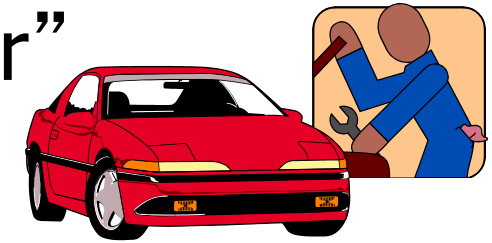


Things That Go “Bump” in the Net

Carey Williamson
Department of Computer Science
University of Calgary

Network Performance (Williamson)

- "Make the Internet go faster"



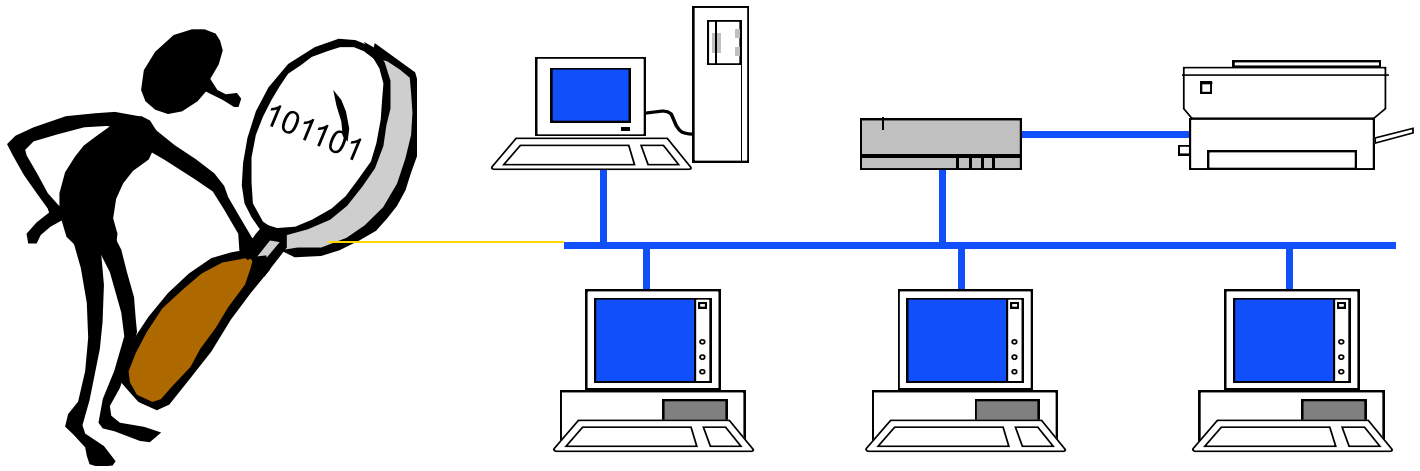
- Research area?
  - Wireless networks, Internet protocols, computer systems performance evaluation
- Approach?
  - Experimental, simulation, analytical
- Key challenges?
  - Citius, Altius, Fortius!

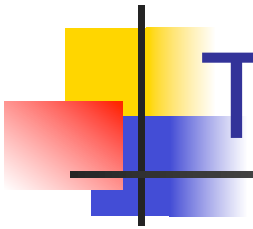


  - Performance, scalability, robustness

Network Traffic Measurement

- Collect and analyze packet-level traces from a live network, using special equipment
- Process traces, statistical analysis
- Diagnose performance problems (network, protocol, application)



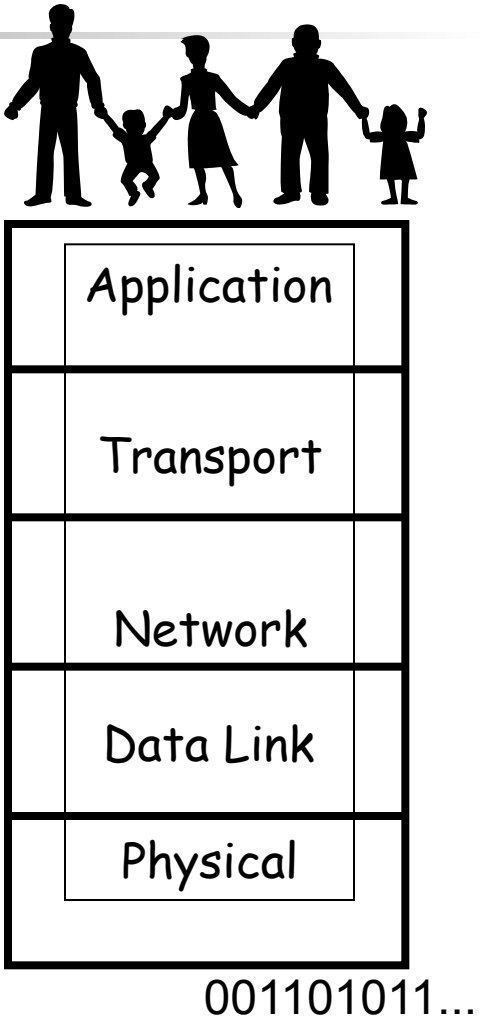


Talk Outline

- Background: Networking 101
- Network Traffic Measurement Basics
- Selected Measurement Results
  - U of C Network Anomalies
  - Wireless Network Weirdness
- Wrap-up and Questions

