GOVERNMENT POLYTECHNIC AHMEDABAD

PROGRAM: DIPLOMA IN COMPUTER ENGG

NETWORK MANAGEMENT AND ADMINISTRATION (3360703)

UNIT-1

Exploring Directory Services and Remote Access

Directory Services

- Directory services are an essential part of today‘s network-centric computing infrastructure.
- Directory-enabled applications -now power almost all the mission critical processes of an enterprise, including resource planning, value chain management, security and firewalls, and resource provisioning.
- So what exactly is a Directory Service?

Directory Services:

- A DS is the collection of software and processes that store information about your enterprise, subscribers, or both.
- Ex. is the Domain Name System (DNS), which is provided by DNS servers. A DNS server stores the mappings of computer host names and other forms of domain name to IP addresses. A DNS client sends questions to a DNS server about these mappings (e.g. what is the IP address of test.example .com?).
- The mapping of host names enables users of the computing resources to locate computers on a network, using host names rather than complex numerical IP addresses.

Directory Services:

- In a telephone directory , the nodes are names and the data items are telephone numbers.
- In the DNS the nodes are domain names and the data items are IP addresses (and alias, mail server names, etc.).
- In a directory used by a network operating system, the nodes represent resources that are managed by the OS, including users, computers, printers and other shared resources.

➢ *A directory service is a shared information infrastructure for locating, managing, administering, and organizing common items and network resources, which can include volumes, folders, files, printers, users, groups, devices, telephone numbers and other objects. A directory service is an important component of a NOS (Network Operating System)*

Directory Services: a directory service can be considered an extension of a database, directory services generally have the following characteristics:

Hierarchical naming model

- A hierarchical name scheme uses a tree structure that reflects the actual structure of a company. At the topmost (first) node of the tree is the organization name, which is usually the company name. After the organization name are organizational units, which you create to suit the structure of the company; you can organize the structure geographically, departmentally, or both.
- A hierarchical name may include these components:
  - Common name (CN) -- Corresponds to a user's name or a server's name. All names must include a common name component.
  - Organizational unit (OU) -- Identifies the location of the user or server in the organization. Domino allows for a maximum of four organizational units in a hierarchical name. Organizational units are optional.
  - Organization (O) -- Identifies the organization to which a user or server belongs. Every name must include an organization component.
  - Country (C) --Identifies the country in which the organization exists. The country is optional.
  - An example of a hierarchical name that uses all of the components is:
  - Julia Herlihy/Sales/East/Renovations/US Typically a name is entered and displayed in this abbreviated format, but it is stored internally in canonical format, which contains the name and its associated components, as shown in the following example:
  - CN=Julia Herlihy/OU=Sales/OU=East/O=Renovations/C=US

Directory Characteristics:

- *Extended search capability*

  Directory services provide robust search capabilities, allowing searches on individual attributes of entries.
- *Distributed information model*

  A directory service enables directory data to be distributed across multiple servers within a network.
- *Shared network access*

  The resources are shared over the network.

Directory Characteristics:

- *Replicated data*
  Directories support replication (copies of directory data on more than one server) which make information systems more accessible and more resistant to failure.
- *Data store optimized for reads*
  The storage mechanism in a directory service is generally designed to support a high ratio of reads to writes.
- *Extensible schema*
  The schema describes the type of data stored in the directory. Directory services generally support the extension of schema, meaning that new data types can be added to the directory.

For example,

- An employee directory for a company will include all employees of that company and certain types of information associated with those employees.
- All useful information must be systematically associated with the entry for each employee in the directory.
- As changes occur (New hires, terminations, promotions, job changes and so on.), The directory needs to be updated to reflect the changes.

Directory structure:

- Directory structure serves as the administrative aspect of directory and fulfills 2 purpose:
  - 1.Object Identification
    - that ensures, all objects within a directory can be uniquely identified.
  - 2. Object Organization
    - The organization of objects represented in a directory also serves to make access to information about the objects in the directory easier.
    - This can also assist in the management of information in the directory through the grouping (or partitioning) in some structured manner so that the groups of objects can be managed separately.

- You should know about five important directory services: Novell eDirectory, Microsoft’s Windows NT domains, Microsoft’s Active Directory, X.500 Directory Access Protocol, and Lightweight Directory Access Protocol

Novell eDirectory

- Novell eDirectory has been available since 1993, introduced as NDS as part of NetWare 4.x.
- **NetWare** is a computer network operating system developed by Novell.
- This product was rapidly implemented in Novell networks, particularly in larger organizations that had many NetWare servers and needed its capabilities.
- eDirectory is a reliable, well made directory service.

- NDS can be installed to run under Windows NT, SunMicrosystems’s Solaris and UNIX and as well as under Novelle’s own Netware.
- So, it can be used to control a multi-platform network.
- You manage the eDirectory tree from a client computer logged in to the network with administrative privileges.

- eDirectory is a hierarchical, object oriented database used to represent certain assets in an organization in a logical tree, including organizations, organizational units, people, positions, servers, volumes, workstations, applications, printers, services, and groups.
- eDirectory can manage more than a billion objects in a tree.

Windows NT Domains

- The Windows NT domain model breaks an organization into chunks called *domains, all* of which are part of an organization.
- The domains are usually organized geographically, which helps minimize domain-to-domain communication requirements across WAN links, although you're free to organize domains as you wish.
- Each domain is controlled by a *primary domain controller (PDC), which might have one or more backup domain controllers (BDCs) to kick in if the PDC fails.*

- All changes within the domain are made to the PDC, which then replicates those changes to any BDCs. BDCs are read-only, except for valid updates received from the PDC.
- In case of a PDC failure, BDCs automatically continue authenticating users. To make administrative changes to a domain that suffers PDC failure, any of the BDCs can be *promoted to PDC.*
- *Once the PDC is ready to come back online, the promoted BDC* can be *demoted back to BDC status.*

- Windows NT domains can be organized into one of four domain models:

  ■ **Single domain**

  In this model, only one domain contains all network resources.

  ■ **Single Master domain**

  The master model usually puts users at the top-level domain and then places network resources, such as shared folders or printers, in lower level domains (called *resource domains). In this model, the resource domains trust* the master domain.

  ■ **Multiple master domain**

  This is a slight variation on the master domain model, in which users might exist in multiple master domains, all of which trust one another, and in which resources are located in resource domains, all of which trust all the master domains.

  ■ **Complete trust**

  This variation of the single-domain model spreads users and resources across all domains, which all trust each other.

- You choose an appropriate domain model depending on the physical layout of the network, the number of users to be served, and other factors.
- Explicit trust relationships must be maintained between domains using the master or multiple master domain model, and must be managed on each domain separately.
- Maintaining these relationships is one of the biggest difficulties in the Windows NT domain structure approach, at least for larger organizations.
- If you have 100 domains, you must manage the 99 possible trust relationships for each domain, for a total of 9,900 trust relationships. For smaller numbers of domains (for example, fewer than 10 domains), management of the trust relationships is less of a problem, although it can still cause difficulties.

X.500 DIRECTORY ACCESS PROTOCOL

- X.500 is a series of computer networking standards covering electronic directory services.
- The X.500 series was developed by ITU-T, formerly known as CCITT, and first approved in 1988.
- ISO was a partner in developing the standards, incorporating them into the Open Systems Interconnection suite of protocols.

X.500 DIRECTORY ACCESS PROTOCOL

- The protocols defined by X.500 include :
  - DAP (Directory Access Protocol) -There are two sub-protocols used to communicate between systems. The communication protocol between a DUA (Client) and a DSA (Server) is called the Directory Access Protocol (DAP). The communication protocol between one DSA (Server) and another DSA is called the Directory System Protocol (DSP).
  - DSP (Directory System Protocol)
  - DISP (Directory Information Shadowing Protocol)
  - DOP (Directory Operational Bindings Management Protocol)
  - As these protocols used the OSI networking stack, a number of alternatives to DAP were developed to allow Internet clients to access the X.500 directory using the TCP/IP networking stack.
  - The most well-known alternative to DAP is Lightweight Directory Access Protocol (LDAP).
  - While DAP and the other X.500 protocols can now use the TCP/IP networking stack, LDAP remains a popular directory access protocol.

X.500 DIRECTORY ACCESS PROTOCOL

- The primary concept of X.500 is that there is a single Directory Information Tree (DIT), a hierarchical organization of entries which are distributed across one or more servers, called Directory System Agents (DSA).
- An entry consists of a set of attributes, each attribute with one or more values.
- Each entry has a unique Distinguished Name, formed by combining its Relative Distinguished Name (RDN), one or more attributes of the entry itself, and the RDNs of each of the superior entries up to the root of the DIT.

X.500 DIRECTORY ACCESS PROTOCOL

- Client –DUA, server-DSA
- There are two sub protocols used to communicate between systems.
- 1. communication protocol between DUA and DSA is called DAP(Directory access protocol).
- 2. communication protocol between one DSA and another DSA is called DSP(Directory System protocol).

X.500 DIRECTORY ACCESS PROTOCOL

- DAP specifies how an X.500 DUA communicates with a DSA to issue a query.
- Using DAP, users can view, modify, delete and search for information stored in the X.500 directory if they have suitable access permission.
- DAP is complex protocol with lot of overhead.
- LDAP is used to access and update directory information in x.500 directories. so, LDAP is more suitable than DAP for implementation on internet.

ACTIVE DIRECTORY ARCHITECTURE

- Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks.
- It is included in most Windows Server operating systems as a set of processes and services.
- Initially, Active Directory was only in charge of centralized domain management. Starting with Windows Server 2008, however, Active Directory became an umbrella title for a broad range of directory-based identity-related services.
- A server running Active Directory Domain Services (AD DS) is called a domain controller. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.

Active Directory Architecture:

Various Components of Active Directory are as below-

OBJECTS

Objects are the network resources. There are basically 3 Type of Objects which are further categorized as below –

Container Objects

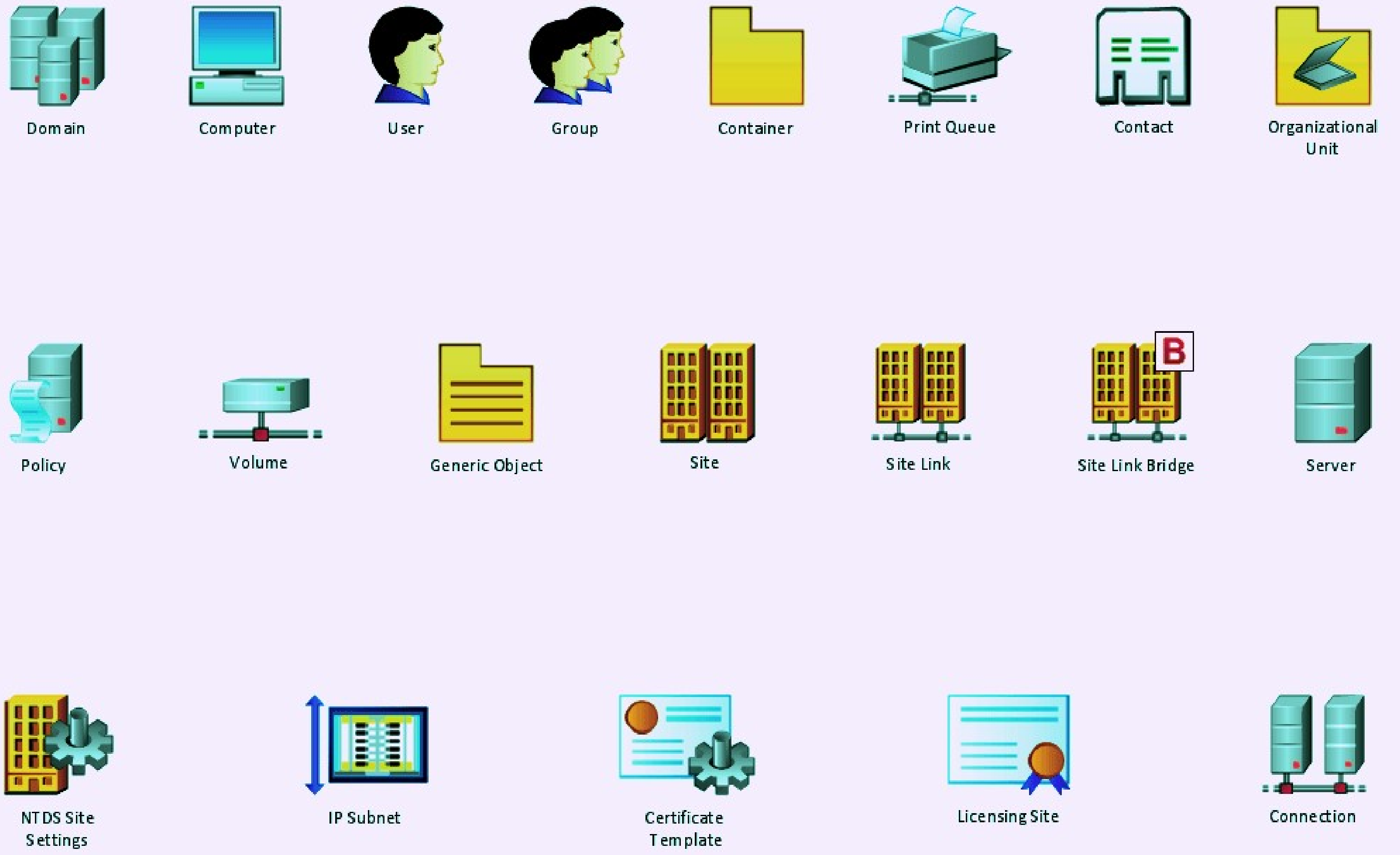
- **Default Container Objects**
  - **Computers**
  - **Users**
  - **Built-in**
  - **Foreign Security Principles**
- **Generic or Created Container Objects**
  - **Domain**
    - **Domain Categories –**
      - **Single Domain**
      - **Master Domain**
      - **Multiple Master Domain**
    - **Domain Terminologies –**
      - **Tree**
      - **Forest**
      - **Trust Relationship –**
        - **Two way Trust**
        - **Transitive Trust**
  - **Site**
  - **Organizational Units**

Leaf Objects

Other Objects

www.gripinit.com

Active Directory Objects



Object types in AD

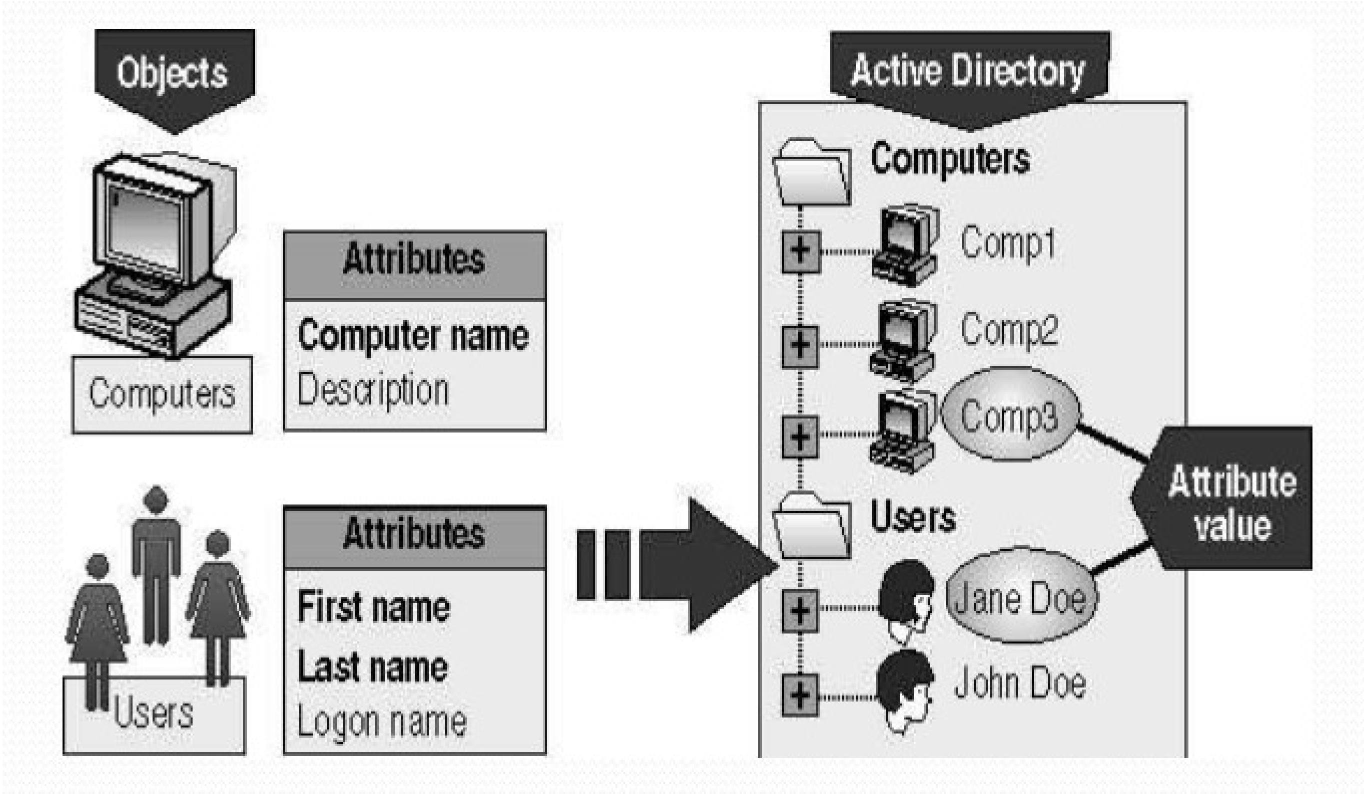
- Container object
- Leaf object

Container Object

- A container object is simply an object that stores other objects.
- Container objects are function as the branches of the tree.
- AD uses container objects such as organizational unit (OUs) and groups to store other objects.
- Container can store other container or leaf objects, such as users and computers.

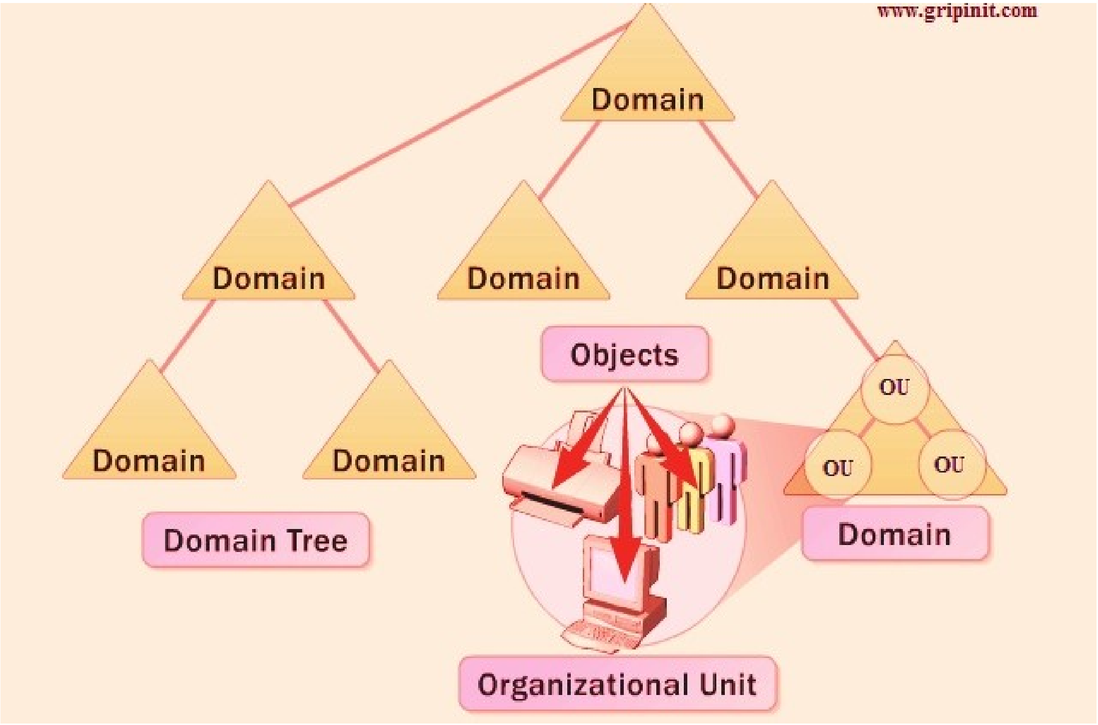
Leaf Object

- A leaf object stands alone and cannot store other objects.



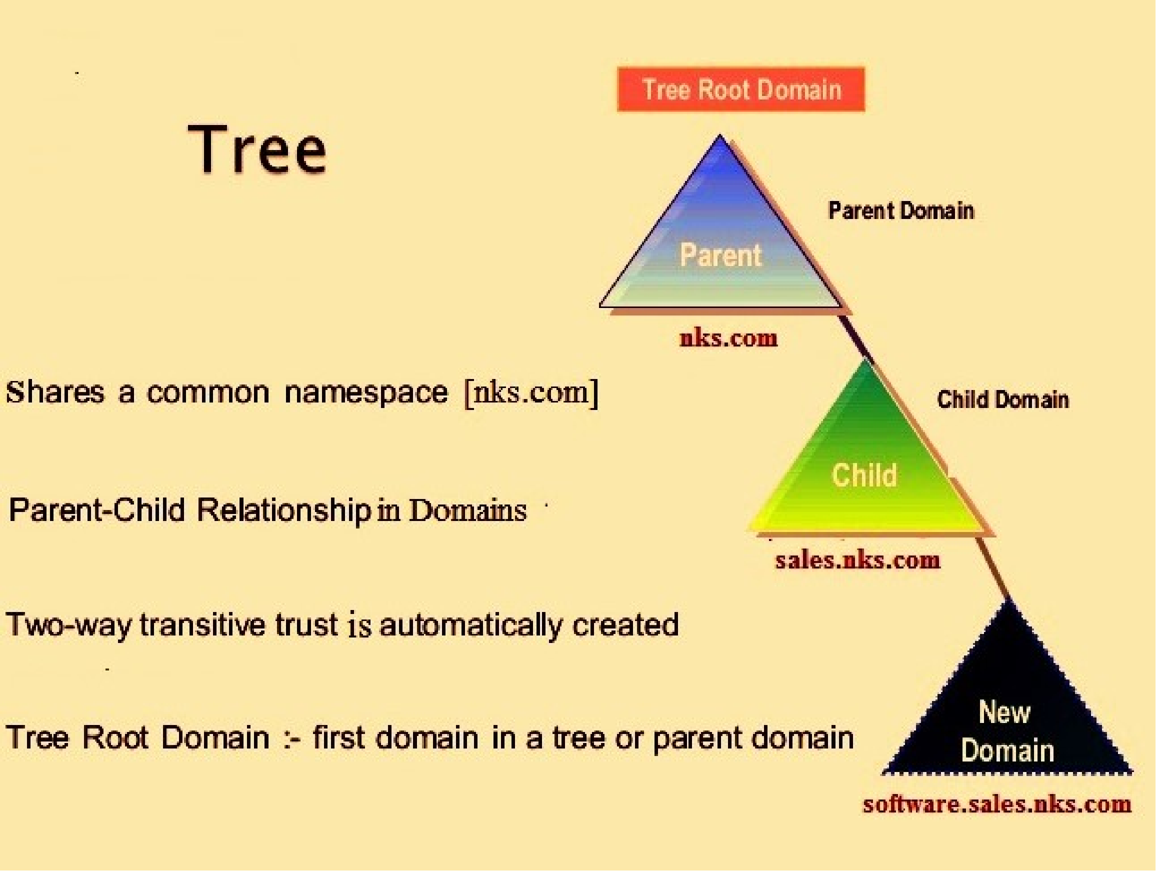
Domains – The domain container holds all of the other objects that are a part of that domain and also hold organizational unit objects and their contents.

-Domains are responsible for creating Trees and Forest as well as maintain trust relationship between each other to access the resources of other domains.



TREES

A tree is a group of domains that have the same DNS name; for example, nks.com (the top domain), sales.nks.com and software.sal es.nks.com (the child domains).



Shares a common namespace [nks.com]

Parent-Child Relationship in Domains

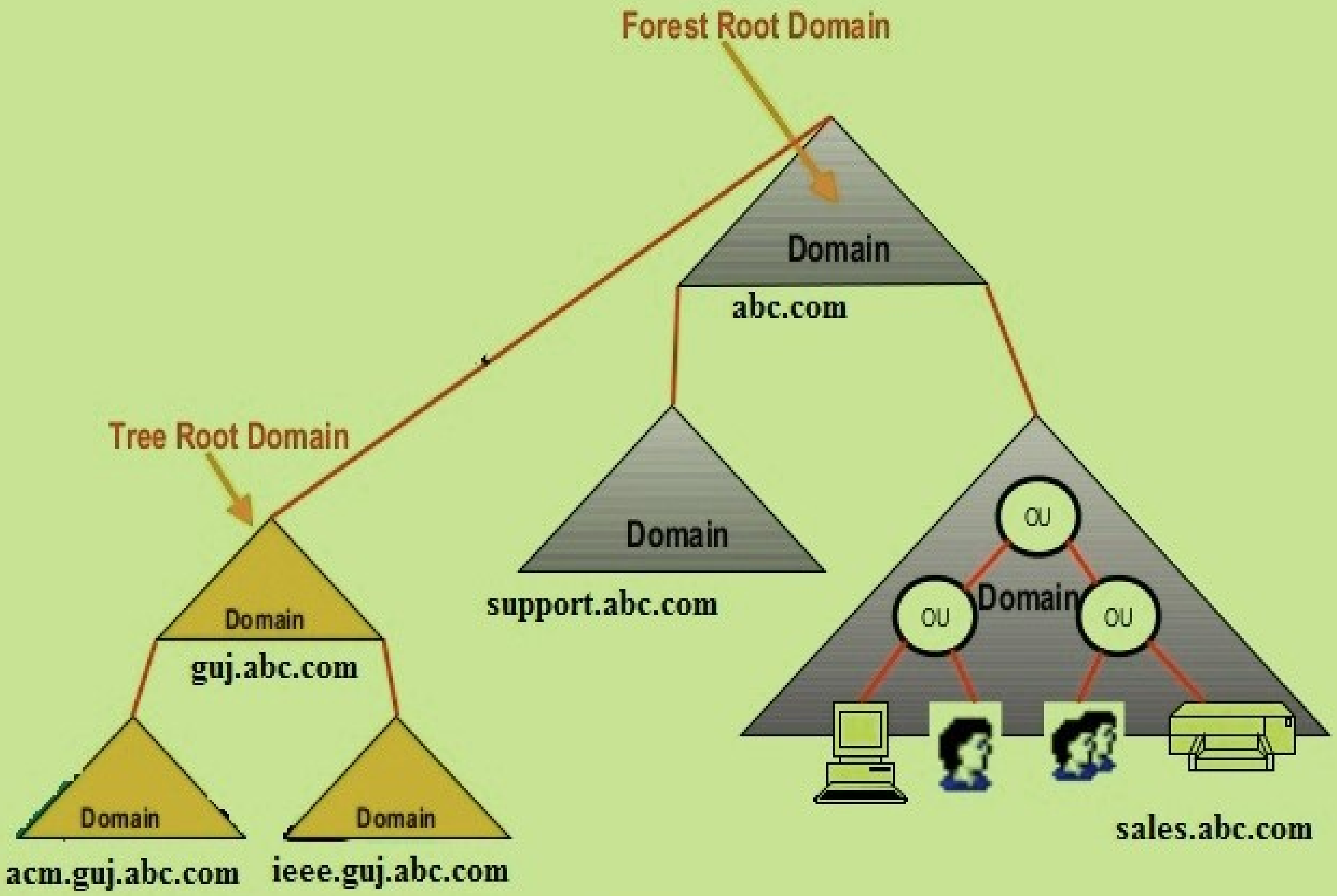
Two-way transitive trust is automatically created

Tree Root Domain :- first domain in a tree or parent domain

FORESTS

- A forest is a collection of trees, which can be treated as one administrative unit and Active Directory automatically manages trusts between domains.
- For security purposes, organizations have set up multiple forests, but trusts between forests must be managed manually by the administrator.
- Because the forest is a security boundary, each forest does not trust or allow access from any other forest by default.
- However, in Windows Server 2003 and higher Active Directory, transitive trust relationships can be manually established between forests to establish cross-forest access to resources, so that users in one forest can access resources in another forest.

The Forest


Forest Root Domain
Domain
abc.com
Tree Root Domain
Domain
support.abc.com
OU
OU
Domain
OU
Domain
guj.abc.com
Domain
Domain
acm.guj.abc.com
ieee.guj.abc.com
sales.abc.com

TRUST RELATIONSHIP

There are basically 2 types of trusts –

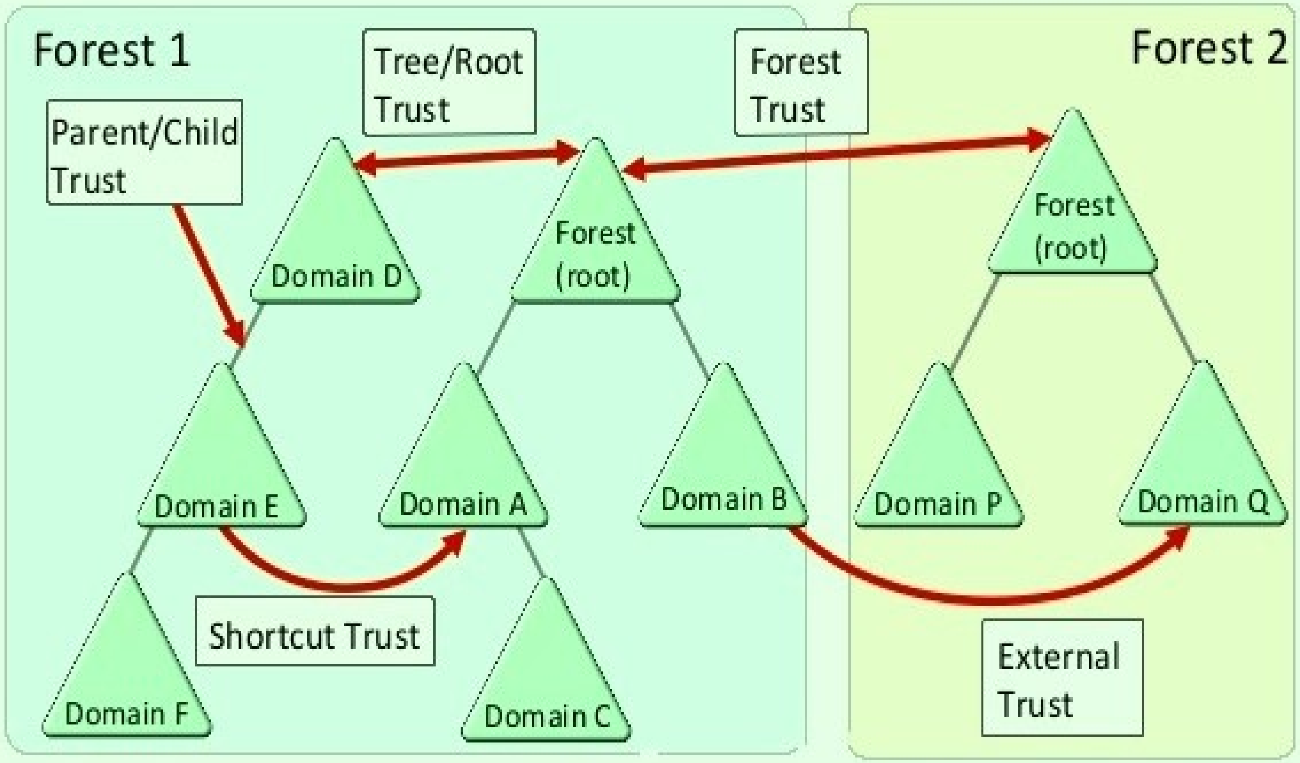
a. TWO WAY

When you create a new child domain, the child domain automatically trusts the parent domain, and vice versa. At the practical level, this means that authentication requests can be passed between the two domains in both directions.

b. TRANSITIVE

An automatic trust association between parent and child domains and between root domains in a Windows Active Directory forest. For example, if domain A trusts B, and B trusts C, then A automatically trusts C.

