Troubleshooting TCP / UDP Issues

Aaron Staines
NETWORK/SYSTEM ENGINEER | CCISO

Module Overview

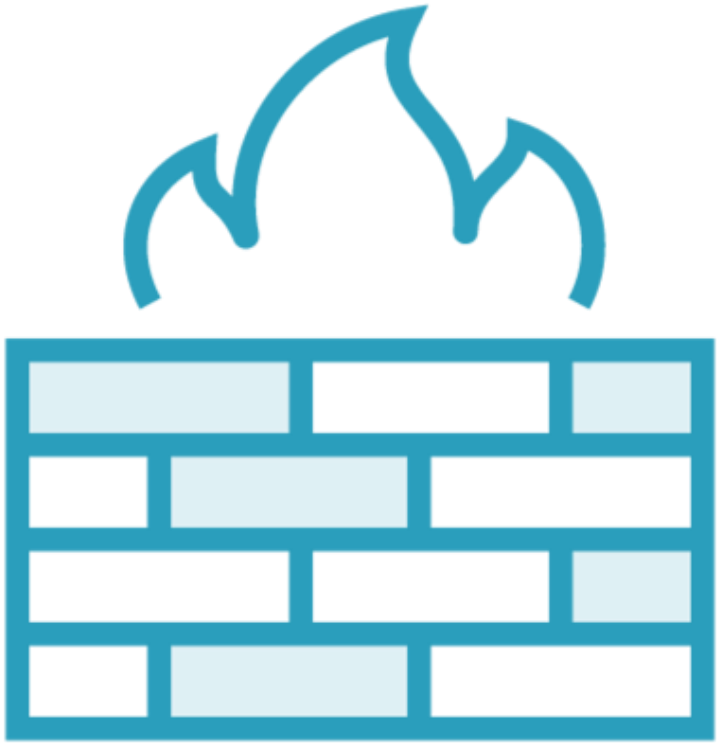
- TCP
  - Firewall issues
  - DNAT
  - VPN – MTU/MSS

Module Overview

- UDP
  - Firewall issues
  - Incorrectly configured services

TCP Firewall Issues

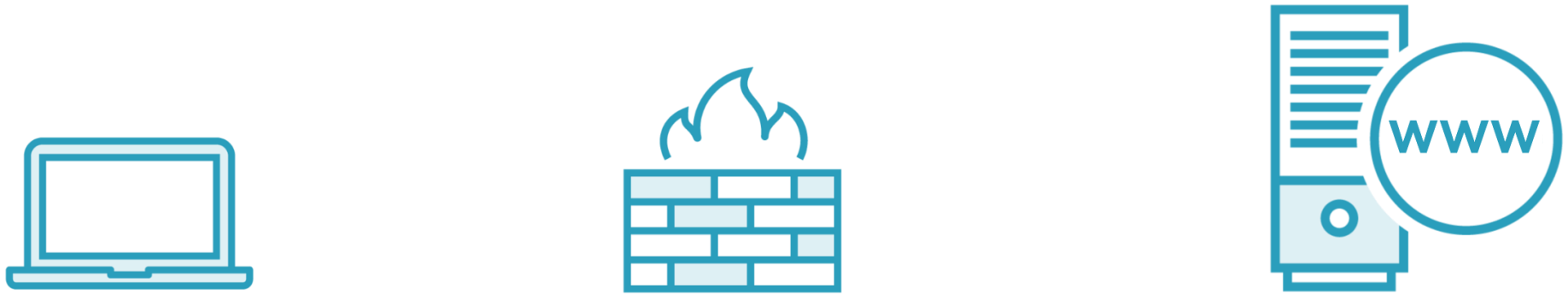
TCP Firewall Issues



Top firewall issues

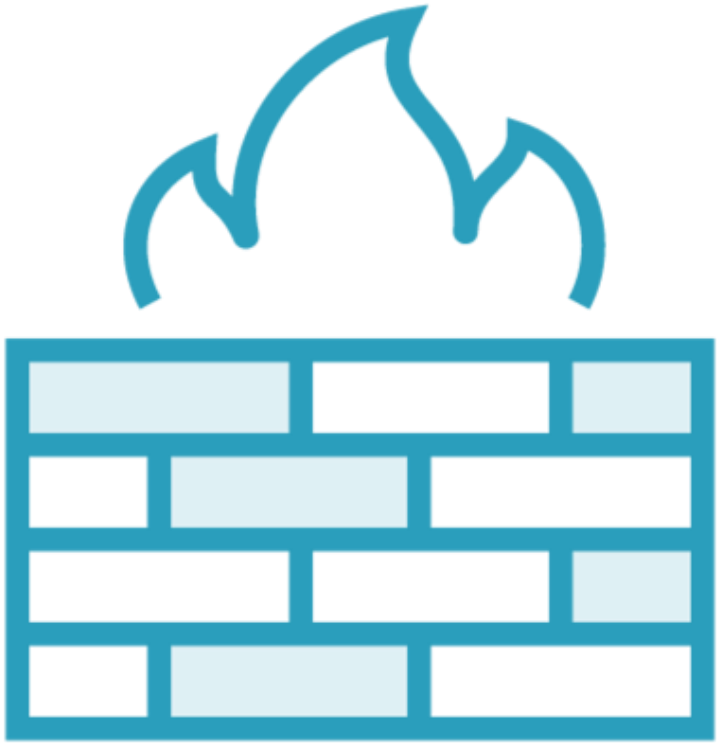
- Misconfigured addresses
- Misconfigured ports
- Incorrect firewall direction/zone
- Incorrect order

TCP Firewall Issues




www

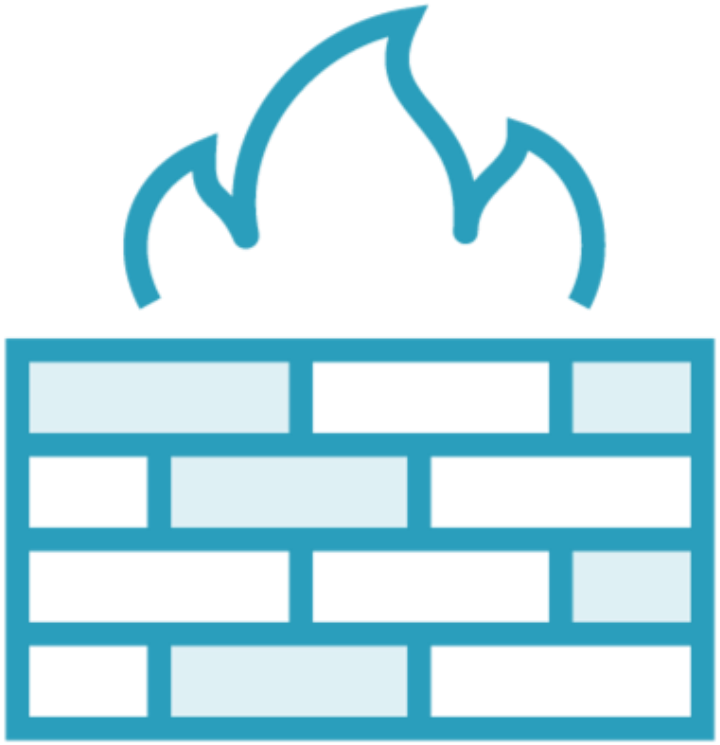
TCP Firewall Issues



Firewall direction

- 2 modes
  - Zone based
    - Default – deny everything

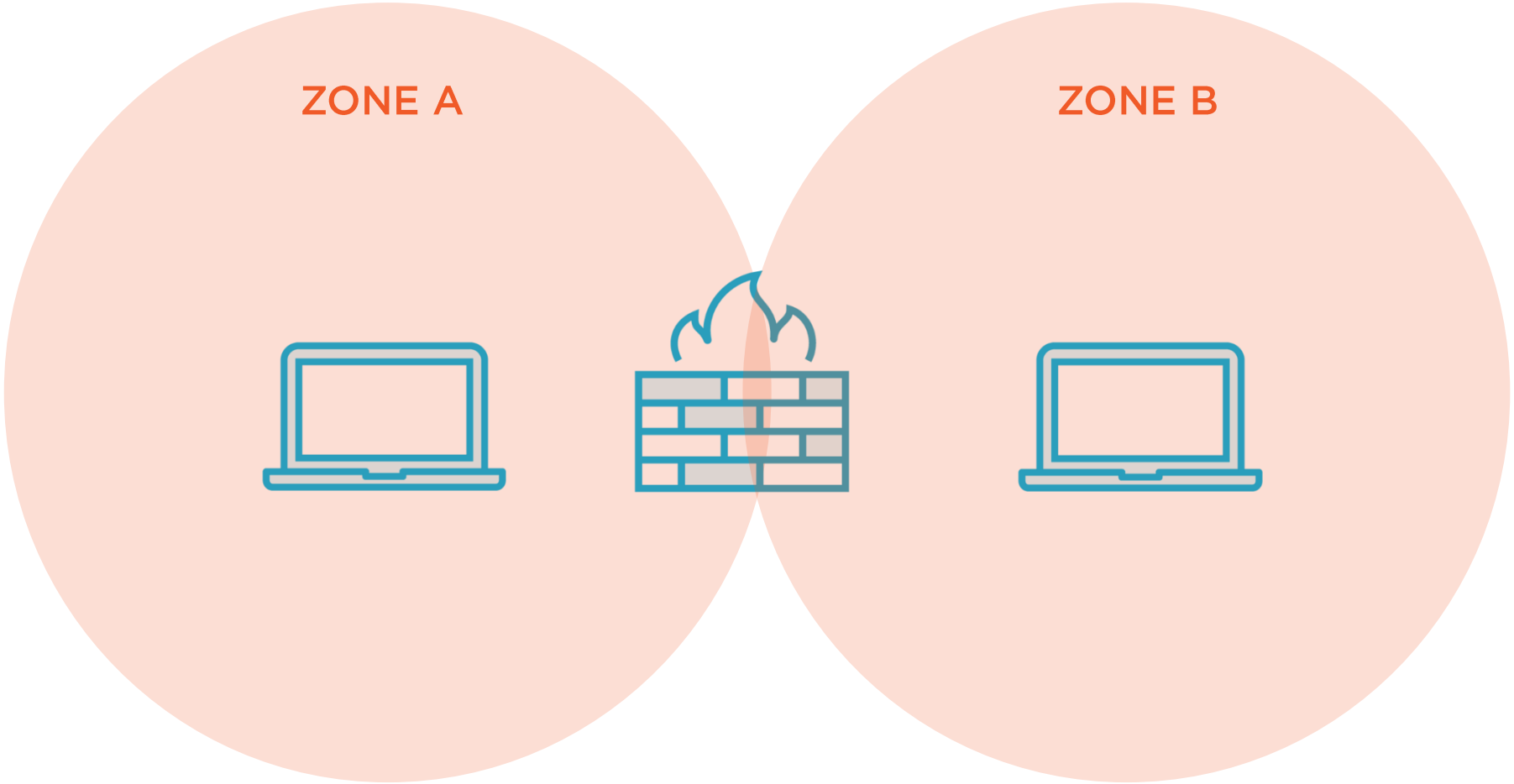
TCP Firewall Issues



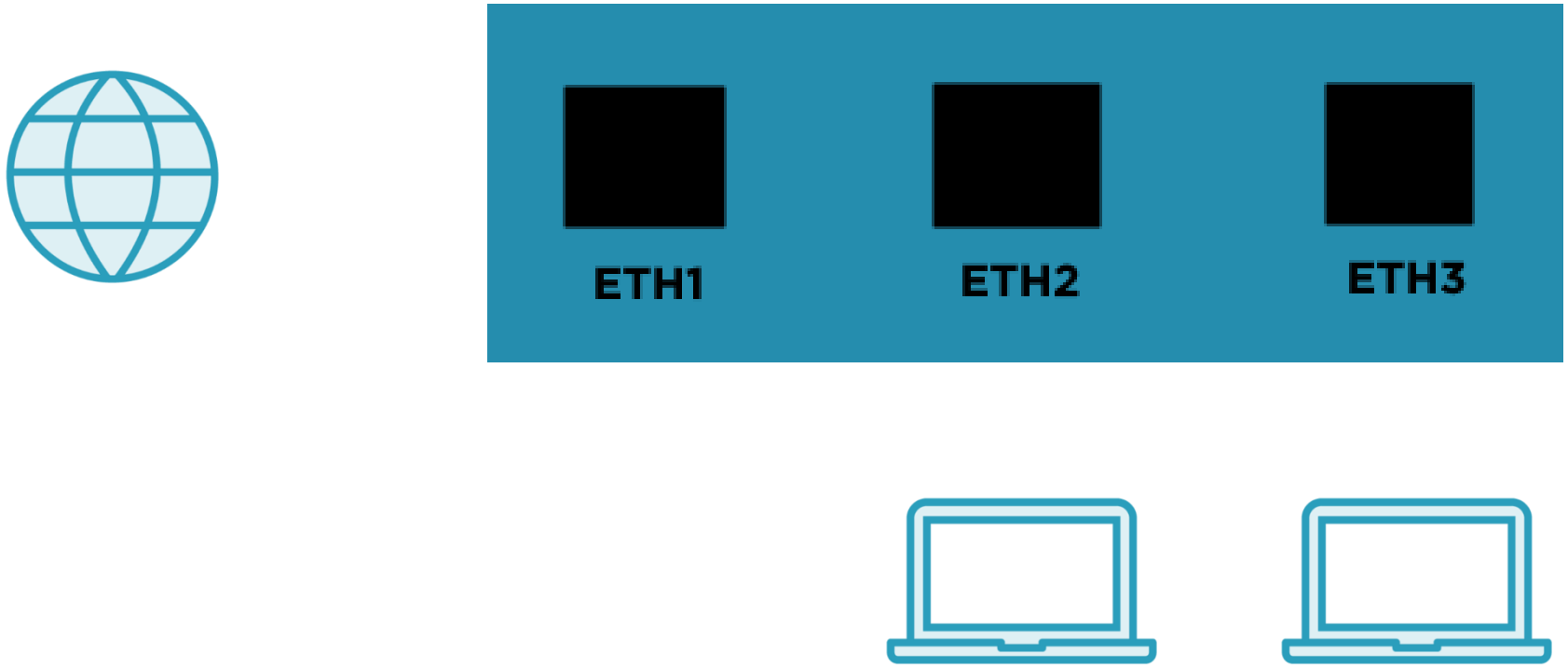
Firewall direction

- Directional based
  - 3 directions
    - In – Inbound to that interface
    - Out – Leaving the interface
    - Local – Traffic destined to firewall

