

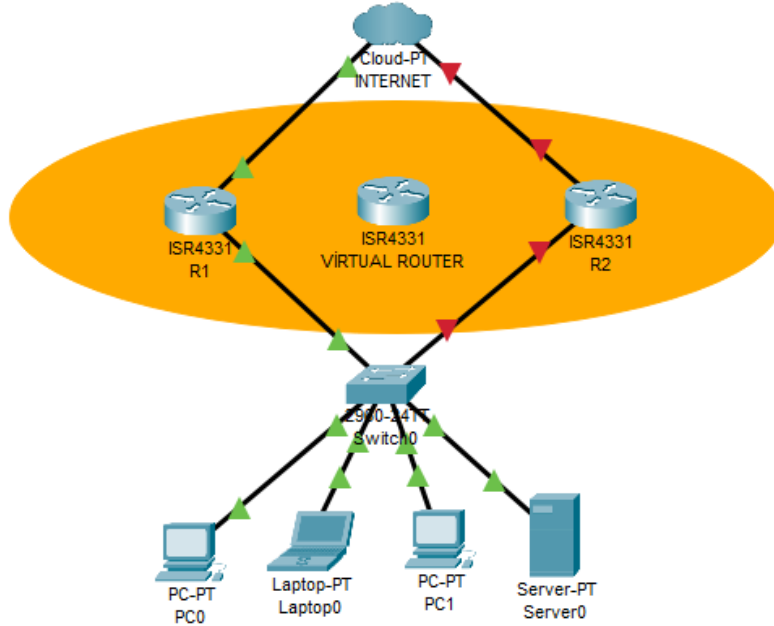
FHRP

FHRP (First Hop Redudancy Protocols), routerlarda yedeklilik sağlamak için kullanılan protokollerin genel adıdır.

Routerlarda yedeklilik sağlamak istendiğinde karşılaşılan ana problemlerden biri routerların networke bağlı arayüzlerinde gateway hizmeti vermesidir. Network içerisindeki istemcilerde normal şartlar altında sadece bir tane gateway adresi tanımlanabildiği için switchlerde olduğu gibi iki router arasına birden fazla kablo çekilerek routerlar arasında yedeklilik sağlanamıyor.

Routerlar arasında yedeklilik sağlayabilmek için çıkarılan protokollerin çalışma prensibine bakıldığında, yedeklenmek istenen routerlar arasında sanal bir ip ve MAC adresi oluşturuluyor. Bu tanımlamalardan sonra yedekleme yapılacak routerlar arasında belirli özelliklere bakılarak aralarından biri aktif router seçiliyor ve oluşturulan mantıksal ip ve MAC adreslerini aktif router üstlenerek hizmet vermeye başlıyor. Aktif router dışındaki routerlar ise Stand-By moduna geçerek kullanılmayı bekliyorlar. Aktif seçilen routerda bir sorun yaşandığında/kesinti olduğunda oluşturulan Stand-By modundaki routerlardan biri aktifliği alarak mantıksal ip ve MAC adreslerini (yine belirli özelliklere bakılarak karar veriliyor) üstleniyor ve hizmet vermeye başlıyor. Bu sayede routerlar arasında yedeklilik sağlanmış oluyor.

| → Oluşturulan sanal ip adresi aynı zamanda hizmet verilen networkteki istemcilerde gateway adresi olarak tanımlanıyor. Bu sayede aktif routerda bir problem olduğunda mantıksal MAC ve ip adreslerini farklı bir router üstlenerek hizmet vermeye devam ettiği için istemcilerde tanımlanan gateway adresinde herhangi bir değişim olmuyor.



IRDP Protokolü

IRDP (ICMP Router Discovery Protocol), routerlarda yedeklilik için çıkarılan ilk protokollerdendir. İstemcilerin kullandığı gateway ip adreslerine sürekli ICMP paketleri göndererek aktifliğini kontrol etmesine dayanan bir protokoldür. Bu protokol manipüle edilerek güvenlik zafiyetlerine neden olabiliyor. Günümüzde kullanılmamaktadır.

HSRP Protokolü

HSRP (Hot Standby Router Protocol), Cisco'ya özel protokolüdür. Çalışma prensibi olarak bir grup tanımlanır ve yedeklenmek istenen routerlar bu gruba dahil edilir. Bu grup numarası yedeklenecek routerlarda aynı olmak zorundadır çünkü bu grup numarasıyla mantıksal MAC adresi oluşturulmaktadır (Cisco'ya özel bir MAC adresinin sonuna grup numarası eklenerek mantıksal MAC adresi oluşuyor - 0000.0c07. acXX -> (grup numarasına göre XX -> 00 – FF arasında değer alıyor)). Bu nedenle yedeklenecek routerlara aynı grup numarası verilerek aynı sanal MAC adresine sahip olması sağlanır. Oluşturulan bu mantıksal MAC adresini kullanan routera aktif router, yedekte bekleyen routera Stand-By router denir.

| → HSRP'nin IPv6 için de desteği bulunmaktadır (HSRPv2).

| → HSRP protokolünde yedeklenen routerlar aralarında haberleşirken Multicast adresler (IPv4 -> 224.0.0.2 / IPv6 -> FF02::66) kullanılır. Aktif router 3 saniyede bir multicast adresine Hello paketleri göndererek ayakta olduğunu gösterir. Eğer ki 10 saniye boyunca aktif seçilen routerdan Hello paketi gelmezse Stand-By durumundaki router kendisini aktif router ilan ederek hizmet vermeye devam eder.

■ Burada verilen süreler varsayılanda kullanılan değerlerdir. Bu değerler değiştirilebilmektedir.

| → Haberleşirken routerların kurum (şirkete ait) routeru olduğunu doğrulamak için aralarında authentication mekanizması kullanır (Detaylı bilgi için https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-sy/fhrp-15-sy-book/fhrp-hsrp-md5.pdf).

| → HSRP protokolünde oluşturulan mantıksal ip adresi routerların fiziksel arayüzlerine verilen ip adreslerinden farklı olmak zorundadır.

HSRP Protokolünde Aktif Router Seçim Prensibi

- Öncelikle HSRP protokolünde Priority değerlerine bakılır. Priority değeri yüksek olan router aktif router seçilir. Varsayılanda bu her router için aynıdır (100).
- Priority değeri aynı olması durumunda routerların bağlı arayüzlerinden en büyük ip adresine sahip router aktif router seçilir.

HSRP Oluşum Adımları

- Initial State, HSRP devreye alındıktan sonra bağlantının devreye girdiği durumdur.
- Learn State, oluşturulan gruptaki cihazlar Hello paketleriyle birbirlerini tanır.
- Listen State, mantıksal ip adresi belirlenir ve gruptaki cihazlara bildirilir.
- Speaking State, hangi routerun aktif router olacağına karar verilir.
- Stand-By, aktif routerda bir sorun yaşandığında aktifliği alacak router adayı belirlenir.
- Active, aktif router seçilir ve gruptaki routerlara düzenli olarak Hello paketleri gönderir.

VRRP Protokolü

VRRP (Virtual Router Redudancy Protocol), HSRP protokolüne benzer prensipte çalışmaktadır. Open standart bir protokoldür.

| → VRRP protokolünde HSRP protokolüne karşılık oluşturulan mantıksal ip adresi fiziksel routerlara verilen ip adreslerinden farklı olmak zorunda değildir.

| → VRRP’de aktif routerdan Stand-By routera geçiş süresi varsayılanda HSRP’ye kıyasla çok daha kısadır.

GLBP Protokolü

GLBP (Gateway Load Balancing Protocol), Ciscoya özel bir protokoldür. GLBP protokolünü diğer protokollerden farklı kılan özellik ise yedeklenmek istenen routerlar arasında biri seçilip kullanılmıyor. Bunun yerine yedeklenmek istenen routerların hepsi aktif olarak kullanılmaktadır. Network trafiği yedeklenen routerlar arasında paylaştırılarak/dengelenerek gönderir. Bu protokole karşılık open standart bir protokol bulunmamaktadır.

Preemption

Preemption özelliğini bir örnek üzerinden açıklamak gerekirse, yedeklenmek istenen R1 ve R2 routerlarından R1’in aktif router seçilip mantıksal ip ve MAC adresleriyle hizmet vermeye başladıktan sonra bir problemle karşılaşıldığında aktiflik R2’ye geçecektir. R2 mantıksal ip ve MAC adresleriyle hizmet vermeye başladıktan sonra R1 ‘deki problem giderilip tekrar hizmet verebilir duruma geldiğinde aktifliğin kimde kalacağına karar vermek için kullanılan özelliktir. Preemption özelliği devrede ise R1 hizmet verebilir duruma geldiğinde aktifliği R2’den alarak hizmet vermeye devam edecektir. Preemption özelliği devrede değilse R1 hizmet verebilir duruma geldiğinde Stand-By duruma geçecek, aktiflik R2’de kalacaktır.

| → Aktifliğin routerlar arasında geçişinde kesintiler yaşanabiliyor. Bu nedenle Preemption özelliği devre dışı bırakılabilir.

| → Her ne kadar Preemption özelliğinin Stand-By durumdaki (aktifliği Priority değeri daha yüksek olan cihaza devredebilmesi için) cihazlarda açılması yeterli olsa da her ihtimale karşı yedeklenmek istenen cihazların tamamında açılması daha doğru olacaktır.


