Mueller says. They certainly are no more private than street addresses, which are regularly collected and resold. And as far as forging is concerned, people have been forging email addresses since the dawn of sendmail. If a Java applet is used to exploit that program's weaknesses, then you cannot blame Java, Mueller explains.

However, Ed Felten, assistant professor of computer sciences at Princeton University, and author of the upcoming book *Java Security: Hostile Applets, Holes, and Antidotes,* says that "Java adds a new twist" to the issue. Felten explains that if you look closely at the header files of forged email, you will be able to see the host from which the email originated: the host from which the hostile applet first came. But, Felten says, email forged with this kind of applet "seems much more convincing." Felten adds that "perhaps Sun hasn't warned people enough about what kind of information leaks [e.g., user names] might happen when you run a Java applet."

JavaSoft might not consider these email applets security violations, but that hasn't prevented some software vendors from responding to users who think they are. Finjan Software (http://www.finjan.com), based in Netanya, Israel, sells a product called SurfinBoard,