Types of Trusts



Transitive Trust: Tree/Root Trust, Forest Trust, External Trust, Shortcut Trust

Two way Trust: Parrent/ Child Trust

Sites

- A site is actually a physical grouping of objects based upon IP Addresses.
- A site cannot span multiple physical locations, but rather encompasses network objects and devices in one area.
- For example, the XYZ company has offices in pune, delhi, and ahmedabad. Each office is a physical location, and therefore is considered as a “site”.
- The site container is a logical representation of what is physically true.
- Specifically, sites are used to distinguish between local and remote locations.

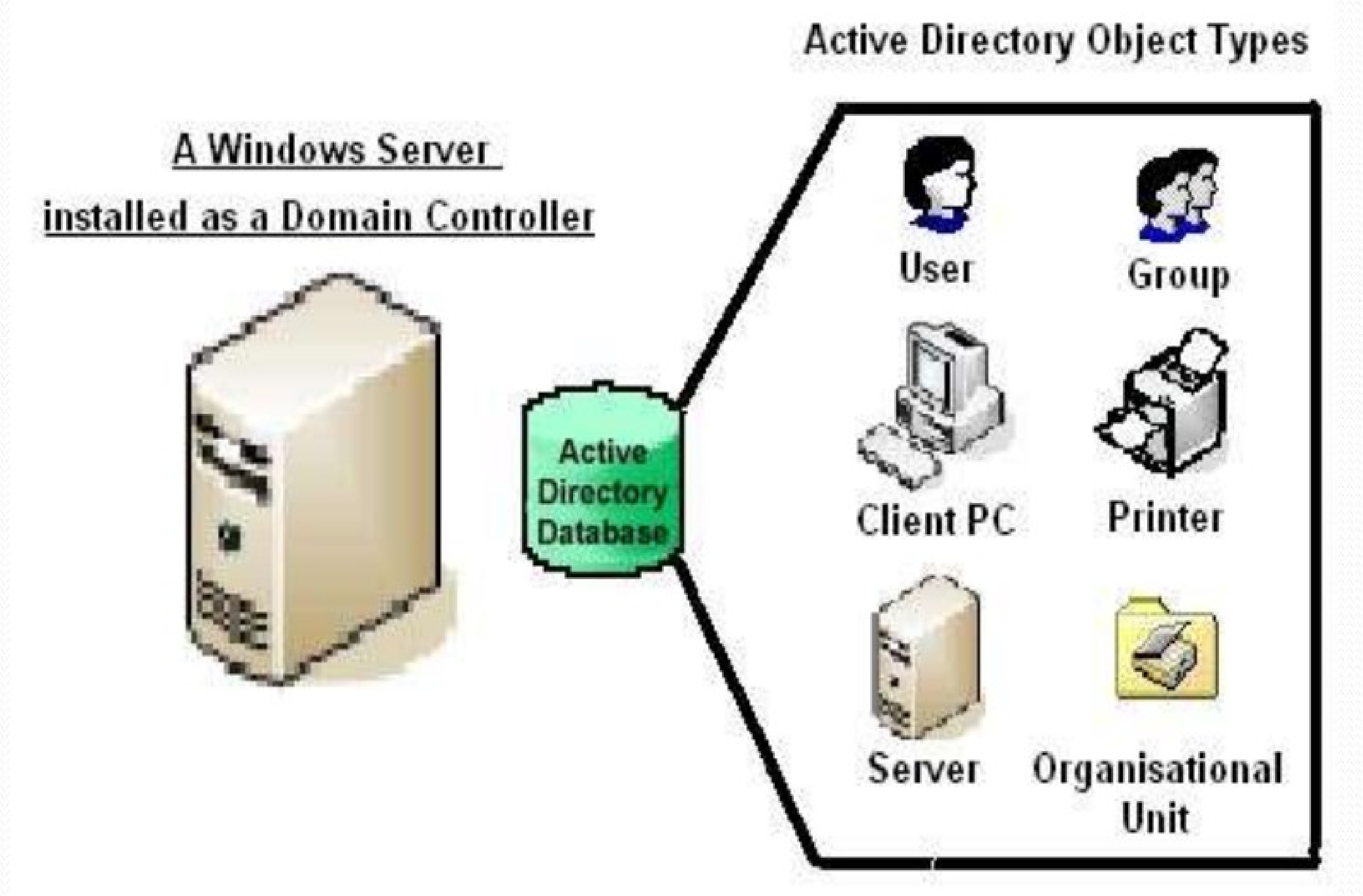
ATTRIBUTES

Attributes are characteristics of objects in the directory. For example, the attributes of a user might include the user’s first and last names, department, and e-mail address

SCHEMA

- The *schema* is the component that defines all object classes and attributes that AD uses to store data.
- It is sometimes referred to as **the blueprint for AD**.
- The schema is **replicated among all domain controllers in the forest**. Any change that is made to the schema is replicated to every domain controller.
- In Schema each attribute is defined only once and can be used in multiple classes. For example, the Description attribute is defined once but is used in many different classes.
- Each class of objects in the Active Directory schema has attributes that ensure:
  - Unique identification of each object in a directory data store.
  - security principals (users, computers, or groups)
  - Compatibility with LDAP standards for directory object names.

Cont..


Active Directory Object Types
A Windows Server
installed as a Domain Controller
Active Directory Database
User
Group
Client PC
Printer
Server
Organisational Unit

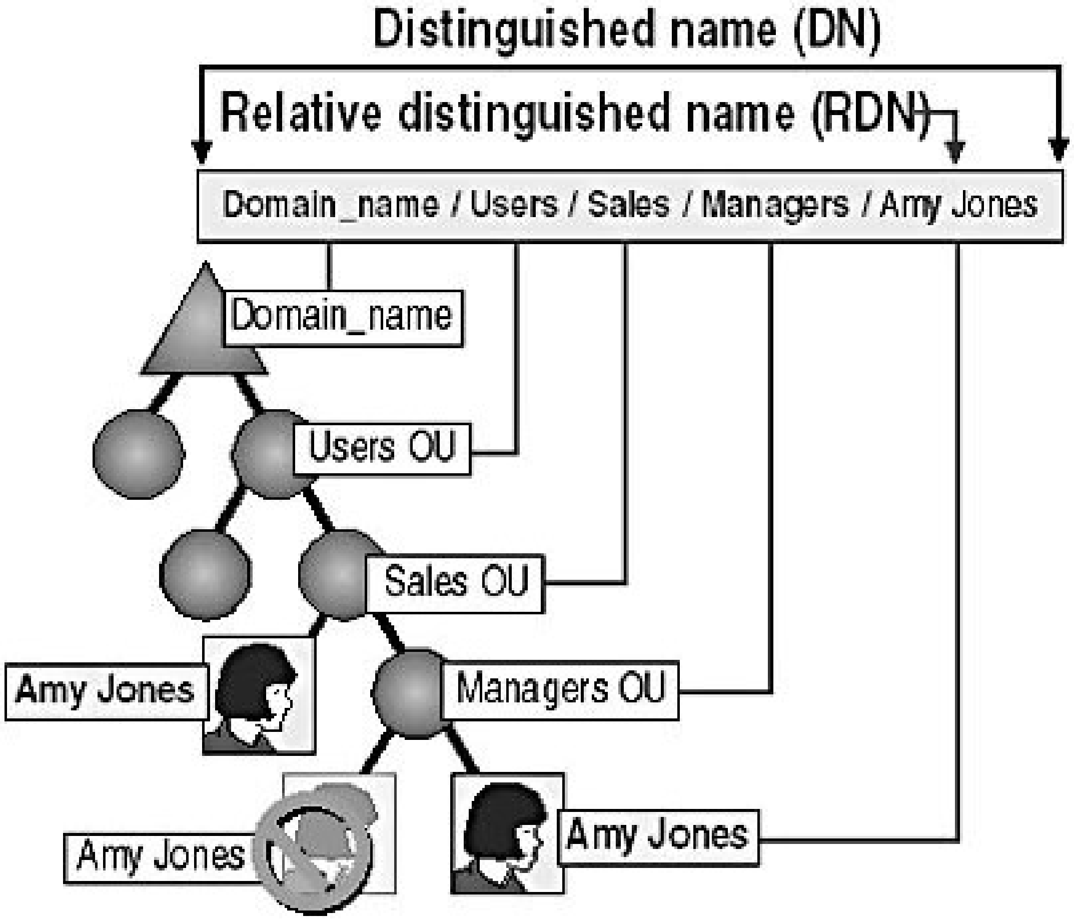
Object naming in AD

- Every object in active directory database is uniquely identified.
- The naming conventions are based on the LDAP standard.
- The distinguished name (DN) of an object consist of the name of the domain in which the object is located, plus the path down the domain tree through the container objects to the object itself.
- The part of object’s name that is stored in the object itself is called its relative distinguished name (RDN)

DN & RDN

- Every object in active directory database is uniquely identified by name that can be expressed in several forms.
- Naming conventions are based on LDAP standard defined by RFC2251 published by IETF.
- The distinguished name(DN) of an object made up of the name of the domain in which the object is located, plus the path down the domain tree through the container objects to the object itself.
- The part of an object’s name that is stored in the object itself is called its relative distinguished name(RDN).

Cont..


Distinguished name (DN)
Relative distinguished name (RDN)
Domain_name / Users / Sales / Managers / Amy Jones
Domain_name
Users OU
Sales OU
Amy Jones
Managers OU
Amy Jones
Amy Jones

Canonical name

- Most AD applications refer to objects using their canonical names.
- Canonical name is DN in which the domain name comes first ,followed by the names of the object’s parent containers working down from the root of the domain and separated by forward slashes, followed by object’s RDN as follows:
- Zacker.com/sales/inside/jdoe

LDAP notation

- DN can also be expressed in LDAP notation.
- LDAP notation reverses the order of the object names, starting with the RDN on the left and the domain name on the right.
- Elements are separated by commas and include the LDAP abbreviations that define each type of element.
- Ldap://cz1.zacker.com/cn=Pruthvi,ou=Computer,ou=GP,dc=gpahmedabad,dc=ac.in
- cn=common name ou=organizational unit dc=domain component

- Zacker.com/sales/inside/Pruthvi <= canonical Name

Globally unique Identifiers (GUID)

- In addition to its DN, every object in the tree has a globally unique identifier(GUID), which is a 128-bit number that is automatically assigned by Directory System Agent when object is created.
- DN can be changed but GUID can not be changed .
- The *directory system agent* (DSA) is a collection of services and processes that run on each Windows 2000 Server and later domain controller and provides access to the data store. The data store is the physical store of directory data located on a hard disk.

User principle names

- DN are used by applications and services when they communicate with AD, but they are not easy for users to understand ,type or remember.
- So each user object has a UPN that consists of username and suffix , separated by @ symbol, just like standard email address.
- User account name. Also known as the logon name. UserName
- Separator. A character literal, the at sign (@).
- UPN suffix. Also known as the domain name. *Example.Microsoft***.com**

LDAP

- Lightweight Directory Access Protocol
- As the name suggests, it is a lightweight client-server protocol for accessing directory services, specifically X.500-based directory services
- Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network.

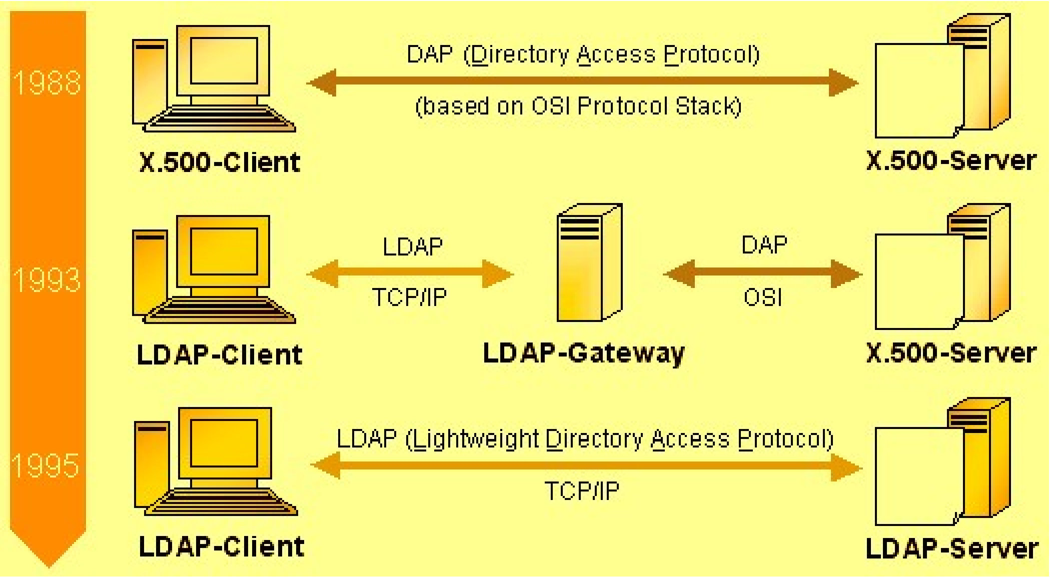
LDAP

- LDAP is software protocol for enabling anyone to locate organization, individuals and other resources such as files and devices in a network, whether on the public internet or on a corporate intranet.
- It is lightweight version of DAP , which is part of X.500, a standard for directory services in a network.
- It is lighter because in its initial version it did not include security features.
- Microsoft includes it as part of what it calls active directory in a number of products including Outlook Express.