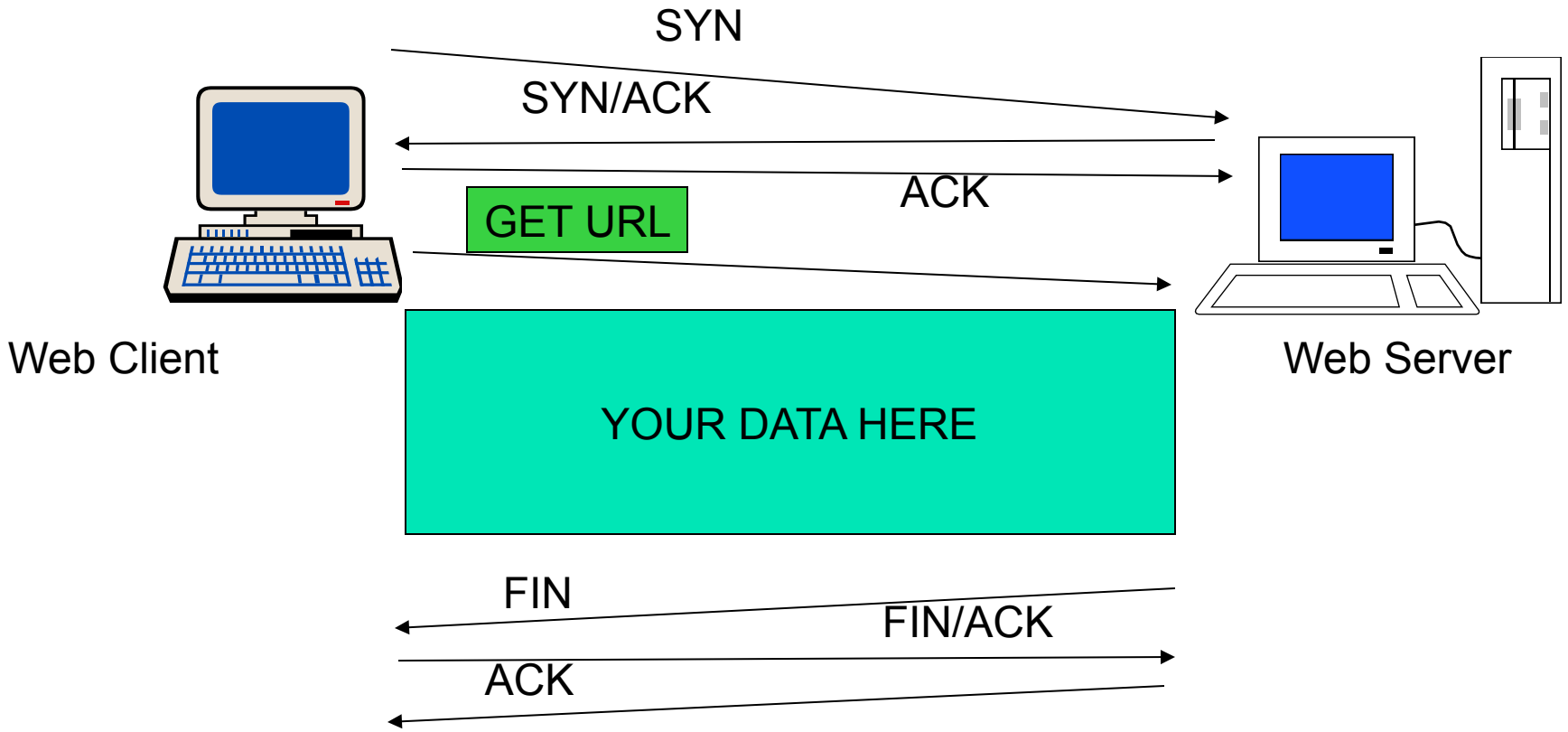
Internet Protocol Stack

- Application: supports end-user services and network applications
  - HTTP, SMTP, DNS, FTP, NTP
- Transport: end to end data transfer
  - TCP, UDP
- Network: routing of datagrams from source to destination
  - IPv4, IPv6, BGP, RIP
- Data Link: channel access, framing, flow/error control, hop by hop basis
  - PPP, Ethernet, IEEE 802.11b
- Physical: transmission of bits

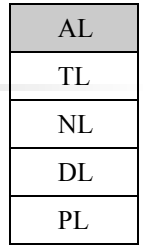


Example: HTTP and TCP

- Downloading a simple Web page



Network Packet Structure



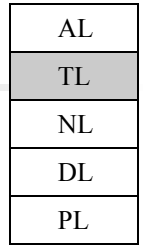
Protocol Headers
(Control Information)

Payload

			HTTP/1.0 200 OK Content-Type: text Content-Length: 4732 <html> Welcome to Sponge Bob's home page! On this site, there are lots of fun activities for you: colouring pages, bath time singalongs, and more. <p> Please click <a> <href="./signup.html"> here to learn more about membership accounts and...

Payload (User Level Data)

Network Packet Structure



Protocol Headers
(Control Information)

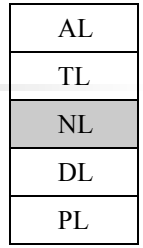
Payload

		SrcPort 80 DstPort 2579 SeqNum 61842 ACK 3756812 Window 8192 Flags: PA	HTTP/1.0 200 OK Content-Type: text Content-Length: 4732 <html> Welcome to Sponge Bob's home page! On this site, there are lots of fun activities for you: colouring pages, bath time singalongs, and more. <p> Please click <a> <href="./signup.html"> here to learn more about membership accounts and...

Transport Layer Header (e.g., TCP)

Payload (User Level Data)

Network Packet Structure



Protocol Headers (Control Information)

Payload

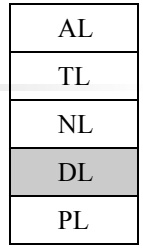
	SrcIP 372.19.44.108 DstIP 136.159.99.114 Length 1500	SrcPort 80 DstPort 2579 SeqNum 61842 ACK 3756812 Window 8192 Flags: PA	HTTP/1.0 200 OK Content-Type: text Content-Length: 4732 <html> Welcome to Sponge Bob's home page! On this site, there are lots of fun activities for you: colouring pages, bath time singalongs, and more. <p> Please click <a> <href="./signup.html"> here to learn more about membership accounts and...

