Digital Imaging and Communications in Medicine (DICOM)

Supplement 67 – Configuration Management

Prepared by:
DICOM Standards Committee, Working Group 6

1300 N. 17th Street

Rosslyn, Virginia 22209 USA

VERSION: Final Text

25 March 2004

Table of Contents

Foreword

The configuration profiles define the use of external (non-DICOM) protocols to perform functions performed during of configuration and operation DICOM networks and network applications. They are defined in response to a white paper giving potential use cases for configuration management. The profiles in this supplement correspond to the use cases that were given the highest importance.

This draft Supplement to the DICOM Standard was developed according to DICOM Committee Procedures. This supplement modifies following parts:

PS 3.1	-	Introduction and Overview
PS 3.2	-	Conformance
PS 3.4	-	Service Class Specifications
PS 3.6	-	Data Dictionary
PS 3.15	-	Security Profiles

Scope and Field

The profiles address the use cases for:

a. Automatic self-configuration on power up
b. Installation of new DICOM equipment
c. Network and device reconfiguration
d. Multiple device time synchronization

The notation of profile, actor, and transaction is adapted from the IHE Technical Framework. The IHE Technical Frameworks can be found at http://www.rsna.org/ihe. It has proved useful as a way to document the specific utilization of protocols that are externally defined. The configuration management tasks are being performed by making explicit requirements that specific external protocols be used with specific selections of options and parameters. The external protocols are only partially described. The descriptions are only to the level needed to clarify the selection of options and parameters. The normative requirements for the external protocols remain in the external protocol documents (usually RFCs from the IETF).

The first annex for Configuration Management is structured so that the transactions for each profile are described together with the profile. This includes all normative text and references to external standards. The second annex contains informative text. It describes the use cases and typical use scenarios for the transactions defined in the first annex.

Add scope of System Management Profiles to PS3.1 Section 6.15:

PS3.15: SECURITY AND SYSTEM MANAGEMENT PROFILES

PS3.15 of the DICOM Standard specifies Security **and System Management** Profiles to which implementations may claim conformance. Security **and System Management** Profiles are defined by referencing externally developed ~~security~~ standard **protocols**, such as **DHCP, LDAP,** TLS, and ISCL**, with attention to their use in a system that uses DICOM Standard protocols for information interchange. Security protocols may** ~~which~~, in turn, need access control …

In the Foreword to each Part of Standard, change the title of PS3.15:

PS 3.15: Security **and System Management** Profiles

Replace PS3.2 Section A.4.3.2 with the following:

A.4.3.2 Additional Protocols

Additional protocols such as used for configuration management are listed here. Any conformance to specific System Management Profiles defined in PS3.15 shall be listed per the following table.

Table A.4.3-1
System Management Profiles Table

Profile Name	Actor	Protocols Used	Optional Transactions	Security Support
Profile (1)	P Client	Protocol_1, Protocol_2	N/A	
Profile (x)	X Client	Protocol_2, Protocol_3	Protocol_3 Option_A supported	

If the implementation conforms to the Basic Network Address Management Profile as a DHCP Client actor (see PS3.15), the use of DHCP to configure the local IP address and hostname shall be described.

Note: The hostname is an alias for the IP address, and has no semantic relationship to AE titles. It is solely a convenience for configuration description.

If the implementation conforms to the Basic Network Address Management Profile as a DNS Client actor (see PS3.15), the use of DNS to obtain IP addresses from hostname information shall be described.

If the implementation conforms to the Basic Time Synchronization profile as an NTP Client or SNTP Client, the available NTP configuration alternatives shall be described. If the implementation conforms to the Basic Time Synchronization Profile as an NTP Server, the available server configuration alternatives shall be described. Any device specific requirements for accuracy or maximum allowable synchronization error shall be described.

Replace PS3.2 Section A.4.4.1 with the following:

A.4.4.1 AE Title/Presentation Address Mapping

An important installation issue is the translation from AE title to Presentation Address. How this is to be performed shall be described in this section.

Note: There does not necessarily have to be a one to one relationship between AE titles and Application Entities. If so, this should be made clear in the tables.

A.4.4.1.1 Local AE Titles

The local AE title mapping and configuration shall be specified. The following table shall be used:

Table A.4.4 - 1
AE Title configuration table

Application Entity	Default AE Title	Default TCP/IP Port
AE (1)	Name	Specify
AE (2)	Name	Specify
AE (x)		

If the implementation conforms to the Application Configuration Management Profile as an LDAP Client actor (see PS3.15), any use of LDAP to configure the local AE titles shall be described. 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.

A.4.4.1.2 Remote AE Title/Presentation Address Mapping

Configuration of address information for remote Application Entities shall be specified here.

A.4.4.1.2.1 Remote SCPs

Configuration of the remote AE Title, port number, hostnames, IP addresses and capabilities shall be specified. If applicable, multiple remote SCP's can be specified.

If the implementation conforms to the Application Configuration Management Profile as an LDAP Client actor (see PS3.15), 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.

Add to Part 6, Table A-1

UID Value	**UID NAME**	**UID TYPE**	**Part**
1.2.840.10008.15.0.3.1	dicomDeviceName	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.2	dicomDescription	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.3	dicomManufacturer	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.4	dicomManufacturerModelName	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.5	dicomSoftwareVersion	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.6	dicomVendorData	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.7	dicomAETitle	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.8	dicomNetworkConnectionReference	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.9	dicomApplicationCluster	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.10	dicomAssociationInitiator	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.11	dicomAssociationAcceptor	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.12	dicomHostname	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.13	dicomPort	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.14	dicomSOPClass	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.15	dicomTransferRole	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.16	dicomTransferSyntax	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.17	dicomPrimaryDeviceType	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.18	dicomRelatedDeviceReference	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.19	dicomPreferredCalledAETitle	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.20	dicomTLSCyphersuite	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.21	dicomAuthorizedNodeCertificateReference	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.22	dicomThisNodeCertificateReference	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.23	dicomInstalled	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.24	dicomStationName	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.25	dicomDeviceSerialNumber	LDAP OID	PS 3.15

1.2.840.10008.15.0.3.26	dicomInstitutionName	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.27	dicomInstitutionAddress	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.28	dicomInstitutionDepartmentName	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.29	dicomIssuerOfPatientID	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.30	dicomPreferredCallingAETitle	LDAP OID	PS 3.15
1.2.840.10008.15.0.3.31	dicomSupportedCharacterSet	LDAP OID	PS 3.15
1.2.840.10008.15.0.4.1	dicomConfigurationRoot	LDAP OID	PS 3.15
1.2.840.10008.15.0.4.2	dicomDevicesRoot	LDAP OID	PS 3.15
1.2.840.10008.15.0.4.3	dicomUniqueAETitlesRegistryRoot	LDAP OID	PS 3.15
1.2.840.10008.15.0.4.4	dicomDevice	LDAP OID	PS 3.15
1.2.840.10008.15.0.4.5	dicomNetworkAE	LDAP OID	PS 3.15
1.2.840.10008.15.0.4.6	dicomNetworkConnection	LDAP OID	PS 3.15
1.2.840.10008.15.0.4.7	dicomUniqueAETitle	LDAP OID	PS 3.15
1.2.840.10008.15.0.4.8	dicomTransferCapability	LDAP OID	PS 3.15

Change the title of PS3.15:

Digital Imaging and Communications in Medicine (DICOM)

Part 15: Security and System Management Profiles

Change Scope and Field of PS3.15 Section 1:

1 Scope and field of application

This part of the DICOM Standard specifies Security **and System Management** Profiles to which implementations may claim conformance. **Security and System Management Profiles are defined by referencing externally developed standard protocols, such as TLS, ISCL, DHCP, and LDAP, with attention to their use in a system that uses DICOM Standard protocols for information interchange.**

1.1 SECURITY POLICIES AND MECHANISMS

The DICOM standard does not address issues of security policies, though clearly adherence to appropriate security policies is necessary for any level of security. The standard only provides …

Add PS 3.15 Section 1.2

1.2 SYSTEM MANAGEMENT PROFILES

The System Management Profiles specified in this Part are designed to support automation of the configuration management processes necessary to operate a system that uses DICOM Standard protocols for information interchange.

This Part assumes that the Application Entities may operate in a variety of network environments of differing complexity. These environments may range from a few units operating on an isolated network, to a department-level network with some limited centralized network support services, to an enterprise-level network with significant network management services. Note that the System Management Profiles are generally addressed to the implementation, not to Application Entities. The same Profiles need to be supported by the different applications on the network.

Add normative references to PS3.15 Section 2:

2 Normative references

The following standards contain provisions that, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibilities of applying the most recent editions of the standards indicated below.

…

RFC 1035	**Domain Name System (DNS)**
RFC 1305	**Network Time Protocol (Version 3) Specification, Implementation**
RFC 2030	**Simple Network Time Protocol (SNTP) Version 4**
RFC 2131	**Dynamic Host Configuration Protocol**
RFC 2132	**Dynamic Host Configuration Protocol Options**
RFC 2136	**Dynamic Updates in the Domain Name System (DNS UPDATE)**
RFC 2181	**Clarifications to the DNS Specification**
RFC 2219	**Use of DNS Aliases for Network Services**
RFC 2251	**Lightweight Directory Access Protocol (v3)**
RFC 2563	**DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients**
RFC 2782	**A DNS RR for specifying the location of services (DNS SRV)**
RFC 2849	**The LDAP Data Interchange Format (LDIF)**

…

Note: Normative RFC's are frequently updated by issuance of subsequent RFC's. The original older RFC is not modified to include references to the newer RFC.

Add abbreviations to PS3.15 Section 4:

4 Symbols and abbreviations

The following symbols and abbreviations are used in this Part of the Standard.

…

CN	**Common Name**
DHCP	**Dynamic Host Configuration Protocol**
DN	**Distinguished Name**
DNS	**Domain Name System**
DDNS	**Dynamic Domain Name System**

IETF	**Internet Engineering Task Force**
LDAP	**Lightweight Directory Access Protocol**
LDIF	**LDAP Interchange Format**
MTU	**Maximum Transmission Unit**
NTP	**Network Time Protocol**
OID	**Object Identifier (analogous to UID)**
RDN	**Relative Distinguished Name**
RFC	**Request For Comment (used for standards issued by the IETF)**
RR	**Resource Record (when used in the context of DNS)**
SNTP	**Simple Network Time Protocol**
SSH	**Secure Shell**
UTC	**Universal Coordinated Time**

Add System Management Profiles to PS3.15 Section 6:

6 Security and System Management Profile Outlines

An implementation may claim conformance to any of the Security **and System Management** Profiles individually. It may also claim conformance to more than one Security **and System Management** Profile. It shall indicate in its Conformance Statement how it chooses which profiles to use for any given transaction.

6.1 SECURE USE PROFILES

…

6.5 NETWORK ADDRESS MANAGEMENT PROFILES

An implementation may claim conformance to one or more Network Address Management Profiles. Such profiles outline the use of non-DICOM network protocols to obtain the network addresses for the implementation.

Network Address Management Profiles are specified in Annex V.

6.6 TIME SYNCHRONIZATION PROFILES

An implementation may claim conformance to one or more Time Synchronization Profiles. Such profiles outline the use of non-DICOM protocols to set the current time for the implementation.

Time Synchronization Profiles are specified in Annex W.

6.7 APPLICATION CONFIGURATION MANAGEMENT PROFILES

An implementation may claim conformance to one or more Application Configuration Management Profiles. Such profiles outline the use of non-DICOM network protocols to obtain the descriptions, addresses and capabilities of other devices with which the implementation may communicate using the DICOM Protocol. They also specify the use of those non-DICOM protocols for the

implementation to publish or announce its description, addresses and capabilities. They also specify how implementation specific configuration information can be obtained by devices.

Application Configuration Management Profiles are specified in Annex X.

Add to Part 15

7 Configuration Profiles

Configuration management support is implemented by means of protocols defined in standards other than the DICOM standard. These protocols are described here in terms of actors, transactions, and profiles.

Actors are analogous to the Application Entities used within the DICOM profile. An actor is a collection of hardware and software processes that perform a particular role. When a device provides or uses a service it will include an actor to handle the relevant network activity. DICOM Configuration actors may co-exist with other Application Entities on a device. Some DICOM Configuration actors exist as parts of general use IT equipment. Like the Application Entity, specification of an Actor does not imply anything about the details of the actual implementation.

The actor interactions are defined in terms of Transactions. Each transaction is given a name. The transaction may in turn comprise a variety of activity. All transactions are defined in terms of actors that are communicating. The relationships between actors in a transaction may be more complex than the simple SCU and SCP roles in DICOM activities. When the transaction includes interactions with a person, the transactions may be implemented by user interfaces, removable media. and other mechanisms. The person is described in terms of being an actor from the perspective of the transaction use case model. More typically the transactions are a series of network activities that perform a specific operation.

A transaction includes both mandatory and optional components. An Actor that is implementing a transaction is required to implement all of the mandatory components.

Some transactions include human actors in the transaction definition. These actors are not defined as actors elsewhere, nor are they included in profile descriptions. They exist to specify that some sort of mechanism must be provided to permit these people to interact with the computer actor. Other details of how that user interface is provided are not specified by this standard. For an example, see the definition of the Configure DHCP transaction.

Conformance is further managed by means of Profiles. A Profile is defined in terms of what transactions are required for an actor and what transactions are optional. An implementation of a specific actor is documented by specifying what optional transactions and transaction components have been implemented. An implementation that omits any required transactions or components cannot claim to be an implementation of that Actor.

For example, in the Network Address Management Profile the DHCP Server is required to perform the three Transactions to configure the DHCP server, find and use DHCP servers, and maintain the DHCP leases. It may also support the transaction to update the DNS server by means of DDNS coordination.

A Profile includes definitions for more than one Actor. It specifies the transactions for all of the actors that cooperate to perform a function. For example, the Network Address Management Profile covers the DHCP Server actor, the DHCP client Actor, and the DNS Server actor. There must be at least one DHCP Server and one DHCP Client for the system to be useful. The DNS Server itself is optional because the DHCP Server need not implement the DDNS Coordination transaction. If the DNS Server is part of the system, the DDNS coordination is required and the DHCP Server will be expected to participate in the DDNS Coordination transaction.

Note: There may be a DNS server present on the same network as a DHCP Server, but if it is not providing the DNS Server actor from this profile it is not part of the DICOM Configuration activities.

The profiles, actors, and transactions are summarized in the following sections. The detailed description of actor and transactions for each specific profile are described in annexes for each profile. The transactions are documented in terms of parameters and terms from their original standards document, e.g. an RFC for Internet protocols. The full details of the transaction are not described in the annex, only particular details that are relevant to the DICOM application of that transaction. The complete details for these external protocols are documented in the relevant standards documents for the external protocols. Compliance with the requirements of a particular profile shall include compliance with these external protocol documents.

7.1 ACTORS

DHCP Server

The DHCP Server is a computer/software feature that is provided with a network configuration description, and that provides startup configuration services in accordance with the DHCP protocol.

DHCP Client

The DHCP Client is a software feature that is used to obtain TCP/IP parameters during the startup of a computer. It continues operation to maintain validity of these parameters.

DNS Server

The DNS server is a computer/software feature that provides IP related information in response to queries from clients utilizing the DNS protocol. It is a part of a federated database facility that maintains the current database relating machine names to IP address information. The DNS server may also be isolated from the worldwide federated database and provide only local DNS services.

DNS Client

The DNS client as a computer/software feature that utilizes the DNS protocols to obtain IP information when given hostnames. The hostnames may be in configuration files or other files instead of explicit IP addresses. The hostnames are converted into IP addresses dynamically when necessary. The DNS client uses a DNS server to provide the necessary information.

NTP Server

The NTP server is a computer/software feature that provides time services in accordance with the NTP or SNTP protocol.

NTP Client

The NTP client is software that obtains time information from an NTP server and maintains the client time in synchronization with the time signals from the NTP server.

SNTP Client

The SNTP client is software that obtains time information from an NTP server and maintains the client time in approximate synchronization with time signals from the NTP server. The SNTP client synchronization is not maintained with the accuracy or precision that NTP provides.

LDAP Server

The LDAP server is a computer/ software feature that maintains an internal database of various directory information. Some of this directory information corresponds to DICOM Configuration schema. The LDAP server provides network access to read and update the directory information. The LDAP server provides a mechanism for external loading, unloading, and backup of directory information. The LDAP server may be part of a federated network of servers that provides a coordinated view of a federated directory database in accordance with the rules of the LDAP protocols.

LDAP Client

The LDAP client utilizes the LDAP protocol to make queries to an LDAP server. The LDAP server maintains a database and responds to these queries based on the contents of this database.

7.2 TRANSACTIONS

The following transactions are used to provide communications between actors in accordance with one or more of the DICOM Configuration protocols.

Configure DHCP Server

This transaction changes the configuration on a DHCP server to reflect additions, deletions, and changes to the IP parameters that have been established for this network.

Find and Use DHCP Server

This transaction is a sequence of network messages that comply with the rules of the DHCP protocol. It allows a DHCP client to find available DHCP servers and select the server appropriate for that client. This transaction obtains the mandatory IP parameter information from the DHCP server and obtains additional optional parameters from the DHCP server.

Configure Client

The service staff uses this transaction to set the initial configuration for a client.

Maintain Lease

This transaction deals with how the DHCP client should behave when its IP lease is not renewed.

DDNS Coordination

This transaction documents whether the DHCP server is coordinating with a DNS server so that access to the DHCP client can be maintained using the hostname assigned to the DHCP client.

Resolve Hostname

This transaction obtains the IP address for a computer when given a hostname.

Maintain Time

These transactions are the activities needed for an NTP or SNTP client to maintain time synchronization with a master time service.

Find NTP Server

This transaction is the autodiscovery procedure defined for NTP. This may use either a broadcast method or a DHCP supported method.

Find LDAP Server

In this transaction the DNS server is queried to obtain the IP address, port, and name of the LDAP server.

Query LDAP Server

In this transaction the LDAP server is queried regarding contents of the LDAP database.

Client Update LDAP Server

This transaction updates the configuration database using LDAP update instructions from the client being configured.

Maintain LDAP Server

This transaction updates the configuration database using local services of the LDAP server.

Figure 7.1-1 shows the actors and their transactions. The usual device will have an NTP Client, DHCP Client, and LDAP client in addition to the other applications actors. The transactions “Configure DHCP Server”, “Configure Client”, and “Maintain LDAP Server” are not shown because these transactions are between a software actor and a human actor. DICOM does not specify the means or user interface. It only requires that certain capabilities be supported.

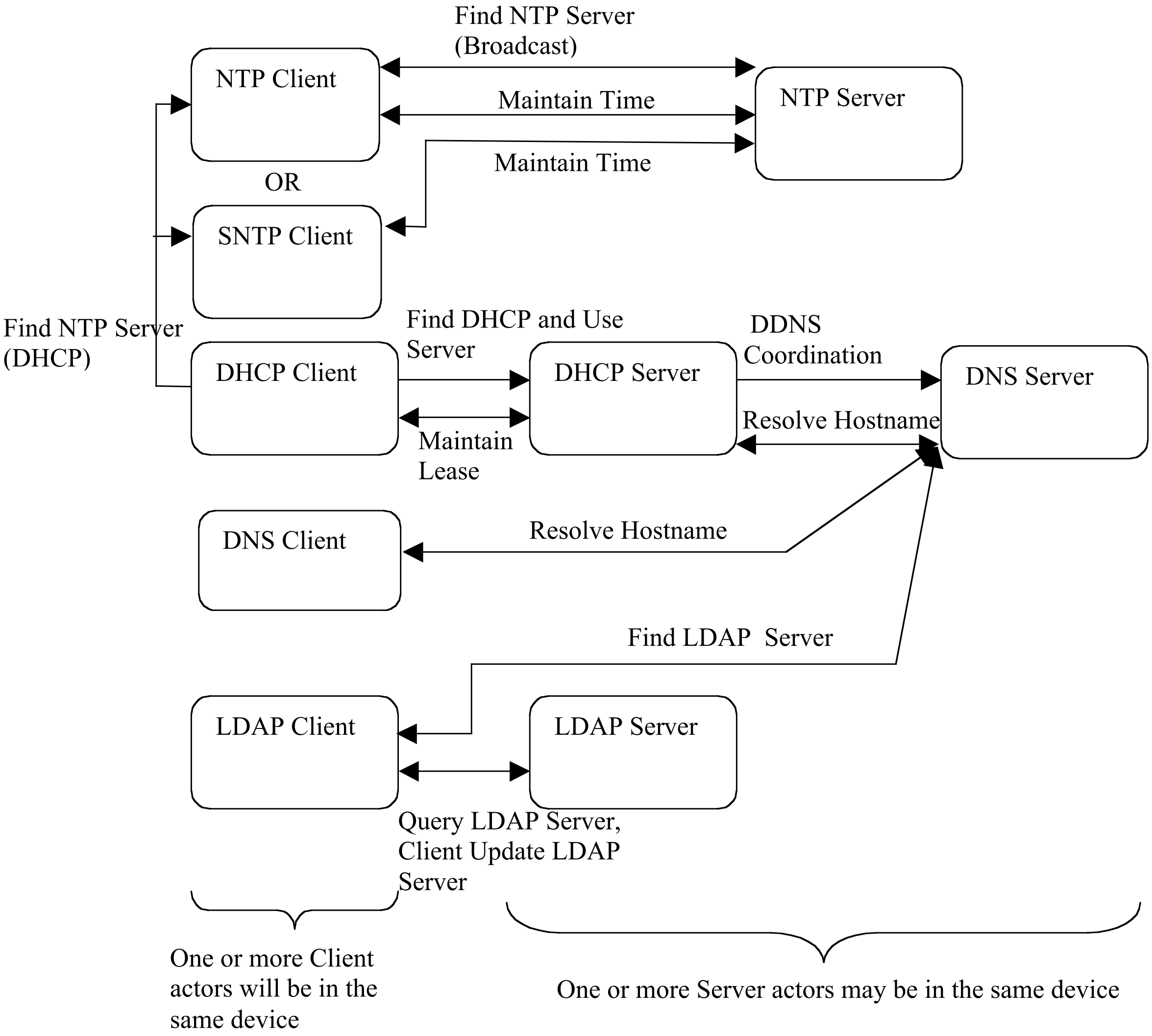

Figure 7.1-1 Transactions and Actors

Add Annex V for Configuration Profiles to Part 15

Annex V Network Address Management Profiles

V.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 V.1-1- Basic Network Address Management Profile

Actor	Transaction	Optionality	Section
DHCP Server	Configure DHCP Server	M	V.1.2
	Find and Use DHCP Server	M	V.1.3
	Maintain Lease	M	V.1.4
	Resolve Hostname	M	V.1.1
	DDNS Coordination	O	V.1.5
DHCP Client	Find and Use DHCP Server	M	V.1.3
	Maintain Lease	M	V.1.4
DNS Server	DDNS Coordination	O	V.1.5
	Resolve Hostname	M	V.1.1
DNS Client	Resolve Hostname	M	V.1.1

V.1.1 Resolve Hostname

V.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.

V.1.1.2 Use Case Roles

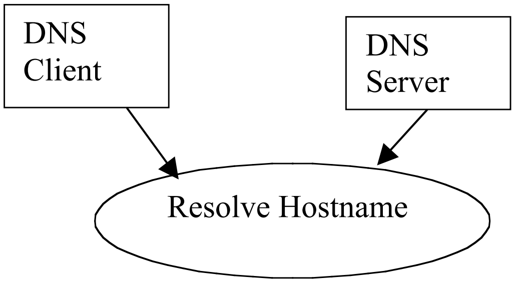

Figure V.1-1 Resolve Hostname

Actor: DNS Client

Role: Needs IP address, has the DNS Hostname

Actor: DNS Server

Role: Provides current IP address when given the DNS Hostname

V.1.1.3 Referenced Standards

The standards and their relationships for the family of DNS protocols are shown in Figure V.1-2 . The details of transactions, transaction diagrams, etc. are contained within the referenced RFC's.

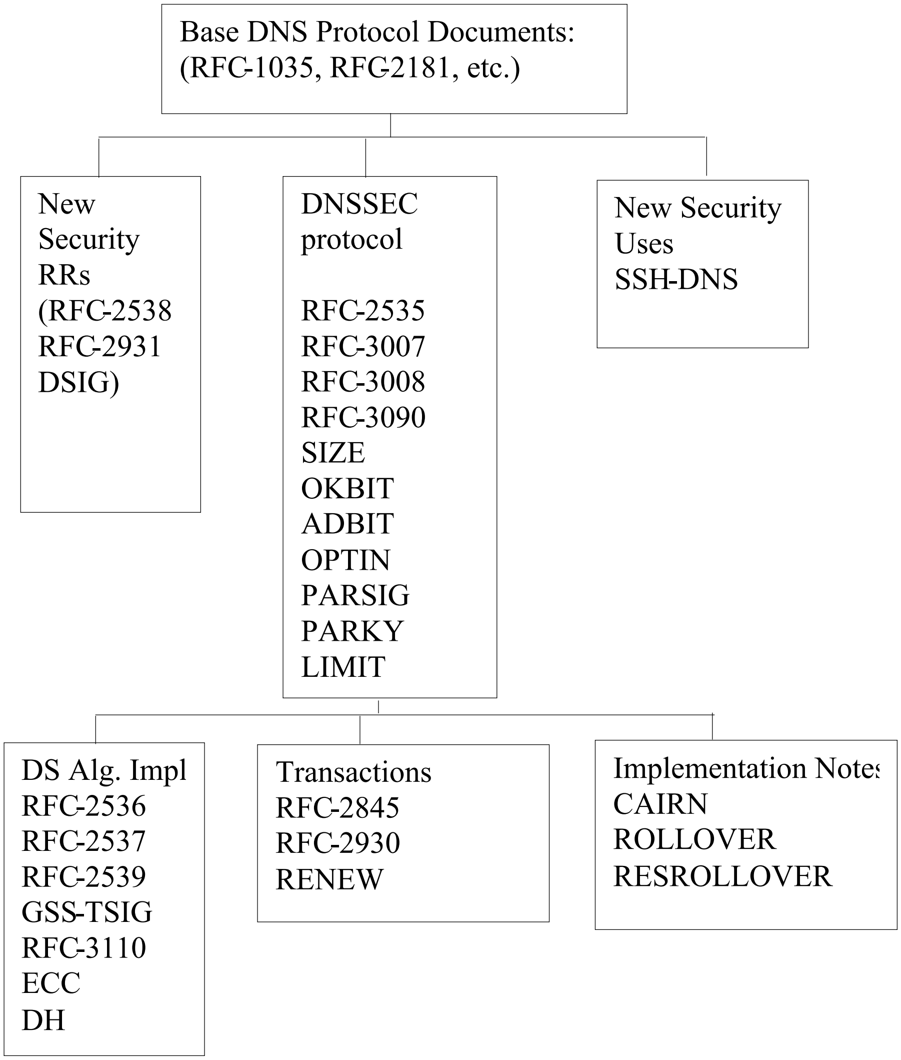

Figure V.1-2 DNS Referenced Standards

V.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 V.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.

V.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.

V.1.2 Configure DHCP Server

V.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.

V.1.2.2 Use Case Roles

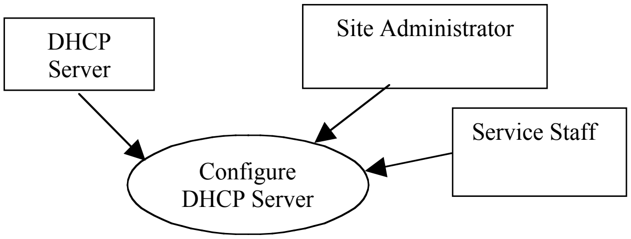

Figure V.1-3 Configure DHCP Server

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.

V.1.2.3 Referenced Standards

None

V.1.3 Find and Use DHCP Server

V.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.

V.1.3.2 Use Case Roles

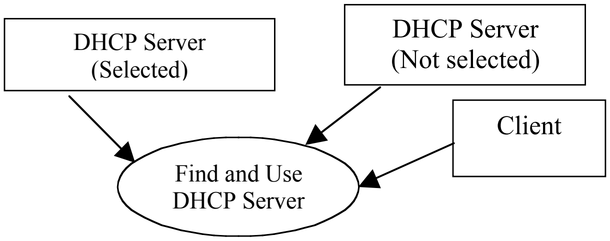

Figure V.1-4 Find and Use DHCP Server

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.

V.1.3.3 Referenced Standards

RFC-2131	DHCP Protocol
RFC-2132	DHCP Options

RFC-2563 Auto Configuration control

V.1.3.4 Interaction Diagram

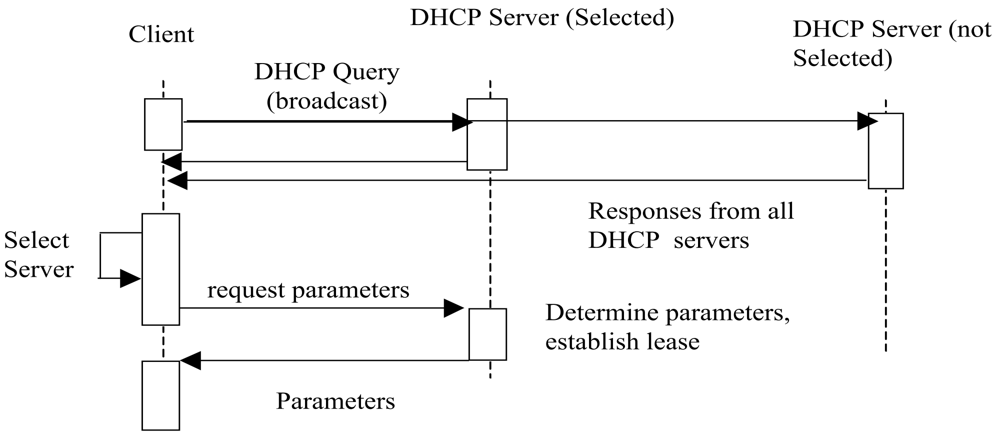
Client
DHCP Server (Selected)
DHCP Server (not Selected)
DHCP Query (broadcast)
Responses from all DHCP servers
Select Server
request parameters
Determine parameters, establish lease
Parameters

Figure V.1-5 DHCP Interactions

The DHCP client shall comply with RFC-2131 (DHCP Protocol), RFC-2132 (DHCP Options), RFC-2563 (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 V.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 V.1-2 DHCP Parameters

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

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

V.1.4 Maintain Lease

V.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.

V.1.4.2 Use Case Roles

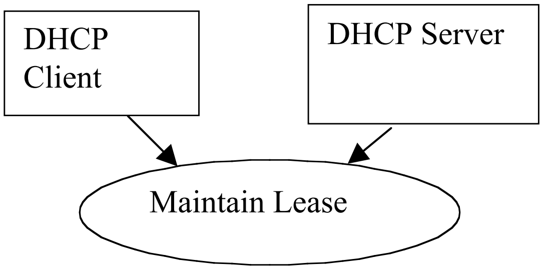

Figure V.1-6 Maintain Lease

Actor:	DHCP client
Role:	Deals with lease renewal and expiration.
Actor:	DHCP Server
Role:	Renewing or deliberately letting leases expire (sometimes done as part of network service operations).

V.1.4.3 Referenced Standards

RFC-2131	DHCP Protocol
RFC-2132	DHCP Options

V.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 RFC-2131 and RFC-2132. 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.

V.1.5 DDNS Coordination

V.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.

A DHCP Server is in compliance 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 the proper hostname/IP relationships in the DNS database.

V.1.5.2 Use Case Roles

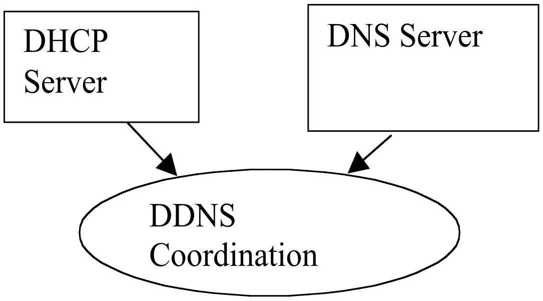

Figure V.1-7 DDNS Coordination

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.

V.1.5.3 Referenced Standards

RFC-2136 Dynamic Updates in the Domain Name System

V.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 assigned to the DHCP client has been given the assigned IP address. The DNS Server updates the DNS database so that subsequent DNS queries for this hostname are given the assigned IP address. When the lease for the IP address expires without renewal, the DHCP server informs the DNS server that the IP address and hostname are no longer valid. The DNS server removes them from the DNS database.

V.1.6 DHCP Security Considerations (Informative)

The Basic Network Address Management Profile 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 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 SectionV.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 V.1.1.4 for a discussion of the DNS security profile standards and drafts.

V.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.

V.1.8 Conformance

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.

Add Annex W for Configuration Profiles to Part 15

Annex W Time Synchronization Profiles

W.1 BASIC TIME SYNCHRONIZATION PROFILE

The Basic Time Synchronization Profile defines services to synchronize the clocks on multiple computers. It employs the Network Time Protocol (NTP) services that have been used for this purpose by many other disciplines. NTP permits synchronization to a local server that provides a local time source, and synchronization to a variety of external time services. The accuracy and precision controls are not explicitly part of the protocol. They are determined in large part by the selection of clock hardware and network topology.

An extensive discussion of implementation strategies for NTP can be found at http://www.ntp.org.

The Basic Time Synchronization Profile applies to the actors DHCP Client, DHCP Server, SNTP Client, NTP Client and NTP Server. The mandatory and optional transactions are described in the table and sections below.

Table W.1-1 - Basic Time Synchronization Profile

Actor	Transaction	Optionality	Section
NTP Server	Maintain Time	M	W.1.2
	Find NTP Servers	O	W.1.1
NTP Client	Maintain Time	M	W.1.2
	Find NTP Servers	O	W.1.1
SNTP Client	Maintain Time	M	W.1.2
DHCP Server	Find NTP Servers	O	W.1.1
DCHP Client	Find NTP Servers	M	W.1.1

W.1.1 Find NTP Servers

The optional NTP protocol elements for NTP autoconfiguration and NTP autodiscovery can significantly simplify installation. The NTP specification for these is defined such that they are truly optional for both client and server. In the event that a client cannot find an NTP server automatically using these services, it can use the DHCP optional information or manually configured information to find a server. Support for these services is recommended but not mandatory.

This transaction exists primarily as a means of documenting whether particular models of equipment support the automatic discovery. This lets installation and operation plan their DHCP and equipment installation procedures in advance.

W.1.1.1 Scope

This applies to any client that needs the correct time, or that needs to have its time stamps synchronized with those of another system. The accuracy of synchronization is determined by details of the configuration and implementation of the network and NTP servers at any specific site.

Both the NTP and SNTP clients shall utilize the NTP server information if it is provided by DHCP and NTP services have not been found using autodiscovery. Manual configuration shall be provided as a backup. Autodiscovery or DHCP are preferred.

W.1.1.2 Use Case Roles

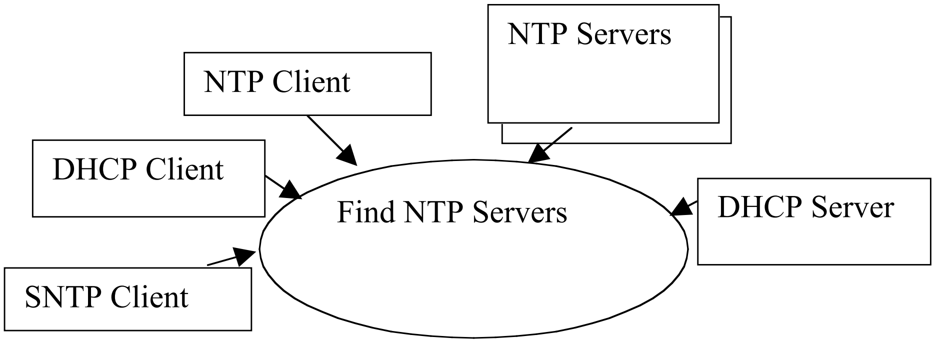

Figure W.1-1 Find NTP Servers

DHCP Server	Provides UTC offset, provides list of NTP servers
DHCP Client	Receives UTC offset and list of NTP servers
NTP Client	Maintains client clock
SNTP Client	Maintains client clock
NTP Servers	External time servers. These may have connections to other time servers, and may be synchronized with national time sources.

W.1.1.3 Referenced Standards

RFC-1305	Network Time Protocol (NTP) standard specification
RFC-2030	Simple NTP

W.1.1.4 Basic Course of Events.

The DHCP server may have provided a list of NTP servers or one may be obtained through optional NTP discovery mechanisms. If this list is empty and no manually configured NTP server address is present, the client shall select its internal clock as the time source (see below). If the list is not empty, the client shall attempt to maintain time synchronization with all those NTP servers. The client may attempt to use the multi-cast, manycast, and broadcast options as defined in RFC-1305. It shall utilize the point to point synchronization option if these are not available. The synchronization shall be in compliance with either RFC-1305 (NTP) or RFC-2030 (SNTP).

If the application requires time synchronization of better than 1s mean error, the client should use NTP. SNTP cannot ensure a more accurate time synchronization.

The DHCP server may have provided a UTC offset between the local time at the machine and UTC. If this is missing, the UTC offset will be obtained in a device specific manner (e.g. service, CMOS). If the UTC offset is provided, the client shall use this offset for converting between UTC and local time.

W.1.1.5 Alternative Paths

If there is no UTC offset information from the DHCP server, then the NTP client will use its preset or service set UTC offset.

If there is no NTP time server, then the NTP client will select its internal battery clock as the source of UTC. These may have substantial errors. This also means that when there are multiple systems but no NTP source, the multiple systems will not attempt to synchronize with one another.

W.1.1.6 Assumptions

The local battery clock time is set to UTC, or the local operating system has proper support to manage both battery clock time, NTP clock time, and system clock time. The NTP time is always in UTC.

W.1.1.7 Postconditions

The client will remain synchronized with its selected time source. In an environment with one or more NTP servers, this will be good time synchronization. In the absence of NTP servers, the selected source will be the internal client clock, with all its attendant errors.

W.1.2 Maintain Time

W.1.2.1 Scope

This applies to any client that needs the correct time, or that needs to have its time stamps synchronized with those of another system. The accuracy of synchronization is determined by details of the configuration and implementation of the network and NTP servers at any specific site.

W.1.2.2 Use Case Roles

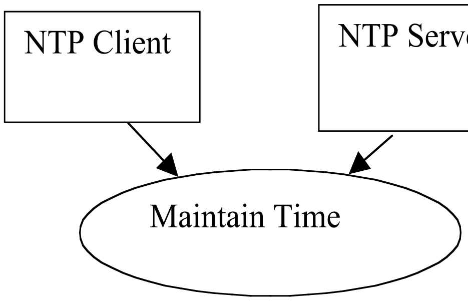

Figure W.2-1 Maintain Time

NTP/SNTP Client	Maintains client clock
NTP Servers	External time servers. These may have connections to other time servers, and may be synchronized with national time sources.

W.1.2.3 Referenced Standards

RFC-1305	Network Time Protocol (NTP) standard specification
RFC-2030	Simple NTP

W.1.2.4 Basic Course of Events.

All the full detail is in RFC-1305 and RFC-2030. The most common and mandatory minimum mode for NTP operation establishes a ping pong of messages between client and servers. The client sends requests to the servers, which fill in time related fields in a response, and the client performs optimal estimation of the present time. The RFCs deal with issues of lost messages, estimation formulae, etc. Once the clocks are in synchronization these ping pong exchanges typically stabilize at roughly 1000 second intervals.

The client machine typically uses the time estimate to maintain the internal operating system clock. This clock is then used by applications that need time information. This approach eliminates the application visible difference between synchronized and unsynchronized time. The RFCs provide guidance on proper implementations.

W.1.3 NTP Security Considerations (Informative)

The Basic Time Synchronization 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 NTP services.
b. Agreements for VPN and other access should require that use only approved NTP servers over the VPN.

This limits the risks to insider denial of service attacks. The service denial is manipulation of the time synchronization such that systems report the incorrect time. The NTP protocols incorporate secure transaction capabilities that can be negotiated. This profile assumes that the above protections are sufficient and does not require support of secure transactions, but they may be supported by an implementation. The SNTP client does not support the use of secured transactions.

Sites with particular concerns regarding security of external network time sources may choose to utilize a GPS or radio based time synchronization. Note that when selecting GPS and radio time sources, care must be taken to establish the accuracy and stability provided by the particular time source. The underlying time accuracy of GPS and radio sources is superb, but some receivers are intended for low accuracy uses and do not provide an accurate or stable result.

W.1.4 NTP Implementation Considerations (informative)

NTP servers always support both NTP and SNTP clients. The difference is one of synchronization accuracy, not communications compatibility. Although in theory both NTP and SNTP clients could run at the same time on a client this is not recommended. The SNTP updates will simply degrade the time accuracy. When other time protocol clients, such as IRIG, are also being used these clients must be coordinated with the NTP client to avoid synchronization problems.

RFC-1305 includes specifications for management of intermittent access to the NTP servers, broken servers, etc. The NTP servers do not need to be present and operational when the NTP process begins. NTP supports the use of multiple servers to provide backup and better accuracy. RFC-1305 specifies the mechanisms used by the NTP client. The site www.ntp.org provides extensive guidance and references regarding the most effective configurations for backups and multiple server configurations.

The local battery clock and client operating system must be properly UTC aware. NTP synchronization is in UTC. This can be a source of confusion because some computers are configured with their hardware clocks set to local time and the operating system set (incorrectly) to UTC. This is a common error that only becomes apparent when the devices attempt to synchronize clocks.

W.1.5 Conformance

The Conformance Statement for the NTP Server and NTP Client shall state whether secure transactions are supported.

The Conformance Statement for the NTP Server shall state whether it is also an NTP Client.

Add Annex X for Configuration Profiles to Part 15

Annex X Application Configuration Management Profiles

X.1 APPLICATION CONFIGURATION MANAGEMENT PROFILE

The Application Configuration Management Profile applies to the actors LDAP Server, LDAP Client, and DNS Server. The mandatory and optional transactions are described in the table and sections below.

Table X.1-1 – Application Configuration Management Profiles

Actor	Transaction	Optionality	Section
LDAP Server	Query LDAP Server	M	X.1.4.2
	Update LDAP Server	O	X.1.4.3
	Maintain LDAP Server	M	X.1.4.4
LDAP Client	Find LDAP Server	M	X.1.4.1
	Query LDAP Server	M	X.1.4.2
	Update LDAP Server	O	X.1.4.3
DNS Server	Find LDAP Server	M	X.1.4.1

X.1.1 Data Model Component Objects

The normative definition of the schema can be found in Section X.1.3. This section gives additional informative descriptions of the objects and information defined in that schema and makes normative statements regarding DICOM system behavior.

The Application Configuration Data Model has the following component objects:

Device – The description of the device

Network AE – The description of the network application entity

Network Connection – The description of the network interface

Transfer Capability – The description of the SOP classes and syntaxes supported by a Network AE.

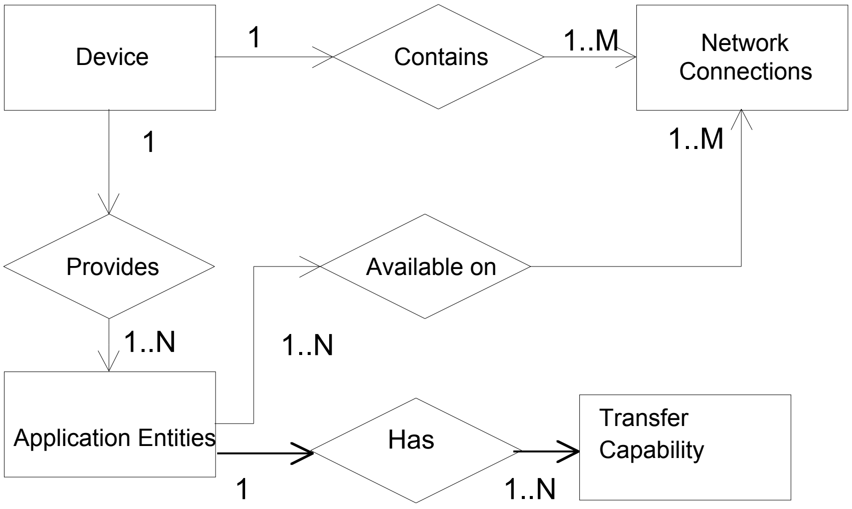

Figure X.1-1
Application Configuration Data Model

In addition there are a number of other objects used in the LDAP schema (see section X.1.2 and Figure X. 1-2) :

DICOM Configuration Root – The root of DICOM Configuration Hierarchy

DICOM Devices Root – The root of the DICOM Devices Hierarchy

DICOM Unique AE-Title Registry Root – The root of the Unique DICOM AE-Title Registry

DICOM Unique AE Title – A unique AE Title within the AE Title Registry

LDAP permits extensions to schema to support local needs (i.e. an object may implement a single structural and multiple auxiliary LDAP classes). DICOM does not mandate client support for such extensions. Servers may support such extensions for local purposes. DICOM Clients may accept or ignore extensions and shall not consider their presence an error.

X.1.1.1 Device

The "device" is set of components organized to perform a task rather than a specific physical instance. For simple devices there may be one physical device corresponding to the Data Model device. But for complex equipment there may be many physical parts to one "device".

The "device" is the collection of physical entities that supports a collection of Application Entities. It is uniquely associated with these entities and vice versa. It is also uniquely associated with the network connections and vice versa. In a simple workstation with one CPU, power connection, and network connection the "device" is the workstation.

An example of a complex device is a server built from a network of multiple computers that have multiple network connections and independent power connections. This would be one device with one application entity and multiple network connections. Servers like this are designed so that individual component computers can be replaced without disturbing operations. The Application Configuration Data Model does not describe any of this internal structure. It describes the network connections and the network visible

Application Entities. These complex devices are usually designed for very high availability, but in the
2 unusual event of a system shutdown the "device" corresponds to all the parts that get shut down.

Table X.1-2 Attributes of Device Object

Information Field	Multiplicity	Description
Device Name	1	A unique name (within the scope of the LDAP database) for this device. It is restricted to legal LDAP names, and not constrained by DICOM AE Title limitations.
Description	0..1	Unconstrained text description of the device.
Manufacturer	0..1	Should be the same as the value of Manufacturer (0008,0070) in SOP instances created by this device.
Manufacturer Model Name	0..1	Should be the same as the value of Manufacturer Model Name (0008,1090) in SOP instances created by this device.
Software Version	0..N	Should be the same as the values of Software Versions (0018,1020) in SOP instances created by this device.
Station Name	0..1	Should be the same as the value of Station Name (0008,1010) in SOP instances created by this device.
Device Serial Number	0..1	Should be the same as the value of Device Serial Number (0018,1000) in SOP instances created by this device.
Primary Device Type	0..N	Represents the kind of device and is most applicable for acquisition modalities. Types should be selected from the list of code values (0008,0100) for Context ID 30 in PS3.16 when applicable.
Institution Name	0..N	Should be the same as the value of Institution Name (0008,0080) in SOP Instances created by this device.
Institution Address	0..N	Should be the same as the value of Institution Address (0008,0081) attribute in SOP Instances created by this device.
Institutional Department Name	0..N	Should be the same as the value of Institutional Department Name (0008,1040) in SOP Instances created by this device.
Issuer of Patient ID	0..1	Default value for the Issuer of Patient ID (0010,0021) for SOP Instances created by this device. May be overridden by the values received in a worklist or other source.
Related Device Reference	0..N	The DNs of related device descriptions outside the DICOM Configuration hierarchy. Can be used to link the DICOM Device object to additional LDAP objects instantiated from other

Information Field	Multiplicity	Description
		schema and used for separate administrative purposes.
Authorized Node Certificate Reference	0..N	The DNs for the certificates of nodes that are authorized to connect to this device. The DNs need not be within the DICOM configuration hierarchy.
This Node Certificate Reference	0..N	The DNs of the public certificate(s) for this node. The DNs need not be within the DICOM configuration hierarchy.
Vendor Device Data	0..N	Device specific vendor configuration information
Installed	1	Boolean to indicate whether this device is presently installed on the network. (This is useful for pre-configuration, mobile vans, and similar situations.)

The “Authorized Node Certificate Reference” is intended to allow the LDAP server to provide the list of certificates for nodes that are authorized to communicate with this device. These should be the public certificates only. This list need not be complete. Other network peers may be authorized by other mechanisms.

The “This Node Certificate Reference” is intended to allow the LDAP server to provide the certificate(s) for this node. These may also be handled independently of LDAP.

Note: A device may have multiple Primary Device Type entries. It may be a multifunctional device, e.g. combined PET and CT. It may be a cascaded device, e.g. image capture and ultrasound.

Table X.1-3 Child Objects of Device Object

Information Field	Multiplicity	Description
Network Application Entity	1..N	The application entities available on this device (see Section X.1.1.2)
Network Connection	1..N	The network connections for this device (see Section X.1.1.3)

X.1.1.2 Network Application Entity

A Network AE is an application entity that provides services on a network. A Network AE will have the same functional capability regardless of the particular network connection used. If there are functional differences based on selected network connection, then these are separate Network AEs. If there are functional differences based on other internal structures, then these are separate Network AEs.

Table X.1-4 Attributes of Network AE Object

Information Field	Multiplicity	Description
AE Title	1	Unique AE title for this Network AE

Information Field	Multiplicity	Description
Description	0..1	Unconstrained text description of the application entity.
Vendor Data	0..N	AE specific vendor configuration information
Application Cluster	0..N	Locally defined names for a subset of related applications. E.g. “neuroradiology”.
Preferred Called AE Title	0..N	AE Title(s) that are preferred for initiating associations.
Preferred Calling AE Title	0..N	AE Title(s) that are preferred for accepting associations.
Association Acceptor	1	A Boolean value. True if the Network AE can accept associations, false otherwise.
Association Initiator	1	A Boolean value. True if the Network AE can accept associations, false otherwise.
Network Connection Reference	1..N	The DNs of the Network Connection objects for this AE
Supported Character Set	0..N	The Character Set(s) supported by the Network AE for data sets it receives. The value shall be selected from the Defined Terms for Specific Character Set (0008,0005) in PS3.3. If no values are present, this implies that the Network AE supports only the default character repertoire (ISO IR 6).
Installed	0..1	A Boolean value. True if the AE is installed on network. If not present, information about the installed status of the AE is inherited from the device

The “Application Cluster” concept provides the mechanism to define local clusters of systems. The use cases for Configuration Management require a “domain” capability for DICOM applications that would be independent of the network topology and administrative domains that are used by DNS and other TCP level protocols. The Application Cluster is multi-valued to permit multiple clustering concepts for different purposes. It is expected to be used as part of a query to limit the scope of the query.

The “Preferred Called AE Title” concept is intended to allow a site administrator to define a limited default set of AEs that are preferred for use as communication partners when initiating associations. This capability is particularly useful for large centrally administered sites to simplify the configuration possibilities and restrict the number of configured AEs for specific workflow scenarios. For example, the set of AEs might contain the AE Titles of assigned Printer, Archive, RIS and QA Workstations so that the client device could adapt its configuration preferences accordingly. The “Preferred Called AE Title” concept does not prohibit association initiation to unlisted AEs. Associations to unlisted AEs can be initiated if necessary.

The “Preferred Calling AE Title” concept is intended to allow a site administrator to define a default set of AEs that are preferred when accepting assocations. The “Preferred Calling AE Title” concept does not prohibit accepting associations from unlisted AEs.

The “Network Connection Reference” is a link to a separate Network Connection object. The referenced Network Connection object is a sibling the AE object (i.e., both are children of the same Device object).

Table X.1-5 Child Objects of Network AE Object

Information Field	Multiplicity	Description
Transfer Capability	1..N	The Transfer Capabilities for this Network AE. See Section X.1.4

X.1.1.3 Network Connection

The “network connection” describes one TCP port on one network device. This can be used for a TCP connection over which a DICOM association can be negotiated with one or more Network AEs. It specifies the hostname and TCP port number. A network connection may support multiple Network AEs. The Network AE selection takes place during association negotiation based on the called and calling AE-titles.

Table X.1-6 Attributes of Network Connection Object

Information Field	Multiplicity	Description
Common Name	0..1	An arbitrary name for the Network Connections object. Can be a meaningful name or any unique sequence of characters. Can be used as the RDN. Note: The “cn” attribute type is a basic LDAP defined type and is a synonym for Common Name.
Hostname	1	This is the DNS name for this particular connection. This is used to obtain the current IP address for connections. Hostname must be sufficiently qualified to be unambiguous for any client DNS user.
Port	0..1	The TCP port that the AE is listening on. (This may be missing for a network connection that only initiates associations.)
TLS CipherSuite	0..N	The TLS CipherSuites that are supported on this particular connection. TLS CipherSuites shall be described using an RFC-2246 string representation (e.g. “TLS_RSA_WITH_RC4_128_SHA”)
Installed	0..1	A Boolean value. True if the Network Connection is installed on the network. If not present, information about the installed status of the Network Connection is inherited from the device.

Inclusion of a TLS CipherSuite in a Network Connection capable of accepting associations implies that the TLS protocol must be used to successfully establish an association on the Network Connection.

A single Network AE may be available on multiple network connections. This is often done at servers for availability or performance reasons. For example, at a hospital where each floor is networked to a single hub per floor, the major servers may have direct connections to each of the hubs. This provides better performance and reliability. If the server does not change behavior based on the particular physical network connection, then it can be described as having Network AEs that are available on all of these multiple network connections. A Network AE may also be visible on multiple TCP ports on the same network hardware port, with each TCP port represented as a separate network connection. This would allow, e.g. a TLS-secured DICOM port and a classical un-secured DICOM port to be supported by the same AE.

X.1.1.4 Transfer Capabilities

Each Network AE object has one or more Transfer Capabilities. Each transfer capability specifies the SOP class that the Network AE can support, the mode that it can utilize (SCP or SCU), and the Transfer Syntax(es) that it can utilize. A Network AE that supports the same SOP class in both SCP and SCU modes will have two Transfer Capabilities objects for that SOP class.

Table X.1-7 Attributes of Transfer Capability Object

Information Field	Multiplicity	Description
Common Name	0..1	An arbitrary name for the Transfer Capability object. Can be a meaningful name or any unqiue sequence of characters. Can be used as the RDN.
SOP Class	1	SOP Class UID
Role	1	Either “SCU” or “SCP”
Transfer Syntax	1..N	The transfer syntax(es) that may be requested as an SCU or that are offered as an SCP.

X.1.1.5 DICOM Configuration Root

This structural object class represents the root of the DICOM Configuration Hierarchy. Only a single object of this type should exist within an organizational domain. Clients can search for an object of this class to locate the root of the DICOM Configuration Hierarchy.

Table X.1-8 Attributes of the DICOM Configuration Root Object

Information Field	Multiplicity	Description
Common Name	1	The Name for the Configuration Root. Should be used as the RDN. The name shall be “DICOM Configuration”.
Description	0..1	Unconstrained text description.

Table X.1-9 Child Objects of DICOM Configuration Root Object

Information Field	Multiplicity	Description
Devices Root	1	The root of the DICOM Devices Hierarchy
Unique AE Titles Registry Root	1	The root of the Unique AE Titles Registry

X.1.1.6 Devices Root

This structural object class represents the root of the DICOM Devices Hierarchy. Only a single object of this type should exist as a child of DICOM Configuration Root. Clients can search for an object of this class to locate the root of the DICOM Devices Hierarchy.

Table X.1-10 Attributes of the Devices Root Object

Information Field	Multiplicity	Description
Common Name	1	The Name for the Devices Root. Should be used as the RDN. The name shall be "Devices".
Description	0..1	Unconstrained text description.

Table X.1-11 Child Objects of Devices Root Object

Information Field	Multiplicity	Description
Device	0..N	The individual devices installed within this organizational domain.

X.1.1.7 Unique AE Titles Registry Root

This structural object class represents the root of the Unique AE-Titles Registry Hierarchy. Only a single object of this type should exist as a child of the DICOM Configuration Root. Clients can search for an object of this class to locate the root of the Unique AE Titles Registry.

Table X.1-12 Attributes of the Unique AE Titles Registry Root Object

Information Field	Multiplicity	Description
Common Name	1	The Name for the Unique AE Titles Registry Root. Should be used as the RDN. The name shall be "Unique AE Titles Registry".
Description	0..1	Unconstrained text description.

Table X.1-13 Child Objects of Unique AE Titles Registry Root Object

Information Field	Multiplicity	Description
Unique AE Title	0..N	The unique AE Titles installed within this organizational domain (see Section X.1.8)

X.1.1.8 Unique AE Title

This structural object class represents a Unique Application Entity Title. Objects of this type should only exist as children of the Unique AE-Titles Registry Root. The sole purpose of this object class is to enable allocation of unique AE Titles. All operational information associated with an AE Title is maintained within a separate Network AE object.

Table X.1-14 Attributes of the Unique AE Title Object

Information Field	Multiplicity	Description
AE Title	1	The Unique AE Titles.

X.1.2 Application Configuration Data Model Hierarchy

The LDAP structure is built upon a hierarchy of named objects. This hierarchy can vary from site to site. The DICOM configuration management function needs to find its objects within this hierarchy in a predictable manner. For this reason, three specific object classes are defined for the three objects at the top of the DICOM hierarchy. These three object classes must not be used in this tree relationship anywhere else in the LDAP hierarchy.

The DICOM portion of the hierarchy shall begin at a root object of class dicomConfigurationRoot with a Common Name of "DICOM Configuration". Below this object shall be two other objects:

a. An object of class `dicomDevicesRoot` with a Common Name of "Devices". This is the root of the tree of objects that correspond to the Application Configuration Data Model structure of Section X.1.1.

b. An object of class `dicomUniqueAETitlesRegistryRoot` with a common name of "Unique AE Titles Registry". This is the root of a flat tree of objects. Each of these objects is named with one of the AE titles that are presently assigned. This is the mechanism for finding available AE titles.

The three object classes `dicomConfigurationRoot, dicomDevicesRoot`, and `dicomUniqueAETitleRegistryRoot` are used by LDAP clients to establish the local root of the DICOM configuration information within an LDAP hierarchy that may be used for many other purposes.

Note: During system startup it is likely that the DICOM configuration application will do an LDAP search for an entry of object class `dicomConfigurationRoot` and then confirm that it has the `dicomDevicesRoot` and `dicomUniqueAETitlesRegistryRoot` entries directly below it. When it finds this configuration, it can then save the full location within the local LDAP tree and use that as the root of the DICOM tree.

The objects underneath the `dicomUniqueAETitlesRegistryRoot` are used to provide the uniqueness required for DICOM AE-titles. The `dicomUniqueAETitle` objects have a single attribute representing a unique AE Title. When a new AE-Title is required, a tentative new name is selected. The new name is reserved by using the LDAP create facility to create an object of class `dicomUniqueAETitle` with the new name under the AE-Title object. If this name is already in use, the create will fail. Otherwise, this reserves the name. LDAP queries can be used to obtain the list of presently assigned AE-titles by obtaining the list of all names under the `dicomUniqueAETitlesRegistryRoot` object.

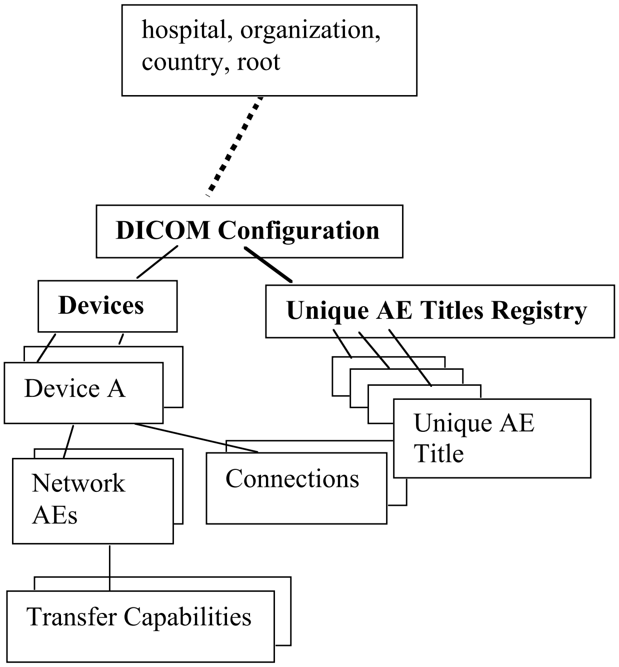

Figure X.1-2 DICOM Configuration Hierarchy

Notes: 1. LDAP uses a root and relative hierarchical naming system for objects. Every object name is fully unique within the full hierarchy. This means that the names of the objects beneath “Unique AE Titles Registry” will be unique. It also means that the full names of Network AEs and Connections will be within their hierarchy context. E.g., the DN for one of the Network AEs in Figure X.1-2 would be:

```
dicomAETitle=CT_01, dicomDeviceName=Special Research CT, cn=Devices,
        cn=DICOM Configuration, o=Sometown Hospital
```

2. In theory, multiple independent DICOM configuration hierarchies could exist within one organization. The LDAP servers in such a network should constrain local device accesses so that DICOM configuration clients have only one DICOM Configuration Hierarchy visible to each client.

3. The merger of two organizations will require manual configuration management to merge DICOM Configuration hierarchies. There are likely to be conflicts in AE-titles, roles, and other conflicts.

X.1.3 LDAP Schema for Objects and Attributes

The individual LDAP attribute information is summarized in the comments at the beginning of the schema below. The formal definition of the objects and the attributes is in the schema below. This schema may be extended by defining an additional schema that defines auxiliary classes, sub-classes derived from this schema, or both.

The formal LDAP schema for the Application Configuration Data Model and the DICOM Configuration Hierarchy is:

```
# 3 Attribute Type Definitions
#
#    The following attribute types are defined in this document:
#
#      Name                                     Syntax         Multiplicity
#      --------------------------------         ------         ------------
#       dicomDeviceName                              string         Single
#       dicomDescription                             string         Single
#       dicomManufacturer                            string         Single
#       dicomManufacturerModelName                   string         Single
#       dicomSoftwareVersion                         string         Multiple
#       dicomVendorData                              binary         Multiple
#       dicomAETitle                                 string         Single
#       dicomNetworkConnectionReference              DN             Multiple
#       dicomApplicationCluster                      string         Multiple
#       dicomAssociationInitiator                    bool           Single
#       dicomAssociationAcceptor                     bool           Single
#       dicomHostname                                string         Single
#       dicomPort                                    integer        Single
#       dicomSOPClass                                OID            Single
#       dicomTransferRole                            string         Single
#       dicomTransferSyntax                          OID            Multiple
#       dicomPrimaryDeviceType                       string         Multiple
#       dicomRelatedDeviceReference                  DN             Multiple
#       dicomPreferredCalledAETitle                  string         Multiple
#       dicomTLSCipherSuite                          string         Multiple
#       dicomAuthorizedNodeCertificateReference      DN             Multiple
#       dicomThisNodeCertificateReference            DN             Multiple
#       dicomInstalled                               bool           Single
#       dicomStationName                             string         Single
#       dicomDeviceSerialNumber                      string         Single
#       dicomInstitutionName                         string         Multiple
#       dicomInstitutionAddress                      string         Multiple
#       dicomInstitutionDepartmentName               string         Multiple
#       dicomIssuerOfPatientID                       string         Single
#       dicomPreferredCallingAETitle                 string         Multiple
#       dicomSupportedCharacterSet                   string         Multiple
#


# 3.1 dicomDeviceName                                string         Single
#
#    This attribute stores the unique name (within the scope of the LDAP database)
#    for a DICOM Device.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Directory String'.
#    Its case is not significant for equality and substring matches.
#

attributetype ( 1.2.840.10008.15.0.3.1
        NAME 'dicomDeviceName'
        DESC 'The unique name for the device'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )

# 3.2 dicomDescription                               string         Single
#
#    This attribute stores the (unconstrained) textual description for a DICOM entity.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Directory String'.
#    Its case is not significant for equality and substring matches.
#

attributetype ( 1.2.840.10008.15.0.3.2
        NAME 'dicomDescription'
        DESC 'Textual description of the DICOM entity'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )
```

```
# 3.3 dicomManufacturer                                       string         Single
#
#    This attribute stores the Manufacturer name for a DICOM Device.
#    Should be identical to the value of the DICOM attribute Manufacturer (0008,0070) [VR=LO]
#    contained in SOP Instances created by this device.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Directory String'.
#    Its case is not significant for equality and substring matches.
#

attributetype ( 1.2.840.10008.15.0.3.3
        NAME 'dicomManufacturer'
        DESC 'The device Manufacturer name'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )


# 3.4 dicomManufacturerModelName                       string         Single
#
#    This attribute stores the Manufacturer Model Name for a DICOM Device.
#    Should be identical to the value of the DICOM attribute Manufacturer
#    Model Name (0008,1090) [VR=LO]
#    contained in SOP Instances created by this device.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Directory String'.
#    Its case is not significant for equality and substring matches.
#

attributetype ( 1.2.840.10008.15.0.3.4
        NAME 'dicomManufacturerModelName'
        DESC 'The device Manufacturer Model Name'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )

# 3.5 dicomSoftwareVersion                                    string         Multiple
#
#    This attribute stores the software version of the device and/or its subcomponents.
#    Should be the same as the values of Software Versions (0018,1020) in
#    SOP instances created by this device.
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'Directory String'.
#    Its case is not significant for equality and substring matches.
#

attributetype ( 1.2.840.10008.15.0.3.5
        NAME 'dicomSoftwareVersion'
        DESC 'The device software version. Should be the same as the values of Software Versions
(0018,1020) in SOP instances created by this device.'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

# 3.6 dicomVendorData                                  binary         Multiple
#
#    This attribute stores vendor specific configuration information.
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'Binary'.
#    Neither equality nor substring matches are applicable to binary data.
#

attributetype ( 1.2.840.10008.15.0.3.6
        NAME 'dicomVendorData'
        DESC 'Arbitrary vendor-specific configuration information (binary data)'
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 )

# 3.7 dicomAETitle                                   name                   Single
#
#    This attribute stores an Application Entity (AE) title.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'IA5 String'.
#    Its case is significant.
#

attributetype ( 1.2.840.10008.15.0.3.7
        NAME 'dicomAETitle'
        DESC 'Application Entity (AE) title'
        EQUALITY caseExactIA5Match
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
        SINGLE-VALUE )


# 3.8 dicomNetworkConnectionReference        DN             Multiple
#
#    This attribute stores the DN of a dicomNetworkConnection object
#    used by an Application Entity.
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'Distinguished Name'.
#

attributetype ( 1.2.840.10008.15.0.3.8
        NAME 'dicomNetworkConnectionReference'
        DESC 'The DN of a dicomNetworkConnection object used by an Application Entity'
        EQUALITY distinguishedNameMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

# 3.9 dicomApplicationCluster                string         Multiple
#
#    This attribute stores an application cluster name for an Application
#    Entity (e.g. "Neuroradiology Research")
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'Directory String'.
#    Its case is not significant for equality and substring matches.
#

attributetype ( 1.2.840.10008.15.0.3.9
        NAME 'dicomApplicationCluster'
        DESC 'Application cluster name for an Application Entity (e.g. "Neuroradiology Research")'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

# 3.10 dicomAssociationInitiator                     bool                   Single
#
#    This attribute indicates if an Application Entity is capable of initiating
#    network associations.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Boolean'.
#

attributetype ( 1.2.840.10008.15.0.3.10
        NAME 'dicomAssociationInitiator'
        DESC 'Indicates if an Application Entity is capable of initiating network associations'
        EQUALITY booleanMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
        SINGLE-VALUE )
```

```
# 3.11 dicomAssociationAcceptor                      bool                  Single
#
#    This attribute indicates if an Application Entity is capable of accepting
#    network associations.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Boolean'.
#

attributetype ( 1.2.840.10008.15.0.3.11
        NAME 'dicomAssociationAcceptor'
        DESC 'Indicates if an Application Entity is capable of accepting network associations'
        EQUALITY booleanMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
        SINGLE-VALUE )


# 3.12 dicomHostname                                 string         Single
#
#    This attribute stores a DNS hostname for a connection.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Directory String'.
#    Its case is not significant for equality and substring matches.
#

attributetype ( 1.2.840.10008.15.0.3.12
        NAME 'dicomHostname'
        DESC 'DNS hostname'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )


# 3.13 dicomPort                                     integer        Single
#
#    This attribute stores a TCP port number for a connection.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Integer'.
#

attributetype ( 1.2.840.10008.15.0.3.13
        NAME 'dicomPort'
        DESC 'TCP Port number'
        EQUALITY  integerMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
        SINGLE-VALUE )

# 3.14 dicomSOPClass                                 OID            Single
#
#    This attribute stores a SOP Class UID
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'OID'.
#

attributetype ( 1.2.840.10008.15.0.3.14
        NAME 'dicomSOPClass'
        DESC 'A SOP Class UID'
        EQUALITY  objectIdentifierMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.38
        SINGLE-VALUE )


# 3.15 dicomTransferRole                             String         Single
#
#    This attribute stores a transfer role (either "SCU" or "SCP").
```

```
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Directory String'.
#    Its case is not significant for equality and substring matches.
#

attributetype ( 1.2.840.10008.15.0.3.15
        NAME 'dicomTransferRole'
        DESC 'Transfer role (either "SCU" or "SCP")'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )


# 3.16 dicomTransferSyntax                           OID            Multiple
#
#    This attribute stores a Transfer Syntax UID
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'OID'.
#

attributetype ( 1.2.840.10008.15.0.3.16
        NAME 'dicomTransferSyntax'
        DESC 'A Transfer Syntax UID'
        EQUALITY  objectIdentifierMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )



# 3.17 dicomPrimaryDeviceType                string         Multiple
#
#    This attribute stores the primary type for a DICOM Device.
#    Types should be selected from the list of code values (0008,0100)
#    for Context ID 30 in DICOM Part 16 when applicable.
#
#    It is a multiple-valued attribute.
#    This attribute's syntax is 'IA5 String'.
#    Its case is significant.
#

attributetype ( 1.2.840.10008.15.0.3.17
        NAME 'dicomPrimaryDeviceType'
        DESC 'The device Primary Device type'
        EQUALITY caseExactIA5Match
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )


# 3.18 dicomRelatedDeviceReference           DN                     Multiple
#
#    This attribute stores a reference to a related device description outside
#    the DICOM Configuration Hierachy.  Can be used to link the DICOM Device object to
#    additional LDAP objects instantiated from other schema and used for
#    separate administrative purposes.
#
#    This attribute's syntax is 'Distinguished Name'.
#    It is a multiple-valued attribute.
#

attributetype ( 1.2.840.10008.15.0.3.18
        NAME 'dicomRelatedDeviceReference'
        DESC 'The DN of a related device description outside the DICOM Configuration Hierachy'
        EQUALITY distinguishedNameMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )


# 3.19 dicomPreferredCalledAETitle                          string                 Multiple
#
```

```
#    AE Title(s) to which associations may be preferably initiated.
#
#    It is a multiple-valued attribute.
#    This attribute's syntax is 'IA5 String'.
#    Its case is significant.
#

attributetype ( 1.2.840.10008.15.0.3.19
        NAME 'dicomPreferredCalledAETitle'
        DESC 'AE Title(s) to which associations may be preferably initiated.'
        EQUALITY caseExactIA5Match
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )


# 3.20 dicomTLSCipherSuite                    string                 Multiple
#
#    The attribute stores the supported TLS CipherSuites.
#    TLS CipherSuites shall be described using a RFC-2246 string representation
#    (e.g. "TLS_RSA_WITH_RC4_128_SHA").
#
#    It is a multiple-valued attribute.
#    This attribute's syntax is 'IA5 String'.
#    Its case is significant.
#

attributetype ( 1.2.840.10008.15.0.3.20
        NAME 'dicomTLSCipherSuite'
        DESC 'The supported TLS CipherSuites'
        EQUALITY caseExactIA5Match
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

# 3.21  dicomAuthorizedNodeCertificateReference              DN     Multiple
#
#    This attribute stores a reference to a TLS public certificate for a DICOM
#    node that is authorized to connect to this node.  The certificate
#    is not necessarily stored within the DICOM Hierarchy
#
#    This attribute's syntax is 'Distinguished Name'.
#    It is a multiple-valued attribute.
#

attributetype ( 1.2.840.10008.15.0.3.21
        NAME 'dicomAuthorizedNodeCertificateReference'
        DESC 'The DN of a Certificate for a DICOM node that is authorized to connect to this node'
        EQUALITY distinguishedNameMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

# 3.22 dicomThisNodeCertificateReference             DN                     Multiple
#
#    This attribute stores a reference to a TLS public certificate for
#    this node.  It is not necessarily stored as part of
#    the DICOM Configuration Hierachy.
#
#    This attribute's syntax is 'Distinguished Name'.
#    It is a multiple-valued attribute.
#

attributetype ( 1.2.840.10008.15.0.3.22
        NAME 'dicomThisNodeCertificateReference'
        DESC 'The DN of a related device description outside the DICOM Configuration Hierachy'
        EQUALITY distinguishedNameMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

# 3.23 dicomInstalled                 bool                   Single
#
#    This attribute indicates whether the object is presently installed.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Boolean'.
```

```
#

attributetype ( 1.2.840.10008.15.0.3.23
        NAME 'dicomInstalled'
        DESC 'Indicates if the DICOM object (device, Network AE, or Port) is presently installed'
        EQUALITY booleanMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
        SINGLE-VALUE )


# 3.24  dicomStationName                             string        Single
#
#    This attribute stores the station name of the device.
#    Should be the same as the value of Station Name (0008,1010) in
#    SOP instances created by this device.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.24
        NAME 'dicomStationName'
        DESC 'Station Name of the device.  Should be the same as the value of Station Name
(0008,1010) in SOP instances created by this device.'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE)



# 3.25  dicomDeviceSerialNumber                      string        Single
#
#    This attribute stores the serial number of the device.
#    Should be the same as the value of Device Serial Number (0018,1000)
#    in SOP instances created by this device.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.25
        NAME 'dicomDeviceSerialNumber'
        DESC 'Serial number of the device. Should be the same as the value of Device Serial Number
(0018,1000) in SOP instances created by this device.'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE)

# 3.26  dicomInstitutionName                         string        Multiple
#
#    This attribute stores the institution name of the device.
#    Should be the same as the value of Institution Name (0008,0080)
#    in SOP Instances created by this device.
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.26
        NAME 'dicomInstitutionName'
        DESC 'Institution name of the device. Should be the same as the value of Institution Name
(0008,0080) in SOP Instances created by this device.'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

# 3.27  dicomInstitutionAddress                      string        Multiple
#
#    This attribute stores the institution address of the device.
#    Should be the same as the value of Institution Address (0008,0081)
#    attribute in SOP Instances created by this device.
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.27
        NAME 'dicomInstitutionAddress'
        DESC 'Institution address of the device.  Should be the same as the value of Institution
Address (0008,0081) attribute in SOP Instances created by this device.'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )


# 3.28  dicomInstitutionDepartmentName               string         Multiple
#
#    This attribute stores the institution department name of the device.
#    Should be the same as the value of Institutional Department Name (0008,1040)
#    in SOP Instances created by this device.
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.28
        NAME 'dicomInstitutionDepartmentName'
        DESC 'Institution department name of the device.  Should be the same as the value of
Institutional Department Name (0008,1040) in SOP Instances created by this device.'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )


# 3.29  dicomIssuerOfPatientID                       string         Single
#
#    This attribute stores the Default value for the Issuer of Patient ID (0010,0021)
#    for SOP Instances created by this device.  May be overridden by the values
#    received in a worklist or other source.
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.29
        NAME 'dicomIssuerOfPatientID'
        DESC 'Default value for the Issuer of Patient ID (0010,0021) for SOP Instances created by
this device.  May be overridden by the values received in a worklist or other source.'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )



# 3.30  dicomPreferredCallingAETitle                 string         Multiple
#
#    AE Title(s) to which associations may be preferably accepted.
#
#    It is a multiple-valued attribute.
#    This attribute's syntax is 'IA5 String'.
#    Its case is significant.
#

attributetype ( 1.2.840.10008.15.0.3.30
        NAME 'dicomPreferredCallingAETitle'
        DESC 'AE Title(s) to which associations may be preferably accepted.'
        EQUALITY caseExactIA5Match
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )


# 3.31  dicomSupportedCharacterSet                   string         Multiple
#
```

```
#    The Character Set(s) supported by the Network AE for data sets it receives.
#    Contains one of the Defined Terms for Specific Character Set (0008,0005).
#    If not present, this implies that the Network AE supports only the default
#    character repertoire (ISO IR 6).
#
#    It is a multiple-valued attribute.
#    This attribute's syntax is 'IA5 String'.
#    Its case is significant.
#
attributetype ( 1.2.840.10008.15.0.3.31
        NAME 'dicomSupportedCharacterSet'
        DESC 'The Character Set(s) supported by the Network AE for data sets it receives.'
        EQUALITY caseExactIA5Match
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )




# 4 Object Class Definitions
#
#    The following object classes are defined in this document.  All are
#    structural classes.
#
#       Name                                  Description
#       ---------------------------           --------------------------
#       dicomConfigurationRoot                root of the DICOM Configuration Hierarchy
#       dicomDevicesRoot                      root of the DICOM Devices Hierarchy
#       dicomUniqueAETitlesRegistryRoot       root of the Unique DICOM AE-Titles Registry Hierarchy
#       dicomDevice                           Devices
#       dicomNetworkAE                        Network AE
#       dicomNetworkConnection                Network Connections
#       dicomUniqueAETitle                    Unique AE Title
#       dicomTransferCapability               Transfer Capability

#
# 4.1 dicomConfigurationRoot
#
#    This structural object class represents the root of the DICOM Configuration Hierarchy.
#    Only a single object of this type should exist within an organizational domain.
#    Clients can search for an object of this class to locate the root of the
#    DICOM Configuration Hierarchy.
#

objectclass ( 1.2.840.10008.15.0.4.1
        NAME 'dicomConfigurationRoot'
        DESC 'Root of the DICOM Configuration Hierarchy'
        SUP top
        STRUCTURAL
        MUST ( cn )
        MAY ( description ) )

#
# 4.2 dicomDevicesRoot
#
#    This structural object class represents the root of the DICOM Devices Hierarchy.
#    Only a single object of this type should exist as a child of dicomConfigurationRoot.
#

objectclass ( 1.2.840.10008.15.0.4.2
        NAME 'dicomDevicesRoot'
        DESC 'Root of the DICOM Devices Hierarchy'
        SUP top
        STRUCTURAL
        MUST ( cn )
        MAY ( description ) )


#
```

```
# 4.3 dicomUniqueAETitlesRegistryRoot
#
#    This structural object class represents the root of the Unique DICOM AE-Titles
#    Registry Hierarchy.
#    Only a single object of this type should exist as a child of dicomConfigurationRoot.
#

objectclass ( 1.2.840.10008.15.0.4.3
        NAME 'dicomUniqueAETitlesRegistryRoot'
        DESC 'Root of the Unique DICOM AE-Title Registry Hierarchy'
        SUP top
        STRUCTURAL
        MUST ( cn )
        MAY ( description ) )

#
# 4.4 dicomDevice
#
#    This structural object class represents a DICOM Device.
#

objectclass ( 1.2.840.10008.15.0.4.4
        NAME 'dicomDevice'
        DESC 'DICOM Device related information'
        SUP top
        STRUCTURAL
        MUST (
                dicomDeviceName $
                dicomInstalled )
        MAY  (
                dicomDescription $
                dicomManufacturer $
                dicomManufacturerModelName $
                dicomSoftwareVersion $
                dicomStationName $
                dicomDeviceSerialNumber $
                dicomInstitutionName $
                dicomInstitutionAddress $
                dicomInstitutionDepartmentName $
                dicomIssuerOfPatientID $
                dicomVendorData $
                dicomPrimaryDeviceType $
                dicomRelatedDeviceReference $
                dicomAuthorizedNodeCertificateReference $
                dicomThisNodeCertificateReference) )

#
# 4.5 dicomNetworkAE
#
#    This structural object class represents a Network Application Entity
#

objectclass ( 1.2.840.10008.15.0.4.5
        NAME 'dicomNetworkAE'
        DESC 'DICOM Network AE related information'
        SUP top
        STRUCTURAL
        MUST (
                dicomAETitle $
                dicomNetworkConnectionReference $
                dicomAssociationInitiator $
                dicomAssociationAcceptor )
        MAY (
                dicomDescription $
                dicomVendorData $
                dicomApplicationCluster $
                dicomPreferredCalledAETitle $
                dicomPreferredCallingAETitle $
                dicomSupportedCharacterSet $
```

```
               dicomInstalled ) )


#
# 4.6 dicomNetworkConnection
#
#    This structural object class represents a Network Connection
#

objectclass ( 1.2.840.10008.15.0.4.6
        NAME 'dicomNetworkConnection'
        DESC 'DICOM Network Connection information'
        SUP top
        STRUCTURAL
        MUST ( dicomHostname )
        MAY (
                cn $
                dicomPort $
                dicomTLSCipherSuite $
                dicomInstalled ) )

#
# 4.7 dicomUniqueAETitle
#
#    This structural object class represents a Unique Application Entity Title
#

objectclass ( 1.2.840.10008.15.0.4.7
        NAME 'dicomUniqueAETitle'
        DESC 'A Unique DICOM Application Entity title'
        SUP top
        STRUCTURAL
        MUST ( dicomAETitle ) )

#
# 4.8 dicomTransferCapability
#
#    This structural object class represents Transfer Capabilities for an Application Entity
#

objectclass ( 1.2.840.10008.15.0.4.8
        NAME 'dicomTransferCapability'
        DESC 'Transfer Capabilities for an Application Entity'
        SUP top
        STRUCTURAL
        MUST (
                dicomSOPClass $
                dicomTransferRole $
                dicomTransferSyntax)
        MAY (
                cn) )
```

X.1.4 Transactions

X.1.4.1 Find LDAP Server

X.1.4.1.1 Scope

The RFC-2782 *A DNS RR for specifying the location of services (DNS SRV)* specifies a mechanism for requesting the names and rudimentary descriptions for machines that provide network services. The DNS client requests the descriptions for all machines that are registered as offering a particular service name. In this case the service name requested will be “LDAP”. The DNS server may respond with multiple names for a single request.

X.1.4.1.2 Use Case Roles

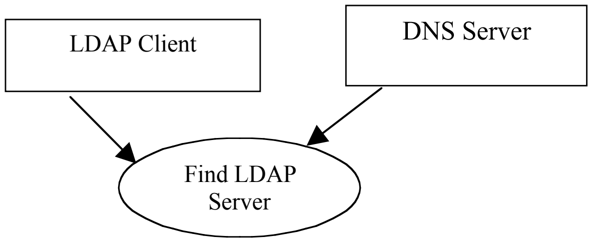

Figure X.1-3 Find LDAP Server

DNS Server	Provides list of LDAP servers
LDAP Client	Requests list of LDAP servers

X.1.4.1.3 Referenced Standards

RFC-2181	Clarifications to the DNS Specification
RFC-2219	Use of DNS Aliases for Network Services
RFC-2782	A DNS RR for specifying the location of services (DNS SRV)

other RFC's are included by reference from RFC-2181, RFC-2219, and RFC-2782.

X.1.4.1.4 Interaction Diagram

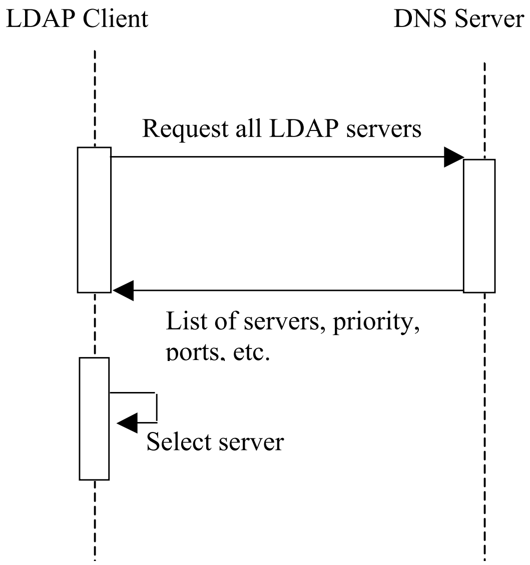

Figure X.1-4 Select LDAP Server

The DNS client shall request a list of all the LDAP servers available. It will use the priority, capacity, and location information provided by DNS to select a server. (RFC-2782 recommends the proper use of these parameters.) It is possible that there is no LDAP server, or that the DNS server does not support the SRV RR request.

Notes: 1. Multiple LDAP servers providing access to a common replicated LDAP database is a commonly supported configuration. This permits LDAP servers to be located where appropriate for best performance and fault tolerance. The DNS server response information provides guidance for selecting the most appropriate server.

2. There may also be multiple LDAP servers providing different databases. In this situation the client may have to examine several servers to find the one that supports the DICOM configuration database. Similarly a single LDAP server may support multiple base DNs, and the client will need to check each of these DNs to determine which is the DICOM supporting tree.

X.1.4.1.5 Alternative Paths

The client may have a mechanism for manual default selection of the LDAP server to be used if the DNS server does not provide an LDAP server location.

X.1.4.2 Query LDAP Server

X.1.4.2.1 Scope

The RFC-2251 “Lightweight Directory Access Protocol (v3)” specifies a mechanism for making queries of a database corresponding to an LDAP schema. The LDAP client can compose requests in the LDAP query language, and the LDAP server will respond with the results for a single request.

X.1.4.2.2 Use Case Roles

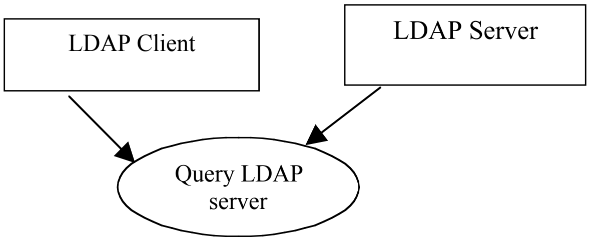

Figure X.1-5 Query LDAP Server

LDAP Server	Provides query response
LDAP Client	Requests LDAP information

X.1.4.2.3 Referenced Standards

RFC-2251 Lightweight Directory Access Protocol (v3). LDAP support requires compliance with other RFC’s invoked by reference.

X.1.4.2.4 Interaction Description

The LDAP client may make a wide variety of queries and cascaded queries using LDAP. The LDAP client and server shall support the Application Configuration Data Model .

Note: Multiple LDAP servers providing access to a common replicated LDAP database is a commonly supported configuration. This permits LDAP servers to be located where appropriate for best performance and fault tolerance. The replications rules chosen for the LDAP servers affect the visible data consistency. LDAP permits inconsistent views of the database during updates and replications.

X.1.4.3 Update LDAP Server

X.1.4.3.1 Scope

The RFC-2251 "Lightweight Directory Access Protocol (v3)" specifies a mechanism for making updates to a database corresponding to an LDAP schema. The LDAP client can compose updates in the LDAP query language, and the LDAP server will respond with the results for a single request. Update requests may be refused for security reasons.

X.1.4.3.2 Use Case Roles

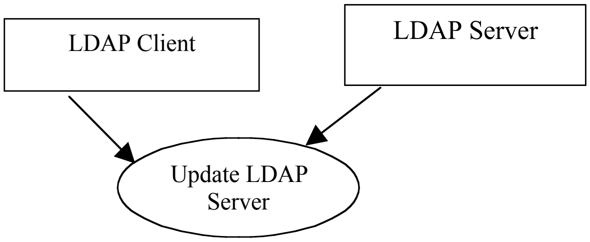

Figure X.1-6 Update LDAP Server

LDAP Server	Maintains database
LDAP Client	Updates LDAP information

X.1.4.3.3 Referenced Standards

RFC-2251 Lightweight Directory Access Protocol (v3). LDAP support requires compliance with other RFC's invoked by reference.

X.1.4.3.4 Interaction Description

The LDAP client may make a request to update the LDAP database. The LDAP client shall support the data model described above. The LDAP server may choose to refuse the update request for security reasons. If the LDAP server permits update requests, is shall support the data model described above.

Note: Multiple LDAP servers providing access to a common replicated LDAP database is a commonly supported configuration. This permits LDAP servers to be located where appropriate for best performance and fault tolerance. Inappropriate selection of replication rules in the configuration of the LDAP server will result in failure for AE-title uniqueness when creating the AE-titles objects.

X.1.4.3.5 Special Update for Network AE Creation

The creation of a new Network AE requires special action. The following steps shall be followed:

a. A tentative AE title shall be selected. Various algorithms are possible, ranging from generating a random name to starting with a preset name template and incrementing a counter field. The client may query the Unique AE Titles Registry sub-tree to obtain the complete list of names that are presently in use as part of this process.

b. A new Unique AE Title object shall be created in the Unique AE Titles Registry portion of the hierarchy with the tentative name. The LDAP server enforces uniqueness of names at any specific point in the hierarchy.

c. If the new object creation was successful, this shall be the AE Title used for the new Network AE.

d. If the new object creation fails due to non-unique name, return to a) and select another name.

