İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

IP ŞEBEKELERİNDE YÖNLENDİRME PROTOKOLLERİ

YÜKSEK LİSANS TEZİ

Müh. Özgür KARAMAN

504031316

Tezin Enstitüye Verildiği Tarih : 8 Mayıs 2006

Tezin Savunulduğu Tarih : 15 Haziran 2006

Tez Danışmanı : Prof.Dr. Günsel DURUSOY

Diğer Jüri Üyeleri Doç.Dr. Işıl CELASUN

Dr. B. Demir ÖNER (M.Ü.)

Haziran 2006

İÇİNDEKİLER

KISALTMALAR

IP : Internet Protocol
CIDR : Classless Interdomain Routing
RIP : Routing Information Protocol
IGRP : Interior Gateway Routing Protocol
EIGRP : Enhanced Interior Gateway Routing Protocol
OSPF : Open Shortest Path First
IS-IS : Intermediate System-to-Intermediate System
OSI : Open Systems Interconnection
SNA : Systems Network Architecture
IPX : Internetwork Packet Exchange
RTMP : Routing Table Maintenance Protocol
AURP : AppleTalk Update-based Routing Protocol
NLSP : NetWare Link-Services Protocol
RTP : Routing Table Protocol, Reliable Transport Protocol
BGP : Border Gateway Protocol
IBGP : Interior BGP
EBGP : Exterior BGP
SPF : Shortest Path First
VLSM : Variable Length Subnet Mask
RFC : Request For Comment
CLNP : ConnectionLess Network Protocol
MTU : Maximum Transmission Unit
AS : Autonomous System
DUAL : Diffusing Update Algorithm
SAP : Service Advertisement Protocol
SRTT : Smooth Round Trip Time
RTO : Retransmission Timeout
HDLC : High-level Data Link Control
PPP : Point to Point Protocol
FR : Frame Relay
LSA : Link State Advertisement
NBMA : Non-Broadcast Multi Access
TOS : Type Of Service
CLNS : ConnectionLess Network Service
MPLS : MultiProtocol Label Switching
LSP : Link State Packet
LSDB : Link State DataBase
MAC : Media Access Control
PDU : Protocol Data Unit
LAN : Local Area Network
IETF : Internet Engineering Task Force

TABLO LİSTESİ

ŞEKİL LİSTESİ

IP ŞEBEKELERİNDE YÖNLENDİRME PROTOKOLLERİ

ÖZET

Bu çalışmada şebeke yönetimi ve trafik mühendisliğinde önemli bir yere sahip olan yönlendirme kavramı ve günümüzdeki şebekelerde en çok tercih edilen üçüncü katman protokolü olan IP'nin yönlendirilmesi için kullanılan protokoller incelenmiştir.

Bu amaçla, öncelikle IP şebekelerinin tarihçesi hakkında bilgi verilmiş, kullanılan teknolojilerin gelişmesi ile yönlendirme protokollerine duyulan ihtiyacın neden arttığı anlatılmıştır. Şebeke teknolojilerinin gelişmesi ile birlikte yönlendirme protokollerinden beklenenlerin protokollerin gelişimine etkileri gözden geçirilmiştir.

Daha sonra temel yönlendirme kavramları üzerinde durularak çeşitli OSI üçüncü katman protokollerini yönlendirebilecek yönlendirme protokolleri ve yönlendirme için kullanılan tablolar, bunların oluşması için gerekli işlemler anlatılmıştır.

Genel yönlendirme kavramları netleştirildikten sonra, IP yönlendirme protokollerinin sınıflandırılması incelenmiştir. Bu sınıfların üstün yönleri ve ortaya çıkarabilecekleri sorunlar ortaya koyularak, bu sorunlara karşı geliştirilen çözümler açıklanmıştır. Yönlendirme protokollerinin işleyişleri ve kullandıkları algoritmalar da detaylı olarak ele alınmıştır.

Yönlendirme protokollerinin sınıflandırması sonrasında, günümüzde IP yönlendirmesinde en yaygın olarak kullanılan RIP, IGRP, EIGRP, OSPF ve IS-IS protokolleri incelenmişlerdir. Bu protokollerin geliştirilmesi, kullandıkları algoritma ve teknolojiler, şebeke tasarımı ve yönetimine etkileri ve paket yapıları hakkında bilgi verilerek, kullanım alanları, elverişli ve elverişsiz yönlerine ışık tutulmuştur.

Son bölümde ise verilen bilgiler doğrultusunda, incelenen bu protokoller karşılaştırılmış ve çeşitli şebeke topolojilerinde hangilerinin kullanılabileceği ile protokollerin avantaj ve dezavantajları belirtilmiştir. Elde edilen bilgiler ışığında, örnek bir senaryo ile, verilen bir topoloji üzerinde kullanılması gereken yönlendirme protokolü belirlenmiştir.

ROUTING PROTOCOLS IN IP NETWORKS

SUMMARY

This study presents routing concepts, which play a very important role on network administration and traffic engineering; and routing protocols, which are produced to route IP, today's most widely used third layer protocol.

For this purpose, the history of IP networks is mentioned; development process and the reasons of the increasing need of the routing protocols are explained first. The effects of the arising requirements with the rapid evolution of network technologies are also mentioned.

The fundamentals of routing are described and routing protocols used to route different OSI third layer protocols are listed. Furthermore, information is given about routing tables and processes to fill these.

After routing basics are made clear, classification of IP routing protocols is given. Advantages and possible problems each class causes are mentioned with the solutions. Also, algorithms which are used by routing protocols are examined in detail.

After the classification, today's most popular IP routing protocols, namely RIP, IGRP, EIGRP, OSPF and IS-IS, are explained. Backgrounds and packet structures of these, the algorithms, technologies and protocols they use and their effects on the network design are revealed, and their uses in different topologies are compared.

Finally, considering the information given, all protocols are compared, their advantages and disadvantages are mentioned and the appropriate networks for each of them are listed. With the information provided, the routing protocol for a given network topology is selected.

1. GİRİŞ

1960lı yıllarda şebeke haberleşmesi denildiğinde, bir ana bilgisayar ve buna bağlı olarak çalışan uç birimleri akla geliyordu. Bu uç birimlerinin özellikleri sınırlıydı ve tüm bağlantıyı daha yüksek kapasiteli ana bilgisayar sağlıyordu. Bağlantıların da çok düşük hızlarda olduğu bu şebekelerde, yapılan tüm işlemleri ana bilgisayar yapıp sonuçlarını uç birimlere iletiyordu. Uç birimlerin sayısı az olduğunda ihtiyaca cevap verebilen SNA veya X25 gibi şebekeler, uç birimlerinin sayısı arttıkça ve şebekenin yapması beklenen işler arttıkça yetersiz kalmışlardır.

Yeni ihtiyaçlar, şebekelerdeki cihazların işlem yükünü paylaşmasını zorunlu kılmıştır, çünkü artık yapılması beklenen işlerin tek bir ana bilgisayar tarafından gerçekleştirilmesi verimli olmaktan çıkmıştır. Bu yük paylaştırılırken işlemlerin aksamaması için çeşitli teknolojiler geliştirilmesi gerekmiştir. Özellikle cihazlar arasındaki senkronizasyon, gönderilen verinin hatasının kontrolü ve düzeltilmesi, veri iletiminde sürekliliğin ve yeterli hızın sağlanması gibi hususlar önem kazanmıştır.

Zaman içinde kişisel bilgisayarların gelişmesi, yaygınlaşması ve internetle beraber IP protokolünün şebekelerde ağırlık kazanması, haberleşme alanında köklü yeniliklerin öncüsü olmuştur. Günümüzde IP şebekeleri üzerinden sadece veri değil gerçek zamanlı ses ve görüntü de taşınabilmektedir. Bunu sağlayabilmek için kullanılan protokollerin eskisinden çok daha fazla özelliği desteklemeleri, daha esnek ve daha kararlı olmaları, hızlı ve kesintisiz çalışmaları gerekmektedir.

Veri haberleşmesinde temel bir rol üstlenen yönlendirme protokolleri de bu ihtiyaçlara cevap verebilmek için zaman içinde gelişmiş, gerçek görevi olan bağlantıyı sağlayıp veri iletimini gerçekleştirmenin yanında, şebekenin tasarımını ve yönetilebilirliğini etkileyen, şebeke üzerinde çalışabilecek uygulamaları belirleyen, şebekeye esneklik kazandıran temel kavramlar arasında yer almıştır.

Internetin çok geliştiği ve halen hızla gelişmekte olduğu günümüzde; özellikle IP protokolünün yönlendirilmesi, şebekelerin herhangi bir sorundan en kısa sürede en az

müdahale ile kurtulması, bağlantı ve yönlendirici kaynaklarının en verimli şekilde kullanılması önem kazanmıştır.

Bu tez kapsamında işte bu görevleri yerine getirmek üzere tasarlanmış olan IP yönlendirme protokolleri incelenmiştir. Öncelikle yönlendirme kavramının temelleri açıklandıktan sonra bu kavramları kullanan yönlendirme protokolleri daha detaylı olarak ele alınmıştır. Protokollerin temel sınıfları ve bunların özellikleri işlendikten sonra günümüzde IP yönlendirmesi için kullanılan protokoller detaylı olarak incelenmiş ve karşılaştırılmıştır.

IP yönlendirme protokollerinin incelenmesinden önce ikinci bölümde yönlendirme ile ilgili temel kavramlar açıklanmış, çeşitli üçüncü katman protokollerini yönlendirebilecek protokoller hakkında ön bilgi verilmiştir.

Üçüncü bölümde, IP yönlendirme protokollerinin çeşitli özelliklerine göre ne şekilde sınıflandırılabileceği açıklanmış, her grubun yararlı yönleri ve yaşanabilecek sorunlar ile ilgili bilgi verilmiştir. Yönlendirme protokollerinin kullandığı algoritmaların ardında yatan mantık açıklanarak, geliştirilme sürecinde karşılaşılan sorunlar ve bunlara karşı bulunan çözümler irdelenmiştir.

Dördüncü bölümde ise günümüzde IP protokolünün yönlendirilmesi için kullanılan en yaygın protokoller olan RIP, IGRP, EIGRP, OSPF ve IS-IS incelenmiştir. Bu protokollerin gelişimi, şebeke tasarımlarına etkileri, kullandıkları çeşitli teknoloji ve protokoller ve paket yapıları ile ilgili bilgi verilerek, her birinin kullanım alanları, elverişli ve elverişsiz yönleri vurgulanmıştır.

Son bölümde verilen bilgiler ışığında, incelenen bu protokoller karşılaştırılmış, çeşitli şebeke tiplerinde kullanıma uygun olanlar belirtilmiştir. Örnek bir senaryo üzerinde verilen topoloji için en uygun yönlendirme protokolü seçilerek bu seçimin nedenleri açıklanmıştır.

2. YÖNLENDİRME

2.1. Yönlendirme Temelleri

Yönlendirme, paketlerin bir şebekeden diğerine iletilmesidir ve OSI referans modelinin üçüncü katmanı olan Şebeke Katmanında gerçekleşen bir işlemdir. Yönlendirmenin sağlanması için mantıksal bir üçüncü katman adreslemesi kullanılır. IP, IPX, Apple Talk gibi adresleme protokolleri kullanılarak paketlerin kaynak şebekeden hedef şebekeye ulaştırılması sağlanır. [1]

Yönlendirme işlemini gerçekleştirmek için yönlendiricinin

- hedef şebeke adresini ve o şebekenin nerede olduğunu
- hedef şebekeye gidilebilecek olası tüm yolları
- bu yollardan en iyisini

bilmesi gerekir.

2.2. Adresleme

Şebekeler arasında yönlendirmenin yapılabilmesi için üçüncü katmanda bir adresleme yapılması gerekir. Bu adreslerin şebeke ve makina adresi olmak üzere iki bölümü vardır. Şebeke kısmı her bir şebekeyi belirtirken, makina adresi şebeke içindeki her bir cihazı belirtir.

Yönlendiriciler hedef şebekeyi tanımlamak için üçüncü katman adresinin şebeke adresi kısmını kullanır. Her yönlendirici, yönlendirme yapacağı şebekeler için şebeke adresleriyle paketi göndereceği arabirimini eşleştirdiği bir yönlendirme tablosu oluşturur. Yönlendirme yapılacağında, veri paketindeki hedef adresiyle yönlendirme tablosundaki şebeke adreslerini eşleştirerek paketi ilgili arabirimden gönderir.

2.3. Yönlendirme Tabloları

Her yönlendirici, işlevini yerine getirebilmek için bir yönlendirme tablosuna ihtiyaç duyar. Bu tablodaki bilgilere göre, bir paketin hedef şebekesine gidebilmesi için yönlendiricinin hangi arabiriminden gönderilmesi gerektiği belirlenir. Paketin hedef şebekesi yönlendirme tablosunda bulunamazsa paket atılır. Bu yüzden yönlendirme tablolarının doğru ve eksiksiz olarak oluşturulması çok önemlidir. Bir yönlendirme tablosundaki alanlar aşağıdaki gibidir:

- **Şebeke Alanı:** Şebeke alanı, bir yönlendiricinin gidilebilecek olarak kabul ettiği tüm hedef şebeke adreslerini içerir. Bu şebekeler şebeke yöneticisi tarafından statik olarak ayarlanabileceği gibi, yönlendirme protokolleri kullanılarak dinamik olarak da öğrenilebilir.
- **Çıkış Arabirimi Alanı:** Bir paketin gönderileceği arabirimi belirtir. Paket bu bilgiye uygun olarak ilgili arabirimdeki kuyruğa dahil edilir. Eğer bir yönlendirme protokolü kullanılıyorsa, bu alan aynı zamanda ilgili şebekeye ait yönlendirme bilgisinin hangi arabirimden duyulduğu ile ilgili bilgi de verir.
- **Metrik Alanı:** Bir şebekeye ulaşmak için kullanılacak yolun metrik değerini belirtir. Metrik değeri kullanılan yönlendirme protokolüne göre değişir ve bir şebekeye ulaşılacak en iyi yolun seçiminde kullanılır.
- **Sonraki Adım Alanı:** Bu alan paketin bir sonraki adımda gönderileceği yönlendiricinin adresini belirtir. Bu adres, veri paketi ilgili yönlendiriciye gönderilirken kullanılacak ikinci katman adresinin belirlenmesi için kullanılır. Sonraki adım alanındaki adres, yönlendiriciye direkt olarak bağlı bir yönlendiriciyi belirttiğinden; alt şebeke maskesi, yönlendirme tablosunu oluşturan yönlendirici tarafından ilgili arabirimdeki alt şebeke maskesine uygun olarak belirlenir.

Örnek bir yönlendirme tablosu şekil 2.1'de gösterilmiştir.

```
router#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M –
mobile, B – BGP, D - EIGRP, EX - EIGRP external, O - OSPF,
IA - OSPF inter area. N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2, E1 - OSPF external type 1, E2 -
OSPF external type 2, E – EGP, i - IS-IS, L1 - IS-IS
level-1, L2 - IS-IS level-2, * - candidate default

        U - per-user static route, o - ODR
        T - traffic engineered route

Gateway of last resort is not set

    10.0.0.0/24 is subnetted, 6 subnets
C       10.1.60.0 is directly connected, Serial0/0
C       10.1.50.0 is directly connected, Ethernet0/0
S       10.1.10.0 [1/0] via 10.1.50.1, Ethernet0/0
S       10.1.11.0 [1/0] via 10.1.50.1, Ethernet0/0
R       10.1.5.0 [120/3] via 10.1.60.2, Serial0/0
R       10.1.4.0 [120/2] via 10.1.60.2, Serial0/0

router#
```

Şekil 2.1: Örnek yönlendirme tablosu

Örnekteki satırları incelersek, satırların başındaki harfler, yönlendirme bilgisinin öğrenildiği kaynağı belirtir. Tablodan önceki açıklamada görüldüğü gibi C direkt olarak yönlendiriciye bağlı şebekeleri gösterir. Bu satırlar yönlendiricinin bir arabirimine adres verildiğinde otomatik olarak yönlendirme tablosuna eklenen satırlardır. S harfi, şebeke yöneticisinin statik olarak belirlediği yönlendirme bilgilerini, R ise yönlendirme bilgisinin RIP protokolü kullanılarak öğrenildiğini belirtir. Satırlardaki ilk adresler şebeke alanını belirler. Bunlar ulaşılabilecek şebekelerdir. Köşeli parantez içindeki ilk sayılar, yönlendirme bilgisinin öğrenildiği kaynağın "yönetimsel uzaklık" değeridir. Bu, kaynağın güvenilirliğini belirten bir değerdir ve sonraki bölümlerde daha detaylı açıklanacaktır. Köşeli parantezin içindeki ikinci sayılar metrik alanını belirler. Satırlardaki ikinci adresler ise sonraki adım alanını belirler. Görüldüğü gibi direkt olarak bağlı şebekeler için başka bir yönlendirici adresi yazmamaktadır. Bu şebekelere gönderilecek paketler şebeke içindeki hedef cihaza zaten bu yönlendirici tarafından gönderilebilmektedir. Satırların en sonundaki bilgiler ise cıkış arabirimi alanını belirtir.

Bu örnekte yönlendiriciye 10.1.5.23 hedef adresli bir paket geldiğinde, hedef şebeke adresi yönlendirme tablosundaki beşinci satırla eşleştirilerek seri arabirimden 10.1.60.2 adresine gönderilecektir. Ancak 10.2.5.23 hedef adresli bir paket geldiğinde, uygun bilgi yönlendirme tablosunda yer almadığından, paket atılacaktır.

Yönlendiriciler birden fazla üçüncü katman protokolünü yönlendirebilir. Böyle bir durumda yönlendirilecek her protokol için ayrı bir yönlendirme tablosu oluşturulur.

2.3.1. Yönlendirme Tablolarının Oluşturulması

Yönlendiricilerin yönlendirme tablolarının oluşturulması statik veya dinamik olmak üzere iki şekilde olur.

2.3.1.1. Statik Yönlendirme

Yönlendirme tablolarının statik şekilde oluşturulması, şebeke yöneticisinin her şebeke için paketin hangi arabirimden gönderileceğini elle belirlemesiyle olur. Bu yöntem kullanıldığında, yönlendiriciler önceden şebeke yöneticisinin belirlediği yolları kullanarak paketleri yönlendirirler. Kendi aralarında bilgi alışverişi yapmalarına gerek olmadığından band genişliğinin tamamını veri paketlerinin iletiminde kullanabilirler. Ancak bu yöntem bağlantılarda oluşabilecek problemlere karşı aktif bir çözüm sunmaz. Bir bağlantı kullanılamaz hale geldiğinde şebeke yöneticisinin yönlendirme tablolarına müdahale etmesi ve yeni yol tanımlamaları yapması gerekir. Statik yönlendirme,

- Band genişliği çok düşük olan bağlantılarda
- Yedek hat olarak kullanılan bağlantılarda
- Bir dış şebekeye giden tek bir yol olduğunda
- Yönlendirici bir yönlendirme protokolü çalıştıracak donanıma sahip olmadığında
- Şebeke yöneticisinin bir bağlantıyı kontrol etmesi gerektiğinde

kullanılabilir.

