Network Working Group

Philip J. Nesser II
Editor
Nesser & Nesser Consulting

draft-ietf-2000-issue-02.txt
Internet Draft
March 1998

The Internet and the Millenium Problem (Year 2000)

Abstract

The Year 2000 Working Group(WG) has conducted an investigation into the millenium problem as it regards Internet related protocols. This investigation only targeted the protocols as documented in the Request For Comments Series (RFCs). This investigation discovered little reason for concern with regards to the functionality of the protocols. A few minor cases of older implementations still using two digit years (ala RFC 850) were discovered, but almost all Internet protocols were given a clean bill of health. Several cases of ''period'' problems were discussed where a time field would ''roll over'' as the size of field was reached. In particular, there are several protocols, which have 32 bit, signed integer representations of the number of seconds since January 1, 1970 which will turn negative at Tue Jan 19 03:14:07 GMT 2038. Areas whose protocols will be effected by such problems have been notified so that new revisions will remove this limitation.

1.0 Introduction

According to the trade press billions of dollars will be spend the upcoming three years on the year 2000 problem, also called the millenium problem (though the third millenium will only start in 2001). This problem consists of the fact that many software packages and some protocols use a two-digit field for the year in a date field. Most of the problems seem to be in administrative and financial programs, or in the hardcoded microcomputers found in electronic equipment. A lot of organizations are now starting to make an inventory of which software and tools they use will suffer from the millenium problem.

With the increasing popularity of the Internet, more and more organizations start to use the Internet as a serious business tool. This means that most organizations will want to analyze the millenium problems due to the use of Internet protocols and popular Internet software. In the trade press the first articles suggest that the Internet will collapse at midnight the 31st of December 1999.

To counter these suggestions (that are obviously wrong) and to avoid that all over the Internet people will redo the same inventory over and over again the WG is to make an inventory of all important Internet protocols and their most popular implementations with respect to the millenium problem. Only software and protocols directly related to the Internet will be considered.

The editor of this document would like to acknowledge the critical contributions of the follow for direct performance of research and the provision of text: Alex Latzko, Robert Elz, Erik Huizer, Gillian Greenwood, Barbara Jennings, R.E. (Robert) Moore, David Mills, Lynn Kubinec, Michael Patton, Chris Newman, Erik-Jan Bos, Paul Hoffman, and Rick H. Wesson. The pace with which this group has operated has only been achievable by the intimate familiarity of the contributors with the protocols and ready access to the collective knowledge of the IETF.

Disclaimer

This RFC is not complete. It is an effort to analyze the Y2K impact on hundreds of protocols but is likely to have missed some protocols and misunderstood others. Organizations should not attempt to claim any legitimacy or approval for any particular protocol based on this document. The efforts have concentrated on the identification of potential problems, rather than solutions to any of the problems that have been identified. Any proposed solutions are only that: proposed. A formal engineering review should take place before any solution is adopted.

Methodology

The first task was dividing the types of RFC's into logical groups rather than the strict numeric publishing order. Fifteen specific areas were identified. They are: "Autoconfiguration" , "Directory Services", "Disk Sharing", "Games and Chat" ,"Information Services &

File Transfer", "Network & Transport Layer", "Electronic Mail", "NTP", Name Serving", "Network Management", "News", "Real Time Services", "Routing", "Security", and "Virtual Terminal". In addition to these categories many hundreds of RFC's were immediately eliminated because of the type of content. That is not to say that all Informational RFC's were not considered, many did contain some technical content or overview which demanded scrutiny.

Each area was assigned to a team for investigation. Although each team used whatever additional investigation techniques which seemed appropriate (including completely reading each RFC, and in some cases the source code for the reference implementation) at minimum each team used an automatic scanning system to search for the following items (case insensitively) in each RFC:

- date
- GMT
- UTCTime
- year
- yy (that is not part of yyyy)
- two-digit, 2-digit, 2digit
- century
- 1900 & 2000

Note that all of these strings except "UTCTime" may occur in conjunction with a date format that accommodates the Year 2000 crossing, as well as with one that does not. So "hits" on these string do not necessarily indicate Year 2000 problems: they simply identify elements that need to be examined.

After the documents were scanned, therefore, each "hit" was examined individually. Those that cause no Year 2000 problems (e.g., those that encode the year as a two-byte integer, or as a four-character display string) are not discussed here. Those that do cause Year 2000 problems are identified in this document, and the nature and impact of the problems they cause are described.

Types of Year 2000 Problems

Summary of Solutions

2.0 **Autoconfiguration**

Summary

The RFC's which were categorized into this group were primarily the BOOT Protocol (BOOTP) and the Dynamic Host Configuration Protocol (DHCP) for both IP version four and six.

Examination of the BOOTP protocols and most popular implementations show no year 2000 problems. All times are references as 32 bit integers in seconds of UTC time. An investigation of all DHCP and the IPv6 autoconfiguration mechanisms produced no year 2000 problems. All references to time, in particular lease lengths, are 32 bit integers in seconds, allowing lease times of well over 100 years.

Specifics

The following RFCs were examined for possible millenium problems: 906, 951, 1048, 1084, 1395, 1497, 1531, 1532, 1533, 1534, 1541, 1542, 1970, & **1971**.   **RFC 951's only reference to time or dates is a two byte filed in** the packet which is number of second since the hosts was booted. RFC's 1048, 1084, 1395, 1497, 1531, & 1532 have either no references to dates and time, or they are the same as the RFCs which obsoleted them discussed in the next paragraph.

RFC 1533 enumerates all the known DHCP field types and a number of these have to do with time. Section 3.4 defines a "Time Offset" field which specifies the offset of the clients subnet in seconds from UTC. This 4 byte field has no millenium issues. Section 9.2 defines the IP Address Lease Time field which is used by clients to request a specific lease time. This four byte field is an unsigned integer containing a number of seconds. Section 9.9 defines a Renewal Time Value field, Section 9.10 defines a Rebinding Time Value,
both of which are similarly 32 bit fields which have no millenium issues.

RFC 1534 has no references to times or dates.

RFC 1541 has two mentions of times/dates. The first is the "secs" field which, similarly to RFC 951, is a 16 bit field for the number of seconds since the host
has booted. There is also a discussion in section 3.3 about "Interpretation and
Representation of Time Values" which while clearly states that there is no millenium or period problems.

RFC 1542 also references the "secs" field mentioned previously.

RFC 1970 mentions a number of variables which are time related. In section 4.2 "Router Advertisment Message Format" the following fields are defined: Router Lifetime, Reachable Time, & Retrans Timer. In section 4.6.2 "Prefix Information"
the following are defined: Valid Lifetime, & Prefered Lifetime. In section **6.2.1 "Router Configuration Variables the following are defined:**
MaxRtrAdvInterval,
MinRtrAdvInterval, AdvReachableTime, AdvRetransTimer, AdvDefaultLifetime, AdvValidLifetime, & AdvPreferredLifetime. All of these fields specify counters of some sort which have no millenium or periodicity problems.

RFC 1971 has some discussion of preferred lifetimes, depreciated lifetimes and valide lifetimes of leases, but only discusses them in an expository way.

3.0 Directory Services

Summary

The RFC's which were categorized into this group were primarily X.500 related RFC's, Whois, Rwhois, Whois++, and the Lightweight Directory Access Protocol (LDAP).

Upon review of the Directory Services related RFC's, no serious year **2000 problems were discovered.** Some minor issues were noted and explained below in the specifics portion of this section.

Specifics

RFCs that mentioned UTC Time or made reference to uTCTimeSyntax could fail to be Y2K compliant. These should be updated to specify the four year version of uTCTimeSyntax rather than giving the option of using a two year date representation. The following RFCs fall into this category:

```
    rfc1274.txt - References UTC date/time
    rfc1276.txt - References UTC date/time for version control.
    rfc1488.txt - References UTC Time as printable strings.
    rfc1608.txt - Refers to uTCTimeSyntax
    rfc1609.txt - Refers to uTCTimeSyntax
    rfc1778.txt - Refers to uTCTimeSyntax
```

Two RFC's have unusual date specifications and specify their own date format. Both of these support Y2K compliant dates.

RFC1714 (RWhois) specifies date formats that are not Y2K compliant, but it also support dates that are. Implementers of the RWhois protocol should only use the %MY4 format

RFC1834 (Whois++) requires the use of dates, but it didn't specify the format, syntax, or representation of the date string to be used.

4.0 Disk Sharing

Summary

The RFC's which were categorized into this group were those related to the Network File System (NFS). Other popular disk sharing protocols like SMB and AFS were referred to their respective trustee's for review.

After careful review, NFS has no year 2000 problems.

Specifics

The reference to time in this protocol are the times of file data modification, file access, and file metadata change (mtime, atime, and time, respectively). These times are kept as 32 bit unsigned quantities in seconds since 1970-01-01, and so the NFS protocol will not experience an Epoch event until the year 2106.

5.0 Games and Chat

Summary

The RFC's which were categorized into this group were related to the Internet Relay Chat Protocol (IRC). No millenium problems exist in the IRC protocol.

Specifics

There is only a single instance of time or date related information in the IRC protocol as specified by RFC 1459. Section 4.3.4 defines a TIME message type which queries a server for its local time. No mention is made of the format of the repy or how it is parsed, the assumption being specific implementations will handle the reply and parse it appropriately.

6.0 Information Services & File Transfer

Summary

The RFC's which were categorized into this group were divided among World Wide Web (WWW) protocols and File Transfer Protocols (FTP). WWW protocols include the Hypertext Transfer Protocol (HTTP), a variety of Uniform Resource formats (URL, URAs, etc.) and the HyperText Markup Language(HTML). FTP protocols include the well known FTP protocol, the Trivial File Transfer Protocol (TFTP) and a variety of extensions to these protocols. Other information services includes the Finger Protocol and the LPD protocol.

HTTP 1.1 requires all newly generated date stamps to conform to RFC 1123 **date formats which are Year 2000 compliant, but it also requires** acceptance of the older non-compliant RFC850 formats. Some specific recommendations are listed below and have been passed to the HTTP WG.

HTML 2.0 could allow a very subtle Year 2000 problem, but once again this recommendation has been passed on the HTML WG.

<<EDITOR'S NOTE: We need some serious help with this section because

there are a lot of things still to check.>>

Specifics

HTTP:

The main IETF standards-track document on the HTTP protocol is RFC2068 on HTTP 1.1. It notes that historically three different date formats have been used, and that one of them uses a two-digit year field. In section 3.3.1 it requires HTTP 1.1 implementations to generate this RFC1123 format:

```
     Sun, 06 Nov 1994 08:49:37 GMT  ; RFC 822, updated by RFC 1123
```

instead of this RFC850 format:

```
     Sunday, 06-Nov-94 08:49:37 GMT ; RFC 850, obsoleted by RFC 1036
```

Unfortunately, many existing servers, serving on the order of one fifth of the current HTTP traffic, send dates in the ambiguous RFC850 format.

Section 19.3 of the RFC2068 says this:

  o HTTP/1.1 clients and caches should assume that an RFC-850 date which appears to be more than 50 years in the future is in fact in the past (this helps solve the "year 2000" problem).

This avoids a "stale cache" problem, which would cause the user to see out-of-date data.

But to avoid unnecessary delays and bandwidth indicated in Scenario 2 **below, this should be extended to say that a date which appears to** be more than 50 years in the past may be assumed to be in the future, if a future date is legal for that field.

Scenario 3 indicates that servers may also want to follow these rules.

Here is some more background and justification for these arguments.

The following headers use full dates:

```
HTTP/1.0:
        Date:
        Expires:                # can be in the future
        If-Modified-Since:      # required to be in the past
        Last-Modified:          # required to be in the past
        Retry-After:            # can be in the future, also takes
                                # relative time - number of seconds
```

```
HTTP/1.1:
        If-Range:
        If-Unmodified-Since:    # required to be in the past
```

Note that clock skew between hosts can lead to confusion here - see the RFC for details.