TCP Firewall Issues



TCP Firewall Issues

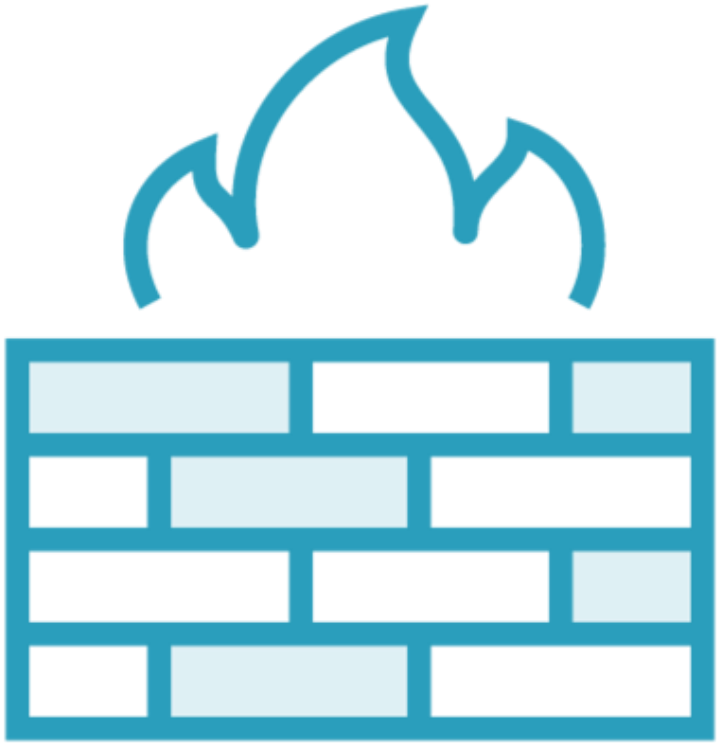


Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.18363.535]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```

TCP Firewall Issues



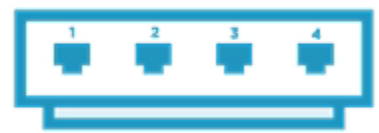
Firewall rule order

- Starts with rule 1
- Processes until match
- Or final default action
  - Usually a drop all rule

TCP Firewall Issues

```
rule 1 {
     action drop
     destination {
          address
192.168.1.0/24
     }
     source {
          address
172.25.1.0/24
```

```
rule 2 {
     action accept
     destination {
          address
192.168.1.0/24
     }
     source {
          address
172.25.1.0/24
```


1
2
3
4

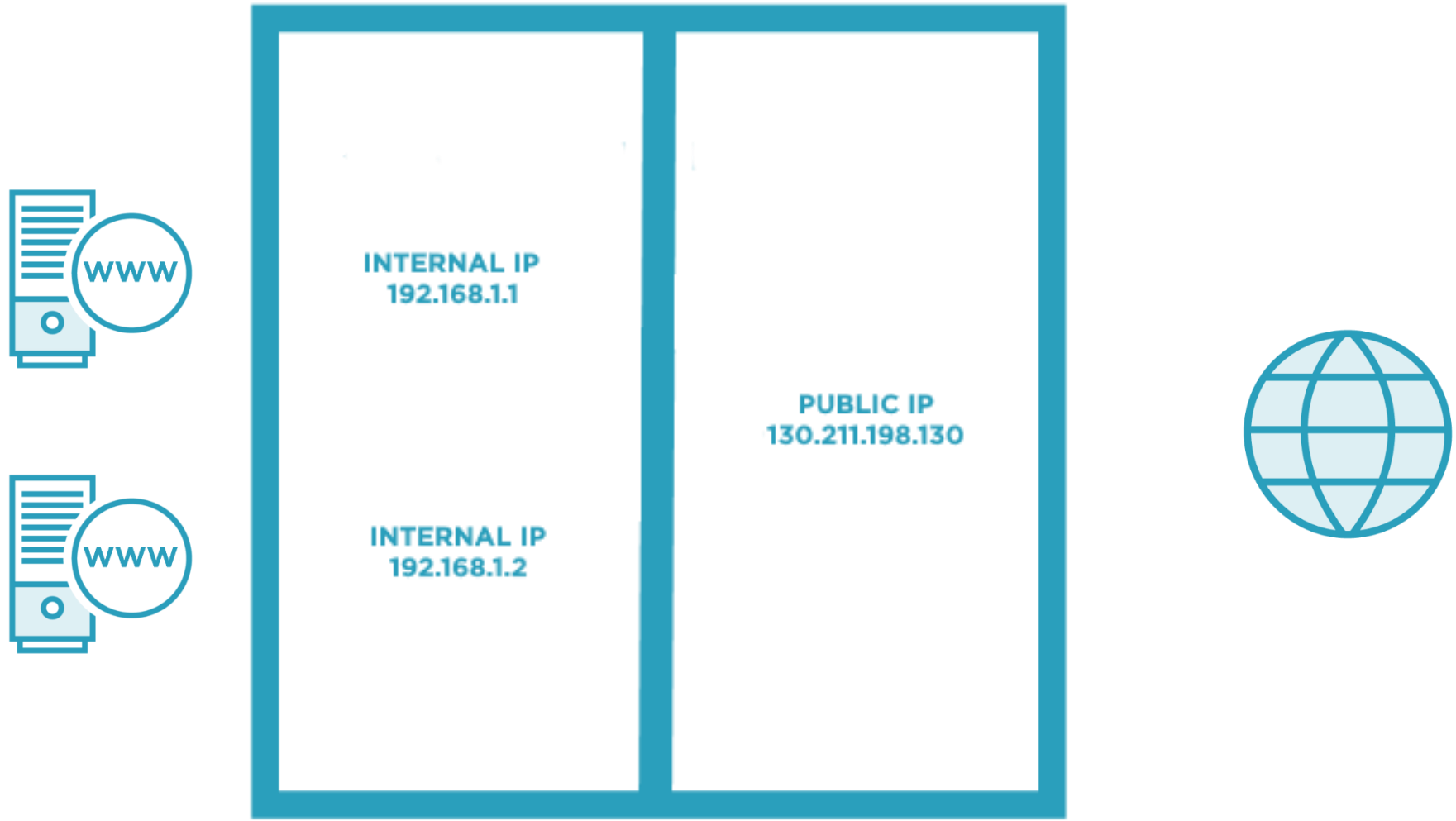
TCP DNAT Issues

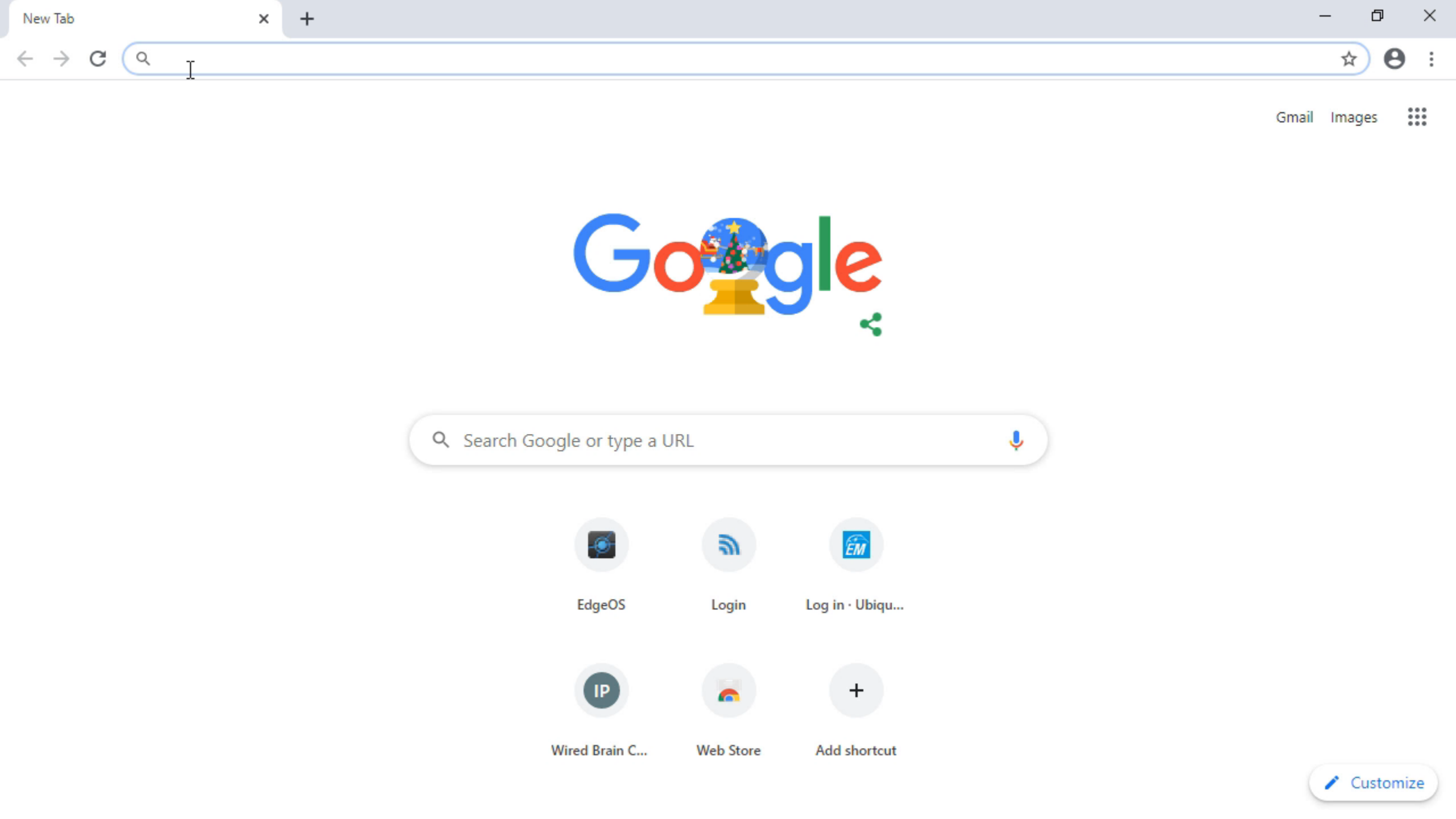
TCP DNAT Issues

DNAT

- Port forward
- Private IP to public IP mapping
- Common issue port assignment

TCP DNAT Issues




New Tab
Gmail
Images
Search Google or type a URL
EdgeOS
Login
Log in · Ubiqu...
Wired Brain C...
Web Store
Add shortcut
Customize

TCP Issues with MTU / MSS

TCP Issues with MTU / MSS

MTU

- Data fragmentation
- 1500 bytes by default

MSS

- Max user data across connection
- Generally MTU minus 40 bytes

TCP Issues with MTU / MSS

192.168.1.0/24

192.168.2.0/24

UDP Common Issues

UDP Common Issues

Main issues

- Firewall
- Incorrectly configured services

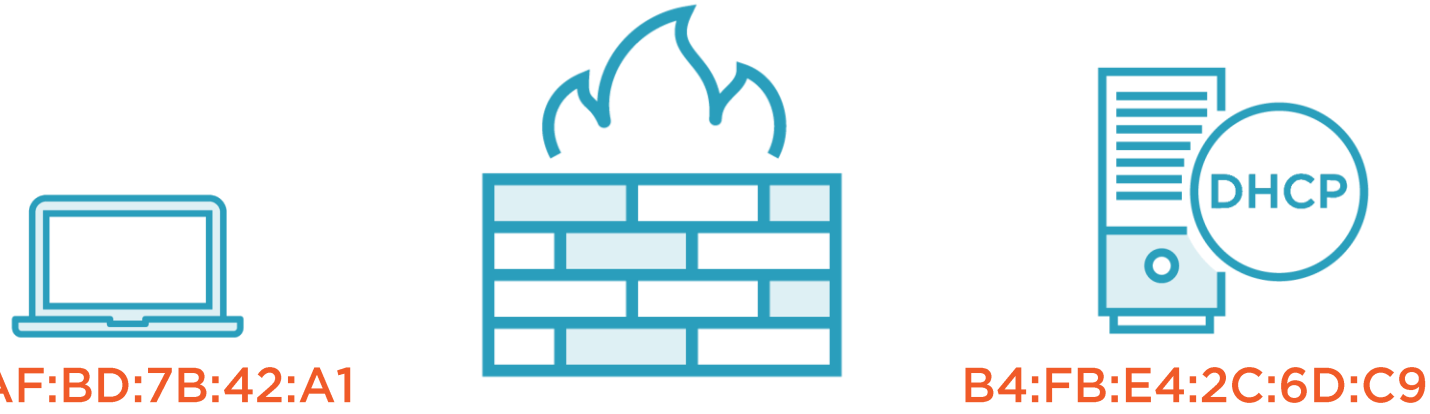
UDP Firewall Issues

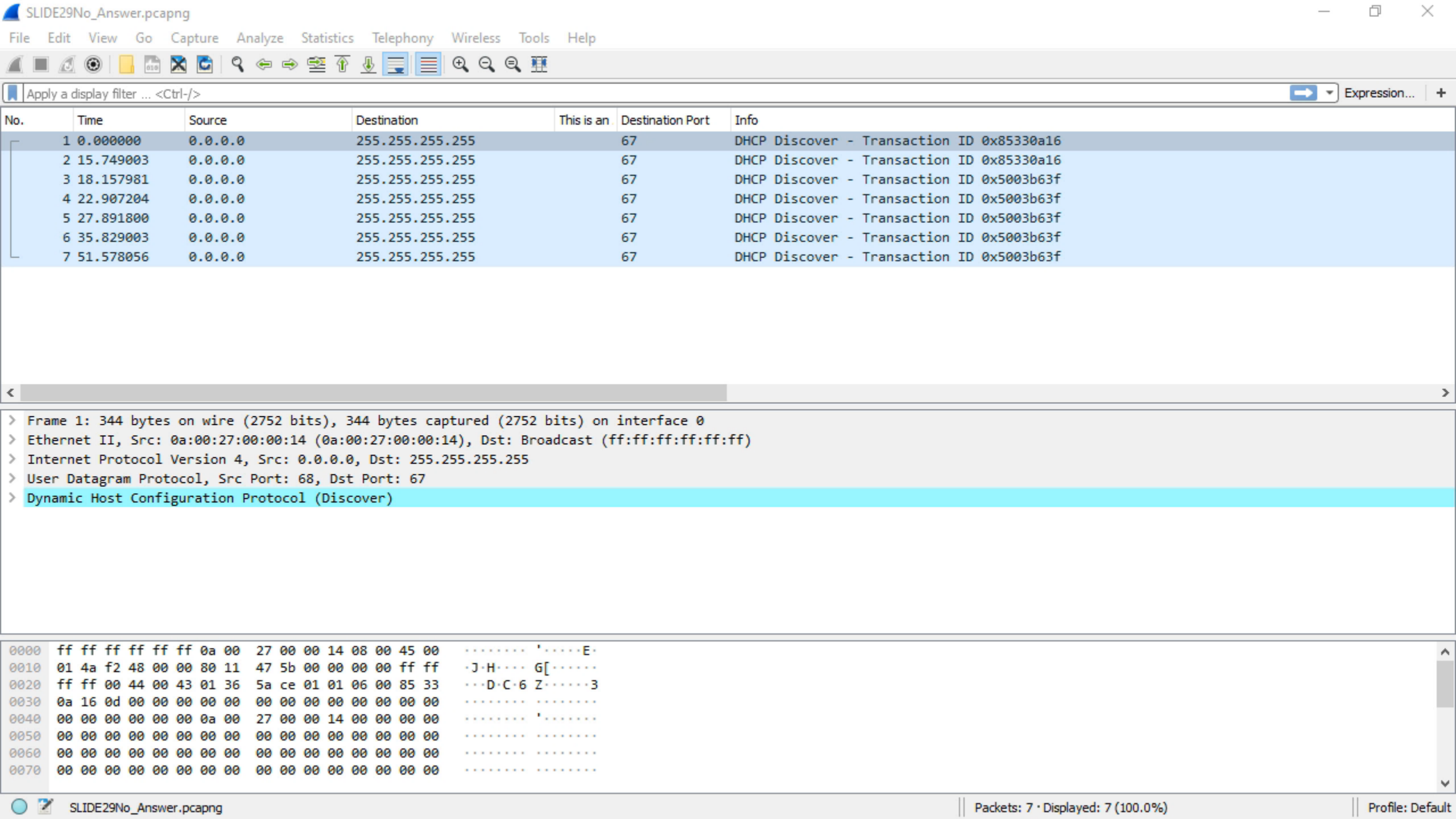
UDP Firewall Issues

Firewall issues

- Same issues as TCP
- DHCP issues
  - Understanding of ports
  - Raw sockets bypass firewall rules

UDP Firewall Issues



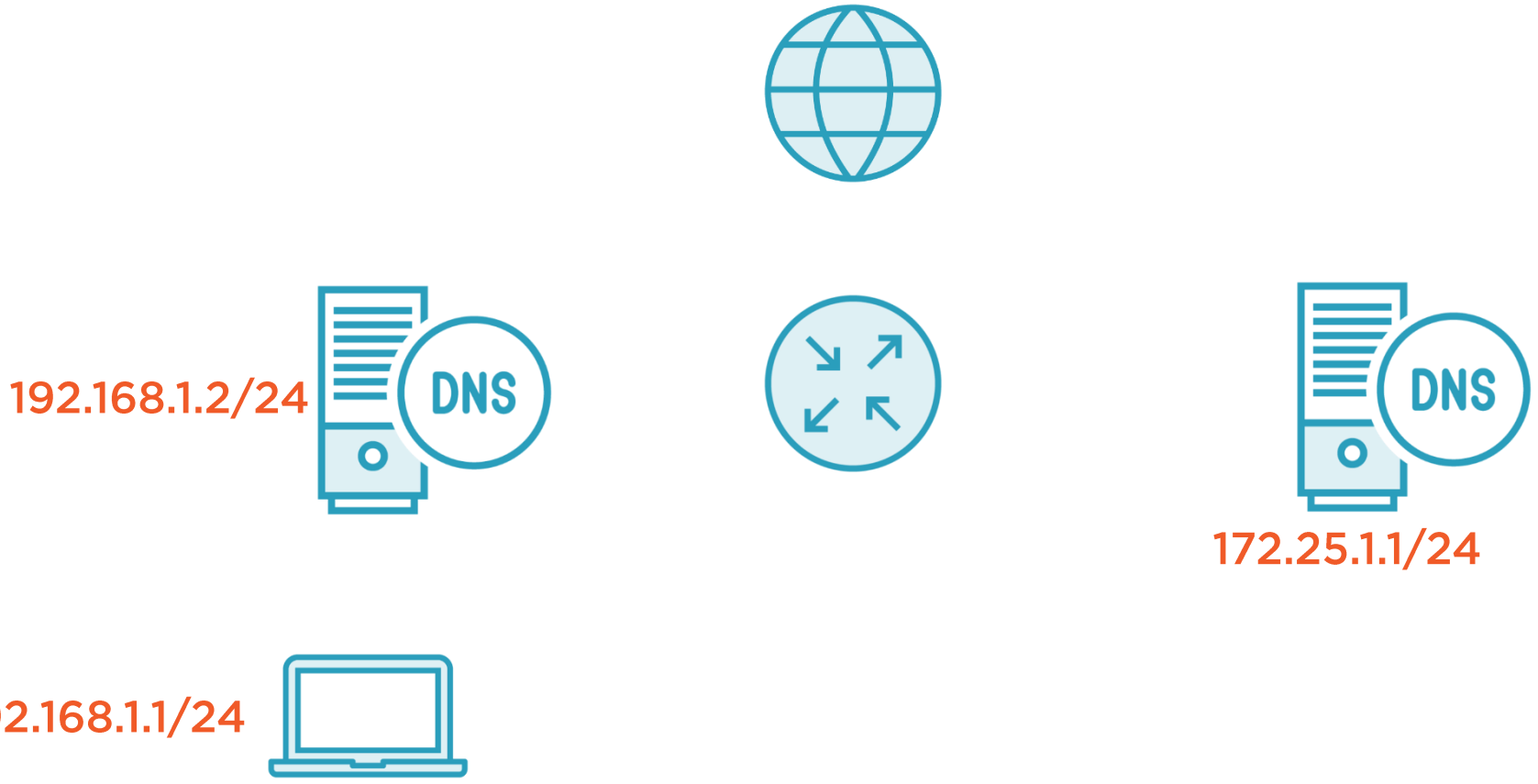

SLIDE29No_Answer.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination This is an Destination Port Info
1 0.000000 0.0.0.0 255.255.255.255 67 DHCP Discover - Transaction ID 0x85330a16
2 15.749003 0.0.0.0 255.255.255.255 67 DHCP Discover - Transaction ID 0x85330a16
3 18.157981 0.0.0.0 255.255.255.255 67 DHCP Discover - Transaction ID 0x5003b63f
4 22.907204 0.0.0.0 255.255.255.255 67 DHCP Discover - Transaction ID 0x5003b63f
5 27.891800 0.0.0.0 255.255.255.255 67 DHCP Discover - Transaction ID 0x5003b63f
6 35.829003 0.0.0.0 255.255.255.255 67 DHCP Discover - Transaction ID 0x5003b63f
7 51.578056 0.0.0.0 255.255.255.255 67 DHCP Discover - Transaction ID 0x5003b63f
Frame 1: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface 0
Ethernet II, Src: 0a:00:27:00:00:14 (0a:00:27:00:00:14), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)
0000 ff ff ff ff ff ff 0a 00 27 00 00 14 08 00 45 00
0010 01 4a f2 48 00 00 80 11 47 5b 00 00 00 00 ff ff
0020 ff ff 00 44 00 43 01 36 5a ce 01 01 06 00 85 33
0030 0a 16 0d 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 0a 00 27 00 00 14 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
SLIDE29No_Answer.pcapng
Packets: 7 · Displayed: 7 (100.0%)
Profile: Default

