Routerlab

Summer semester 2018

Worksheet 4
Group 08

Valentin Franck, 364066
Nikhil Singh, 387694

Pages: 9

Submission Date: May 31, 2018

Part 1, Question 1

1a

In Unicast data is sent from one interface to the another interface. It is also known as one to one network communication. In Unicast there is only one sender and one receiver. For instance browsing a website where we receive data from the server to our computer. IPv6 unicast address are of four different types- Global Unicast - 2000::/3 Unique Local unicast - FC00::/7 Link local unicast - FE80::/10 Site local unicast - FEC0::/10

In Multicast data is sent to a group of devices on the network. These groups are identified by IPv6 multicast addresses. IPv6 multicast address starts with FF00::/8.

In Anycast same IP address is assigned to different nodes and these nodes are the nodes of the anycast group. It is used to reduce the latency and provide high availabilty with good quality of services. The scope of anycast addresses are the same as unicast. If a packet is sent to a anycast address only the nearest node (according to the routing metrics) will receive the packet. This means anycast requires support by the routers like multicast does.

1b

Global unicast addresses are of this form 2000::/3. These are similar to IPv4 public addresses and are routable on the internet. They consist of a global routing prefix, a subnet ID and the interface ID, which makes them more hierarchically structured than IPv4 addresses.

However, link local addresses are used to communicate between the devices which are in the same network (because these addresses are not routable). It is not guaranteed that they are unique beyond single network segments. In IPv6 they are assigned with address block fe80::/10. We have to use address and interface to refer to link local address. Link local addresses are use for neighbor discovery, for automatic address configuration and when no routers are present.

1c

Interface identifier is used to identify host's network interface on a link. It is the last part of IPv6 unicast or anycast address. Interface ID is usually of 64 bits (with the exception of 000 unicast addresses) and created by adding FFFE in the middle of the MAC address. For instance, if 00:XX:GG:MM:77:99 is the MAC address then Interface ID will be 00XXGGFFFEMM7799 and it is commonly known as modified Extended unique identifier 64 (EUI-64). The IPv6 interface identifier is computed from EUI-64 for SLAAC (Stateless Address Auto Configuration) and LL (Link Local addresses) by flipping the universal/local bit.

The same identifier should only be used once on a link or in a subnet, but can be reused in different networks. However the identifier can be globally unique. For privacy reasons the identifier can be set to be created randomly instead of from the MAC address.

In case of IPv4-Compatible IPv6 Addresses the identifier is created from the IPv4 address.

Part 1, Question 2

2a

/128

2b

/48

2c

/56

2d

/64

2e

As per the IPv6 address plan manual for point to point link between two routers /112 seems like the best non /64 alternative. However, as per RFC 4291 we should not use subnet prefix size other than /64. RFC 6164 on the other hand recommends /127 addresses, although it was discouraged by RFC 3627 and 5375, because it works in practice and is more secure. Therefore we would probably go with the /127 as it also most naturally resembles /31 used in IPv4.

Part 1, Question 3

3a

BOOTP was the predecessor of DHCP and was designed to provide IP address while the computer is booting up. It points the client to the image file which has an operating system. By default it has 30 days lease on IP address. BOOTP is especially good with diskless computer systems to locate its image file. However, DHCP is the successor of BOOTP which was designed to replace BOOTP. DHCP by default has 8 days lease on IP address and It provides IP addresses to the machines which relocate very frequently. It can easily renew their leases without restarting the system unlike BOOTP. The BOOTP files have to be configured manually while DHCP uses auto configuration and therefore is not as prone to errors as BOOTP. DHCP is compatible with BOOTP but not vice versa.

3b

DHCP solves this chicken and egg problem by using the technique known as Broadcasting. It sends the DHCP Discover which is basically a request "Can someone give me an IP address?" (which also serves the purpose of finding the DHCP server) and then it gets a (unicast) response from the DHCP server as DHCP Offer which leases the IP address to our computer then our computer responds with a DHCP Request message to confirm that the IP address that has been offered is accepted and then it gets an acknowlegement from the DHCP server as DHCP Acknowledged. There are more messages types in DHCP, for example to retrieve particular information or to deny a DHCPrequest.

Broadcasting is required not only at the Network Layer but also at the Link layer. Therefore DHCP needs help ob a layer below itself, which can be considered a layering violation.

Part 1, Question 4

4a

No. Because IPv6 stateless autoconfiguration doesn't require manual configuration of hosts. It allows hosts to engender its own addresses by combination of locally available information and information advertised by the routers. Hosts generate interface identifier which identifies the interface uniquely on the subnet and router advertises the prefixes which identifies the subnet associated with the link. This means the host assigns itself a link local address for the initial configuration with the router. The host is then able to find the routers using NDP by using a multicast request to all routers in the network segment. If there is no router, hosts can generate link local addresses automatically which allows them to communicate between the devices in the same network.

4b

As mentioned in the slides Client sends an information request message to all relay agents and servers multicast address. Then server sends a reply message with the configuration information. In SLAAC client picks their own address from the advertised prefix on the connected interface. It uses EUI-64 format for the address assignment. In Stateless Address Autoconfiguration (SLAAC) there is no server that keeps track of address asignments unlike in DHCPv6, where the server assigns addresses and keeps track of that. If we combine DHCPv6 and SLAAC, the DHCPv6 server does not assigns addresses (which is already taken care of by SLAAC) but only gives information on DNS servers, domain names etc. by using the M(Managed), O(Otherconfig) and A(Autonomous) flags. This is not supported by SLAAC alone. The combination of SLAAC and DHCPv6 is also called Stateless DHCPv6.

4c

In DHCPv4 after booting up client sends broadcast message to the local network looking for the DHCP server. It announces itself and seeks the IP address information. This information is then given out and stored for a very limited duration in the form of a table which has the information like Client name, Interface, IP address, MAC address, Expire time etc. It uses 4 message statefule exchange between client and server - DORA (Discover, Offer, Request, Acknowledge). Apart from this basic functionality it also offers to provide clients information on DNS server, gateways, NTP servers etc.

DHCPv6 also uses 4 message stateful exchange SARR (Solicit, Advice, Request, Reply) between client and server. It uses DHCP Unique identifiers DUIDs. After receiving a valid request DHCP server assigns IP address from its pool of addresses with other network configuration parameters like default gateway and subnet mask, Domain Name System (DNS) server addresses, domain names, Simple Network Time Protocol (SNTP) etc. DHCPv6 offers the same services as DHCP in IPv4 but optionally also offers to provide further information to clients.

In IPv6 SLAAC enables each node connected to LAN which is connected to the internet via router or gateway to self configure its own info like IP address. We already mentioned the differences to DHCPv6, e.g. SLAAC does not allow to provide information on DNS servers etc. SLAAC is combined with NDP which allows to provide more information than ARP in IPv4, e.g. it provides a router and prefix list (network topology).

Part 2, Question 1

We are using the topology as shown in Figure 1.

```
root@group08-lg2:~# ip a s eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    state UP group default qlen 1000
    link/ether 00:16:3e:af:08:21 brd ff:ff:ff:ff:ff:ff
    inet 10.8.2.2/29 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fd00:470:525b:f802::2/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::216:3eff:feaf:821/64 scope link
       valid_lft forever preferred_lft forever
```

Part 2, Question 2

We ran the dhcp server on lg4 like this:

```
root@group08-lg4:~# ps -aux | grep dhcp
```

