National Security and Emergency Preparedness

Telecom News

2000, Issue 3

Published by the Office of the Manager, National Communications System, for the national security and emergency preparedness (NS/EP) community

TABLE OF CONTENTS

Raytheon's Burnham is New NSTAC Chairman

By Steve Barrett, Customer Service Division, OMNCS

President Clinton appointed Raytheon's Daniel P. Burnham as the new Chairman of the President's National Security Telecommunications Advisory Committee (NSTAC), effective September 25, 2000.

Burnham is Chairman and Chief Executive Officer (CEO) of Raytheon Company, headquartered in Lexington, Massachusetts. He replaces Van B. Honeycutt, the President, Chairman, and CEO of Computer Sciences Corporation (CSC). Honeycutt became the NSTAC Chairman in September 1998.

The President's NSTAC is composed of up to 30 Presidentially appointed industry leaders (usually chief executive officers). In its advisory role to the President, the NSTAC provides industry-based analyses and recommendations on a

See New Chairman, page 3

Daniel P. Burnham, Chairman, President and CEO of Raytheon Company, accepts the gavel from White House National Security Advisor Samuel Berger as he assumes the position of chair for the President's National Security Telecommunications Advisory Committee. Burnham became the NSTAC Chair on September 25, 2000, replacing Van Honeycutt, Chairman, CEO, and President of Computer Sciences Corporation. (White House photo)

NS/EP Telecom News is published quarterly under the auspices of Ms. Diann McCoy, Deputy Manager, National Communications System (NCS), to provide readers with analytical reports on issues relating to NS/EP telecommunications. Articles printed herein are for informational purposes only and do not necessarily represent official OMNCS or NSTAC positions. We invite NCS member organizations and other readers to comment on articles and suggest future topics for consideration.

▲ ▲ ▲

For further information or additional copies, please contact:

Stephen Barrett
Office of the Manager
National Communications System

Customer Service Division
701 S. Court House Road,
Arlington, VA
22204-2198

PHONE: (703) 607-6211
FAX: (703) 607-4826

Home Page:
http://www.ncs.gov

Internet Security Requires Collaboration

Editorial by Guy L. Copeland, Computer Sciences Corporation

The very trait that has sparked the Internet's phenomenal growth—an open and free environment—poses a major threat to its survival. This free-flowing environment, coupled with the growing mission-critical use of the Web by industry and Government, requires a delicate balancing act between preserving open access and improving security.

The recent Love Bug computer virus, which followed a rash of distributed denial-of-service attacks on major Web sites, underscores a harsh reality: no one is truly safe from attack. So far, these attacks have not had devastating consequences, but we may not be as lucky next time. It's inevitable that more attacks will occur, and some may cause far worse repercussions than temporary denial of service, digital disruption and slowing of e-mail.

Because hackers tend to target large computer systems connected to high-bandwidth networks, large organizations will remain vulnerable until industry and Government work closer together to address the problem. Absolute security may never be achieved, but much can be done to reduce the impact of future attacks.

President Clinton's announcement in February 2000 that the Government would begin exploring ways to tighten Internet security is a step in the right direction. His meeting with industry representatives brought renewed visibility to the need for better security. Government can lead by example in helping remove barriers to collaboration, for instance, and by crafting international agreements that foster open access, innovation and privacy while reducing security risks.

Without compromising the openness of the Internet, companies in the information technology industry, Internet Service Providers (ISP) and Government agencies must work cooperatively on a global basis. They must ensure that security tools and procedures are sophisticated enough, and that system administrators have sufficient information to thwart future attacks.

In addition, companies and Government agencies alike need to establish and enforce security policies, install more secure operating systems, increase training and undertake internal vulnerability assessments—even enlisting "white-hat hackers"—to probe for network vulnerabilities. Compromising security for speed, convenience or cost is a dangerous trade-off.

The ISP community must do its part to help filter out suspicious Internet traffic. Procedures should be established to examine network-traffic anomalies. Statistical

analyses of volume and content, for example, may help define thresholds that could trigger access limitations. One reason it's so difficult to defend against hackers is that the current environment, in which users are difficult to trace, makes it virtually impossible to find and cut off the responsible parties in a timely manner. Systems that are poorly configured, or left inactive or unmonitored, are prime targets for exploitation.

We need to establish effective processes and forums where all sectors share information to reduce the likelihood of cyber-attacks, or at least minimize their impact. This can be done through cooperative efforts such as the President's National Security Telecommunications Advisory Committee (NSTAC), which provides industry advice to the President on matters regarding national security/emergency preparedness telecommunications and information systems.

Finally, we need to educate Internet users from an early age. Last September, a host of high-tech companies joined with the Information Technology Association of America and the Department of Justice to create an alliance promoting computer ethics and civic responsibility to students as young as 8 years old.

"We need to educate Internet users from an early age."

The alliance, called the Cybercitizen Partnership, is driven by the belief that Government and industry, working together, can better protect information and systems. Its goals are to develop awareness of the dangers and consequences of cyber crime, increase cooperation to enhance the protection of the Internet and, perhaps most importantly, promote the evolution of a creative and secure cyber culture. These goals are truly ambitious, but essential to our future.

Guy L. Copeland, Vice President of Information Infrastructure Advisory Programs for Computer Sciences Corporation (CSC), acts as a liaison with Government and industry in matters pertaining to security issues and protection of critical infrastructure. He is the company's full-time representative to the NSTAC's Industry Executive Subcommittee.❖

(Courtesy of Computer Sciences Corporation)

New Chairman, cont'd from page 1

wide range of policy and technical issues related to telecommunications, information assurance, infrastructure protection, and other national security and emergency preparedness concerns.

Prior to his arrival at Raytheon in July 1998, Burnham served with AlliedSignal, holding a variety of leadership positions. He most recently served as Vice Chairman and as a member of the company's Board of Directors.

He joined AlliedSignal in 1982 as Vice President and Controller, then served 2 years as Vice President and General Manager of the Engineered Plastics Division in AlliedSignal's Engineered Materials Sector. In 1986, Burnham was named President of the sector's Plastics and Performance Materials Group. Two years later, he was named President of its Fibers Group.

In 1990, he joined the company's Aerospace Sector and served as President of its AiResearch Group. From 1992 to 1997, Burnham served as President of AlliedSignal Aerospace, AlliedSignal's largest business and the world's largest supplier of equipment and subsystems to the aerospace industry.

Prior to joining AlliedSignal, he held positions of increasing responsibility with The Carborundum Company from 1971 to 1982.

Burnham received a bachelor's degree in 1968 in economics from Xavier University in Cincinnati, Ohio, and a master of business administration from the University of New Hampshire in Durham, New Hampshire, in 1970.

He is the Chairman of the Board of Governors of the Aerospace Industries Association (AIA), a trustee for Xavier University, a member of the Business Council, and a member of the FleetBoston Financial Corporation Board of Directors.❖

Six Others Named to NSTAC, Sugar Departs for Litton Position

By Steve Barrett, Customer Service Division, OMNCS

In addition to naming Raytheon's Daniel Burnham as the new chair of the President's National Security Telecommunications Advisory Committee (NSTAC), President Clinton has named six other senior executives to the committee since March 2000.

Prior to the NSTAC XXIII conference on May 16, 2000, in Colorado Springs, Colorado, the President officially named Clayton M. Jones of Rockwell International, John T. Chambers of Cisco Systems, and Dr. Ronald D. Sugar of TRW to the NSTAC. Soon after the meeting, the President announced that G. William Ruhl of the D&E Telephone Company (representing the U.S. Telecom Association), Craig Mundie of Microsoft and Christopher Galvin of Motorola would also become members.