Bazı durumlarda statik yönlendirme, varsayılan yol tanımlamak için de kullanılabilir. Varsayılan yol, yönlendirme tablosunda uygun satır bulunamazsa paketin yollanacağı arabirimi belirtir. [2]

2.3.1.2. Dinamik Yönlendirme

Yönlendirme tablolarının dinamik şekilde oluşturulması ise yönlendirme protokollerinin kullanılmasını gerektirir. Bu yöntem kullanıldığında, yönlendiriciler kendi aralarında bu protokolleri kullanarak haberleşir ve birbirleriyle yönlendirme bilgilerini paylaşırlar. Yönlendirici, bir şebekeye giden olası tüm yolları öğrendikten sonra kullanılan protokolün ölçülerine göre en uygun yolu seçer ve bu yolu yönlendirme tablosunda saklar. Yönlendiricilerin kendi aralarındaki haberleşmesi şebekeye bir miktar trafik yükü getirse de dinamik yönlendirme bağlantılarda oluşacak problemlere karşı şebeke yöneticisinin müdahalesine gerek kalmadan çözüm üretir. Bunun nedeni, yönlendirme bilgilerinin o anda şebeke içinde toplanan bilgilerle hesaplanmasıdır. Toplanan bilgiler, kullanılan yönlendirme protokolünün algoritmasına göre değerlendirilerek bir şebekeye giden en uygun yol belirlenir. Bir bağlantıda sorun olması durumunda yönlendirme protokolü, yeni duruma uygun bir en iyi yol bularak yönlendirme işlemini otomatik olarak bu yoldan yapmaya başlar. En iyi yol belirlenirken her yönlendirme protokolü kendi için belirlenen bir metrik değerini dikkate alır. Metrik değerleri; adım sayısı, bant genişliği, gecikme, güvenilirlik veya yük gibi bilgilerin biri veya birkaçı dikkate alınarak hesaplanır.

Kullanılacak yönlendirme protokolünün belirlenmesinde; şebeke yapısı, kullanılan cihazların sayısı ve üreticisi, yönlendirilecek protokol gibi kavramlar etkili olur. Her protokol her üretici tarafından desteklenmediği gibi, her protokol tüm üçüncü katman protokollerini yönlendiremez. Tablo 2.1'de çeşitli üçüncü katman protokollerinin hangi yönlendirme protokolü tarafından yönlendirilebileceği gösterilmiştir.

Tablo 2.1: Yönlendirilen protokoller ve yönlendirme protokolleri

Yönlendirilen protokoller	Yönlendirme protokolleri
AppleTalk	RTMP, AURP, EIGRP
IPX	RIP, NLSP, EIGRP
Vines	RTP
DECNet IV	DECNet
IP	RIPv1, RIPv2, OSPF, IS-IS, IGRP, EIGRP

2.3.2. Yönetimsel Uzaklık

Dinamik yönlendirme kullanılan bir şebekede çeşitli nedenlerle birden fazla yönlendirme protokolü kullanılabilir. Bu durumda bir şebekeye gidilebilecek yol birden fazla yönlendirme protokolü ile öğrenilebilir. Öğrenilen bu yolların hangisinin kullanılacağını yönetimsel uzaklık değeri belirler. Yönetimsel uzaklık, bir yolun kaynağının ne kadar güvenilir olduğunu belirten, 0-255 arasında bir tam sayıdır. Küçük yönetimsel uzaklık değerleri daha güvenilir kaynakları belirtir. Bir şebekeye giden birden fazla yol farklı kaynaklardan öğrenilmiş ise, en düşük yönetimsel uzaklık değerine sahip olan kaynaktan öğrenilen olan yol kullanılır.

Her yönlendirme protokolü için belirlenmiş varsayılan yönetimsel uzaklık değerleri olmakla beraber, kullanım ihtiyaçlarına göre bu değerler değiştirilebilir. Tablo 2.2'de varsayılan yönetimsel uzaklık değerleri gösterilmiştir. [2]

Tablo 2.2: Varsayılan yönetimsel uzaklık değerleri

Yol Kaynağı	Yönetimsel Uzaklık
Bağlı arabirim	0
Statik yol	1
EIGRP özeti	5
Dış BGP	20
EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
Dış EIGRP	170
İç BGP	200
Bilinmeyen	255

Bu tablodaki varsayılan yönetimsel uzaklık değerlerini kullanan bir yönlendirici, bir şebekeye giden yolu hem IGRP hem de RIP'ten öğrendiğinde, yönlendirme tablosuna IGRP'den aldığı yol bilgisini koyacak ve yönlendirme işlemini buna göre yapacaktır. Genelde varsayılan değerler kullanıldığında herhangi bir sorunla karşılaşılmaz; ancak bazı özel durumlarda şebeke yöneticisi varsayılan yönetimsel uzaklık değeri daha yüksek olan protokole öncelik vermek ya da yazdığı statik yolların ancak yönlendirme protokollerinde bir sorun olması durumunda kullanılmasını isteyebilir. Bu durumda yapılması gereken, yönetimsel uzaklık değerlerini amaca uygun şekilde değiştirmektir.

2.3.3. Ön Ekler

Çeşitli şebekelere giden en iyi yollar öğrenildikten ve yönlendirme tablosu oluşturulduktan sonra yönlendirme işlemini etkileyen bir diğer kavram ise şebeke adreslerinin ön ekleridir. Eger gelen paket yönlendirme tablosundaki birden fazla hedef şebeke bilgisine dahil ise en uzun ön ekli yönlendirme satırına göre yönlendirilir. Bunu bir örnekle incelersek:

Bir yönlendirici üzerinde EIGRP, RIP ve OSPF çalışmakta ve her protokol ile aşağıdaki hedef şebeke bilgileri öğrenilmiş olsun.

EIGRP: 192.168.32.0/26

RIP: 192.168.32.0/24

OSPF: 192.168.32.0/19

Bu durumda her üç hedef şebeke de farklı alt şebeke maskesine sahip olduğundan, yönetimsel uzaklık değerlerinden bağımsız olarak, hepsi yönlendirme tablosuna yazılacaktır. Oluşacak yönlendirme tablosu Şekil 2.3te gösterilmiştir.

Bu örnekte yönlendiriciye 192.168.32.1 adresine yönlendirilmesi gereken bir paket geldiğinde, paket 10.1.1.1 adresi üzerinden gönderilir. Bunun nedeni 192.168.32.1 adresinin her üç yönlendirme bilgisindeki şebekeye de dahil olması, ancak 192.168.32.0/26 bilgisindeki ön ek olan 26'nın diğerlerinden daha uzun olmasıdır. Aynı şekilde 192.168.32.100 adresinde yönlendirilecek bir paket de sadece son iki yönlendirme bilgisine uyacağından, bunlardan ön eki uzun olana göre 10.1.2.1 adresi üzerinden yönlendirilir. [3]

```
router#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B – BGP, D - EIGRP, EX - EIGRP external, O - OSPF,
IA - OSPF inter area. N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2, E1 - OSPF external type 1, E2 -
OSPF external type 2, E – EGP, i - IS-IS, L1 - IS-IS
level-1, L2 - IS-IS level-2, * - candidate default

        U - per-user static route, o - ODR
        T - traffic engineered route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 3 subnets
C       10.1.1.0 is directly connected, Serial0/0
C       10.1.2.0 is directly connected, Ethernet0/0
C       10.1.3.0 is directly connected, Serial0/1
D       192.168.32.0/26 [90/25789217] via 10.1.1.1
R       192.168.32.0/24 [120/4] via 10.1.2.1
O       192.168.32.0/19 [110/229840] via 10.1.3.1
router#
```

Şekil 2.2: Ön ekler örnek yönlendirme tablosu

3. YÖNLENDİRME PROTOKOLLERİNİN SINIFLANDIRILMASI

3.1. Uygulama Alanlarına Göre

Yönlendirme protokolleri kullanım alanlarına göre iç yönlendirme protokolleri ve dış yönlendirme protokolleri olarak ikiye ayrılabilir. Bu ayrımın daha iyi anlaşılmasını sağlamak için otonom sistem kavramının açıklanması yerinde olacaktır.

Otonom sistem, bir yönetimsel merkezden yönetilen şebekeleri tanımlar. Internete bağlı her servis sağlayıcının kendi adına kayıtlı bir otonom sistem numarası vardır ve kendi şebekelerinde bu otonom sistem numarasını kullanırlar. Bunların dışındaki firmalar zaten servis sağlayıcılardan hizmet aldıklarından, genelde kullandıkları otonom sistem numarasının yalnızca kendi şebekeleri içinde önemi vardır. Buna uymayan ender durumlarda firmanın internete bağlantısı birden fazla servis sağlayıcıdan alınan hatlar ile sağlanır. Bu durumda firma kendi otonom sistem numarasını almak isteyebilir.

İç yönlendirme protokolleri bir otonom sistemin içinde kullanılacak yönlendirme protokolleridir. RIPv1, RIPv2, IGRP, EIGRP, OSPF, IS-IS ve IBGP iç yönlendirme protokollerine örnektir. Bu protokoller tek merkezden yönetilen bir organizasyonun içinde çalıştırıldığından dış yönlendirme protokollerine göre daha basittir.

Dış yönlendirme protokolleri ise otonom sistemler arasında çalışan yönlendirme protokolleridir. EBGP dış yönlendirme protokollerine bir örnektir. Dış yönlendirme protokolleri farklı merkezlerden yönetilen, bu yüzden de içeride birbirinden farklı yönlendirme protokollerini kullanabilecek organizasyonlar arasında yönlendirme bilgilerinin güncellenmesini sağlar. Otonom sistemlerin içinde kullanılan protokolden bağımsız olarak çalışabilmesi, iç yönlendirme protokollerinden daha karmaşık olmasını gerektirir. Çalışma prensipleri ve çalışma alanları iç yönlendirme protokollerinden tamamen farklı olan dış yönlendirme protokolleri bu tez kapsamında incelenmemiştir.

3.2. İşleyişlerine Göre

Yönlendirme protokolleri işleyişlerine göre üç sınıfa ayrılabilirler, bunlar uzaklık vektörü, bağlantı durumu ve melez yönlendirme protokolleridir.

- Uzaklık vektörü protokolleri, bir şebekeye gidilecek en iyi yolu gidilebilecek tüm şebekeleri ve bunların uzaklıklarını paylaşarak tespit ederler. [4]
- Bağlantı durumu protokolleri, bağlı olan tüm yönlendiricilerin tüm şebeke topolojisinin bilgisine sahip olması ve buna göre en iyi yolları belirlemesine dayanır.
- Melez yönlendirme protokolleri ise hem uzaklık vektörü protokollerinin hem de bağlantı durumu protokollerinin çeşitli özelliklerini kullanırlar.

3.2.1. Uzaklık Vektörü Protokolleri

Uzaklık vektörü protokolleri, yönlendiricilerin yönlendirme tablolarının kopyalarını diğer yönlendiricilerle paylaşmaları esasına dayanır. Bu paylaşım belli zaman aralıkları ile tekrarlanır, böylece yönlendiriciler topoloji değişikliklerinden haberdar olur ve yeni duruma göre en iyi yolu bulabilirler. Uzaklık Vektörü protokolleri aldıkları yönlendirme tablolarını Bellman-Ford algoritmasına göre incelerler.

Eğer *i* noktasından *j*'ye başka bir ağ geçidinden geçilmeden gidilebiliyorsa, yani *i* ve *j* direkt olarak bağlılarsa, d(*i*, *j*) şeklinde bir değer aradaki bağlantının metrik değeri olarak tanımlanabilir. Eğer *i* ve *j* direkt bağlı değillerse d(*i*, *j*) sonsuz olarak kabul edilir. Bir yolun tamamının metrik değerinin bulunması için yapılacak işlem, yoldaki tüm bağlantıların metrik değerlerinin toplanmasıdır. Metrik değerleri pozitif tam sayılardır.

D(*i*, *j*) ise *i* ile *j* arasındaki en iyi yol olsun. Bu durumda,

$$D(i, i) = 0, \qquad \text{her } i \text{ için,}$$

$$D(i, j) = \min_{k} [d(i, k) + D(k, j)], \qquad \text{diğer}$$

Görüldüğü gibi ikinci eşitlik *i*nin komşuları olan *k*lar ile sınırlanabilir, çünkü diğerleri için d(*i*, *k*) değeri sonsuzdur. [4]

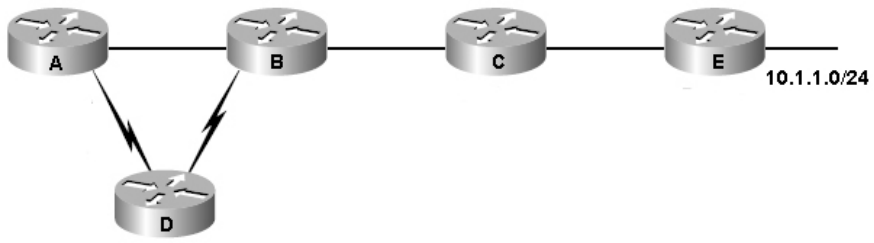
Bu algoritmaya göre çalışan uzaklık vektörü protokollerinde her yonlendirici (*i*), tüm komşularından (*k*) yönlendirme tablolarını alır. Bu tablolarda *j* hedef şebekesi için görünen metrik değerlerine kendisi ile tabloyu aldığı komşusu arasındaki bağlantının metrik değerini ekleyerek *j* şebekesine gitmek için kullanılabilecek yolun metrik değerini bulur. Daha sonra hesapladığı tüm olası yollardan en düşük metrik değerine sahip olanı seçer. Bulunan bu en iyi yol şebeke topolojisi değişmediği sürece sabit kalacaktır.

Görüldüğü gibi uzaklık vektörü protokollerinde yönlendiriciler bir hedef ağa olan uzaklığı bilmekle beraber şebeke topolojisinin tamamını bilmezler.

Uzaklık Vektörü Protokollerinde Döngülerin Engellenmesi:

Yönlendirme protokolleri özellikle şebeke üzerinde bir noktaya ulaşmak için kullanılabilecek birden fazla yol olduğunda kullanılırlar. Ancak birden fazla yol olması aynı zamanda yönlendirme döngülerinin oluşması tehlikesini de beraberinde getirir. Yönlendirme protokollerinin bu döngüleri engellemesi beklenir.

Döngü oluşmasına yol açan en önemli sebep, yönlendiricilerin şebekede oluşan topoloji değişikliklerini geç algılamalarıdır. Şekil 3.1'de bir yönlendirme döngüsünün oluşumu açıklanmıştır. [5]



Şekil 3.1: Yönlendirme döngüsünün oluşması

Şebekede herhangi bir sorun olmadığında tüm yönlendiriciler 10.1.1.0/24 hedef şebekesine giden yolu E yönlendiricisinden duymuşlardır. A ve D bu hedefe gitmek için B üzerinden paketleri yollamaktadır.

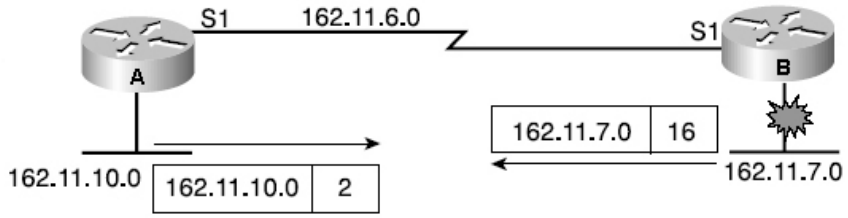
E yönlendiricisi üzerinde 10.1.1.0/24 şebekesine giden yol kullanılamaz hale geldiğinde, E bunu C'ye duyurur. Bu C'nin artık bu hedefe gitmek için E'ye paket göndermemesini sağlar. Ancak durumdan henüz diğer üç yönlendiricinin haberi

yoktur. C kendisine gelen bilgiyi B'ye iletirken diğer yönlendiriciler de belli aralıklarla yaptıkları güncellemelerini göndeririler. Bu durumda B, 10.1.1.0/24 şebekesine C üzerinden gidemeyeceğini öğrenir ama aynı zamanda A'dan da 10.1.1.0/24 şebekesine 3 atlama ile gidebileceğini öğrenir. Bu yapıda ilgili şebekeye gönderilecek bir paket önce A'ya oradan da B'ye gönderilir. Son bilgi doğrultusunda B de paketi A'ya gönderecektir. Bu durum yönlendirme döngüsüne bir örnektir. Bu şekildeki güncellemeler devam ettikçe A, B ve D arasında sonsuza sayma denen sorun da oluşacaktır. Bu durumda aslında ulaşılamayan bir hedef şebeke için güncellemeler yapılmaya devam edecek ve bu şebeke için yönlendiricilerdeki metrik değeri sürekli artacaktır.

Sonsuza sayma sorunu metrik değerleri için bir üst sınır belirlenerek çözülebilir. Bu durumda sorun oluştuğunda metrik değerleri bu üst sınıra kadar artacaktır ve bu değere ulaştığında hedef şebeke ulaşılamaz kabul edilecektir. Bu çözüm döngülerin oluşmasını engellemez. Sadece döngünün sonsuza kadar devam etmesini engeller.

Uzaklık Vektörü protokolleri yönlendirme döngülerini önlemek için çeşitli araçlar kullanırlar. Uzaklık vektörü protokollerinde oluşabilecek sorunlar ve bunlara ilişkin çözümler tablo 3.1'de gösterilmiştir. [6]

Split Horizon: Split horizon kuralına göre bir hedef şebekeye gitmek için kullanılan arabirimden gönderilen güncellemelerde o şebekeye ait bilgi bulunmaz. Bu kural uygulanarak iki yönlendirici arasında oluşabilecek sonsuza sayma sorunu önlenmiş olur. Şekil 3.2'de bu kuralın işleyişi görülmektedir.



