Advanced SUSE Linux Enterprise Server Administration (Course 3038)

Chapter 3

Configure Network Services

Objectives

- Configure a DNS Server Using BIND
- Deploy OpenLDAP on a SLES 9 Server
- Configure an Apache Web Server
- Configure a Samba Server as a File Server

Configure a DNS Server Using BIND

- Objectives
  - Understand the Domain Name System
  - Install and Configure the BIND Server Software
  - Configure a Caching-Only DNS server
  - Configure a Master Server for Your Domain
  - Configure One or More Slave Servers
  - Configure the Client Computers to Use the DNS Server
  - Use Command-Line Tools to Query DNS Servers
  - Find More Information About DNS

Understand the Domain Name System

- How name resolution worked in the early days of the Internet
  - Computers communicate using IP addresses
  - For humans it is simpler to use a computer name
    - Requires some kind of conversion
  - File at the Network Information Centre (NIC) of the Stanford Research Institute in California
    - Provided exactly this conversion
  - In 1984, Paul Mockapetris created the Domain Name System (DNS)
    - Guarantees unique computer names worldwide

Understand the Domain Name System (continued)

- The Internet Domain Concept
  - DNS consists of several domains that can be divided into subdomains
  - Top level of this structure is the root domain
  - There are over 13 computers worldwide
    - That act as root name servers
  - First layer beneath root domain contains the top level domains (TLDs)
  - Fully qualified domain name (FQDN)
    - Made from the actual computer name, the domain name, and the name of the TLD

Understand the Domain Name System (continued)

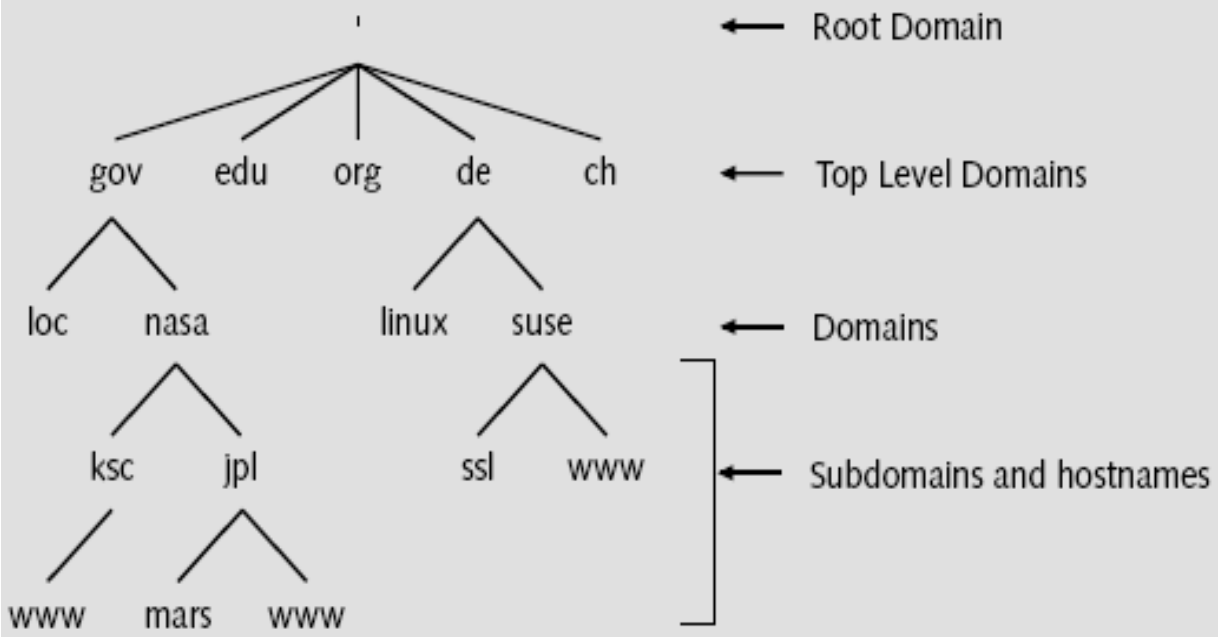

Figure 3-1

Understand the Domain Name System (continued)

- How Name Servers work
  - Domains are administered locally
    - Instead of using a global authority
  - For each domain there is one DNS server
    - Known as the master server
  - Slave servers
    - Distribute the load and serve as backups
    - Keep a copy of the information on the master server
    - Update this information at regular intervals
      - This update is called zone transfer

Understand the Domain Name System (continued)

Table 3-1

Master server	Has the main responsibility for a domain. Gets its data from local files.
Slave server	Gets its data from the master server using zone transfer.
Caching-only server	Queries data from other DNS servers and stores the information in the cache until its expiration date. All replies are nonauthoritative.
Forwarding server	All queries the server cannot answer authoritatively are forwarded to other DNS servers.

Understand the Domain Name System (continued)

- How to query DNS
  - Resolver
    - Makes a request to a DNS server
    - Interprets the answer
    - Sends back this information to the program that called it up
  - DNS server receives a request from a resolver
    - DNS server provides the required information to the resolver
    - DNS server queries the responsible authority
      - The data is stored in the cache of the DNS server

Understand the Domain Name System (continued)