The President's National Security Telecommunications Advisory Committee, established by Executive Order 12382, provides the President with technical information and advice on national security telecommunications policy. Up to 30 members from the telecommunications and information technology industries may hold seats on the NSTAC.

Clayton M. Jones, President of Rockwell Collins, was named to the President's National Security Telecommunications Advisory Committee by President Clinton on April 26, 2000. (Photo courtesy of Rockwell International)

Mr. Jones, a native of Nashville, Tennessee, was named to NSTAC on April 26, 2000. He is President of Rockwell Collins and is a corporate officer and Senior Vice President of Rockwell International. Mr. Jones assumed this position in January 1999, having served as Executive Vice President of Rockwell Collins since November 1996.

Before becoming Executive Vice President, Mr. Jones served as Vice President and General Manager of the Collins Air Transport Division, a position he was appointed to in September 1995. Earlier that year he was appointed Corporate Senior Vice President of Government and International Operations in Washington, D.C., where he represented all Rockwell businesses to international and domestic customers.

He joined Rockwell International in 1979 as senior marketing representative after serving in the U.S. Air Force as a fighter pilot. A graduate of the University of Tennessee, Mr. Jones also holds a master's degree in business administration from George Washington University in Washington, D.C.

Currently, Mr. Jones serves on the Board of Directors of the General Aviation Manufacturers Association. He is also a member of the American Institute of Aeronautics and Astronautics (AIAA) and has served as Vice President, Public Policy, as well as a member of the AIAA Board of Directors.

In addition, Mr. Jones is a member of the Board of Directors of the Cedar Rapids, Iowa, Area Chamber of Commerce and of the Cedar Rapids Symphony Organization. He is also a member of the Iowa Business Council.

On May 4, 2000, President Clinton appointed Mr. Chambers to serve on NSTAC. Mr. Chambers is President and Chief Executive Officer (CEO) of Cisco Systems, the worldwide leader in networking for the Internet and joined the company as the second in command when Cisco had $70 million in annual sales and a market cap of $600 million.

During the past 3 1/2 years as President and CEO, Mr. Chambers has led Cisco from $1.2 billion in annual revenues to its current rate of $10 billion by establishing leadership in key technology sectors of the networking industry and aggressively pursuing new

John T. Chambers, President and Chief Executive Officer of Cisco Systems, was named to the President's National Security Telecommunications Advisory Committee by President Clinton on May 4, 2000. (Photo courtesy of Cisco Systems)

market opportunities.

Among other distinctions, Mr. Chambers was named to UPSIDE Magazine's 1998 UPSIDE Elite 100 list and was also designated "CEO of the Year" for 1997 in a poll of industry executives conducted by Electronic Business magazine. In addition, BusinessWeek voted him one of its top 25 managers in 1996. Mr. Chambers also serves on President Clinton's Committee for Trade Policy.

Mr. Chambers joined Cisco in January 1991, as Senior Vice President of Worldwide Operations. He was promoted in May of 1994 to Executive Vice President with responsibilities for Research and Development, Manufacturing, Worldwide Sales, Marketing and Support. Prior to joining Cisco, he spent 8 years at Wang Laboratories, the last 2 as Senior Vice President of U.S. Operations. Mr. Chambers began his career by spending 6 years with IBM.

Holder of a master of business administration in finance and management from Indiana University, Mr. Chambers received a doctorate and his undergraduate degree in business from West Virginia University.

Dr. Sugar, of Moreland Hills, Ohio, became an NSTAC Principal on March 7, 2000. At the time of his appointment, he was President and Chief Operating Officer of TRW Aerospace and Information Systems as well as a member of TRW's Chief Executive Office and Management Committee. Upon joining the TRW staff in 1981, Dr. Sugar directed advanced research and development programs.

G. William Ruhl, Chief Executive Officer of D&E Telephone Company and a board member of the U.S. Telecom Association (USTA), has joined the President's National Security Telecommunications Advisory Committee. President Clinton approved the nomination on July 26, 2000. (Photo by Theodore E. Chavez, U.S. Space Command)

Dr. Ronald D. Sugar—appointed to the President's National Security Telecommunications Advisory Committee on March 7, 2000—departed TRW to become the President and Chief Operating Officer of Litton Industries. TRW has nominated David Cote to replace Dr. Sugar on the NSTAC. (Photo courtesy of TRW)

However, Dr. Sugar departed TRW soon after the NSTAC XXIII meeting and accepted the position of President and Chief Operating Officer of Litton Industries, Inc. TRW has nominated David M. Cote, its President and Chief Operating Officer, to replace Dr. Sugar on the NSTAC.

In his role with NSTAC, Mr. Ruhl represents the United States Telecom Association (USTA) where he currently serves as one of its Board members. As the Chief Executive Officer of D&E Telephone Company—a subsidiary of D&E Communications Inc.—Mr. Ruhl is responsible for the engineering, construction,

information systems, customers service, planning, and central office departments. He is also Senior Vice President of D&E Communications, Inc., where he is responsible for strategic planning.

Mr. Ruhl came to the D&E Telephone Company in 1991 as Senior Vice President. He supervised Red Rose Communications, Inc.—now known as D&E Telephone and Data Systems—which provides telecommunications systems sales and service as well as personal communications products throughout a 10-county area of south central Pennsylvania. Prior to joining D&E, Mr. Ruhl served at Bell Atlantic Corporation and Bell of Pennsylvania for 30 years.

In addition to serving on the Boards of D&E and USTA, Mr. Ruhl also serves with the Alliance for Telecommunications Industry Solutions (ATIS) and Technology Council of Central Pennsylvania. He is also a member of the Kutztown University College of Business Advisory Council and the Lancaster County Economic Development Company's International Trade Steering Commerce.

He is a graduate of Lehigh University with degrees in electrical engineering and is a licensed professional engineer in the State of Pennsylvania. In his spare time, Mr. Ruhl performs with the Central Pennsylvania Symphony and serves as President of its Board of Directors.

Craig Mundie, Microsoft's Senior Vice President of Consumer Strategy, became one of six new members to the President's National Security Telecommunications Advisory Committee. President Clinton approved the nomination on July 26, 2000. (Photo courtesy of Microsoft)

As Senior Vice President of Consumer Strategy, Mr. Mundie reports to Microsoft CEO Bill Gates and works with him on developing a comprehensive strategy for Microsoft's offerings to consumers. In addition, he coordinates implementation of the products and services across all Microsoft product groups. Mr. Mundie focuses on refining Microsoft's vision for Web lifestyle products and services.

From 1992 until November 1998, Mr. Mundie formed and ran the Consumer Platforms Division, which developed Microsoft's non-PC platform and service offerings. This included the development of the Windows CE operating system, the Handheld PC, Palm-size PC and Auto PC. He also started Microsoft's digital TV efforts and acquired and managed the WebTV Networks Inc. subsidiary.

Mr. Mundie also continues to be responsible for representing Microsoft in Washington, D.C., in policy-related activities including critical infrastructure security, encryption and telecom regulation. He also coordinates all standards-related activities for Microsoft in areas related to current and future consumer technologies.

Before joining Microsoft in 1992, Mr. Mundie was a co-founder and CEO of Alliant Computer Systems Corp., where he led the development of the CAMPUS Massively Parallel Supercomputer System. Before assuming the role of CEO at Alliant, Mr. Mundie served in various roles, including vice president of research and development and vice president of marketing.

Mundie attended the Georgia Institute of Technology (Georgia Tech) in Atlanta, Georgia. He received a bachelor's degree in electrical engineering and a master of science degree in information theory and computer science.

On October 26, 2000, the President named Mr. Galvin, Chairman and Chief Executive Officer of Motorola, Inc., to the NSTAC. Mr. Galvin began his service with Motorola in 1973. In May of 1988, Mr. Galvin was elected to the Board of Directors of Motorola, Inc. and assumed the positions of Chairman and Chief Executive Officer in 1997. Mr. Galvin is a Director of the Rand Corporation and the Illinois Coalition for Science and Technology.

