CS 455 – Computer Security Fundamentals

Dr. Chen-Yeou (Charles) Yu

- A mild introduction to computer networks
  - IPv4
    - Subnetting and CIDR
  - IPv6 (will be covered in the next time)

A mild introduction to computer networks

- Before you grow into a computer security specialist, there are a couple of things you might need to know.
- When, you use some tools / software in doing security-related testing, most of the time, it is related with networking.
- You need to read the outputs from the software
- No matter it is the internet or intranet, we need to at least understand the computer networks, even though it is the most fundamental know-how.

A mild introduction to computer networks

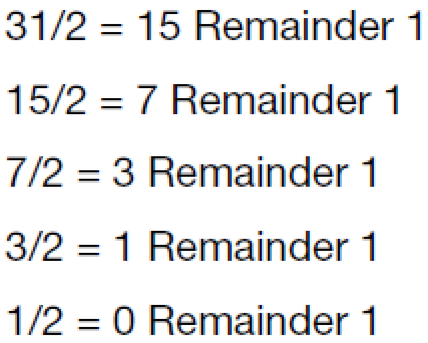
- With tens of thousands of networks and millions of individual computers communicating and sending data, we need to ensure the data packets go to the correct computer. It is like a postman need to a correct address. Otherwise, he was unable to deliver the mails.
- In the network communications, this address is a special one, referred to as an “IP” address. The IP addresses in the practices now can be IPv4 or IPv6

IPv4

- An *IP address* is a series of four values, separated by periods. (An example would be 107.22.98.198)
- For each of the three-digit numbers, they must be between 0 and 255
- So, an address of 107.22.98.466 would not be a valid one.
- Each of these numbers is really just a decimal representation of 8 bits
- Since it is 8 bits for each of the number, the range would be like this:
    - 0~255. 0~255. 0~255. 0~255
    - Or you can say it is a 8 x 4 = 32 bits representation
    - So, 107.22.98.198 is 8 bits + 8 bits + 8 bits + 8 bits
- In the "good old days", the beginning of the internet, this is amazing! We have about 4.2 billion addresses to assign to computers / servers.

IPv4

- However, the “good old days” is not lasting long --- it is used up quickly!
- Here is an example to convert the decimal to binary.



31/2 = 15 Remainder 1

15/2 = 7 Remainder 1

7/2 = 3 Remainder 1

3/2 = 1 Remainder 1

1/2 = 0 Remainder 1

- But did you remember that we need to do some “padding” jobs, because it is 8 bits right? So it is not 11111. Instead, it is 00011111

IPv4

- Wait! You haven’t talk about the issue --- insufficient IP address!
- Yes! It is! But before we are introducing the solutions, we need to talk about the types of IP Addresses
    - Public
    - Private
- The public IP addresses are for computers discoverable in the Internet.
- Not two public IP addresses can be the same. It is like you wouldn’t like to confuse the postman by giving him multiple addresses. Then, he will have problem in the mail delivery

IPv4

- However, a private IP address, such as a computer in a company network (mostly), this guy only has to be unique in that network. (Because it is a private network, not open to the public (internet))
- In the US., from my observation, if an organization deploys a private network, they like to choose the one begins with “10”, such as 10.102.230.17
- So, in this world, if CompanyA has a 10.102.230.17, CompanyB might have the same one.
- Now we can talk about the way to get us out of the jam --- insufficient IP address

IPv4

- The 1st approach:
  - Dynamic Host Configuration Protocol (DHCP)
    - An ISP might purchase a pool of public IP addresses and assign them to you **when you log on**
    - For example, an ISP might own 1,000 public IP address and have 10,000 customers.
    - Because all 10,000 customers will not be online at the same time, the ISP simply assigns an IP address to a customer when this guy is online logs on, and the ISP unassigns the IP address when the customer logs off.
- Now, the 1st byte (1st decimal number) of the network address has a lot of secret. It tell you what class of network a machine belongs.

IPv4

- Here is the summary of classes. Note that, in this place, we only talk about the 1st byte (or the first 8 bits)

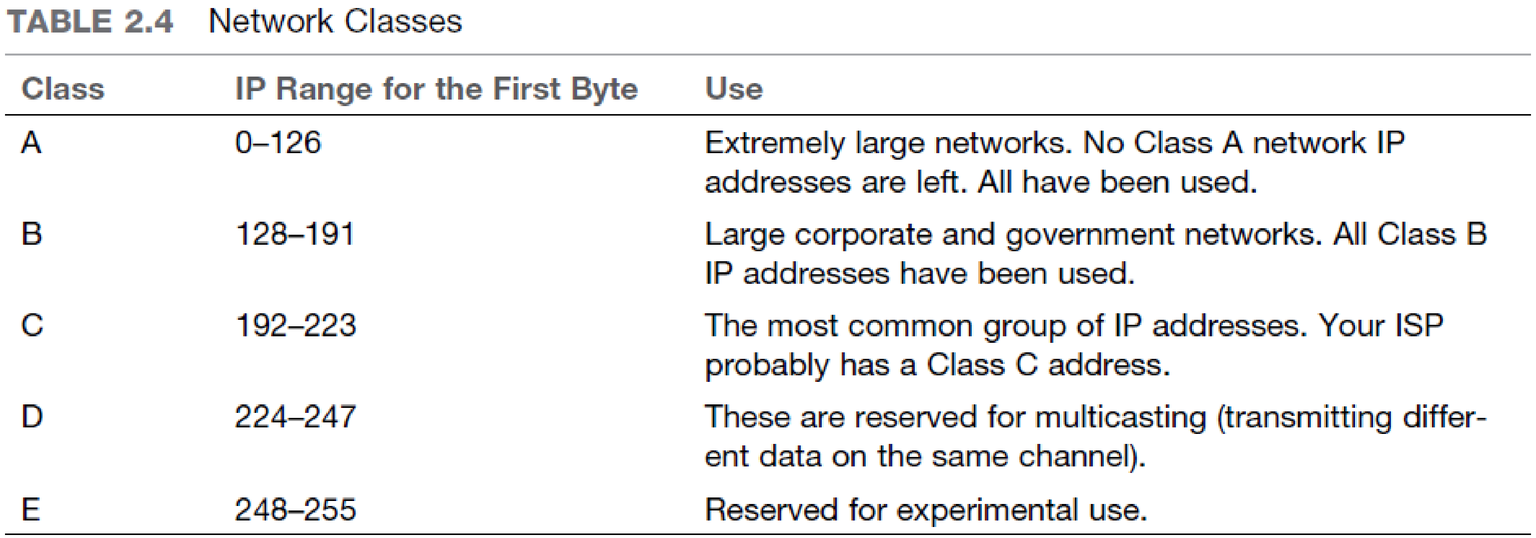


TABLE 2.4 Network Classes

Class	IP Range for the First Byte	Use
A	0–126	Extremely large networks. No Class A network IP addresses are left. All have been used.
B	128–191	Large corporate and government networks. All Class B IP addresses have been used.
C	192–223	The most common group of IP addresses. Your ISP probably has a Class C address.
D	224–247	These are reserved for multicasting (transmitting different data on the same channel).
E	248–255	Reserved for experimental use.

- What about our Truman? We have most of the machine begins with 150, right? Remember the slide about Dr. Alan’s machine?

IPv4

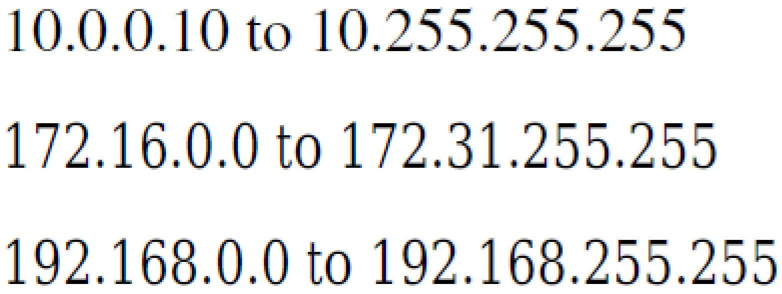
- Wait! Truman? Class B? Do we have so many machines? Of course not! This involves one technology called “Subnetting”. We only own a small portion of Class B ☺
- Imagine that there is a router, the job of this router is to perform network address translation (NAT). The router needs to have a public IP Address facing the public internet.
- A router, serves as a gatekeeper and he can manage a private network
- When, there is an outgoing packet from a machine hiding behind the private network. If router just get packet, it takes the private IP address on outgoing packets and replaces it with the public IP address of the that router. (but still keep the sender’s information)
- In this way, the packet can be routed through the Internet
- computer (in priv. net.) → router → some computer in the internet

IPv4

- All right, we know the outgoing packet, but what about the incoming packet?
- NAT! The router uses some table to check what are the machine I’m managing by doing a translation. So the packet can be correctly send to the destination from public internet to a machine hiding in the private network.
- computer (in priv. net.) ← router ← some computer in the internet
- This is the 2nd approach to handle insufficient IP Address issue: Private networks creation

IPv4

- Certain ranges of IP addresses have been reserved for use within networks
- These cannot be used as public IP addresses but can be used for internal workstations and servers, including



10.0.0.10 to 10.255.255.255

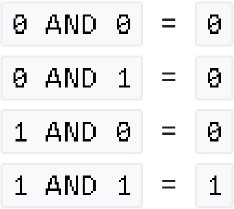
172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

- So, those are the addresses reserved for devices in the private networks.

Subnetting and CIDR

- The 3rd approach: Subnetting and CIDR
  - *Subnetting* is simply chopping up a network into smaller portions
  - For example, if you have a network using the IP address 192.168.1.X (x being whatever the address is for the specific computer), then you have allocated 255 possible IP addresses.
  - Subnetting uses the computation of “logical AND”



0 AND 0	=	0
0 AND 1	=	0
1 AND 0	=	0
1 AND 1	=	1

  - But how? Normally, if we do not want to have 255 addresses on 192.168.1.X, we need to cut that.

Subnetting and CIDR

- Subnetting is accomplished by using subnet mask
- The subnet mask is a 32-bit number that is used to divide the 32-bit binary IP address into network (You can say 4 octal numbers separated by dots)
- There are some rigid rules, we cannot just put in any number we want
    - The first value of a subnet mask must be 255
    - The remaining three values can be 255, 254, 252, 248, 240, or 224.
- Here are some examples:
    - If you have a Class A IP address, your subnet mask is 255.0.0.0
    - If you have a Class B IP address, then your subnet mask is 255.255.0.0
    - If you have a Class C IP address, then your network subnet mask is 255.255.255.0
- Now, if you want to have fewer than 255 nodes in your subnet, then you might need a subnet like 255.255.255.240

Subnetting and CIDR

- If you convert 240 to binary, it is 11110000
- So, the subnet mask is 11111111.11111111.11111111.11110000 (in our example)
- That means the first three octets and the first 4 bits of the last octet define the network.
- This means you could have as many as 1111 (in binary) or 15 (in decimal) nodes (machines) on this subnetwork
- The most important thing! The “AND” computation happens in the router!
- In this case, what if we have an incoming packet to the IP Address (computer) like this: 11111111.11111111.11111111.11110100, which equals 255.255.255. 244
- The router will firstly convert 255.255.255.240 (subnet mask)and 255.255.255. 244 into binary representations, respectively

Subnetting and CIDR

- After the AND is performed in the router, we will get:

11111111.11111111.11111111.11110000

11111111.11111111.11111111.11110100 (AND

11111111.11111111.11111111.11110000

- This means? The router knows, I am going to send this packet to 11111111.11111111.11111111.11110000 (this subnet)
- Because the router might be in charge of several subnets

Subnetting and CIDR

- CIDR is Classless Interdomain Routing
- Rather than defining a subnet mask, you have the IP address followed by a slash and a number.
- That number can be any number between 0 and 32. That means, for how many bits we use that for networking address?
- As you know, we can roughly say, an IP address is divided 2 parts: networking part + host address
- Networking part means, what is the network this device is in?

Subnetting and CIDR

- For example, 192.168.1.10/24 (basically a Class C IP address)
  - We have 8 bits left to freely allocate our machines so the range will be from:
  - 11000000. 10101000.00000001.00001010 (192.168.1.10), to
  - 11000000. 10101000.00000001.11111111 (192.168.1.255)
- Another example, 198.128.128.192/27
  - We have 5 bits (32-27=5) left to freely allocate our machines so the range will be from
  - 11000110. 10000000. 10000000. 11000000 (198.128.128.192), to
  - 11000110. 10000000. 10000000. 11011111 (198.128.128.223)
- CIDR is actually doing the subnetting job without relying on subnet masks which is commonly used today.