# Laboratorio di Amministratore di Sistema

## 4. Panoramica sui servizi di rete

*[Cisco ITESS II - Chapter 5]*

Università di Venezia – Facoltà di Informatica
feb-mag 2014 - A. Memo

**ver 2.2**

## Overview of Network Services

5.1 – Network Services
5.2 – Remote Administration and Access Services
5.3 – Directory Services
5.4 – Other NOS Services

# An Introduction to Network/NOS Services

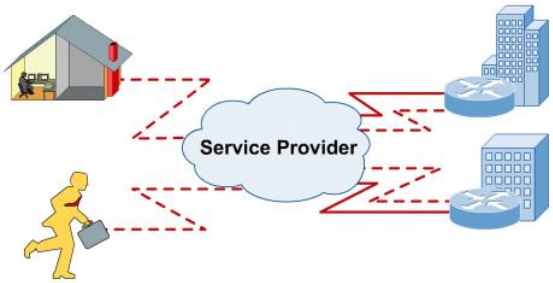
- Networking operating systems are designed to provide network processes to clients and peers.
- Network services include the World Wide Web (WWW), file sharing, mail exchange, directory services, remote management, and print services.

| Service | TCP/IP Protocol |
|---|---|
| World Wide Web Server | HTTP |
| File Transfer | FTP, TFTP |
| File Sharing | NFS |
| Internet Mail | SMTP, POP3, IMAP |
| Remote Administration | Telnet |
| Directory Services (Internet) | DNS, LDAP |
| Automatic Network Address Configuration | DHCP |
| Network Administration | SNMP |

- Most popular network processes rely on the TCP/IP suite of protocols

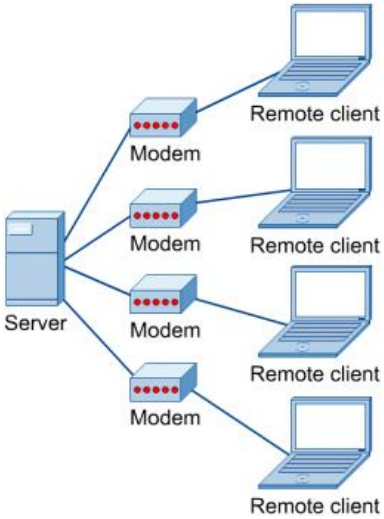
*Services vs Daemon*

# What is Remote Access?




- With a remote access connection, employees can access the corporate remote access server and log in to the network with their regular user account.
- Employees can then use all the resources that would be available from the office desktop computer.

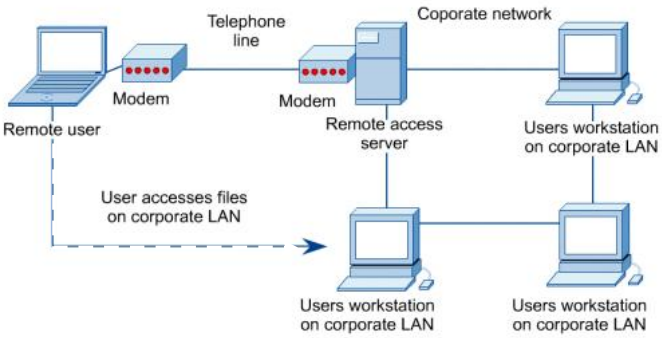
# Telecommuting




- Telecommuting (*telelavoro*) is attractive to employees because it saves travel time and other costs associated with working in an office.
- It saves the company money as well because office space for telecommuting employees is not required.
- Each modem requires its own separate telephone line.

# Mobile Users

- It can be difficult or impossible to store all the files needed on a laptop or notebook computer.



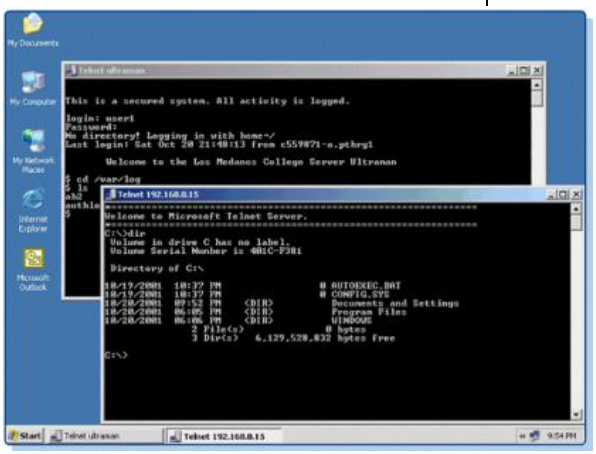

- It is a security threat as well because the laptop and its contents could be physically stolen.
- A better solution is for mobile users to dial in to the company LAN.

# Accesso Remoto - osservazioni

- Richiede che entrambi i nodi abbiano accesso ad Internet
- Il controllato deve avere installato un server dedicato
- Il controllato dovrebbe avere un IP statico o identificabile
- L'accesso può avvenire in modalità testo o a finestre
- Operazioni effettuabili:
  - accessione/spegnimento
  - visione o modifiche di setup e/o filesystem
  - accesso a periferiche hacking, malware, back door
- Windows: Remote Desktop, Terminal Services, Remote Microsoft Management Console
- Linux: VNC, SSH + Telnet, OpenSSH, Puppet

# Terminal Emulation Services

- Terminal emulation is the process of accessing a remote system via a local computer terminal.
- The local terminal runs software that emulates the look of the remote system terminal.
- The local user can type commands and execute programs on the remote system.

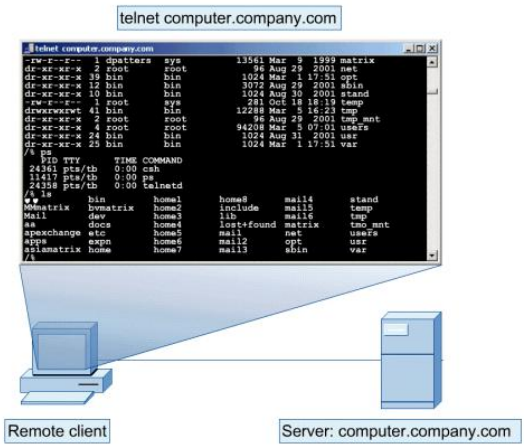



- The most common terminal emulation application is Telnet, which is part of the TCP/IP protocol suite.

