실무 네트워크 Design - 8 : LAN design model(3가지) 분석

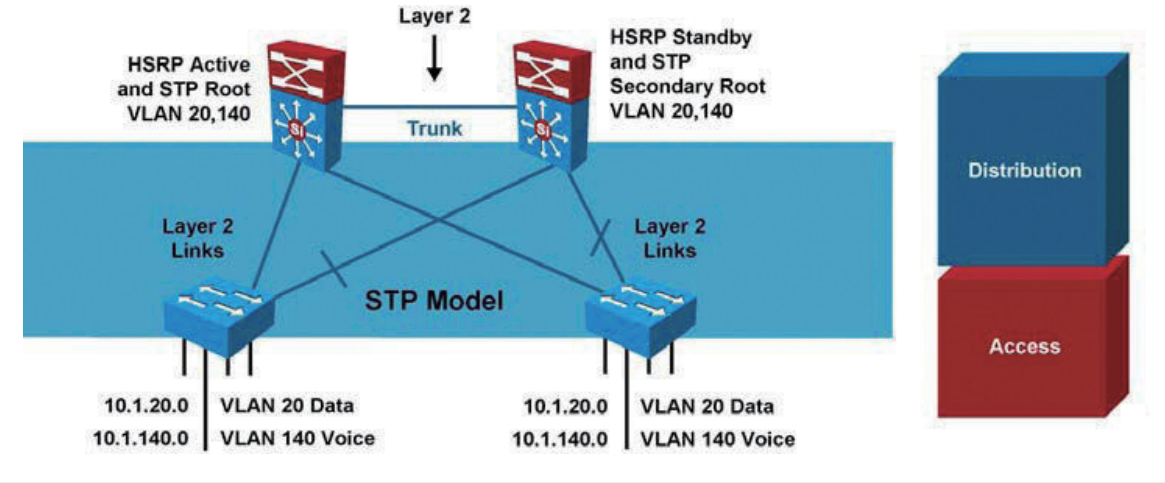
김해중 KBS 보도기술국

이번 시간에는 대표적인 네트워크 기업인 cisco에서 권장하는, LAN design model 3종류를 설명하고자 합니다. 사실 네트워크에 대한 원리를 잘 모르더라도, 3개의 모델과 똑같이 구축한다면 큰 문제없이 동작합니다. 수많은 네트워크 관리자들이 많은 시행착오를 거쳐서, 오랜 시간 동안 검증된 모델이기 때문입니다. 그래서 국내의 많은 회사들도 거의 이 3개의 모델을 바탕으로 해서 LAN을 구축합니다.

1st (End to End VLAN Design)

먼저 end to end vlan을 복습해볼까요? end to end vlan은, 위치와 무관하게 업무별로 vlan을 할당하는 방식입니다. [그림 1]을 통해 end to end vlan 구조를 확인해 보겠습니다. data 전송용도인 vlan(20)이 두 군데의 access switch에 분산되어 있으며, voice vlan(140)도 두 군데 access switch에 분산되어 있습니다. voice vlan은 지난 시간에 배웠듯이, IP 전화기에 대한 traffic을 구분하기 위해 사용하는 vlan입니다.

end to end vlan을 design 할 때, 고려해야 할 중요한 몇 가지를 아래에 정리해 보도록 하겠습니다.



[그림 1]

① Distribution switch가 STP의 root 역할을 하는 것을 권장합니다

Distribution switch가 STP의 root switch 역할을 할 때, traffic이 가장 자연스럽게 전송이 됩니다. 또 다른 이유로는 distribution switch가 access switch보다 안전성이 보장된 고가의 장비라, 중요 역할인 STP의 root switch 역할을 맡습니다. [그림 1]을 보면 좌

김해중
KBS 보도기술국

측 distribution switch가 STP의 root 역할을 하고 있음을 알 수 있습니다. 그리고 root switch 역할을 하지 않는, 우측 distribution switch는 secondary root 역할을 합니다. 만약 root switch의 장애 발생 시, secondary root 역할을 하는 switch가 root switch 역할을 대체합니다.

② RSTP 사용을 권장합니다

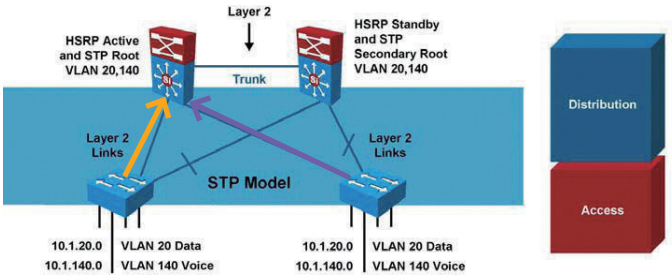
STP는 장애 발생 후 복구하는데 30~50초가 걸리지만, RSTP는 장애발생 후 1~2초 이내로 빠른 장애 복구가 가능해, 반드시 RSTP를 사용해야 합니다. 모든 access, distribution switch는 RSTP로 동작시켜야 합니다. 참고로 juniper, cisco 장비를 혼합해서 사용하는 환경이라면, spanning-tree의 path-cost 기준을 맞추어야 합니다. cisco는 short path-cost를 사용하고, juniper는 표준인 long path-cost를 사용하기 때문입니다.

③ Distribution switch 장애를 대비해 FHRP를 사용해야 합니다

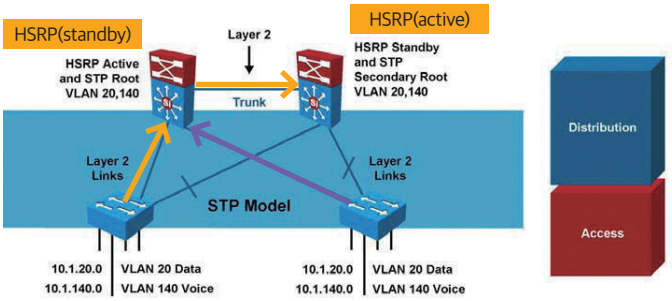
FHRP(VRRP, HSRP)를 사용하면, active 역할을 하는 distribution switch에 장애 발생 시, 각 PC는 세팅변경 없이 통신을 지속할 수 있습니다. cisco 제품만을 사용하는 환경이면 HSRP를 권장하며, cisco와 Juniper 등의 장비가 혼합된 환경이라면 표준인 VRRP를 사용해야 합니다.

자연스러운 traffic 흐름을 위해, STP의 root switch가 FHRP의 active 역할을 하는 것을 권장하며, 그때의 traffic 흐름은 [그림 2(a)]와 같습니다. [그림 2(b)]는 STP root switch가 HSRP의 active가 아닌 standby switch 역할을 하는 디자인입니다. 이때 외부로 나가는 모든 traffic은 STP root switch를 경유해서 HSRP(active)로 가게 됩니다. 즉 장비 1개를 더 통과하는 현상이(총 2hop) 문제점으로 발생합니다.

(a) 권장 design



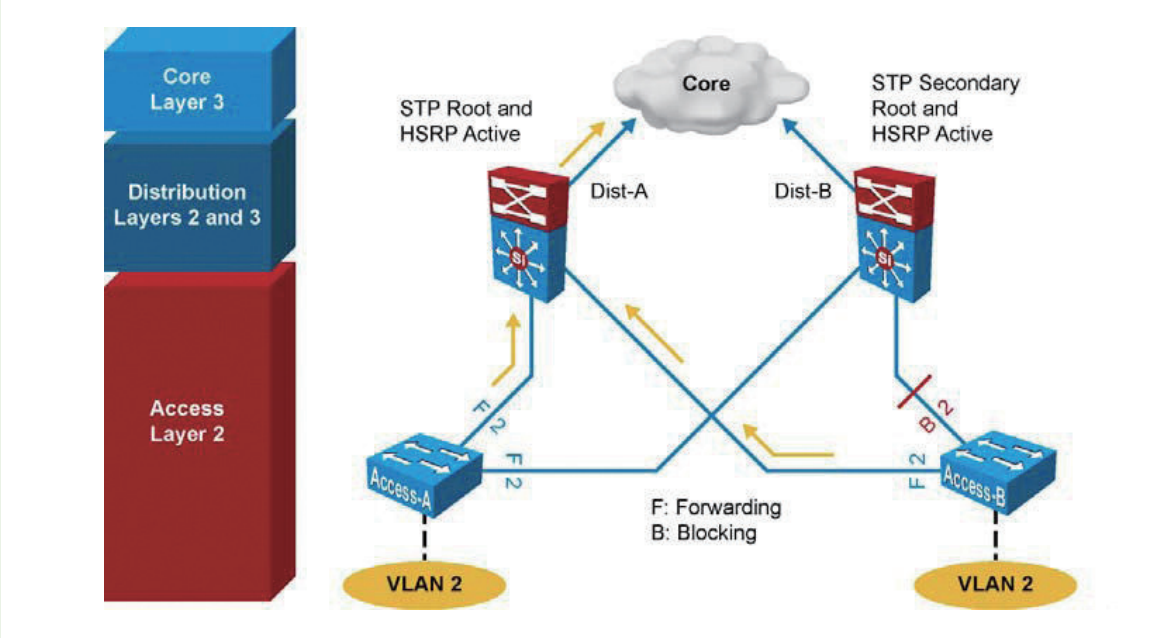
(b) 권장하지 않는 design



[그림 2]

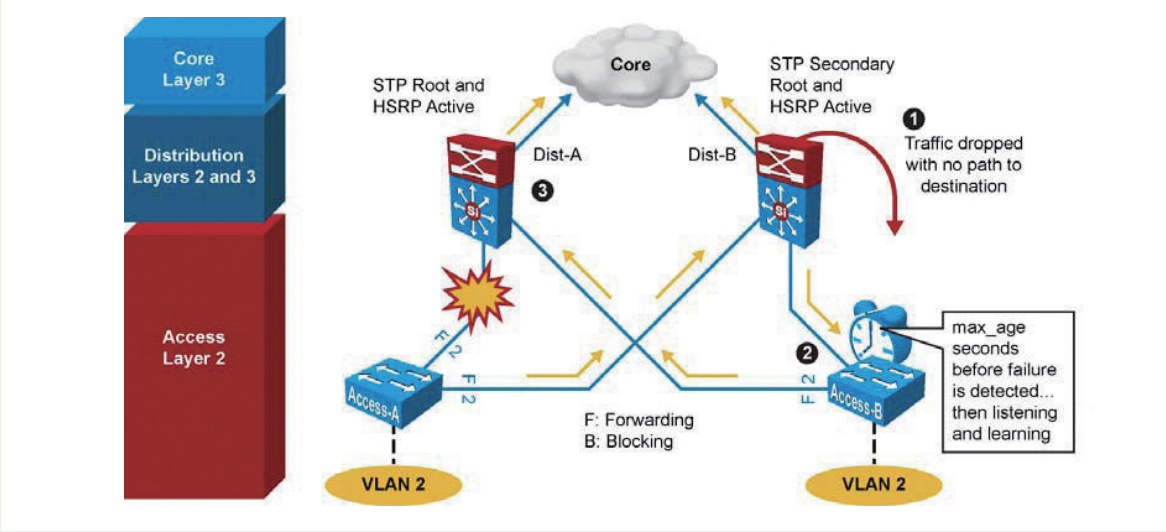
④ Distribution switch 간은 L2 trunk로 연결하는 것을 권장합니다.

distribution switch 간에 연결된 L2 link가 없을 때는, [그림 3]처럼 HSRP/VRRP의 hello 패킷이 access switch를 경유하게 됩니다. 예비 L2 link가 있다면, 그 link를 통해서 직접 HSRP/VRRP의 hello 패킷을 주고받으면 되는데, 예비 link가 없어서 우회하게 되는 문제점이 발생합니다.



[그림 3] 평상 시 backup L2경로가 없을 때(HSRP의 hello 패킷이 access switch를 경유하게 됩니다)

장애 발생 시, backup L2 link가 없다면 중요한 문제점이 발생합니다. [그림 4]처럼 좌측 access switch에서 좌측 distribution switch로 가는 uplink가 장애가 발생했다고 가정해 보겠습니다.



[그림 4] 장애 발생 시 backup L2 경로가 없을 때(일정시간 동안 모든 traffic이 단절된다)>

uplink 장애로 인해 distribution switch 간에는 FHRP(HSRP, VRRP) hello 패킷교환이 안 됩니다. 그래서 standby 역할인 우측의 distribution switch는 "좌측 distribution switch에 장애가 발생했구나"라고 생각해, 자신이 FHRP의 active 역할을 하게 됩니다. 이 때 active 역할을 가져오기까지는 traffic drop 현상이 발생합니다.

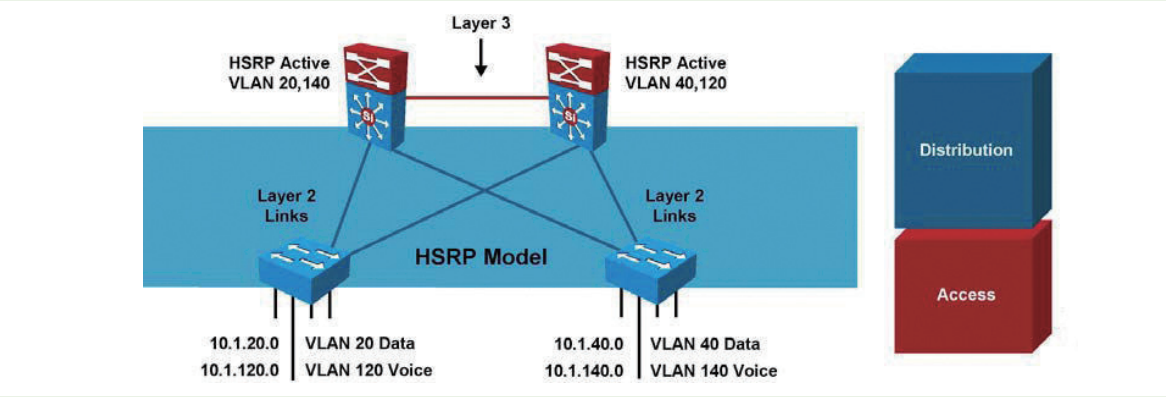
그리고 STP는 link 장애가 발생했기에, 기존에 block한 port를 사용하게 됩니다. 그러다 보니 기존 block link(우측, access switch와 우측 distribution switch 간의 link)를 active 상태로 만듭니다. 이 link가 active 되자마자 다시 FHRP의 hello 패킷이 흐르게 됩니다. 그러면 다시 좌측 distribution switch가 FHRP의 active 역할을 다시 가져오게 됩니다. 이 순간 traffic drop 현상이 또 발생합니다.

김해중
KBS 보도기술국

최종적으로 traffic 흐름을 보면, 좌측 access switch가 보낸 traffic이 우측 distribution switch를 통과하고, 다시 우측 access switch를 통과해서, 다시 좌측 distribution switch로 갑니다. 즉 traffic이 8자 모양으로 모든 switch를 경유하는 문제점이 발생합니다.
설명이 너무 복잡하죠? 저도 처음에 공부할 때는 잘 이해가 안 되었습니다^^. 하지만 실제 구축할 때는 distribution switch 간에 cable 1가닥만 layer 2 trunk로 서로 연결하면 모든 문제가 해결됩니다. 예비 link에 대한 중요성을 설명하기 위해 복잡하게 설명해 드렸습니다.

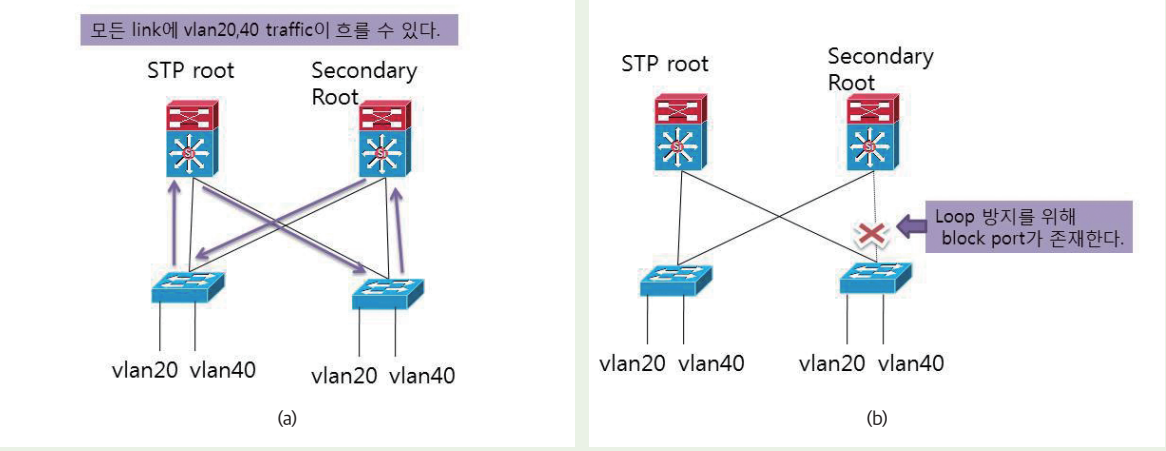
2nd (Local VLAN Design)

이번에는 local vlan을 복습해볼까요? local vlan은 업무와 무관하게, 위치별로 vlan을 할당하는 방식입니다. [그림 5]를 통해 local vlan 구조를 확인할 수 있습니다. end to end vlan과 다르게, vlan20은 좌측 access switch에만 존재하고, vlan40은 우측 access switch에만 존재함을 알 수 있습니다.



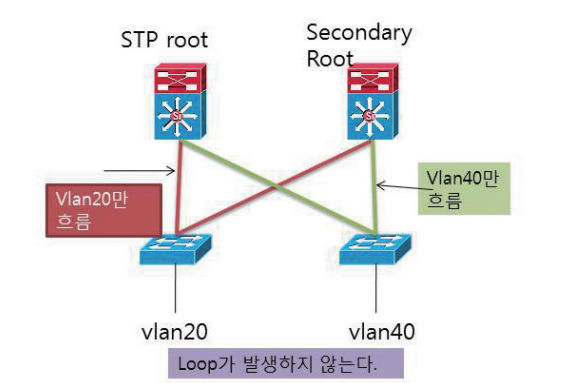
[그림 5] Local VLAN design

end to end vlan에 설명한 대부분의 내용이, local vlan에 적용하면 되기에, 차이점에 대해서만 간단히 설명을 하도록 하겠습니다. end to end vlan에서는 [그림 6(a)]처럼 모든 link에 vlan20, 40의 traffic이 존재하기에 loop 현상이 발생할 수 있습니다. 그래서 [그림 6(b)]처럼 STP가 동작해서 block port를 만듭니다.

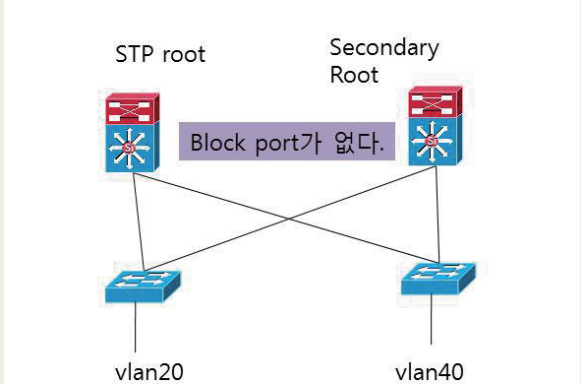


[그림 6] end to end vlan에서는 loop현상이 발생할 수 있기에 block port가 존재한다

그러나 local vlan을 [그림 7(a)]처럼 구현했을 때는, loop 현상이 발생하지 않기에, [그림 7(b)]처럼 block port가 존재하지 않습니다. 이때 cabling이 U자 모양으로 되어 있어, U design이라고 하며, STP 없이도 잘 동작해, NO-STP design이라고도 합니다. 하지만 관리자가 실수로 잘못된 config를 입력하거나, cabling 실수가 발생할 수 있어, 반드시 RSTP를 예비로 동작시킵니다.



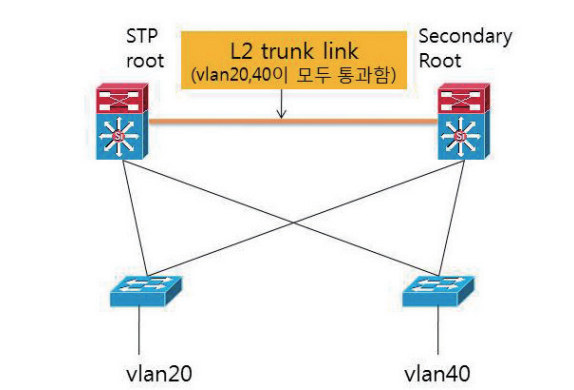
(a) U-design(NO-STP)



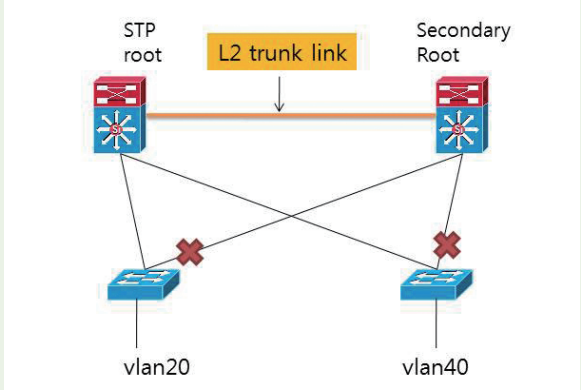
(b) block port가 존재하지 않는다

[그림 7]

이때 [그림 8(a)]처럼 local vlan에서 distribution switch 간에 Layer2 trunk를 예비로 구현하면, trunk에는 vlan 20, 40의 traffic이 모두 흐를 수 있기에 loop가 발생합니다. 그래서 [그림 8(b)]처럼 반드시 RSTP를 동작시켜 특정 port를 block 해야 합니다. 사실 [그림 8(b)]의 표현은 cisco에서 권장하지는 않지만, 현업에서는 가장 많이 사용되고 있습니다. 이렇게 설계를 하면, end to end vlan과 논리적인 구조가 거의 같아집니다.

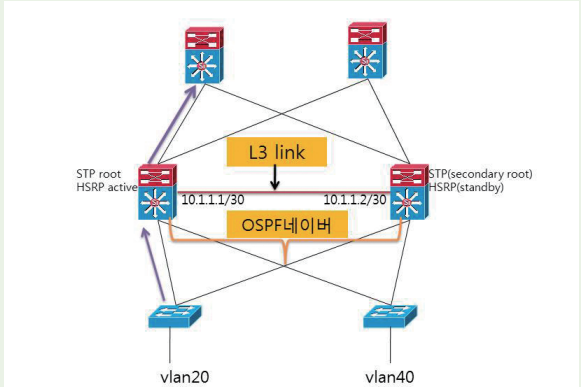


(a) L2 trunk로 예비 link를 구현했다

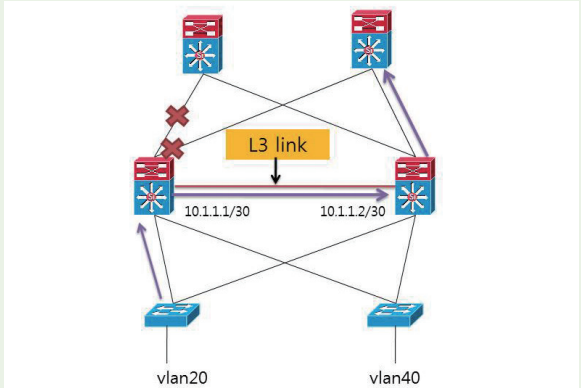


(b) loop 방지를 위해, block port가 있다

[그림 8] distribution switch간 L2 link로 연결된 local vlan design



(a) L3 link로 구현해 IP가 필요하며,
둘 사이에 routing protocol을 동작 시킵니다



(b) active router가 사용하는 모든 uplink의 장애 발생 시,
예비 link를 사용 한다

[그림 9] distribution switch간에 L3 link로 연결된 local vlan design

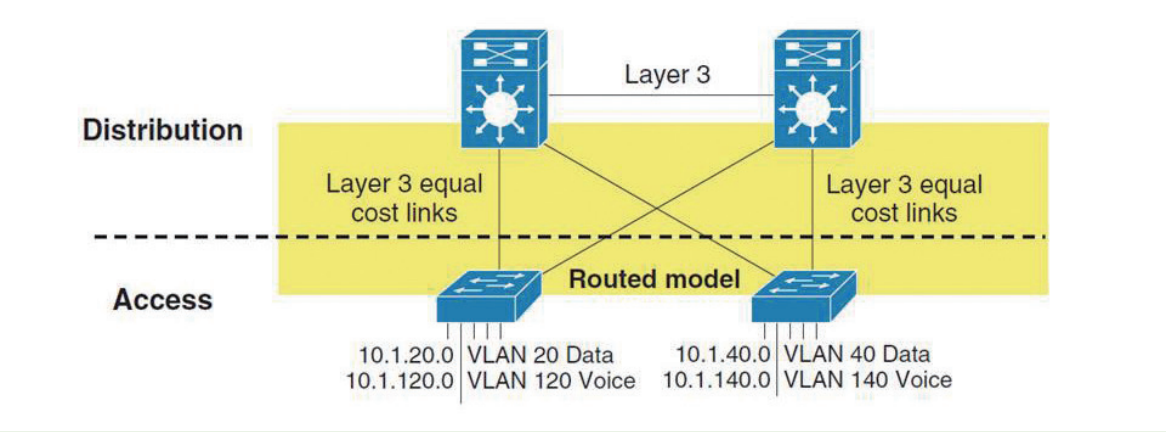
김해중
KBS 보도기술국

이번에는 [그림 9(a)]처럼 distribution switch 간 link를 layer 3로 구현해볼까요? L3 link이기에 IP가 필요하며, 둘 사이에 routing protocol(OSPF, EIGRP)을 동작시켜서 네이버를 만듭니다. 이 link는 평상시에는 거의 사용되지 않지만, [그림 9(b)]처럼 HSRP의 active switch의 모든 uplink에 문제가 발생했을 때, 예비 link를 사용하게 됩니다.

