INTRODUCTION

Network:- Inter Connection of Communication.

NETWORKING:- Communication between the Inter Connected devices.

Types of NETWORKS:-

Local Area Network:- operate with in a geographical location provides full-time Connectivity to local services.

METRO POLITAN AREA NETWORK:- Spans with in a city provides full time & part-time Connectivity.

WIDE AREA NETWORK:- In Implements DQDB Architecture. DQDB (Distributed que Dual Bus) operator over a large geographical location provides full time & part time Connectivity.

Requirements to establish a N/W

1. Systems.
2. Mediam:- Technically Called
   guided media Ex:- Co-axial Cable, optical cable
   Un guided media Ex:- Infrared, Blue tooth, Satelite Comm-
3. NIC (Network Interface Card):- Technically Called Network Adaptor. it gives physicall Id to System Called MAC ADDRESS → 12 digit Code. first-Six digits are Manufacturer's another Six given by NIC organization.

NIC :- → MEDIA ACCESS CONTROL

MAC CHIP

↓

MAC ADDRESS

↓

48 bit binary

↓

12 digit hexa decimal

Ex:- A 2B 3C 40 5E 6F

↓ ↓

Manufacture NIC organizat

vender ID

to get MAC ADDRESS

in windows xp => getmac (or) ipconfig

win 98 => win ipcfg

Types of NIC CARDS:-

1. ARC Net
2. TOKEN NET. } → Not using now.
3. ETHERNET.

ethernet cards:-

① standard → 10 MBPS DTR

② fast → 100 MBPS DTR

③ Gigabyte → 1000 MBPS DTR.

DTR ↖ 10 base 2 } → Not using now
10 base 5 } → Not using now
10 base (T) → Twisted pair cable
100 base T
1000 base T
10 base (F) → Fiber optic cable.

» Mbps

MEDIA :—

1. Guided media :— it's have particular physical path Ex :— Cables.
2. Unguided Media :— it's don't have any particular path Ex :- wireless, satelite Signals.

CABLES :—

1. Co-axial cables.
2. Twisted pair cable.
3. Fiber optic cable.

Twisted pair Cable :—

→ wires are twisted.
→ 1 pair is for Sending Signals.
2 pair is for Recieving Signals.
→ More Number Twists to get More DTR
→ Twisted pair Cable Types.

① STP ② UTP
↓ ↓
Shielded T.P Unshielded T.P


UTP :-

RJ (Register Jecou

Category	No. of pairs	DTR	USER
Cat 1	2 (4 wires)	2 Mbps	Telepho
Cat 2	4 (8 wires)	4 Mbps	
Cat 3	4 wires.	10 mbps	RJ 45
Cat 4	"	16-20 mbps	Net
Cat 5	"	100 mbps	purp
Cat 5e	"	500 mbps	
Cat-6	"	1000 mbps	

Transmition types :-

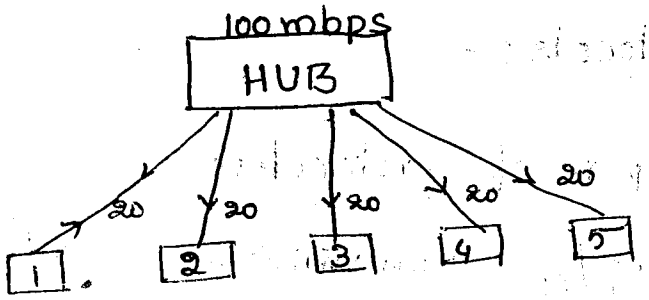
1) unicast → one to one Communication. uni-di
ional Transmission.
2) Broad Cast → one to all
3) Multi Cast → one to group (server / clients

Topology :-

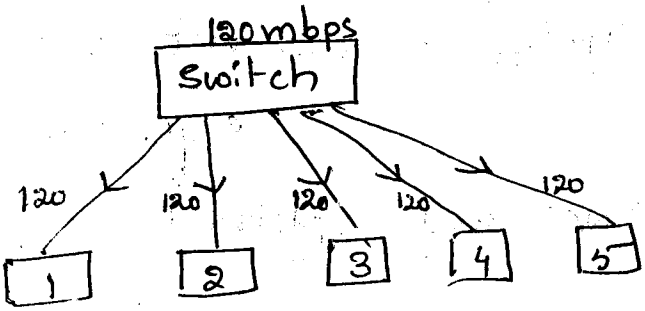
Types of Topologies.

1. Bus. } → Not using Now
2. RING. }
3. STAR.
4. MESH.
5. TREE.
6. Hybrid.

STAR :- All System Connect in to a
Centralised device it May be HUB / swit



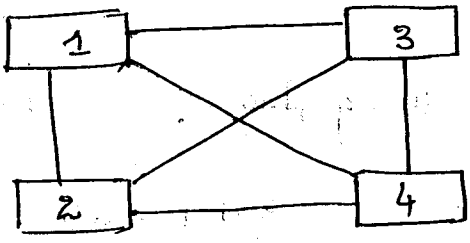
With HUB All System's sharig band width.



With Switch All System's get same band width.
first time Switch Taken All System Mac Codes
after than work like Not share the data.

HUB	Switch
1. Any time works like Broad Cast	1. first time Broad Cast After words unicast.
2. shared Band width.	2. No sharing.
3. DUMMY	3. Intelligent.
4. less Expensive	4. More Expensive.

MESH:-



Each every System Connected to all other System. this is used for Man network.

protocols :-

Types of protocoles :-

① Tcp/Ip :- Transmission control protocol/ Internet protocol

② Ipx/spx :- Interviet packet Enchange / sequential packet Enchange.

③ NET BEUI :- Network BIOS Extended us Interface.

④ APPLE :- (apple.

I/P ADDRESSING :-

there are Two versions

IpV4	IpV6
↓	↓
32 bit width	128 bit width.
(0's & 1's)	(0's & 1's)
↓	↓
2^{32} Combinations.	2^{128} Combinations.
↓	↓
This are using now	for future purpose

IpV4 :- 32bit width

↓

(0's & 1's)

↓

xxxxxxxx . xxxxxxxx . xxxxxxxx . xxxxxx xx

quode dotted decimal notation.

n=0 => 00000000.00000000.00000000.00000000

0.0.0.0

n=1 => 11111111.11111111.11111111.11111111

255.255.255.255

Range of IPv_4

0.0.0.0 to 255.255.255.255

priority bit:- Left most bit of the first octet. with this help IPv_4 classified 5 classes.

class	priority bit	Range.
class A	0	0.0.0.0 to 127.255.255.255
class B	10	128.0.0.0 to 191.255.255.255
class C	110	192.0.0.0 to 223.255.255.255
class D	1110	224.0.0.0 to 239.255.255.255
class E	1111	240.0.0.0 to 255.255.255.255

Ip ADDRESS is divided into Network & Host portion

→ class A => N.H.H.H → one Network, 3 Hosts

→ class B => N.N.H.H → Two Networks, Two Hosts

→ class C => N.N.N.H → Three Networks, one Host.

INTRODUCTION

Network:- Inter Connection of Communication.

NETWORKING:- Communication between the Inter Connected devices.

Types of NETWORKS:-

Local Area Network:- operate with in a geographical location provides full-time Connectivity to local services.

METRO POLITAN AREA NETWORK:- Spans with in a City provides full time & part-time Connectivity.

WIDE AREA NETWORK:- In Implements DQDB Architecture. DQDB (Distributed que Dual Bus) operator over a large geographical location provides full time & part time Connectivity.

Requirements to establish a N/W

1. Systems.
2. Mediam:- Technically Called
   guided media Ex:- Co-axial Cable, optical Cable
   Un guided media Ex:- Infrared, Blue tooth, Satelite Comm-
3. NIC (Network Interface Card):- Technically Called Network Adaptor. it gives physical Id to System Called MAC ADDRESS → 12 digit Code. first Six digits are Manufacturer's another Six given by NTC organization.

4. Types of N/W DEVICES:-

(a) HUB:- it is generally used to Connect all devices on a network so that they can Communicate with each other. it always do broadcasting it's reduces the Network perfor this is the back drop of the HUB.

(b) SWITCH:- like Hub, It is also used to connect all devices on a network. So that t can Communicate with each other. But fi time it will do broadcasting New- it do point to point Communication.