X.1.4.4 Maintain LDAP Server

The LDAP server shall support a separate manual or automated means of maintaining the LDAP database contents. The LDAP server shall support the RFC-2849 file format mechanism for updating the LDAP database. The LDAP Client or service installation tools shall provide RFC-2849 formatted files to update LDAP server databases manually. The LDAP server may refuse client network updates for security reasons. If this is the case, then the maintenance process will be used to maintain the LDAP database.

The manual update procedures are not specified other than the requirement above that at least the minimal LDAP information exchange file format from RFC 2849 be supported. The exact mechanisms for transferring this information remain vendor and site specific. In some situations, for example the creation of AE-titles, a purely manual update mechanism may be easier than exchanging files.

The conformance statement shall document the mechanisms available for transferring this information. Typical mechanisms include:

a. floppy disk

b. CD-R

c. SSH

d. Secure FTP

e. FTP

f. email

g. HTTPS

Notes: 1. There are many automated and semi-automatic tools for maintaining LDAP databases. Many LDAP servers provide GUI interfaces and updating tools. The specifics of these tools are outside the scope of DICOM. The LDAP RFC-2849 requires at least a minimal data exchange capability. There are also XML based tools for creating and maintaining these files.

2. This mechanism may also be highly effective for preparing a new network installation by means of a single pre-planned network configuration setup rather than individual machine updates.

X.1.5 LDAP Security Considerations (Informative)

X.1.5.1 Threat Assessment

The threat and value for the LDAP based configuration mechanisms fall into categories:

a. AE-uniqueness mechanism

b. Finding (and updating) Network AE descriptions

c. Finding (and updating) device descriptions

These each pose different vulnerabilities to attack. These are:

a. *Active Attacks*
   1. The AE-title uniqueness mechanism could be attacked by creating vast numbers of spurious AE-titles. This could be a Denial of Service (DoS) attack on the LDAP server. It has a low probability of interfering with DICOM operations.
   2. The Network AE information could be maliciously updated. This would interfere with DICOM operations by interfering with finding the proper server. It could direct connections to malicious nodes, although the use of TLS authentication for DICOM connections would detect such misdirection. When TLS authentication is in place this becomes a DoS attack.
   3. The device descriptions could be maliciously modified. This would interfere with proper device operation.

b. *Passive Attacks*
   1. There is no apparent value to an attacker in obtaining the current list of AE-titles. This does not indicate where these AE-titles are deployed or on what equipment.
   2. The Network AE information and device descriptions might be of value in determining the location of vulnerable systems. If it is known that a particular model of equipment from a particular vendor is vulnerable to a specific attack, then the Network AE Information can be used to find that equipment.

X.1.5.2 Available LDAP Security Mechanisms

The security mechanisms for LDAP are highly variable in actual implementations. They are a mixture of administrative restrictions and protocol implementations. The widely available options for security methods are:

a. Anonymous access, where there is no restriction on performing this function over the network.
b. Basic, where there is a username and password exchange prior to granting access to this function. The exchange is vulnerable to snooping, spoofing, and man in the middle attacks.
c. TLS, where there is an SSL/TLS exchange during connection establishment.
d. Manual, where no network access is permitted and the function must be performed manually at the server, or semi-automatically at the server. The semi-automatic means permit the use of independently exchanged files (e.g. via floppy) together with manual commands at the server.

The categories of functions that may be independently controlled are:

a. Read related, to read, query, or otherwise obtain a portion of the LDAP directory tree
b. Update related, to modify previously existing objects in the directory tree
c. Create, to create new objects in the directory tree.

Finally, these rules may be applied differently to different subtrees within the overall LDAP structure. The specific details of Access Control Lists (ACLs), functional controls, etc. vary somewhat between different LDAP implementations.

X.1.5.3 Recommendations (Informative)

The LDAP server should be able to specify different restrictions for the AE-Title list and for the remainder of the configuration information. To facilitate interoperability, Table X.1-15 defines several patterns for access control. They correspond to different assessments of risk for a network environment.

Table X.1-15 LDAP Security Patterns

	TLS	**TLS-Manual**	**Basic**	**Basic-Manual**	**Anonymous**	**Anonymous-Manual**
Read AE-title	Anonymous, TLS	Anonymous, TLS	Anonymous, Basic	Anonymous, Basic	Anonymous	Anonymous
Create AE-Title	TLS	Manual	Basic	Manual	Anonymous	Manual
Read Config	TLS	TLS	Basic	Basic	Anonymous	Anonymous
Update Config	TLS	Manual	Basic	Manual	Anonymous	Manual
Create Config	TLS	Manual	Basic	Manual	Anonymous	Manual

TLS This pattern provides SSL/TLS authentication and encryption between client and server. It requires additional setup during installation because the TLS certificate information needs to be installed onto the client machines and server. Once the certificates are installed the clients may then perform full updating operations.

TLS-Manual

This pattern provides SSL/TLS controls for read access to information and require manual intervention to perform update and creation functions.

Basic This pattern utilizes the LDAP basic security to gain access to the LDAP database. It requires the installation of a password during client setup. It does not provide encryption protection. Once the password is installed, the client can then perform updates.

Basic-Manual

This pattern utilizes basic security protection for read access to the configuration information and requires manual intervention to perform update and creation functions.

Anonymous

This pattern permits full read/update access to all machines on the network.

Anonymous-Manual

This pattern permits full read access to all machines on the network, but requires manual intervention to perform update and creation.

A client or server implementation may be capable of being configured to support multiple patterns. This should be documented in the conformance claim. The specific configuration in use at a specific site can then be determined at installation time.

X.1.6 Implementation Considerations (Informative)

The LDAP database can be used as a documentation tool. Documenting the configuration for both managed and legacy machines makes upgrading easier and reduces the error rate for manually configured legacy equipment.

There are various possible implementation strategies for clients performing lookups within the LDAP database. For example, before initiating a DICOM association to a specific AE, a client implementation could either:

a. Query the LDAP database to obtain hostname and port for the specific AE Title immediately prior to initiating a DICOM association.

b. Maintain a local cache of AE Title, hostname and port information and only query the LDAP database if the specific AE Title is not found in the local cache.

The advantages of maintaining a local cache include performance (by avoiding frequent lookups) and reliability (should the LDAP server be temporarily unavailable). The disadvantage of a cache is that it can become outdated over time. Client implementations should provide appropriate mechanisms to purge locally cached information.

Client caches may cause confusion during updates. Manual steps may be needed to trigger immediate updates. LDAP database replication also may introduce delays and inconsistencies. Database replication may also require manual intervention to force updates to occur immediately.

One strategy to reduce client cache problems is to re-acquire new DNS and LDAP information after any network association information. Often the first symptom of stale cache information is association failures due to the use of obsolete configuration information.

Some LDAP servers do not support a “modify DN” operation. For example, in the case of renaming a device on such a server, a tree copy operation may be needed to create a new object tree using the new name, followed by removal of the old object tree. After such a rename the device may need to search using other attributes when finding its own configuration information, e.g. the device serial number.

X.1.7 Conformance

The Conformance Statement for an LDAP Client or LDAP Server implementation shall specify the security pattern(s) that it supports.

Add Annexes Y and Z for Configuration Profiles to Part 15

Annex Y Configuration Use Cases (Informative)

The following use cases are the basis for the decisions made in defining the profiles specified in Annexes V, W, and X. Where possible specific protocols that are commonly used in IT system management are specifically identified.

Y.1 INSTALL A NEW MACHINE

When a new machine is added there need to be new entries made for:

a. TCP/IP parameters
b. DICOM Application Entity related Parameters

The service staff effort needed for either of these should be minimal. To the extent feasible these parameters should be generated and installed automatically.

The need for some sort of ID is common to most of the use cases, so it is assumed that each machine has sufficient non-volatile storage to at least remember its own name for later use.

Updates may be made directly to the configuration databases or made via the machine being configured. A common procedure for large networks is for the initial network design to assign these parameters and create the initial databases during the complete initial network design. Updates can be made later as new devices are installed.

One step that specifically needs automation is the allocation of AE-titles. These must be unique. Their assignment has been a problem with manual procedures. Possibilities include:

a. Fully automatic allocation of AE-titles as requested. This interacts with the need for AE title stability in some use cases. The automatic process should permit AE-titles to be persistently associated with particular devices and application entities. The automatic process should permit the assignment of AE titles that comply with particular internal structuring rules.
b. Assisted manual allocation, where the service staff proposes AE-titles (perhaps based on examining the list of present AE-titles) and the system accepts them as unique or rejects them when non-unique.

These AE-titles can then be associated with the other application entity related information. This complete set of information needs to be provided for later uses.

The local setup may also involve searches for other AE's on the network. For example, it is likely that a search will be made for archives and printers. These searches might be by SOP class or device type. This is related to vendor specific application setup procedures which are outside the scope of DICOM.

Y.1.1 Configure DHCP

The network may have been designed in advance and the configuration specified in advance. It should be possible to preconfigure the configuration servers prior to other hardware installation. This should not preclude later updates or later configuration at specific devices.

The DHCP servers have a database that is manually maintained defining the relationship between machine parameters and IP parameters. This defines:

a. Hardware MAC addresses that are to be allocated specific fixed IP information.
b. Client machine names that are to be allocated specific fixed IP information.
c. Hardware MAC addresses and address ranges that are to be allocated dynamically assigned IP addresses and IP information.
d. Client machine name patterns that are to be allocated dynamically assigned IP addresses and IP information.

The IP information that is provided will be a specific IP address together with other information. The present recommendation is to provide all of the following information when available.

The manual configuration of DHCP is often assisted by automated user interface tools that are outside the scope of DICOM.   Some people utilize the DHCP database as a documentation tool for documenting the assignment of IP addresses that are preset on equipment. This does not interfere with DHCP operation and can make a gradual transition from equipment presets to DHCP assignments easier. It also helps avoid accidental re-use of IP addresses that are already manually assigned. However, DHCP does not verify that these entries are in fact correct.

Y.1.2 Configure LDAP

There are several ways that the LDAP configuration information can be obtained.

a. A complete installation may be pre-designed and the full configuration loaded into the LDAP server, with the installation attribute set to false. Then as systems are installed, they acquire their own configurations from the LDAP server. The site administration can set the installation attribute to true when appropriate.
b. When the LDAP server permits network clients to update the configuration, they can be individually installed and configured. Then after each device is configured, that device uploads its own configuration to the LDAP server.
c. When the LDAP server does not permit network clients to update configurations, they can be individually installed and configured. Then, instead of uploading their own configuration, they create a standard format file with their configuration objects. This file is then manually added to the LDAP server (complying with local security procedures) and any conflicts resolved manually.

Y.1.2.1 Pre-configure

The network may have been designed in advance and the configuration specified in advance. It should be possible to preconfigure the configuration servers prior to other hardware installation. This should not preclude later updates or later configuration at specific devices.

LDAP defines a standard file exchange format for transmitting LDAP database subsets in an ASCII format. This file exchange format can be created by a variety of network configuration tools. There are also systems that use XML tools to create database subsets that can be loaded into LDAP servers. It is out of scope to specify these tools in any detail. The use case simply requires that such tools be available.

When the LDAP database is preconfigured using these tools, it is the responsibility of the tools to ensure that the resulting database entries have unique names. The unique name requirement is common to any LDAP database and not just to DICOM AE-titles. Consequently, most tools have mechanisms to ensure that the database updates that they create do have unique names.

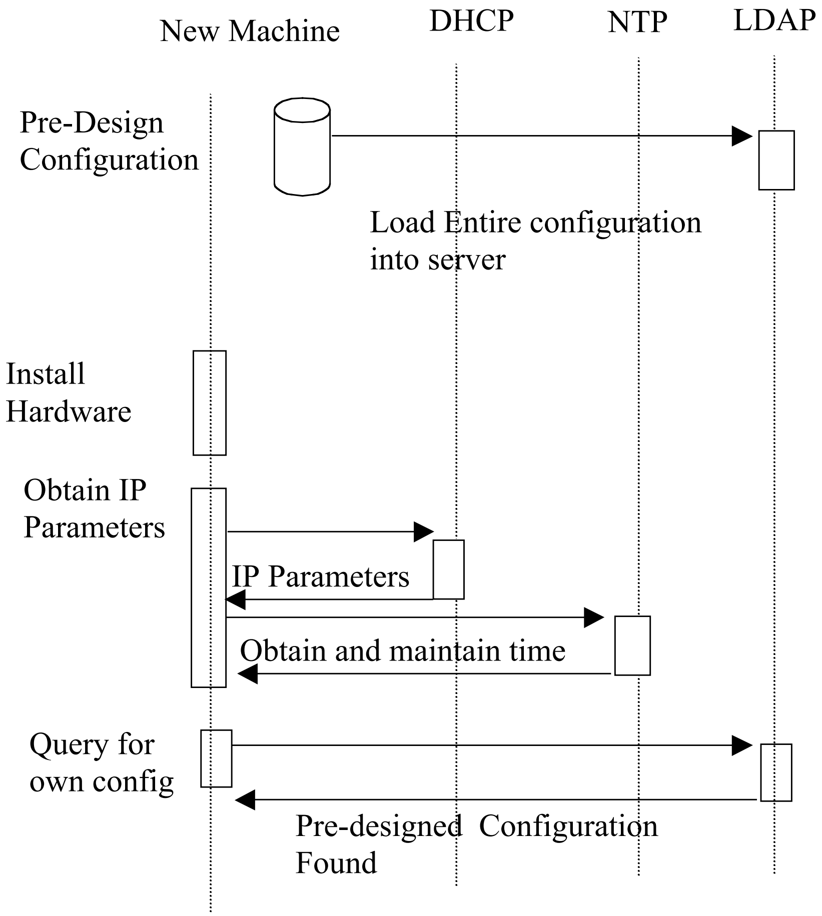

Figure Y.1-1 System Installation with Pre-configured Configuration

At an appropriate time, the installed attribute is set on the device objects in the LDAP configuration.

Y.1.2.2 Updating configuration during installation

The "unconfigured" device startup begins with use of the pre-configured services from DHCP, DNS, and NTP. It then performs device configuration and updates the LDAP database. This description assumes that the device has been given permission to update the LDAP database directly.

a. DHCP is used to obtain IP related parameters. The DHCP request can indicate a desired machine name that DHCP can associate with a configuration saved at the DHCP server. DHCP does not guarantee that the desired machine name will be granted because it might already be in use, but this mechanism is often used to maintain specific machine configurations. The DHCP will also update the DNS server (using the DDNS mechanisms) with the assigned IP address and hostname information.

   Legacy note: A machine with preconfigured IP addresses, DNS servers, and NTP servers may skip this step. As an operational and documentation convenience, the DHCP server database may contain the description of this preconfigured machine.

b. The list of NTP servers is used to initiate the NTP process for obtaining and maintaining the correct time. This is an ongoing process that continues for the duration of device activity. See Time Synchronization below.

c. The list of DNS servers is used to obtain the address of the DNS servers at this site. Then the DNS servers are queried to get the list of LDAP servers. This utilizes a relatively new addition to the DNS capabilities that permit querying DNS to obtain servers within a domain that provide a particular service.

d. The LDAP servers are queried to find the server that provides DICOM configuration services, and then obtain a description for the device matching the assigned machine name. This description includes device specific configuration information and a list of Network AEs. For the unconfigured device there will be no configuration found.

Note: These first four steps are the same as a normal startup (described below).

e. Through a device specific process it determines its internal AE structure. During initial device installation it is likely that the LDAP database lacks information regarding the device. Using some vendor specific mechanism, e.g. service procedures, the device configuration is obtained. This device configuration includes all the information that will be stored in the LDAP database. The fields for “device name” and “AE Title” are tentative at this point.

f. Each of the Network AE objects is created by means of the LDAP object creation process. It is at this point that LDAP determines whether the AE Title is in fact unique among all AE Titles. If the title is unique, the creation succeeds. If there is a conflict, the creation fails and “name already in use” is given as a reason.

   LDAP uses propose/create as an atomic operation for creating unique items. The LDAP approach permits unique titles that comply with algorithms for structured names, check digits, etc. DICOM does not require structured names, but they are a commonplace requirement for other LDAP users. It may take multiple attempts to find an unused name.

   This multiple probe behavior can be a problem if “unconfigured device” is a common occurrence and name collisions are common. Name collisions can be minimized at the expense of name structure by selecting names such as “AExxxxxxxxxxxxxx” where “xxxxxxxxxxxxxx” is a truly randomly selected number. The odds of collision are then exceedingly small, and a unique name will be found within one or two probes.

g. The device object is created. The device information is updated to reflect the actual AE titles of the AE objects. As with AE objects, there is the potential for device name collisions.

h. The network connection objects are created as subordinates to the device object.

i. The AE objects are updated to reflect the names of the network connection objects.

The “unconfigured device” now has a saved configuration. The LDAP database reflects its present configuration.

In the following example, the new system needs two AE-titles. During its installation another machine is also being installed and takes one of the two AE-titles that the first machine expected to use. The new system then claims another different AE-title that does not conflict.

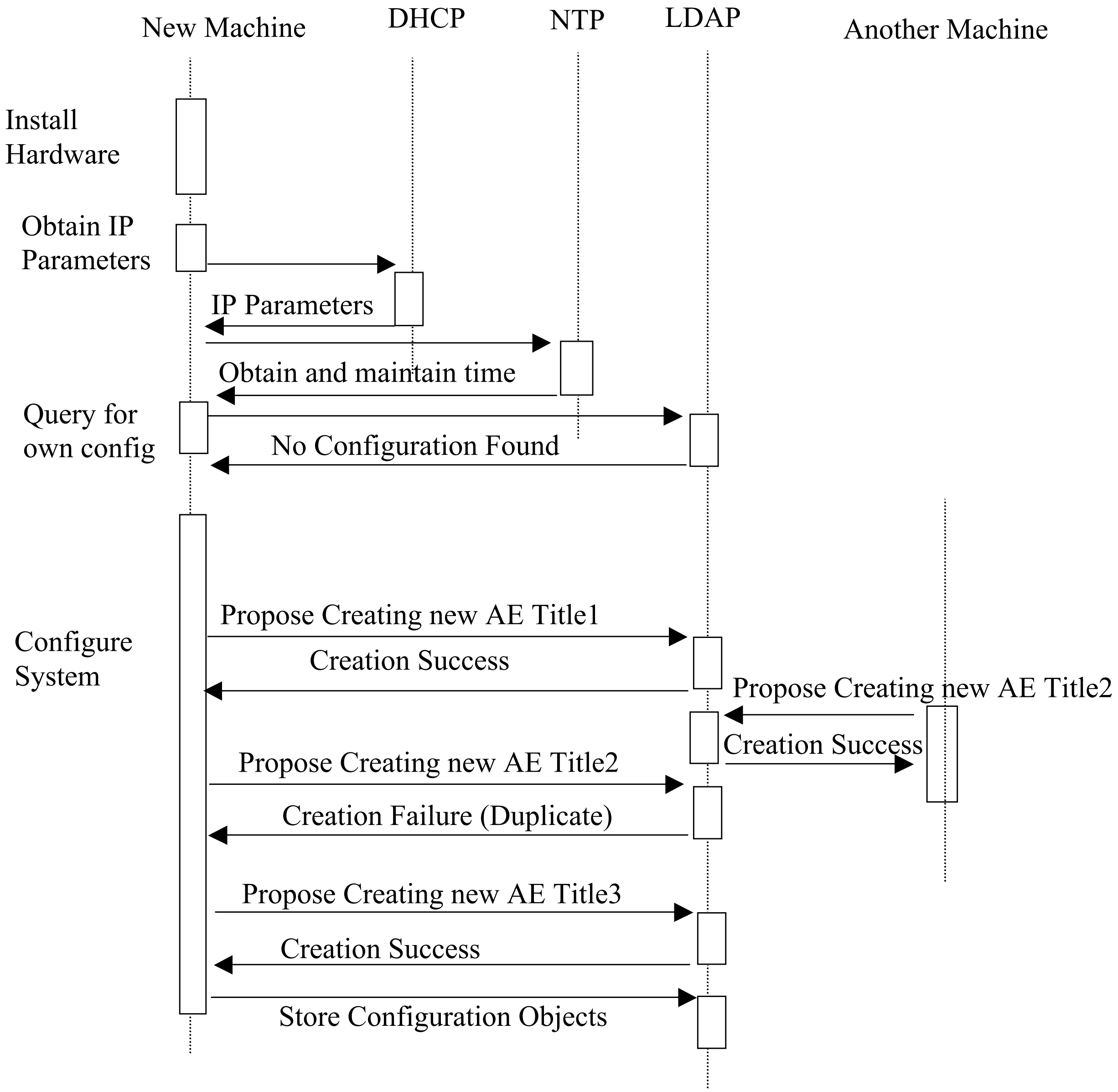

Figure Y.1-2 – Configuring a System when network LDAP updates are permitted

Y.1.2.3 Configure Client then update Server

Much of the initial startup is the same for restarting a configured device and for configuring a client first and then updating the server. The difference is two-fold.

The AE-title uniqueness must be established manually, and the configuration information saved at the client onto a file that can then be provided to the LDAP server. There is a risk that the manually assigned

AE-title is not unique, but this can be managed and is easier than the present entirely manual process for assigning AE-titles.

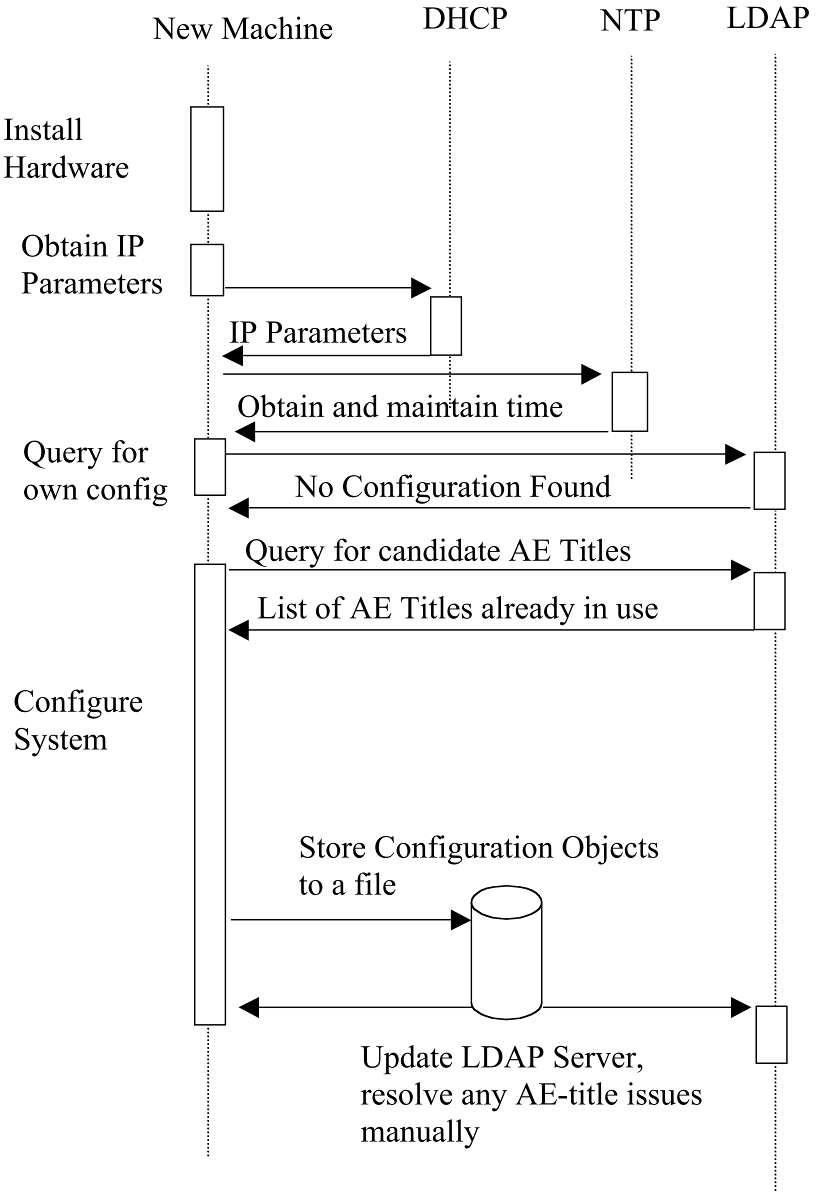
New Machine
DHCP
NTP
LDAP
Install Hardware
Obtain IP Parameters
IP Parameters
Obtain and maintain time
Query for own config
No Configuration Found
Query for candidate AE Titles
List of AE Titles already in use
Configure System
Store Configuration Objects to a file
Update LDAP Server, resolve any AE-title issues manually

Figure Y.1-3 Configuring a system when LDAP network updates are not permitted

Y.1.3 Distributed update propagation

The larger enterprise networks require prompt database responses and reliable responses during network disruptions. This implies the use of a distributed or federated database. These have update propagation issues. There is not a requirement for a complete and accurate view of the DICOM network at all times. There is a requirement that local subsets of the network maintain an accurate local view. E.g., each hospital in a large hospital chain may tolerate occasional disconnections or problems in viewing the network information in other hospitals in that chain, but they require that their own internal network be reliably and accurately described.

LDAP supports a variety of federation and distribution schemes. It specifically states that it is designed and appropriate for federated situations where distribution of updates between federated servers may be slow. It is specifically designed for situations where database updates are infrequent and database queries dominate.

Y.2 LEGACY COMPATIBILITY

Legacy devices utilize some internal method for obtaining the IP addresses, port numbers, and AE-titles of the other devices. For legacy compatibility, a managed node must be controlled so that the IP addresses, port numbers, and AE-titles do not change. This affects DHCP because it is DHCP that assigns IP addresses. The LDAP database design must preserve port number and AE-title so that once the device is configured these do not change.

DHCP was designed to deal with some common legacy issues:

a. Documenting legacy devices that do not utilize DHCP. Most DHCP servers can document a legacy device with a DHCP entry that describes the device. This avoids IP address conflicts. Since this is a manual process, there still remains the potential for errors. The DHCP server configuration is used to reserve the addresses and document how they are used.

   This documented entry approach is also used for complex multi-homed servers. These are often manually configured and kept with fixed configurations.

b. Specifying fixed IP addresses for DHCP clients. Many servers have clients that are not able to use DNS to obtain server IP addresses. These servers may also utilize DHCP for startup configuration. The DHCP servers must support the use of fixed IP allocations so that the servers are always assigned the same IP address. This avoids disrupting access by the server’s legacy clients.

   This usage is quite common because it gives the IT administrators the centralized control that they need without disrupting operations. It is a frequent transitional stage for machines on networks that are transitioning to full DHCP operation.

There are two legacy-related issues with time configuration:

a. The NTP system operates in UTC. The device users probably want to operate in local time. This introduces additional internal software requirements to configure local time. DHCP will provide this information if that option is configured into the DHCP server.
b. Device clock setting must be documented correctly. Some systems set the battery-powered clock to local time; others use UTC. Incorrect settings will introduce very large time transient problems during startup. Eventually NTP clients do resolve the huge mismatch between battery clock and NTP clock, but the device may already be in medical use by the time this problem is resolved. The resulting time discontinuity can then pose problems. The magnitude of this problem depends on

the particular NTP client implementation.

Y.3 OBTAIN CONFIGURATION OF OTHER DEVICES

Managed devices can utilize the LDAP database during their own installation to establish configuration parameters such as the AE-title of destination devices. They may also utilize the LDAP database to obtain this information at run time prior to association negotiation.

Y.3.1 Find AE When Given Device Type

The LDAP server supports simple relational queries. This query can be phrased:

```
Return devices where
DeviceType == <device type>

Then, for each of those devices, query

Return Network AE where
[ApplicationCluster == name]
```

The result will be the Network AE entries that match those two criteria. The first criteria selects the device type match. There are LDAP scoping controls that determine whether the queries search the entire enterprise or just this server. LDAP does not support complex queries, transactions, constraints, nesting, etc. LDAP cannot provide the hostnames for these Network AEs as part of a single query. Instead, the returned Network AEs will include the names of the network connections for each Network AE. Then the application would need to issue LDAP reads using the DN of the NetworkConnection objects to obtain the hostnames.

Y.4 DEVICE STARTUP

Normal startup of an already configured device will obtain IP information and DICOM information from the servers.

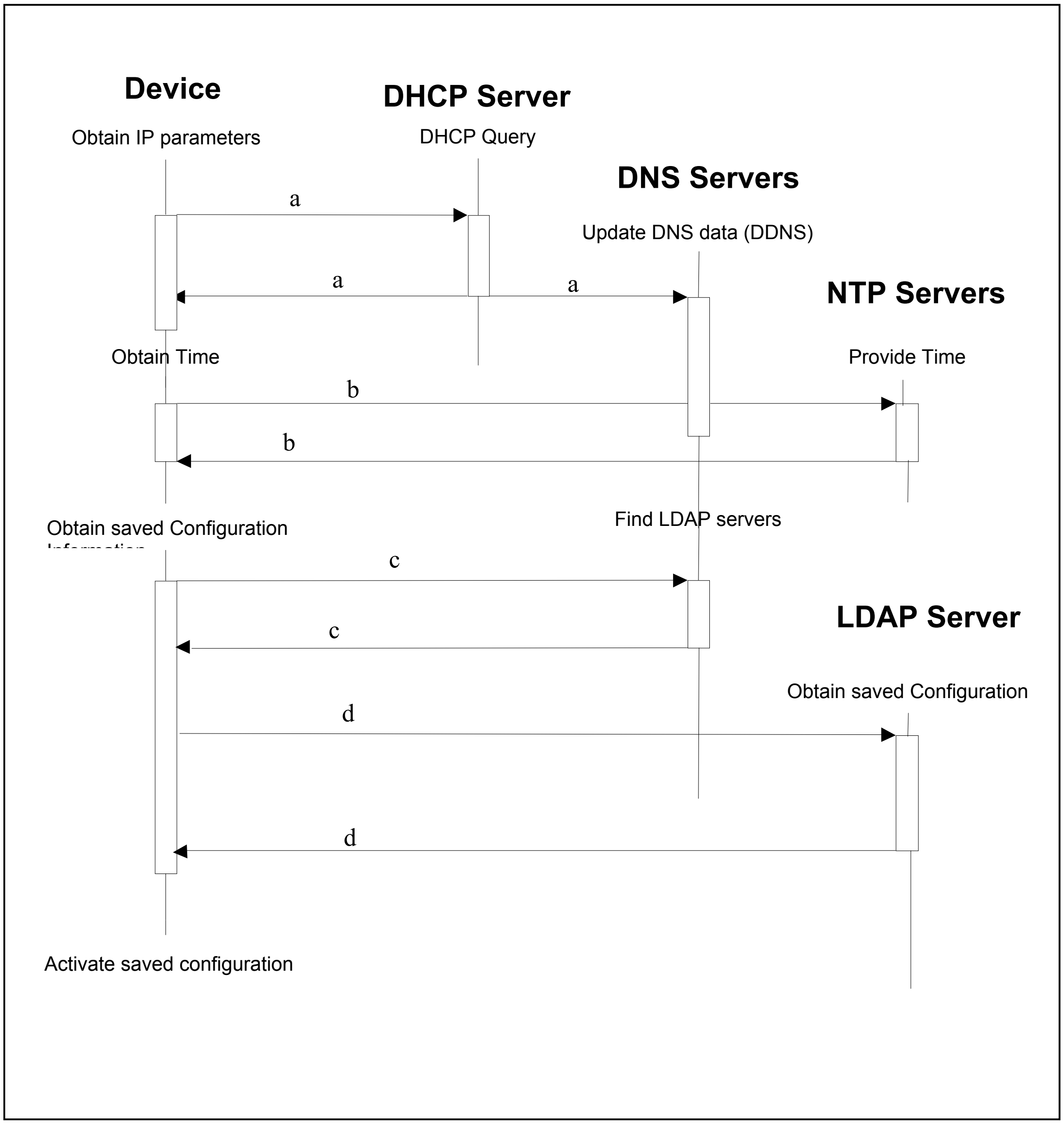

Figure Y.4–1 Configured Device Startup (Normal Startup)

The device startup sequence is:

a. DHCP is used to obtain IP related parameters. The DHCP request can indicate a desired machine name that DHCP can associate with a configuration saved at the DHCP server. DHCP does not guarantee that the desired machine name will be granted because it might already be in use, but this mechanism is often used to maintain specific machine configurations. The DHCP will also update the DNS server (using the DDNS mechanisms) with the assigned IP address and hostname information.

Legacy note: A machine with preconfigured IP addresses, DNS servers, and NTP servers may skip this step. As an operational and documentation convenience, the DHCP server database may contain the description of this preconfigured machine.

b. The list of NTP servers is used to initiate the NTP process for obtaining and maintaining the correct time. This is an ongoing process that continues for the duration of device activity. See Time Synchronization below.

c. The list of DNS servers is used to obtain the list of LDAP servers. This utilizes a relatively new addition to the DNS capabilities that permit querying DNS to obtain servers within a domain that provide a particular service.

d. The "nearest" LDAP server is queried to obtain a description for the device matching the assigned machine name. This description includes device specific configuration information and a list of Network AEs.

Note: A partially managed node may reach this point and discover that there is no description for that device in the LDAP database. During installation (as described above) this may then proceed into device configuration. Partially managed devices may utilitze an internal configuration mechanism.

e. The AE descriptions are obtained from the LDAP server. Key information in the AE description is the assigned AE-title. The AE descriptions probably include vendor unique information in either the vendor text field or vendor extensions to the AE object. The details of this information are vendor unique. DICOM is defining a mandatory minimum capability because this will be a common need for vendors that offer dynamically configurable devices.

The AE description may be present even for devices that do not support dynamic configuration. If the device has been configured with an AE-title and description that is intended to be fixed, then a description should be present in the LDAP database. The device can confirm that the description matches its stored configuration. The presence of the AE-title in the description will prevent later network activities from inadvertently re-using the same AE-title for another purpose.

The degree of configurability may also vary. Many simple devices may only permit dynamic configuration of the IP address and AE-title, with all other configuration requiring local service modifications.

f. The device performs whatever internal operations are involved to configure itself to match the device description and AE descriptions.

At this point, the device is ready for regular operation, the DNS servers will correctly report its IP address when requested, and the LDAP server has a correct description of the device, Network AEs, and network connections.

Y.5 SHUTDOWN

Y.5.1 Shutdown

The lease timeouts eventually release the IP address at DHCP, which can then update DNS to indicate that the host is down. Clients that utilize the hostname information in the LDAP database will initially experience reports of connection failure; and then after DNS is updated, they will get errors indicating the device is down when they attempt to use it. Clients that use the IP entry directly will experience reports of connection failure.

Y.5.2 Online/Offline

A device may be deliberately placed offline in the LDAP database to indicate that it is unavailable and will remain unavailable for an extended period of time. This may be utilized during system installation so that preconfigured systems can be marked as offline until the system installation is complete. It can also be used for systems that are down for extended maintenance or upgrades. It may be useful for equipment that is on mobile vans and only present for certain days.

For this purpose a separate Installed attribute has been given to devices, Network AE's, and Network Connections so that it can be manually managed.

Y.6 TIME SYNCHRONIZATION

Medical device time requirements primarily deal with synchronization of machines on a local network or campus. There are very few requirements for accurate time (synchronized with an international reference clock). DICOM time users are usually concerned with:

a. local time synchronization between machines
b. local time base stability. This means controlling the discontinuities in the local time and its first derivative. There is also an upper bound on time base stability errors that results from the synchronization error limits.
c. international time synchronization with the UTC master clocks

Other master clocks and time references (e.g. sidereal time) are not relevant to medical users.

Y.6.1 High accuracy time synchronization

High accuracy time synchronization is needed for devices like cardiology equipment. The measurements taken on various different machines are recorded with synchronization modules specifying the precise time base for measurements such as waveforms and multi-frame images. These are later used to synchronize data for analysis and display.

Typical requirements are:

Local synchronization

Synchronized to within approximately 10 millisecond. This corresponds to a few percent of a typical heartbeat. Under some circumstances, the requirements may be stricter than this.

Time base stability

During the measurement period there should be no discontinuities greater than a few milliseconds. The time base rate should be within 0.01% of standard time rate.

International Time Synchronization

There are no special extra requirements. Note however that time base stability conflicts with time synchronization when UTC time jumps (e.g. leap seconds).

Y.6.2 Ordinary Time Synchronization

Ordinary medical equipment uses time synchronization to perform functions that were previously performed manually, e.g. recordkeeping and scheduling. These were typically done using watches and clocks, with resultant stability and synchronization errors measured in seconds or longer. The most stringent time synchronization requirements for networked medical equipment derive from some of the security protocols and their record keeping.

Ordinary requirements are:

Local synchronization

Synchronized to within approximately 500 milliseconds. Some security systems have problems when the synchronization error exceeds 1 second.

Time base stability

Large drift errors may cause problems. Typical clock drift errors approximately 1 second/day are unlikely to cause problems. Large discontinuities are permissible if rare or during startup. Time may run backwards, but only during rare large discontinuities.

International Time Synchronization

Some sites require synchronization to within a few seconds of UTC. Others have no requirement.

Y.6.3 Background

Y.6.3.1 Unsynchronized Time

The local system time of a computer is usually provided by two distinct components.

a. There is a battery-powered clock that is used to establish an initial time estimate when the machine is turned on. These clocks are typically very inaccurate. Local and international synchronization errors are often 5-10 minutes. In some cases, the battery clock is incorrect by hours or days.

b. The ongoing system time is provided by a software function and a pulse source. The pulse source “ticks” at some rate between 1-1000Hz. It has a nominal tick rate that is used by the system software. For every tick the system software increments the current time estimate appropriately. E.g., for a system with a 100Hz tick, the system time increments 10ms each tick.

This lacks any external synchronization and is subject to substantial initial error in the time estimate and to errors due to systematic and random drift in the tick source. The tick sources are typically low cost quartz crystal based, with a systematic error up to approximately 10^{-5} in the actual versus nominal tick rate and with a variation due to temperature, pressure, etc. up to approximately 10^{-5}. This corresponds to drifts on the order of 10 seconds per day.

Y.6.3.2 Network Synchronized Time

There is a well established Internet protocol (NTP) for maintaining time synchronization that should be used by DICOM. It operates in several ways.

The most common is for the computer to become an NTP client of one or more NTP servers. As a client it uses occasional ping-pong NTP messages to:

a. Estimate the network delays. These estimates are updated during each NTP update cycle.

b. Obtain a time estimate from the server. Each estimate includes the server’s own statistical characteristics and accuracy assessment of the estimate.

c. Use the time estimates from the servers, the network delay estimates, and the time estimates from the local system clock, to obtain a new NTP time estimate. This typically uses modern statistical methods and filtering to perform optimal estimation.

d. Use the resulting time estimate to

   1. Adjust the system time, and

2. Update drift and statistical characteristics of the local clock.

The local applications do not normally communicate with the NTP client software. They normally continue to use the system clock services. The NTP client software adjusts the system clock. The NTP standard defines a nominal system clock service as having two adjustable parameters:

a. The clock frequency. In the example above, the nominal clock was 100Hz, with a nominal increment of 10 milliseconds. Long term measurement may indicate that the actual clock is slightly faster and the NTP client can adjust the clock increment to be 9.98 milliseconds.
b. The clock phase. This adjustment permits jump adjustments, and is the fixed time offset between the internal clock and the estimated UTC.

The experience with NTP in the field is that NTP clients on the same LAN as their NTP server will maintain synchronization to within approximately 100 microseconds. NTP clients on the North American Internet and utilizing multiple NTP servers will maintain synchronization to within approximately 10 milliseconds.

There are low cost devices with only limited time synchronization needs. NTP has been updated to include SNTP for these devices. SNTP eliminates the estimation of network delays and eliminates the statistical methods for optimal time estimation. It assumes that the network delays are nil and that each NTP server time estimate received is completely accurate. This reduces the development and hardware costs for these devices. The computer processing costs for NTP are insignificant for a PC, but may be burdensome for very small devices. The SNTP synchronization errors are only a few milliseconds in a LAN environment. They are very topology sensitive and errors may become huge in a WAN environment.

Most NTP servers are in turn NTP clients to multiple superior servers and peers. NTP is designed to accommodate a hierarchy of server/clients that distributes time information from a few international standard clocks out through layers of servers.

Y.6.3.3 External Clocks

The NTP implementations anticipate the use of three major kinds of external clock sources:

External NTP servers

Many ISPs and government agencies offer access to NTP servers that are in turn synchronized with the international standard clocks. This access is usually offered on a restricted basis.

External clock broadcasts

The US, Canada, Germany, and others offer radio broadcasts of time signals that may be used by local receivers attached to an NTP server. The US and Russia broadcast time signals from satellites, e.g. GPS. Some mobile telephone services broadcast time signals. These signals are synchronized with the international standard clocks. GPS time signals are popular worldwide time sources. Their primary problem is difficulties with proper antenna location and receiver cost. Most of the popular low cost consumer GPS systems save money by sacrificing the clock accuracy.

External pulse sources

For extremely high accuracy synchronization, atomic clocks can be attached to NTP servers. These clocks do not provide a time estimate, but they provide a pulse signal that is known to be extremely accurate. The optimal estimation logic can use this in combination with other external sources to achieve sub microsecond synchronization to a reference clock even when the devices are separated by the earth's diameter.

The details regarding selecting an external clock source and appropriate use of the clock source are outside the scope of the NTP protocol. They are often discussed and documented in conjunction with the NTP protocol and many such interfaces are included in the reference implementation of NTP.

Y.6.4 SNTP restrictions

In theory, servers can be SNTP servers and NTP servers can be SNTP clients of other servers. This is very strongly discouraged. The SNTP errors can be substantial, and the clients of a server using SNTP will not have the statistical information needed to assess the magnitude of these errors. It is feasible for SNTP clients to use NTP servers. The SNTP protocol packets are identical to the NTP protocol packets. SNTP differs in that some of the statistical information fields are filled with nominal SNTP values instead of having actual measured values.

Y.6.5 Implementation Considerations

There are several public reference implementations of NTP server and client software available. These are in widespread use and have been ported to many platforms (including Unix, Windows, and Macintosh). There are also proprietary and built-in NTP services for some platforms (e.g. Windows 2000). The public reference implementations include sample interfaces to many kinds of external clock sources.

There are significant performance considerations in the selection of locations for servers and clients. Devices that need high accuracy synchronization should probably be all on the same LAN together with an NTP server on that LAN.

Real time operating system (RTOS) implementations may have greater difficulties. The reference NTP implementations have been ported to several RTOSs. There were difficulties with the implementations of the internal system clock on the RTOS. The dual frequency/phase adjustment requirements may require the clock functions to be rewritten. The reference implementations also require access to a separate high resolution interval timer (with sub microsecond accuracy and precision). This is a standard CPU feature for modern workstation processors, but may be missing on low end processors.

An RTOS implementation with only ordinary synchronization requirements might choose to write their own SNTP only implementation rather than use the reference NTP implementation. The SNTP client is very simple. It may be based on the reference implementation or written from scratch. The operating system support needed for accurate adjustment is optional for SNTP clients. The only requirement is the time base stability requirement, which usually implies the ability to specify fractional seconds when setting the time.

The conflict between the user desire to use local time and the NTP use of UTC must be resolved in the device. DHCP offers the ability to obtain the offset between local time and UTC dynamically, provided the DHCP server supports this option. There remain issues such as service procedures, startup in the absence of DHCP, etc.

The differences between local time, UTC, summer time, etc. are a common source of confusion and errors setting the battery clock. The NTP algorithms will eventually resolve these errors, but the final convergence on correct time may be significantly delayed. The device might be ready for medical use before these errors are resolved.

Annex Z Legacy Transition for Configuration Management (Informative)

There will usually be a period of time where a network will have some applications that utilize the configuration management protocols coexisting with applications that are only manually configured. The transition issues arise when a legacy Association Requestor interacts with a managed Association Acceptor or when a managed Association Requestor interacts with a legacy Association Acceptor. Some of these issues also arise when the Association Requestor and Association Acceptor support different configuration management profiles. These are discussed below and some general recommendations made for techniques that simplify the transition to a fully configuration managed network.

Z.1 LEGACY ASSOCIATION REQUESTOR, CONFIGURATION MANAGED ASSOCIATION ACCEPTOR

The legacy Association Requestor requires that the IP address of the Association Acceptor not change dynamically because it lacks the ability to utilize DNS to obtain the current IP address of the Association Acceptor. The legacy Association Requestor also requires that the AE-title of the Association Acceptor be provided manually.

Z.1.1 DHCP Server

The DHCP server should be configurable with a database of hostname, IP, and MAC address relationships. The DHCP server can be configured to provide the same IP address every time that a particular machine requests an IP address. This is a common requirement for Association Acceptors that obtain IP addresses from DHCP. The Association Acceptor may be identified by either the hardware MAC address or the hostname requested by the Association Acceptor.

The IP address can be permanently assigned as a static IP address so that legacy Association Requestor can be configured to use that IP address while managed Association Requestor can utilize the DNS services to obtain its IP address.

Z.1.2 DNS Server

No specific actions are needed, although see below for the potential that the DHCP server does not perform DDNS updates.

Z.1.3 LDAP Server

Although the managed Association Acceptor may obtain information from the LDAP server, the legacy Association Requestor will not. This means that the legacy mechanisms for establishing AE-Titles and related information on the Association Requestor will need to be coordinated manually. Most LDAP products have suitable GUI mechanisms for examining and updating the LDAP database. These are not specified by this standard.

An LDAP entry for the Association Requestor should be manually created, although this may be a very abbreviated entry. It is needed so that the AE-Title mechanisms can maintain unique AE-titles. There must be entries created for each of the AEs on the legacy Association Requestor.

The legacy Association Requestor will need to be configured based on manual examination of the LDAP information for the server and using the legacy procedures for that Association Requestor.

Z.2 MANAGED ASSOCIATION REQUESTOR, LEGACY ASSOCIATION ACCEPTOR

Z.2.1 DHCP Server

The DHCP server may need to be configured with a pre-assigned IP address for the Association Requestor if the legacy Association Acceptor restricts access by IP addresses. Otherwise no special actions are needed.

Z.2.2 DNS Server

The legacy Association Acceptor hostname and IP address should be manually placed into the DNS database.

Z.2.3 LDAP Server

The LDAP server should be configured with a full description of the legacy Association Acceptor, even though the Association Acceptor itself cannot provide this information. This will need to be done manually, most likely using GUI tools. The legacy Association Acceptor will need to be manually configured to match the AE-Titles and other configuration information.

Z.3 NO DDNS SUPPORT

In the event that the DHCP server or DNS server do not support or permit DDNS updates, then the DNS server database will need to be manually configured. Also, because these updates are not occurring, all of the machines should have fixed pre-assigned IP addresses. This is not strictly necessary for clients, since they will not have incoming DICOM connections, but may be needed for other reasons. In practice maintaining this file is very similar to the maintenance of the older hostname files. There is still a significant administrative gain because only the DNS and DHCP configuration files need to be maintained, instead of maintaining files on each of the servers and clients

Z.4 PARTIALLY MANAGED DEVICES

It is likely that some devices will support only some of the system management profiles. A typical example of such partial support is a node that supports:

a. DHCP Client,
b. DNS Client, and
c. NTP Client

Configurations like this are common because many operating system platforms provide complete tools for implementing these clients. The support for LDAP Client requires application support and is often released on a different cycle than the operating system support. These devices will still have their DICOM application manually configured, but will utilize the DHCP, DNS, and NTP services.

Z.5 ADDING THE FIRST MANAGED DEVICE TO A LEGACY NETWORK

The addition of the first fully managed device to a legacy network requires both server setup and device setup.

Z.5.1 New Servers required

The managed node requires that servers be installed or assigned to provide the following actors:

a. DHCP Server

b. DNS Server
c. NTP Server
d. LDAP Server

These may be existing servers that need only administrative additions, they may be existing hardware that has new software added, and these may be one or multiple different systems. DHCP, DNS, and NTP services are provided by a very wide variety of equipment.

Z.5.2 NTP

The NTP server location relative to this device should be reviewed to be sure that it meets the timing requirements of the device. If it is an NTP client with a time accuracy requirement of approximately 1 second, almost any NTP server location will be acceptable. For SNTP clients and devices with high time accuracy requirements, it is possible that an additional NTP server or network topology adjustment may be needed.

If the NTP server is using secured time information, certificates or passwords may need to be exchanged.

Z.5.3 Documenting Managed and Unmanaged Nodes (DHCP, DNS, and LDAP)

Z.5.3.1 DHCP Documentation

There are advantages to documenting the unmanaged nodes in the DHCP database. This is not critical for operations, but it helps avoid administrative errors. Most DHCP servers support the definition of pre-allocated static IP addresses. The unmanaged nodes can be documented by including entries for static IP addresses for the unmanaged nodes. These nodes will not be using the DHCP server initially, but having their entries in the DHCP database helps reduce errors and simplifies gradual transitions. The DHCP database can be used to document the manually assigned IP addresses in a way that avoids unintentional duplication.

The managed node must be documented in the DHCP database. The NTP and DNS server locations must be speciified.

If this device is an association acceptor it probably should be assigned a fixed IP address. Many legacy devices cannot operate properly when communicating with devices that have dynamically assigned IP addresses. The legacy device does not utilize the DNS system, so the DDNS updates that maintain the changing IP address are not available. So most managed nodes that are association acceptors must be assigned a static IP address. The DHCP system still provides the IP address to the device during the boot process, but it is configured to always provide the same IP address every time. The legacy systems are configured to use that IP address.

Z.5.3.2 DNS Documentation

Most DNS servers have a database for hostname to IP relationships that is similar to the DHCP database. The unmanaged devices that will be used by the managed node must have entries in this database so that machine IP addresses can be found. It is often convenient to document all of the hostnames and IP addresses for the network into the DNS database. This is a fairly routine administrative task and can be done for the entire network and maintained manually as devices are added, moved, or removed. There are many administrative tools that expect DNS information about all network devices, and this makes that information available.

If DDNS updates are being used, the manually maintained portion of the DNS database must be adjusted to avoid conflicts.

There must be DNS entries provided for every device that will be used by the managed node.

Z.5.3.3 LDAP Documentation

The LDAP database should be configured to include device descriptions for this managed device, and there should be descriptions for the other devices that this device will communicate with. The first portion is used by this device during its startup configuration process. The second portion is used by this device to find the services that it will use.

The basic structural components of the DICOM information must be present on the LDAP server so that this device can find the DICOM root and its own entry. It is a good idea to fully populate the AE-title registry so that as managed devices are added there are no AE-title conflicts.

Z.5.3.4 Descriptions of other devices

This device needs to be able to find the association acceptors (usually SCPs) that it will use during normal operation. These may need to be manually configured into the LDAP server. Their descriptions can be highly incomplete if these other devices are not managed devices. Only enough information is needed to meet the needs of this device. If this device is manually configured and makes no LDAP queries to find services, then none of the other device descriptions are needed.

There are some advantages to manually mantaining the LDAP database for unmanaged devices. This can document the manually assigned AE Titles. The service and network connection information can be very useful during network planning and troubleshooting. The database can also be useful during service operations on unmanaged devices as a documentation aid. The decision whether to use the LDAP database as a documentation aid often depends upon the features provided with the LDAP server. If it has good tools for manually updating the LDAP database and good tools for querying and reporting, it is often a good investment to create a manually maintained LDAP database.

Z.5.4 Description of this device

This device needs its own LDAP entry. This is used during the system startup process. The LDAP server updates must be performed.

Z.6 SWITCHING A NODE FROM UNMANAGED TO MANAGED IN A MIXED NETWORK

During the transition period devices will be switched from unmanaged to managed. This may be done in stages, with the LDAP client transition being done at a different time than the DHCP, DNS, and NTP client. This section describes a switch that changes a device from completely unmanaged to a fully managed device. The device itself may be completely replaced or simply have a software upgrade. Details of how the device is switched are not important.

Z.6.1 DHCP and DNS

If the device was documented as part of an initial full network documentation process, the entries in the DHCP and DNS databases need to be checked. If the entry is missing, wrong, or incomplete, it must be corrected in the DHCP and DNS databases. If the entries are correct, then no changes are needed to those servers. The device can simply start using the servers. The only synchronization requirement is that the DHCP and DNS servers be updated before the device, so these can be scheduled as convenient.

If the device is going to be dynamically assigned an IP address by the DHCP server, then the DNS server database should be updated to reflect that DDNS is now going to be used for this device. This update should not be made ahead of time. It should be made when the device is updated.

Z.6.2 NTP

The NTP server location relative to this device should be reviewed to be sure that it meets the timing requirements of the device. If it is an NTP client with a time accuracy requirement of approximately 1 second, almost any NTP server location will be acceptable. For SNTP clients and devices with high time accuracy requirements, it is possible that an additional NTP server or network topology adjustment may be needed.

If the NTP server is using secured time information, certificates or passwords may need to be exchanged.

Z.6.3 Association Acceptors on This Node

The association acceptors may be able to simply utilize the configuration information from the LDAP database, but it is likely that further configuration will be needed. Unmanaged nodes probably have only a minimal configuration in the database.

Z.6.4 Association Requestors on Legacy Nodes

These will probably remain unchanged. The IP address must be pre-allocated if there are legacy nodes that cannot

Z.6.5 Association Requestors on Managed Nodes

If the previous configuration had already been described in the LDAP database, the managed nodes can continue to use the LDAP database. The updated and more detailed entry describing the now managed association acceptor will be used.