Networking Troubleshooting

Hands-On Activity 5A (from CIS 2347)

Trinity Klein
UNIVERSITY OF HOUSTON Professor Jose Martinez CIS 3367 Section 15873

Trinity Klein
23 October 2024

Network Troubleshooting

Table of Contents

Task 1: Complete Networking Hands-On Activity 5A (from CIS 2347)

Using TCP/IP

IPCONFIG

```
C:\Users\trini>whoami
ssense\trini

C:\Users\trini>date/t
Wed 10/23/2024

C:\Users\trini>time/t
03:56 PM

C:\Users\trini>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : SSENSE
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : attlocal.net

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 68-7A-64-C4-4A-9C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : attlocal.net
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
   Physical Address. . . . . . . . . : 68-7A-64-C4-4A-9B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2600:1700:407c:30f:dd41:56b3:d9fb:19d8(Preferred)
   Temporary IPv6 Address. . . . . . : 2600:1700:407c:30f:ac13:a338:ee47:2d4a(Preferred)
   Link-local IPv6 Address . . . . . : fe80::3d0e:3ece:2f7:539%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.63.1.29(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Lease Obtained. . . . . . . . . . : Tuesday, October 22, 2024 10:22:27 PM
   Lease Expires . . . . . . . . . . : Wednesday, October 23, 2024 10:22:26 PM
   Default Gateway . . . . . . . . . : fe80::ea9f:80ff:fed5:4702%12
                                       10.63.1.1
   DHCP Server . . . . . . . . . . . : 10.63.1.1
   DHCPv6 IAID . . . . . . . . . . . : 107510372
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2E-8D-DB-7A-68-7A-64-C4-4A-9B
   DNS Servers . . . . . . . . . . . : 10.63.1.1
                                       2600:1700:407c:30f:ea9f:80ff:fed5:4702
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       attlocal.net

C:\Users\trini>
```

Every computer on the Internet will need an IP address, the same way everyone who drives on the road needs a driver's license—to facilitate safe communication between others while identifying the users/computers. IP addresses allow data to be sent and communicated to the correct device when sending out information online.

PING, Finding Other Computers

PING Commands

```
C:\Users\trini>whoami
ssense\trini

C:\Users\trini>date/t
Wed 10/23/2024

C:\Users\trini>time/t
03:57 PM

C:\Users\trini>ping 10.63.1.29

Pinging 10.63.1.29 with 32 bytes of data:
Reply from 10.63.1.29: bytes=32 time<1ms TTL=128
Reply from 10.63.1.29: bytes=32 time<1ms TTL=128
Reply from 10.63.1.29: bytes=32 time<1ms TTL=128
Reply from 10.63.1.29: bytes=32 time<1ms TTL=128

Ping statistics for 10.63.1.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\trini>ping google.com

Pinging google.com [2607:f8b0:4023:1004::64] with 32 bytes of data:
Reply from 2607:f8b0:4023:1004::64: time=15ms
Reply from 2607:f8b0:4023:1004::64: time=15ms
Reply from 2607:f8b0:4023:1004::64: time=16ms
Reply from 2607:f8b0:4023:1004::64: time=16ms

Ping statistics for 2607:f8b0:4023:1004::64:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 16ms, Average = 15ms

C:\Users\trini>ping www.cityu.edu.hk

Pinging az-cityuwaf.eastasia.cloudapp.azure.com [20.205.100.61] with 32 bytes of data:
Reply from 20.205.100.61: bytes=32 time=290ms TTL=103
Reply from 20.205.100.61: bytes=32 time=289ms TTL=103
Reply from 20.205.100.61: bytes=32 time=201ms TTL=103
Reply from 20.205.100.61: bytes=32 time=210ms TTL=103

Ping statistics for 20.205.100.61:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 201ms, Maximum = 290ms, Average = 247ms

C:\Users\trini>ping www.anu.edu.au

Pinging terra-web.anu.edu.au [130.56.67.33] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 130.56.67.33:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\trini>ping www.uh.edu

Pinging www.uh.edu [129.7.97.54] with 32 bytes of data:
Reply from 129.7.97.54: bytes=32 time=79ms TTL=239
Reply from 129.7.97.54: bytes=32 time=25ms TTL=239
Reply from 129.7.97.54: bytes=32 time=24ms TTL=239
Reply from 129.7.97.54: bytes=32 time=24ms TTL=239

Ping statistics for 129.7.97.54:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 79ms, Average = 38ms

C:\Users\trini>
```

ARP: Displaying Physical Addresses

ARP -A Commands

```
C:\Users\trini>arp -a

Interface: 10.63.1.29 --- 0xc
  Internet Address      Physical Address      Type
  10.63.1.1             e8-9f-80-d5-47-02     dynamic
  10.63.1.92            e8-9f-80-d2-8e-a4     dynamic
  10.63.1.154           e4-f0-42-2a-52-9a     dynamic
  10.63.1.228           74-d6-37-e8-19-67     dynamic
  10.63.1.255           ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.253       01-00-5e-7f-ff-fd     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\trini>whoami
ssense\trini

C:\Users\trini>date/t
Wed 10/23/2024

C:\Users\trini>time/t
04:04 PM
```

ARP -A Commands Continued

```
C:\Users\trini>ping 10.63.1.1

Pinging 10.63.1.1 with 32 bytes of data:
Reply from 10.63.1.1: bytes=32 time=1ms TTL=64
Reply from 10.63.1.1: bytes=32 time=1ms TTL=64
Reply from 10.63.1.1: bytes=32 time=2ms TTL=64
Reply from 10.63.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 10.63.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\trini>arp -a

Interface: 10.63.1.29 --- 0xc
  Internet Address      Physical Address      Type
  10.63.1.1             e8-9f-80-d5-47-02     dynamic
  10.63.1.92            e8-9f-80-d2-8e-a4     dynamic
  10.63.1.154           e4-f0-42-2a-52-9a     dynamic
  10.63.1.228           74-d6-37-e8-19-67     dynamic
  10.63.1.255           ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.253       01-00-5e-7f-ff-fd     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\trini>whoami
ssense\trini

C:\Users\trini>date/t
Wed 10/23/2024

C:\Users\trini>time/t
05:14 PM
```

ARP tables are used to map IP addresses to the MAC addresses in a local network. When a device wants to communicate with another device, it needs the MAC address of the destination, and the ARP will store this data. The lack of entries in an ARP table can be a problem, but it will depend on whether network communication has started or not. If network communication is expected and the table is empty, then it becomes a problem: but if communication has not started yet, then it is not a problem. If there are frequent problems with latency or efficiency, then the table will be continuously empty, meaning there may be a problem at hand.

DNS Cache

IPCONFIG /DISPLAYDNS

```
C:\Users\trini>whoami
ssense\trini

C:\Users\trini>date/t
Wed 10/23/2024

C:\Users\trini>time/t
04:06 PM

C:\Users\trini>ipconfig /displaydns

Windows IP Configuration

    fe3cr.delivery.mp.microsoft.com
    ----------------------------------------
    Record Name . . . . . : fe3cr.delivery.mp.microsoft.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 951792
    Data Length . . . . . : 8
    Section . . . . . : Answer
    CNAME Record  . . . . : fe3.delivery.mp.microsoft.com


    Record Name . . . . . : fe3.delivery.mp.microsoft.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 951792
    Data Length . . . . . : 8
    Section . . . . . : Answer
    CNAME Record  . . . . : glb.cws.prod.dcat.dsp.trafficmanager.net


    Record Name . . . . . : glb.cws.prod.dcat.dsp.trafficmanager.net
    Record Type . . . . . : 28
    Time To Live  . . . . : 951792
    Data Length . . . . . : 16
    Section . . . . . : Answer
    AAAA Record . . . . . : 2603:1030:408:7::3d


    fe3cr.delivery.mp.microsoft.com
    ----------------------------------------
    Record Name . . . . . : fe3cr.delivery.mp.microsoft.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 951734
    Data Length . . . . . : 8
    Section . . . . . : Answer
    CNAME Record  . . . . : fe3.delivery.mp.microsoft.com
```

There are approximately 980 entries in my cache.

IPCONFIG /DISPLAYDNS | FIND /C 'Record Name'

```
C:\Users\trini>ipconfig /displaydns | find /c "Record Name"
980

C:\Users\trini>whoami
ssense\trini

C:\Users\trini>date/t
Wed 10/23/2024

C:\Users\trini>time/t
05:02 PM
```

IPCONFIG /DISPLAY DNS of www6.ietf.com

```
www6.ietf.com
----------------------------------------
Record Name . . . . . : www6.ietf.com
Record Type . . . . . : 5
Time To Live  . . . . : 953802
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : www10.smartname.com


www6.ietf.com
----------------------------------------
No records of type AAAA


Record Name . . . . . : www6.ietf.com
Record Type . . . . . : 5
Time To Live  . . . . : 954004
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : www10.smartname.com


Record Name . . . . . : www10.smartname.com
Record Type . . . . . : 1
Time To Live  . . . . : 954004
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 15.197.204.56
```

NSLOOKUP: Finding IP Addresses

NSLOOKUP Command

```
C:\Users\trini>whoami
ssense\trini

C:\Users\trini>date/t
Wed 10/23/2024

C:\Users\trini>time/t
04:12 PM

C:\Users\trini>nslookup www.google.com
Server:  Sniffme.attlocal.net
Address:  10.63.1.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2607:f8b0:4023:1006::69
          2607:f8b0:4023:1006::93
          2607:f8b0:4023:1006::63
          2607:f8b0:4023:1006::68
          142.250.114.103
          142.250.114.106
          142.250.114.104
          142.250.114.105
          142.250.114.147
          142.250.114.99


C:\Users\trini>nslookup www.cnn.com
Server:  Sniffme.attlocal.net
Address:  10.63.1.1

Non-authoritative answer:
Name:    cnn-tls.map.fastly.net
Addresses:  2a04:4e42:2b::773
          151.101.183.5
Aliases:  www.cnn.com
```

TRACERT: Finding Routes Through the Internet

TRACERT Command

```
C:\Users\trini>whoami
ssense\trini

C:\Users\trini>date/t
Wed 10/23/2024

C:\Users\trini>time/t
04:19 PM

C:\Users\trini>tracert www.google.com

Tracing route to www.google.com [2607:f8b0:4023:1004::69]
over a maximum of 30 hops:

  1     1 ms     3 ms     1 ms  2600:1700:407c:30f:ea9f:80ff:fed5:4702
  2     *        *        *     Request timed out.
  3    63 ms     4 ms     3 ms  2001:506:6000:12f:69:235:120:248
  4    64 ms     4 ms     4 ms  2001:506:6000:12f:69:235:120:246
  5     *        *        *     Request timed out.
  6    68 ms    11 ms    11 ms  2001:1890:fff:f6e:12:255:10:124
  7    72 ms    14 ms    15 ms  2607:f8b0:825e::1
  8    71 ms    16 ms    14 ms  2001:4860:0:1::6ff8
  9    73 ms    12 ms    12 ms  2001:4860:0:1::88fa
 10    69 ms    12 ms    12 ms  2001:4860::c:4001:e559
 11    82 ms    14 ms    15 ms  2001:4860::c:4002:17b0
 12    72 ms    17 ms    14 ms  2001:4860::cc:4002:c2d7
 13    71 ms    12 ms    12 ms  2001:4860:0:1::41f3
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25    14 ms    13 ms    11 ms  rq-in-f105.1e100.net [2607:f8b0:4023:1004::69]

Trace complete.

C:\Users\trini>
```

It took about 25 hops on the network for the packet to reach Google. The shortest hop, in terms of time, was the first hop at 3ms. It was the shortest hop because it had the least amount of distance to travel on the internet – thus making it take a lesser amount of time.

Task 2: List possible failure points for a request

1. User device or network failure
2. DNS (AWS Route 53) resolution failure
3. CloudFront distribution problems
4. API gateway issues
5. ELB failure
6. EC2 instance failure
7. Auto scaling group misconfiguration
8. NAT gateway issues
9. AWS lambda failure
10. RDS unavailability
11. AWS VPC misconfiguration
12. Misconfiguration IAM Policy

Works Cited

OpenAI. (2024). *ChatGPT* [Large language model]. https://chatgpt.com

Reference Architecture Examples and Best Practices. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/architecture/?cards-all.sort-by=item.additionalFields.sortDate&cards-all.sort-order=desc&awsf.content-type=