Outline of This Lecture

- Intruders on Internet: An Attack (Live Demo?)
- Defending the Network
  - Perimeter Level (Firewalls)
  - Application/Services Level
- Network Management (Live Demos?)
The Victim: An organization on Internet

- Assume company’s domain name is ushacomm.co.in
- Has legal IP addresses obtained from ISP.
- Has 20-30 machines and runs services email, www, ftp, ...
- Goal: Break-in on some machines
Map the Victim’s network

- Find the IP addresses of machines
- Several methods

```plaintext
% nslookup
Default Server: dns.iitb.ac.in
Address: 202.54.44.116

> set query=any
> ushacomm.co.in.
Server: dns.iitb.ac.in
Address: 202.54.44.116

Non-authoritative answer:
ushacomm.co.in nameserver = hansel.ushacomm.co.in
ushacomm.co.in nameserver = gretel.ushacomm.co.in
ushacomm.co.in preference = 10, mail exchanger = hansel.ushacomm.co.in

Authoritative answers can be found from:
ushacomm.co.in nameserver = hansel.ushacomm.co.in
ushacomm.co.in nameserver = gretel.ushacomm.co.in
hansel.ushacomm.co.in internet address = 202.54.54.177
gretel.ushacomm.co.in internet address = 202.54.54.188
```
Probe further

> server 202.54.54.177
Default Server: [202.54.54.177]
Address: 202.54.54.177

> ls ushacomm.co.in.
[[202.54.54.177]]
$ORIGIN ushacomm.co.in.

ftpsrv 1H IN A 202.54.54.186
hansel 1H IN A 202.54.54.177
ubestftp 1H IN A 202.54.54.178
gretel 1H IN A 202.54.54.188

- Now we know 4 machines addresses
- Can probe each of them using (ping, finger, telnet, ..)
- Super tools (e.g. nmap) make life easier

finger guest@202.54.54.177
[202.54.54.177]
Account Name: guest
Email address: guest@ushacomm.co.in

Can you guess the password?

G. Sivakumar
Computer Science and Engineering  IIT Bombay  siva@iitb.ac.in
Network Security- Part 2
Nmap: A Hacker’s Dream

NAME
nmap - Network exploration tool and security scanner

SYNOPSIS
nmap [Scan Type(s)] [Options] <host or net #1 ... [#N]>

DESCRIPTION
Nmap is designed to allow system administrators and curious individuals to scan large networks to determine which hosts are up and what services they are offering. nmap supports a large number of scanning techniques such as: UDP, TCP connect(), TCP SYN (half open), ftp proxy (bounce attack), Reverse-ident, ICMP (ping sweep), FIN, ACK sweep, Xmas Tree, SYN sweep, and Null scan. See the Scan Types section for more details. nmap also offers a number of advanced features such as remote OS detection via TCP/IP fingerprinting, stealth scanning, dynamic delay and retransmission calculations, parallel scanning, detection of down hosts via parallel pings, decoy scanning, port filtering detection, fragmentation scanning, and flexible ...
Interesting ports on (202.54.54.187):

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Protocol</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>open</td>
<td>tcp</td>
<td>ftp</td>
</tr>
<tr>
<td>25</td>
<td>open</td>
<td>tcp</td>
<td>smtp</td>
</tr>
<tr>
<td>53</td>
<td>open</td>
<td>tcp</td>
<td>domain</td>
</tr>
<tr>
<td>80</td>
<td>open</td>
<td>tcp</td>
<td>http</td>
</tr>
<tr>
<td>135</td>
<td>open</td>
<td>tcp</td>
<td>loc-srv</td>
</tr>
<tr>
<td>139</td>
<td>open</td>
<td>tcp</td>
<td>netbios-ssn</td>
</tr>
<tr>
<td>1032</td>
<td>open</td>
<td>tcp</td>
<td>iad3</td>
</tr>
<tr>
<td>1352</td>
<td>open</td>
<td>tcp</td>
<td>lotusnote</td>
</tr>
</tbody>
</table>

TCP Sequence Prediction: Class=trivial time dependency
Difficulty=15 (Easy)

Sequence numbers: C061748 C061B90 C062018 C06247C C062918 C062D72
Remote operating system guess: Windows NT4 / Win95 / Win98
What next?

- A chain is as strong as its **weakest** link.
- Known vulnerabilities for many OS, Applications.
- rootshell.com posts new exploits regularly.
- Break into **one** machine first, then easier to attack rest.
- Try some UDP ports (used for snmp management)
Information using **snmpwalk**

```
%snmpwalk 202.54.44.177 public
system.sysDescr.0 = "Sun SNMP Agent, Ultra-5_10"
system.sysObjectID.0 = OID: enterprises.42.2.1.1
system.sysUpTime.0 = Timeticks: (17913559) 2 days, 1:45:35.59
system.sysContact.0 = "System administrator"
system.sysName.0 = "hansel"
system.sysLocation.0 = "System administrators office"
    ...
at.atTable.atEntry.atIfIndex.1.1.172.16.1.121 = 1
at.atTable.atEntry.atIfIndex.1.1.172.18.1.2 = 1
at.atTable.atEntry.atIfIndex.1.1.192.9.200.14 = 1
at.atTable.atEntry.atIfIndex.1.1.192.9.200.15 = 1
at.atTable.atEntry.atIfIndex.1.1.192.9.200.25 = 1
    ...
  ipRouteNextHop.192.67.184.64 = IpAddress: 202.54.54.185
  ipRouteNextHop.198.6.100.21 = IpAddress: 202.54.54.185
    ...
  ipNetToMediaPhysAddress.1.172.18.1.2 = 0:10:7b:3a:87:9f
  ipNetToMediaPhysAddress.1.192.9.200.4 = 0:c7:4c:24:8f
```

- How many subnets in use?
- How **ARP** is done for other networks? (ICMP redirect)
- Can we inject such messages (spoofing) into the network?
Other tools- Ethereal

G. Sivakumar
Computer Science and Engineering  IIT Bombay  siva@iitb.ac.in
Network Security- Part 2
Other tools - Ethereal

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0000000</td>
<td>AlliedTe_21:bb:a5</td>
<td>Spanning-tree-(for-bi) STP</td>
<td>Conf. Root = 32768/00:0c:46:21:9a:40</td>
<td></td>
</tr>
<tr>
<td>10.064034</td>
<td>10.161.251.1</td>
<td>Broadcast</td>
<td>ARP</td>
<td>10.161.251.1 is at 00:40:0d:98:4e:37</td>
</tr>
<tr>
<td>11.803803</td>
<td>10.161.251.2</td>
<td>Broadcast</td>
<td>ARP</td>
<td>10.161.251.2 is at 00:40:0d:98:54:f0</td>
</tr>
<tr>
<td>11.400643</td>
<td>Mototech_S1:c7:8f</td>
<td>NETBIOS- Domain/Workgroup Announcement WORKGROUP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.963519</td>
<td>Cisco f5:99:c7</td>
<td>CDP/VTP</td>
<td>DTP</td>
<td>Dynamic Trunking Protocol</td>
</tr>
</tbody>
</table>

Frame 8 (64 bytes on wire, 64 bytes captured)
Ethernet II, Src: 00:40:0d:98:54:f0, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (reply)

0000 ff ff ff ff ff ff 00 40 0d 98 54 f0 08 06 00 01 .......@ ..T.....
0010 08 00 06 04 00 02 00 40 0d 98 54 f0 0a a1 fb 02 ........@ ..T.....
0020 00 00 00 00 00 00 00 a1 fb 02 00 00 00 00 00 00 ............
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 27 52 c9 80 ............'R..

File: (Untitled) 7427 Bytes 00:00:49 P: 69 D: 69 M: 0 Drops: 0
Other tools - Tcptrack

<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
<th>State</th>
<th>Idle</th>
<th>A</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>134.76.11.100:56487</td>
<td>10.100.5.173:39171</td>
<td>ESTABLISHED</td>
<td>0s</td>
<td>32 KB/s</td>
<td></td>
</tr>
<tr>
<td>10.102.1.1:53815</td>
<td>212.122.69.69:20</td>
<td>ESTABLISHED</td>
<td>1s</td>
<td>1 KB/s</td>
<td></td>
</tr>
<tr>
<td>10.209.13.4:42113</td>
<td>10.13.2.64:80</td>
<td>SYN_SENT</td>
<td>1s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.209.4.1:53093</td>
<td>10.102.1.1:80</td>
<td>CLOSED</td>
<td>2s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.209.13.1:47323</td>
<td>10.13.2.64:80</td>
<td>SYN_SENT</td>
<td>13s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.209.13.1:47388</td>
<td>10.13.2.64:80</td>
<td>SYN_SENT</td>
<td>13s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.209.13.1:47324</td>
<td>10.13.101.15:80</td>
<td>SYN_SENT</td>
<td>16s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.209.13.1:47380</td>
<td>10.13.1.35:80</td>
<td>SYN_SENT</td>
<td>18s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.209.4.1:53111</td>
<td>10.100.5.1:80</td>
<td>CLOSED</td>
<td>27s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.209.4.1:53112</td>
<td>10.100.5.1:80</td>
<td>CLOSED</td>
<td>27s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.129.100.64:46203</td>
<td>216.155.193.186:5050</td>
<td>ESTABLISHED</td>
<td>36s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.209.13.6:60354</td>
<td>10.13.2.64:80</td>
<td>SYN_SENT</td>
<td>36s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.209.4.2:58128</td>
<td>10.105.1.3:80</td>
<td>CLOSED</td>
<td>37s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.209.3.2:42325</td>
<td>10.129.1.1:25</td>
<td>RESET</td>
<td>37s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.7.2.80:45823</td>
<td>216.155.193.128:5050</td>
<td>ESTABLISHED</td>
<td>37s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.3.3.40:32776</td>
<td>216.155.193.134:5050</td>
<td>ESTABLISHED</td>
<td>37s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.3.3.43:2986</td>
<td>207.46.107.6:1863</td>
<td>ESTABLISHED</td>
<td>37s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.5.1.46:3366</td>
<td>207.46.106.34:1863</td>
<td>ESTABLISHED</td>
<td>37s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.129.1.1:42313</td>
<td>10.209.3.2:113</td>
<td>RESET</td>
<td>37s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.209.13.1:47237</td>
<td>10.13.1.35:80</td>
<td>SYN_SENT</td>
<td>37s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.209.13.6:60350</td>
<td>10.13.2.64:80</td>
<td>SYN_SENT</td>
<td>37s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>216.155.193.158:5050</td>
<td>10.4.1.12:2666</td>
<td>ESTABLISHED</td>
<td>37s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>216.155.193.128:5050</td>
<td>10.3.2.7:4691</td>
<td>ESTABLISHED</td>
<td>37s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.12.15.8:43020</td>
<td>216.155.193.172:5050</td>
<td>ESTABLISHED</td>
<td>38s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.200.12.114:54237</td>
<td>10.209.3.1:22</td>
<td>CLOSED</td>
<td>38s</td>
<td>0 B/s</td>
<td></td>
</tr>
<tr>
<td>10.12.41.27:35678</td>
<td>216.155.193.140:5050</td>
<td>ESTABLISHED</td>
<td>38s</td>
<td>0 B/s</td>
<td></td>
</tr>
</tbody>
</table>
Keeping **every** system secure is a good goal. But, ...
Firewalls are systems that control the flow of traffic between the Internet and internal networks and systems. Like a **guard post** in the lobby of a building. Single “choke point” is easier to control/defend from outside hackers (and inside spies!).
Benefits of Firewall

1. Internet security can be monitored and alarms generated.
2. Network Address Translator (NAT) alleviates IP address shortage.
3. Audit and log Internet Usage. Useful for justifying expense, identifying bottlenecks.
4. Central point of contact (email, www and ftp). Converse: single point of failure?
5. Caching WWW proxy servers (squid). Ideal for low bandwidth WAN connections esp. in India!
Types of Firewalls

1. Packet-Filtering Firewalls
2. Circuit-level gateways
3. Application-level Gateways (proxies)
Packet Filtering Firewall

Filters based on:
1. Source IP address
2. Destination IP address
3. Source Port
4. Destination Port

Default deny vs. Default allow
Filtering Rules

**Service-Dependent Filtering**

- Permit incoming Telnet sessions only to a specific list of internal hosts
- Permit incoming FTP sessions only to specific internal hosts
- Permit all outbound Telnet sessions
- Permit all outbound FTP sessions
- Deny all incoming traffic from specific external networks

**Service-Independent Filtering**

- Deny SNMP options like giving routing table
- Inspect for specific IP options
  - Source Routing Attacks
  - Tiny Fragment Attacks
- Checking for a special fragment offset
Circuit-Level Gateway

Variously known as *Stateful Packet Filter, Network Address Translation* and *IP masquerading/IP Chains/Iptables.*

http://www.iptables.org/

- Packet Filtering in the Kernel
- Rules to decide which ones to allow/deny.
- Allows set up of:
  - Traditional Proxies (proxy-aware clients)
  - Transparent Proxies (address rewriting/masquerading)

Invaluable for an organization connected to Internet.
Bastion Host Firewall

- Login to Bastion Host first
- Not very convenient
- Overloads a *single* host for multiple services
Insiders are a threat too! (80%!)
IIT Bombay’s Old Screened Subnet

Will use this first (for simplicity).
Real Solution (today’s) later...

G. Sivakumar
Computer Science and Engineering  IIT Bombay  siva@iitb.ac.in
Network Security- Part 2
iitbvsnl-cisco>show ip route
Codes:  C - connected,  S - static,  I - IGRP,  R - RIP,  M - mobile,  B - BGP
        D - EIGRP,  EX - EIGRP external,  O - OSPF,  IA - OSPF inter area
        N1 - OSPF NSSA external type 1,  N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1,  E2 - OSPF external type 2,  E - EGP
        i - IS-IS,  L1 - IS-IS level-1,  L2 - IS-IS level-2,  * - candidate default
        U - per-user static route,  o - ODR

Gateway of last resort is 202.54.44.250 to network 0.0.0.0

144.16.0.0/32 is subnetted, 2 subnets
S   144.16.111.81 [1/0] via 202.54.44.114
S   144.16.108.50  [1/0] via 202.54.44.114

202.54.44.0/24 is variably subnetted, 3 subnets, 2 masks
C   202.54.44.240/28 is directly connected, Serial0
C   202.54.44.112/28 is directly connected, Ethernet0
S   202.54.44.123/32  [1/0] via 202.54.44.119
S*  0.0.0.0/0    [1/0] via 202.54.44.250

Note the route above for 202.54.44.123 (hint: traffic shape)
TCP is a very **elegant** and **adaptive** protocol which does excellent “congestion” control by adjusting to the “bottlenecks” and reducing “window” size.
So, add an extra “slow” router.
What is Traffic Control (TC) in Linux Kernel

Shaping of Outgoing Traffic

Application/User Space

Kernel Space

IP

Ethernet Driver

Packet Classifiers

Virtual Devices

Queueing disciplines

32 Kbps

64 Kbps

128 Kbps

14.4 Kbps

32 Kbps
Firewall Limitations

1. Attacks that do not go through the firewall
   - Unrestricted dial-out!
   - Copying sensitive data onto floppy disks
   - Virus-infected software or files
   - Internal Network Sniffing, Password attacks

2. Some forms of denial of service attacks
Overview

- **Campus Network Infrastructure**
  - Academic Area
  - Hostels
  - Residential
  - **Hardware and Network** *(the easy part!)*
    - Gigabit L3 switches
    - 10 Mbps Internet *(4 Links)*
    - 5000+ nodes

- **Applications** *(Complex enough)*
  - Mail
  - Web Browsing/Hosting

- **Users and Management** *(Nightmare begins)*
  - MisUse *(mp3, movie, porn, hacking, fake mails, ...)*
  - CCTeam
    - We carry your Bytes
    - Our T-shirt *(cows, dogs, leopards!)*
Campus Backbone

IIT Bombay’s Backbone Connectivity

Computer Science Dept.
Avaya – P580

Hostel 1 - Active Patch
P133G2

Core - Computer Centre
Extreme BlackDiamond - 6908

Hostel 3
Avaya – P580

Hostel 5 - Active Patch
P133G2

Hostel 8
Avaya – P580

12 core MM fiber

24 core MM fiber

6 core MM fiber

24 core MM fiber

12 core MM fiber
Detailed Lan Layout

G. Sivakumar Computer Science and Engineering IIT Bombay siva@iitb.ac.in

Network Security- Part 2
Fibre Rack at CC
IIT Bombay’s Residential Area Connectivity

To IIT Bombay’s Backbone Network

Residential Router Specifications:
- CPU - Intel 3 Ghz
- Memory - 1 GB RAM
- HDD - 40 GB
- Network Cards - 5 100Mbps fiber cards
- OS - Fedora core 2
- Packages - IPTables, Bandwidthhd, Ntop, Tcptrack

100Mbps Fiber Links

Segment - 10.161.x.x Area - Lakeside
Segment - 10.162.x.x Area - Central Area1
Segment - 10.163.x.x Area - Central Area2
Segment - 10.164.x.x Area - HillSide1
Segment - 10.165.x.x Area - HillSide2
Where all does **security** figure?
Important LAN Issues

Important Considerations

- Virus, Spware
- Wrong IP addresses
- Wireless Access (guest house, conference halls)
- Static MAC-IP mapping
- Software Piracy
- Illegal Content (pornography,...)
- ...

Good LAN design can help a lot with this...
Critical Network Services

- **Firewall (Security *sine qua non*)**
  
  www.netfilter.org and www.iptables.org

  Free firewall software distributed under GNU General Public License

- **Domain Name Service (DNS) [http://cr yp.to/djbdns/]**

- **Directory Services (LDAP)**

- **Virus Scanning** clamav.elektrapro.com

  Clam AntiVirus Homepage
Critical Network (WAN) Services

- E-mail (www.qmail.org)
- Newsgroups (inn)
- Web Proxy
- WWW Servers (httpd.apache.org)
Network Servers Rack

- All **Vanilla** Intel Boxes running GNU/Linux
- Most services **load balanced. Hot Swappable** (at the machine level itself)
Inside IIT we have 50 IP subnets.

Over 5000 nodes.

All Private addresses 10.x.y.z

4 Different WAN subnets
  - 128, 64, 32, 32 address only!

**iptables** (www.iptables.org) to the rescue.

Selective services/machines opened up
  - Incoming ssh to different dept. servers.
  - Outgoing ssh, Yahoo/MSN chat
  - Outgoing port for SciFinder
  - Outgoing ftp from select machines

Making a **good policy** is the hardest!
# VSNL 1: All Interfaces.
#
ip link set eth1 up  #garbo1
ip addr flush dev eth1
ip addr add 203.197.74.140/25 brd 203.197.74.255 dev eth1

ip link set eth1:141 up  #garbo1
ip addr add 203.197.74.141/25 brd 203.197.74.255 dev eth1 label eth1:141

....

# VSNL 2: All Interfaces.
#
ip link set eth2 up
ip addr flush dev eth2
ip addr add 203.199.51.149/24 brd 203.199.51.255 dev eth2

ip link set eth2:21 up
ip addr add 203.199.51.21/24 brd 203.199.51.255 dev eth2 label eth2:21

# VSNL 3/4: All Interfaces.
#
ip link set eth3 up
ip addr flush dev eth3
ip addr add 203.199.81.149/24 brd 203.199.81.255 dev eth3

# VSNL 5: All Interfaces.
#
ip link set eth4 up
ip addr flush dev eth4
ip addr add 203.197.52.149/24 brd 203.197.52.255 dev eth4

ip link set eth4:21 up
ip addr add 203.197.52.21/24 brd 203.197.52.255 dev eth4 label eth4:21
Stateful firewalling. See [www.netfilter.org](http://www.netfilter.org)

**IP Filter**

- Used to filter packets
- The command to enter a rule is called *iptables*
- The framework inside kernel is called Netfilter
- Full matching on IP, TCP, UDP and ICMP packet headers
- Lesser matching on other packet headers possible
Basic Functionalities

- **NAT** (Network Address Translation)
  - **DNAT** - Destination Network Address Translation
  - **SNAT** - Source Network Address Translation
  - Requires *connection tracking* to keep states and expectations

- **Packet Mangling**
  - Strip all IP options
  - Change TOS values
  - Change TTL values
  - ...
  - Mark packets/connections within kernel
Packet Traversal Diagram

Kernelspace Structure

PREROUTING  FORWARD  POSTROUTING

INPUT  LOCAL PROCESS  OUTPUT
Example of NAT

How to **get into** a IIT-Bombay machine actually using *private address*.

siva@stdwww: hostname
stdwww.iimahd.ernet.in
siva@stdwww: host login.iitb.ac.in
login.iitb.ac.in has address 203.197.74.149
siva@stdwww: telnet login.iitb.ac.in 10623
Trying 203.197.74.149...
Connected to login.iitb.ac.in.
Escape character is ..

SunOS 5.8
+ * * * * * * * * * * * * * * * * * *
    pawan.cc.iitb.ac.in
    Intranet Server for
    C O M P U T E R   C E N T R E
+ * * * * * * * * * * * * * * * * +

login:
# NAT Rules on login.iitb.ac.in

# Incoming servers (telnet+ssh)

# AERO
iptables -t nat -A PREROUTING -p tcp -i eth1
   -d $IP1 --dport 1022 -j DNAT --to 10.101.1.1:22
iptables -t nat -A PREROUTING -p tcp -i eth1
   -d $IP1 --dport 1023 -j DNAT --to 10.101.1.1:23

# CHE
iptables -t nat -A PREROUTING -p tcp -i eth1
   -d $IP1 --dport 3022 -j DNAT --to 10.102.1.1:22
iptables -t nat -A PREROUTING -p tcp -i eth1
   -d $IP1 --dport 3023 -j DNAT --to 10.102.1.1:23

Of course, ssh is the preferred option.
## DNS Report for iitb.ac.in


<table>
<thead>
<tr>
<th>Status</th>
<th>Test Name</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASS</td>
<td>Missing Direct Parent check</td>
<td>OK. Your direct parent zone exists, which is good. Some domains (usually third or fourth level domains, such as example.co.us) do not have a direct parent zone ('co.us' in this example), which is legal but can cause confusion.</td>
</tr>
<tr>
<td>INFO</td>
<td>NS records at parent servers</td>
<td>Your NS records at the parent servers are: &lt;br&gt; dns2.iitb.ac.in. [203.199.51.159] [TTL=86400] [IN] &lt;br&gt; dns3.iitb.ac.in. [203.199.81.159] [TTL=86400] [IN] &lt;br&gt; dns4.iitb.ac.in. [203.199.81.159] [TTL=86400] [IN]  &lt;br&gt;[These were obtained from ns-ext.vix.com]</td>
</tr>
<tr>
<td>PASS</td>
<td>Parent nameservers have your nameservers listed</td>
<td>OK. When someone uses DNS to look up your domain, the first step (if it doesn't already know about your domain) is to go to the parent servers. If you aren't there, you can't be found. But you are listed there.</td>
</tr>
<tr>
<td>PASS</td>
<td>Glue at parent nameservers</td>
<td>OK. The parent servers have glue for your nameservers. That means they send the IP address of your nameservers, as well as their host names.</td>
</tr>
<tr>
<td>INFO</td>
<td>NS records at your nameservers</td>
<td>Your NS records at your nameservers are: &lt;br&gt; dns1.iitb.ac.in. [203.197.74.159] [TTL=172800] [IN]  &lt;br&gt; dns2.iitb.ac.in. [203.197.74.159] [TTL=172800] [IN]  &lt;br&gt; dns3.iitb.ac.in. [203.199.51.159] [TTL=172800] [IN]  &lt;br&gt; dns4.iitb.ac.in. [203.199.81.159] [TTL=172800] [IN]</td>
</tr>
</tbody>
</table>
How DNS works?

First accept packets

```
# Rules to accept inward DNS queries thru ogarbo
$IPTABLES -t FORWARD -p udp -i $WAN1_IFACE --dport 53 -j ACCEPT
$IPTABLES -t FORWARD -p udp -i $WAN2_IFACE --dport 53 -j ACCEPT
$IPTABLES -t FORWARD -p udp -i $WAN3_IFACE --dport 53 -j ACCEPT
$IPTABLES -t FORWARD -p udp -i $WANS_IFACE --dport 53 -j ACCEPT
```

Then DNAT them to internal server

```
# Pass on allowed packets to 'real' servers inside DMZ using DNAT
#
$IPTABLES -t nat -A PREROUTING -p udp -i $LAN_IFACE --dport 59 -j DNAT --to 10.200.1.59
$IPTABLES -t nat -A PREROUTING -p tcp -i $LAN_IFACE --dport 25 -j DNAT --to 10.200.1.25
$IPTABLES -t nat -A PREROUTING -p tcp -i $LAN_IFACE --dport 220.197.62.160 -m multiport
  -dport 80,8000,8080,8081 -j DNAT --to 10.200.1.80
```

Finally, allow responses to go out with SNAT

```
# Access given to machines for DNS
#
$IPTABLES -t nat -A POSTROUTING -p udp -s 10.200.12.101 --dport 53 -o $WAN1_IFACE -j SNAT --to $WAN1_DNSIP
$IPTABLES -t nat -A POSTROUTING -p udp -s 10.200.12.101 --dport 53 -o $WAN2_IFACE -j SNAT --to $WAN2_DNSIP
$IPTABLES -t nat -A POSTROUTING -p udp -s 10.200.12.101 --dport 53 -o $WAN3_IFACE -j SNAT --to $WAN3_DNSIP
$IPTABLES -t nat -A POSTROUTING -p udp -s 10.200.12.101 --dport 53 -o $WANS_IFACE -j SNAT --to $WANS_DNSIP
```

Connection tracking is important!
<table>
<thead>
<tr>
<th>INFO</th>
<th>MX Record</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Your 2 MX records are:</td>
</tr>
<tr>
<td></td>
<td>5 mailrly1.iitb.ac.in. [TTL=43200] IP=203.197.62.141 [TTL=43200] [IN]</td>
</tr>
<tr>
<td></td>
<td>IP=203.197.74.141 [TTL=43200] [IN]</td>
</tr>
<tr>
<td></td>
<td>IP=203.199.51.141 [TTL=43200] [IN]</td>
</tr>
<tr>
<td></td>
<td>IP=203.199.81.141 [TTL=43200] [IN]</td>
</tr>
<tr>
<td></td>
<td>7 mailrly2.iitb.ac.in. [TTL=43200] IP=203.199.81.141 [TTL=43200] [IN]</td>
</tr>
<tr>
<td></td>
<td>IP=203.199.51.141 [TTL=43200] [IN]</td>
</tr>
<tr>
<td></td>
<td>IP=203.197.74.141 [TTL=43200] [IN]</td>
</tr>
<tr>
<td></td>
<td>IP=203.197.62.141 [TTL=43200] [IN]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PASS</th>
<th>Invalid characters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OK. All of your MX records appear to use valid hostnames, without any invalid characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PASS</th>
<th>All MX IPs public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OK. All of your MX records appear to use public IPs. If there were any private IPs, they would not be reachable, causing slight mail delays, extra resource usage, and possibly bounced mail.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PASS</th>
<th>MX records are not CNAMEs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OK. Looking up your MX record did not just return a CNAME. If an MX record returns a CNAME, extra processing is required, and some mail servers are not able to handle it.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PASS</th>
<th>MX A lookups have no CNAMEs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OK. There appear to be no CNAMEs returned for A records lookups from MX records (CNAMEs are prohibited in MX records, according to RFC974, RFC 3.6.2, RFC1912 2.4, and RFC2181 10.3).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PASS</th>
<th>MX is host name, not IP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OK. All of your MX records are host names (as opposed to IP addresses, which are not allowed in MX records).</td>
</tr>
</tbody>
</table>
### Open relay test

**PASS**

OK: All of your-mail servers appear to be closed to relaying. This is not a thorough check, you can get a thorough one [here](http://www.abuse.net/relay.html).

mail@i1.iitb.ac.in: OK: 553 sorry, that domain isn't in my list of allowed rcpt hosts (#5.7.1)

mail@i2.iitb.ac.in: OK: 553 sorry, that domain isn't in my list of allowed rcpt hosts (#5.7.1)

### SPF record

**PASS**

You have an SPF record. This is very good, as it will help prevent spammers from abusing your domain. Your SPF record is:

```
v=spf1 ptr asmxtp1.iitb.ac.in asmxtp2.iitb.ac.in -all [TTL=300]
```

### WWW Record

**INFO**

Your www.iitb.ac.in A record is:

- www.iitb.ac.in: A 203.199.61.160 [TTL=43200] [IN]
- www.iitb.ac.in: A 203.199.51.160 [TTL=43200] [IN]
- www.iitb.ac.in: A 203.197.74.160 [TTL=43200] [IN]
- www.iitb.ac.in: A 203.197.62.160 [TTL=43200] [IN]

### All WWW IPs public

**PASS**

OK. All of your WWW IPs appear to be public IPs. If there were any private IPs, they would not be reachable, causing problems reaching your web site.

---

**Open Relays:** [http://www.abuse.net/relay.html](http://www.abuse.net/relay.html)
Sender Policy Framework

http://spf.pobox.com/

SPF lookup of sender siva@iitb.ac.in from IP 128.175.7.4:

SPF string used: v=spf1 ptr a:smtp1.iitb.ac.in a:smtp2.iitb.ac.in ~all.

Processing SPF string: v=spf1 ptr a:smtp1.iitb.ac.in a:smtp2.iitb.ac.in ~all.
Testing 'ptr' on IP=128.175.7.4, target domain iitb.ac.in, CIDR 32, default=PASS. No match.
Testing 'a:smtp1.iitb.ac.in' on IP=128.175.7.4, target domain smtp1.iitb.ac.in, CIDR 32, default=PASS. No match.
Testing 'a:smtp2.iitb.ac.in' on IP=128.175.7.4, target domain smtp2.iitb.ac.in, CIDR 32, default=PASS. No match.
Testing 'all' on IP=128.175.7.4, target domain iitb.ac.in, CIDR 32, default=SOFTFAIL. MATCH!

Result: SOFTFAIL

Possible Results:

- **Pass** - This IP is authorized to send E-mail from this domain.
- **Fail** - This IP is not authorized to send E-mail from this domain.
- **SoftFail** - This IP probably is not authorized to send E-mail from this domain, but the domain does not know if the IP is allowed to send E-mail or not.
- **Neutral** - The domain does not know if the IP is allowed to send E-mail or not.
- **TempError** - A temporary error occurred. The E-mail should be retried later.
- **PermError** - A permanent error was encountered. The E-mail should be rejected.
- **None** - No SPF record was found. It cannot be determined if the IP is allowed to send E-mail.
Virtual Server as frontend. Real Servers as backend. Explanation by example.

# Ldirectord will periodically connect to each real server
# and request a known URL. If the data returned by the server
# does not contain the the expected response then the
# test fails and the real server will be taken out of the available
# pool. The real server will be added back into the pool once the
# test succeeds. If all real servers are removed from the pool then
# localhost is added to the pool as a fallback measure.
#
# Based on the sample ldirectord.cf provided with ldirectord
#
# Prepared: March 2003
#
# Global Directives
checktimeout=100
checkinterval=60
autoreload=yes
logfile="/var/log/ldirectord.log"
logfile="local0"
quiescent=yes

# Virtual Server for HTTP
virtual=203.197.74.160:80
    #fallback=127.0.0.1:80
    #real=203.197.74.161:80 gate
    #real=203.197.74.162:80 gate
real=10.209.4.1:80 masq 1
real=10.209.4.2:80 masq 1
service=http
# Virtual Server for SMTP
virtual=203.197.74.141:25
    #fallback=127.0.0.1:25
    real=10.209.3.1:25 masq 1
    real=10.209.3.2:25 masq 1
    service=smtp
    scheduler=wrr
    #persistent=300
    protocol=tcp
    checktype=connect

# Virtual UDP Server for DNS
virtual=203.197.74.159:53
    #fallback=127.0.0.1:53
    real=10.209.4.1:53 masq 1
    real=10.209.4.2:53 masq 1
    service=none
    scheduler=wrr
    #persistent=600
    protocol=udp
    checktype=on

# Virtual TCP Server for DNS
Load Balancing

[root@wum2 root]# ipvsadm -L -n
IP Virtual Server version 1.0.9 (size=65536)
Prot LocalAddress:Port Scheduler Flags
   -> RemoteAddress:Port         Forward  Weight ActiveConn InActConn
TCP  203.197.74.141:25 wrr
   -> 10.209.3.1:25             Masq 1 7  23
   -> 10.209.3.2:25             Masq 1 7  26
TCP  203.197.74.159:53 wrr
   -> 10.209.4.2:53             Masq 1 0  0  0
   -> 10.209.4.1:53             Masq 1 0  0  0
UDP  203.197.74.159:53 wrr
   -> 10.209.4.2:53             Masq 1 0 528
   -> 10.209.4.1:53             Masq 1 0 526
TCP  203.197.74.160:80 wrr persistent 600
   -> 10.209.4.2:80             Masq 1 8  57
   -> 10.209.4.1:80             Masq 1 11 68
Load Balancing

```
[root@wum2 root]# ipvsadm -L -n --stats
IP Virtual Server version 1.0.9 (size=65536)
Prot LocalAddress:Port Conns InPkts OutPkts InBytes OutBytes
        -> RemoteAddress:Port
TCP  203.197.74.141:25 314557 6310573 6306136 3546M 339093K
    -> 10.209.3.1:25    198754 4132343 4109182 2409M 220332K
    -> 10.209.3.2:25    122884 2423641 2422927 1345M 130739K
TCP  203.197.74.159:53  128  167  139   8832  5648
    -> 10.209.4.2:53     53   68   57   3604  2280
    -> 10.209.4.1:53     53   67   56   3580  2240
TCP  203.197.74.160:80 574628 13015422 17511823 1421M 19265M
    -> 10.209.4.2:80    294739  6719506 9086398  713645K  9935M
    -> 10.209.4.1:80    298984  6685160 8919697  813342K  9812M
UDP  203.197.74.159:53 1247665 5274880 408240  345279K  49825999
    -> 10.209.4.2:53   623895  2611849 203456  170972K  24839089
    -> 10.209.4.1:53   623889  2663297 204800  174324K  24988998
UDP  203.197.74.160:80 574628 13015422 17511823 1421M 19265M
    -> 10.209.4.2:80  294739  6719506 9086398  713645K  9935M
    -> 10.209.4.1:80  298984  6685160 8919697  813342K  9812M
```
```
[root@wum2 root]# ipvsadm -L -n --rate
IP Virtual Server version 1.0.9 (size=65536)

<table>
<thead>
<tr>
<th>Prot</th>
<th>LocalAddress:Port</th>
<th>CPS</th>
<th>InPPS</th>
<th>OutPPS</th>
<th>InBPS</th>
<th>OutBPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>203.197.74.141:25</td>
<td>1</td>
<td>11</td>
<td>11</td>
<td>4381</td>
<td>636</td>
</tr>
<tr>
<td></td>
<td>→ 10.209.3.1:25</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>883</td>
<td>291</td>
</tr>
<tr>
<td></td>
<td>→ 10.209.3.2:25</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>3498</td>
<td>345</td>
</tr>
<tr>
<td>TCP</td>
<td>203.197.74.159:53</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>→ 10.209.4.2:53</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>→ 10.209.4.1:53</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>UDP</td>
<td>203.197.74.159:53</td>
<td>4</td>
<td>12</td>
<td>1</td>
<td>776</td>
<td>136</td>
</tr>
<tr>
<td></td>
<td>→ 10.209.4.2:53</td>
<td>2</td>
<td>7</td>
<td>1</td>
<td>459</td>
<td>91</td>
</tr>
<tr>
<td></td>
<td>→ 10.209.4.1:53</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>317</td>
<td>45</td>
</tr>
<tr>
<td>TCP</td>
<td>203.197.74.160:80</td>
<td>1</td>
<td>16</td>
<td>19</td>
<td>1578</td>
<td>16232</td>
</tr>
<tr>
<td></td>
<td>→ 10.209.4.2:80</td>
<td>0</td>
<td>6</td>
<td>7</td>
<td>578</td>
<td>7386</td>
</tr>
<tr>
<td></td>
<td>→ 10.209.4.1:80</td>
<td>0</td>
<td>10</td>
<td>12</td>
<td>1000</td>
<td>8846</td>
</tr>
</tbody>
</table>
```
Outgoing Traffic via Ogarbo

Multiple **routing tables** available in *iproute2*.

```bash
### Custom Routing Tables

```
ip rule add prio 200 from 203.197.74.128/25 table 200  
ip route add default via 203.197.74.129 dev eth1 src 203.197.74.149  
proto static table 200

ip rule add default via 203.199.51.1 dev eth2 src 203.199.51.149  
proto static table 201

ip route add default via 203.199.51.1 dev eth2 src 203.199.51.200  
proto static table 201

ip route append default table 200 metric 1 proto static

ip rule add prio 201 from 203.199.61.0/24 table 201

ip route add default via 203.199.81.1 dev eth3 src 203.199.81.149  
proto static table 202

ip route add default via 203.199.81.1 dev eth3 src 203.199.81.200  
proto static table 202

ip route append default table 201 metric 1 proto static

ip rule add prio 202 from 203.199.61.0/24 table 202

ip route add default via 203.197.62.0/24 dev eth4 src 203.197.62.149  
proto static table 203

ip route add default via 203.197.62.1 dev eth4 src 203.197.62.200  
proto static table 203

ip route append default table 202 metric 1 proto static

ip rule add prio 203 from 203.197.62.0/24 table 203
```

```bash
#garbo1
```

```bash
ip rule add prio 222 table 222

ip route add default table 222 proto static nexthop via 203.197.74.129 dev eth1  
nexthop via 203.199.51.1 dev eth2  
nexthop via 203.199.81.1 dev eth3 weight 2  
nexthop via 203.197.62.1 dev eth4

ip route add 10.0.0.0/8 via 10.209.250.1 dev eth0
```
Use the netfilter machine as *default route*
It will decide what to allow, what to filter...

# *** Telnet
```
iptables -t nat -A POSTROUTING -p tcp
   -s 10.0.0.0/8 --dport 23 -j SNAT --to $IP1
```

# *** MSN
```
iptables -t nat -A POSTROUTING -p tcp
   -s 10.0.0.0/8 --dport 1863 -j SNAT --to $IP1
```

# *** Yahoo, SciFinder, ssh, telnet
Web Browsing
Squid Features

- Authentication and Filtering at Layer 1
- Caching and Ad-blocking and Bandwidth shaping at Layer 2
- Several load balancing controls available
  - Journal sites and good sites via fast link!
  - zebra, ripd for link failure tolerance!
Shaping the Traffic

Use **tc** (traffic control) in Linux Kernel. Different types of traffic such as web, mail, ssh and so on. We want to make sure that any particular traffic does not dominate our WAN link so we need to limit rate for different types of traffic. This can be achieved as follows:

1. select a base queueing discipline that we want to use.
2. create classes for different types of traffic that we want to shape.
3. create filters to classify different types of traffic
Hierarchical Token Bucket (HTB) queuing discipline

tc qdisc add dev eth0 root handle 1: htb default 15

## CEIL = 75% of your upstream bandwidth

tc class add dev eth0 parent 1: classid 1:1 htb rate ${CEIL}mbit ceil ${CEIL}mbit
tc class add dev eth0 parent 1:1 classid 1:10 htb rate 0.8mbit ceil 0.8mbit prio 0
tc class add dev eth0 parent 1:1 classid 1:11 htb rate 0.8mbit ceil ${CEIL}mbit prio 1
tc class add dev eth0 parent 1:1 classid 1:12
    htb rate 0.2mbit ceil ${CEIL}mbit prio 2

We have just created a htb tree with one level depth.

+---------+
| root 1: |
+---------+
     |
+-----------------------+
| class 1:1 |
+-----------------------+
    |
      +---+ +---+ +---+
     |1:10| |1:11| |1:12|
    +---+ +---+ +---+
Now Mangle Packets

```bash
## Http packets
iptables -t mangle -A PREROUTING
   -p tcp --dport 80 -j MARK --set-mark 0x2

## Mail packets
iptables -t mangle -A PREROUTING
   -p tcp --dport 25 -j MARK --set-mark 0x3

## ssh packets
iptables -t mangle -A PREROUTING
   -p tcp -m tcp --sport 22 -j MARK --set-mark 0x1
```

and queue accordingly!

Above is quite simplistic. Complex variations with dynamic shaping is possible.
Network, Services and User Management

Eternal vigilance is the price of liberty!

- How is network doing?
- Are all services up?
- How much email in/out? How many viruses?
- Who’s using Web proxy? For what?
- Are User’s happy?

www.gnu.org/software/gnats
IITB WAN Links

Traffic Analysis for 203.197.31.153 -- router-vsnnl-radio.iitb.ac.in

Traffic Analysis for 203.199.44.101 -- router-vsnnl-ll.iitb.ac.in

Traffic Analysis for 202.68.142.226 -- proxy-bses-ll
Performace of Link to Hostel 5.
### Status Summary For All Host Groups

<table>
<thead>
<tr>
<th>Host Group</th>
<th>Host Status</th>
<th>Service Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVAYA switches (backbone-switches)</td>
<td>7 U</td>
<td>7 OK</td>
</tr>
<tr>
<td>Cisco Routers (cisco-routers)</td>
<td>3 U</td>
<td>1 OK</td>
</tr>
<tr>
<td>Department Caching DNS servers (dept-dns-servers)</td>
<td>2 U</td>
<td>1 OK</td>
</tr>
<tr>
<td>DNS Servers (dns-servers)</td>
<td>4 U</td>
<td>12 OK</td>
</tr>
<tr>
<td>DNSSCACHE Servers (dnscache-servers)</td>
<td>5 U</td>
<td>5 OK</td>
</tr>
<tr>
<td>FTP servers (ftp-servers)</td>
<td>1 U</td>
<td>1 OK</td>
</tr>
<tr>
<td>NAT boxes (gnos-boxes)</td>
<td>4 U</td>
<td>1 OK</td>
</tr>
<tr>
<td>LDAF servers (ldap-servers)</td>
<td>2 U</td>
<td>1 OK</td>
</tr>
<tr>
<td>Mail servers (mail-servers)</td>
<td>9 U</td>
<td>25 OK</td>
</tr>
<tr>
<td>met.iitb.ac.in servers (met-servers)</td>
<td>2 U</td>
<td>10 OK</td>
</tr>
<tr>
<td>News servers (news-servers)</td>
<td>2 U</td>
<td>5 OK</td>
</tr>
<tr>
<td>Proxy servers (proxy-servers)</td>
<td>3 U</td>
<td>10 OK</td>
</tr>
<tr>
<td>RESNET Embedded Servers (resnet-pico-servers)</td>
<td>40 U</td>
<td>14 OK</td>
</tr>
<tr>
<td>RESNET Web Servers (resnet-web-servers)</td>
<td>8 U</td>
<td>2 CRITICAL</td>
</tr>
<tr>
<td>Web servers (web-servers)</td>
<td>2 U</td>
<td>1 OK</td>
</tr>
<tr>
<td>WINS servers (wins-servers)</td>
<td>1 U</td>
<td>1 OK</td>
</tr>
</tbody>
</table>
## Mail Usage Statistics

### Email Logs for January 2003

<table>
<thead>
<tr>
<th>Date</th>
<th>Incoming</th>
<th></th>
<th>Outgoing</th>
<th></th>
<th>Top 25</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Count (K) Size (MB)</td>
<td>Count (K) Size (MB)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>34</td>
<td>534</td>
<td>17</td>
<td>451</td>
<td>Top 25</td>
</tr>
<tr>
<td>2</td>
<td>33</td>
<td>548</td>
<td>12</td>
<td>381</td>
<td>Top 25</td>
</tr>
<tr>
<td>3</td>
<td>33</td>
<td>522</td>
<td>11</td>
<td>373</td>
<td>Top 25</td>
</tr>
<tr>
<td>4</td>
<td>27</td>
<td>373</td>
<td>8</td>
<td>259</td>
<td>Top 25</td>
</tr>
<tr>
<td>5</td>
<td>21</td>
<td>255</td>
<td>6</td>
<td>154</td>
<td>Top 25</td>
</tr>
<tr>
<td>6</td>
<td>33</td>
<td>463</td>
<td>13</td>
<td>345</td>
<td>Top 25</td>
</tr>
<tr>
<td>7</td>
<td>36</td>
<td>495</td>
<td>14</td>
<td>375</td>
<td>Top 25</td>
</tr>
<tr>
<td>8</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>79</td>
<td>1140</td>
<td>24</td>
<td>800</td>
<td>Top 25</td>
</tr>
<tr>
<td>10</td>
<td>38</td>
<td>672</td>
<td>12</td>
<td>463</td>
<td>Top 25</td>
</tr>
<tr>
<td>11</td>
<td>28</td>
<td>376</td>
<td>6</td>
<td>273</td>
<td>Top 25</td>
</tr>
<tr>
<td>12</td>
<td>23</td>
<td>257</td>
<td>5</td>
<td>198</td>
<td>Top 25</td>
</tr>
<tr>
<td>13</td>
<td>39</td>
<td>813</td>
<td>25</td>
<td>429</td>
<td>Top 25</td>
</tr>
<tr>
<td>14</td>
<td>41</td>
<td>615</td>
<td>12</td>
<td>318</td>
<td>Top 25</td>
</tr>
<tr>
<td>15</td>
<td>38</td>
<td>743</td>
<td>12</td>
<td>419</td>
<td>Top 25</td>
</tr>
<tr>
<td>16</td>
<td>39</td>
<td>518</td>
<td>12</td>
<td>254</td>
<td>Top 25</td>
</tr>
<tr>
<td>17</td>
<td>38</td>
<td>516</td>
<td>12</td>
<td>372</td>
<td>Top 25</td>
</tr>
<tr>
<td>18</td>
<td>31</td>
<td>394</td>
<td>9</td>
<td>254</td>
<td>Top 25</td>
</tr>
<tr>
<td>19</td>
<td>24</td>
<td>314</td>
<td>8</td>
<td>281</td>
<td>Top 25</td>
</tr>
<tr>
<td>20</td>
<td>31</td>
<td>453</td>
<td>13</td>
<td>576</td>
<td>Top 25</td>
</tr>
<tr>
<td>21</td>
<td>39</td>
<td>673</td>
<td>23</td>
<td>450</td>
<td>Top 25</td>
</tr>
<tr>
<td>22</td>
<td>40</td>
<td>560</td>
<td>12</td>
<td>425</td>
<td>Top 25</td>
</tr>
</tbody>
</table>
# Mail Usage Statistics

## Email Logs for January 23, 2003

<table>
<thead>
<tr>
<th>No</th>
<th>Count</th>
<th>Size</th>
<th>Email</th>
<th>Count</th>
<th>Size</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>162</td>
<td>675771</td>
<td>upadhyay@me</td>
<td>12</td>
<td>14932933</td>
<td>hvs@it</td>
</tr>
<tr>
<td>2</td>
<td>147</td>
<td>1104446</td>
<td>bhati@cse</td>
<td>32</td>
<td>13523092</td>
<td>krithi@cse</td>
</tr>
<tr>
<td>3</td>
<td>137</td>
<td>1079126</td>
<td>n9511012@ccs</td>
<td>4</td>
<td>10061910</td>
<td>amitgangrade@iitb</td>
</tr>
<tr>
<td>4</td>
<td>125</td>
<td>673293</td>
<td>ranoo@ee</td>
<td>18</td>
<td>6854607</td>
<td>sudarsha@cse</td>
</tr>
<tr>
<td>5</td>
<td>125</td>
<td>1051961</td>
<td>n8002025@ccs</td>
<td>11</td>
<td>6434209</td>
<td>kulkarni@admin</td>
</tr>
<tr>
<td>6</td>
<td>121</td>
<td>894408</td>
<td>agarg@me</td>
<td>8</td>
<td>6415804</td>
<td>aknur@admin</td>
</tr>
<tr>
<td>7</td>
<td>121</td>
<td>1144970</td>
<td>kadam7ue@ccs</td>
<td>3</td>
<td>6390252</td>
<td>jadhav@admin</td>
</tr>
<tr>
<td>8</td>
<td>117</td>
<td>935533</td>
<td>raieev@me</td>
<td>6</td>
<td>5968048</td>
<td>gaur@som</td>
</tr>
<tr>
<td>9</td>
<td>114</td>
<td>902665</td>
<td>sach7ue@ccs</td>
<td>12</td>
<td>5546487</td>
<td>sudarsha@cse</td>
</tr>
<tr>
<td>10</td>
<td>110</td>
<td>782916</td>
<td>jaywant@cse</td>
<td>16</td>
<td>4986539</td>
<td>vikram@met</td>
</tr>
<tr>
<td>11</td>
<td>109</td>
<td>822038</td>
<td>pyush7dl@ccs</td>
<td>10</td>
<td>44448193</td>
<td>subodh@che</td>
</tr>
<tr>
<td>12</td>
<td>106</td>
<td>781754</td>
<td>mtpor8poc@ccs</td>
<td>1</td>
<td>4391040</td>
<td>gzezala@cc</td>
</tr>
<tr>
<td>13</td>
<td>106</td>
<td>772337</td>
<td>ac_pradhan@idc</td>
<td>1</td>
<td>4391040</td>
<td>bmaru@888888</td>
</tr>
<tr>
<td>14</td>
<td>104</td>
<td>1489373</td>
<td>gracas@cse</td>
<td>11</td>
<td>4249557</td>
<td>kapli@me</td>
</tr>
<tr>
<td>15</td>
<td>99</td>
<td>723276</td>
<td>n9512009@ccs</td>
<td>2</td>
<td>4054800</td>
<td>ashpurik@cse</td>
</tr>
<tr>
<td>16</td>
<td>98</td>
<td>771955</td>
<td>n8420210@ccs</td>
<td>1</td>
<td>3725463</td>
<td>felix0us@iitb</td>
</tr>
<tr>
<td>17</td>
<td>98</td>
<td>765575</td>
<td>n8004021@ccs</td>
<td>3</td>
<td>3706312</td>
<td>harshad@it</td>
</tr>
<tr>
<td>18</td>
<td>97</td>
<td>687013</td>
<td>punee@me</td>
<td>1</td>
<td>3606614</td>
<td>shubha@cse</td>
</tr>
<tr>
<td>19</td>
<td>95</td>
<td>394031</td>
<td>shivaji@ee</td>
<td>5</td>
<td>3100016</td>
<td>sri@ee</td>
</tr>
<tr>
<td>20</td>
<td>95</td>
<td>1260585</td>
<td>lakshmi@cse</td>
<td>7</td>
<td>3058951</td>
<td>sudhakar@aero</td>
</tr>
<tr>
<td>21</td>
<td>94</td>
<td>577376</td>
<td>ganeshk@ee</td>
<td>12</td>
<td>3030999</td>
<td>dbp@it</td>
</tr>
<tr>
<td>22</td>
<td>93</td>
<td>660940</td>
<td>bhure@me</td>
<td>2</td>
<td>2925456</td>
<td>z2004014@online</td>
</tr>
<tr>
<td>23</td>
<td>93</td>
<td>576049</td>
<td>m1ssyyad@civil</td>
<td>9</td>
<td>2774134</td>
<td>mvnhalgi@che</td>
</tr>
<tr>
<td>24</td>
<td>93</td>
<td>575850</td>
<td>muralikrishna@iitb</td>
<td>2</td>
<td>2765009</td>
<td>ss@iitb</td>
</tr>
<tr>
<td>25</td>
<td>93</td>
<td>574548</td>
<td>prasad@iitb</td>
<td>12</td>
<td>2658090</td>
<td>rsven@ee</td>
</tr>
</tbody>
</table>
Health check for ldnsl

Thu Feb  3 18:28:00 IST 2005

Disk space Occupancy

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>1K-blocks</th>
<th>Used</th>
<th>Available</th>
<th>Use%</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hda1</td>
<td>2016316</td>
<td>601592</td>
<td>1312012</td>
<td>32%</td>
<td>/</td>
</tr>
<tr>
<td>none</td>
<td>1970414</td>
<td>0</td>
<td>1970414</td>
<td>0%</td>
<td>/dev/shm</td>
</tr>
<tr>
<td>/dev/hda3</td>
<td>4082124</td>
<td>1370244</td>
<td>2457052</td>
<td>38%</td>
<td>/usr</td>
</tr>
<tr>
<td>/dev/hda5</td>
<td>34265792</td>
<td>637548</td>
<td>3186744</td>
<td>2%</td>
<td>/var</td>
</tr>
<tr>
<td>/dev/hda6</td>
<td>34599976</td>
<td>1129844</td>
<td>31700028</td>
<td>4%</td>
<td>/home</td>
</tr>
</tbody>
</table>

Memory Usage

```
Mem:                  3944800          3742492          198168
-/+ buffers/cache:    2538886          1401912
Swap:                 2048276          0
```

Routing Table

```
10.200.0.0/18 dev eth0 scope link
127.0.0.0/8 dev lo scope link
default via 10.200.250.1 dev eth0
```

QMAIL Status

```
/service/qmail: up (pid 27924) 17279 seconds
/service/qmail/log: up (pid 1259) 1823829 seconds
/service/qmail: up (pid 27920) 17279 seconds
/service/qmail/log: up (pid 1269) 1823829 seconds
messages in queue: 3
messages in queue but not yet preprocessed: 0
```

Recipient for pending Mail are in the following domains:

1mitra.iitb.ac.in
1cse.iitb.ac.in
1cece.iitb.ac.in

Results of last 20 mail delivery successes:

```
```
Mail Server Statistics

Mail stats since: Nov 22 04:02:07
Total mail scanned: **2790643**
Total viruses stopped: **339817**
Total spam found: **270**
Spam percentage: **0.01**
Page last generated: Thu Feb 3 12:48:19 2005
Scan starts every 5 minutes.

**TOP 10 viruses**
- Worm.SomeFool.P : 7897
- Worm.Zafi.D : 2893
- Trojan.Downloader.Small-165 : 483
- Worm.SomeFool.AA-2 : 272
- Disallowed characters found in MIME headers : 221
- Worm.Lovgate.X : 150
- Worm.Mydoom.Gen-unp : 144
- Disallowed breakage found in header name - potential virus : 139
- HTML.Phishing.Bank-1 : 138
- Worm.SomeFool.Gen-1 : 134

---

**qmail scanner statistics**

**qmail sstats (daily)**

**qmail sstats (weekly)**

---

G. Sivakumar
Computer Science and Engineering  IIT Bombay  siva@iitb.ac.in

Network Security- Part 2
## Web Proxy Usage

### Top 10 of 2768 Total Sites By KBytes

<table>
<thead>
<tr>
<th>#</th>
<th>Hits</th>
<th>Files</th>
<th>KBytes</th>
<th>Visits</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2300204</td>
<td>1954967</td>
<td>9000096</td>
<td>35</td>
<td>sunfire.ccc.iitb.ac.in</td>
</tr>
<tr>
<td>2</td>
<td>49016</td>
<td>20856</td>
<td>5061216</td>
<td>84</td>
<td>10.41.39</td>
</tr>
<tr>
<td>3</td>
<td>54586</td>
<td>24700</td>
<td>4878457</td>
<td>76</td>
<td>10.9.3.91</td>
</tr>
<tr>
<td>4</td>
<td>1487299</td>
<td>12892</td>
<td>2680488</td>
<td>108</td>
<td>10.9.3.82</td>
</tr>
<tr>
<td>5</td>
<td>18507</td>
<td>12992</td>
<td>2483622</td>
<td>92</td>
<td>broiapower.it.iitb.ac.in</td>
</tr>
<tr>
<td>6</td>
<td>49110</td>
<td>34427</td>
<td>2446135</td>
<td>50</td>
<td>10.11.89</td>
</tr>
<tr>
<td>7</td>
<td>1322118</td>
<td>11660</td>
<td>2421988</td>
<td>95</td>
<td>10.2.1.91</td>
</tr>
<tr>
<td>8</td>
<td>23451</td>
<td>11526</td>
<td>2229159</td>
<td>68</td>
<td>masterspace.iitb.ac.in</td>
</tr>
<tr>
<td>9</td>
<td>32531</td>
<td>18997</td>
<td>2184972</td>
<td>122</td>
<td>10.7.26.61</td>
</tr>
<tr>
<td>10</td>
<td>24981</td>
<td>12278</td>
<td>2173792</td>
<td>108</td>
<td>10.2.2.30</td>
</tr>
</tbody>
</table>

### Top 50 of 3498 Total Usernames

<table>
<thead>
<tr>
<th>#</th>
<th>Hits</th>
<th>Files</th>
<th>KBytes</th>
<th>Visits</th>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>130008</td>
<td>129383</td>
<td>451413</td>
<td>35</td>
<td>macmca</td>
</tr>
<tr>
<td>2</td>
<td>107859</td>
<td>65692</td>
<td>241420</td>
<td>62</td>
<td>bhupelpp</td>
</tr>
<tr>
<td>3</td>
<td>106038</td>
<td>45537</td>
<td>362243</td>
<td>83</td>
<td>atishGun</td>
</tr>
<tr>
<td>4</td>
<td>95258</td>
<td>44446</td>
<td>242074</td>
<td>49</td>
<td>pujulog17</td>
</tr>
<tr>
<td>5</td>
<td>82716</td>
<td>49001</td>
<td>513423</td>
<td>131</td>
<td>deepsh_singh</td>
</tr>
<tr>
<td>6</td>
<td>78798</td>
<td>55019</td>
<td>319427</td>
<td>77</td>
<td>loversofmaths</td>
</tr>
<tr>
<td>7</td>
<td>73376</td>
<td>31508</td>
<td>402674</td>
<td>86</td>
<td>mitulah</td>
</tr>
<tr>
<td>8</td>
<td>71457</td>
<td>52494</td>
<td>596424</td>
<td>114</td>
<td>gaganakal</td>
</tr>
<tr>
<td>9</td>
<td>70301</td>
<td>59964</td>
<td>268065</td>
<td>85</td>
<td>kvaroon</td>
</tr>
<tr>
<td>10</td>
<td>69064</td>
<td>23446</td>
<td>205399</td>
<td>80</td>
<td>kkanya</td>
</tr>
<tr>
<td>11</td>
<td>67278</td>
<td>39453</td>
<td>519232</td>
<td>127</td>
<td>kartikgupta</td>
</tr>
<tr>
<td>12</td>
<td>65738</td>
<td>43688</td>
<td>885925</td>
<td>86</td>
<td>san_munde</td>
</tr>
</tbody>
</table>
Web Server Hits

Summary by Month

<table>
<thead>
<tr>
<th>Month</th>
<th>Daily Avg</th>
<th>Monthly Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hits</td>
<td>Files</td>
</tr>
<tr>
<td>Feb 2003</td>
<td>13483</td>
<td>9488</td>
</tr>
<tr>
<td>Jan 2003</td>
<td>13789</td>
<td>11260</td>
</tr>
<tr>
<td>Dec 2002</td>
<td>17121</td>
<td>10661</td>
</tr>
<tr>
<td>Nov 2002</td>
<td>16729</td>
<td>10952</td>
</tr>
<tr>
<td>Totals</td>
<td>3279665</td>
<td>112751</td>
</tr>
</tbody>
</table>
Putting it all together

Using **free** tools, one can achieve all the following.

- Security (Firewall)
- Harnessing Multiple WAN links seamlessly
- Shaping the traffic for each application reliably
- Achieving reliability using virtual services

Challenging, but exciting job.

**Swatantra** Software. Resource Centre. (OSSRC)