

Exploring LDAP

By
Valmiki Mukherjee
Seethal Nagalla
Hemakumar Rangineni

**Seminar Series on Computer
Network Protocols**
CSCI 5780 Spring 2005

Session -1

Introduction to LDAP

By Seethal Nagalla

- What is LDAP
- RFC, Origin and Progress
- LDAP Standard
- LDAP Protocol Stack
- LDAP Functions
- How LDAP Works...

What is LDAP

- **LDAP is Lightweight Directory Access Protocol**
- LDAP is a protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.
- LDAP is a "lightweight" (*smaller amount of code*) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.
- LDAP is called lighter because in its initial version it did not include security features. – *Not the case anymore!*

RFC, Origin and Progress

- **RFCs for LDAP are**
 - LDAP v1: RFC – 1487 (Enhancement over X.500)
 - LDAP v2: RFC – 1777 (Current Version)
 - LDAP v3: RFC – 2251 (Under Development)
- LDAP originated at the University of Michigan
- LDAP is endorsed by at least 40 companies.
 - Netscape includes it in its latest Communicator suite
 - Microsoft includes in Active Directory in a number of products including Outlook Express.
 - Novell's NetWare includes it in Directory Services.
 - Cisco also supports it in its networking products

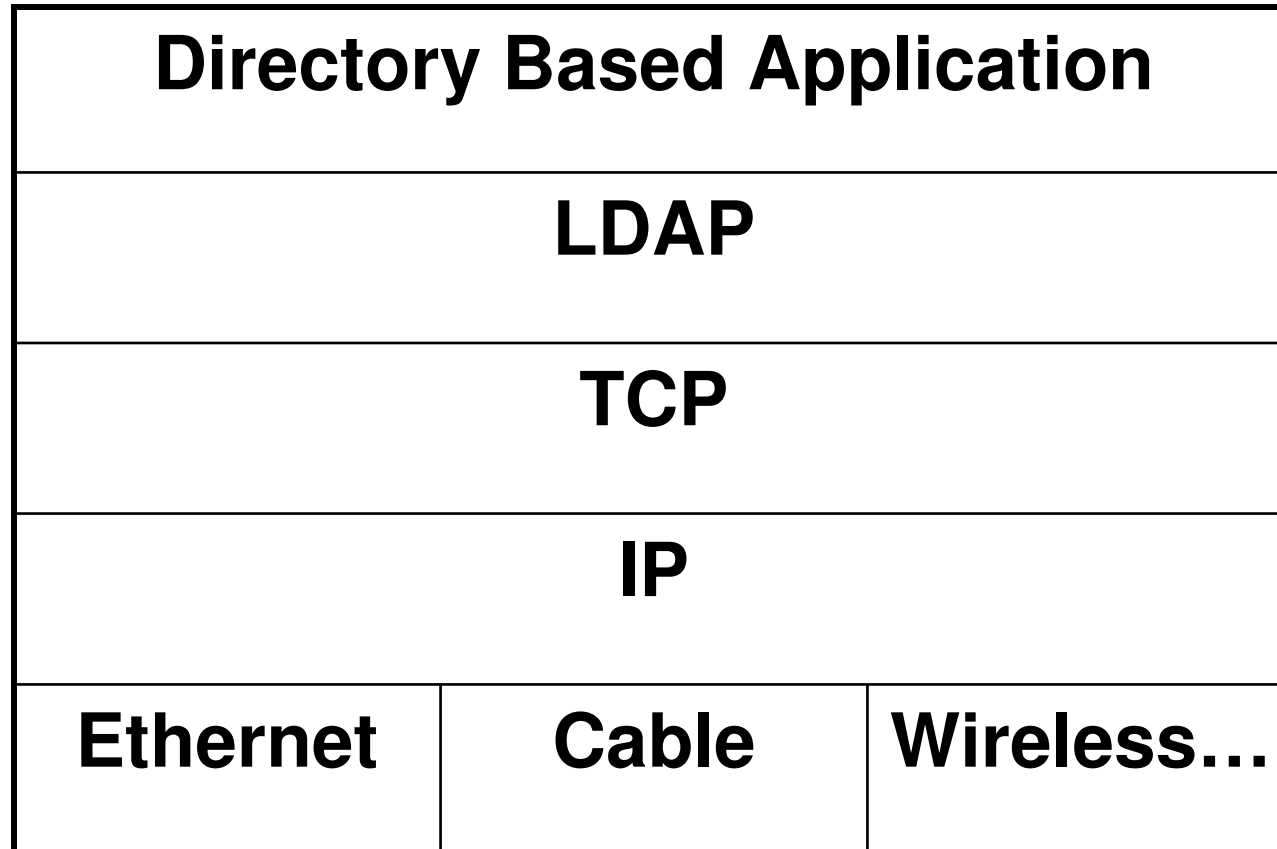
Directory Service

- **A Directory is like a database...**
- **It is *specialized*. Some typical characteristics are...**
 - designed for reading more than writing
offers a static view of the data
 - simple updates without transactions
- **Directory Services Include...**
 - a network protocol used to access the directory
 - a replication scheme
 - a data distribution scheme

LDAP standard

- **The LDAP Standard Defines the following:**
 - **A network protocol for accessing information in the directory**
 - **An information model defining the form and character of the information**
 - **A namespace defining how information is referenced and organized**
 - **An emerging distributed operation model defining how data may be distributed and referenced (v3)**
 - **Both the protocol itself and the information model are *extensible***

LDAP Protocol Stack



LDAP Functions

- **The LDAP protocol is the *vehicle* for accessing the directory...**
- **it defines the operations one may perform...**
 - search,
 - add,
 - delete,
 - modify,
 - change name
- **it defines how operations and data are conveyed**

How LDAP Works

- **The information model and namespace are based on *Entries*...**
- **Each attribute has a *type* and one or more *values***
- **E.g...**
 - **cn = test entry**
 - **cn = another commonName value for test entry**
 - **mail = entry@someHost.someDomain**

LDAP - Common Elements

- The Protocol Data Unit for LDAP is a Message Envelope
- For the purposes of protocol exchanges, all protocol operations are encapsulated in a common envelope, the LDAPMessage
- The function of the LDAPMessage is to provide an envelope containing common fields required in all protocol exchanges. At this time the only common fields are the message ID and the controls.

```
LDAPMessage ::= SEQUENCE {  
  
    messageID      MessageID,  
    protocolOp     CHOICE {  
        bindRequest      BindRequest,  
        bindResponse     BindResponse,  
        unbindRequest    UnbindRequest,  
        searchRequest     SearchRequest,  
        searchResEntry   SearchResultEntry,  
        searchResDone    SearchResultDone,  
        searchResRef     SearchResultReference,  
        modifyRequest    ModifyRequest,  
        modifyResponse   ModifyResponse,  
        addRequest       AddRequest,  
        addResponse      AddResponse,  
        delRequest       DelRequest,  
        delResponse      DelResponse,  
        modDNRequest     ModifyDNRequest,  
        modDNResponse    ModifyDNResponse,  
        compareRequest   CompareRequest,  
        compareResponse  CompareResponse,  
        abandonRequest   AbandonRequest,  
        extendedReq      ExtendedRequest,  
        extendedResp     ExtendedResponse },  
    controls        [0] Controls OPTIONAL }  
  
MessageID ::= INTEGER (0 .. maxInt)  
  
maxInt INTEGER ::= 2147483647 -- (231 - 1) --
```

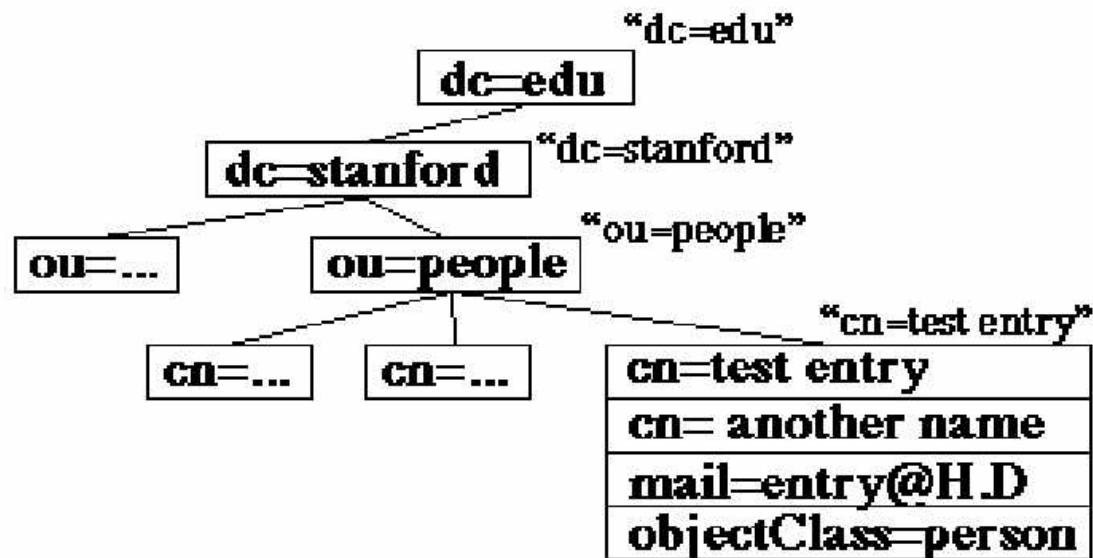
Typed Entries

- **Entries *themselves* are "typed". This is accomplished by the `objectClass` attribute...**
 - "cn = test entry"
 - cn = test entry
 - cn = another commonName value for test entry
 - mail = entry@someHost.someDomain
 - objectclass = person

Distinguished Names

- The namespace is hierarchical, so it has the concept of fully-qualified names called
- *Relative Distinguished Names* (RDN)...
- Test Entry's RDN is...
- "cn=test entry, ou=people, dc=unt, dc=edu"

Hierarchical Structure



LDAP Hierarchical Structure

Accessing with LDAP

- **Accessing an LDAP-based directory is accomplished by using a combination of DN, *filter*, and *scope*...**
- **A *base DN* indicates where in the hierarchy to begin the search**
- **A filter specifies attribute types, assertion values, and matching criteria**
- **Scope indicates what to search:**
 - the base DN itself
 - one level below the base DN
 - the entire subtree rooted at the base DN

Accessing with LDAP...

- **E.g. the query...**
- **<I want all the person entries for My Co. whose commonNames end with "entry">**
- **..may be expressed as...**
- **base DN: dc = MyCo, dc = com**
- **scope: entire subtree**
- **filter: objectClass = person & cn = "*entry"**
- **(though the filter in this example is not *syntactically* correct)**

Type of Data for LDAP

- **You can put just about anything you want into the directory...**
 - Text
 - Photos
 - URLs
 - Pointers to whatever
 - Binary data
 - Public Key Certificates
- **Though, there may be implementation-dependent limitations on the amount of data of a given type you can store.**

SECTION 2

DEPLOYING LDAP

By Valmiki Mukherjee

- Use of LDAP
- Key Points in LDAP
- White Page
- Attribute Mapping
- LDAP Deployment
 - Small Workgroup
 - Large Workgroup
- Deployment Case studies

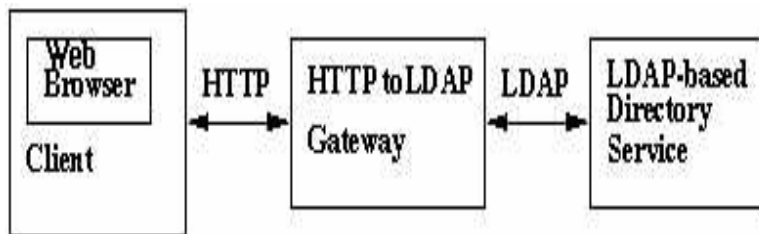
Use of LDAP!

- **White Pages**
 - "I want to look up so-and-so and get their email address and phone number..."
- **Yellow Pages**
 - "List me all the printers..."
- **Attribute Mapping**
 - "Give me the company ID number of the person whose login ID is...###"
 - "Gimme the email routing address of this person..."
- **Namespace Implementation**
 - "If a supposed name of an entity isn't in the directory, then it isn't (yet) a name."
 - iPlanet Server for NIS

LDAP - Platform Independence

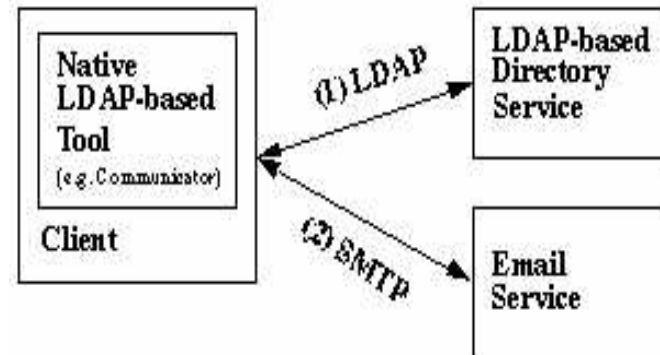
- **LDAP is a vendor-independent, open, network protocol standard**
- **Supports *multi-vendor interoperability* -- in the same fashion as TCP/IP, SMTP, DNS, and others**
- **Writing gateways between it and other protocols or systems is relatively straightforward.**
- **These gateways currently exist...**
 - LDAP to X.500 and X.500 to LDAP
 - HTTP to LDAP
 - WHOIS++ to LDAP
 - FINGER to LDAP
 - Email to LDAP
- **People are working on...**
 - ODBC to LDAP

White Pages



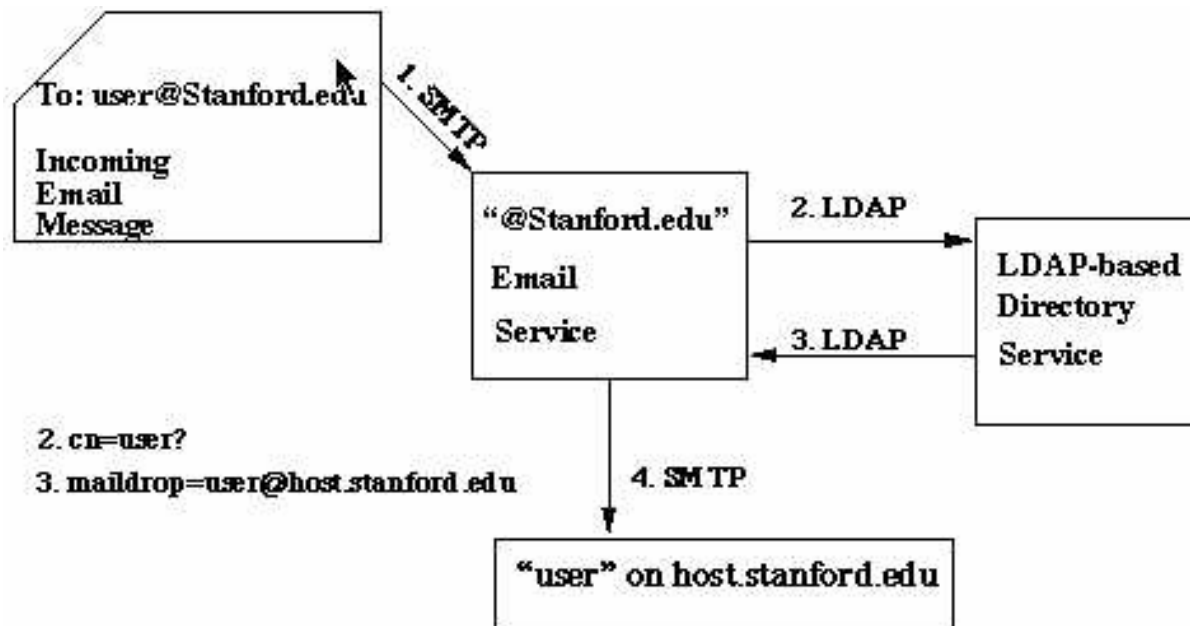
Via a web browser...

- Via an LDAP-enabled tool...
- Netscape Communicator
- E.g. a user may use Communicator's Address Book tool to browse the directory for a person, and then, say, opens the mail tool and the "To:" field will automatically be filled-in with the person's email address



Attribute Mapping

- **Domain-based Email addresses via a directory...**



LDAP Association

ID	Association State Description	Action	Next State
S1	Anonymous no Authentication ID is associated with the LDAP connection no Authorization ID is in force	A1 A2 A3 A4	S1 S1 S2 no change
S2	Authenticated Authentication ID = I Authorization ID = X	A5 A6 A7	no change or S3* no change or S3* S3
S3	Invalidated		
ID	Action		
A1	Client bind request fails		
A2	Client successfully performs anonymous simple bind or unauthenticated simple bind		
A3	Client successfully binds producing an authentication ID of I. Authentication ID I maps to authorization ID X. Depending on the bind mechanism and associated parameters authorization ID X was either derived from authentication ID I or was explicitly requested as part of the bind operation.		
A4	Client StartTLS request fails		
A5	Client StartTLS request succeeds		
A6	Client or Server: graceful TLS layer removal		
A7	Server decides to invalidate current association state		

The table here list the valid association states and provides a description of each state. The ID for each state is used in the state transition table



LDAP Deployment For Small Workgroups

- **Small Workgroups...**
- **10's to perhaps small 100's of people**
- **Probably will run mostly "shrink-wrap" apps & services "out of the box"**
 - e.g. Netscape and/or Microsoft application/server suites
- **Relatively basic entity representation requirements**
 - **Most entries laid out by the apps and services**

LDAP Deployment...

- **Small workgroup considerations...**
- **Client configurability**
 - What attributes does the client use to search for entries?
 - With which filters?
 - How are these configured?
 - How do I distribute them to all the various client instances?
- **Service configurability**
 - Can I define attributes and object classes?
 - How do I lay out my directory hierarchy?
 - Are there tools to help me?

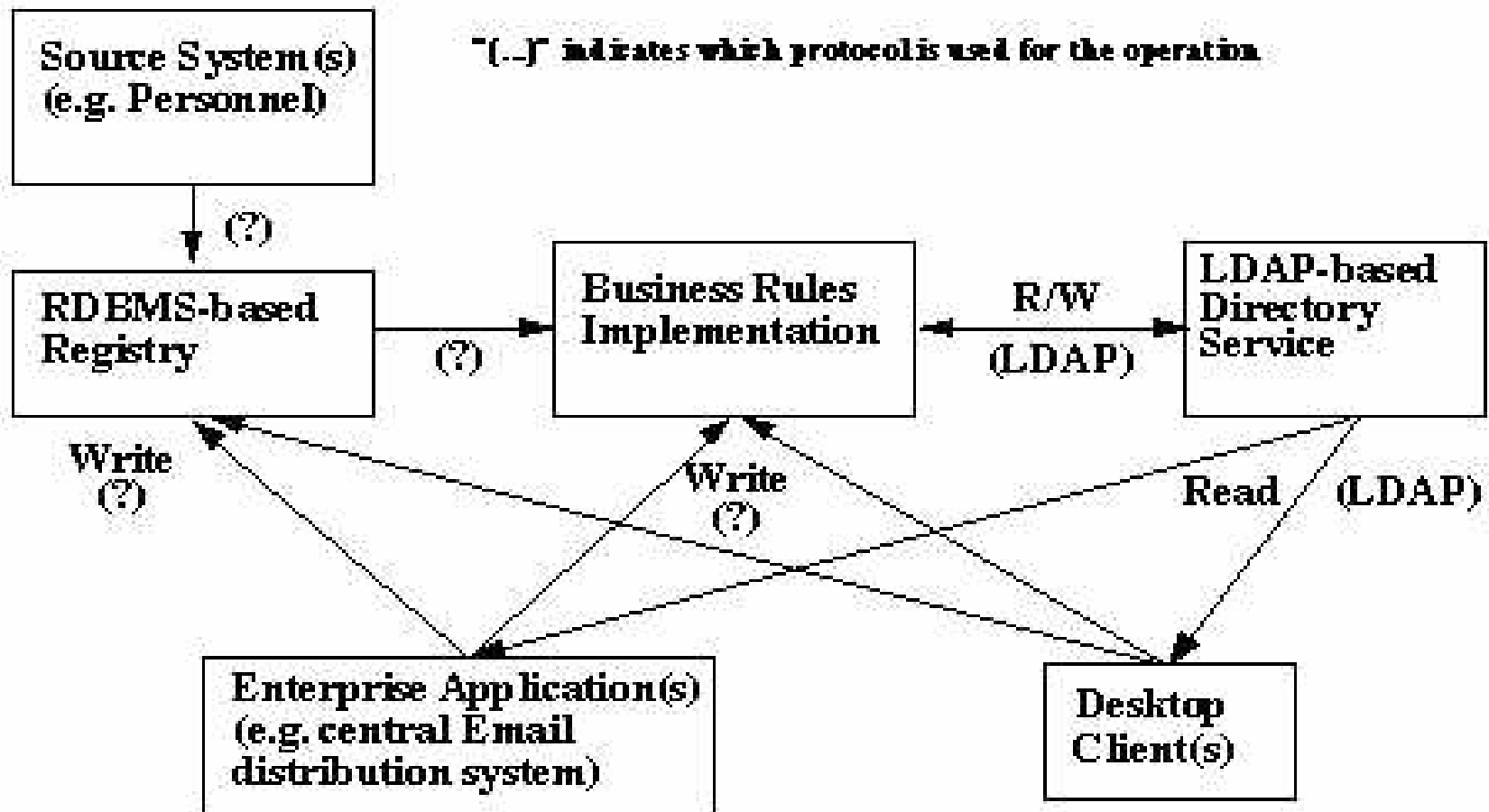
Enterprise Considerations

- **Non-trivial schema design**
- **Use data modeling techniques**
- **Namespace architecture**
- **Mapping multiple identifiers to a given object**
- **Different nameforms for various contexts**