*Xterm, PuTTY*

# Telnet services

- Telnet is the main Internet protocol for creating a connection with a remote machine.
- To be on one computer system and do work on another.
- Telnet has the following security considerations:
  - Hacking
  - Password guessing
  - Denial of Service (DoS)
  - Packet sniffing




*VNC (Virtual Network Computing)*
*RDP (Remote Desktop Protocol)*

# Configuring Remote Access for a Client

- Today most computers are connected to the network on a permanent basis through the systems network card.
- Sometimes establishing a remote connection to a computer must be done in other ways when the computer is located somewhere that is not connected to the network.
  - dialup connection
  - ISDN connection
  - DSL broadband connection

# Configuring Remote Access for a Client - PPP

- Point-to-Point Protocol (PPP) establishes a TCP/IP link between two computers using a modem.
- A PPP connection is designed to be in use for only short periods of time because it is not considered an “always-on” Internet connection.
- There are two ways to create a PPP connection, text-based utilities and GUI Dialer.

# Configuring Remote Access for a Client - PPP

1. Make an entry in the file

/etc/ppp/pap-secrets or /etc/ppp/chap-secrets

**The /etc/ppp/chap-secrets File**

```
# Secrets for authentication using CHAP
# client          server          secret          IP addresses
  00A0CC24BA02    *               asfc5934        *
  0002B388011A    *               56&#QRB         *
  00A0BB011A01    *               $%&GSDEYI       *
```

MAC address of the client

Server name that are connecting to

password

IP address of the server system

* = *any*

**P**assword **A**uthentication **P**rotocol - **C**hallenge **H**andshake **A**uthentication **P**rotocol

# Configuring Remote Access for a Client - PPP

2. Copy the files ppp-on and ppp-on-dialer from /usr/share/doc/ppp-2.3.11/scripts in a directory that is on a path, like /usr/local/bin
3. Edit this files with your ISP information

Konsole - rtalbot@Linux1-RNT:/usr/share/doc/ppp-2.4.1/scripts - Konsole

File Sessions Settings Help

```
#!/bin/sh
#
# Script to initiate a ppp connection. This is the first part of the
# pair of scripts. This is not a secure pair of scripts as the codes
# are visible with the 'ps' command.  However, it is simple.
#
# These are the parameters. Change as needed.
TELEPHONE=555-1212        # The telephone number for the connection
ACCOUNT=george            # The account name for logon (as in 'George Burns')
PASSWORD=gracie           # The password for this account (and 'Gracie Allen')
LOCAL_IP=0.0.0.0          # Local IP address if known. Dynamic = 0.0.0.0
REMOTE_IP=0.0.0.0         # Remote IP address if desired. Normally 0.0.0.0
NETMASK=255.255.255.0     # The proper netmask if needed
#
# Export them so that they will be available at 'ppp-on-dialer' time.
export TELEPHONE ACCOUNT PASSWORD
#
# This is the location of the script which dials the phone and logs
# in.  Please use the absolute file name as the $PATH variable is not
# used on the connect option.  (To do so on a 'root' account would be
# a security hole so don't ask.)
#
DIALER_SCRIPT=/etc/ppp/ppp-on-dialer
#
# Initiate the connection
#
# I put most of the common options on this command. Please, don't
# forget the 'lock' option or some programs such as mgetty will not
# work. The asyncmap and escape will permit the PPP link to work with
# a telnet or rlogin connection. You are welcome to make any changes
# as desired. Don't use the 'defaultroute' option if you currently
# have a default route to an ethernet gateway.
#
exec /usr/sbin/pppd debug lock modem crtscts /dev/ttyS0 38400 \
        asyncmap 20A0000 escape FF kdebug 0 $LOCAL_IP:$REMOTE_IP \
        noipdefault netmask $NETMASK defaultroute connect $DIALER_SCRIPT
~
```

New Konsole

telephone number

User ID
Password

client IP address
ISP IP address
Subnet Mask

*shared information for the PPP daemon*

*script location*

*correct configuration for the modem*

The ppp-on-dialer handles the “chat” sequence of the identification process

Konsole - rtalbot@Linux1-RNT:/usr/share/doc/ppp-2.4.1/scripts - Konsole

File Sessions Settings Help

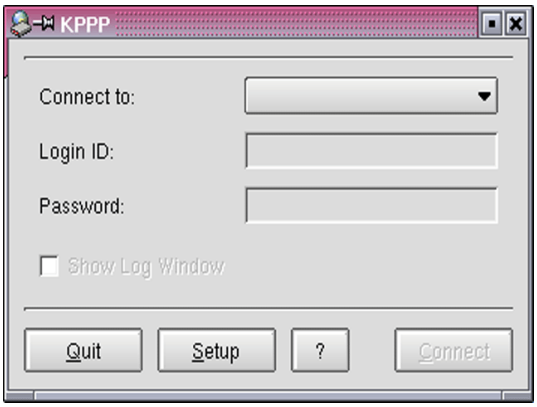
```
#!/bin/sh
#
# This is part 2 of the ppp-on script. It will perform the connection
# protocol for the desired connection.
#
exec chat -v                                            \
        TIMEOUT         3                               \
        ABORT           '\nBUSY\r'                      \
        ABORT           '\nNO ANSWER\r'                 \
        ABORT           '\nRINGING\r\n\r\nRINGING\r'    \
        ''              \rAT                            \
        'OK-+++\c-OK'   ATH0                            \
        TIMEOUT         30                              \
        OK              ATDT$TELEPHONE                  \
        CONNECT         ''                              \
        ogin:--ogin:    $ACCOUNT                        \
        assword:        $PASSWORD
~
~
~
"ppp-on-dialer" [readonly] 17L, 397C
```

New Konsole

# Configuring Remote Access for a Client - PPP

- PPP configuration can also be done from the GUI using the GUI dialing utilities.
- The GUI PPP dialer that comes with KDE is the KPPP dialer.

