Homework 2 for Evolving Internet

Gabriele Genovese

24 October 2024

1 Exercise 1

1.1 First point

The first line means that any IP address in the range 208.12.0.0 to 208.12.255.255 (determined by the /16 prefix, which uses the first 16 bits as the network identifier) will be forwarded to Router 2.

The second line means that any IP address in the range 208.12.16.0 to 208.12.16.255 will be forwarded to Router 4.

1.2 Second point

1. 135.46.63.10 corresponds to `10000111.00101110.00111111.00001010`. 135.46.60.0/22 corresponds to `11111111.11111111.00111100.00000000` and the first 22 bits match. Therefore, we route to Router 3.
2. 135.46.57.14 corresponds to `10000111.00101110.00111001.00001110`. 135.46.56.0/22 corresponds to `10000111.00101110.00111000.00000000` and the first 22 bits match. Therefore, we route to Router 4.
3. 208.12.16.0 corresponds to `11010000.00001100.00010000.00000000`. It exactly matches the second entry in the table for 24 bits. Therefore, we route to Router 4, but the IP addresses it's reserved because it's a network IP, then at some point it will be dropped.
4. 208.12.31.0 corresponds to `11010000.00001100.00011111.00000000`. 208.12.0.0/16 corresponds to `11010000.00001100.00000000.00000000` and the first 16 bits match. Therefore, we route to Router 2 (we do not drop the packet because it's a valid IP for an host for CIDR).

2 Exercise 2

2.1 First point

The prefix `/20` means that 20 bits are used for the network part, leaving 12 bits for the host part. The total number of IPs in this network is $2^{12} = 4096$. Excluding the reserved network and broadcast addresses, the number of usable addresses for hosts is $4096 - 2 = 4094$.

2.2 Second point

- 17.46.64.0/19 can be allocated because it does not overlap with the original class A network;
- 134.15.0.0/20 can be allocated with the original class B network, because it does not overlap with it;
- 194.65.32.0/21 cannot be allocated because 21 bits are used for the network and 11 for hosts but the original class C allocation has 24 network bits, leaving 8 bits for hosts. So, the two subnetworks overlaps and 194.65.32.0/21 cannot be allocated.

2.3 Third point

Class A network provides 2^{24} addresses (16777216) for host and it's too much. Class B network provides 2^{16} addresses (65536) for host and it's also too much. Class C network provides 2^8 addresses (256) for

host and they are too few addresses. So, they need 4 class C networks at minimum but this is not really optimal because the the address space is fragmented.

2.4 Fourth point

The ISP owns the 202.0.64.0/18 block, which provides a total of $2^{14} = 16384$ addresses (spanning from 202.0.64.0 to 202.0.127.255). A `/22` prefix provides $2^{10} = 1024$ addresses, which is sufficient to accommodate $800 + 2$ addresses asked from the customer. Since the first free address is 202.0.80.0, the ISP would allocate the block 202.0.80.0/22. This block of addresses covers the range from 202.0.80.0 to 202.0.83.255.

3 Exercise 3

3.1 First point

Tab. 1: Startup distance vectors

	A	**B**	**C**	**D**	**E**
A	0	1	4	∞	∞
B	1	0	1	1	∞
C	4	1	0	∞	4
D	∞	1	∞	0	1
E	∞	∞	4	1	0

Tab. 2: End distance vectors

	A	**B**	**C**	**D**	**E**
A	0	1	2	2	3
B	1	0	1	1	2
C	2	1	0	2	3
D	2	1	2	0	1
E	3	2	3	1	0

3.2 Second point

The Split Horizon technique avoids routing loops by not advertising routes back in the direction from which they were learned. Poison Reverse explicitly marks the route back to the source as unreachable (infinity). Both techniques reduce the chance of routing loops, mitigating the Count To Infinity problem.

So, the DV sent by D to B is going to be $[\infty, \infty, \infty, 0, 1]$ and DV sent by E to C is going to be $[3, 2, 3, 1, 0]$.

3.3 Third point

When the connection between nodes B and A fails, B will update its DV of A to ∞. At time 125, B will broadcast this change in its distance vector to C and D. D will adjust its distance to A at ∞ and C adjust its distance to A at 4 (direct link). E will learn of A through D and it will also update its distance to A to ∞ upon hearing that D can no longer reach A. C will broadcast its new distance, triggering the update of all the distances to A of the nodes B, D and E to respectevly 5, 6, 7.

Count to infinity will not occur because the split horizon and poison reverse techniques are used.

3.4 Fourth point

When the connection between nodes A and C fails, C updated its DV of A at ∞. Node A is now unreachable from any node. But E will brodcast at time 290 its outdated DV at C (with cost 7 to go to

A because the split horizon with poison reverse doesn't apply in this case because we route through D) as its cost-to-go to A. E will update its DV of A to 10, with next hop E. This will lead to a Count To Infinity.

3.5 Fifth point

If we consider the "triggered updates", C will broadcast the change to B and E immediatelly, but only B will update its value. E will then broadcast its value, leading to a Count To Infinity. With DUAL version, E will now freeze its routing table, leaving time to the update to propage to D. Therefore, the problems is now solved thanks to the freeze property.

4 Exercise 4

4.1 First point

A *provider-customer transit link* refers to a relationship where one AS agrees to offer full connectivity to the global internet for another AS. The provider allows the customer to route its traffic to any destination on the internet, often with a fee.

A *peering link* is an arrangement where two AS agree to exchange traffic directly between their networks without any financial settlement. Both parties benefit from this approach because it reduces costs and improves performance.

4.2 Second point

BGP route import and selection rules reflect commercial relationships between AS. The import rules prioritize routes from customers to maximize revenue, followed by peers, and providers (to minimize costs). The export rules determine which routes an AS shares. To customers, the AS shares all routes, including those from other customers, peers, and providers. To peers, the AS only shares routes from itself and its customers, avoiding routes from other peers or providers to prevent acting as free transit. To providers, the AS shares only its own routes and those of its customers, excluding routes learned from peers or other providers.

4.3 Third point

The customer's router should manipulate the LOCAL_PREF attribute. It should set a high LOCAL_PREF for routes announced over the primary link, indicating the preference for this path. For the backup link, the customer should use a lower value for the LOCAL_PREF attribute. This assures that packets uses the primary link, and only switches to the backup link in the event of a failure.

4.4 Fourth point

The previous solution proposed does not work in this case because LOCAL_PREF is not enought to ensure that AS3 does not become an active path for traffic. We can also use the AS_PATH attribute to prepend its AS number when announcing routes to AS3, AS2 can ensure that AS1 remains the primary link while AS3 acts as a backup.

4.5 Fifth point

The Community attribute is a way to label routes, making it easier to manage them. It helps with filtering routes and directing traffic. This also allows different networks to communicate preferences about how routes should be handled. This could be used as solution for the previous scenario. For example, use the label `primary` for routes from the first provider and `backup` for the route from the second provider. Set also the LOCAL_PREF attribute according the solution for 3).