LDAP

- LDAP allows you to search for an individual without knowing where they’re located.
- LDAP directory is organized in a simple “tree” hierarchy consisting of the following levels:
  - The root directory, which branches out to
  - Countries, each of which branches out to
  - Organizations, which branch out to
  - Organizational units, which branches out to
  - individuals

Cont..


1988
X.500-Client
DAP (Directory Access Protocol)
(based on OSI Protocol Stack)
X.500-Server
1993
LDAP-Client
LDAP
TCP/IP
LDAP-Gateway
DAP
OSI
X.500-Server
1995
LDAP-Client
LDAP (Lightweight Directory Access Protocol)
TCP/IP
LDAP-Server

Forests, Trees, Roots and Leaves

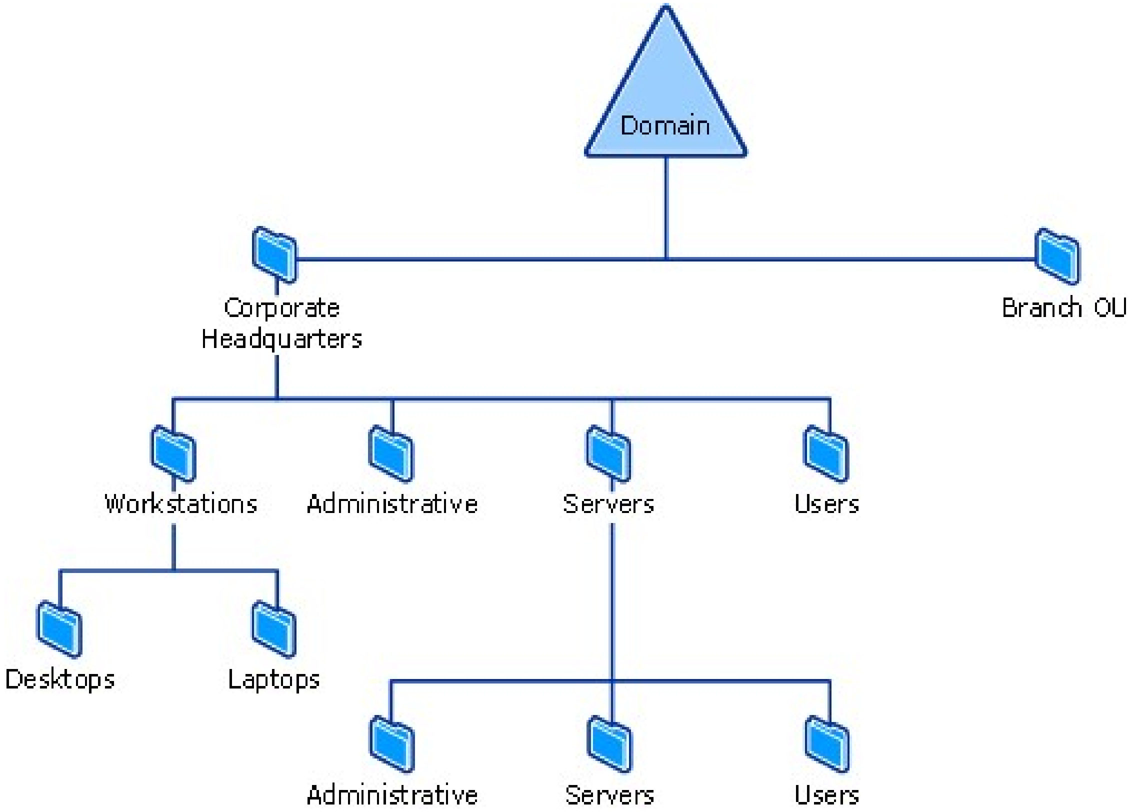
Forest:--

- A forest is a collection of one or more Active Directory domains. The first domain installed in a forest is called the forest root domain.
- A forest contains single definition of network configuration and share a common global catalog, directory schema, logical structure and directory configuration.
- No data is replicated by Active Directory outside the boundaries of the forest. Therefore, the forest defines a security boundary.
- At the top of each directory tree is the root.

Trees:--Trees are created within the forest. If a domain is a subdomain of another domain, the two domains are considered a tree.

Leaves:--

A leaf object represents an actual resource on the network, such as a workstation, printer, shared directory, file, or user account. Leaf objects can not contain other objects.


Domain
Corporate Headquarters
Branch OU
Workstations
Administrative
Servers
Users
Desktops
Laptops
Administrative
Servers
Users

- A Windows domain is a form of a computer network in which all user accounts, computers, printers and other security principals, are registered with a central database (called a directory service) .
- Authentication takes place on domain controllers.
- Each person who uses computers within a domain receives a unique user account that can then be assigned access to resources within the domain
- Windows domains can be organized into following domain models.
- **Single domain:** In this model, only one domain contains all network resources.
- **Master domain:** The master model usually puts users at the top-level domain and then places network resources, such as shared folders or printers, in lower-level domains (called resource domains). In this model, the resource domains trust the master domain.
- **Multiple master domains:** This is a slight variation on the master domain model, in which users might exist in multiple master domains, all of which trust one another, and in which resources are located in resource domains, all of which trust all the master domains.

Organizational Units

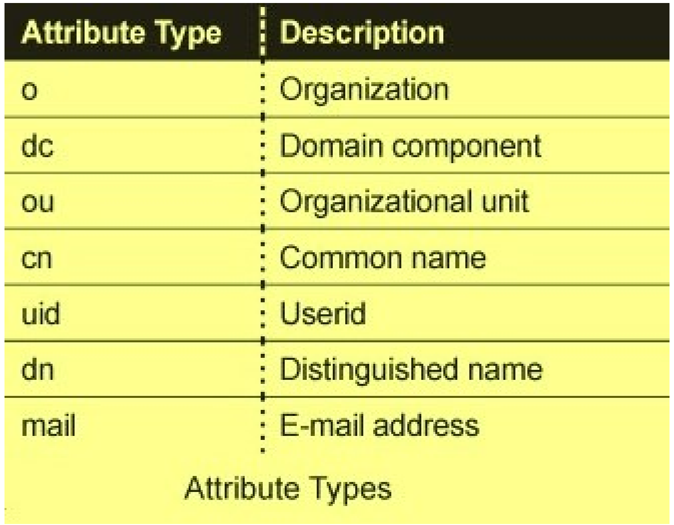
- They are simple a container that the administrator creates that he can use for any purpose.
- Most administrators will create logical organizational units and place users and/or groups inside them in order to setup specific permissions or policy.
- For example, he may create an organizational unit called “Accounting” and place the executives and the accounting department into it in so that they can have access to specific resources that are not available to the rest of the network.

LDAP NOTATION

Three object naming formats that are supported by AD are –

LDAP DN and RDN names

- LDAP defines operations for adding, searching, modifying, and deleting directory entries.
- An LDAP server is required to provide a LDAP directory service.
- *LDAP is based on entries; an entry is a set of attributes identified by a globally unique Distinguished Name (DN).*
- *Each of a directory entry's attributes has a type and one or more values.*
- *The attributes in a directory entry's distinguished name(DN) are arranged in a hierarchy from right to left with the rightmost attribute as the top entry and with the leftmost attribute(s) that are unique to its level called a Relative Distinguished Name (RDN).*
- *A DN is a sequence of RDNs.*



Attribute Type	Description
o	Organization
dc	Domain component
ou	Organizational unit
cn	Common name
uid	Userid
dn	Distinguished name
mail	E-mail address

Attribute Types

LDAP URL’s

- An LDAP URL begins with the prefix “LDAP,” and then it names the server holding Active Directory services followed by the attributed name of the object (the distinguished name). For example:
- ***LDAP://ADserver.example.com/cn=nikhil, ou=People, dc=example, dc=com***

LDAP based canonical names

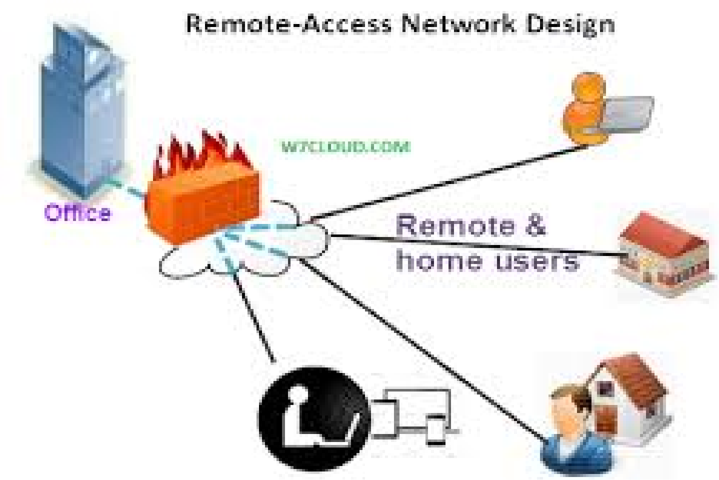
- By default, Active Directory administrative tools display object names using the *canonical name* format, which lists the RDNs from the root downward and without the RFC 1779 naming attribute descriptors (dc=, ou=, or cn=).
- The canonical name uses the DNS domain name format
- ***DN:*** *cn=nikhil, ou=People, dc=example, dc=com*
- ***Canonical Name:*** *example.com/people/nikhil*

Remote Network Access

- What is Remote Network Access?
- The remote access technology allows logging into system as an authorized user from any location.

- Where it is Used?
- Remote access is commonly used on corporate computer network but can also be utilized on home network.

- If only the file or network service are needed , then remote access network is the best solution.



- Why Remote Access Network?

- Internet Access
- Remote access to stored private or shared files on the LAN
- Access centralized Database
- Access hosted web Application
- For send or receive E-mail
- Remote access to a centralized application , such as an accounting system

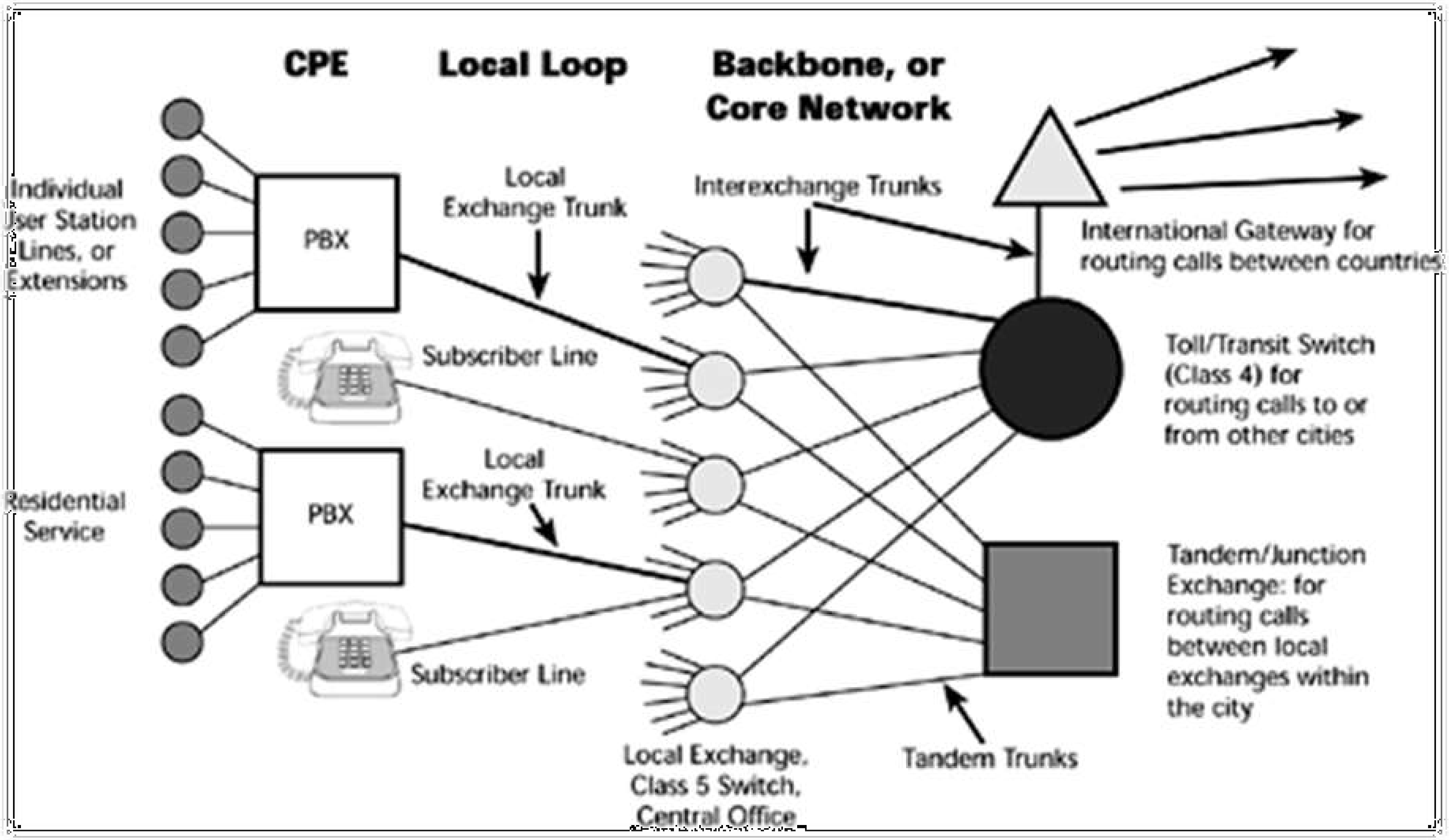
PSTN NETWORK

What is PSTN?

PSTN - short for public switched telephone network, also knows as the plain old telephone system(POTS) is basically the inter-connected telephone system over which telephone calls are made via copper wires.