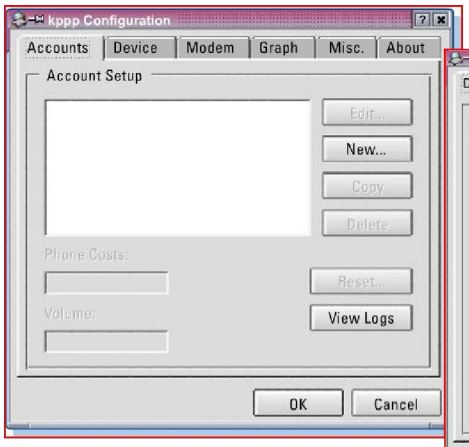
1. type kppp at the shell



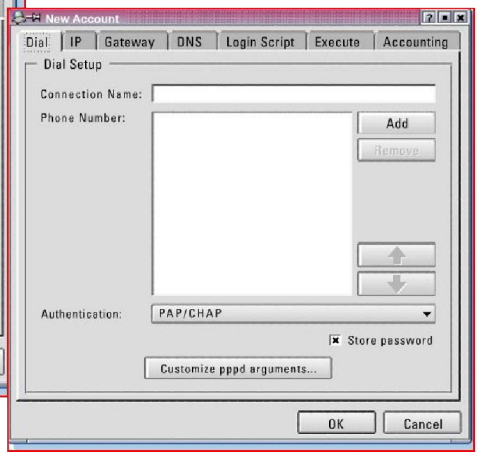

2. click on Setup

# Configuring Remote Access for a Client - PPP

3. click on New



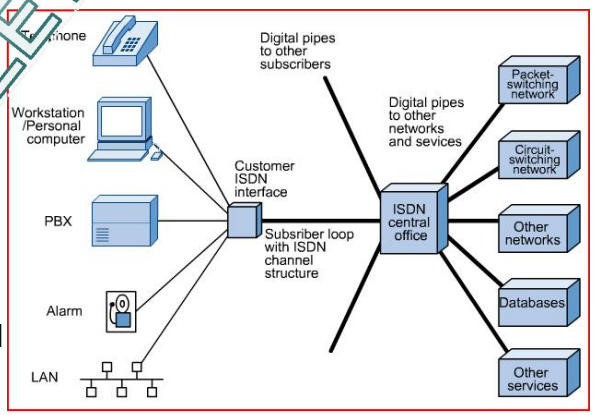

4. insert the data




# Configuring Remote Access for a Client - ISDN

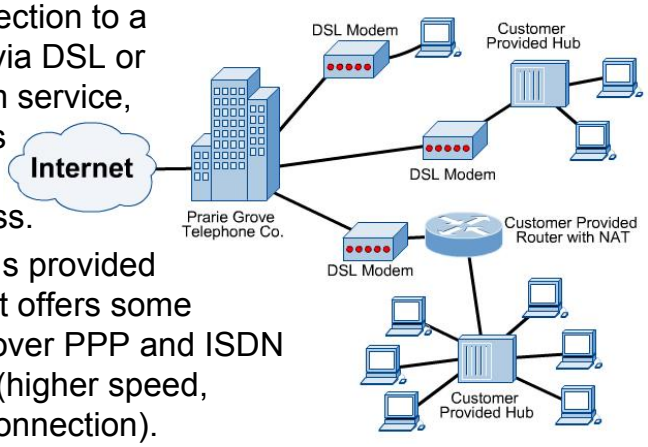
- ISDN has many advantages over using telephones lines.
- It uses a pair of 64 Kbps digital lines to connect, which provides a total of 128 Kbps throughput.
- This is better than using a telephone line that connects at a maximum speed of 56 Kbps.
- Instead of using a modem to connect to a remote computer, ISDN uses a terminal adapter.





# Configuring Remote Access for a Client - DSL

- A popular means of establishing a remote connection to a computer is via DSL or cable modem service, referred to as broadband remote access.
- This service is provided by an ISP but offers some advantages over PPP and ISDN connections (higher speed, permanent connection).




# Configuring Remote Access for a Client - DSL

- Dealing with Linux, two issues will arise using DSL service
  - hardware compatibility
    - internal modem (the drivers are hard to find)
    - external is the preferred method of connection
  - IP address assignement method
    - static IP address
    - DHCP
    - PPP over Ethernet (PPPoE)
    - PPP over ATM (PPPoA)

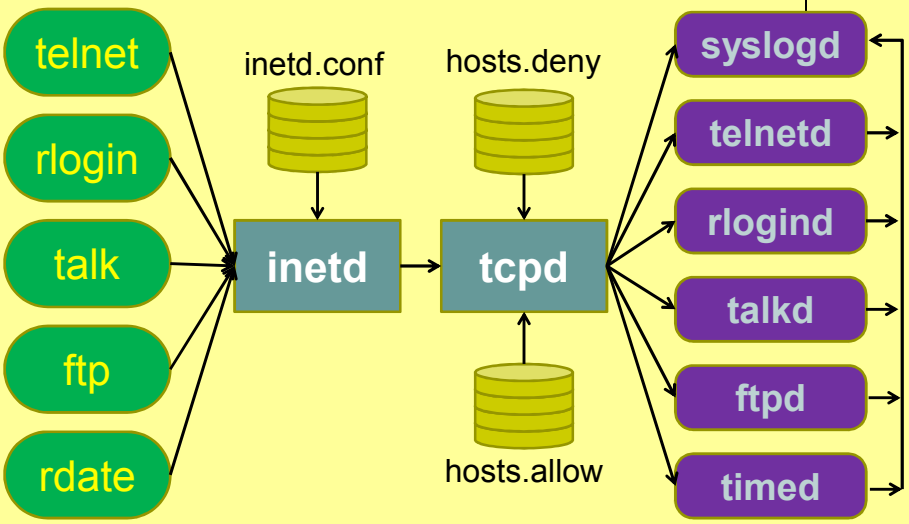
## Controlling Remote Access Rights - firewall

- When setting up a server for remote access, it is important to maintain a strict access rights policy.
- A **firewall** acts a barrier between one network, like the Internet for example, and another network, for example the network that the user is in charge of controlling security for.
- The firewall is placed between where these two networks interface, thus blocking unwanted traffic.
- The traditional way to setting up a firewall is to install a router that can block and control undesired traffic in and out of a network.

