Network Management and Administration
Code:3360703

UNIT – I

Exploring Directory Services and Remote Access

Prepared By:

Chirag Patel

Lecturer in Computer Engineering,
K D Polytechnic, Patan

1.A Directory Service (May-2015)

- A network service that identifies all resources on a network and makes them accessible to users and applications.
- Here resources mean e-mail addresses, computers, and peripheral devices such as printers.
- **A directory service** is the collection of software and processes that store information about your enterprise, subscribers, or both.
- **A directory service or name service**, maps the names of network resources to their respective network addresses.
- With the help of name service type of directory, a user does not have to remember the physical address of a network resource. You can locate the resource by simply providing a name.
- Each resource on the network is considered an object on the directory server. Information about a particular resource is stored as attributes of that object.

1.A Directory Service (May-2015)

- **An example** of a directory service 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.
- Ideally, the directory service should make the physical network topology and protocols transparent so that a user on a network can access any resource without knowing where or how it is physically connected.
- There are a number of directory services that are used widely.
- Two of the most important ones are **LDAP**, which is used primarily for e-mail addresses, and **Netware Directory Service (NDS)**, which is used on Novell Netware networks.
- Virtually all directory services are based on the X.500 ITU standard, although the standard is so large and complex that no vendor complies with it fully.

1b. Types of Directory Service and Directories access protocol

1. Novell e Directory Services
2. Windows NT Domains
3. MS Active Directory
4. X.500 Directory Access Protocol
5. Lightweight Directory Access Protocol

1. Novell directory service (NDS)

- **Novell directory service (NDS)** is a popular software product for managing access to computer resources and keeping track of the users of a network.
- Using NDS, a network administrator can set-up a database of users and manage them using a directory with an easy-to-use graphical user interface.
- Users of computer at remote location can be added, updated and managed centrally.
- Application can be distributed electronically and maintained centrally.
- NDS can be installed to run under Windows NT, Sun-Microsystems's Solaris and UNIX and as well as under Novelle's own Netware.
- So, it can be used to control a multi-platform network.
- It also called edirectory.

2. Windows NT Domain

- Windows NT Directory Services, or NTDS, is the directory services used by Microsoft Windows NT to locate, manage, and organize network resources.
- The Windows NT domain model breaks an organization into chunks called *domains;* all these domains 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 domaincontrollers* (BDCs) to kick in if the PDC fails.

2. Windows NT Domain

- Windows NT Directory Services, or NTDS, is the directory services used by Microsoft Windows NT to locate, manage, and organize network resources.
- The Windows NT domain model breaks an organization into chunks called *domains;* all these domains 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 domaincontrollers* (BDCs) to kick in if the PDC fails.

3. MS Active Directory

- For smaller networks Windows NT domains work relatively well but they can become difficult to manage for larger networks.
- In addition to this the system is not nearly as comprehensive as eDirectory.
- To overcome all the above problem Microsoft developed a directory service called Active Directory, which is a comprehensive directory service that runs on Windows 2000 Server and later.
- Active Directory is fully compatible with LDAP (versions 2 and 3) and also with the Domain Name System (DNS) used on the Internet.
- Active Directory is an integral part of the windows 2000 architecture.
- Such as Novell Directory Services (NDS), Active Directory is a centralized and standardized system that automates network management of user data, security, and distributed resources.

3. MS Active Directory

- It also enables interoperation with other directories.
- Active Directory is designed especially for distributed networking environments.
- Active Directory uses a peer approach to domain controllers; all domain controllers are full participants at all times.
- Active Directory is built on a structure that allows “trees of trees,” which is called a ***forest***.

3. MS Active Directory

- **Features of Active Directory**
- Support for the X.500 standard for global directories.
- The capability for secure extension of network operations to the Web.
- A hierarchical organization that provides a single point of access for system administration (for example management of user accounts, clients, servers, and applications) to reduce redundancy and errors.
- An object-oriented storage organization, which allows easier access to information.
- Support for the Lightweight Directory Access Protocol (LDAP) to enable inter-directory operability.
- Designed to be both backward compatible and forward compatible.

4. X.500 DIRECTORY ACCESS PROTOCOL

- The X.500 directory service is a global directory service.
- Its components cooperate to manage information about objects such a countries, organizations, people, machines, and so on in a worldwide scope.
- It provides the capability to look up information by name and to browse and search for information.
- The information is held in a directory information base (DIB). Entries in the DIB are arranged in a tree structure called the directory information tree (DIT).
- Each entry is a named object and consists of a set of attributes.
- Each attribute has a defined attribute type and one or more values.
- The directory schema defines the mandatory and optional attributes for each class of object (called the object class).
- The X.500 namespace is hierarchical. An entry is unambiguously identified by a distinguished name (DN).

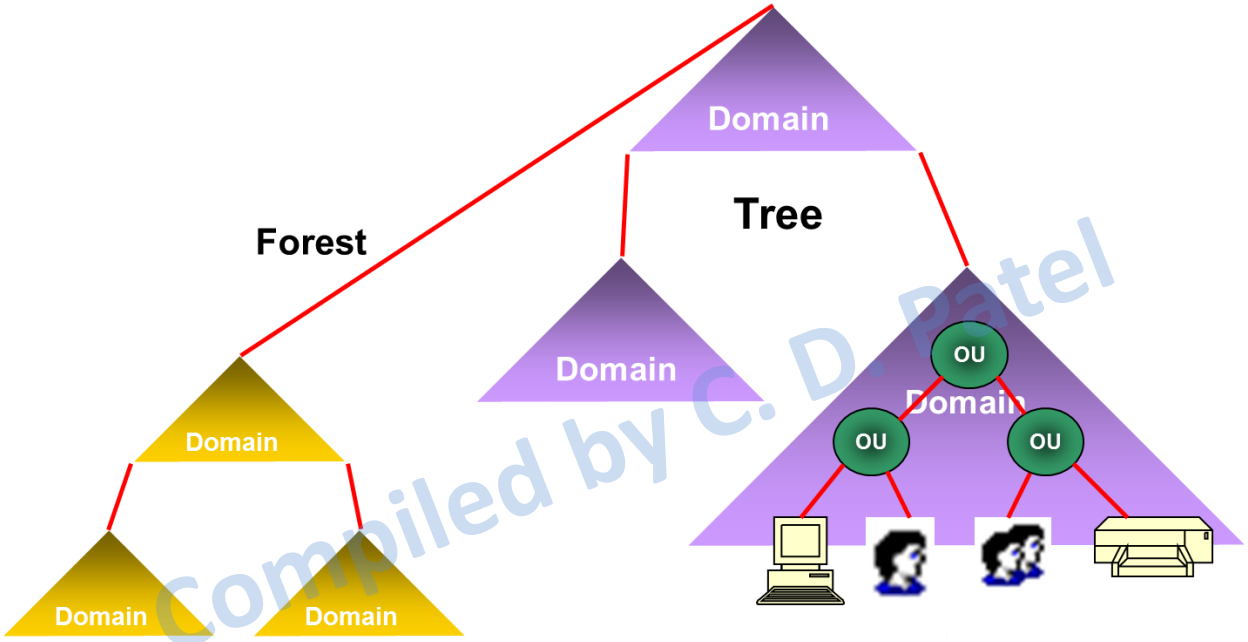
4. X.500 DIRECTORY ACCESS PROTOCOL

- A distinguished name is the concatenation of selected attributes from each entry, called the relative distinguished name (RDN), in the tree along a path leading from the root down to the named entry.
- Users of the X.500 directory may (subject to access control) modify the entries and attributes in the DIB.
- The X.500 directory tree starts with a root, just like the other directory trees, and
- then breaks down into country (C), organization (O), organizational unit (OU), and common name (CN) fields.
- To specify an X.500 address fully, you provide five fields, as in the following:
- CN=user name, OU=department, OU=division, O=organization, C=country
- For example, you might configure the fields as follows:
- **CN=Prashant Viradiya, OU=Networking Books, OU= NMA Books, O=GTP Publication, C=India**

5. LDAP - Lightweight Directory Access Protocol (May-2015)

- LDAP a subset of X.500 was introduced to address the complexity problems involved with full X.500 DAP.
- LDAP provides 90 percent of the power of X.500, but at only 10 percent of the processing cost.
- LDAP runs over TCP/IP and uses a client/server model.
- Its organization is much the same as that of X.500, but with fewer fields and fewer functions.
- LDAP is a set of protocols for accessing information directories.
- Because it's a simpler version of X.500, LDAP is sometimes called X.500-lite.
- LDAP provides a common language that client applications and servers use to communicate with one another.
- LDAP-based applications can easily search, add, delete and modify directory entries.

5. Domain, Tree and Forest
(May-2015, Dec- 2015)



5. Domain, Tree and Forest
(May-2015, Dec- 2015)

- **Domain**
- Domain is base element or building block of Active Directory.
- Active Directory is made up of one or more domain so domains are fundamental units of AD.
- A domain is defined as a logical group of network objects (computers, users, devices) that share the same Active Directory database.
- Domain is a sub-network comprised of a group of clients and servers under the control of one security database.
- Dividing LANs into domains improves performance and security.
- Here all resources are under the control of a single computer system.
- Domains are Physically Implemented on Domain Controllers (DC).
- **Microsoft.com**
- Domains provide border for Replication Traffic
- System Policies
- Administration

5. Domain, Tree and Forest
(May-2015, Dec- 2015)

- A tree is a group of domains that have the same DNS name; for example, abc.com (the top domain), sales.abc.com and support.abc.com (the child domains).

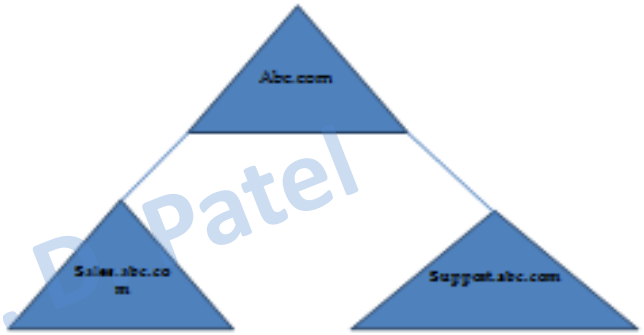


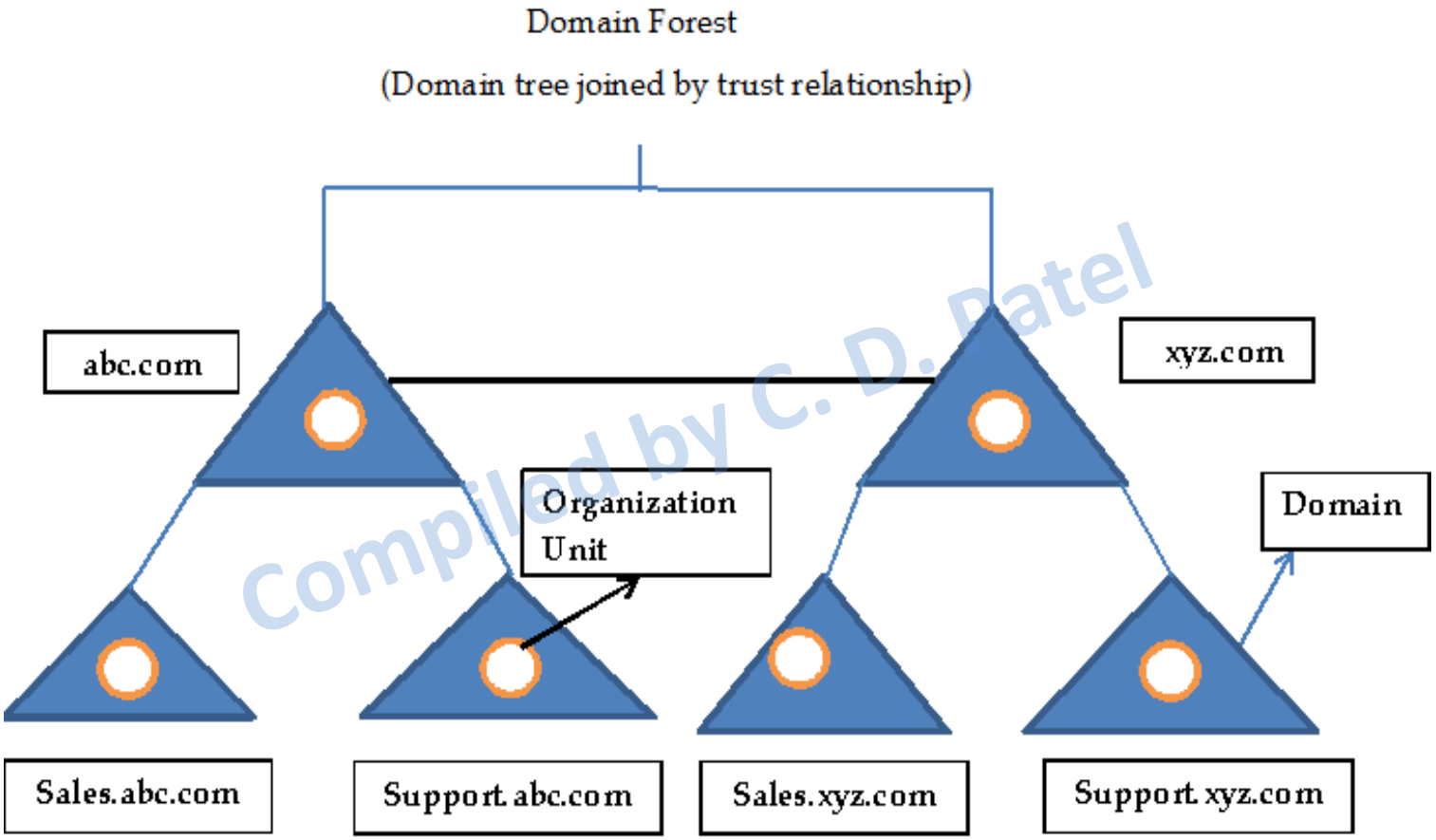
Fig.6 Tree

- An Active Directory tree is a collection of domains within a Microsoft Active Directory network.
- The term refers to the fact that each domain has exactly one parent, leading to a hierarchical tree structure.
- A tree may consist of a single domain or multiple domains.
- A domain added to a tree becomes a child of the tree root domain.
- The domain to which a child domain is attached is called a parent domain.

5. Domain, Tree and Forest
(May-2015, Dec- 2015)

- A group of Active Directory trees is known as a forest.
- A forest is a collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration.
- Forest is a collection of trees, which can be treated as one administrative unit by the user designated as Enterprise Administrator (EA), 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.

5. Domain, Tree and Forest
(May-2015, Dec- 2015)



1.2 Active Directory Architecture

We can break down the architecture of Active Directory services into several primary architectural components as described below.

- Objects
- Attributes
- Schema

1.2 Active Directory Architecture

- **Objects**
- Active Directory objects are the entities that make up a network.
- Here objects represent the various resources on a network, such as users, user groups, servers, printers, and applications.
- An object is a collection of attributes that defines the resource, and then it gives a name, list its capabilities and it also specify who should be permitted to use it.

1.2 Active Directory Architecture

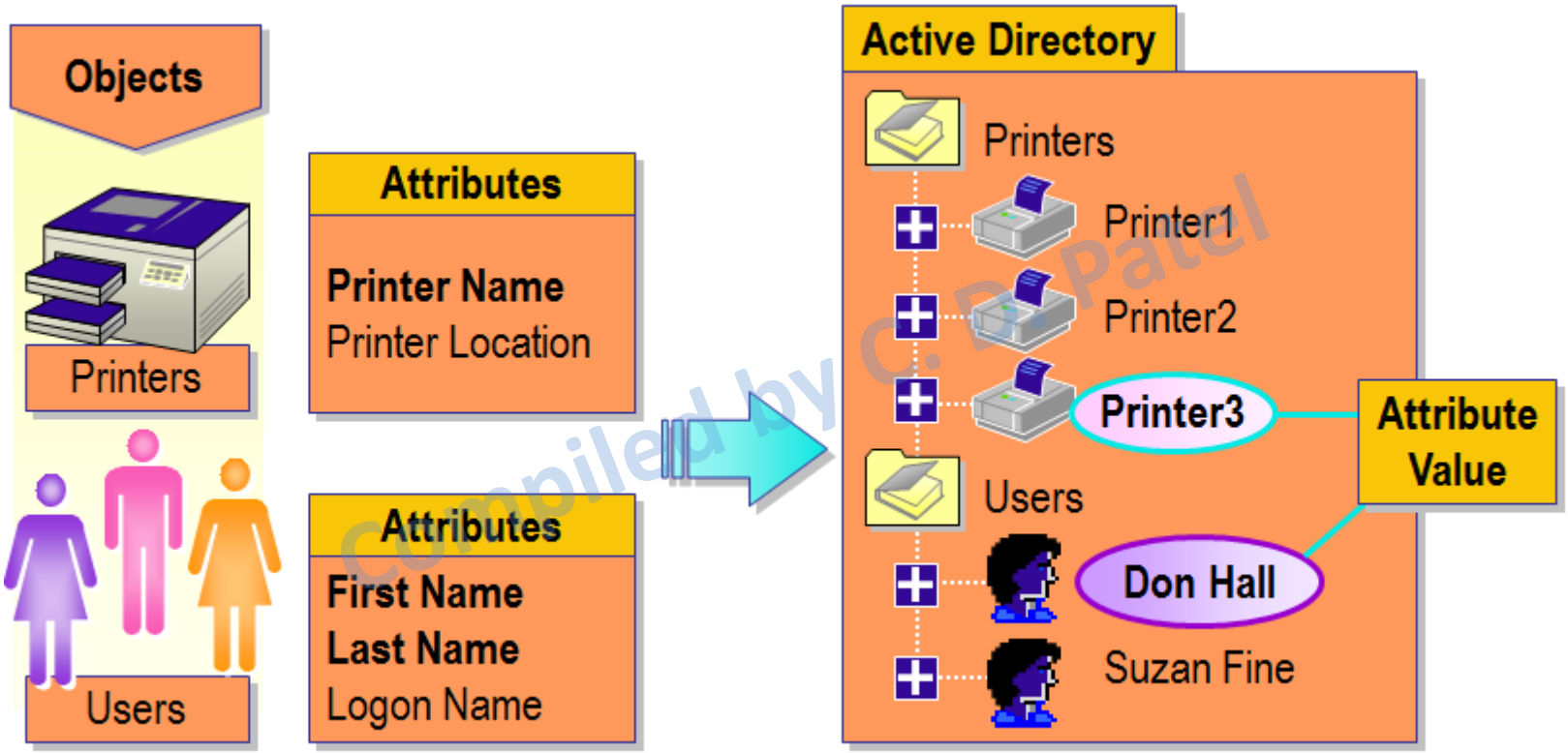


Fig. 1 Active Directory Objects

1.2 Active Directory Architecture

- **Attributes**
- An attributes describes an object means it stores information about an objects.
- For Example, name and passwords are example of user objects.
- Here different objects will have a different set of attributes that define them.
- But different objects may also share their attributes.
- For Example, a printer and Windows 2000 Professional Workstation may both have an IP address as an attribute.
- **Schema**
- Active Directory Schema defines what are the types of objects that can be created in the directory.
- It also defines how those objects are related to one another, and what the mandatory and optional attributes of each object are.

1.2.1 Object Types

- **1.2.1 Object Types**
- In Active Directory, There are two types of objects as listed below
- Container Objects
- Leaf Objects

1.2.1 Object Types

1. Container Objects

- The term "container" refers to one of two things:
- An object of the container structural class.
- An object that has child objects.
- For example, an organizational unit is a container object, although its class is organizational Unit, not container.
- A container object is simply an object that stores other objects.

1.2.1 Object Types

2. Leaf Objects

- A leaf object is an object that has no child objects.
- Leaf objects are objects such as
- Users and
- Computers which cannot contain other objects.
- So a leaf object stands alone and cannot store other objects.

1.2.2 Object Naming

- Every object in the active directory database is uniquely identified by a name that can be expressed in several forms.
- So Active Directory uses the Lightweight Directory Access Protocol (LDAP) to supply the naming convention for objects.
- There are two basic concepts available that are
- 1)Distinguished Names(DN) and
- 2)Common Names.
- Distinguished Names are the complete "path" through the hierarchical tree structure to a specific object.

1.2.2 Object Naming

- The following are the components that make up a Distinguished Name:
- **OU - Organizational Unit.**
- This attribute is used to divide a namespace based on organizational structure.
- An OU usually is associated with an Active Directory container or folder.
- **DC - Domain Component.**
- A distinguished name that uses DC attributes will have one DC for every domain level below root.
- Another way of thinking of this would be that there would be a DC attribute for every item separated by a dot in the domain name.
- **CN - Common Name.**
- This attribute represents the object itself within the directory service.
- Here is an example of a distinguished name:
  CN=Chirag Patel, CN=Users, DC=KDPPatan,DC=COM

1.2.3 Canonical Names

- Most Active Directory Applications refer to objects by using their canonical names.
- A Canonical Name is a 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 the object's RDN.
- **Example:**
- **KDPPatan.com/Computer Department/Staff/Chirag Patel**
- In this example, **Chirag Patel** is a user object in the **Staff** container, which is in **the Computer Department** container, which is in the **KDPPatan.com** domain.
- A canonical name is the properly denoted host name of a computer or network server.

1.2.4 LDAP Notation (Dec-2015)

- The same DN can also be expressed in LDAP notation, which would looks like as below:
- **CN=** Chirag Patel, **OU=**Staff, **OU =** Computer Department, **DC=** KDPPatan, **DC=** com
- It is also possible to express an LDAP name in a URL format, as defined in RFC 1959, which looks like as below:
- LDAP: //KDPPatan.com/cn= Chirag Patel, ou = Staff, ou = Computer Department, dc = KDPPatan, dc = com
- This notation enables users to access Active Directory information using a standard web browser.

1.2.5 Globally Unique Identifiers

- Active Directory uses GUIDs internally to identify objects.
- For example, the GUID is one of an object's properties that are published in the global catalog.
- It is a 128-bit numbers assigned by the Directory System Agent when the object is created.
- It is used to identify a particular component, application, file, database entry, and/or user.
- For instance, a website may generate a GUID and assign it to a user's browser to record and track the session.
- The GUID cannot be altered or removed.
- It is stored in an attribute, objectGUID, which is a required attribute for every object.

1.2.6 User Principle Names (UPN)

- Distinguished names are used by applications and services when they communicate with Active Directory, but they are not easy for user to understand, type or remember.
- So in Active Directory each user object has a User Principal Name (UPN).
- Format of UPN is as below
- **<User>@ <DNS-domain-name>**
- This has the same format as your email address:
- Like chirag.patel@gmail.com
- If you have a user named Chirag under Active Directory domain Domain01.local, the UPN will be Chirag@Domain01.Local
- In AD you can create custom UPNs too, which means you can also add Chirag@Domain01.com or Chirag@xyz.com as UPN for above mentioned object.
- The UPN is independent of the user object's DN, so a user object can be moved or renamed without affecting the user login name.

1.2.7 Domain, Forest and Tree

- **Domain** is base element or building block of Active Directory.
- Active Directory is made up of one or more domain so domains are fundamental units of AD.
- A domain is defined as a logical group of network objects (computers, users, devices) that share the same Active Directory database.
- Domain is a sub-network comprised of a group of clients and servers under the control of one security database.
- Dividing LANs into domains improves performance and security.
- Here all resources are under the control of a single computer system.
- Domains are Physically Implemented on Domain Controllers (DC).

1.3 Remote Network Access

- **Definitions**
- Remote access is the ability to get access to a computer or a network from a remote distance.
- **For instance:**
- Allowing staff to log in to your customer database from home.
- Setting up a project workspace where clients can share and view files.
- Allowing employees to send and receive email from any computer.
- **Remote Network Access** involves setting up a virtual private network (VPN) connection between the remote computer using VPN client software and a special gateway router that allows access to the university network over the Internet.
- This requires a high-speed connection to the Internet via an Internet Service Provider.
- Access is granted to users by login, using an account name and password combination.

1.3.1 Need of Remote Network

- Before implementing any remote access system, you must define clearly the types of remote access required by the users in the company.
- The following are some examples of remote access needs:
- Easy remote access to e-mail and to files stored in e-mail
- It is required to stored private or shared files on the LAN.
- Remote access to a centralized application, such as an accounting system or a sales order system
- Remote access to groupware programs or custom applications
- Internet access
- Intranet/extranet access, including any hosted web-based applications on those systems
- Remote access to any of the previous features from a fixed location, such as a remote sales office
- Home users get access to the Internet through remote access to an Internet service provider

1.3.2 PSTN

- **What Does PSTN Stand For?**
- PSTN stands for Public Switched Telephone Network. This network is also referred to as the Plain Old Telephone Service (POTS).
- Before the PSTN, two telephones needed to be connected over a copper wire in order to make a phone call. Because of the small number of connections, very few people could actually call each other.
- Soon enough, there was a demand for the PSTN. A copper wire connected individual landline telephones to a local telephone exchange, creating the PSTN.
- When two telephones are connected, analog voice data is transmitted over the copper wires of the PSTN.
- The voice data is then converted into electrical signals which are eventually routed in the switching centers. Finally, a connection is made and communication is possible.

1.3.2 PSTN

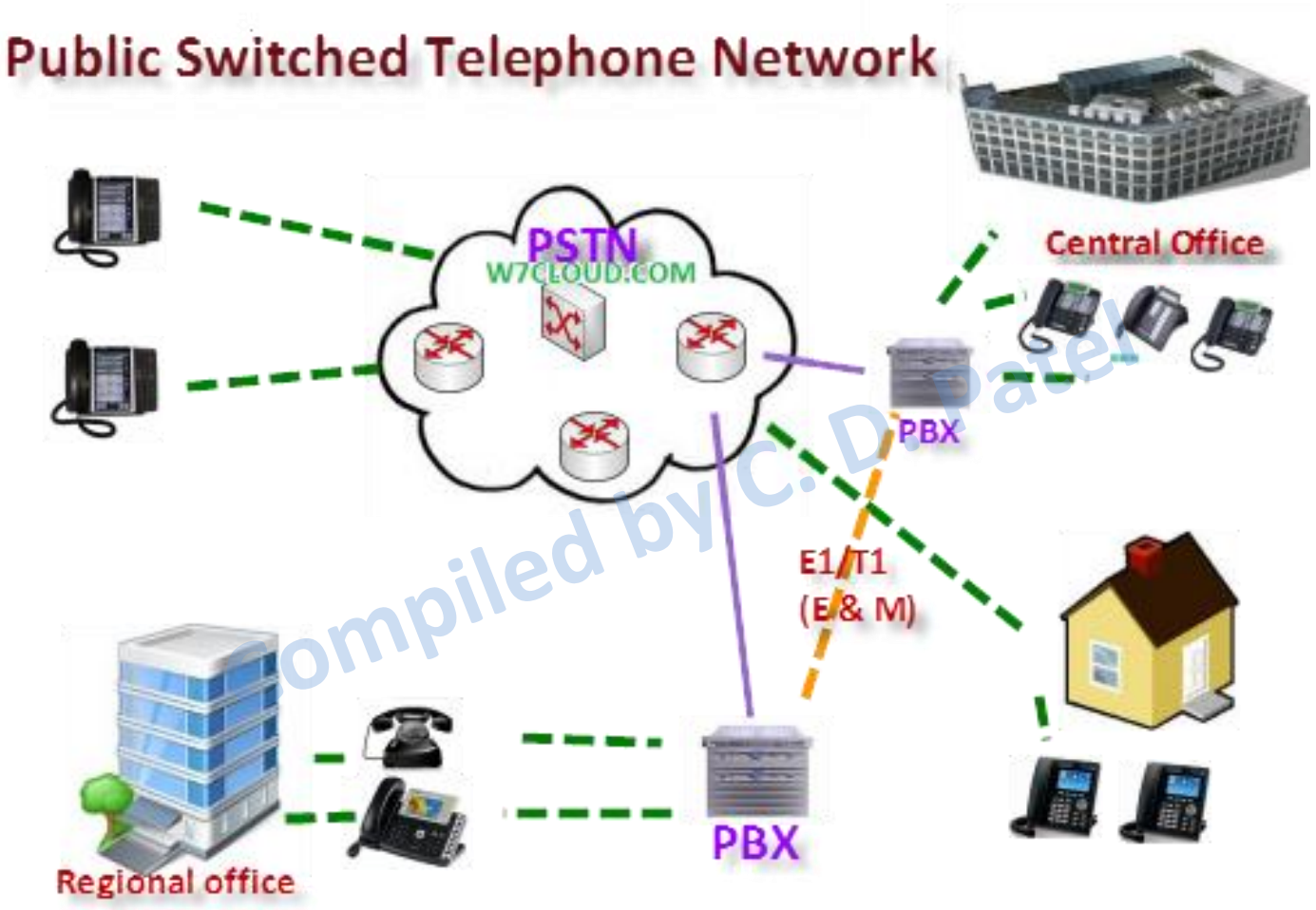
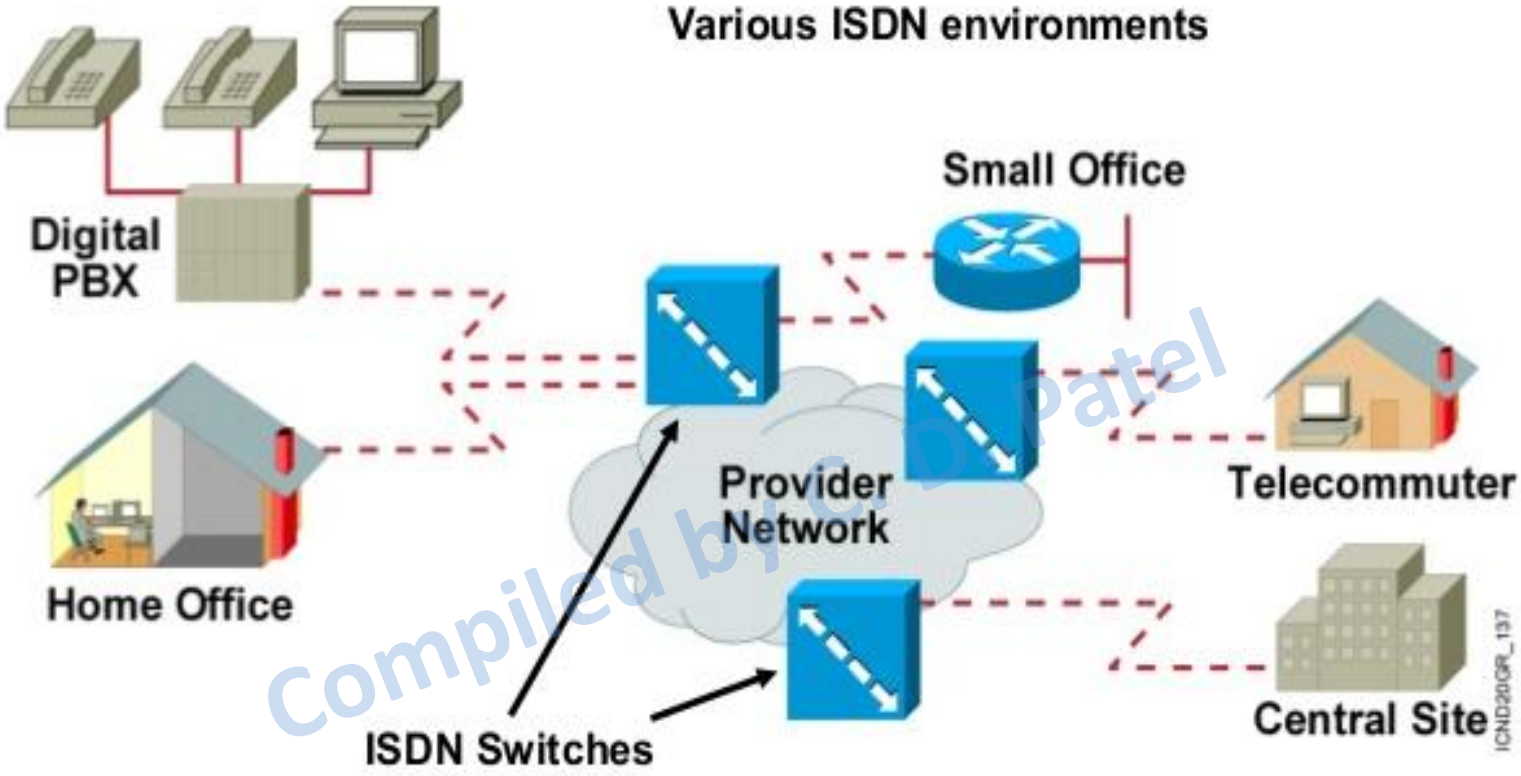


Fig. PSTN

1.3.3 ISDN

- In telecommunications technology, the abbreviation ISDN stands for the technical term "**Integrated Services Digital Network**" and refers to a digital standard for telephone networks.
- ISDN is an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires.
- ISDN supports data transfer rates of 64 Kbps (64,000 bits per second).
- There are two types of ISDN:
  - **Basic Rate Interface (BRI)** -- consists of two 64-Kbps B-channels and one D-channel for transmitting control information.
  - **Primary Rate Interface (PRI)** -- consists of 23 B-channels and one D-channel (U.S.) or 30 B-channels and one D-channel (Europe).
- The original version of ISDN employs baseband transmission.
- Another version, called B-ISDN, uses broadband transmission and is able to support transmission rates of 1.5 Mbps.
- B-ISDN requires fiber optic cables and is not widely available.

1.3.3 ISDN



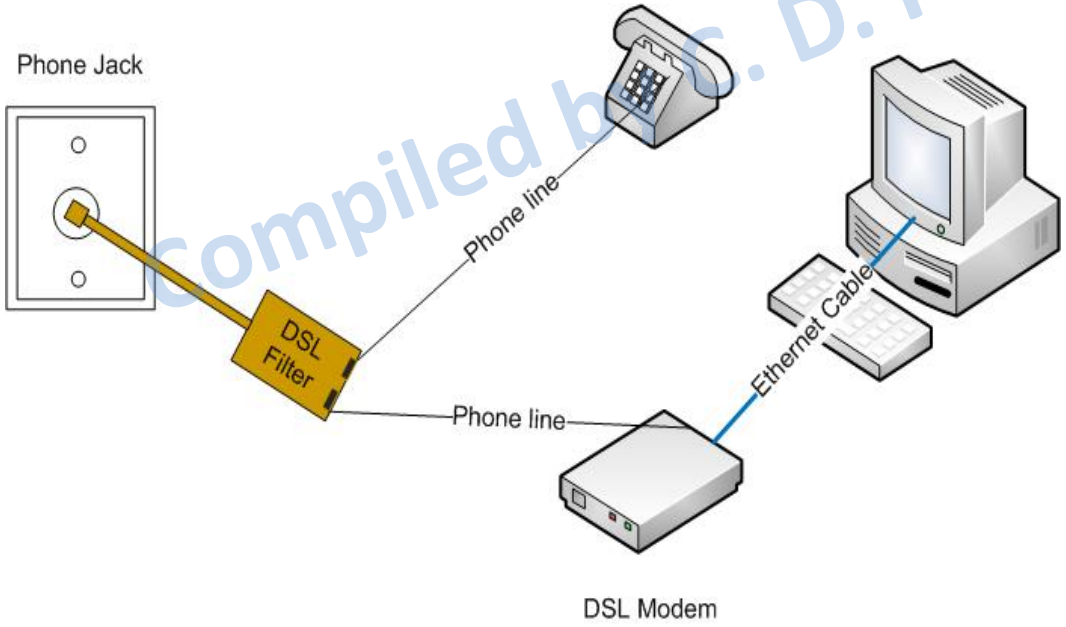
- Voice, data, video, and special services

PBX = Private Branch Exchange

Fig. ISDN

1.3.4 DSL (Dec- 2015)

- Consider DSL Internet, a **Digital Subscriber Line**, the big brother to dial-up. DSL uses telephone wires to send information. DSL providers provide Internet access without special wires and cables**.**



1.3.4 DSL (Dec- 2015)

- **Advantages of DSL:**
- You can leave your Internet connection open and still use the phone line for voice calls.
- The speed is much higher than a regular modem
- DSL doesn't necessarily require new wiring; it can use the phone line you already have.
- The company that offers DSL will usually provide the modem as part of the installation.

1.3.4 DSL (Dec- 2015)

- **Disadvantages:**
- A DSL connection works better when you are closer to the provider's central office. The farther away you get from the central office, the weaker the signal becomes.
- The connection is faster for receiving data than it is for sending data over the Internet. The service is not available everywhere.

1.3.5 CATV (Dec-2015)

- **Definition:**
- *CATV* is a shorthand term for **Cable Television Service**. Many providers offer cable Internet service together with television to their customers over the same CATV links.
- **Community Antenna Television**: a cable television system that receives television broadcasts by antenna and relays them by cable to paying subscribers in areas where direct reception is either poor or not possible.
- Cable television - CATV is a broadcast distribution system that uses a network of cables to deliver multiple types of media services
- **CATV Connectors**
- To hook up a television to CATV service, a coaxial cable must typically be plugged into the TV. The same type of cable is used to connect a cable modem to Internet service. These cables use a standard "F" style connector often called a CATV connector, although these are same connectors that were commonly used with analog TV setups over the past few decades.

1.3.5 CATV (Dec-2015)

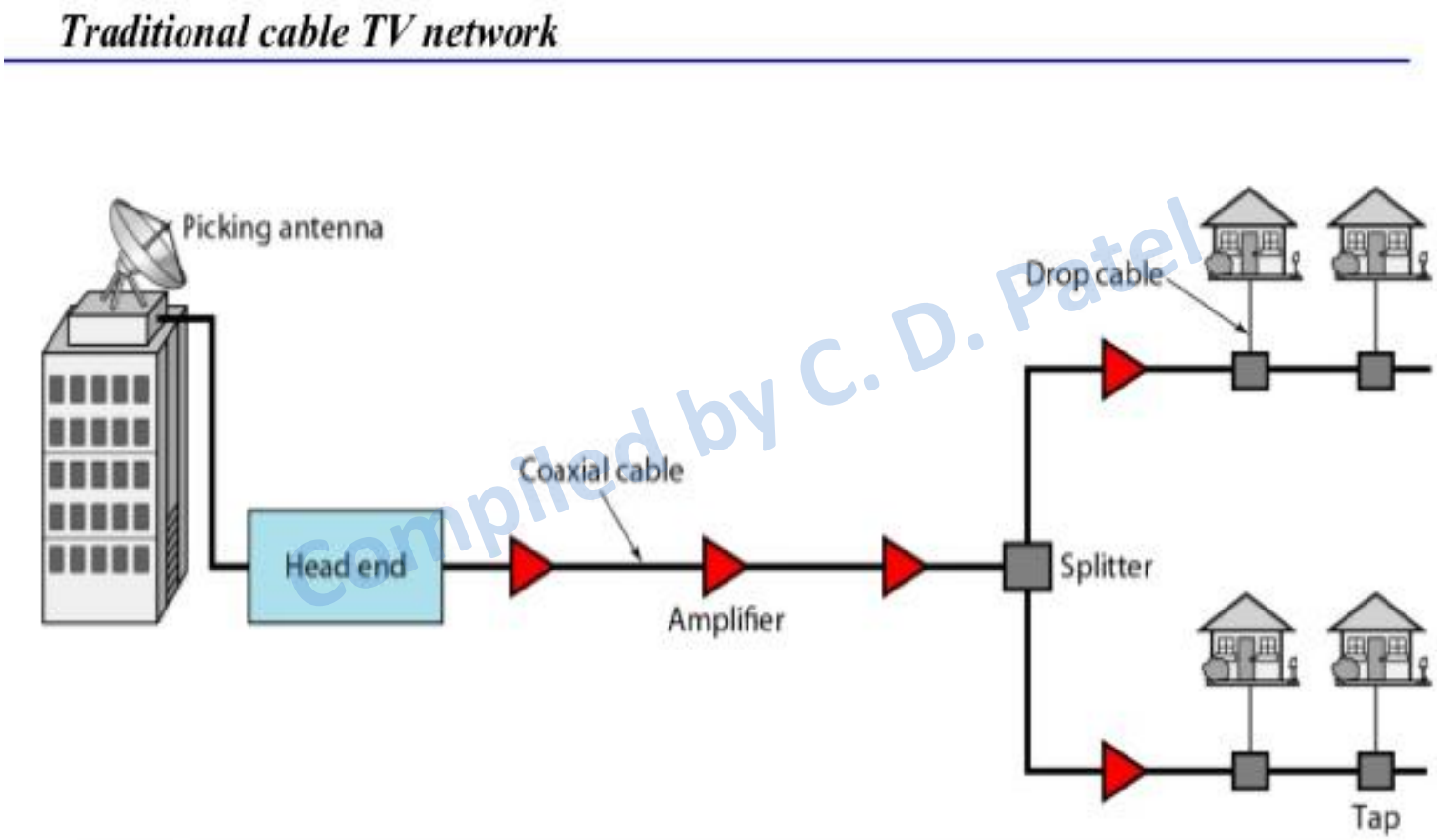


Fig. Traditional cable TV network

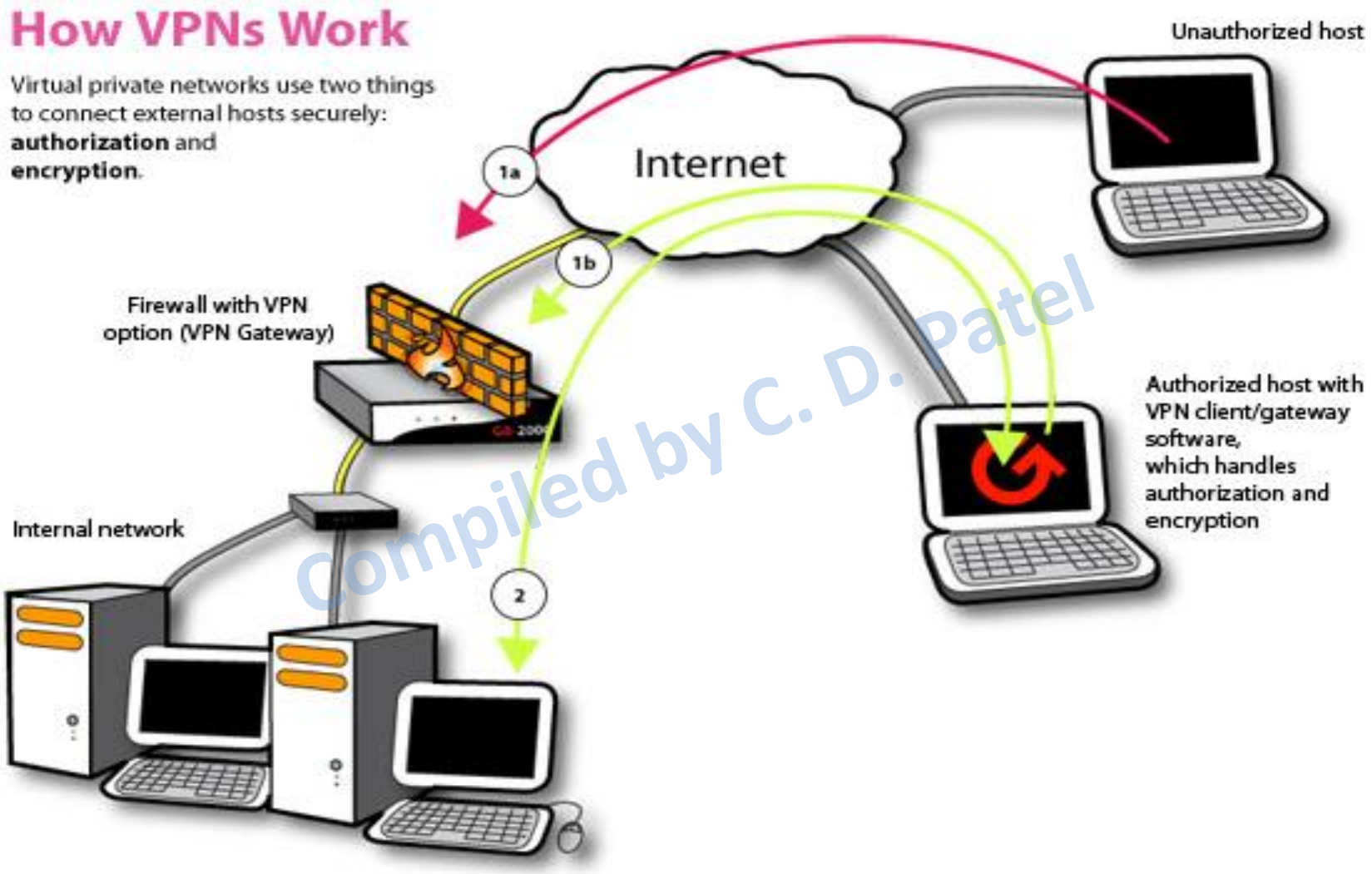
1.4 Virtual Private Network (Dec-2015)

- **Virtual**
- Virtual means not real or in a different state of being.
- In a VPN, private communication between two or more devices is achieved through a public network the Internet.
- Therefore, the communication is virtually but not physically there.
- **Private**
- Private means to keep something secret from the general public.
- Although those two devices are communicating with each other in a public environment, there is no third party who can interrupt this communication or receive any data that is exchanged between them.
- **Network**
- A network consists of two or more devices that can freely and electronically communicate with each other via cables and wire.

1.4 Virtual Private Network (Dec-2015)

- **What is a VPN?**
- 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.
- A VPN can connect multiple sites over a large distance just like a Wide Area Network (WAN).
- The VPN uses strong encryption and restricted, private data access which keeps the data secure from the other users of the underlying network.
- The underlying network could often be a public network like the Internet.

1.4 Virtual Private Network (Dec-2015)



1.4.1 VPN Protocol (May-2015, Dec-2015)

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

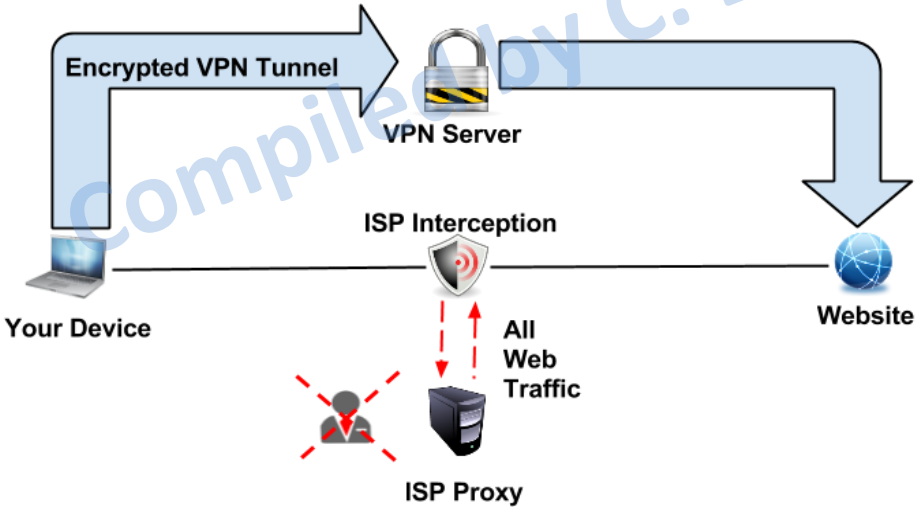


Fig. Working of VPN Protocols

Point-To-Point Tunneling Protocol (PPTP)

- It enable authorized remote users to connect to the VPN network using their existing Internet connection and then log on to the VPN using password authentication.
- They don’t need extra hardware and the features are often available as inexpensive add-on software.
- **Advantages**
- Easy to setup.
- Virtually supported on every device with VPN support.
- Low overhead and thus good speeds.
- **Disadvantages**
- Low encryption at 128 bit.
- Relatively unstable. you might know that sometimes it does take more than once to connect. And connections might drop randomly.
- Relatively easy to block by ISPs.

L2TP/IPSEC

- L2TP or Layer 2 Tunneling Protocol does not do any encryption by itself.
- It simply does provide the routing tunnel.
- VPN providers generally use IPsec for encryption.
- L2TP is a protocol used to tunnel data communications traffic between two sites over the Internet.
- L2TP is often used in tandem with IPSec to secure the transfer of L2TP data packets over the Internet.
- Unlike PPTP, a VPN implementation using L2TP/IPSec requires a shared key or the use of certificates.

L2TP/IPSEC

- **Advantages**
- Supported on most modern devices.
- Encryption at 256bit.
- Easy to setup on MAC and Windows as it is natively supported.
- No known major vulnerabilities.
- **Disadvantages**
- Higher encryption means more CPU, but in general that is not a bigger issue for modern devices.
- Most challenging to configure on a Linux server.
- Higher encryption with double encapsulation results in B/W hit. How much depends on your device and the VPN Server/Provider.
- Relatively easy to block by ISP.
- Slower than OpenVPN
- May be compromised by the NSA

OPENVPN

- OpenVPN is a fairly new open source application with a custom encryption protocol based on SSL/TLS key exchanges.
- It is used to provide a strong and reliable VPN solution.
- **Advantages**
- Supports hardware acceleration with improves speeds.
- Highly configurable
- Very secure (probably even against the NSA)
- Can bypass firewalls
- Can use a wide range of encryption algorithms
- **Disadvantages**
- It needs third party software.
- It can be fiddly to set up.
- Support on mobile devices is improving, but is not as good as on the desktop.

SSTP

- **SSTP stands for** Secure Socket Tunneling Protocol.
- It uses TLS 3.0 over TCP port 443 “HTTPS” at the time of writing.
- This makes it secure and hard to block.
- It uses cryptography to secure communications over the Internet.
- To successfully initiate a connection, an authentication process involving certificates is used.
- Certificates are cryptographic keys that are stored on both the server and client.

SSTP

- **Advantages**
- High Encryption.
- Very secure (depends on cipher, but usually very strong AES)
- Completely integrated into Windows (Windows Vista SP1, Windows 7, Windows 8)
- Microsoft support
- Can bypass most firewalls
- **Disadvantages**
- Not supported by all VPN Providers.
- A Microsoft proprietary protocol, not available for public inspection. Microsoft is known for its security issues and cooperation with various government agencies.
- Limited support for Non-MSDevices.

1.4.2 Types of VPN

- **Remote-access VPNs**
- A remote-access VPN allows individual users to establish secure connections with a remote computer network. Those users can access the secure resources on that network as if they were directly plugged in to the network's servers.
- There are two components required in a remote-access VPN. The first is a **network access server** (NAS, usually pronounced "nazz" conversationally), also called a media gateway or a remote-access server (RAS). A NAS might be a dedicated server, or it might be one of multiple software applications running on a shared server.
- The other required component of remote-access VPNs is **client software**. In other words, employees who want to use the VPN from their computers require software on those computers that can establish and maintain a connection to the VPN.

1. Remote-access VPNs

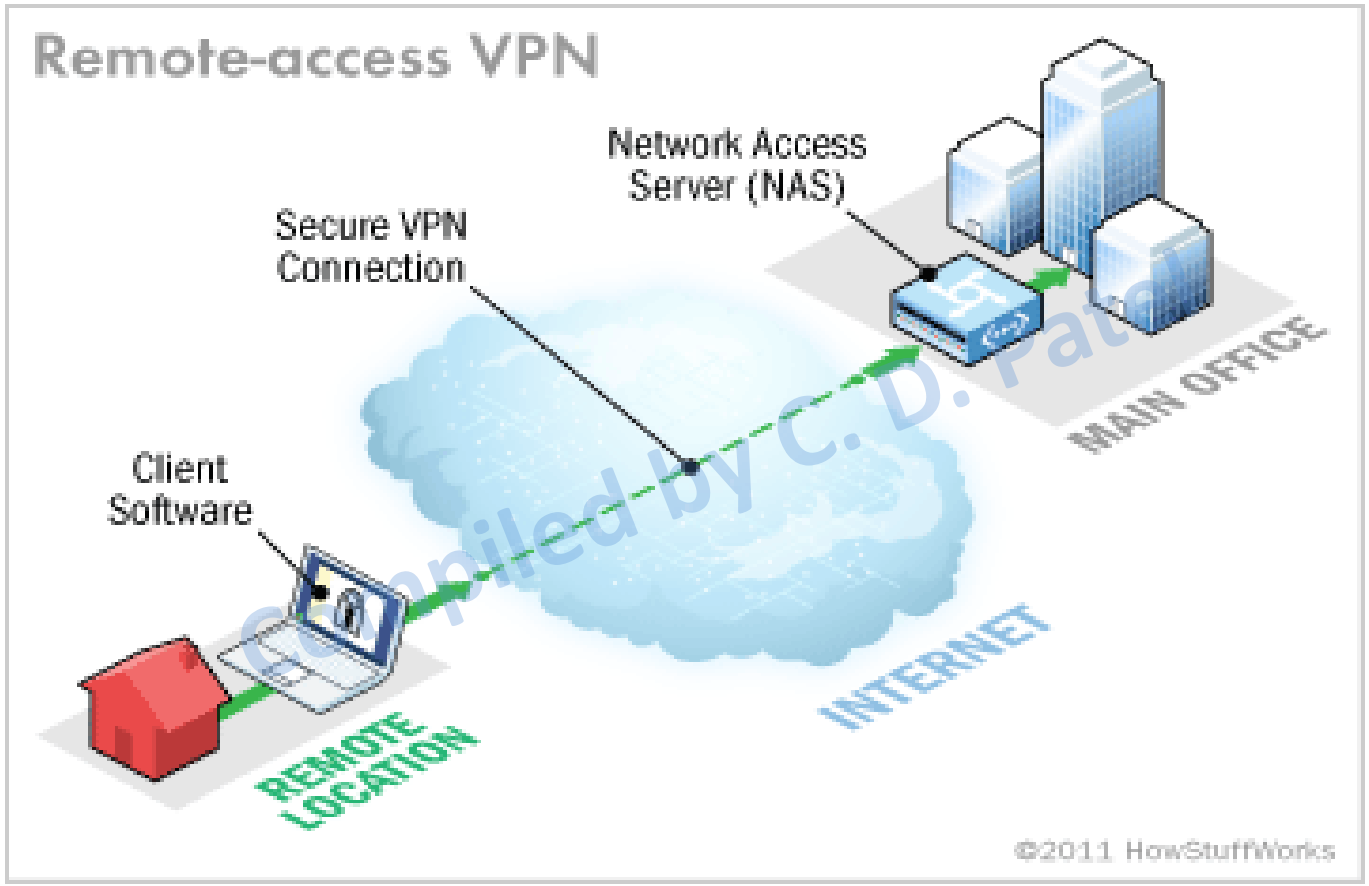


Fig. Remote-access VPN

2. Site-to-site VPNs

- A site-to-site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations. An example of a company that needs a site-to-site VPN is a growing corporation with dozens of branch offices around the world.

2. Site-to-site VPNs

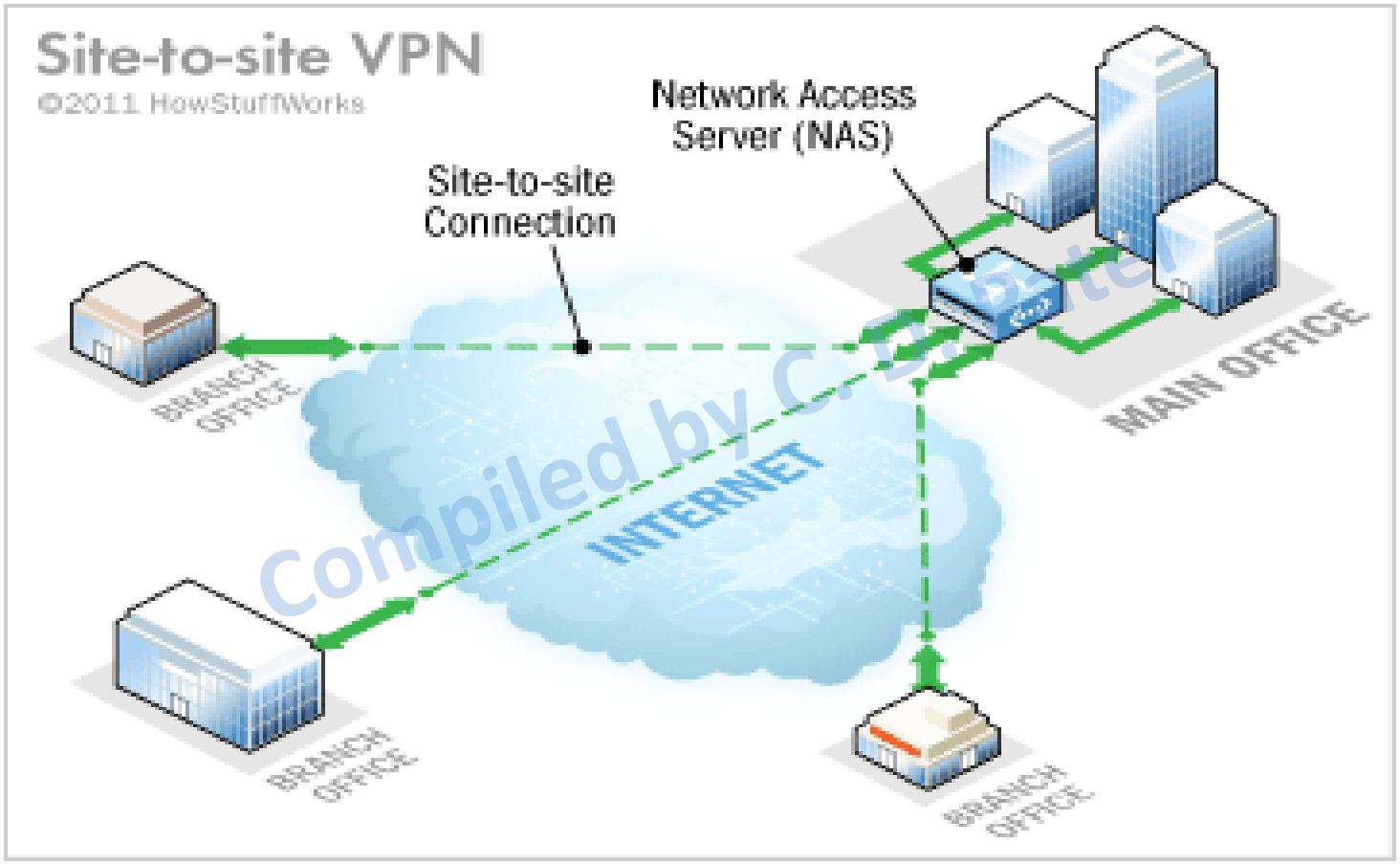


Fig. Site-to-site VPN

1.4.3 VPN Clients

- A VPN client on one computer connects to a VPN server on another computer by using encryption and other security measures, so no one can see which type of information is being exchanged.
- The different types of VPN Client available in market are as below:
  - Cisco VPN Client
  - SSL VPN Client
  - IPSec VPN Client
  - Open VPN Client
- The Cisco Systems VPN Client was a software application for connecting to a virtual private network

1.4.4 SSL VPN

- A Secure Sockets Layer Virtual Private Network (SSL VPN) is a kind of VPN that runs on Secure Socket Layers technology and is accessible via https over web browsers.
- It permits users to establish safe and secure remote access sessions virtually
- from any Internet connected browser.
- Before a connection is established traditional VPN requires the installation of IPSec client software on a client machine whereas SSL VPN has no such requirement.
- Users are able to access confidential applications or shared files on standard web browsers.
- The main benefit of SSL VPN technology is that because it is user-based, not device-based, any authorized user can login from web-enabled PCs for secure, remote access of confidential files.

Questions Asked In GTU

- **May-2015 (Regular)**
- **2 Marks Questions**
- Define Tree
- Define Forest.
- **3 or 4 MARKS Questions**
- Explain Directory Service
- Explain Light Weight Directory Access Protocol.
- List Virtual Private Network Protocol. Explain any One Protocol
- Explain X.500 directory access protocol.

Questions Asked In GTU

- **Dec-2015 (Remedial)**
- **2 Marks Questions**
- Explain X.500 – directory access protocol
- Write a full form of PSTN, ISDN, VPN & DHCP
- Explain LDAP notation
- Define forest, tree, and root
- **3 or 4 MARKS Questions**
- Explain DSL in detail
- Explain CATV Architecture
- Explain VPN in detail
- List out VPN protocol and explain any one protocol