

Huawei Genel Notlar

Normal şartlar altında network üzerinde istemcilere tek bir Gateway adresi tanımlanabiliyor. Bu nedenle routerlar arasında doğrudan kablolama yapılarak routerlar arasında yedeklilik sağlanamıyor. Routerların Gateway görevi yaptığı arayüzlerinde yedeklilik sağlayabilmek için FHRP protokolleri kullanılıyor. Bu yazıda Huawei routerlar arasında yedeklemenin nasıl gerçekleştirildiği açıklanmaya çalışılacaktır.

Huawei routerlarda yedeklilik için Open Standart olan VRRP protokolü kullanılıyor. VRRP protokolünün çalışma mekanizması Cisco notlarında açıklanmıştır. VRRP konfigürasyonu için;

- İlk olarak cihaz üzerinde VRRP konfigürasyonu uygulanacak fiziksel portun arayüzüne giriş yapılarak temel ip adresi konfigürasyonu yapılmalıdır.
 - o Konfigürasyon L3 switch üzerinde yapılıyorsa portların L3'de çalışıp çalışmadığı kontrol edilmelidir.
 - o Temel ip konfigürasyonu yapılmadığı takdirde VRRP protokolü çalışacak ama arayüzlerin ip adresi/network bilgisi yönlendirme tablosunda tanımlı olmayacağı için routerlar arasında haberleşme gerçekleştirilemeyecektir.
- Temel ip konfigürasyonu yapıldıktan sonra **"vrrp vrid <VRRP Group Id> virtual-ip <Virtual ip Address>"** komutu kullanılarak arayüz bir VRRP grubuna dâhil edilirken burada kullanacağı sanal ip adresi de belirtiliyor.
 - o Burada tanımlanan sanal ip adresi bu VRRP grubuna eklenecek diğer router arayüzlerinde de aynı tanımlanmalıdır.
 - o Fiziksel arayüzlerde kullanılan ip adreslerinden birisi aynı zamanda VRRP grubu için sanal ip adresi olarak da kullanılabilir.

```
[~CE6800-2-SW]int ge 1/0/0
[~CE6800-2-SW-GE1/0/0]undo portswitch
[~CE6800-2-SW-GE1/0/0]ip address 10.0.1.2 24
[~CE6800-2-SW-GE1/0/0]undo sh
[~CE6800-2-SW-GE1/0/0]quit
[~CE6800-2-SW]
[~CE6800-2-SW]int ge 1/0/0
[~CE6800-2-SW-GE1/0/0]vrrp vrid 1 virtual-ip 10.0.1.1
[~CE6800-2-SW-GE1/0/0]quit
[~CE6800-2-SW]commit
```

```
[~CE6800-3-SW]int ge 1/0/0
[~CE6800-3-SW-GE1/0/0]undo portswitch
[~CE6800-3-SW-GE1/0/0]ip address 10.0.1.3 24
[~CE6800-3-SW-GE1/0/0]undo sh
[~CE6800-3-SW-GE1/0/0]quit
[~CE6800-3-SW]
[~CE6800-3-SW]int ge 1/0/0
[~CE6800-3-SW-GE1/0/0]vrrp vrid 1 virtual-ip 10.0.1.1
[~CE6800-3-SW-GE1/0/0]quit
[~CE6800-3-SW]commit
```

```
[~CE6800-2-SW]display vrrp state-change interface GE 1/0/0 vrid 1
Time                SourceState      DestinationState Reason
-----
2024-03-27 09:47:11 Backup          Master          Protocol timer expired
2024-03-27 09:47:08 Initialize      Backup          Interface up
[~CE6800-2-SW]
```

Portları açılıp kapatıldıktan sonraki VRRP protokolünün durum değişimi aşağıdaki gibidir.

```
[~CE6800-2-SW-GE1/0/0]display vrrp state-change interface GE 1/0/0 vrid 1
Time                SourceState      DestinationState Reason
-----
2024-03-27 10:02:38 Backup          Master          Protocol timer expired
2024-03-27 10:01:42 Initialize      Backup          Interface up
2024-03-27 10:00:30 Master          Initialize      Interface down
2024-03-27 09:47:11 Backup          Master          Protocol timer expired
2024-03-27 09:47:08 Initialize      Backup          Interface up
```