## Controlling Remote Access Rights - firewall

- Linux can be configured to provide firewall services, using four different methods:
  - **manually** (the most difficult but flexible)
  - **GUI** configuration tool (as Firestarter and Guarddog); they generate the scripts for users
  - **website** configuration, similar to GUI tools, but using web
  - **TCP wrappers**: normally a server is called by a client using the inetd (or xinetd) program. With TCP-wrappers inetd (or xinetd) calls tcpd program first; tcpd controls if the client is authorized to access the server. TCP wrappers use two files: /etc/hosts.allow and /etc/hosts.deny

## Funzioni del TCP wrapper




## Logica del TCP wrapper

Quando arriva una richiesta al TCP wrapper:

- **SE** la richiesta soddisfa una o più regole di */etc/hosts.allow*

  **ALLORA** l'accesso è accordato
- **ALTRIMENTI**
  - **SE** la richiesta soddisfa una o più regole di */etc/hosts.deny*

    **ALLORA** l'accesso è negato
  - **ALTRIMENTI** l'accesso è **accordato**

## Esempi di righe di *hosts.deny*

**daemon_list : client_list [ : shell_command ]**

*dove*

**daemon_lis***t è una lista di uno o più nomi di processi, separati da uno spazio o una virgola;*
**client_list** *è una lista di uno o più nomi o indirizzi di host, separati da uno spazio o una virgola;*
**shell_command** *è un comando di shell (è opzionale, viene eseguito se la condizione impostata è valida).*

Per *accettare* richieste SSH da IP del dominio example.com eseguendo …

```
sshd : .unive.it : spawn /bin/echo '/bin/dati'
```

*Per negare tutti i servizi TRANNE finger da pirati.net*

```
all EXCEPT in.fingerd : pirati.net
```

*Per negare gli accessi remoti:*

```
in.telnetd,in.sshd,in.rlogind: ALL
```

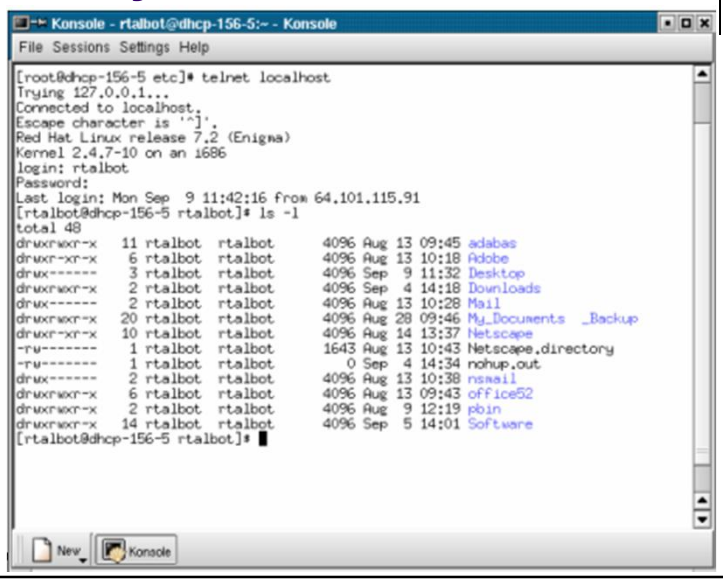
## Controlling Remote Access Rights - password and file permission

- A very useful method to control remote access to a server is setting up **passwords**
- Passwords are very useful when specifying who has access to servers such as e-mail servers, FTP, and Telnet severs for example.
- Enforcing a password forces the user to authenticate themselves in some way to the servers to gain access to the server resources.
- **File permissions** can be useful to give general access to files or certain directories without having to specify any particular user.

# Remote Administration to Linux System – text mode

- There are several tools for remote administration: text-mode login, GUI login, file transfer and dedicated protocols
- A user can use **Telnet** or **SSH** to remotely administer the Linux server.
- The correct command syntax for using Telnet in Linux is **telnet *hostname***, where hostname is the DNS name of the system the user are attempting to gain access to.
- SSH works the same way, however it does not use the **login:** prompt.
- SSH passes the current username to the system that the user is attempting to access remotely to authenticate the user.

# Remote Administration to Linux System – text mode



## Remote Administration to Linux System – GUI, file transfer

- To use a **GUI login**, the users will need to install X server
- A **file transfer** tool such as FTP can be used to transfer files from one system to another, edit them, and then send them back.
- The user can download the configuration files from the administrated server, locally edit them and upload on the same server.
- Lack of security and high vulnerability

## Remote Administration to Linux System – dedicated protocols

- Linux provides several tools to enable an administrator to remotely manage a computer:
  - SNMP (no diffused on Linux systems)
  - Samba Web Administration Tool (SWAT)
    - users can access the server remotely using a web browser, on port 901; allows only the access to the SAMBA functions of the server
  - Webmin
    - another web-based tool, uses port 10000
- The user will need to install the server version of this tools on the administrated system, and the client version on the administration system.

# Samba

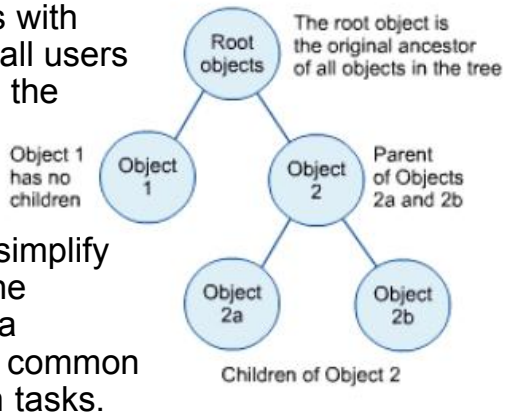
- **Samba** is a re-implementation of SMB/CIFS networking protocol (where **Server Message Block** is the standard protocol used by the Microsoft Windows network file system to share resources).
  - **smbclient** program works much like the interface of the FTP program, and allow you to get files from the server to the local machine, put files from the local machine to the server, retrieve directory information from the server, and so on.
  - **smbmount** is used to mount a network drive

# Remote Administration to Linux System – rmon & ssh

- **RMON** (Remote MONitoring) is a standard based on SNMP, that enables servers and clients to exchange network-monitoring data
- **SSH** (Secure SHell) is the most popular remote administration tool for Linux
  - SSH offers command line access over an encrypted tunnel
  - Two important SSH settings are:
    - PermitRootLogin → No
    - X11 Forwarding → No (for CLI) or Yes (for GUI)
- PuTTY is the most popular client-side software (for SSH, Telnet and rlogin)

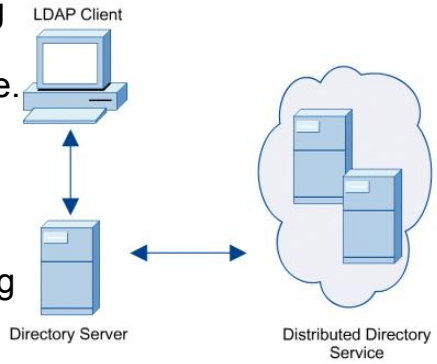
## What is a Directory Service?

- A directory service provides system administrators with centralized control of all users and resources across the entire network.
- They provide the ability to organize information and help simplify the management of the network by providing a standard interface for common system administration tasks.




## What is a Directory Service?

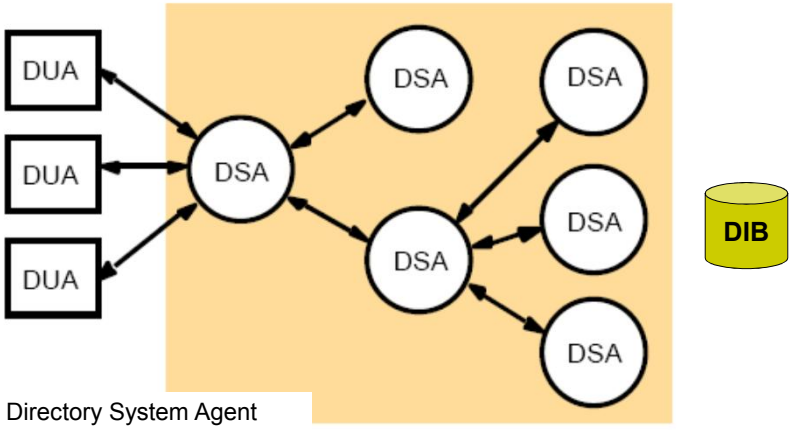
- Shared resources are published to the directory
- Users can locate and access them without ever knowing on which machine the resources physically reside.
- The files, directories, and shares that users access from a single point can be distributed across multiple servers and locations using distributed directory and replication services.



# Directory Service Standards

- To operate within a NOS, different directory services need to have a common method of naming and referencing objects.
- X.500 defines the Electronic Directory Service (EDS) standards.
- X.500 has three primary components:
  - DSA (Directory System Agent), manages the directory data
  - DUA (Directory User Agent), gives user access to the services
  - DIB (Directory Information Base), the information database
- An X.500-compliant directory service uses DAP (Direct Access Control)

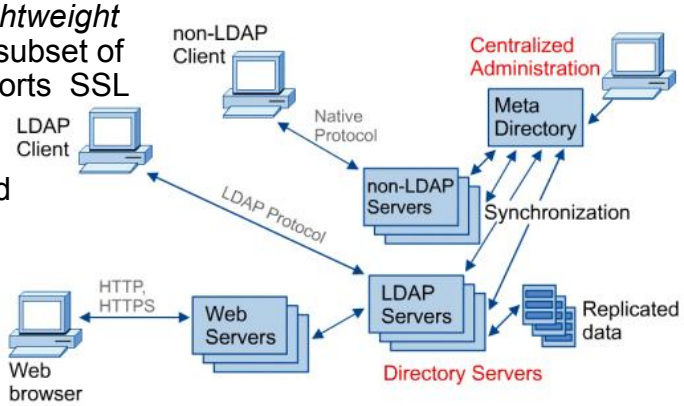
# X.500




DSA Directory System Agent
DUA Directory User Agent
DIB Directory Information Base

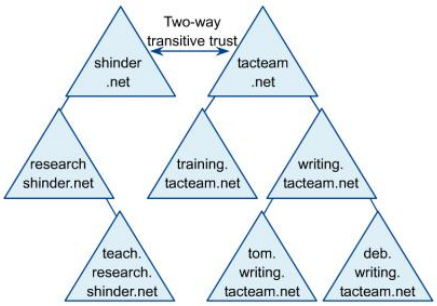
# Directory Service Standards

- **DAP** (*Directory Access Protocol*) manage the communication between DUA and DSA, but has a high overhead (OSI, layer 7)
- **LDAP** (*Lightweight DAP*) is a subset of DAP, supports SSL (Secure Sockets Layer), and integrates directories from different vendors.