3rd (Routed model)

앞에서 설명한 2가지 디자인에서, routing과 switching의 경계는 distribution layer입니다. 즉 distribution layer의 아래쪽은 switching이 담당하고, distribution layer 위쪽은 routing이 담당합니다.

하지만 세 번째 design은 [그림 10]과 같이 L3 switch를 access layer에 배치해, routing protocol을 동작시킵니다. 즉 switching과 routing의 boundary가 access layer로 이동하는 것입니다.



[그림 10] access layer에 L3 switch를 배치하여 routing protocol을 동작시킨다

과거에는 L2 switch와 L3 switch의 장비 가격차가 컸으나, 현재는 가격차가 많이 줄어들어 이 방법을 권장합니다. 하지만 국내 현업에서 실제 이렇게 사용하고 있는 곳은 드뭅니다. 그 첫 번째 이유로는 여전히 routing은 switching에 비해 많이 느리다는 잘못된 인식 때문입니다. 과거에 switching은 hardware로 처리하고, routing은 software로 처리해서 속도가 많이 느렸습니다. 하지만 이제는 routing도 hardware로 처리해서 switching 할 때 속도차가 거의 없어졌습니다. 두 번째 이유로는 아직 이 디자인을 사용하는 reference site가 많이 없어서, 유지 보수에 부담을 느끼는 것 같습니다. 세 번째 이유로는 local vlan 방식에만 적용할 수 있기 때문입니다.

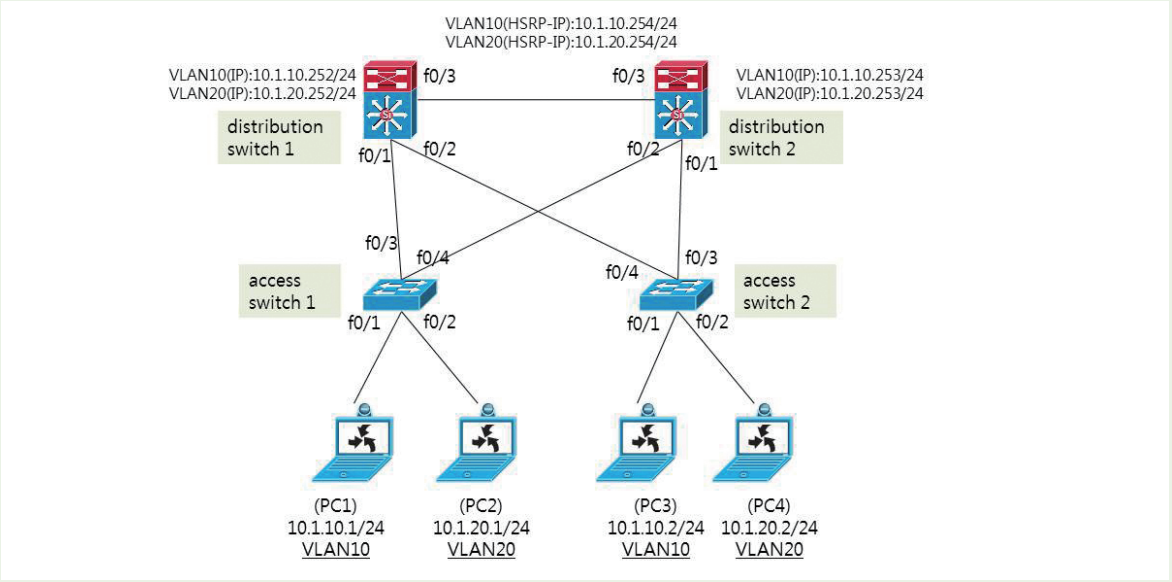
이 방법이 가지는 특징을, [표 1]에 정리해 보았습니다.

특징	설 명
loop-free	loop가 존재하지 않아, STP를 동작하지 않아도 되는 NO-STP 구조입니다. 하지만 예비로 RSTP를 동작을 시킵니다.
NO FHRP	routing protocol을 통해, 자동으로 load balance 되기에, FHRP(HSRP/VRRP)가 불필요합니다.
local VLAN에만 적합	이 방식은 end to end vlan에서는 사용할 수가 없습니다.
추가적인 IP 필요	access와 distribution간 연결이 L3라서, 추가적인 IP할당이 필요합니다.

[표 1] routed model의 특징

실전 LAB(end to end design)

이제는 end to end design [그림 11]을 실제로 구축해보도록 하겠습니다. cisco(IOS) 기준으로 명령어를 설명하겠습니다.



[그림 11]

1) 모든 switch에 vlan10과 vlan20을 만듭니다.

access switch 1	acc1(config)#vlan 10 acc1(config-vlan)#vlan 20
access switch 2	acc2(config)#vlan 10 acc2(config-vlan)#vlan 20
distribution switch 1	Dis1(config)#vlan 10 Dis2(config-vlan)#vlan 20
distribution switch 2	Dis2(config)#vlan 10 Dis2(config-vlan)#vlan 20

2) 모든 switch에 RSTP를 동작 시킵니다.

access switch 1	acc1(config)#spanning-tree mode rapid-pvst
access switch 2	acc2(config)#spanning-tree mode rapid-pvst
distribution switch 1	Dis1(config)#spanning-tree mode rapid-pvst
distribution switch 2	Dis2(config)#spanning-tree mode rapid-pvst

3) STP의 root switch를 결정합니다.

VLAN별로 load-balancing을 위해, vlan 10과 vlan 20에 대한 STP의 root switch를 다르게 합니다. vlan10에서는 좌측 distribution switch가 root switch이고, 우측 distribution switch가 secondary root switch입니다. vlan20에서는 그 반대입니다.

distribution switch 1	Dis1(config)#spanning-tree vlan 10 root primary → VLAN10에 대해 root switch로 만든다. Dis1(config)#spanning-tree vlan 20 root secondary → VLAN20에 대해 secondary root로 만든다.
distribution switch 2	Dis2(config)#spanning-tree vlan 10 root secondary → VLAN10에 대해 secondary root로 만든다. Dis1(config)#spanning-tree vlan 20 root primary → VLAN20에 대해 root switch로 만든다.

4) 이제는 각 switch의 interface 세팅을 해보겠습니다.

trunk port 세팅을 할 때는, 먼저 trunk 방식인 ISL과 802.1Q 중 무엇을 사용할지 미리 결정해야 합니다. 하지만 특정 switch는 더 이상 ISL을 지원하지 않고, 802.1Q만 지원하기에 선택하지 않아도 됩니다. 다음 config를 보면 access switch는 trunk 방식을 선택하지 않는 기종이고, distribution switch는 trunk 방식을 미리 선택해야 하는 기종입니다.

김해중
KBS 보도기술국

access switch 1	acc1(config)#interface fastEthernet0/1 acc1(config-if)#switchport mode access acc1(config-if)#switchport access vlan 10 → 해당 port를 VLAN10으로 세팅 acc1(config)#interface fastEthernet0/2 acc1(config-if)#switchport mode access acc1(config-if)#switchport access vlan 20 → 해당 port를 VLAN20으로 세팅 acc1(config)#interface fastEthernet0/3 acc1(config-if)#switchport mode trunk → 해당 port를 trunk port로 세팅 acc1(config)#interface fastEthernet0/4 acc1(config-if)#switchport mode trunk → 해당 port를 trunk port로 세팅
access switch 2	acc2(config)#interface fastEthernet0/1 acc2(config-if)#switchport mode access acc2(config-if)#switchport access vlan 10 → 해당 port를 VLAN10으로 세팅 acc2(config)#interface fastEthernet0/2 acc2(config-if)#switchport mode access acc2(config-if)#switchport access vlan 20 → 해당 port를 VLAN20으로 세팅 acc2(config)#interface fastEthernet0/3 acc2(config-if)#switchport mode trunk → 해당 port를 trunk port로 세팅 acc2(config)#interface fastEthernet0/4 acc2(config-if)#switchport mode trunk → 해당 port를 trunk port로 세팅
distribution switch 1	Dis1(config)#interface fastEthernet0/1 Dis1(config-if)#switchport trunk encapsulation dot1q → trunk 방식 미리지정 Dis1(config-if)#switchport mode trunk Dis1(config)#interface fastEthernet0/2 Dis1(config-if)#switchport trunk encapsulation dot1q → trunk 방식 미리지정 Dis1(config-if)#switchport mode trunk Dis1(config)#interface fastEthernet0/3 Dis1(config-if)#switchport trunk encapsulation dot1q → trunk 방식 미리지정 Dis1(config-if)#switchport mode trunk
distribution switch 2	Dis2(config)#interface fastEthernet0/1 Dis2(config-if)#switchport trunk encapsulation dot1q → trunk 방식 미리지정 Dis2(config-if)#switchport mode trunk Dis2(config)#interface fastEthernet0/2 Dis2(config-if)#switchport trunk encapsulation dot1q → trunk 방식 미리지정 Dis2(config-if)#switchport mode trunk Dis2(config)#interface fastEthernet0/3 Dis2(config-if)#switchport trunk encapsulation dot1q → trunk 방식 미리지정 Dis2(config-if)#switchport mode trunk

5) 앞부분은 Layer 2 세팅이었고, 이제는 Layer 3 세팅을 해보겠습니다.

먼저 L3 switch가 routing 기능을 하기 위해서는, 먼저 routing 기능을 enable 해야합니다.

Distribution switch 1	Dis1(config)#ip routing → L3 switch에 routing 기능 enable
Distribution switch 2	Dis2(config)#ip routing → L3 switch에 routing 기능 enable

이제는 L3 switch의 SVI interface에 IP 세팅을 합니다.

distribution switch 1	Dis1(config)#interface vlan 10 Dis1(config-if)#ip add 10.1.10.252 255.255.255.0 Dis1(config-if)#no shutdown Dis1(config)#interface vlan 20 Dis1(config-if)#ip add 10.1.20.252 255.255.255.0 Dis1(config-if)#no shutdown
distribution switch 2	Dis2(config)#interface vlan 10 Dis2(config-if)#ip add 10.1.10.253 255.255.255.0 Dis2(config-if)#no shutdown Dis2(config)#interface vlan 20 Dis2(config-if)#ip add 10.1.20.253 255.255.255.0 Dis2(config-if)#no shutdown

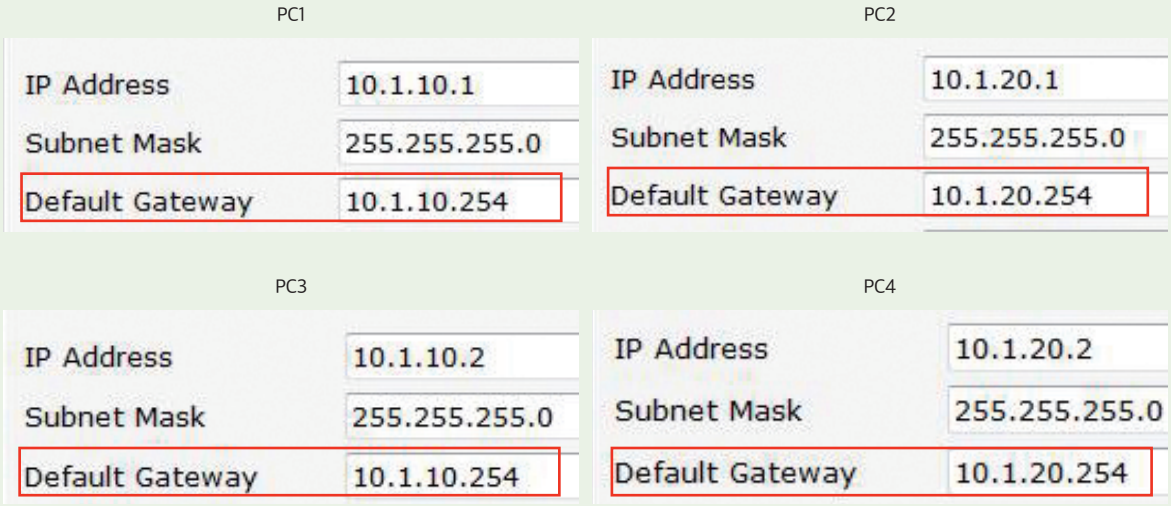
6) 게이트웨이 이중화 기술인 HSRP를 세팅합니다.

앞에서 배운 것과 같이, STP의 root switch와 HSRP의 active router를 일치시킨다고 했습니다. 그래서 VLAN10에 대해서는 좌측 distribution switch가 active 역할을 하고, VLAN20에 대해서는 우측 distribution switch가 active 역할을 합니다. active switch로 만들기 위해 priority를 기본값인 100보다 높은 150으로 세팅했습니다.

Distribution switch 1	Dis1(config)#interface vlan 10 Dis1(config-if)#standby 10 ip 10.1.10.254 Dis1(config-if)#standby 10 priority 150 -->priority를 높게 해 active로 만든다 Dis1(config)#interface vlan 20 Dis1(config-if)#standby 20 ip 10.10.20.254
Distribution switch 2	Dis2(config)#interface vlan 10 Dis2(config-if)#standby 10 ip 10.1.10.254 Dis2(config)#interface vlan 20 Dis2(config-if)#standby 20 ip 10.10.20.254 Dis2(config-if)#standby 20 priority 150 -->priority를 높게 해 active로 만든다

7) 각 PC에서 IP, subnet mask, default-gateway를 세팅합니다.

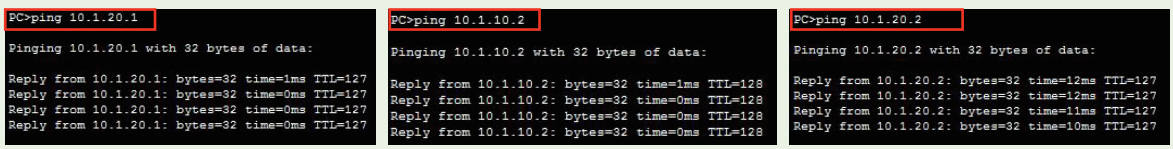
주의 사항으로는 [그림 12]와 같이, 각 PC에서 세팅하는 default-gateway IP는 HSRP에서 사용하는 virtual-IP를 입력해야 합니다.



[그림 12]

8) 마지막으로, 각 PC에서 통신이 되는지를 Ping을 통해 확인합니다.

PC1에서 PC2, PC3, PC4의 IP로 ping을 하니, 통신이 잘 됨을, [그림 13]을 통해 확인할 수 있습니다.



(a) PC1과 PC2의 통신 (b) PC1과 PC3의 통신 (c) PC1과 PC4의 통신

[그림 13]

다음 시간에는 switch 가상화(이중화) 기술에 대해서 알아보도록 하겠습니다.