VRRP protokolü aynı konfigürasyon yedeklenecek diğer routerlarda da uygulandıktan sonra kullanılmaya başlanabilir. İsteğe bağlı olarak çeşitli özelleştirmeler uygulanabiliyor. Uygulanabilecek özelleştirmelere bakıldığında;

- Yedeklenen routerlar arasında “**vrrp vrid <VRRP Group Id> priority <Priority Value>**” komutuyla Priority değerleri üzerinde oynamalar yapılarak Master router seçimine müdahale edilebilir.
 - o Yedeklenen routerlar arasında ayrıca bir Priority değeri ayarlanmadığı sürece VRRP protokolünün ilk devreye alındığı router Master router seçilecektir. Preemption özelliği devredeyse arayüzlerine atanan ip adresi en yüksek router Master olarak seçilecektir.

```
[*CE6800-2-SW]int ge 1/0/0
[*CE6800-2-SW-GE1/0/0]vrrp vrid 1 priority ?
    INTEGER<1-254> The level of priority(the default is 100)
[*CE6800-2-SW-GE1/0/0]vrrp vrid 1 priority 150
[*CE6800-2-SW-GE1/0/0]quit
```

- Master seçilen router üzerinde yaşanan bir problem giderildikten sonra tekrar Master router olması isteniyorsa “**vrrp vrid <VRRP Group Id> preempt timer delay <Delay Time>**” komutuyla Preemption özelliği devreye alınırken, Master olması gereken cihazın Master rolünü devralmadan önce beklemesi gereken süre belirtilmelidir.
 - o Preemption özelliği devreye alınmadan önce VRRP Advertisement paketlerinin öğrenilme özelliğinin devreye alınması gerekiyor. Bu sayede Backup rolündeki routerlar Master rolündeki routerun VRRP Advertisement paketlerini gönderdiği aralığı öğrenecektir ve bu doğrultuda kendi aralıklarını Master routerdan öğrendiği aralıkla güncelleyecektir (Aksi takdirde yedeklenen bütün routerlar aynı anda Master rolü üstlenebilir).
 - Komuttan da anlaşılacağı üzere (komut sonunda “enable” değil de “disable” kullanılıyor. Gördüğüm kadarıyla varsayılanda devre dışı geldiğinde komut sonunda “enable” kullanılıyor) bu özellik varsayılanda devrede geliyor. İsteğe bağlı olarak “**vrrp timer advertise learning disable**” komutuyla devre dışı bırakılabilir.
 - Her ne kadar Huawei’in kendi sayfasında bu şekilde ifade edilse de ben “**undo vrrp timer advertise learning**” komutuyla bu özelliği devreye aldığım (komutu kullandığımda özellik varsayılanda devrede geldiği için herhangi bir değişim algılanmadı) her iki routerun da birbirinden bağımsız hareket ettiğini gördüm (her ikisi de Master rolüne sahip oldu. Master rolündeki routerun portunu kapattığımda Preemption özelliği devrede olmasına rağmen Master rolünü Backup rolündeki routera devretmediğini gördüm). Aşağıdaki görselde 1. VRRP grubuna dahil edilen iki router için sahip oldukları roller gösterilmiştir (Master router nerede ?) (<https://support.huawei.com/enterprise/en/doc/EDOC1100064352/ed1a4d3/vrrp-timer-advertise-learning-enable>).