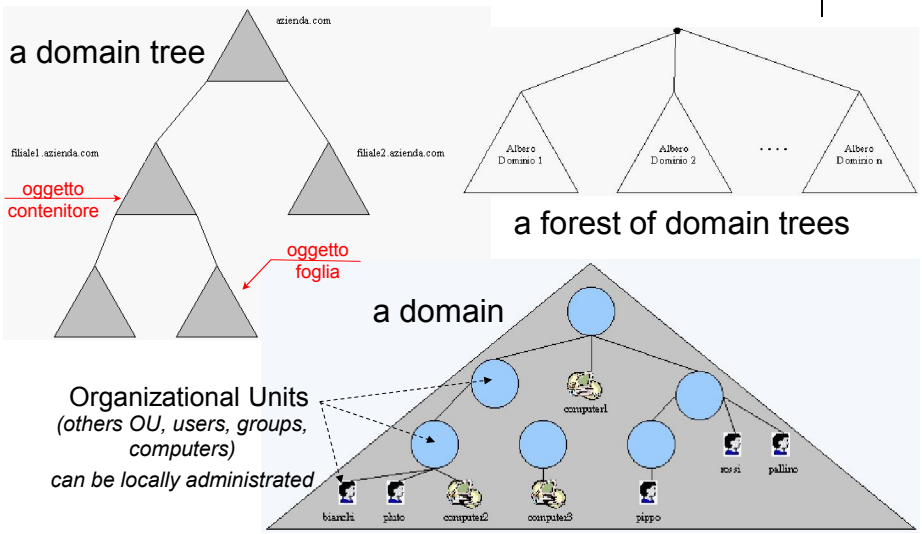



# Windows 2000 Active Directory

- The logical structure of the Active Directory is based on units called **Domains**.
- Windows 2000 networks can have multiple domains, organized into domain trees.
- These trees can be joined to other trees to form **forests**.
- Active Directory uses **Organizational Units** (OUs) to organize resources within domains.



# Windows 2000 Active Directory
## - terminology




# Windows 2000 Active Directory
## – DNS and Domain Controller

- **Active Directory** uses DNS naming conventions, there must be a DNS server on every network, and support Dynamic DNS
- To use Active Directory, at least one server must be configured as a **Domain Controller** (DC).
- It is recommended that there be at least two DCs in each domain, for fault tolerance.
- Windows relies on Active Directory <u>multimaster replication model</u> to update all the DCs of the forest when a change is made to any other DC
- All DCs contain a read/write copy of the Active Directory partition.

## Windows 2000 Active Directory – replication

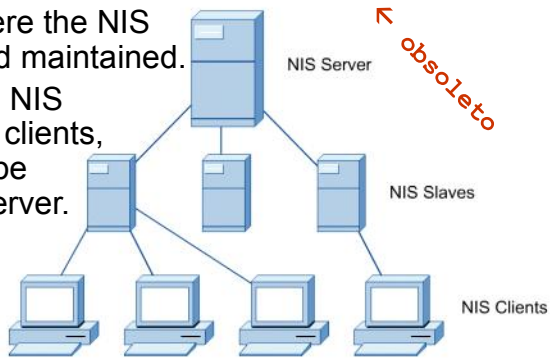
- Replication is the process of copying data from one computer to one or more other computers and synchronizing that data so that it is identical on all systems.
- Active Directory uses multimaster replication to copy directory information between the domain controllers in a domain.
- Administrator can establish replication policies (when and how often)

## Windows 2000 Active Directory – security and compatibility

- Each object in Active Directory has an **Access Control List** (ACL) that contains all access permissions associated with that object. Permissions can be either explicitly allowed or denied.
- There are two types of permissions:
  - Assigned permissions
  - Inherited permissions
- Active Directory run only on Windows Servers, but is LDAP-compatible and can be accessed and exchanged with other LDAP directory services.

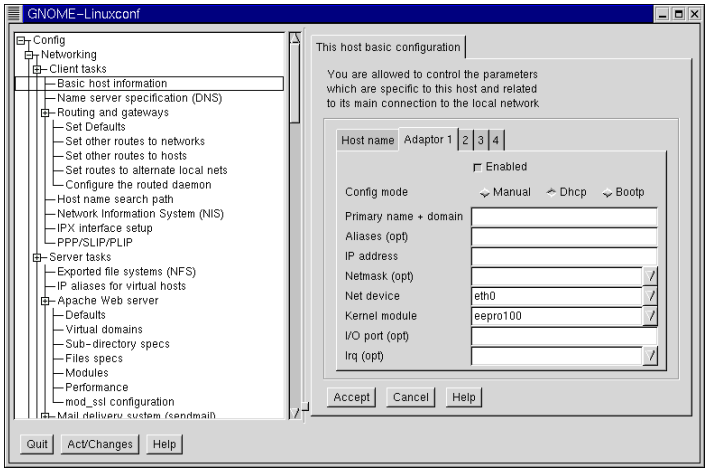
# Network Information Service (NIS) - structure

- Linux uses its own version of Directory Services called the **Network Information Service** (NIS).
- The network consists of the NIS server, slaves, and clients.
- The NIS Servers is where the NIS database is created and maintained.
- The NIS slaves provide NIS directory information to clients, but any changes must be performed in the NIS server.
- The NIS databases are copied to all the NIS slave servers.




# Network Information Service (NIS) - configuration

- If a user is configuring NIS during the installation of Linux, select its option and select the NIS domain name as well as the IP address of the NIS server.
- To configure NIS after installing Linux, the user uses the **linuxconf** utility to configure an NIS client.



## Network Information Service (NIS) – yppasswd

- The yppasswd command changes the network password in the NIS database (it is only a link to the passwd command)
- You obtain the same results with passwd –r nis
- To be able to use yppasswd the yppasswdd daemon must be running
- To make it possible to update the NIS password map from remote machines, the yppasswdd must be running on the NIS server
- The yypasswdd can be (remotely) started and stopped with:
  - startsrc –s yppaswdd
  - stopsrc –s yppaswdd

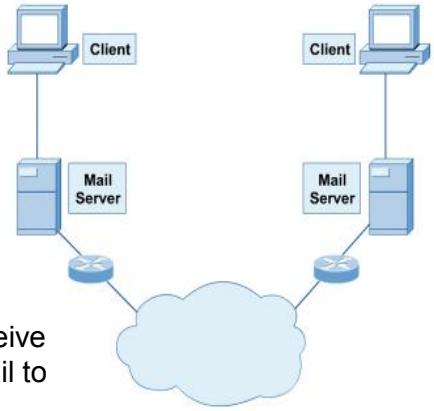
yp = yellow pages

## Network Information Service (NIS) – ypinit

- The ypinit command sets up NIS maps on a NIS master server or NIS slave server
  - /usr/sbin/ypinit [ -o] [ -n] [ -q] –m [*SlaveName* …]
  - /usr/sbin/ypinit –s*MasterName*

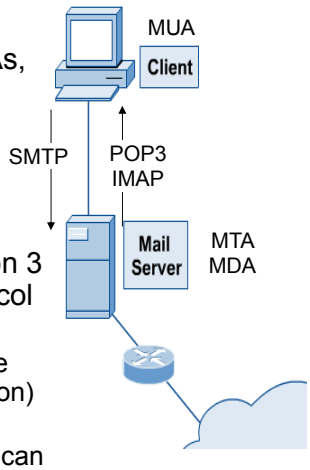
# Mail

- Virtually all mail services rely on TCP/IP or can at least act as a gateway between proprietary and TCP/IP mail services.
- Mail services are comprised of a combination of the following components:
  - Mail User Agent (**MUA**)
  - Mail Transfer Agent (**MTA**)
  - Mail Delivery Agent (**MDA**)
- **Sendmail** is the name of the most popular MTA used on UNIX and Linux servers.
- *Sendmail* relies on Simple Mail Transfer Protocol (SMTP) to receive mail from clients and forward mail to other mail servers.



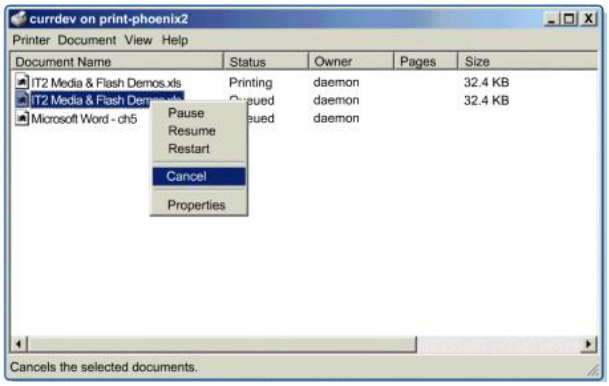

# Mail

- Popular mail clients (MUAs) include Microsoft Outlook, Eudora, and Pine.
- MUAs can compose and send mail to MTAs, such as Sendmail.
- MDA is a program that is responsible for routing received mail to the appropriate mailboxes on the mail server.
- To retrieve mail from a mail server, remote mail clients use Post Office Protocol version 3 (POP3) or Internet Message Access Protocol (IMAP).
  - POP3 is used by mail clients to authenticate mail servers and retrieve mails (no encryption)
  - IMAP stores e-mail on the mail server and allow users to access from multiple clients (can encrypt passwords)



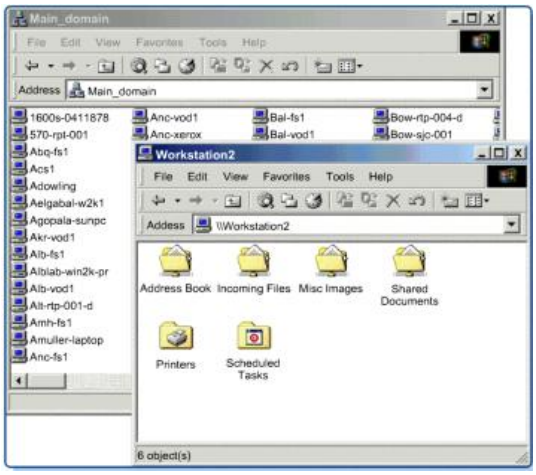
# Printing

- When a user decides to print in a networked printing environment, the job is sent to the appropriate queue for the selected printer.
- Print queues stack the incoming print jobs and service them using a "First In, First Out" (FIFO) order.
- The tools to manage the large number of print jobs give the ability to prioritize, pause and delete waiting print jobs



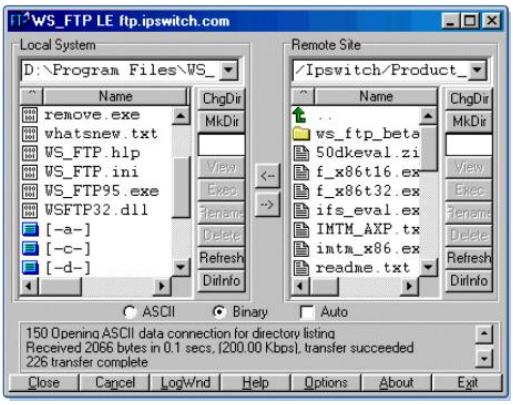

# File Sharing

- Typically, file sharing within a home or office network is based on Windows File Sharing or Network File Sharing protocols
- File sharing on the Internet is often done using the File Transfer Protocol (FTP).
- Peer-to-peer networking is popular among home users, but the technology has yet to be deployed as a widespread business solution.



# FTP (File Transfer)

- Many organizations make files available to remote employees, customers, and to the general public via File Transfer Protocol (FTP).
- FTP servers can be configured to allow anonymous access.
- FTP is a session-oriented protocol.
- FTP connections are established through GUI programs or CLI commands.




# FTP (File Transfer)

- Standard CLI command:

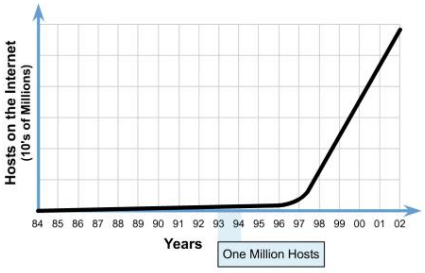
  ftp *hostname* or ftp *IP_Address*

- FTP services are typically not enabled by default on NOSs.
- FTP server have historically been a target of DoS attack.

| Action | Command syntax |
|---|---|
| Enable binary transfer mode | binary |
| Enable ASCII transfer mode | ascii |
| Enable hash mark progress indicators | hash |
| Change local directory | lcd <local-directory> |
| Change remote directory | cd <remote-directory> |
| Download a file | get <remote-file> |
| Upload a file | put <local-file> |
| Change remote directory | bye |

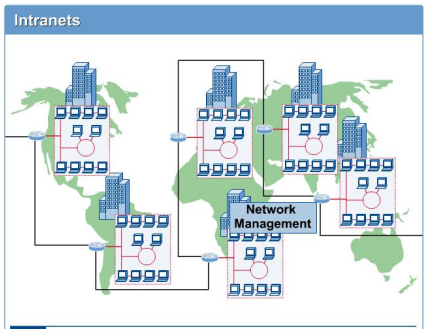
# Web Services

- The World Wide Web is now the most visible network service.
- In less than a decade, the World Wide Web has become a global network of information, commerce, education, and entertainment.
- In the early 1990s HTTP was used to transfer static pages composed of text and images (in HTML)
- Now HTTP delivers dynamic contents and transfers files
- HTTPS supports data sent securely over the Internet
- The most common web server software packages are Microsoft Internet Information Services (IIS) and Apache Web Server




# Intranet

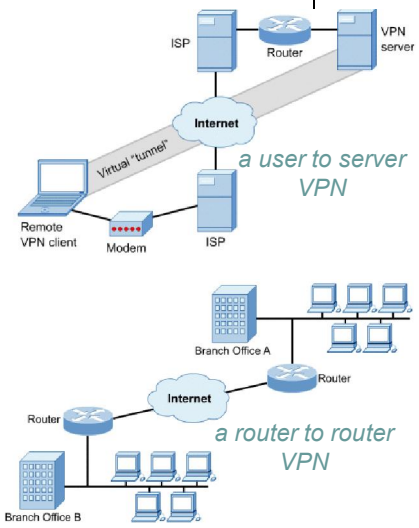
- **Intranet**s use the same technology used by the Internet, including HTTP over TCP/IP, web servers, and web clients.
- The difference is that intranets do not allow public access to private servers.
- One approach to building intranets is to configure them so that only on-site users can access the intranet servers.
- This is typically accomplished by using an Internet firewall.




*inter == between*
*intra == within*

# Extranet

- **Extranets** are configured to allow employees and customers to access the private network over the Internet.
- To prevent unauthorized access to the private network, extranet designers must use a technology such as **virtual private networking**.
- VPNs rely on encryption software, usernames, and passwords to ensure that communication occurs privately, and only among authorized users.




# Extranet

| Network Types | |
|---|---|
| Internet | • Spans the entire globe<br>• Unrestricted public access |
| Intranet | • Network hardware used to create boundries and restrict access<br>• Access is only granted to members of that Intranet, typically within a single organization |
| Extranet | • Network hardware used to create boundries and restrict access<br>• Access is only granted to members of that Extranet, including both internal members and external members |

## Automating Tasks with Scripts Services

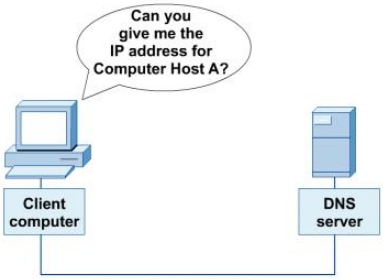
- A script is a simple text program that allow the user to perform many automated tasks efficiently
- Scripts are considered to be much simpler than the standard programs and applications found in a NOS.
- The operating system sequentially processes the lines of code in a script file whenever the file is run.
- Many different scripting languages exist, and each offers their own advantages to the user:
  - Visual Basic script (VBScript), in Windows systems
  - JavaScript, in web pages
  - Linux shell scripting
  - Perl, PHP, TCL, REXX, Python, ....

## Automating Tasks with Scripts Services

- The majority of scripting is performed by system administrators and experienced users.
- The following examples demonstrate common scenarios where scripts are an appropriate solution:
  - Logging on to the NOS, with additional tasks
  - Printing messages to the screen
  - Installing software
  - Automating complicated commands

# Domain Name Service (DNS)

- The Domain Name Service protocol translates the Internet name into an IP address (directory lookup service)
- Hostnames and the DNS services that computer systems run are all linked together.
- The Internet name that the DNS resolves to the IP address is also called the Hostname.
- The first part of the hostname is called the Machine Name and the second part is called the Domain Name (like Internet domains).




# Domain Name Service (DNS) – basic configuration

- BIND (Berkley Internet Name Domain) is the project which maintains the DNS suite
- named is the daemon process that responds to DNS queries from remote machines
- To start named you can
  - start the daemon with # /etc/init.d/named start
  - or configure BIND to stat automatically with # chkconfig –level 35 named on
- The file /etc/resolv.conf is used by DNS clients to determine both the location of their DNS server and the domains to wich they belong.
- The file /etc/hosts lists the name and IP address of local hosts
- The utility **dig** is a flexible tool for interrogating DBS name servers ( # dig server name type)

## DHCP

- Dynamic Host Configuration Protocol (DHCP) enables computers on an IP network to receive network configurations from the DHCP server.
- These servers have no information about the individual computers until information is requested.
- DHCP also allows for recovery and the ability to automatically renew network IP addresses through a leasing mechanism.
- This mechanism allocates an IP address for a specific time period, releases it and then assigns a new IP address.
- Linux can use three different DHCP clients: pump, dhclient, dhcpd

## DHCP - configuration

- When DHCP starts it reads the file /etc/dhcp.conf (a sample copy in /usr/share/doc/dhcp-???/dhcpd.conf)
- For the first time, you need the file dhcpd.leases. Create it with

  #touch /var/lib/dhcp/dhcpd.leases
- To start dhcpd you can
  - start the daemon with # /etc/init.d/dhcpd start
  - or configure dhcpd to stat automatically with # chkconfig –level 35 dhcpd on

# Domains

- A **domain** is a logical grouping of networked computers that share a central directory or database.
- Domains have several advantages:
  - Centralized administration since all user information is stored centrally.
  - A single logon process that enables users to access network resources as well as specify permissions that control who can and cannot access these services.
  - The ability to expand a network to extremely large sizes throughout the world.