Computer Network Laboratory Lab 1

- Computer networking is built on **Open Systems Interconnection (OSI) Reference Model**, including **physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer**. **IP addressing** protocol lies in the network layer.
- **IP datagram** is heavily overheaded, with 20 bytes of IP metadata, and anthoer 20 bytes of TCP metadata, just in order to send or receive a small datagram packet.
- **IP address** is a 32-bit identifier for each interface of a host/router. **Interface** is the connection between the host/router and physical links. Routers typically have multiple interfaces, whereas a host typically has only one interface. Here is an example: 223.1.1.1 = 11011111.00000001.00000001.00000001.
- An IP address has 2 parts: the first n bits are the **subnet part**, and the last 32-n bits are the **host part**. The n (and its corresponding **subnet mask**) is determined by **CIDR (Classless InterDomain Routing) notation**, and denoted by "/n", e.g. 223.1.3.0/24 and its subnet mask 255.255.255.0.
- A **subnet** is a collection of device interfaces with same subnet part of IP address, e.g. 223.1.3.27/24, 223.1.3.1/24, and 223.1.3.2/24.
- The number of available IP addresses under 32-bit protocol cannot accommodate the growing number of machines in the world. Therefore, several techniques are proposed to get around this problem. Two of them are **DHCP** and **NAT**.
- **DHCP (Dynamic Host Configuration Protocol)** allows a host to dynamically obtain its IP address from the DHCP router when it joins the network. Several properties of this protocol are as follows:
    - When a device is shut down or idle, IP address will be released for reuse by other machines.
    - DHCP assumes that the devices within the network would never be connected to the network all at once.
    - A device is not able to connect the internet if all IP addresses are used up.
    - A device using a DHCP address can never become a server because a server should be always on a fixed IP address.
- There are four steps for a DHCP router to authorize an IP address to its DHCP clients: **discover**, **offer**, **request**, and **ack**. Worth noticing is that DHCP discover and offer have the same transaction ID, and that DHCP request and ack have the same transaction ID.
- **NAT (Network Address Translation)** is a method of remapping one IP address space into another. It has several properties:
    - All datagrams leaving local network have same single source NAT IP address, also called the

WAN-side address.
    - Local network uses IP addresses that are meaningful within the local network, also called the **LAN**-side address.
    - A NAT router can change addresses of devices in the local network without notifying the outside world.
    - Devices inside the local network are not explicitly addressable, or visible by the outside world (*a security plus*).
- A NAT router must implement the following steps:
    - Replace the *source* LAN-side address(and port#) of every outgoing datagram.
    - Remember the mapping of the LAN-side address(and port#) to the WAN-side address(and port#).
    - Replace the *destination* WAN-side address(and port#) of every incoming datagram.
- Port# is a *16-bit* number, meaning that a NAT router is able to provide up to 65536 LAN-side addresses.
- NAT is controversial in that:
    - Routers should only process up to layer 3, i.e. network layer.
    - NAT violates end-to-end communication.
    - Address shortage should instead be solved by IPv6.
- NAT traversal problem can be solved by:
    - statically configure NAT to forward incoming connection requests at given port to server
    - Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol
    - relaying (used in Skype)
- Network security contains 4 components: *confidentiality*, *authentication*, *message integrity*, *access and availability*.
- An intruder can potentially perform **eavesdropping**, *modification* of message, **impersonation/spoofing**, **hijacking**, **denial of service**, etc.
- A **firewall** isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.
- Three types of firewalls are **stateless packet filters**, **statefull packet filters**, and **application gateways**.
- **Access control list (ACL)** is a table of rules to decide whether to accept or reject a packet.
- There is always a tradeoff between the *degree of communication with outside world* and the *level of security*.