**NETWORK DESIGN PROPOSAL FOR INTERNET CAFÉ**

**TEAM 9**

RA1811027010012 – Anurag Nimonkar

RA1811027010013 – Nivetha Jayakumar

RA1811027010023 – Sahil Rao

RA1811027010034 – Tamojit Sarkar

**ABSTRACT**

This project presents a design and prototype implementation of a cybercafé to support 30 users who all share the same ADSL network, where the access to certain sites(servers) are blocked with the help of a firewall. The café has a printing facility too. A wireless network (ADSL connection) has to be designed that gives users access to certain sites. There are 31 Client computers and a printer to print the files. Three servers are used in the ADSL side to show the working of these computers. The DNS server, the server for Google and YouTube. The IP for YouTube is blocked with the help of a firewall. All 30 PCs are configured to share the same network. A billing software like True café will be installed in all PCs. A common cloud storage will also be used for users to download and print files. This common shared storage avoids cluttering of the PCs’ local storage with unnecessary data and the need to manually clean them out after every use.

**NETWORK DESIGN REQUIREMENT**

To design a network for an internet café which has 30 users. The internet café has one ADSL which is to be shared among the users. Certain websites must be blocked on all computers in the café. A café billing management system must be configured and deployed in the café.

**PROBLEMS FACED**

* PHYSICAL

1. Cluster of wires- the WAN network of wires require a good amount of wiring, so it should be properly managed.
2. Printer Management- as there are only three printers, customers will have to wait to use them.
3. Speed- laying high quality wires (Optical Fiber) is necessary for a WAN network else the reception of data will be slowed down.
4. Complexity- the model is a bit complicated but efficient. Care should be taken while making the connections between various devices.

* TECHNICAL

1. Loss of internet access and packets
2. Lack of ability to print
3. Security of the PC and data associated
4. Common storage has to be cleaned out on a daily basis.
5. Billing software must be up to date and accurate.
6. Low or Insufficient bandwidth may result in slowed down results and functioning

**OBJECTIVES**

1. Proper and careful management of cluster of wires
2. Check proper functioning of all devices on a regular basis.
3. Use high quality materials to ensure the quality remains up to the mark
4. Use of firewall to ensure the security of the incoming and outgoing data
5. Using the most efficient layout of devices
6. Properly calibrated switches for the proper allocation of data

**DESIGN REQUIREMENT ANALYSIS**

The internet café is to support 30 users. So, 30 Desktop computers would be required. For the local network of computers, a switch would be required. Since 30 computers need to be networked, a switch with 30 ports would be required. Switches typically come with 24 ports or 48 ports. Since a 24-port switch would not suffice the requirement, a 48-port switch is recommended. But in our implementation, to make the design more efficient we use two switches each with 24 port, and 15 computers are connected to the first switch and 16 computers, and 3 printers to the second one.

An ADSL router which is capable of NAT (Network Address) is required. NAT is a mandatory feature which is required on the router, for sharing the ADSL internet connection.

Although not mandatory, a DHCP server is preferred for providing dynamic IP addresses to the users. The availability of the feature on the router rules out the need to setup and configure an additional DHCP server for this network

In our scenario, we use a firewall coupled with the DSL router-modem, with the configurations made directly within the former.

