FHRP

○ First Hop Redundancy Protocol(게이트웨이 이중화 프로토콜)

- PC나 서버처럼 라우팅 기능이 없는 장비들은 게이트웨이를 통하여 자신과 다른 네트워크에 연결된 장비들과 통신
- 게이트웨이 역할을 하는 라우터나 L3 스위치를 복수개로 구성하고, 하나가 다운되면 다른 하나가 그 역할을 계속 수행하게 하는 프로토콜

1. HSRP(Hot Standby Router Protocol)

- 시스코에서 개발한 게이트웨이 이중화 프로토콜
- HSRP 장비중 하나가 Active Router 역할을 하며, 이것이 게이트웨이 주소가 목적지인 패킷을 처리한다.
- Standby Router는 Active Router를 감시한다. 만약 Active Router가 다운되면 대기상태의 라우터가 그 역할을 이어받아 게이트웨이 역할을 한다.

○ HSRP 동작 방식

- Standby 그룹별로 하나의 Active Router와 하나의 Standby Router를 뽑는다.
- HSRP는 버전 1과 2가 있으며, IOS 12.2 SE부터 두가지 버전 모두를 지원하나 기본적으로는 버전 1이 동작한다.
- 버전 1은 목적지 IP주소가 멀티캐스트 주소 224.0.0.2를 사용한다. 이는 CGMP(Cisco Group Management Protocol)과 동일한 주소여서 HSRP와 CGMP를 동시에 사용할 수 없다. 그러나 버전 2에서는 목적지 IP주소를 224.0.0.102를 사용한다. 두 버전 모두 UDP 포트번호 1985를 사용한다.
- 버전 1과 2는 호환되지 않는다. 그러나 인터페이스별로 서로 다른 버전을 사용할 수는 있다.

○ HSRP 인터페이스의 상태 변화

1. Initial State: HSRP 시작 상태, HSRP 미동작 상태
2. Learn State: 가상 IP 주소가 결정되지 않은 상태
3. Listen State: 가상 IP 주소가 결정된 상태, 헬로 메시지 대기 상태
4. Speak State: 주기적 헬로 메시지 전송 상태, Active/Standby 선출 참여
5. Standby State: Active Router의 후보가 될 수 있음, 그룹 내 1개의 Standby만 존재
6. Active State: 가상 Mac 주소로 전송된 패킷을 수신하여 라우팅시키는 상태

○ HSRP 설정(인터페이스)

```
R(c-if)# standby 1 ip ...
R(c-if)# standby 1 priority ...
R(c-if)# standby 1 preempt (delay minimum 180)
```

R(c-if)# standby 1 track 인터페이스명

* HSRP의 그룹번호는 0 - 255 사이의 수를 사용할 수 있다.

* **Delay Minimum 초**

많은 경우 인터페이스가 활성화되어도 라우팅 테이블은 아직 미완성이라 특정 목적지에 대한 라우팅이 불가능할 수 있다. 따라서 **인터페이스가 활성화되어도 바로 Active Router 역할을 수행하지 않고 라우팅 테이블이 완성된 다음에 Active Router 역할을 하기 위해 적절한 지연값을 지정**

○ **확인 명령어**

show standby brief

show standby

○ **HSRP MAC Address**

기본적으로 HRSP 라우터가 사용하는 Virtual IP 주소에 대한 Mac 주소는 **0000.0c07.acNN**이다. 이때 **NN은 16진수로 표시한 HSRP 그룹 번호**이다. 예를 들어 그룹 10의 가상 Mac 주소는 0000.0c07.ac0a이다.

확인은 **show standby** 명령어를 사용한다.

use-bia 옵션을 사용하여 Active Router 자신의 고유한 MAC 주소를 사용할 수도 있다.

○ **Gratuitous ARP**

HSRP Active Router가 변경되면 HSRP 라우터들이 접속된 스위치의 MAC 주소 테이블도 변경되어야 한다. 이를 위해 사용되는 것이 Gratuitous ARP이다. 상대방이 요청하지 않은 자발적인 ARP 응답을 보내는 것이다.

○ **MHSRP(Multiple HSRP, Multigroup HSRP)**

2개 이상의 HSRP 그룹을 만들어 각 그룹별로 서로 다른 Active 라우터를 지정하는 방법

R1(c-if)# standby 1 ip 주소1
R1(c-if)# standby 1 priority 105
R1(c-if)# standby 1 preempt delay minimum 180
R1(c-if)# standby 1 track 인터페이스명
!
R1(c-if)# standby 2 ip 주소2
R1(c-if)# standby 2 preempt

R2(c-if)# standby 1 ip 주소1
R2(c-if)# standby 1 preempt
!
R2(c-if)# standby 2 ip 주소2
R2(c-if)# standby 2 priority 105
R2(c-if)# standby 2 preempt delay minimum 180

R2(c-if)# standby 2 track 인터페이스명

○ **HSRP 인증**

HSRP 인증 기능을 사용하면 공격자의 PC가 Active로 설정되는 HSRP Spoofing 공격을 완화시킬 수 있다.

- **Text 인증**

  R(c-if)# **standby 1 authentication text** cisco
- **MD5 인증**

  R(c-if)# **standby 1 authentication md5 key-string** cisco
- **Key-Chain 생성후 인터페이스 적용 방법**

  key chain HSRP

  key 1

  key-string cisco

  !

  standby 1 authentication md5 key-chain HSRP

2. VRRP(Virtual Router Redundancy Protocol)

- HSRP와 달리 표준이므로 시스코가 아닌 다른 회사의 제품에서도 지원되므로 Multi-Vendor 환경에서 게이트웨이 이중화 프로토콜로 많이 사용된다.

○ **VRRP 동작 방식**

- 게이트웨이 역할을 하는 장비를 Master Router라 하고, 마스터 라우터 장애시 역할을 이어받는 장비들을 Backup Router라 한다.
- Master Router는 목적지 주소 224.0.0.18, 프로토콜 번호 112인 패킷을 사용하여 기본적으로 1초에 한번씩 VRRP 우선순위 및 상태를 광고한다.
- 인터페이스에 설정된 실제 IP주소를 가상 IP 주소로 사용할 수도 있고, 별도의 가상 IP 주소를 사용해도 된다.
- Master Router 결정 우선순위

  1) 가상 IP 주소와 인터페이스 IP 주소가 같은 라우터(Owner)

  2) VRRP 우선순위값이 높은 라우터

  3) 인터페이스 IP 주소가 높은 라우터

○ **VRRP 설정**

R(c-if)# vrrp 1 ip ...

R(c-if)# vrrp 1 preempt delay minimum 180

R(c-if)# vrrp 1 priority 105

R(c-if)# vrrp 1 track 1

R(c-if)# vrrp 1 timers advertise 1

R(c-if)# vrrp 1 timers learn

!
R(config)# track 1 interface f0/1 line-protocol

* vrrp 1 timers advertise 1
VRRP 광고 주기를 1초로 지정. 기본값이 1초이므로 그대로 사용하려면 별도로 설정하지 않아도 된다. 필요시 msec 단위로 지정할 수도 있다.
vrrp 1 timers learn 명령어를 사용하지 않고, VRRP 라우터들간에 vrrp 1 timers advertise 명령어에 의해 설정된 광고주기가 다르다면 VRRP가 동작하지 않는다. 즉 모든 라우터들이 VRRP Mater가 된다.

* vrrp 1 timers learn
Master Router에 설정된 VRRP 광고주기값을 배우도록 설정. Backup Router가 될 때 적용

* vrrp 1 track 1
특정 인터페이스의 상태를 감시하다가 장애가 발생하면 기본적으로 VRRP 우선순위를 10만큼 감소시켜 광고한다.

* track 1 interface f0/1 line-protocol
상태를 감시할 인터페이스나 경로를 지정한다. line-protocol 옵션은 해당 인터페이스의 Layer 2 상태에 따라 업 또는 다운 상태를 판단하다.

* 네트워크 존재 여부를 트래킹하는 방법
track 2 ip route 1.1.1.1/32 reachability

○ 확인 명령어
show vrrp brief
show vrrp
show track

○ VRRP 인증
VRRP 인증기능을 사용하면 공격자의 PC가 마스터가 되는 VRRP Spoofing 공격을 완화시킬 수 있다.
- Text 인증
  vrrp 1 authentication text cisco
- MD5 인증
  vrrp 1 authentication md5 key-string cisco
- Key Chain 생성후 인터페이스 적용 방법
  key chain VRRP
  key 1
  key-string cisco
  !

vrrp 1 authentication md5 key-chain VRRP

○ **VRRP 부하 분산**

```
R1(c-if)# vrrp 1 ip 주소1
R1(c-if)# vrrp 1 preempt delay minimum 180
R1(c-if)# vrrp 1 priority 105
R1(c-if)# vrrp 1 track 1
R1(c-if)# vrrp 1 timers advertise 1
R1(c-if)# vrrp 1 timers learn
!
R1(c-if)# vrrp 2 ip 주소2
R1(c-if)# vrrp 2 timers advertise 1
R1(c-if)# vrrp 2 timers learn
!
R1(config)# track 1 interface f0/1 line-protocol

R2(c-if)# vrrp 1 ip 주소1
R2(c-if)# vrrp 1 timers advertise 1
R2(c-if)# vrrp 1 timers learn
!
R2(c-if)# vrrp 2 ip 주소2
R2(c-if)# vrrp 2 preempt delay minimum 180
R2(c-if)# vrrp 2 priority 105
R2(c-if)# vrrp 2 track 1
R2(c-if)# vrrp 2 timers advertise 1
R2(c-if)# vrrp 2 timers learn
!
R2(config)# track 1 interface f0/1 line-protocol
```

3. GLBP(Gateway Load Balancing Protocol)

- 게이트웨이 이중화 기능을 제공하면서, 별도의 설정없이 부하분산 기능을 제공한다.

○ **GLBP 동작 방식**

- 단일 가상 IP와 복수개의 MAC 주소를 사용한다.
- 3초마다 224.0.0.102, UDP 3222(출발지, 목적지 번호 동일)번으로 통신한다.
- 그룹당 하나의 AVG(Active Virtual Gateway)를 뽑는다.

▶ **AVG 주요 역할**

- 각 멤버들에게 가상 MAC 주소를 할당

AVG는 각 멤버들에게 가상 MAC 주소를 할당하며, 이 멤버들을 해당 가상 MAC 주소의 **AVF(Active Virtual Forwarder)**라고 한다. **각 AVF들은 자신에게 할당된 가상 MAC이 목적지로 설정된 프레임의 전송을 담당한다.**

- 게이트웨이 주소 ARP 요청 응답
  PC 등이 보내는 게이트웨이 IP 주소에 대한 ARP 요청에 대해 AVF에게 할당한 MAC 주소들로 응답하여 자동으로 부하분산이 일어난다.

▶ **AVG 결정 우선순위**
1) GLBP 우선순위값이 높은 라우터
2) 인터페이스 IP 주소가 높은 라우터

- **그룹당 4개의 가상 MAC 주소를 사용할 수 있다.** GLBP에서 하나의 라우터가 AVG가 되면, 다른 하나는 Standby, 나머지들은 Listen 상태에 놓인다. AVG가 다운되면 Standby Router가 AVG가 되며, Listen 상태의 라우터들중 새로운 Standby Router를 뽑는다.

○ **GLBP 설정**

```
R(c-if)# glbp 1 ip ...
R(c-if)# glbp 1 priority 105
R(c-if)# glbp 1 preempt delay minimum 60
R(c-if)# glbp 1 timers 2 6
R(c-if)# glbp 1 forwarder preempt delay minimum 50
R(c-if)# glbp 1 weighting 100 lower 90 upper 100
R(c-if)# glbp 1 weighting track 1 decrement 20
R(c-if)# glbp 1 load-balancing round-robin
!
R(config)# track 1 interface f0/1 line-protocol
```

* GLBP의 그룹번호는 0부터 1023까지 총 1024개를 설정할 수 있다.

* **glbp 1 timers ... ...**
  GLBP Hello와 Hold Timer를 지정한다. 기본값은 Hello 3초, Hold 10초이다.

* **glbp 1 forwarder preempt delay minimum ...**
  AVF Preemption 설정. 장애가 발생하여 다른 라우터에게 AVF 역할을 넘겨주었다가 장애처리 후 다시 AVF의 역할을 수행하게 한다. AVG Preemption과 달리 AVF Preemption은 기본적으로 활성화되어 있으며, 지연값은 30초이다.

* **glbp 1 weighting 100 lower 90 upper 100**
  전송가중치를 100으로 설정한다. 이 가중치 비율로 패킷을 전송할 수 있다. glbp 1 load-balancing weighted 명령어를 사용하면 설정한 Weight(가중치) 비율에 따라 부하분산을

하게 된다. 그러나 기본적인 부하분산 방식은 Weight와 무관한 round-robin으로 ARP 요청별로 2개의 GLBP 가상 MAC 주소를 번갈아 알려준다.

가중치가 90이 되면 상대에게 AVF 역할을 넘기고, 100이 되면 다시 AVF 역할을 받아오겠다는 의미를 가진다. 만약 상한값을 지정하지 않으면 가중치값이 상한값이 된다.

* glbp 1 weighting track 1 decrement 20

관찰대상 번호 1이 다운되었을 때 가중치의 값이 20 감소시킨다. decrement 옵션을 사용하지 않으면 기본적으로 10을 감소시킨다.

* glbp 1 load-balancing round-robin

부하분산 방식을 정의한다. 별로로 정의하지 않으면 round-robin으로 호스트들의 ARP 요청별로 2개의 GLBP Router들이 가상 MAC 주소를 번갈아 알려주어 로드밸런싱을 구현한다.

Host-dependent는 round-robin과 비슷하나 동일한 호스트에게는 동일한 가상 MAC 주소를 알려준다.

Weighted 옵션은 GLBP 라우터별 웨이트 비율에 따라 부하분산을 하게 된다.

* 네트워크 존재 여부 트래킹하기

track 2 ip route 1.1.1.1/32 reachability

○ **GLBP 확인**

show glbp brief
show glbp
show arp

○ **GLBP 인증**

GLBP 인증기능을 사용하면 공격자의 PC가 AVG나 AVF가 되는 GLBP Spoofing 공격을 완화시킬 수 있다.

- Text 인증

  glbp 1 authentication text cisco
- MD5 인증

  glbp 1 authentication md5 key-string cisco
- Key Chain 이용한 인터페이스 적용

  key chain GLBP
  key 1
  key-string cisco
  !
  glbp 1 authentication md5 key-chain GLBP