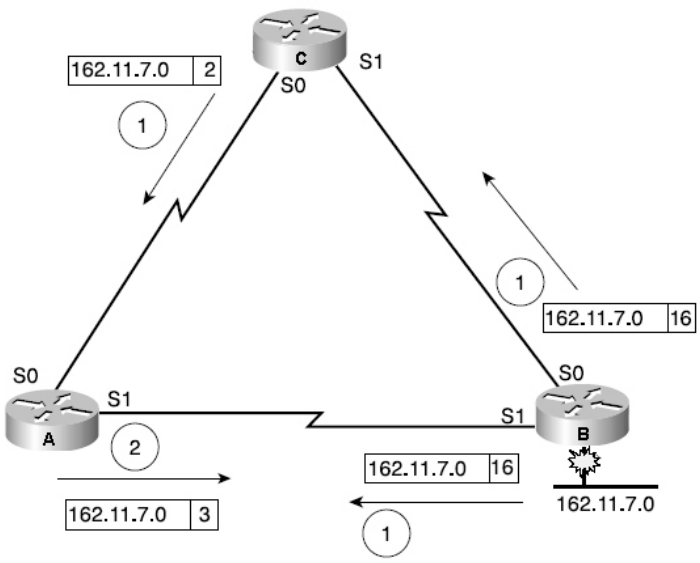
Şekil 3.2: Split Horizon kuralının işleyişi

Burada güncelleme bilgilerinin iki yönlendirici tarafından aynı anda gönderildiğini düşünelim. İlk güncellemeler sonunda eğer split horizon kullanılmazsa A yönlendiricisi 162.11.7.0 şebekesine gidilemeyeceğini öğrenir, ancak B yönlendiricisi A'dan aldığı güncellemeye göre bu şebekeye A üzerinden 3 adımda ulaşabileceğini düşünür. Split horizon kuralı uygulandığında ise, A yönlendiricisi 162.11.7.0 şebekesine giden yolu zaten B'den öğrendiği için, yolladığı güncellemeye bu şebekeye ait bilgiyi koymaz. Böylece sonsuza sayma sorunu engellenmiş olur. Aynı kurala göre B yönlendiricisinin yolladığı güncellemede de A'dan öğrendiği 162.11.10.0 şebekesine ait bilgi bulunmaz. Bu şekilde gönderilen güncelleme paketlerinin boyutu da küçüldüğünden bağlantı üzerindeki yük de azalmış olur.

Tablo 3.1: Birden fazla yol olan şebekelerde uzaklık vektörü protokolleri ile ilgili sorunlar ve çözümleri

Sorun	Çözüm
Aynı hedef şebekeye giden birden fazla yolun aynı metrik değerine sahip olması	Uygulamaya göre öğrenilen ilk yolun kullanılması veya yönlendirme tablosuna tüm yol bilgilerinin yazılması mümkündür.
Tek bağlantı üzerinden güncellemelerin bağlantının iki ucuna sürekli aktarılması	**Split Horizon –** Bir arabirimden alınan güncelleme ile öğrenilen yol bilgileri aynı arabirim kullanılarak duyurulmaz. **Split Horizon (poison reverse ile) –** Topolojide sorun yoksa split horizon kuralları kullanılır. Bir yol kullanılamaz duruma geçerse, bu yol sonsuz kabul edilen bir metrik ile tüm arabirimlerden duyurulur.
Farklı yollar üzerinden gelen güncellemeler yüzünden oluşan döngüler	**Route Poisoning –** Bir hedef şebeke ulaşılamaz olursa sonsuz kabul edilen metrik ile duyurulur.
Sonsuza sayma	**Hold-down Sayacı –** Bir hedef şebeke ulaşılamaz olursa, yönlendirici bu şebeke için gelen diğer yol bilgilerini dikkate almadan önce bir süre bekler. **Tetiklenmiş Güncellemeler –** Bir yol kullanılamaz olursa güncelleme için periyodik güncelleme beklenmeden anında güncelleme gönderilir.

Hold-down Sayacı: Split Horizon kuralı sonsuza sayma sorununu tek bir bağlantı için çözer ancak birden fazla bağlantı olduğunda aynı sorunu sadece split horizon kullanarak engellemek mümkün değildir. Şekil 3.3te bunu açıklayan bir örnek gösterilmiştir.



Şekil 3.3: Hold-down sayacı kullanımı gereken bir sonsuza sayma sorunu

Burada 162.11.7.0 şebekesine bağlantı kesildiğinde B yönlendiricisi bunu sonsuz kabul edilen bir metrikle duyurur. Ancak C'nin güncellemesi de aynı anda yollanıyorsa A yönlendiricisi bu şebekeye B üzerinden gidilemeyeceğini öğrendiği anda C üzerinden 2 adımda gidebileceğini öğrenir ve bu bilgiyi yönlendirme tablosuna yazar ve kendi güncelleme zamanı geldiğinde bunu B'ye de duyurur. Bu da yeni bir sonsuza sayma durumunu oluşturur.

Hold-down sayacı kullanıldığında yönlendiriciler bir şebekeye giden yolun kullanılamaz olduğunu öğrendikten sonra, bu sayaç süresi dolana kadar o şebeke ile ilgili gelen güncellemeleri dikkate almazlar. Bu kural kullanıldığında A yönlendiricisi B'den ve C'den aynı anda güncelleme almış olsa da, hold-down sayacı dolana kadar C'den aldığı bilgiyi dikkate almaz. Bu süreden sonra tüm yönlendiriciler zaten ilgili şebekeye ulaşılamayacağını öğrenmiş olduklarından, sonsuza saymanın veya oluşabilecek herhangi bir yönlendirme döngüsünün önüne geçilmiş olur.

Tetiklenmiş Güncellemeler: Uzaklık vektörü protokolleri belli aralıklarla güncellemeler gönderirler. Ancak önceki örneklerde görüldüğü gibi oluşan sorunlar genellikle normal işleyişte değil, bir şebekeye giden yolun kullanılamaz olduğu durumlarda ortaya çıkar. Bu yüzden bazı uzaklık vektörü protokolleri tetiklenmiş güncellemeleri kullanır. Tetiklenmiş güncelleme, bir şebekeye giden yol kullanılamaz olduğunda periyodik güncelleme zamanı beklenmeden güncelleme bilgisinin komşu yönlendiricilere gönderilmesi demektir. Bu şekilde kullanılamayacak yola ilişkin bilgi şebeke üzerinde mümkün olan en kısa sürede duyurulur, ayrıca komşu yönlendiricilerde hold-down sayaçlarının daha çabuk başlatılması sağlanır.

3.2.2. Bağlantı Durumu Protokolleri

Bağlantı durumu protokolleri, uzaklık vektörü protokollerinin aksine tüm yönlendirme tablolarını diğer yönlendiricilere yollamazlar. Bunun yerine daha karmaşık bir veri tabanı kullanırlar. Buradaki bağlantı kelimesi, yönlendiriciler arasındaki fiziksel veya mantıksal bağlantıları belirtmek için kullanılır. İsminden de anlaşılacağı gibi, bağlantı durumu protokolleri, birbirlerine bu bağlantıların durumu değiştiğinde güncellemeler yollarlar. Örneğin A ve B yönlendiricileri arasındaki bağlantı kullanılamaz hale geldiğinde, hem A hem de B yönlendiricisi tüm şebekeye aralarındaki bağlantının yeni durumunu, yani kullanılamaz olduğunu duyururlar.

Uzaklık vektörü protokollerinin aksine, gönderilen bilgi yönlendiriciye bağlı olan bağlantılar ile ilgili bilgiyi içerir, tüm yönlendirme bilgisini içermez. Bu bağlantılarla ilgili bilgi tüm şebekeye her yönlendirici tarafından yayılır ve bu sayede tüm yönlendiriciler tüm şebeke topolojisi hakkında ortak bir bilgiye sahip olurlar.

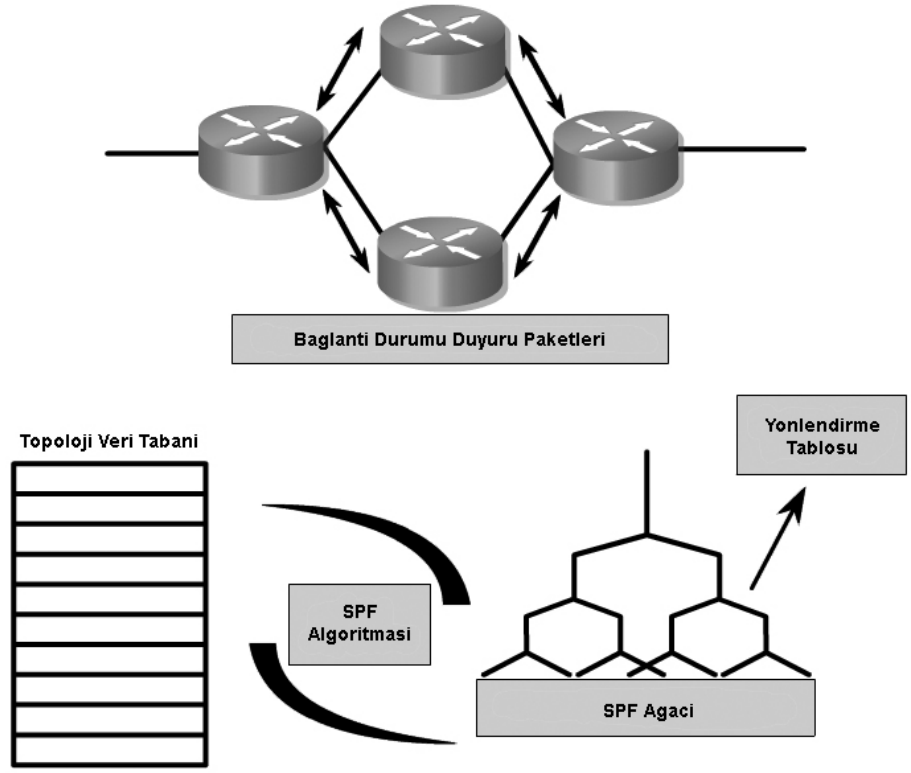
Tüm yönlendirme tablosu yerine sadece bağlantılarla ilgili bilgi gönderilmesi verimli bir yöntemdir. Bir bağlantı bir çok yönlendirmeyi etkileyebilir ve bilgiyi alan yönlendiriciler yeni bağlantı durumunun etkilerini kendileri hesaplarlar. Görüldüğü gibi burada band genişliği uzaklık vektörü protokollerinden daha az kullanılır ancak yönlendiriciler üzerinde daha fazla işlemci ve hafıza kullanılmasını gerektirir. [2]

3.2.2.1. Bağlantı Durumu Protokollerinin Çalışması

Bağlantı durumu protokolleri kullanıldığında, aynı bağlantı üzerindeki yönlendiriciler arasında bir komşuluk ilişkisi kurulur. Bunun için yönlendiriciler belli aralıklarla birbirlerine merhaba paketleri gönderirler. Merhaba paketleri karşılıklı gönderildiği sürece komşuluk ilişkisi devam eder. Bu paketlerin sürekli yollanıyor olması aradaki bağlantıdaki bir değişikliğin en kısa sürede farkedilmesini de sağlamaktadır.

Bir yönlendirici, komşusundan gelecek merhaba paketlerini belirli bir süre boyunca alamazsa, aradaki bağlantının kullanılamaz olduğuna karar verir. Böyle bir sorun algılandığında, yönlendirici güncelleme zamanının dolmasını beklemeden güncelleme mesajlarını gönderir. Bu güncelleme mesajındaki bilgi sadece şebekedeki bu değişikliği duyurur. Böylece band genişliği mümkün olan en az oranda kullanılarak veri akışının en az miktarda etkilenmesi sağlanır. Özellikle büyük şebekelerde tüm yönlendirme tablosu yerine bu şekildeki daha küçük güncellemelerin gönderilmesi tercih edileceğinden, bu gibi şebekelerde bağlantı durumu protokolleri daha fazla kullanılır.

Bağlantı durumu protokollerinin kullandığı en önemli kavramlar, bağlantı durumu güncellemeleri, yönlendiricilerin kullandığı topoloji veri tabanı, en kısa yol önceliklidir (SPF – Shortest Path First) algoritması ve bu bilgiler kullanılarak oluşturulan yönlendirme tablosudur. Bu kavramlar ve işleyişleri Şekil 3.4'te gösterilmiştir.



Şekil 3.4: Bağlantı durumu yönlendirme protokollerinin temel kavramları ve çalışması

Bağlantı durumu protokollerinin şebekeyi öğrenme süreci aşağıdaki gibidir:

- Öncelikle her yönlendirici doğrudan kendisine bağlı şebekeleri hesaplayarak bağlantı durumu güncellemelerini şebekeye yollar.
- Güncellemeler alındıktan sonra her yönlendirici aldığı bu bilgileri kullanarak bir topoloji veri tabanı oluşturur.
- Bu veri tabanı üzerinde SPF algoritması çalıştırılarak bir SPF ağacı oluşturulur. Bu ağacın kökünde yönlendiricinin kendisi, dallarında ise diğer yönlendiriciler bulunur. Böylece yönlendirici, diğer yönlendiricilere ulaşabileceği yollar arasından en kısa yolu seçebilir.
- En kısa yollar bulunduktan sonra yönlendirme tablosu oluşturularak yönlendirme işlemine başlanır.

Bir yönlendirici yeni bir bağlantı durumu duyurusu aldığında yukarıdaki işlemler tekrarlanarak yeni bir SPF ağacı oluşturulur. Bu süreç tamamlanmadan veri paketlerinin yönlendirilmesine başlanmaz.

Bağlantı durumu protokollerinin kullanıldığı çoklu erişime açık şebekelerde bağlantıdaki güncelleme trafiğinin azaltılması için bazı yönlendiriciler seçilerek güncellemelerin sadece bu yönlendiricilere gönderilmesi sağlanabilir.

3.2.2.2. Bağlantı Durumu Protokollerinin Zayıf Yönleri

Bağlantı durumu protokollerinde, protokolün kullanılmaya başlandığı zaman ve kullanım boyunca olmak üzere üç temel sorunla karşılaşılabilir.

1. Yönlendiricilerin işlemci ve hafızalarının yetersiz kalması: Daha önce de belirtildiği gibi, bağlantı durumu yönlendirme protokolleri kullanıldığında, uzaklık vektörü protokollerine göre, şebeke üzerindeki güncelleme trafiği yükü azalır ancak buna karşın yönlendiriciler üzerinde kullanılan işlemci ve hafıza yükü artar. Bu yük SPF algoritması çalıştığı sırada yönlendiricinin çalışması için gerekli kaynakları da tüketerek soruna neden olabilir. Bu yüzden şebeke yöneticisi, bir bağlantı durumu protokolü kullanacağı zaman şebekedeki yönlendiricilerin işlemci ve hafıza kapasitelerini çok iyi planlamalıdır. Bağlantı durumu protokollerinin daha çok büyük boyutlu şebekeler için tercih edildiği önceden belirtilmişti. Ancak özellikle büyük boyutlu şebekelerde bu planlama daha da önem kazanır, çünkü bu durumda yönlendiricinin hafızasında saklanması gereken topoloji ve yönlendirme tabloları daha büyük olacak, ayrıca SPF algoritmasının daha büyük veri tabanı üzerinde çalıştırılması daha fazla işlemci gücü gerektirecektir.
2. İlk çalışma sırasındaki band genişliği sorunu: Bağlantı durumu protokolleri ilk çalıştığında, tüm yönlendiriciler şebekeyi öğrenmek için bağlantı durumu güncellemelerini gönderirler. Şebeke çok büyük olduğunda yönlendirici sayısı fazla olacağından, bu sırada oluşan trafik yükü veri akışını engelleyecek boyuta çıkabilir. Bu sorun protokole ilk çalıştığında ortaya çıkabilecek bir sorundur, daha önce belirtildiği gibi normal çalışma sırasında sadece bir topoloji değişikliği olursa ilgili yönlendirici bunu duyurmak için güncelleme gönderir.

3. Eş zamanlı olmayan güncellemeler: Bağlantı durumu protokolleri kullanıldığında, bir bağlantı kullanılamaz olduğunda veya tekrar kullanılabilir hale geldiğinde buna bağlı yönlendiriciler güncelleme yollar. Ancak bu güncellemeler eş zamanlı yapılmazsa soruna neden olabilir. Bir bağlantı kısa süreliğine kesilip tekrar kullanılır olduğunda, yönlendiricilerden biri kullanılamaz güncellemesini diğerlerinden daha geç gönderirse, bu güncelleme şebekedeki yönlendiricilere bağlantının tekrar çalışır olduğu bilgisinden daha sonra ulaşabilir. Bu durumda aslında kullanılabilir olan bir bağlantı kullanılamaz olarak değerlendirilebilir.

Bağlantı durumu protokollerinde oluşabilecek bu gibi sorunları engellemek için çeşitli önlemler alınabilir:

- Şebeke yöneticisi periyodik güncellemelerin aralıklarını arttırarak bu paketlerin yarattığı trafik yükünü azaltabilir. Bu süre uzatıldığında topoloji değişiklikleri ile tetiklenen güncellemeler etkilenmez. Böylece periyodik güncellemelerin yükü azaltılır ancak topoloji değişikliklerinin öğrenilmesi eskisi gibi hızla gerçekleştirilir.
- Özellikle çoklu erişime açık şebekelerde bazı yönlendiriciler seçilerek güncellemelerin sadece bu yönlendiriclere yapılması sağlanabilir. Diğer yönlendiriciler ise seçilen bu yönlendiricilerden gelen güncellemelere dikkat ederler.
- Güncellemelerin eş zamanlı olması için çeşitli sayaçlar, paketlerin karışıklığa yol açmaması için de numaralandırma gibi çözümler kullanılabilir.
- Büyük şebekelerde ana şebeke daha küçük bağımsız alanlara ayrılabilir. Bu alanlardaki yönlendiriciler sadece kendi alanlarındaki topoloji bilgisini saklarlar. Bu sayede yönlendiriciler üzerinde protokolün kullandığı işlemci ve hafıza azaltılabieceği gibi güncellemelerin de bu alanlar içinde kalması sayesinde güncelleme trafiği de çok daha az olur.

3.2.3. Melez Yönlendirme Protokolleri

Melez yönlendirme protokolleri adından da anlaşılacağı gibi hem uzaklık vektörü protokollerinin hem de bağlantı durumu protokollerinin özelliklerini kullanır. Bazı kaynaklarda melez protokollerden gelişmiş uzaklık vektörü protokolleri olarak da söz edilir.

