Networking

- IPv6
  - IPv6 CLI commands
- IPv4
  - How ARP works
- Routing
  - BGP figure out networks belonging to AS
- Operating
  - How to test if 9000 MTU/Jumbo Frames are working
- Links & Tools
  - tcpdump Cheat Sheet
  - Wireshark Sample Captures
  - Useful Network Diagnostic CLI commands

IPv6

IPv6 CLI commands

IPv6 Commands

Below are the most important helpful commands for checking and diagnosing the IPv6 environment

Windows 8 / 10

Command	Function
ipconfig /all	displays all interface details
ping ::1	Test IPv6 protocol host internally (localhost)
netsh interface ipv6 show interface	Interface status (all) and IPv6 addresses
netsh interface ipv6 showaddress	IPv6 addresses including validity displays
netsh interface ipv6 show privacy **netsh interface ipv6 show global**	See IPv6 Configuration and Privacy Extensions
netsh interface ipv6 show route **route print -6**	Show IPv6 routing table
netsh interface ipv6 show neighbors	Mapping IPv6 addresses to MAC addresses
netsh interface ipv6 show destination	Destination cache incl. PMTU values
netsh interface ipv6 dump	show all changes
netsh interface ipv6 reset	reset all changes

Linux

Command	Function
ifconfig -a **ifconfig eth0 | grep inet6**	displays all interface details ETH0 only IPv6 addresses
ping6 ::1	Test IPv6 protocol host internally (localhost)
ip -6 address show **ip -6 maddr show**	Interface status (all) and IPv6 addresses show multicast groups
netsh interface ipv6 showaddress	IPv6 addresses including validity displays
ip -6 route show **route -A inet6 -n**	Show IPv6 routing table

ip -6 neighb show	Mapping IPv6 addresses to MAC addresses
ip -6 route get to {ipv6_addr}	Destination cache incl. PMTU values
test -f /proc/net/if_inet6 && echo	check if IPv6 is active

macOS since 10.7

Command	Function
ifconfig -a **ifconfig -L**	displays all interface details shows the period of validity of the addresses
ping6 ::1 **traceroute6 {ipv6-host}**	Test IPv6 protocol host internally (localhost)
netstat-f inet	show all IPv6 connections
netstat -g	show multicast groups
netstat -rnf inet6	Show IPv6 routing table
ndp -a	Mapping IPv6 addresses to MAC addresses
dscacheutil -flushcache	clear DNS cache
nettop -n -m route	View routing statistics in real time
nettop -n	Show TCP & UDP sockets in real time

IPv4

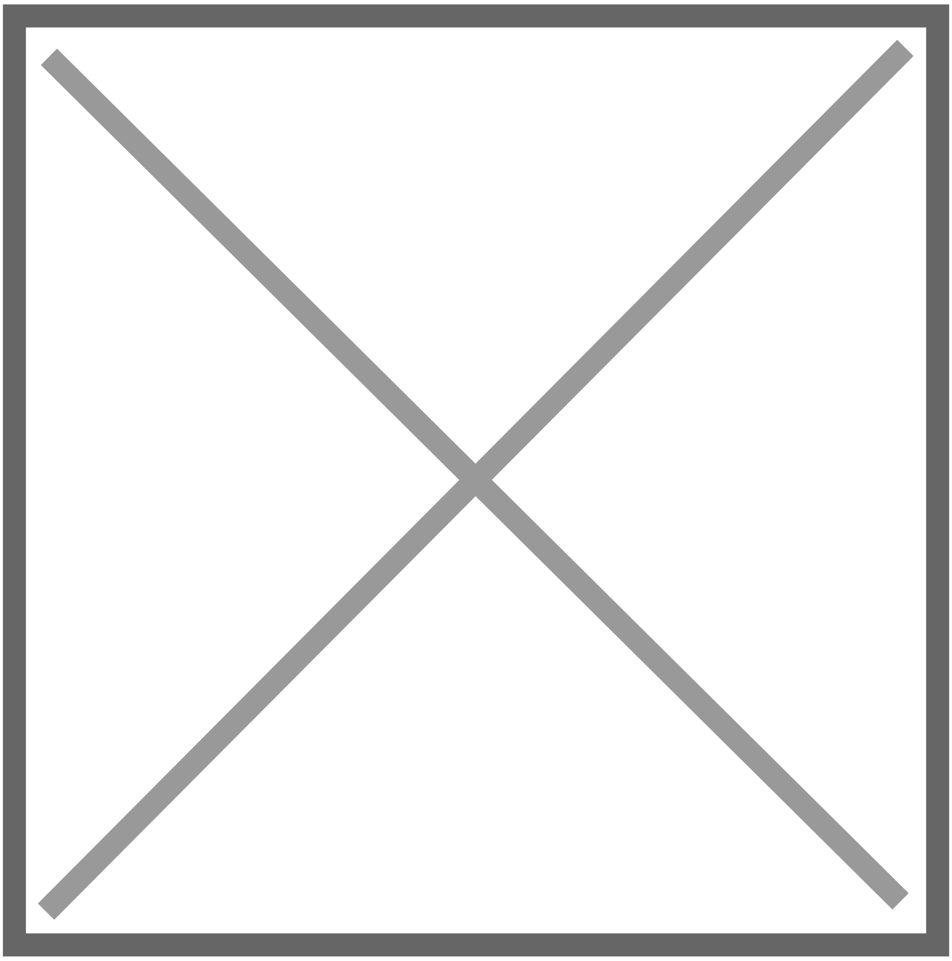
IPv4

How ARP works

Very good explanation how ARP in IPv4 works:

https://www.tummy.com/articles/networking-basics-how-arp-works/

https://www.geeksforgeeks.org/arp-reverse-arprarp-inverse-arp-inarp-proxy-arp-and-gratuitous-arp/



Routing

Routing

BGP figure out networks belonging to AS

BGP List prefixes

To list all prefixes originated on AS1759 against the Routing Assets Database (RADb), issue the command below.

```
whois -h whois.radb.net -- '-i origin AS1759' | grep -Eo "(route:|route6:).*"
route:      139.157.0.0/16
route:      147.44.0.0/16
route:         193.178.133.0/24
....
route6:         2001:2003::/32
route6:         2a00:8a00:4000::/35
route6:         2a03:62a0:3501::/48
```

Thanks to this Link: https://www.noction.com/knowledge-base/bgp-filtering

Operating

Operating

How to test if 9000 MTU/Jumbo Frames are working

Description

You setup mtu 9000 on your interfaces and want now to test if it works. There're different possibilities to do this on the different operating system.

The following shows how to test it.

Linux

```
ping -M do -s 8972 <ip>
```

macOS

```
ping -D -s 8184 <ip>
```

Windows

```
ping -f -l 9000 <ip>
```

Links

Thanks to: https://blah.cloud/hardware/test-jumbo-frames-working/

Links & Tools

Links & Tools

tcpdump Cheat Sheet

tcpdump Cheat Sheet (https://www.comparitech.com/net-admin/tcpdump-cheat-sheet/)

tcpdump cheat sheet

Links & Tools

Wireshark Sample Captures

If you need to see how different protocols behave on the network here are some sample captures from Wireshark

- https://wiki.wireshark.org/SampleCaptures
- https://packetlife.net/captures/
- https://www.netresec.com/?page=PcapFiles
- https://tshark.dev/search/pcaptable/

Links & Tools

Useful Network Diagnostic CLI commands

Useful CLI commands to do network diagnostics with tcpdump / tshark etc.

tcpdump

Command	Description
tcpdump -nni <network-interface> icmp	show icmp packets
tcpdump -nni <network-interface> "icmp[0] == 0"	ICMP type 0 echo reply
tcpdump -nni <network-interface> "icmp[0] == 3"	ICMP destination unreachable
tcpdump -nni <network-interface> "icmp[0] == 4"	ICMP source quench
tcpdump -nni <network-interface> "icmp[0] == 5"	ICMP redirect
tcpdump -nni <network-interface> "icmp[0] == 8"	ICMP echo request
tcpdump -nni <network-interface> "icmp[0] == 11"	ICMP time exceeded
tcpdump -nni <network-interface> "tcp[tcpflags] & (tcp-rst) !=0"	Detect tcp reset and ICMP packets