UDP Firewall Issues

Firewall issues

- DNS
  - Operational port 53
  - Dual protocol
  - 512 bytes and under is UDP
  - Over 512 bytes is TCP

UDP Firewall Issues

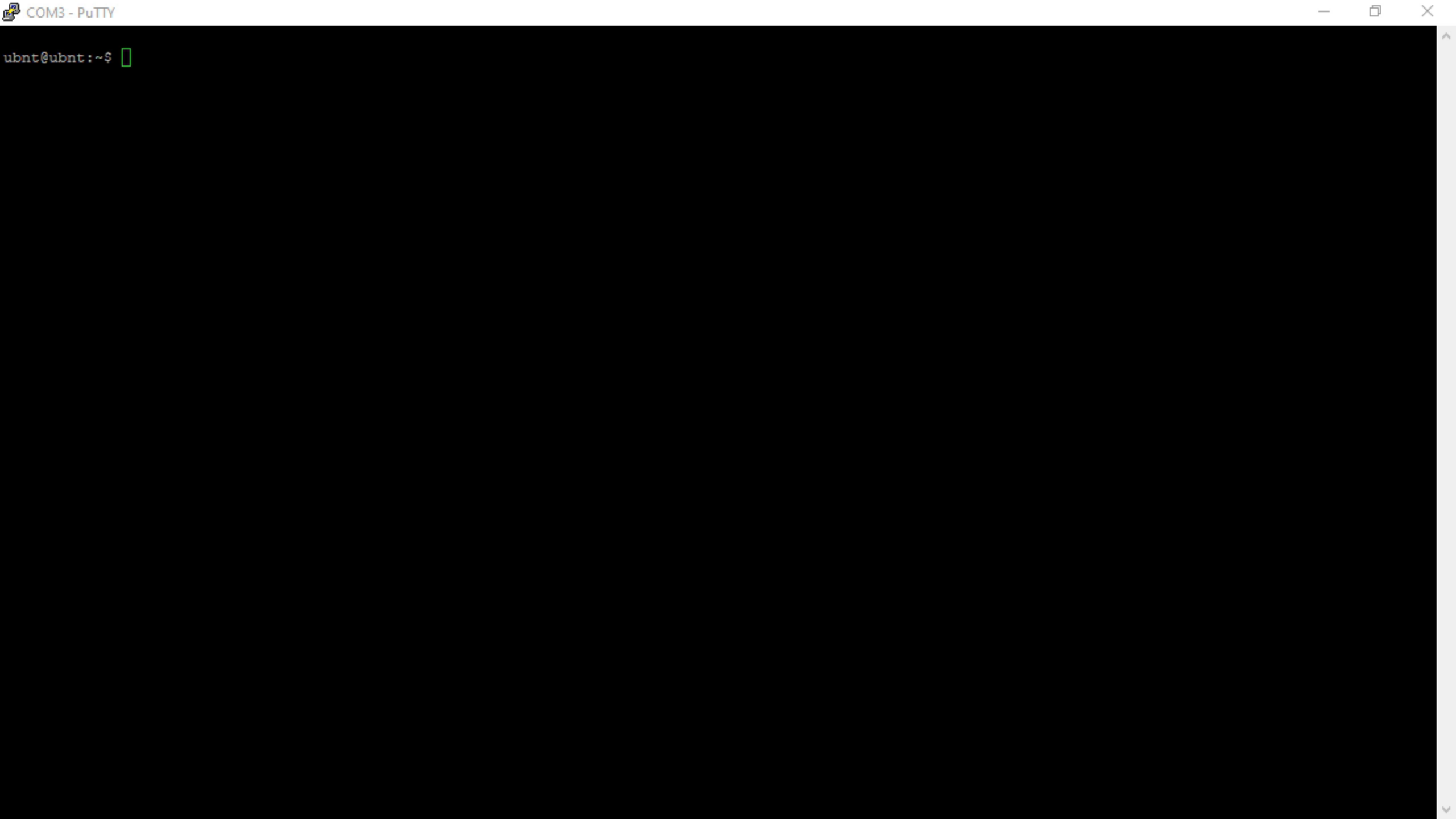


UDP Service Issues

UDP Service Issues

Service issues

- TCP and UDP rely on services
- UDP service issues more common
- Top 3
  - DHCP
  - DNS
  - NTP


COM3 - PuTTY
ubnt@ubnt:~$

Module Review

Syntax is key for addresses and ports

Know you directions

Zones require traffic pairing

Order of operations matter

Module Review

DNAT – Watch for port overlap

MTU / MSS – WISP, and VPN

UDP firewall misconfiguration

UDP services reload clears memory