"The Network Is Down ..."

Capt. Cathy Walter
Headquarters, Air Force Communications Agency

This articles discusses critical network components that must be assessed for year 2000 (Y2K) compliance, what kind of errors to expect, and how to determine if the devices are at risk of Y2K faulty logic.

War fighters may laugh at the title, but the Air Force cannot support flying operations without its data networks. Until recently, the focus of Y2K efforts has been the renovation of mainframe-based software. But the day of the dedicated circuit and mainframe system is quickly disappearing. What am I talking about? Many Air Force command, control, communications, computers, intelligence, and logistics systems are designed to run on the Internet via the base's client-server data network, for example, the Global Command and Control System, the Global Transportation Network, the Core Automated Maintenance System, and the Standard Base Supply System. And do not forget basic E-mail service—who could survive without it? The Air Force air and space operational mission has become dependant on the information exchange E-mail offers.

Network device hardware and component software functions derive dates from embedded real-time clock (RTC) chips, basic input/output system (BIOS) firm or flash read-only memory, or network time-server hosts. These items pass date information to hosts, clients, network devices, and selected software applications. This article discusses the critical network components that must be assessed for Y2K compliance, what kind of errors you might expect, and how to determine if the devices you operate and maintain are at risk of Y2K faulty logic. A candidate list of network components for Y2K consideration is provided in the sidebar below.

Network Protocols

The underlying construct for all networks is the network protocols. According to a March 1998 paper by the Internet Engineering Task Force, most of the current implementations of these protocols will not be impacted by Y2K logic errors. However, transport layer, e.g., TCP, network layer, e.g., IP, application layer, e.g., HTTP, and protocol con-

Candidate Components for Y2K Consideration

Network Types

- Multiplexers with date-dependent channel or bandwidth controls.
- Routed networks with date-dependent routing metrics.
- Multicast radio nets with date-dependent controls.
- Point-to-point radio nets with date-dependent controls.
- Satellite networks with a shared date and time-dependent transponder.
- Cable networks with pre-programmed scheduling.

Network Systems

- Operating System services (Windows NT, HP UX, and NetWare).
- Domain Name Service (DNS) implementation.
- Network Information Service (NIS) implementation.
- Novell Directory Service (NDS) implementation.
- Network Time Protocol (NTP) Service implementation.
- Managed systems with date or scheduling processes (UNIX cron tabs).
- Automated backup systems.
- Messaging systems.
- Network management subsystems.
- Operational test equipment with date log.
- Dedicated server (Web proxy and time).

Devices

- Simple Mail Transport Protocol (SMTP) gateways.
- Managed modem banks (for remote access).
- Switches (voice, data, and video).
- Routers.
- Bridges.
- Firewalls or guards.
- Intelligent hubs.
- Multiplexers.
- Wireless controllers and managers.
- Date dependent CSUs and DSUs.
- Management modules.
- Token ring NIC cards using RTC functions.
- Any device that maintains time with an RTC.

Application Software

- Network, system, or application management utilities.
- Office automation.
- E-mail applications.
- Job control and scheduling.
- Scheduling.
- Metering software.
- Anti-virus software.
- Databases.
- Client-server applications.
- Date and time-dependent controls.

structs have not been fully investigated. At least one significant potential problem has been identified that may affect Web operations. Version 1.1 of HTTP, as defined by RFC (Request for Comment) 2068, requires the transmission of dates in a four-digit format as defined by RFC 1123. More than one-fifth of the Web servers on the Internet use a noncompliant two-digit format that was defined in the outdated RFC 850. Implementation of RFC 2068-compliant code will partially alleviate this problem. Older implementations of network protocols, e.g., RFC 850, that use two-digit dates are not Y2K compliant. For complete details, see The Internet and the Millennium Problem (Year 2000) on the Internet Engineering Task Force Web site at http://www.ietf.org/ids.by.wg/2000.html.

Another network construct of vital interest is the Network Time Protocol (NTP). It is used by network time-server applications to synchronize the date and time on all networked devices—from routers to supercomputers. The date format used by NTP has always been a four-digit format, so it is Y2K compliant. Devices that feed or use the date processed by NTP must adhere to the same date storage and maintenance format to also be Y2K compliant. In the Air Force, the date and time reference for NTP is drawn from traceable date and time references, e.g., Global Positioning System, and is compatible with Version 3 of the Network Time Protocol (RFC 1305). It is the transfer of incompatible, garbled, or truncated date and time information from network devices such as routers, application servers, e.g., time servers, and database hosts (Figure 1) that is a potential killer for our networks.

Workstations, Servers, and Minicomputers

The most common source of potential Y2K impact for networked data systems is from servers and workstations. Although the operating systems of networked devices may take the date and time from a network time server on boot-up, some applications tap the BIOS chip for this date information. Some communication system interfaces do not rely on a BIOS capability but use quasi-analog interfaces to track real-time clock transitions. What could it mean if the clock reference system, the digital BIOS or RTC is noncompliant? You could suddenly find you are no longer authorized to use your office automation system, your network connection is severed, or that your mission-critical networked files and E-mail have been deleted. An application server could grind to a halt under a flood of log data filling up a shared storage device. If you are fortunate, your resourceful local area network administrator or Network Control Center wizard may be able to recover and re-enter the corrupted user data. But what if the backup utility also fails, or you cannot wait for data restoration?

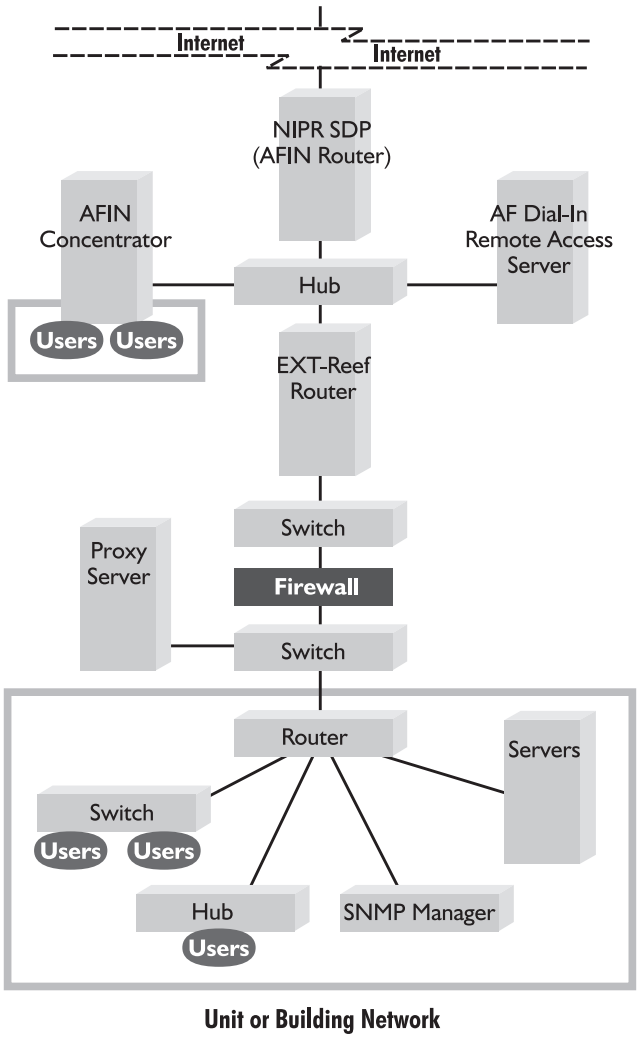
To give you an idea how pervasive and potentially critical this problem is, Figure 1 (items in gray) show where personal computers or workstations may be in use on your network. Note that noncompliance of any of these components could lead to serious problems during or after critical dates such as Sept. 9, 1999, Dec. 31, 1999, Jan. 1, 2000, and Feb. 29, 2000. One test conducted by the Air Force Communications Agency Technology Directorate found 35 percent of PCs will fail the Y2K rollover, but almost all of those can be fixed with a BIOS update or patch.

Fortunately, fixing a noncompliant PC is straightforward, since software patches and numerous utilities are available from original equipment manufacturers (OEM) and independent software vendors. However, before trying any new patch or utility, make sure you virus-check any new files or utilities you download, and back up all critical or time-sensitive data. Since some license agreements (especially on UNIX) may have expiration triggers, make sure you have validated access to all installed software before you attempt any date-change testing. If you have important but troublesome hardware for which none of the popular software patches work, RTC cards may be obtained for as little as $150 per machine. The RTC hardware replacement method is a viable option if BIOS updates or patches fail, or you do not want to rely on an external date and time clock reference.

Operating Systems and Applications

If the RTC or the BIOS chip does not get your network, the operating system or a faulty utility might. The most common

Figure 1. *The typical Air Force network topology.*



network operating systems in the Air Force, e.g., Windows NT and Novell NetWare, use different time utilities and synchronization methods to set the date and time on clients and servers. Beware that security functions, business applications, anti-virus software, management utilities, directory caching, and file and print services also rely on operating system dates. E-mail products, like other network-based services, are driven in large measure by date and time stamps. Messages may be deleted or rejected by the component utilities because the software thinks its shelf life has expired. Message measurement and tracking utilities also are vulnerable. Verify that your hardware is compliant and upgrade to a Y2K compliant version of the software.

Routers, Switches, and Hubs

On the diagram of a typical Air Force network (Figure 1), you will notice that if a network device is not a PC or workstation, it is probably a router, a switch, or a hub. A base may have anywhere from one to 50 of these devices, depending on the configuration of the base network. Routers, switches, and hubs do not require date and time stamps to forward packets, but operation and maintenance may experience problems if the associated operating software or controlling management application is noncompliant. Network events are logged in these devices, and the Y2K rollover could result in lost or misrouted error information.

Fortunately, most Air Force routers are the newer Cisco 4000 and 7000 models that can be upgraded into compliance through free patches available from the vendor. At some bases, older Cisco AGS/AGS+ routers also are prevalent. According to Cisco System representatives, these older routers are at the end of their lifecycle and will not be tested for Y2K compliance. Check your manufacturer's Web site for Y2K compliance and upgrade information. A listing of some key OEM Web sites are available on the Air Force Year 2000 Web site under Y2K Toolkit/Resources & Links.

Putting It All Together

After you have inventoried, determined compliance, and upgraded all these items, the next step is to perform operational assessments. Air Force functional communities are conducting functional integration and interoperability assessments to ensure mission continuity in the year 2000.

Focus on the Network

Air Force networks are mission critical to the operational mission of the Air Force. More and more deployed environments reach back to the fixed base architecture for communication support. It is also the one mission-critical piece of communications that has been wholly designed, funded, and acquired by base units. People at the bases are the only ones who know what is in use and can fix it. We have less than one year to ensure operations beyond the year 2000. Base Communication Squadrons must focus on this mission-critical asset.

How to Contact Us

For more about the Air Force Y2K program, contact us at the below numbers. You may also visit our Web page at http://year2000.af.mil for information on commercial-off-the-shelf compliance and testing and the status of centrally managed communication and information infrastructure items, e.g., voice switches. The site also includes Air Force Y2K guidance packages and links to other Web sites, including sites focused on the impact of Y2K on communications infrastructure. ◆

About the Author

Capt. Cathy Walter has been in the Air Force for nine years. She is the Air Force Y2K communication and information functional manager in the Air Force Y2K Program Management Office.

AF Y2K Program Management Office
HQ Air Force Communications Agency
203 W. Losey Street
Scott AFB, IL 62225-5222
Voice: 618-256-5761 DSN 576-5761
E-mail: AFCA-AFY2K@scott.af.mil

Inventory Your Network with Simple Network Management Protocol

Have you been trying to collect a complete list of network infrastructure components on your base for Y2K certification? Although this can be a difficult task, your network management system (NMS) can help get the project off the ground. HP OpenView, for example, is a common NMS with the capability to query network components for system information.

What information is needed to verify Y2K compliance for a device? The key information is node name, node type (router, hub, etc.), vendor, model number, and software version. An example description of a Cisco router would be "Bldg. 100, router, Cisco, 3000, IOS 11. 1(6)." NMS systems can be used to gather this data since it is contained in a standard management information base called system description, or sysdescr, on all simple network management protocol (SNMP)-manageable devices. You can use OpenView to check the system description by highlighting the component and selecting System Information from the Configuration menu.

A complete inventory requires information from nonmanaged network infrastructure components as well. The primary network managers at your base should be able to identify the key network equipment that is not visible on the NMS console. This can be traced to one of three causes: The device has no SNMP capability, SNMP has not been enabled on the device, or the community string for the device is not entered properly on the NMS. If the system cannot be managed using SNMP, the system data will have to be gained manually. Devices that are SNMP-manageable should be configured to be visible in your NMS not just for this project but to enhance overall network visibility and management. As a general security measure, ensure that community strings on your network equipment are not set to "public." See http://www.afca.scott.af.mil/pa/public/98may/intercom.htm to view other Air Force Y2K articles.

1st Lt. Mike Witzman
Staff Sgt. Kevin Nichols
Voice: 618-256-8513 DSN 576-8513
AFCA Scope Network