[~CE6800-2-SW]display vrrp state-change interface GE 1/0/0 vrid 1				[~CE6800-3-SW-GE1/0/0]display vrrp state-change interface GE 1/0/0 vrid 1			
Time	SourceState	DestinationState	Reason	Time	SourceState	DestinationState	Reason
2024-03-30 08:54:09	Backup	Master	Protocol timer expired	2024-03-30 09:00:52	Initialize	Backup	Interface up
2024-03-30 08:53:44	Initialize	Backup	Interface up	2024-03-30 08:54:06	Master	Initialize	Interface down
2024-03-30 08:53:13	Master	Initialize	Interface down	2024-03-30 08:53:16	Backup	Master	Protocol timer expired
2024-03-30 08:51:23	Backup	Master	Protocol timer expired	2024-03-30 08:51:44	Initialize	Backup	Interface up
2024-03-30 08:51:04	Initialize	Backup	Interface up	2024-03-30 08:51:22	Master	Initialize	Interface down
2024-03-30 08:50:35	Master	Initialize	Interface down	2024-03-30 08:50:36	Backup	Master	Protocol timer expired
2024-03-30 08:49:27	Backup	Master	Protocol timer expired	2024-03-30 08:49:35	Initialize	Backup	Interface up
2024-03-30 08:49:23	Initialize	Backup	Interface up				

- İsteğe bağlı olarak VRRP konfigürasyonu uygulanan fiziksel portun arayüzü altında “**vrrp vrid <VRRP Group Id> timer advertise <Advertiesment Interval>**” komutuyla VRRP Advertisement paketlerinin gönderilme aralığı belirtilebilir (varsayılanda 1 saniye gelmektedir).
- İsteğe bağlı olarak cihaz geneline uygulanması için System-view arayüzü altında, arayüz bazlı uygulanması için ilgili fiziksel portun arayüzü altında “**vrrp recover-delay <Recovery Delay>**” komutuyla Master rolünün yedek cihaza aktarılmadan önce Up kalma süresinin kontrol edilmesi sağlanabilir.
 - Flap Link gibi bir problem yaşanması durumunda sürekli Master/Backup değişimi yaşanarak kesintilerin oluşmaması için Recovery Delay süresi ayarlanarak Master rolünü alacak cihazın bu komutla ayarlanan gecikme süresince Up kalıp kalmadığı kontrol edilir. Up olursa Master rolü devredilir.

```
[*CE6800-2-SW]int ge 1/0/0
[*CE6800-2-SW-GE1/0/0]undo portswitch
[*CE6800-2-SW-GE1/0/0]ip address 10.0.1.2 24
[*CE6800-2-SW-GE1/0/0]undo sh
[*CE6800-2-SW-GE1/0/0]quit
[*CE6800-2-SW]
[*CE6800-2-SW]int ge 1/0/0
[*CE6800-2-SW-GE1/0/0]vrrp vrid 1 virtual-ip 10.0.1.1
[*CE6800-2-SW-GE1/0/0]vrrp vrid 1 preempt timer delay 10
[*CE6800-2-SW-GE1/0/0]vrrp vrid 1 timer advertise 1
[*CE6800-2-SW-GE1/0/0]vrrp recover-delay 10
[*CE6800-2-SW-GE1/0/0]quit
```

- VRRP protokolünde güvenliği sağlamak amacıyla “**vrrp vrid <VRRP Group Id> authentication-mode { simple {plain <key> | cipher <Cipher Key>} | md5 <MD5 key>}**” komutuyla kimlik doğrulama mekanizması devreye alınabilir.

```
[*CE6800-2-SW]int ge 1/0/0
[*CE6800-2-SW-GE1/0/0]vrrp vrid 1 authentication-mode ?
md5      MD5 authentication mode
simple    Simple authentication mode

[*CE6800-2-SW-GE1/0/0]vrrp vrid 1 authentication-mode md5 ?
STRING<1-8>/<24>/<32>/<48>/<108> Plain text with length of 1-8, DES encrypted
                                     text with length of 24(only for
                                     compatibility with older versions), AES
                                     encrypted text with length of 32, 48 or 108

[*CE6800-2-SW-GE1/0/0]vrrp vrid 1 authentication-mode md5 Hua.123!
```