Network Layer Header (e.g., IP)

Transport Layer Header (e.g., TCP)

Payload (User Level Data)

Network Packet Structure



Protocol Headers (Control Information)

Payload

Src 12:BD:07: AF:B0:6E Dst 37:F9:14: FD:C1:08 CRC 0xFC147E	SrcIP 372.19.44.108 DstIP 136.159.99.114 Length 1500	SrcPort 80 DstPort 2579 SeqNum 61842 ACK 3756812 Window 8192 Flags: PA	HTTP/1.0 200 OK Content-Type: text Content-Length: 4732 <html> Welcome to Sponge Bob's home page! On this site, there are lots of fun activities for you: colouring pages, bath time singalongs, and more. <p> Please click <a> <href="./signup.html"> here to learn more about membership accounts and...

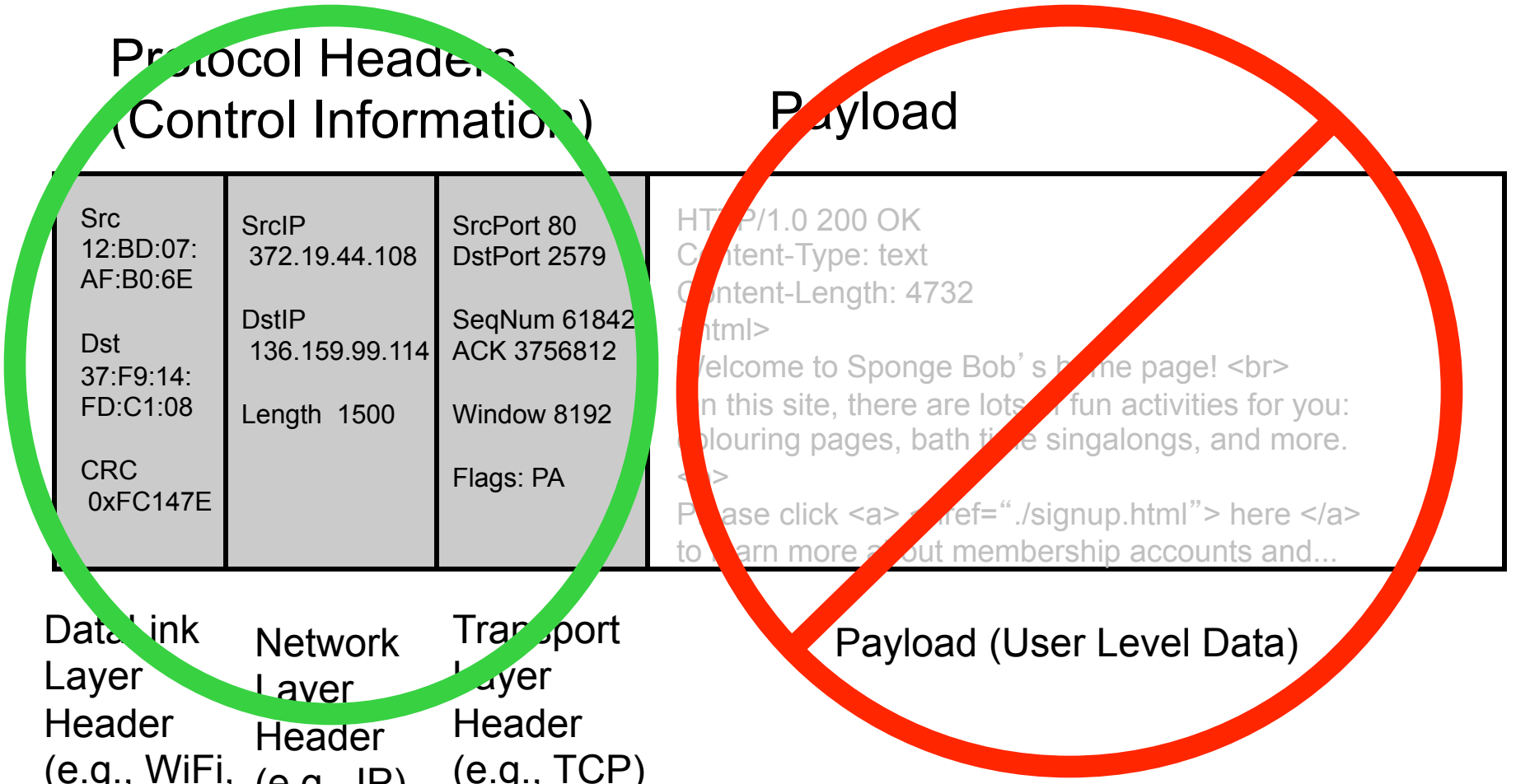
DataLink Layer Header (e.g., WiFi, Ethernet)

Network Layer Header (e.g., IP)

Transport Layer Header (e.g., TCP)

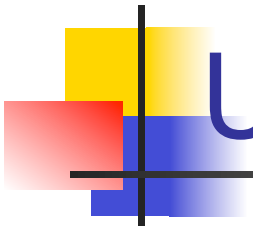
Payload (User Level Data)

