Internet Networking - Homework 3

Yosef Goren & Ori Evron

May 27, 2023

Contents

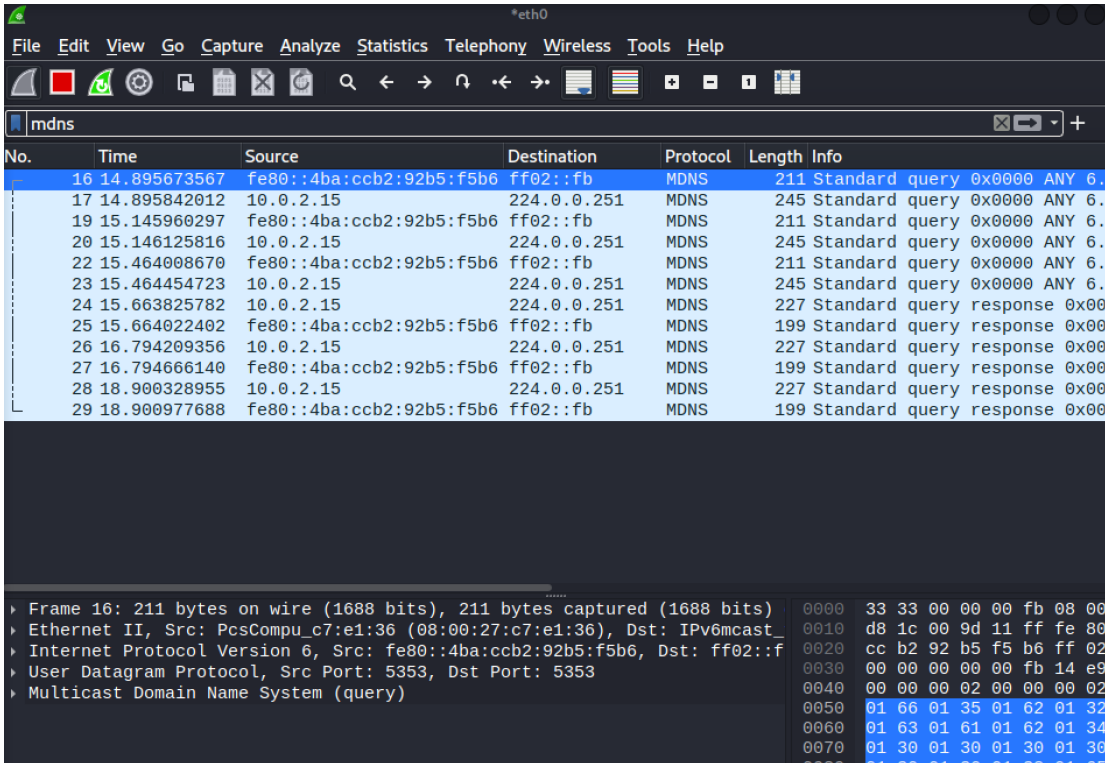
1 BGP Business Relations

2 Multicast DNS LAB

Solutions in this sections based on specification RFC-6762.

2.1

The packets were sent to the IPv4 address 224.0.0.251, this IPv4 address is reserved for mDNS, which means a host can't have it.



2.2

- **Advantage**: Other hosts now know and can cache the MDNS to IP mapping so that when they require it - they do not need to request for it; moreover - they will be able to answer queries of others regarding the same hostname.
- **Disadvantage**: Sending the response using brodcast can and will cause un-nessecery traffic since it will often send the response packets to hosts that already know the mapping or ones that otherwise will not make use of it.

2.3

The main resone we can think of is that brodcast generally cannot be sent outside of the same LAN [1], as opposed to multicast which can - so using brodcast would limit the avalibility of the MDNS network to just one LAN, or would require solving futher issues that would come with using brodcast in remote networks.

2.4

There are generally 3 options for how the end users or their client applications might be able to know the addresses of internet devices.

1. Standard DNS.
2. Manually seaching for the IP address allocated by DHCP.
3. Using MDNS.

Option 1 would not be practical for the purpose of IOT devices, as it would require each such device to have it's own hostname at the global DNS (which would be very expensive) - or would cause the user to manually configure a local DNS service which is not a resonable request from the end user.

