AC31008 – Networks and Data Communication – Assignment 1

Part 2: Investigating Network First Pings

Traffic right at network initialization:

On network initialization, a few things occur. Mainly ARP and DHCP type Packets are show up in the simulation view. (Only the ARP, DHCP, EIGRP, FTP, HTTP, HTTPS, ICMP & NTP packets are displayed in the filter, as they are the only protocols/relevant packets to us)

Vis.	Time(sec)	Last Device	At Device	Type
	0.865	--	EA-Visitor-1	DHCP
	0.865	--	EA-Visitor-1	DHCP
	0.866	--	EA-Visitor-2	DHCP
	0.866	EA-Visitor-1	EA-Wireless	DHCP
	0.866	--	EO-Boss-Ta...	DHCP
	0.867	EA-Wireless	EA-Router	DHCP
	0.867	--	EA-Router	ARP
	0.868	EA-Router	EA-Switch	ARP
	0.869	EA-Switch	EA-PC-1	ARP
	0.869	EA-Switch	EA-PC-2	ARP
	0.869	EA-Switch	EA-DHCP	ARP
	0.870	EA-DHCP	EA-Switch	ARP
	0.871	EA-Switch	EA-Router	ARP

The ARP Packets stay within the network they originate in, and the DHCP Packets stay within the Experimental Area (as the DHCP server is only configured to assign IPs within the Experimental Area). An Example of these can be seen in the screenshot on the left, taken at network initiation. (EA on the device means Experimental Area)

It makes sense that the ARP protocol stays within one network, as it is a Link Layer protocol, it is communicated withing the bounds of a single network, not routed across internetwork nodes.

From this we can assume that these routes within the same network are traversed by ARP packets at the time that the network devices are booted. As such, these routes are "initialized" or cached in the remote routers ARP cache.

This is reflected in both real-time and simulation testing in Packet Tracer, even right after an all-device reboot. Pings within the same network (Wifi, Wireless, and in between) all succeed on the first try.

So why do pings fail on first try across networks?

From the information we've gathered analyzing the traffic at launch, and how that leads to no failed pings within networks. We can assume the reason pings are failing on first try across networks is because the routes across networks are not cached in the routers. This makes sense as there is no cross-network traffic right at launch for such a cache to be created from.

Watching the packets in simulation view shows us that the packet makes it to the router in the Network, but not further. This is because the router in the Network must put the ping on hold to send out an ARP broadcast to get the MAC address of remote devices that connect to the other networks. This delay is probably too long, so the first ping times out and comes across as a fail. But, pings after that succeed as the router on the local network knows the remote router on the other networks MAC Address. An example of this can be seen when trying to ping across networks in the command prompt view:

```
C:\>
C:\>ping 10.0.4.30 -n 8

Pinging 10.0.4.30 with 32 bytes of data:

Request timed out.
Reply from 10.0.4.30: bytes=32 time<1ms TTL=126
Reply from 10.0.4.30: bytes=32 time<1ms TTL=126
Reply from 10.0.4.30: bytes=32 time<1ms TTL=126
Reply from 10.0.4.30: bytes=32 time<1ms TTL=126
Reply from 10.0.4.30: bytes=32 time<1ms TTL=126
Reply from 10.0.4.30: bytes=32 time=15ms TTL=126
Reply from 10.0.4.30: bytes=32 time=11ms TTL=126

Ping statistics for 10.0.4.30:
    Packets: Sent = 8, Received = 7, Lost = 1 (13% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 3ms
```

This screenshot is a ping from the R-PostDoc PC (IP: 10.0.6.5) in the Research Area Network (Network 10.0.6.0/23), across networks to the IT-Nerd Laptop (IP: 10.0.4.30) in the IT-Techs Network (Network: 10.0.4.0/27), in the IT Services area.

In the command prompt, I used the '-n 8' flag to send 8 pings, so that we could see how the fail-then-success played out. As expected, the first ping times out, but subsequent pings make it across networks, and receive a reply.

Name: Taha Kashaf
Student ID: 108820889
AC31008 Assignment 1