CS 455 – Computer Security Fundamentals

Dr. Chen-Yeou (Charles) Yu

- A mild introduction to computer networks
  - ~~IPv4~~
    - ~~Subnetting and CIDR~~
  - IPv6
    - The reason why we need to study the networking
  - SSID, BSSID, ESS (or ESSID)

The reason why we need to study the networking

- This is not about the IPv6 yet!
- In this class, we do not want to discuss the detail in the networking, because this is not the Computer Networks class
- We still need to know the most fundamentals of the networking.
- Before I'm explaining the reason why we need to study, there is a very EVIL tool called "**sniffer**":
  - Oh! What is it?
  - If someone in the "intranet" (it could be a device very close to you. Close means, the hops to router, not necessarily the physical distance), sending the packet to the "internet" (i.e. not encrypted password), you can use the sniffer to see this guys data easily.
  - How this kind of function or mechanism is implemented?

The reason why we need to study the networking

- For example, at least you guys need to know this, when you are using “sniffers”:
  - Our Ethernet card, it has **“Normal mode”** and **“Promiscuous mode”**
  - **Normal mode**
    - When, someone’s packet is sending through the Ethernet, our machine uses the **MAC address** information in the packet for comparison to check, if we need to **intercept** this Ethernet **frame** or not?
    - Normally (normal mode), the Ethernet card just discard the packet if it is found not belongs to me
  - **Promiscuous mode**
    - Ethernet card do not deal with **MAC address** information in the packet for receiver comparison. When the card gets everything, it will pass everything directly to the upper level. (OSI 7 layers, remember?). Usually, this mode is used by the router to do network monitoring, or when the time we are using sniffer software.

IPv6

- IPv6 is an extension of IPv4
- Even with the use of private IP addresses (in the private networks), we still run out of available IP addresses quickly
- IPv6 utilizes a 128-bit address (instead of 32), so there is no chance of running out of IP addresses in the foreseeable future
- IPv6 also utilizes a “hex numbering” method in order to avoid long addresses.
- IPv6’s format: 128 bits is divided by 16 bits into 8 blocks. For each of the “block” is 16 bits and is represented by 4 x “hex digits”

IPv6

- For example,
  - ABCD:0F01:2345:6789:ABCD:0F01:2345:0089
- There are some rules, very specific to IPv6
  - Sometimes, this is VERY confusing to the people who are the 1st time reviewing their specs
  - The prefix-zeros can be removed. In our previous example, it can be expressed as follows:
    - ABCD: F01:2345:6789:ABCD:F01:2345:89
  - But for each of the block, it needs to have at least one hex number. For example, 2001:0DB8:0000:0000:0008:0800:020C:417A, this address can be re-written as: 2001:DB8:0:0:8:800:20C:417A

IPv6

- In order to do some compressions, for some addresses, if they have a consecutive blocks are all filled by zeros, it can be compressed by "::"
  - For example, 2001:DB8:0:0:8:800:20C:417A, this address can be compressed as 2001:DB8::8:800:20C:417A
  - For example, FF01:0:0:0:0:0:0:101, this address can be compressed as FF01::101 ← This kind of compression is super aggressive!
  - 0:0:0:0:0:0:0:1, can be compressed as, ::1
  - 0:0:0:0:0:0:0:0, can be compressed as, ::
- The compression for "consecutive-zero" blocks into "::" can only be used ONE time!
  - For example, 2001:0db8:0000:0000:abcd:0000:0000:0234, this address can be compressed as 2001:db8 :: abcd:0000:0000: 234
  - For the rest of the consecutive 2 x 0000:0000 cannot get compressed anymore!

IPv6

- Supposedly, IPv6 has large enough pool of IP addresses
- IPv6 uses CIDR
- The “network portion” is “indicated” by a slash followed by the number of bits in the address that are assigned to the network portion.
- It is totally like IPv4’s style, but we need to remember that the IPv6 has 128 bits. So, it is like /48 or /64.
  - This means, the front 48 bits or 64 bits are used as the network portion. The rest of the length, 128-48 = 80 bits, or 128-64=64 bits can be used for host addresses

IPv6

- The “network portion” in IPv6 is the “prefix” part of the IPv6 address.
- For example, the part of the “prefix length” can be written as:

```
|--Prefix Length--||---Interface id---|
2001:0db8:0000:0000:abcd:0000:0000:0234
2001:db8::/64
```

- So, in this example, the Interface id part, I can only make use of the rest of 128 – 64 = 64 bits
- Like we said earlier, IPv6 uses CIDR. It doesn’t use mask

IPv6

- The loopback address for IPv6 is written as ::/128.
  - This would be different from 127.0.0.1 as our loopback in IPv4
- Basically, IPv6 and IPv4 are now “co-existing” in our current systems. IPv4 is there for over 20+ years and is really hard to be totally replaced in the near future.
- Tools? The tools we use are almost the same
- There is one more thing. IPv6 is a kind of spec, but is your OS supporting IPv6? Not necessarily!
- Windows 10 is supported by default. How about the Kali Linux?

IPv6

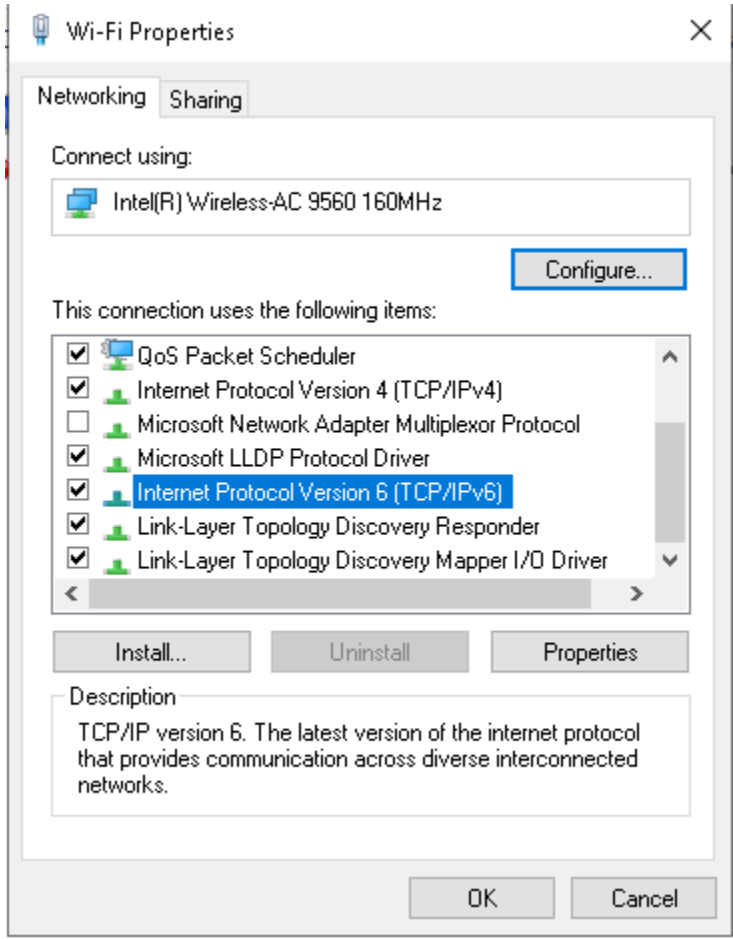
- The way to check if the IPv6 in Windows 10 is enabled:

Settings → Network and Internet →

Change Adapter Options →

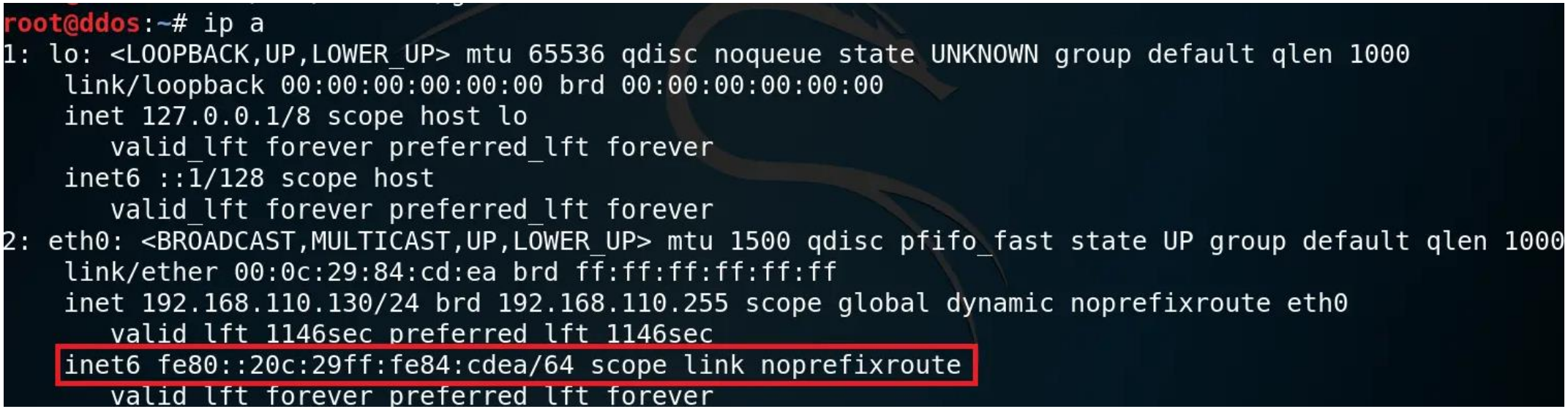
“right click” the WiFi Adapter → properties →

scroll down and see if this one is checked?



IPv6

- In Kali Linux (in the virtual machine), you can try this command and see if IPv6 is working?
- In my screen it is working by default



IPv6

- Sometimes, for the very special purpose, we need to disable / enable the IPv6 in the Kali, how to do that?
- Disable IPv6:
  - Temporarily

```
sysctl -w net.ipv6.conf.all.disable_ipv6=1
sysctl -w net.ipv6.conf.default.disable_ipv6=1
sysctl -w net.ipv6.conf.lo.disable_ipv6=1
```

  - Permanently

```
echo "net.ipv6.conf.all.disable_ipv6=1" >> /etc/sysctl.conf
echo "net.ipv6.conf.default.disable_ipv6=1" >> /etc/sysctl.conf
echo "net.ipv6.conf.lo.disable_ipv6=1" >> /etc/sysctl.conf
```

IPv6

- Enable IPv6
  - Temporarily

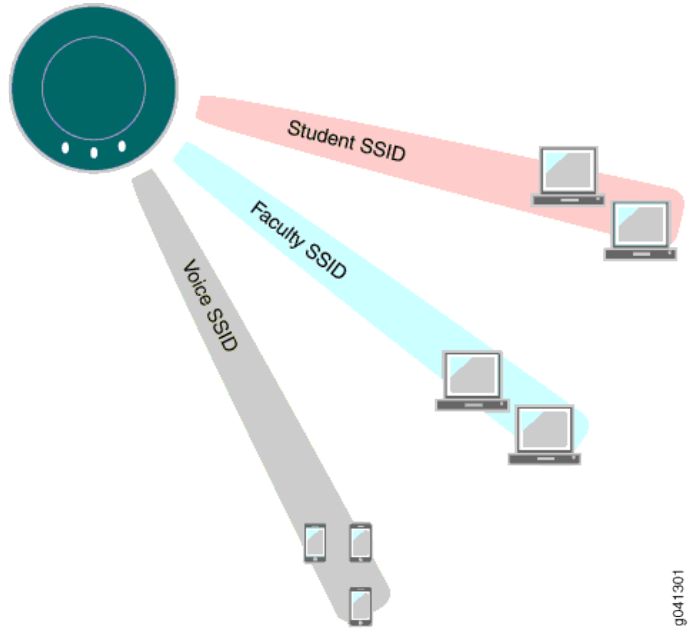
```
sysctl -w net.ipv6.conf.all.disable_ipv6=0
sysctl -w net.ipv6.conf.default.disable_ipv6=0
```

  - Permanently
    - Do the same thing, use the “echo” command to put the string appended to the bottom of the /etc/sysctl.conf
    - Similarly, we can set the 3 different “parameters” to disable the IPv6 to 1

```
echo "net.ipv6.conf.all.disable_ipv6=1" >> /etc/sysctl.conf
echo "net.ipv6.conf.default.disable_ipv6=1" >> /etc/sysctl.conf
echo "net.ipv6.conf.lo.disable_ipv6=1" >> /etc/sysctl.conf
```

SSID, BSSID, ESS (or ESSID)

- Still remember the video talking about hacking into the Wifi AP?
- Some of terminologies you need to know!
- SSID are just the “names” of network.
- For example, in this AP (Access Point), we configured 3 names
  - Student
    - Less restrictions on some websites
  - Faculty
    - Better protection in security controls
    - More restrictions on some websites
  - Voice
    - Possibly for the meeting rooms

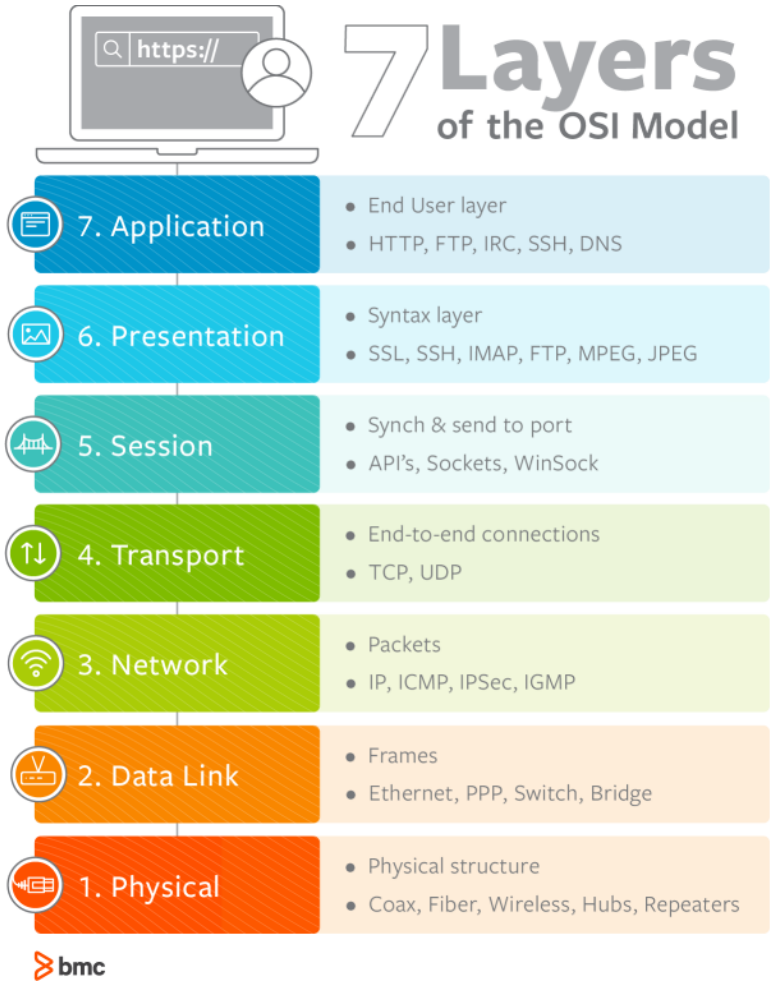


SSID, BSSID, ESS (or ESSID)

- In this way, you might not have access to all SSIDs—the authentication and access privileges are usually different for different WLANs and their associated SSIDs.
- If a Faculty tried to connect to a “Student” SSID by typing its user name and password, it might not working.

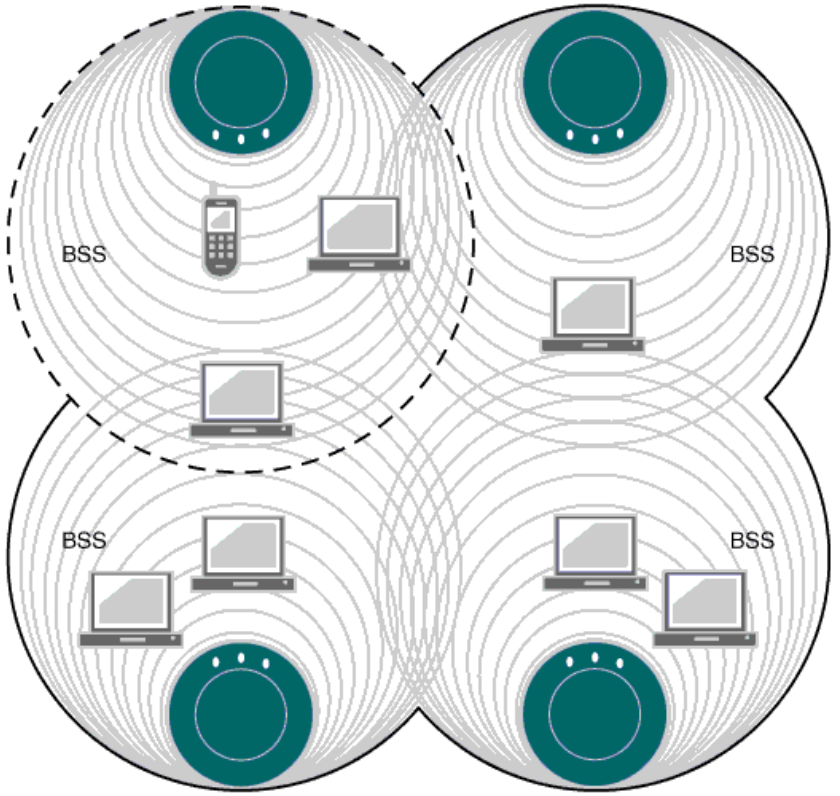
SSID, BSSID, ESS (or ESSID)

- BSSID (basic service set identifier) is the Layer 2, MAC address of an AP, provided by the hardware manufacturer.
- So, for example, the “Student” SSID represents the “logical” network around the campus but it could be composed of so many hardware --- APs



SSID, BSSID, ESS (or ESSID)

- In this example, there are 4 APs (4 WiFi base stations).
- Totally, 4 BSSID (MAC) and 1 SSID (“logical” network name)
- When you are moving your laptop around the rooms or buildings, you might not feel anything different
- But the network administrator might be interested to keep monitoring the network loadings, or try to pinpoint the trouble making APs, or even a single host



SSID, BSSID, ESS (or ESSID)

- In this example, 1 SSID for 4 x BSSID
- SSID is widely used
- But sometimes, ESS (extended basic service set) is used from network administrator's perspective
- However, SSID is more commonly used, since they are the same thing.
- SSID is more like the end-user's perspective.