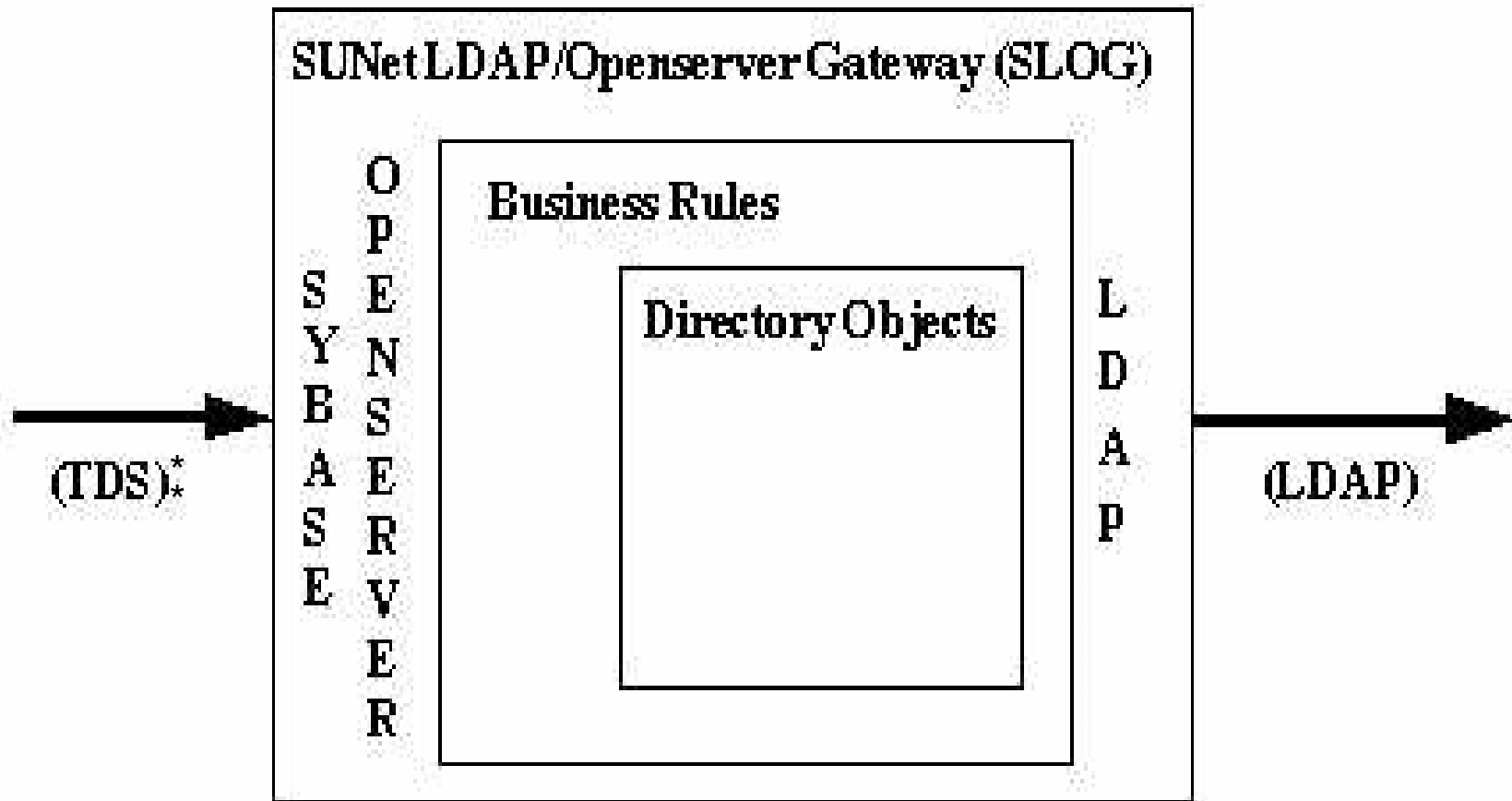
Enterprise Applications...

- **Enterprise Givens...**
- **100's to 1000's of people**
- **Multi-vendor mixture of shrink-wrap and custom applications & services**
- **Rich set of data representation requirements**
 - **Many site-specific entities to represent**
 - **Many non-people things to represent**
 - **Many app-specific objects from multiple vendors**

Enterprise Considerations...

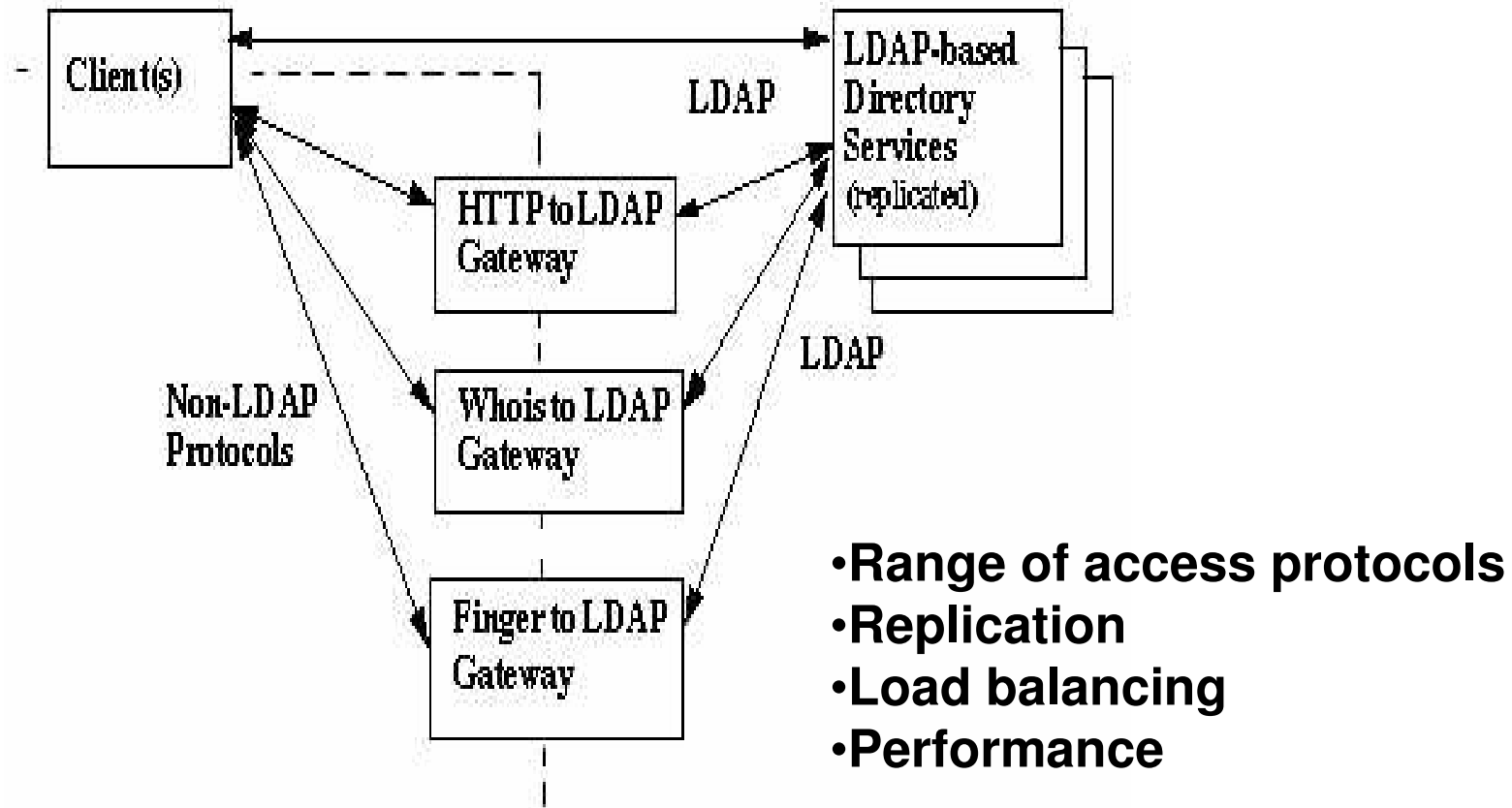


Enterprise Considerations...

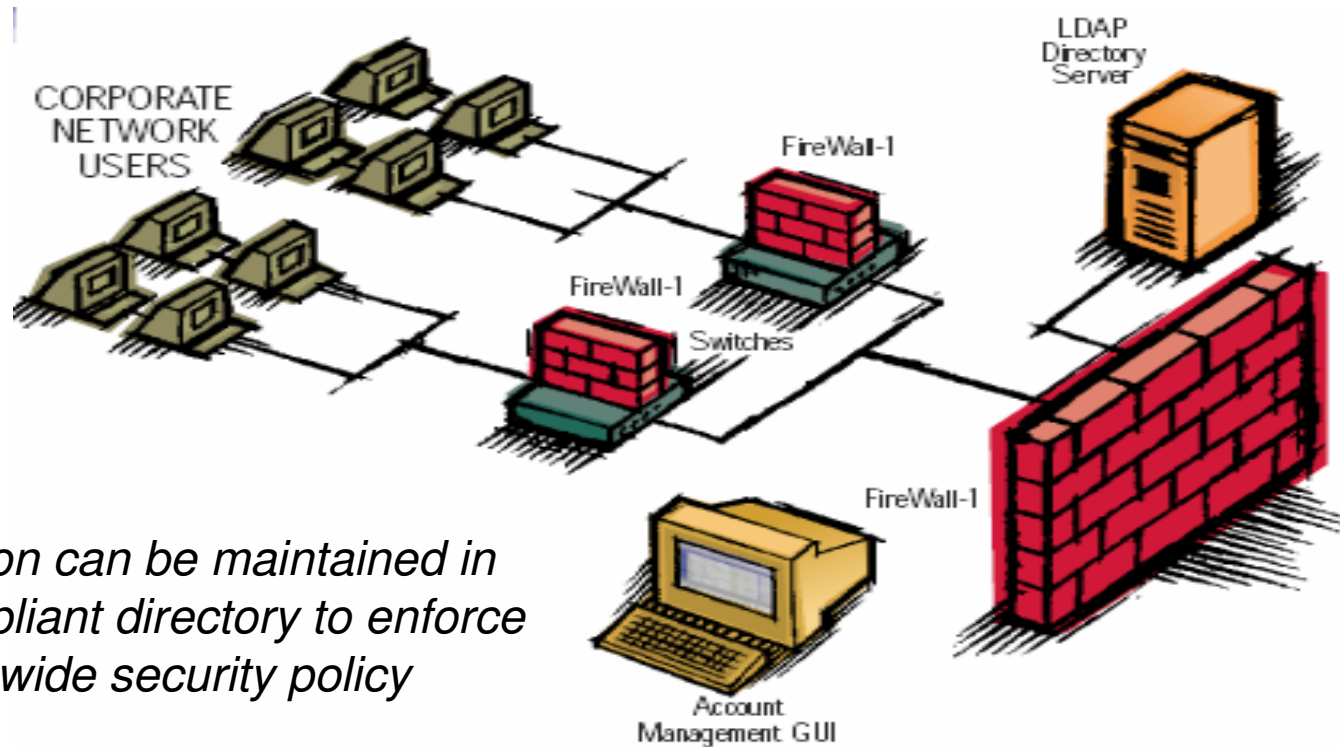


* Tabular data Stream

Deployment Architecture



LDAP Deployment A Case Study - 1



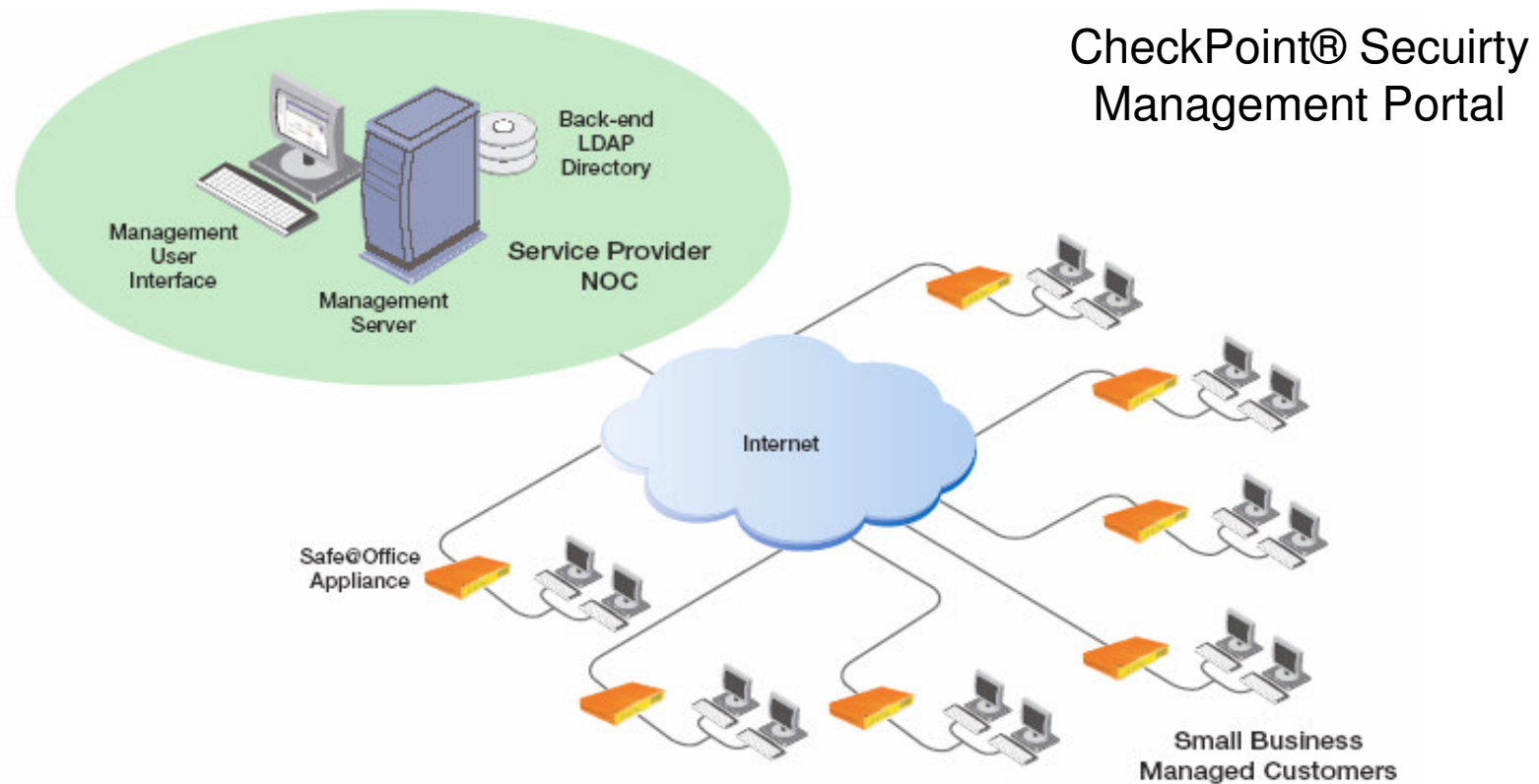
User information can be maintained in an LDAP-compliant directory to enforce the enterprise-wide security policy