Konfigürasyonlar

- HSRP Konfigürasyonu

- İlk olarak yedeklenmek istenen routerların arayüzlerine girilerek ip adresleri tanımlanıyor.
- Kullanılmak istenen versiyona göre “**standby version <Version Number>**” komutuyla ayrıca HSRP versiyonu belirtilebiliyor. Varsayılanda HSRPv1’ de geliyor (Aynı gruba alınan routerların aynı HSRP versiyonunda çalışması gerekiyor).
- Bu tanımlamalardan sonra “**standby <Group Number> ip <Ip Address>**” komutuyla oluşturulan grup için (burada 1 numaralı grup) için mantıksal ip adresi tanımlanıyor (Burada tanımlanan sanal ip adresi aynı gruba dahil edilecek bütün routerlarda da aynı tanımlanmalıdır).
- İsteğe bağlı olarak herhangi bir routerda Priority değeri “**standby <Group Number> priority <Priority Number>**” komutuyla değiştirilerek aktif router seçimine müdahale edilebiliyor (Bu değer varsayılanda 100’dür).
- İsteğe bağlı olarak “**standby <Group Number> preempt**” komutuyla Preemption özelliği devreye alınabiliyor. Varsayılanda bu özellik kapalı geliyor. Preempt komutunu kullanırken dikkat edilmesi gereken nokta gruba dahil her routerda

tanımlanması gerekiyor. Aksi takdirde preemption özelliği devreye alınmayan routerlarda aktiflik durumu gereken routera devredilmeyecektir.

- Timer sürelerini özelleştirmek için “**standby <Group Number> timers <Seconds | msec Milliseconds> <Seconds | msec Milliseconds>**” komutu kullanılabiliyor (komuttaki ilk süre Hello paketi gönderme aralığı, ikinci süre ise aktif seçilen cihazdan Hello paketi gelmediğinde bir problem olduğunun anlaşılması için kullanılan tanımlamadır).
- Kimlik doğrulama mekanizması için “**standby <Group Number> authentication <Password | text Password | md5 key-chain Key-Chain | md5 key-strings Key-Strings>**” komutu kullanılabiliyor.
- Son olarak da yine “**no sh**” komutuyla port fiziksel olarak kullanıma açılıyor.

```
R1(config)#interface gi 0/0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#standby version 1
R1(config-if)#standby 1 ip 192.168.1.2  Virtual Ip Address
R1(config-if)#standby priority 150
R1(config-if)#standby 1 preempt
R1(config-if)#no sh
R1(config-if)#exit
```

- VRRP Konfigürasyonu

- VRRP konfigürasyonu ise HSRP konfigürasyonuna benzemektedir. Sadece “standby” komutu yerine “**vrrp**” komutu kullanılarak tanımlanıyor. Konfigürasyonu için <https://www.pearsonitcertification.com/articles/article.aspx?p=2141275> sayfasını inceleyebilirsiniz.

SORU : Routerlarda yedekleme yapılırken yedeklenmek istenen routerların fiziksel arayüzlerine ayrıca ip adresi atamadan da HSRP protokolü devreye alınabilir mi? (zaten mantıksal bir ip adres tanımlanıyor)

Bu şekilde çalışmıyor çünkü, routerların arayüzlerine ip adresleri verildiğinde yönlendirme tablolarında doğrudan bağlı network olarak görünüyor. Bu nedenle routerların fiziksel arayüzlerine ip adresleri vermeden doğrudan HSRP konfigürasyonu yapıldığında HSRP konfigürasyonu çalışıyor ama yönlendirme tablosunda networklere ait bilgiler bulunmadığı için haberleşme gerçekleştirilemiyor (Packet Tracer’da uygulaması yapıldı).

NOT :

- HSRP protokolünde mantıksal MAC adresi oluşturulurken HSRPv1’de son 2 hane değişiyor. HSRPv2’de ise son 3 hane değişmektedir.

Terminolojiler

- VSS (Virtual Switching System), Cisco cihazlar arasında bağlantı kurularak tek bir cihaz gibi görünmesini sağlayan teknolojidir. Birbirine fiziksel olarak yakın cihazlar arasında yedekleme yapabilmek için kullanılabiliyor.

| → Cihazlar arasında kurulan bağlantı koptuğunda cihazlar aralarında haberleşemedikleri için her iki cihaz da kendini aktif seçiyor ve Dual-Active denilen durum ortaya çıkıyor.

- Stacking, Cisco model switchlerde birden fazla cihazın birbirine bağlanarak tek bir cihaz gibi çalışabilmesini sağlayan özelliğe denilmektedir.
- Track özelliği, routerlarda çeşitli durumların kontrol ettirilebilmesini sağlayan bir özelliktir. Yedekleme yapılan routerlar arasında aktifliği alan routerun internete bağlantısı kesilebilir. Router halen aktif olduğu için aktifliği standby durumundaki routera vermeyecektir. Bu durumda hizmet verilen networkteki cihazlar internete çıkamayacaktır. Track özelliği ile routerların internete çıkıp çıkmadığı takip edilerek internete çıkamayan routerların öncelik değerlerinin belirli miktarda düşürülmesi sağlanabiliyor. Öncelik değeri düşürülen router ise aktifliği öncelik değeri yüksek olan/internete bağlantısı olan routera devredebiliyor. Bu sayede hizmet verilen networkteki istemciler internete çıkabiliyor.

Kontrol Komutları

- Sh standby
- Sh standby brief