Melez yönlendirme protokolünün özelliklerini açıklamadan önce uzaklık vektörü ve bağlantı durumu protokollerinin özelliklerini kısaca özetlemek yerinde olacaktır:

- Uzaklık vektörü protokolleri, tüm topoloji bilgisini yönlendirme tablosundan elde eder. Bu yüzden şebekenin tüm topolojisini bilmez. Oysa bağlantı durumu protokolleri ayrı bir topoloji tablosuna sahiptir. Tüm yönlendiriciler şebekenin tamamının topolojisini bilir.
- Uzaklık vektörü protokolleri, güncellemelerinde tüm yönlendirme tablolarını gönderirler, aldıkları bilgiye aradaki bağlantının metrik değerini ekleyerek en iyi yolu hesaplarlar. Bağlantı durumu protokolleri ise en iyi yolu topoloji tablosundan SPF algoritması ile hesaplarlar.
- Uzaklık vektörü protokollerinde güncellemeler periyodik olarak sık aralıklarla yapılır. Bağlantı durumu protokollerinde ise periyodik güncellemeler çok seyrektir, topoloji değişikliği ile tetiklenen güncellemeler kullanılır.
- Uzaklık vektörü protokolleri yönlendirme paketleri yüzünden daha fazla trafik yükü getirir ancak bağlantı durumu protokolleri de yönlendiriciler üzerinde daha fazla işlemci ve hafızaya gerek duyar.
- Bağlantı durumu protokolleri şebeke tasarımı sırasında daha fazla dikkat gerektirir. Özellikle büyük şebekeler tasarlanırken alanlara ayrılacaksa buna uygun hiyerarşik bir adresleme ve bağlantı planı kullanılmalıdır.

Melez yönlendirme protokolleri en iyi yolu seçerken uzaklık vektörü protokolleri gibi metrikleri kullanır. Ancak güncellemeler bağlantı durumu protokollerinde olduğü gibi topoloji değişiklikleri ile tetiklenir. Ayrıca melez yönlendirme protokolleri bağlantı durumu protokolleri gibi bir komşu ve topoloji tablosu da

oluşturarak en iyi yol seçiminde bunları da kullanırlar. Bu özellikleri sayesinde melez yönlendirme protokolleri bağlantı durumu protokolleri gibi hızlı bir öğrenme sağlarken onlar kadar yüksek işlemci ve hafızaya gerek duymazlar. Melez yönlendirme protokolüne EIGRP protokolü örnek gösterilebilir.

3.3. IP Adreslerini Değerlendirmelerine Göre

Yönlendirme protokolleri IP adreslerini iki şekilde değerlendirebilir. Daha eski yönlendirme protokolleri IP adreslerini genelde sınıflı olarak değerlendirirken, sonradan geliştirilen yönlendirme protokolleri, sınıflı protokollerin getirdiği kısıtlamaları aşmak için adresleri sınıfsız olarak değerlendirmişlerdir.

3.3.1. IP adresi sınıfları

IP adreslemesi ilk oluşturulduğunda çeşitli büyüklüklerdeki şebekelerde kullanıma uygunluklarına göre sınıflara ayrılmış ve bu sınıflara göre alt şebeke maskeleri belirlenmiştir. Bu sınıflandırma yapılırken adreslerin ilk oktetlerine dikkat edilmiş ve Tablo 3.2deki ilk oktet kuralı uygulanmıştır. [2]

Tablo 3.2: İlk oktet kuralı

İlk oktet bit dizilimi	Adres sınıfı	İlk oktetin alabileceği değerler
0	A	0-127
10	B	128-191
110	C	192-223
1110	D	224-239
1111	E	240-255

Bu kurala göre oluşturulan sınıflardan ilk üçü internette adresleme için kullanılabilir olarak belirlenmiştir. D sınıfı adresler özel uygulamaların multicast olarak paket göndermeleri için ayrılmıştır. E sınıfı adresler ise test amaçları için ayrılmıştır. Bu iki sınıf internet üzerinde adresleme için kullanılmazlar. Bu kurala göre adresleme için kullanılan sınıflara belirli alt şebeke maskeleri atanmış ve her IP şebekesinin tek bir fiziksel şebekede kullanılması gerekmiştir. Tablo 3.3te adresleme için kullanılan adresler ve alt şebeke maskeleri gösterilmiştir.

Tablo 3.3: Adresleme için kullanılabilir şebeke numaraları

	A Sınıfı	B Sınıfı	C Sınıfı
İlk oktet değerleri	1 - 126	128 - 191	192 – 223
Kullanılabilir şebeke numaraları	1.0.0.0 - 126.0.0.0	128.1.0.0 – 191.254.0.0	192.0.1.0 – 223.255.254.0
Alt şebeke maskesi	255.0.0.0	255.255.0.0	255.255.255.0
Bu sınıftaki şebekelerin sayısı	2^7 - 2	2^{14} - 2	2^{21} – 2
Şebeke başına adres sayısı	2^{24} - 2	2^{16} - 2	2^8 - 2

Görüldüğü gibi ilk oktet kuralına göre bu sınıflara dahil olan bazı şebeke numaraları da kullanılabilir şebekeler arasında yer almaz. Örneğin 0.0.0.0 şebekesi başlangıçta broadcast adresi olarak kullanılmak için düşünülmüştür, 127.0.0.0 şebekesi ise halen cihazların kendilerini tanımlamak için (loopback adresi) kullanılmaktadır. Bunlar dışında 128.0.0.0, 191.255.0.0, 192.0.0.0 ve 223.255.255.0 şebekeleri de ayrılmış şebeke numaralarıdır ve kullanılmamaktadır. [6]

IP bloğu almak isteyen bir firmaya bu sınıflandırmaya göre adresler verildiğinde çeşitli sorunlar ortaya çıkmaktadır. Böyle bir durumda 50 adrese ihtiyacı olan bir firma için C sınıfı bir blok ayırmak, 800 kadar adrese ihtiyacı olan bir firmaya B sınıfı bir blok veya birkaç C sınıfı bloğu ayırmak gerekiyordu. Ancak 800 IP adresine ihtiyacı olan bir firmaya bir B sınıfı blok ayrılırsa bu bloktaki 65534 kullanılabilir adresten 64734 tanesi kullanılmayacaktır. Aynı firmaya 4 tane C sınıfı blok ayrıldığında yeterli sayıda IP adresi verilmiş olacak ancak bu kez de firma içinde birden fazla şebeke kullanılacak ve yönlendirme gereksinimi ortaya çıkacaktır. Daha da önemli olan sorun, internet üzerinde bu firma için yönlendirme tablolarına 4 satır yazılması olacaktır. Bu da yönlendirme tablolarının çok fazla büyümesi demektir.

Internet zamanla geliştikçe sınıflı adresleme kullanımı sınırlar hale geldi. Yönlendirmeyi sağlayan cihazlardaki yönlendirme tabloları sınır değerlere kadar büyüdüğü halde aslında dağıtılan adreslerin pek azı kullanılıyordu. Bu da hem adres yetersizliğine hem de yavaş yönlendirmeye neden oluyordu.

3.3.2. CIDR

Önceki bölümde bahsedilen sorunlara çözüm olarak Sınıfsız - Alanlar Arası Yönlendirme (CIDR – Classless InterDomain Routing) kavramı geliştirilmiştir. CIDR kullanıldığında bir firmaya ihtiyacını karşılayacak sayıda sınıflı adres bloğu verilir ancak bu adresler sınıflar için belirlenmiş alt şebeke maskeleri yerine, verilen blokların hepsini tek bir şebeke olarak ifade edecek bir alt şebeke maskesi ile kullanılır. Böylece verilen bloklar hem firma içinde tek blok gibi kullanılabilir, hem de internette yönlendirme tabloları üzerinde tek bir özetleme ile belirtilebilir. CIDR kullanılarak internet yönlendirme tabloları önemli ölçüde küçültülmüştür. Bu da yönlendiriciler üzerindeki işlemci ve hafıza yükünü azaltmış, ayrıca yönlendirme işleminin de daha hızlı gerçekleşmesini sağlamıştır.

Önceki örnekteki 800 adrese ihtiyacı olan firmaya dönersek, CIDR kullanıldığında bu firmaya yine 4 tane C sınıfı blok ayrılır. Ancak varsayılan 255.255.255.0 (/24 ön ekli) alt şebeke maskesi yerine 255.255.252.0 (/22 ön ekli) alt şebeke maskesi kullanılır. Verilen blokların 200.10.20.0 – 200.10.21.0 – 200.10.22.0 ve 200.10.23.0 olduğunu düşünürsek, bu blokların 200.10.20.0/22 şeklinde tek blok olarak özetlenebileceğini görebiliriz. Özet blok 200.10.20.1 ile 200.10.23.254 arasındaki kullanılabilir adresleri kapsamaktadır. Bu, C sınıfı blokların adreslerini karşılamanın yanında boşa gidecek bazı şebeke ve broadcast adreslerinin de cihaz adreslemesinde kullanımına imkan verir. Görüldüğü gibi internetteki herhangi bir yönlendiricinin bu özet bloğa ait yönlendirme bilgisini bilmesi, firmanın kullandığı herhangi bir IP adresine erişim için yeterlidir.

CIDR kullanımının yararlarını aşağıdaki gibi özetlemek mümkündür:

- Yönlendirme tablolarının önemli ölçüde küçülmesi
- Şebekedeki trafiğin ve cihazlardaki işlemci ve hafıza yükünün azalması
- Şebekelere adres dağıtılırken sınıflı adreslemeye göre çok daha esnek olunabilmesi

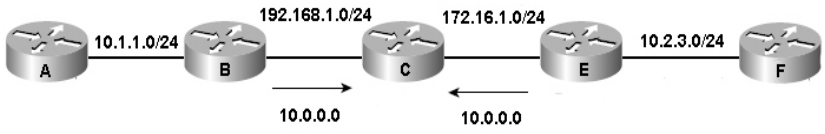
3.3.3. Sınıflı Yönlendirme Protokolleri

Sınıflı yönlendirme protokolleri güncelleme paketlerinde alt şebeke maskesi bilgisini göndermezler ve IP adreslerini sınıflı olarak değerlendirirler. Bu özellikleri yüzünden şebeke tasarımında kısıtlamalar getirirler. RIPv1 ve IGRP protokolleri sınıflı yönlendirme protokollerine örnektir.

Sınıflı yönlendirme protokollerinde,

- Şebeke sınırlarında otomatik özetleme yapılır.
- Farklı ana şebekeler arasında yönlendirme bilgileri iletilirken şebekenin sınıflı hali ile özetlenerek güncelleme yollanır.
- Aynı ana şebeke içinde (sınıflı bir blok içinde) yönlendirme güncellemeleri alt şebeke maskesi gönderilmeden yapılır.
- Bir ana şebeke içinde kullanılan alt şebeke maskesinin sabit olduğu varsayılır.

Sınıflı yönlendirme protokolleri kullanıldığında, alt şebeke maskesi güncellemelere dahil olmadığından çeşitli sorunlar meydana gelebilir. Bunlardan biri Şekil 3.5'te gösterilmiştir.



Şekil 3.5: Sınıflı yönlendirme protokollerinde ortaya çıkabilecek sorunlar

Burada görüldüğü gibi 10.0.0.0 ana şebekesine dahil 10.1.1.0/24 alt şebekesi, B yönlendiricisi tarafından 192.168.1.0 ana şebekesine ait bir bağlantı üzerinden C yönlendircisine duyurulmaktadır. Ancak daha önce belirtilen kurallara uygun olarak, farklı bir ana şebeke üzerinden duyurulduğu için, 10.0.0.0 olarak sınıflı bazda özetlenerek ve alt şebeke maskesi olmadan özetlenmiştir. Aynı şekilde E yönlendiricisi de 10.2.3.0/24 alt şebekesini farklı bir ana şebeke üzerinden (172.16.0.0) özetleyerek C yönlendiricisine duyurmaktadır. Bu durumda C yönlendiricisi, 10.0.0.0 şebekesine B üzerinden de E üzerinden de ulaşabileceğini düşünür. C yönlendiricisine 10.1.1.23 adresine gönderilmesi gereken paketler

geldiğinde ise bu bilgiye dayanarak B ve E yönlendiricilerine bağlantıları üzerinde yük dağılımı uygulayacaktır. Bunun anlamı ise, bir paketi B yönlendiricisine gönderirken, hemen sonraki paketi E yönlendiricisine yollaması ve paketlerin yarısının gitmesi gereken hedefe ulaşmamasıdır.

Sınıflı yönlendirme protokolü kullanılacak bir şebekede adresleme yapılırken sorun çıkmaması için dikkatli olunmalıdır. Yukarıdaki gibi bir sonuç oluşmaması için, şebekede bir ana şebekenin alt şebekelerinden adresler verilen kısımları birbirine bağlı olmalı, aralarına başka bir ana şebekeye ait bağlantılar girmemelidir. Bu durumda, sınırlarda özetleme yapılsa da yönlendirmede bir sorun ortaya çıkmayacaktır.

Sınıflı bir yönlendirme protokolü kullanıldığında, sorun çıkmaması için gerekli tasarım ilkelerine dikkat edilse de, tüm şebeke üzerinde alt şebeke maskelerinin sabit olmasının gerekmesi adreslerin verimsiz kullanılmasına yol açar. Eğer şebekenin bir bölümündeki 200 cihaz adreslenirken /24 ön ekli alt şebeke maskesi kullanılırsa, tüm şebekedeki bölümler ve bağlantılarda bu maske kullanılmak zorundadır. Oysa iki yönlendirici arasındaki noktadan noktaya bir bağlantı için sadece 2 IP adresi yeterli olacaktır. Böyle bir bağlantıya /24 ön ekli adresler verildiğinde bloktaki 254 adresin 252 tanesi boşa gitmiş olacaktır.

3.3.4. Sınıfsız Yönlendirme Protokolleri

Sınıfsız yönlendirme protokolleri, sınıflı yönlendirme protokollerinin getirdiği kısıtlamaları aşmak için geliştirilmiştir. RIPv2, OSPF, IS-IS ve EIGRP sınıfsız yönlendirme protokollerine örnektir. Özellikleri aşağıda belirtilmiştir:

- Yönlendirme güncellemeleri ile alt şebeke maskesi bilgisi de gönderilir.
- Aynı ana şebekeye ait alt şebekelerde farklı alt şebeke maskeleri kullanılabilir, buna Değişken Uzunluklu Alt Şebeke Maskesi (VLSM – Variable-Length Subnet Mask) denir.
- CIDR kullanımına imkan verirler.
- Bir ana şebeke içinde de özetleme yapılabilir. Bu şebeke yöneticisinin elle ayarlaması gereken bir işlemdir.

4. YÖNLENDİRME PROTOKOLLERİ

4.1. RIP

Yönlendirme Bilgisi Protokolü RIP (Routing Information Protocol), ilk geliştirilen ve en basit uzaklık vektörü protokollerinden biridir. Basit olması dolayısıyla çok geniş olmayan otonom sistemlerin içinde kullanılır. Ancak kolay uygulanabilmesini sağlayan basitliği uygulamada pek çok kısıtlamayı da beraberinde getirir.

RIP'in ilk sürümü (RIPv1) 1988 yılında RFC 1058 belgesi ile belirlenmiştir. RIP'in bu ilk sürümü sınıflı bir yönlendirme protokolüdür. IP adreslerinin kullanıldığı şebekeler zamanla sayıca artmış, boyutları da büyümüş ve bu yüzden RIP'in getirdiği kısıtlamalar, kullanımını engeller hale gelmiştir. Bu engellerin bazıları 1994te yayınlanan RFC 1723 belgesi ile tanımlanan RIPv2, RIP güncelleme paketlerinin daha fazla bilgi taşımasına imkan sağlıyordu. Bu sayede alt şebeke maskesi de güncellemelerde taşınabilir hale geldi, yani RIPv2 sınıfsız olarak kullanıma imkan sağladı. Ayrıca, güncelleme paketlerinde taşınan ek bilgi, yönlendirme güncellemelerinin basit bir kimlik doğrulama işlemi ile yapılabilmesini ve daha güvenli güncellemeleri sağladı. RIPv2'nin getirdiği başka bir iyileştirme ise güncellemelerin broadcast olarak değil multicast olarak gönderilmesidir. Görüldüğü gibi RIPv2 ile RIPv1'in çalışma ilkeleri tamamen değiştirilmemiş, bazı eklemelerle kısıtlamalarının ortadan kalkmasına çalışılmıştır. Her iki RIP sürümü de metrik olarak adım sayısını kullanmaktadır.

RIP'in eski ve basit bir yönlendirme protokolü olması ve yeni geliştirilen yönlendirme protokolleri, RIP'in artık gereksiz bir protokol olduğu anlamına gelmez. RIP uygun şebekelerde kararlı bir yapı sunar ve basit olduğundan kurulumu kolaydır. Bu bölümde RIP'in işleyişi ve her iki sürümünün paket yapıları açıklanmıştır.

4.1.1. RIP Güncellemeleri

RIP bir uzaklık vektörü protokolü olduğundan güncelleme için belirli aralıklarla yönlendirme tablosunu bağlı yönlendiricilere gönderir. Ancak çabuk öğrenim sağlamak için tetiklenmiş güncellemeler de kullanır. Bir yönlendirici güncelleme mesajı aldığında, bu mesaj kullanılan yollarda bir değişiklik bildiriyorsa, öncelikle kendi yönlendirme tablosunu günceller. Bunun için, gelen güncelleme mesajında ilgili şebekeye ait metrik değeri bir arttırılır ve güncellemeyi gönderen yönlendirici sonraki adım olarak belirlenir. RIP kullanan yönlendiriciler, bir şebekeye gidilecek sadece en iyi yolu tutarlar, bu yüzden önceden sahip olunan daha yüksek metrikli yola ait bilgi saklanmaz.

Yönlendirici kendi yönlendirme tablosunu güncelledikten sonra, şebekedeki diğer yönlendiricilerin de değişikliği öğrenebilmesi için güncelleme mesajları yollamaya başlar. Burada gönderilen güncelleme mesajları, periyodik gönderilen güncellemeleri etkilemez, güncelleme zamanı dolduğunda periyodik güncelleme mesajları da gönderilir.