- Kullanılan VRRP versiyonu System-view modu altında “**vrrp version {v2 | v3}**” komutuyla belirlenebiliyor. Burada VRRP protokolü kullanılacak bütün cihazların aynı versiyona sahip olması gerektiği unutulmamalıdır.
 - Kullanılan cihaz destekliyorsa isteğe bağlı olarak VRRP Advertisement paketlerinin hangi VRRP versiyonuna göre gönderileceği belirlenebiliyor. Bu durumun cihaz genelinde ayarlanması için System-view modu altında “**vrrp version-3 send-packet-mode {v2-only | v3-only | v2v3-both}**” komutu kullanılırken, port bazında ayarlamak için fiziksel portun arayüzü altında “**vrrp vrid <VRRP Group Id> version-3 send-packet-mode {v2-only | v3-only | v2v3-both}**” komutunun kullanılması gerekiyor.

```
[~CE6800-2-SW]vrrp version ?
2 Specify the device to support V2 for VRRP(default is v2)
3 Specify the device to support V3 for VRRP
```

```
[*HUAWEI-GE1/0/0]vrrp vrid 1 compatible-version ?
2 Specify the device to send VRRP v2 advertisement packet only
3 Specify the device to send VRRP v3 advertisement packet only(default
  send-mode)
all Specify the device to send VRRP v2v3 advertisement packets both
```

| → Huawei CE6800 cihaz için kullanılan komut yukarıdaki gibidir. Bu komut fiziksel portun arayüzü altında kullanılabildiği gibi System-view modu altında cihaz geneline de uygulanabiliyor.

- Sanal ip adresine Ping atılabilmesi için (varsayılanda bu özellik kapalıysa) System-view modu altında “**undo vrrp virtual-ip disable**” komutuyla devreye alınabilir.

```
[~CE6800-2-SW]vrrp virtual-ip ?
ping          Specify the configuration of virtual IP address ping
route-advertise Route advertise
[~CE6800-2-SW]undo vrrp virtual-ip ping disable
```

- İsteğe bağlı olarak oluşturulan VRRP grubu ile **BFD Session** özelliği ilişkilendirilerek VRRP grubu içerisinde oluşan hataların tespit edilmesi ve bu doğrultuda aksiyon alınabilmesi sağlanabilir. Detaylı bilgi için https://support.huawei.com/enterprise/en/doc/EDOC1100269507/7aa6d9e7/vrrp-configuration#EN-US_TASK_0172361773 adresi ziyaret edilebilir.
- Her ne kadar günümüzde yaygın kullanılsa da router arayüzlerinde VLAN’ları internete çıkarabilmek için Sub-Interface tanımları oluşturulabiliyordu. VRRP protokolünde de yedeklenen fiziksel portların arayüzleri altında “**dot1q vrrp vid <VLAN Id>**” komutu kullanılarak tanımlanacak VLAN etiketinin oluşturulan grup içerisinde tanımlı sanal ip adresiyle eşleştirilmesi ve bu sayede VLAN trafiklerinin internete çıkarılması sağlanabiliyor.

Tracking

Yedeklenen routerlardan Master rolündeki routerun Gateway olarak hizmet verdiği arayüzünde erişim problemi olmasa da erişilmesi gereken bir kaynağa erişimi kesilmiş olabilir (internet ortamına veya herhangi bir sunucu olabilir). Bu durumda Master rolüne sahip olduğu sürece hizmet verdiği network erişmesi gereken kaynağa erişim sağlayamayacaktır. Bu gibi durumlarla karşı karşıya kalmamak için **Object Tracing** özelliğiyle erişilmesi istenen kaynağa erişim durumunun kontrol edilmesi gerekiyor. Hedef kaynağa erişim kesildiğinde Master rolündeki arayüzün Priority değerinin düşürülmesi sağlanarak Backup rolündeki routerun Priority değeri ön plana çıkması sağlanır ve Master rolünü devralması sağlanarak erişimin sürekliliği sağlanabiliyor. Object Tracing konfigürasyonu için ilgili arayüz altında VRRP konfigürasyonu yapıldıktan sonra “**vrrp vrid 1 track <Track Object> <Object Information> {increase | reduce} <Increase/Reduce Value>**” komutuyla Tracing edilecek kaynak ve bu kaynağa erişim kesildiğinde gerçekleşmesi istenen aksiyon belirtilmelidir.