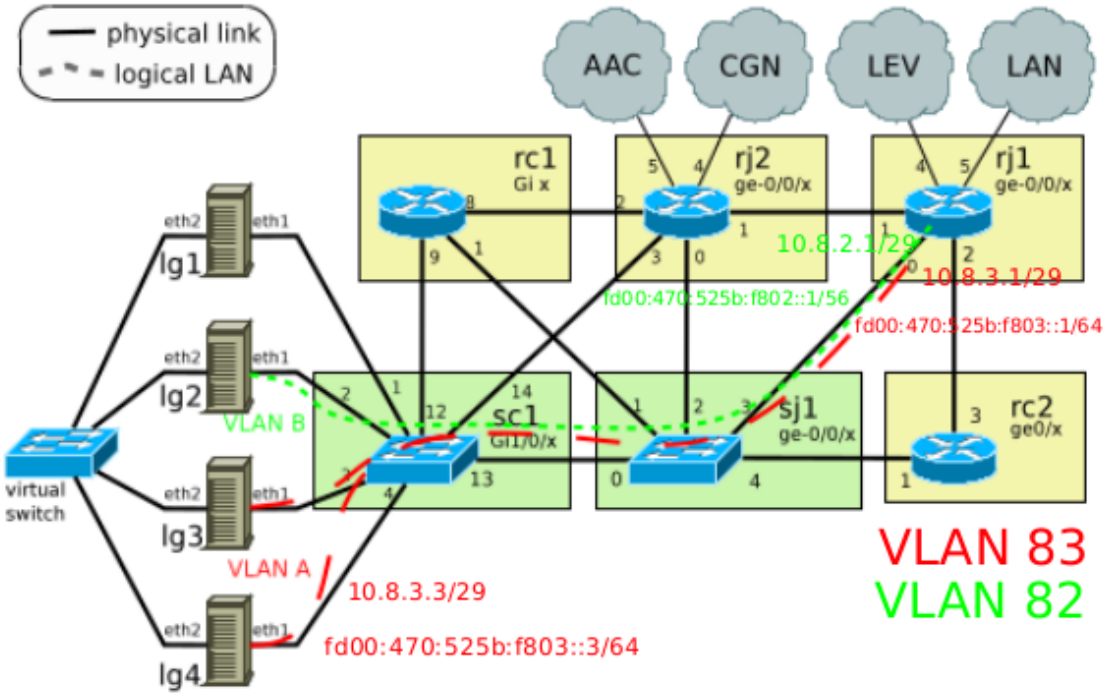

Figure 1: The topology we use.

```
root        5740  0.0  0.2  20476  2944 ?        Ss   07:02   0:00 /sbin/
    dhclient -4 -v -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/
    dhclient.eth0.leases -I -df /var/lib/dhcp/dhclient6.eth0.leases
    eth0
root        7085  0.0  0.2  21908  2804 hvc0     T    15:33   0:00 nano /
    etc/default/isc-dhcp-server
root        7658  0.0  0.9  35544  9448 ?        Ss   16:26   0:00 /usr/
    sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf eth1
root        7663  0.0  0.0  11116   968 hvc0     S+   16:27   0:00 grep
    dhcp
```

The relevant parts from our /etc/dhcp/dhcpd.conf:

```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# option definitions common to all supported networks...
# option domain-name "example.org";
# option domain-name-servers ns1.example.org, ns2.example.org;
default-lease-time 600;
max-lease-time 7200;
option domain-name "mylan.blabla";
option domain-name-servers 172.16.255.254;

subnet 10.8.3.0 netmask 255.255.255.248 {
 range 10.8.3.4 10.8.3.6;
 option routers 10.8.3.1;
 option broadcast-address 10.8.3.7;
 option domain-name-servers 172.16.255.254;
```

```
 option domain-search "routerlab", "dmz.routerlab", "inet.tu-berlin.de
     ";
 option ntp-servers 172.16.0.2;
}
subnet 10.8.2.0 netmask 255.255.255.248 {
 range 10.8.2.2 10.8.2.6;
 option routers 10.8.2.1;
 option broadcast-address 10.8.2.7;
 option domain-name-servers 172.16.255.254;
 option domain-search "routerlab", "dmz.routerlab", "inet.tu-berlin.de
     ";
 option ntp-servers 172.16.0.2;
}
# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;
```

Our /etc/default/isc-dhcp-server:

```
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID
    instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests
    ?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="eth1"
#INTERFACESv6="eth1"
```

Part 2, Question 3

3a

```
root@group08-lg3:~# tcpdump -vvvv -X -i eth1 -n src host 10.8.3.3
[2796311.087646] device eth1 entered promiscuous mode
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size
    262144 bytes
16:45:10.267686 ARP, Ethernet (len 6), IPv4 (len 4), Reply 10.8.3.3 is-
    at 00:16:3e:af:08:41, length 46
        0x0000:  0001 0800 0604 0002 0016 3eaf 0841 0a08  ..........>..
            A..
        0x0010:  0303 0016 3eaf 0831 0a08 0304 0000 0000
            ....>..1........
        0x0020:  0000 0000 0000 0000 0000 0000 0000
            ..............
```

```
16:45:10.270005 IP (tos 0x0, ttl 64, id 25323, offset 0, flags [DF],
    proto UDP (17), length 366)
     10.8.3.3.67 > 10.8.3.4.68: [udp sum ok] BOOTP/DHCP, Reply, length
        338, xid 0x5366534c, Flags [none] (0x0000)
          Client-IP 10.8.3.4
          Your-IP 10.8.3.4
          Client-Ethernet-Address 00:16:3e:af:08:31
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: ACK
            Server-ID Option 54, length 4: 10.8.3.3
            Lease-Time Option 51, length 4: 600
            Subnet-Mask Option 1, length 4: 255.255.255.248
            BR Option 28, length 4: 10.8.3.7
            Default-Gateway Option 3, length 4: 10.8.3.1
            Domain-Name Option 15, length 12: "mylan.blabla"
            Domain-Name-Server Option 6, length 4: 172.16.255.254
            T119 Option 119, length 36:
                158494581,1952805484,1633812483,1684896448,289134,1702103412,196590858

            NTP Option 42, length 4: 172.16.0.2
            END Option 255, length 0
         0x0000:  4500 016e 62eb 4000 4011 bc7d 0a08 0303  E..nb.@.@
            ..}....
         0x0010:  0a08 0304 0043 0044 015a 4a28 0201 0600  .....C.D.ZJ
            (....
         0x0020:  5366 534c 0000 0000 0a08 0304 0a08 0304  SfSL
            ............
         0x0030:  0000 0000 0000 0000 0016 3eaf 0831 0000
            .........>..1..
         0x0040:  0000 0000 0000 0000 0000 0000 0000 0000
            ................
         0x0050:  0000 0000 0000 0000 0000 0000 0000 0000
            ................
         0x0060:  0000 0000 0000 0000 0000 0000 0000 0000
            ................
         0x0070:  0000 0000 0000 0000 0000 0000 0000 0000
            ................
         0x0080:  0000 0000 0000 0000 0000 0000 0000 0000
            ................
         0x0090:  0000 0000 0000 0000 0000 0000 0000 0000
            ................
         0x00a0:  0000 0000 0000 0000 0000 0000 0000 0000
            ................
         0x00b0:  0000 0000 0000 0000 0000 0000 0000 0000
            ................
         0x00c0:  0000 0000 0000 0000 0000 0000 0000 0000
            ................
         0x00d0:  0000 0000 0000 0000 0000 0000 0000 0000
            ................
         0x00e0:  0000 0000 0000 0000 0000 0000 0000 0000
            ................
         0x00f0:  0000 0000 0000 0000 0000 0000 0000 0000
            ................
         0x0100:  0000 0000 0000 0000 6382 5363 3501 0536  ........c.Sc5
            ..6
```

```
        0x0110:  040a 0803 0333 0400 0002 5801 04ff ffff  .....3....X
            .....
        0x0120:  f81c 040a 0803 0703 040a 0803 010f 0c6d
            ...............m
        0x0130:  796c 616e 2e62 6c61 626c 6106 04ac 10ff  ylan.blabla
            .....
        0x0140:  fe77 2409 726f 7574 6572 6c61 6200 0364  .w$.routerlab
            ..d
        0x0150:  6d7a c000 0469 6e65 7409 7475 2d62 6572  mz...inet.tu-
            ber
        0x0160:  6c69 6e02 6465 002a 04ac 1000 02ff       lin.de
            .*......
16:45:15.281185 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has
    10.8.3.4 tell 10.8.3.3, length 46
        0x0000:  0001 0800 0604 0001 0016 3eaf 0841 0a08  ..........>..
            A..
        0x0010:  0303 0000 0000 0000 0a08 0304 0000 0000
            ................
        0x0020:  0000 0000 0000 0000 0000 0000 0000
            ..............
```

3b

We added this to /etc/network/interfaces on lg2 and lg3:

```
# Get our IP address from any DHCP server
auto eth1
iface eth1 inet dhcp

root@group08-lg3:~# service networking restart; ifconfig eth1
[2796216.999241] device eth1 left promiscuous mode
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.8.3.4  netmask 255.255.255.248  broadcast 10.8.3.7
        inet6 fe80::216:3eff:feaf:831  prefixlen 64  scopeid 0x20<link>
        ether 00:16:3e:af:08:31  txqueuelen 1000  (Ethernet)
        RX packets 216508  bytes 501516827 (478.2 MiB)
        RX errors 0  dropped 40  overruns 0  frame 0
        TX packets 26100  bytes 1782751 (1.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3c

We used the same configuration for the DHCP server as before.

Open Questions:

How should the DHCP server on lg4 know it has to assign an IP address from the 10.8.2.0/29 subnet, if the request is just forwarded from the router? We assume, we could not get lg2 to retrieve an IP address from the DHCP server, because the relay agent was not configured properly. Especially we had problems to configure the firewall such, that it would allow dhcp packets. We used this configuration on lev-rj1:

```
root@lev-rj1# show forwarding-options
dhcp-relay {
    server-group {
        dhcp-server {
            10.8.3.3;
        }
    }
    active-server-group dhcp-server;
```

```
    group dhcp {
        interface ge-0/0/0.0;
    }
}
```

We used this command to set the security policy, but were not able to commit and could not resolve the issue without creating other issues:

```
root@lev-rj1# set security zones security-zone trust interfaces ge
    -0/0/0 host-inbound-traffic system-services dhcp
```

We checked on lg-4 by using tcpdump and confirmed that the DHCPDISCOVER messages were never received. So the problem is located on rj1 we assume, which does not forward the message as intended.

3d

See our problems at 3c.