DICOM Correction Proposal

F Network Address Management Profiles

F.1 BASIC NETWORK ADDRESS MANAGEMENT PROFILE

The Basic Network Address Management Profile utilizes DHCP to provide services to assign and manage IP parameters for machines remotely. The DHCP server is manually configured to establish the rules for assigning IP addresses to machines. The rules may be explicit machine by machine assignments and may be assignment of a block of IP addresses to be assigned dynamically as machines are attached and removed from the network. The DHCP client can obtain its IP address and a variety of related parameters such as NTP server address from the DHCP server during startup. The DHCP server may dynamically update the DNS server with new relationships between IP addresses and DNS hostnames.

The DNS Client can obtain the IP number for another host by giving the DNS hostname to a DNS Server and receive the IP number in response. This transaction may be used in other profiles or in implementations that do not conform to the Basic Network Address Management Profile.

The Basic Network Address Management Profile applies to the actors DHCP Server, DHCP Client, DNS Server, and DNS Client. The mandatory and optional transactions are described in the table and sections below.
Table F.1-1 Basic Network Address Management Profile

<table>
<thead>
<tr>
<th>Actor</th>
<th>Transaction</th>
<th>Optionality</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server</td>
<td>Configure DHCP Server</td>
<td>M</td>
<td>F.1.2</td>
</tr>
<tr>
<td></td>
<td>Find and Use DHCP Server</td>
<td>M</td>
<td>F.1.3</td>
</tr>
<tr>
<td></td>
<td>Maintain Lease</td>
<td>M</td>
<td>F.1.4</td>
</tr>
<tr>
<td></td>
<td>Resolve Hostname</td>
<td>M</td>
<td>F.1.1</td>
</tr>
<tr>
<td></td>
<td>DDNS Coordination</td>
<td>O</td>
<td>F.1.5</td>
</tr>
<tr>
<td>DHCP Client</td>
<td>Find and Use DHCP Server</td>
<td>M</td>
<td>F.1.3</td>
</tr>
<tr>
<td></td>
<td>Maintain Lease</td>
<td>M</td>
<td>F.1.4</td>
</tr>
<tr>
<td>DNS Server</td>
<td>DDNS Coordination</td>
<td>O</td>
<td>F.1.5</td>
</tr>
<tr>
<td></td>
<td>Resolve Hostname</td>
<td>M</td>
<td>F.1.1</td>
</tr>
<tr>
<td>DNS Client</td>
<td>Resolve Hostname</td>
<td>M</td>
<td>F.1.1</td>
</tr>
</tbody>
</table>

F.1.1 Resolve Hostname

F.1.1.1 Scope
The DNS Client can obtain the IP number for a host by giving the DNS hostname to a DNS Server and receive the IP number in response.

F.1.1.2 Use Case Roles

Figure F.1-1. Resolve Hostname

Actor: DNS Client
Role: Needs IP address, has the DNS Hostname
Actor: DNS Server
Role: Provides current IP address when given the DNS Hostname

F.1.1.3 Referenced Standards
The standards and their relationships for the family of DNS protocols are shown in Figure F.1-2. The details of transactions, transaction diagrams, etc. are contained within the referenced RFC's.
F.1.1.4 DNS Security Considerations (Informative)

The issue of security is under active development by the Internet Engineering Task Force and its various working groups. The security related RFCs and drafts are identified in Figure F.1-2. Some of these are completed. Others are still in the draft stage. The Basic Network Address Management Profile does not include specific requirements for support of DNS security extensions by the DNS Client.

The Basic Network Address Management profile should not be used outside a secured environment. At a minimum there should be:

a. Firewall or router protections to ensure that only approved external hosts are used for DNS services.

b. Agreements for VPN and other access should require that DNS clients use only approved DNS servers over the VPN.

Other network security procedures such as automated intrusion detection may be appropriate in some environments. Security features beyond this minimum should be established by the local security policy and are beyond the scope of DICOM.

The purpose of the selected security is to limit the scope of the threat to insider attacks. The DNS system discloses only hostnames and IP addresses, so there is little concern about eavesdropping. The protections are to limit the exposure to denial of service attacks by counterfeit servers or clients.

F.1.1.5 DNS Implementation Considerations (Informative)

Client caches may cause confusion during updates. Many DNS clients check for DNS updates very infrequently and might not reflect DNS changes for hours or days. Manual steps may be needed to trigger immediate updates. Details for controls of cache and update vary for different DNS clients and DNS servers, but DNS caching and update propagation delays are significant factors and implementations have mechanisms to manage these issues.
DNS Server failure management should be considered. Redundant servers and fallback host files are examples of possible error management tools.

F.1.1.6 Support For Service Discovery
The DNS server may provide additional optional information in support of configuration management. See Section H.2 for the specification of this information and additional RFC’s to be supported.

F.1.2 Configure DHCP server
F.1.2.1 Scope
The DHCP server shall be configurable by site administration so that

a. DHCP clients can be added and removed.

b. DHCP clients configurations can be modified to set values for attributes used in later transactions.

c. pre-allocation of fixed IP addresses for DHCP clients is supported

This standard does not specify how this configuration is to be performed.

Note
Most DHCP servers support the pre-allocation of fixed IP addresses to simplify the transition process for legacy systems. This permits a particular device to switch to DHCP while retaining the previously assigned IP address. This enables the use of a central site management of IP addresses without breaking compatibility with older systems that require fixed IP addresses.

F.1.2.2 Use Case Roles

Figure F.1-3. Configure DHCP Server

Actor: DHCP Server
Role: Maintains internal configuration files.

Actor: Site Administrator
Role: Updates configuration information to add, modify, and remove descriptions of clients and servers.

Actor: Service Staff
Role: Provides initial configuration requirements for many devices when installing a new network, and for individual devices when installing or modifying a single device.

F.1.2.3 Referenced Standards
None
F.1.3 Find and Use DHCP Server

F.1.3.1 Scope
This is the support for the normal startup process. The DHCP client system boots up, and very early in the booting process it finds DHCP servers, selects one of the DHCP servers to be its server, queries that server to obtain a variety of information, and continues DHCP client self-configuration using the results of that query. DHCP servers may optionally provide a variety of information, such as server locations, normal routes. This transaction identifies what information shall be provided by a compliant DHCP server, and identifies what information shall be requested by a compliant DHCP client. A compliant DHCP server in not required to provide this optional information.

F.1.3.2 Use Case Roles

![Diagram of Find and Use DHCP Server]

Figure F.1-4. Find and Use DHCP Server

- **Actor:** DHCP Server
  - **Role:** Responds to DHCP acquisition queries. Multiple actors may exist. The DHCP client will select one.
- **Actor:** DHCP client
  - **Role:** Queries for DHCP Servers. Selects one responding server.

F.1.3.3 Referenced Standards
- RFC2131  DHCP Protocol
- RFC2132  DHCP Options
- RFC2563  Auto Configuration control

F.1.3.4 Interaction Diagram
The DHCP client shall comply with RFC2131 (DHCP Protocol), RFC2132 (DHCP Options), RFC2563 (Auto Configuration Control), and their referenced RFCs.

The DHCP client shall query for available DHCP servers. It shall select the DHCP server to use.

The DHCP client shall query for an IP assignment. The DHCP Server shall determine the IP parameters in accordance with the current DHCP configuration, establish a lease for these parameters, and respond with this information. (See below for lease maintenance and expiration.) The DHCP client shall apply these parameters to the TCP/IP stack. The DHCP client shall establish internal lease maintenance activities.

The DHCP client shall query for the optional information listed in Table F.1-2 when required by additional profiles used by the client system. If the DHCP server does not provide this information, the default values shall be used by the DHCP client.

<table>
<thead>
<tr>
<th>DHCP Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP</td>
<td>List of NTP servers</td>
<td>Empty list</td>
</tr>
<tr>
<td>DNS</td>
<td>List of DNS servers</td>
<td>Empty list</td>
</tr>
<tr>
<td>Router</td>
<td>Default router</td>
<td>Empty list</td>
</tr>
<tr>
<td>Static routes</td>
<td></td>
<td>Nil</td>
</tr>
<tr>
<td>Hostname</td>
<td></td>
<td>Requested machine name</td>
</tr>
<tr>
<td>Domain name</td>
<td></td>
<td>Nil</td>
</tr>
<tr>
<td>Subnet mask</td>
<td></td>
<td>Derived from network value</td>
</tr>
<tr>
<td>Broadcast address</td>
<td></td>
<td>Derived from network value</td>
</tr>
<tr>
<td>Default router</td>
<td></td>
<td>Nil</td>
</tr>
<tr>
<td>Time offset</td>
<td></td>
<td>Site configurable</td>
</tr>
<tr>
<td>MTU</td>
<td></td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Auto-IP permission</td>
<td></td>
<td>From NVRAM</td>
</tr>
</tbody>
</table>

The DHCP client shall make this information available for other actors within the DHCP client machine.

F.1.4 Maintain Lease

F.1.4.1 Scope

The DHCP client normally maintains the IP lease in compliance with the RFCs. Sometimes the server will not renew the lease. Non-renewal is usually part of network service operations. The loss of the IP lease requires connections using that IP address to cease.

F.1.4.2 Use Case Roles
F.1.4.3 Referenced Standards

RFC2131  DHCP Protocol
RFC2132  DHCP Options

F.1.4.4 Normal Interaction

The DHCP client shall maintain a lease on the IP address in accordance with the DHCP protocol as specified in RFC2131 and RFC2132. There is a possibility that the DHCP Server may fail, or may choose not to renew the lease.

In the event that the DHCP lease expires without being renewed, any still active DICOM connections may be aborted (AP-Abort).

Note There is usually a period (typically between several minutes and several days) between the request for lease extension and actual expiration of the lease. The application might take advantage of this to perform a graceful association release rather than the abrupt shutdown of an AP-Abort.

F.1.5 DDNS Coordination

F.1.5.1 Scope

DHCP servers may coordinate their IP and hostname assignments with a DNS server. This permits dynamic assignment of IP addresses without interfering with access to DHCP Clients by other systems. The other systems utilize the agreed hostname (which DHCP can manage and provide to the client) and obtain the current IP address by means of DNS lookup.

Dynamic DNS (DDNS) provides for capability to the client to update DNS records hosted on the DNS server. The client can be a DHCP server, Active Directory or LDAP servers, or even an application announcing the systems IP address and optionally any available services.

A DHCP Server is in compliance complies with this optional part of the Basic Network Address Management Profile profile if it maintains and updates the relevant DNS server so as to maintain entry the proper hostname and IP relationships in the DNS database when they change.
Figure F.1-7. DDNS Coordination

Actor: DHCP Server
Role: Responded to DHCP acquisition queries and assigned IP address to client.

Actor: DNS Server
Role: Maintains the DNS services for the network.

F.1.5.3 Referenced Standards
RFC2136 Dynamic Updates in the Domain Name System

F.1.5.4 Basic Course of Events

After the DHCP server has assigned an IP address to a DHCP client, the DHCP server uses DDNS to inform the DNS server that the hostname associated with the DHCP client has been given the assigned IP address. The DNS server updates the DNS database and links the IP address to the hostname, so that subsequent DNS queries for this hostname are directed to the assigned IP address. When the lease for the assigned IP address expires without renewal, the DHCP server informs the DNS server and it updates the DNS database, that the IP address and hostname are no longer valid. The DNS server removes them from the DNS database.

F.1.6 DHCP Security Considerations (Informative)

The Basic Network Address Management Profile has two areas of security concerns:

a. Protection against denial of service attacks against the DHCP client/server traffic.
b. Protection against denial of service attacks against the DHCP server to DDNS server update process.

The Basic Network Address Management Profile should not be used outside a secured environment. At a minimum there should be:

a. Firewall and or router protections to ensure that only approved hosts are used for DHCP and DNS services.
b. Agreements for VPN and other access should require that DNS clients on the hospital network use only approved DHCP or DNS servers over the VPN.

Other network security procedures such as automated intrusion detection may be appropriate in some environments. Security features beyond this minimum should be established by the local security policy and are beyond the scope of DICOM.

The purpose of the selected security is to limit the scope of the threat to insider attacks. The DHCP and DNS systems disclose only hostnames and IP addresses, so there is little concern about eavesdropping. The protections are to limit the exposure to denial of service attacks by counterfeit servers or clients. The specific DNS security extensions are described in Section F.1.1.4. This profile does not utilize the DHCP security extensions because they provide very limited added security and the attacks are insider denial of service attacks. Intrusion detection and other network level protection mechanisms are the most effective next level of protections for the DHCP process.

The DNS update is optional in this profile to accommodate the possibility that the DHCP server and DNS server cannot reach a mutually acceptable security process. Support of this option may require support of
the DNS security protocols that are in the process of development. See Section F.1.1.4 for a discussion of the DNS security profile standards and drafts.

F.1.7 DHCP Implementation Considerations (Informative)

The DHCP configuration file can be a very useful form of documentation for the local network hardware configuration. It can be prepared in advance for new installations and updated as clients are added. Including information for all machines, including those that do not utilize DHCP, avoids accidental IP address conflicts and similar errors.

Most DHCP servers have a configuration capability that permits control of the IP address and other information provided to the client. These controls can pre-allocate a specific IP address, etc. to a machine based on the requested machine name or MAC address. These pre-allocated IP addresses then ensure that these specific machines are always assigned the same IP address. Legacy systems that do not utilize DNS can continue to use fixed tables with IP addresses when the DHCP server has pre-allocated the IP addresses for those services.

F.1.8 Conformance

The Conformance Statement for an application that supports this profile shall specify whether it supports DHCP as DHCP Client or DHCP Server.

If the application supports this profile as a DHCP Client, the Conformance Statement shall specify how the DHCP Server is discovered (see F.1.3).

The Conformance Statement shall state whether the application supports DNSSEC (RFCs 4033, 4034, 4035). If DNSSEC is supported, either the options supported shall be stated or a reference provided to the DNSSEC support for this product.

The Conformance Statement for an LDAP Client shall describe its use of LDAP to configure the local AE titles. Any conformance to the Update LDAP Server option shall be specified, together with the values for all component object attributes in the update sent to the LDAP Server. Any use of LDAP to configure the remote device addresses and capabilities shall be described. The LDAP queries used to obtain remote device component object attributes shall be specified.

Note—In particular, use of LDAP to obtain the AE Title, TCP port, and IP address for specific system actors (e.g., an Image Archive, or a Performed Procedure Step Manager) should be detailed, as well as how the LDAP information for remote devices is selected for operational use.