CheckPoint® Account Management Module

LDAP User Information for AMS

Identification	Full username, login name, Email Address, Directory Branch, Associated Template
Authentication	Authentication Schema, Authentication Server and Password
Access Control	Authorized Sources, Authorized Destinations
Time Restrictions	Time and Day Access Privileges
Encryption	Key Negotiation Scheme, Encryption Algorithm, Data Integrity Method
Groups	Group Members

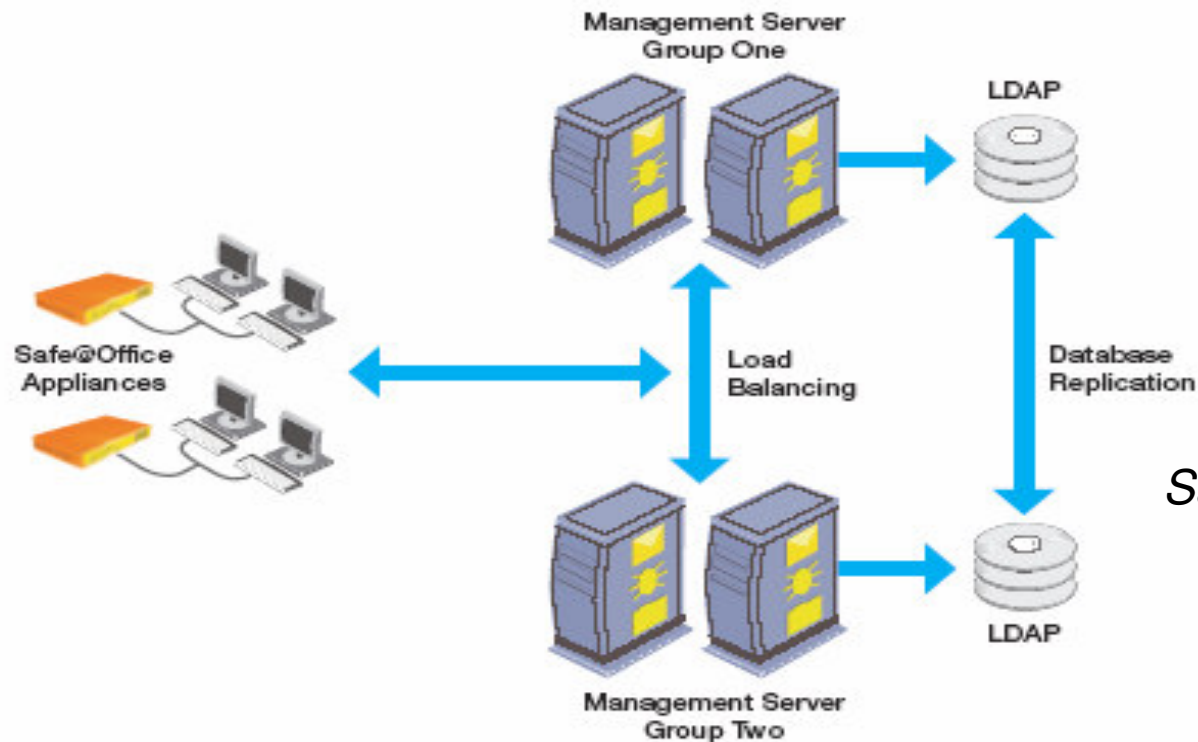
LDAP Deployment A Case Study -2



Security Management Portal enables the delivery of cost-effective, comprehensive managed security services to small businesses.

