

Network Assessment

Full Detail Report



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Scan Date: 07/08/2025

Prepared for: EndUsers

Prepared by: TEL5

07/08/2025

Table of Contents

01	Discovery Tasks
02	Assessment Summary
03	Other Endpoints
	3.1 Users
	3.2 Service Accounts
	3.3 Computers
	3.4 Server Aging
	3.5 Workstation Aging
04	Non A/D Devices
05	Servers
	5.1 MS SQL Servers
	5.2 Web Servers
	5.3 Time Servers
	5.4 Exchange Servers
	5.5 DHCP Servers
	5.6 Hyper-V Servers
	5.7 MacOS Database Servers
06	Printers
07	Network Shares
08	Major Applications
09	Patch Summary
10	Endpoint Security and Backup

1 - Discovery Tasks

This table contains a listing of all tasks which were performed as part of this assessment. Items which do not contain a check were not performed.

TASK	DESCRIPTION
✗ Detect Domain Controllers	Identifies domain controllers and online status.
✗ FSMO Role Analysis	Enumerates FSMO roles at the site.
✗ Enumerate Organization Units and Security Groups	Lists the organizational units and security groups (with members).
✗ User Analysis	Lists the users in AD, status, and last login/use, which helps identify potential security risks.
✓ Detect Local Accounts	Detects local accounts on computer endpoints.
✓ Detect Added or Removed Computers	Lists computers added or removed from the Network since the last assessment.
✗ Detect Local Mail Servers	Detects mail server(s) on the network.
✗ Detect Time Servers	Detects server(s) on the network.
✓ Discover Network Shares	Discovers the network shares by server.
✓ Detect Major Applications	Detects all major apps / versions and counts the number of installations.
✓ Detailed Domain Controller Event Log Analysis	Lists the event log entries from the past 24 hours for the directory service, DNS server and file replication service event logs.
✓ Web Server Discovery and Identification	Lists the web servers and type.
✓ Network Discovery for Non-A/D Devices	Lists the non-Active Directory devices responding to network requests.
✓ Internet Access and Speed Test	Tests Internet access and performance.
✓ SQL Server Analysis	Lists the SQL Servers and associated database(s).
✓ Internet Domain Analysis	Queries company domain(s) via a WHOIS lookup.

TASK		DESCRIPTION
✓	Missing Security Updates	Identifies computers missing security updates.
✓	System by System Event Log Analysis	Discovers the file system and app event log errors for servers.
✗	External Security Vulnerabilities	Lists the security holes and warnings from External Vulnerability Scan.

2 - Assessment Summary

LOCAL ACCOUNTS

# Enabled	2
Last Login Within 30 Days	1
Last Login Older Than 30 Days	1
# Disabled	11
Last Login Within 30 Days	0
Last Login Older Than 30 Days	11

ACTIVE DIRECTORY SECURITY GROUPS

Groups with Users	0
# Total Groups	0

OTHER COMPUTERS

Total Computers	4
Last Login Within 30 Days	3
Last Login Older Than 30 Days	1

OTHER COMPUTERS BY OS

Windows 11 Business Version 24H2	1
----------------------------------	---

OTHER COMPUTERS BY OS

Windows 11 Pro Version 24H2

2

MISCELLANEOUS

Non-A/D Systems

12

MX Records

1

MS SQL Servers

0

Web Servers

23

Printers

7

Exchange Servers

0

Network Shares

0

Installed Applications

76

Potential Insecure Listening Ports

0

3 - Other Endpoints

This section and corresponding sub-sections contain a comprehensive view of other endpoints not part of a Active Directory Domain or Workgroup.

3.1 - Users

This section contains a list of accounts with information on each account. Disabled accounts are highlighted in gray. Inactive users, defined as those that have not logged in 30 days, are highlighted in the Last Login column in **RED BOLD**. Accounts where passwords are set to never expire are highlighted in the Password Expires column in **RED**. Users with passwords that have expired are indicated in the Password Expires column in **RED BOLD**.

Accounts where compromised credentials were found using Dark Web ID after the most recent password change have their Password Last Set dates highlighted in **RED**.

COMPUTER NAME	ACCOUNT NAME	DISPLAY NAME	ENABLED	GROUPS	LAST LOGIN
LAPTOP-GEPIT4MJ	administrator		disabled	Administrators	<never>
LAPTOP-GEPIT4MJ	defaultaccount		disabled	System Managed Accounts Group	<never>
LAPTOP-GEPIT4MJ	guest		disabled	Guests	<never>
LAPTOP-GEPIT4MJ	wdagutilityaccount		disabled		<never>
EndUsersROY	administrator		enabled	Administrators	13/01/2025 9:08:55 AM
EndUsers-ROY	defaultaccount		disabled	System Managed Accounts Group	<never>
EndUsersROY	guest		disabled	Guests	<never>
EndUsersROY	wdagutilityaccount		disabled		<never>
EndUsers-NETDETECTI	administrator		disabled	Administrators	<never>
EndUsers-NETDETECTI	defaultaccount		disabled	System Managed Accounts Group	<never>

COMPUTER NAME	ACCOUNT NAME	DISPLAY NAME	ENABLED	GROUPS	LAST LOGIN
EndUsers-NETDETECTI	guest		disabled	Guests	<never>
TEndUsersNETDETECTI	EndUsersnetwork detect		enabled	Administrators	8/07/2025 9:33:37 AM
EndUsers-NETDETECTI	wdagutilityaccount		disabled		<never>

3.2 - Service Accounts

This section contains a list of service accounts with information on each account.

Enabled Service Accounts

No service accounts were found.

Disabled Service Accounts

No service accounts were found.

3.3 - Computers

This section contains a listing of other computers identified. Computers which have not logged in for over 30 days are highlighted in red.

Active Computers

COMPUTER NAME	IP ADDRESS(ES)	NETMASK	CIDR	DNS ENTRY	ENABLED	OPERATING SYSTEM	LAST LOGIN
LAPTOP-GEPI4MJ	fe80::cd97:3c91:8050:88a3%60,fe80::39a4:b7c0:f79d:d04a%59,fe80::ea35:28f3:2470:5b82%58,fe80::9317:1f17:f763:8e61%10,fe80::20b6:d085:c315:f769%16,fe80::3969:ea43:3316:e0ba%24,fe80::b68:94f0:bf28:a8c%23,fe80::c3a3:1817:bf07:6683%19,fe80::79bb:75b0:cd8b:4d0f%7,192.168.12.1,192.168.11.1,172.16.16.1,192.168.88.88,192.168.1.8,192.168.17.1,192.168.9.1,192.168.124.1,10.10.1.233	255.255.255.0	10.10.1.0/24	laptop-gepit4mj	enabled	Microsoft Windows 11 Business	08/07/2025 9:44:43 AM
T5-ROY	fe80::1c04:c6a7:84ed:238e%10,10.10.1.145	255.255.255.0	10.10.1.0/24	t5-roy	enabled	Microsoft Windows 11 Pro	08/07/2025 9:44:43 AM
EndUsers-NETDETECTI	10.10.1.180	255.255.255.0	10.10.1.0/24	tel5-netdetecti	enabled	Microsoft Windows 11 Pro	08/07/2025 9:44:43 AM

Inactive Computers

TEL5 PTY LTD
WWW.TEL5.COM.AU
0881005255
INFO@TEL5.COM.AU

Prepared for:
EndUsers
Scan Date:
07/08/2025

COMPUTER NAME	IP ADDRESS(ES)	NETMASK	CIDR	DNS ENTRY	ENABLED	OPERATING SYSTEM	LAST LOGIN
EndUsers- NETDETECTIVEPRO	104.21.94.65,172.67 .220.85			tel5- netdetectivepro.EndUser: m.au	enabled	Windows 10 Pro Version 24H2	

3.4 - Server Aging

This section is an indicator of the age of the active servers based on the date their operating system was installed. The actual age of the server may vary if the operating system was re-installed for any reason. Older systems are highlighted in red and much older systems are bolded. Excludes computers that we were unable to retrieve an OS Install Date.

No Servers with OS Install Date information were found.

3.5 - Workstation Aging

This section is an indicator of the age of the active workstations based on the date their operating system was installed. The actual age of the workstation may vary if the operating system was re-installed for any reason. Older systems are highlighted in red and much older systems are bolded. Excludes computers that we were unable to retrieve an OS Install Date.

COMPUTER	OPERATING SYSTEM	OS INSTALL DATE	AGE (MONTHS)
EndUsers-ROY	Windows 11 Pro Version 24H2	02/23/2025 3:12:10 AM	5
LAPTOP-GEPIT4MJ	Windows 11 Business Version 24H2	04/06/2025 8:12:38 PM	3
EndUsers-NETDETECTI	Windows 11 Pro Version 24H2	06/24/2025 6:55:17 PM	1

4 - Non A/D Devices

This section contains a listing of all devices which were not joined to a domain or workgroup.

IP ADDRESS	COMPUTER NAME	LISTENING PORT(S)	DEVICE TYPE
10.10.1.15		DNS (53/TCP), HTTP (80/TCP), HTTPS (443/TCP)	
10.10.1.22		DNS (53/TCP), HTTP (80/TCP), HTTPS (443/TCP)	
10.10.1.27	ADAM-LAPTOP.LOCAL		
10.10.1.33		DNS (53/TCP), HTTP (80/TCP), HTTPS (443/TCP)	
10.10.1.40		HTTP (80/TCP)	GS110TP
10.10.1.41		HTTP (80/TCP), HTTPS (443/TCP)	
10.10.1.74			
10.10.1.78	THEG6XBEAST.LOCAL		
10.10.1.80			
10.10.1.90	CAMERA.TEL5.COM.AU	HTTP (80/TCP)	DNVRS-Webs
10.10.1.112	DB1.LOCAL	HTTPS (443/TCP), HTTP (8080/TCP)	
10.10.1.137			
10.10.1.138			
10.10.1.140	TINA.LOCAL		

IP ADDRESS	COMPUTER NAME	LISTENING PORT(S)	DEVICE TYPE
10.10.1.162		DNS (53/TCP), HTTP (80/TCP), HTTPS (443/TCP)	
10.10.1.164			
10.10.1.173	EndUsers-BACKUPS.LOCAL	HTTPS (443/TCP), HTTP (8080/TCP)	
10.10.1.175	PRINTER.EndUsers	HTTP (80/TCP), HTTPS (443/TCP)	Lexmark CX921de version CXTMH.230.329 kernel 5.4.254- yocto-standard All-N-1
10.10.1.179		SSH (22/TCP), HTTP (80/TCP)	Apache/2.4.62 (Debian)
10.10.1.188	EndUsers-SUPPORT.LOCAL	RDP (3389/TCP)	
10.10.1.195		HTTP (80/TCP), HTTPS (443/TCP)	embed httpd
10.10.1.209		SSH (22/TCP), HTTP (80/TCP), HTTPS (443/TCP)	openresty
10.10.1.210		SSH (22/TCP)	
10.10.1.211			
10.10.1.213	LT-03.LOCAL		
10.10.1.216			
10.10.1.221		HTTP (80/TCP), HTTPS (443/TCP)	
10.10.1.225		DNS (53/TCP), HTTP (80/TCP), HTTPS (443/TCP)	
10.10.1.227			
10.10.1.230		SSH (22/TCP)	
10.10.1.232		SSH (22/TCP)	

IP ADDRESS	COMPUTER NAME	LISTENING PORT(S)	DEVICE TYPE
10.10.1.241	SIP-T46U_DYLAN.TEL5.COM.AU	DNS (53/TCP), HTTP (80/TCP), HTTPS (443/TCP)	
10.10.1.243		HTTP (80/TCP), HTTPS (443/TCP)	
10.10.1.246		DNS (53/TCP), HTTP (80/TCP), HTTPS (443/TCP)	
10.10.1.247		DNS (53/TCP), HTTP (80/TCP), HTTPS (443/TCP)	embed httpd
10.10.1.248		DNS (53/TCP), HTTP (80/TCP), HTTPS (443/TCP)	
10.10.1.249		DNS (53/TCP), HTTP (80/TCP), HTTPS (443/TCP)	
10.10.1.250		SSH (22/TCP)	
10.10.1.251		SSH (22/TCP), HTTP (80/TCP), SFTP (115/TCP), HTTPS (443/TCP)	XCC Web Server
10.10.1.254	MY.FIREWALL	SSH (22/TCP), DNS (53/TCP), HTTP (80/TCP), POP (110/TCP), IMAP (143/TCP), HTTPS (443/TCP)	

5 - Servers

This section and corresponding sub-sections contain a comprehensive listing of servers by type, which are then categorized by domain or workgroup membership.

5.1 - MS SQL Servers

No MS SQL servers were discovered.

5.2 - Web Servers

Other

IP ADDRESS	WEB SERVER NAME	LISTENING PORT(S)	SERVER TYPE
10.10.1.15		80/TCP, 443/TCP	
10.10.1.22		80/TCP, 443/TCP	
10.10.1.33		80/TCP, 443/TCP	
10.10.1.40		80/TCP	Web Server
10.10.1.41		80/TCP, 443/TCP	
10.10.1.90	CAMERA	80/TCP	DNVRS-Webs
10.10.1.112	DB1	443/TCP, 8080/TCP	
10.10.1.162		80/TCP, 443/TCP	

IP ADDRESS	WEB SERVER NAME	LISTENING PORT(S)	SERVER TYPE
10.10.1.173	EndUsers-BACKUPS	443/TCP, 8080/TCP	
10.10.1.175	PRINTER	80/TCP, 443/TCP	Web_Server
10.10.1.179		80/TCP	Apache/2.4.62 (Debian)
10.10.1.195		80/TCP, 443/TCP	embed httpd
10.10.1.209		80/TCP, 443/TCP	openresty
10.10.1.221		80/TCP, 443/TCP	
10.10.1.225		80/TCP, 443/TCP	
10.10.1.241	SIP-T46U_DYLAN	80/TCP, 443/TCP	
10.10.1.243		80/TCP, 443/TCP	
10.10.1.246		80/TCP, 443/TCP	
10.10.1.247		80/TCP, 443/TCP	embed httpd
10.10.1.248		80/TCP, 443/TCP	
10.10.1.249		80/TCP, 443/TCP	
10.10.1.251		80/TCP, 443/TCP	XCC Web Server
10.10.1.254	MY	80/TCP, 443/TCP	

5.3 - Time Servers

No Time Servers were discovered.

5.4 - Exchange Servers

No Exchange Servers were discovered.

5.5 - DHCP Servers

IP ADDRESS(ES)	SERVER NAME	ERRORS (LAST 24 HOURS)
10.10.1.254	my.firewall	

5.6 - Hyper-V Servers

No Hyper-V Servers were discovered.

5.7 - MacOS Database Servers

No macOS Servers were discovered.

6 - Printers

This section contains a listing of all printers categorized by a combination of domain or workgroup membership and method of access. Alerts for SNMP-enabled printers are also displayed in red.

Other (from WMI)

IP ADDRESS	PRINTER NAME	ACCESSED FROM	LOCATION	COMMENT
192.168.12.1, 192.168.11.1, 172.16.16.1, 192.168.88.88, 192.168.1.8, 192.168.17.1, 192.168.9.1, 192.168.124.1, 10.10.1.233	EndUsers-CX921de	LAPTOP-GEPIT4MJ	http://10.10.1.175:65001	
10.10.1.145	AnyDesk Printer			
10.10.1.145	Brother HL-L2350DW series			Brother HL-L2350DW series
10.10.1.145	ET788C77EA71DC		http://10.10.1.174:65001	
10.10.1.145	KONICAMINOLTA-bizhub-C300i-47-5F-ED			KONICAMINOLTA-bizhub-C300i-47-5F-ED
10.10.1.145	ZDesigner ZQ521 (ZPL)			

Networked (from SNMP)

IP ADDRESS	PRINTER NAME	HOSTNAME	DESCRIPTION	ALERTS
10.10.1.175	Tel5-CX921de	PRINTER.TEL5.COM.AU	Lexmark CX921de version	

TEL5 PTY LTD
WWW.TEL5.COM.AU
0881005255
INFO@TEL5.COM.AU

Prepared for:
EndUsers
Scan Date:
07/08/2025

IP ADDRESS	PRINTER NAME	HOSTNAME	DESCRIPTION	ALERTS
			CXTMH.230.329 kernel 5.4.254- yocto-standard All-N-1	

7 - Network Shares

This section contains a listing of all network shares categorized first by domain or workgroup membership, and then by machine.

Other

HOSTED BY	SHARE UNC
LAPTOP-GEPIT4MJ	\\LAPTOP-GEPIT4MJ\ADMIN\$, \\LAPTOP-GEPIT4MJ\C\$, \\LAPTOP-GEPIT4MJ\IPC\$
EndUsers-ROY	\\T5-ROY\ADMIN\$, \\T5-ROY\C\$, \\T5-ROY\IPC\$
EndUsers-NETDETECTI	\\TEL5-NETDETECTI\ADMIN\$, \\TEL5-NETDETECTI\C\$, \\TEL5-NETDETECTI\IPC\$
EndUsersNETDETECTIVEPRO	\\10.10.1.180\ADMIN\$, \\10.10.1.180\C\$, \\10.10.1.180\IPC\$

No NFS Shares were discovered.

8 - Major Applications

This section contains a listing of major applications with corresponding version numbers and the number of computers the application was detected on. Applications that appear on more than three computers are highlighted in gray for easy recognition.

Other

Windows Applications

APPLICATION NAME	VERSION	# COMPUTERS
4G Mobile Hotspot	1.0	1
7-Zip 24.09 (x64)	24.09	1
Adobe Acrobat (64-bit)	25.001	1
Advanced IP Scanner 2.5.1	2.5	2
Advanced Port Scanner 2.5	2.5	1
Angry IP Scanner	3.9	1
AnyDesk	ad 9.0	1
Bing Wallpaper	2.0	1
Check Point SmartConsole R81.20	6.10	1
Check Point VPN	98.61	1
Customer Support	1.0	1
draw.io 27.0.9	27.0	1
Driver Support One	2.7	1

APPLICATION NAME	VERSION	# COMPUTERS
Microsoft Bing Service	2.0	1
Microsoft Edge	137.0	2
Microsoft Edge WebView2 Runtime	122.0	1
Microsoft OneDrive	25.095	1
Microsoft OneDrive	25.105	1
Microsoft Teams Meeting Add-in for Microsoft Office	1.25	2
Microsoft Update Health Tools	5.72	2
Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030	11.0	1
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501	12.0	2
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501	12.0	2
Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.40.33810	14.40	1
Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.44.35208	14.44	1
Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.38.33135	14.38	1
Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.40.33810	14.40	1
Microsoft Visual Studio Installer	3.6	1
Mozilla Firefox (x64 en-US)	139.0	1
Mozilla Maintenance Service	138.0	1
Network Detective Remote Data Collector	1.0	1
Nmap 7.97	7.97	2
Node.js	20.12	1

TEL5 PTY LTD
WWW.TEL5.COM.AU
0881005255
INFO@TEL5.COM.AU

Prepared for:
EndUsers
Scan Date:
07/08/2025

APPLICATION NAME	VERSION	# COMPUTERS
Npcap	1.82	2
OpenVPN 2.6.5-l001 amd64	2.6	1
PuTTY release 0.78 (64-bit)	0.78	1
PuTTY release 0.83 (64-bit)	0.83	1
Python Launcher	3.12	1
ScreenConnect Client (b629293d870707cd)	25.4	2
Sophos Connect	2.4	1
Splashtop for RMM	3.5	1
TeamViewer	15.42	1
VanDyke Software SecureCRT and SecureFX 9.6	9.6	1
Visual Studio Build Tools 2019	16.11	1
VMware Workstation	17.6	1
WeChat	3.9	1
Windows 11 Installation Assistant	1.4	1
Windows Driver Package - Lexmark International Printer (01/28/2016 2.15.0.0)	01/28/2016 2.15	1
Windows Driver Package - Lexmark International Printer (10/02/2015 3.0.6.0)	10/02/2015 3.0	1
Yealink USB Connect	4.40	1
Zebra Font Downloader		1
Zebra Setup Utilities	1.1	1

APPLICATION NAME	VERSION	# COMPUTERS
Zebra Status Monitor 5.1.3		1
ZebraDesigner 3	3.2	1
Zoom Workplace	6.5	1
Zoom Workplace (64-bit)	6.4	1



9 - Patch Summary

This section contains the patching status of computers determined through Windows Update. Windows Update checks the local computer for all non-hidden updates. Missing updates in both areas are highlighted in red. Security and critical updates are bolded.

Windows Updates





ISSUE	RESULT	ASSESSMENT
Drivers: BenQ - Display - BenQ GL2440H (Digital)	Failed (non-critical)	1 update is missing.
Drivers: Dell Inc. - Bus Controllers and Ports, Display - Dell P2210 (Analog)	Failed (non-critical)	1 update is missing.
Drivers: Intel - System - 9/19/2017 12:00:00 AM - 11.7.0.1000	Failed (non-critical)	1 update is missing.
Drivers: Intel Corporation - HDC - 17.8.1.1066	Failed (non-critical)	1 update is missing.
Drivers: Intel Corporation - System - 10/8/2018 12:00:00 AM - 30.100.1841.2	Failed (non-critical)	1 update is missing.
Drivers: Lenovo Ltd. - Firmware - 1.50.0.0	Failed (non-critical)	1 update is missing.
Drivers: Realtek - Net - 7/5/2017 12:00:00 AM - 10.19.705.2017	Failed (non-critical)	1 update is missing.
Updates	Failed (non-critical)	1 update is missing.
Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
Drivers: BenQ - Display - BenQ GL2440H (Digital)	Failed (non-critical)	1 update is missing.

10 - Endpoint Security and Backup

This section contains a listing of detected anti-virus, anti-spyware, firewall, and backup information as detected through  Security Center and/or  Installed Services for major vendors. This list is categorized by domain or workgroup membership.

The 'Name' column contains either the name of the product, **None** indicating the that machine returned information but no product was found, or <empty> indicating that information was not obtainable. Additionally, a status of ✓ indicates 'yes', ✗ indicates 'no', or <empty> indicates that a status was not available.

Other

COMPUTER NAME	ANTI-VIRUS			ANTI-SPYWARE			FIREWALL		BACKUP	
	NAME	ON	CURRENT	NAME	ON	CURRENT	NAME	ON	NAME	CURRENT
LAPTOP-GEPI4MJ	 Windows Defender	✓	✓	 Windows Defender	✓	✓	 Windows Firewall	✓	None	
EndUsers-ROY	 Windows Defender	✓	✓	 Windows Defender	✓	✓	 Windows Firewall	✓	None	
EndUsers-NETDETECTI	 Windows Defender	✓	✓	 Windows Defender	✓	✓	 Windows Firewall	✓	None	

11 - Remote Listening Ports

This section contains a list of common ports/protocols assessed, and is categorized by domain or workgroup membership. Items with a red check indicate a potential risk.

Other

IP ADDRESS	COMPUTER NAME	SSH (22/TCP)	DNS (53/TCP)	HTTP (80/TCP)	POP (110/TCP)	SFTP (115/TCP)	IMAP (143/TCP)	HTTPS (443/TCP)	RDP (3389/TCP)	HTTP (8080/TCP)
10.10.1.15			✓	✓				✓		
10.10.1.22			✓	✓				✓		
10.10.1.33			✓	✓				✓		
10.10.1.40				✓						
10.10.1.41				✓				✓		
10.10.1.90	CAMERA			✓						
10.10.1.112	DB1							✓		✓
10.10.1.162			✓	✓				✓		
10.10.1.173	EndUsers-BACKU							✓		✓
10.10.1.175	PRINTER			✓				✓		
10.10.1.179		✓		✓						

12 - Internet Access

This section lists the latency between the computer and both Google and Yahoo, as well as a trace route to Google for further diagnostics if needed.

INTERNET ACCESS

Latency Tests:

Retrieval time for Google.com: 200 ms

Retrieval time for Yahoo.com: -1 ms

Internet trace route to Google.com:

Tracing route to www.google.com [142.250.70.132] over a maximum of 30 hops:

```
13 msmy.firewall [10.10.1.254]
23 ms125-254-76-36.static.as58511.net [125.254.76.36]
33 msvl5.cor1.ydch.au.as58511.net [103.30.217.42]
45 mspo10-7.bdr1.ydch1.au.as58511.net [103.30.216.5]
512 msvl7.cor1.ydch.au.as58511.net [103.30.216.4]
612 msae2.cor101.ydch1.au.as58511.net [103.30.216.106]
712 mshu0-0-1-0.msr101.ydch1.au.as58511.net [103.30.216.99]
815 msbe2.msr102.ndcm1.au.as58511.net [103.30.217.22]
94851 ms
1012 msae0-200g.bdr101.m1.au.as58511.net [103.30.217.149]
1115 msas15169.lnk.as58511.net [103.17.220.121]
1216 ms142.250.234.151
1314 ms142.250.230.159
1415 msmel04s01-in-f4.1e100.net [142.250.70.132]
```

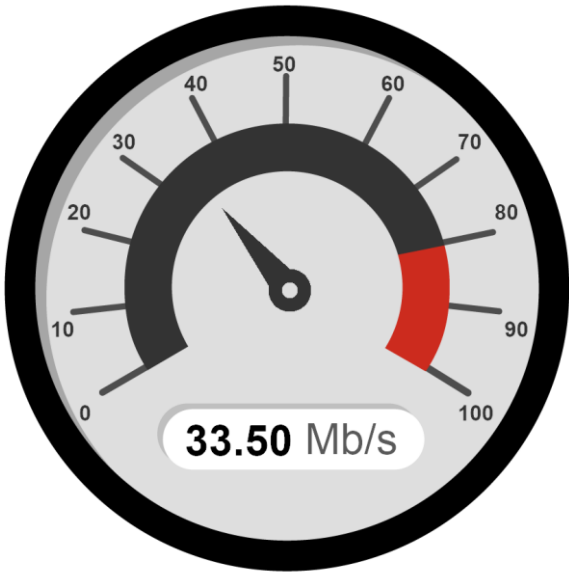
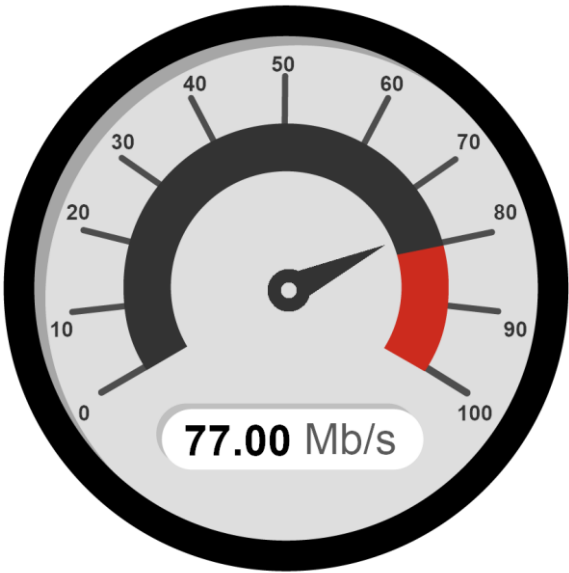
Trace complete.

13 - External Speed Test

This section displays upload and download speed.

DOWNLOAD SPEED: 77.0 MB/S

UPLOAD SPEED: 33.5 MB/S



NDT SERVER	LOCATION	DOWNLOAD	UPLOAD
ndt-mlab1-chs02.mlab-oti.measurement-lab.org	Atlanta, Georgia	45.0 Mb/s	7.6 Mb/s
ndt-mlab1-mel02.mlab-oti.measurement-lab.org	CLOSEST	77.0 Mb/s	33.5 Mb/s
ndt-mlab3-ord06.mlab-oti.measurement-lab.org	Chicago, Illinois	43.4 Mb/s	7.2 Mb/s