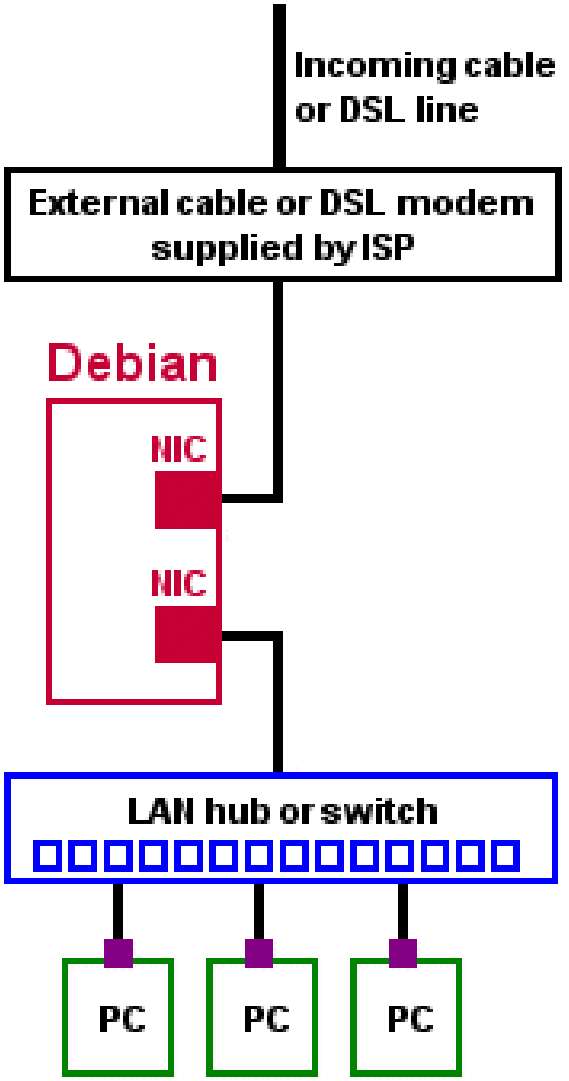
CONFIGURATION OF NAT ON DEBIAN SYSTEMS

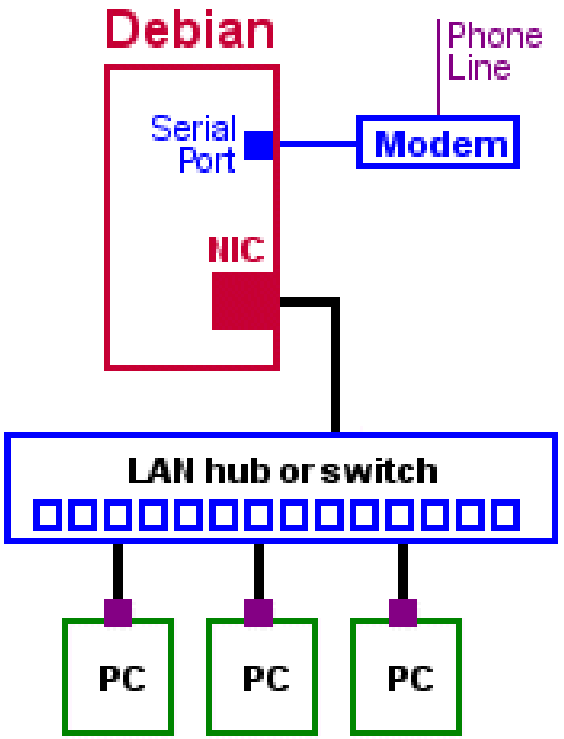
By : Reena Yadav
Hrishikesh Tak

Proxy Server or NAT

Sharing Your Broadband Connection



Sharing a Modem Connection



Proxy Server

- Proxy server is a "dual-homed" system. In other words, it needs two network interfaces. The "internal" interface (a NIC card) connects to the internal LAN and the "external" interface connects to the outside network (typically the Internet).

Network Address Translation (NAT)

- Network Address Translation allows a single device, such as a router, to act as an agent between the Internet (or "public network") and a local (or "private") network.
- This means that only a single, unique IP address is required to represent an entire group of computers.
- Short for Network Address Translation, an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

Setup of wired connection b/w 3 Debian Systems

- **Router** is required , connect 3 systems to router using **LAN**
- **step 1 :** Root permission will required

  step 2 : edit the file /etc/network/interfaces with following commands on each system .

On Node A

- auto eth0
- iface eth0 inet static
- address 192.168.1.90
- gateway 192.168.1.1
- netmask 255.255.255.0

On Node B

- auto eth0
- iface eth0 inet static
- address 192.168.1.91
- gateway 192.168.1.1
- netmask 255.255.255.0

On Node C

- auto eth0
- iface eth0 inet static
- address 192.168.1.92
- gateway 192.168.1.1
- netmask 255.255.255.0

- Save the file and exit the editor
- Reboot your System
- **To test, ping node A from node B:**
- **Ping 192.168.1.91**
- **Ping 192.168.1.1**

- Make one system (Node A) as Proxy Server with enabled wireless
- Disable wireless from other (Node B & Node C) systems using following command :
- **“sudo service network-manager stop”**
- **Ifconfig**
- Setup Node A as Proxy Server/NAT using following script

How To Set Up A Debian Linux Proxy Server

Section A

- Enter your internal interface designation (INTIF)
- Enter your external interface designation (EXTIF)

Section B

- If your external interface uses a static IP address
- Uncomment the EXTIP line and enter your static IP address

Section C

- If your external interface uses a dynamic IP address
- Uncomment the EXTIP line

- #!/bin/sh
- # === SECTION A
- INTIF="eth0"
- EXTIF="wlan0"
- # === SECTION B
- # -FOR THOSE WITH STATIC PUBLIC IP ADDRESSES
- #EXTIP="your.static.IP.address"

- # === SECTION C
- # -FOR THOSE WITH DYNAMIC PUBLIC IP ADDRESSES
- #EXTIP="`/sbin/ifconfig wlan0 | grep 'inet addr' | awk '{print $2}' | sed -e 's/.*://'`"

- echo "Loading required stateful/NAT kernel modules..."

- /sbin/depmod -a
- /sbin/modprobe ip_tables
- /sbin/modprobe ip_conntrack
- /sbin/modprobe ip_conntrack_ftp
- /sbin/modprobe ip_conntrack_irc
- /sbin/modprobe iptable_nat
- /sbin/modprobe ip_nat_ftp
- /sbin/modprobe ip_nat_irc

- echo "   Enabling IP forwarding..."
- echo "1" > /proc/sys/net/ipv4/ip_forward
- echo "1" > /proc/sys/net/ipv4/ip_dynaddr

  # Clearing any existing rules and setting default policy
- iptables -P INPUT ACCEPT
- iptables -F INPUT
- iptables -P OUTPUT ACCEPT
- iptables -F OUTPUT
- iptables -P FORWARD DROP
- iptables -F FORWARD
- iptables -t nat -F

- # FWD: Allow all connections OUT and only existing and related ones IN
- iptables -A FORWARD -i $EXTIF -o $INTIF -m state --state ESTABLISHED,RELATED -j ACCEPT
- iptables -A FORWARD -i $INTIF -o $EXTIF -j ACCEPT

- # Enabling SNAT (MASQUERADE) functionality on $EXTIF
- iptables -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE

- After successful running of script on Node A , change **DEFAULT GATEWAY** from other Systems .
- To change gateway use following command on Node B & Node C:
- **Sudo route add default gw 192.168.1.90**
- 192.168.1.90 : ip address of proxy server

- To check internet connection on other systems use
- **ping www.google.com or**
- **ping 8.8.8.8**
- To check the route to connect to remote server use
- **traceroute 8.8.8.8**
- **8.8.8.8 is** google-public-dns-a.google.com

Linux Squid Proxy Server

- Configuring the squid in transparent mode, special configuartion is not required on the client side. All the requests originatinating from client and going to internet on port 80 are automatically redirected by proxy.
- Squid is caching proxy server, which improves the bandwidth and the reponse time by caching the recently requested web pages.

Installing the Squid Proxy

- Sudo apt-get install squid
- To configure squid proxy server we need to edit the /etc/squid/squid.conf file
- Providing a name for the proxy server machine.

  Example: visible_hostname name
- Specifying the interface and port number on which the proxy server should listen.

  http_port <ip address belonging to LAN>:<port number>

- Assigning Access Controls

  acl any_name src (n/w_address)/(n/w_mask)

  acl mylan src 192.168.60.0/255.255.255.0
- Allow or Deny based on Access Control.

  http_access allow mylan
- Saving the changes and exit the Editor
- Starting the squid proxy services

  /etc/init.d/squid start

Thank You !!!