- Bu konfigürasyonun doğru çalışabilmesi için Preemption özelliğini açmayı unutma! Aksi takdirde erişimi kesilen router Master rolünü Backup rolündeki router devretmeyecektir.

```
[~CE6800-2-SW-GE1/0/0]vrrp vrid 1 track ?
admin-vrrp   Specify configuration information of the administrator VRRP
bfd          Specify a BFD session
interface    Specify the interface
ip           Specify IP protocol
link-bfd     Specify link BFD
nqa         Specify NQA test class

[~CE6800-2-SW-GE1/0/0]vrrp vrid 1 track ip route ?
X.X.X.X      Specify prefix of the route

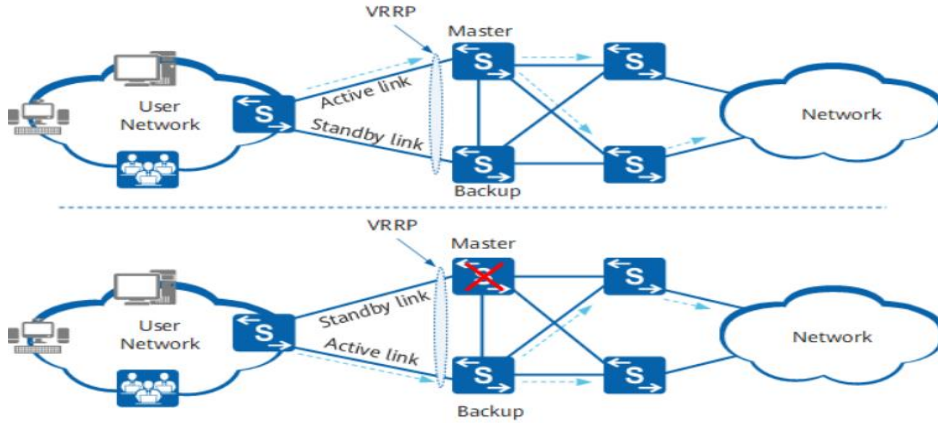
[~CE6800-2-SW-GE1/0/0]vrrp vrid 1 track ip route 10.0.0.10 32 ?
increase     Increased value of the VRRP backup group priority
reduce       Reduced value of the VRRP backup group priority
vpn-instance VPN instance
<cr>

[~CE6800-2-SW-GE1/0/0]vrrp vrid 1 track ip route 10.0.0.10 32 reduce ?
INTEGER<1-255> Reduced value of priority

[~CE6800-2-SW-GE1/0/0]vrrp vrid 1 track ip route 10.0.0.10 32 reduce 30
```

Backup-Forward

VRRP protokolü ile yedeklenen routerlar arasında Master router üzerinde bir problem olduğunda Backup routerun Master rolüne geçene kadarki süreçte gönderilen trafikler kaybedilecektir. Bu kaybın önüne geçebilmek adına her router üzerinde ilgili fiziksel portun arayüzü altında “**vrrp vrid <VRRP Group Id> backup-forward**” komutu kullanılarak routerlar arasındaki rol geçişinin tamamlanması beklemeden Backup rolündeki routerun hizmet trafiğini iletmesi sağlanır. Bu sayede yedeklenen routerlar arasındaki rol değişim sürecinde kaybedilen trafik miktarı en aza indirilmiş olur.



MVRRP (Multiple VRRP)

İki router arasında birden fazla network için VRRP konfigürasyonu yapılmış olabilir. Bu durumda her bir network için routerlardan ayrı ayrı VRRP Adversament paketi gönderilecek, dolayısıyla gereksiz yere bant genişliği kullanımına neden olacaktır. Bunun önüne geçebilmek için VRRP gruplarından birisini **mVRRP** olarak belirlemek gerekiyor. Belirlenen mVRRP grubuna iki router arasında tanımlı diğer VRRP gruplarının da dâhil edilmesi gerekiyor. Bu sayede her bir VRRP grubu için ayrı ayrı VRRP Adversament paketi göndermek yerine tek bir VRRP Adversament paketi içerisinde iki router arasında tanımlı bütün VRRP gruplarının bilgileri paylaşılmış oluyor. Konfigürasyonuna bakıldığında;

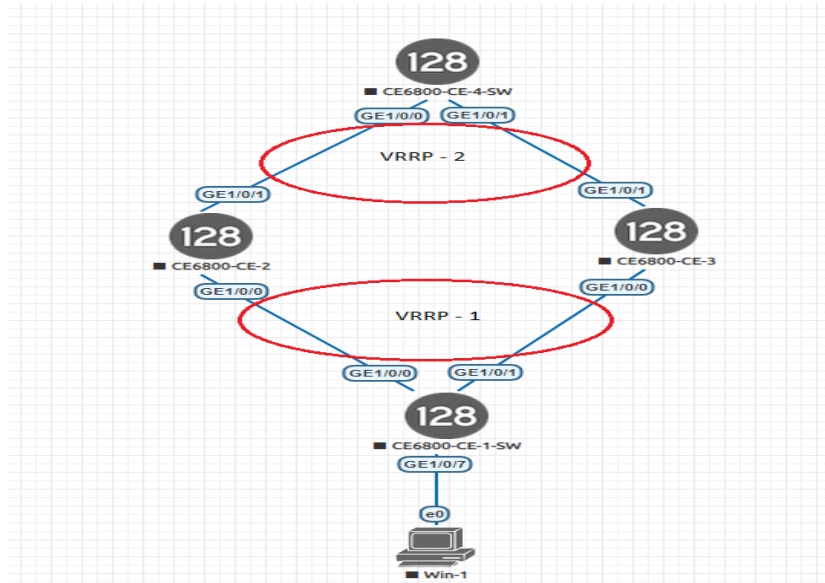
- İlk olarak iki router arasında kullanılan VRRP gruplarından birisi için fiziksel portlarının arayüzüne giriş yapılarak “**vrrp vrid <VRRP Group Id> admin [ignore-if-down]**” komutu kullanılarak mVRRP grubu oluşturulur.
 - o “**ignore-if-down**” parametresi VRRF gruplarından birisinde bir Master routerlar üzerinde bir problem yaşanması durumunda diğer VRRP gruplarında da kesintiye neden olmaması için kullanılıyor.
 - o Burada “**vrrp vrid <VRRP Group Id> holding-multiplier <Timer Value>**” komutuyla mVRRP grubu için bir başlatma durumu Hold Time süresi yapılandırılabilir.
- İki router arasındaki diğer VRRP gruplarını mVRRP grubuna dâhil etmek için ilgili fiziksel portların arayüzlerine giriş yapılarak “**vrrp vrid <VRRP Group Id - 1> track admin-vrrp interface <Interface Id> vrid <VRRP Group Id - 2> [unflowdown]**” komutunun kullanılması gerekiyor.
 - o *Unflowdown, Upstream ve Downstream yollarının aynı olmasının gerekmediği bir ağda kullanılır. Unflowdown, mVRRP grubunun bağlı VRRP grubunun durumlarını belirlemesine izin verecek şekilde yapılandırılabilir. Bu Upstream trafiğinin Master*

üzerinden geçerek Upper-Layer ağına ulaştığı ve Downstream trafiğinin Master veya Backup üzerinden geçerek kullanıcıya ulaştığı anlamına gelir.

```
[~CE6800-2-SW]int ge 1/0/0
[~CE6800-2-SW-GE1/0/0]undo portswitch
[~CE6800-2-SW-GE1/0/0]ip address 10.0.0.2 24
[~CE6800-2-SW-GE1/0/0]undo sh
[~CE6800-2-SW-GE1/0/0]quit
[~CE6800-2-SW]
[~CE6800-2-SW]int ge 1/0/1
[~CE6800-2-SW-GE1/0/1]undo portswitch
[~CE6800-2-SW-GE1/0/1]ip address 20.0.0.2 24
[~CE6800-2-SW-GE1/0/1]undo sh
[~CE6800-2-SW-GE1/0/1]quit
[~CE6800-2-SW]int ge 1/0/0
[~CE6800-2-SW-GE1/0/0]vrrp vrid 1 virtual-ip 10.0.0.1
[~CE6800-2-SW-GE1/0/0]vrrp vrid 1 preempt timer delay 10
[~CE6800-2-SW-GE1/0/0]vrrp vrid 1 admin ignore-if-down
[~CE6800-2-SW-GE1/0/0]vrrp vrid 1 holding-multiplier 3
[~CE6800-2-SW-GE1/0/0]quit
[~CE6800-2-SW]
[~CE6800-2-SW]int ge 1/0/1
[~CE6800-2-SW-GE1/0/1]vrrp vrid 2 virtual-ip 20.0.0.1
[~CE6800-2-SW-GE1/0/1]vrrp vrid 2 preempt timer delay 10
[~CE6800-2-SW-GE1/0/1]vrrp vrid 2 track admin-vrrp interface ge 1/0/0 vrid 1 unflowdown
[~CE6800-2-SW-GE1/0/1]quit
```