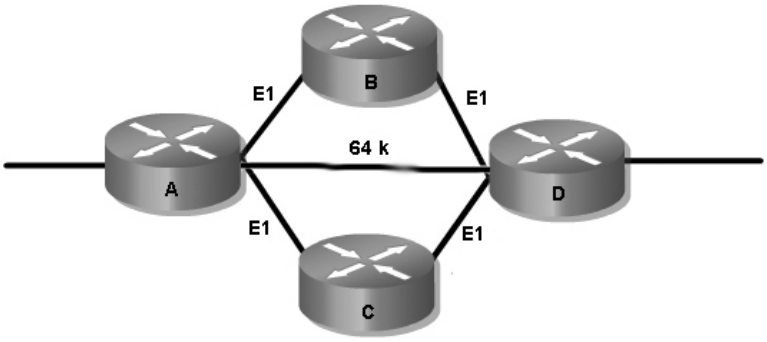
4.1.2. RIP Metriği

RIP'in her iki sürümü de bir hedef şebekeye olan uzaklığı belirlemek için adım sayısını metrik olarak kullanır. Hedef şebekeye ulaşmak için kullanılan yoldaki her yönlendirici bir adım olarak düşünülebilir ve her adım genelde 1 değerinde bir metrik ile ifade edilir. Bir yönlendirici güncelleme mesajı aldığında, bu mesajdaki şebekelere ait metrik değerlerine 1 ekleyerek yeni metrik değerlerini bulur, eğer herhangi bir şebeke için bulunan metrik yönlendirme tablosunun güncellenmesini gerektiriyorsa önceki bölümde anlatıldığı şekilde tablosunu günceller.

RIP geliştirilirken üst metrik değeri 15 olarak belirlenmiştir. Bunun nedeni, temel tasarımın daha büyük şebekelerde kullanıma uygun olmadığının düşünülmesiydi [4]. Bir yönlendiricinin aldığı güncelleme mesajında bir şebeke için metrik değeri bir arttırıldığında 16 oluyorsa, ki bu değer RIP için sonsuz anlamına gelir, o şebeke ulaşılamaz olarak kabul edilir. Bu kısıtlama yüzünden RIP protokolü, ancak en uzun yolu 15 adım olan şebekelerde kullanıma uygundur.

RIP'in metrik değerinin getirdiği diğer bir dezavantaj ise adım sayısının şebeke durumu veya aradaki bağlantıların özellikleri ile ilgili bilgi içermemesidir. Eğer

şebekedeki bağlantılar yakın özellikdelerse bu bir sorun oluşturmaz, ancak bazı bağlantıların band genişliği diğerlerinden çok daha azsa RIP'in sadece adım sayısına bakarak seçtiği en iyi yollar pratikte kullanılması istenen yollardan farklı olabilir. Buna bir örnek şekil 4.1'de gösterilmiştir.



Şekil 4.1: RIP metriğinin sorun yaratacağı durum

Bu örnekte A yönlendiricisinin D yönlendiricisi arkasındaki bir şebekeye paket göndereceğini düşünelim. RIP metrik olarak adım sayısını kullandığından en iyi yol olarak paketleri doğrudan D yönlendiricisine bağlı olduğu arabiriminden gönderecektir. Oysa B veya C yönlendiricisi üzerinden paketleri göndermesi, bu bağlantıların band genişlikleri göz önüne alındığında çok daha verimli olacaktı.

4.1.3. RIP'in kullandığı sayaçlar

RIP, performansını ayarlamak için çeşitli sayaçlar kullanır. Bunlar:

- **Yönlendirme güncellemeleri sayacı:** Periyodik güncellemeler için kullanılır. Varsayılan değeri 30 sn.dir. Her sıfırlandığında çakışmaları engellemek için rasgele bir süre eklenir
- **Yönlendirme geçersiz sayacı:** Bu sayaç boyunca bir yol bilgisi ile ilgili güncelleme alınmazsa bu bilginin geçersiz olduğuna karar verilir. Hold down sayacı başlatılır ve komşu yönlendiricilere bu şebekenin ulaşılamaz olduğu duyurulur. Ancak bilgi, yönlendirme silme sayacı sıfırlanmadan yönlendirme tablosundan silinmez. Varsayılan değeri 180 sn.dir.
- **Hold down sayacı:** Bu süre boyunca, ulaşılamadığı düşünülen bir şebeke ile ilgili gelen güncellemeler dikkate alınmaz. Varsayılan değeri 180 sn.dir.

- **Yönlendirme silme sayacı:** Bu süre dolduğunda geçersiz yol artık tablodan silinir. Varsayılan değeri 240 sn.dir.

4.1.4. RIP'in Kararlılık Özellikleri

RIP, uzaklık vektörü yönlendirme protokollerinin hızlı topoloji değişikliklerinde yaşadığı sorunlar için geliştirilmiş pek çok kararlılık özelliği kullanır. Örneğin yanlış yönlendirme bilgilerinin yayılmasını ve yönlendirme döngülerinin oluşmasını engellemek için "split horizon" ve "hold down sayacı" kurallarını kullanır. Ayrıca çabuk öğrenim sağlamak için topoloji değişikliklerinde tetiklemeli güncellemeler yapar.

Metrik değerine getirilmiş olan üst sınır ise sonsuza sayma sorununu ve yönlendirme döngülerinin sürekliliğini engeller [7].

4.1.5. RIP Güncelleme Paket Yapısı

RIP'in ikinci sürümü güncelleme paketinde daha fazla bilgi taşınmasına izin vermiştir. Dolayısıyla iki sürümün paket yapıları farklıdır. Şekil 4.2'de RIPv1 paketinin yapısı görülmektedir.

1	1	2	2	2	4	4	4	4
A	**B**	**S**	**C**	**S**	**D**	**S**	**S**	**E**

A: Kontrol
B: Sürüm
C: Adres Ailesi Belirleyicisi
D: Adres
E: Metrik
S: Sıfır

Şekil 4.2: RIPv1 paketi

Şekilde alanlar üzerindeki sayılar byte olarak alanın büyüklüğünü belirtir. Alanların açıklamaları aşağıda belirtilmiştir:

- **Kontrol:** Güncelleme paketinin amacını belirtir. Değeri 1 ise talep paketidir. Talep paketi ile paketi alan yönlendiriciden yönlendirme tablosunun tamamının veya bir kısmının gönderilmesi istenir

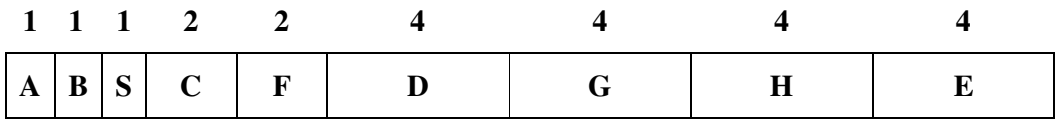
  Değeri 2 ise bu bir yanıt paketidir. Yönlendirme tablosunun tamamını veya bir kısmını içeren yanıt paketleri, talep paketlerine cevaben gönderilebileceği gibi güncelleme paketi de olabilirler.

3 ve 4 değerleri dikkate alınmaz, 5 değeri ise Sun Microsystems firmasının kullandığı bazı uygulamalar için ayrılmıştır.

- **Sürüm:** RIP sürümünü belirtir. İlk sürüm için 1 değerini alır.
- **Adres Ailesi Belirleyicisi:** Yönlendirilen 3. katman protokolünü belirtir. RIP çeşitli protokolleri yönlendirebilmek için geliştirilmiştir, bu yüzden her protokolün bir adres ailesi vardır. IP için bu değer 2'dir.
- **Adres:** Gidilecek hedef şebekeyi belirtir.
- **Metrik:** İlgili şebekeye ulaşmak için kaç adım gerektiğini belirtir. 1-15 arası değerler alabilir. Eğer değeri 16 ise ulaşılamayan bir şebekeyi ifade eder.
- **Sıfır:** Kullanılmayan alanlardır. 0 değeri verilir.

Bir RIP paketi içinde Adres Ailesi Belirleyicisi alanından Metrik alanına kadar olan kısım 25 kez tekrar edebilir. Bu şekilde 25 hedef şebekenin bilgisi tek bir RIP paketi ile diğer yönlendiricilere iletilebilir.

RIPv2 paketinin yapısı ise Şekil 4.3'te görülebilir.



A: Kontrol
B: Sürüm
C: Adres Ailesi Belirleyicisi
D: Adres
E: Metrik
F: Yönlendirme Etiketi
G: Alt Şebeke Maskesi
H: Sonraki Adım
S: Sıfır

Şekil 4.3: RIPv2 paketi

Görüldüğü gibi RIPv2 ilk sürüme oranla daha fazla bilgi taşıyabilmektedir. Alanların açıklamaları aşağıda belirtilmiştir:

- **Kontrol:** Güncelleme paketinin amacını belirtir. Değeri 1 ise talep paketidir. Talep paketi ile paketi alan yönlendiriciden yönlendirme tablosunun tamamının veya bir kısmının gönderilmesi istenir.

  Değeri 2 ise bu bir yanıt paketidir. Yönlendirme tablosunun tamamını veya bir kısmını içeren yanıt paketleri, talep paketlerine cevaben gönderilebileceği gibi güncelleme paketi de olabilirler.

3 ve 4 değerleri dikkate alınmaz, 5 değeri ise Sun Microsystems firmasının kullandığı bazı uygulamalar için ayrılmıştır.

- **Sürüm.** RIP sürümünü belirtir. RIPv2 için değeri 2'dir.
- **Adres Ailesi Belirleyicisi:** Yönlendirilen 3. katman protokolünü belirtir. RIP çeşitli protokolleri yönlendirebilmek için geliştirilmiştir, bu yüzden her protokolün bir adres ailesi vardır. IP için bu değer 2'dir. Eğer mesajdaki ilk değeri 0xFFFF ise paket kimlik sorgusu içeriyor anlamına gelir. Kimlik sorgulaması kullanılan durumlarda sonraki yönlendirme etiketi alanı sorgu tipini, kalan 16 oktetlik kısım ise şifre bilgisini taşır.
- **Yönlendirme etiketi:** RIP ile öğrenilen veya farklı bir kaynaktan öğrenilen bilgileri ayırmak için kullanılır. Eğer Kimlik sorgusu için kullanılacaksa değeri sorgu tipini belirtir ve 2 olur.
- **Adres:** Gidilecek hedef şebekeyi belirtir.
- **Alt Şebeke Maskesi:** İlgili adres için alt şebeke maskesi bilgisini içerir. Değeri 0 ise herhangi bir maske bilgisi belirtilmemiş anlamına gelir.
- **Sonraki Adım:** Gidilecek hedef şebeke için paketlerin gönderileceği sonraki yönlendiricinin adresini belirtir.
- **Metrik:** İlgili şebekeye ulaşmak için kaç adım gerektiğini belirtir. 1-15 arası değerler alabilir. Eğer değeri 16 ise ulaşılamayan bir şebekeyi ifade eder.
- **Sıfır:** Kullanılmaz. 0 değerini alır.

Kimlik sorgusu kullanılacağında 16 oktetlik son kısımda şifre bilgisi vardır. Eğer şifre 16 oktetten kısaysa sola dayalı şekilde yazılarak sağdaki kalan kısım sona kadar 0 ile doldurulur.

Bir RIP paketi içinde Adres Ailesi Belirleyicisi alanından Metrik alanına kadar olan kısım 25 kez tekrar edebilir. Bu şekilde 25 hedef şebekenin bilgisi tek bir RIP paketi ile diğer yönlendiricilere iletilebilir. Eğer kimlik sorgusu kullanılıyorsa sadece 24 hedef şebeke bilgisi taşınabilir.

4.2. IGRP

İç Şebeke Geçidi Yönlendirme Protokolü IGRP (Interior Gateway Protocol), Cisco Systems firması tarafından 1980lerde geliştirilmiş bir uzaklık vektörü protokolüdür. Cisco'nun IGRP'yi geliştirmesinin amacı, o sıralarda yaygın kullanımda olan RIPv1'in eksikliklerini gidererek otonom sistem içinde kararlı ve güvenilir yönlendirme yapabilen bir protokol oluşturmaktı.

1980lerin ortalarında en çok kullanılan iç yönlendirme protokolü RIPv1'di. Ancak RIPv1, küçük boyuttaki ve homojen bağlantılara sahip şebekelerde sorunsuzca kullanılsa da, daha büyük veya farklı bağlantı tipleri içeren şebekelerde kullandığı metrik (adım sayısı) ve metriğinin üst sınırı (16 metrik sonsuz kabul ediliyordu) yüzünden yeterince verimli olamıyordu. Ayrıca RIP'in sadece eş metrikli yollarda yük dağılımı uygulayabilmesi istenen esnekliği sağlayamıyordu.

IGRP'nin dezavantajı ise Cisco Systems firmasına ait olması ve bu yüzden sadece Cisco yönlendiriciler üzerinde çalıştırılabilmesiydi. IGRP'nin ilk geliştirilen sürümü, IP şebekelerinde çalıştırılmıştır. Ancak geliştirilmesi sırasında her türlü şebekede çalışması amaçlandığından, kısa süre sonra OSI Bağlantısız Şebeke Protokolleri (OSI CLNP – ConnectionLess Network Protocol) kullanılan şebekelerde de kullanılabilir hale getirilmiştir. Bu gelişmelerden sonra, hem Cisco yönlendiriclerinin çok tercih edilmesi, hem de IGRP'nin büyük şebekelerde daha güvenilir olması sayesinde IGRP pek çok firma tarafından RIP yerine kullanılmaya başlamıştır. IGRP'nin bu başarısında, tasarımı sırasında RIP'in çalışma ilkelerine benzerliğin korunması, RIP'in verimli özelliklerinin devam ettirilmesi ancak eksikliklerinin de başarılı şekilde tamamlanmasının etkisi büyüktür.

RIPv1'in pek çok eksiğini tamamlamasına rağmen IGRP de günümüzde yetersiz kalabilmektedir. Özellikle sınıflı bir yönlendirme protokolü olması, kullanımında pek çok sınırlamalar getirmiştir. IGRP için, RIP'e yapıldığı gibi eklentiler yapılarak ikinci bir sürüm çıkarılmamış, bunun yerine 1990'larda yine Cisco tarafından Geliştirilmiş IGRP (EIGRP) adıyla yeni bir protokol geliştirilmiştir. EIGRP protokolü ileri bölümlerde detaylı olarak incelenmiştir.

4.2.1. IGRP Güncellemeleri

IGRP, bir uzaklık vektörü yönlendirme protkolüdür ve güncellemelerinde diğer uzaklık vektörü protokollerinin kullandığı ilkeleri uygular. Güncellemeleri, RIP kadar sık olmasa da periyodiktir. İleri bölümlerde IGRP sayaçları ile ilgili daha detaylı bilgi verilecektir. IGRP, periyodik güncellemeler dışında, çabuk öğrenim sağlamak için topoloji değişiklikleriyle tetiklenen güncellemeler de kullanır. Bu güncellemeler tüm yönlendirme tablosunun bir özetini içerir ve komşu yönlendiricilere gönderilir [2].

Bir yönlendirici güncelleme mesajı aldığında, diğer uzaklık vektörü protokollerinde olduğu gibi, ilgili şebeke için mesajda belirtilen metrik değerine, gönderen ile arasındaki bağlantının metrik değerini ekleyerek bu şebekeye ulaşmak için kullanılabilecek yolun metrik değerini bulur. Eğer gerekiorsa yönlendirme tablosunu günceller.

IGRP sınıfsız bir yönlendirme protokolü olduğundan güncelleme mesajlarında alt şebeke maskesi bilgisi bulunmaz. Ayrıca güncellemeler broadcast olarak gönderilir.

4.2.2. IGRP Metriği

IGRP metrik olarak pek çok değerin bir kombinasyonunu kullanır. IGRP metriğinin hesaplanmasında bağlantının band genişliği, güvenilirliği, yükü, yaşanan gecikme ve Azami İletim Birimi (MTU) değerleri, şebeke yöneticisinin belirleyeceği ağırlıklarla formüle dahil olarak kullanılabilirler. Aslında tasarımda MTU metrik olarak kullanılmak için düşünülmüş olsa da, değeri takip edilir ancak hesaplamada kullanılmaz. IGRP metriği,

$$metrik = \left[K1 * BW + \frac{K2 * BW}{256 - L} + K3 * D \right] * \frac{K5}{R + K4} \qquad \textbf{(4.1)}$$

formülü ile hesaplanabilir. Formülde BW band genişliğini, L yükü, D gecikmeyi R ise güvenilirliği ifade eder. K1 – K5 arası değerler şebeke yöneticisinin belirleyebileceği ağırlık sabitleridir. K5 = 0 seçilirse son terim hesaplamaya dahil edilmez.

BW = 10^7 / band genişliği (kbit/s), D = gecikme (µs) / 10 olarak hesaplanır. L ve R değerleri ise bağlantı durumuna göre 0-255 arası tam sayı değerler alır.

Şebeke yöndeticisi ağırlıkları belirlemezse, varsayılan değerlerde K1 ve K3 1, diğerleri 0 değerini alır. Bu da metriğin sadece band genişliği ve gecikmeye göre hesaplanması demektir. Buradaki değerlerde bağlantı yükü ve güvenilirliği 1 ile 255; band genişliği 1200 bit/s ile 10 Gbit/s; gecikme ise 1 ile 2^{24} arasında değerler alabilir. Görüldüğü gibi metrik için oldukça geniş bir aralıkta değerler hesaplanabilir, bu da daha sağlıklı karar alınmasını sağlar. Formüldeki değerlerin ağırlıklarının belirlenmesi de şebeke yöneticisinin kontrolünde olduğundan en iyi yol seçiminde esneklik elde edilmiş olur [7].

IGRP'nin esneklik sağlayan başka bir özelliği ise metrikleri eşit olmayan yollar üzerinde de yük dağılımını desteklemesidir. Varsayılan ayarlarda eş metrikli yollar üzerinde yük dağılımı uygulanır, bağlantılardan birinin kullanılamaz hale gelmesi durumunda trafik tümüyle diğer hatta geçer. Şebeke yöneticisinin varsayılan ayarları değiştirmesi durumunda aynı özellik farklı metriklere sahip yollar üzerinde de kullanılabilir. Bunun için yapılması gereken, ayarlardaki varyans değerini (varsayılan değer = 1) isteğe uygun olarak değiştirmektir. Örneğin bu değer 2 yapıldığında, en iyi yolun metriğinin 2 katına kadar metrik değerine sahip yollara da yük dağılımı uygulanır. Bu durumda, en iyi yol diğer yoldan 2 kat fazla kullanılacak ancak ikinci yol da tamamen boş kalmamış olacaktır.

IGRP metriğinin RIP'e göre bir avantajı da adım sayısının üst sınırının varsayılan olarak 100, azami 255 olabilmesidir. Adım sayısı IGRP metriğine doğrudan dahil olmasa da paketlerin şebekedeki yaşama süresini belirlemek için kullanılır [2] Bu sayede IGRP daha geniş şebekelerde kullanılabilir.

