

Internet Networking - Homework 3

Yosef Goren & Ori Evron

May 27, 2023

Contents

1	BGP Business Relations	1
2	Multicast DNS LAB	1
2.1	2
2.2	2
2.3	3
2.4	3
3	Stiner Tree	3
4	Mininet BGP LAB	3
4.1	3
4.2	3
4.3	4
4.4	4
4.5	5
4.6	5
4.7	5
4.8	5
4.9	6
4.10	7
4.11	8
4.12	8
4.13	9
4.14	10

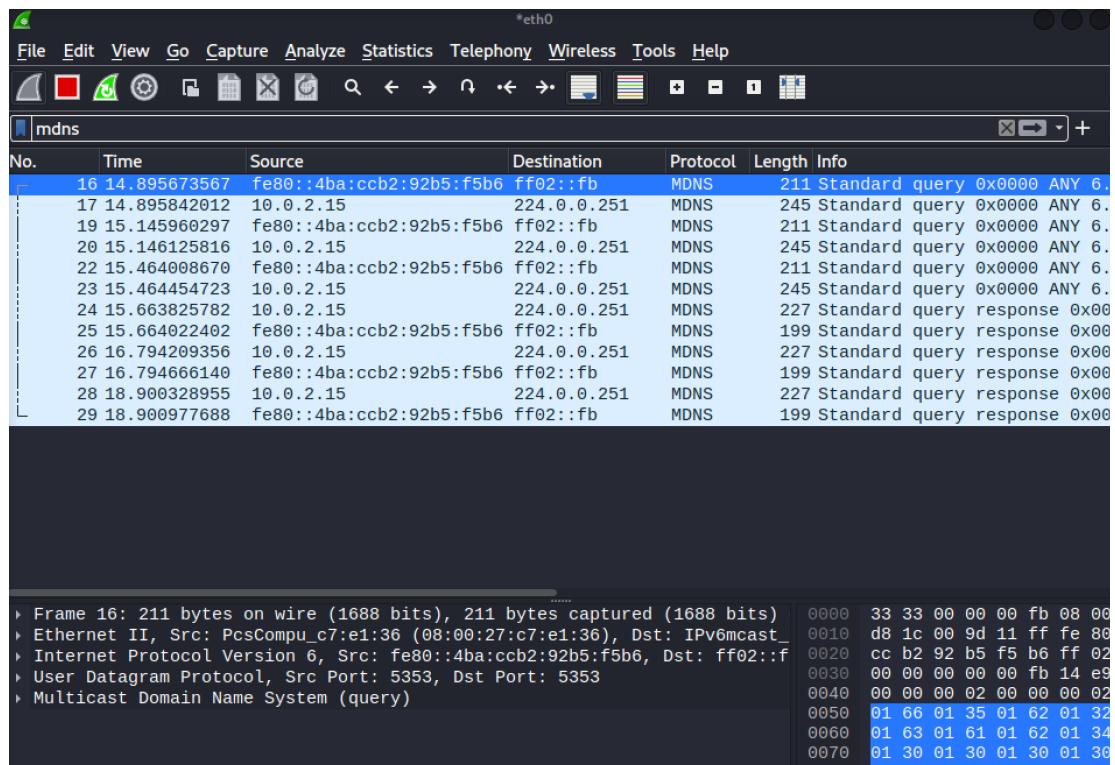
1 BGP Business Relations

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 broadcast can and will cause unnecessary 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 reason we can think of is that broadcast generally cannot be sent outside of the same LAN¹, as opposed to multicast which can - so using broadcast would limit the availability of the MDNS network to just one LAN, or would require solving further issues that would come with using broadcast 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 searching 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 its 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 reasonable request from the end user.

Similarly - **Option 2** also requires manual configuration and knowledge 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 network as shown:

¹broadcast is generally not possible from outside networks since enabling it would expose the receiving network to DOS attacks - hence it is often disallowed at the firewall.

```

R1> 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

C>* 1.1.1.1/32 is directly connected, lo
B>* 2.2.2.0/24 [20/0] via 192.168.1.2, R1-eth1, 00:03:16
B>* 3.3.3.0/24 [20/0] via 192.168.1.2, R1-eth1, 00:02:46
B>* 4.4.4.0/24 [20/0] via 192.168.1.2, R1-eth1, 00:02:16
B>* 5.5.5.0/24 [20/0] via 192.168.1.2, R1-eth1, 00:01:46
B>* 6.6.6.0/24 [20/0] via 192.168.1.2, R1-eth1, 00:02:46
B>* 7.7.7.0/24 [20/0] via 192.168.1.2, R1-eth1, 00:02:16
C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.1.0/24 is directly connected, R1-eth1
R1> enable

```

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 controlled 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 entries in the table are inserted from different sources, and each such source might add its 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.

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

X "Node: R5"

```
Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
bgpd-R5> show ip bgp
BGP table version is 0, local router ID is 5.5.5.5
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
* 1.1.1.0/24        192.168.4.1          0 4 7 6 2 1 3 1 i  I
* 2.2.2.0/24        192.168.4.1          0 4 3 2 i
* 3.3.3.0/24        192.168.4.1          0 4 3 i
* 4.4.4.0/24        192.168.4.1          0 4 i
* 5.5.5.0/24        0.0.0.0             0 32768 i
* 6.6.6.0/24        192.168.4.1          0 4 7 6 i
* 7.7.7.0/24        192.168.4.1          0 4 7 i

Total number of prefixes 7
```

4.9

The AS1 manager added AS's 3 1 to the AS-PATH attribute of each route advertised 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 wire-shark).

The screenshot shows a Wireshark capture of network traffic. The packet list is filtered to show BGP keepalive messages. The columns in the table are: No., Time, Source, Destination, Protocol, Length, and Info.

No.	Time	Source	Destination	Protocol	Length	Info
7	60.000986000	192.168.4.1	192.168.4.2	BGP	85	KEEPALIVE Message
8	60.001036000	192.168.4.2	192.168.4.1	BGP	85	KEEPALIVE Message
9	60.001042000	192.168.4.1	192.168.4.2	TCP	66	bgp > 34177 [ACK] Seq=39 Ack=39 Win=57 Len=0 TStamp=486838 TSrc=r=486838
10	65.014952000	c6:06:09:3a:ab:0a	72:12:36:41:1e:bc	ARP	42	Who has 192.168.4.1? Tell 192.168.4.2
11	65.014945000	72:12:36:41:1e:bc	c6:06:09:3a:ab:0a	ARP	42	Who has 192.168.4.2? Tell 192.168.4.1
12	65.015015000	c6:06:09:3a:ab:0a	72:12:36:41:1e:bc	ARP	42	192.168.4.2 is at c6:06:09:3a:ab:0a
13	65.015025000	72:12:36:41:1e:bc	c6:06:09:3a:ab:0a	ARP	42	192.168.4.1 is at 72:12:36:41:1e:bc
14	120.00952000	192.168.4.1	192.168.4.2	BGP	85	KEEPALIVE Message
15	120.00862800	192.168.4.2	192.168.4.1	BGP	85	KEEPALIVE Message
16	120.00964000	192.168.4.1	192.168.4.2	TCP	66	bgp > 34177 [ACK] Seq=58 Ack=58 Win=57 Len=0 TStamp=501839 TSsrc=r=501839
17	125.01372400	c6:06:09:3a:ab:0a	72:12:36:41:1e:bc	ARP	42	Who has 192.168.4.1? Tell 192.168.4.2
18	125.01372000	72:12:36:41:1e:bc	c6:06:09:3a:ab:0a	ARP	42	Who has 192.168.4.2? Tell 192.168.4.1
19	125.01377100	c6:06:09:3a:ab:0a	72:12:36:41:1e:bc	ARP	42	192.168.4.2 is at c6:06:09:3a:ab:0a
20	125.01377800	72:12:36:41:1e:bc	c6:06:09:3a:ab:0a	ARP	42	192.168.4.1 is at 72:12:36:41:1e:bc
21	180.00598900	192.168.4.1	192.168.4.2	BGP	85	KEEPALIVE Message
22	180.00613100	192.168.4.2	192.168.4.1	BGP	85	KEEPALIVE Message
23	180.00614900	192.168.4.1	192.168.4.2	TCP	66	bgp > 34177 [ACK] Seq=77 Ack=77 Win=57 Len=0 TStamp=516840 TSsrc=r=516840
24	185.01371000	c6:06:09:3a:ab:0a	72:12:36:41:1e:bc	ARP	42	Who has 192.168.4.1? Tell 192.168.4.2
25	185.01370700	72:12:36:41:1e:bc	c6:06:09:3a:ab:0a	ARP	42	Who has 192.168.4.2? Tell 192.168.4.1
26	185.01379600	c6:06:09:3a:ab:0a	72:12:36:41:1e:bc	ARP	42	192.168.4.2 is at c6:06:09:3a:ab:0a
27	185.01374100	72:12:36:41:1e:bc	c6:06:09:3a:ab:0a	ARP	42	192.168.4.1 is at 72:12:36:41:1e:bc

Frame details:

- > Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
- > Ethernet II, Src: R1 (72:12:36:41:1e:bc) [ether], Dst: R2 (c6:06:09:3a:ab:0a) [ether]
- > Internet Protocol Version 4, Src: 192.168.4.1 (192.168.4.1), Dst: 192.168.4.2 (192.168.4.2)
- > Transmission Control Protocol, Src Port: bgp (179), Dst Port: 34177 (34177), Seq: 1, Ack: 1, Len: 19
- > Border Gateway Protocol - KEEPALIVE Message

4.12

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

No.	Time	Source	Destination	Protocol	Length	Info
13	65.016240000	c6:06:09:3a:ab:0a	72:12:36:41:1e:bc	ARP	42	192.168.4.2 is at c6:06:09:3a:ab:0a
14	65.016251000	72:12:36:41:1e:bc	c6:06:09:3a:ab:0a	ARP	42	192.168.4.1 is at 72:12:36:41:1e:bc
15	120.001827000	192.168.4.1	192.168.4.2	BGP	85	KEEPALIVE Message
16	120.001990000	192.168.4.2	192.168.4.1	BGP	85	KEEPALIVE Message
17	120.002011000	192.168.4.1	192.168.4.2	TCP	66	bgp > 34177 [ACK] Seq=58 Ack=58 Wir=57 Len=66
18	125.016088000	c6:06:09:3a:ab:0a	72:12:36:41:1e:bc	ARP	42	Who has 192.168.4.1? Tell 192.168.4.2
19	125.016085000	72:12:36:41:1e:bc	c6:06:09:3a:ab:0a	ARP	42	Who has 192.168.4.2? Tell 192.168.4.1
20	125.016119000	c6:06:09:3a:ab:0a	72:12:36:41:1e:bc	ARP	42	192.168.4.2 is at c6:06:09:3a:ab:0a
21	125.016126000	72:12:36:41:1e:bc	c6:06:09:3a:ab:0a	ARP	42	192.168.4.1 is at 72:12:36:41:1e:bc
22	170.264505000	192.168.4.1	192.168.4.2	BGP	93	UPDATE Message
23	170.304168000	192.168.4.2	192.168.4.1	TCP	66	34177 > bgp [ACK] Seq=58 Ack=85 Wir=60 Len=66
24	175.272222000	72:12:36:41:1e:bc	c6:06:09:3a:ab:0a	ARP	42	Who has 192.168.4.2? Tell 192.168.4.1
25	175.272277000	c6:06:09:3a:ab:0a	72:12:36:41:1e:bc	ARP	42	192.168.4.2 is at c6:06:09:3a:ab:0a

22 170.264505000 192.168.4.1 192.168.4.2 BGP 93 UPDATE Message

- ▷ Frame 22: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0
- ▷ Ethernet II, Src: 72:12:36:41:1e:bc (72:12:36:41:1e:bc), Dst: c6:06:09:3a:ab:0a (c6:06:09:3a:ab:0a)
- ▷ Internet Protocol Version 4, Src: 192.168.4.1 (192.168.4.1), Dst: 192.168.4.2 (192.168.4.2)
- ▷ Transmission Control Protocol, Src Port: bgp (179), Dst Port: 34177 (34177), Seq: 58, Ack: 58, Len: 93
- ▼ Border Gateway Protocol - UPDATE Message
 - Marker: ffffffffffffffffffffff
 - Length: 27
 - Type: UPDATE Message (2)
 - Unfeasible routes length: 4 bytes
 - ▼ Withdrawn routes:
 - ▽ 1.1.1.0/24
 - Withdrawn route prefix length: 24
 - Withdrawn prefix: 1.1.1.0 (1.1.1.0)
 - Total path attribute length: 0 bytes

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    3 i
*->  4.4.4.0/24        0.0.0.0          0    32768 i
*->  5.5.5.0/24        192.168.4.2          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    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:

