

**SET-UP OF NETWORK ADDRESS TRANSLATION
(NAT) TO MAP PRIVATE TO PUBLIC ADDRESS FOR
INTERNET ACCESS.
PART-2 (EVALUATION OF LAB DEMO)**

CLIENT: FOZIA NOREEN

Introduction.

Today most of the organizations have their own LAN. Usually clients of the LAN are assigned with special categories of IP addresses known as private ip. This is primarily of two reasons.

- 1) The number of global IP addresses is limited and vanishing fast. The ISP or the Address Registry controls the number of public addresses to any organization. They allot only limited such addresses. So if an organization has a large number of clients inside a network it cannot provide to all clients.
- 2) A client having a public ip address can have direct access to the internet and vice versa. This means the identities of the clients are exposed to the global internet and thus exposing those to the threats coming from internet.

As long as the clients communicate within own network there is no need of public ip address. But with private ip address they cannot directly access internet.

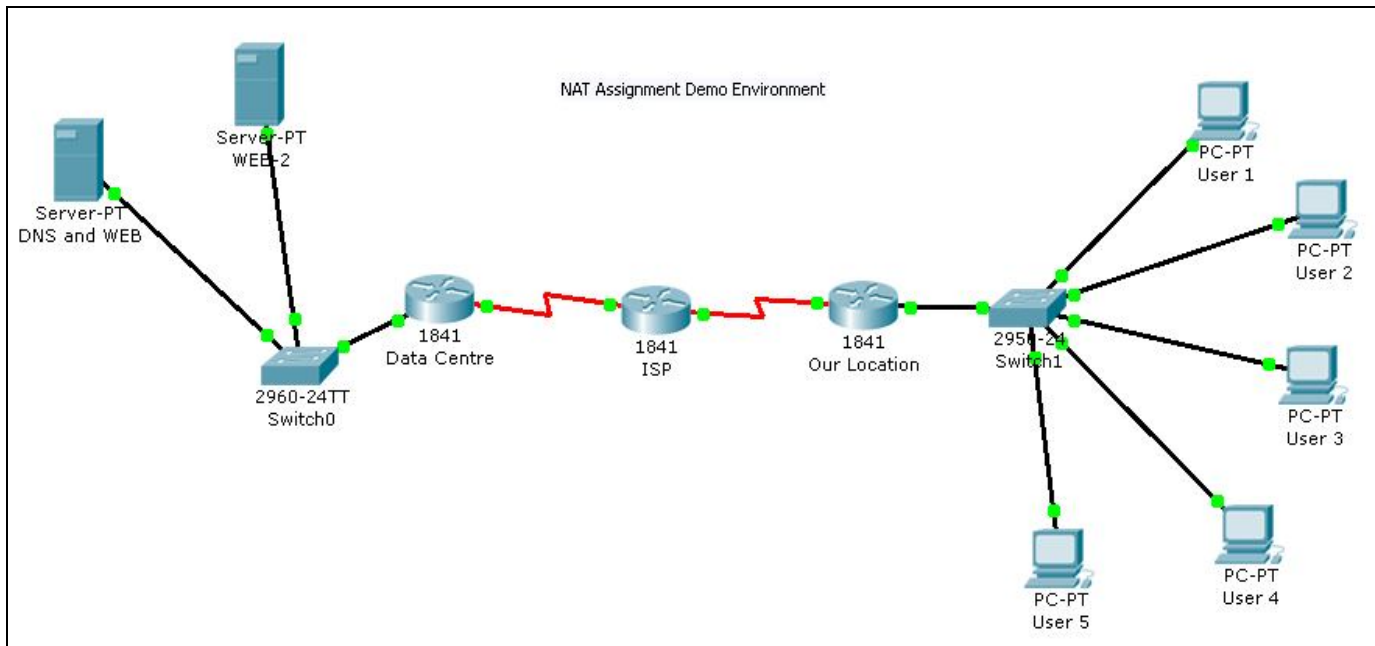
There are various methods of solving this problem. And my chosen lab topic i.e. “ Network Address Translation (NAT)” is one of the simplest and effective such methods.

“Connecting a network to the Internet using private addresses requires translating the private addresses to public addresses. This translation process is called Network Address Translation (NAT)” *Cisco Networking Academy Program, CCNA 1 and 2 Companion Guide (Anon. , 2003, p.1101)*

In the following sections I shall discuss the demo topic, its configuration, results and alternatives.

Evaluation of Demo Network

Demo Network Topology:



In my lab I have created web server and DNS server. I shall treat this as Internet servers. I have also created a subnet as "our location" where my users are located. I shall treat these users as internal users. All the clients inside "our location" have ip addresses from private ip pool 192.168.0.0/24 and thus cannot access Internet directly. There are total 30 users in the subnet (for testing I would take only 5 clients.) My ISP has provided us public ip subnet 74.85.96.0/29 for my use. The subnet has only 6 useable ip address

Equipments used:

I have used Cisco packet tracer to simulate the demo environment. And I have selected following hardware platform for it.

- Cisco 1841 routers (3 nos)
- Cisco 2960 Managed Layer 2 switches (2 nos)
- Standard tolr servers (2 nos)
- Standard PCs (2 nos)

My Goal:

- To provide Internet access to all the clients.

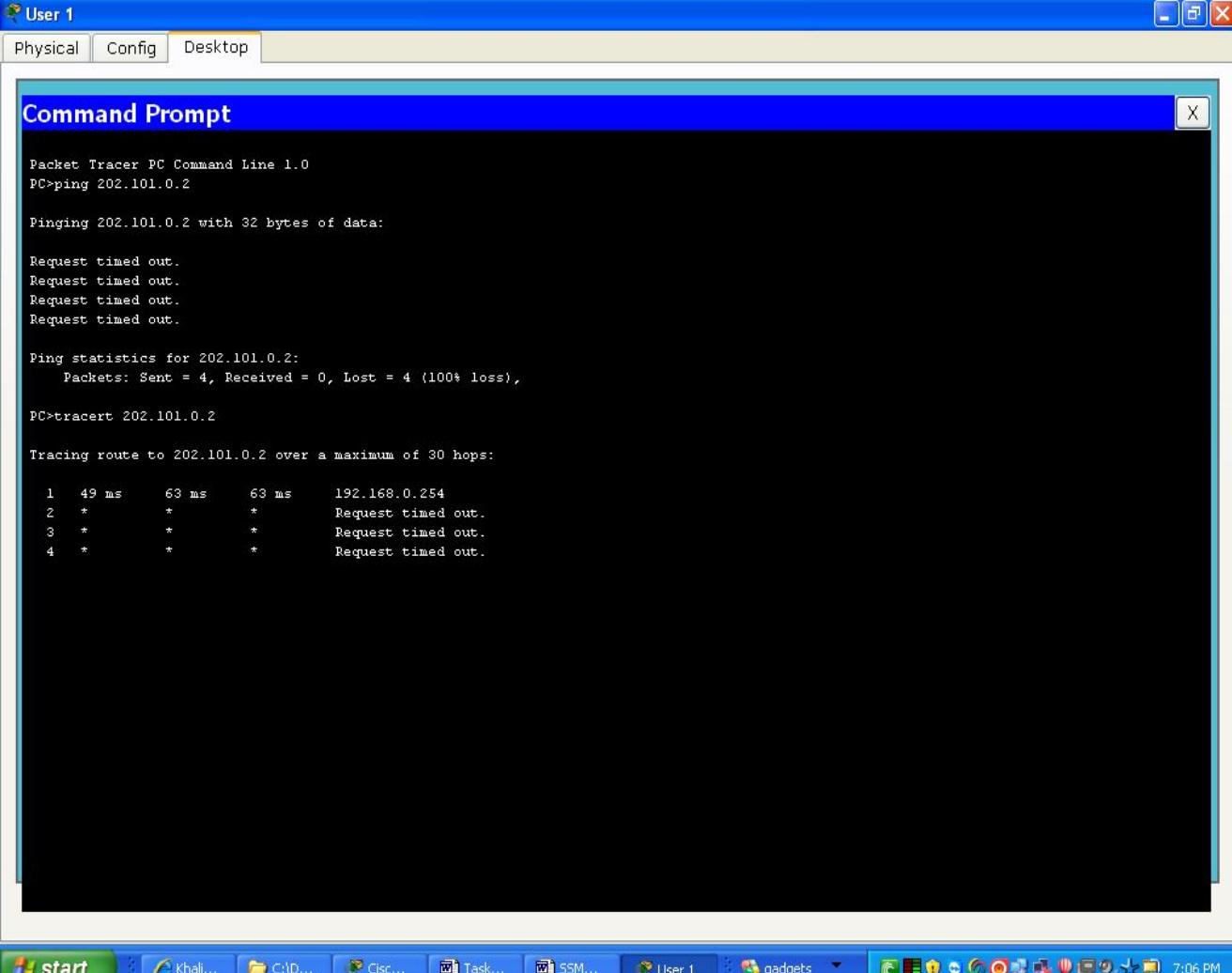
- Hide the identity of clients from Internet.

My solution:

Any outbound request has a private ip at the source address field when it enters the router. In normal condition this packet would be dropped at ISP router. After I configure NAT the router would transparently replace this private address with my public addresses so that the packet is not dropped at ISP routers.

Tests and results:

I have tried to PING the internet servers from internet clients before the NAT was configured. But I failed. A TRACE ROUTE showed that the ISP router drops the packets originated from internal clients. (Ref Figure-2)



The screenshot shows a Packet Tracer PC Command Line window. The window title is "User 1" and it has tabs for "Physical", "Config", and "Desktop". The command prompt shows the following output:

```
Packet Tracer PC Command Line 1.0
PC>ping 202.101.0.2

Pinging 202.101.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 202.101.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>tracert 202.101.0.2

Tracing route to 202.101.0.2 over a maximum of 30 hops:

  0  49 ms  63 ms  63 ms  192.168.0.254
  1  *      *      *      Request timed out.
  2  *      *      *      Request timed out.
  3  *      *      *      Request timed out.
  4  *      *      *      Request timed out.
```

Figure-2

After the NAT was configured in the router I repeated the same tests and this time I was able to successfully PING the servers. I also successfully browsed the web server by its domain name from another client. (Ref Figure-3)

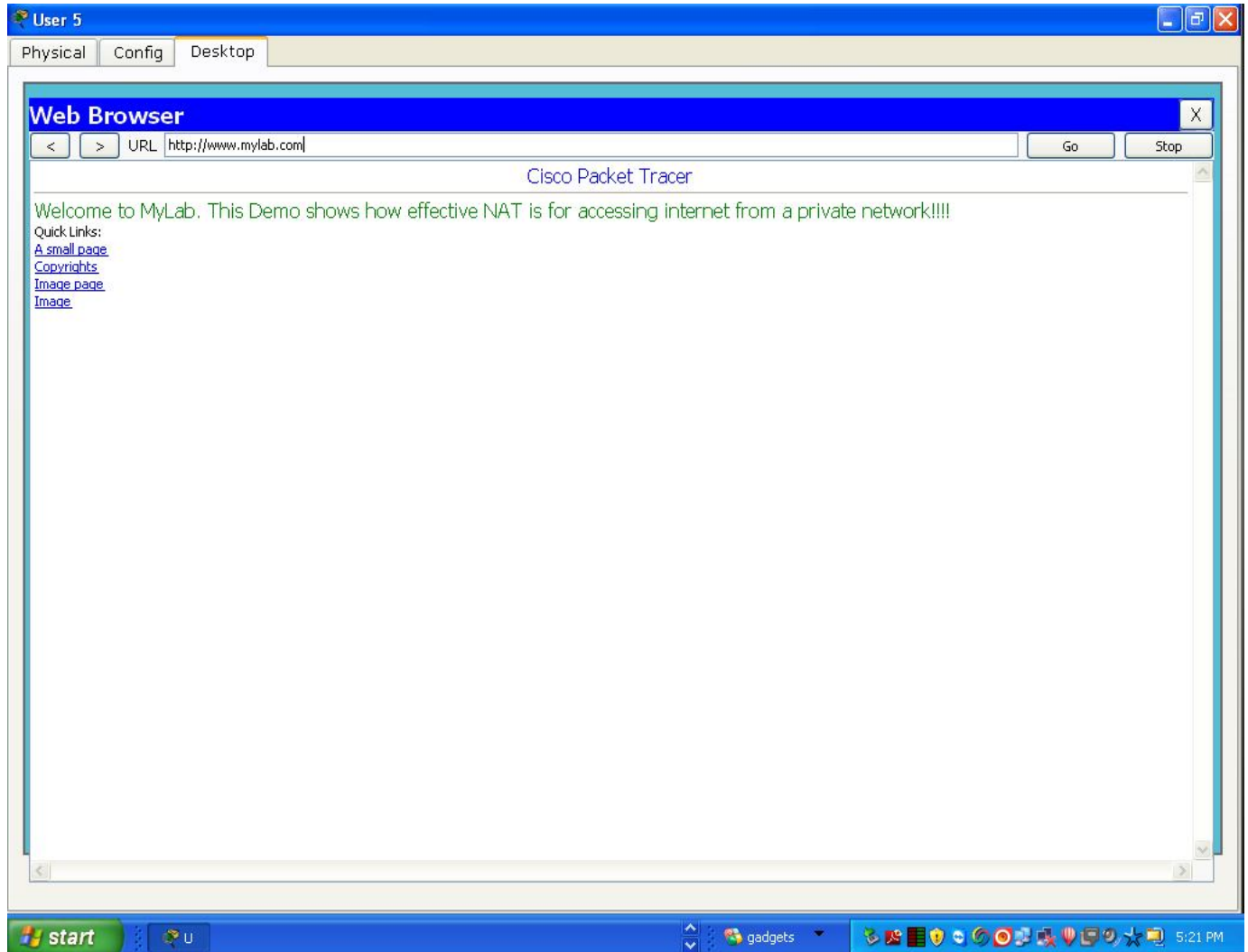


Figure-3

This proves that after NAT implementation HTTP, DNS and other packets originated from internal clients and bound to internet are not dropped by the ISP routers.

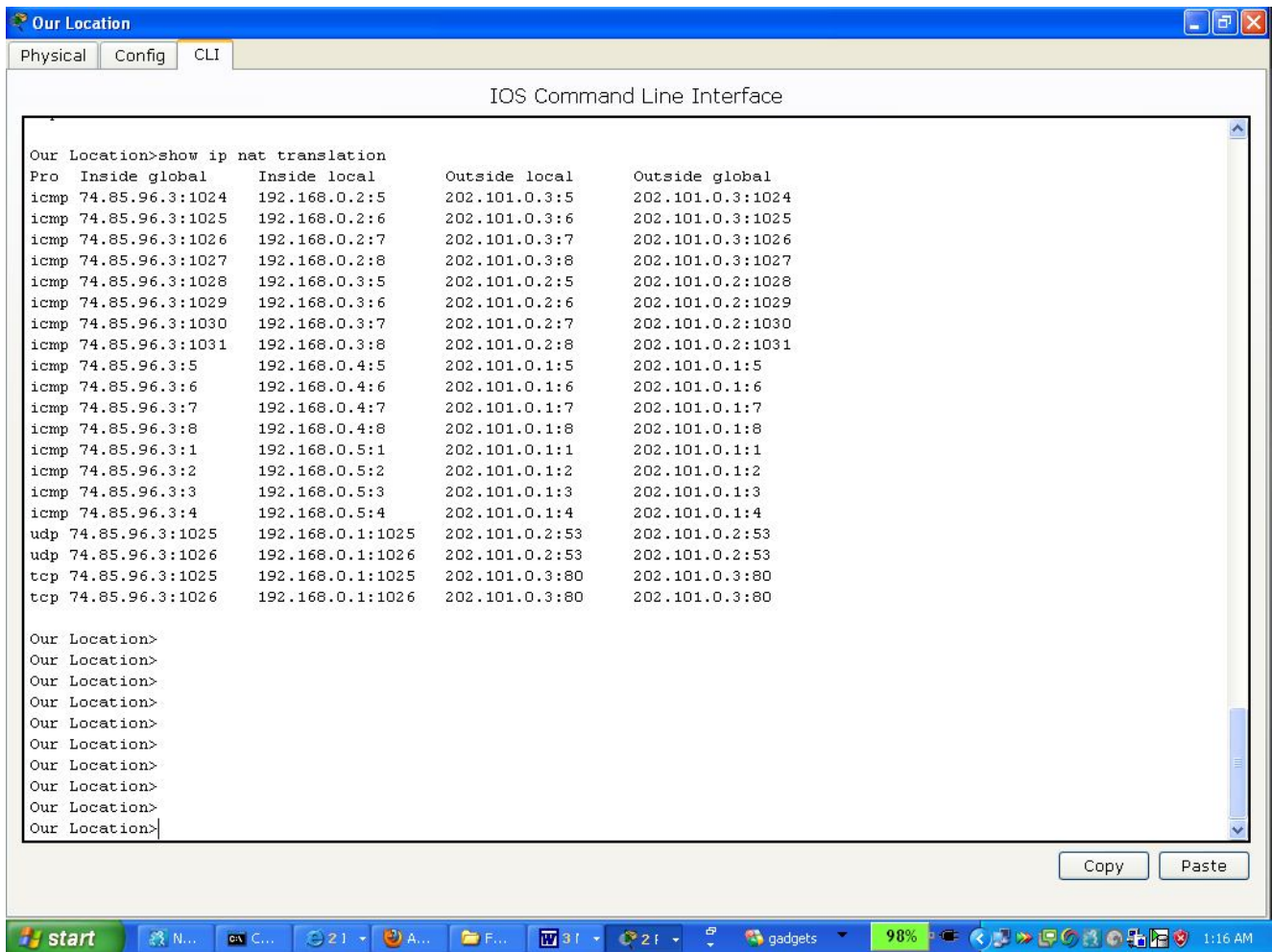


Figure-4

The above figure shows the NAT table of the router. It clearly shows that how client addresses (Inside local) are translated to public addresses (Inside global) by the router.

Router configuration for NAT and explanation:

interface FastEthernet0/0 (LAN side of router)

ip address 192.168.0.254 255.255.255.0

ip nat inside (defines the inside network i.e. the source of packets which are to be done NAT)

duplex auto

speed auto

!

interface Serial0/0/0 (Internet side of router)

ip address 74.85.96.2 255.255.255.252

ip nat outside (defines the outbound direction of translated packets. A packet would only be translated if it is bound to move outside this interface)

clock rate 56000

!

```
!  
!  
access-list 1 permit 192.168.0.0 0.0.0.31 (This access list defines the list of internal ip addresses  
which are allowed to participate in NAT. An administrator can selectively allow or disallow its clients  
to access internet by using NAT. In that case he has to define this access list accordingly)  
!  
ip nat pool global 74.85.96.3 74.85.96.6 netmask 255.255.255.248 ( Defines the list of public  
addresses to be used for NAT. So internal clients addresses would be replaced by one of this ips in  
the pool)  
!  
ip nat inside source list 1 pool global overload ( This is the actual NAT statement . This says router to  
NAT the packets sourced from inside network i.e. LAN for all the clients that are permitted by access-  
list 1 . It also directs the router to uses the ip addresses defined in the NAT pool for this purpose. The  
last word overload means the router would be using port address translation so that one public ip  
can be mapped with multiple private ip addresses)  
ip classless  
ip route 0.0.0.0 0.0.0.0 74.85.96.1  
!
```

- Some of the running configurations are deleted and only parts relevant to my assignment are kept.

Problem encountered:

In my network I have 30 clients (5 are used for demo) and have only 6 usable private ip address. More over two are used for serial link between my router and ISP. So practically I have 4 public addresses to use for NAT. I found that no more than 4 internal clients are able to access internet simultaneously. Because first 4 hosts are occupying the 4 public addresses. And others can only access internet when any of those occupied NAT relation times out.

Trouble shooting:

I used the verification commands to check the NAT table of the router and found first 4 hosts are occupying the 4 public addresses. And others can only access internet when any of those occupied NAT relation times out. To solve this problem I used "over loading" NAT (often called PAT or Port address translation) to solve this problem.

"Overloading is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address (many-to-one) by using different ports. Therefore, it's also known as port address translation (PAT)." *CCNA: Fast Pass* (Todd Lammle, p.13)

Alternative solution to NAT

Many organizations prefer to use proxy server in place of NAT for Internet Access from internal network.

“In computer networks, a proxy server is a server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server.” (Wikipedia, 2008)

A proxy server usually has two interface cards. One is configured with public ip address and another with private address. The public ip receives HTTP, FTP requests from internal clients and send the same request to the desired internet servers. The outbound packets bear public address of proxy server as source ip and thus not dropped in internet. The proxy server receives the packets from internet and delivers it to the client who has originally requested it.

Topology with proxy server:

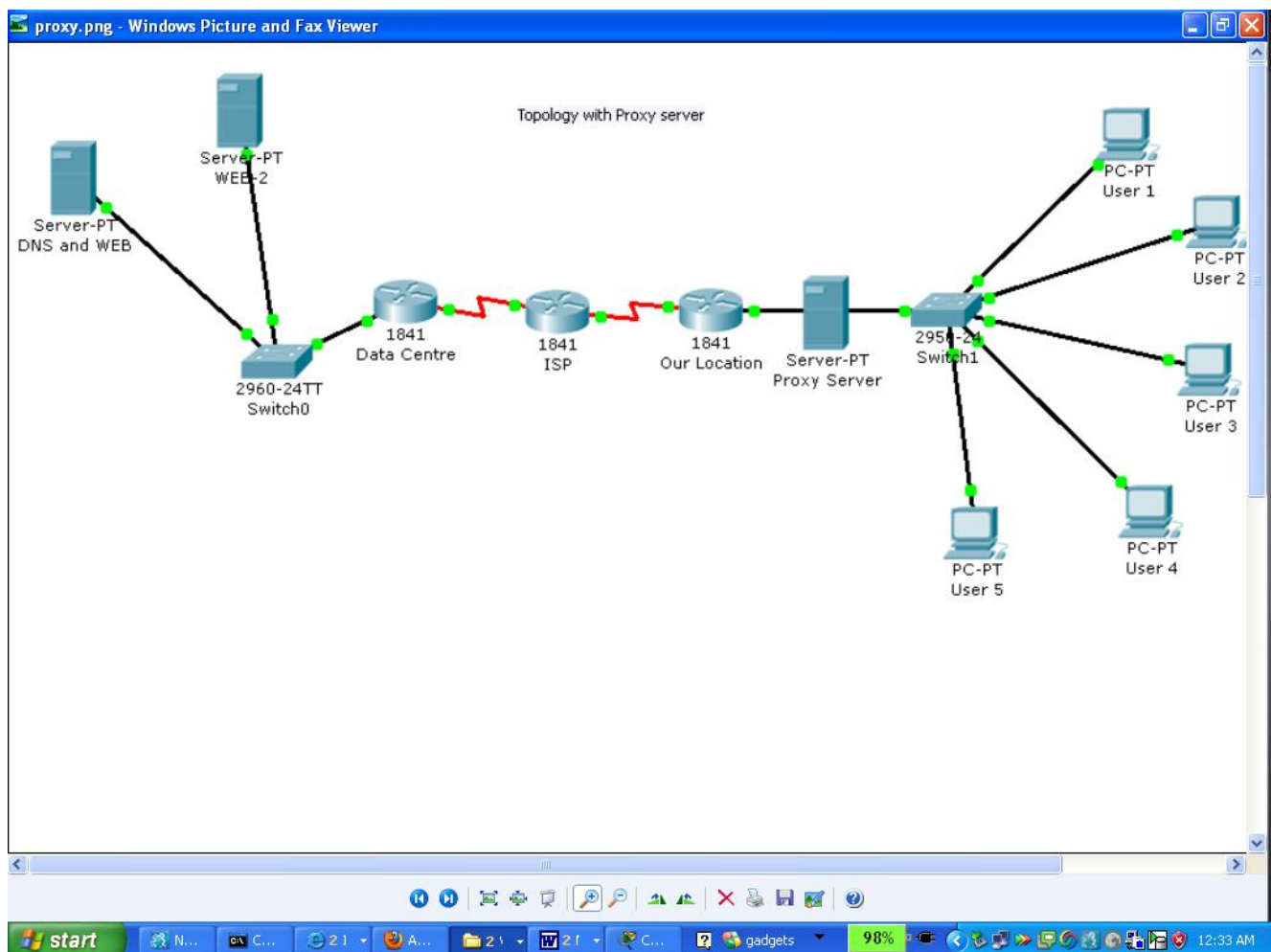


Figure-4

Equipments required:

- 1) A router to connect to the ISP
- 2) One server with two NIC
- 3) Switches depending upon the number of clients to be connected.

Comparison between proxy and NAT:

Proxy	NAT
In this technique additional hardware in the form of server is required.	No additional hardware is required and can be implemented in the router itself.
Proxy can save a reasonable volume of bandwidth by delivering most visited sites locally from its local cache. (If this feature is enabled)	In NAT all the requests are transparently sent over internet so no saving on bandwidth is possible.
It can very well support standard applications like HTTP, HTTPS, FTP etc. But running applications those use non-standard ports behind proxy can be very difficult.	NAT can transparently support practically all services.
Proxy servers can work up to application layer so advanced filtering features like content blocking, time limited access etc is possible in it.	NAT only works in network and transport layer. So though packet and port filtering is possible but application layer based filtering is not possible.
It can provide real time access log so that administrator can monitor user activities.	No such real time activity log is usually possible with router based NAT implementation.
Running internet servers behind proxy is very difficult.	Servers can be and mostly hosted behind NAT.
Suitable for Large to Medium sized networks.	NAT uses a good amount of system resources. So when implemented in general routers it is suitable for small networks. When implemented in firewalls and high end routers very much suitable to be used in medium to large networks.

Conclusion

Based on all the facts and research I have chosen NAT as the technology to allow internet access to my internal clients. This is because my network is small and the router I have selected i.e. 1841 has default RAM of 32 MB which is quite sufficient to implement NAT in my demo.

References and research materials

Printed materials

Cisco Networking Academy Program
CCNA 1 and 2 Companion Guide, Third Edition
(Helped in understanding NAT)

Todd Lammle
CCNA: Fast Pass
(Helped with NAT configuration of Cisco routers)

Electronic Materials.

IP addresses
Wikipedia (http://en.wikipedia.org/wiki/IP_address)
(Helped in understanding private and public ip addresses)

Private IP and Public IP
about.com (<http://compnetworking.about.com/od/workingwithipaddresses/f/privateipaddr.htm>)
(Helped in understanding private and public ip addresses)

Network address translation
Wikipedia (http://en.wikipedia.org/wiki/Network_address_translation)
(Helped in understanding concept of NAT)

Network Address Translation (NAT)
Cisco system (http://www.cisco.com/en/US/tech/tk648/tk361/tk438/tsd_technology_support_sub-protocol_home.html)
(Helped with NAT configuration of Cisco routers)