- PSTN is based on the principles of circuit switching
- Therefore when a call is made a particular dedicated circuit activates which eventually deactivates when the call ends
- Telephone calls transmits as analogue signals across copper wires

Structure of the PSTN



CPE
Local Loop
Backbone, or Core Network
Individual User Station Lines, or Extensions
PBX
Local Exchange Trunk
Interexchange Trunks
International Gateway for routing calls between countries
Subscriber Line
Toll/Transit Switch (Class 4) for routing calls to or from other cities
Residential Service
PBX
Local Exchange Trunk
Tandem/Junction Exchange: for routing calls between local exchanges within the city
Subscriber Line
Local Exchange, Class 5 Switch, Central Office
Tandem Trunks

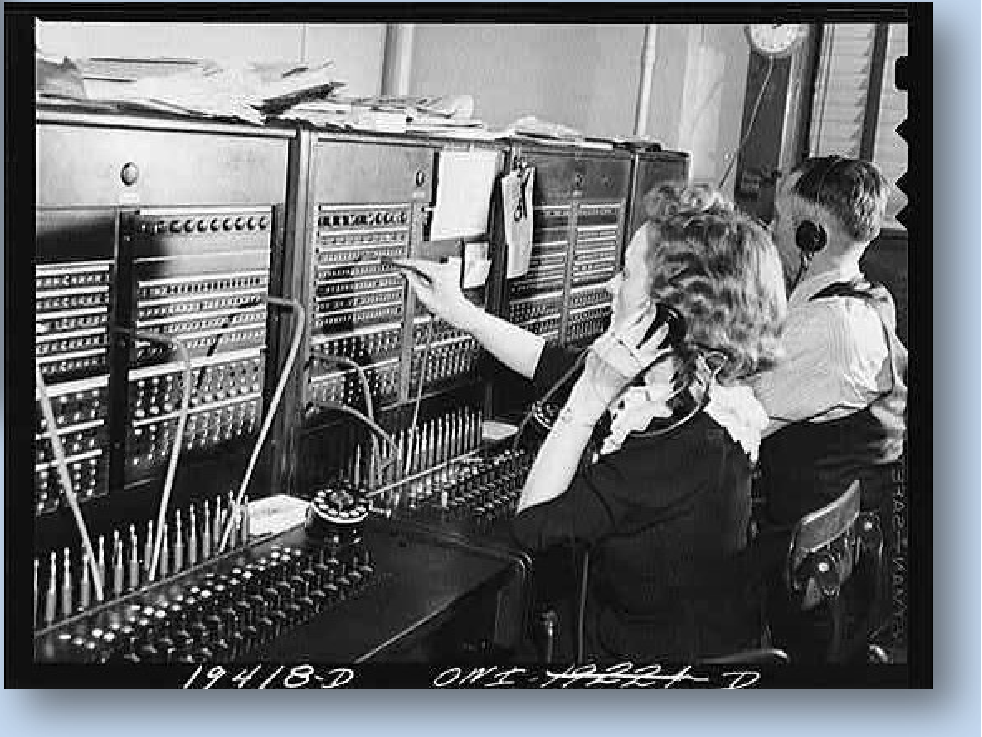
Evolution of PSTN

Inception

- 1876 – Invention of the first telephone by sir **Alexander Graham Bell**
  - Telephones were sold in pairs and the customers were supposed to lay out there own cables
  - Connectivity type – point to point connections
  - Network structure – mesh topology
- 28th January 1878 – Worlds' first telephone exchange was established at New-Haven in Connecticut in the USA
  - Network structure – star topology
  - Switching technique – manual switching

Manual exchanges

Manual switch board



Manual switching

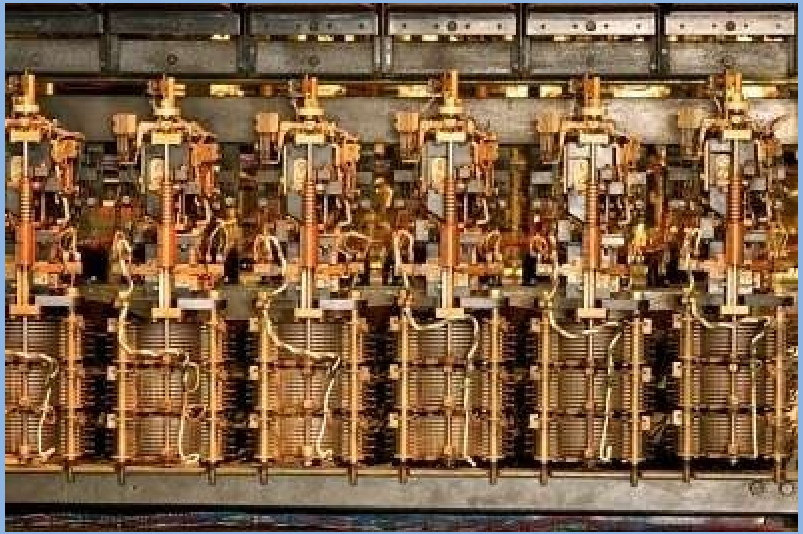
Intermediate

- 1887 – Almon Brown Strowger invented the first electromechanical switch, known as the Strowger switch or step by step switch
  - Switch operated according to the train of pulses generated by the customer premises telephone
  - Pulses were generated by a telegraph key on the telephone until the dial was introduces
- 1920's – Rotary dial telephones enters service

Intermediate

- 1935 – Crossbar switches were introduced
  - Intersecting bars move to make contact in order to complete the circuit
  - Markers were used to control exchanges
  - Takes only 1/10 of a second to complete a call
- 1950 – Time division multiplexing (TDM) is introduced
- 1960's – touch tone pad phones were introduces
- 1968 – stored program control switching was introduces
  - An electronic switch
  - Upgradable to new versions since software dependant
  - Call set-up is controlled by programmed software's
  - calls are completed within nano seconds

Electro-mechanical exchanges



Strowger switch

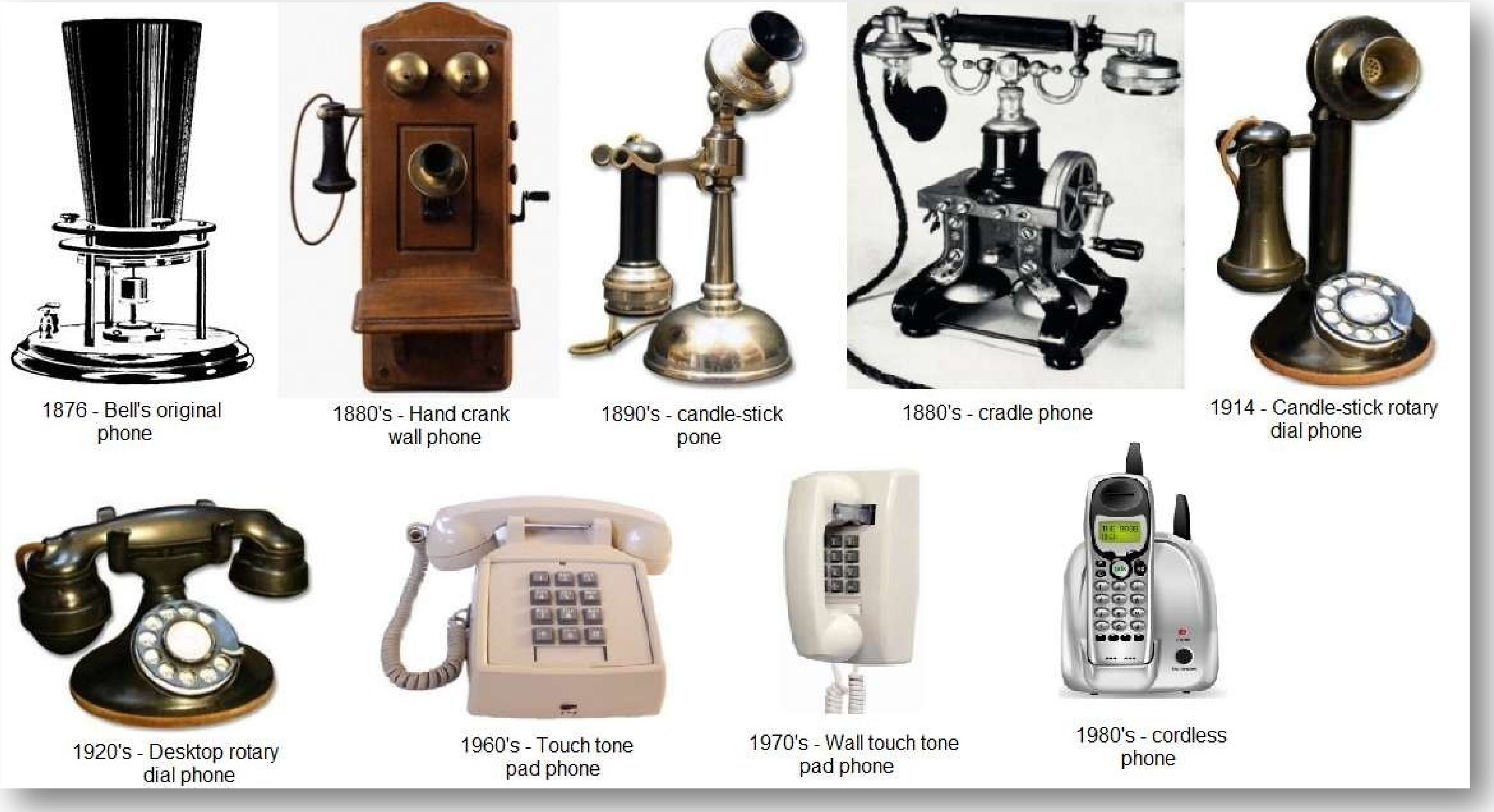
Crossbar switch

Present

- ❑ In today’s PSTN, call routing from source to destination is predominantly controlled by digital switches that were introduced in the 1970’s
- ❑ Apart from voice communications, data communications are also provided via the PSTN at present

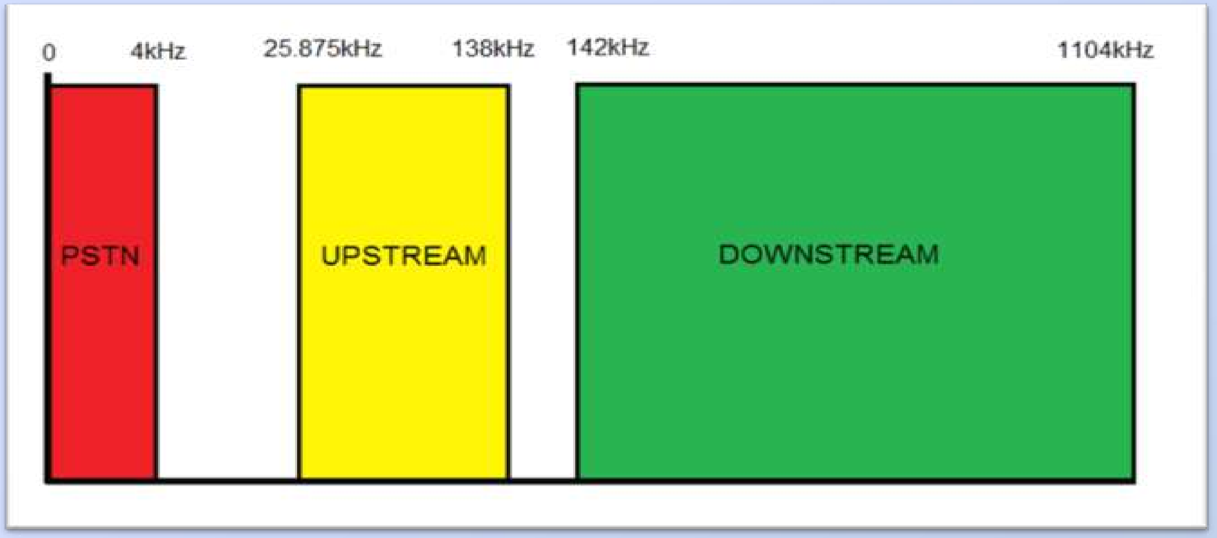
DMS - 100 digital switch

Evolution of the Telephone


1876 - Bell's original phone
1880's - Hand crank wall phone
1890's - candle-stick pone
1880's - cradle phone
1914 - Candle-stick rotary dial phone
1920's - Desktop rotary dial phone
1960's - Touch tone pad phone
1970's - Wall touch tone pad phone
1980's - cordless phone

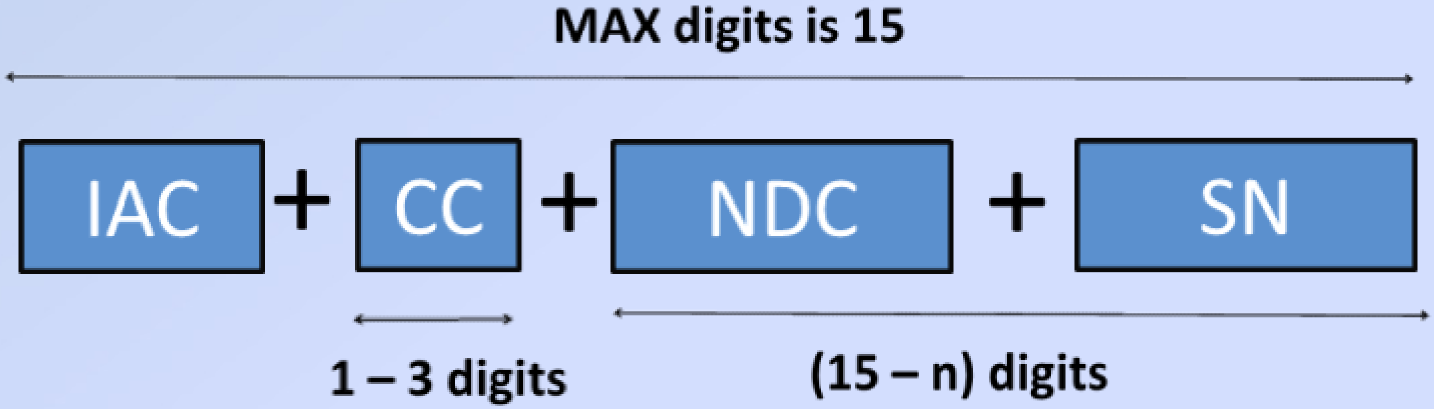
Bandwidth allocation

- ❑ voice bandwidth – 300 – 3400Hz
- ❑ DSL frequency bands
  - Up stream – 25.875kHz – 138kHz
  - Down stream – 142kHz – 1104kHz



Numbering schemes

- A PSTN number comprises of,
  - A international access code/exit code (IAC/EC)
  - A country code (CC)
  - A national destination code also know as an area code (NDC/AC)
  - A subscriber number (SN)
- Maximum length of a number is 15digits



- n = country code + international access code
- most international access code are either (00) or (011) except for few exceptions like (009 - Nigeria) and (119 - Cuba)

Signaling

- Signaling is the controlling of communications
- Basically anything but voice transmission is signaling
- Ex : call setup, call termination, billing , caller ID etc…
- There are types of signaling
  - Channel associated signaling (CAS) - signaling information is transmitted within the same voice channels
  - Also know as in-band signaling

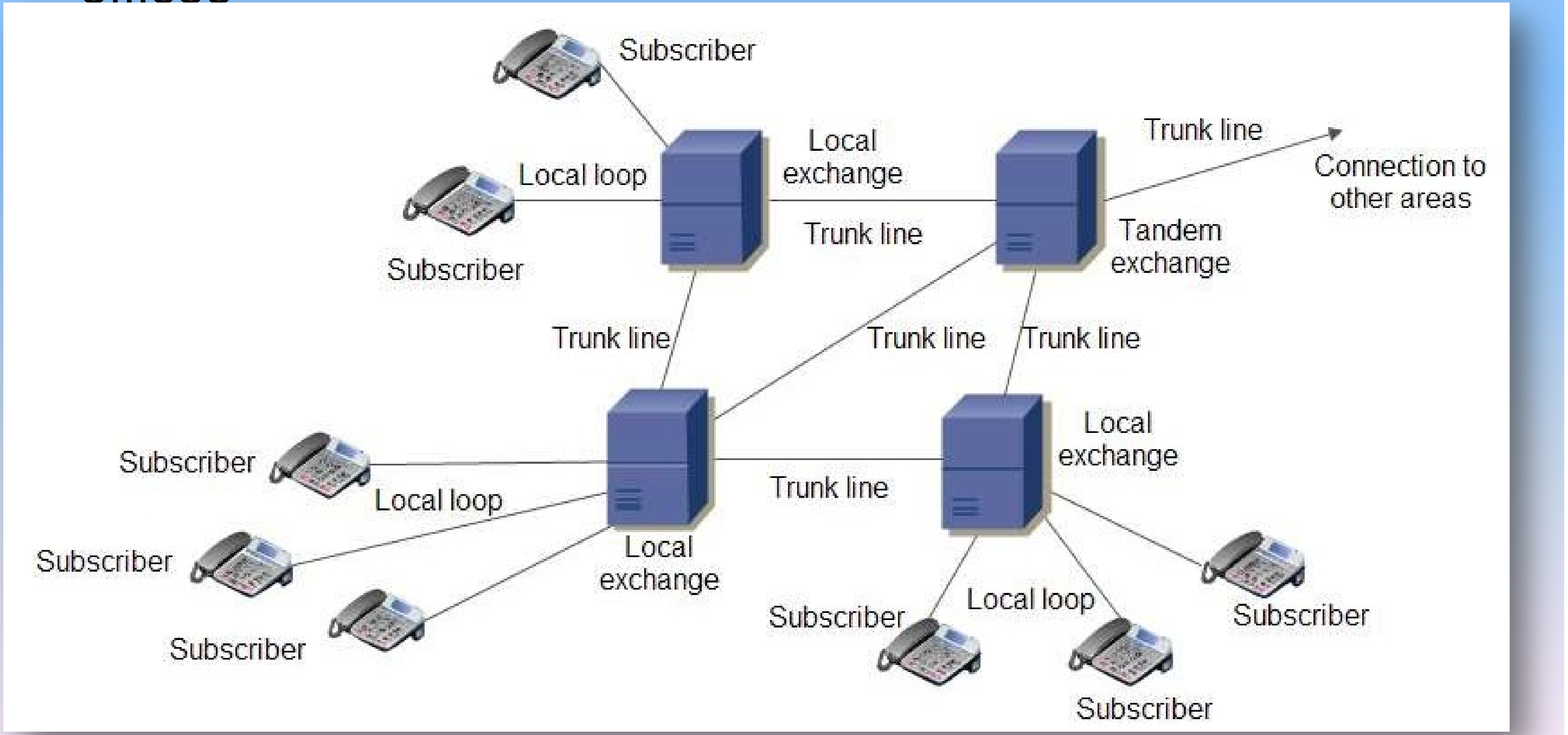
Ex : Dual tone multi frequency signaling (DTMF)

  - Common channel signaling (CCS) - signaling information is transmitted via a separate channel
  - Also know as out-band signaling

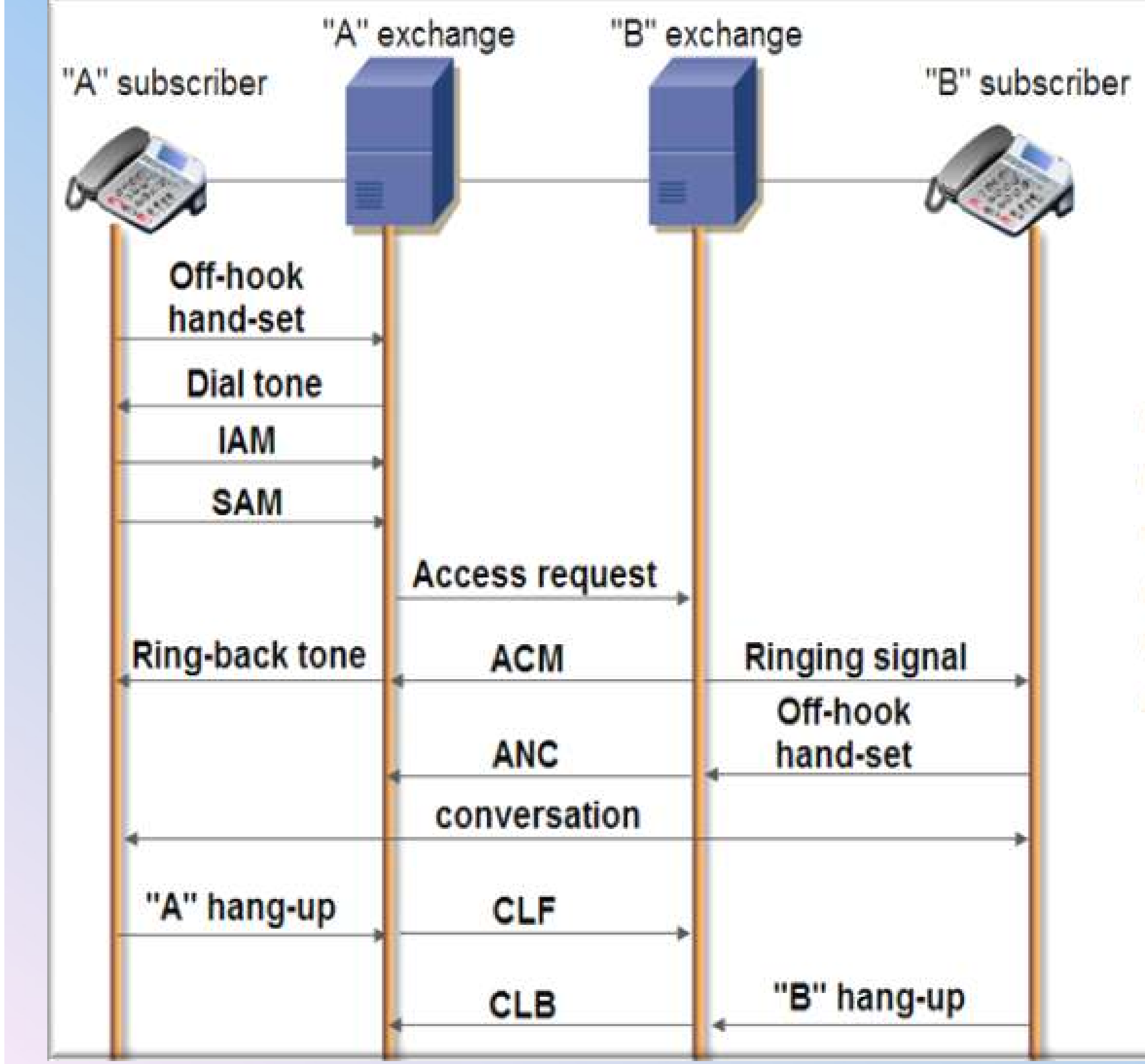
Ex : signaling system #7 (SS7)

Switching systems

- ❖ Switching systems, basically are what determines the routing pathway of a call
- ❖ Switches are contained in local exchanges and central offices



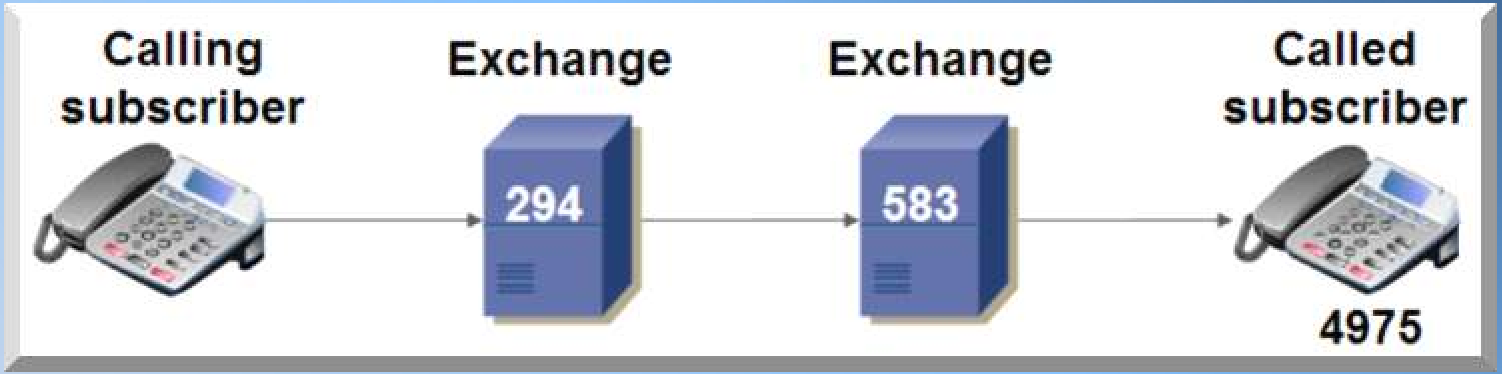
Call setup process



- Initial address message (IAM)
- Subsequent address message (SAM)
- Address complete message (ACM)
- Answer signal and charging (ANC)
- Clear forward (CLF)
- Clear back (CLB)

Call setup process

Example : Suppose the calling subscriber dialed “5834975”



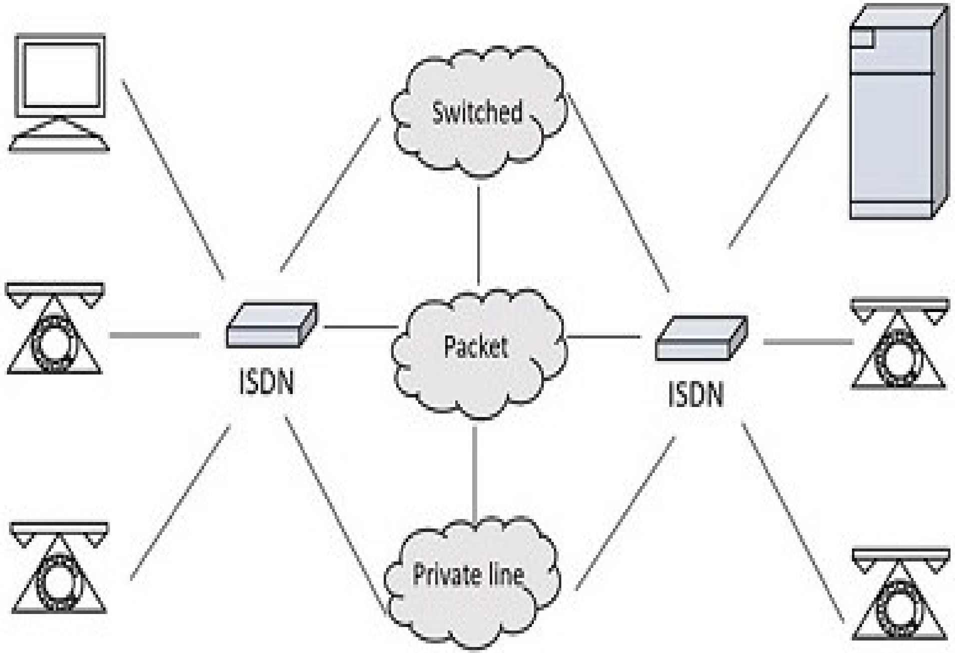
- At first the exchange(294) which the calling subscriber is directly connected to, examines the dialed digits “583-4975”
- Secondly it acts upon the first three digits and access its look up table to rout the call to the “583” exchange
- Then the “583” exchange acts upon the information
- It identifies the dialed number and connects the correct subscriber loop which matches the “4975” number
- Then ring current is applied to the loop to alert the called subscriber and when the call is answered conversation begins

INTEGRATED SERVICES DIGITAL NETWORK (ISDN)

INTRODUCTION

- **Integrated Services Digital Network (ISDN)** is a set of communication standards for digital telephone connection and the transmission of voice and data over a digital line.

- **Integrated Service Digital Network (ISDN)** is a set of CCITT/ITU standards.



WORKING OF ISDN

- Home and business users who install an ISDN adapter receive Web pages at up to **128Kbps** compared with the maximum **56Kbps** rate of a modem connection.

- ISDN requires adapters at both ends of the transmission, so your access provider also needs an ISDN adapter.

- There are two levels of service:

1. **The Basic Rate Interface (2B+D)** – Intended for the home and small enterprise. (Consist of two 64Kbps B-channels and one 16Kbps D-channel. Thus user can have up to 128Kbps service.)

   (B channel is a telecommunications term which refers to the ISDN channel in which the primary data or voice communication is carried. It has a bit rate of 64 kbit/s in full duplex. D channel is a telecommunications term which refers to the ISDN channel in which the control and signalling information is carried. The bit rate of the D channel of a basic rate interface is 16 kbit/s, whereas it amounts to 64 kbps on a primary rate interface.)

1. **The Primary Rate Interface(23B+D)** – Intended for larger users. (Consist of 23 B-channels and one 64Kbps D-channel In the United States or 30 B-channels and 1 D-channel in Europe.)

ISDN channel Types

- Bearer channel (B channel) :
  - A bearer channel is defined at a rate of 64 Kbps. It is the basic user channel and can carry any type of digital information in full-duplex mode as long as the required transmission rate does not exceed 64 Kbps.
- Data Channel (D channel) :
  - A data channel can be either 16 or 64 Kbps, depending on the needs of the user. The name says data but the primary function of a D channel is to carry control signaling for the B channel.
- Hybrid channel (H channel) :
  - Hybrid channels are available with data rates of 384 Kbps (H0), 1536 Kbps (H11), or 1920 Kbps (H12). These rates suit H channels for high data-rate applications such as video, teleconferencing and so on.

Cont..

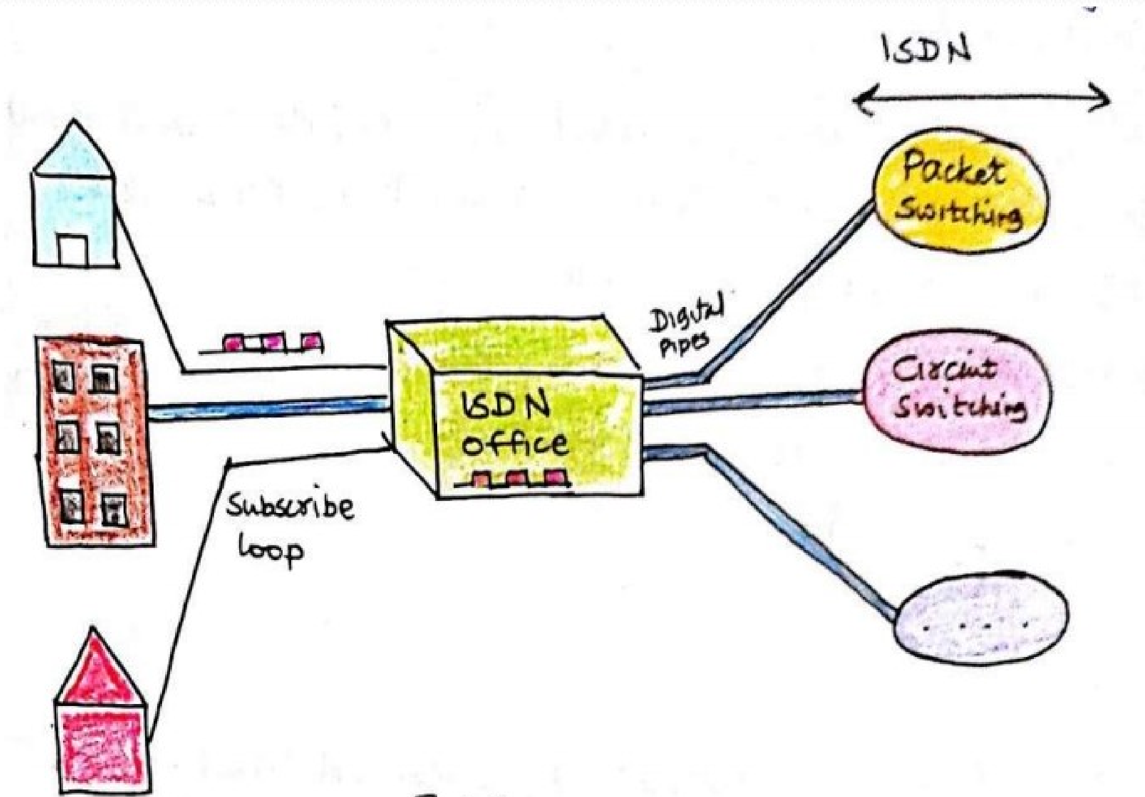

ISDN
Packet Switching
Digital Pipes
Circuit Switching
ISDN office
Subscribe loop

Fig 1:

SUPPORTED SERVICES

- Voice calls
- Facsimile
- Videotext
- Teletext
- Electronic Mail
- Database access
- Data transmission and voice
- Connection to internet
- Electronic Fund transfer
- Image and graphics exchange
- Document storage and transfer
- Audio and Video Conferencing
- Automatic alarm services to fire stations, police, medical etc.

Cont..

- ISDN is concept is the integration of both Analog or voice data together with digital data over the same network.

- Although the ISDN you can install is integrating these on a medium designed for Analog transmission, broadband ISDN is intended to extend the integration of both services throughout the rest of the end-to-end path using fiber optic and radio media.

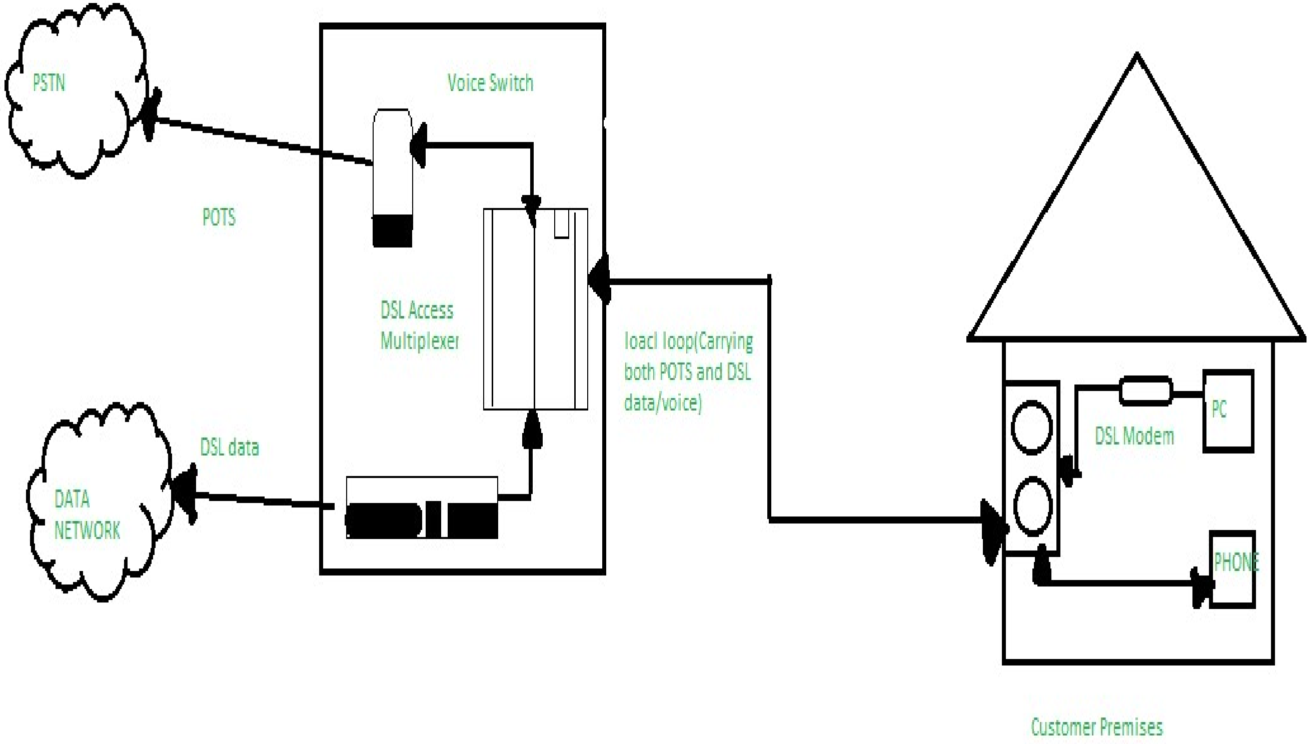
DSL (Digital Subscriber Line)

❖ What is DSL ?

- Digital Subscriber Line (DSL, *originally*, **digital subscriber loop**) is a communication medium, which is used to transfer internet through copper wire telecommunication line.
- DSL is a technology which uses the existing transmission medium (telephone wire) to provide high – speed transfer of information across the internet.
- Along with cable internet, DSL is one of the most popular ways *ISP's* provide broadband internet access.
- DSL allows simultaneous voice and high – speed data service such as super fast internet access over a single pair of copper telephone wire.
- Although the transmitted information is in digital form, the transmission medium is usually an **analog carrier signal** (or the combination of many analog carrier signals) that is modulated by the digital information signal.

❖ How DSL Works ?

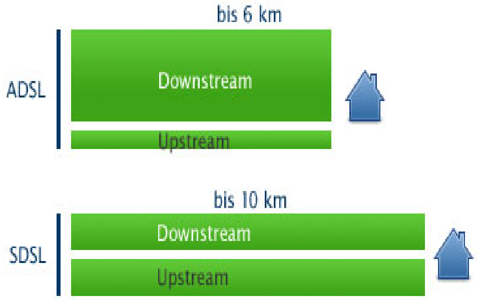
- The underlying technology of transport across DSL facilities uses high-frequency sinusoidal carrier wave modulation, which is an analog signal transmission.
- A DSL circuit terminates at each end in a modem which modulates patterns of bits into certain high-frequency impulses for transmission to the opposing modem.
- Signals received from the far-end modem are demodulated to produce a corresponding bit pattern that the modem retransmits, in digital form, to its interfaced equipment, such as a computer, router, switch, etc.
- If we ask that how we achieve such thing i.e., both telephone and internet facility, then the answer is by using *splitters or DSL filters*. Basically, the use of *splitter* is to splits the frequency and make sure that they can’t get interrupted.


PSTN
Voice Switch
POTS
DSL Access
Multiplexer
loacl loop(Carrying
both POTS and DSL
data/voice)
DSL data
DATA
NETWORK
DSL Modem
PC
PHONE
Customer Premises

❖ Types of DSL :

- **There are Two Types of DSL's :**

1) **Symmetric DSL –** SDSL, *splits* the upstream and downstream frequencies evenly, providing equal speeds to both uploading and downloading data transfer. This connection may provide *2 Mbps* upstream and downstream. It is mostly preferred by small organizations.
2) **Asymmetric DSL –** ADSL, provides a wider frequency range for downstream transfers, which offers several times faster downstream speeds. An ADSL connection may offer *20 Mbps downstream and 1.5 Mbps upstream*, It is because most users download more data than they upload.



- ADSL are widely used DSL modems. There are Two Splitting Methods used.

❖ Advantages of DSL :

- Broadband Internet and Phone can be used at same time. And it is because the voice is transferred on other frequency and digital signals are transferred on others.
- Faster internet above 2 Mbps. (Dial up connection provides 52 Kbps connection).
- No special wiring is needed.
- DSL internet is a very cost-effective method and is best in connectivity.
- User can choose between different connection *speeds* and *pricing* from various providers.

❖ Disadvantages of DSL :

- DSL Internet service only works over a limited physical distance and remains unavailable in many areas where the local telephone infrastructure does not support DSL technology.
- Your DSL connection works faster if you live closer to provider’s central office. The farther your home is from ISP’s office the more your speed will reduce.
- The connection is faster for receiving data than it is for sending data over the Internet.

CATV

History

- CATV origins date back to 1924 when some cable broadcasting was done using cable in European cities.
- In 1948, community antenna received were built where over-the-air signal reception was limited.
- Today, CATV offers Analog and digital channels. Receiving digital channels typically requires a cable box conversion.
- The abbreviation CATV is often used for cable television. It originally stood for Community Access Television or Community Antenna Television, from cable television's origins in 1948. In areas where over-the-air TV reception was limited by distance from transmitters or mountainous terrain, large "community antennas" were constructed, and cable was run from them to individual homes.

CATV

- Community Access Television(CATV) is also commonly known as Cable TV.
- Cable television is a system of delivering television programming to consumers via radio frequency (RF) signals transmitted through coaxial cables, or in more recent systems, light pulses through fiber-optic cables.
- This contrasts with broadcast television (also known as terrestrial television), in which the television signal is transmitted over the air by radio waves and received by a television antenna attached to the television.
- satellite television, in which the television signal is transmitted by a communications satellite orbiting the Earth and received by a satellite dish on the roof.

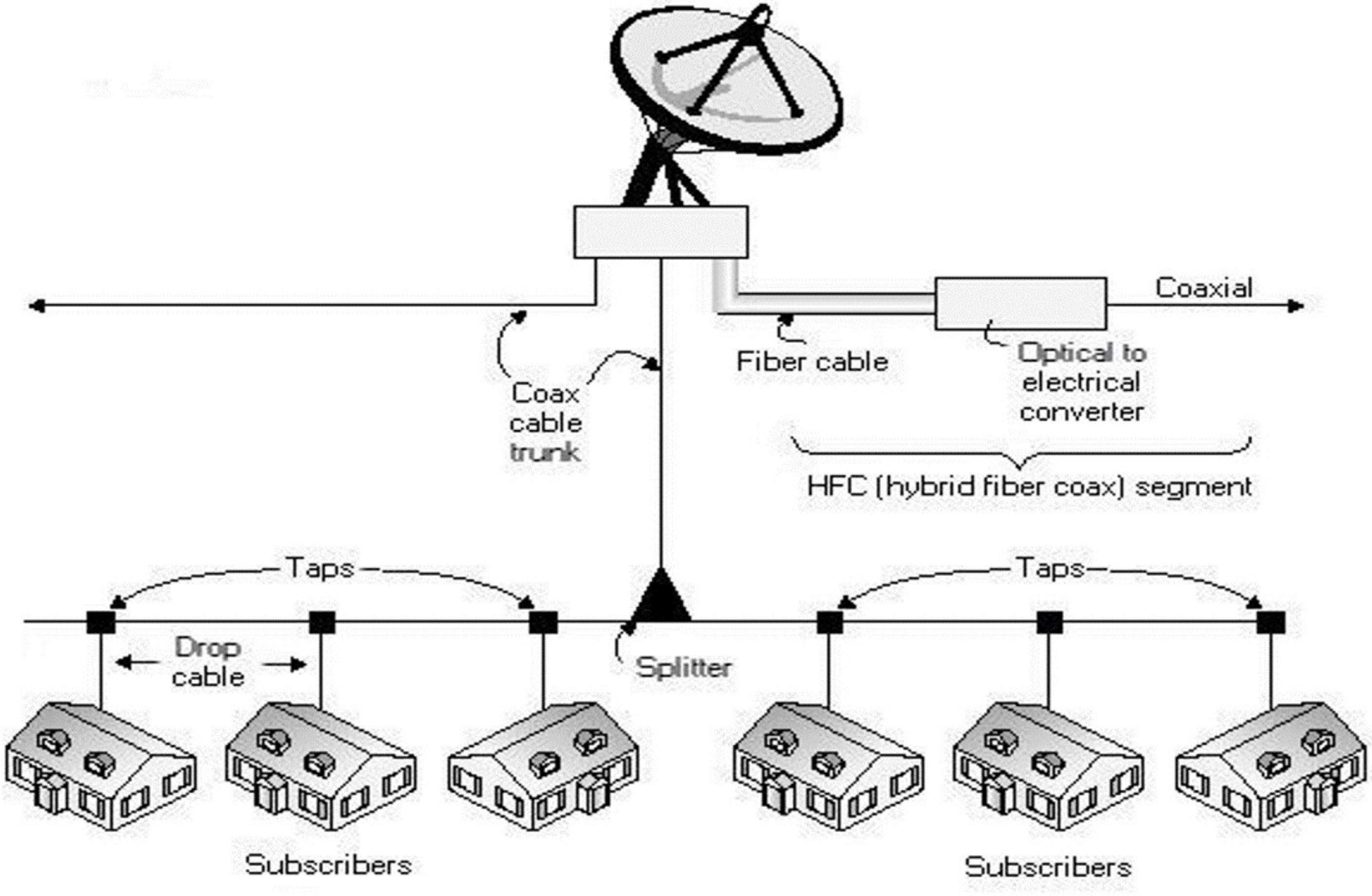
Basics of CATV

- In this type of Television system signals are transmitted through coaxial cables and optical fiber cables.
- For CATV, it needs to have distribution system.
- CATV has two standards, older one is analog TV and newer one is Digital TV.

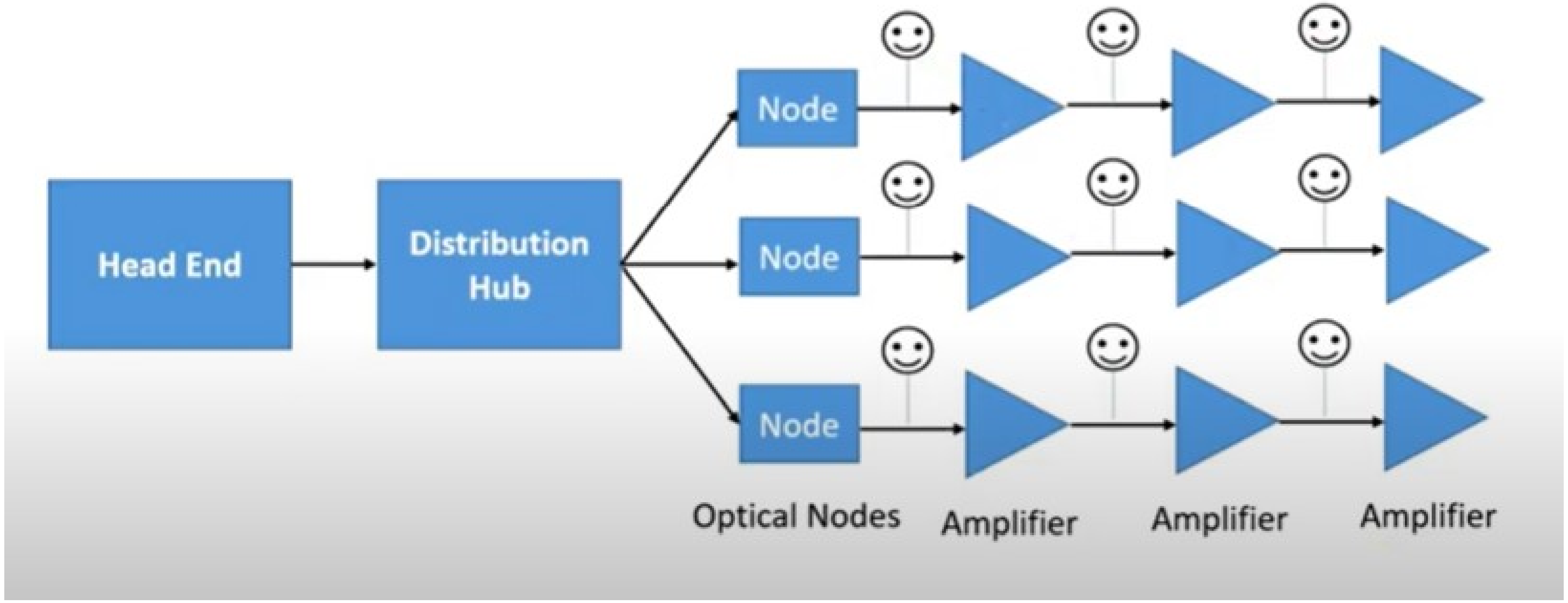
Components of CATV

- Following components are there with CATV system.
  - Cable Network (Coaxial or Optical)
  - Nodes
  - Line Amplifier
  - Power Supply

CATV


Coaxial
Fiber cable
Optical to electrical converter
Coax cable trunk
HFC (hybrid fiber coax) segment
Taps
Taps
Drop cable
Splitter
Subscribers
Subscribers

Block diagram of CATV



Working of CATV

- Television channel transmitted by Head at particular frequency.
- Distribution hub is having amplifier at reasonable distance to keep signal strong.
- Separate TV signals do not interfere here with this channel.

Advantages of CATV

- Cable TV are available at low cost.
- Cable TV gives good service.
- They offers good packages of programs.
- Service cost is cheap.
- Cable TV provides good signals in bad weather conditions like heavy rainfall.

Disadvantages of CATV

- Some private company has different cost.
- Video ON Demand is not available.
- Internet is not available.
- Gaming is not available.

Virtual Private Network

Explanation

- Virtual :

  Virtual means not real or in a different state of being.

- Private :

  Private means to keep something secret from the general public.

- Network :

  A network consists of two or more devices that can freely and electronically communicate with each other via cables and wire.

Definition

- VPN, Virtual Private Network, is defined as a network that uses public network paths but maintains the security and protection of private networks.
- It can transmit information over long distances effectively and efficiently.
- Large corporations, educational institutions, and government agencies use VPN technology to enable remote users to securely connect to a private network.
- The VPN uses strong encryption and restricted, private data access which keeps the data secure from the other users of the underlying network.

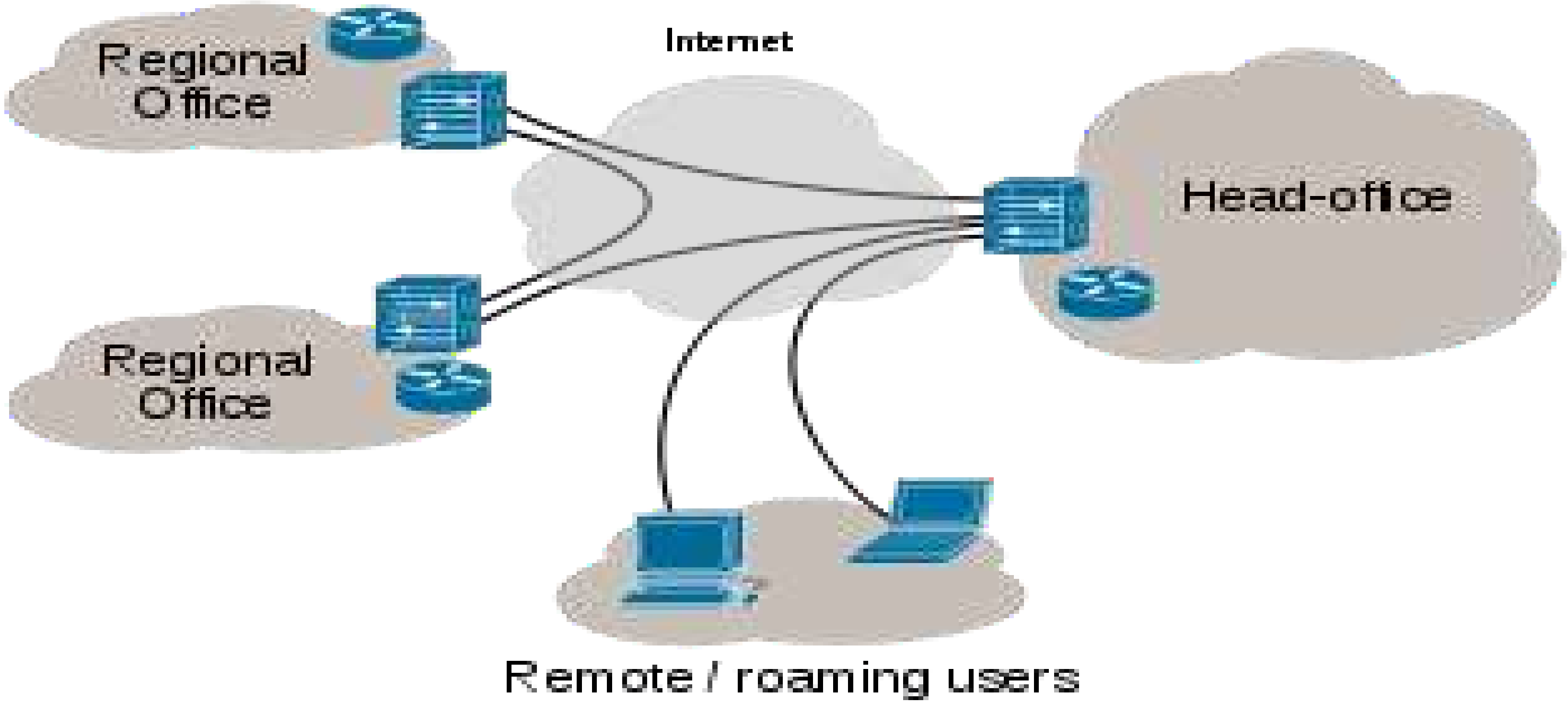
VPN

- A **virtual private network** (**VPN**) extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
- Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network

- Virtual Private Networks may allow employees to securely access a corporate intranet while located outside the office.
- They are used to securely connect geographically separated offices of an organization, creating one cohesive network. Individual Internet users may secure their wireless transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers for the purpose of protecting personal identity and location.
- However, some Internet sites block access to known VPN technology to prevent the circumvention of their geo-restrictions

- A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.
- A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

Internet VPN



- VPNs cannot make online connections completely anonymous, but they can usually increase privacy and security. To prevent disclosure of private information, VPNs typically allow only authenticated remote access using tunneling protocols and encryption techniques.
- The VPN security model provides:
- Confidentiality such that even if the network traffic is sniffed at the packet level (see network sniffer and Deep packet inspection), an attacker would only see encrypted data
- Sender authentication to prevent unauthorized users from accessing the VPN
- Message integrity to detect any instances of tampering with transmitted messages

Tunneling

- In computer networks, a **tunneling protocol** allows a network user to access or provide a network service that the underlying network does not support or provide directly.
- One important use of a tunneling protocol is to allow a foreign protocol to run over a network that does not support that particular protocol; for example, running IPv6 over IPv4.
- Another important use is to provide services that are impractical or unsafe to be offered using only the underlying network services; for example, providing a corporate network address to a remote user whose physical network address is not part of the corporate network.
- Because tunneling involves repackaging the traffic data into a different form, perhaps with encryption as standard, a third use is to hide the nature of the traffic that is run through the tunnels.

Cont..

- The tunneling protocol works by using the data portion of a packet (the payload) to carry the packets that actually provide the service.
- Tunneling uses a layered protocol model such as those of the OSI or TCP/IP protocol suite, but usually violates the layering when using the payload to carry a service not normally provided by the network.
- Typically, the delivery protocol operates at an equal or higher level in the layered model than the payload protocol.

Types of VPN

- **Remote Access VPN**:- Also called as Virtual Private dial-up network (VPDN) is mainly used in scenarios where remote access to a network becomes essential. Remote access VPN allows data to be accessed between a company's private network and remote users through a third party service provider; Enterprise service provider
- **Site to Site VPN – Intranet based**: This type of VPN can be used when multiple Remote locations are present and can be made to join to a single network. Machines present on these remote locations work as if they are working on a single network.
- **Site to Site VPN – Extranet based**: This type of VPN can be used when several different companies need to work in a shared environment. E.g. Distributors and service companies. This network is more manageable and reliable

VPN Protocols

- A ‘VPN Protocol’ is the set of procedures a VPN service uses to keep you protected online.
  - IP security (IPSec)
  - Secure Sockets Layer (SSL)
  - Point-To-Point Tunneling Protocol (PPTP)
  - Layer 2 Tunneling Protocol (L2TP)

PPTP

- PPTP (Point-to-Point Tunneling Protocol) it’s the most widely supported VPN method among Windows users and it was created by Microsoft in association with other technology companies.
- The disadvantage of PPTP is that it does not provide encryption and it relies on the PPP (Point-to-Point Protocol) protocol to implement security measures
- But compared to other methods, PPTP is faster and it is also available for Linux and Mac users.

L2TP

- L2TP (Layer 2 Tunneling Protocol) it’s another tunneling protocol that supports VPNs. Like PPTP, L2TP does not provide encryption and it relies on PPP protocol to do this.
- The difference between PPTP and L2TP is that the second one provides not only data confidentiality but also data integrity.
- L2TP was developed by Microsoft and Cisco as a combination between PPTP and L2F(Layer 2 Forwarding).

IPsec

- IPsec protocol can be used for encryption in correlation with L2TP tunneling protocol. It is used as a “protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream”. IPSec requires expensive, time consuming client installations and this can be considered an important disadvantage.

SSL

- SSL (Secure Socket Layer) is a VPN accessible via https over web browser. The advantage of this SSL VPN is that it doesn’t need any software installed because it uses the web browser as the client application. Through SSL VPNs the user’s access can be restrict to specific applications instead of allowing access to the whole network.

VPN CLIENT & SSL VPNs

VPN Client

- A VPN client is a software based technology that establishes a secure connection between the user and a VPN server.
- Some VPN clients work in the background automatically, while others have front-end interfaces that allow users to interact with and configure them.
- VPN clients are often applications that are installed on a computer, though some organizations provide a purpose-built VPN client that is a hardware device pre-installed with VPN software.
- Both sides of VPN connection must be running compatible VPN software using compatible protocols.
- For the remote access VPN solutions, the software you install depends on the VPN itself.

VPN Client

- Dedicated VPN solutions also sell client software that we can distribute to our users. Usually this software carries a per-copy charge.
- Mainly there are two types of VPN clients:
  a) Native or built-in VPN clients
  b) Third Party VPN clients
- Some of the VPN Software which are used now a days are as listed below:
  1. Cisco System VPN Client
  2. SoftEther VPN
  3. OpenVPN Client

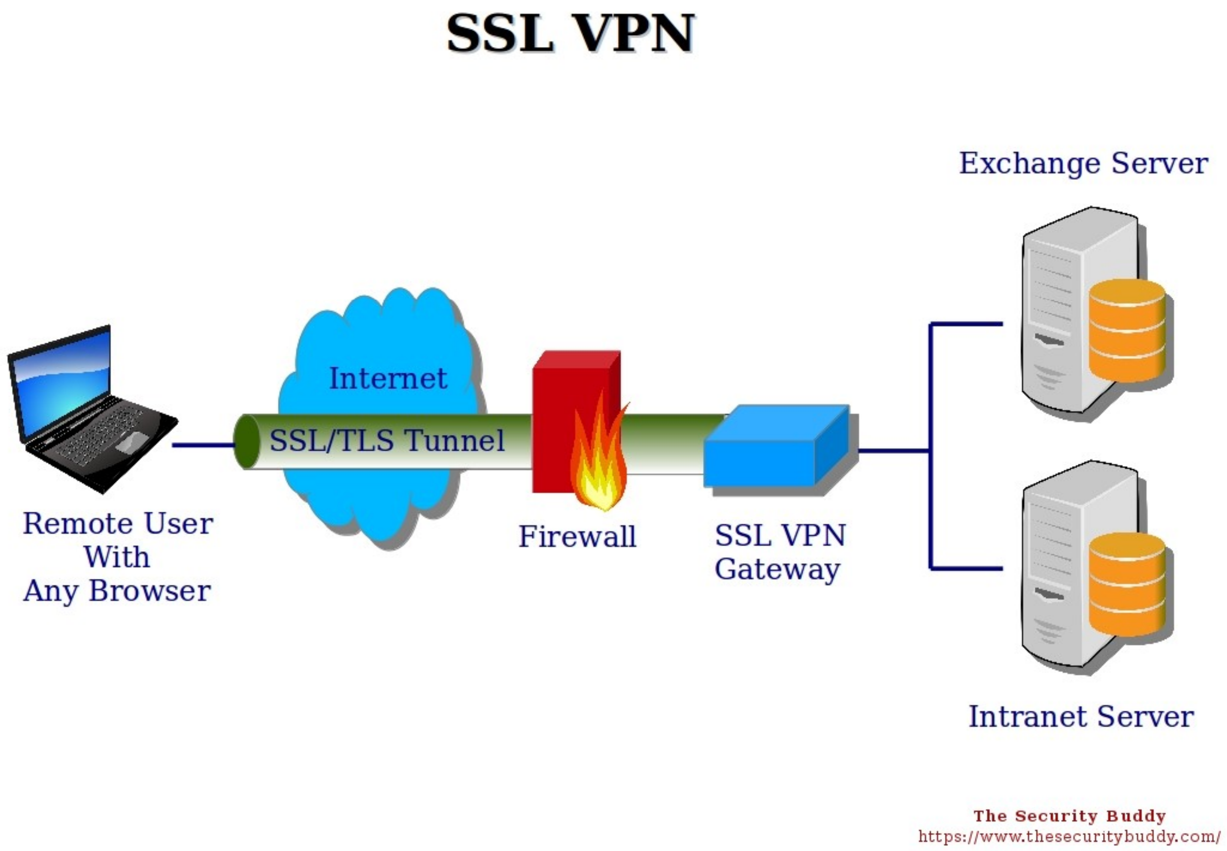
SSL VPN

- SSL VPN means **S**ecure **S**ocket **L**ayer **V**irtual **P**rivate **N**etwork.
- An SSL VPN is a form of VPN that can be used with a standard Web browser. In contrast to the traditional Internet Protocol Security (IPSec) VPN.
- This VPN does not required the installation of specialized client software on the end user's computer.
- It's used to give remote users with access to Web applications, client/server applications and internal network connections.

SSL VPN

- VPN provides a secure communications mechanism data and other information transmitted between two endpoints.
- SSL VPN consists of one or more VPN devices to which the users connects by using his Web browser.
- The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol or its successor, the Transport Layer Security protocol.
- An SSL VPN offers versatility, ease of use and granular control for the range of users on a variety of computers, accessing recourses from many locations.

SSL VPN


SSL VPN
Exchange Server
Internet
SSL/TLS Tunnel
Remote User With Any Browser
Firewall
SSL VPN Gateway
Intranet Server
The Security Buddy
https://www.thesecuritybuddy.com/

Types of SSL VPN

1. **SSL Portal VPN: -**
   - This type of SSL VPN allows for a single SSL connection to a Web site so the end user securely access multiple network services.
   - The site is called portal because it is one door that leads to many other resources.
   - **The remote user accesses the SSL VPN Gateway using any modern Web browser**, identifies himself or herself to the gateway using an authentication method supported by the gateway and is then presented with a web page that acts as the portal to the other services.

Types of SSL VPN

2. **SSL Tunnel VPN: -**

    - This type of SSL VPN allows a Web browser to securely access multiple network services, including applications and protocols that are not Web based, through a tunnel that is running under SSL.
    - SSL tunnel VPNs require that the Web browser be able to handle active content, which allows them to provide functionally that is not accessible to the SSL portal VPNs.
    - Example of active content include Java, JavaScript, Active X or Flash applications or plug-ins.