

Internet Measurement Conference

Stephen Strowes
`sds@dcs.gla.ac.uk`

17 November 2010
ENDS Seminar, Glasgow

Outline

Preamble

Paper: Home Gateway Characteristics

Conference Papers

Summary

Outline

Preamble

Paper: Home Gateway Characteristics

Conference Papers

Summary

Preamble

- ▶ 10th Internet Measurement Conference (IMC)
 - ▶ Melbourne, Australia

Preamble

- ▶ 10th Internet Measurement Conference (IMC)
 - ▶ Melbourne, Australia
- ▶ 211 submissions

Preamble

- ▶ 10th Internet Measurement Conference (IMC)
 - ▶ Melbourne, Australia
- ▶ 211 submissions
- ▶ 47 accepted; 22.3% accept rate:
 - ▶ 24 long papers (12 pages)
 - ▶ 23 short papers (6 pages + references)

Preamble

- ▶ 10th Internet Measurement Conference (IMC)
 - ▶ Melbourne, Australia
- ▶ 211 submissions
- ▶ 47 accepted; 22.3% accept rate:
 - ▶ 24 long papers (12 pages)
 - ▶ 23 short papers (6 pages + references)
- ▶ 11 accepted prior to TPC

Outline

Preamble

Paper: Home Gateway Characteristics

Conference Papers

Summary

An Experimental Study of Home Gateway Characteristics

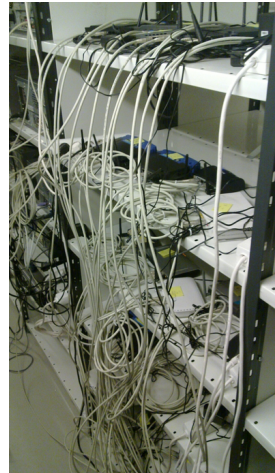
- ▶ Seppo Hätönen, University of Helsinki
- ▶ Aki Nyrhinen, University of Helsinki
- ▶ Lars Eggert, Nokia Research Center
- ▶ Stephen Strowes, University of Glasgow
- ▶ Pasi Sarolahti, HIIT
- ▶ Markku Kojo, University of Helsinki

An Experimental Study of Home Gateway Characteristics

- ▶ Common home gateway function is network address translation (NAT)
- ▶ Best current practices: RFC 4787, RFC 5382
- ▶ Lots of anecdotal evidence suggests behaviour is varied
- ▶ This affects protocol design, application design, user experience

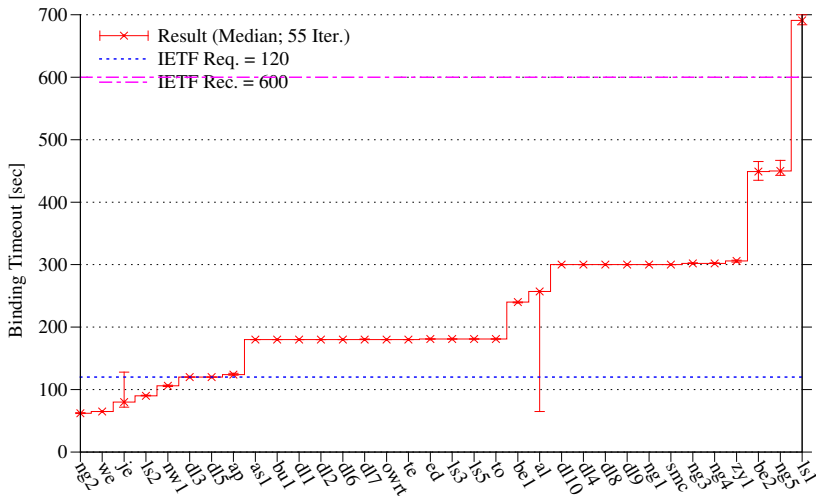
An Experimental Study of Home Gateway Characteristics

- ▶ 34 NATs
- ▶ Two servers
- ▶ Run some tests...

