

Program: MCA & IBCA

Course Code: MCAS9250

Course Name: N/w Mgt. & System Adm.

Semester: Vth & IX

GALGOTIAS
UNIVERSITY

LDAP

The **Lightweight Directory Access Protocol** is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network.

As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory.

Similarly, a telephone directory is a list of subscribers with an address and a phone number.

LDAP

- LDAP is specified in a series of Internet Engineering Task Force (IETF) Standard Track publications called Request for Comments (RFCs), using the description language ASN.
- **The latest specification is Version 3, published as RFC 4511.**
- A common use of LDAP is to provide a central place to store usernames and passwords. This allows many different applications and services to connect to the LDAP server to validate users.

LDAP

- LDAP is based on a simpler subset of the standards contained within the X.500 standard. Because of this relationship, LDAP is sometimes called X.500-lite.
 - AGENDA
 - Understanding LDAP
 - LDAP Servers
 - Information Structure
 - Protocol Overview
 - LDAP operations

GALGOTIAS
UNIVERSITY

Understanding LDAP

- LDAP stands for Lightweight Directory Access Protocol.
- It is an internet protocol for accessing distributed directory services.
- It uses the TCP/IP protocols for its operations
- It also forms the standard for allowing directories to be managed.

GALGOTIAS
UNIVERSITY

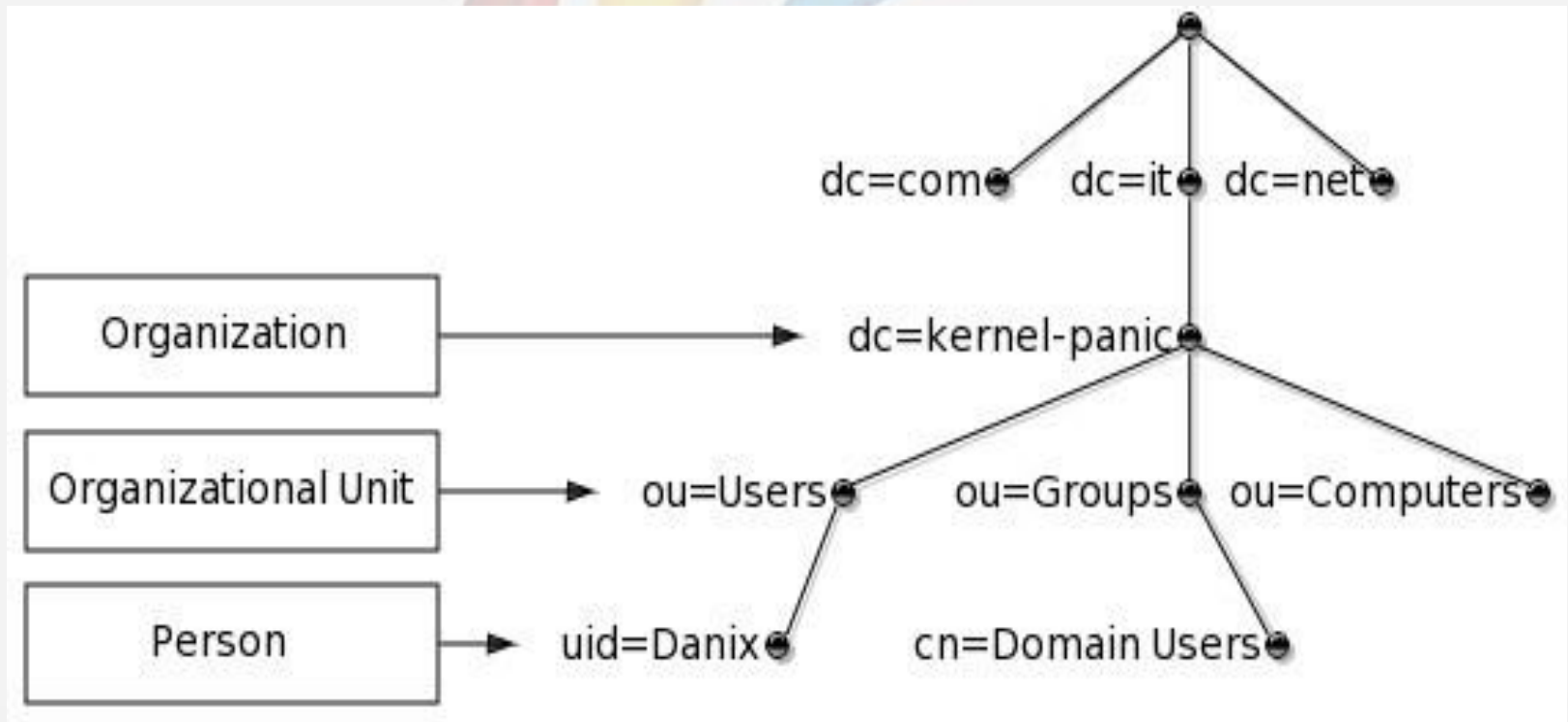
LDAP Servers

- OpenLDAP
- Active directory
- Apache Directory Server
- FreeIPA
- OpenDS
- Novell eDirectory
- Sun Java System Directory Server
- IBM Tivoli Directory Server

