The ICSI Netalyzr Beta

Introduction » Analysis » Results

Result Summary

static-71-242-253-198.phlapa.east.verizon.net / 71.242.253.198

Recorded at 21:25 EDT (01:25 UTC next day) on Thu, August 27 2009. Permalink. Transcript. Wildcard DNS content.

Noteworthy Events

Major Abnormalities

- We received unexpected and possibly dangerous results when looking up important names

Minor Aberrations

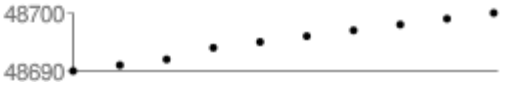
- Network packet buffering may be excessive
- Your DNS resolver returns results even when no such server exists
- Your computer's clock is slightly fast

Address-based Tests

NAT detection: NAT Detected

Your global IP address is 71.242.253.198 while your local one is 192.168.182.82. You are behind a NAT. Your local address is in unroutable address space.

Your NAT renumbers TCP source ports sequentially. The following graph shows connection attempts on the X-axis and their corresponding source ports on the Y-axis.



DNS-based host information: OK

You are not a Tor exit node for HTTP traffic.

You are not listed on any Spamhaus blacklists.

The SORBS DUHL believes you are using a statically assigned IP address.

Reachability Tests

General connectivity: OK

Basic UDP access is available.

Direct UDP access to remote DNS servers (port 53) is allowed.
The applet was also able to directly request a small DNS response with EDNS enabled.
The applet was also able to directly request a medium sized (~1400B) DNS response.
The applet was also able to directly request a large (~1800B) DNS response.

Direct UDP access to remote MSSQL servers (port 1434) is allowed.

- Direct TCP access to remote FTP servers (port 21) is allowed.
- Direct TCP access to remote SSH servers (port 22) is allowed.
- Direct TCP access to remote SMTP servers (port 25) succeeds, but does not return the expected content.
  This suggests that your network enforces a mandatory SMTP proxy which may or may not allow you to send email directly from your system. This is probably a countermeasure against malware abusing infected machines for generating spam. You ISP also likely provides a specific mail server that is permitted. Also, webmail services remain unaffected.

  The applet received the following reply instead of our expected header:
  "220 harrier.ovatn.net ESMTP Postfix "
- Direct TCP access to remote DNS servers (port 53) is allowed.
- Direct TCP access to remote HTTP servers (port 80) is allowed.
- Direct TCP access to remote POP servers (port 110) is allowed.
- Direct TCP access to remote RPC servers (port 135) is allowed.
- Direct TCP access to remote NetBIOS servers (port 139) is allowed.
- Direct TCP access to remote IMAP servers (port 143) is allowed.
- Direct TCP access to remote SNMP servers (port 161) is allowed.
- Direct TCP access to remote HTTPS servers (port 443) is allowed.
- Direct TCP access to remote SMB servers (port 445) is allowed.
- Direct TCP access to remote SMTP/SSL servers (port 465) is allowed.
- Direct TCP access to remote secure IMAP servers (port 585) is allowed.
- Direct TCP access to remote authenticated SMTP servers (port 587) is allowed.
- Direct TCP access to remote IMAP/SSL servers (port 993) is allowed.
- Direct TCP access to remote POP/SSL servers (port 995) is allowed.
- Direct TCP access to remote SIP servers (port 5060) is allowed.
- Direct TCP access to remote BitTorrent servers (port 6881) is allowed.

Network Access Link Properties

Network latency measurements: Latency: 120ms Loss: 0.0%

- The round-trip time (RTT) between your computer and our server is 120 msec, which is good.
- We recorded no packet loss between your system and our server.

TCP connection setup latency: 140ms

- The time it takes your computer to set up a TCP connection with our server is 140 msec, which is good.

Network bandwidth measurements: Upload 770 Kbit/sec, Download 5.6 Mbit/sec

- **Your Uplink:** We measured your uplink's sending bandwidth at 770 Kbit/sec. This level of bandwidth works well for many users.
- **Your Downlink:** We measured your downlink's receiving bandwidth at 5.6 Mbit/sec. This level of bandwidth works well for many users.

Network buffer measurements: Uplink 5100 ms, Downlink 100 ms

- We estimate your uplink as having 5100 msec of buffering. This is quite high, and you may

experience substantial disruption to your network performance when performing interactive tasks such as web-surfing while simultaneously conducting large uploads. With such a buffer, real-time applications such as games or audio chat can work quite poorly when conducting large uploads at the same time.

We estimate your downlink as having 100 msec of buffering. This level may serve well for maximizing speed while minimizing the impact of large transfers on other traffic.

HTTP Tests

Address-based HTTP proxy detection: OK

There is no explicit sign of HTTP proxy use based on IP address.

Header-based HTTP proxy detection: OK

No HTTP header or content changes hint at the presence of a proxy.

HTTP proxy detection via malformed requests: OK

Deliberately malformed HTTP requests arrive at our server unchanged. We are not able to detect a proxy along the path to our server using this method.

Filetype-based filtering: OK

We did not detect file-content filtering.

HTTP caching behavior: OK

There is no suggestion that a transparent HTTP cache exists in your network.

JavaScript-based tests: OK

The applet was not run from within a frame.

Your web browser reports the following cookies for our web page:

- netAlizEd = BaR (set by our server)
- netalyzrComplete = True (set by our server)

Your web browser was unable to fetch an image using IPv6.

DNS Tests

Restricted domain DNS lookup: OK

We are able to successfully lookup a name which resolves to the same IP address as our webserver. This means we are able to conduct many of the tests on your DNS server.

Unrestricted domain DNS lookup: OK

We are able to successfully lookup arbitrary names from within the Java applet. This means we are able to conduct all test on your DNS server.

DNS resolver address: OK

The IP address of your ISP's DNS Resolver is 208.67.217.6, which resolves to bld2.nyc.opendns.com.

DNS resolver properties: Lookup latency: 270ms

Your ISP's DNS resolver requires 270 msec to conduct an external lookup, and 33 msec to

lookup an item in the cache.

Your resolver is using QTYPE=A for default queries.

Your resolver also performs IPv6 queries in addition to IPv4 queries.

Your DNS resolver does not use EDNS.

Your resolver does not use 0x20 randomization, but will pass names in a case-sensitive manner.

Your ISP's DNS resolver respects a TTL of 0 seconds.

Your ISP's DNS resolver respects a TTL of 1 seconds.

DNS glue policy: OK

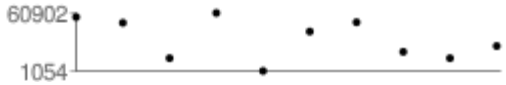
Your ISP's DNS resolver accepts generic glue records located in subdomains of the queried domain.

Your ISP's DNS resolver accepts additional (glue) records for nameservers located in subdomains of the queried domain.

Your ISP's DNS resolver follows CNAMEs when it is in the same domain.

DNS resolver port randomization: OK

Your ISP's DNS resolver properly randomizes its local port number.
The following graph shows DNS requests on the x-axis and the detected source ports on the y-axis.



DNS lookups of popular domains: Warning

You appear to be using OpenDNS as your DNS resolver. OpenDNS acts as a Man-in-the-Middle for some servers, returning the address of one of their servers that acts as an intermediary, rather than the final result. As a result, 1 lookup appears to be anomalous.

Name	IP Address	Reverse Name/SOA
www.google.com	208.67.217.230	google.navigation.opendns.com

74 of 74 popular names were resolved successfully. Show all names.

2 popular names have a mild anomaly. The ownership suggested by the reverse name lookup does not match our understanding of the original name. The most likely cause is the site's use of a Content Delivery Network. Show all names.

1 popular name has a mild anomaly: we are unable to find a reverse name associated with the IP address provided by your ISP's DNS server. This is most likely due to a slow responding DNS server or misconfiguration on the part of the domain owner. Show all names.

DNS results wildcarding: OpenDNS

You appear to be using OpenDNS. OpenDNS, by default, deliberately returns addresses even for domain names which should not resolve. Instead of an error, the DNS server returns an address of 208.67.217.132, which resolves to hit-nxdomain.opendns.com. You can inspect the resulting HTML content here.

This is central to OpenDNS's business model. In order to support an otherwise free service, OpenDNS presents the users with advertisements whenever they make a typo in their web browser. You can disable this behavior through the OpenDNS Dashboard.

The big problem with this behavior is that it can potentially break any network application which relies on DNS properly returning an error when a name does not exist.

The following lists your DNS server's behavior in more detail.

- www.{random}.com is mapped to 208.67.217.132.
- www.{random}.org is mapped to 208.67.217.132.
- fubar.{random}.com is mapped to 208.67.217.132.
- www.yahoo.cmo [sic] is mapped to 208.67.217.132.
- nxdomain.{random}.netalyzr.icsi.berkeley.edu is mapped to 208.67.217.132.

Host Properties

System clock accuracy: Warning

Your computer's clock is 41 seconds fast.

Browser properties: OK

The following parameters are sent by your web browser to all web sites you visit:

- User Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.1.2) Gecko/20090803 Fedora/3.5.2-2.fc11 Firefox/3.5.2
- Accept: text/html,application/xhtml+xml,application/xml; q=0.9,*/*; q=0.8
- Accept Language: en-us,en;q=0.5
- Accept Encoding: gzip,deflate
- Accept Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Feedback

Please take a moment to tell us about your network. All fields are optional. If you would like to contact us with questions about your results, please contact us with your session ID, or get in touch on the mailing list.

How is your machine connected to the network?

○ Wireless ○ Wired

Where are you right now?

○ At home

○ At work

○ In a public setting (wifi hotspot, Internet cafe, etc.)

○ Other (please describe in comments below)

Feel free to leave additional comments below.

Your email address:

Send Feedback

ID 43ca253f-12493-dde83883-62a5-4e15-8589 FAQs + ICSI