Here are some scenarios of the implications of RFC850 dates, which include stale caches, unnecessary requests for things which are validly cached, delays for the user, extra bandwidth, and presenting incorrect information to the user.

Some cases involve comparisons with the current time, and others may involve comparisons between dates from different sources. The abbreviation "/99" is used to imply an RFC850 date with the value "99" for the year.

RFC850 date from server

Scenario 1:

If a client gets an Expires /99 date after the year 2000, it should interpret it as 1999, to avoid ending up with a stale cache entry.

This is as already specified in RFC2068.

Scenario 2:

If a client gets an Expires /00 date before the year 2000, and subsequently is faced with a choice to either retrieve the document from its cache or look for an updated copy, it may interpret it as the year 2000, to avoid the unnecessary delay and bandwidth of an extra request.

RFC850 date from client

Scenario 3:

If a server gets an If-Modified-Since /99 date from a client after the year 2000, it should interpret it as 1999 when comparing with the local modification date, in order to possibly avoid sending a full GET response rather than a HEAD response.

Note that an If-Modified-Since header must never be in the future.

HTML

In RFC1866, on HTML 2.0,the <META> tag allows the embedding of recommended values for some HTTP headers, including Expires. E.g.

```
    <META HTTP-EQUIV="Expires"
          CONTENT="Tue, 04 Dec 1993 21:29:02 GMT">
```

Servers should rewrite these dates into RFC1123 format if necessary.

7.0 Network & Transport Layer

Summary

The RFC's which were categorized into this group were the Internet Protocol (IP) versions four and six, the Transmission Control Protocol (TCP), the User Datagram Protocol (UDP), the Point-to-Point Protocol (PPP) and its extensions, Internet Control Message Protocol (ICMP), the Address Resolution Protocol (ARP) and Remote Procedure Call (RPC) protocol. A variety of less known protocols were also examined.

Specifics

<<EDITOR'S NOTE: Not done yet but Robert Elz is almost finished>>

8.0 Electronic Mail

Summary

The RFC's which were categorized into this group were the Simple Mail Transfer Protocol (SMTP), Internet Mail Access Protocol (IMAP), Post Office Protocol (POP), Multipurpose Internet Mail Exchange (MIME), and **X.400 to SMTP interaction.**

After reviewing all mail-related RFCs, it was discovered that while some obsolete standards required two-digit years, all currently-used standards require four-digit years and are thus not prone to typical Year 2000 problems.

Specifics

RFCs 821 and 822, the main basis for SMTP mail exchange and message format, originally required two-digit years. However, both of these RFCs were later modified by RFC 1123 in 1989, which strongly recommended 4-digit years. Although there might be a few very old SMTP systems using two-digit years, it is believed that almost all mail sent over the Internet today uses four-digit years. Mail that contains two-digit years in its SMTP headers will not "fail", but might be missorted in message stores and mail user agents. This problem is avoided entirely by taking the RFC 1123 change as a requirement, rather than merely as a recommendation.

IMAP versions 1, 2, and 3 used two-digit years, but IMAP version 4 (defined in RFCs 1730 and 1732 in 1994) requires four-digit years. There are still a few IMAP 2 servers and clients in use on the Internet today, but IMAP version 4 has already take over almost all of the IMAP market. Mail stored on an IMAP server or client with two-digit years will not "fail", but could possibly be missorted or prematurely expired.

RFC 1153 describes a format for digests of mailing lists, and uses two-digit dates. This format is not widely used. The use of two-digit dates could possibly cause missorting of stored messages.

RFC 1327, which describes mapping between X.400 mail and SMTP mail, uses the UTCTime format.

RFC 1422 describes the structure of certificates that were used in PEM (and are expected to be used in many other mail and non-mail services). Those certificates use dates in UTCTime format. Poorly-written software might prematurely expire or validate a certificate based on comparisons of the date with the current date, although no current software is known to do this.

9.0 Network Time Protocols

Summary

The RFC's which were categorized into this group were the Network Time Protocol (NTP), and the Time Protocol.

NTP has been certified year 2000 compliant, while the Time Protocol will "roll over" at Thu Feb 07 00:54:54 2036 GMT. Since NTP is the current defacto standard for network time this does not seem to be an issue.

Specifics

There is no reference anywhere in the NTP specification or implementation to any reference epoch other than 1 January 1900. In short, NTP doesn't know anything about the millennium.

From the Time Protocol RFC (868):

```
    S: Send the time as a 32 bit binary number.

    ...
```

The time is the number of seconds since 00:00 (midnight) 1 January 1900 GMT, such that the time 1 is 12:00:01 am on 1 January 1900 GMT; this base will serve until the year 2036.

10.0 Name Services

Summary

The RFC's which were categorized into this group were the Domain Name System (DNS), it's advanced add on features (Incremental Zone Transfer, etc.).

Specifics

<<EDITOR'S NOTE: Still need this information>>

11.0 Network Management

Summary

The RFC's which were categorized into this group were the Simple Network Management Protocol (SNMP), a large number of Management Information Bases (MIBs) and the Common Management Information Protocol (CMIP).

Although a few discrepancies have been found and outlined below, none of them should have an impacts on interoperability.

Specifics

1. Use of GeneralizedTime in CMOT (RFCs 1095 and 1189)

The standards for CMIP over TCP/IP specify an unusual use for the GeneralizedTime type. (GeneralizedTime has a four-digit representation of the year.)

If the system generating the PDU does not have the current time, yet does have the time since last boot, then GeneralizedTime can be used to encode this information. The time since last boot will be added to the base time "0001 Jan 1 00:00:00.00" using the Gregorian calendar algorithm.

This is really a "Year 0" problem rather than a Year 2000 problem, and in any case, CMOT is not currently deployed.

2. UTCTime in SNMP Definitions

UTCTime is an ASN.1 type that includes a two-digit representation of the year. There are several options for UTCTime in ASN.1, that vary in precision and in local versus GMT, but these options all have two-digit years. The standards for SNMP definitions specify one particular format:

```
       YYMMDDHHMMZ
```

The first usage of UTCTime in the standards for SNMP definitions goes all the way back to RFC 1303. It has persisted unchanged up through the current specifications in RFC 1902. The role of UTCTime in SNMP definitions is to record the history of an SNMP MIB module in the module itself, via two ASN.1 macros:

- o LAST-UPDATED
- o REVISION

Applications that store and use MIB modules need to be smart about interpreting these UTCTimes, but with one exception, the times do not actually flow in the network. This one exception is the appnNodeMibVersion object in the APPN MIB (currently draft-ietf-snanau-appnmib-04.txt, but soon to be published as an RFC), which returns the value of LAST-UPDATED from the version of the APPN MIB that an agent has implemented. An application that can correctly interpret UTCTimes, by prepending a "19" or a "20" as appropriate, in the MIB modules it has stored locally will be able to interpret the value of this object correctly as well.

3. Objects in the Printer MIB (RFC 1559)

There are two objects in the Printer MIB that allow use of a date as an object value with no explicit guidance for formatting the value. The objects are prtInterpreterLangVersion and prtInterpreterVersion. Both are defined with a syntax of OCTET STRING. The descriptions for the objects allow the object value to contain a date, version code or other product specific information to identify the interpreter or language. The descriptions do not include an explicit statement recommending use of a four-digit year when a date is used as the object value.

4. Dates in Mobile Network Tracing Records (RFC 2041)

The RFC specifies trace headers and footers with date fields that are character arrays of size 32. While 32 characters certainly provide enough room for a four-digit year, there's no explicit statement that these years must be represented with four digits.

12.0 Network News

Summary

The RFC's which were categorized into this group were related to the Network News Protocol (NNTP).

There does exist a problem in both NNTP and the Usenet News Message Format. They both specify two digit year format. A working group has been formed to update the network news protocols in general, and addressing this problem is on their list of work items.

Specifics

<<EDITOR'S NOTE: Still need someone to look over the specifics but Paul Hoffman pointed this out in passing.>>

13.0 Real Time Services

Summary

The RFC's which were categorized into this group were related to IP Multicast, RTP, and Internet Stream Protocol.