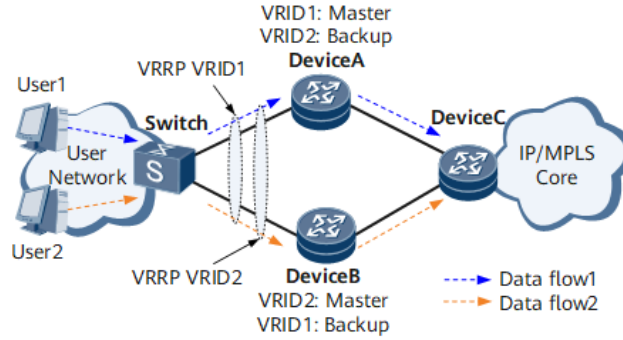
```
[~CE6800-2-SW]display vrrp interface ge 1/0/0
Type:
N: Normal
A: Administrator
M: Member
L: Load-Balance
LM: Load-Balance-Member
Total:1 Master:1 Backup:0 Non-active:0
VRID State Interface Type Virtual IP
-----
1 Master GE1/0/0 A 10.0.0.1
[~CE6800-2-SW]display vrrp interface ge 1/0/1
Type:
N: Normal
A: Administrator
M: Member
L: Load-Balance
LM: Load-Balance-Member
Total:1 Master:1 Backup:0 Non-active:0
VRID State Interface Type Virtual IP
-----
2 Master GE1/0/1 M 20.0.0.1
```

- Çıktıdan da görülebileceği gibi Wireshark ile network trafiği dinlendiğinde 2 numaralı VRRP Grubu için VRRP trafiği oluşmadığı gözlemlendi (bu süreçte kontrol ettim 2 numaralı VRRP grubu sorunsuzca çalışıyordu). Sadece 1 numaralı VRRP Grubu için VRRP Advertisement paketleri gönderiliyordu.



Notlar

- İki router arasında birden fazla VRRP grubu kullanıldığı durumda her bir VRRP grubu için farklı routerun Master seçilmesi sağlanarak bağlantılar arasında yük dengeleme işlemi yapılması sağlanabiliyor.



Terminolojiler

- VRRP Advertisement paketi**, bir VRRP grubundaki tüm Backup cihazlara Master cihazın önceliğini ve durumunu bildirmek için kullanılıyor.
- Bidirectional Forwarding Detection (BFD)** [RFC5880] (Çift Yönlü İletim Algılama), bir bağlantıyla bağlanan iki router veya switch arasındaki hataları algılamak için kullanılan bir network protokolüdür.

Kontrol Komutları

- display vrrp state-change interface vrid
- display vrrp binding
- display vrrp load-balance
- display vrrp protocol-information
- display vrrp bfd session
- display vrrp statistics
- display vrrp <Options>

Kaynaklar

- https://support.huawei.com/enterprise/en/doc/EDOC1100278760/7aa6d9e7/vrrp-configuration#EN-US_TASK_0172361749
- <https://support.huawei.com/enterprise/en/doc/EDOC1100008296/d979d919/vrrp-recover-delay>
- <https://support.huawei.com/enterprise/en/doc/EDOC1100262565/7bb81741/enabling-a-backup-device-to-forward-service-traffic>
- <https://support.huawei.com/enterprise/en/doc/EDOC1000178176/6a2a456/optional-enabling-the-backup-device-in-a-vrrp-backup-group-to-forward-traffic>
- <https://info.support.huawei.com/info-finder/encyclopedia/en/BFD.html>