4.2.3. IGRP'nin Kullandığı Sayaçlar

Diğer uzaklık vektörü protokolleri gibi, IGRP de performansını ayarlamak için çeşitli sayaçlar kullanır. Bunlar:

- **Yönlendirme güncellemeleri sayacı:** Periyodik güncellemeler için kullanılır. Varsayılan değeri 90 sn.dir
- **Yönlendirme geçersiz sayacı:** Bu sayaç boyunca bir yol bilgisi ile ilgili güncelleme alınmazsa bu bilginin geçersiz olduğuna karar verilir. Hold down sayacı başlatılır ve komşu yönlendiricilere bu şebekenin ulaşılamaz olduğu duyurulur. Ancak bilgi, yönlendirme silme sayacı sıfırlanmadan yönlendirme

tablosundan silinmez. Varsayılan değeri güncelleme sayacının 3 katıdır (270 sn)

- **Hold down sayacı:** Bu süre boyunca, ulaşılamadığı düşünülen bir şebeke ile ilgili gelen güncellemeler dikkate alınmaz. Varsayılan değeri güncelleme sayacının 3 katı artı 10sn'dir. (280 sn)
- **Yönlendirme silme sayacı:** Bir yol bilgisinin yönlendirme tablosundan silinmesi için geçmesi gereken zanaı belirler. Varsayılan değeri güncelleme sayacının 7 katıdır. (630 sn)

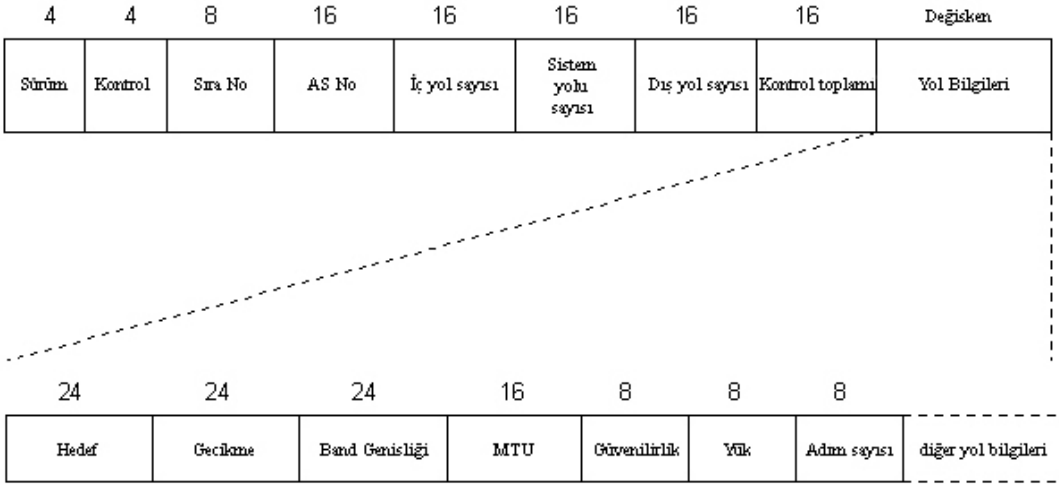
4.2.4. IGRP'nin Kararlılık Özellikleri

IGRP bir uzaklık vektörü protokolü olduğundan, kararlılık sağlamak, yönlendirme döngülerini engellemek ve yanlış yönlendirme bilgilerinin yayılmasını engellemek için çeşitli araçlar kullanır. Bunlar "split horizon" kuralı, "hold-down" sayaçları ve "poison reverse" güncellemeleridir.

IGRP ayrıca sonsuza sayma sorununu da, eğer bilinen bir yolun adım sayısı artarsa, o yolu yönlendirme tablosundan çıkararak çözer. Burada yönlendiricinin değerlendirmesi, başka bir yönlendircinin yolu ulaşılmaz olarak duyurduğu fikrine dayanır [2]

4.2.5. IGRP Güncelleme Paket Yapısı

Şekil 4.4'te IGRP paketinin yapısı görülmektedir. [8]



Şekil 4.4: IGRP paket yapısı

Şekilde alanların üzerindeki sayılar bit olarak alanların büyüklüğünü belirtmektedir. Alanların açıklamaları aşağıdadır:

- **Sürüm:** IGRP sürümünü belirtir. Her zaman 0x01 değerini alır
- **Kontrol:** Paketin istek mi yoksa güncelleme mi olduğunu belirtir. 0x01 değeri istek, 0x02 değeri güncelleme anlamına gelir.
- **Sıra No:** Her güncellemede bir arttırılır. Böylece paketi alan yönlendiricinin eski bir güncellemeyi kullanmaması sağlanır.
- **AS No:** IGRP işleminin numarasıdır.
- **İç Yol Sayısı:** Bu güncellemedeki doğrudan bağlı şebekelerin sayısını gösterir.
- **Sistem Yolu Sayısı:** Bu güncellemedeki doğrudan bağlı olmayan şebekelerin sayısını gösterir.
- **Dış Yol Sayısı:** Bu güncellemedeki AS dışından alınan yol bilgilerinin sayısını gösterir.
- **Kontrol Toplamı:** Paketin iletimde zarar görüp görmediğinin kontrolü içindir.
- **Hedef:** Hedef şebeke adresidir.
- **Gecikme:** Yol bilgisinin gecikme değeridir.
- **Band Genişliği:** Yol bilgisinin band genişliği değeridir.
- **MTU:** Yol üzerindeki bağlantıların en küçük MTU değeridir.
- **Güvenilirlik:** Yolun güvenilirlik değeridir. 0x01 ile 0xFF arasında değer alır. 0xFF güvenli demektir.
- **Yük:** Bağlantının yük durumu değeridir. 0x01 ile 0xFF arasında değer alır. 0xFF tamamen dolu olduğu anlamına gelir.
- **Adım Sayısı:** Hedef şebekenin uzaklığını adım sayısı olarak gösterir. 0x00 ile 0xFF arasında değer alır. 0x00 doğrudan bağlı şebekeleri belirtir.

4.3. EIGRP

EIGRP protokolü, Cisco Systems firması tarafından IGRP temel alınarak geliştirilmiş bir yönlendirme protokolüdür. Önceki bölümlerde belirtildiği gibi hem RIP hem de IGRP gelişen şebeke teknolojilerinin ihtiyaçlarını karşılamakta yetersiz kalmışlardır. Bu yüzden EIGRP geliştirilirken bağlantı durumu protokollerin özellikleri, uzaklık vektörü protokollerinin özellikleri ile birleştirilmiş, ancak çalışması sırasında kullandığı algoritma tamamen yenilenmiştir. EIGRP'nin kullandığı algoritmaya Yayılan Güncelleme Algoritması (DUAL – Diffusing Update Algorithm) adı verilir, bu algoritma Dr. J. J. Garcia-Luna-Aceves tarafından geliştirilmiştir.

EIGRP, IGRP temel alınarak geliştirildiğinden, IGRP kullanılan yönlendiriciler ile tamamen uyumlu ve ortak çalışmaya imkan sağlar. Otomatik bir yeniden dağıtım mekanizması sayesinde IGRP yönlendirme bilgileri EIGRP'ye; EIGRP yönlendirme bilgileri de IGRP'ye aktarılabilir. Bu sayede halen IGRP kullanılan bir şebekesinin adım adım EIGRP'ye geçirilmesi kolay olabilmektedir. Bu iki protokolün metrikleri doğrudan birbirlerine çevrilebildiğinden birinin diğerinden aldığı yol bilgilerinin kendi elde ettiği yol bilgileri ile kıyaslanması kolay ve güvenlidir.

EIGRP de IGRP gibi sadece Cisco yönlendiricilerde kullanılabilen bir protokoldür. Hem uzaklık vektörü hem de bağlantı durumu protokollerinin özelliklerini kullandığından melez bir yönlendirme protokolü olarak adlandırılır. Bazı kaynaklarda gelişmiş uzaklık vektörü protokolü olarak da adlandırılmaktadır. Günümüzdeki protokoller içinde en geniş olanakları sunan protokoldür ve özellikle kullanımının kolay olması; IP, IPX ve Apple Talk gibi çeşitli protokolleri desteklemesi nedeniyle pek çok şebekede tercih edilebilir bir yönlendirme protokolüdür. [7]

4.3.1. EIGRP özellikleri

EIGRP'yi diğer yönlendirme protokollerinden ayıran temel özellikleri, hem uzaklık vektörü hem bağlantı durumu protokollerinin özelliklerini taşıması, çabuk öğrenim sağlaması, değişken uzunluklu alt şebeke maskesi (VLSM) kullanımını desteklemesi, birden fazla üçüncü katman protokolünü yönlendirebilmesi ve kısmi güncellemelere olanak vermesidir.

EIGRP kullanılan bir yönlendirici, komşularının yönlendirme tablolarını bir yol kullanılamaz olduğunda alternatif yolları hızla bulabilmek amacıyla saklar. Bu bilgilerden yeni bir yol bulunamazsa, yönlendirici bu kez komşularını alternatif bir yol bulunması için sorgular. Bu sorgu işlemi, yeni bir yol bulunana kadar devam ettirilir.

EIGRP'nin VLSM kullanımını desteklemesi sayesinde şebeke sınırlarında yönlendirme bilgileri otomatik olarak özetlenebilir. Ayrıca şebeke yöneticisi gerekli ayarları yaptığı taktirde, şebekenin herhangi bir yerindeki yönlendiricinin herhangi bir arayüzünde özetleme yapılabilir.

EIGRP, birden fazla şebeke katmanı protokolünü yönlendirebilir. Bu protokollerden bazıları IP, Novell Netware ve Apple Talk'tır. IP için kullanıldığında, OSPF, RIP, IGRP, IS-IS ve BGP protokollerinden öğrenilen yönlendirme bilgilerini yeniden dağıtabilir. Novell Netware versiyonu, Novell RIP veya SAP (Service Advertisement Protocol) ile öğrenilen yönlendirme bilgilerini dağıtır. Apple Talk için kullanıldığında ise RTMP (Routing Table Maintenance Protocol) ile öğrenilen bilgileri yeniden dağıtır.

EIGRP, periyodik güncelleme yapmaz. Sadece bir şebekeye ulaşılan yolun metrik değeri değiştiğinde kısmi güncellemeler gönderir. Bu kısmi güncellemelerin yayılması otomatik olarak sınırlanarak yalnızca bu bilgiye ihtiyacı olan yönlendiricilerin güncellenmesi sağlanır. Bu özellikleri sayesinde EIGRP, güncellemeler için IGRP'ye göre çok daha az band genişliği kullanır.

4.3.2. EIGRP'nin Kullandığı Alt İşlemler ve Teknolojiler

EIGRP, en iyi yönlendirme performansını sağlamak için, kendisini diğer yönlendirme protokollerinden ayıran dört temel teknolojiyi kullanır. Bunlar, komşuluk kurulması/yenilemesi, Güvenli İletim Protokolü (RTP – Reliable Transport Protocol), DUAL algoritmasi ve protokole bağlı modüllerdir.

Komşuluk kurulması ve yenilenmesi işlemi, EIGRP kullanılan yönlendiricilerin doğrudan bağlı oldukları şebekelerdeki diğer yönlendiricileri dinamik olarak öğrenmesini sağlar. Yönlendiriciler komşu olarak algıladıkları diğer yönlendiricilerin ulaşılamaz veya kullanılamaz olduğunu da farketmelidir. Bunu sağlamak için belirli aralıklarla gönderilen, küçük ve şebekeye az yük getiren merhaba paketleri kullanılmaktadır. Yönlendirici, komşusundan merhaba paketlerini düzenli olarak aldığı sürece o komşusunun ulaşılabilir olduğunu ve yönlendirme bilgilerinin karşılıklı olarak iletilebileceğini anlar.

RTP protokolü, EIGRP paketlerinin tüm komşu yönlendiricilere garantili ve sıralı şekilde ulaşmasından sorumludur. RTP, EIGRP paketlerinin multicast veya unicast gönderilebilmesini destekler. Verimlilik düşünülerek sadece belirli EIGRP paketleri güvenli olarak iletilir. Ethernet gibi çoklu erişime açık şebekelerde merhaba paketlerinin her komşuya ayrı ayrı gönderilmesi gereksizdir; böyle durumlarda EIGRP, onaylanmasına gerek olmadığı belirtilen tek bir multicast paketi gönderir. Güncelleme paketleri gibi bazı paketler için ise onay gerekmektedir. RTP protokolünün, onay gerektiren paketler beklemedeyken multicast paketlerini hızlı bir şekilde yollamasını sağlayan özelliği, değişken bağlantı hızlarının olduğu bir şebekede öğrenim süresini kısaltır.

DUAL sonlu durum mekanizması, bütün yönlendirme kararlarında tüm komşu yönlendiricilerin duyurduğu tüm yol bilgilerini takip eder. DUAL algoritması, en iyi ve kesinlikle döngüsüz yolları seçerken uzaklık bilgisini kullanır. En iyi yolları seçerken en iyi ikinci yolları da alternatif yol bilgisi olarak bir tabloda saklar. Buradaki alternatif yol, bir yönlendirme döngüsü oluşturmadan bir şebekeye paket gönderilebilecek komşu yönlendiriciyi belirler. Bir komşu ulaşılamaz olduğunda veya bir topoloji değişikliği yaşandığında, DUAL algoritması alternatif yolları tarar. Eğer ilgili şebekeye ulaşmak için bir alternatif yol var ise, yeni bir hesaplamaya gerek kalmadan bu alternatif yol kullanılmaya başlanır. Bu şekilde herhangi bir

topoloji değişikliğinde paketlerin yollanmasındaki kesinti en aza indirgenmiş olur. Eğer kontrolde bir şebeke için alternatif bir yol bulunamazsa ancak komşu yönlendiricilerden halen duyuruluyorsa, yeni bir hesaplama yapılması gerekecektir. Bu yeniden hesaplama işlemci gücünü çok fazla kullanmıyor olsa da, öğrenim süresini uzatacağından gereksiz yeniden hesaplamalardan kaçınmak faydalıdır.

Protokole bağlı modüller, yönlendirilen üçüncü katman protokolüne özel ihtiyaçlardan sorumludur. Örneğin IP-EIGRP modülü, IP ile zarflanan EIGRP paketlerinin gönderilip alınmasından sorumludur. IP-EIGRP, DUAL algoritması ile bulunan IP şebekesi yollarını IP yönlendirme tablosunda tutar, ayrıca diğer IP yönlendirme protokollerinden öğrenilen yönlendirme bilgilerinin yeniden dağıtımını gerçekleştirir. EIGRP, her üçüncü katman protokolü için farklı bir yönlendirme tablosu oluşturur.

4.3.3. EIGRP Yönlendirme Kavramları

EIGRP dört temel yönlendirme kavramına dayanır. Bunlar, komşu tablosu, topoloji tablosu, yol durumu ve yol etiketidir. Bu kavramlara daha detaylı göz atarsak:

Komşu tablosu: Bir yönlendirici yeni bir komşu keşfettiğinde, bu komşu yönlendiricinin adresini ve bağlı olduğu arayüzü komşu tablosuna kaydeder. Her yönlendirilen üçüncü katman protokolü için ayrı bir komşu tablosu oluşturulur. Yönlendirici, komşusundan merhaba paketlerini aldığı sürece komşuluk ilişkisi devam eder; ancak bir tutma zamanı boyunca merhaba paketi alınmazsa komşuya ulaşılamadığına karar verilir ve DUAL algortiması topoloji değişikliğinden haberdar edilir. Örnek bir komşu tablosu Şekil 4.5'te görülmektedir. Hemen sonrasında da tablodaki bilgiler açıklanmıştır. [2]

```
Router# show ip eigrp neighbors
IP-EIGRP Neighbors for process 100
Address         interface    Holdtime   Uptime    Q      Seq      SRTT      RTO
                             (secs)     (h:m:s)   Count  Num      (ms)      (ms)
140.100.48.22   Ethernet1    13         0:00:41   0      11       4         20
140.100.32.22   Ethernet0    14         0:02:01   0      10       12        24
140.100.32.31   Ethernet0    12         0:02:02   0      4        5         2
```

Şekil 4.5: EIGRP komşu tablosu

- **Adres:** Komşu yönlendiricinin adresidir.
- **Arabirim:** Yönlendircinin merhaba mesajını aldığı arabirimidir.
- **Tutma Zamanı:** Bu komşunun ulaşılamaz kabul edilmeden önce merhaba paketi beklenecek zamanı belirtir. Alınan her merhaba paketinde bu sayaç baştan başlatılır. Varsayılan değeri 15 sn'dir.
- **Komşuluk süresi:** Karşı yönlendirici ile kurulan komşuluğun başladığı zamandan o ana kadar geçen süreyi gösterir.
- **Kuyruk Sayacı:** Kuyrukta gönderilmeyi bekleyen EIGRP paketlerinin (güncelleme, sorgu ve cevap) sayısını gösterir.
- **Sıra numarası:** Komşu yönlendiricden alınan son paketin sıra numarasını gösterir.
- **SRTT (Smooth Round Trip Time):** Komşu yönlendirciye bir paketin gönderilmesi ile o pakete onay gelmesi arasında geçen süreyi gösterir.
- **RTO (Retransmisson Timeout):** Bir paket tekrar gönderilmeden önce ne kadar süre daha onay bekleneceğini gösterir. Bu süre boyunca onay gelmezse paket yeniden gönderilir.

Bu tablodaki sıra numarası, RTO gibi bilgiler aynı zamanda RTP protokolünün çalışması için de gerekli bilgilerdir.

