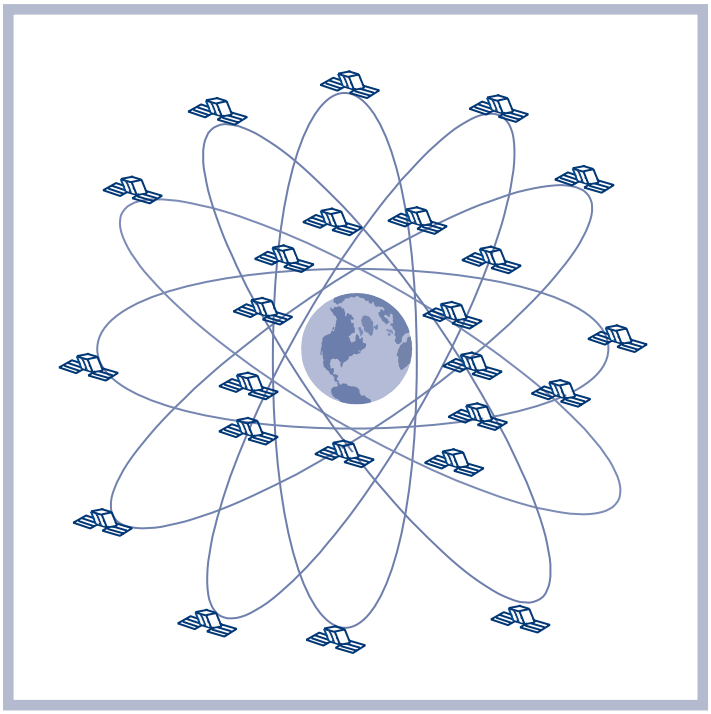
National Security and Emergency Preparedness
Telecom News
1999, Issue 2
Published by the Office of the Manager, National Communications System, for the national security and emergency preparedness (NS/EP) community

NS/EP Implications of GPS Timing

By LeeAnne Brutt
Technology and Programs Division, OMNCS



The Global Positioning System (GPS) is a satellite-based positioning and navigation system that is funded and operated by the U.S. Department of Defense. Although originally developed for use by the U.S. military, GPS now supports thousands of civilian users worldwide and is employed in a wide range of applications.

Overview of GPS

GPS provides two levels of operation: standard positioning service (SPS) and precise positioning service (PPS). SPS is available to all users—free of charge—on a continuous, worldwide basis. It is able to provide a predictable 95 percent positioning and time transfer accuracy, which translates to approximately 100 meters in the horizontal direction, 156 meters vertically, and timing to within 340 nanoseconds.

PPS maintains an even greater level of accuracy, with a predictable horizontal accuracy to within 22 meters, 27.7 meters in the vertical direction, and timing to within 100 nanoseconds. However, this higher level of service is secured through encryption and is only available for use by U.S. military and other approved users.

GPS is composed of a space segment, a control segment, and a user segment. The space segment consists of a constellation of 24 satellites along with several spares. Each satellite orbits the Earth once every 12 hours on one of six orbital planes. The GPS constellation is positioned such that at any given time, 5 to 8 satellites are visible from any point on Earth.

The control segment is a system of monitor stations, ground antennas, and a master control station. The monitor

See GPS Timing, page 11

TABLE OF CONTENTS

NS/EP Telecom News is published quarterly under the auspices of Ms. Diane Fountaine, 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

Basic Internet Structures Expected to be Y2K Ready

The overall structure of the Internet is expected to make a successful transition to the Year 2000.

However, John A. Koskinen, Chair of the President's Council on Year 2000 Conversion, said a large number of participants in the Internet community make it impossible to rule out the existence of date change problems.

Koskinen made those remarks at a recent press conference where he joined Internet community representatives who participated in a Council-sponsored July 30 roundtable meeting on the Year 2000 (Y2K) readiness of the Internet.

"The good news is that the basic foundation of the Internet is expected to be ready for the Year 2000," said Koskinen. "Overall, the Internet is a very redundant system that should continue to function even if there are Y2K problems. But the vast number of networks and companies involved in providing services to users makes it impossible to guarantee that someone, somewhere won't experience temporary problems in using the Internet that are caused by the date change."

The Internet roundtable meeting brought together roughly 100 organizations and individuals representing small and large Internet Service Providers (ISPs), equipment vendors, root nameserver and domain registries, exchange points, network time servers, industry associations, and government agencies. The purpose of the meeting was to assess the Y2K readiness of the Internet and to help members of the Internet community better coordinate efforts to maintain Internet performance and reliability during the Year 2000 transition.

Roundtable participants discussed Y2K challenges for core Internet services, such as root nameservers, exchange points, backbone providers, and ISPs and explored how to provide consumers with more information on service provider Y2K readiness. ISPs were encouraged to post information about their Y2K efforts on their Web pages and on www.nety2k.org.

As a follow-up to the roundtable meeting, Internet.com is adding to its ISP list a field for listing those ISPs that have posted Y2K readiness statements. Key discussion points from the roundtable were released recently.