Similarly - **Option 2** also requires manual configuration and knowladge that the end user does not have to implement.

Hence the best option we are left with is **Option 3** (MDNS) - which enables 'Plug and Play' usage of the IOT devices.

3 Stiner Tree

4 Mininet BGP LAB

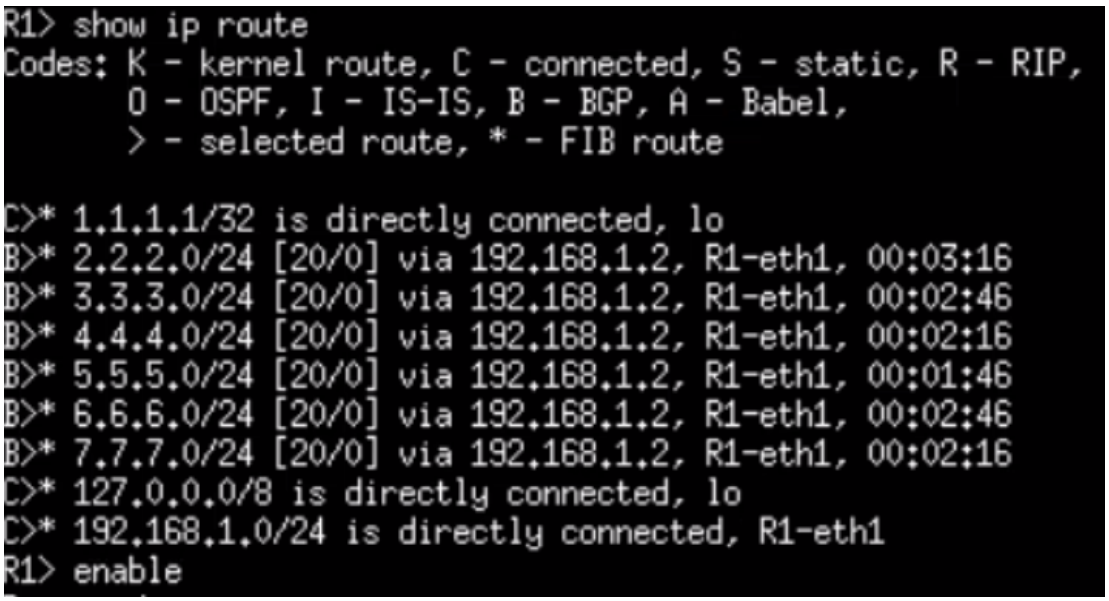
4.1

The address is `192.168.1.1`.

4.2

The routing table consists of a list of pathways for the way to each each network as shown:

[1] brodcast is generally not possbile from outside networks since enabling it would expose the reciving network to DOS attacks - hence it is often disallowed at the firewall.



It appears all of the routes are through `192.168.1.2`, accept the loopback connection, and the `192.168.1.0` device.
Different entries in the table are controled by different applications or methods: `1.1.1.1`, loopback and `192.168.1.0` have been added to the table since they are directly connected to the device, while the rest of the entries in the table have been added by the BGP protocol.
The timestamp at the end of the BGP entries shown when BGP has added the specific entry to the table.

4.3

Different parts of the table are filled in different ways; the entries for directly connected devices are added automatically - likely by the operating system or an associated daemon, while the indirect routings marked with 'B' have been added by the local BGP application (`bgpd`).
Generally - different enties in the table are inserted from different sources, and each such source might add it's own entries based on how the specific protocol is defined.

4.4

The data stored in the BGP table represents the next hop, which is the next router on our network where we want our messages to be sent. In our case, where AS1 is only connected to AS2, all our messages need to be routed through AS2 to reach their destinations. We can also see the path the packets need to go through in the net...

4.5

The route from `R1` to `R5` shown in the BGP table is shown as "`0 2 3 4 5 i`", which means the route goes through `R3` and `R4`.
The reason the path going through `R6` and `R7` is not shown is because it is was not considered an optimal path by BGP [2] and hence it was not saved.

4.6

`R2` shows two routes to `R5`, one through `R6` and the other through `R3`; the one through `R3` is the one used, as it is the shortest one considering the AS-hop-counte metric.

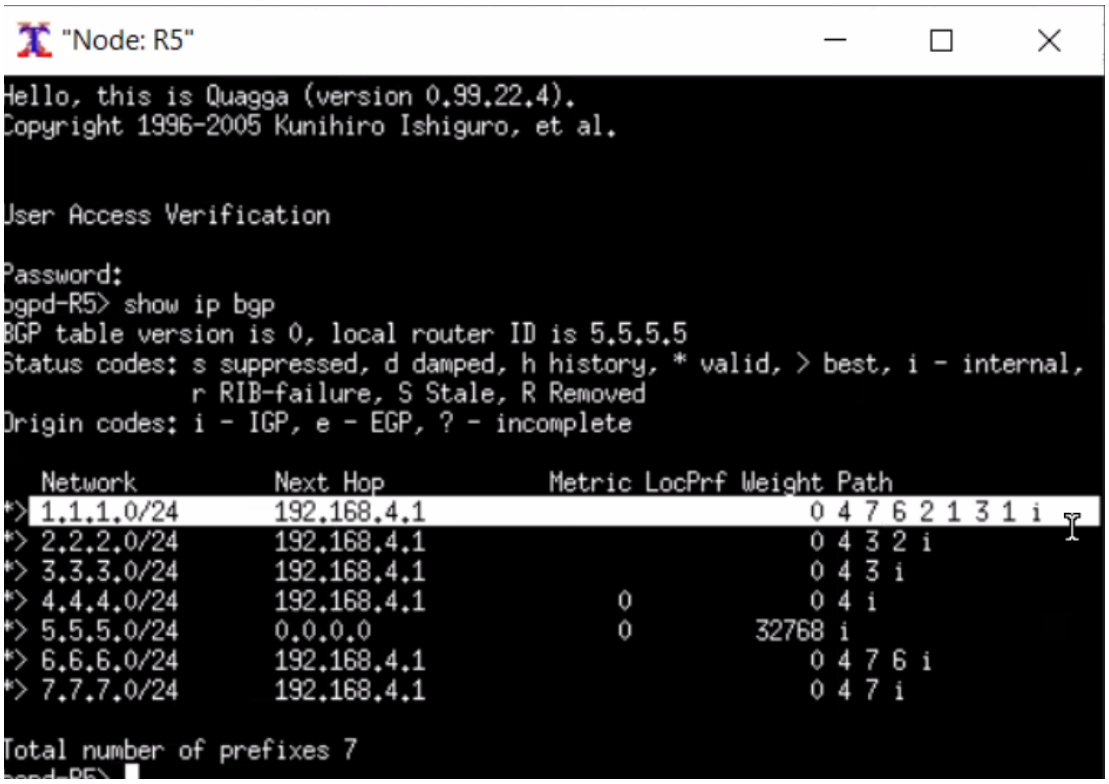
4.7

If all metrics are equal to zero, then the routing is dicated by taking the shortest path in terms of the number of hops between AS's, if that does not break the tie - then random / lexicographic selection is used.

4.8

It seems the path in the bgp table from textttR5 to textttR1 `0 4 7 6 2 1 3 1 i`.

[2] The metric is determined by the configuration - the number of hops between AS's and the weight/cost of each hop



4.9

The AS1 manager added AS's `3 1` to the AS-PATH attribute of each route advretized by it, now the AS3 router that gets information about the path, sees the `1 3 1` and reject the advertisement, because it wants to prevent loops.

```
!
hostname bgpd-R1
password en
enable password en
log stdout
!
router bgp 1
 bgp router-id 1.1.1.1
 network 1.1.1.0/24
 neighbor 192.168.1.2 remote-as 2
 neighbor 192.168.1.2 route-map rm_peer_1_out out
!
ip prefix-list pl_peer_1_out seq 5 permit 1.1.1.0/24
!
route-map rm_peer_1_out permit 5
 match ip address prefix-list pl_peer_1_out
 set as-path prepend 3 1
!
line vty
!
```