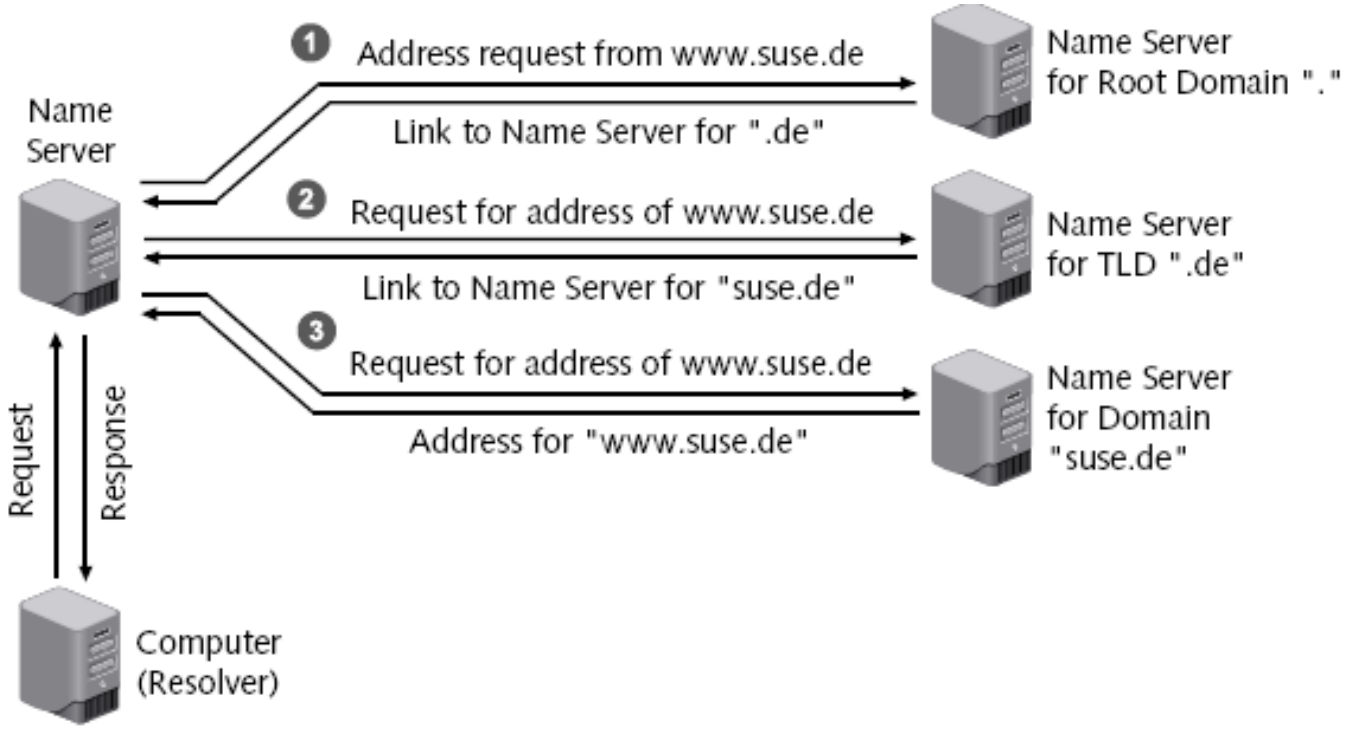

Figure 3-2

Install and Configure the BIND Server Software

- Install the following packages:
  - bind
  - bind-utils
- Start the server
  - rcnamed start
- Stop a running server
  - rcnamed stop
- Have DNS server start automatically
  - insserv named

Configure a Caching-Only DNS Server

- Caching-only DNS server
  - Does not manage its own databases
  - Accepts queries and forwards them to other servers
- DNS server configuration is defined in the file /etc/named.conf
  - Directory /var/lib/named/ contains database files
  - Entries needed for every DNS server
    - Entry for root DNS servers
    - Forward resolution for localhost
    - Reverse resolution for network 127.0.0.0
  - Define up to three DNS servers in the options block

Configure a Master Server for Your Domain

- Adapt the main server configuration file
  - Adapt configuration for the caching-only DNS server
    - Global options are followed by definitions for the database files
  - At least two files are necessary for each domain
    - Forward resolution
    - Reverse resolution
  - One file for each subnet must be created for reverse resolution
  - Each definition begins with the instruction *zone*
  - Zone name is always followed by an “in” for Internet

Configure a Master Server for Your Domain (continued)

- Create the zone files
  - Structure of the files
    - reference [TTL] class type value
  - The file /var/lib/named/master/digitalairlines.com.zone
    - BIND 9 requires you to specify a default TTL
    - Structure
      - TTL entry
      - SOA entry
      - Entry for the name server
      - Allocation of IP addresses to host names
  - The file /var/lib/named/master/10.0.0.zone
    - Structure similar to previous file

Configure a Master Server for Your Domain (continued)

Table 3-2

Record Type	Meaning	Value
SOA	Start of Authority (term for the authority)	Parameter for the domain
NS	DNS server	Name of one of the DNS servers for this domain
MX	Mail exchanger	Name and priority of a mail server for this domain
A	Address	IP address of a computer
PTR	Pointer	Name of a computer
CNAME	Canonical name	Alias name for a computer

Configure a Master Server for Your Domain (continued)

- Create the zone files
  - The file /var/lib/named/master/localhost.zone

```
$TTL 1W
@         IN SOA        @               root (
                        42              ; serial (d. adams)
                        2D              ; refresh
                        4H              ; retry
                        6W              ; expiry
                        1W )            ; minimum

          IN NS         @
          IN A          127.0.0.1
```

Configure a Master Server for Your Domain (continued)

- Create the zone files
  - The file /var/lib/named/master/127.0.0.zone

```
$TTL 1W
@       IN SOA      localhost.     root.localhost. (
                    42          ; serial (d. adams)
                    2D          ; refresh
                    4H          ; retry
                    6W          ; expiry
                    1W )        ; minimum

        IN NS       localhost.
1       IN PTR      localhost.
```

Configure a Master Server for Your Domain (continued)

- Create additional resource records
  - Define mail servers for the domain
    - MX (Mail Exchange) entry must be made in the database file for forward resolution
    - Several mail servers can be given
  - Assign aliases for computers
    - Define CNAME (canonical name) entries in the database file for forward resolution

Configure One or More Slave Servers

- Configure at least one more DNS server
  - Besides the master server
- Slave server
  - Receives copies of the zone files from the master server (called a zone transfer)
  - Queries the master server at regular intervals
  - Master server sends a message to all listed slave servers (called notify)

Configure One or More Slave Servers (continued)

- Configuration file /etc/named.conf
  - Contains at least two entries that define it as the master server
  - They are two zone definitions for loopback network
  - There may also be a zone definition for the root DNS server
- Instruct master server to inform slave servers about modifications
- Slave servers must be entered as DNS servers in the database files

Configure The Client Computers to Use the DNS Server

- Use YaST to configure a client computer
  - Enter the IP address of the DNS server
  - Add some information about your domain
- Information is written to the file /etc/resolv.conf
  - Types of entries
    - search
    - nameserver
- Another important file for the clients: /etc/nsswitch.conf
  - Configures the name service switch

Use Command-Line Tools to Query DNS Servers

- host command
  - Syntax: host *computer nameserver*
  - host contacts the servers listed in /etc/resolv.conf
  - By default, host returns the IP address or the host name
    - For additional information use option –t
- dig command
  - Syntax: dig *@nameserver computer type query_options*
  - Dig does not use the domain list from /etc/resolv.conf

Use Command-Line Tools to Query DNS Servers (continued)

Table 3-3

Option	Description
nameserver	The IP address or name of the DNS server that should be queried. If not specified, dig checks all DNS servers listed in /etc/resolv.conf.
computer	The resource record to query about (such as a host name, an IP address, or a domain name).
type	The type of resource record to be returned, such as A (IP address), NS (DNS server), MX (mail exchanger), -x (pointer), or ANY (all information).
query_options	Defines how the query is done and how the results are displayed. Each query option starts with a plus sign (+).