(c) ROUTER:- ROUTER is device which allow communication between two (or) more diffe network present in different geographical locations.

5. operating System:- it provides interfac between user and Hard ware device.

6. I/P ADDRESS:- which provides logical Identity for System with in the Netwo

The HISTORY M.S N/W operating Syste

WIN NT 3.01 → 1993
3.51 → 1994
4.0 W→ 1996
5.0 WOSR renamed as win Server

NT 4.0 :—

flavours :—

WIN NT work station
WIN NT SERVER EDITION
WIN NT Terminal service Edition.

WINDOWS 2000 :—

flavours :—

1. Windows 2000 professional.
2. windows 2000 Server.
3. windows Advance Server
4. windows 200 Data Center Server.

WINDOWS 2003 :—

Flavours :—

1. windows 2003 standard Edition
2. windows 2003 Enterprise Edition
3. windows 2003 Data Center Server
4. windows 2003 web Edition.

FEATURES OF WINDOWS 2003

→ Built on NT Technology.
→ 32/64 bit operating System.
→ Availability.
→ Scalable.
→ Easy Installation.
→ Larger Hard ware Support / Supports plug & play.
→ Inbuilt Terminal service
→ ACTIVE DIRECTORY

→ Second logon service.
→ Remote Installation Service.
→ Improved security.
  (i) kerberos version 5 (one of the protocol na
  (ii) Internet protocol security.
  (iii) Support for Smart Card.
→ Distributed file System.
→ Centralized deployment of Applications.
→ DNS Dependency.
→ Back up on any Media.
→ Supports FAT16, FAT32, NTFS(EFS)
→ volume Shadow Copy.
→ DISK Quotas.

I/p ADDRESSING :— it has been classified in
Ipv_4 which is a 32 bit length Address. IPv
which is 128 bit length Address. Ipv_4 it Conta
32 bit Address is in the form binary notat
These 32 bit length as been divided into
decimal notation based on octet.

1 octect = 8bits.

Minimum :— 00000000 . II . III . IV → 0.0.0.0
Maximum :— 11111111 . II . III . IV → 255.255.255

The total range of Ip Address are
0.0.0.0 to 255.255.255.255 which is n
to be near 4.2 billion Addresses. The
Total Range Ip Address are classified in

(1) class A → 0 — priority bit

(2) class B → 10 — "

(3) class C → 110 — "

(4) class D → 1110 — "

(5) class E → 1111 — "

class A, B, C are in Lan & wan purpose.

class D is for multicasting.

class E is for Research & Development.

To Identify the Range of each class a bit called priority is used. it is the left most bits in the first octet.

class	Range
A	0.0.0.0 – 127.255.255.255
B	128.0.0.0 – 191.255.255.255
C	192.0.0.0 – 223.255.255.255
D	224.0.0.0 – 239.255.255.255
E	240.0.0.0 – 255.255.255.255

0.0.0.0 is Called Global ID

255.255.255.255 is Called Broad Cast ID

127.0.0.0 Network is use to check of Compatibility of TCP/IP properties.

IP ADDRESS is divided into Network & Hal-portion

→ class A is written as N.H.H.H

→ class B " " " N.N.H.H

→ class C " " " N.N.N.H

TO ASSIGN IP ADDRESS

Right click on Network properties

↓

properties

↓

Local Area connection

↓

Select TCP/IP

↓

USE THE FOLLOWING IP ADDRESS

↓

GIVE IP ADDRESS (ok) (CLOSE)

private Range I/p ADDRESSES :—

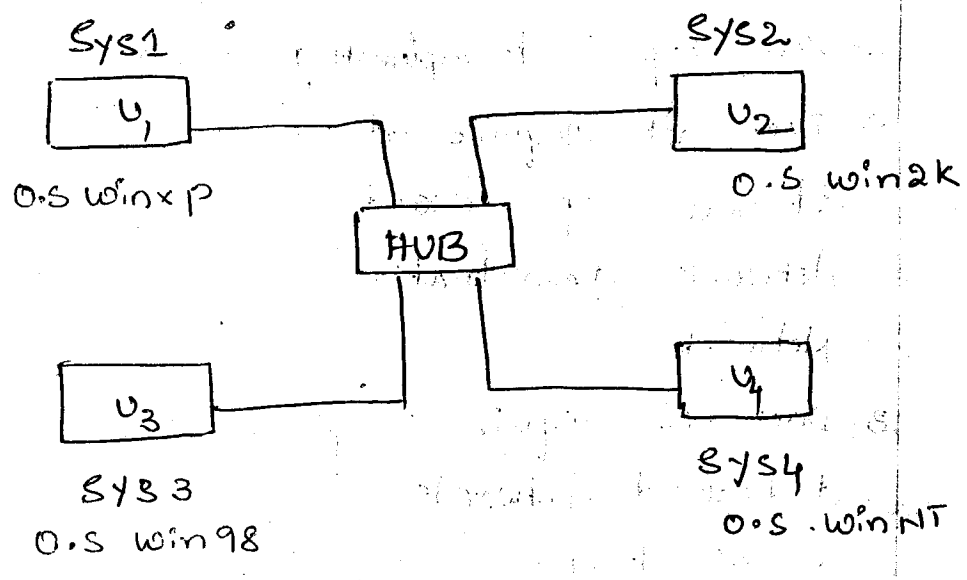
class A 10.0.0.0 to 10.255.255.255

class B 172.16.0.0 to 172.31.255.255

class C 192.168.0.0 to 192.168.255.255

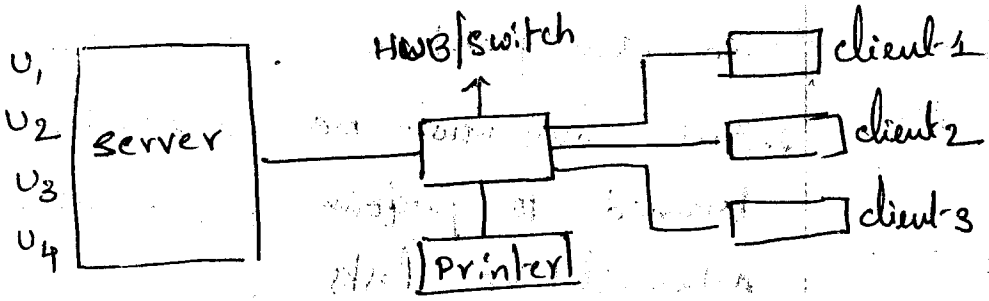
Logical Topologies

1 :- WORK GROUP MODEL / PEER TO PEER :-



logical grouping of Computer which access the resources are (or) more Systems. There is no centralized management optimised for Smaller Network.

2. DOMAIN MODEL / client - Server network :-



The logical grouping of Computers which as across the resources from are (or) more Systems with Centralized Data base for management this preffered for client- Server Environment. All the Systems has depends on System called as Server.

ADVANTAGES:→

PEER-PER NETWORK	client/server Net
1. Less Expensive to implement	1. provides better Sec
2. Does not require additional specalized Network administration Network.	2. Easier to administ when the Networ large because Admi tion is Centralized
3. Does not require a dedicated Network administrator.	3. All data can be up from one location.

DIS ADVANTAGES:—

PEER - PEER NETWORK	CLIENT / SERVER N
1. If network is large administration becomes un manageable.	1. Requires Expens more powerful Hoo for server.
2. Each user must be trained to perform Adminstative tasks.	2. Requires a profe Administrator.
3. Less Secure.	3. Have a single failure user data ble. if server is d

ACTIVE DIRECTORY (7.0 - 294)

Active directory is a Directory Service which contains information of all user accounts and shared resources on a network.

features:-

→ Active directory is a centralized Hierachical directory Data base.
→ centralizes control of Network Resources.
→ centralizes & Decentralizes resource management.
→ stores object securely in a logical structure.
→ optimizes Network traffic.
→ provides user logon and authentication service using kerberos.
→ To organize and manage.
  (i) user Accounts (ii) Computers
  (iii) groups (iv) Network resources.
→ Enables authorized user to easily locate N/w resources.
→ Fully Integrated Security.
→ Easy Administration using group policy.
→ Scalable to any size network.
→ Flexible

NEW FEATURES IN AD 2003:-

→ Rename Computer name and Domain name
→ Cross Forest Trust Relationship

TO INSTALL ACTIVE DIRECTORY

Requirements :-

1. windows server 2003 work group station.
2. A static IP ADDRESS.
3. 250 MB ∧ space (NTFS partition)
4. DNS
5. operating system CD.

