Willie de Klerk

Student Number: 20230254

Student Year: 2 (2024)

Module: WIL620

Exit Level Outcome: 4

CTU training solutions
Private Tertiary Education Provider

Declaration of Authenticity

A critical aspect of any assignment is *authenticity*. Because you are completing much of the work for the assignments *unsupervised*, the examiner must be convinced that it is all your work. For this reason, you must complete the *Declaration of Authenticity* provided in the study guide and have it counter-signed by your manager, mentor, or lecturer.

NB	The declaration of authenticity is a legal document, and if found that you have made a false declaration, then not only will your results be declared null and void, but you could also have criminal charges brought against you. It is not worth taking the risk!

Please complete the declaration of authenticity below for all assignments:

DECLARATION OF AUTHENTICITY

I _____WILLIE DE KLERK_____ hereby

declare that the contents of this assignment are entirely my work except for the following documents: (List the documents and page numbers of work in this portfolio that were generated in a group)

Activity	Date
WIL620 Exit Level Outcome 4	**2024/07/26**

Signature: _____  _____ **Date:** _____**2024/07/26**____

Company/Mentor Stamp

Contents

Declaration of Authenticity *1*
An overview **3**
Diving into the mtr tool **3**
Some prerequisite knowledge 4
Hosting provider 4
ISP 4
3 Tier ISP Networking Model 5
Running mtr from campus **6**
Running mtr from home to linode server **7**
Creating a diagnostic baseline with mtr **8**
Bibliography **9**

An overview

The mtr tool can be used to visualize diagnostic path based information with regards to the hops my data takes to certain destinations. The mtr tool and the reports generated by its use serves the purpose of identifying the specific fault domain that is causing high packet loss (or complete packet loss) and abnormal latency.

The fault domains can be viewed as and split into administrative domains, of which am noticing a few key main categories:

1. Infrastructure provider

You can have faults before you even reach the internet service provider. This responsibility would fall onto your respective infrastructure provider. Examples of what you can expect to find here would be client access, the first hop router, the modem, the last mile and the kerb box, and the transmission systems towards the isp.

You cannot blame your Infrastructure Provider when you have issues with your hosting provider's administrative domain, however a last mile issue, or someone breaking into and messing with the kerb box would be valid at this domain.

It is important to note that there is a Demarcation point that would split the responsibility of the Infrastructure provider and the Customer. A key point found here would be the Customer Premises Equipment if the customer would be supplying it themselves via alternative means not provided or administered by the isp or infrastructure provider. Demarcation Point (Halabi & McPherson, 2000) Customer Premises Equipment (Halabi & McPherson, 2000)

2. Internet Service Provider

ISPs have their own core infrastructure, data centres and peerings with upstream networks. You cannot blame your internet service provider for problems with your infrastructure experiencing localized congestion.

3. The "internet"

The "internet" can be seen as a fault domain with there being numerous tier 1 networks and submarine cables that can have problems causing severe packet loss and high latency.

4. Hosting Provider or destination node

Hosting providers have redundancy and resiliency, however unlikely systems do fail. You can have issues with the setup of a destination node that is outside of the hosting provider's line of responsibility and into the customer's line of responsibility, making it their sys admin's problem. You cannot blame your hosting provider for not opening, or closing a port on your vps after you have launched and accessed it. AWS Shared Responsibility Model (aws.amazon.com, 2024)

Diving into the mtr tool

mtr is a network diagnostic tool that combines the functionality found in traceroute and ping tools into one package.

When running an mtr scan the tool will determine the next hop address of each network hop between the nodes. ICMP echo requests are used to determine link quality between each of the nodes, printing the statistics for each hop.(www.bitwizard.nl)

In addition to outlining the route that traffic takes across the Internet there is information collected by mtr such as state, connection and the response time between the hosts in an intermediate format.

What is ICMP and how does it work?

ICMP is a connectionless protocol used for error handling at the network layer to report and troubleshoot errors. Fundamentally ICMP works to respond and report errors if there are two devices struggling to communicate on the network layer.

This reporting in tools such as mtr takes place through messages such as the echo request and echo reply along with the time exceeded message and redirect message. (ICMP)

Some prerequisite knowledge

An understanding of concepts such as a hosting provider and the three tier isp networking model is required along with foundational knowledge regarding connection and peering types.

Hosting provider

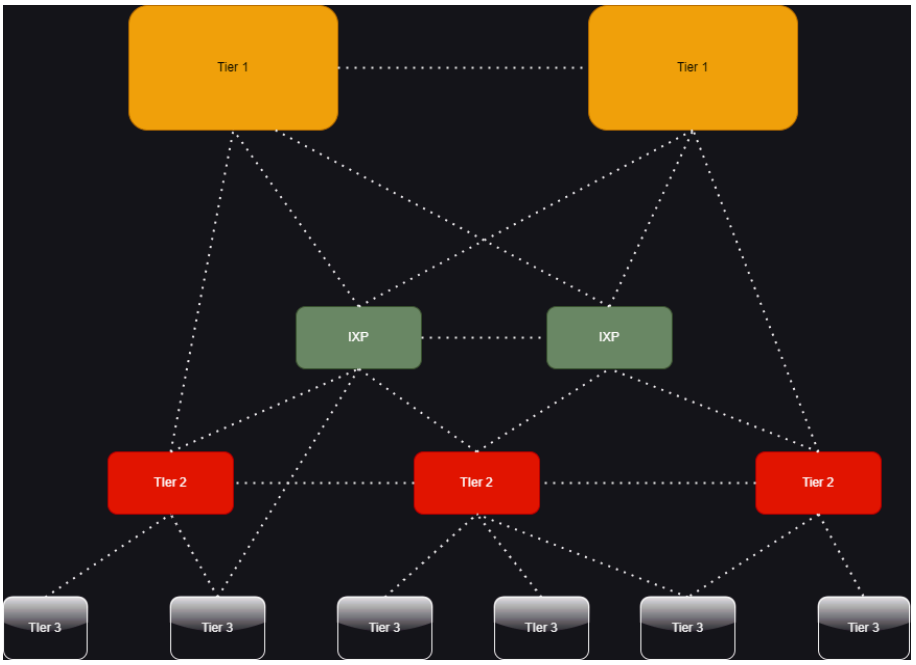
A hosting provider provides a company with infrastructure needed for hosting their programs and business products.This includes the computational infrastructure and network infrastructure. They provide cost savings and flexible pricing based on a businesses personal needs and work on a pay-as-you-go pricing model. Examples of hosting providers would include: AWS, Akamai (linode).

This would be where companies such as CTU Training Solutions would be hosting their website: ctutraining.ac.za. Or a personal use would be where a student is hosting their blog server. williedeklerk.com

ISP

Broken down to the basic conceptual view, an ISP is not the internet as we will see at a later section. An Internet Service provider only connects businesses and homes to the internet. They are only the “last mile” in the path that packets from the “internet” take to get to your local network. Broadly speaking, when most people refer to an ISP they are referring to either tier 2 or tier 3 networks.

3 Tier ISP Networking Model



Tier 1:

They are seen as the backbone of the internet. They build or lease the cables on the ocean floor between continents, and thereby have a global reach. All other ISPs connect to this network, however end users and businesses do not connect to them. A list of tier 1 networks can be found here: [Tier 1 network - Wikipedia]

The tier 2 networks that connect to the tier 1 networks have to buy access to their network (pay transit fees). The tier 1 networks have links between each other, but they do not charge for those connections and connect through private BGP peerings. They connect to internet exchange points as well. They can be thought of as the core layer.

Tier 2:

They are service providers that pay transit fees to the Tier 1 networks. They often connect to each other as well as internet exchange points. Another key distinction is that they do not have global reach and they are categorized to have a regional or statewide reach. They can be thought of as the distribution layer.

Tier 3:

These service providers are connecting to tier 2 networks and they pay transit fees for everything that they do. Although unlikely, they can have leases from more than one tier 2 networks as well as a connection to an Internet Exchange Point (IXP).

These networks often have a local reach and can be thought of as the access layer if compared to the ent routing and switching 3 tier model. With that being said, they connect the businesses (through private peerings) and homes (PPPoE) to the global internet.

BGP Public and Private Peerings.

Private Peering:

A direct, physical connection between two ISPs, eg. the link between the two tier 1 networks with an agreement on traffic exchange. Another example of a private peering would be where a company connects to an ISP network through BGP (Typical in dual-homed environments).

Public Peering:

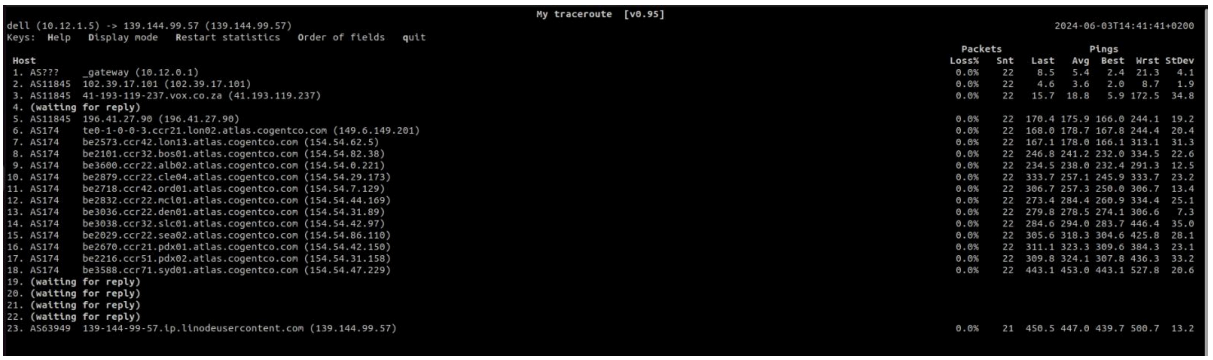
A public peering relationship is formed at internet exchange points, and is used for the exchange of traffic across service provider networks.

ISP 3-Tier Model Reference 1 (Cisco Thousand Eyes, 2024)

ISP 3-Tier Model Reference 2 (geeksforgeeks, 2020)

Tier 1 ISP Networks Reference (Winther, 2006)

Running mtr from campus



Above is an mtr run that I performed from my pc at CTU potchefstroom campus to a vps with the hosting being provided by linode.

At first glance

LAN 10.12.0.0 255.255.254.0

Starting from above we can see that my pc (dell) has a local IP address of 10.12.1.5 provided by the campus dhcp server. My pc has been given the default route of 10.12.0.1 through which we will be sending out our traffic to the regional ISP known as Vox Telecom.

ISP AS11854

When our traffic reaches the assigned IP address of 102.39.17.101 we will be entering the ISP's network with internal hops towards their connection with the tier 1 network through an internet exchange point.

AS174

At an exchange point not shown in the mtr output we find a connection from our Vox Telecom isp network into the Global Tier 1 network known as Cogent Communications.

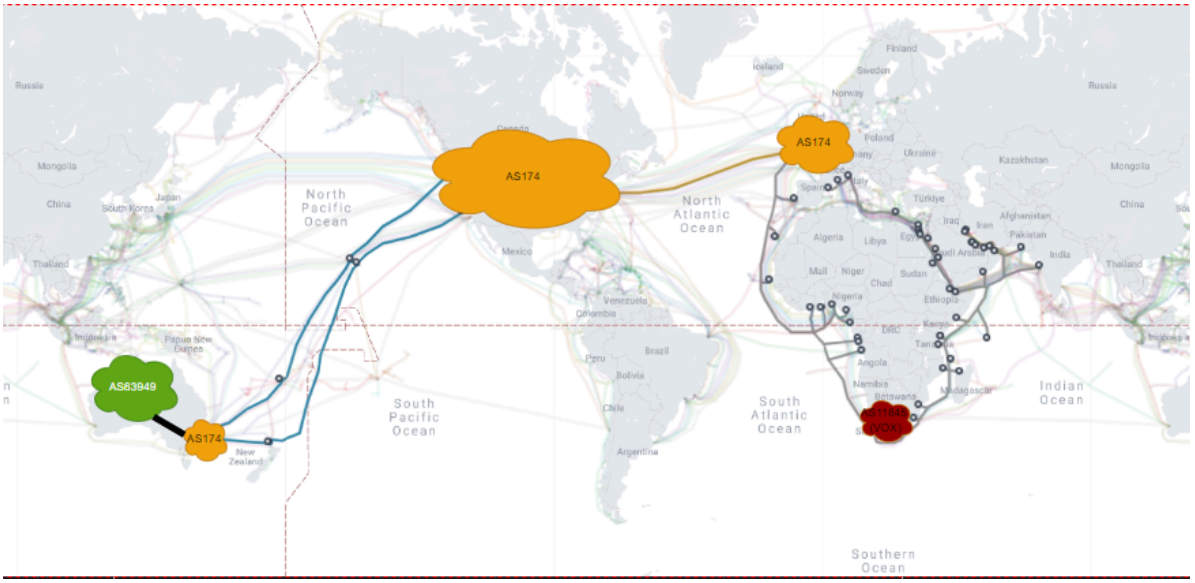
Within Cogent Communications we take a path internal to their AS going through multiple hops going through continents and cities towards the exit point where the packets reach the hosting provider's network.

AS63949 Hosting Provider

This is the network of the hosting provider where the vps is located.

ASN	IP Addresss	Country	Region	City	LAT	LONG
AS11845	102.39.17.101	South Africa	Gauteng	Johannesburg	-26.2022	28.0436
AS11845	41.193.119.237	South Africa	Gauteng	Johannesburg	-26.2022	28.0436
AS174	149.6.149.201	United Kingdom	England	London	51.5085	-0.1257
AS174	154.54.62.5	United Kingdom	England	London	51.5085	-0.1257
AS174	154.54.82.38	United States	Massachussets	Boston	42.3585	-71.0601
AS174	154.54.0.221	United States	Albany	New York	42.6526	-73.7562
AS174	154.54.29.173	United States	Ohio	Cleveland	41.4992	-81.6959
AS174	154.54.7.192	United States	District of Columbia	Washington	38.8954	-77.0395
AS174	154.54.44.169	United States	Missosouri	Kansas City	39.0997	-94.5786
AS174	154.54.31.89	United States	Colarado	Denver	39.7394	-104.9836
AS174	154.54.42.97	United States	Utah	Salt Lake City	40.7608	-111.8911
AS174	154.54.86.110	United States	Washington	Seattle	47.6043	-122.3298
AS174	154.54.54.150	United States	District of Columbia	Washington	38.9016	-77.0508
AS174	154.54.31.158	United States	Oregon	Portland	45.5235	-122.6765
AS174	154.54.47.229	Austrailia	New South Wales	Sydney	-33.8678	151.2070
AS63949	139.144.99.57	Austrailia	New South Wales	Sydney	-33.8678	151.2070

Taking the following values into account we can see that our tier 1 network does in fact have a global reach. I am unsure which cables are exactly used however this is a good estimate if we take the location data into account. The highlighted values indicate where there would be an international hop through an underwater cable. I have left out any exchange points that may be in place since I am not able to see them within the mtr output.

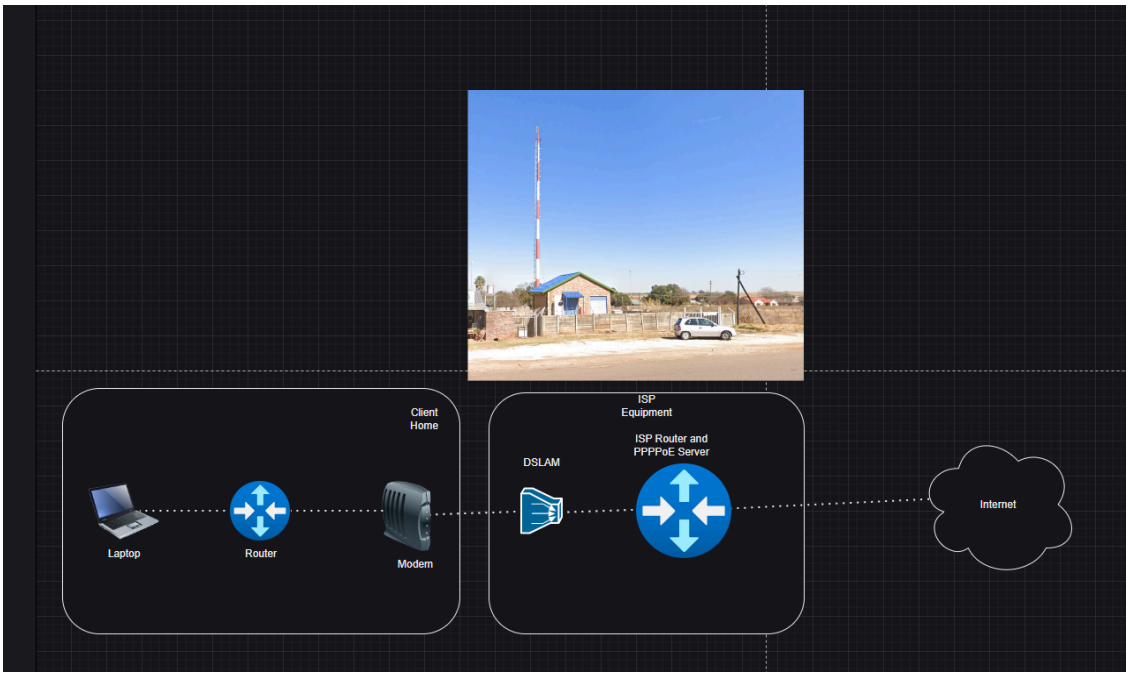


Running mtr from home to linode server

```
                                                My traceroute  [v0.95]
dell (192.168.88.12) -> 139.144.99.57 (139.144.99.57)                                                2024-06-03T22:19:10+0200
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                                                  Packets               Pings
 Host                                                                          Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. AS???    _gateway (192.168.88.1)                                           0.0%    16    2.6   2.8   2.2   5.3   1.0
 2. AS7018   adsl-172-10-0-1.dsl.sndg02.sbcglobal.net (172.10.0.1)             0.0%    16    7.5   7.6   7.0   8.4   0.4
 3. AS328137 core.cr-xe-01.jb1.za.wecom.net.za (160.119.232.77)               0.0%    16    7.3   8.0   7.3  11.0   1.1
 4. AS328137 core.pe-xe-ip01.jb1.za.ws.net.za (160.119.224.18)                0.0%    16    8.0   8.9   7.4  25.5   4.5
 5. AS3491   63.222.112.192 (63.222.112.192)                                   0.0%    16    9.0   8.8   8.0  11.8   1.0
 6. AS3491   63.218.151.2 (63.218.151.2)                                       0.0%    16    8.5   8.4   7.1  11.0   0.8
 7. AS174    be4429.ccr41.lon13.atlas.cogentco.com (154.54.5.34)               0.0%    16  169.1 169.7 168.3 172.9   1.1
 8. AS174    be2099.ccr31.bos01.atlas.cogentco.com (154.54.82.34)              0.0%    16  243.5 247.9 243.2 309.0  16.3
 9. AS174    be3599.ccr21.alb02.atlas.cogentco.com (66.28.4.237)               0.0%    16  244.8 244.6 243.9 247.3   0.9
10. AS174    be2878.ccr21.cle04.atlas.cogentco.com (154.54.26.129)             0.0%    16  257.2 257.5 256.9 259.2   0.5
11. AS174    be2717.ccr41.ord01.atlas.cogentco.com (154.54.6.221)              0.0%    16  257.4 273.1 255.9 386.2  36.1
12. AS174    be2831.ccr21.mci01.atlas.cogentco.com (154.54.42.165)             0.0%    16  277.0 286.4 276.8 411.0  34.5
13. AS174    be3035.ccr21.den01.atlas.cogentco.com (154.54.5.89)               0.0%    16  285.9 291.3 285.4 368.8  21.4
14. AS174    be3037.ccr21.slc01.atlas.cogentco.com (154.54.41.145)             0.0%    16  308.0 308.6 307.9 310.9   0.7
15. AS174    be3284.ccr22.sea02.atlas.cogentco.com (154.54.44.73)              0.0%    15  319.8 322.3 318.6 345.8   6.8
16. AS174    be2670.ccr21.pdx01.atlas.cogentco.com (154.54.42.150)             0.0%    15  310.6 311.1 310.5 312.4   0.6
17. AS174    be2216.ccr51.pdx02.atlas.cogentco.com (154.54.31.158)             0.0%    15  325.9 330.0 323.6 409.2  21.9
18. AS174    be3588.ccr71.syd01.atlas.cogentco.com (154.54.47.229)             0.0%    15  329.8 329.4 326.9 357.4   7.8
19. AS???    204.130.243.7 (204.130.243.7)                                     0.0%    15  341.6 329.8 326.2 341.6   5.9
20. (waiting for reply)
21. (waiting for reply)
22. (waiting for reply)
23. AS63949  139-144-99-57.ip.linodeusercontent.com (139.144.99.57)            0.0%    15  326.6 326.8 325.6 328.5   0.6
```

Looking at this mtr output I can see that my internal network is 192.168.88.0 with my default gateway being 192.168.88.1, from there I can see that I am connecting to my ISP's infrastructure via a modem and authenticating myself via PPPoE.

My packets then make their way to my ISP's Tier 2 network, through their core infrastructure and then to the "internet" via two Tier 1 networks with a global reach, finally making it to my hosting provider and my vps.



Creating a diagnostic baseline with mtr.

Having a baseline mtr report to compare against when trouble finds you along your path is a good practice that can help businesses to identify new paths or latency spikes.

Implementation of mtr in tcp mode is not good for route based diagnosis. Implementing an mtr report in tcp mode is an exceptionally resourceful way of determining whether firewall rules on a router along the way are blocking a specific protocol or port. Without good data troubleshooting will be a nightmare. Advanced MTR techniques

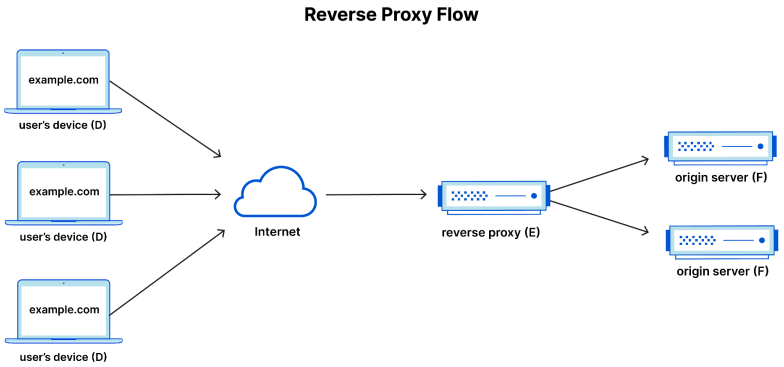
A problem such as the above could arise when changes are made to port forwarding rules. (IP Tables)

Example of something that should be blocked

```
masteryoda@dell:~$ sudo mtr -4 --tcp --port 22 --report -b --report-cycles 10 www.news24.com
Start: 2024-06-04T13:54:53+0200
HOST: dell                          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- _gateway (192.168.88.1)      0.0%    10   27.2  13.7   1.1  89.4  27.7
  2.|-- adsl-172-10-0-1.dsl.sndg0    0.0%    10  149.4  38.8   7.5 149.4  53.0
  3.|-- core.cr-xe-01.jb1.za.weco    0.0%    10   99.2 125.9   6.3 1026. 318.2
  4.|-- core.pe-xe-ip01.jb1.za.ws    0.0%    10   48.9  15.0   7.3  48.9  13.0
  5.|-- cloudflare.ixp.joburg (19    0.0%    10    7.9  23.0   6.1 139.2  41.0
  6.|-- 172.68.41.3                  0.0%    10  153.0 146.6   8.5 1034. 317.0
        197.234.240.21
  7.|-- ???                         100.0    10    0.0   0.0   0.0   0.0   0.0
```

In the mtr report output shown above I have set mtr to make use of tcp mode and port 22. I limited report-cycles since generating more traffic will not open the port.

Looking at this it is visible that the particular news outlet that I have chosen (www.news24.com) is making use of cloudflare's features to proxy their website. reverse proxy



Looking at the above it is visible that all traffic is being dropped at our last node (loss = 100.0%). In this specific case, this is good news since we do not want anyone to just have access to ports such as port 22 just for the fun of it. Other ports include ports to database servers. Zero Trust Model

Example of something that should be open.

```
masteryoda@dell:~$ sudo mtr -4 --tcp --port 443 --report -b --report-cycles 10 www.news24.com
Start: 2024-06-04T13:55:23+0200
HOST: dell                        Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- _gateway (192.168.88.1)    0.0%    10    0.8   0.8   0.7   0.8   0.0
  2.|-- adsl-172-10-0-1.dsl.sndg0  0.0%    10    4.9   6.4   4.9  10.6   1.6
  3.|-- core.cr-xe-01.jb1.za.weco  0.0%    10 1024. 108.1   5.7 1024. 322.0
  4.|-- core.pe-xe-ip01.jb1.za.ws  0.0%    10    6.1   6.2   5.2   6.6   0.4
  5.|-- cloudflare.ixp.joburg (19  0.0%    10    7.1  13.3   7.1  33.1   9.5
  6.|-- 197.234.240.21             0.0%    10    5.5   7.3   5.5   9.7   1.1
      172.68.41.3
  7.|-- 104.17.250.6               0.0%    10    6.6 107.3   6.1 1015. 319.0
masteryoda@dell:~$
```

In the example shown above, I have chosen to once again run mtr in tcp mode however on port 443 (used for https) which should allow an illustration of how things should look for a news website that is reachable with no loss at the last node. If there was a fault we would have seen loss indicating the port is blocked via firewall rules.

It is important to have a baseline to compare to before you make changes to a service,if something changes and indicates a fault you will have something to show you how things should be.

A tcp mtr can be executed on a daily basis and the report data can be aggregated to create a comprehensive report to log a fault with the appropriate support team or service/hosting provider.

Bibliography

aws.amazon.com, 2024. Shared Responsibility Model. [Online] Available at: https://aws.amazon.com/compliance/shared-responsibility-model/#:~:text=Customers%20are%20responsible%20for%20managing,also%20extends%20to%20IT%20controls. [Accessed 04 06 2024].

BitWizardB.V., 2024. BitWizard B.V. MTR | What is MTR?. [Online] Available at: https://www.bitwizard.nl/mtr/ [Accessed 04 06 2024].

Cisco Thousand Eyes, 2024. Cisco Thousand Eyes | ISP 3-Tier Model. [Online] Available at: https://www.thousandeyes.com/learning/techtorials/isp-tiers [Accessed 04 06 2024]. developers.cloudflare.com, 2024.

Cloudflare Docs | What is a reverse proxy?. [Online] Available at: https://developers.cloudflare.com/learning-paths/zero-trust-webaccess/concepts/reverse-proxy-server/ [Accessed 04 06 2024]. developers.cloudflare.com, 2024.

Cloudflare Docs | What is Zero Trust?. [Online] Available at: https://developers.cloudflare.com/learning-paths/zero-trust-webaccess/concepts/zero-trust/ [Accessed 04 06 2024].

geeksforgeeks, 2020. geeks for geeks | Internet Service Provider (ISP) hierarchy. [Online] Available at: https://www.geeksforgeeks.org/internet-service-provider-isp-hierarchy/ [Accessed 04 06 2024]. geeksforgeeks, 2024.

Geeks for Geeks | Internet Control Message Protocol (ICMP). [Online] Available at: https://www.geeksforgeeks.org/internet-control-message-protocol-icmp/ [Accessed 04 06 2024].

Halabi, S. & McPherson, D., 2000. Internet Routing Architectures, Second Edition | The Contemporary Internet | ISP Services and Characteristics | ISP Service Pricing, ServiceLevel Agreements, and Techinical Characteristics //Customer Premises Equipment. [Online] Available at:https://learning.oreilly.com/library/view/internet-routing-architectures/157870233X/157870233X_ch02lev1sec2.html#:-:text=Customer%20Premises%20Equipment,of%20ISP%20packages.. [Accessed 04 06 2024].

Halabi, S. & McPherson, D., 2000. Internet Routing Architectures, Second Edition | The Contemporary Internet | ISP Services and Charactersitics | ISP Service Pricing, ServiceLevel Agreements, and Technical Characteristics//Demarcation Point. [Online] Available at: https://learning.oreilly.com/library/view/internet-routing-architectures/157870233X/157870233X_ch02lev1sec2.html#:-:text=Demarcation%20Point,a%20customer%20network.[Accessed 04 06 2024].

Kalpan, B., 2018. Diagnosing Network Issues with MTR | Advanced MTR Techniques. [Online] Available at: https://www.linode.com/docs/guides/diagnosing-network-issues-with-mtr/ [Accessed 04 06 2024]. Kaplan, B., 2018.

Akamai Docs | Diagnosing Network Issues with MTR. [Online] Available at: https://www.linode.com/docs/guides/diagnosing-network-issues-with-mtr/ [Accessed 04 06 2024].

TeleGeography, 2024. Submarine Cable Map. [Online] Available at: https://www.submarinecablemap.com/ [Accessed 04 06 2024].

Winther, M., 2006. White Paper | Tier 1 ISPs: What They Are and Why They Are Important. [Online] Available at: https://web.archive.org/web/20100803003541/http://www.us.ntt.net/downloads/papers/IDC_Tier1_ISPs.pdf [Accessed 04 06 2024].

PeeringDB, 2024. PeeringDB. [Online] Available at: https://www.peeringdb.com/ [Accessed 04 06 2024].