김해중
KBS 보도기술국

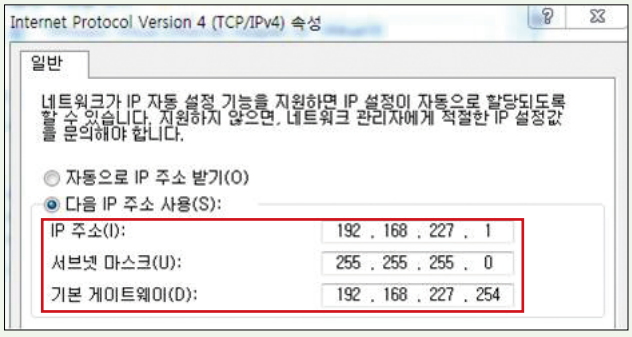
실무 네트워크 Design - 5 : FHRP(First hop redundancy protocol)

김해중 KBS 보도기술국

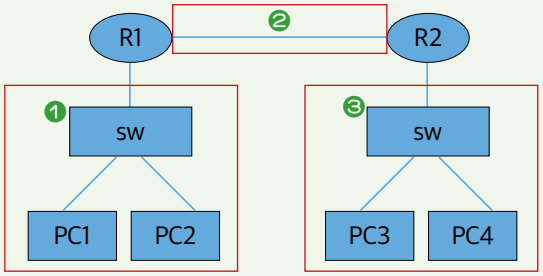
이번 시간에는 네트워크의 기본개념인 default-gateway와 ARP에 대해서 간단히 정리한 후에, router 장애를 대비한 default-gateway 이중화 기술인 FHRP에 대해서 알아보도록 하겠습니다. FHRP에는 3가지 방식인 HSRP, GLBP, VRRP가 있는데, HSRP와 GLBP는 cisco의 고유방식이며, VRRP는 IEE 표준기술입니다. 현재 cisco 장비를 사용하는 회사들은 HSRP를 주로 사용하고 있으며, cisco 이외의 장비를 사용하는 회사들은 VRRP를 주로 사용하는 추세입니다.

PC의 default-gateway

window OS에서는 [그림 1]처럼 IP, subnet-mask, default-gateway를 세팅합니다. 그럼 default-gateway는 도대체 무엇을 의미하는 것일까요? default-gateway란 해당 PC와 같은 network에 존재하는 router의 interface IP를 의미합니다.

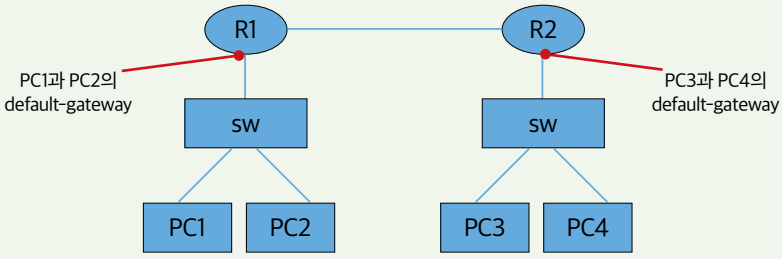


[그림 1] window os에서 default-gateway 세팅



[그림 2] 3개의 네트워크로 구성된 구조

[그림 2]를 보면, 3개의 네트워크로 구성되어 있음을 알 수 있습니다. 그럼 PC1과 PC2의 default-gateway는 어디일까요?
먼저 해당 PC와 동일 network에 존재하는 router를 찾습니다. 바로 R1 router겠죠, 그래서 R1 router의 interface 가 PC1, 2와 동일 네트워크 interface IP입니다. [그림 3]을 보면 쉽게 이해할 수 있습니다.



[그림 3] PC에서 세팅한 default-gateway의 개념

그럼 default-gateway는 어떤 역할을 하는 것일까요? PC에 입력된 IP와 subnetmask 정보를 통해서, 해당 PC는 자신이 어떤 IP 대역에 속하는지 알 수 있습니다. 만약 목적지 PC의 IP가 출발지 PC와 동일한 IP 대역이 아니라면, 목적지 PC는 자신의 네트워크가 아닌 외부 네트워크에 존재할 것입니다.

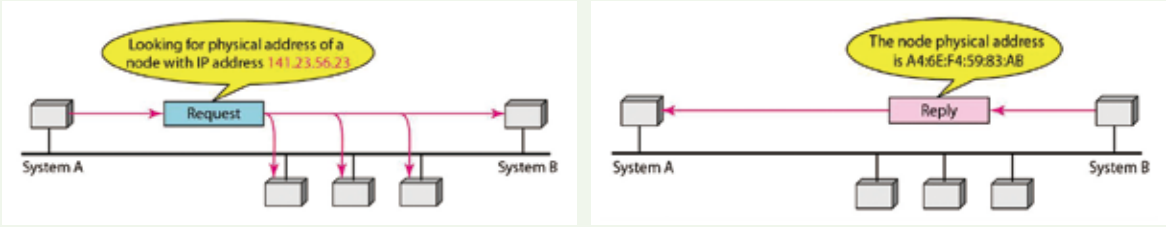
이러한 경우에 [그림 3]처럼 해당 PC는 자신의 네트워크 중에 유일하게 외부 정보를 알고 있는(외부와 연결된) 장비인 router에게 패킷을 보냅니다. 즉 PC는 자신의 default-gateway의 MAC 주소를 목적지로 해서, 해당 frame을 router에 전달하면, 해당 frame을 수신한 router는 지난 시간에 배운 routing을 통해서 목적지 PC로 전달하게 되는 것입니다.

ARP(Address resolution protocol)

ARP 개념

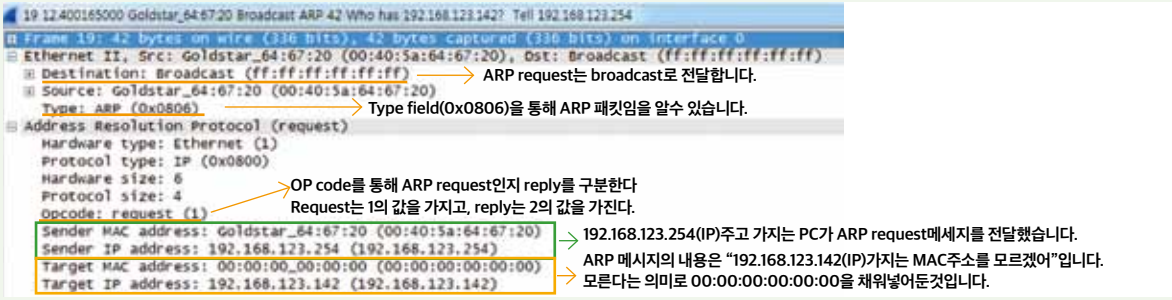
ARP는 워낙 유명한 protocol이라 다 알고 계시겠지만, FHRP는 실제 ARP를 기반으로 하고 있기에 간단히 정리하겠습니다. ARP는 목적지의 IP 주소는 아는데, 목적지의 MAC address를 모를 때 사용합니다.

[그림 4]를 보면서 설명하겠습니다. A 장비가 B 장비의 IP 주소(141.23.56.23)는 아는데, MAC 주소를 몰라서 ARP request를 보냅니다. ARP request는 broadcast로 전송되어서 모든 장비에 전달됩니다. ARP를 수신한 모든 장비 중에, 해당 IP를 가진 B 장비는 ARP reply를 통해 자신의 MAC address를 전달하고, 당연히 이때는 B 장비만이 A 장비에 보내기에 unicast로 전달합니다.



[그림 4] ARP의 동작방식

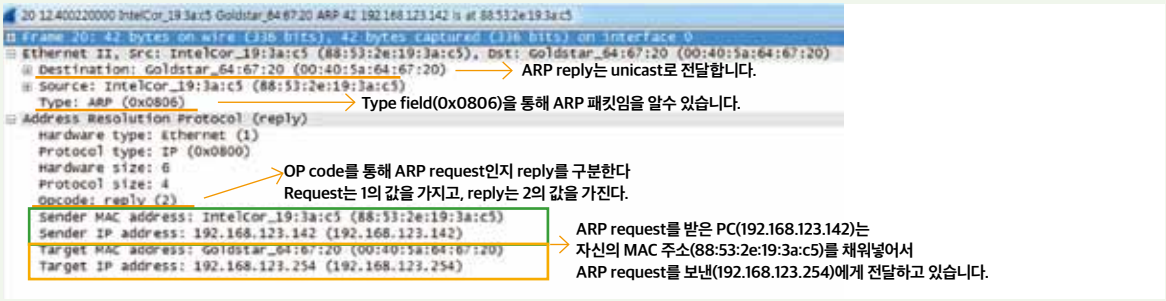
wireshark 프로그램을 통해서 캡처한 ARP request 패킷을 [그림5]를 통해 살펴보도록 하겠습니다.



[그림 5] 192.168.123.254가 192.168.123.142에 보낸 ARP request 메세지

김해중
KBS 보도기술국

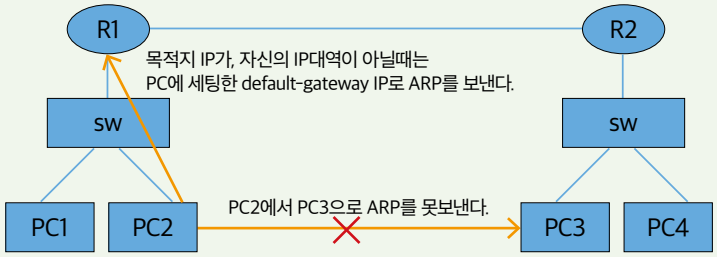
그럼 [그림 5]처럼 ARP request 메시지에 대한 ARP reply 패킷도 [그림 6]을 통해 살펴볼까요?



[그림 6] 192.168.123.142가 192.168.123.254에게 보낸 ARP reply 메세지

ARP는 broadcast 메시지라서 router를 통과하나요? router는 broadcast 패킷을 차단하기에, ARP request 메시지는 router 통과를 못 합니다. 그러면 [그림 7]처럼 PC2가 PC3의 IP 주소는 아는데, ARP 패킷이 갈 수 없어서 MAC 주소를 영원히 알 수가 없으니 통신이 불가능한 것인가요? 아니죠, 바로 여기서 앞에서 설명한 default gateway와 ARP 개념이 합쳐집니다.

각 PC는 자신이 입력한 IP, subnet-mask를 통해 자신의 network 대역을 안다고 했습니다. 그래서 목적지 IP 주소가 자신의 IP 대역이 아니면, 누구에게 보낸다고 했나요? 바로 default-gateway라고 했습니다. 그래서 이때 PC2는 ARP를 자신의 PC에 세팅한 default-gateway의 IP로 보내서, ARP reply를 받으면 일단 패킷을 R1에 전달합니다. 향후 R1은 routing을 통해서 목적지인 PC3으로 전달하게 됩니다.



[그림 7] 목적지 IP주소가 출발지 주소 IP 대역과 다를 때는 default-gateway의 IP주소로 ARP를 보낸다

GARP(Gratuitous ARP)

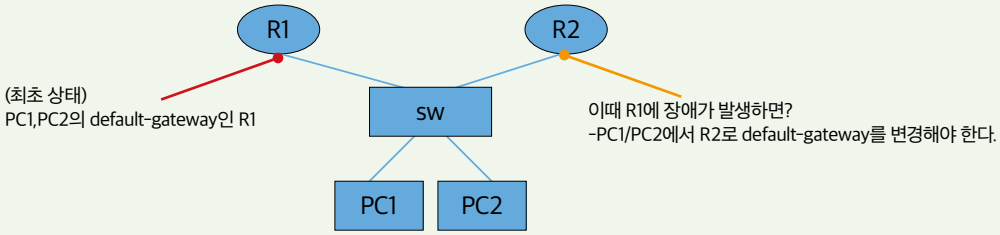
특수한 ARP인 GARP(Gratuitous ARP)를 살펴보도록 하겠습니다. GARP는 출발지와 목적지 IP주소가 동일한, 즉 자신의 IP주소에 대해서 ARP를 보내는 것입니다. 처음에 GARP을 공부할 때 "이게 왜 필요하지? 자신의 MAC 주소는 아는데, 굳이 자신의 IP로 ARP를 보낼 필요가 있나?" 라는 생각이 들었습니다. 하지만 용도를 알게 되신다면 아하! 하게 되실 겁니다.

일반적으로 window OS는 처음에 부팅하고 나면, 자신의 IP에 대해서 GARP를 던집니다. 당연히 자신의 IP에 대해서 ARP를 보냈으니, 아무도 응답하면 안 되겠죠? 그런데 이때 누군가 ARP reply를 보내는 아주 돌연변이 같은 상황이 발생했습니다. 이것을 무엇을 의미할까요? 바로 누군가와 나와 동일한 IP를 가지고 있다는 것입니다. windows OS를 처음 부팅한 후 '누군가가 자신과 동일한 IP를 쓰고 있다는 충돌 메시지'를 한번은 겪어 보셨을 건데요, 바로 그것이 GARP를 통해서 알게 된 것입니다.

GARP는 한 가지 용도가 더 있습니다. GARP를 수신한 PC와 router들은 자신의 ARP table을 새롭게 갱신하며, L2 switch는 자신의 switching table을 새롭게 갱신하게 됩니다. 지금까지 설명한 ARP의 개념을 확실히 알고 계셔야 FHRP를 이해하실 수 있습니다.

FHRP(First hop redundancy protocol)

등장 배경



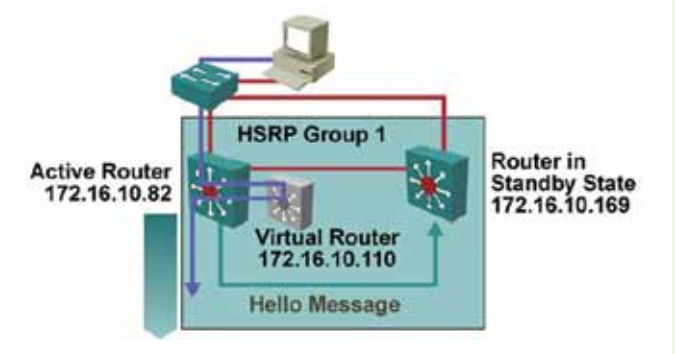
[그림 8] 장애를 대비한 router 2중화

일반적으로 대부분의 회사는 장애를 대비해서 default-gateway(즉 router) 이중화를 [그림 8]처럼 구현합니다. Router 2대를 배치해 두었지만, 실제 PC에서는 default-gateway를 1개만 세팅할 수 있습니다. 이때 PC1과 PC2에서 R1을 default-gateway로 세팅해 두었는데, R1에 장애가 발생하면 어떻게 될까요? 모든 PC에 들어가서 default-gateway를 R2로 변경해주면 됩니다.

그러나 위 방법은 2가지 문제점을 가지고 있습니다. 첫 번째는 R1에 장애 발생시, 각 PC에서 세팅을 변경하지 않으면 통신두절이 발생한다는 것입니다. 두 번째는 PC가 많은 경우(약 100대) PC마다 변경하려면 관리자의 관리 부담이 증가합니다. 즉 아무리 router를 예비로 많이 배치해 두더라도, 장애가 발생했을 때 큰 도움이 안 되는 문제를 해결하기 위해 FHRP가 등장하였습니다.

기본 동작방식

FHRP는 [그림 9]처럼 물리적인 여러 대의 router를 1대의 virtual router(가상의 router)로 만들어서, virtual-router에 virtual IP(V-IP)를 부여하는 방식을 사용합니다. 그리고 각 PC들은 물리적인 router의 IP 주소가 아닌, 가상 router의 V-IP를 default-gateway로 세팅합니다. [그림 9]를 보면 2대의 물리적 router는 172.16.10.82, 172.16.10.169의 IP를 가지고 있으며, virtual router에는 별도의 V-IP(172.16.10.110)를 할당했습니다.



[그림 9] FHRP에서 사용하는 Virtual-router 개념

물리적인 router에 priority를 부여해서 priority가 높은 쪽이 active router 역할을 하게 되며, priority가 낮은 쪽이 standby router 역할을 하게 됩니다.

active router는 크게 2가지 역할을 하는데, 첫 번째는 virtual-IP(V-IP)에 대한 ARP에 reply를 보냅니다. 두 번째는 수신한 패킷을 전달하는 역할을 합니다. 그럼 standby router는 무엇을 할까요? 평상시에는 그냥 쉬다가, active router에서 장애 발생 시, active router 역할을 대체합니다.

FHRP를 사용하는 router들은 hello 패킷을 서로 간에 주고받아서, 서로 간의 누가 active router가 되어야 할지를 결정합니다. FHRP를 사용하면 active router에서 장애가 발생하더라도 PC에 세팅된 default-gateway는 V-IP이기에, PC의 default-gateway를 변경할 필요가 없어서, 장애 시간을 감소시키며, 더불어 관리자의 관리 부담이 감소됩니다.

종류

FHRP는 현재 3가지가 존재합니다. cisco 전용 기술인 HSRP, GLBP와 표준 기술인 VRRP가 존재합니다. 일반적으로 cisco 장비를 사용하는 회사들은 HSRP를 대부분 사용하며, Juniper 장비를 사용하는 회사들은 VRRP를 사용하고 있습니다. cisco의 GLBP는 국내에서 거의 사용되고 있지 않습니다.

김해중
KBS 보도기술국

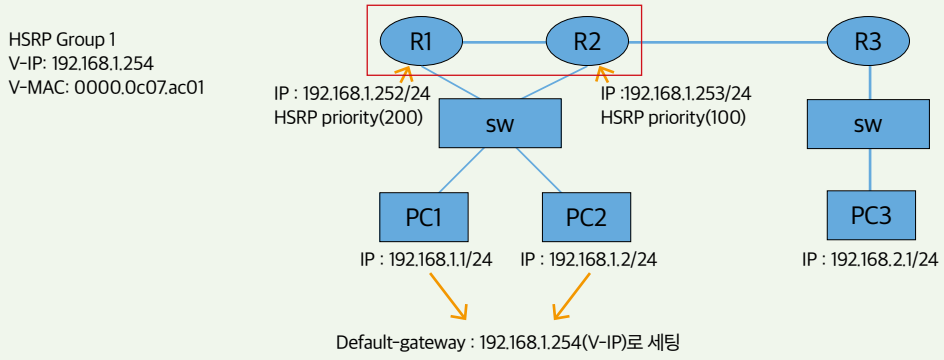
Virtual-MAC address(V-MAC)

Virtual-router에서 사용하는 V-IP에는 V-MAC 주소가 부여되며, HSRP일 때는 [그림 10]과 같은 규칙을 사용합니다. MAC address의 앞의 3byte(0000.0c)는 cisco를 의미하며, 07ac는 HSRP를 사용함을 의미하고, 뒤의 xx는 HSRP가 사용하는 group 번호를 16진수로 표현한 것입니다.

[그림 10] HSRP에서 사용하는 Virtual-mac address(V-MAC)

HSRP 동작

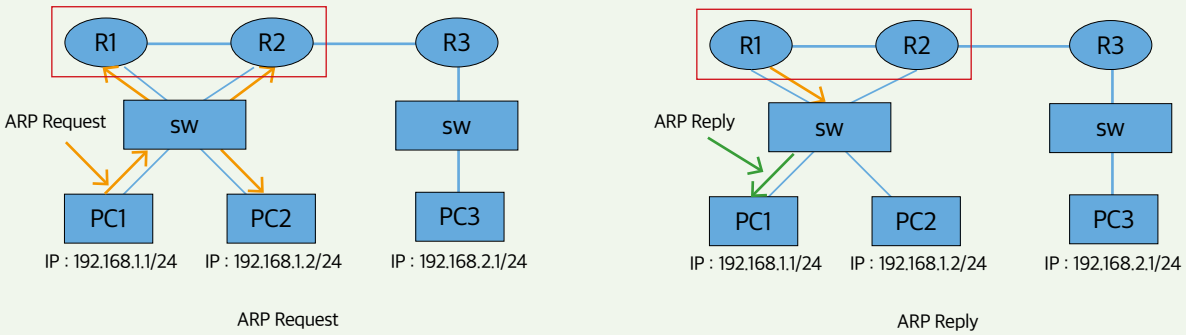
앞에서 배운 내용을 [그림 11]을 통해서 모두 정리해 보도록 하겠습니다. [그림 11]은 PC1이 다른 subnet에 위치하고 있는 PC3과 통신한다고 가정합니다.



[그림 11]

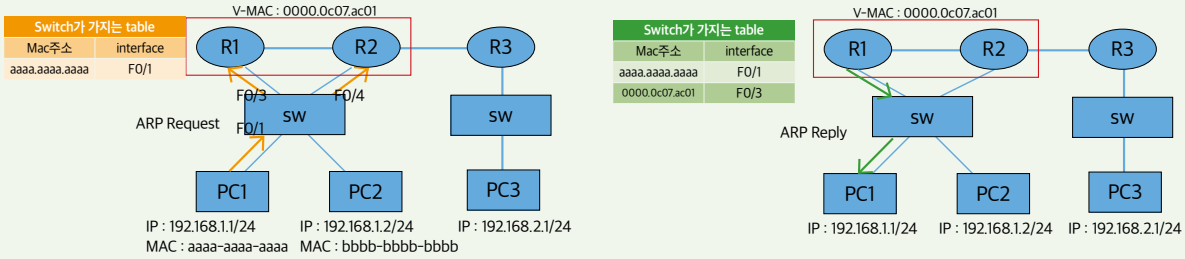
[그림 11]을 보면 HSRP를 구현하고 있고, V-MAC 주소가 0000.0c07.ac01(끝이 01) 통해서 HSRP group 1을 사용하고 있음을 알 수 있습니다. PC1과 PC2는 default-gateway의 IP 주소로 V-IP 주소인 192.168.1.254를 사용하고 있습니다.

[그림 11]에서 누가 active router일까요? 당연히 priority가 높은 R1이 active입니다. active router는 무슨 역할을 한다고 했죠? V-IP에 대한 ARP를 받으면 ARP reply를 보낸다고 했습니다. 그때 standby router는 그냥 쉰다고 했죠? 즉 ARP를 무시합니다. 최초에 PC1이 PC3와 통신하려면 ARP를 해야 하겠죠, 그런데 PC3은 다른 네트워크에 있기에 default-gateway의 IP인 V-IP로 ARP request를 보냅니다. ARP는 broadcast라서 active, standby router 모두에 도착하겠죠. 이때 active router만 V-MAC 주소로 ARP reply를 보내고, standby router는 무시할 겁니다.



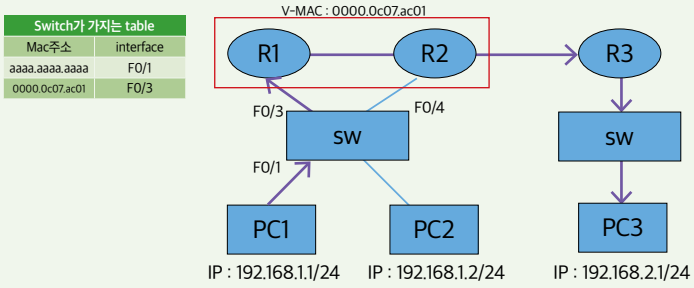
[그림 12] HSRP 구현시의 ARP 동작방식

그럼 ARP가 발생할 때, switch는 어떻게 자신의 MAC-address-table을 생성할까요? switch는 항상 들어오는 source 주소를 가지고 table을 만듭니다. 그러면 ARP request가 발생할 때는 그림 [13-(a)]처럼 table이 만들어지고, ARP reply가 발생할 때는 [13-(b)]처럼 table이 만들어집니다.



[그림 13] HSRP 구현 시의 switch가 가지는 mac-address-table

이제 PC1이 PC3으로 패킷을 보내면 [그림 14]와 같이 전달됩니다. PC1의 패킷을 수신한 switch는 자신의 MAC-address table을 확인한 후에, f0/3 포트를 통해서 R1에 보냅니다. 그러면 R1은 routing을 통해서, 목적지인 PC3에 전달합니다.

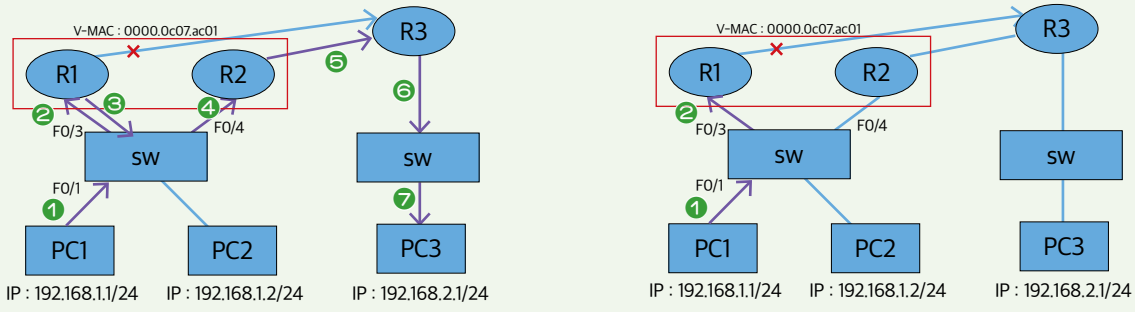


[그림 14] HSRP를 사용했을 때의 PC1에서 PC3으로 패킷 전달 과정

interface tracking

만일 [그림 15]처럼 active router(R1)의 uplink에서 장애가 발생한다면 어떻게 될까요? 이때는 2가지 경우가 발생합니다. 첫 번째는 R1과 R2가 OSPF를 사용하고 있다고 가정했을 때, R1과 R2가 OSPF 네이버라면 PC1이 보낸 패킷이 R1까지 갔다가, 다시 R2로 보내지는 redirect가 발생합니다.

두 번째는 R1과 R2가 OSPF 네이버가 아닐 때입니다. OSPF는 기본적으로 hello 패킷을 보내서 OSPF 네이버가 됩니다. 하지만 보안을 위해서 access switch 단으로 hello 패킷을 보내지 않는 기술(passive-interface)을 사용합니다. 이런 경우는 R1과 R2가 hello 패킷을 주고받지 않아 OSPF 네이버가 되지 않습니다. 그래서 R1까지 도착한 패킷은 routing table에 다른 네트워크에 대한 경로가 없기에(R1은 어떤 OSPF 네이버도 없기에) 패킷 drop이 발생합니다.

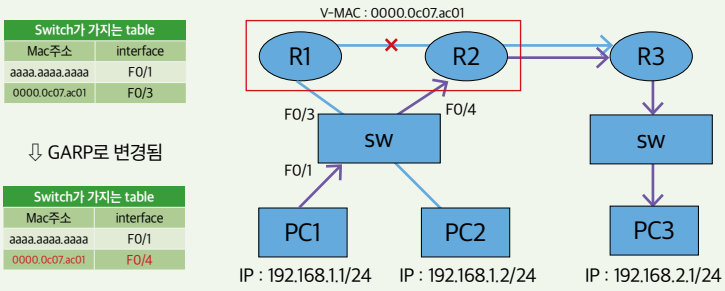


[그림 15] uplink 장애 발생 시 traffic 흐름의 문제점

김해중
KBS 보도기술국

active router의 uplink 장애 시 발생한 문제점에 대한 해결책으로 interface tracking이 등장합니다. R1의 uplink가 죽으면, R1의 priority를 감소시켜서 더 이상 active 역할을 못 하게 하고, standby인 R2가 active router가 되게 하는 것입니다.

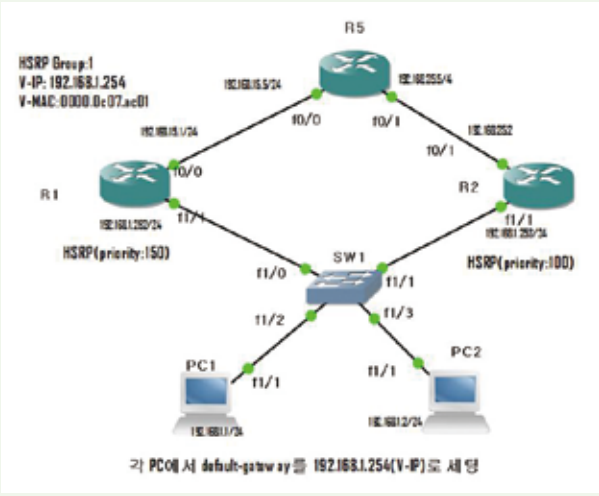
그런데 R2가 active router가 되더라도, switch의 MAC-address-table은 변하지 않기에 여전히 패킷은 R1으로 갈 것입니다. 이것을 방지하기 위해서 R2는 active router가 되자마자, 자신이 V-IP에 해당되는 V-MAC 주소를 가지고 있다는 것을 알리기 위해서 GARP를 broadcast 합니다. GARP를 받은 switch는 기존에 f0/3 포트에 기록하고 있던 V-MAC 주소(0000.0c07.ac01)를 f0/4번 port로 변경하게 됩니다. 이제 switch는 PC1에서 패킷을 받자마자, R2로 스위칭하게 됩니다.



[그림 16] interface tracking 사용 후의 traffic 흐름

실전 HSRP 세팅

[그림 17]에 그려진 간단한 네트워크를, cisco의 IOS 명령어 기준으로 HSRP를 구현해 보았습니다. 앞에서 설명을 복잡하게 하였지만 실제 명령어는 정말 간단합니다. 네트워크를 공부할 때 가장 놀라운 점이, 이론은 몇 십 page로 방대한데, 실제 구현하는 명령어는 단 몇 줄밖에 되지 않아서 때로는 너무 허탈하기도 합니다.

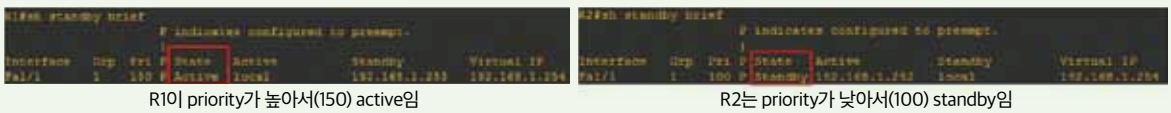


(R1)
int f1/1
ip add 192.168.1.252 255.255.255.0
standby 1 ip 192.168.1.254 (V-IP를 192.168.1.254로 세팅함)
standby 1 priority 150 (active router로만들기 위해 150으로 세팅함)
standby 1 track f0/0 100 (uplink f0/0 장애시 priority 100감소해 50됨)
standby 1 preempt (R1이 장애 후 복귀시 다시 active역할을 한다)
※ group 1에 대한 HSRP라서 standby 1 명령어를 넣었다.

(R2)
int f1/1
ip add 192.168.1.253 255.255.255.0
standby 1 ip 192.168.1.254 (V-IP를 192.168.1.254로 세팅함)
standby 1 priority 100
standby 1 preempt (R1의 uplink장애시 R2가 active역할을 뺏아옴)

[그림 17] cisco router에서의 HSRP 세팅

cisco router에서 HSRP를 세팅한 후에, show standby brief 명령어를 입력하시면 R1이 active router, R2가 standby router임을 알 수 있습니다.

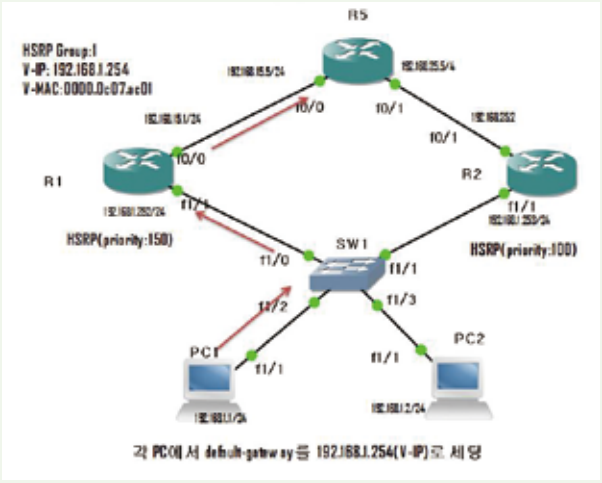


R1이 priority가 높아서(150) active임

R2는 priority가 낮아서(100) standby임

[그림 18] show standby brief명령어를 통해서 HSRP 상태를 알 수 있다

PC1에서 R5(192.168.15.5)로 가는 경로를 보면, active router인 R1(192.168.1.252)을 거쳐서 R5로 도착함을 [그림 19]를 통해 알 수 있습니다.




```
PC1#traceroute 192.168.15.5

Type escape sequence to abort.
Tracing the route to 192.168.15.5

  1 192.168.1.252 68 msec 32 msec 36 msec
  2 192.168.15.5 48 msec 28 msec 68 msec
```

[그림 19] R3에서 R5(192.168.15.5)로 갈 때는 active router(R1)을 이용함을 알 수 있다

그리고 switch(sw1)에서의 MAC-address table[그림 20]을 보면 V-MAC 주소인(0000.0c07.ac01)가 active router가 존재하는 interface fastEthernet 1/0으로 학습되어 있음을 알 수 있습니다.

```
sw1#sh mac
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
c406.2a2c.0000          Self          1     Vlan1
0000.0c07.ac01          Dynamic       1     FastEthernet1/0
c401.28c0.f101          Dynamic       1     FastEthernet1/1
c400.28c0.f101          Dynamic       1     FastEthernet1/0
```

[그림 20] switch(sw1)의 MAC-address-table

요약

용 어	개 념
ARP	목적지의 IP 주소는 아는데, MAC 주소를 모를 때 사용한다. ARP request는 broadcast로 전송하고, ARP reply는 unicast로 전송한다.
GARP	출발지와 목적지의 IP 주소가 같은 특수한 ARP이다. PC와 router의 ARP table을 갱신하거나, L2 switch의 MAC table을 갱신할 때 사용한다.
FHRP	라우터 장애를 대비해서 2대의 router를 가상의 1대의 router로 만들어 사용하는 router 이중화 기술이다.
Active router	HSRP에서 실제로 목적지로 패킷을 전송하며, virtual IP에 대한 ARP request에 응답하는 router이다.
Standby router	HSRP에서 active router 장애 발생시, active router 역할을 대체하는 router이다.
interface tracking	FHRP를 사용하는 환경에서, uplink 장애 발생시 active router의 priority를 감소시켜서 standby router로 만드는 기술이다.

다음 시간에는 지금까지 배운 모든 내용을 정리하면서, LAN design에 대해서 조금 더 깊게 다루어 보도록 하겠습니다.