Mr. Galvin received his bachelor of science degree from Northwestern University and his master of science degree in Management from the Kellogg School of Northwestern.❖

CSC's Honeycutt Thanked for Service as NSTAC Chair

White House National Security Advisor Samuel Berger (left) presents a plaque to Computer Sciences Corporation Chairman, Chief Executive Officer and President Van B. Honeycutt for serving as Chair of the President's NSTAC. Honeycutt chaired the Presidential Committee from September 9, 1998, until September 25, 2000, and remains an NSTAC Principal. (White House photo)

National Communications System Assigned to Administer Priority Access Service

By David Scott, Operations Division, OMNCS

The Federal Communications Commission (FCC) has assigned the Office of the Manager, National Communications System (OMNCS) responsibility for the day-to-day administration of Priority Access Service (PAS), effective October 10, 2000. The NCS will support any national security and emergency preparedness (NS/EP) user request on or after October 1—if and when wireless providers offer the service. The FCC will maintain oversight responsibility.

In an FCC Second Report and Order dated July 13, 2000, the FCC determined there is a need and demand for PAS, by Government agencies at all levels and by non-Government NS/EP personnel, such as those working in public utilities, medical services and facilities and transportation.

The FCC determined there is a need and demand for PAS.

This Report and Order will permit, but not require, commercial mobile radio service (CMRS) providers to offer PAS to NS/EP personnel. PAS will allow authorized NS/EP users in emergencies to gain access to the next available wireless channel. However, PAS calls would not preempt calls in progress.

Although the offering of PAS by wireless service providers is voluntary, any provider that chooses to offer PAS is required to adhere to uniform operating protocols, which establish five priority levels for NS/EP users. Those levels, with user examples, are:

1. Executive Leadership and Policy Makers
   - President of the United States
   - Secretary of Defense
   - Federal Senior Staff
   - State Governor, Lieutenant Governor, Cabinet-level for public safety and health
   - Mayors, County Commissioners, senior staff

2. Disaster Response/Military Command and Control
   - Federal emergency operations center coordinators
   - State emergency services directors, National Guard leadership
   - Federal, State, and local personnel with continuity of government responsibility
   - Incident Command Center Managers
   - Local emergency managers
   - Federal personnel with intelligence and diplomatic responsibilities

3. Public Health, Safety and Law Enforcement Command
   - Federal law enforcement command
   - State police leadership
   - Local fire and law enforcement command
   - Emergency medical service leaders
   - Search and rescue team leaders
   - Emergency communications coordinators

4. Public Services/Utilities and Public Welfare
   - Army Corps of Engineers leadership
   - Power, water and sewage, and telecommunications utilities
   - Transportation leadership

5. Disaster Recovery
   - Medical recovery operations leadership
   - Detailed damage assessment leadership
   - Disaster shelter coordination and management
   - Critical Disaster Field Office support personnel

The FCC Report and Order directs the use of authorizing agents, who will validate the user's request for PAS. The OMNCS will solicit participation of authorizing agents within the Federal departments and agencies and at the State and Territorial level for State and local NS/EP personnel. The OMNCS will issue the authorization code number and approve the appropriate priority level for each PAS request.

Because PAS is a voluntary offering, the OMNCS recommends that potential PAS users contact their present wireless service provider(s) and inquire whether the company will offer Priority Access Service. A demand from potential subscribers will encourage the providers to determine if there is sufficient user demand for PAS to justify offering this service.

If you have any questions related to the Priority Access Service, you can obtain a copy of the document at http://www.fcc.gov/Bureaus/Wireless/Orders/2000/fcc00242.doc. For information on PAS from the NCS, please contact:

David K. Scott
National Communications System, ATTN: N3
701 South Court House Road,
Arlington, VA 22204-2198
703-607-4993
scottd@ncs.gov
703-607-4998 (fax),

or

Maj. Jean Trakinat, (USAF)
National Communications System, ATTN: N2
701 South Court House Road
Arlington, VA 22204-2198
703-607-6113
trakinaj@ncs.gov
703-607-4830 (fax)❖

FCC Takes Steps to Implement the Wireless Communications and Public Safety Act of 1999

The Federal Communications Commission (FCC) has taken important steps to implement the Wireless Communications and Public Safety Act of 1999 (911 Act). In the adopted item, the FCC designates 911 as the universal emergency number and seeks comment on a limited number of related issues.

The FCC's actions seek to implement Congressional goals for an expanded, improved nationwide emergency communications system across the United States. Picking up the telephone is usually the first and most important thing to do when an emergency strikes. Making 911 the universal emergency number for both

wireline and wireless services and promoting the use of technologies that help emergency service providers locate wireless 911 callers will improve the nation's emergency 911 communications systems and save lives.

The 911 Act was enacted on October 26, 1999, to enhance public safety by encouraging and facilitating the prompt deployment of a nationwide, seamless communications infrastructure for emergency services that includes wireless communications.

To ensure a comprehensive approach to emergency service throughout the country, the 911 Act directs the FCC to make 911 the universal emergency number for wireline and wireless telephone service and to establish appropriate transition periods for areas in which 911 is not in use as an emergency telephone number on the date of enactment of the 911 Act. It further directs the FCC to encourage and support the States in developing comprehensive emergency communications throughout the United States so that all jurisdictions offer seamless networks for prompt emergency service.

The following are specifics of the FCC actions:

- Designate 911 as the universal emergency telephone number within the United States for reporting an emergency to appropriate authorities and requesting assistance, effective upon the release of the FCC's Order.
- Comments are sought on appropriate transition periods for areas in which 911 is not currently in use as an emergency number, including service area-specific circumstances and capabilities that the FCC should address before carriers can deploy 911 as the uniform emergency number.
- Comments are sought on how the FCC should facilitate States' efforts to deploy comprehensive emergency communications systems, such as through guidelines, meetings, or other information-sharing measures, in a manner that does not impose obligations or costs on any person.

The action became effective under the FCC's August 24, 2000, Fourth Report and Order, Third Notice of Proposed Rulemaking, and was led by Chairman William Kennard and Commissioners Susan Ness, Harold Furchtgott-Roth, Michael Powell and Gloria Tristani.❖

(Courtesy of the Federal Communications Commission)

Hogan, Miller to Serve on NCS Committee of Principals

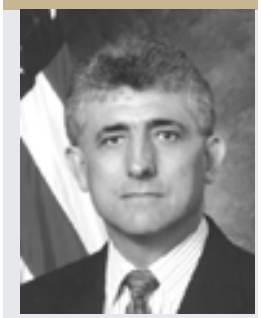
By Stephen Barrett, Customer Service Division, OMNCS

Karen F. Hogan, who leads the Chief Information Officer (CIO) Digital Department/Electronic Government initiative in the Department of Commerce, and Robert Miller, the Director of Telecommunications Services Staff at the Department of Justice, were recently named to represent their departments on the National Communications System's Committee of Principals (COP).

The COP is an interagency group, formed by Executive Order 12472, that provides advice and recommendations on national security and emergency preparedness (NS/EP) telecommunications to the Executive Office of the President. The COP is composed of high-level Government officials representing Federal organizations in the areas of operations, policy, regulatory issues and enforcement.

The NCS's diverse representation across 22 Federal departments and agencies embraces the full spectrum of Federal telecommunications assets and responsibilities. As an interagency group, it serves as a forum for members to review, evaluate, and present views and

Karen Hogan



Robert Miller

recommendations on current or prospective NCS programs to the Manager, the Executive Agent and the Executive Office of the President.