<<EDITOR'S NOTE: No input on this section to date.>>

Specifics

14.0 Routing

Summary

The RFC's which were categorized into this group were Routing Information Protocol (RIP), the Open Shortest Path First (OSPF) protocol, Classless InterDomain Routing (CIDR),the Border Gateway Protocol (BGP), and the InterDomain Routing Protocol (IDRP).

After careful examination both BGP and RIP have been found Year 2000 compliant.

<<EDITOR'S NOTE: We need more here. The RIP statement is from Robert Elz's statement in Munich.>>

Specifics

BGP4

The BGP4 protocol or the BGP4 FSM do not have knowledge of absolute time. There is a notion of relative time inside BGP4, and this is visible in the fact that BGP4 has five timers.

The five timers are not a problem, since they keep relative time, as stated above. Below excerpts for proof from the RFC can be found:

* Hold timer:

The calculated value indicates the maximum number of seconds that may elapse between the receipt of successive KEEPALIVE, and/or UPDATE messages by the sender.
[...]

The suggested value for the Hold Time is 90 seconds.

* ConnectRetry timer:

The value of the initial timer shall be 60 seconds. The time shall be doubled for each consecutive retry.
[...]

The suggested value for the ConnectRetry timer is 120 seconds.

* KeepAlive timer:

KeepAlive messages are sent periodically to ensure the liveness of the connection.
[...]

The suggested value for the KeepAlive timer is 30 seconds.

* MinRouteAdvertisementInterval:

The parameter MinRouteAdvertisementInterval determines the minimum amount of time that must elapse between advertisement of routes to a particular destination from a single BGP speaker.
[...]

The suggested value for the MinRouteAdvertisementInterval is 30 seconds.

* MinASOriginationInterval:

The parameter MinASOriginationInterval determines the minimum amount of time that must elapse between successive advertisements of UPDATE messages that report changes within the advertising BGP speaker's own autonomous systems.
[...]

The suggested value for the MinASOriginationInterval is 15 seconds.

15.0 Security

Summary

The RFC's which were categorized into this group were kerberos authentication protocol, Remote Authentication Dial In User Service (RADIUS), One Time Password System (OTP), Privacy Enhanced Mail (PEM), security extensions to a variety of protocols including (but not limited to) RIPv2, HTTP, MIME, PPP, IP, Telnet and FTP. Encryption and authentication algorithms are also examined.

<<EDITOR'S NOTE: We still need input for this section. I can tell you that OTP is compliant, but we need more input.>>

Specifics

16.0 Virtual Terminal

Summary

The RFC's which were categorized into this group were Telnet and its many extensions, as well as the Secure SHell (SSH) protocol. The X window systems was not considered since it is not an IETF protocol. Official acknowledgement by the trustee's of the X window system was given that the protocol will be examined by them.

Unencrypted Telnet and TN3270 have both been found to be Year 2000 Compliant. The SSH protocols are also Year 2000 compliant.

Specifics

17.0 Security Considerations

Although this document does consider the implications of various security protocols, there is no need for additional security considerations. The effect of a potential year 2000 problem may cause some security problems, but those problems are more of specific applications rather than protocol deficiencies introduced in this document.

18.0 References

Because of the exhaustive nature of this investigation, the reader is referred to the list of published RFC's evailable from the IETF Secretariat or the RFC Editor, rather than republishing them here.

19.0 Editors Address

Philip J. Nesser II
Nesser & Nesser Consulting
13501 100th Ave N.E.
Suite 5202
Kirkland, WA 98052
(425)481-4303 (voice)
(425)482-9721 (fax)
pjnesser@nesser.com
pjnesser@martigny.ai.mit.edu

20.0 Appendices

There were several appendices in the first draft of this document, but they have not changed, and it was decided to leave them out of the final version. If the reader wished to see any of the following information they should obtain the -00 version of this draft:

```
Appendix A:  List of RFC's divided by Area
Appendix B:  Automatic Script to Implement Methodology
Appendix C:  Output of the script in Appendix B on all RFC's from 1
             through 2134
```