Ip Services

Networklerde log tutulması (özellikle Throubleshooting sürecinde), belirli zaman dilimlerinde parola değişimi gibi çeşitli işlemler için konfigüre edilmiş daha birçok hizmetin sağlıklı çalışabilmesi için cihazlar arasında zaman senkronizasyonuna ihtiyaç duyulmaktadır. Bunu sağlayabilmek için de NTP sunucularından faydalanılmaktadır. NTP sunucuları, networkteki cihazların saat ve tarih bilgilerini senkronize etmek için kullanılan protokoldür. UDP 123. Portu kullanır. Zaman bilgisi merkezi bir NTP sunucusu üzerinden networkteki bütün cihazlara öğretilir. Bu süreçte cihazların kaynak cihaza (saat ve tarih bilgisi sağlayan ana cihaz) olan uzaklığı/Stratum değeri önemlidir. Saat bilgisini veren cihaz kaynak cihaza ne kadar uzaksa ana kaynak ile arasındaki zaman kayması da o denli büyük olacaktır (ms'ler mertebesinde) (**Detaylı bilgi için CCNA - 3.08 - Network Management notlarını inceleyebilirsin**). Bu nedenle yedekli NTP sunucusu tanımlarında (zaman bilgisi almak için birden fazla NTP sunucusu tanımladığında) öncelik her zaman Stratum değeri düşük olan kaynaktan alınan bilgiler kullanılmaktadır.

- NTP protokolü konfigürasyonu için Global konfigürasyon moduna girilerek "**ntp server <Server Ip Address>"** komutuyla NTP sunucusunun ip adresi tanımlanıyor (Bir cihazda birden fazla NTP server tanımı yapılabiliyor) (Komut sonuna "**prefer**" anahtar kelimesi eklenerek tanımlı ip adresinden/NTP sunucusundan gelen zaman bilgisinin öncelikli olarak tetcih edilmesi de sağlanabiliyor).

- Networkte kullanılan bir cihazı NTP sunucusu yapabilmek için Global konfigürasyon modunda "**ntp master <Stratum Value>**" komutu kullanılıyor.

- Cihazlara NTP sunucuları tanımlanmasına rağmen bu sunucularda bir kesinti yaşanması durumunda zaman bilgisini başka bir NTP istemci cihazından alması isteniyorsa (yani hem NTP sunuculuğu hem de NTP istemciliği yapılmasıı isteniyorsa) "**ntp peer <Ip Address>**" komutuyla zaman bilgisini öğrenmesi istenen cihazın ip adresi tanımlanıyor (yani cihazların NTP sunucusuna bağğlantıları kesindiğinde zaman bilgisini tanımlanan Peer cihazından öğrenmesi sağlanıyor).

  |→ Bunun yerine cihazlarda doğrudan ikinci bir NTP server tanımı daha eklenebilir.

- NTP protokolünde kimlik denetimi yapılmak isteniyorsa (Daha fazlası için https[:]// www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/ntp.html - https[:]//www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/fundamentals/cisco_mds9000_fundamentals_config_guide_8x/configuring_ntp.pdf adresini ziyaret edebilirsin)

Zaman damgasında mili saniyelik/nano saniyelik zaman kaymalarının dahi önemli olduğu bir networkte ise zaman bilgilerini senkronize etmek için NTP protokolü yerine **PTP (Precision Time Protocol)** protokolü kullanılmaktadır.

FHRP (First Hop Redudancy Protocol)

FHRP, L3' de yedeklilik sağlamak için kullanılan protokollere verilen genel isimdir. L3' de yedeklilik sağlama sürecinde yaşanılan sorun routerların/L3 switchlerin LAN'lara bakan arayüzlerinde Gateway hizmeti veriyor olmalarıydı. LAN içerisinde istemcilere Gateway adresi olarak tek bir adres girilebildiği için yedeklenecek cihazlar aktif duruma geçtiğinde aynı ip adresini kullanmaları gerekiyordu. Bunun için bir tür sanal adresler (Ip ve MAC adresi) tanımıyordu. Aktifliği alan/kullanılan cihaz oluşturulan sanal adres tanımlarını üstlenerek hizmet vermeye başlıyordu (Bu süreçte

yedeklenen diğer cihazlar Stand-By moduna alınıyor). Bu sayede yedeklenecek routerlar değişse de istemcilerde tanımlanan ip bilgilerinde herhangi bir değişiklik yapılmasına gerek kalmıyor (**Detaylar için CCNA - 2.09 – FHRP notlarını inceleyebilirsin**). Bu protokollerden birkaçına bakıldığında;

- **HSRP** (Hot Standby Router Protocol), Cisco'ya özel bir protokoldür. HSRP devreye alındığında yedekli cihazlar aralarında iletişime geçerek birinin aktif router seçilmesi sağlanıyor ve oluşturulan sanal adresleri üstlenerek hizmet vermeye başlar (diğer routerlar Stand-by moduna geçer). Aktif router hizmet vermeye devam ettiği sürece Stand-by modundaki cihazlarla iletişim kurmaya devam eder (Belirli aralıklarda Hello paketi gönderir). Aktif routerdan bilgi alınamadığı durumda Aktif durumundaki routerda bir problem olduğu anlaşılarak Stand-by modundaki routerlardan biri aktifliği üzerine alır ve hizmet vermeye başlar (Aktif seçilen routerun hizmet vermediğinin anlaşılıp Stand-by modundaki routerlardan birine geçmesi HSRPv1 için yaklaşık 10 saniye sürerken HSRPv2 için milisaniyeler (Hello Time = 250 ms, Hold Time = 750ms'ye kadar düşürülebiliyor) mertebesine kadar düşürülmüştür.

  HSPR protokolünün diğer yedeklilik protokollerinden farkına bakıldığında;

  - Routerlar 224.0.0.2 Multicast adresini kullanarak aralarında haberleşirler.
  - Varsayılanda 3 saniye aralıklarla Hello paketleri gönderilir, 10 saniye boyunca Hello paketi alınamzsa Standby modundaki routerlardan biri sanal adresleri üzerine alarak hizmet veremye başlar.
  - Yedeklenecek router arayüzlerine verilen ip adresleri ile oluşturulan sanal ip adresi farklı olmak zorundadır (Yani tanımlanan sanal ip adresi, yedeklenecek routerların arayüzlerinde tanımlanan ip adeslerinden birisiyle aynı olamaz). Bu durum fazladan ip kullanılmasına neden olmaktadır. Sınırlı ip adresine sahip networkler için problem olabilir (örneğin /30 prefix uzunluğuna sahip bir network).
  - Routerlar arasında iletişim sürecinde Authentication özelliği vardır (MD5 kullanılıyor).
  - Toplamda 16 grup oluşturulabiliyor.

- **VRRP** (Virtual Router Reduddancy Protocol), Open Standart bir protokoldür. HSRP protokolünde routerlar Aktif ve Standby olarak isimlendirilirken VRRP'de Master ve Backup olarak isimlendiriliyor. Genelde network üzerindeki kesintilerin hassas olduğu yerlerde Timer süreleri (Hello time ve Hold time) için tercih edilmektedir.

  VRRP protokolünün diğer yedeklilik protokollerinden farkına bakıldığında;

  - HSRP protokolünden farklı olarak VRRP'de sanal ip adresi yedeklenecek routerların arayüzlerine verilen ip adreslerinden biriyle aynı olabilir (yedekleme sürecinde bir tür ip tasarrufu sağlıyor).
  - Routerlar ise aralarına 224.0.0.18 Multicast adresini kullanarak haberleşir.
  - Varsayılanda 1 saniye aralıklarla Hello paketleri gönderilir, 3 saniye boyunca Hello paketi alınmadığı taktirde Aktif routerun hizmet veremediği anlaşılarak Backup routerlardan biri Master seçilir ve sanal adresleri üzerine alarak hizmet vermeye başlar.
  - Routerlar arasında iletişim sürecinde Authentication (kimlik denetimi) özelliği bulunmamaktadır bBazı Cisco model switchlerde bulunmaktadır ama VRRP protokolünün genelinde yoktur). Bu durumda saldırgan routerlarla komşuluk kurup

Priority değerini yüksek göstererek kendisini Aktif router seçtirebilir ve bunun üzerinden çeşitli saldırılar gerçekleştirebilir.

- HSRP de varsayılanda Preemption özelliği kapalıyken VRRP de bu özellik varsayılanda açık gelmektedir.
- Toplamda 256 grup oluşturulabiliyor.

- **GLBP** (Gateway Load Balancing Protocol), diğer FHRP protokollerinden farklı kılan nokta yedeklenen routerların her ikisi de aktif kullanılarak arasında yük dengeleme işlemi yapıyor olmasıdır (Felsefe olarak switchlerdeki EtherChannel teknolojisine benzetilebilir. Bu işlemin benzeri HSRP veya FRRP protokollerinde farklı VLAN'ların farklı routerları aktif seçmesi sağlanarak bir noktaya kadar dengeleme yaptırılabilse de aynı VLAN içerisinde yük dengeleme işlemi yapılamamaktadır).
  - GLBP protokolünde aktif ve Standby router yerine **AVG** (Active Virtual Gateway) ve **AVF** (Active Virtual Forwarder) rolleri bulunmaktadır.
  - GLBP protokolü ile yedeklenen routerların hepsi çalıştığı için tanımlanan sanal ip adesini aynı anda kullanıyor ama farklı sanal MAC adreslerine sahip oluyorlar. Bu durumda istemciler bir ARP sorgusu yaptığında tek bir MAC adresiyle cevap verilebilmesi için AVG router seçiliyor. Seçim süreci ise yine Priority değeri veya arayüzlerine tanımlanan ip adreslerini büyüklüğü göz önünde bulundurularak yapılıyor.
  - Load Balancing işlemi ise varsayılanda Round Robin adı verilen teknik kullanılarak gerçekleştiriliyor.
    - Round Robin yönteminde gönderilen paketler eşit sırada routerlara dağıtılması sağlanıyor. Bu özellik ayrıca devreye alınmak istendiğinde "**glbp <Group Number> round-robin**" komutu kullanılıyor.
    - Yedeklenen routerlar arasında biri daha yüksek özelliklere sahip ise her 3 paketin ikisini bu Router gönderilmesi için ilgili routerun arayüzüne girilerek "**glbp <Group Number> weighted <Weighted>**" komutuyla Weighted tanımı yapılabiliyor.
    - Aynı cihazdan çıkan paketlerin aynı router üzerinden gönderilmesi isteniyorsa "**glbp <Group Number> host-dependet**" komutuyla Host Dependet özelliği devreye alınabilir.
  - AVG router belirleme sürecinde Preemprion özelliği açılabiliyor. Bu durumda AVG seçilen routerun aktif olduğu sürece AVG router olarak hizmet vermeye devam etmesi sağlanabiliyor (varsayılanda kapalı geliyor).
  - Konfigürasyonu HSRP ve VRRP protokolleri ile aynı. Sadece anahtar kelime olarak HSRP veya VRRP erine GLBP kullanılıyor.

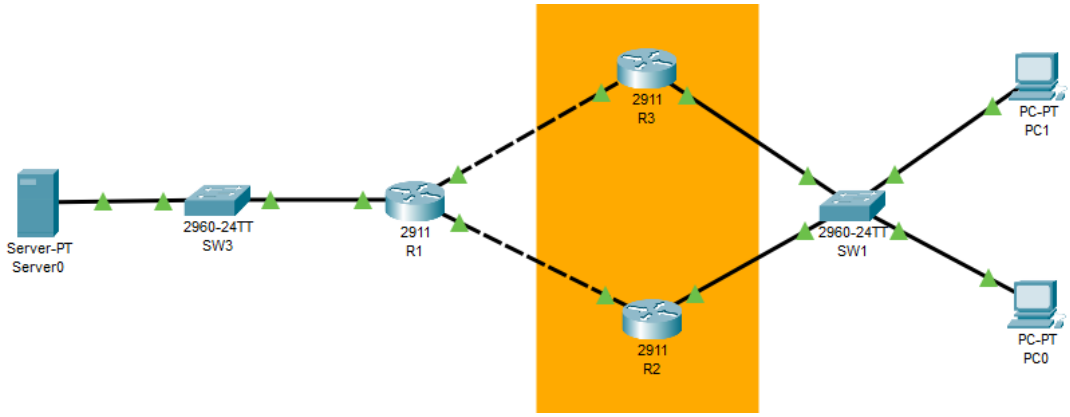
Object Tracking

Object Tracking, network cihazları üzerinde çeşitli durumların daimi olarak kontrol edilmesini sağlayan özelliktir (network arayüzlerinin durumları). Bu kontrol sürecinde olumlu bir durum varsa

True, olumsuz bir durum varsa False değeri döndürür. Bu sayede kontrol edilen kaynak üzerinde olumlu veya olumsuz durum değişikliklerine göre gerçekleştirilmesi istenen işlemler tanımlanabiliyor.

Object Tracking özelliğini aşağıdaki örnek görsel üzerinden açıklamak gerekirse;

- Topolojide PC0 ve PC1'in Server0'a erişiminin kesilmemesi isteniyor. HSRP protokolü kullanılarak aralarında yedeklenen R2 ve R3 cihazları arasında ise aktifliği R2'nin alıp tanımlanan sanal ip ve MAC adresleriyle hizmet vermeye başladığını düşünelim.
- R2'nin R1'e erişimi kesildiğinde PC0 ve PC1'in Server0'a erişimleri de kesilecektir. Bu durumda R2, R1'e erişimini yeniden kazanmadığı sürece aktiflik R2'de kalacağı için (aktiflik R3'e geçmediği sürece) kesinti devam edecektir. Bu gibi durumlarda aktifliğin R3'e geçmesi için Object Tracing özelliğinden yararlanılıyor.
- Object Tracing özelliği ile R2'nin R1'e olan bağlantısının kontrol edilmesi sağlanıyor. Oluşabilecek herhangi bir kesinti sonucu R2'nin Priority değeri düşürülerek (R3'ün Priority değerinden daha düşük olacak şekilde) R3'ün aktifliği alması sağlanıyor. Bu sayede R3 aktifliği alarak hizmet vermeye başlıyor ve istemcilerin Server0'a erişebilmesi sağlanıyor.



Konfigürasyonuna bakıldığında; (KONFİGÜRASYONA EN SON TEKRAR BAKILACAK-ÇALIŞMADI–48.43)

- İlk olarak Global konfigürasyon modunda "**track <Track Number> (interface interface-id (line-protocol | ip routing} | ip route ip-address/prefix-length (metric threshold | reachability) | list (boolean (and | or)) | (threshold (weight | percentage)))**" komutuyla izlenmesi istenen arayüz ve izlenmek istenen özellik tanımlanır.
- Track tanımı yapıldıktan sonra "**standby <Standby Group Number> track <Track Number> decrement <Decrement Value>**" komutuyla tanımlı Track değeri ifade edilerek Öündüreceği değer doğrultusunda (True - False) yapılması istenen komutlar tanımlanır (Görselde erişimi kesilen arayüzün Priority değeri düşürülüyor. Arayüz devreya alındığında router eski Priority değerini geri kazanıyor ve Preemption özelliği de açıksa aktifliği alarak hizmet vermeye devam ediyor).

  Aynı komutlar üzerinde "**Standby**" yerine "**vrrp**" yazarak Object Track özelliği devreye alınabilir (HSRP protokolünde nesne ve arayüz takibi yapılabilirken VRRP protokolünde sadece nesne takibi yapılabiliyor).

NAT (Network Address Translation)

Günümüzde daha çok Ipv4 adreslerin daha tasarruflu kullanılmasını sağlamak için kullanılan bir teknolojidir (bunun dışında aynı ip bloğunu kullanan networklerin haberleştirilmesi gerektiğinde ip çakışmasını önlemek için de kullanılabiliyor). Private - Public ip adres dönüşümü gerçekleştirir. Bu sayede kurum içinde kullanılan (hatta günümüzde çoğu zaman ev kullanıcılarına da veriliyor) Private ip adreslerini Public ip adreslerine dönüştürerek cihazların internete çıkmasını sağlıyor. Bu işlemin olumlu yönleri olduğu gibi (ip tasarrufu, güvenlik gibi) olumsuz tarafları da (İnternete dönük hizmet verememe, adres dönüşüm sürecinde yaşanan gecikmeler gibi) bulunmaktadır. Private ip adres aralığına bakıldığında;

```
10.0.0.0/8
100.64.0.0/10
172.16.0.0/12
192.168.0.0/16
```

NAT teknolojisinde ip dönüşümü için Inside Local, Inside Global, Outside Local ve Outside Global ip adres tanımları bulunmaktadır. Bunlar;

- **Inside Local address** - > Kaynak cihazın kullandığı Private ip adrestir.
- **Inside Global address** - > Kaynak cihazın internete çıkmak için kullandığı Global ip adrestir.
- **Outside Local addres** -> Hedef cihazın kullandığı Local adres adrestir
- **Outside Global address** -> Hedef cihazın kullandığı Global ip adresidir.

Üç farklı NAT tipi vardır (Detaylar için **CCNA-3.04-NAT** notlarını inceleyebilirsin);

- Static NAT, bir Private ip adresinin manuel olarak bir Public ip adresiyle eşleştirildiği NAT yöntemidir. Bu konfigürasyon sonunda cihaz üzerinde Ip NAT Translations tablosuna bu kayıt eklenir. Bu kayıt sayedinde bu cihaza internet üzerinden herhangi bir istemci erişebilir. Erişim sağlayan istemcilerin kayıtları da Ip NAT Translation tablosunda tutulmaya devam eder.
    - Bu kullanım şeklinde her Public ip adresi bir Private ip adresiyle eşleştirilebildiği için ip tasarrufu sağlanmıyor.
- Dynamic NAT (Pooled), cihaz üzerinde içerisinde Public ip adresleri bulunan bir NAT havuzu belirlenir. İnternete çıkmak isteyen istemciler bu havuzda kullanılmayan bir Public ip adresiyle eşleştirilerek internete çıkarılır. Public ip adresi ile işi bitiğinde ip adresi NAT havuzuna tekrar bırakılır. Bu süreçte aynı anda sadece NAT havuzundaki Public ip adres sayısı kadar istemci internete çıkarılabiliyor. Yani yeni bir istemci internete çıkmak istediğinde NAT havuzunda kullanılmayan ip adresi kalmamışsa internete çıkarılamıyor.

```
RX(config)#ip nat inside source static 192.168.20.5 209.162.160.4
RX(config)#int gi 0/0
RX(config-if)#ip address 192.168.20.1 255.255.255.0
RX(config-if)#no sh
RX(config-if)#ip nat inside
RX(config-if)#exit
RX(config)#int gi 0/1
RX(config-if)#ip address 209.162.160.4 255.255.255.192
RX(config-if)#no sh
RX(config-if)#ip nat outside
RX(config-if)#exit
```

- Ip adresleri istemcilere dinamik olarak verildiği için internet üzerinden bağlantı kurmak isteyen kullanıcıların istekleri reddediliyor.
- İşleyişinden de anlaşılacağı gibi bu haliyle de ip tasarrufu sağlamıyor.
- Komut sonunda Subnet bilgisi tanımlanmasının nedeni Public ip adres aralığının başlangıç ve bitiş değerlerini belirtirken Network ve Broadcast adresleri de dahil edilerek yazıldığında cihazın Subnet bilgisinden bunu belirlemesi ve bu adresleri kullanmaması için tanımlanıyor.

```
RX(config)#ip nat pool NAT_POOL 209.155.159.226 209.155.159.240 netmask 255.255.255.224
RX(config)#access-list 10 permit 192.168.10.0 0.0.0.255
RX(config)#ip nat inside source list 10 pool NAT POOL
RX(config)#int gi 0/0
RX(config-if)#ip nat inside
RX(config-if)#exit
RX(config)#int gi 0/1
RX(config-if)#ip nat outside
RX(config-if)#exit
```

- PAT (Port Address Translation), tek bir Public ip adresiyle birçok Private ip adresine sahip cihazı internete çıkarabilmeyi sağlayan yöntemdir. Bunu internete çıkmak isteyen istemcileri kaynak port adreslerini göz önünde bulundurarak gerçekleştiriliyor. İnternete çıkmak isteyen istemcinin eşleştirildiği Public ip adres ve kaynak port numarasını NAT tablosuna kaydediyor (Tek bir Public ip adresi kullanılması durumunda aynı kaynak port numarasıyla internete çıkarılacak iki paket gönderildiğinde paketlerden birinin kaynak port numarası değiştirilerek kaydediliyor ki hedeflerden gelen paketler ayırt edilebilsin. Hedef cihazdan gönderilen dönüş paketi NAT tablosuna ulaştığında port numarası da eski değeriyle değiştirilerek ilgili cihaza gönderiliyor). Hedeften dönen paket içerisinde eşleştirilen Public ip adresi ve kaynak port numarası hedef olarak tanımlandığı için hedeften gönderilen paket NAT tablosuna ulaştığında hedef ip ve port numarasına bakılarak isteğin gönderildiği Private ip adresi tespit ediliyor ve ip adres dönüşümü yapılarak network içersindeki ilgili cihaza yönlendiriliyor.

```
RX(config)#access-list 10 permit 192.168.20.0 0.0.0.255
RX(config)#ip nat inside source list 10 interface GigabitEthernet 0/1 overload
RX(config)#int gi 0/0
RX(config-if)#ip nat inside
RX(config-if)#exit
RX(config)#int gi 0/1
RX(config-if)#ip nat outside
RX(config-if)#exit
```

- Konfigürasyonunda Dynamic NAT konfigürasyonunda farklı olarak Ip NAT tanımının sonuna “**overload**” anahtar kelimesi ekleniyor.
- NAT tablosundaki kayıtlar network içerisinden bir talep olduğunda oluşturulduğu için internet üzerinden gönderilen bağlantı talepleri reddedilecektir. Bu durum bir noktaya kadar güvenlik sağlamaktadır.
- Tek bir Public ip adresiyle birçok Private ip adresine sahip cihaz internete çıkarılabildiği için ip tasarrufu da sağlanmaktadır.

NOTLAR

- Public NTP sunucuları da bulunuyor. Bu sunucular üzerinden de saat güncellemeleri yapılabiliyor.
- VRRP veya HSRP konfigürasyonunda komutları ayrı ayrı yazmak yerine "**(standby | vrrp) <HSRP/VRRP Group Number> address family (ipv4 | ipv6)**" komutuyla konfigürasyon arayüzüne girip komut başına hsrp veya vrrp kelimelerini eklemeden doğrudan konfigürasyon yapılabiliyor.
- Kurum içeridinde Private ip adresleri kullanılabildiği gibi Public ip adresleri de kullanılabilir. Ancak bu durumda kullanılan Public ip adresine sahip sayfalara internet üzerinde erişim sağlanamaz çünkü, kurum içerisinden bu ip adreslerine bir istek gönderildiğinde hedef cihaz kurum içerisinde görüneceği için paket internete çıkarılmayacaktır.
- NAT tablosundaki kayıtlar "**clear ip nat translations {*|<Ip Address>**" komutu kullanılarak belirli ip adresleri veya tablonun tamamı silinebiliyor (RAM üzerinde yer kaplıyor).
- Bir durum oluşması durumunda kullanıcı takibinin yapılabilmesi için NAT tablosunun kayıtlarının tutulması çok önemlidir.

Kontrol Komutları

- sh ntp status
- sh standby brief
- sh track <Track Number>