4.10

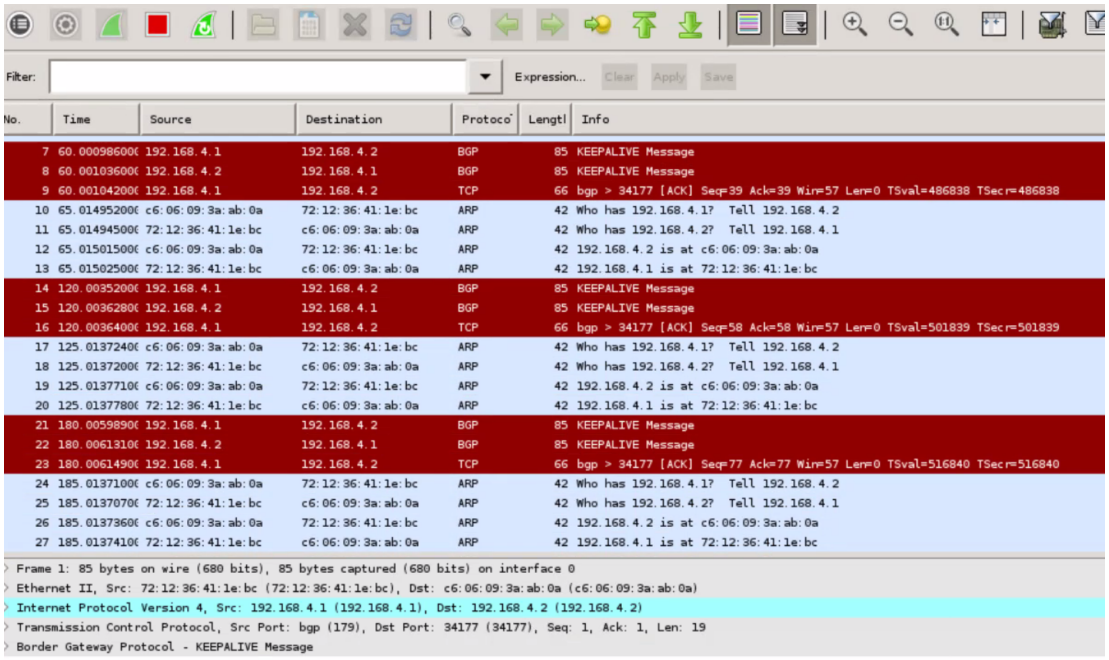
```
R4> show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

B>* 1.1.1.0/24 [20/0] via 192.168.7.2, R4-eth3, 01:44:32
B>* 2.2.2.0/24 [20/0] via 192.168.3.1, R4-eth1, 01:45:10
B>* 3.3.3.0/24 [20/0] via 192.168.3.1, R4-eth1, 01:45:10
C>* 4.4.4.4/32 is directly connected, lo
B>* 5.5.5.0/24 [20/0] via 192.168.4.2, R4-eth2, 01:45:07
B>* 6.6.6.0/24 [20/0] via 192.168.7.2, R4-eth3, 01:45:02
B>* 7.7.7.0/24 [20/0] via 192.168.7.2, R4-eth3, 01:45:02
C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.3.0/24 is directly connected, R4-eth1
C>* 192.168.4.0/24 is directly connected, R4-eth2
C>* 192.168.7.0/24 is directly connected, R4-eth3
R4>
```

we can also see the line "`192.168.7.0 is directly connected, R4-eth3`", at the end. which tells us that the packets to AS1 are transported through AS7.

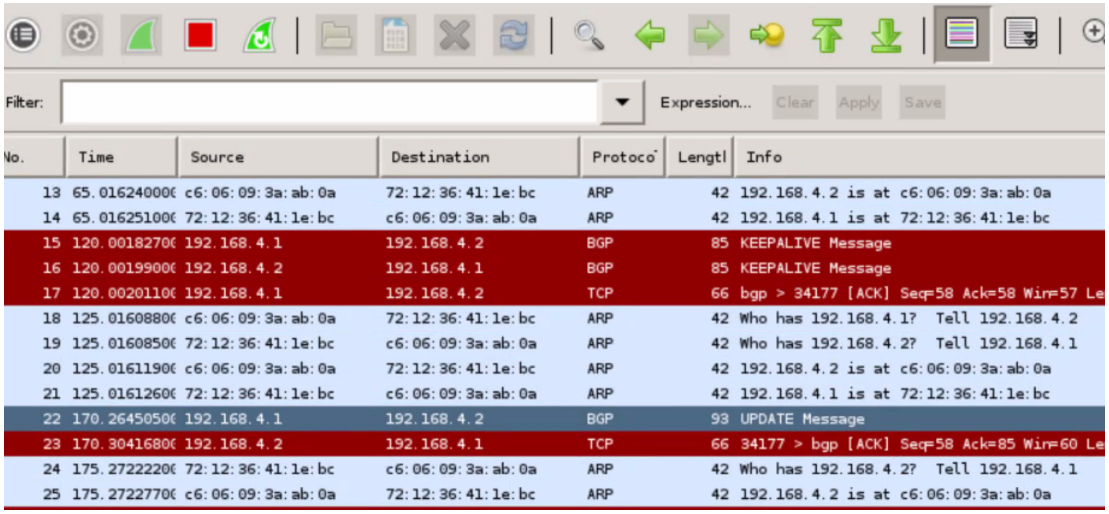
4.11

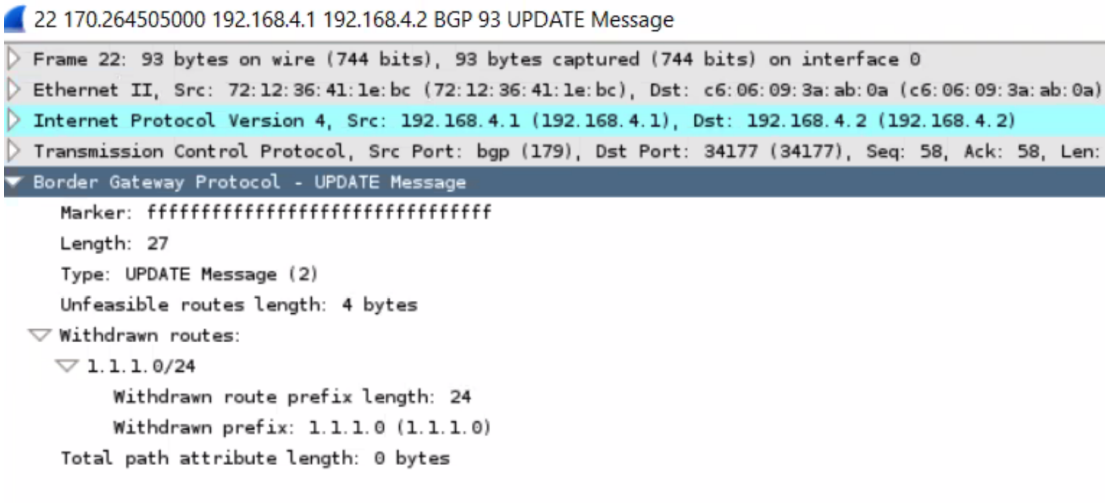
It appears that the BGP keepalive packets arrive at a frequency of one per minute (you can see the time intervals by looking at the time column in wireshark).



4.12

`R5` recived the `BGP Update` message from `R4`, and it conatins instructions to withdraw (cancel) a routing to the prefix `1.1.1.1` which is the one in AS1.





4.13

We can see that `R4` does not know how to reach the prefix `1.1.1.1` by seeing that it has no routing entry that reaches `1.1.1.1`:

```
bgpd-R4> show ip bgp
BGP table version is 0, local router ID is 4.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  2.2.2.0/24       192.168.7.2                           0 7 6 2 i
*>                  192.168.3.1                           0 3 2 i
*> 3.3.3.0/24       192.168.3.1              0            0 3 i
*> 4.4.4.0/24       0.0.0.0                  0        32768 i
*> 5.5.5.0/24       192.168.4.2              0            0 5 i
*  6.6.6.0/24       192.168.3.1                           0 3 2 6 i
*>                  192.168.7.2                           0 7 6 i
*> 7.7.7.0/24       192.168.7.2              0            0 7 i

Total number of prefixes 6
```

4.14

Now the `BGP Update` message contains instructions to add a new route to the prefix `1.1.1.1`: