Summary of Changes

- BNF per RFC 2234; updated examples to reflect new BNF
- Added back multiple list of attributes; removed collections
- updated/expanded set of permissions and their descriptions
- Clarification of interactions of precedences and evaluations
- added access decision algorithm so nothing intuited from examples
- Added strength of authentication option into ACI syntax based on ldap bind
- Incorporated authmeth id format into subject component of ldapaci (removed kerberos format)
- ipAddress format expanded to include domain names and wildcards

Summary of Changes (continued)

- added ability to control access to ACI; removed policy owner
- defined ldapACISubEntry to allow specification of any access control mechanism anywhere in the tree
- addressed how alias de-referencing and referrals work with respect to access control
- Versioning ldapACI: concluded that a different attribute would be used in subsequent RFCs on ldap access control
- updated the security considerations sections
- updated/expanded description of the access control model
- removed terminology section

New Comments on Draft

- discloseOnError: change from server basis to a permission?
- Delete permission: clarify it works on leaf entry (per X.500)
- Search permission: revisit/update permissions b, r, s
- Rename permission: rename perm or combination of w, o, i, e perms?
- Should ldapACI attribute be split into subtreeACI and entryACI attributes?
- Clarify use of “[all]” and “[entry]” wrt subtree scope
- Authentication level: clarify how it works with deny; should additional explicit choices be specified, e.g. X509?
- Use of filters in ACI?
- Dependency on ldapSubEntry specification?
- Specificity precedence
- Misc clarifications (e.g. add, import, export perms; empty grant list; subject definitions)
- Update control/extended operation to reflect correct conventions