CS 2204-01 Communications and Networking

Instructor: Professor Sharon Sisitzky

Name: Anonymos

Written Assignment Unit 4

**1. For each IPv4 network prefix given (with length), identify which of the subsequent IPv4 addresses are part of the same subnet.**

**(a). 10.0.130.0/23: 10.0.130.23, 10.0.129.1, 10.0.131.12, 10.0.132.7**

**(b). 10.0.132.0/22: 10.0.130.23, 10.0.135.1, 10.0.134.12, 10.0.136.7**

**(c). 10.0.64.0/18: 10.0.65.13, 10.0.32.4, 10.0.127.3, 10.0.128.4**

**(d). 10.0.168.0/21: 10.0.166.1, 10.0.170.3, 10.0.174.5, 10.0.177.7**

**(e). 10.0.0.64/26: 10.0.0.125, 10.0.0.66, 10.0.0.130, 10.0.0.62**

To answer this question, it is necessary to determine whether each IPv4 address belongs to a given network prefix. This can be determined by identifying the range indicated by the network address.

(a) 10.0.130.0/23: This network address indicates a range from 10.0.130.1 to 10.0.131.255. Therefore,

Belongs to subnet: 10.0.130.23, 10.0.131.12

Not belonging to subnet: 10.0.129.1, 10.0.132.7

(b) 10.0.132.0/22: This network address indicates the range 10.0.132.1 to 10.0.135.254. Therefore,

Belongs to subnet: 10.0.135.1, 10.0.134.12

Not belonging: 10.0.130.23, 10.0.136.7

(c) 10.0.64.0/18: This network address indicates a range of 10.0.64.1 to 10.0.127.255. Therefore,

Belongs to subnet: 10.0.65.13, 10.0.127.3

Not belonging: 10.0.32.4, 10.0.128.4

(d) 10.0.168.0/21: This network address indicates a range of 10.0.168.1 to 10.0.175.255. Therefore,

Belongs to subnet: 10.0.170.3, 10.0.174.5

Not belonging to subnet: 10.0.166.1, 10.0.177.7

(e) 10.0.0.64/26: This network address indicates a range of 10.0.0.1 to 10.0.7.255. Therefore,

Belongs to subnet: 10.0.0.125, 10.0.0.66, 10.0.0.130, 10.0.0.62

Not belonging: None

**2. Convert the following subnet masks to /k notation, and vice-versa:**

To convert a subnet mask to "/k" notation, count the number of 1's in the subnet mask. Conversely, to convert a subnet mask from "/k" notation to a subnet mask, place a 0 after the 1 in the specified number of bits.

(a). 255.255.240.0 -> /20

(b). 255.255.248.0 -> /21

(c). 255.255.255.192 -> 26

(d). /20 -> 255.255.240.0

(e). /22 -> 255.255.252.0

(f). /27 -> 255.255.255.224

**3. Suppose an Ethernet packet represents a TCP acknowledgment; that is, the packet contains an IPv4 header with no options and a 20-byte TCP header but nothing else. Is the IPv4 packet here smaller than the Ethernet minimum packet size, and, if so, by how much? What if the packet is IPv6 with no extension headers?**

The minimum size of an Ethernet frame is 64 bytes, which includes the Ethernet header (14 bytes), payload (46 bytes minimum), and 4 bytes of frame check sequence (FCS). The payload portion is the sum of the data and padding and must be a minimum of 46 bytes. If the payload is less than 46 bytes, it is increased to 46 bytes by padding.

The standard size of the IPv4 header is 20 bytes, and the TCP header is also 20 bytes; if the IPv4 packet has no options and contains only the TCP header, the total payload size is 40 bytes.

Thus, compared to the Ethernet minimum payload requirement (46 bytes), this IPv4 packet is 6 bytes smaller than the minimum size. To make up the difference, the Ethernet frame requires 6 bytes of padding.

For IPv6, the header size is 40 bytes. If an IPv6 packet has no extension header and also has a TCP header of 20 bytes, the total payload size is 60 bytes. This is still short of the Ethernet minimum payload requirement, which requires 6 bytes of padding.

In summary, both IPv4 and IPv6 packets are smaller than the Ethernet minimum packet size, each requiring 6 bytes of padding.

**4. In newer implementations, repeat ARP queries about a timed-out entry are first sent unicast, in order to reduce broadcast traffic. What would have to happen to create a situation where the repeated unicast query for a given IP address fails, but a follow-up broadcast query for that same IP address succeeds?**

With respect to ARP query behavior in the new implementation, certain network conditions and settings may be influential in creating a situation where a unicast ARP query for a timed-out entry fails and a subsequent broadcast ARP query succeeds. The following are scenarios that may create such a situation

1. cache invalidation or expiration: If the MAC address associated with the target IP address has been removed from the ARP cache or has expired, the device will need to retrieve this information again. If unicast queries do not reach the target or the target is not responding (e.g., powered off, disconnected from the network, etc.), a broadcast query may provide a response by sending a more extensive query.

2. security policy or firewall settings: If security policies or firewalls in the network restrict unicast traffic, certain unicast ARP requests may be blocked. This may cause unicast queries to fail and broadcast queries to succeed without being affected by such restrictions. 3.

3. network configuration changes: Network configuration changes may cause unicast queries to fail to reach the target device. For example, unicast ARP queries may be blocked if the port security settings on the switch have been changed to allow only traffic from certain MAC addresses. The broadcast query is then sent across the network and succeeds when the target device responds.

4. network failure or instability: Unicast ARP queries may not be delivered successfully due to temporary network failure or instability. The broadcast query may then succeed when network conditions improve.

Word-Count: 656

References

Dordal, P. (2019). *An introduction to computer networks.*

(n.d.). *Computer networks.*