START

↓

RUN

↓

DCPROMO

↓

welcome WIZard O.S Compatibility

↓

select Domain Controller for New Domain

↓

Select a Domain a new forest

↓

give the Domain name

↓

INET BIOS NAME

↓

DATA BASE ∧ Log folders

↓

Sys vol folder

Select INSTALL DNS

↓

select- permission Compatable (only with w-2000 & w-2003)

↓

DSRN, Confirm password

↓

finish & restart now.

To get type:—

START

↓

RUN

↓

GET TYPE

after Installing AD

START

↓

RUN

↓

CMD

↓

NETACCOUNTS.

AD FILES:-

DIRECTORY

1. ADDT (ACTIVE DOMAINS & TRUSTS)
2. ADSS (ACTIVE DIRECTORY SITES & SERVI
3. ADUC (" " users & Computers
4. DCSP (Domain Controller Security policy)
5. DSP (Domain Security policy)

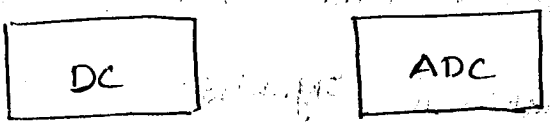
Short Cuts in RUN:-

1. DOMAIN.MSC (ADDT)
2. DS SITE.MSC (ADSS)
3. DSA.MSC (ADUC)
4. DCpol.MSC (DCSP)
5. DOMpol.MSC (MSP)

AD
↓
NTDS
↓
NTOS.DIT → Directory Information Tre
↓
Net work Technology Directory Service

To maintain the Active DIRECTORY Data base in another Syste we need to Configure additional Domain Control (ADC).

ADC :- Maintains the Complete directory - Service information as a back up Existing Domain troller to Configure ADC.



I.p ADDRESS:- 10.0.0.101 10.0.0.102

DOMAIN :- 10.0.0.101 10.0.0.101

START

↓

RUN (DCPROMO)

↓

NEXT

↓

NEXT

↓

Select ADC

↓

NEXT

↓

Give the Administrator name & password & Domain name

↓

NEXT

↓

BROWSE & select Domain name.

↓

NEXT

↓

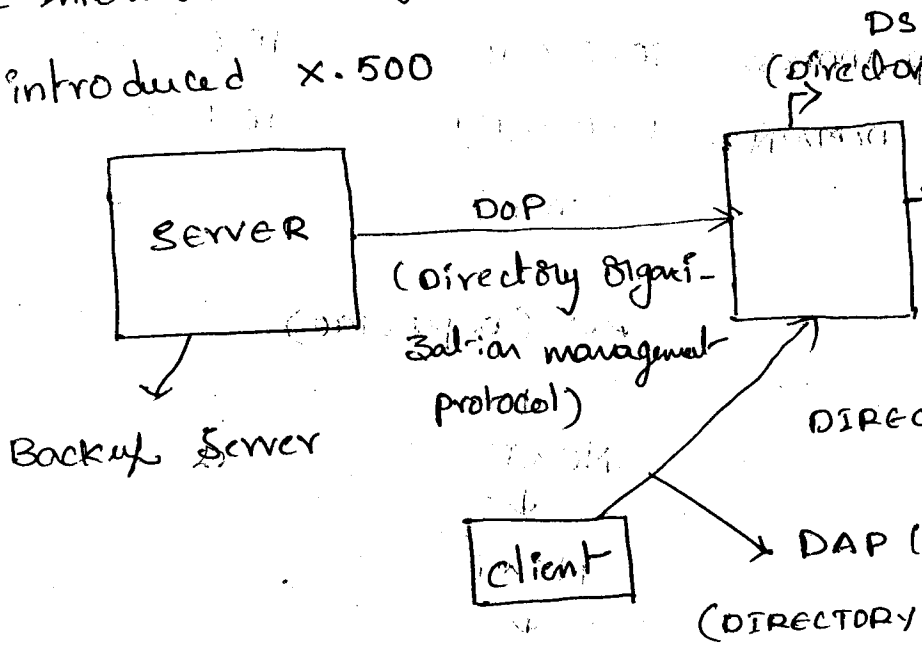
NEXT

↓

FINISH

TO DIRECTORY SERVICES EVOLVE

Earlier we had no data base standard
ITU (International Telecommunication union) & IS
(International organization for standardizati
introduced X.500



→ Active DIRECTORY Is based on LDAP proto

DAP:- Directory Access protocol is based o
OSI layers it was first Introduced in
"BANYAN VINES" & DATA BASE was named
as "STREET TALK"

LDAP:- Light weight Directory Access proto
based on TCP/IP layer. It was fir
Introduced by "novell" & data base wa
Named as "NDS (NETWORK DOMAIN SERVI

Logical Components of AD

1. Domain.
2. TREE.
   - → parent / Root.
   - → child / Branch.
3. FOREST.

DOMAIN:-

→ Domain is a logical secure, administrative boundary.

→ Creating the initial domain Controller in a network also creates the domain. You can't have a domain without at least one domain Controller.

→ Each domain in the directories identified by a DNS Domain name.

TREE:-

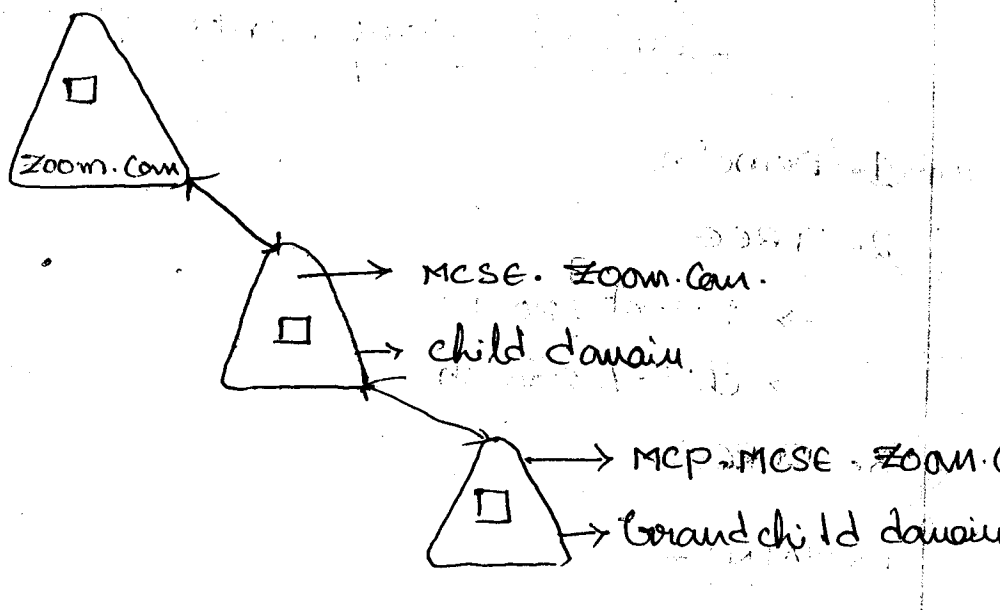
→ Tree is a set of one (or) more domains with Contiguos name.

→ If more than one domain exists, you can do Multiple domains into heirarchical Tree structure.

→ The first domain Created is the root domain of tree.

→ other domains in the same domain tree domains

→ [illegible]



TOCREATE THE CHILD DOMAIN

START

↓

RUN (DCPROMO)

↓

NEXT

↓

NEXT

↓

Select domain Controller for New Domain

↓

Select child domain in an Existing domain Tree

↓

give the pregicious.

↓

Browse (select the Domain name)

↓

NEXT

↓

NEXT

↓

FINISH.

FOREST :-

→ Multiple domain tree within a Single forest- donot form a contiguous New Space.

→ Although trees in a forest- don't share a nearness space, a forest- will have a Single root- domain, called the forest- root domain.

→ The forest- root- domain is the first-domain created in the forest.

→ There two forest- wide predifined groups in forest- root domain.

(i) Enter prise Administrator.

(ii) SCHEMA ADMINISTRATOR.

NEW DOMAIN EXISTING FOREST

START

↓

RUN(DCPROMO)

↓

NEXT

↓

NEXT

↓

SELECT DOMAIN

for NEW DOMAIN

↓

Select- New Domain Tree

in Existing forest-

↓

give the pregicious

Restart the System

↑

NEXT

↑

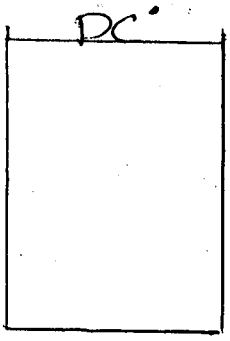
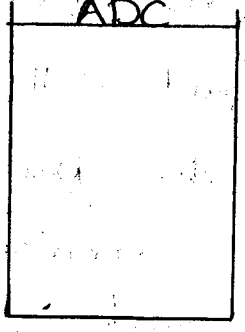
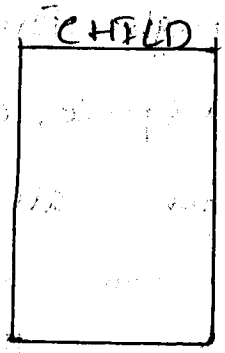
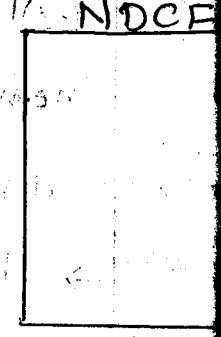
NEXT

↑

give the New domain

↑ name

MCSE.

Zoom.com	Zoom.com	Zoom.com	Zoom.sio.
DC	ADC	CHILD	NDCE
			
Ip :. 10.0.0.1	10.0.0.2	10.00.3	10.0.0
D:- 10.0.0.1	10.0.0.1	10.0.0:1	10.0.0
primary	back up	primary	prime

In Active directory domain Construct we can observe the Total tree Configuration.

DIRECTORY PARTITIONS

1. SCHEMA :— Contains definations and rules Creating and manipulating all objects and Attributes.
2. CONFIGURATION :— Contains information about Active DIRECTORY structure.
3. DOMAIN :— Contains information about all domain - Specific objects Created in AD.
4. Application :— Contains Application DATA
   - → FOREST DNS ZONE.
   - → Domain DNS ZONE.

PHYSICAL COMPONENTS

1. Domain Controller.
2. Sites.

Sites:-

→ A set of well-connected Subnets.

→ Site can be generally used for locating Services (e.g. log on), Replecation, Group policy, Applications.

→ Sites are Connected with Site links.

→ A site can span multiple Domains.

→ A Domain can span multiple Sites.

Replication:- updating the data other Addition Domain Controller with in the network.

Intra Site Replication:- Replecation which happens with in the site.

Intra Site Replication:- Replecation which Happen Between Sites. The default Interwell is 180 minutes. In order to update the data between data Controllers "KCC" is the Responsible Service.

STEPS TO CREATE SITE

GOTO ADSS Right click on the Sites

↓

Select the New Site

↓

Give the Name

Select default first site

↓

Rename default-first-site name.

TO CREATE SITE LINK:—

Expand Intersite Transport—

↓

Right click on IP

↓

New site link

↓

Give the Link NAME(OK)

TO CONFIGURE SCHEDULE:—

Double click on the link Created

↓

Change Schedule

↓

Select Replecation Not avaidable

↓

give the schedule

↓

Select Replecation available (ok)

↓

change Replecation every to 15 minutes

↓

TO MOVE THE SERVERS

↓

RIGHT CLICK on the SERVER

↓

MOVE

MEMBER SERVER

A System which is having Server operating System in work Group is Joined Existing domain it is Called as Member server. O.S may be windows NT 4.0, windows-2000, windows-2003 using Member Servers we can Configure Servers such as.

→ Application Server (sql / oracle).
→ DNS SERVER.
→ DHCP SERVER.
→ WEB SERVER.
→ FTP SERVER.
→ RAS SERVER.
→ TERMINAL SERVER.
→ RIS SERVER etc.

CLIENT :— A System which is having client operating System. is joint to the Existing domain is Called as client.

~~USER MANAGEMENT~~

HOW TO CONFIGURE A MEMBER SERVER

Right click My Computer
↓
properties
↓
Computer name

↓

Change Select the member of Domain

↓

• GIVE THE DOMAIN NAME

↓

OK

↓

GIVE THE ADMINISTATOR pregiciou

↓

OK

↓

Restart the System.

To find the System whether member Serve

(or) work group

START

↓

RUN

↓

CMD

↓

GET TYPE

for xp give

START

↓

RUN

↓

CMD

↓

Net accounts

USER MANAGEMENT

Types of USERS:-

→ Local users.

→ Domain users.

STEPS TO ~~CONFIGURE~~ CREATE DOAMAIN USER

Go TO ADUC

↓

Right click on users

↓

give the user name (NEXT)

↓

GIVE THE PASS WORD (NEXT)

↓

finish.

By default a user will not having pregicious to log on to domain Computer. when user to log on to DC shows message "LOCAL POLICIES OF THE SYSTEM DOES NOT PERMIT YOU Logon Interactiver"

STEPS TO GIVE PREGICIOUS FOR USER TO LOGON to DC

In Domain Controller go to ocsp

↓

local policies

USER → writes Assignment

↓

Double click on Allow logon locally

↓

BROWSE (ADVANCED find now select the u

(OK)

↓

Apply

(OK)

↓

START

↓

RUN

↓

GP UPDATE

PASS WORD POLICIES

1 password must be Complexity Requirements :— B default this statement will be enable if you want a pass word must be simple characters (words) you have to disable password Complexity.

2. Minimum password length :— By default 7 characters. we can chang the value as our requirement 0 to 14.

3. Minimum pass word age :— By default 4 days we can change the value as our requirement to 998 days.

4. Maximum pass word age:- By default 42 days. we can change the value as our Requirement set to 999 days.

NOTE:- In a real time better to the pass-word age in between 30-60 days.

5. ENFORCE PASS WORD HISTORY:- when a user a changing the pass word a new pass word must not be a part of previous password. By default it's value is 24. you can set this value according to requirement.

STEPS TO MODIFY THE PASS WORD POLICIES

GO TO DOMAIN SECURITY POLICY

↓

ACCOUNT POLICIES

↓

PASS WORD POLICY

↓

double click on enfore pass word History set the value (or) Apply (ok.)

↓

double click on minimum password length set the value as our requirement (Apply (OK))

↓

double click on. pass word must be complexity as our requirements select disable (apply (OK))

↳ START → RUN → gpupdate

PERMIT A USER LOG ON TO SPECIFIC SYS

GO TO ADUC

↓

Right click user Select properties

↓

Account—

↓

logon to

↓

add the System to which user to logon (o

↓

Apply (OK)

STEPS TO GIVE TIME RESTRICTIONS

GO TO ADUC

↓

Right click on user Account—
Select properties.

↓

Account—

↓

log on Hours

↓

Select the time

↓

OK

↓

Apply (OK)

TO Apply Lock OUT THRESHOLD

Go To Domain Security policies

↓

Account policies

↓

Account lock out policy

↓

Double click lockout threshold

↓

Set the value as requirement Apply (OK)

↓

Double click on lock out Counter duration

↓

Set the Counter value 2 minutes

↳ START - RUN - GPUPDATE

STEPS TO CREAT LOCAL USER ACCOUNT

In member Server Right click My Computer

↓

manage local users & groups

↓

Right click on user Container

↓

New USER

↓

GIVE THE USERNAME, password, Create.

PERMISSIONS

Allowing (or) Denying the Access for Resour to the users.

Types of permissions:—

→ Shared level permission.

→ Security level permission.

Share Level PERMISSION:— this permissions a Apply to Restrict the users across the Network. In 2003 by default every one will be havin read only memory.

In 2000 every one will be having Full contr Share permission can be implemented on FAT, FAT 32, NTFS File Systems. Share level permissions are

→ Full Control ☐

→ Change ☐

→ READ ☐

STEPS TO Apply SHARE Level PERMISSIONS

CREATE A FAT PARTITION

↓

To create FAT PARTITION:—

Right click on My Computer

↓

Manage

Disk Manage

↓

Right- click on free space (black colour)

↓

New partition

↓

NEXT

↓

GIVE PARTITION SIZES (NEXT)

↓

SELECT DRIVE LETTER

↓

select FAT32 and check the block perform a clive

↓

NEXT

↓

NEXT (finish)

CREATE USERS IN ADUC

Go to the partition created a folder share(by) any name Set-

↓

Right- click on floder sharing & securities.

↓

select share disk folder

↓

permissions

↓

Add the USERS

↓

Apply the permissions

(Apply → OK)

↓

Apply → OK

ACCESS THE RESOURCE

Go to MEMBER SERVER

↓

logon with the user Account

↓

My Network places

↓

Entire Network

↓

MICROSOFT windows Network

↓

open the Domain name, System name

↓

Access the Respective Share folder and check the permission levels.

TO Access the SHARE DIRECTORY :-

START

↓

RUN

↓

System name (or) \\10.0.0.1\

SECURITY PERMISSIONS

this permission for Apply to Restrict the user locally. that is. to control the user access where as the sources located (or) permission. Security permission can be Apply an NTFS partition security permissions are

- → Full control
- → Modify
- → Read & Execute
- → List folder Contents
- → READ
- → WRITE

STEPS TO APPLY SECURITY PERMISSIONS

CREATE A FOLDER with NTFS PARTITION

↓

Right click the folder properties

↓

Security

↓

Advance.

↓

Then check the box Allow Inheritable permission

↓

Apply (yes) (ok)

↓

Add the user

↓

A. N. (start... now)

logon a user and access the shared res
ces locally (to my computer)

Combination of Security Permission

Sharing	Securities	N/w	Local
READ	READ	READ	READ
change (R/w)	READ	READ	READ
READ	WRITE	A/d	A/d
Full CONTROL	READ	READ	READ
READ	FULLCONTROL	F.C	F.C

whenever we apply Combination that is security & sharing security permissions will be having the higher priority across the network.

PROFILES

profiles is the user state environment. which contains the personal setting of the user like → My Documents
→ Desktop
→ favourites
→ Cookies
→ Application data
→ Start menu etc.

Types of profiles :-

1. local profile.
2. roaming profile.
3. mandatory profile.

LOCAL PROFILE :- A local user profile is created the first time you log on to a computer and is stored on a computer's local Hard disk. Any changes made to your local user profile are specific to the computer on which you made the changes.

Draw backs :- multiple profiles are created on different systems, when user is log on. This profile you can't access over the network.

TO CREATE LOCAL PROFILE

CREATE USER ACCOUNT

↓

Logon with the user account and to verify

Right click my Computer (properties)

↓

Advance (user profile settings)

Roaming profile:— A roaming user profile is created by your system administrator and is stored on a server. This profile available every time you log on to any computer on the network. Changes made to your roaming user profile are updated on the server.

STEPS TO CREATE ROAMING PROFILE

CREATE A SHARE FOLDER

↓

Add the user to the share folder

↓

give full control to the user

↓

Go to ADUC Right click on the user (properties)

↓

give the path (\\ System name \ share name \ user name)

(Ex:- (\\ Sys1 \ Roam \ Ramu)

↓

logon to the System as a user and verify the profile

↓

Save some data on the desk top

↓

log off

↓

log on to the other System (member

MANDATORY PROFILE :— A mandatory user profile is a roaming profile can be used to specify particular settings for individuals or an entire group of users only system administatory can make change to mandatory user profiles.

Mandatory profile are given for the users to control the users his saving un-necessary data.

TO CREATE MANDATORY PROFILE

CREATE Roaming profile

↓

As a Administator open the roaming profile of the user (ACCESS is denied)

↓

Take the owner ship (steps)

↓

Right click on profile folder

↓

properties

↓

Security

↓

OK

↓

advance

↓

owner

↓

select administator

check the box Replace permission

↓

Apply (yes) (OK)

↓

Open the user profile folder

↓

Rename the file NTUSER.DAT to NTUSER.MAN

↓

Replace the owner ship on parent folder (steps)

↓

Right click on parent folder

↓

properties

↓

security

↓

Add the user and give full control (Advance)

↓

check the box Replace permission

↓

(Apply) (yes) (OK)

↓

(Apply) (OK)

↓

logon as a user and verify the profile

HOME FOLDER

→ Home folder is a centralized location of the users personals file (DATA).

→ Home directories any my Documents make it easier for an administator to back up user files and manage user accounts by collecting many or all of a user's files in one location.

STEPS TO CREATE HOME FOLDER

TO CREATE SHARE FOLDER

↓

ADD THE USER

↓

GIVE Full control

↓

GO TO ADUC (Right click on user (properties))

↓

profile (select Connect)

↓

give the path (\\ System name\ directory \username)

↓

Apply (OK)

↓

logon as user very the Home folder.

DISK QUOTA

→ you can use disk quotas on drives formatted with the NTFS file system monitor and limit the amount of disk space available to individual users.

→ Disk quota tracks and control disk space use for NTFS partition prevent further disk space use and logon event when a user exceeds a specified disk space limit.

STEPS TO ENABLE DISK QUOTA

Right click on the drive

↓

properties

↓

quota

↓

click the box Enable quota Management

↓

quota Entries

↓

quota

↓

New quota Entry

↓

Add the user

↓

GIVE DISK SPACE

↓

SET THE WARNING LEVEL (Apply → ok → close

↓

ROLES OF ACTIVE DIRECTORY

1. Domain Naming master } → forest wide Role
2. SCHEMA MASTER
3. RID MASTAR } → Domain wide role.
4. PDC EMULATOR
5. INTRA STRUCTER MASER

1. Domain naming master:—

→ checks and maintains the uniqueness of the Domain names in the whole forest.

→ It is responsible for Adding, removing and Renaming the domain name in the whole forest. naming

→ Domain master Agent will be present at root of the forest. So it is called as forest wide role.

2. SCHEMA MASTER:—

→ Schema is a set of rules which is used to define the structure of AD

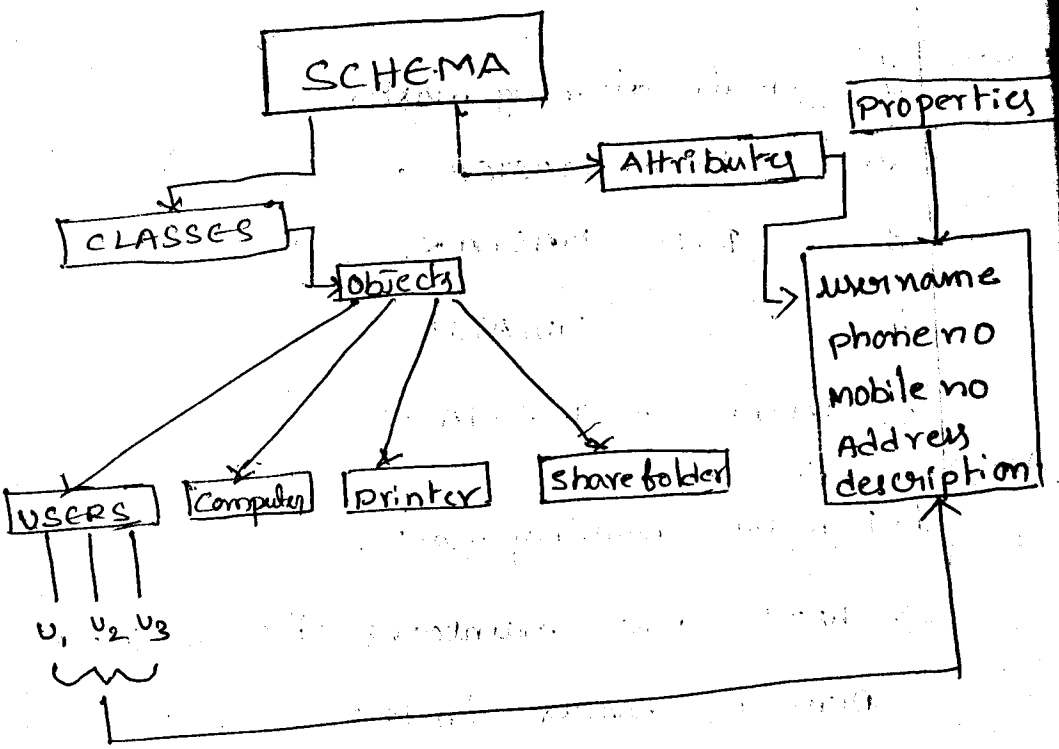
→ Schema Contains Definations of all objects which are stored in AD

→ Schema is a forest wide role.

→ it is classified 2 Types:

→ classes:— classes is a Template which is used to creat an object.

→ Attribute:— Attributes are properties of



Relative Identifier (RID MASTER) :—

→ Allocates pool of Relative IDs (RIDs) to all domain Controllers

→ It assign ID's to the objects which a created in the Domain

Security Identifier (SID): Domain Identifier (DI Relate Identifier (RID).

PDC EMULATOR :—

→ Acts as a PDC for windows NT4.0 BDC in the domain.

→ processes all password updates for clients not running AD client software.

→ Receives immediate updates from other domain Controllers when a user's password

→ It Synchronizes the time between the domains.

→ The Directory Service present in NT4.0 is NTDS. the Data base is SAM (Security Account Manager) DATABASE The Size of Data base is 40mb. where we can Create 40,000 objects.

→ In NT 4.0 The System which is having Directory Service is called as primary Domain Controller (PDC), the back up to the PDC is called BDC (Back up domain Controller)

→ In 2000 & 2003 The data base is NTDS.

→ In 2000 the Size of Data base is 16mb it Supports 16 million objects.

→ In 2003 the Size of data base is 12mb which Supports 1 billion + objects.

→ In 2000 & 2003 the Size of data base is not fix. it is an "Extansable Storage Engine"

Infrastructure MASTER :—

→ Infrastructure Master Maintains and updates the universal group membership information.

→ It used for Intra Domain operations.

GLOBAL CATALOG :-

→ Global catalog Contains Complete information of Host Domain & particular information of other Domains in a forest.

→ By searching against the GC, individual domains, don't have to be required in most cases - GC can resolve.

→ Globals that hold a copy of the global catalog are called Global Catalog services.

ROLES Tranfer :-

Roles can tranfor through 2 ways.

1. Through command prompt area.
2. Through GUI.

ROLES TRANSFER THROUGH COMMAND PROMPT AREA

START

↓

RUN

↓

CMD

↓

NTDS UFIL

↓

ROLES

CONNECTION

↓

CONNECT TO SERVER (SYS2) → (ADC(C.name))

↓

quit

↓

?

↓

TRANSFER Domain naming master

(YES)

↓

TRANSFER INFRASTRUCTURE MASTER

(YES)

↓

TRANSFER PDC (YES)

↓

TRANSFER RID MASTER (YES)

↓

TRANSFER SCHEMA MASTER

(YES)

↓

quit

↓

quit

↓

Net accounts...

ROLES TRANS FER THROUGH GUI

→ TO SCHEMA MASTER TRANSFER

Before Transfering schema master we need to Register the schema using

START

↓

RUN

↓

Reg SUR 32 schmmgmt.dll

after than Transfering

START

↓

RUN

↓

MMC

↓

FILE

↓

ADD REMOVE SNAP-IN

↓

Add

↓

SELECT AD SCHEMA

(ADD) (CLOSE) (OK)

↓

click on AD SCHEMA

RIGHT click on AD SCHEMA

↓

CHANGE Domain Controller

↓

Select specify name

↓

give the name of ADC (ok)

↓

RIGHT click AD SCHEMA

(CHANGE) (OK) (CLOSE)

STEPS TO TRANSFER DN MASTER

GO TO AD Domains & Trusts

↓

Right click ADDT

↓

Connect to domain Controller

↓

Select the Domain Controller

(ADC) (OK)

↓

Right click on ADDT

↓

OPERATION MASTER

↓

Change

(ok)

STEPS TO TRANSFER RID, PDC, INFRASTRUCTU

MASTERS

- Go to ADUC
- Right click on Domain name
- Connect to domain Controller
- Select the domain name (OK)
- Right click domain name
- operation master
- Select RID (change) (YES) (OK)
- Select PDC (change) (YES) (OK)
- Select (Infrastructure) (change) (YES) (OK)
- close

Techi cally These roles are also called as "flexible Single Master operation role (or) "FSMO roles."

TRUST ⁂ RELATIONSHIP

→ Secure Communication paths that allow objects in one domain to be authenticated and accepted in other domain.

→ Some Trusts are automatically Created.
(i) parent - child domains trust each other.
(ii) Tree root domains Trust Root domain.

→ other Trusts are manually Created.

→ Forest - Forest Transitive Trust relationships can be Created windows Sever-2003 forests only.

Types OF TRUSTS :—

(i) Default—
(ii) Shortcut.
(iii) External Trust.
(IV) Forest Trust—
(V) Realm Trust—.

Default :—

Two way Transitive kerberous Trust (Intra-forest)

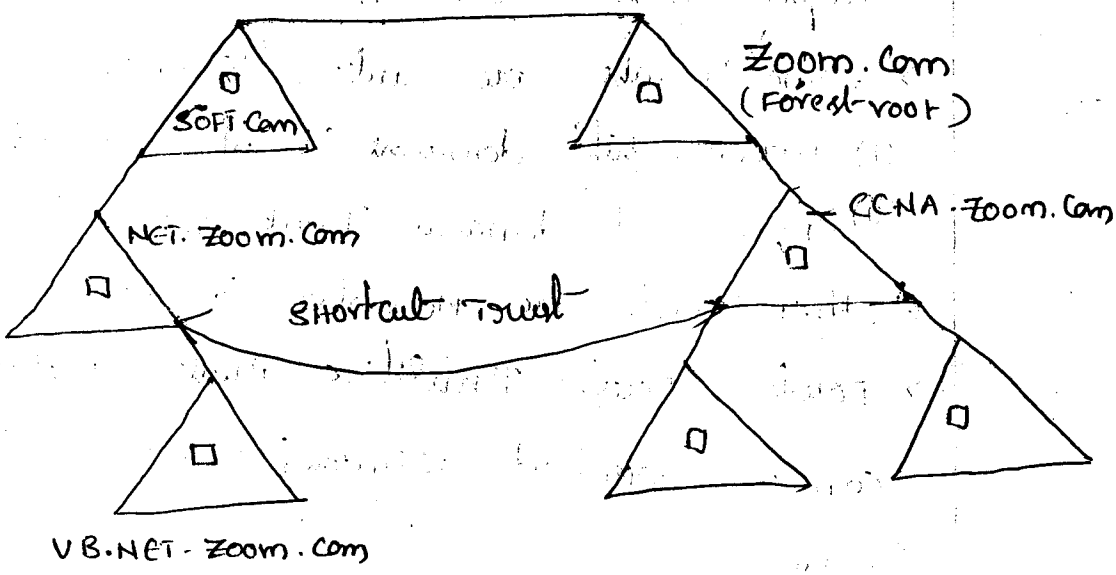
→ it is Automatically Created.
→ Transitive Trust—
→ Two-way Transitive.

Shortcut Trust :— one or Two way Transitive kerberous Trusts (Intraforest) Reduce Authentication Requests.

→ Reduces Authentication time in Complex forests.

→ It is partially Transitive.

→ It can be one way (or) Two way.



External Trust:- It is a non Transitive NTLM (New Technology Lan manager) Trust.

→ A Trust that is many Created between.

(i) Two Active directory domains located in different forests.

(iii) An Active directory domain and a windows NT 4.0 (or) earlier domain.

→ NON Transitive Trust-

→ one-way Trust.

REALM TRUST:-

→ It is a Trust between a kerberous realm and an Active directory domain

→ It can be Transitive (or) Non-Transitive

→ Can be one way (or) Two-way.

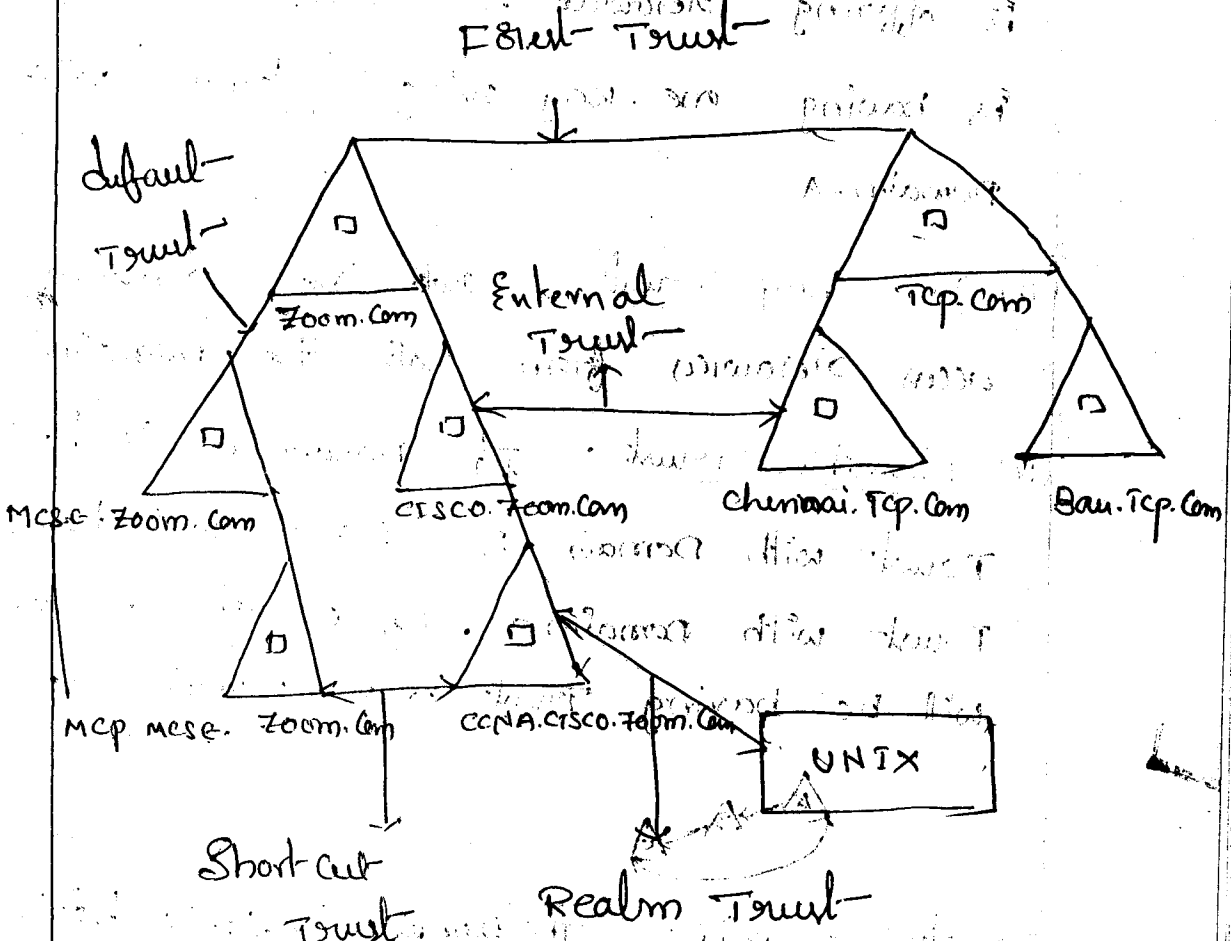
FOREST TRUST :—

→ A Forest- trust- is a trust between two windows server- 2003 forests.

→ forms the Trust- relationship between every domain in both forests.

→ It is Created between the forests involved & the Trust-.

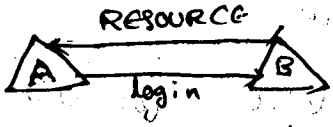
→ It is Transitive for all of the domain in the forest-



DIRECTION OF TRUST

(i) one-way incoming Trust :—

when a user is accessing resources from domain B. the resources are incoming to domain A. Then it is called one-way incoming Trust—



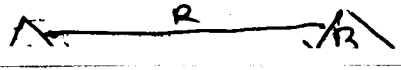
(ii) one-way out going Trust :— when Domain is offering resources to domain A. then Domain is having one-way out-going trust with Domain-A

(ii) Two-way Trust :— Both the domains can access resources from Both the Domains.

(iv) Transitive Trust :— If Domain A is having Trust with Domain B, Domain B is having Trust with Domain C. By default Domain A will be having Trust with Domain C.

Trusted Domain :— The Domain which is having user Accounts to access the resource is called Trusted Domain.

Trusting Domain :— The Domain which is having resources to offer : it is called Trusting Domain.



FUNCTIONAL LEVELS

→ Functional levels Determine.
(i) Supported Domain controll operating System
(ii) Active Directory features will be available.

→ Domain functional level can be raised independently of other Domains.

→ Raising forest- functional level is performed by Enterprise Administrator.

→ Requires all Domain functional levels to be at windows 2000 native (or) windows Server 2003 functional levels.

functional level Combinations :-

windows 2000 mixed mode — win NT4.0, WIN 2000, 2003

windows Native mode — WIN 2000, WIN 2003

windows Interminal mode — WIN NT4.0, WIN 2003

WINDOWS SERVER 2003 mode — All window 2003 Servers.

TO CONFIGURE CROSS FOREST TRUST RELATION

IP :-	10.0.0.1	10.0.0.2
PRDNS :-	10.0.0.1	10.0.0.2
ALTDNS :-	10.0.0.2	10.0.0.1

STEPS TO RAISE THE FUNCTIONAL LEVEL

Go to Active Directory Domain & Controller

↓

click on Domain name

↓

Select Raise Domain functional level

↓

Select windows server 2003

↓

Raise (OK) → OK.

STEPS TO RAISE FOREST FUNCTIONAL LEVEL

Right- click AD Domains & Trusts

↓

Raise forest- functional level

↓

Raise (OK) → OK

STEPS TO ESTABLISH TRUST

Go TO AD Domains & Trusts

↓

Right- click on Domain name

↓

Select- properties

↓

Trust-

↓

New Trust-

↓

GIVE THE Domain name (specified)

↓

Select forest Trust (NEXT)

↓

Select TWO Way (NEXT)

↓

Select the Both the This domain under specified

Deney

↓

give the user pregidious of specified Domain

(NEXT).

↓

Select forest wide Authentication

(NEXT)

↓

NEXT

↓

NEXT

↓

NEXT

↓

Select yes, Confirm out-going Trust

(NEXT)

↓

Select yes, Confirm in-coming Trust

(NEXT)

↓

STEPS TO PERMIT USER TO Log on to the a Specified Domain

GO TO Domain Controller Security policies

↓

local policies

↓

user rights Assignment

↓

Double click Allow logon locally

↓

Add a user Group

↓

Browse (locations) Select the Specified Domain

↓

OK

↓

ADD the user (OK)

↓

OK

↓

Apply (OK)

↓

START

↓

RUN

↓

gpupdate

GROUP policy

It is a set of rules which is apply to a Computer logon to restrict the access of Resource over the network.

→ IN NT 4.0 System policies. we are present System policies we can controlls the users partially.

→ the policies are very less in number.

→ If you apply a policies on a System. It will make permenent change to the System Registry.

→ using group policies we can control the users Completely.

→ Directly we can't apply group policies for users.

→ group policies can be applied an specified administrative boundaries such as O.U, domain level, Site level.

ORGANISATIONAL UNIT :— (OU) :— A small Administrative boundary such as users, Computers subcons and share Resources.

STEPS TO CREATE OU

Go TO ADUC

↓

Right click on Domain name

↓

new

↓

organisational unit

↓

DELIGATION OF CONSTRUCT

it is partially organizes the Administrative previllage to the specific user to control a specific administrative boundary (e.g. domain)

STEPS TO GIVE DELIGATION CONTROL

Go to ADUC

↓

Create OU with some user Account

↓

Right click on top created

↓

deligation control (Next)

↓

Add the user

↓

Next

↓

Select the tasks

↓

Next

↓

finish

verification :- logon as a user and check the deligate controls.

STEPS TO Apply GROUP policies

Go to ADUC

↓

Right click on OU

properties

↓

GROUP policy

↓

New

↓

Give the name (Hide My Computer)

↓

Edit under user Configuration

↓

Expand Administrative Templates

↓

desktop

↓

Right-click on Remove My Computer icon on the desktop

↓

Select Enable (Apply)

↓

Ok

verification:- logon as a user and verify the policies Apply.

Case1:- HIDE MY COMPUTER ✓

Case2:- SHOW MY COMPUTER ✗

whenever we are Confild user (i.e) the policy which is for denied and access on a Some object. In this case the

policy which is present on top most level will highest priority and it will Applicable.

→ if you want to bottom level policy to be Applicable to change the policy position

SHOW MY COMPUTER	✓
HIDE MY COMPUTER	×

Case - III :- with out interchanging of bottom level policy to be Applicable select the option "no overwrite".

HIDE MY COMPUTER
SHOW MY COMPUTER - NO OVERWRITE ☑

PATH TO RETRICTION DRIVE

Right click on 'OU'
↓
properties
↓
group policies
↓
new (restrict Drives)
↓
Edit
↓
under user Configuration
↓
Expand Admin. Templates
↓
windows Components

click on windows Explorer

↓

click on prevent access for Drives

from My Computer

↓

Select Enable to selected drives

↓

Apply (ok)

PATH TO RESTRICT INTERNET EXPLORER

Right click on

↓

properties

↓

group policies

↓

New (Restrict ips)

↓

Edit

↓

under user Configuration

↓

Admin. Templates

↓

System

↓

Double click on Don't run Specified

windows Applications

↓

Select Enabled

↓

add

↓

give Internet Explorer .exe

↓

OK

↓

Apply (OU)

Domain level policy:— when we apply policy on domain level it will be Applicable. for all the user of domain including Administator. The policies are going to be interfied to child objects (O.U & sub O.U's).

STEPS TO Apply policy

Go TO ADUC

↓

Right click on domain name

↓

properties

↓

Group policy

↓

New

↓

give the name

↓

Edit

↓

Apply the policy (OK)

verification:— logon as Administrator and verify the domain level policy.

STEPS TO EXECUTE THE Admin. Gpo policy

Right click Domain name

↓

properties

↓

group policy

↓

Select the policy

↓

Properties

↓

Security

↓

Add the Administator

↓

check box is Deny for apply Gp

↓

Apply (yes) (ok)

Block policy INHERITANCE

Domain level policies will inherit to the O.U if we want to block the policy inheritance enable the block inheritance at the specific levels.

Right click on O.U

↓

properties

↓

Gp

↓

check the box (Block policy inheritance at Bottom)

↓

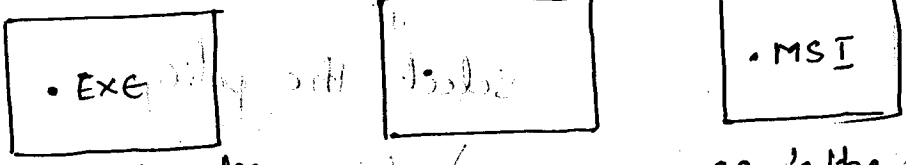
GROUP policy - II

Soft ware Deployment :-

win installe
phase - I
Before snap shot

CE 2003
phase - II
Run Application

phase - III
After snap shot



scan the Registory for currently Installing Application

Install the Application

scan's the Registory for Newly Installed Application.

→ Soft ware Deplogment is used to Delay a specific Application to a specipic user (or) Carputi So that whenever the users logon to the n/w, they can run the Application.

(i) .exe Application can't be deployed over the Network.

(ii) .exe Application should be Converted to .MSI So to do this we require a third party Application Called as "WIN INSTALL CE 2003"

→ using "WIN INSTLL CE 2003" we Convert .ex to .MSI In three phases.

Phase 1 :- Before snap shot :-

It scans the System Registry for Correctly Installed Application store the information in a Temporary folder.

phase 2 :- RUN THE Application :-

Install the Application which you are planning to Delay (Acrobat, WIN ZIP) etc.

phase 3 :- AFTER Snap shot

It scans the System register for newly install Application and Compares with the previous snap shot. it going to give the Extention .MSI

STEPS TO Deploy the Software

→ Install WIN INSTALL LE 2003

→ CONVERT .EXE to .MSI

→ Deploy the Soft ware using group policy.

→ verify the deployed Software.

(+) STEPS TO Install WININSTALL LE 2003 Soft ware

Go TO Application folder

↓

RUN Installe .EXE file (NEXT)

↓

NEXT

↓

Select I accept the Terms

↓

↓

Install → finish.

(ii) Convert .exe to .MSI :—

create a share folder with MSI file Give full Control to Everyone

↓

WIN INSTALLE 2003

↓

Right-click on wininstall packages

↓

RUN DISCOVER (OK) (NEXT)

↓

give the Application name

↓

Browse (my N/w places)

↓

Entire network

↓

Micro Soft- win Network

↓

Domain, System name

↓

Select MSI folder

↓

give the file name

↓

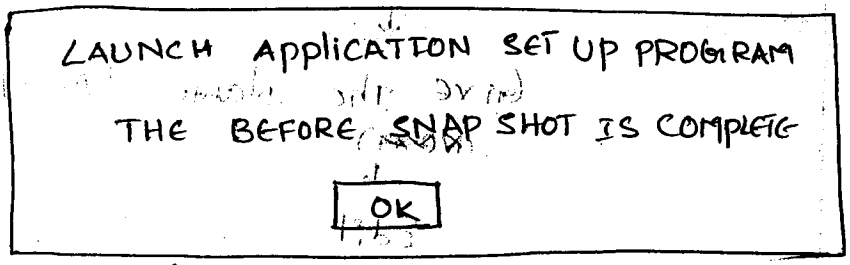
open (NEXT)

↓

Select the drives (NEXT)

↓

D...I



↓

OK

Install the Application (Acrobat) which you are planning to Deploy with this Application only.

(ii) After snapshot :-

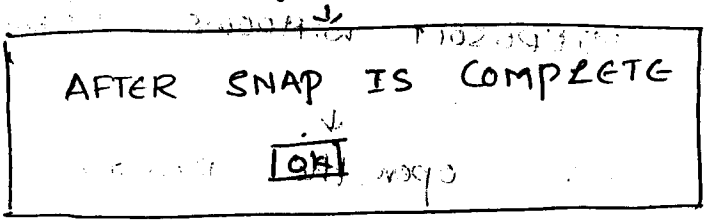
Right click on Install packages

↓

RUN DISCOVER (OK) (NEXT)

↓

finish



(iii) STEPS TO Deploy the Soft ware :-

Go TO ADUC

↓

Create an O.U with users

↓

Right click on OU

↓

properties

↓

group policy

↓

↓

Give the Name (Acrobat)

↓

Edit

↓

under user Configuration Expand

Software settings

↓

Right click on Soft-ware install

↓

New package

↓

My Net-work places

↓

Entire Network

↓

MICROSOFT WINDOWS Network

↓

open the Domain

↓

System

↓

Open MSI folder

↓

Double click on .MSI folder

↓

Select Assign

↓

OK

verification :— logon as user and verify the

Software can be Deployed using Three Modes.

→ publishing Mode
→ Assign mode
→ Advance mode.

publish Mode:- if we deploy the Application using publish user has to install the Application from Controlpanel.

Assign mode:- If you deploy the using Assign the user can find the Application on the Desktop and programs under start menu.

Advance mode:- It is used to upgrade the already installed Application with the help of service packs & patch files.

FOLDER REDIRECTION

It is used to collect the user created data to one centralized location. which helps to take the back up the user created data and to monitor the Mandatory user properties.

STEPS TO CREATE FOLDER

Create a share folder with full Control

↓

Right click on OU

↓

Properties

↓

↓

New (give the name)

↓

Edit

↓

under user Configuration

↓

Expand windows settings

↓

folder redirection

↓

Right click desktop

↓

property

↓

select- basic redirect everyone's folder

↓

select redirect to the following location.

↓

Browse

↓

My network places

↓

select the folder Restriction

share folder (ok)

↓

give the username

↓

verification :— create some files on desktop as a administator check & and Contents Redirection (or) not.

scripts :— Scripts are used to automate user process. that is to intimate related to the Rotin Tasks.

STEPS TO CONFIGURE SCRIPT

create a share folder and give full control to everyone

↓

Go to ADUC

↓

Right click on OU

↓

properties

↓

group policy

↓

New

↓

give the name (scripts)

↓

Edit

↓

under windows & settings

↓

Double click on logon

↓

Add

↓

Browse

↓

My Network places

↓

Select the script folder

↓

select script file

↓

Apply (OK)

wscript.echo "Install the Application from Controlpanel"

↓

save the file .vbs