NASA hw0 Network Administration

Student

- Name: 林楷恩
- ID: B07902075

True or False

1. **False.** To be more accurate, DNS servers do not store "all" of the records locally, and there are many kinds of name servers that work in different ways. For example, authoritative servers store the records of the zone which they are responsible for and just send a referal when queried addresses belong to other zones, while some servers are responsible for solving addresses by recursively querying other servers and they don't have to store any records(except temporary cache).
   *** ref.**
   - UNIX and Linux System Administration Handbook 5th edition, Chapter 16

2. **False.** Though TCP does provide reliable data transfer, it becomes slower because of its complexity. Instead, UDP can provide a fast data transfer, and it could be preferable in some services such as voice over IP(VoIP).
   *** ref.**
   - https://www.diffen.com/difference/TCP_vs_UDP

3. **True.** There are 3 cases may increase download speed:
   1. The connection may be slow because the delay on typical routing path. Since traffic should go to VPN server first, it might solve the problem by avoid passing through the part that causing slowness.
   2. The VPN provider may have a better connection with the destined netwotk than your ISP does.
   3. The ISP may do "Bandwidth Throttling", which slows down the traffic for the specific type of data. By VPN, ISP cannot inspect our traffic, so the rules they set for throttling will not match anymore, thus solving the problem.

   *** ref.**
   - https://www.fastestvpnguide.com/can-a-vpn-increase-internet-speed/

4. **True.** Without NAT, private addresses will duplicate in public network many times.
   *** ref.**
   - UNIX and Linux System Administration Handbook 5th edition, Chapter 13, p.392

5. **False.** We can manually configure it.
   *** ref.**
   - http://linux.vbird.org/linux_server/0340dhcp.php

6. **False.** IP is associated with "network interface" and a device may have multiple network interfaces, so a device may have multiple IP at a time.
   *** ref.**
   - UNIX and Linux System Administration Handbook 5th edition, Chapter 13, p.384

7. **False.** Because of NAT, a public IP can be associated with many devices.
   *** ref.**
   - UNIX and Linux System Administration Handbook 5th edition, Chapter 13, p.392

8. **False.** The 1Gbps is just a upper bound obtained in laboratory condition. In daily use, there are many factors that can reduce network speed, such as congestion.
   *** ref.**
   - https://www.howtogeek.com/165321/why-you-probably-arent-getting-the-internet-speeds-youre-paying-for-and-how-to-tell/

9. **True.** For example, Netfilter is a firewall service built in Linux kernel and we can configure its rule through iptables.
   *** ref.**
   - https://www.digitalocean.com/community/tutorials/what-is-a-firewall-and-how-does-it-work
   - https://en.wikipedia.org/wiki/Netfilter

10. **False.** There have been several security issues discovered in WPA2, such as the KRACK attack.
    *** ref.**
    - https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#Security_issues

11. **False.** Traffic inside the same LAN still have to pass through switch to be directed to correct devices.
    *** ref.**
    - UNIX and Linux System Administration Handbook 5th edition, Chapter 14, p.465

12. **False.** Not all cases. Since 5G wireless band has lower range, it might not be preferable in case of the need of wider range.
    *** ref.**
    - https://superuser.com/questions/541554/what-is-the-difference-between-2-4g-and-5g-wireless

Short answer

1.
   - **Layer 1 (Physical Layer)**: responsible for the conversion between digital bits and electrical, radio, and optical signal, as well as the transmission and reception of these unstructured raw data.
     ex. autonegotiation.
   - **Layer 2 (Data Link Layer)**: responsible for transfer between two directly connected nodes in the same link. It also detects and maybe correct errors that may occur in physical layer.
     ex. ARP
   - **Layer 3 (Network Layer)**: provides means of transfering packets from one node to another node connected in different network. It finds a proper path based on the information transport layer provides and the destination addresses, and routes the packets through intermediate nodes.
     ex. IP
   - **Layer 4 (Transport Layer)**: establishes and controls connections between applications. It assigns port number to applications and control the reliability and speed through flow control, segmentation/desegmentation, and error control(e.g. sending ACK to ensure the success of transmission).

ex. TCP
- **Layer 5 (Application Layer)**: defines protocols or interfaces for different applications to take use of transport layer.
  ex. HTTP

*** ref.**
- https://en.wikipedia.org/wiki/Internet_protocol_suite
- http://microchipdeveloper.com/tcpip:tcp-ip-five-layer-model

2.
   1. Definition: IPv4 exhaustion is the drain of unallocated IPv4 addresses.
   2. Causes:
      - **Birth Defect**: The capacity of IPv4 is extremely insufficient because of the original design of 32-bits address.
      - **Drastic growth of Internet**: With the rise of mobile devices, Internet of Things, the trend of multiple interfaces on a device, and the universalization of Internet, the demand of IP addresses has been growing too quickly for IPv4 to afford.
      - **Classful network**: In the early days of Internet, organizations were allocated far more IP addresses than they actually required, because the "classful network" allocation method, since the class A blocks contained too many address while the size of class B, C were extremely less than it (2^24 vs 2^16). This led to the inefficient use of IP and it was often a large waste on the class A blocks.
   3. Workarounds:
      - **NAT (Network Address Translation)**: It makes a large private network able to use one public IP connecting with Internet, so the private IPs can be reused many times in different private network.
      - **IPv6**: uses a 128-bits address, whose capacity is far more than IPv4's.

*** ref.**
- https://en.wikipedia.org/wiki/IPv4_address_exhaustion

3. DoS is the abbreviation of Denial-of-Service. This kind of cyber-attack makes a service inaccessible to its users by flooding the server with a large number of packets, and thus overloading the bandwidth or computing resources of the targets. DDoS, which means Distributed-Denial-of-Service, is similar to DoS, but the different points are the method and the result. DoS attacks the targets with one computer and one connection, while DDoS utilizes many computers and many connections which may be hijacked by the attacker. Therefore, the result of DDoS is often much more severe and hard to defense than normal DoS.

*** ref.**
- http://www.security-faqs.com/dos-vs-ddos-what-is-the-difference.html

4. MAC address (Media Access Control address) is a 48-bits address which is typically shown as six groups of two hexadecimal digits. It served as a unique identifier of a network interface controller(NIC) for communications in the media access control sublayer of data link layer. MAC addresses are mostly hard-coded on hardware by manufacturers.

   MAC address is used to identify hosts in data link layer. It is the lowest level address so every packets in ethernet transfered from one MAC address to another MAC address. The packet receiver compares the destination MAC address with its own MAC address, if they are different, it discards it(except the broadcast address). There are several usage example:
   1. Switch use it to determine which hosts to forward.
   2. ARP takes use of MAC broadcast address to ask every host in one link for the purpose of knowing each IP's corresponding MAC address.

*** ref.**
- https://www.howtogeek.com/169540/what-exactly-is-a-mac-address-used-for/
- https://en.wikipedia.org/wiki/MAC_address

Command line utility

1. `$ dig +trace @8.8.8.8 csie.ntu.edu.tw`

```
; <<>> DiG 9.11.3-1ubuntu1.3-Ubuntu <<>> +trace @8.8.8.8 csie.ntu.edu.tw
; (1 server found)
;; global options: +cmd
.                       244148  IN      NS      b.root-servers.net.
.                       244148  IN      NS      a.root-servers.net.
.                       244148  IN      NS      m.root-servers.net.
.                       244148  IN      NS      d.root-servers.net.
.                       244148  IN      NS      e.root-servers.net.
.                       244148  IN      NS      c.root-servers.net.
.                       244148  IN      NS      f.root-servers.net.
.                       244148  IN      NS      k.root-servers.net.
.                       244148  IN      NS      i.root-servers.net.
.                       244148  IN      NS      j.root-servers.net.
.                       244148  IN      NS      g.root-servers.net.
.                       244148  IN      NS      l.root-servers.net.
.                       244148  IN      NS      h.root-servers.net.
.                       244148  IN      RRSIG   NS 8 0 518400 20190213050000 20190131040000 16749 . QBJvQT9GU4wqJTIYBZnRRV3OBG
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 18 ms

tw.                     172800  IN      NS      a.dns.tw.
tw.                     172800  IN      NS      b.dns.tw.
tw.                     172800  IN      NS      c.dns.tw.
tw.                     172800  IN      NS      d.dns.tw.
tw.                     172800  IN      NS      e.dns.tw.
tw.                     172800  IN      NS      f.dns.tw.
tw.                     172800  IN      NS      g.dns.tw.
tw.                     172800  IN      NS      h.dns.tw.
tw.                     172800  IN      NS      ns.twnic.net.
tw.                     172800  IN      NS      anytld.apnic.net.
tw.                     86400   IN      DS      40792 8 2 A05DB4B0DEB971031361BB621E8BB1B8D7346665A3D1B06EC1431ADB 7D015EE9
tw.                     86400   IN      RRSIG   DS 8 1 86400 20190213050000 20190131040000 16749 . EBgSzvgPqXBNveYYKb1gK6tiUOh
;; Received 976 bytes from 193.0.14.129#53(k.root-servers.net) in 16 ms

edu.tw.                 3600    IN      NS      d.twnic.net.tw.
edu.tw.                 3600    IN      NS      c.twnic.net.tw.
edu.tw.                 3600    IN      NS      a.twnic.net.tw.
edu.tw.                 3600    IN      NS      moemoon.edu.tw.
edu.tw.                 3600    IN      NS      b.twnic.net.tw.
edu.tw.                 3600    IN      NS      moestar.edu.tw.
edu.tw.                 300     IN      DS      40234 8 2 289D061D208C871915EB07F63FB175B21022422D5365D4E945BCE397 104A9C08
edu.tw.                 300     IN      DS      40234 8 1 5A8AB67C461F4330D146EE4E2E5A08CE279B7BEB
edu.tw.                 300     IN      RRSIG   DS 8 2 300 20190302080412 20190131080412 12261 tw. P1lJX9sGOIJkXgO+8mZCUgXdL7S
;; Received 648 bytes from 204.61.216.119#53(h.dns.tw) in 159 ms

ntu.edu.tw.             300     IN      NS      dns.ntu.edu.tw.
ntu.edu.tw.             300     IN      NS      dns.tp1rc.edu.tw.
ntu.edu.tw.             300     IN      NS      ntu3.ntu.edu.tw.
J9LEL04B9O4SSTE16PE1HPKFUN2F9UVM.edu.tw. 300 IN NSEC3 1 0 10 D68832F6B3 J9VF6HK048TRSO20948PI0V8SUJN7TDF  NS
J9LEL04B9O4SSTE16PE1HPKFUN2F9UVM.edu.tw. 300 IN RRSIG NSEC3 8 3 300 20190203235339 20190130225737 9888 edu.tw. bUMBsnqmRUSIl+p
;; Received 410 bytes from 13.248.142.26#53(a.twnic.net.tw) in 91 ms

csie.ntu.edu.tw.        86400   IN      NS      csman2.csie.ntu.edu.tw.
csie.ntu.edu.tw.        86400   IN      NS      csman3.csie.ntu.edu.tw.
csie.ntu.edu.tw.        86400   IN      NS      csman.csie.ntu.edu.tw.
couldn't get address for 'csman3.csie.ntu.edu.tw': not found
;; Received 182 bytes from 140.112.254.4#53(dns.ntu.edu.tw) in 135 ms

csie.ntu.edu.tw.        600     IN      A       140.112.30.28
csie.ntu.edu.tw.        600     IN      NS      csman.csie.ntu.edu.tw.
csie.ntu.edu.tw.        600     IN      NS      ntuns.ntu.edu.tw.
csie.ntu.edu.tw.        600     IN      NS      csman2.csie.ntu.edu.tw.
;; Received 153 bytes from 140.112.30.14#53(csman2.csie.ntu.edu.tw) in 17 ms
```

*** ref.**

- https://serverfault.com/questions/247671/is-it-possible-to-trace-the-delegation-path-for-a-dns-lookup

2. `$ traceroute -A google.com`

```
traceroute to google.com (172.217.160.110), 30 hops max, 60 byte packets
 1  gateway (140.112.30.254) [AS17716/AS17709]  2.225 ms  2.958 ms  3.519 ms
 2  140.112.149.121 (140.112.149.121) [AS17716/AS17709]  0.702 ms  0.643 ms  0.700 ms
 3  140.112.0.214 (140.112.0.214) [AS17716/AS17709]  0.458 ms  0.384 ms  0.326 ms
 4  140.112.0.206 (140.112.0.206) [AS17716/AS17709]  1.742 ms  1.686 ms  1.418 ms
 5  140.112.0.34 (140.112.0.34) [AS17716/AS17709]  1.557 ms  1.493 ms  1.442 ms
 6  72.14.196.229 (72.14.196.229) [AS15169]  2.946 ms  2.402 ms  2.332 ms
 7  108.170.244.97 (108.170.244.97) [AS15169]  2.224 ms  2.153 ms  2.332 ms
 8  216.239.48.135 (216.239.48.135) [AS15169]  2.759 ms  6.587 ms  6.527 ms
 9  tsa03s06-in-f14.1e100.net (172.217.160.110) [AS15169]  2.407 ms  2.348 ms  2.474 ms
```

*** ref.**

- `man traceroute`

3. `$ ip link show`

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 52:54:00:55:64:3e brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 52:54:00:43:3f:d5 brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 52:54:00:f6:e6:eb brd ff:ff:ff:ff:ff:ff
6: eth0.30@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode DEFAULT group default qlen 1000
    link/ether 52:54:00:55:64:3e brd ff:ff:ff:ff:ff:ff
```

*** ref.**

- `UNIX and Linux System Administration Handbook 5th edition, Chapter 13, Linux Networking (p.417)`