The ICSI Netalyzr

Start » Analysis » Results

Result Summary + – (help)

p54B93D72.dip0.t-ipconnect.de / 84.185.61.114

Recorded at 09:12 UTC (09:12 UTC), Jun 05 2018. Permalink. Client/server transcript.

Summary of Noteworthy Events + –

Major Abnormalities –

- We received unexpected and possibly dangerous results when looking up important names ↓
- Your DNS resolver returns IP addresses for names that do not exist ↓

Minor Aberrations –

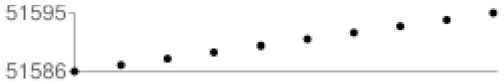
- Certain TCP protocols are blocked in outbound traffic ↓
- Network packet buffering may be excessive ↓
- Not all DNS types were correctly processed ↓
- Certain TCP protocols are blocked in outbound traffic ↓
- The path between our system and your network does not appear to handle fragmented IPv6 traffic properly ↓

Address-based Tests + –

NAT detection (?): NAT Detected –

Your global IP address is 84.185.61.114 while your local one is 192.168.2.102. You are behind a NAT.

Your machine numbers TCP source ports sequentially. The following graph shows connection attempts on the X-axis and their corresponding source ports used by your computer on the Y-axis.



TCP ports are not renumbered by the network.

Local Network Interfaces (?): OK –

Your computer reports the following network interfaces, with the following IP addresses for each one:

- eth0: (an ethernet interface)
- eth1: (an ethernet interface)
- eth10: (an ethernet interface)
- eth11: (an ethernet interface)
- eth12: (an ethernet interface)
- eth2: (an ethernet interface)
- eth3: (an ethernet interface)
- eth4: (an ethernet interface)
- eth5: (an ethernet interface)
- eth6: (an ethernet interface)
- eth7: (an ethernet interface)
- eth8: (an ethernet interface)
- eth9: (an ethernet interface)
- lo: (a local loopback interface)
  - 127.0.0.1 (an IPv4 loopback address)
  - ::1 (an IPv6 loopback address)

- net0:
- net1:
- net2:
- net3:
- net4:
- net5:
- net6:
- ppp0:
- wlan0:
  - 192.168.2.102 [DESKTOP-C6MBBBB.speedport.ip] (a private IPv4 address)
  - 2003:ce:8bcb:5739:1859:b2da:1fe4:b555 (probably a public IPv6 address)
  - 2003:ce:8bcb:5729:1859:b2da:1fe4:b555 [p200300CE8BCB57291859B2DA1FE4B555.dip0.t-ipconnect.de] (probably a public IPv6 address)
  - 2003:ce:8bcb:5729:21d5:cdbf:2e84:66ef (probably a public IPv6 address)
  - 2003:ce:8bcb:5739:21d5:cdbf:2e84:66ef (probably a public IPv6 address)
  - fe80::1859:b2da:1fe4:b555 [DESKTOP-C6MBBBB.speedport.ip] (a link-local IPv6 address)
- wlan1:
  - fe80::e9de:c8cc:fa9e:8eae (a link-local IPv6 address)
- wlan10:
- wlan11:
- wlan12:
- wlan13:
- wlan14:
- wlan15:
- wlan16:
- wlan17:
- wlan18:
- wlan19:
- wlan2:
  - fe80::29c3:678a:56da:42be (a link-local IPv6 address)
- wlan3:
- wlan4:
- wlan5:
- wlan6:
- wlan7:
- wlan8:
- wlan9:

DNS-based host information (?): OK –

You are not a Tor exit node for HTTP traffic.

You are listed on the Spamhaus Policy Based Blacklist, meaning that your provider has designated your address block as one that should only be sending authenticated email, email through the ISP's mail server, or using webmail.

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

NAT support for Universal Plug and Play (UPnP) (?): Not found –

UPnP broadcasts for NAT devices remained unanswered. Therefore your NAT does not appear to support UPnP, or your computer's firewall is filtering multicast responses.

Reachability Tests

TCP connectivity (?): Note –

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) is prohibited.
This means you cannot send email via SMTP to arbitrary mail servers. Such blocking is a common countermeasure against malware abusing infected machines for generating

spam. Your ISP likely provides a specific mail server that is permitted. Also, webmail services remain unaffected.

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 POP3 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 blocked.

Direct TCP access to remote secure IMAP servers (port 585) is allowed.

Direct TCP access to remote authenticated SMTP servers (port 587) is blocked.

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 OpenVPN servers (port 1194) is allowed.

Direct TCP access to remote PPTP Control servers (port 1723) is allowed.

Direct TCP access to remote SIP servers (port 5060) is allowed.

Direct TCP access to remote BitTorrent servers (port 6881) is allowed.

Direct TCP access to remote TOR servers (port 9001) is allowed.

UDP connectivity (?): OK

Basic UDP access is available.
The client was able to send fragmented UDP traffic.
The client was able to receive fragmented UDP traffic.

Direct UDP access to remote DNS servers (port 53) is allowed.

Direct UDP access to remote NTP servers (port 123) is allowed.

Direct UDP access to remote NetBIOS NS servers (port 137) is allowed.

Direct UDP access to remote NetBIOS DGM servers (port 138) is allowed.

Direct UDP access to remote IKE key exchange servers (port 500) is allowed.

Direct UDP access to remote OpenVPN servers (port 1194) is allowed.

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

Direct UDP access to remote L2 tunneling servers (port 1701) is allowed.

Direct UDP access to remote IPSec NAT servers (port 4500) is allowed.

Direct UDP access to remote RTP servers (port 5004) is allowed.

Direct UDP access to remote RTCP servers (port 5005) is allowed.

Direct UDP access to remote SIP servers (port 5060) is blocked.

Direct UDP access to remote VoIP servers (port 7078) is allowed.

Direct UDP access to remote VoIP servers (port 7082) is allowed.

Direct UDP access to remote SCTP servers (port 9899) is allowed.

Direct UDP access to remote Steam gaming servers (port 27005) is allowed.

Direct UDP access to remote Steam gaming servers (port 27015) is allowed.

Traceroute (?): OK

It takes 20 network hops for traffic to pass from our server to your system, as shown below. For each hop, the time it takes to traverse it is shown in parentheses.

1. *
2. *
3. *
4. *

5. *
6. 100.65.11.161 (0 ms)
7. 205.251.244.217 (1 ms)
8. 54.239.108.228 (2 ms)
9. 54.239.109.35 (2 ms)
10. 100.91.23.2 (6 ms)
11. 54.240.229.148 (6 ms)
12. 100.91.131.101 (6 ms)
13. 52.93.4.45 (7 ms)
14. 52.93.4.100 (6 ms)
15. ae-25.a01.nycmny01.us.bb.gin.ntt.net (6 ms)
16. ae-6.r08.nycmny01.us.bb.gin.ntt.net (6 ms)
17. ae-0.a01.nycmny13.us.bb.gin.ntt.net (6 ms)
18. 62.159.61.217 (6 ms)
19. 91.23.213.41 (97 ms)
20. p54B93D72.dip0.t-ipconnect.de (120 ms)

Path MTU (?): OK

The path between your network and our system supports an MTU of at least 2037 bytes, and the path between our system and your network has an MTU of 552 bytes. The bottleneck is at IP address 172.30.1.206.

Hidden Proxy Detection (?): OK

We detected no proxies using this test.

Network Access Link Properties

Network performance (?): Latency: 130 ms, Loss: 0.0%

The round-trip time (RTT) between your computer and our server is 130 ms, which is good.

We recorded no packet loss between your system and our server.

TCP connection setup latency (?): 120ms

The time it takes your computer to set up a TCP connection with our server is 120 ms, which is good.

Background measurement of network health (?): no transient outages

During most of Netalyzr's execution, the client continuously measures the state of the network in the background, looking for short outages. During testing, the client observed no such outages.

Network bandwidth (?): Upload 1.7 Mbit/s, Download 4.5 Mbit/s

Your Uplink: We measured your uplink's sending bandwidth at 1.7 Mbit/s. This level of bandwidth works well for many users.

Your Downlink: We measured your downlink's receiving bandwidth at 4.5 Mbit/s. This level of bandwidth works well for many users.
During this test, the client observed 2 reordered packets.

Network buffer measurements (?): Uplink 450 ms, Downlink 60 ms

We estimate your uplink as having 450 ms of buffering. This level may serve well for maximizing speed while minimizing the impact of large transfers on other traffic.

We estimate your downlink as having 60 ms 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

We detected no explicit sign of HTTP proxy via IP address changes.

Content-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

We detected no signs of a transparent HTTP cache in your network path.

JavaScript-based tests (?): OK

The client did not execute within a frame.

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

- netAlizEd = BaR (set by our server)
- netalyzrStatus = running (set by our server)

Your web browser is able to fetch an image using IPv6. Your network is IPv6 enabled.

Sensitive proxy-introduced HTTP headers (?): OK

No sensitive headers found.

DNS Tests

Restricted domain DNS lookup (?): OK

We can successfully look up 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 can successfully look up arbitrary names from the client. 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 217.237.151.89, which resolves to m-dns-a09.isp.t-ipnet.de. Additional nameservers observed for your host: 217.237.151.91, 217.237.151.94, 217.237.151.95.

DNS resolver properties (?): Lookup latency 350 ms

Your ISP's DNS resolver requires 350 ms to conduct an external lookup. It takes 160 ms for your ISP's DNS resolver to lookup a name on our server.

Your resolver correctly uses TCP requests when necessary.

Your resolver is using QTYPE=A for default queries.

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

Your DNS resolver requests DNSSEC records.

Your DNS resolver advertises the ability to accept DNS packets of up to 1680 bytes.

Your DNS resolver can successfully receive a smaller (~1400 byte) DNS response.

Your DNS resolver is unable to receive a large (>1500 byte) DNS response successfully, even though it advertises itself as EDNS-enabled.

Your DNS resolver accepts DNS responses of up to 1680 bytes.

Your resolver does not use 0x20 randomization.

Your ISP's DNS server cannot use IPv6.

No transport problems were discovered which could affect the deployment of DNSSEC.

Direct probing of DNS resolvers (?)

Internal Server Error on Test Report

DNS glue policy (?): OK

Your ISP's DNS resolver does not accept generic additional (glue) records — good.

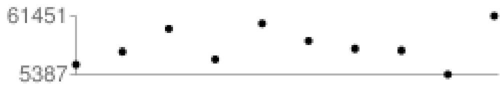
Your ISP's DNS resolver does not accept additional (glue) records which correspond to nameservers.

Your ISP's DNS resolver does not follow CNAMEs.

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

One popular name has a significant anomaly. The ownership suggested by the reverse name lookup does not match our understanding of the original name. This could be caused by an error somewhere in the domain information, deliberate blocking or redirection of a site using DNS, or it could be that your ISP's DNS Server is acting as a DNS "Man-in-the-Middle".

We attempted to download HTTP content from the IP addresses that your ISP's DNS server returned to you for these names. Where the download succeeded, you can click on the IP address in the table below to download a compressed file containing an HTTP session transcript.

Note! The session content is potentially harmful to your computer when viewed in a browser, so use caution when examining it.

Name	IP Address	Reverse Name/SOA
mail.live.com	204.79.197.212	a-0010.a-msedge.net

100 of 100 popular names were resolved successfully. Show all names.

48 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.

7 popular names have 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 external proxy (?): OK

Your host ignores external DNS requests.

DNS results wildcarding (?): Warning

Your ISP's DNS server returns IP addresses even for domain names which should not resolve. Instead of an error, the DNS server returns an address of 62.138.239.45, which does not resolve. You can inspect the resulting HTML content here.