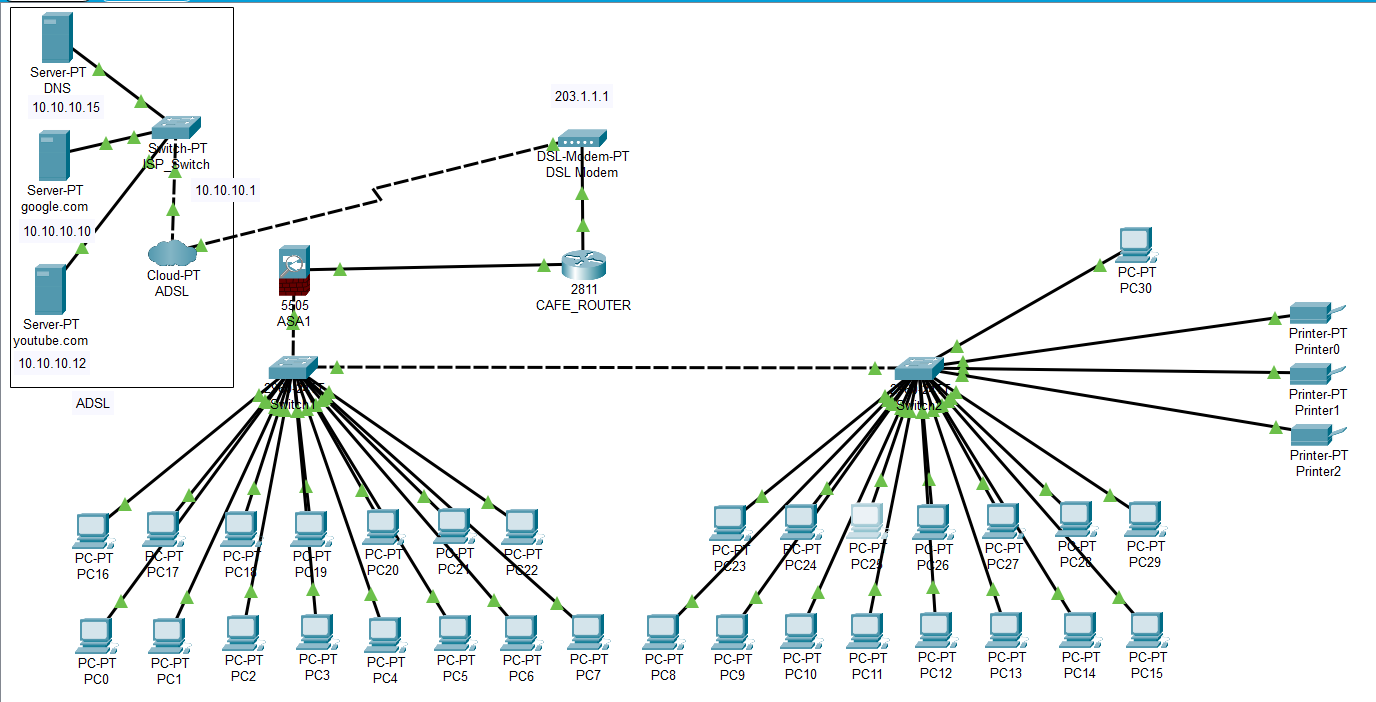
An ISP router is responsible for connecting all the PC’s to the internet.

Three servers are used in this implementation one server for the DNS, and the rest two being that of Google and YouTube, where the google server is accessible by all the 30 PC’s and the access of the site youtube.com is prohibited by the café’s guidelines.

As the users in the café needs to be managed with a billing system, additional software must be installed and configured on the appropriate operating system for which it is supported. Here we would use software like TrueCafe which is usually installed on the admin computer and rolled out to the other users.

**NETWORK DIAGRAM**

* The computers corresponding to the users connect to the ports on the switches. As Shown in the fig. above.
* The switches are 24 port switches each. The computer connects to the switch using Ethernet RJ 45 cables.
* The café management software is installed on the appropriate operating system and set up on the network.
* The firewall along with the ADSL router-modem is deployed as shown in the diagram. This has two interfaces. WAN interface of the router is connected to the internet and the LAN interface is switch.
* The ADSL router is configured for NAT. When the feature is enabled, internal users would be able to share the IP Address which would be available on the WAN interface of the router.
* The DHCP feature on the firewall is configured for NAT. When the right command is called, it would provide appropriate IP Address, subnet mask, default gateway and DNS server IP Addresses for the user’s computers.



**IP ADDRESS DESIGN**

* The internal private IP Address range for the users and other devices within the café is 192.168.1.2-36.
* The subnet masks of all the devices are the same – 255.255.255.0
* The IP Addresses of the LAN interface of the firewall and computer on which the café management system is setup should be configured with static IP Addresses (192.168.10.1) belonging to the 192.168.1.0/31.
* It should be ensured that the static IP Addresses provided for the LAN interface of the firewall and the café management system is excluded from the DHCP scope configured on the router for avoiding duplicate IP addressing.
* The default gateway and the DNS server which is to be provided in the DHCP scope would be the IP address of the LAN interface of the firewall.
* The default gateway for the three servers, i.e., the DNS server, Google server and YouTube server, is the same – 10.10.10.1
* The IP addresses and the ports used for making the connections are as follows:

DNS server – IP = 10.10.10.15

Default Gateway – 10.10.10.1

Port (server to switch) = Fast Ethernet 0 to Fast Ethernet 0/1 of the switch

DNS Service = ON

Resource Records = [www.google.com](http://www.google.com) (10.10.10.10)

[www.youtube.com](http://www.youtube.com) (10.10.10.12)