Topoloji Tablosu: EIGRP topoloji tablosu, komşu yönlendiriciler tarafından duyurulan tüm hedef şebekelerin tutulduğu tablodur. Diğer tablolar gibi, yönlendirilen her üçüncü katman protokolü için ayrı bir topoloji tablosu oluşturulur. Topoloji tablosundaki her kayıt, hedef şebeke adresini ve bu adresi duyuran komşu yönlendiricilerin bilgisini içerir. Her komşu için bu tabloda, komşunun hedef şebeke için duyurduğu metrik değeri de kaydedilir. Bu değer, komşu yönlendiricinin yönlendirme tablosunda, o şebeke için görülen metrik değeridir. Ayrıca hedef şebekeye ulaşmak için yönlendiricinin kullanacağı metrik değeri de bu tablo üzerinde hedef adresi ile ilişkilendirilir. Bu metrikler, kendisine duyurulan metrik değerlerine aradaki bağlantıların metrik değerlerinin eklenmesi ile bulunan değerlerdir. Şekil 4.6. da örnek bir EIGRP topoloji tablosu görülmektedir.

```
Router# show ip eigrp topology
IP-EIGRP Topology Table for process 100
Codes:P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status
P 140.100.56.0 255.255.255.0, 2 successors, FD is 0
via 140.100.32.22 (46251776/46226176), Ethernet0
via 140.100.48.22 (46251776/46226176), Ethernet1
via 140.100.32.31 (46277376/46251776), Ethernet0
P 140.100.48.0 255.255.255.0, 1 successors, FD is 307200
via Connected, Ethernet1
via 140.100.48.22 (307200/281600), Ethernet1
140.100.32.22 (307200/281600), Ethernet0
via 140.100.32.31 (332800/307200), Ethernet0
```

Şekil 4.6: EIGRP topoloji tablosu

Bu tablodaki kodların anlamı aşağıdadır:

- P: Pasif. Yönlendirci herhangi bir komşudan herhangi bir EIGRP duyurusu almamıştır ve şebeke kararlıdır.
- A: Aktif. Bir yol kullanılamaz olduğunda eğer alternatif bir yol da yoksa komşu yönlendiriciler sorgulanarak yeni bir yol bulunmaya çalışılır. Bu yeniden hesaplama süresince yönlendirici aktif durumdadır.
- U: Güncelleme. Yönlendiricnin komşusuna bir güncelleme paketi gönderdiğini belirtir.
- Q: Sorgu. Yönlendircinin komşusuna bir sorgu paketi gönderdiğini belirtir.
- R: Yanıt. Yönlendiricinin komşusuna bir yanıt paketi gönderdiğini belirtir.
- r: Sorgu sayacıyla beraber kullanılır. Yönlendircinin komşusuna bir sorgu paketi gönderdiğini ve yanıt beklediğini gösterir.

Bu kodlardan biri ile başlayan satırlarda hedef şebeke adresleri ve alt şebeke maskeleri görülebilir. Altlarındaki satırlarda ise bu hedef şebekeye gidilebilecek tüm olası yollar bulunur. Parantez içindeki sayılar metriklerdir. İlk sayı yönlendirinin kendi kullanacağı metrik; ikinci sayı, komşunun duyurduğu metrik değeridir[2].

Yol Durumu: Bir yol bilgisi iki durumda olabilir. Bunlardan biri pasif durumdur. Pasif durumda yönlendirci herhangi bir hesaplama yapmıyordur ve şebeke kararlı durumdadır. Eğer bir yol kullanılamaz olursa yönlendirici alternatif yollarının olup olmadığına bakar. Alternatif bir yola sahipse yeniden hesaplamaya gerek duymadan o yolu kullanır. Ancak alternatif bir yola sahip değilse komşularını sorgulamak ve aldığı bilgiler ile yeni bir hesaplama yapmak zorundadır. Bu hesaplama sırasında ise aktif duruma geçer. Bu durumda ilgili hedefe yönlendirme yapılamayacağından veri akışında kesinti olur.

Sorgu durumu gerektiğinde, yönlendirici tüm komşularına bir sorgu paketi gönderir. Komşular eğer ilgili şebekeye ulaşılabilecek alternatif bir yol biliyorlarsa bunu yanıt olarak gönderirler. Eğer komşuların da alternatif bir yolu yoksa onlar da tekrar hesaplama durumuna geçerler. Tüm komşulardan sorguya yanıt gelene kadar hedef şebekeye ait yol bilgisi pasif duruma geçemez. Tüm komşuların yanıtı ulaştığında yeniden hedef şebekeye ulaşılabilecek en iyi yol seçilir ve yönlendirme işlemine başlanabilir.

Yol Etiketi: EIGRP iç ve dış yönlendirme bilgilerini destekler. İç yönlendirme bilgileri EIGRP'ye tanımlı olan otonom sistem içindeki yollardır. Bu yüzden EIGRP kullanan her doğrudan bağlı şebeke iç yönlendirme bilgisi ile algılanır ve tüm EIGRP otonom sisteminde bu şekilde duyurulur. Dış yönlendirme bilgileri ise diğer yönlendirme protokollerinden öğrenilmiştir veya statik olarak yönlendirme tablosuna şebeke yöneticisi tarafından yazılmışlardır. Dış yönlendirme bilgileri kaynaklarını belirtir şekilde etiketlenirler. Yol etiketleri aşağıdaki bilgileri içerir:

- Dış yol bilgisini dağıtan EIGRP yönlendiricisinin kimliği
- Hedef şebekenin otonom sistem numarası
- Şebeke yöneticisinin ayarlayabileceği yönetimsel etiket
- Dış yönlendirme protokolünün kimliği
- Dış yönlendirme protokolünün metrik değeri
- Varsayılan yol için bit işaretleri

Yol etiketleri, yönlendirme bilgilerinin ayırt edilmesini sağlayarak şebeke yöneticisine kontrolde esneklik sağlar[7].

4.3.4. EIGRP Metriği

EIGRP metriği temelde IGRP metriğine benzer. Aradaki fark EIGRP metriğinin 32 bitlik bir alanda tutulmasıdır. Bu da kararların daha detaylı ve daha ince yapılmasına olanak sağlar.

Metrik için IGRP ile aynı formül kullanılır:

$$metrik = \left[K1 * BW + \frac{K2 * BW}{256 - L} + K3 * D \right] * \frac{K5}{R + K4} \quad \textbf{(4.2)}$$

Varsayılan değerlerde IGRP'de olduğu gibi K1 ve K3 1 değerini, diğerleri 0 değerini alır. K5 = 0 olduğunda son terim hesaplamaya dahil edilmez.

EIGRP de metrik değerleri eşit olan yollar arasında otomatik olarak yük dağılımı yapar. Metrik değerleri eşit olmayan yollar üzerinde yük dağılımı uygulamak için şebeke yöneticisinin varsayılan varyans değerini isteğe uygun olarak değiştirmesi gerekir.

4.3.5. EIGRP Paketleri

EIGRP, merhaba, onay, güncelleme, sorgu ve yanıt paketlerini kullanır.

Merhaba Paketleri: Bu paketler komşuluk ilişkisinin başlaması ve sürmesi için belirli aralıklarla gönderilen paketlerdir. Multicast olarak ve onay gerektirmeyecek şekilde gönderilirler. Kullanılan bağlantıya bağlı olarak gönderim periyodu değişir. Merhaba paketlerinin gönderim zamanları Tablo 4.1'de gösterilmiştir.

Tablo 4.1: EIGRP Merhaba periyotları

		Merhaba periyodu (sn)
Yerel Alan Arabirimi	Hepsi	5
Geniş Alan Arabirimi	HDLC ve PPP	5
	FR, X25 (BW < T1)	60
	FR, X25 (BW > T1)	5
	FR, X25 (Noktadan noktaya alt arabirim tanımlanmışsa	5

Onaylama Paketleri: Bu paketler güvenli iletilmesi gereken paketler alındığında, göndericiye paketin alındığını iletmek için gönderilirler. Herhangi bir veri taşımayan merhaba paketleridir. Sıfırdan farklı bir onay numarası içerirler ve sadece alıcının adresine gönderilirler.

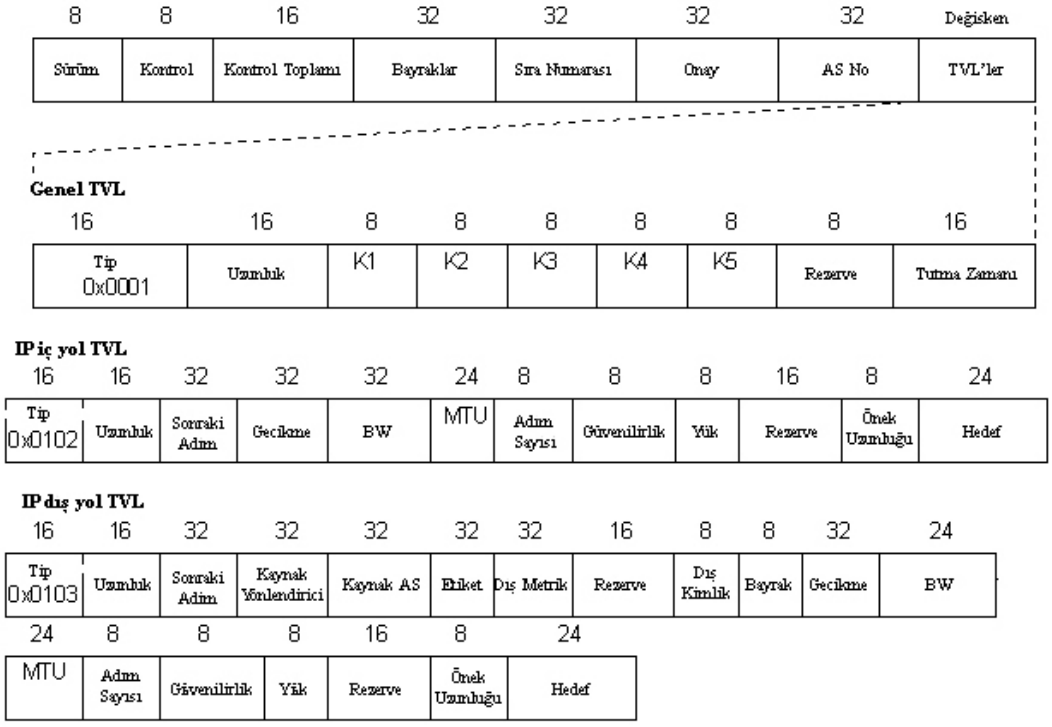
Güncelleme Paketleri: Bu paketler hedef şebekelerin ulaşılabilirliğini duyurmak için kullanılırlar. Yeni bir komşu keşfedildiğinde, topoloji tablosunu oluşturabilmei için, o komşunun adresine güncelleme mesajı gönderilir. Bir topoloji değişikliği durumunda ise güncelleme paketleri multicast olarak tüm komşuların alacağı şekilde gönderilir. Tüm güncelleme paketleri güvenilir olarak iletilir ve onay mesajı istenir.

Sorgu Paketleri: Bu paketler bir yol kullanılamaz olduğunda yönlendiric alternatif bir yola sahip değilse gönderilir. Multicast olarak güvenilir şekilde gönderilir.

Yanıt Paketleri: Bu paketler sorgu paketlerine cevaben, alternatif yol bilgisinin bulunduğunu iletmek için gönderilir. Yanıt paketleri sorguyu yapan yönlendiricinin adresine güvenilir olarak gönderilir.

4.3.5.1. EIGRP Paket Yapısı:

Şekil 4.7'de EIGRP paket yapısı görülmektedir. [8]



Şekil 4.7: EIGRP paketi

Şekilde alanların üzerindeki sayılar bit olarak alanların büyüklüğünü belirtmektedir. Alanların açıklamaları aşağıdadır:

- **Sürüm:** IGRP sürümünü belirtir. Her zaman 0x01 değerini alır
- **Kontrol:** EIGRP Paket tipini belirler. Güncelleme paketi için 1, sorgu paketi için 3, yanıt paketi için 4, merhaba paketi için 5, IPX SAP paketi için 6 değerini alır.
- **Kontrol Toplamı:** Paketin iletimde zarar görüp görmediğinin kontrolü içindir.
- **Bayraklar:** Çeşitli kontroller için gerekli işaretlerdir
- **Sıra Numarası:** RTP tarafından kullanılan sıra numarasıdır.
- **Onay:** Komşudan son duyulan paket numarasıdır. Sıfırdan farklı onay değerine sahip merhaba paketleri onay paketidir.
- **AS no:** EIGRP alanının otonom sistem numarasıdır.
- **TVL (Time/Length/Value):** Hepsi tip ve uzunluk alanları ile başlayan çeşitli TVL'ler vardır. Ortak olan ilk iki alandan sonra TVL tipine göre alanlar farklılık gösterir.
- **Genel TVL:** Metrik için kullanılan K değerlerini belirler.
- **IP İç Yol TVL:** İç yönlendirme bilgilerini taşır.
  - **Tip:** 0x0102 değerini alır
  - **Uzunluk:** TVL'nin uzunluğunu belirtir.
  - **Sonraki Adım:** Bu şebekeye ulaşmak için paketin gönderileceği yönlendiricinin adresidir.
  - **Gecikme, Band Genişliği, MTU, Güvenilirlik ve Yük:** Metrik hesabı için kullanılan değerlerdir.
  - **Adım sayısı:** 0x00 ve 0xFF arasında değer alır. 0x00 doğrudan bağlı şebekeyi ifade eder.
  - **Önek Uzunluğu:** Hedef şebekenin alt şebeke maskesini belirtir.
  - **Hedef:** Hedef şebeke adresidir.

- **Rezerve:** 0x0000 değeri alır ve kullanılmaz.

- **IP Dış Yol TVL:** Dış yönlendirme bilgilerini taşır.
  - **Tip:** 0x0103 değerini alır.
  - **Uzunluk:** TVL paketinin uzunluğunu belirtir.
  - **Sonraki Adım:** Bu şebekeye ulaşmak için paketin gönderileceği yönlendiricinin adresidir.
  - **Kaynak Yönlendirici:** Yönlendirme bilgisini dağıtan yönlendiricinin adresidir.
  - **Kaynak AS:** Yönlendirme bilgisinin geldiği otonom sitemin numarasıdır.
  - **Etiket:** Yönlendirme haritaları ile yol bilgilerini izlemek için kullanılır.
  - **Dış Metrik:** Yönlendirme bilgisinin öğrenildiği protokolün kullandığı metrik değeridir.
  - **Dış Kimlik:** Yönlendirme bilgisinin öğrenildiği protokolü tanımlar.
  - **Bayrak:** Çeşitli kontroller için gerekli işaretlerdir.
  - **Gecikme, Band Genişliği, MTU, Güvenilirlik ve Yük:** Metrik hesabı için kullanılan değerlerdir.
  - **Adım sayısı:** 0x00 ve 0xFF arasında değer alır. 0x00 doğrudan bağlı şebekeyi ifade eder.
  - **Önek Uzunluğu:** Hedef şebekenin alt şebeke maskesini belirtir.
  - **Hedef:** Hedef şebeke adresidir.
  - **Rezerve:** 0x0000 değeri alır ve kullanılmaz.

4.4. OSPF

Açık - En Kısa Yol Önceliklidir (OSPF – Open Shortest Path First) protokolü, IETF tarafından IP kullanılan şebekelerde yönlendirmeyi gerçekleştirmek için geliştirilmiştir. OSPF'in geliştirilme sebebi, o dönemde kullanılan RIP protokolünün büyük ve farklı bağlantılar içeren şebekelerde kullanıma uygun olmamasıydı.

OSPF'in iki temel özelliği vardır. İlki OSPF'in açık bir protokol olması, yani özelliklerinin herkesin erişimine açık olmasıdır. Bu özellikler RFC 1247 belgesi ile yayınlanmıştır. İkinci özelliği ise dayandığı SPF algoritmasıdır. Bu algoritma bazen algoritmayı geliştiren kişinin adı ile Dijkstra Algoritması olarak da adlandırılır.

OSPF bir bağlantı durumu protokolüdür. Aynı hiyerarşik alandaki yönlendiricler birbirlerine bağlantı durumu duyuruları (LSA – Link State Advertisement) gönderirler. Bu paketlerde bağlı bulunan arayüzler, kullanılan metrik değerleri ve kullanılan diğer değişkenlerle ilgili bilgiler taşınır. Yönlendirciler bu paketlerdeki bilgileri toplayarak her yönlendiriciye ulaşabilecekleri en kısa yolu hesaplayabilirler.

Bağlantı durumu protokolü olarak OSPF, RIP ve IGRP gibi uzaklık vektörü protokollerinden yönlendiricilerin tüm yönlendirme tablolarını birbirlerine yollamamaları ile ayrılır.

4.4.1. OSPF Yönlendirme Hiyerarşisi

RIP ve IGRPden farklı olarak OSPF bir hiyerarşi düzeninde yönlendirme yapar. OSPF yönlendirme hiyerarşisindeki en büyük yapı, OSPF'in çalıştığı otonom sistemdir. OSPF, bir iç yönlenrime protokolü olmasına rağmen kendi otonom sistemi dışından da yönlendirme bilgisi alabilir, dış otonom sistemlere yönlendirme bilgisi gönderebilir.

OSPF yönlendirme hiyerarşisinde, otonom sistemler, birbirinden bağımsız alt alanlara ayrılabilirler. Bu alanlar birbirine bağlı şebekeler ve bu şebekelere bağlı kullanıcılardan oluşur. Bir yönlendirici tümüyle bir alan içinde çalışabileceği gibi farklı arabirimleri farklı alanlara dahil olabilir. Bu durumdaki yönlendiricilere Alan Sınırı Yönlendiricileri denir ve bunlar dahil oldukları her alan için farklı bir topoloji tablosu tutarlar.

Topoloji veri tabanı, yönlendiricilerin ilişkide oldukları şebekenin genel görüntüsüdür. Bu veri tabanı, bir alandaki tüm yönlendiricilerin gönderdiği LSA

paketlerinden alınan bilgilerle oluşturulur. Bir alan içindeki tüm yönlendiriciler gönderilen LSA paketlerini aldıklarından ortak bir topoloji veri tabanına sahip olurlar.

