

RPI/ACM Network Overview

Mark Kamichoff prox@prolixium.com

[http://www.prolixium.com/files/rpinet.\[ppt/pdf\]](http://www.prolixium.com/files/rpinet.[ppt/pdf])

Some Statistics

- ▶ Network “connections” on campus: 15,840
- ▶ Internet traffic: 116,645 GB/semester
 - Up 2% from FY 2002 (113,948 GB/semester)
- ▶ Internet2 traffic: 25,323 GB/semester
 - Up 21% from FY 2002 (20,936 GB/semester)

Internet Service Providers

- ▶ Primary ISP – Broadwing Communications
 - OC3 (155Mbit)
 - Previously AppliedTheory
 - ▶ Chapter 11, bought by FASTNET and ClearBlue
- ▶ I2 ISP – NYSERNet – New York State Educational Network
 - OC3 (155Mbit)
- ▶ Link to Rensselaer Hartford Graduate Center

Address Space

▶ IPv4 (AS 91: RPI-AS)

- 128.113.0.0/16 – RPI Campus
 - ▶ (/16: 65536 addresses)
- 128.213.0.0/16 – Computer Science Network
- 205.232.210.0/24 – Troy High School

▶ IPv6

- 2001:468:903::/48 – Computer Science Network
 - ▶ Delegated via NYSERNet's 2001:468:900::/40 address block
 - ▶ (/48: 1208925819614629174706176 addresses)

Firewalling

- ▶ RESNet/CoreNet
 - Selective blocking of new incoming TCP/UDP connections
 - Blocking all non-[TCP/UDP/ICMP] protocols
 - ▶ Ex: No IPSec/GRE/IPIP, etc
 - ICMP Ratelimiting/Blocking
 - ▶ Temporary, due to Nachi/Welchia worm

Firewalling (cont.)

▶ TCP

- No completely “open” ports
- Proxied TCP ports (partially open)
 - ▶ tcp/80 (www)
 - HTTP request cannot exceed one packet, will be dropped
 - Restricts HTTP upload and large forms
 - ▶ tcp/113 (auth/ident)
 - Old-style authentication, currently used by some mail and IRC servers
 - Only ident request/response allowed, other data dropped

Firewalling (cont.)

▶ UDP

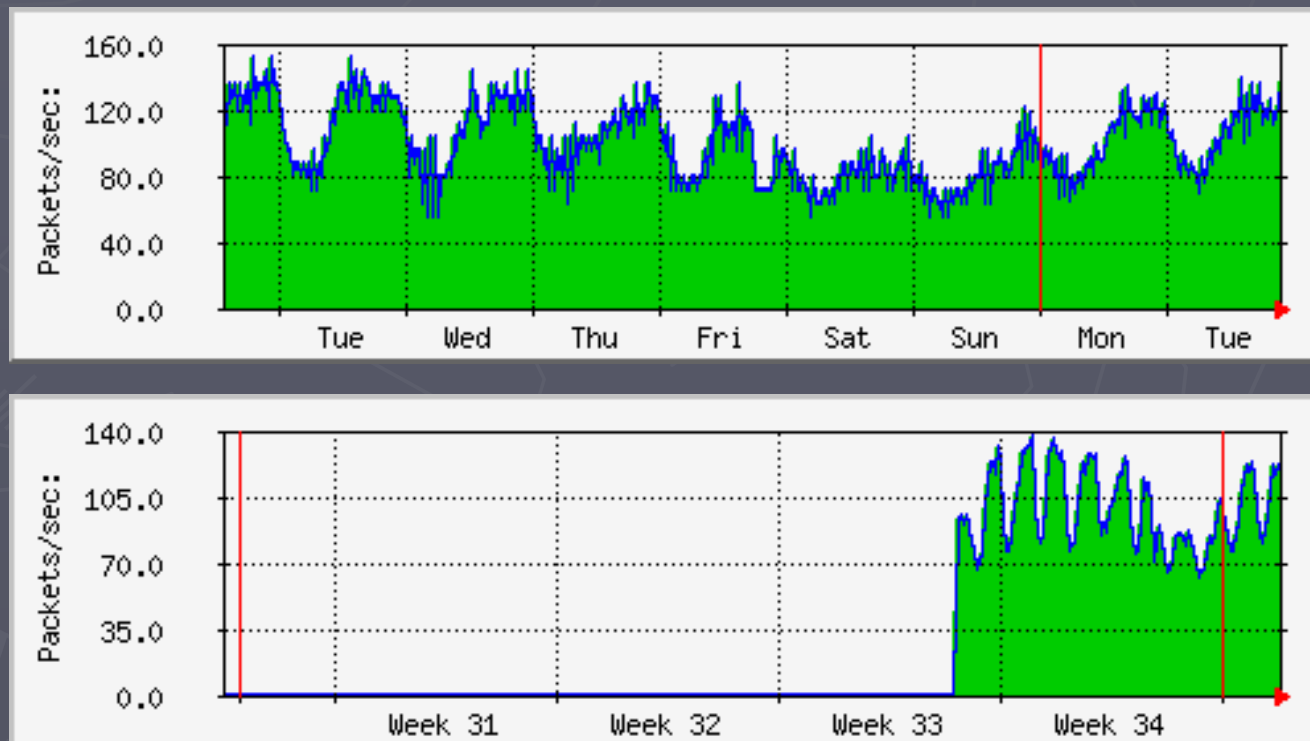
- Only incoming connections to some ports dropped
 - ▶ 135-139 (miscellaneous NetBIOS)
 - ▶ 143,220 (imap2/3)
 - ▶ 161,162 (snmp/snmp-trap)
 - ▶ 421 (ariel2?)
 - ▶ 445 (microsoft-ds)
 - ▶ 2049 (nfs)
- Supposedly ratelimited (high value)

▶ ICMP

- Unrestricted, under normal conditions
- Ratelimited (high limit)
- ICMP echo request/reply currently blocked due to Nachi/Welchia worms
 - ▶ ICMP scanning for exploitable hosts

Impact of Welchia/Nachi

► ICMP echo-request messages on ResNet



- Samples taken from 128.113.144.0/21 (quad/north/e) subnet
- Numbers multiplied by 100

ACMNet

- ▶ ACM machines graciously hosted by RPI's computer science department
- ▶ 100Mbit/sec link to RPI's network
- ▶ Shell/Web/Mail Services
- ▶ All dues-paying members may obtain accounts on ACMNet

ACMNet Machines

▶ Remote Access Machines

- apollo.acm.rpi.edu
 - ▶ UltraSPARC Iii 333MHz
 - ▶ Linux 2.4 (Debian)
- neroon.acm.rpi.edu
 - ▶ Pentium 4 2.00GHz
 - ▶ FreeBSD 5.0
- torque.acm.rpi.edu
 - ▶ Pentium 4 2.00GHz
 - ▶ Linux 2.4 (Gentoo)

ACMNet Services

- ▶ Gentoo portage rsync mirror
 - rsync18.us.gentoo.org
- ▶ Proposed services
 - Gentoo distfiles mirror
 - Debian Linux mirror
- ▶ Proposed hardware upgrades
 - Large RAID array, to accommodate mirrors
 - New file server

End of Line

▶ [http://www.prolixium.com/files/rpinet.\[ppt/pdf\]](http://www.prolixium.com/files/rpinet.[ppt/pdf])