Google server – IP = 10.10.10.10

Default Gateway – 10.10.10.1

Port (server to switch) = Fast Ethernet 0 to Fast Ethernet 1/1 of the switch

HTTP Service – ON

HTTPS Service - ON

YouTube server – IP = 10.10.10.12

Default Gateway – 10.10.10.1

Port (server to switch) = Fast Ethernet 0 to Fast Ethernet 2/1 of the switch

HTTP Service – ON

HTTPS Service – ON

* The switch is connected to Ethernet 6 of the cloud via port Fast Ethernet 3/1 with the help of a Copper Cross-Over.
* The cloud is connected to modem 4 with the help of a Phone cable. The name of the modem and the port used for connection are added under DSL service of the cloud.
* The IP of the interface between the ADSL connection and the café modem is the default gateway used for the servers, i.e., 10.10.10.1
* The IP of the interface between the modem and the router of the café is the default gateway used earlier, i.e., 10.10.10.1. The port used is Fast Ethernet 0/0 of the router.
* The IP of the interface between the router and the firewall device is the default gateway of the router, i.e., 203.1.1.1. The port used is Fast Ethernet 0/1 of the router and Ethernet 0/0 of the firewall.
* Router configuration :

Router(config)#interface FastEthernet 0/0

Router(config-if)#ip address 203.1.1.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface FastEthernet 0/1

Router(config-if)#ip address 10.10.10.1 255.255.255.0

Router(config-if)#no shutdown

Router(config)#router ospf 1

Router(config-router)#network 203.1.1.0 0.0.0.255 area 0

Router(config-router)#network 10.10.10.0 0.0.0.255 area 0

* Cisco ASA 5505 configuration :

ciscoasa(config)#interface vlan 1

ciscoasa(config-if)#no ip address

ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.35 inside

ciscoasa(config)#interface vlan 1

ciscoasa(config-if)#ip address 192.168.10.1 255.255.255.0

ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#nameif inside

ciscoasa(config-if)#security-level 100

ciscoasa(config-if)#exit

ciscoasa(config)#interface vlan 2

ciscoasa(config-if)#ip address 203.1.1.2 255.255.255.0

ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#nameif outside

ciscoasa(config-if)#security-level 0

ciscoasa(config-if)#exit

ciscoasa(config)#interface ethernet 0/1

ciscoasa(config-if)#switchport access vlan 1

ciscoasa(config)#interface ethernet 0/0

ciscoasa(config-if)#switchport access vlan 2

ciscoasa(config-if)#exit

ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 203.1.1.1

ciscoasa(config)#object network LAN

ciscoasa(config-network-object)#subnet 192.168.10.0 255.255.255.0

ciscoasa(config-network-object)#nat (inside,outside) dynamic interface

ciscoasa(config-network-object)#exit

ciscoasa(config)#access-list al extended deny ip 10.10.10.12 0.0.0.255 any

ciscoasa(config)#access-list al extended permit tcp any any

ciscoasa(config)#access-list al extended permit icmp any any

ciscoasa(config)#access-group al in interface outside

* The firewall is connected to the first switch via port FastEthernet 0/17.
* The default gateways of all the 31 PCs and the printers is the IP used at the interface for the firewall, i.e, 192.168.10.1.
* All the PCs are connected to the switches via their port Fa0.
* The first switch is connected to the second via ports Fa0/1 and Fa0/18 of the first and second switch respectively.
* IP configurations of the PCs along with the port of the switch they are connected to :

PC0 :

IPv4 address = 192.168.10.36

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/3

PC1 :

IPv4 address = 192.168.10.5

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/5

PC2 :

IPv4 address = 192.168.10.10

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/7

PC3 :

IPv4 address = 192.168.10.9

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/9

PC4 :

IPv4 address = 192.168.10.11

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/11

PC5 :

IPv4 address = 192.168.10.13

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/13

PC6 :

IPv4 address = 192.168.10.15

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/15

PC7 :

IPv4 address = 192.168.10.16

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/16

PC8 :

IPv4 address = 192.168.10.18

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/1

PC9 :

IPv4 address = 192.168.10.20

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/3

PC10 :

IPv4 address = 192.168.10.22

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/5

PC11 :

IPv4 address = 192.168.10.24

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/12

PC12 :

IPv4 address = 192.168.10.26

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/13

PC13 :

IPv4 address = 192.168.10.28

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/14

PC14 :

IPv4 address = 192.168.10.30

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/15

PC15 :

IPv4 address = 192.168.10.32

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/16

PC16 :

IPv4 address = 192.168.10.17

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/2

PC17 :

IPv4 address = 192.168.10.4

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/4

PC18 :

IPv4 address = 192.168.10.6

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/6

PC19 :

IPv4 address = 192.168.10.8

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/8

PC20 :

IPv4 address = 192.168.10.10

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/13

PC21 :

IPv4 address = 192.168.10.12

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/12

PC22 :

IPv4 address = 192.168.10.14

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/14

PC23 :

IPv4 address = 192.168.10.19

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/2

PC24 :

IPv4 address = 192.168.10.21

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/4

PC25 :

IPv4 address = 192.168.10.23

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/6

PC26 :

IPv4 address = 192.168.10.25

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/13

PC27 :

IPv4 address = 192.168.10.27

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/15

PC28 :

IPv4 address = 192.168.10.29

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/9

PC29 :

IPv4 address = 192.168.10.31

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/10

PC30 :

IPv4 address = 192.168.10.33

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/11

Printer0 :

IPv4 address = 192.168.10.34

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/17

Printer1 :

IPv4 address = 192.168.10.35

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/19

Printer2 :

IPv4 address = 192.168.10.37

Subnet mask = 255.255.255.0

Default gateway = 192.168.10.1

DNS Server = 10.10.10.15

Port = Fa 0/20

**HARDWARE AND SOFTWARE**

* **Item**

1. ADSL and ISP Router
2. 3 Switches
3. 31 Client Computers
4. 3 Printers
5. 1 Firewall
6. 3 Servers
7. 1 Modem
8. 1 Cloud Service
9. 1 billing software (TrueCafe)

* **Specifications**

1. Router 2811(NM-ESW-161 port) and Router 1841



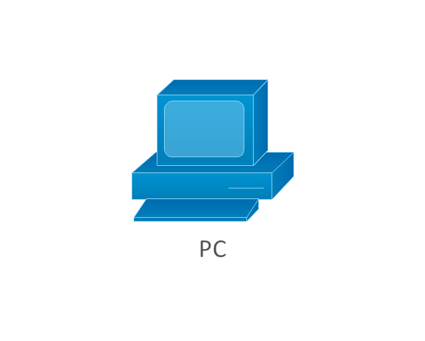
The Cisco 1841 router is designed for secure data connectivity and provides significant additional value compared to prior generations of Cisco 1700 Series routers by offering more than a fivefold performance increase and integrated hardware-based encryption enabled by an optional Cisco IOS ® Software security image. The Cisco 1841 dramatically increase interface card slot performance and density over the Cisco 1700 Series while maintaining support for more than 30 existing WAN interface cards (WICs) and multiflex trunk cards

1. 2960-24TT Switches



Cisco Catalyst 2960 Series Switches with LAN Lite software are fixed-configuration, standalone switches that provide desktop Fast Ethernet connectivity for entry-level wiring closet and small branch-office networks . These switches simplify the migration from non-intelligent hubs and unmanaged switches to a fully scalable managed network. Cisco Catalyst 2960 Series Switches have lower cost of ownership with features such as intelligent switch configuration using Auto Smart Ports, installation with Auto Install and enhanced troubleshooting to facilitate ease of use.

1. PC-PT Computers



A device that performs processes, calculations and operations based on instructions provided by a software or hardware program. It has the ability to accept data (input), process it, and then produce outputs.

1. Printer-PT



A Printer is a peripheral device which makes a persistent representation of graphics or text, usually on paper. While most output is human-readable, bar code printers are an example of an expanded use for printers.

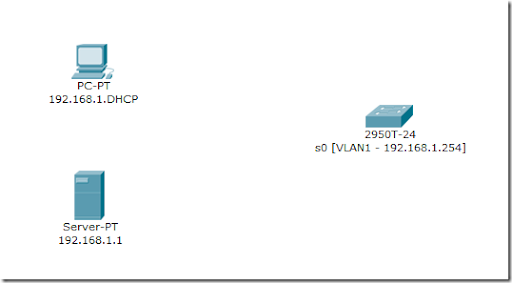
1. Cisco ASA 5505



Cisco ASA 5500 Series Adaptive Security Appliances are purpose-built solutions that integrate world-class firewall, unified communications security, VPN, intrusion prevention (IPS), and content security services in a unified platform.

The Cisco ASA 5500 Series provides intelligent threat defense that stops attacks before they penetrate the network perimeter, controls network and application activity, and delivers secure remote access and site-to-site connectivity. The result is a powerful multifunction network that provides security breadth, precision, and depth for protecting the café network, while reducing the overall deployment and operations costs associated with implementing comprehensive multilayer security.