Find More Information About DNS

- BIND writes verbose messages to the file /var/log/messages
  - Messages contain information on the filename and the line in which this error occurs

Exercise 3-1 Configure a DNS Server

- In this exercise, you will do the following:
  - Part I: Install BIND
  - Part II: Configure a DNS Master Server
  - Part III: Configure the DNS Slave Server

Deploy OpenLDAP on a SLES 9 Server

- Objectives
  - The Concept of a Directory Service
  - The Basics of LDAP
  - How to Install and Set Up an OpenLDAP Server
  - How to Add Entries to the LDAP Server
  - How to Query Information from the LDAP Server
  - How to Delete and Modify Entries of the LDAP Server
  - How to Use Graphical LDAP Applications

The Concept of a Directory Service

- Directory
  - Specialized database that is optimized for reading, browsing, and searching
  - Contains descriptive, attribute-based information and supports sophisticated filtering
  - Tuned to give quick responses to high-volume lookup or search operations
  - There are local and global directories
- SLES9 uses OpenLDAP
  - For user management and some configuration purposes

The Basics of LDAP

- Lightweight Directory Access Protocol (LDAP)
  - Lightweight protocol for accessing directory services
  - Runs over TCP/IP or other connection-oriented transfer services
- LDAP information model is based on entries
  - Collection of attributes that has a globally-unique distinguished name (DN)
  - Each attribute has a type and one or more values
- Entries are arranged in a hierarchical tree structure

The Basics of LDAP (continued)

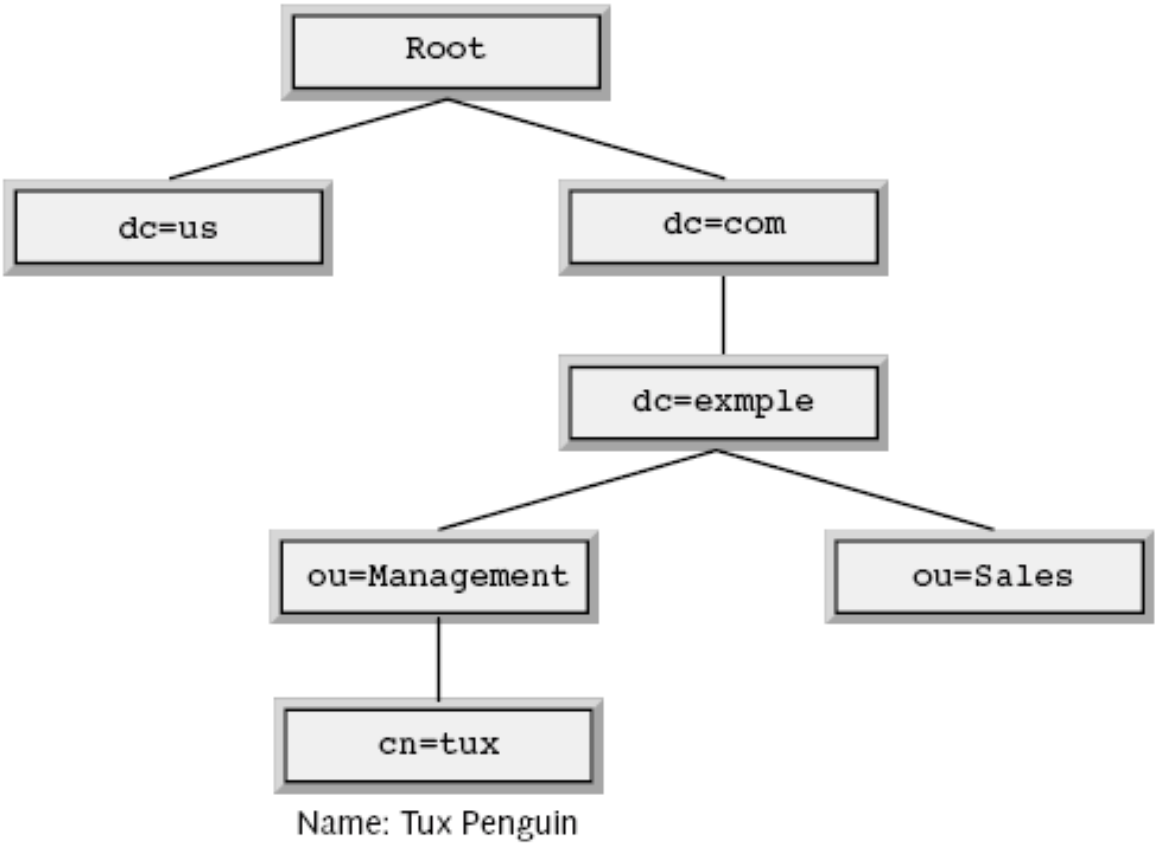

Figure 3-3

The Basics of LDAP (continued)

- LDAP allows you to control which attributes are required and allowed
  - Through the use of objectClasses
- Create a tree structure using container objects
  - Which can contain other objects, such as
    - Root
    - c
    - o
    - ou
    - dc

The Basics of LDAP (continued)

Table 3-4

Attribute Abbreviation	Description
uid	Login of the user
uidNumber	Numerical user ID
gid	Group name
gidNumber	Numerical group ID
homeDirectory	Home directory
loginShell	Login shell
shadowLastChange	Date of the last password change

How to Install and Set Up an OpenLDAP Server

- Install the required software and start the server
  - YaST sets up an OpenLDAP server
    - During the installation process of SLES 9
  - Manually install the following software packages
    - openldap2
    - openldap2-client
- Edit the OpenLDAP configuration files
  - Located in the directory /etc/openldap/
  - Configuration files
    - sldap.conf
    - ldap.conf

How to Install and Set Up an OpenLDAP Server (continued)

- sldap.conf configuration options
  - suffix “dc=your-domain,dc=com”
  - rootdn “cn=Manager,dc=example,dc=com”
  - rootpw secret
    - Create an encrypted password using:
      - slappasswd -s your_password
- Start the server
  - rcldap start
- Start the LDAP server automatically
  - insserv ldap

How to Install and Set Up an OpenLDAP Server (continued)

- ldap.conf configuration options
  - host localhost
  - base dc=suse,dc=de

How to Add Entries to the LDAP Server

- Command ldapadd
  - Inserts data that is in LDIF format into the directory
- An LDIF file contains the following entries:
  - dn
  - objectclass
  - attribute
- Every entry in an LDIF file does the following:
  - Sets the distinguished name of the entry
  - Lists the object classes used for the entry
  - Lists the attributes and their corresponding values

How to Add Entries to the LDAP Server (continued)

- LDAP uses Unicode (UTF-8)
  - You need to edit the LDIF file with a Unicode editor
  - You can convert a LDIF file using:
    - recode lat1.utf8 *ldif_file*
- Insert a data set that exists as an LDIF file
  - ldapadd -x -D dn_of_the_administrator -W -f file. ldif
    - Use -x if you haven't configured SASL authentication
    - Use -D to specify who can access the directory
    - Use -W to display a password prompt
    - Specify the LDIF file with the option -f

How to Add Entries to the LDAP Server (continued)

- Example

```
dn: uid=geeko,ou=people,dc=suse,dc=de
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
uid: geeko
uidNumber: 1010
gidNumber: 100
cn: Geeko Chameleon
givenName: Geeko
sn: Chameleon
homeDirectory: /home/geeko
loginShell: /bin/bash
shadowMax: 99999
shadowWarning: 7
shadowInactive: -1
```

How to Query Information from the LDAP Server

- Command ldapsearch
  - Reads data from the LDAP directory
  - Syntax: ldapsearch –x
    - -x forces to use the simple authentication method
  - Reads the search base for the query from file /etc/openldap/ldap.conf
    - Use –b option to specify a different search base
  - Add a filter expression
    - ldapsearch -x “(uid=g*)”
  - Displays the result in LDIF format

How to Delete and Modify Entries of the LDAP Server

- Modify an LDIF file
  - And apply the changes with the ldapmodify tool
- To apply the changes, use the following command:
  - ldapmodify -x -D “cn=Manager,dc=example,dc=com” -W -f geeko. ldif
- Delete an entry from the LDAP directory with:
  - ldapdelete -D cn=Administrator,dc=example,dc=com -x -W “cn=geeko,dc=example, dc=com”

How to Use Graphical LDAP Applications

- SLES 9 comes with the graphical LDAP browser GQ
- Search the directory
  - Use default page that opens after you start GQ
- Browse the directory
  - See Figure 3-5
- Explore the schema definitions
  - See Figure 3-6

How to Use Graphical LDAP Applications (continued)

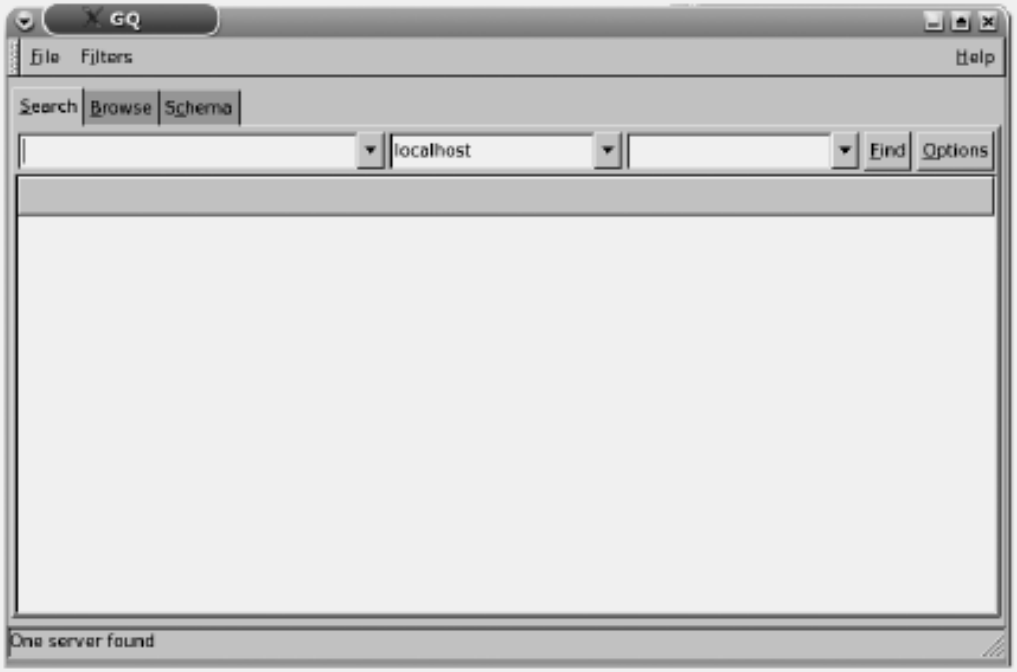

Figure 3-4

How to Use Graphical LDAP Applications (continued)

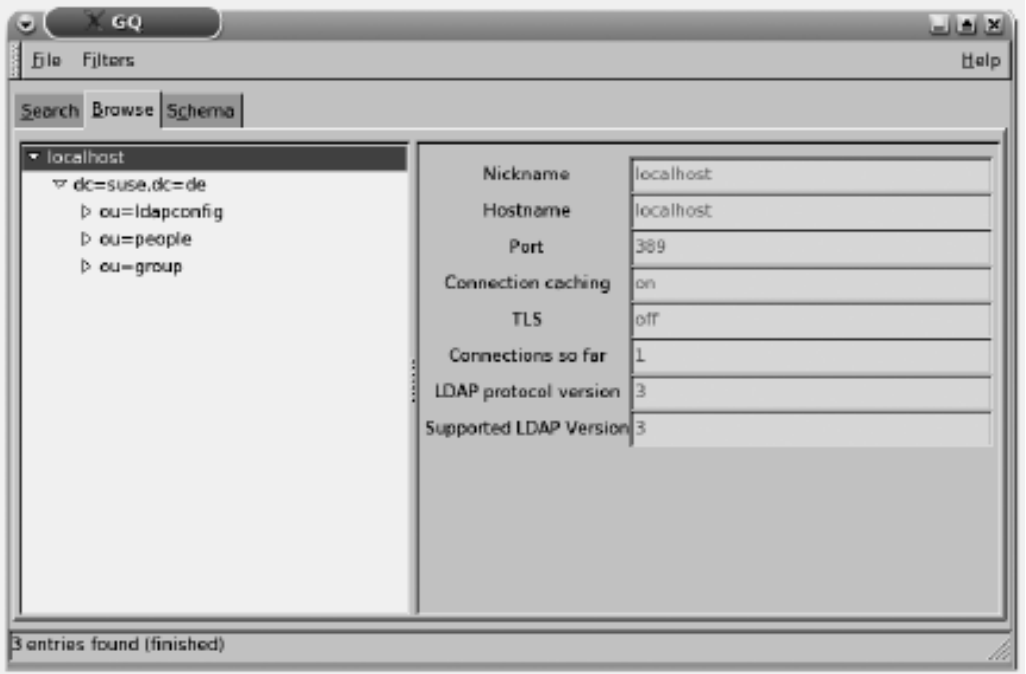

Figure 3-5

How to Use Graphical LDAP Applications (continued)

