

## DICOM Correction Item

Correction Number CP- 659	
Log Summary: IPv6 Support	
Type of Modification Addition	Name of Standard PS 3.2, 3.8 2006
<p>Rationale for Correction:</p> <p>IP version 6 support needs to be defined to enable support of newer networks that have chosen IPv6. This change proposal makes the changes needed for support of IPv6. These changes are very small textual changes. Almost all of the DICOM standard is independent of whether the underlying network support uses IPv4 or IPv6. The change to toolkits and applications may be similarly small because the bulk of IPv6 support is an operating system feature.</p> <p>The primary impact of this change is to the internal data structures, service structures and support, configuration management, and security management whenever IP addresses are stored or processed. The commonly understood motivation for the transition to IPv6 is the increased number of IP addresses made available using the IPv6 headers. Instead of being a 32-bit field, the IP address is now a 64-bit field.</p> <p>Equally important, there are other less widely advertised motivations for the transition to IPv6:</p> <ol style="list-style-type: none"><li>The security mechanisms of IPSEC are integrated into the IPv6 mechanisms. This means that instead of using add-on mechanisms like TLS, IPv6 implementations can have integrated security mechanisms. These are generally easier to manage and maintain than the add-on mechanisms of IPv4. This CP does not incorporate the changes needed to define this.</li><li>The mechanisms for support of mobile equipment, e.g., wireless networking, is far superior in IPv6. The IPv4 mobility extensions are very inefficient, wasteful of networking facilities, hard to administer, and difficult to maintain because they were done as after the fact add-ons that could not modify the underlying IPv4 structure. Mobile devices are supported by design in IPv6.</li><li>Performance at the very high end is superior using IPv6. The header layout and management of options was designed to permit the use of custom VLSI processing in IPv6. For example, all optional header extensions are the exact same size and are identified with the same identity field. This avoids the need for byte by byte processing of IP extensions and permits intermediate nodes to skip and bypass processing of unknown options. As a result, routers have substantially higher throughput for IPv6 packets. (In practice this only matters at extremely high packet rates.)</li><li>IP Configuration management was integrated into IPv6. Instead of having a series of add-on protocols like DHCP, IPv6 has integrated address discovery procedures. These were designed and have been shown in trials to be more reliable and easier to manage than the various configuration management add-ons for IPv4. See RFC 3736 for example.</li></ol> <p>The experiences with the implementation of IPv6 support is that there are several kinds of problems that are found. These are potentially significant implementation impacts, but do not directly affect the DICOM standard. The major problems that people experience are:</p> <ol style="list-style-type: none"><li>Internal programmatic storage of network header blocks and components. There are generic networking header blocks, but most existing code is found to have made the assumption that only the IPv4 header would be stored in the header blocks. All of the code needs to be checked every place that a header block is referenced, stored, copied, or modified. The references need to be made appropriately generic and data size allocations enlarged for the generic objects. Where the headers are processed and examined, appropriate "if" clauses are needed for both the IPv4 and IPv6 structures. Where sub-components are processed, the data types must be adjusted. For example, a 32-bit integer is not sufficient to store an IPv6 IP address.</li></ol>	

Experience has shown that there are usually problems found. For example, although Microsoft's underlying Windows 2000 and XP operating systems both support IPv6, a great many applications that use these operating systems cannot use IPv6 because of one or more of the problems described above.

- b. The user interfaces, both data entry and data display, are not prepared to properly display or validate the entry of IPv6 addresses. The fixes needed are generally small, but before the product is complete there has to be a thorough examination of all the configuration, service, diagnostic, logging, documentation, and other uses where IP parameters might be used. This is time consuming.
- c. Service and administration procedures need to be adjusted. It is relatively easy to establish small islands of IPv6 routing at individual sites. It is relatively uncommon to find IPv6 backbone service between sites. There is a "6on4" protocol that is presently used to establish bridges of connectivity between IPv6 islands. The service and administrative staff needs to actively maintain the local connectivity tables to establish 6on4 bridges as necessary, and to update these tables when backbone connectivity is changed. This is just one of several IPv6 related activities that will be needed from service and administrative staff during the many years when IPv4 and IPv6 will co-exist. This kind of administrative activity does not affect the DICOM standard itself, but does affect the support tools and training needed when DICOM applications begin using IPv6.

Sections of documents affected

Part 2, sections A.4.3, B.4.3, C.4.3, D.4.3, E.4.3, F.4.3

Part 8, section 9.1.1

Correction Wording:

*Add to PS 3.2 Section A.4.3.3 IPv6 Support*

#### A.4.3.3 IPv4 and IPv6 Support

The support for specific IPv4 and IPv6 features and associated optional IPv6 security and configuration facilities shall be documented.

*Amend PS 3.2 Section A.7.1 as follows:*

An implementation shall declare which level of security features it supports, including such things as:

- a. The conditions under which the implementation preserves the integrity of Digital Signatures (e.g. is the implementation bit-preserving).
- b. The conditions under which the implementation verifies incoming Digital Signatures.
- c. The conditions under which the implementation replaces Digital Signatures.
- d. **IPv6 Security capabilities**

*Add to PS 3.2 Section X.4.3.3 to each of the examples in annexes B, C, D, E, F*

#### **B.4.3.3 IPv4 and IPv6 Support**

This product only supports IPv4 connections.

#### **C.4.3.3 IPv4 and IPv6 Support**

This product supports both IPv4 and IPv6. It does not utilize any of the optional configuration identification or security features of IPv6.

#### **D.4.3.3 IPv4 and IPv6 Support**

This product supports both IPv4 and IPv6. It does not utilize any of the optional configuration identification or security features of IPv6.

#### **E.4.3.3 IPv4 and IPv6 Support**

This product supports both IPv4 and IPv6. It does not utilize any of the optional configuration identification or security features of IPv6.

#### **F.4.3.3 IPv4 and IPv6 Support**

This product supports both IPv4 and IPv6. It does not utilize any of the optional configuration identification or security features of IPv6.

*Add to PS 3.8 Section 2 Normative References the IPv6 RFCs to the list of RFC's*

## **2.2 Other Documents**

...

RFC 950, Internet Subnetting

**RFC 1881, IPv6 Address Allocation Management**

**RFC 2460, Internet Protocol, Version 6 (IPv6) Specification**

*Amend PS 3.8 Section 9.1.1 as follows:*

The Services provided by the TCP Transport Services are not formally documented. This section, therefore, makes use of "commonly" used terms in a number of TCP Programming Interface Implementations (e.g. Sockets). However, the following RFCs shall be required for TCP/IP support. **They specify the support needed for IPv4.**

- a) RFC 793, Transmission Control Program - DARPA Internet Protocol Specification
- b) RFC 791, Internet Protocol - DARPA Internet Protocol Specification
- c) RFC 792, Internet Control Message Protocol - DARPA Internet Program Protocol Specification
- d) RFC 950, Internet Subnetting

**In addition, devices that support IPv6 shall comply with:**

- a) **RFC 1881, IPv6 Address Allocation Management**
- b) **RFC 2460, Internet Protocol, Version 6 (IPv6) Specification**

**Note: There are many other RFC's that may also apply to a particular implementation depending upon specific selections of hardware and software features.**