Xicada.net

Building the ultimate private network

Derek Konigsberg

octo@logicprobe.org

A project originated among students in ACM/SIG-Networking at

Rensselaer Polytechnic Institute

Introduction

- Casually experimenting with large-scale networks isn't easy
- The networks we're connected to are usually owned by other people
  - Internet Service Providers
  - Universities (i.e. UCF)
  - Corporations

Problems with ISPs

- Limited IP address availability
  - Network Address Translation (NAT)
  - Everyone is forced to use conflicting ranges of private IPs
- Limited upstream bandwidth
- Firewalls
- Essentially, the Internet is cumbersome for networking with your peers, as ISPs basically treat your machines as client-only parts of the network.

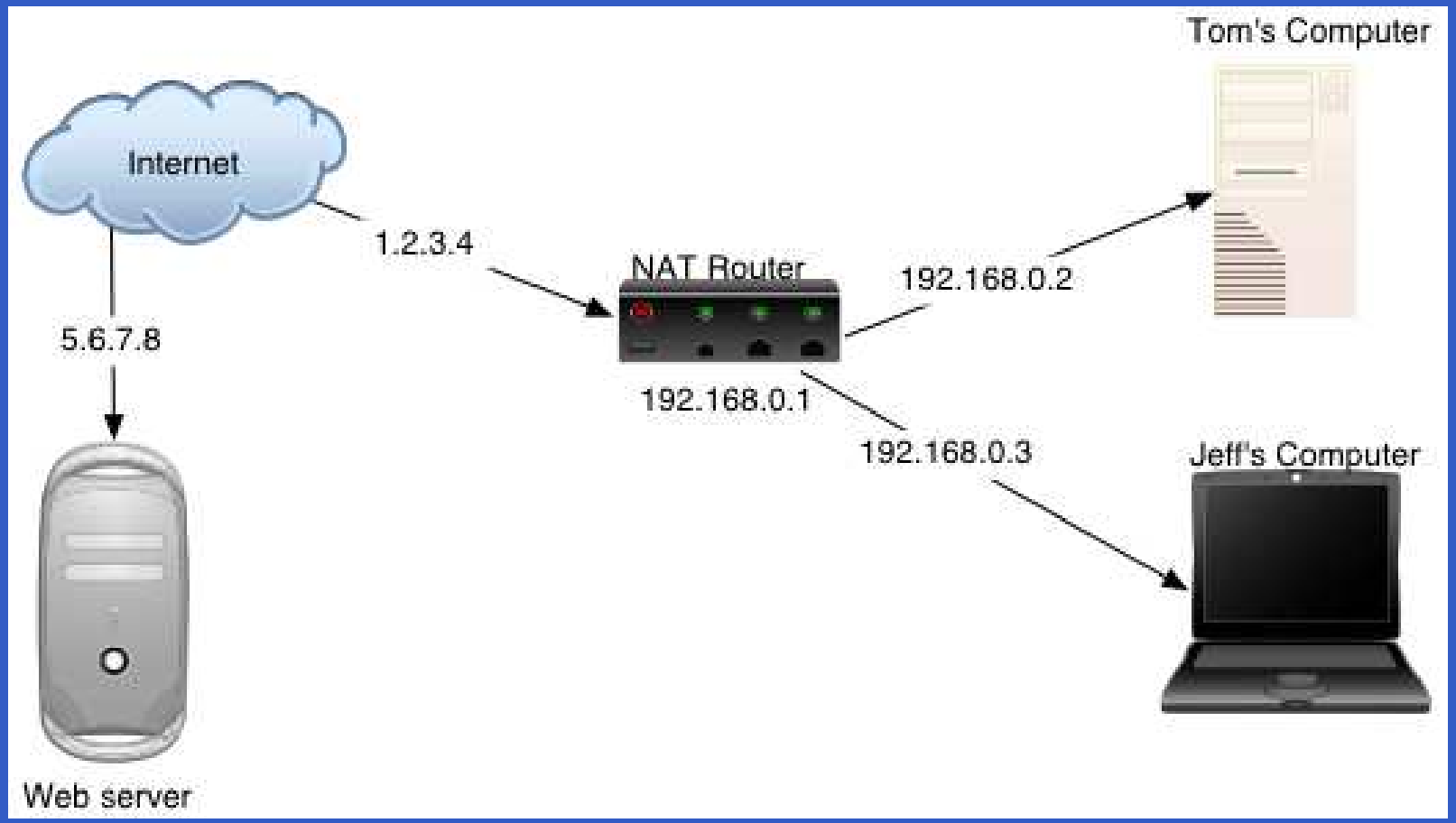
NAT: What is it?

- Network Address Translation is essentially a hack
- It allows you to connect multiple computers to the internet while only using a single IP address
- NAT works by keeping a translation table, which tracks of all the connections between your computers and other computers on the internet

TCP/IP and Ports

- When you connect to a machine on the internet, you have a source port and a destination port.
- Having a unique source port for each connection on your end allows you to make multiple independent connections to a server.
- Having well-known destination ports on the remote server allows you to explicitly connect to different services
  - Port 80 - HTTP (web server)
  - Port 22 - SSH (secure shell server)

NAT: A typical home network



Where do private IPs come from?

- Three ranges of IP addresses have been designated specifically for private use and are not routable on the global internet.
  - 10.0.0.0 - 10.255.255.255
  - 172.16.0.0 - 172.31.255.255
  - 192.168.0.0 - 192.168.255.255

NAT: How does it work?

- In a hypothetical situation, both Tom and Jeff want to connect to the same web server.
- The NAT software then creates a mapping table

Local	Internet	Remote
192.168.0.2:42000	1.2.3.4:36001	5.6.7.8:80
192.168.0.3:42000	1.2.3.4:36002	5.6.7.8:80

NAT: Summary

- A dynamically created table is used to translate addresses and ports within packets traveling between internal computers and servers on the internet
- It is also possible to manually create entries in the table so people elsewhere on the internet can connect to servers within your network.
- However, when using standard ports, you can only make one server of each type visible to the internet.

How do we fix this?

- Let's build our own network!
  - Private IP space will be delegated to avoid conflicts
- We'll build it on top of and around existing infrastructure using:
  - Secure network tunnels
  - Point-to-point wireless
- Routing will be managed dynamically

Delegated IP space

- We use IPs that are private to the whole project, instead of just private to one person's network.
- Chunks of the 10.0.0.0/8 network range are delegated to each site
- Effectively, each site is merely a subnet of the greater project network
  - 10.1.1.0/24 - Bithose
  - 10.4.1.0/24 - Logicprobe
  - etc.

Network tunneling

- Creates a virtual permanent connection between two machines on the internet
- Allows these two machines to behave as if they were directly connected
- Simulates an additional network interface on each end
- Traffic on these tunnels can be encrypted for security
- Tunnels form the foundation on which Xicada is built

Dynamic routing

- Building a full-mesh network of tunnels is too hard and impractical
- Configuring static network routes is also too hard and impractical
- Dynamic routing allows everyone's routers to talk to each other, and figure out their routing tables all by themselves.
- We do this with a protocol called OSPF (Open Shortest Path First)

What do I need to join the network?

- An internet connection with a functionally static IP address
- Optional: Wireless line-of-sight to another participant
- A computer to function as a router on the edge of your network
  - Needs two network interface cards
  - Should run an OS such as: OpenBSD, FreeBSD, Linux
  - Could also use a real router (i.e. Cisco) capable of OSPF and IPSec

How else can I help out?

- Project documentation
- Network configuration management
- Figuring out network setups
- Infrastructure services (DNS, search engines, etc.)
- Applications (distributed filesystems, VoIP, etc.)

Questions? Comments?

If interested, please e-mail me at:
octo@logicprobe.org

For scattered project notes and mailing list archives:
`http://www.xicada.net`

Slides produced with Prosper and LaTeX
`http://prosper.sourceforge.net`