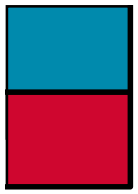
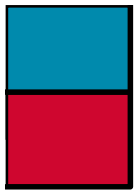
Linux IP Masquerading

Brian Vargyas
XNet Information Systems



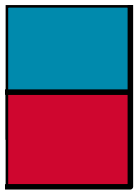
Agenda

- What is IP Masquerade
- How does it work
- Example
- Setting Up IP Masquerade
- References



What not to expect

- Teaching you how to set up Redhat Linux 5.1
- How to compile and install a new kernel

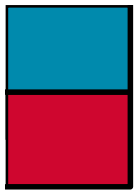


Why is IP Masquerading HOT?

- **Demand to share a single Internet address across multiple machines.**
- **Demand to save Internet IPv4 address space.**
- **Demand for better internal network security.**

Emerging Applications

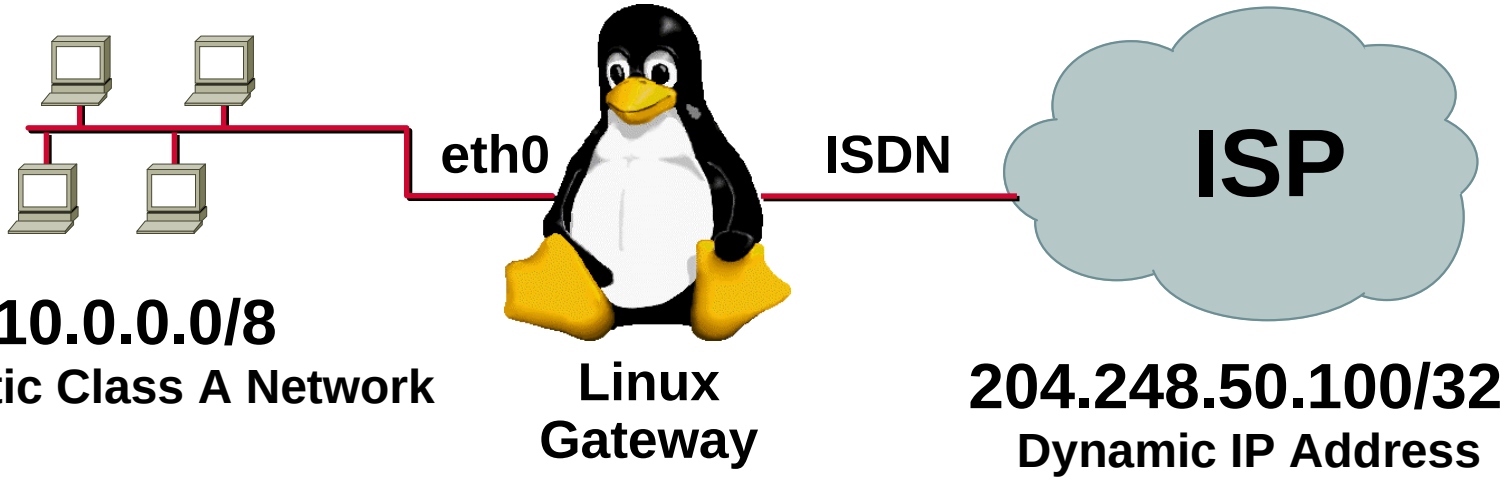
- Network Hiding
- Cable Modem Solutions
- xDSL Solutions
- Dial on Demand Internet

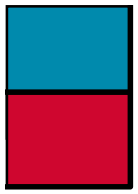


So what is it?

- A Developing networking function built in to RedHat Linux 5.1
- Allows machines connected to the Linux system to access the Internet as if they were coming from a single IP address.
- Provides a secure way of hiding internal networks.

A Simple Setup



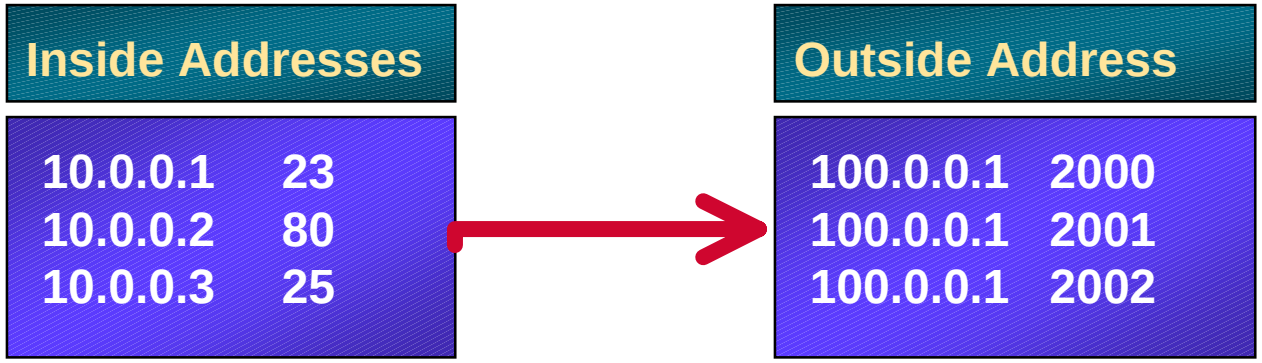


How it works

- **Translation Tables Manage Inside to Outside Address Translation**
- **IPFWADM (IP Firewall Administration)**
- **IPPORTFW (IP Port Forwarding)**
- **Loadable kernel modules for special IP services like FTP, IRC, QUAKE.**

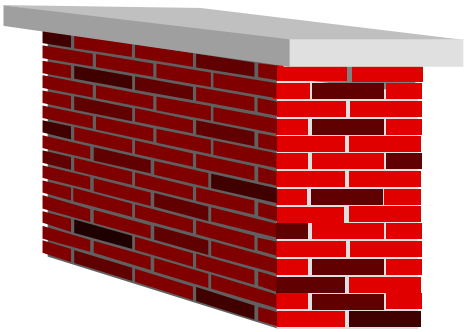
IP Translation Tables

- **Maintains IP Address Source/Dest. Port Pairs.**
- **Pool of 4096 Ports.**

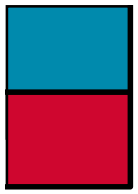


Address / Dest. Port Pairs **Address / Source Port Pairs**

IPFWADM (Firewall)

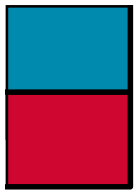


- **Manages Permit/Deny Firewall Access Lists**
- **Controls which networks are allowed to IP Masquerade**
- **Deny access to all other networks.**



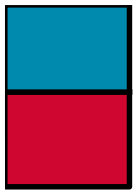
IPPORTFW (Port Forwarding)

- Controls mapping of incoming port requests to a inside address.
- Lets you run mail/web server on another host inside your network.
- Provides complete flexibility on where to place IP services.
- Not included in standard Redhat 5 distribution.



Loadable Kernel Modules

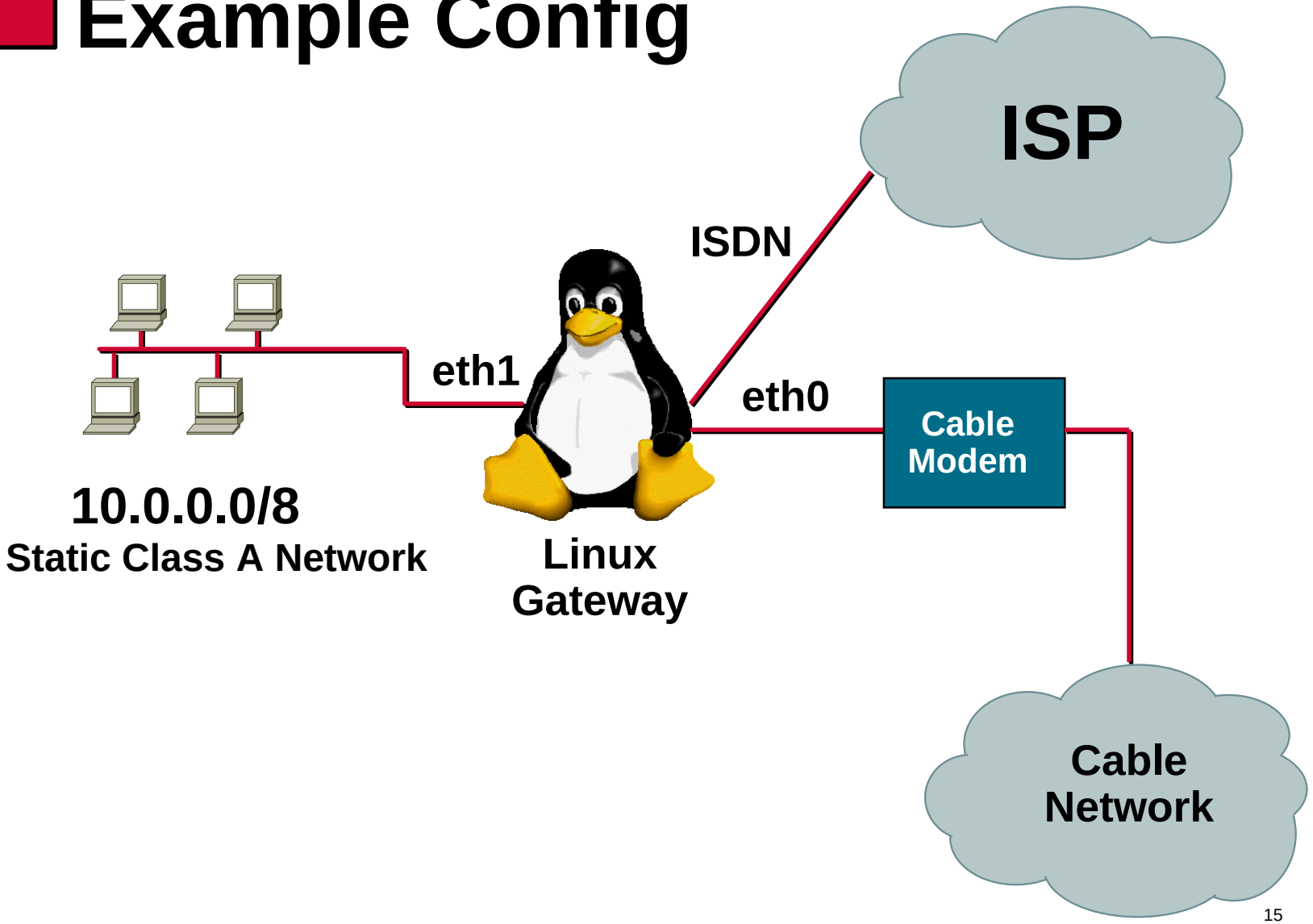
- Lets special IP services such as FTP operate correctly. I.E. Back Channel Data (Not Passive).
- Only loads into memory if needed
- Some services not supported.
- PPTP Patches.

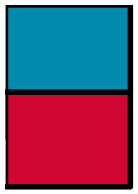


Example (My Home)

- 3 Machines needs Internet access
- 1 DHCP dynamic address provided from Cable Company.
- Backup ISDN dialup
- Windows NT web/mail server

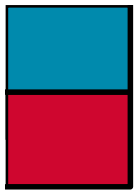
Example Config





Setup Procedure

- **Configure all system interfaces. Make sure you can ping remote machines. Verify connectivity to your ISP is working.**
- **Install IPPORTFW Kernel Patches, Rebuilt Kernel, Install and Reboot. (Kernel 2.0.33/2.0.34) Compile IPPORTFW utility and install in /bin.**
- **Edit your /etc/rc.d/rc2.d/S99local file and include the necessary IPFWADM and IPPORTFW configuration.**
- **Make sure you have a default route (0.0.0.0/0) pointed at your ISP Interface.**



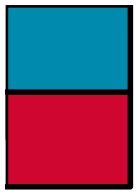
Setup Configuration (S99local)

```
# S99local
echo "1" > /proc/sys/net/ipv4/ip_forwarding

/sbin/ipfwadm -F -p deny
/sbin/ipfwadm -F -a m -S 10.0.0.0/24 -D 0.0.0.0/0

/sbin/ipportfw -A -t 24.131.169.80/80 -R 10.0.0.3/80
/sbin/ipportfw -A -t 24.131.169.80/25 -R 10.0.0.3/25

route add default 24.131.169.1
```



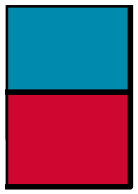
Verify Configuration

```
[root@bv-gw /]# netstat -M
IP masquerading entries, free ports: UDP 4095  TCP 4096
prot   expire source              destination          ports
udp   4:52.95 10.0.0.3            204.91.243.41        1085 -> 4000 (61058)

[root@bv-gw /]# ipfwadm -F -l
IP firewall forward rules, default policy: deny
type  prot source               destination          ports
acc/m all  10.0.0.0/24          anywhere             n/a

[root@bv-gw /]# ipportfw -L
Prot Local Addr/Port > Remote Addr/Port

TCP 24.131.169.80/25 > 10.0.0.3/25
TCP 24.131.169.80/80 > 10.0.0.3/80
```

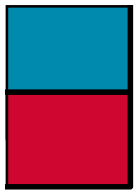


Problems

- **Not every IP protocol works**
- **Difficult to run web/mail when you have a DHCP address that keeps changing.**
- **DNS needs to be hosted by ISP**

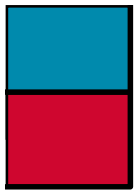
Private IP Address Space (RFC 1918)

- **Must use following address space for internal networks:**
- **10.0.0.0/8 255.0.0.0**
- **172.16.0.0/12 255.240.0.0**
- **192.168.0.0/16 255.255.0.0**



Illegal Address Space Issues

- Problems getting to the network being used. (DNS Related Issues)
- Need to use another vendor implementation to solve problem
- IP NAT Overlapping (CISCO)



References

- **IP Masquerade Web Page**
  `http://ipmasq.home.ml.org/`
- **Port Forwarding Web Page**
  `http://www.ox.compsoc.org.uk/~steve/portforwarding.html`
- **My Web Page**
  `http://www.xnet.com/~brianv`