Network Traffic Measurements



Example: tcpdump Trace

Time	IP Source Addr		IP Dest Addr	Size	Prot	SPort	DPort	TCP Data SeqNumber	TCP AckNum	Window	Flags
0.000000	192.168.1.201	->	192.168.1.200	60	TCP	4105	80	1315338075 : 1315338075	0	win: 5840	S
0.003362	192.168.1.200	->	192.168.1.201	60	TCP	80	4105	1417888236 : 1417888236	1315338076	win: 5792	SA
0.009183	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338076 : 1315338076	1417888237	win: 5840	A
0.010854	192.168.1.201	->	192.168.1.200	127	TCP	4105	80	1315338076 : 1315338151	1417888237	win: 5840	PA
0.014309	192.168.1.200	->	192.168.1.201	52	TCP	80	4105	1417888237 : 1417888237	1315338151	win: 5792	A
0.049848	192.168.1.200	->	192.168.1.201	1500	TCP	80	4105	1417888237 : 1417889685	1315338151	win: 5792	A
0.056902	192.168.1.200	->	192.168.1.201	1500	TCP	80	4105	1417889685 : 1417891133	1315338151	win: 5792	A
0.057284	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338151 : 1315338151	1417889685	win: 8688	A
0.060120	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338151 : 1315338151	1417891133	win: 11584	A
0.068579	192.168.1.200	->	192.168.1.201	1500	TCP	80	4105	1417891133 : 1417892581	1315338151	win: 5792	PA
0.075673	192.168.1.200	->	192.168.1.201	1500	TCP	80	4105	1417892581 : 1417894029	1315338151	win: 5792	A
0.076055	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338151 : 1315338151	1417892581	win: 14480	A
0.083233	192.168.1.200	->	192.168.1.201	1500	TCP	80	4105	1417894029 : 1417895477	1315338151	win: 5792	A
0.096728	192.168.1.200	->	192.168.1.201	1500	TCP	80	4105	1417896925 : 1417898373	1315338151	win: 5792	A
0.103439	192.168.1.200	->	192.168.1.201	1500	TCP	80	4105	1417898373 : 1417899821	1315338151	win: 5792	A
0.103780	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338151 : 1315338151	1417894029	win: 17376	A
0.106534	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338151 : 1315338151	1417898373	win: 21720	A
0.133408	192.168.1.200	->	192.168.1.201	776	TCP	80	4105	1417904165 : 1417904889	1315338151	win: 5792	FPA
0.139200	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338151 : 1315338151	1417904165	win: 21720	A
0.140447	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338151 : 1315338151	1417904890	win: 21720	FA
0.144254	192.168.1.200	->	192.168.1.201	52	TCP	80	4105	1417904890 : 1417904890	1315338152	win: 5792	A