Figure 3-6

Exercise 3-2 Use the SLES 9 OpenLDAP Server

- In this exercise, you will do the following:
  - Part I: Install GQ
  - Part II: Search the SLES 9 OpenLDAP Server
  - Part III: Browse the SLES 9 OpenLDAP Server
  - Part IV: Use an LDIF File to Add a User

Configure an Apache Web Server

- Objectives
  - The Basic Functionality of a Web Server
  - How to Install and Set Up a Basic Apache Web Server
  - The Structure and the Basic Elements of the Apache Configuration Files
  - The Basic Apache Configuration
  - How to Configure Virtual Hosts
  - How to Limit Access to the Web Server
  - How to Configure OpenSSL for Connection Encryption

The Basic Functionality of a Web Server

- Delivers data that is requested by a Web browser
- Data can have different formats such as
  - HTML files, image files, Flash animations, or sound files
- Web browsers and Web servers communicate using HTTP (Hyper Text Transfer Protocol)
- Web server can perform tasks such as
  - Limiting access to specific Web sites
  - Logging access to a file
  - Encrypting connection between a server and browser

The Basic Functionality of a Web Server (continued)

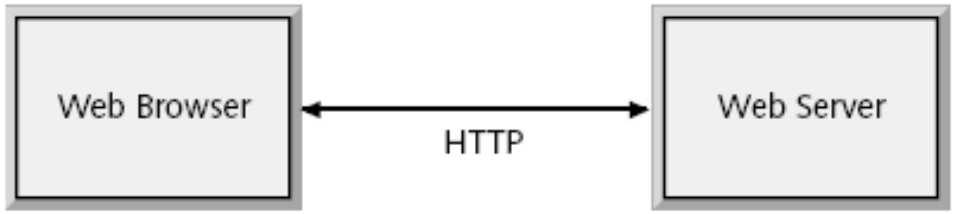

Figure 3-7

How to Install and Set Up a Basic Apache Web Server

- Install the required software packages
  - Packages
    - apache2
    - apache2-prefork
    - apache2-example-pages
  - SLES 9 ships with Apache versions series 1 and 2
- Start and test the Web server
  - Start the Web server
    - rcapache2 start
  - Stop the Web server
    - rcapache2 stop

How to Install and Set Up a Basic Apache Web Server (continued)

- Start and test the Web server (continued)
  - Automatically start the Web server
    - insserv apache2
  - Test the Web server
    - Open a Web browser and connect to http://localhost
  - Remotely connect to your Web server
    - Open a Web browser and enter http://your_system_IP_address

How to Install and Set Up a Basic Apache Web Server (continued)

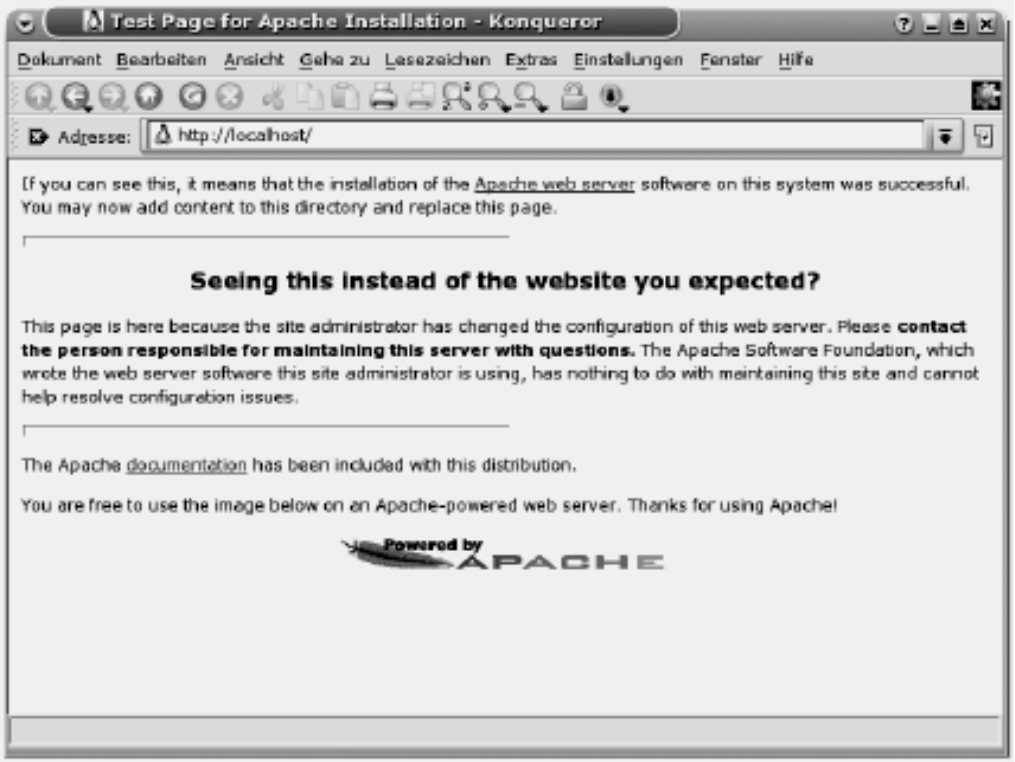

Figure 3-8

How to Install and Set Up a Basic Apache Web Server (continued)

- Locate the DocumentRoot of the Web server
  - Default directory of the data provided by Apache is /srv/www/htdocs
    - Called the *DocumentRoot*
  - Replace data in DocumentRoot directory
    - To display your own Web server content
  - Access subdirectories in DocumentRoot
    - http://your_server/name_of_subdirectory
  - If no specific file is requested in the address
    - Apache looks for a file with the name index.html

The Structure and the Basic Elements of the Apache Configuration Files

- Locate the Apache Configuration files
  - Directory /etc/apache2
  - Files
    - httpd.conf
    - default-server.conf
    - vhost.d
    - uid.conf
    - listen.conf
    - server-tuning.conf
    - error.conf
    - ssl-global.conf

The Structure and the Basic Elements of the Apache Configuration Files (continued)

- Understand the basic rules of the configuration files
  - Directives
    - Options of the Apache configuration files
    - Directives are case sensitive
    - Can be grouped so that they do not apply to the global server configuration
  - Example

```
<Directory "/srv/www/htdocs">
        Options None
        AllowOverride None
        Order allow,deny
        Allow from all
</Directory>
```

The Structure and the Basic Elements of the Apache Configuration Files (continued)

- Understand the basic rules of the configuration files (continued)
  - Reload the Web server
    - rcapache2 reload
  - Stop and restart the Web server
    - rcapache2 restart
  - Verify the syntax of the configuration files
    - apache2ctl configtest

The Basic Apache Configuration

- Main Apache Web server configuration file
  - /etc/apache2/default-server.conf

Table 3-5

Directive	Description
DocumentRoot	Specifies the DocumentRoot of the Web server.
Directory *"dir_name"*/Directory	All directives used within this block apply only to the specified directory.
Options	With this directive, additional options can be applied to logical blocks like directories.
AllowOverride	Determines whether other directives are allowed to be overwritten by a configuration found in a .htaccess file of a directory.
Alias *"fakename" "realname"*	Allows you to create an alias to a directory.
ScriptAlias	Allows you to create an alias to a directory containing scripts for dynamic content generation.

How to Configure Virtual Hosts

- The concept of virtual hosts
  - Apache server can be reached using:
    - http://localhost
    - http://*web_server_IP_address*
    - http://*web_server_hostname*
  - Apache serves the same files located in the DocumentRoot directory
  - Apache lets you set up multiple virtual Web servers
    - On one physical system
    - Needs to have an entry in the DNS for every virtual host

How to Configure Virtual Hosts (continued)

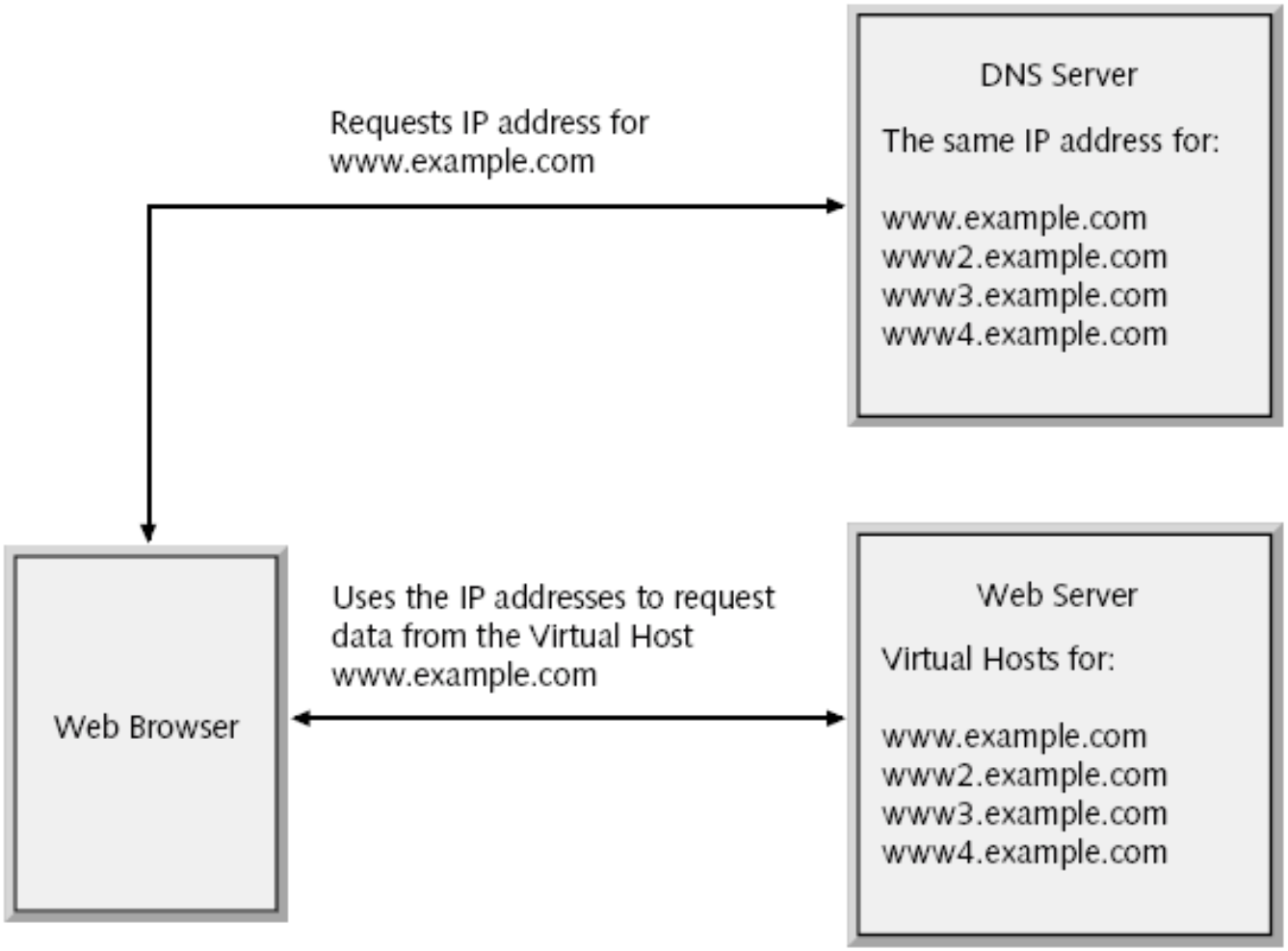

Figure 3-9

How to Configure Virtual Hosts (continued)

- How to configure a virtual host
  - Create a configuration file in the directory /etc/apache2/vhosts.d/
    - Name of the configuration file must end with .conf
  - You can find a template file vhost.template
    - In the directory /etc/apache2/vhosts.d/

How to Configure Virtual Hosts (continued)

Table 3-6

Directive	Description
ServerAdmin	Enter the e-mail address of the Virtual Host administrator here.
ServerName	Enter the hostname of the virtual host as it's configured in the DNS.
DocumentRoot	Set the DocumentRoot of the virtual host. The directory and the files in the directory must be readable by the user wwwrun.
ErrorLog	Enter a filename for the error log. The file must be writable for the user wwwrun.
CustomLog	Enter a filename for the general log file. The file must be writable for the user wwwrun.
ScriptAlias	Set the ScriptAlias to a directory of your choice. The directory must not be under the DocumentRoot of the virtual host. If you don't need scripts for dynamic content creation, delete this directive.
<Directory "script_dir">	If you set a ScriptAlias before, you have to adjust the settings for script directory accordingly. If you are not using a script directory, delete this directory block.
<Directory "document_root">	You need to adjust the path name of this directory directive to the path of your DocumentRoot.

How to Limit Access to the Web Server

- Limit access on an IP address basis
  - Apache directives
    - See Table 3-7
  - Example

```
<Directory "/srv/www/htdocs">
        Order deny,allow
        Deny from all
        Allow from 10.0.0.0/24
</Directory>
```

How to Limit Access to the Web Server (continued)

Table 3-7

Directive	Description
allow	IP addresses or networks listed after this directive are allowed to access the Web server.
deny	IP addresses or networks listed after this directive are not allowed to access the Web server.
order	This directive sets the order in which the allow and deny directives are evaluated.

How to Limit Access to the Web Server (continued)

- Limit access with user authentication
  - Users are required to log in before they can access the data
  - Create password file and an account for the user tux
    - htpasswd2 -c /etc/apache2/htpasswd tux
  - Add more users
    - htpasswd2 /etc/apache2/htpasswd username
  - Delete a user from the password file
    - htpasswd2 -D /etc/apache2/htpasswd *username*

How to Limit Access to the Web Server (continued)

- Limit access with user authentication (continued)
  - Add following lines to the directory block
    - Of the directory that should be restricted

```
AuthType Basic
AuthName "Restricted Files"
AuthUserFile /etc/apache2/htpasswd
Require user tux
```

How to Configure OpenSSL for Connection Encryption

- The basics of SSL encryption
  - Often data is transmitted across a network in encrypted form by using RSA keys
  - Encryption is based on a private key and a public key
  - Public and private keys can also be used to sign data
  - Problem with the encryption procedure
    - Determine who the owner of a public key is
  - Certificate Authority (CA)
    - Signs the public keys with its own private keys
  - Certificate
    - Public key signed by a CA

How to Configure OpenSSL for Connection Encryption (continued)

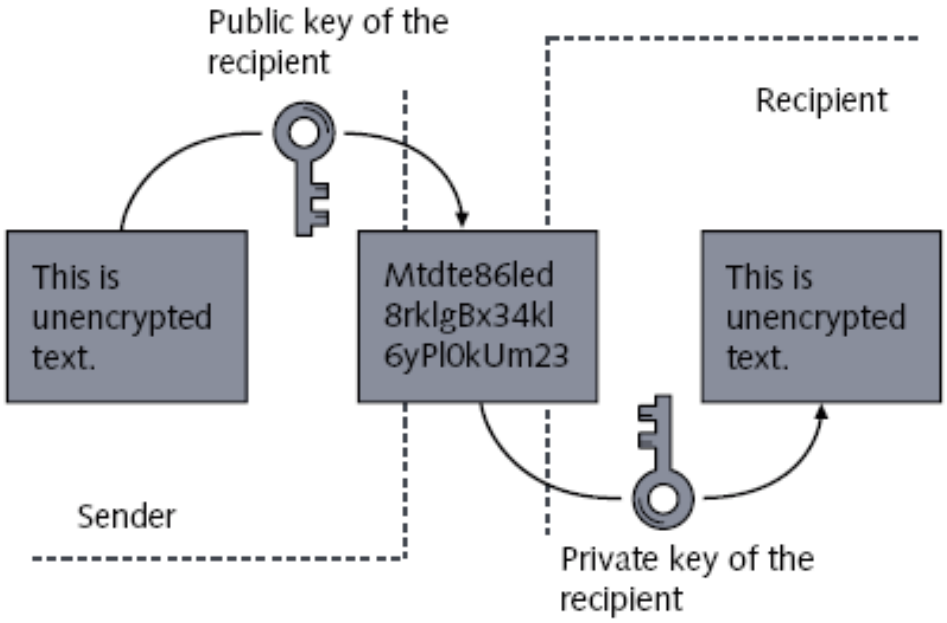

Figure 3-10

How to Configure OpenSSL for Connection Encryption (continued)

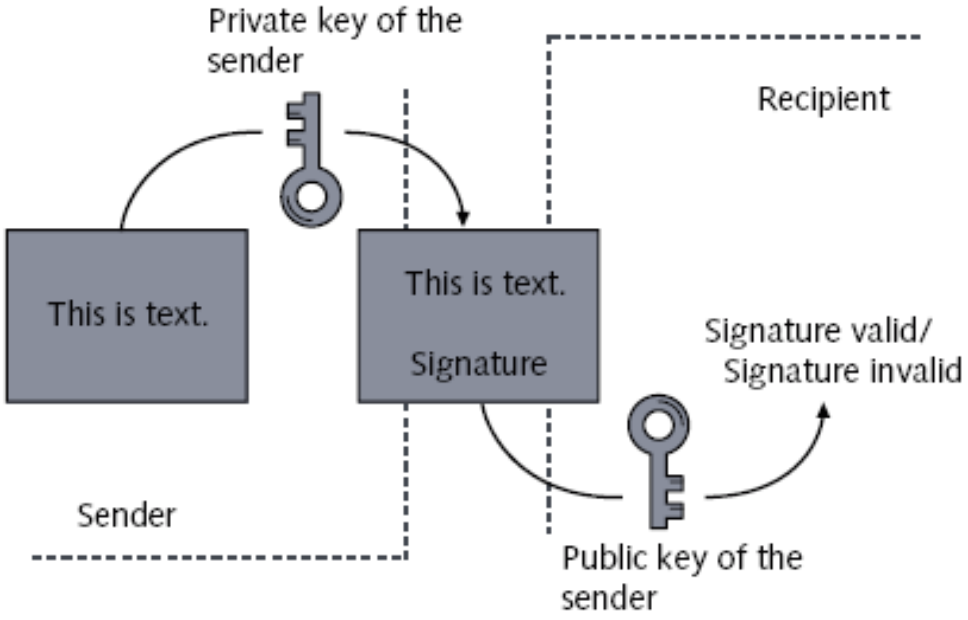

Figure 3-11

How to Configure OpenSSL for Connection Encryption (continued)

- The basics of SSL encryption (continued)
  - Process of using a CA with SSL encryption:
    - Browser recognizes Web address starting with https://
    - Web browser asks the server for its public RSA key
    - Web server sends the public key to the Web browser
    - Web browser verifies the key of the server with the public key of the CA that signed the key
    - If the key is valid, Web browser and Web server establish a secure connection

How to Configure OpenSSL for Connection Encryption (continued)

- How to create a test certificate
  - Create an RSA key pair
    - You need a file with as many random numbers as possible
    - Generate the key pair by entering
      - opensslgenrsa -des3 -out server.key -rand /tmp/random 1024
    - You are prompted to enter a password
  - Sign the public key to create a certificate
    - Enter the following command
      - openssl req -new -x509 -key server.key -out server.crt

How to Configure OpenSSL for Connection Encryption (continued)

- How to configure Apache to use SSL
  - Change two settings in the file /etc/sysconfig/apache2
    - APACHE_START_TIMEOUT="10"
    - APACHE_SERVER_FLAGS="SSL"
  - Configure the main server to use SSL encryption
    - Add directives to /etc/apache2/default-server.conf

```
SSLEngine on
SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
SSLCertificateFile /etc/apache2/ssl.crt/server.crt
SSLCertificateKeyFile /etc/apache2/ssl.key/server.key
```

  - Configure a virtual host to use SSL encryption
    - Define virtual host with a directive such as:
      - <VirtualHost *your_hostname*:443>

How to Configure OpenSSL for Connection Encryption (continued)

- The limitations of the SSL configuration
  - SSL setup as described in this section is a very basic configuration
  - For more information go to http://httpd.apache.org/docs-2.0/

Exercise 3-3 Configure an Apache Web Server

- In this exercise, you will do the following:
  - Part I: Install Apache
  - Part II: Test the Installation
  - Part III: Configure a Virtual Host for the Accounting Department
  - Part IV: Configure User Authentication
  - Part V: Configure SSL

Configure a Samba Server as a File Server

- Objectives
  - The Purpose and the Possibilities of Samba
  - How to Install and Set Up a Basic Samba Server
  - The Structure and Elements of the Samba Configuration File
  - How to Use the Samba Tools to Access SMB Shares from a Linux Computer
  - How to Configure a File Server With User Authentication
  - Additional Possibilities with Samba

The Purpose and the Possibilities of Samba

- Server Message Block (SMB) protocol
  - Network protocol that provides file and print services in a Windows network
- Samba enables Linux to use SMB
  - Use Samba server to provide file and print services for Windows clients
  - Use Samba tools to access SMB file and print services on a Linux system
  - Use Samba as a domain controller for Windows clients
- SMB services are provided by the NetBIOS protocol

The Purpose and the Possibilities of Samba (continued)

- The server side of Samba consists of two parts:
  - nmbd
  - smbd
- Samba tools to integrate Linux as client in a Windows environment
  - nmblookup
  - smbclient

How to Install and Set Up a Basic Samba Server

- Install following packages using YaST
  - samba
  - samba-client
  - samba-doc
- Start Samba daemons
  - rcnmb start
  - rcsmb start
- Automatically start Samba daemons
  - insserv nmb
  - insserv smb

The Structure and Elements of the Samba Configuration Files

- Configuration file /etc/samba/smb.conf
- Create a Section for the General Server Configuration

```
[global]
    workgroup = DigitalAirlines
    netbios name = Fileserver
    security = share
```

- Create a Section for the Files to be Shared

```
[data]
    comment = Data
    path = /srv/data
    read only = Yes
    guest ok = Yes
```

- Test syntax of configuration file with testparm

How to Use the Samba Tools to Access SMB Shares from a Linux Computer

- Use nmblookup for name resolution in a NetBIOS network
  - nmblookup Fileserver
- Use smbclient to access SMB shares
  - Browse the shares provided by a server
    - smbclient –L //Fileserver
    - smbclient –L //Fileserver –U tux (if authentication is required)
  - Access files provided by an SMB server
    - smbclient //Fileserver/data
    - Smbclient can be used as a command-line FTP client

How to Use the Samba Tools to Access SMB Shares from a Linux Computer (continued)

- Use smbclient to access SMB shares (continued)
  - Print on printers provided by an SMB server
    - smbclient //Printserver/laser –c ‘print letter.ps’
- Mount SMB shares into the Linux File system
  - mount -t smbfs //Fileserver/data /mnt
  - mount -t smbfs -o username=tux,password=novell //Fileserver/data /mnt

How to Configure a File Server with User Authentication

- Prepare the server for user authentication
  - Change the security option in the smb.conf file
    - security = user
  - User Level Security
    - Windows-compatible encrypted password file is stored in the file /etc/samba/smbpasswd
  - Sets an SMB password for the user tux
    - smbpasswd -a tux

How to Configure a File Server with User Authentication (continued)

- Configure a share that is accessible to only one user

```
[tux-dir]
    comment = Tux Directory
    path = /srv/share
    valid users = tux
    read only = no
```

- Configure shared access for a group of users

```
[accounting]
    comment = Accounting department
    path = /srv/share
    valid users = @accounting
    force user = tux
    force group = accounting
    read only = no
```

How to Configure a File Server with User Authentication (continued)

- Configure the export of home directories

```
[homes]
    comment = Home Directories
    valid users = %S
    read only = No
    browseable = No
```

Additional Possibilities with Samba

- You could:
  - Use Samba as member server of a Windows domain
  - Use Samba as domain controller
- Find more information about Samba at
  - The samba-doc package in the directory
    - /usr/share/doc/packages/samba/
  - The man page of smb.conf
  - The Samba project site at www.samba.org/

Exercise 3-4 Configure a File Server with Samba

- In this exercise, you will do the following:
  - Part I: Install Samba
  - Part II: Configure a Share for the User Geeko
  - Part III: Access the Share of the User Geeko With smbclient
  - Part IV: Mount Geeko's Share

Summary

- DNS comprises a hierarchical namespace
- FQDNs and their associated IP addresses
  - Are stored on authoritative DNS servers in a zone file
- Query a DNS server
  - Forward lookup
  - Reverse lookup
- DNS server uses BIND server software
- The host and dig commands may be used to test DNS name resolution

Summary (continued)

- LDAP directory service
  - Allows network users to query information for a wide range of uses
- LDAP resources are organized into a hierarchical tree structure
- Edit /etc/openldap/slapd.conf or use YaST
  - To configure LDAP server
- GQ LDAP browser allows you to query an LDAP database
- Apache Web server is the most common Web server on Linux systems

Summary (continued)

- Apache may be used to host several Web sites on a single computer (virtual hosts)
- OpenSSL may be used with Apache
  - To provide encryption for Web content
- Become a Samba server
  - Start the Samba and NetBIOS daemons
- testparm command
  - Detects syntax errors in Samba configuration file
- Connect to a Windows or Samba file server
  - Using the mount and smbclient commands