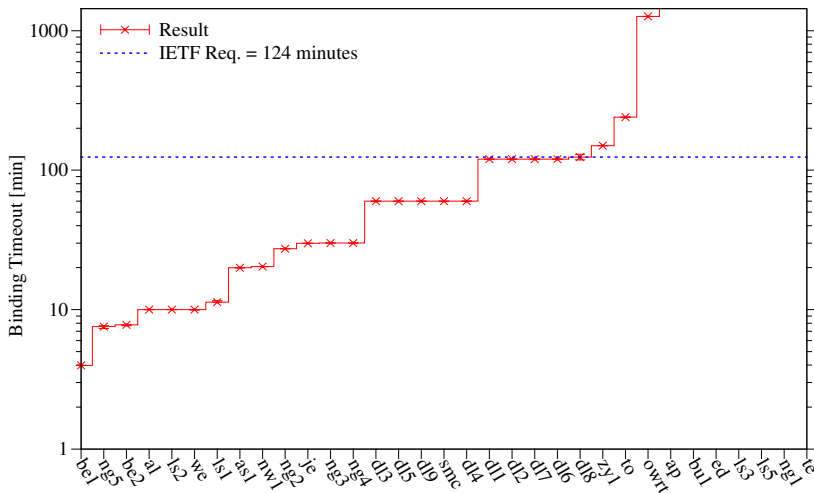


Results: UDP Binding Timeouts

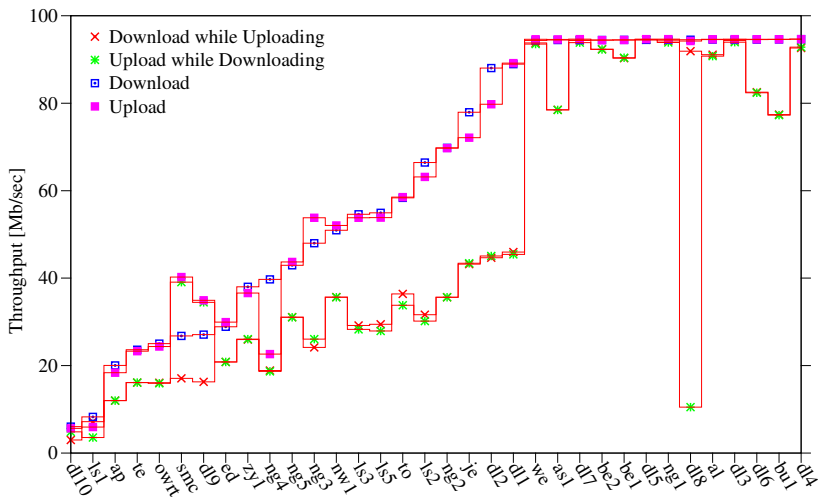
Results: UDP Binding Timeouts



Results: TCP Binding Timeouts



Results: TCP Throughputs



Results

- ▶ There is high variability in performance
- ▶ Some behaviour seems at odds with a working Internet connection at all...

Results

- ▶ There is high variability in performance
- ▶ Some behaviour seems at odds with a working Internet connection at all...
- ▶ Many timeouts are remarkably short
- ▶ Throughput tests: 2/3 of devices cannot sustain 100Mbps

Results

- ▶ There is high variability in performance
- ▶ Some behaviour seems at odds with a working Internet connection at all...
- ▶ Many timeouts are remarkably short
- ▶ Throughput tests: 2/3 of devices cannot sustain 100Mbps
- ▶ ICMP handling: Many devices only support some message types; all but one translate at least “port unreachable” and “TTL exceeded”
- ▶ DCCP: Fails in all cases
- ▶ SCTP: Passes on 18 of 34 NATs

Outline

Preamble

Paper: Home Gateway Characteristics

Conference Papers

Summary

Eyeball ASes: From Geography to Connectivity

Eyeball ASes: From Geography to Connectivity

- ▶ Amir H. Rasti, University of Oregon
- ▶ Nazanin Magharei, University of Oregon
- ▶ Reza Rejaie, University of Oregon
- ▶ Walter Willinger, AT&T Labs

Eyeball ASes: From Geography to Connectivity

- ▶ Aim: To determine geographical footprint of AS based on locations of its users

Eyeball ASes: From Geography to Connectivity

- ▶ Aim: To determine geographical footprint of AS based on locations of its users
- ▶ Determine geo-footprint of ASes using the geo-location of its end users
 - ▶ Collect IP addresses from users
 - ▶ Map IP addresses to geolocation
 - ▶ Group end users by AS

Eyeball ASes: From Geography to Connectivity

- ▶ Aim: To determine geographical footprint of AS based on locations of its users
- ▶ Determine geo-footprint of ASes using the geo-location of its end users
 - ▶ Collect IP addresses from users
 - ▶ Map IP addresses to geolocation
 - ▶ Group end users by AS
- ▶ 48 million users in 1,233 ASes
- ▶ Kernel density estimation to estimate probability density of customer population

Eyeball ASes: From Geography to Connectivity

- ▶ Aim: To determine geographical footprint of AS based on locations of its users
- ▶ Determine geo-footprint of ASes using the geo-location of its end users
 - ▶ Collect IP addresses from users
 - ▶ Map IP addresses to geolocation
 - ▶ Group end users by AS
- ▶ 48 million users in 1,233 ASes
- ▶ Kernel density estimation to estimate probability density of customer population
- ▶ Detects ISP points of presence
- ▶ Evaluated against “ground truth” of some known PoPs

Towards an AS-to-Organisation Map

Towards an AS-to-Organisation Map

- ▶ Xue Cai, USC/ISI
- ▶ John Heidemann, USC/ISI
- ▶ Balachander Krishnamurthy, AT&T Labs
- ▶ Walter Willinger, AT&T Labs

Internet Background Radiation Revisited

Internet Background Radiation Revisited

- ▶ Eric Wustrow, Merit Network Inc.
- ▶ Manish Karir, Merit Network Inc.
- ▶ Michael Bailey, University of Michigan
- ▶ Farnam Jahanian, University of Michigan
- ▶ Geoff Huston, Asia Pacific Network (APNIC)

Internet Background Radiation Revisited

- ▶ Characterise background noise on four unused /8's
 - ▶ Malicious traffic, misconfiguration

Internet Background Radiation Revisited

- ▶ Characterise background noise on four unused /8's
 - ▶ Malicious traffic, misconfiguration
- ▶ Using:
 - ▶ 1/8, 50/8, 107/8 over the period of 1 week
 - ▶ 35/8 over the period of 5 years
- ▶ Advertise, and passively monitor
- ▶ Each prefix attracts tens of billions of packets during the weeks monitored

Internet Background Radiation Revisited

- ▶ Results include:
 - ▶ 1.*.168.0/24 attracts some traffic
 - ▶ Last octet is often 192. That is, 192.168.x.1 in host-byte order for little-endian hosts.
 - ▶ Likewise, 1.*.0.10

Internet Background Radiation Revisited

- ▶ Results include:
 - ▶ 1.*.168.0/24 attracts some traffic
 - ▶ Last octet is often 192. That is, 192.168.x.1 in host-byte order for little-endian hosts.
 - ▶ Likewise, 1.*.0.10
 - ▶ 50.153.199.194 is another hotspot
 - ▶ Misinterpretation of config: "062", octal, == 50, decimal
 - ▶ Offending network has offered to firewall this address

Internet Background Radiation Revisited

- ▶ Results include:
 - ▶ 1.*.168.0/24 attracts some traffic
 - ▶ Last octet is often 192. That is, 192.168.x.1 in host-byte order for little-endian hosts.
 - ▶ Likewise, 1.*.0.10
 - ▶ 50.153.199.194 is another hotspot
 - ▶ Misinterpretation of config: "062", octal, == 50, decimal
 - ▶ Offending network has offered to firewall this address
 - ▶ Within 1/8, 1.1.1.0/24 attracts 44% of packets, 58.7% of bytes
 - ▶ Majority is to 1.1.1.1:15206
 - ▶ Payload type 0x8000
 - ▶ Malicious SIP INVITE attack; server responds with RTP stream

Internet Background Radiation Revisited

"The number you have dialled is not in service. Please check the number and try again."

Internet Background Radiation Revisited

- ▶ There is scope for testing any blocks prior to allocation
- ▶ Cleanup space if possible
- ▶ Identify addresses which *should not be allocated* to ISPs

Netalyzer: Illuminating the Edge Network

Netalyzer: Illuminating the Edge Network

- ▶ Christian Kreibich, ICSI
- ▶ Nicholas Weaver, ICSI
- ▶ Boris Nechaev, HIIT & Aalto Univerisity
- ▶ Vern Paxson, ICSI & UC Berkeley

“Like a breathalyser. Is your ISP sober enough to drive your traffic?”

Netalyzer: Illuminating the Edge Network

- ▶ <http://netalyzer.icsi.berkeley.edu/>

The screenshot shows a web browser window with the URL <http://netalyzer.icsi.berkeley.edu/>. The page title is "The ICSI Netalyzer". Below the title is a navigation bar with links for "Introduction", "Analysis", and "Results", and a "Language" dropdown menu. The main heading is "Debug your Internet.". Below this is a three-step process diagram: 1. "What's up with my network?" (Some services seem broken? Things are very slow? Is there something wrong?), 2. "Run the Netalyzer." (We test your Internet connection for signs of trouble.), and 3. "Understand your connectivity." (A detailed report shows performance & security issues.). Below the diagram, there is a paragraph: "Learn more, see an [example report](#), check out the [NetaMap](#), or look at the [FAQ](#). Netalyzer requires Java to operate." At the bottom, there is a large red button that says "Start analysis »".

Netalyzer: Illuminating the Edge Network

The screenshot shows a web browser window with the address bar displaying `http://n1.netalyzer.icsi.br`. The page title is "The ICSI Netalyzer". Below the title, there are navigation links: "Introduction", "Analysis", and "Results" (which is highlighted). The main content area is titled "Result Summary +/- (help)". Below this, the target IP address is displayed: `cpc14-broo7-2-0-cust223.14-2.cable.virginmedia.com / 82.9.16.224`. A timestamp and recording information are shown: "Recorded at 18:24 EST (23:24 UTC), Nov 16 2010. [Permalink](#). [Client/server transcript](#)." Below this, there is a section titled "Summary of Noteworthy Events –". Under this section, there is a sub-section titled "Minor Aberrations" which contains a list of three items, each followed by a downward arrow icon: "Certain TCP protocols are blocked in outbound traffic", "The network measured bursts of packet loss", and "Network packet buffering may be excessive". Below the "Minor Aberrations" section, there is another section titled "Address-based Tests –". Under this section, there is a sub-section titled "NAT detection (?): NAT Detected" which contains two paragraphs of text: "Your global IP address is 82.9.16.224 while your local one is 192.168.1.3. You are behind a NAT. Your local address is in unroutable address space." and "Your machine numbers TCP source ports sequentially. The following graph shows".

Netalyzer: Illuminating the Edge Network

- ▶ Accumulated 130,000 traces over the last few years
- ▶ 12% of whom use OpenDNS (“geek bias” in data)

Netalyzer: Illuminating the Edge Network

- ▶ They have a lot of data on blocked ports, upstream and downstream throughput, in-network buffering, DNS behaviour (e.g., wildcarding)
- ▶ Interesting oddities, like: 42% of HTTP proxies do not cache data if they could; 35% of caches will store strongly uncacheable content
- ▶ Overbuffering, probably in home gateways; buffers often 128KB or 256KB

Netalyzer: Illuminating the Edge Network

- ▶ They have a lot of data on blocked ports, upstream and downstream throughput, in-network buffering, DNS behaviour (e.g., wildcarding)
- ▶ Interesting oddities, like: 42% of HTTP proxies do not cache data if they could; 35% of caches will store strongly uncacheable content
- ▶ Overbuffering, probably in home gateways; buffers often 128KB or 256KB
- ▶ ... And lots more in the paper
- ▶ Unfortunately they haven't released code, far as I can tell

Outline

Preamble

Paper: Home Gateway Characteristics

Conference Papers

Summary

Summary

- ▶ There was lots of interesting work here. Examples:
 - ▶ A couple of papers on packet capture on commodity hardware (“up to a gigabit stream”)
 - ▶ Network tomography
 - ▶ Identifying router aliases using IP timestamping
 - ▶ Event detection from mining logs from many routers

Summary

- ▶ The quality of the work here was pretty good.
- ▶ Culture of data sharing: only papers with associated public data are eligible for “best paper”
- ▶ This seems a worthwhile venue!
- ▶ IMC is in Berlin next year
 - ▶ November 2-4
 - ▶ <http://conferences.sigcomm.org/imc/2011/>
 - ▶ Submission deadline ~May 2011, based on 2010's schedule

Questions?