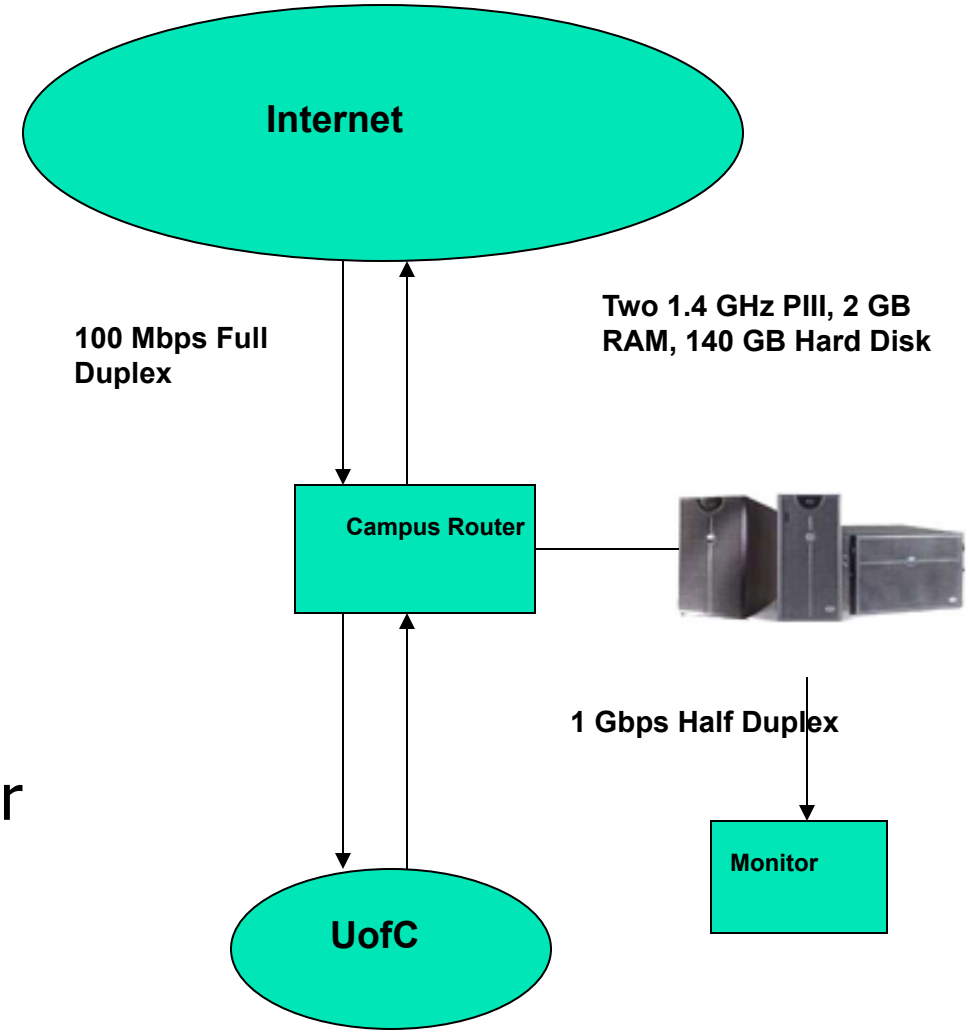


U of C Traffic Measurement

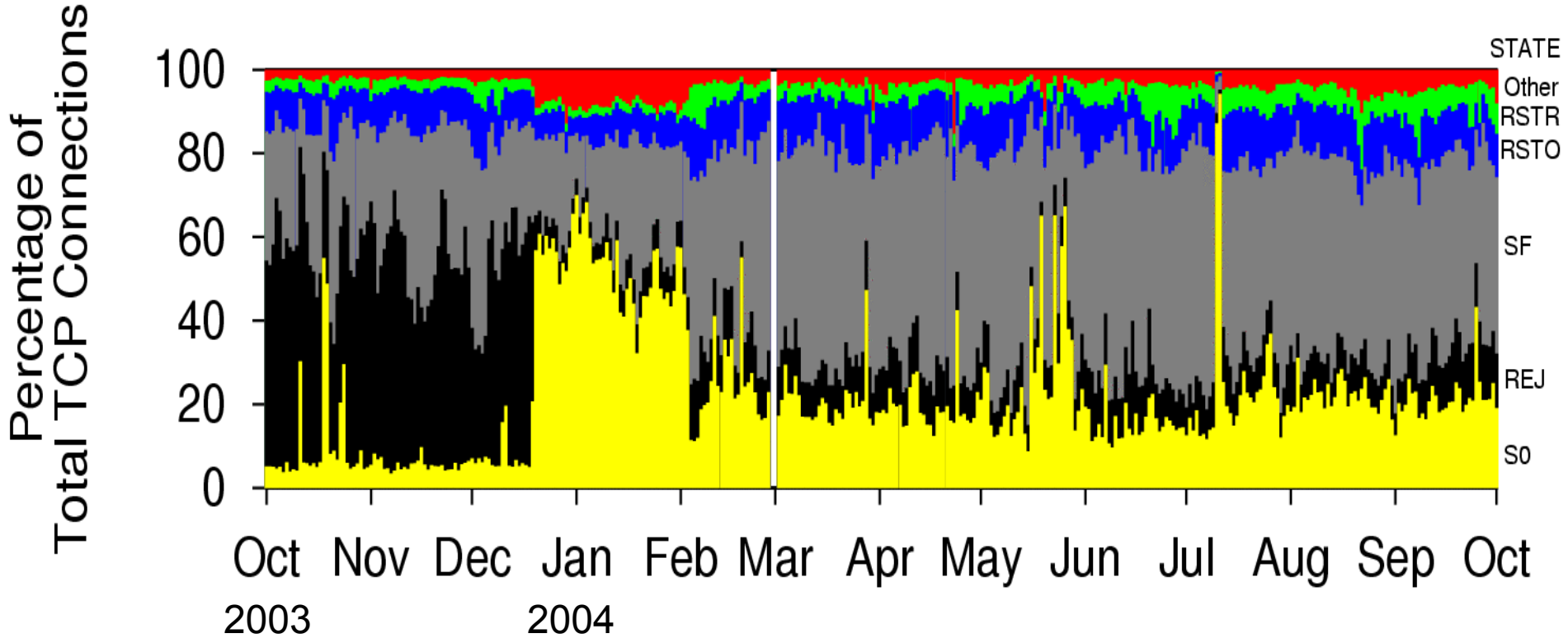
- Continuous monitoring of U of C traffic on commercial Internet link
- 24 months of data and counting…
- Specific measurement studies to date:
  - TCP reset behaviour (Arlitt)
  - Network intrusion detection (Obied)
  - P2P traffic evolution (Madhukar)
- Campus WLAN measurement study underway now in 2006 with UCIT

Data Collection Methodology

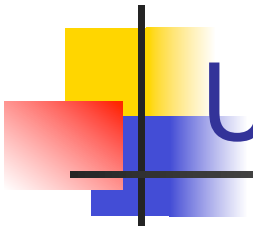
- Use tcpdump as network monitor on U of C campus Internet connection
- Data collection started in September 2003
- TCP/IP packet headers (SYN/FIN/RST)
- 2 years of data available for analysis



TCP Connection Analysis (1 yr)



M. Arlitt and C. Williamson, "An Analysis of TCP Reset Behaviour on the Internet", ACM Computer Communication Review, Vol. 35, No. 1, pp. 37-44, January 2005



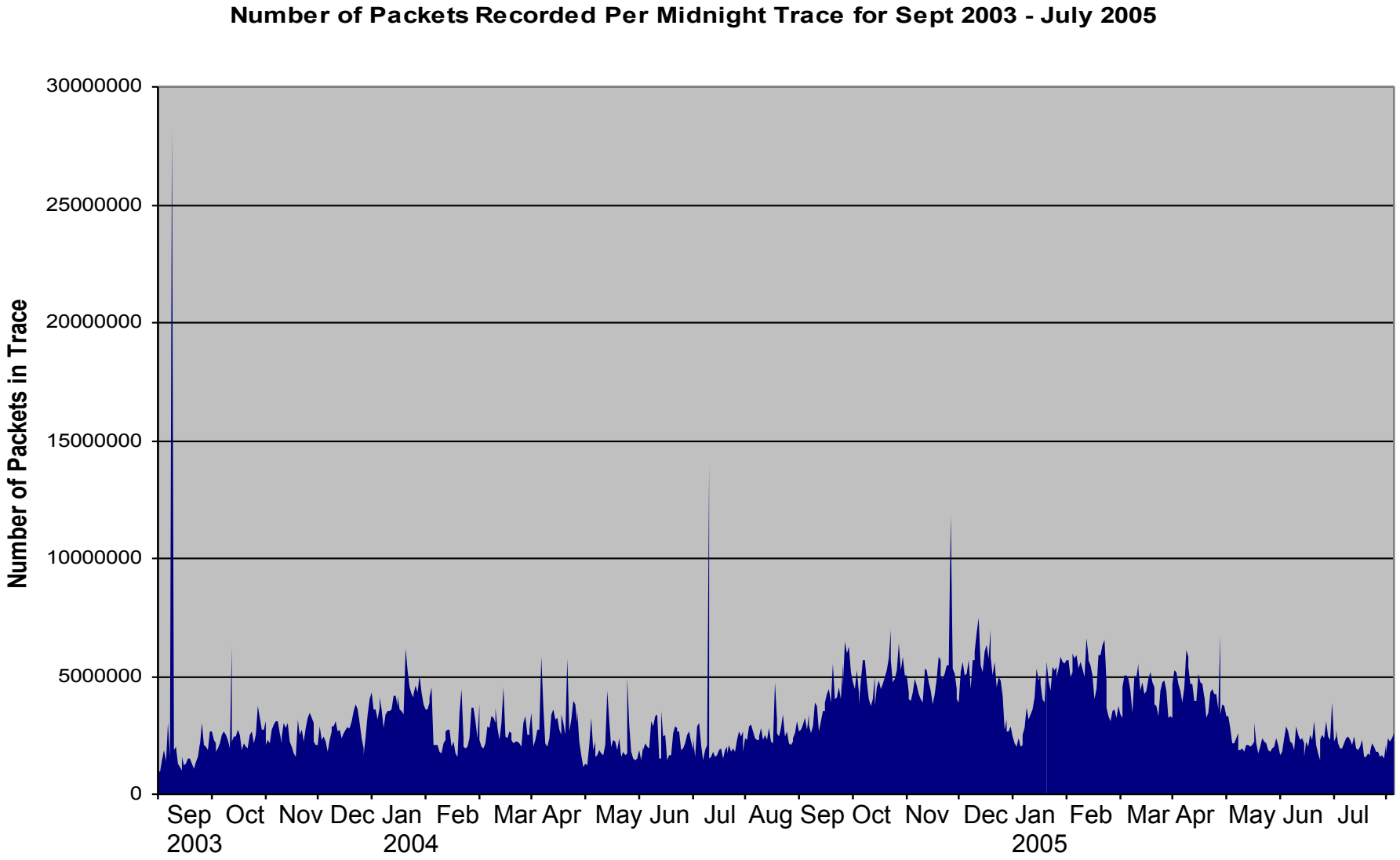
U of C P2P Traffic Study

- What proportion of U of C's Internet traffic is Peer-to-Peer (P2P) file sharing traffic, like KaZaA, BitTorrent, etc...?
  - (a) about 1%
  - (b) about 10%
  - (c) about 25%
  - (d) about 50%
  - (e) about 90%

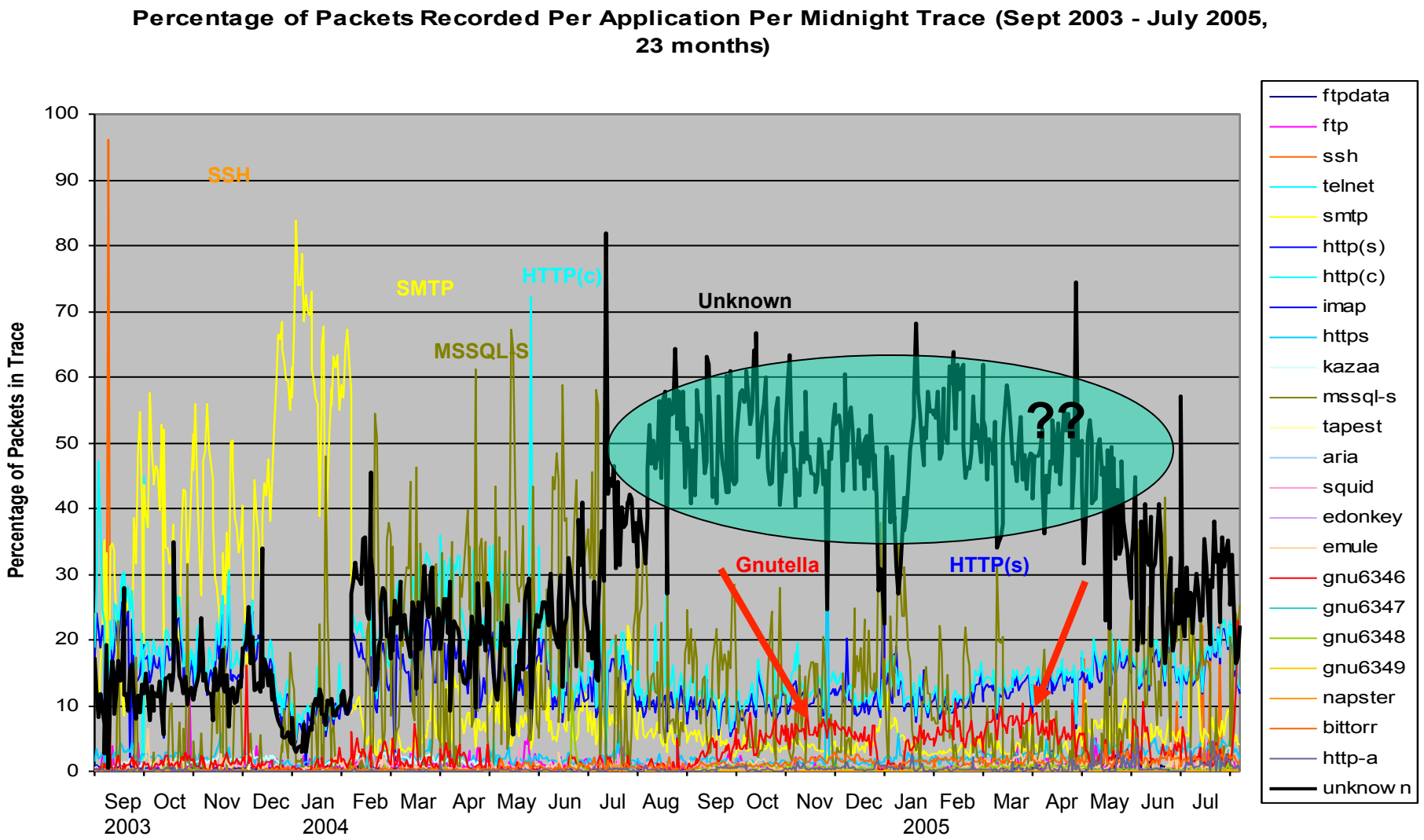
Correct!



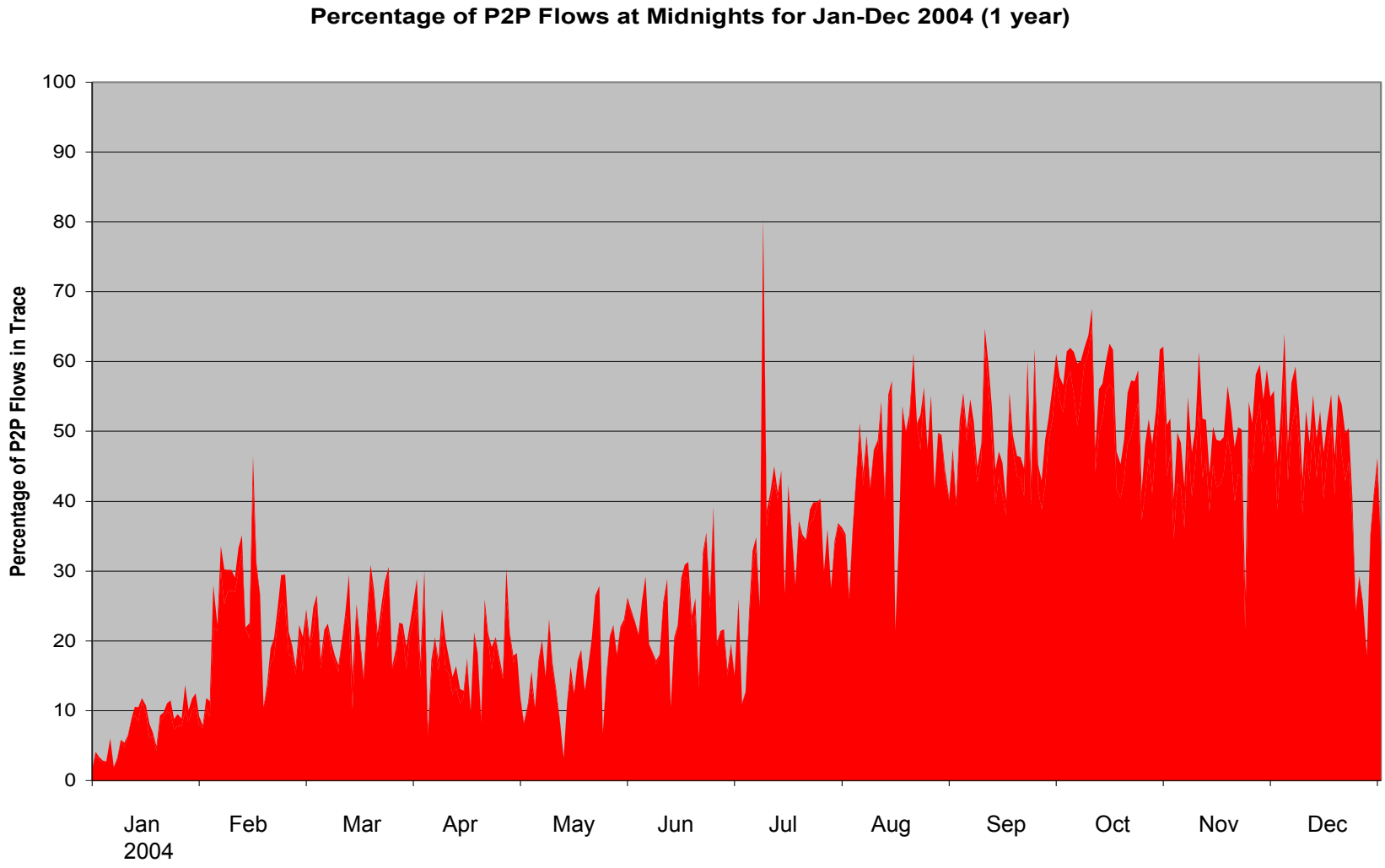
Network Activity (Sept/03–July/05)



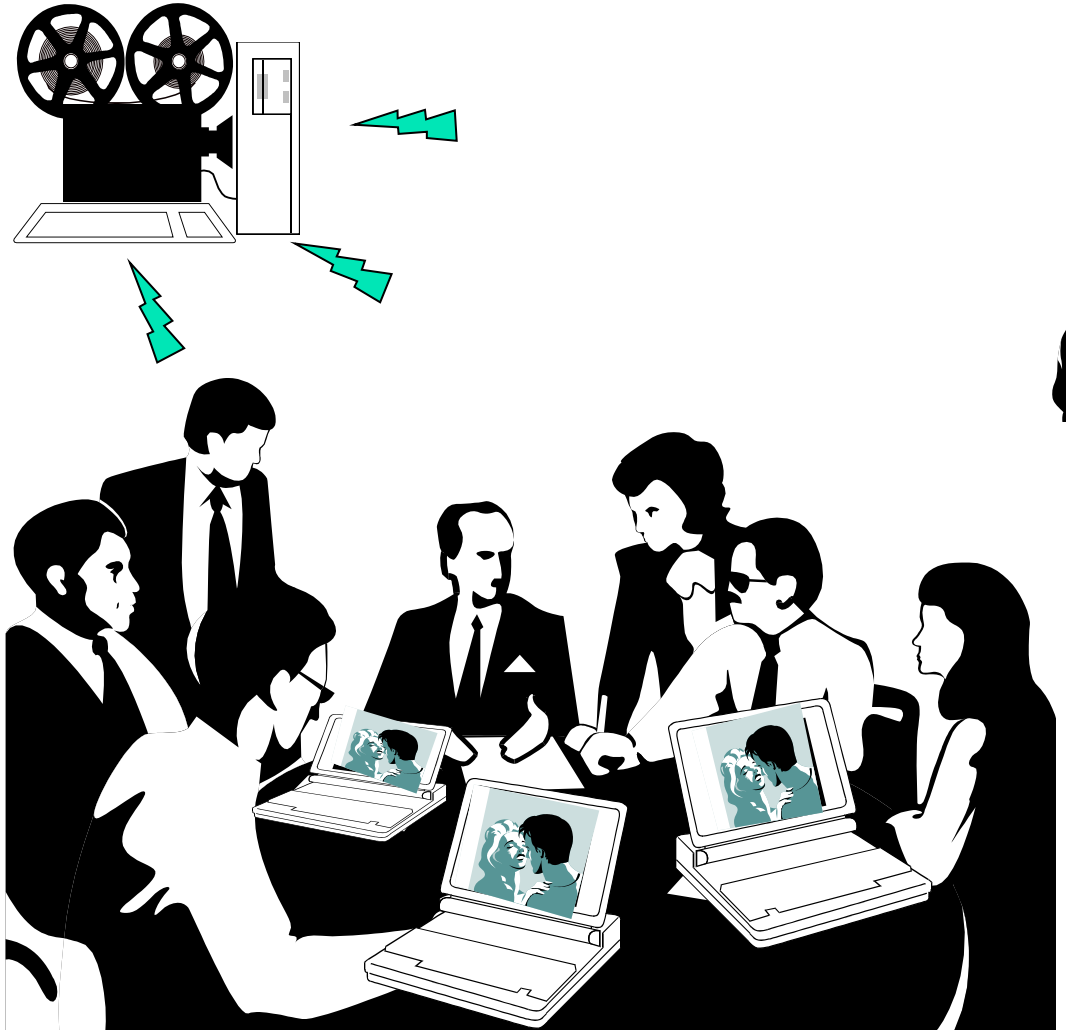
Port Analysis Results



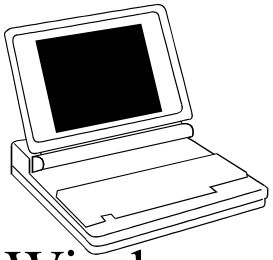
Results for Transport-Layer Method



Wireless Media Streaming

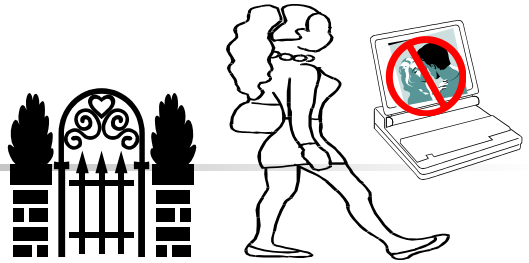


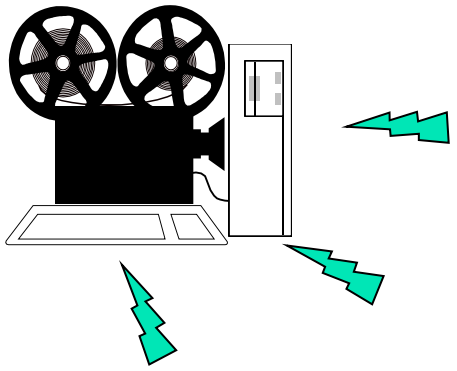




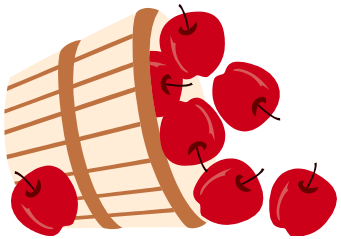
Wireless Sniffer

Mobility Issues



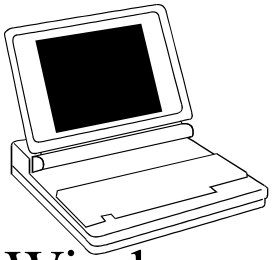


"bad apple" phenomenon

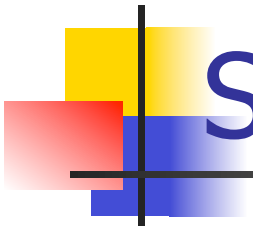






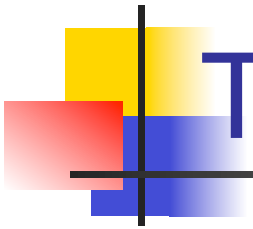


Wireless Sniffer



Summary

- Network traffic measurement is a useful technique for networking researchers
- Much is known about the general characteristics of Internet traffic, but new surprises arise all the time
- Internet traffic is changing and evolving
- Network measurement is essential for understanding current/future Internet



Thank You!

- For more information:
  - Email: carey@cpsc.ucalgary.ca
  - WWW: www.cpsc.ucalgary.ca/~carey
- Credits: UCIT, Martin Arlitt, Jean Cao
- Questions?