1. Server-PT servers



Servers are an entirely different breed when compared to other end devices. They have various functionalities and also have space for two network interfaces. The modules available for servers are the same as PC modules, except that the servers do not have the PC-HOST-NM-1AM module.

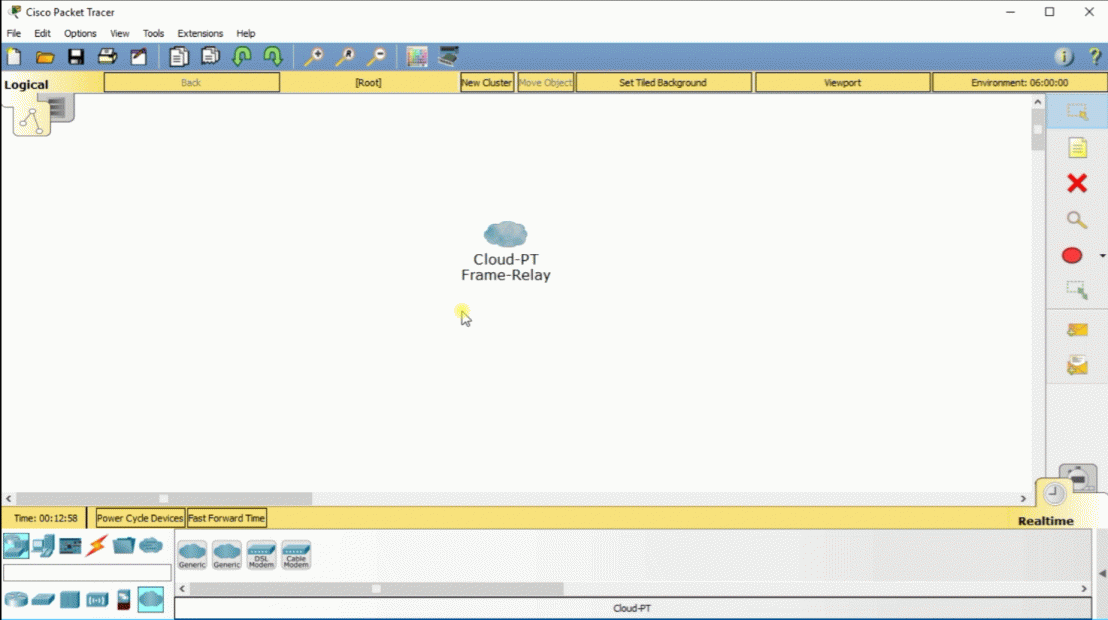
1. DSL-Modem-PT



A [digital subscriber line](https://en.wikipedia.org/wiki/Digital_subscriber_line) (DSL) [modem](https://en.wikipedia.org/wiki/Modem) is a device used to connect a [computer](https://en.wikipedia.org/wiki/Computer) or [router](https://en.wikipedia.org/wiki/Router_(computing)) to a telephone line which provides the [digital subscriber line](https://en.wikipedia.org/wiki/Digital_subscriber_line) service for connection to the [Internet](https://en.wikipedia.org/wiki/Internet), which is often called DSLbroadband.

The term DSLmodem is technically used to describe a modem which connects to a single computer, through an Ethernet port, USB port, or is installed in a computer PCI slot. The more common DSLrouter is a standalone device that combines the function of a DSL modem and a [router](https://en.wikipedia.org/wiki/Routing), and can connect multiple computers through multiple

1. Cloud-PT(Multiuser)



Cloud allows us to implement cloud computing in our project. Cloud computing is the delivery of on-demand computing services -- from applications to storage and processing power -- typically over the internet and on a pay-as-you-go basis.

1. TrueCafe

Its an internet café software, which helps in the management of the café by providing features like wireless billing(Wi-Fi hotspot supported),print management, power management, web reports etc.

This software plays a key role in managing the café efficiently.

**INFERENCE**

A network design for an internet cafe supporting 30 users has been created successfully. All users share a common ADSL network. Certain websites have been blocked using an extended ACL in the firewall. A billing software has been installed on all the PCs to monitor usage. The cafe also has printing, FAX and Xerox facilities. The PCs are coupled with a common storage for the users to download and print files.

All the possible issues have been considered and suitable measures have been taken to avoid them. The devices have been configured and a working model of the network has been created on a simulator (Cisco Packet Tracer) successfully.

**REFRENCES**

* [**https://www.google.co.in/**](https://www.google.co.in/)
* [**https://www.youtube.com**](https://www.youtube.com)
* [**https://www.wikipedia.org**](https://www.wikipedia.org)
* [**https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer**](https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer)