

Requirement		draft-ietf-ldup-model-06.txt
G1.	LDAP Replication MUST support models 2 (Eventual Consistency) and 3 (Limited Effort Eventual Consistency)	Section 3.6 - Consistency Models
G2.	LDAP Replication SHOULD NOT preclude support for model 1 (Transactional Consistency) in the future	Section 3.6 - Consistency Models. Without knowing what requirements Transactional Consistency will require, we can't say this is covered. However, the authors believe that there is a good chance that at least the log-based mechanism described in the architecture will be able to be extended to support replication of transactional information. We do have our doubts about the ability of any state-based replication scheme to do so, though.
G3.	LDAP replication SHOULD have minimal impact on both the system and network performance	Section 10 - Incremental Update Transfer Protocol
G4.	The LDAP Replication Standard SHOULD NOT limit the replication transaction rate	No artificial constraints are specified. However, consumers of incremental updates are permitted to restrict the number of simultaneous replication sessions requiring it to receive updates to 1.
G5.	The LDAP replication standard SHOULD NOT limit the size of an area of replication or a replica	No artificial constraints are specified. The area of replication ("replication context" in the document) is defined to be a contiguous subtree of the Directory Information Tree (see Section 3.5).
G6.	Meta-data collected by the LDAP replication mechanism MUST NOT grow without bound	Section 11 - Purging State Information. Note that log-based systems must be especially vigilant, and may be subject to denial of service attacks that create change state logging information faster than it can be purged.

Requirement		draft-ietf-ldup-model-06.txt
G7.	All policy and state data pertaining to replication MUST be accessible via LDAP	Policy information is available via LDAP (see section 5 - Information Model, and [INFOMOD]). Replication state information is available via LDAP (see section 10.1 - Update Vector and section 11.1 - Purge Vector). For change state information (CSNs for entries, attributes and values), see Management Operations.
G8.	LDAP replication MUST be capable of replicating the following	N/A
G8.1	all userApplication attribute types	No artificial constraints.
G8.2	all directoryOperation and distributedOperation attribute types defined in the LDAP "core" specifications (RFC 2251-2256, 2829-2830)	No artificial constraints.
G8.3	attribute subtypes	No artificial constraints.
G8.4	attribute description options (e.g. ";binary" and Language Tags)	No artificial constraints.
G9.	LDAP replication SHOULD support replication of directoryOperation and distributedOperation attribute types defined in standards track LDAP extensions	No artificial constraints.
G9.1	Future standards track specifications SHOULD include a "Replication Considerations" section which indicates how and whether the new feature operates in a replicated environment.	N/A
G10.	LDAP replication MUST NOT support replication of dsaOperation attribute types as such attributes are DSA-specific	Note that this REQUIRES that changes to RootDSE information be maintained OUTSIDE of LDUP, either directly via Management Operations, or as side effects of those Management Operations.
M1.	The model MUST support the following triggers for initiation of a replica cycle	N/A
M1.a1	A configurable set of scheduled times	Section 5.6.1 - Replication Schedule and [INFOMOD]
M1.a2	the specific trigger(s) and related parameters for a given server MUST be identified in a well-known place defined by the standard, e.g. the Replication Agreement(s).	See [INFOMOD]
M1.b1	Periodically, with a configurable period between replica cycles	Section 5.6.1 - Replication Schedule and [INFOMOD]
M1.b2	the specific trigger(s) and related parameters for a given server MUST be identified in a well-known place defined by the standard, e.g. the Replication Agreement(s).	See [INFOMOD]

Requirement		draft-ietf-ldup-model-06.txt
M1.c1	A configurable maximum amount of time between replica cycles	Section 5.6.1 - Replication Schedule and [INFOMOD]
M1.c2	the specific trigger(s) and related parameters for a given server MUST be identified in a well-known place defined by the standard, e.g. the Replication Agreement(s).	See [INFOMOD]
M1.d1	A configurable number of accumulated changes	Not Supported
M1.d2	the specific trigger(s) and related parameters for a given server MUST be identified in a well-known place defined by the standard, e.g. the Replication Agreement(s).	Not Supported
M1.e1	Change in the value of a critical OID	Not Supported
M1.e2	the specific trigger(s) and related parameters for a given server MUST be identified in a well-known place defined by the standard, e.g. the Replication Agreement(s).	Not Supported
M1.f1	As the result of an automatic rescheduling after a replication initiation conflict	Section 7.2.2 - Start Replication Response (Requirements document needs to be modified to call out this response option)
M1.f2	the specific trigger(s) and related parameters for a given server MUST be identified in a well-known place defined by the standard, e.g. the Replication Agreement(s).	It's not clear that the "rescheduled time" should be stored in the directory itself...and by whom? The supplier or the consumer, the initiator or the responder? Should such information be replicated, or be specific to the DSA wanting to remember it? Should it be accessible via LDAP? What security issues, in the way of denial of service attacks, would this create?
M1.g	A manual request for immediate replication	See Management Operations.
M2	The replication model MUST support both master-slave and multi-master relationships	Section 3.6 - Consistency Models and Section 3.7 - LDAP Constraints
M3	An attribute in an entry must eventually converge to the same set of values in every replica holding that entry.	Section 3.6 - Consistency Models
M4	LDAP replication MUST encompass schema definitions, attribute names and values, access control information, knowledge information, and name space information.	Section 6 - Replication of Directory Administrative Policy Information

Requirement		draft-ietf-ldup-model-06.txt
M5	LDAP replication MUST NOT require that all copies of the replicated information be complete, but MAY require that at least one copy be complete.	No artificial constraints.
M5.1	The model MUST support Partial Replicas.	Section 4.1.4 - Fractional Replicas
M6	The determination of which OIDs are critical MUST be configurable in the replication agreement.	See [INFOMOD]
M7	The parameters of the replication process among the members of the replica-group, including access parameters, necessary authentication credentials, assurances of confidentiality (encryption), and area(s) of replication MUST be defined in a standard location (e.g. the replication agreements).	Section 6 - Replication of Directory Administrative Policy Information
M8	The replication agreements SHOULD accommodate multiple servers receiving the same area of replication under a single predefined agreement.	See [INFOMOD]
M9	LDAP replication MUST provide scalability to both enterprise and Internet environments, e.g. an LDAP server must be able to provide replication services to replicas within an enterprise as well as across the Internet.	No artificial constraints.
M10	While different directory implementations can support different/extended schema, schema mismatches between two replicating servers MUST be handled. One way of handling such mismatches might be to raise an error condition.	Section 10.5 - Update Resolution Procedures and see [URP]
M11	There MUST be a facility that can update, or totally refresh, a replica-group from a standard data format, such as LDIF format [RFC2849].	Section 9 - LDUP Full Update Transfer Protocol
M12	An update received by a consumer more than once MUST NOT produce a different outcome than if the update were received only once.	See [URP]
P1	The replication protocol MUST provide for recovery and rescheduling of a replication session due to replication initiation conflicts (e.g. consumer busy replicating with other servers) and or loss of connection (e.g. supplier cannot reach a replica).	Section 7.2.2 - Start Replication Response (Requirements document needs to be modified to call out this response option)
P2	LDUP replication SHOULD NOT send an update to a consumer if the consumer has previously acknowledged that update.	Section 10.1 - Update Vector
P3	The LDAP replication protocol MUST allow for full update to facilitate replica initialization and reset loading utilizing a standardized format such as LDIF [RFC2849] format.	Section 9 - LDUP Full Update Transfer Protocol
P4	Incremental replication MUST be allowed.	Section 10 - Incremental Update Transfer Protocol
P5	The replication protocol MUST allow either a master or slave replica to initiate the replication process.	Section 7.1.2 - Consumer Initiated and Section 7.1.3 - Supplier Initiated

Requirement		draft-ietf-ldup-model-06.txt
P6	The protocol MUST preserve atomicity of LDAP operations as defined in RFC2251 [RFC2251]. In a multi-master environment this may lead to an unresolvable conflict. MM5 and MM6 discuss how to handle this situation.	Section 10.5 - Update Resolution Procedures and see [URP]
P7	The protocol MUST support a mechanism to report schema mismatches between replicas discovered during a replication session.	Section 10.5 - Update Resolution Procedures and see [URP]
SC1	A standard way to determine what replicas are held on a server MUST be defined.	Section 5.2 - Root DSE Attributes and see [INFOMOD]
SC2	A standard schema for representing replication agreements MUST be defined.	Section 5.6 - Replication Agreement Object Class and Entries and see [INFOMOD]
SC3	The semantics associated with modifying the attributes of replication agreements MUST be defined.	Section 5.1 - Entries, Semantics and Relationships and see [INFOMOD]
SC4	A standard method for determining the location of replication agreements MUST be defined.	Section 5.1 - Entries, Semantics and Relationships and see [INFOMOD]
SC5	A standard schema for publishing state information about a given replica MUST be defined.	Section 5.4 - Replica Object Class and Entries and see [INFOMOD]
SC6	A standard method for determining the location of replica state information MUST be defined.	Section 10.1 - Update Vector
SC7	It MUST be possible for appropriately authorized administrators, regardless of their network location, to access replication agreements in the DIT.	Section 12 - Replication Configuration and Management
SC8	Replication agreements of all servers containing replicated information MUST be accessible via LDAP.	Section 5.6 - Replication Agreement Object Class and Entries and see [INFOMOD]
SC9	An entry MUST be uniquely identifiable throughout its lifetime.	Section 4.4 - Unique Identifiers
SM1	A Single Master system SHOULD provide a fast method of promoting a slave replica to become the master replica.	Section 4.1 - Replica Types and see Management Operations
SM2	The master replica in a Single Master system SHOULD send all changes to read-only replicas in the order in which the master applied them.	Supported for log-based systems, but not state-based systems, by definition.
MM1	The replication protocol SHOULD NOT saturate the network with redundant or unnecessary entry replication.	Section 10 - Incremental Update Transfer Protocol
MM2	The initiator MUST be allowed to determine whether it will become a consumer or supplier during the synchronization startup process.	Section 7.2.1 - Start Replication Request
MM3	During a replica cycle, it MUST be possible for the two servers to switch between the consumer and supplier roles.	Not supported in the current Model document
MM4	When multiple master replicas want to start a replica cycle with the same replica at the same time, the model MUST have an automatic and deterministic mechanism for resolving or avoiding replication initiation conflict.	Section 7.2.2 - Start Replication Response (Requirements document needs to be modified to call out this response option)

Requirement		draft-ietf-ldup-model-06.txt
MM5	Multi-master replication MUST NOT lose information during replication.	Section 10.5 - Update Resolution Procedures and see [URP]
MM5.1	If conflict resolution would result in the loss of directory information, the replication process MUST store that information, notify the administrator of the nature of the conflict and the information that was lost, and provide a mechanism for possible override by the administrator.	Section 10.5 - Update Resolution Procedures and see [URP]
MM6	Multi-master replication MUST support convergence of the values of attributes and entries. Convergence may result in an event as described in MM5.	Section 10.5 - Update Resolution Procedures and see [URP]
MM7	Multi-master conflict resolution MUST NOT depend on the in-order arrival of changes at a replica to assure eventual convergence.	Section 10.5 - Update Resolution Procedures and see [URP]
AM1	Replication agreements MUST allow the initiation of a replica cycle to be administratively postponed to a more convenient period.	See [INFOMOD]
AM2	Each copy of a replica MUST maintain audit history information of which servers it has replicated with and which servers have replicated with it.	Not presently supported. And would you want the audit information replicated?
AM3	Access to replication agreements, topologies, and policy attributes MUST be provided through LDAP.	Section 5 - Information Model, Section 12 - Replication Configuration and Management, and see [INFOMOD]
AM4	The capability to check the differences between two replicas for the same information SHOULD be provided.	See Management Operations.
AM5	A mechanism to fix differences between replicas without triggering new replica cycles SHOULD be provided.	See Management Operations.
AM6	The sequence of updates to access control information (ACI) and the data controlled by that ACI MUST be maintained by replication.	Not supported for State Based replication
AM7	It MUST be possible to add a 'blank' replica to a replica-group, and force a full update from (one of) the Master(s), for the purpose of adding a new directory server to the system.	Section 12 - Replication Configuration and Management
AM8	Vendors SHOULD provide tools to audit schema compatibility within a potential replica-group.	N/A
S1	The protocol MUST support mutual authentication of the source and the replica directories during initialization of a replication session.	Section 7.1.1 - Authentication
S2	The protocol MUST support mutual verification of authorization of the source to send and the replica to receive replicated data during initialization of a replication session.	Section 5.6 - Replication Agreement Object Class and Entries and see [INFOMOD]
S3	The protocol MUST also support the initialization of anonymous replication sessions.	Not supported - conflicts with requirement S2 <eer>

Requirement		draft-ietf-ldup-model-06.txt
S4	The replication protocol MUST support transfer of data with data integrity and data confidentiality.	Section 7.5 - Integrity & Confidentiality
S5	The replication protocol MUST support the ability during initialization of a replication session for an authenticated source and replica to mutually decide to disable data integrity and data confidentiality within the context of and for the duration of that particular replication session.	Section 7.5 - Integrity & Confidentiality (TLS might let you do this - see [PROTO])
S6	To promote interoperability, there MUST be a mandatory-to-implement data privacy mechanism.	Section 7.5 - Integrity & Confidentiality
S7	The transport for administrative access MUST permit assurance of the integrity and privacy of all data transferred.	See Management Operations.