GALGOTIAS
UNIVERSITY

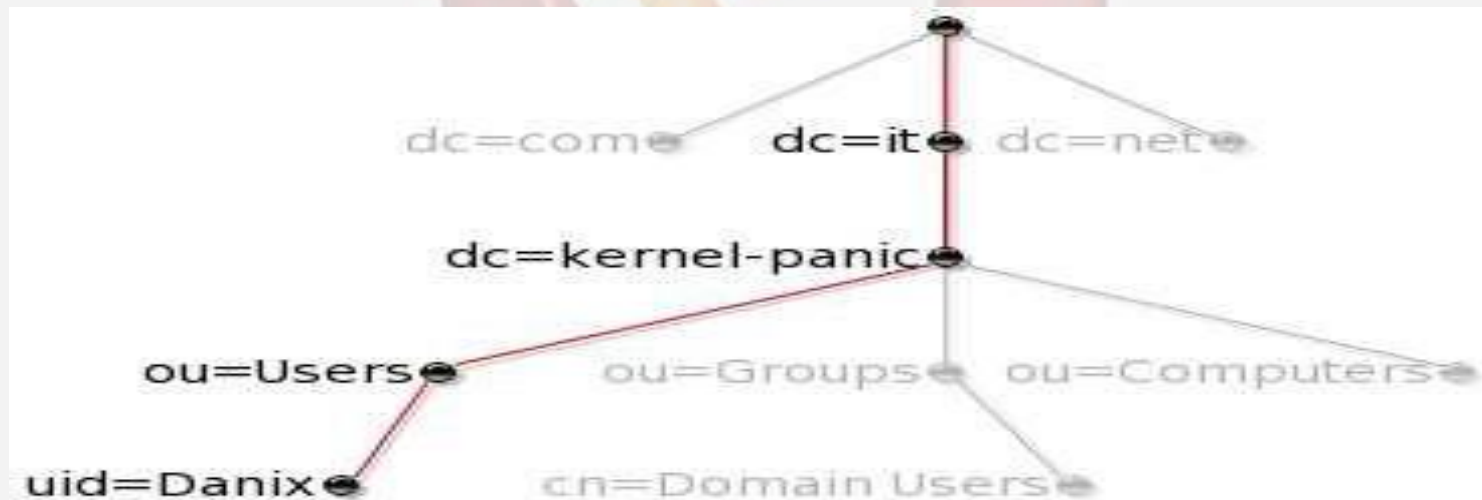
Information Structure

- It has a DIT (Directory Information Tree) which help present information in the hierarchical tree format
- Example of a DIT is as below.



Information Structure

- Each node in the LDAP tree is called an entry and is uniquely identified by its Distinguished Name (DN)
- For instance, the DN of the entry highlighted in the following picture below.



UNIVERSITY

Information Structure

- The DN for the above tree can then be written as below
- “ui=Danix,ou=Users,dc=kernel-panic,dc=it”
- See RFC4514 for full description of the DN format.
- An entry consists of a set of attributes, each attribute has a name or type and one or more values.
- “dc” stands for Domain Component
- “cn” stands for Common Name
- Objectclasses define the attribute structure of an LDAP entry.
- Both ObjectClasses and Attributes are defined within schemas

Information Structure

- O stands for organization
- OU stands for Organizational unit
- SN stands for Surname
- Givenname stands for First Name
- UID stands for Userid
- Mail stands for Email address
- C stands for country
- L stands for location
- St stands for Status

GALGOTIAS
UNIVERSITY

Information Structure

- Entries can be represented in a human-readable format by using the LDIF format as in example below.

```
dn: uid=danix,ou=Users,dc=kernel-panic,dc=it
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: sambaSamAccount
cn: Daniele Mazzocchio
sn: Mazzocchio
givenName: Daniele
uid: Danix
uidNumber: 2000
gidNumber: 513
homeDirectory: /home/danix
```

UNIVERSITY

Protocol Overview

- Client starts an LDAP session by connecting to an LDAP Server
- The default TCP port is 389
- Bind to the server through an authentication process
- Client then sends an operation request to the server
- The Server sends responses in return

GALGOTIAS
UNIVERSITY

LDAP Operations

Operation	What it does
Search	Search directory for matching directory entries
Compare	Compare directory entry to a set of attributes
Add	Add a new directory entry
Modify	Modify a particular directory entry
Delete	Delete a particular directory entry
Rename	Rename or modify the DN
Bind	Start a session with an LDAP server
Unbind	End a session with an LDAP server
Abandon	Abandon an operation previously sent to the server
Extended	Extended operations command

U N I V E R S I T Y

SUMMARY

- LDAP
- Understanding LDAP
- LDAP Servers
- Information Structure
- Protocol Overview
- LDAP Operations

The logo of Galgotias University is a stylized, circular emblem. It features a central white 'G' shape formed by three overlapping, curved bands. The top band is yellow, the middle band is blue, and the bottom band is red. The entire emblem is set against a light red circular background.

GALGOTIAS
UNIVERSITY



Thank You