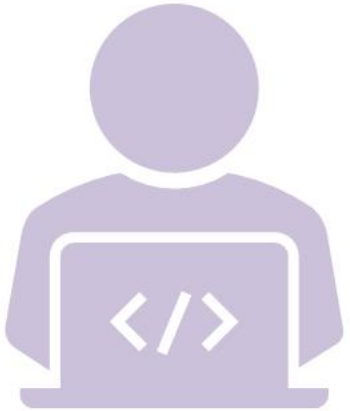
[CISCO Networking] part 10, 11

[GBC20190027] Network

Agenda

- Part 10. 세상은 넓고 네트워킹은 계속된다
- Part 11. 선이 없는 세상, 무선으로의 여행



10-1. WAN은 어렵다?

1. WAN(Wide Area Network)이란?

- LAN과 LAN을 연결하는, 서로 멀리 떨어진 지역의 네트워크 연결
- 내가 직접 네트워크 케이블을 깔아서 통신을 연결할 수 없을 때 사용하는 네트워킹 방식

2. WAN의 방법

1) 전용선 방식

- 전화국과 같은 통신사업자에게 통신회선 임대 받아서 쓰는 방식

  ex) 서울에서 부산까지 통신을 해야 한다면 통신사업자가 서울에서 부산까지 이미 설치해 놓은 회선 중 하나를 우리는 돈을 내고 대여해서 쓰는 것

- 보안에 큰 신경 쓸 필요 없지만, 비용이 많이 든다는 단점

2) 회선 스위칭 방식

- 내가 통신을 하는 순간에만 나에게 필요한 회선을 열어주고 통신이 끝나면 회수하는 방식
- 서킷 스위칭 방식 : 통신하는 순간에만 나에게 회선을 쓸 수 있게 해주는 방식 (ex. 전화)

3) 패킷 스위칭 방식

- 패킷 하나하나가 나누어서 통신회선을 타고 목적지까지 전달되는 방식
- 통신회선을 다른 사람들과 나눠서 쓰는 방식 (통신회선 전체를 다 빌려주는 것이 아님)
- 내가 가진 회선이 없지만 마치 내가 목적지까지의 회선을 가지고 있고, 데이터를 그 회선을 통해 전달하는 것처럼 동작하도록 해주어야 함 → virtual circuit

11-1. 무선으로의 여행

1. AP (Access Point)

- 무선과 유선을 서로 연결해주는 역할

2. CSMA/CA(Carrier Sense Multiple Access / Collision Avoidance)

- 무선랜의 통신 방식
- 이더넷의 CSMA/CD와 같이 전송 전에 미리 Carrier를 Sense해서 현재 통신이 일어나고 있는지 확인하고, 통신이 없으면 아무나 보낼 수 있는 것
- 이더넷은 Collision Detection인 반면 무선은 CA

3. 데이터를 보내는 방식

1) Listen Air Space(radio wave) : 현재 통신이 일어나고 있는지 살핀다
2) Set random wait timer before sending frame : 랜덤한 시간 동안 기다린다
3) After timer has passed, listen again and send : 랜덤한 시간이 지나고, 다시 한 번 통신이 일어나고 있는지 살핀 후 프레임 전송
4) Wait for an Ack : 무선 통신의 경우 보낸 데이터가 잘 도착했는지 알 수 없으므로, 보내고 나서 잘 받았다는 신호(ACK)를 기다리게 됨
5) If no Ack, resend the frame : 정해진 시간 동안 ACK를 받지 못하면, 전송 실패 한 것으로 생각하고 1)번으로 돌아가 전송 재시도

11-2. 무선 랜에서 두 가지 중요한 모드

1. Ad Hoc 모드

- '특별한' 또는 '임시변통의'라는 의미로 해석됨
- 앞에서 무선 네트워킹에 꼭 필요하다는 AP를 사용하지 않고, PC에 무선 랜 카드만을 꽂아서 임시변통으로 통신하는 방식

2. Infrastructure 모드

- AP를 사용해서 무선 통신이 일어남
- 무선 랜 카드가 장착된 PC는 데이터를 AP에 전달하고, AP가 이 데이터를 상대방 PC에 전달해주는 방식

1) BSS(Basic Service Set) : AP 1대를 이용해서 무선 랜을 구성하는 방식
2) ESS(Extended Service Set) : AP 여러 대를 이용해서 무선 랜을 구성하는 방식

→ ESS와 같이 AP 여러 대를 사용해서 무선 랜을 구성하는 이유 :
무선 랜을 구성하는 지역이 AP 한대로 커버되지 않는 넓은 지역이거나
접속하는 무선 장비들이 AP 한대로 커버하기에 용량이 부족할 경우

3) IBSS(Independent BSS) : Ad Hoc 모드에서 제공되는 Service Set

11-3. 무선 랜의 통신 표준

1. 무선 랜에서 사용되는 표준 통신 방식

무선 표준	IEEE802.11b	IEEE802.11g	IEEE802.11a
승인 연도	1999	2003	1999
최대 속도	11Mbps	54Mbps	54Mbps
지원 속도	1, 2, 5.5, 11Mbps	6, 9, 12, 18, 24, 36, 48, 54Mbps	6, 9, 12, 18, 24, 36, 48, 54Mbps
사용 주파수	2.4GHz	2.4GHz	5GHz
지원채널	11채널(한국 13)	11채널(한국 13)	23채널(한국 19)
비중첩 채널	3채널	3채널	23채널(한국 19)

→ 최대 속도와 지원 속도로 나눈 이유 : AP로부터 가까울 때는 최대 속도를 사용하다가 멀어지게 되면 속도를 낮추면서 계속 통신이 되도록 하기 위해, 여러 가지 속도 지원

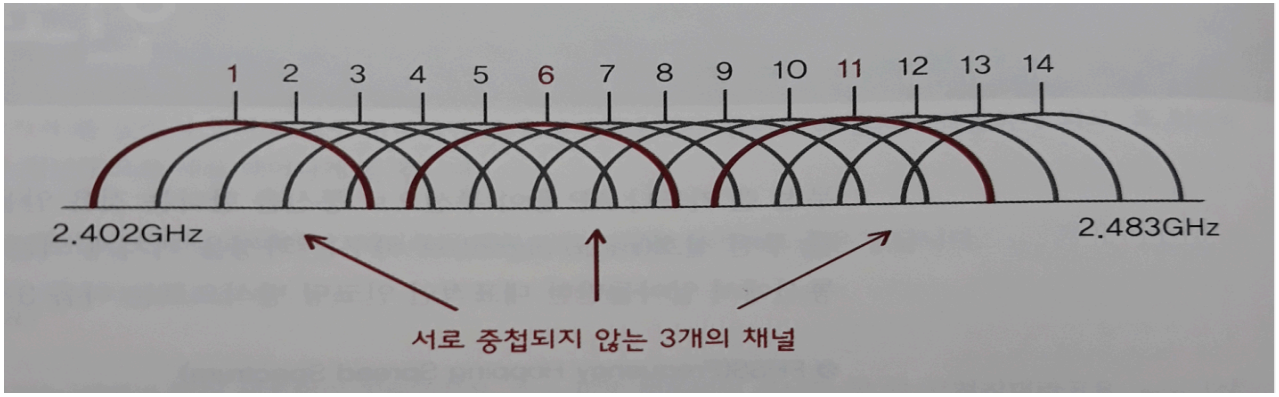
11-4. 무선 통신에서의 인코딩 3가지

1. FHSS

- 주파수 호핑 확산 스펙트럼 방식
- 무선 신호를 많은 주파수 채널로 빠르게 바꿔가면서 전송하는 방식
- 잡음과 간섭 같은 통신 문제에 강점
- 802.11a방식

2. DSSS

- 여러 개의 채널 중에서 하나를 잡고 계속 그 채널로만 전송을 하는 방식
- 신호를 매우 작은 전력으로 넓은 대역으로 전송하기 때문에 잡음 영향 적고, 보안 우수
- IEEE802.11b 무선 통신에서 사용하는 인코딩 방식 → 2.4GHz 대역에서 사용
- ESS 구성을 할 때, 비중첩 채널 이용 (같은 채널 쓰는 AP 2대 놓으면, 이 두 대의 AP에서 나오는 주파수는 충돌 발생 → 비중첩 채널 사용 | 전파 충돌X , 동시에 통신 가능)



11-4. 무선 통신에서의 인코딩 3가지

3. OFDM

- 주파수 분할 다중 방식은 하나의 시그널을 여러 개의 주파수로 나누어 보내는 방식
- 직교가 붙어있는 의미 | 전파에서 직교성을 이용하면 주파수가 서로 겹쳐도 간섭이 일어나지 않아 좀 더 많은 주파수 분할 가능
- IEEE802.11a와 802.11g

11-5. 무선 네트워크 _ SSID

1. SSID (Service Set Identifier)

- 무선 네트워크에서 사용하는 이름
- 길이는 32바이트로 구성, 같은 무선 네트워크 안에 있는 무선 장비들은 모두 같은 SSID
- 어떤 무선 장비가 현재 무선 네트워크의 SSID를 제대로 갖고 있지 않다면 , 이 무선 네트워크에 연결될 수 없게 됨
- SSID는 디폴트로 100ms마다 브로드캐스트 되는 모드지만, disable 해줄 수도 있는데, 이것을 SSID cloaking이라 함 → cloaking되면 무선 네트워크 보기에서는 보이지 않으며, 수동으로 SSID 직접 입력해주어야 접속 가능해짐

11-6. 무선 네트워크 _ 보안

1. 인증 (Authentication)
- 어딘가에 접속하고 할 때 이 장비에게 접속을 허가할 건지 아닌지를 결정하는 것

2. 암호화 (Encryption)
- 접속이 된 다음 서로 간에 데이터를 주고받는 과정에서 누가 훔쳐보는 걸 방지하기 위해 데이터 자체를 암호화하는 것 의미

3. WEP (Wired Equivalent Privacy)
- 맨 처음 무선 네트워크에 사용된 보안 표준
- 무선 네트워크에 접속하려고 하는 클라이언트 장비와 액세스 포인트가 같은 key값을 나눠 가지고 있다가 접속이 시도되면 key값을 확인해, 접속 허락하는 방식.

4. 802.1X 사용자 인증 방식
- username과 password 입력하고, 맞아야 접속 허락

5. WPA
- 802.1X 사용자 보안 도입 | static + Dynamic 키 분배 방식 | TKIP 사용
- 기존 wep암호화를 보완한 암호화 기법 사용했으나 표준은 X

6. 802.lli / WPA2
- 표준 | TKIP보다 강화된 암호화 방식 AES