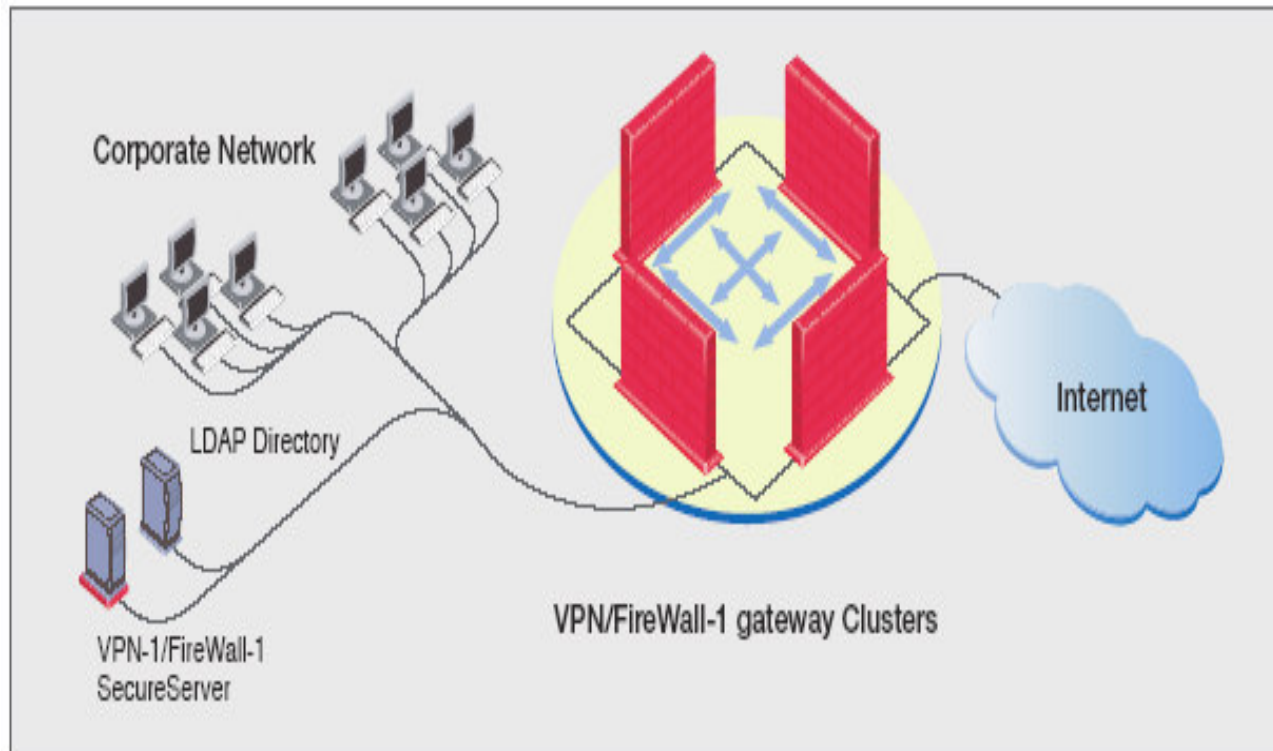
LDAP Deployment

A Case Study - 3



Clusters of management and LDAP servers may be deployed to provide non-stop access to tens of thousands of gateways.

LDAP Deployment A Case Study - 4



Checkpoint®
Cluster XL
Technology

Provision of seamless fail-over and load sharing for mission-critical gateway deployments

SECTION 3

Vulnerabilities and Security Issues in LDAP

By Hemakumar Rangineni

- Vulnerabilities in LDAP
- Issues in LDAP
- Correction to issues
- Summary
- Questions
- References

LDAP Vulnerabilities

- VU#276944 - iPlanet Directory Server contains multiple vulnerabilities in LDAP handling code

Impact:

One or more of these vulnerabilities allow a remote attacker to execute arbitrary code with the privileges of the Directory Server.

LDAP Vulnerabilities...

- VU#505564 - IBM SecureWay Directory is vulnerable to denial-of-service attacks via LDAP handling code

Impact:

Allows a remote attacker to crash affected SecureWay Directory servers, resulting in a denial-of-service condition.

LDAP Vulnerabilities...

- VU#869184 - Oracle Internet Directory contains multiple vulnerabilities in LDAP handling code

Impact:

One or more of these vulnerabilities allow a remote attacker to execute arbitrary code with the privileges of the Oracle server. The server typically runs with system privileges.

LDAP Vulnerabilities...

- VU#763400 - Microsoft Exchange LDAP Service is vulnerable to denial-of-service attacks

Impact:

Allow a remote attacker to crash the LDAP component of vulnerable Exchange 5.5 and Exchange 2000 servers, resulting in a denial-of-service condition within the LDAP component.

LDAP Vulnerabilities...

- Solution

Possible solution is to apply a patch from the vendor.

Security Issues

- **The basic threats to ldap directory service are**
 - Unauthorized access to data via data fetching operations
 - Unauthorized modification of data
 - Unauthorized modification of configuration

Security Issues..

- Unauthorized or excessive use of resources (denial of service)
- Spoofing of directory: Tricking a client into believing that information came from the directory when in fact it did not, either by modifying data in transit or is directing the client's connection

Protecting LDAP Security

- Client authentication by means of the SASL mechanism set; possibly backed by the TLS mechanism
- Client authorization by means of access control based on the requestor's authenticated identity
- Data integrity protection by means of the TLS protocol or data-integrity SASL mechanisms

Cont..

- Resource limitation by means of administrative limits on service controls
- Server authentication by means of the TLS protocol or SASL mechanism

Review Questions

- Q1. Name three functions of LDAP
- Soln:
 - Serves as a vehicle for accessing the directory
 - it defines the operations one may perform...
 - search, add, delete, modify, change name
 - it defines how operations and data are conveyed

- Q2. Where is LDAP used?
- Soln.
 - White Pages, Yellow Pages, Attribute Mapping

- Q3. Name an Application that is LDAP Compliant
- Soln
 - Netscape Suite of application

Summary

- **LDAP is an**
 - extensible,
 - vendor-independent,
 - network *protocol* standard -- it supports hardware,
 - software, and
 - network heterogeneity
- **An LDAP-based directory supports *any* type of data**
- **It may be configured to play essentially *any* role you wish**
- **The LDAP protocol directly supports various forms of *strong security* (authentication, privacy, and integrity) technology**
- **We can use LDAP, to glue together disparate facets of cyberspace, e.g. email, security, white- & yellow-pages directories, collaborative tools, MBone, etc.**

References

- Acknowledgement:

We acknowledge the material used in this presentation to their respective authors and copyright holders. We do not claim any originality of the material except for the organization. These slides are prepared for instructional purposes only.

- References:

- www.ietf.org

- <http://www.rfc-editor.org/rfcsearch.html>

- <http://www.sofaware.com>

- <http://www.sun.com/blueprints>

- <http://www.bind9.net/rfc-ldap>

- <http://www.stanford.edu/~hodges/talks/WebSec99/>

- <http://www.kb.cert.org/vuls>

- <http://www.vulnwatch.org/>

- <http://www.gracion.com/server/whatldap.html>

- <http://www.stanford.edu/~hodges/talks/mactivity.ldap.97>