Mrs. Hogan was selected in June 1999 to lead the Digital Department initiative and continues to serve the Department of Commerce. She has also been recently named as the Acting Deputy Chief Information Officer. Her task is to ensure that the Department uses electronic means for conducting as much of its internal and external business as possible by 2003.

Prior to this assignment, Mrs. Hogan was the Associate Director for Information Technology and Chief Information Officer at the U.S. Census Bureau. There, she directed programs for automated data processing operations and telecommunications services and oversaw the total systems environment of the Census Bureau.

In 1995, Mrs. Hogan was appointed to the Senior Executive Service as the Administrator for Computer and Telecommunications Operations at the U.S. Patent and Trademark Office (USPTO), also a bureau of the Department of Commerce. In that position, she directed the network and data center operations of one of the largest data processing centers in the Federal Government.

Prior to joining the USPTO, Mrs. Hogan served 17 years in the Department of Defense. There, she gained experience in all areas of information technology, including strategic planning to support the business processes, aligning the technology plan and budget to agency priorities, standardization to improve support, and major system acquisitions and development.

Mrs. Hogan earned her bachelor's degree in Harrisonburg, Virginia, and master of science in Information Systems from the George Washington University in Washington, D.C. She has earned the Defense Meritorious Service Medal, the Joint Meritorious Unit Award, and the Special Act Award. While at the USPTO, she was a member of an acquisition team which received the Department of Commerce's Bronze Medal Award.

Mr. Miller has over 15 years of experience in managing the development, procurement, and delivery of information technology solutions. Before assuming the Telecommunications Services Director position, Mr. Miller served as Assistant Director, Network Services, on the Telecommunications Services Staff, and as Program Manager for the Justice Consolidated Network, leading the planning, design, and implementation of this critical department's Information Technology (IT) infrastructure project.

During his tenure at Justice, Mr. Miller has led many intradepartment and interagency initiatives such as the Federal-wide Drug Information System. His skills include IT investment planning, project management, systems development life cycle planning, and acquisition management.

He has successfully formed strategic partnerships with technical integrators and service providers, other Federal agencies, and the Justice Department's major law enforcement and litigating organizations to deliver critical IT systems.

Mr. Miller's background also includes experience in project management and systems development at the Department of Defense Computer Institute and the Navy Recruiting Command. He holds a degree in Information Systems Management from the University of Maryland in College Park, Maryland.❖

OMNCS Network Design and Analysis Capability

By Greg Parma, Technology and Programs Division, OMNCS

The National Communications System (NCS), as directed by Executive Order 12472, conducts technical studies and analyses on the commercial carrier telecommunications switching infrastructure and the public network (PN). These NCS studies determine the impact of natural and man-made disruptions to the PN and identify improved approaches and network optimizations which may assist Federal entities in fulfilling national security/emergency preparedness (NS/EP) telecommunications objectives.

In support of this mission, the Office of the Manager, NCS

(OMNCS), developed a robust computer modeling and analysis capability. Working with different network databases, studies are customized using various network design and analysis software tools (Figure 1).

These databases contain the location and description of Internet and telecommunications assets, network topologies, long-distance trunk transmission and switched services paths. The data is obtained, directly or indirectly, from the commercial carriers and public databases.

The network design and analysis capabilities can help assess and provide timely reporting on national telecommunications capabilities during national disaster response and recovery activities. Past studies include modeling and network performance predictions for threats such as natural and technological hazards, terrorist attacks, electronic intrusion incidents and nuclear and chemical attack scenarios. In addition, the OMNCS used these modeling and analysis tools to prepare for Y2K.

Based on study results, analysts can pinpoint PN vulnerabilities, including single points of failure, and model network performance degradation over time brought on by wireline and cellular connectivity congestion and reduced network resources. Other modeling and analysis tools help to examine the NS/EP impacts on the PN brought on by emerging technologies. Additionally, a baseline normal operating PN can be compared against stressed conditions with programmed reliability/

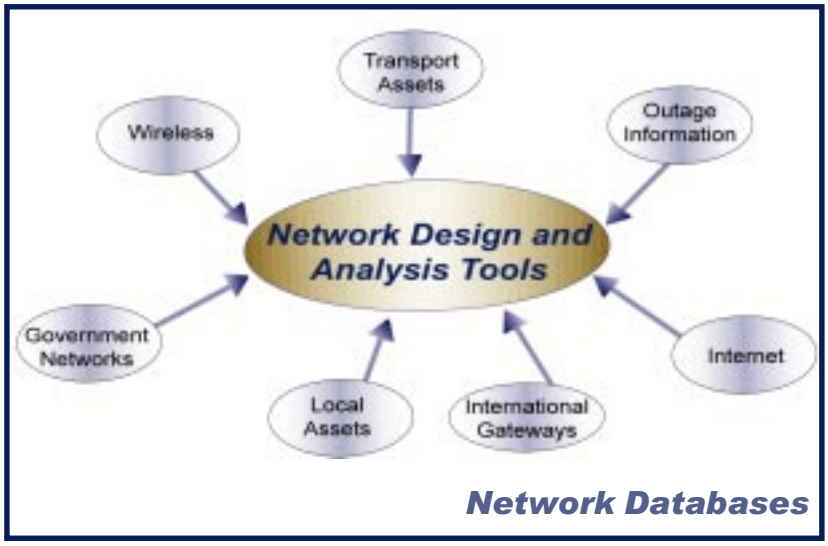


Figure 1 Tools and Databases

interoperability/survivability characteristics. For example, a comparison of priority call treatment can help predict the Government Emergency Telecommunications Service (GETS) increased call completion probability and establish end-to-end user connectivity benefits provided to NS/EP users.

To provide accurate analyses, the OMNCS is making continual efforts to acquire updated information from the service providers in order to provide a valid representation of commercial carrier facilities. Revisions of model structures and assumptions are necessary to accurately account for changes being made to the telecommunications networks.

Past developments include models for Synchronous Optical Network Transmission and Asynchronous Transfer Mode, which allow new services provided by some commercial carriers to be modeled. Future enhancements include models for cellular networks that are integrated into the existing models, as well as models that provide more accurate representations of new routing techniques at the local exchange and inter-exchange carrier levels. Also, tools are being enhanced to provide better visualization capabilities.

The functional architecture (Figure 2) supports application-level requirements and provides a seamless interface into the OMNCS telecommunications resource. Interactive access via a user-friendly Web page hierarchy assists in navigating and retrieving existing information from the different databases.

Microsoft® Internet Information Server™ (IIS) (Version 3.0) software supports authentication, logging, profiling, file transfer, and access control requirements. It responds to service requests from browsers on its network via hypertext transfer protocol. The Web server then invokes ColdFusion® 4.0 to dynamically generate a Web page or retrieve a static hypertext markup language (HTML) file from the server's file system. The page is then forwarded to the

requesting browser.

ColdFusion® (Version 4.0) (Allaire™ Corporation) generates dynamic Web pages as the primary software component supporting the requirement for ad-hoc querying. Translating between HTML and Cold Fusion Markup Language (CFML), Cold Fusion® performs well in database manipulation providing flexibility with seamless integration between the Microsoft® IIS™ Web server and Oracle® database server.

LECMap is a stand-alone application that can produce a database of local exchange carrier (LEC) network topology data. By invoking MapXtreme™, network topologies can be generated from data retrieved from the OMNCS Telecommunications Resource and visually mapped by graphical region, by carrier, or by telephone exchanges.

MapXtreme™ (MapInfo Corporation) software supports the LECMap application by geographically mapping network topology data. Interaction between its two major modules, HAHTsite™ and MapX™ can be used to produce interactive LEC network maps.

