

IP Routing Essentials

Routerların ilk ve en önemli görevi kendisine gönderilen ip paketleri hedef networküne ulaştırmak için en uygun yolun tespit edip yönlendirmesidir. Bu işlem için routerlar yönlendirme tablolarını kullanıyor. Yönlendirme tablolarında tanımlanan/öğrenilen adresler göz önüne bulundurularak paketlerin hangi arayüzlerinden yönlendirileceğine karar veriliyor.

Yönlendirme tablosunda routerlara doğrudan bağlı networkler için adres tanımları kendiliğinden oluşturulurken Remote networkler için Static veya Dynamic olarak rota tanımı yapılması gerekiyor.

- Static routing, network yöneticisinin routerlarda her network için ayrı ayrı manuel rota tanımı yapmasıdır.
- Dynamic routing, routerlar öğrendikleri network bilgilerini birbirleriyle paylaşarak en iyi rotayı tespit etmeye çalışmasıdır. Bu süreçte toplanan bilgiler belirli algoritmalara tabi tutularak hedef networkler için kullanılacak en iyi rotalar hesaplanıp yönlendirme tablosuna işlenir. Bu işlem için kullanılan protokollere bakıldığında;
 - o RIPv2 – EIGRP – OSPF – IS-IS – BGP

Dinamik yönlendirme protokolleri kullandıkları algoritmalara göre iki gruba ayrılıyorlar. Bu algoritmalar Distance Vector ve Link-State algoritmalarıdır.

- **Distance Vector**, topolojideki her router öğrendiği network bilgilerini ve bu networklere ulaşmak için kullandığı en kısa rotaların Distance Vector değerlerini komşu routerlarla paylaşır (Yani routing konusunda komşu routerlardan alınan bilgilere güveniliyor). Komşu router ise aldığı routing bilgileriyle kendisine en uygun rotaları tespit ederek yönlendirme tablosunu düzenler.
 - o Normalde routerlar komşu routerlardan öğrendikleri rota bilgilerine bağlı oldukları için Loop oluşma ihtimali vardır. Koruma mekanizmaları sayesinde Loop oluşumunun önüne geçilebilmektedir (Bu koruma mekanizmaları çalışma hızını düşürüyor).
 - o RIPv2, EIGRP, BGP, Distance Vector algoritmasını kullanan protokollerdir.
- **Link-State**, her router tüm topoloji haritasını çıkarır. Bu haritayı her router kendisine bağlanan networklere ait link bilgilerini içeren bir paket oluşturur ve bunu (OSPF -> Link-State Advertisement (LSAs) , IS-IS -> Link-State Packets (LSPs) kullanılıyor) topolojideki her routerla paylaşır. Alınan bu paketler toplanarak her routerda Topology Table (Link-State Database içerisinde) adında bir tablo oluşturulur. Oluşturulan Topology Table kullanılarak her router kendi üzerinde belirli algoritmalar (SPF – Dijkstra Algorithm) çalıştırır. Bu algoritmalar sonucunda her router, networklere ulaşmak için kendisine en uygun/en iyi rotaları tespit eder ve bu rotaları yönlendirme tablosuna işler (Detaylar için **CCNA - 3.01-3.02 – OSPF** notlarına göz atabilirsiniz).
 - o Günün sonunda her ne kadar her routerda Topology Table tablosu aynı olsa da her router networkler için kullanacağı rotaları kendisi hesapladığı için yönlendirme tabloları farklı oluyor.
 - o Her router, topolojideki network için rota hesabını kendisi yaptığı için Loop-Free bir yapı ortaya çıkıyor.
 - o OSPF, IS-IS Link-State algoritmasını kullanan protokollerdir.

Enhanced Distance Vector Algoritması

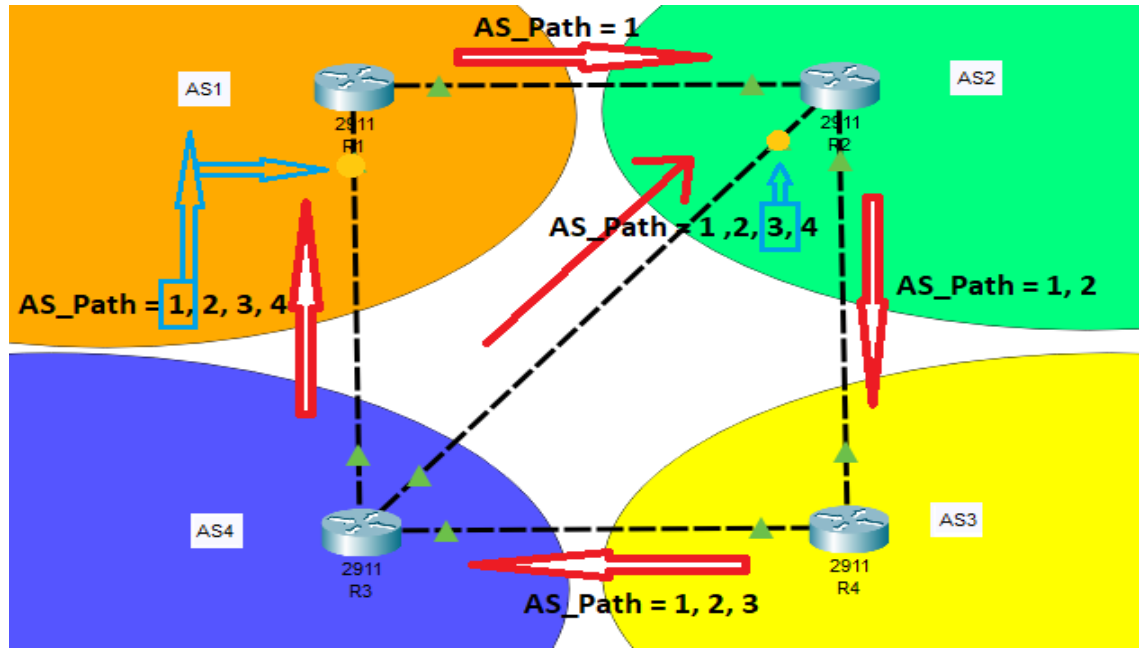
Enhanced Distance Vector Algorithm, Cisco'nun dinamik yönlendirme protokollünde (EIGRP) kullandığı algoritmadır. Distance Vector algoritmasını temel almaktadır. Üzerinde geliştirmeler yapılmıştır. Bu geliştirmelere bakıldığında;

- Rapid Convergence Time, topolojideki değişimleri bütün routerların çok daha hızlı öğrenebilmesi sağlanıyor.
- Distance Vector temelli protokollerde normalde belirli sıklıklarda komşu routerlardan güncelleme paketleri gönderilirken Enhanced Distance Vector algoritmasında sadece topolojide bir değişiklik meydana geldiğinde güncelleme paketleri gönderiliyor.
- Komşu routerlar ile komşuluk kurma süreci getirilmiştir (OSPF algoritmasında gibi).
- En iyi rota seçimi yapılırken metrik olarak tek bir özellik (bandwidth) kullanmak yerine birçok özellik değerlendirilerek (bandwidth, delay, reliability, load, MTU size ...) karar veriliyor.

BGP ve Path Vector Algoritması

BGP, temelde Path Vector Algoritmasını kullanır. Path Vector algoritması da felsefe olarak Distance Vector algoritmasına benziyor (Path Vector algoritmasında güncellemeler komşu router yerine komşu AS'dan alınıyor).

- BGP protokolünde en iyi rota seçimi Attribute (autonomous system path – AS_Path , multi-exit discriminator - MED, next hop, local preference, atomic aggregate, aggregator) değerlerine bakılarak karar verilir.
- Diğer protokollere kıyasla en yavaş çalışan protokoldür. BGP protokolünde asıl özelliği loop-free ve stabil bir routing protokolü olmasıdır. Nedeni çok büyük routing tablosuna sahip olabiliyor (dünya genelinde networkleri yönlendirebilmek için kullanılıyor. Dünya genelinde kullanılan networklerin hepsini routing tablosunda bulunduruyor. Yani BGP çalıştırılan bir router dünyadaki bütün networkleri öğrenebiliyor). Doğal olarak bu kadar network bilgisi arasından en iyi rotayı hesaplamak zaman alıyor (Bu yavaşlığın nedenleri arasında en iyi rota seçimi için uyguladığı karar verme mekanizmasının da etkisi var).
 - o BGP Protokolünde Loop-Free mekanizmasının çalışma prensibine bakıldığında; AS'ler arasında rota bilgileri paylaşılırken paket içerisinde AS_Path adında bir Attribute değişkeni tutuluyor. Bu sayede her rota bilgisi AS'lere öğretilirken, geçtiği her routerun dahil olduğu AS numarası depolanıyor. Bu sayede paketin yol boyunca üzerinde geçtiği her AS bilgisi kayıt altına alınıyor. Paketin daha önce kayıt altına aldığı bir routerdan tekrar geçirildiği görülürse burada loop oluştuğu anlaşılabilir ve bağlantı bloklanıyor.
 - o Bunu aşağıdaki görsel üzerinde açıklamak gerekirse, R1'den R2'ye güncellemeler gönderilirken AS_Path değerine R1'in bulunduğu AS değeri ekleniyor. R2'den R3'e güncellemeler gönderilirken AS_Path değerine R2'nin bulunduğu AS değeri de ekleniyor. Son durumda R4 komşusu olan R1'e güncellemeler gönderildiğinde ise R1 AS_Path içerisinde kendi (R1'in) AS değerinin olduğunu görüyor ve loop oluşturmaması için R4 ile arasındaki bağlantıyı bloklanıyor (Detaylar için **CCNP – 05 – EIGRP** notlarını inceleyebilirsiniz). Bnezer şekilde R4 ve R2 arasındaki bağlantı da bloklanıyor.



Rota Seçimi

Rota seçimi yapılırken göz önünde bulundurulan üç temel özellik vardır. Bu özellikler öncelik sırasına göre değerlendirildiğinde (Detaylı bilgi ve örnek için **CCNA - 2.14 - Routing Concepts** notlarına bakabilirsiniz);

- 1- Prefix Length, subnet maskesidir. Ip adresinin hangi bölümünün network adresini, hangi bölümünün Host adresini gösterdiğini tanımlamak için kullanılır.
 - a. Paketler yönlendirilirken öncelik hedef ip adresiyle en uzun eşleşen (longest prefix length) rota tanımı olacaktır.
- 2- Administrative Distance, dinamik yönlendirme protokollerinde bir network adresi için öğrenilen rotaların kalitesini belirlemede kullanılan özelliktir. Her dinamik yönlendirme protokolü metrik olarak farklı birimler kullanır (RIP -> Hop Count, OSPF -> Bandwidth). Birimler farklı olduğu için dinamik yönlendirme protokollerini arasında karşılaştırma yapılamıyor. Bu nedenle dinamik yönlendirme protokollerinin belirlediği en iyi rotaların kalitesini belirlemek için AD değerleri kullanılıyor.
 - a. Paketler yönlendirilirken öncelik en düşük AD değerine sahip rota olacaktır.

Route Source (Protocol)	Default AD
Connected interface	0
Static route out an interface	0
Static route to a next hop	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP v1 and RIP v2	120
EGP	140
External EIGRP	170
Internal BGP	200
Unknown	255

- 3- Metrics, dinamik yönlendirme protokollerinde en iyi rotayı belirlemek için kullanılan kritere verilen isimdir.

- a. Paketler yönlendirilirken öncelik en düşük metrik değerine sahip rota olacaktır.

Yönlendirme tablosunda aynı Prefix uzunluğuna, AD değerine ve Metrik değerine sahip birden fazla rota tanımlı olduğunda, bu rotalar arasında yük dengeleme (Load-Balance) yapılarak paketler iletilir. Buna **Equal-Cost Multipathing-ECMP veya Equal-Cost Load Balancing** deniliyor.

İstisna olarak EIGRP protokolünde Prefix uzunluğu ve AD değerleri aynı olup Cost değerleri farklı olan iki rota arasında da yük dengeleme (Load-Balance) yapılabilir ("variance" değeri set edilerek gerçekleştiriliyor. Detaylı bilgi için -> <https://www.thebryantadvantage.com/videos-and-tutorials/ccna-and-ccent-tutorials/eigrp-unequal-cost-load-balancing/>). Buna **Unequal-Cost Load Balancing** deniliyor (rotalar arasında gecikme farklı olması durumunda network felç olacaktır. Bu nedenle bilinçli kullanılması gerekiyor).

Static Routing

Her ne kadar dinamik yönlendirme protokolleri topolojideki rota seçim sürecini büyük ölçüde gerçekleştirirse de default rota tanımlı gibi çeşitli durumlarda halen statik rota tanımlarına ihtiyaç duyulmaktadır. Statik rota tanımının olumlu yanlarına bakıldığında;

- Routerda rota tespiti için ayrıca CPU veya hafıza alanını harcamaz.
- Dinamik yönlendirme protokolleriyle belirlenen rotalara müdahale edebilme imkanı sunuyor (AD değeri 0 olduğu için en uzun prefix değeri sahip iki rota arasında kalındığında paketler statik tanımlanan rota üzerinden gönderiliyor).

Statik rota tanımlı üç farklı şekilde yapılabilir. Bunlar (Detaylı bilgi ve örnek için **CCNA - 2.15 - Static Routing** notlarına bakabilirsiniz);

- **"ip route <Network Address> <Subnet Mask> <Exit Interface ID>"** komutuyla tanımlanabiliyordu. Bu şekilde tanımlanmasına **"Directly Attached Static Routes"** deniliyor. **Ethernet topolojisinde bu kullanım geçerli değil çünkü**, hedef routerun ip adresi belirtilmediği için ARP sorgusu yapılamıyor. Dolayısıyla paketi bir sonraki router'a göndermek için L2'de hedef MAC adresi eklenemiyor. Paket bir sonraki router'a gönderilemiyor (**Uygulamasını Lab -> Çalışma -> Static Routing dizininde bulabilirsiniz**).
 - o ip route 10.0.1.0 255.255.255.0 serial 0/0/0

- “**ip route <Network Address> <Subnet Mask> <Next Hop Router Ip Address>**” komutuyla tanımlanabiliyordu. Bu şekilde tanımlanmasına “**Recursive Static Route**” deniliyor. Recursive Static denmesinin nedeni, router paketi yönlendirirken ilk olarak paketi göndereceği routerun (Next Hop) ip adresini öğrenmek için yönlendirme tablosuna bakıyor. Göndermesi gereken ip adresini öğrenmek için tekrar yönlendirme tablosuna baktığından dolayı Recursive Static Routing veya Recursive Lookup deniliyor (Günümüzde bu işlemler Data Plane’e yaptırıldığı için her yönlendirme işleminde yönlendirme tablosuna bakılmadığı için Recursive Lookup işlemi yapılmıyor).
 - o `ip route 10.0.1.0 255.255.255.0 20.0.0.2`
- “**ip route <Network Address> <Subnet Mask> <Exit Interface ID> <Next Hop Router Ip Address>**” komutuyla tanımlanabiliyordu. Bu şekilde tanımlanmasına “**Fully Specified Route**” deniliyor.
 - o `ip route 10.0.1.0 255.255.255.0 serial 0/0/0 20.0.0.2`

Floating Static Routing

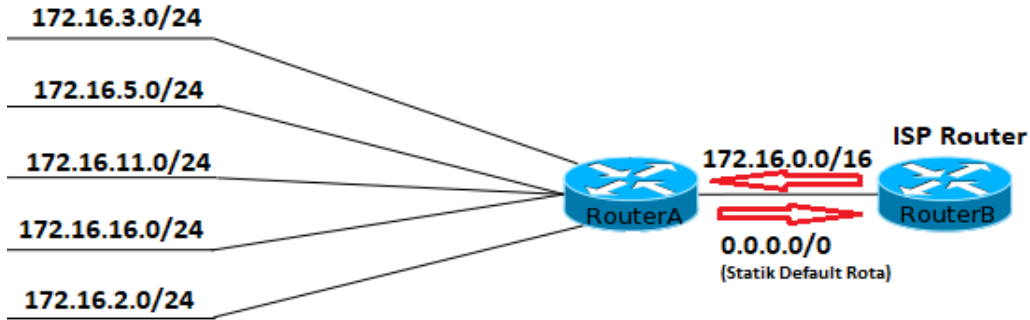
Normalde öğrenilen her rotanın öğrenildiği yonteme bağlı olarak (Directly Connected, Static, Dynamic-> OSPF, BGP,RIP...) belirli bir Administrative Distance değeri vardır. Prefix uzunluğu AD değeri ve Cost değerleri aynı olan rota tanımları arasında Load Balance yapıldığından daha önce de bahsedilmişti. Bazı durumlarda yük dengeleme yapılması istenmeyebilir (Yük dengeleme yapılacak rotalar arasında gecikme değerleri farklı olabilir, Rotalardan biri ISP’ye bağlıdır ve kullandıkça masrafa neden olabilir ...) veya dinamik yönlendirme protokolüyle kullanılması istenmeyen bir rota seçilmiş olabilir. Bu ve benzeri durumlarda statik rota tanımları yapılarak rotaların varsayılanda gelen AD değerleri değiştirilebiliyor. Bu sayede kullanılacak rota seçimine müdahale edilebiliyor. Buna Floating Static Routing deniliyor. AD değerini manipüle etmek için statik rota tanımının sonuna AD değeri belirtiliyor “**ip route <Network Address> <Subnet Mask> <Next Hop Ip Address> <Administrative Distance Value>**”.

```
RX(config)#ip route 10.0.0.0 255.255.255.0 20.0.0.2 ?
<1-255> Distance metric for this route
<cr>
RX(config)#
```

Static Null Interface

istenmeyen bir adrese/networke paket gönderilmesini önlemek için kullanılan sanal bir arayüzdür. Bu arayüze yönlendirilen paketler Drop edilir. Paketleri Null 0 arayüzüne yönlendirmek için “**ip route <Ip Address> <Subnet Mask> null 0**” komutu kullanılıyor (ACL kuralı yazılarak da bu işlem gerçekleştirilebiliyor). Kullanılabilecek durumlara örnek vermek gerekirse;

- Networkte bulunan zararlı yazılım yüklenmiş cihazlar (Botnet) belirli bir ip adresine/adres aralığına DDoS saldırısı yapıyor olabilir. Bu durumda saldırı yapılan ip adresine/adres aralığına gönderilen paketler Null 0 arayüzüne yönlendirilerek paketlerin drop edilmesi sağlanabiliyor. Bu sayede gereksiz yere networkün bant genişliğinin işgal edilmesi önlenabiliyor.
- **Statik rota tanımlamalarında eksik rota tanımlamaları yapıldığında (Default Static Rota tanımı, Summarization yapıldığında) Loop oluşabiliyor. Nasıl oluştuğuna örnek olarak;**



| -> Görselde, ISP’den alınan ip adres aralığına gönderilen paketler kurum networküne, kurum networkünde tanımlı olmayan networkler ise internete yönlendirildiği görülmektedir. Bu durumda internet üzerinden kurum networkünde kullanılmayan bir network aralığına paket gönderilmesi durumunda (örneğin 172.16.15.1, 172.16.7.5 gibi) bu adresler routerun yönlendirme tablosunda tanımlı olmayacağı için Default Statik Rota kullanılarak paketler tekrar ISP routeruna yönlendirilecektir. ISP routerunda da paketin hedef ip adres bilgisi kurum networkünü göstereceği için paket sürek (TTL veya Hop Count değeri sıfırlanana kadar)ı kurum routeru ile ISP routeru arasında Loop oluşturacaktır.

Bu oluşumu önlemek için kurumun internete çıkış yaptığı routerunda kullanılmayan her network trafiğinin Null 0 arayüzüne yönlendirilmesi gerekiyor (IPv6 için de IPv4 için de bu tanımlama yapılmalı. Aksi taktirde Loop oluşacaktır).

(Görsel için örnek verilecek olursa; “ip route 172.16.1.0 255.255.255.0 null0”, “ip route 172.16.4.0 255.255.255.0 null0”...)

(Lab -> Çalışma -> Summ-Loop dizini altında örnek bir uygulamasını bulabilirsin – tam simüle edemedim)

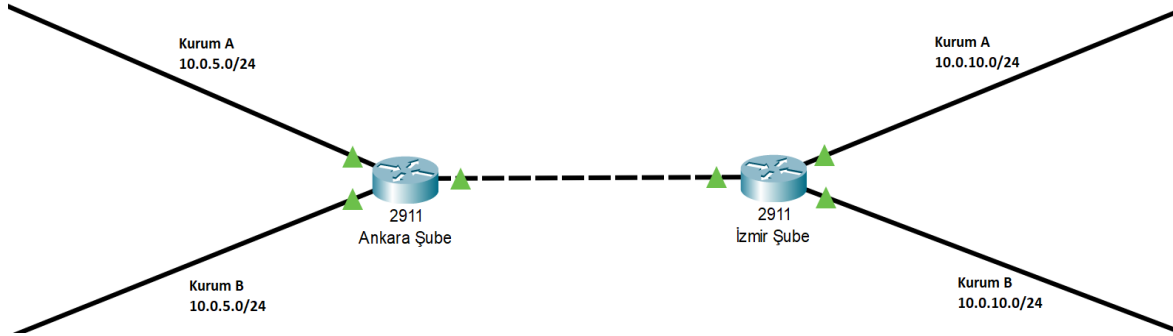
IPv6 Static Routing Konfigürasyonu

IPv4 Static Routing konfigürasyonu ile neredeyse aynı. Farklı olarak IPv’da farklı olarak;

- Routerların Link Local adres alabilmesi için “**ipv6 unicast-routing**” komutunun kullanılması gerekiyor.
- Statik Rota tanımında ise “**ipv6 routing <IPv6 Network Address /Prefix> <Next Hop Router Address>**” komutu kullanılıyor. Örnek vermek gerekirse;
 - o `ipv6 route 2001:db8:acab:1::/64 2001:db8:22::1`
 - o `ipv6 route 2001:db8:acab:1::/64 null 0`

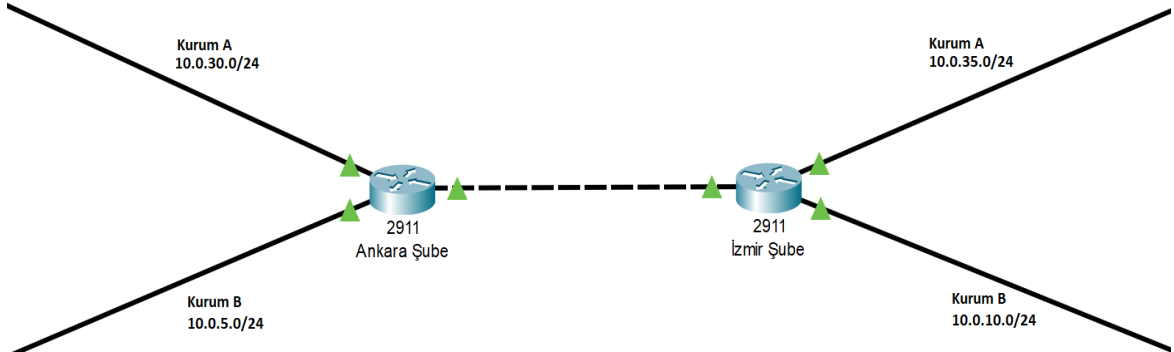
VRF (Virtual Routing and Forwarding)

Bir router üzerinde birden fazla sanal router oluşturmayı sağlayan teknolojidir. Daha çok L2’de kullanılan VLAN teknolojisine benzetilebilir. L3’te tek bir router/altyapı kullanarak kurum networklerinin birbirinden izole olacak şekilde yönlendirilmesi sağlanabiliyor. Daha iyi anlaşılması adına örnek vermek gerekirse;



| → Aynı private ip adres aralığını kullanan A ve B kurumları aynı routerları/altyapıyı kullanılarak internet üzerinden İzmir ve Ankara şubelerini haberleştirmek isteyebiliyor (Internet üzerinde Private ip adresleriyle nasıl yönlendirilecek diyebilirsin. MPLS teknolojisiyle gerçekleştiriliyor ama burada konuyu dağıtmamak için detaylandırılmadı. Daha detaylı bilgi için **CCNA - 3.06 – WAN** ve **CCNA - 3.07 - VPN and IPSec** notlarına göz atabilirsin). Bu durumda her kurum trafiği için routerlar üzerinde ayrı sanal routerlar oluşturularak kurum trafiklerinin birbirinden izole şekilde yönlendirilmesi sağlanıyor.

| → Aşağıdaki görselde olduğu gibi kurumlar farklı ip adres aralıkları kullanıyorsa trafikler VRF kullanılmadan da tek bir yönlendirme tablosu kullanılarak internet üzerinden yönlendirilebilir. VRF kullanılmadan yönlendirme işlemi yapıldığında kurumlar aralarında birbirilerine erişebilir durumda oluyor (Yani 10.0.30.0 networkü 10.0.10.0 networküne erişebiliyor). Kurum trafiklerini birbirinden izole edebilmek için ayrıca ACL tanımlanması gerekiyor.



VRF Konfigürasyonu

- İlk olarak “**vrf definition <VRF Name>**” komutuyla VRF tanımı (isim veriliyor) yapılıyor.
- “**address-family <Ip Protocol>**” komutuyla kullanılacak ip protokolü (IPv4 – IPv6) tanımı yapılıyor.
- VRF tanımı yapıldıktan sonra VRF içerisinde kullanılması istenen arayüzlere giriş yapılarak “**vrf forwarding <VRF Name>**” komutu kullanılıyor.
 - Bu komut sonrasında arayüz sıfırlanmış durumda VRF için kullanıma açılıyor. Bu nedenle cihazın yönlendirme (ana yönlendirme tablosu) tablodunda bu arayüz üzerinden gidilen bütün rota tanımları silinecektir.
 - Bu izolasyon router içerisinde yapıldığı için (yani VLAN’da olduğu gibi paket içerisinde taşınan bir bilgi yok) portlarda karşılıklı yapılması gerekmiyor.

```

RX(config)#vrf definition VRF1
RX(config-vrf)#address-family ipv4
RX(config-vrf-af)#exit
RX(config-vrf)#int fa 0/0
RX(config-if)#vrf forwarding VRF1
RX(config-if)#ip address 10.0.0.2 255.255.255.0
RX(config-if)#no sh
RX(config-if)#exit
RX(config)#

```

- Bu adımdan sonra statik network tanımları yapılırken de tanımın hangi VRF için uygulanacağı ayrıca belirtilmesi gerekiyor. Bu işlem için “**ip route <VRF Name> <Network Address> <Subnet Mask> <Next Hop Ip Address>**” komutu kullanılıyor.
- Benzer şekilde VRF’e arayüzler eklendiğin dinamik yönlendirme protokollerinde de tanımlamalar yapılırken hangi VRF için çalışacağı belirtiliyor. Örnek olarak OSPF protokolünde “**router ospf <Process ID> vrf <VRF Name>**” komurutla OSPF Prosesi oluşturulduktan sonra “**network <Network | Ip Address> <Wildcard Mask> area <Area ID>**” komutuyla VRF için çalışan arayüzden yayınlanması istenen network bilgileri tanımlanıyor.
 - o Konfigürasyonun kullanıldığı topolojiye bağlı olarak “**capability vrf-lite**” komutuyla VRF yönlendirme tablolarının doğru şekilde doldurulması sağlanabiliyor (https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/command/iro-cr-book/ospf-a1.html#wp2582896905).

(Örmek OSPF uygulamasını “Lab -> Çalışma -> VRF” dizini altında bulabilirsin)

```

R2(config)#
R2(config)#vrf definition VRF1
R2(config-vrf)#address-family ipv4
R2(config-vrf-af)#exit
R2(config-vrf)#exit
R2(config)#
R2(config)#vrf definition VRF2
R2(config-vrf)#address-family ipv4
R2(config-vrf-af)#exit
R2(config-vrf)#exit
R2(config)#

```

1

```

R2(config)#int fa 0/0
R2(config-if)#vrf forwarding VRF1
R2(config-if)#ip address 10.0.0.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#
R2(config)#int fa 0/1
R2(config-if)#vrf forwarding VRF2
R2(config-if)#ip address 20.0.0.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#

```

2

```

R2(config)#router ospf 10 vrf VRF1
R2(config-router)#network 10.0.0.2 0.0.0.255 area 5
R2(config-router)#exit
R2(config)#
R2(config)#router ospf 11 vrf VRF2
R2(config-router)#network 20.0.0.2 0.0.0.255 area 5
R2(config-router)#exit
R2(config)#

```

3

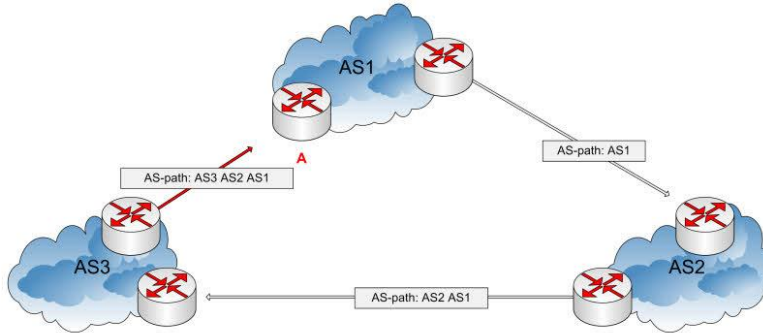
NOT

- Yönlendirme protokollerini sınıflandırmak için kullanılan ikinci bir ayırım ise protokollerin kullanıldığı yerleridir. Protokoller kurum içinde/şubeler veya birimler arasında (**IGP** – Inter Gateway Protocol) kullanılan ve kurum dışında/kurumlar arasında (**EGP** - Exterior Gateway Protocol) kullanılan protokoller olarak sınıflandırılıyor.
- VRF konfigürasyonu sonrasında router üzerinden bir cihaza ping atılmak istendiğinde (VRF’in yönlendirme tablosunu gerektirecek) doğrudan ping komutu kullanılamıyor. Nedeni Ping

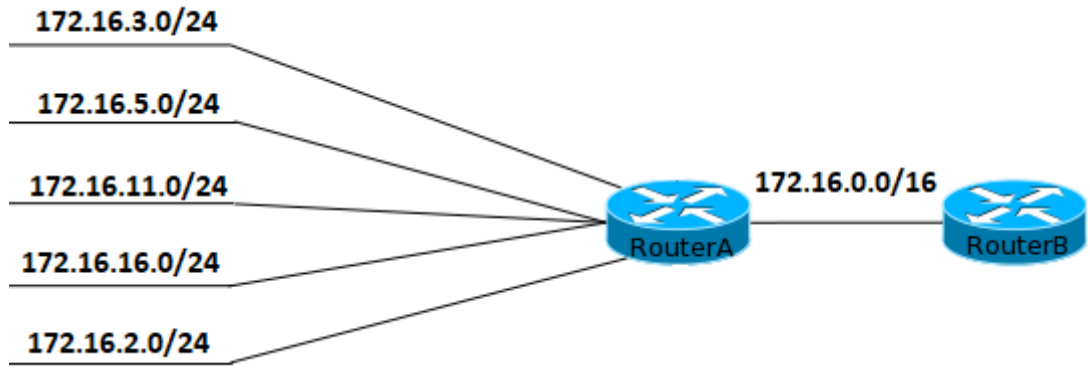
komutu kullanıldığında cihazın ana yönlendirme tablosu göz önünde bulundurulurken ping atılıyor. Tanımlanan VRF'in yönlendirme tablosu kullanılarak ping atılmak isteniyorsa “**ping vrf <VRF Name> <Destination Ip Address>**” komutu kullanılıyor. Benzer şekilde SSH gibi çeşitli durumlarda da kullanılacak VRF tanımının belirtilmesi gerekiyor.

Terminolojiler

- Best Loop-Free, L2'de (switchler arasında) olduğu L3'de (routerlar arasında) loop oluşabiliyor. Best loop-free ise üzerinde döngü oluşturmayan rotalar (L3) için kullanılıyor (Her ne kadar L3'de Hop/TTL gibi değerler bulunduğu için sonsuz döngüler oluşmasa da sonuç olarak paket hedef networke ulaşamayacaktır).
 - Dinamik yönlendirme protokollerinde Loop oluşma ihtimali yoktur ama Statik rota tanımlamalarında Loop oluşma riski vardır.
- Remote Network, routera doğrudan bağlı olmayan, farklı routerlar üzerinden erişilebilen networkler için kullanılan terimdir.
- AS (Autonomous System), bir kuruma ait ve aynı yönlendirme politikası altında yönetilen bölge anlamına gelmektedir. Routing Domain de denilmektedir. Her AS'ye, AS'yi tanımlayan bir numara olan benzersiz bir ASN değeri atanır.
 - Örnek olarak AS1'i X isimli ISP yönetirken AS2'yi Y isimli ISP yönetiyor. Sonuç olarak farklı ISP'lerin yönettiği ağlar da aralarında haberleşmesi gerekiyor.



- Convergence Time, bütün routerların topolojideki değişiklikleri öğrenmesi için geçen süredir. Örnek olarak topolojiden bir network çıkarıldığı zaman bunu topolojideki tüm routerların öğrenmesi için geçen süredir.
- Summarization, belirli aralıkta bulunan network adreslerinin tek bir özet ip adresiyle temsil edilmesine deniliyor. Örnek vermek gerekirse;
 - 172.16.4.0/24 , 172.16.1.0/24 , 172.16.3.0 /24 , 172.16.4.0/24 adresleri -> 172.16.0.0/16 adresiyle temsil edilebiliyor. Bu durumda 172.16.0.0/16 adresi özet adres oluyor.



Kontrol Komutları

- sh li route connected
- sh ip route <Ip Address>
- sh vrf
- sh ip route vrf <VRF Name>