There are several possible explanations for this behavior. The most likely cause is that the ISP is attempting to profit from customer's typos by presenting advertisements in response to bad requests, but it could also be due to an error or misconfiguration in the DNS server.

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 62.138.239.45.
- www.{random}.org is mapped to 62.138.238.45.
- fubar.{random}.com is mapped to 62.138.239.45.
- www.yahoo.cmo [sic] is mapped to 62.138.238.45.

- nxdomain.{random}.netalyzr.icsi.berkeley.edu is mapped to 62.138.238.45.

DNS-level redirection of specific sites (?): OK –

Your ISP does not appear to be using DNS to redirect traffic for specific websites.

Direct probing of DNS roots (?): OK –

We checked which DNS root server instances your computer can reach. All root servers responded. Show them.

IPv6 Tests

DNS support for IPv6 (?): OK –

Your system can successfully look up IPv6 addresses. Your DNS resolver is on Google's IPv6 "whitelist", which means that Google enables IPv6 access to their services for you.

IPv4, IPv6, and your web browser (?): OK –

Your browser successfully fetched a test image from our IPv6 server. Your browser prefers IPv6 over IPv4.

IPv6 connectivity (?): OK –

Your host was able to contact our IPv6 test server successfully. The requests originated from 2003:ce:8bcb:5739:21d5:cdbf:2e84:66ef.

It takes 224 ms for your computer to fetch a response from our test server using IPv6, while it takes 225 ms for the same host to fetch a response using IPv4 from the same server.

IPv6 TCP connectivity (?): Note –

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) is prohibited.
This means you cannot send email via SMTP to arbitrary mail servers. Such blocking is a common countermeasure against malware abusing infected machines for generating spam. Your ISP likely provides a specific mail server that is permitted. Also, webmail services remain unaffected.

Direct TCP access to remote POP3 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 blocked.

Direct TCP access to remote secure IMAP servers (port 585) is allowed.

Direct TCP access to remote authenticated SMTP servers (port 587) is blocked.

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 OpenVPN servers (port 1194) is allowed.

Direct TCP access to remote PPTP Control servers (port 1723) is allowed.

Direct TCP access to remote SIP servers (port 5060) is allowed.

Direct TCP access to remote BitTorrent servers (port 6881) is allowed.

Direct TCP access to remote TOR servers (port 9001) is allowed.

IPv6 Path MTU (?): Warning –

Your system can send and receive fragmented traffic with IPv6. The path between our system and your network does not appear to handle fragmented IPv6 traffic properly.

IPv6 Traceroute (?): Failed to complete

The test failed to execute completely, or the required results did not get uploaded to our server completely.

Network Security Protocols

DNSSEC Support from the DNS Roots (?): OK

All DNS root server instances returned proper DNSSEC information.

Host Properties

System clock accuracy (?): OK

Your computer's clock agrees with our server's clock.

Browser properties (?): OK

Your web browser sends the following parameters to all web sites you visit:

- User Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; LCTE; rv:11.0) like Gecko
- Accept: text/html, application/xhtml+xml, image/jxr, */*
- Accept Language: en-IN
- Accept Encoding: gzip, deflate
- Accept Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Java identifies your operating system as Windows 10.

Uploaded data (?): OK

The client uploaded the following additional content:

- apache_404
- custom_404
- nxpage
- plain_404
- raw_http_content

Feedback

User-provided feedback

Feel free to update your feedback below.

If you'd like to give us a way to contact you at a later time, please provide an email address. We will never share your address with anyone.

How is your machine/device connected to the local network?

● WiFi
○ Wired
○ Tethered via USB
○ Tethered via WiFi

Where are you right now?

☑ At home
□ At work
□ In a public setting (wifi hotspot, internet cafe, etc)
□ Other (please describe)

Feel free to leave additional comments here.

Update feedback

ID 369839a0-15435-9fde5a0d-7ae6-4fcb-8cdc

FAQs + Blog + Papers + Links + ICSI