HAHTsite™, as a fully integrated development system for building Internet and intranet Web applications, processes common gateway interface (CGI) scripts issued by the Microsoft® IIS™ and sends instructions to MapX™. MapX™ generates maps and returns the mapping information to HAHTsite™, which generates readable HTML code for the browser.

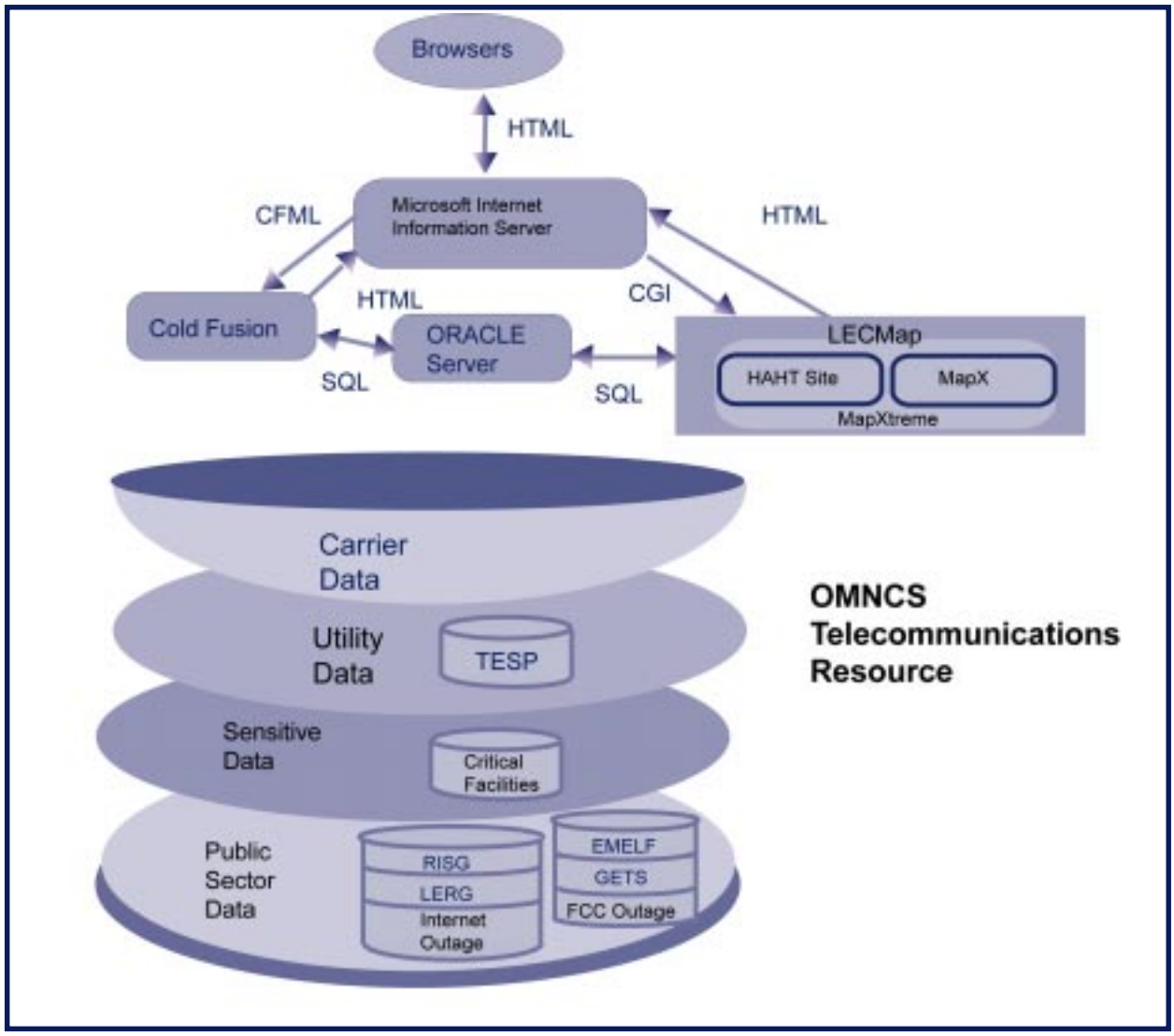


Figure 2 Functional Architecture

Oracle® Server (Version 8.0) contains the relational database management system that manages the outward flow of the proprietary and non-proprietary information stored on the database server. The Oracle® Server interacts with the Microsoft® IIS™ through translation files created through Cold Fusion® 4.0 via outside database connectivity and Oracle® Net8 communication utilities. The Oracle® Server interfaces with the LECMap application in a similar fashion.

The OMNCS Telecommunications Resource, serving as a core resource, draws information from a collection of proprietary and public sector databases in producing custom network studies. A study baseline and related impact or a vulnerability scenario is engineered by integrating different proprietary and public sector data sources through tailored programming queries.

The Carrier Data is available under special acquisition provisioning. Commercial carriers provide network switch type and location data used in building network topologies. Since this information along with critical facility locations is sensitive, access is strictly limited to designated personnel.

The Critical Facilities Database is a compilation of critical government facilities location data including address, and telephone numbers as listed in the 1999 Caroll's Federal Directory. Through cross-reference, this information can identify what PN assets support a particular location.

The Telecommunications Electric Service Priority (TESP) provides a cross-reference database that maps identified PN critical assets with the supporting electric utility provider. Queries produce point of contact names, addresses, and phone numbers for both the telecommunications carrier and the corresponding electric utility. Access to these proprietary files is limited to authorized personnel.

The Roaming Implementation Service Guide (RISG) database is a monthly publication which is maintained by the Cellular Telecommunications Industry Association. The RISG contains a listing of all cellular mobile switching centers and cellular numbering plan area-central office code assignments (NPA-COCs). Similar to the Local Exchange Routing Guide (LERG), the NPA-COCs can provide the homing information for every cellular phone account.

The LERG is a monthly publication provided by Bellcore. Primarily useful in identifying the interconnection points between LECs and Interexchange carriers, the LERG describes every switching entity with respect to the following:

- Functionality and services provided
- Geographical location
- Operating company
- Logical connectivity
- NPA-COC assignments.

With the NPA-COCs information, every wireline phone number can be logically homed to a switching entity.

The Enhanced Microwave Environmental Link File (EMELF) database indicates the locations of nonfederal Government radio antennas. Maintained by the FCC, more than 500,000 wireless links exist in the database.

The Government Emergency Telecommunications Service database identifies the switching facilities which are equipped to handle the GETS service.

The Federal Communications Commission (FCC) Outage database contains records on telecommunications outages as reported by common carriers. This non-proprietary data source includes dates, carriers, duration, and explanation for the outage.

The Internet Outage Database contains records of reported outages in the Internet Service Provider networks. This information comes from non-proprietary sources provided over the public Internet.

Clearly, the OMNCS network design and analysis capability provides a powerful resource that addresses member agency modeling and simulation requirements, helps in Telecommunications Service Priority planning and supports the National Coordinating Center for Telecommunications operations. Additionally it offers a flexible means to evaluate possible NS/EP impacts resulting from emerging technologies. To continue as a valuable and unique NCS asset, this capability will be uniformly enhanced to match the increasing challenge of modeling a more robust, complex PN.❖

DBS Could Provide Nationwide Coverage for NS/EP Issues

By Robert Fenichel, Technology and Programs Division, OMNCS

Radio broadcasting has entered a new era. Only 2 decades after Direct Broadcast Satellite (DBS) television home dish antennas first appeared on the market, one company has started broadcasting DBS radio to listeners in Africa and the Middle East. Within the next few years, two other companies plan to begin broadcasting to listeners in the United States.

To the average user, these systems will look very similar to conventional AM/FM radio systems, whether they are used in the home, office, or on the road. However, the real difference is in what the listener won't see. Rather than receiving a signal from a tower antenna of a local radio station, these new radios will receive signals from a set of satellites in geosynchronous orbit. Programming will be uplinked from ground stations to the satellites and then broadcast back to large geographic areas, such as the contiguous United States.

Direct broadcast satellite (DBS) radio stations would use a ground station to upload programming to orbiting satellites. With the proper receiver (and a paid subscription), customers could listen to up to 100 radio stations from any point in the Nation.

NS/EP Applications

The utility of DBS radio as a national security and emergency preparedness resource depends on the degree of market penetration. The cost of DBS radios will probably be $100 to $200 more than existing AM/FM radios, and subscriptions to largely commercial-free services are expected to be $9.95 per month.

The two companies planning U.S. DBS radio over the next 2 years—XM Satellite Radio and Sirius Satellite Radio—view the 110 million automobile commuters in the U.S. as a primary market. That large a number of automobile radios could provide an effective capability for national emergency audio broadcasting.

Broadcasting Overseas

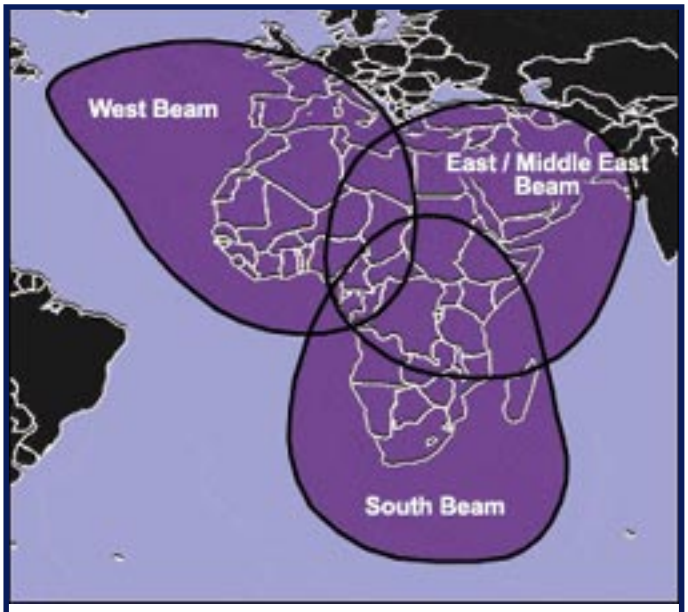
DBS radio is already fielded in Africa and the Middle East. WorldSpace Corporation, headquartered in Washington, is broadcasting DBS radio programs to listeners in Africa and the Middle East using their AfriStar satellite. AfriStar has three spot beams covering the areas of Southern Africa, Western Africa (including

Spain, France, and Italy), and the Middle East and Northeastern Africa (including Turkey), respectively. Each spot beam can cover approximately 14 million square kilometers (5 million square miles).

Unlike other planned U.S. services, WorldSpace charges no monthly subscription fee and revenue is generated by advertisements on the audio channels.

AfriStar is positioned in a 21 degrees East geosynchronous orbit and is controlled by the WorldSpace Operations Center located in Washington. The prime contractor for the satellite is Alcatel Space Industries, and Matra Marconi Space built the EuroStar 2000+ satellite bus. The uplink frequencies are 7.025–7.075 GHz, and the downlink frequencies are 1.452–1.492 GHz.

Each AfriStar downlink spot beam has capacity for 96 16 kbit/s mono-AM-quality signals that can be combined for fewer channels of higher audio quality. The downlink signals in each spot beam are combined into two Time Division Multiple Access (TDMA) carriers. Uplink signals can be accepted as TDMA signals from control stations or, individually, as Frequency Division Multiple Access (FDMA) signals from originating program locations.



AfriStar, a Direct Broadcast Satellite (DBS), has three spot beams covering Southern Africa, Western Africa (including Spain, France, and Italy), and the Middle East and Northeastern Africa (including Turkey), respectively. Each spot beam can cover approximately 14 million square kilometers (5 million square miles).

WorldSpace also launched AsiaStar in March 2000, a DBS radio satellite that currently covers Asia (105 degree East orbit). In late 2000, WorldSpace plans to launch AmeriStar (95 degrees West orbit) to cover Latin America.

XM Satellite Radio and Sirius Satellite Radio

In the United States, XM Satellite Radio and Sirius Satellite Radio plan to offer Satellite Digital Radio Service (SDARS). In October 1997, the Federal Communications Commission (FCC) granted SDARS licenses for U.S. DBS radio systems to both firms.

Within the next few years, these companies plan to launch systems similar to the WorldSpace systems, with up to 100 audio channels. They expect to charge a $9.95 monthly subscription fee for largely commercial-free programming.

Last February, the two companies announced plans to develop a unified standard so that a common radio can receive both XM and Sirius programming. However, prior to this announcement, each company had already started independent product development. It remains to be seen if the two companies will start service with separate, incompatible receivers or delay introduction of their products until a standard U.S. DBS radio receiver has been developed.

A major thrust of both companies' business plans is to develop alliances with the major automobile manufacturers to build DBS-capable radios in new automobiles. XM Satellite Radio has an agreement in place with General Motors (GM), and Sirius Satellite Radio has agreements in place with Ford and Daimler-Chrysler. Both companies also have agreements in place with major radio manufacturers.

One of XM's slogans is "first there was AM, then FM, and soon XM Satellite Radio" (to be known as AM/FM/XM radio). Subject to a possible delay due to the redesign

to meet a common U.S. standard, automobile manufacturers are planning to introduce DBS radios as an option in automobiles in 2001.

To support these services, XM Satellite Radio plans to launch two HS702 15 kW geostationary satellites built by Hughes Space and Communications which will contain Alcatel Space Industries' payloads. Launch services will be provided by Sea Launch, which is 40 percent owned by Boeing. Sea Launch uses Russian and Ukrainian rocket stages launched from a floating platform that is sailed from Long Beach, CA, to the equator for each launch.

XM plans to position the two satellites at 85 degrees West and 115 degrees West, and the downlink will be in the 2.33–2.34 GHz frequency range. A spare satellite will be kept on the ground for emergencies.

Examples of automobile and portable radios with Direct Broadcast Satellite (DBS) receivers.

Sirius Satellite Radio has similar plans, except it plans to launch three satellites to achieve U.S. coverage.

Both companies plan to employ terrestrial repeaters in major cities where buildings would block satellite reception.❖

Digital Subscriber Line Technology

By Ray Young

Digital subscriber line (DSL) is one of several access methods competing to bring broadband connectivity to the small office/home office (SOHO) market. As demand for access to the Internet soars, demand for faster access has also increased.

Today, the typical SOHO user reaches the Internet via a dial-up analog modem with a maximum access speed of 56 kilobits per second (kbps). DSL, on the other hand, promises connection speeds up to 100 times faster by using a digital modem (or splitter) instead of an analog modem.

How Does DSL Work?

DSL travels over the twisted-pair copper telephone lines that already link the public switched network (PSN) central office (CO) and the SOHO premises. It works by exploiting unused bandwidth in these copper wires. Voice traffic over copper uses only the lower end of the wire's frequency range (300 Hertz [Hz] to 3.4 kilohertz [kHz]).

DSL takes advantage of the fact that copper telephone lines can carry broadband signals at a much higher frequency (between 5 kHz and 1.4 megahertz [MHz]). However, the distance that DSL can travel over copper wires is limited to 18,000 feet from a central office.

Although the DSL distribution path subsists in existing twisted pair copper, DSL does require the addition of new equipment at the central office and the SOHO premises. Like the analog solution, DSL requires modems at the SOHO.

At the central office, DSL access multiplexers (DSLAM) are the key pieces of equipment for providing DSL service to multiple users. In the near future, DSLAMs will provide not only DSL service, but also "edge" services and management controls to Internet service providers (ISP) and their customers.

The modem and the DSLAM split the voice and data signals using frequency division multiplexing. Because voice and data are transmitted over different

frequency ranges, DSL can operate independently of voice services. If the DSL modem or the DSLAM fail, voice services should remain unaffected.

DSL allows data traffic to completely bypass the CO switch. Once data signals have been separated from voice signals, voice calls can be carried over the circuit-switched PSN, and data traffic can be aggregated with other incoming data traffic to be routed to the Internet.

xDSL

Many companies are developing alternative "flavors" of DSL, known collectively as xDSL. These xDSL types include asymmetric DSL (ADSL), rate adaptive DSL (RADSL), and symmetric DSL (SDSL).

ADSL is by far the most common version of DSL and is perhaps the simplest and least expensive way to provide DSL to the end user. "Asymmetric" refers to the asymmetric rates for upstream (SOHO to central office) and downstream (central office to SOHO) data. ADSL takes advantage of the fact that most customers receive more data (Web pages, graphics, e-mail attachments) than they send; therefore, it is much cheaper and easier to push data downstream to the customer than it is for the data to be sent upstream from the customer.

Upstream rates for ADSL tend to peak at around 128 kbps, whereas downstream rates can reach as high as 6 megabits per second (Mbps), or roughly 100 times faster than a typical download using an analog modem.

Competing Technologies

Broadband access for the SOHO market is not restricted to telephone access. DSL is only one choice among many for providing broadband data access. Other competing technologies include cable modems and wireless broadband.

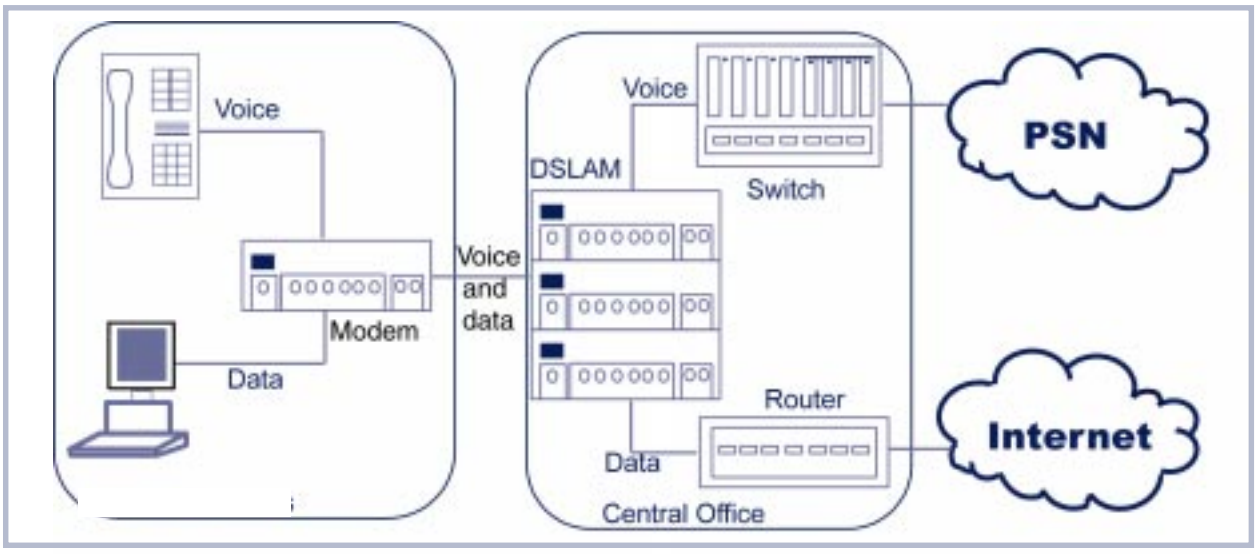
Broadband access via cable television wiring, commonly known as cable modem service, is a nearly direct competitor to DSL. Cable service providers are pursuing the same SOHO market as DSL, but with two notable differences.

First, cable has not traditionally been installed in office buildings, therefore limiting its use for business. Second, unlike DSL, cable signals do not dissipate over distances; therefore, theoretically, anyone with cable TV could purchase cable modem service if his or her cable company offers the service.

How Do Cable Modems Work?

Cable modem service provides bi-directional Internet access via asymmetric cable modems and cable coaxial wires. Previously, first-generation cable modem service required the use of a telephone line for the upstream data connection. However, today's cable modem services use cable coaxial wires to carry data downstream and upstream.

Broadband access speeds can reach up to 3 Mbps



Typical example of a Digital Subscriber Line (DSL) Configuration.

upstream and 2.5 Mbps downstream. Like DSL, cable modem service uses a combination of existing wiring and new equipment. Downstream data is modulated and sent via a 6-MHz-wide television channel, in the frequency range from 50 MHz to 750 MHz.

Theoretically, this will allow for a downstream speed of 27 Mbps. However, because most computers are incapable of connecting at this speed, most service providers will limit downstream data rates to 1 to 3 Mbps. Upstream data is transmitted in the range of 5 to 42 MHz, with data rates as high as 10 Mbps. However, because most users do not require access at this high rate, most cable modems are manufactured to provide service at 0.5 to 2.5 Mbps.

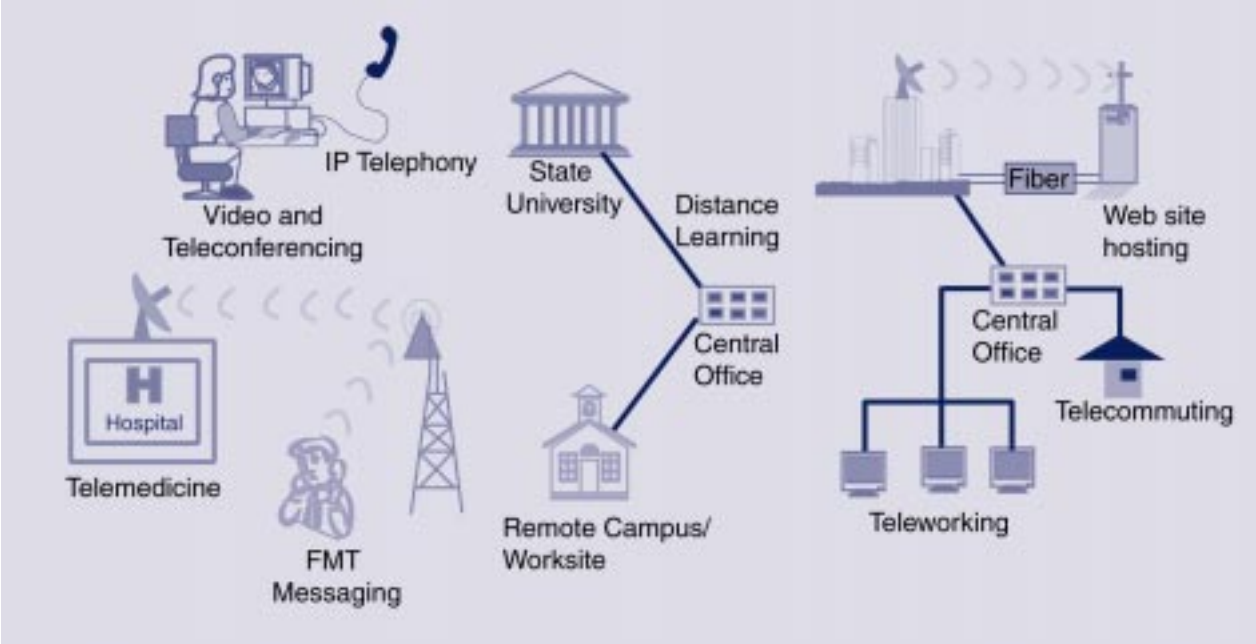
Like DSL, cable modem service requires investment in new equipment. At the SOHO premises, a cable modem is required, which is typically leased from the service provider. At the cable plant, the service provider must install a cable modem termination system (CMTS). The CMTS is the key hardware for connecting the cable TV network to the Internet or other data networks.

Wireless Broadband

Many wireless equipment vendors and service providers are moving aggressively to offer wireless broadband to the SOHO market. Like wired broadband, wireless broadband (also known as fixed wireless, broadband wireless local loop, and wireless digital subscriber) is a network access alternative for the delivery of data, Internet, voice, video, and multimedia applications. Broadband wireless access uses licensed spectrum to transmit signals within cells that are several kilometers wide. It is a short-haul, line-of-sight (LOS) technology.

Among the technologies being developed for this market are local multipoint distribution service (LMDS) and multichannel multipoint distribution service (MMDS). LMDS operates in the 28 gigahertz (GHz) and 31 GHz bands. MMDS operates in the 2.5 GHz band. Other frequencies also in use are the 24 GHz, 26 GHz, 38 GHz, and 39 GHz bands. Generally speaking, frequencies above 10 GHz are known as LMDS. Unlicensed spectrum also exists in the 2.4 GHz and 5.8 GHz bands.

The wireless broadband technology uses fixed wireless antennas that are highly directional and bolted to rooftops. These antennas possess large data capacities and do not support roaming. The narrowband antennas do not use satellites. To deliver



There are numerous ways that wireless broadband can assist users ranging from video conferencing and distance learning to providing communications in a national security and emergency preparedness (NS/EP) environment.

wireless broadband Internet, a combination of technology platforms are used, from fixed wireless for the first mile connection to fiber rings that connect hub site buildings, to long-haul fiber that connects cities.

Wireless broadband connections and other fixed-wireless connections deliver data rates from T1 to 155 Mbps. These wireless connections serve the same function as a wireline, interconnecting private networks, bypassing a local exchange carrier, or connecting to the Internet.

ADVANTAGES	DISADVANTAGES
- High bandwidth service - Low cost for medium number of users - Voice, data and video support - An "always on" service	- Not ubiquitous - Expensive for small number of users - Sometimes difficult to install - Not portable - Security issues

Advantages and disadvantages of broadband access

How Does Wireless Broadband Work?

When a user sends data, data packets stream to an antenna. The antenna then uses the spectrum to transmit the packets in a tight beam aimed at another antenna within LOS. This second antenna is co-located with a hub that receives transmissions—such as voice, video, and data—simultaneously from many customers, aggregates the transmissions, and pushes them out onto a backbone for network distribution.

Data going from the backbone to the customer is received at the hub. The hub sorts the packets and distributes them as transmissions aimed at the rooftop antennas on surrounding buildings. A combination of point-to-point and point-to-multipoint radios (or transceivers) carry the signals, but only if the service supports point-to-multipoint (most do not at this time). Audio signals can be digitized and sent as data packets; therefore, industry hopes to combine data and voice communications within a single transmission within this decade.

Applications, Advantages, and Disadvantages

The “always on” nature of DSL and its high bandwidth capabilities make it a good candidate for several applications. From support of a SOHO to advanced video teleconferencing, there are many potential uses for DSL and other broadband applications.

Although DSL and other broadband technologies offer greater data access rates at a relatively low cost per user, drawbacks to broadband access also exist. The system is not portable and is difficult to install. Broadband is not ubiquitous and may be expensive for small numbers of users.

Security

One selling point of broadband is that a connection always exists on the Internet. Continuous access eliminates the downtime associated with dialing in via an analog modem. However, the convenience of a continuous connection does not come without a price. Unfortunately, that price is a lack of security.

Continuous connections make computers vulnerable to hackers and snoopers. For the typical analog modem-to-ISP connection, the ISP will assign a dynamic Internet Protocol (IP) address at random with each new Internet session. However, because broadband connections are continuous, they tend to use static IP addressing. Static IP addressing makes it easier for hackers and snoopers to target and track an individual’s personal computer (PC).

Cable modems have another vulnerability. Using a cable modem is analogous to using a local area network, in which many users share common cabling. This means that “neighbors” who are using the same cable modem networks theoretically can intercept data packets sent between the end user and the ISP.

Several steps can be taken to address these security concerns. A good place to start is with the ISP. End users should ask their ISP if any security systems are currently in place to detect or prevent hackers and snoopers—dynamic IP addresses, protective software to encrypt data, or a firewall.

If the ISP does not provide dynamic IP addressing, the best protection is to disconnect the computer from the Internet when it is not in use. This can be accomplished either by disconnecting the cable or telephone line or by turning off the system. In addition, if the ISP

does not provide encryption, a firewall, and antihacking software, the end user can purchase these for self-installation.❖

(Ray Young, formerly with the OMNCS Technology and Programs Division, now works with the National Security Agency at Fort George G. Meade, MD.)

Commerce Department Announces Winner of Global Information Security Competition

By Philip Bulman, National Institute of Standards and Technology (NIST)

A worldwide competition to develop a new encryption technique that can be used to protect computerized information ended today when Secretary of Commerce Norman Y. Mineta announced the Nation's proposed new Advanced Encryption Standard (AES).

Mineta named the Rijndael (pronounced Rhine-doll) data encryption formula as the winner of a 3-year competition involving some of the world's leading cryptographers.

"Once final, this standard will serve as a critical computer security tool supporting the rapid growth of electronic commerce," Mineta said. "This is a very significant step toward creating a more secure digital economy. It will allow e-commerce and e-Government to flourish safely, creating new opportunities for all Americans," he said.

Computer scientists at the National Institute of Standards and Technology (NIST), an agency of the Commerce Department's Technology Administration, organized the international competition in a drive to develop a strong information encryption formula to protect sensitive information in Federal computer systems. Many businesses are expected to use the AES as well.

The proposed selection of Rijndael as the AES will be formally announced in the Federal Register in several months, and NIST then will receive public comments on the draft Federal Information Processing Standard for 90 days.

Researchers from 12 different countries worked on developing advanced encoding methods during the global competition. NIST invited the worldwide cryptographic community to "attack" the encryption formulas in an effort to break the codes.

After narrowing the field down from 15 formulas to five, NIST invited cryptographers to intensify their attacks on the finalists. The agency and the world cryptographic community also evaluated the encoding formulas for factors such as security, speed and versatility.

The Rijndael developers are Belgian cryptographers Joan Daemen (pronounced Yo'-ahn Dah'-mun) of Proton World International and Vincent Rijmen (pronounced Rye'-mun) of Katholieke Universiteit Leuven. Both are highly regarded experts within the international cryptographic community. NIST organized and managed the competition with considerable private-sector cooperation.

NIST requested proposals for the AES on September 12, 1997. Each of the candidate algorithms was required to support key sizes of 128, 192 and 256 bits. NIST evaluated the candidate algorithms and received invaluable assistance from cryptographers at computer security companies and universities around the world.

Good security was the primary quality required of the winning formula, but factors such as speed and versatility across a variety of computer platforms also were considered.

NIST and leading cryptographers from around the world found that all five finalist algorithms had a very high degree of security. Rijndael was selected because it had the best combination of security, performance, efficiency, implementability and flexibility.

The AES competition was organized by computer scientists in NIST's Information Technology Laboratory. A lengthy technical analysis of the AES candidates is being posted on NIST's Web site at www.nist.gov/aes.

After the public comment period, NIST will revise the proposed standard—if appropriate—and submit it to the Secretary of Commerce for adoption as an official Federal standard. This process is expected to be complete by the spring of 2001.❖

(Story courtesy of NIST)