"Individuals and businesses across the country depend upon the Internet for information and commerce," said Koskinen. "In addition to checking to see whether your own PC is Y2K compliant, it makes good sense to determine the Y2K readiness of your personal ISP."

The President's Council on Year 2000 Conversion, established on February 4, 1998, by Executive Order 13073, is responsible for coordinating the Federal Government's efforts to address the Year 2000 problem. The Council's more than 30 member agencies are working to promote action on the problem and to offer support to public and private sector

organizations within their policy areas. More information on the Council is available on the Internet at www.y2k.gov.

For consumer information on the Year 2000 problem, call the Council's free information line at 1-888-USA-4Y2K.

(Courtesy of the President's Council on Y2K Conversion.)❖

John A. Koskinen, Chair of the President's Council on Y2K Conversion, said the overall structure of the Internet is expected to make a successful transition to the Year 2000. (Photo by Robert Flores, Defense Information Systems Agency.)

Intelligence on the Edge

By Gabor Luka
Technology and Programs Division, OMNCS

Rapid advances in microelectronics and wireless technologies are sparking a consumer love affair with portable electronic devices. At the same time, mass acceptance of the Internet as an important productivity tool makes connectivity to networked information sources indispensable.

These market forces are migrating access to network "intelligence" nearer to the edge of public and private networks, and further away from traditional Public Network (PN) switches. Intelligence means software and hardware that allows us to define our service parameters and modify our user profiles individually.

Examples of intelligent communication tools include increasingly commonplace items such as Personal Digital Assistants (PDAs) and digital wireless phones, as well as more futuristic-sounding items like "smart" cards and intelligent appliances. Each of these devices uses embedded computer chips to support one or more applications. These tools may simplify everyday tasks, facilitate added network and information security, and play a key role in how users interact with the network. The network of the future is evolving to include a variety of intelligent devices for the end user.

A strong argument can be made that smart card—or chip card—technology has great potential to change the way we live and work. A smart card is a plastic card that has an embedded microprocessor and a memory chip, or only a memory chip, with non-programmable logic. Microprocessor cards add, delete, and otherwise manipulate information on the card, while memory-chip cards such as prepaid phone cards only undertake predefined operations.

See Intelligence on the Edge, page 4

Intelligence on the Edge, cont'd from page 3

Smart cards, unlike magnetic stripe cards, carry all necessary functions and information on the card; they do not require access to remote databases at the time of the transaction. Smart cards might function as credit or debit cards, electronic wallets, calling cards, insurance and medical history cards, driver's licenses, local transit cards, and loyalty cards which validate user transactions and privileges. The same card could improve security by storing passwords.

In addition, smart cards may plug into wireless phones to provide Subscriber Identification Module (SIM) card functions, or plug into TV set-top boxes to secure satellite or cable transmissions. Efforts are even underway to enable more powerful devices which could integrate World Wide Web based capabilities like Sun Microsystems' Java technology.

Smart cards can include a standard set of Application Programming Interfaces (APIs) that allow Java applets to run directly on the card. The most recent version of this technology, Java Card API 2.1, includes support for secure inter-applet communication.

An impediment to adoption of smart card technology is lack of interoperability. Smart cards are worthless if card readers cannot interface with them. Standards groups and forums have sprung up to address these interoperability issues and promote smart card technology.

Another significant technology with implications for everyday tasks is the PDA, which is essentially a handheld computer. These handsets evolved from simple electronic address books to multipurpose devices that include an interface to synchronize information with personal computers (PCs).

Another significant technology with implications for everyday tasks is the PDA, which is essentially a handheld computer.

Interfaces to these terminals now include e-mail via modem and even wireless messaging using Short Message Services (SMS). Innovation continues on ways to facilitate communication between these palmtop computers, the user's PC, and the Internet. As this technology matures users will be able to execute functions to control and manipulate data on the network.

PDAs have made a quick and strong entry in the market place, unlike smart card or chip card technology. User penetration has been extremely successful due to their compact size, wide range of functionality, and great flexibility. Common applications such as personal organizers, wireless communication, and Web surfing are available. Uses include keeping track of appointments and meetings, or staying in touch with the office via e-mail or fax.

Three categories have been defined for this technology: 1) pocket-sized personal computers; 2) Wireless Intelligent Terminals (WITs); and 3) wireless software applications. Pocket-sized personal computers are portable devices that contain built-in applications such as a calendar, address book, calculator, and "To Do List" which conveniently fits into the user's pocket. The PDA is often linked to a PC that synchronizes the applications between the PDA and the PC.

Some pocket-sized personal computers such as Casio's CASSIOPEIA and the 3Com Palm Pilot have similar features except they use Microsoft's Windows CE operating system, which provides compatibility with a Windows-based desktop computer. This allows the use of reduced versions of Microsoft applications such as MS Word and MS Excel. In addition, MS Windows CE-capable equipment has e-mail and Web browser capabilities along with the ability to send and receive information when

used with one-way or two-way pagers.

WITs are more geared towards accessing online services via the Web and communication of voice and data. They are very similar to cellular phones and are used as a wireless communication device for voice, as well as a medium for transferring data, communicating faxes, PCs, pagers, and sending/receiving e-mail.

For example, Motorola's Envoy Wireless Communicator can interface with the Internet in one of two ways. It can use a built-in two-way wireless packet data modem or it can connect to a telephone line with its built-in data and fax modem.

The Envoy Wireless Communicator uses two wireless communication services—AT&T PersonaLink Services and Radio Mail. The AT&T PersonaLink service provides packet data service and an electronic mailbox over wireless. This service is currently being implemented nationwide and includes “full end-to-end encryption.” The Radio Mail service will allow communication with other electronic mail users via the Internet and commercial mail systems.

The Envoy Wireless Communicator also has built-in software that allows it to communicate with online services such as America Online (AOL) and Official Airline Guides.

AT&T PocketNet provides a similar capability which adds a menu-based keypad interface with a graphical screen capability. The main feature is an ability to download Web pages in a condensed format. By using High Definition Mark-up Language (HDML), Web page information can be received without significant transmission delay to the handset. To accomplish this, each Web page transmits only a subset of the original content, consisting of the pages' value-added content. Graphic and multimedia content is removed resulting in quicker transmission of text only data.

The Envoy Wireless Communicator can interface with the Internet in one of two ways.

Information resources currently available in HDML are weather reports for some major sites, stock quotes, sports scores, and United States white pages phone directory with an auto-dialer. Corporate price lists, workgroup calendars, and warehouse inventory are other future possibilities for information resources.

Cellular Digital Packet Data (CDPD) network is the technology enabler for these wireless instruments, which allows voice and data traffic to coexist. Wireless software applications provide services that use the Internet via wireless or wireline PN devices. The goal of wireless software applications is to make the connection between the Internet and wireless telephony seamless and transparent to the user.

One example of a family of wireless software applications by Telcordia Technologies—formerly known as Bellcore—is called AirBoss. It provides wireless access to the World Wide Web, speech recognition, wireless and wireline integrated messaging, and wireless access to corporate information databases.

Smart Messaging developed by Nokia is another example of wireless applications. Smart Messaging is similar to AirBoss in that it provides access to the Internet but from any wireless phone. Smart Messaging uses Tagged Text Markup Language (TTML) technology to optimize the narrow bandwidth between the server and

See Intelligence on the Edge, page 6

Intelligence on the Edge, cont'd from page 5

the phone. This process removes logos and graphics from Web pages.

The next generation wireless phone is known as the smart phone. New intelligent features allow subscribers to access custom online information services, many Internet-based services, and corporate databases. The industry is developing wireless networking protocols such as the Wireless Application Protocol (WAP) and Wireless Markup Language (WML) that will allow sharing of data and applications across platforms and geographic boundaries.

Smart appliances are now a reality with increased microprocessing power and permanent Internet connections. In-home devices may connect via cable modems or digital subscriber line technology, while office appliances would connect to the corporate Local Area Network (LAN). Sun Microsystems' Jini project (pronounced "genie") advances will boost the market for connected consumer products.

Jini builds on Sun's Java programming language and allows any computing device to connect to a network as easily as a phone plugs into a wall. Once connected, a device would announce itself to the network and provide details to the network about what it is able to do. These intelligent devices and appliances would remain on the edge of the network, ready to perform functions for any authorized user on the network.

For many emerging applications, the intelligence is migrating to the device at the edge of the network. For others, the intelligence evolves so that edge communication tools and network elements will share responsibility. Many of the applications depend on nearly permanent network connections for these edge devices, whether provided via wireless connectivity or by LAN, cable modem, or wireline.

The shifts in location of intelligence and constant connectivity represent fundamental changes in how users interact with the network. As intelligent communication tools and applications gain acceptance in the home and workplace, end user behavior and expectations will change. End users will incorporate these tools into their normal tasks, and even depend on them in crisis situations. Several examples of commercially available tools exist and more viable alternatives are being developed every day.

The national security and emergency preparedness (NS/EP) telecommunications community will need to monitor intelligent device usage patterns, assess NS/EP-specific issues, influence the fledgling technology, and capitalize on opportunities to enhance NS/EP telecommunications use of intelligent communications tools and applications.

The OMNCS Advanced Intelligence Network Program Office will continue to address network intelligence opportunities as they evolve throughout the Public Network.❖

Hamre "Cuts" JTF-CND Operations Center Ribbon, Thanks Cyberwarriors

By Jim Garamone
American Forces Press Service

Deputy Defense Secretary John Hamre presided over an August 11 "virtual" ribbon-cutting ceremony officially opening the Joint Task Force - Computer Network Defense operations center.

The Joint Task Force (JTF), located at the headquarters of the Defense Information Systems Agency, is the focal point for defense of Department of Defense (DOD) computer systems and networks. Hamre called the task force an investment America must make.

"Several times I've testified and talked on Capitol Hill about the future electronic Pearl Harbor that might happen to the United States," Hamre told the standing room only crowd. "I've used that expression not to talk about surprise attacks.... The most important message about Pearl Harbor was the way in which we had actually prepared well in advance for the war that came."

He said the designs for the capital ships the Navy used during World War II were finished before December 7, 1941. Most of the designs for Army Air Forces combat aircraft were also finished before America entered the war. "They had the foresight to see [the war] coming and do something about it," Hamre said. "That really was the message of Pearl Harbor.

The Joint Task Force - Computer Network Defense is "about growing that human resource needed for when that next Pearl Harbor comes," Deputy Defense Secretary John Hamre said as he presided over a ribbon-cutting ceremony to open the task force operations center. (Photo by John Kandrac, Defense Information Systems Agency.)

It wasn't that we got hit. It was that we were ready to respond."

That's what drives the task force—DOD is not just about fighting America's battles now, but also those in the future. "It's buying the infrastructure, in advance, that we know we are going to need at some point in time," he said. "It's [about] building the infrastructure and the resources, the talents and the skills. It's about growing that human resource needed for when that next Pearl Harbor comes."

Hamre said defending DOD's computer systems and networks is "stretching everyone's imagination." The task force achieved initial operating capacity on December 30, 1998, and full operating capacity on June 30. Establishing the office has not been easy, he noted, because the personnel had to start up while at the same time, fight a cyberwar. "[DOD] has been at cyberwar for the last half a year," Hamre said. "At least we have a place now that can do something about it."

Air Force Maj. Gen. John H. Campbell, task force commander, said his organization brings an operator's eye to the table. His staff, he said, can assess what an attack is doing to a system and can tell what effect the attack would have on operations.

"The JTF is the first DOD-wide

See Operations Center, page 8

Operations Center, cont'd from page 7

organization that can actually direct the military services to take actions to defend DOD systems and networks," Campbell said.

DOD officials have said 80 to 100 computer "events" occur daily in department systems. Of these, about 10 require further analysis. To date, DOD officials have no knowledge of a breach of a classified system. But the JTF is running into increasingly sophisticated attackers. Officials believe the technology for detecting and tracking violators is keeping up with the attackers.

"DOD has come a long way, and the JTF has given DOD a mechanism that allows more coordination between services and agencies that just didn't exist before," said JTF spokesperson Melissa Bohan. "The JTF… looks across the department and monitors computer incidents. However, this is an area for continuing research and development."

Operations specialists constantly monitor the DOD networks at the operations room of Joint Task Force - Computer Network Defense. (DOD photo)

Army LTG David J. Kelley, Director, Defense Information Systems Agency and Manager, National Communications System; Arthur Money, Senior Civilian Official for Command, Control, Communications and Intelligence (C3I); Deputy Defense Secretary John Hamre; and Air Force Maj. Gen. John Campbell, Joint Task Force - Computer Network Defense Commander, get ready to initiate a "virtual" ribbon-cutting ceremony to formally open the JTF-CND. (Photo by John Kandrac, Defense Information Systems Agency.)

Joint Task Force - Computer Network Defense has already made itself felt throughout the department. It recently issued a directive instructing all the services and other DOD organizations to complete a number of actions to improve network and system security. The actions included changing administrative and user passwords and then restarting operating systems with a "warm boot"—like using a home computer's "reset" button rather than its on-off switch.

"DOD organizations are implementing this advisory as their own management deems appropriate," Bohan said. "The JTF's service

components and the Defense Information Systems Agency's DOD Computer Emergency Response Team, and other nonintelligence DOD agencies, must comply. For the intelligence-based DOD agencies and the commanders in chief, this message was for coordination and information only. The change is still ongoing."

Hamre said all of DOD must become more concerned about computer security, and he thanked the members of the JTF for their efforts. "When [cyberwar] becomes really serious, the department will be ready, thanks to your efforts," Hamre said.❖

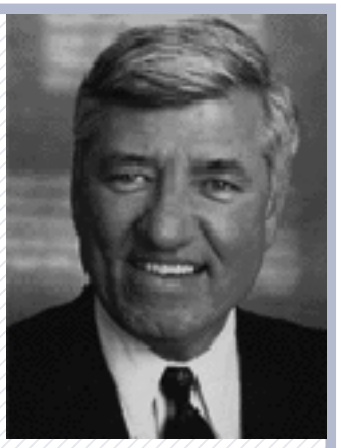
President Clinton Names Richard Brown to the President's National Security Telecommunications Advisory Committee

The President announced his intention to appoint Richard Brown to serve as a member of the President's National Security Telecommunications Advisory Committee (NSTAC).

Brown, of Texas, is currently the Chairman and Chief Executive Officer (CEO) of Electronic Data Systems, Inc. He has served as Chief Executive of Cable & Wireless PLC and as a member of the Board of Directors since July 1, 1996.

Brown has served as Chairman of the Board of CompuServe Inc., and Vice Chairman, and has been a member of the Board of Directors at Chicago-based Ameritech Corp., where he led a corporate restructuring that organized the company by product rather than geography.

Brown has been in the telecommunications industry for 28 years, holding a number of executive level posts, including President and CEO of Ameritech subsidiary Illinois Bell and Vice President of Operations of United Telecommunications, the forerunner of Sprint. He received a Bachelor of Science degree cum laude in communications from Ohio University.



Richard Brown is currently the Chairman and Chief Executive Officer (CEO) of Electronic Data Systems, Inc. He has served as Chief Executive of Cable & Wireless PLC and as a member of the Board of Directors since July 1, 1996.

The NSTAC provides the President with information and advice from the industry's perspective regarding specific measures to maintain, protect, and enhance the nation's telecommunications resources that support national security and emergency preparedness capabilities.

The Committee addresses telecommunications issues throughout the year and periodically reports directly to the President, and also to the Secretary of Defense in his capacity as the Executive Agent for the National Communications System (NCS). The NSTAC has made a number of major contributions to the NCS mission.❖

(Courtesy of the White House Press Office.)

OMNCS Reaches for the Stars!

Memorandum Establishes Collaborative Effort with Mobile Satellite Service Provider ICO

By Gabor Luka
Technology and Programs Division, OMNCS

The Office of the Manager, National Communications System (OMNCS) and ICO Global Communications Services, Inc., signed a memorandum of understanding on July 7, 1999, outlining both organizations' intent to explore National Security/Emergency Preparedness (NS/EP) solutions on ICO's satellite-based network.

The non-binding relationship with ICO will permit OMNCS collaboration and technical support of ICO's priority access development efforts, without future obligation or special consideration by the OMNCS towards ICO or its product line.

The OMNCS' Wireless Priority Service (WPS) Program Office is working with the wireless industry to identify technologies that would benefit NS/EP users. Several mobile satellite technologies provide viable alternatives for call completion during emergencies. In particular, the recent emergence of several Earth orbiting satellite systems, such as Globalstar, ICO, and Iridium, has created a potential resource for NS/EP telecommunications.

ICO Global Communications Services, Inc., an emerging major satellite service provider, conducted an initial meeting with the OMNCS on January 20, 1999, to explore the possibility of implementing a priority access service on the ICO network. ICO use of the Global System for Mobile Communications priority service standard enables development of a multi-tier priority access service. ICO recognition of the critical role satellite services can provide to emergency users during times of crises is evident through their support of the WPS requirements.

Several mobile satellite technologies provide viable alternatives for call completion during emergencies.

Members of the WPS Program Office initiated a collaborative working group with ICO and their satellite vendor—Hughes Global Services. Work is now underway to develop a feature requirements document as a first step in producing a priority access service within the ICO constellation.

Service launch is planned for August 2000. With a unique system design of 10 middle earth orbit (MEO) satellites, service will be available from any outdoor location on the globe. ICO's system integrates mobile satellite technology and terrestrial networks to provide digital voice, data, fax and messaging on a handset slightly larger than a cellular phone.

The OMNCS received direction for this effort from a White House memorandum dated January 11, 1995. The memorandum states that "...the National Communications System (NCS) should continue its effort to implement a single nationwide wireless priority access capability for NS/EP users." The significance of this milestone effort with ICO is its potential to produce a nationwide emergency wireless communications capability as initially envisioned.❖

GPS Timing, cont'd from page 1

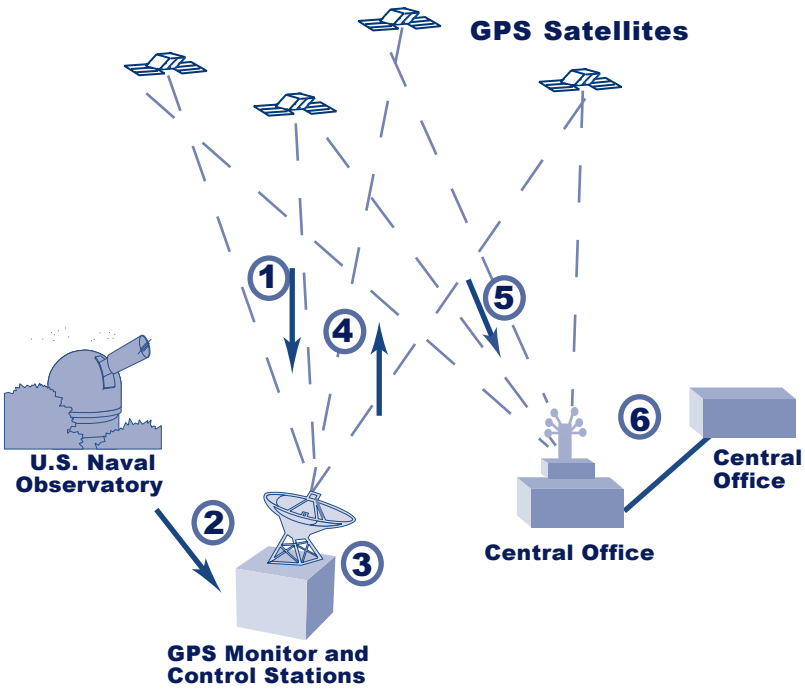
stations measure signals from all visible satellites. The accumulated data is then processed by the master control station to calculate satellite orbits and to update satellite navigation messages, including clock corrections.

The revised information is transmitted back to the satellites via the ground antennas, and finally data is transferred over radio signals to GPS receivers. The receivers comprise the user segment, which is the portion of the GPS system that converts signals into timing and positioning information for users.

To perform positioning and timing calculations, GPS employs a triangulation technique. With this method, GPS receivers measure and compare the travel time of radio signals sent from four visible satellites with known positions. Three of the measurements are used to calculate the receiver's position in three dimensions, and the fourth is used to determine time. These signals, known as pseudo-random code (PRC), are unique to each satellite. This uniqueness allows all the signals to broadcast over the same frequency.

One caveat to this method of computation is that GPS users often reduce their costs by employing receivers with less accurate clocks. Although this has the potential of introducing error into positioning and timing calculations, GPS avoids this problem by taking an extra satellite range measurement during the triangulation phase. This allows the system to correct any timing offset and thus maintain GPS' overall high level of accuracy.

Nevertheless, the triangulation technique requires that each of the satellites transmit its PRC in a highly synchronous manner. A timing error of just 1/1000 of a second would produce a measurement error of nearly 200 miles. Therefore, precise timing is a critical element for the proper implementation of GPS.



GPS Timing Sequence

1. Satellite clock information is transmitted to the monitor stations.
2. The U.S. Naval Observatory provides a timing reference, UTC (USNO), to the master control station.
3. The master control station compares satellite clock times with UTC (USNO).
4. Clock corrections are sent back to the satellites.
5. Receivers obtain updated clock data from the satellites as part of the navigation message. Corrections are made for leap seconds and other timing offsets.
6. Precise timing information is available for telecommunications network synchronization.

GPS Timing

The standard international reference for accurate time and frequency is known as Coordinated Universal Time,

See GPS Timing, page 12

GPS Timing, cont'd from page 11

denoted UTC. Developed in 1970 by the International Telecommunication Union, official UTC time is generated at the *Bureau International des Poids et Mesures*, located near Paris, France.

However, UTC is not directly available as a real-time clock. Therefore, many timing centers worldwide generate a localized estimate, which is accurate to within 100 nanoseconds of UTC. The time scale generated at the United States Naval Observatory (USNO) is one example. Known as UTC (USNO), the USNO Master Clock's approximation of official UTC is used as the timing reference for GPS.

GPS keeps its own system time that is derived from a composite clock consisting of all operational satellite clocks and the USNO timing standard. Each GPS satellite contains four atomic clocks (two cesium and two rubidium), offering a very high level of precision. The satellites transmit clock information as part of the signals that are sent to the monitor stations.

The master control station then gathers the data to calculate timing errors and make appropriate clock corrections. When the revised timing signal is uploaded to the satellites, GPS system time can be broadcast to the receivers during the satellite navigation message.

As part of its error analysis of the satellite timing signals, the master control station compares the satellite clock times with the timing standard generated at the USNO. GPS system time is steered to remain within one microsecond of UTC (USNO). However, GPS does not allow for leap seconds, as does UTC, because any discontinuity would offset the receivers.

GPS keeps its own system time, derived from a composite clock consisting of all operational satellite clocks and the U.S. Naval Observatory timing standard.

As a result, GPS time is ahead of UTC by several seconds. The receivers compensate for this difference automatically during their signal conversions, and so the timing information that is passed to the user is, in fact, a very close approximation of UTC (USNO).

The GPS records both the number of seconds that have passed in a given week and the number of weeks that have elapsed since the GPS time zero point (established at midnight (UTC) on January 6, 1980). The GPS week number cycles every 1024 weeks. After week 1023, the week number count is reset to zero, during what is called the week number rollover (WNRO) or end of week (EOW) rollover, approximately every 19.6 years.

The first GPS rollover occurred just before midnight on August 21, 1999. The rollover caused a few non-compliant civilian receivers (such as car navigation systems) to fail, but no major problems were reported. For the most part, the rollover occurred as expected.

Network Timing and Synchronization

Precise time dissemination is critical for the synchronization of telecommunications networks. Within both wireline and wireless systems, consistent pulses and time intervals are used to manage information flow through the network nodes.

In particular, the Public Switched Network (PSN) relies on accurate timing information for the proper digital transmission of voice and data. Because of the high degree of accuracy of the GPS,

special-purpose GPS receivers are often employed as a timing source.

In addition to its use in telecommunications, GPS is used in other applications as a timing reference for wide-area synchronization. These include electric power systems, distributed computer networks, banking (for money transfers and bank time locks), manufacturing, and metrology.

NS/EP Vulnerabilities

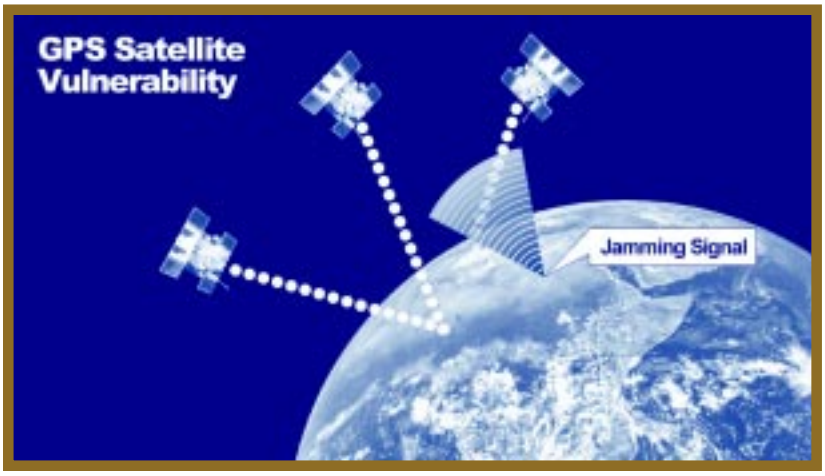
Because GPS is commonly used as a timing source for telecommunications, any system vulnerabilities concern the NS/EP community.

One limitation of GPS is its susceptibility to interference. GPS signals are extremely weak, with satellites transmitting at power levels which measure only -160 dBW at the receiving antenna. This compares to the amount of light that can be seen from a 25-watt bulb at a distance of 10,000 miles. As a result, the GPS signals can be affected by both intentional and unintentional sources.

The deliberate interference with GPS signaling is known as "jamming." It has been shown that, using readily available materials, a one-watt jammer can be constructed to tamper with GPS reception from a distance of more than 60 kilometers. Even the best of receivers are susceptible to jamming. Additionally, signals whose fundamental frequencies are within the bandwidth of a GPS receiver could unintentionally cause problems.

Possible sources of interference include emissions from both ground-based and aeronautical satellite communications equipment, wide-band noise from electrical devices, and ultra high frequency (UHF)/very high frequency (VHF) communications. Regardless of the intention, interference with GPS signaling has the potential to decrease timing precision or even cause receivers to lose signal lock.

Another NS/EP concern is that the use of GPS as a timing reference could be jeopardized by selective availability. This is the military's current practice of introducing intentional random error into the SPS signal to limit hostile use of the service.



However, telecommunications applications rely on real-time outputs. By adding random errors to the signal, peak-to-peak variations on the order of hundreds of nanoseconds can result, thereby affecting synchronization. This problem will be alleviated with the scheduled elimination of selective availability in 2006.

The pending date and time changes due to WNRO and the year 2000 (Y2K) have also caused some concern in the NS/EP community. The GPS Joint Program Office has certified that the space and control segments are WNRO/Y2K compliant. However, the compliance of the user segment, in particular, the receivers, will vary according to manufacturer and model. It is unclear what problems will occur as a result of receiver noncompliance. One scenario is that user equipment may experience delays while locating GPS satellites or while making position and date calculations.

It is also possible that satellites might not be located at all. Even if receivers do properly access the satellite signals, they might display inaccurate timing and position information. Although it is uncertain how widespread such problems might be, it is expected that only older equipment would be affected. Newer models have been programmed to properly account for the date and time transitions.❖

U.S. Telecommunications Industry on Track to Achieve Year 2000 Readiness

The U.S. telecommunications industry is on track to continue providing uninterrupted local and long distance services into the next century according to the Federal Communications Commission's advisory council responsible for assessing Year 2000 (Y2K) readiness.

In a report to the FCC, the Network Reliability and Interoperability Council (NRIC) announced that their findings were based on surveying companies across the telecommunications industry. As of March 1999, approximately 90 percent of local and 99 percent of long distance switches in the U.S. Public Switched Telephone Network (PSTN) were expected to be Y2K ready. NRIC reported that 100 percent of large Local Exchange Carrier (LEC) and major Inter-Exchange Carrier (IXC) switches were expected to be fully Y2K ready by the end of June 1999.

NRIC suggests equipment owners conduct a thorough evaluation of their systems to ensure that any required upgrades are identified and obtained.

Mid-sized LECs, while trailing their larger company counterparts, appear to be on track to achieve Y2K readiness in the third and fourth quarters of 1999. Because many smaller LECs still need to report progress, several industry associations, whose membership includes these smaller companies, have agreed to communicate these results to their members to increase awareness of the situation and to promote information sharing of their Y2K compliance efforts.

NRIC also reported that major LECs and IXCs have completed network interoperability testing or have plans in place to complete these tests. Based on completion of these tests, the majority of access and inter-exchange switch and signaling vendors identified no major interoperability gaps.

The NRIC report also provided specifics on the readiness of customer premises equipment (CPE) and systems that interface with the PSTN. The report was generally positive about the efforts of the CPE industry (which includes PBXs, key systems, faxes, modems, and wireless devices) to achieve Y2K readiness. NRIC recognizes the importance of 911 emergency calls, as well as assuring that customers have dial tone.

It was reported that while the PSTN is expected to continue to deliver 911 calls to Public Safety Answering Positions (PSAP), which are utilized by local governments in responding to 911 calls, some

PSAPs may not be able to process calls with all of their ancillary features unless upgraded to be Y2K ready. Many large LECs are working with local governments to identify PSAP requirements for Y2K readiness.

The NRIC report urged CPE owners to take responsibility to find out about the Y2K date issues associated with their devices and systems. NRIC suggests equipment owners do the following: conduct a thorough evaluation of their systems to ensure that any required upgrades are identified and obtained, and visit manufacturers' Y2K Web sites for product-by-product matrix listings that provide specifics on readiness; whether testing has been done; if upgrades are required; etc.

Based on a compilation of various public and private assessments of countries that represent approximately 96 percent of international traffic to and from the U.S., NRIC reported that some 75 percent of those countries have an increased risk in achieving Y2K readiness, as compared with the Council's January assessment.

Of eight geographic regions sampled, six were perceived as high risk-–with a strong indication that some countries in the region may not achieve Y2K readiness by January 1, 2000; and two as medium risk. Based on information provided, 191 countries have been assessed for Y2K readiness by NRIC.

For those countries whose Y2K telecommunications readiness may be an issue to the U.S., NRIC is working with the Department of State and other Government agencies, as well as other industry sectors, prioritizing countries that are at significant risk in achieving Y2K readiness.

In its report, NRIC also focused on industry-wide Y2K contingency planning efforts. A primary focus of the industry is communications among participants in the unlikely event of network outages associated with Y2K.

In its report, NRIC indicated that a national system is being planned that could be used as a communications tool to share information on real-time Y2K experiences with counterparts around the world. This communications system will allow a global approach for the coordination and resolution of telecommunications problems, regardless of their nature or location but also could be beneficial in providing information that systems are working properly.

Overall, NRIC reported the U.S. telecommunications industry is effectively approaching Y2K readiness, well in advance of the turn-of-the century, and that public telecommunications networks are expected to continue to reliably function, interoperate and interconnect on and after January 1, 2000.❖

(Courtesy of the Federal Communications Commission.)

- **Some PSAPs may not be able to process calls with all of their ancillary features unless upgraded to be Y2K ready.**

- **Of eight geographic regions sampled, six were perceived as high risk and two as medium risk.**

Gov. Ridge Leads Regional Agreement for Cooperative Information Sharing on Year 2000 Challenge

Governors from four other states sign proclamation

Pennsylvania Gov. Tom Ridge announced on May 28 that four other state governors have joined him in signing a proclamation to promote broad public awareness of the Year 2000 (Y2K) computer challenge within their states and to encourage cooperative information sharing among them.

Governors joining Ridge in signing the proclamation were John Engler of Michigan, Virginia's James Gilmore III, Christine Todd Whitman of New Jersey, and Delaware's Thomas Carper.

"The impact of the Year 2000 computer 'bug' does not stop at a state's borders," Ridge said. "We are all better served by working in unison to alert our citizens to this threat and to share information on the progress we are making. "I'm pleased that Pennsylvania could lead this effort to encourage the exchange of accurate information within our region, and I hope that other states will join us as proactive Y2K partners."

Work on the proclamation began following a summit of utility and telecommunications regulatory officials from nine states co-hosted by the Ridge Administration and the Pennsylvania Public Utility Commission in Hershey, Pennsylvania, last December.

The summit highlighted the need for coordinated action to address potential Year 2000 impacts shared between neighboring states. At that time, chief information officers from the five signing states raised the idea of developing a proclamation to encourage broader regional information sharing on the Y2K problem.

The summit highlighted the need for coordinated action to address potential Year 2000 impacts shared between neighboring states.

According to the new Year 2000 pact, the five governors agreed to make concerted efforts to resolve the date-change problem within their respective states. They will engage in Y2K public awareness activities and work to promote intrastate and interstate cooperation on the Year 2000 problem. They will also encourage the exchange of accurate information on Y2K progress in each of their states.

The signed proclamation has been presented to Carper, chairman of the National Governors' Association, for consideration by other states.

Pennsylvania State Government has been recognized frequently by Year 2000 experts and prominent publications as a national Year 2000 leader. More information on the state's Year 2000 progress can be found on Pennsylvania's home page at www.state.pa.us (see "Technology Initiatives") and at the Pa2K Web site providing Year 2000 informational materials, www.Pa2K.org.❖

(Story courtesy of the Pennsylvania Y2K Public Affairs Office.)