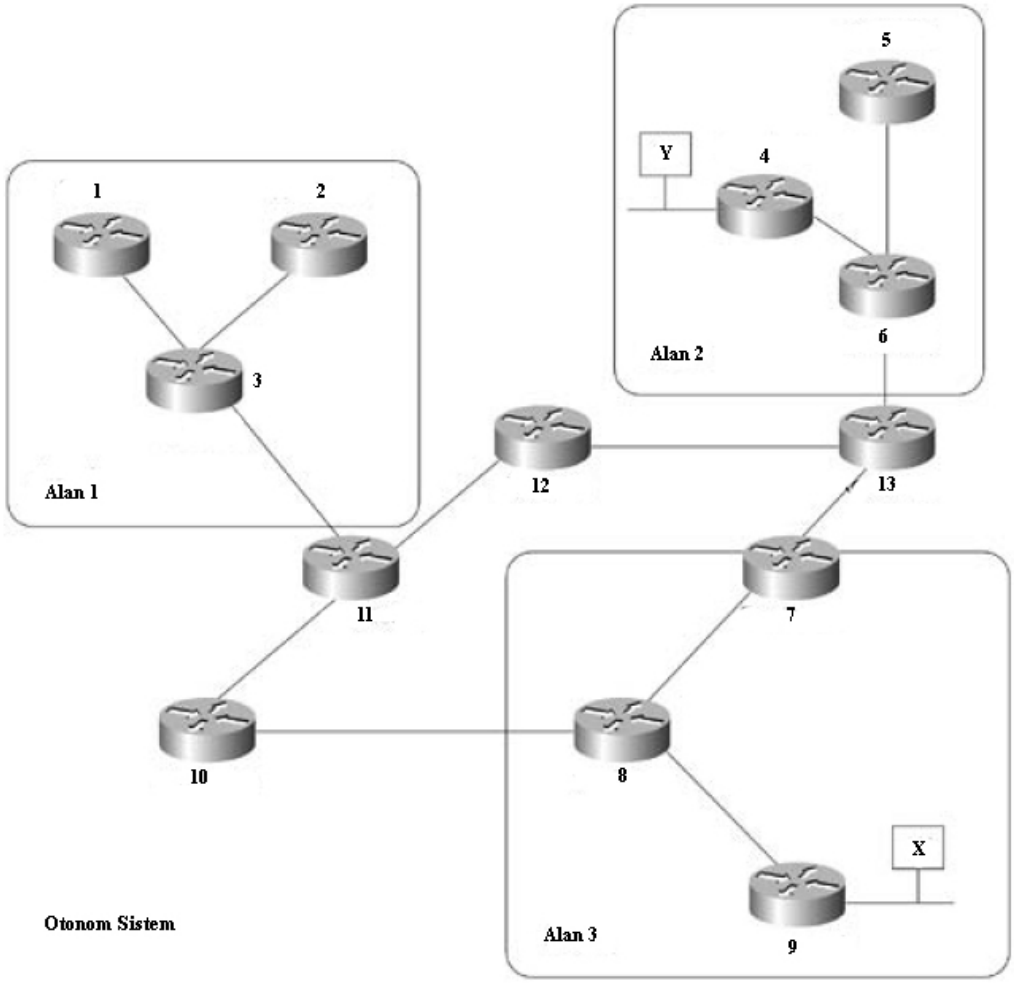
Alan terimi, aynı topolojik veri tabanına sahip yönlendircilerin oluşrutduğu şebekeyi belirtmek için kullanılabileceği gibi, sık sık otonom sistem terimi yerine de kullanılabilmektedir.

Bir alanın topoloji bilgisi, alanın dışındaki yönlendiriciler tarafından bilinmez. Bunun nedeni, LSA paketlerinin alan içinde sınırlanmasıdır. OSPF, bu şekilde yönlendirme ve güncelleme için yarattığı trafiği azaltmış olur.

Şebekeyi alanlara ayırmak, kaynak ve hedef şebekelerin aynı ya da farklı alanlarda bulunmalarına bağlı olarak iki çeşit OSPF yönlendirmesi tanımlanmasına neden olur. İç-alan yönlendirmesinde kaynak ve hedef şebekeler aynı alan içindedir. Kaynak ve hedef şebekeler farklı alanlara dahillerse, gerçekleşen yönlendirmeye dış-alan yönlendirmesi denir.

Tüm alanlar OSPF omurgasına bağlıdırlar. OSPF omurgası, bu alanlar arasındaki dış-alan yönlendirmesinden sorumludur ve tüm Alan Sınırı Yönlendiricileri, herhangi bir alana dahil olmayan şebekeler ve bunlara bağlı yönlendiricilerden oluşur. Şekil 4.8'de örnek bir OSPF yönlendirme hiyerarşisi ve alanlar görülmektedir.

Şekilde görüldüğü gibi otonom sistem üç alt alana ayrılmış ve bu alanlar OSPF omurgası üzerinden birbirlerine bağlanmışlardır. 7, 10, 11, 12, 13 yönlendircileri OSPF omurgasını oluşturmaktadır. Böyle bir yapıda alan 3'teki X kullanıcısı, Alan 2'deki Y kullanıcısına paket göndermek isterse, öncelikle paketi kendi bağlı olduğu 9 numaralı yönlendiriciye gönderecektir. Paket daha sonra 8 numaralı yönlendirciye ve oradan da Alan Sınırı Yönlendiricisi olan 7 numaralı yönlendirciye iletilecektir. Bu şekilde omurgaya ulaşan paket, OSPF omurgası üzerinden hedef alanın Alan Sınırı Yönlendircisi olan 13 numaralı yönlendirciye gelecektir. Daha sonra ise, iç alan yönlendirmesi ile sırasıyla 6 ve 4 numaralı yönlendircilere iletilecek, buradan da Y kullanıcısına ulaşacaktır.



Şekil 4.8: OSPF Hiyerarşisi ve Alanlar

OSPF omurgası da aslında bir OSPF alanıdır yani tüm omurga yönlendiricileri de herhangi bir alandaki yönlendircilerle aynı işlemleri ve algoritmaları kullanarak omurga içinde gerekli yönlendirme bilgilerini elde ederler. Omurganın topolojisi diğer alanlardaki yönlendiricilere görünmez olduğu gibi, omurgadaki yönlendiriciler de diğer alanların topolojilerinden haberdar değillerdir.

Normal tasarımda, alanlar birbirleri ile bağlı değillerdir ve hepsi omurga üzerinden birbirlerine bağlanırlar. Ancak omurganın sürekli olmadığı veya bir alanın omurgaya doğrudan bağlanamadığı durumlarda, bağlantılar sanal bağlantılar tanımlanarak sağlanır. Sanal bağlantılar, omurga dışındaki bir alan üzerinden bağlanan iki yönlendirici arasında tanımlanır ve bunların birbiri ile doğrudan bağlılarmış gibi çalışması sağlanır.

4.4.2. SPF Algoritması

En Kısa Yol Önceliklidir (SPF – Shortest Path First) algoritması, OSPF işlemlerinin temelini oluşturur. SPF kullanan bir yönlendirici çalıştırıldığında, kendi yönlendirme protokolünün veri yapılarını oluşturur ve daha sonra alt katman protokollerinden arayüzlerinin çalıştığına dair işaretler gelmesini bekler.

Yönlendirici, kendi arabirimlerinin çalışır durumda olduğuna emin olduktan sonra, ortak bir ağa bağlı arayüzleri bulunan yönlendiriciler arasından, OSPF merhaba paketlerini kullanarak komşular edinmeye çalışır. Yönlendirici komşularına merhaba paketleri göndermeyi ve komşularının gönderdiği merhaba paketlerini almayı sürdürür. Bu mesajlar, komşuluk ilişkilerinin kurulmasını sağlamanın yanında, gönderen yönlendiriclerin halen çalışır olduğunun anlaşılmasını sağlayan canlı-tut mesajı görevini de üstlenirler. Örnek bir OSPF komşu tablosu Şekil 4.9'da gösterilmiştir.

```
Router#sh ip ospf 65100 neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.12.25     0   FULL/  -        00:00:37    192.168.19.178 Serial6/4:0
192.168.12.3      0   FULL/  -        00:00:33    192.168.19.122 Serial4/4:0
192.168.12.13     1   2WAY/DROTHER     00:00:32    192.168.9.8    FastEthernet0/0
192.168.12.27     1   2WAY/DROTHER     00:00:31    192.168.9.12   FastEthernet0/0
192.168.12.30     1   2WAY/DROTHER     00:00:37    192.168.9.9    FastEthernet0/0
192.168.12.39     5   2WAY/DROTHER     00:00:30    192.168.9.1    FastEthernet0/0
192.168.12.41     1   2WAY/DROTHER     00:00:38    192.168.9.20   FastEthernet0/0
192.168.12.50     1   2WAY/DROTHER     00:00:39    192.168.9.10   FastEthernet0/0
192.168.12.52     1   2WAY/DROTHER     00:00:33    192.168.9.7    FastEthernet0/0
192.168.12.53     1   2WAY/DROTHER     00:00:30    192.168.9.16   FastEthernet0/0
192.168.12.57     1   FULL/DR          00:00:33    192.168.9.14   FastEthernet0/0
192.168.12.70     1   FULL/BDR         00:00:39    192.168.9.31   FastEthernet0/0
```

Şekil 4.9: OSPF komşu tablosu

Çoklu erişime açık şebekelerde (ikiden fazla yönlendiricinin bağlanabileceği şebekeler) merhaba paketleri bir atanmış yönlendirici ve bir de yedek atanmış yönlendirici seçer. Atanmış yönlendirciler, diğer görevleri yanında, tüm çoklu erişim şebekesine gönderilecek LSA paketlerinin oluşturulmasından sorumludur. Bu yönlendirciler şebekedeki trafiğini ve topoloji veri tabanının büyüklüğünü azaltırlar.

Şekil 4.10'da OSPF çalıştıran bir yönlendiricinin arabirim özelliklerini ve OSPF için seçilen atanmış yönlendircileri görmek mümkündür.

```
Router#sh ip ospf interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.168.9.13/24, Area 0
  Process ID 65100, Router ID 192.168.12.2, Network Type BROADCAST, Cost: 2
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.12.57, Interface address 192.168.9.14
  Backup Designated router (ID) 192.168.12.70, Interface address 192.168.9.31
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 40
  Last flood scan time is 0 msec, maximum is 28 msec
  Neighbor Count is 10, Adjacent neighbor count is 2
    Adjacent with neighbor 192.168.12.57  (Designated Router)
    Adjacent with neighbor 192.168.12.70  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

Şekil 4.10: OSPF çoklu erişim arabirim parametreleri

İki komşu yönlendircinin bağlantı durumu veri tabanları senkronize olduğunda, yönlendircilerin eşleştiği söylenir. Çoklu erişim şebekelerinde, atanmış yönlendirciler hangi yönlendiricilerin eşleşeceğini belirler. Topoloji veri tabanları eşleşmiş yönlendirciler arasında senkronize edilirler. Şekil 4.11.de bir OSPF topoloji tablosu görülmektedir.

Her yönlendirici, kendisinin eşleşme durumu ile ilgili bilgi vermek ve diğer yönlendiricileri herhangi bir yönlendiricinin durumunun değiştiği hakkında uyarmak için periyodik olarak LSA paketleri gönderir. Kurulan eşleşmelerle bağlantı durumlarının karşılaştırılması ile kullanılamaz durumdaki yönlendiriciler hızla farkedilir ve şebeke topolojisi buna uygun olarak güncellenebilir. LSAlarla toplanan bilgilerden oluşturulan topoloji veri tabanını kullanarak, her yönlendirici kendisinin kökte bulunduğu bir SPF ağacı oluşturur. Bu ağaç kullanılarak da yönlendirme tablosu oluşturulur[7].

```
Router#sh ip ospf database

        OSPF Router with ID (192.168.12.2) (Process ID 65100)

            Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.12.2    192.168.12.2    599         0x80007A76 0x007AE5 12
192.168.12.3    192.168.12.3    968         0x800037CC 0x00F4C2 5
192.168.12.4    192.168.12.4    1966        0x800011E5 0x001BF3 5
192.168.12.5    192.168.12.5    973         0x800073FB 0x0014A2 10
192.168.12.7    192.168.12.7    1724        0x800018B0 0x007686 1

            Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
192.168.9.14    192.168.126.57  1541        0x80002906 0x006199
192.168.19.1    172.16.103.29   625         0x80000428 0x008F80
192.168.19.18   192.168.12.40   546         0x80001038 0x00CCB1
172.16.72.1     192.168.12.8    172         0x80000DD2 0x0098EB
172.16.76.3     192.168.12.49   693         0x80000B99 0x00B6E2
172.16.111.4    192.168.12.65   1716        0x80003C2B 0x0098B2
172.16.113.72   192.168.12.7    1725        0x800003E8 0x0091B6
172.16.124.6    192.168.12.81   617         0x80000C53 0x0085F8

            Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
192.168.12.6    192.168.12.9    1335        0x80000BFE 0x0073AD
192.168.12.7    192.168.12.7    1465        0x800018AF 0x00E282
192.168.12.11   192.168.12.40   546         0x8000087E 0x0090EF
192.168.12.18   192.168.12.17   34          0x8000109B 0x0082E8
192.168.12.20   192.168.12.19   1578        0x80004731 0x009109
192.168.12.22   192.168.12.21   1592        0x80001D99 0x001F39


            Type-10 Opaque Link Area Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Opaque ID
1.0.0.0         192.168.12.2    600         0x800030C5 0x00BB7B 0
1.0.0.0         192.168.12.5    473         0x8000246C 0x00C4FA 0
1.0.0.0         192.168.12.9    1335        0x800003EB 0x00C5F5 0
1.0.0.0         192.168.12.12   872         0x800003EB 0x0093FE 0
1.0.0.0         192.168.12.17   34          0x8000019F 0x0097F5 0

            Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         192.168.12.36   795         0x80000301 0x008949 65100
0.0.0.0         192.168.12.52   1382        0x8000257E 0x00F9F0 65100
0.0.0.0         172.16.103.29   625         0x80000428 0x00A5B6 65100
1.1.1.1         192.168.12.42   1571        0x8000042B 0x001132 0
7.7.7.7         192.168.12.42   1571        0x80000427 0x00042B 0
```

Şekil 4.11: OSPF topoloji tablosu

4.4.3. OSPF Paket Yapısı

OSPF paketinin yapısı Şekil 4.12'de gösterilmiştir.

1	1	2	4	4	2	2	8	Değişken
Sürüm	Tip	Paket Uzunluğu	Yönlendirici Kimliği	Alan Kimliği	Kontrol Toplamı	Kimlik Sorgu Tipi	Kimlik Sorgusu	Veri

Şekil 4.12: OSPF paketi

Şekilde alanların üzerindeki sayılar bit olarak alanların büyüklüğünü belirtmektedir. Alanların açıklamaları aşağıdadır:

- **Sürüm:** Kullanılan OSPF sürümünü gösterir. Günümüzde kullanımda olan sürüm 2'dir.
- **Tip:** OSPF paketinin tipini belirtir.
  - Merhaba Paketi: Komşuluk ilişkisini kurar ve devam ettirir. Tip değeri 1'dir.
  - Veri Tabanı Açıklaması: Topoloji veri tabanının içeriğini açıklar. Bu paketler bir eşleşme durumu sağlandığında gönderilir. Tip değeri 2'dir.
  - Bağlantı Durumu İsteği: Komşu yönlendiricilerden topoloji veri tabanının parçalarını talep eder. Bu paketler, bir yönlendirici topoloji veri tabanının bazı parçalarının güncelliğini kaybettiğini fark etmesi sonucu gönderilir. Tip değeri 3'tür.
  - Bağlantı Durumu Güncellemesi: Bağlantı durumu istek paketlerine yanıt olarak gönderilirler. LSA paketleri için de kullanılabilirler. Birden fazla LSA paketi tek bağlantı durumu güncellemesi içinde gönderilebilir. Tip değeri 4'tür.
  - Bağlantı Durumu Onayı: Bağlantı durumu güncellemelerini onaylamak için gönderilirler. Tip değeri 5'tir.
- **Paket Uzunluğu:** OSPF başlığı ile beraber paketin toplam uzunluğunu bayt cinsinden gösterir.
- **Yönlendirici Kimliği:** Paketin kaynağı olan yönlendiriciyi belirtir.

- **Alan Kimliği:** Paketin ait olduğu alanı belirtir. Her OSPF paketi tek bir alan ile ilişkilendirilir.
- **Kontrol Toplamı:** Paketin iletimde zarar görüp görmediğinin kontrolü içindir.
- **Kimlik Sorgu Tipi:** Kullanılan kimlik sorgusunun tipini belirtir. Tüm OSPF işlemleri kimlik sorgulaması ile yapılır. Kimlik sorgulaması tipi alan bazında ayarlanabilir.
- **Kimlik Sorgusu:** Kimlik sorgusu için gerekli bilgiyi içerir.
- **Veri:** Zarflanmış üst katman bilgisini içerir.

4.4.4. OSPF Durumları

OSPF komşuluk ilişkisinin kapalı, deneme, init, 2-yol, başlangıç, alışveriş, yükleme ve tam eşleşmiş olmak üzere 8 durumu vardır. Bunların anlamları aşağıda verilmiştir.

- **Kapalı:** İlk komşuluk ilişkisi durumudur. Bu durumda henüz ilgili komşudan merhaba paketi alınmamıştır, ancak komşu yönlendiriciye merhaba paketi gönderilebilir. Tam eşleşmiş durumdaki bir komşudan belirli bir süre merhaba paketi alınmazsa ya da şebeke yönedicisinin eklediği komşu bilgisi konfigurasyondan çıkarılırsa, komşuluk ilişkisi kapalı durumuna geçer.
- **Deneme:** Bu durum sadece Broadcast Olmayan Çoklu Erişim şebekelerde (NBMA - Non-Broadcast Multi Access) şebekelerde yönetici tarafından eklenmiş komşular için geçerlidir. Bu durumda yönlendirici, belirli bir süre merhaba paketi almadığı komşusunun adresine belirli aralıklarla merhaba paketleri gönderir.
- **Init:** Bu durum, yönlendiricinin komşusundan bir merhaba paketi aldığını ancak yönlendirici kimliğinin bu pakette bulunmadığını gösterir. Bir yönlendirici merhaba paketi aldığında, bunu onaylamak için komşusunun yönlendirici kimliğini kendi merhaba paketine eklemek zorundadır.
- **2-Yol:** Bu durum, iki yönlendirici arasında iki yönlü haberleşme sağlandığını gösterir. Bunun anlamı her iki yönlendiricinin de birbirlerinin merhaba paketlerini alabiliyor olmasıdır. Bir yönlendirici aldığı merhaba paketlerinde kendi yönlendirici kimliğini gördüğünde bu duruma geçilebilir. 2-Yol

durumundaki bir yönlendirici, karşı yönlendirici ile eşleşip eşleşmeyeceğine karar vermelidir. Broadcast ve NBMA şebekelerde bir yönlendirici sadece atanmış yönlendirici ve yedek atanmış yönlendirici ile tam eşleşme durumuna geçer. Diğer yönlendiriciler ile 2-Yol durumunda kalır. Noktadan noktaya ve noktadan çok noktaya bağlantılarda tüm bağlı yönlendiriciler ile tam eşleşme durumuna geçer. Bu durumun sonunda atanmış yönlendirici ve yedek atanmış yönlendirici seçilmiş olur.

- **Başlangıç:** Atanmış yönlendirici ve yedek atanmış yönlendirici seçildikten sonra, yönlendiriciler arasında bağlantı durumu bilgileri alışverişini sağlayan esas işlemlere başlanır. Bu durumda, yönlendirici ile atanmış yönlendirici arasında yönlendiricilerin kimliklerine bağlı olarak bir efendi-köle ilişkisi kurulur. Burada efendi durumunda olan yönlendirici eşleşme bilgileri için bir sıra numarası belirler.
- **Alışveriş:** Bu durumdaki yönlendiriciler karşılıklı olarak veri tabanı açıklaması paketleri gönderirler.
- **Yükleme:** Bu durumda gerçek bağlantı durumu bilgileri gönderilir. Yönlendirciler, veri tabanı açıklaması paketlerindeki bilgilere göre bağlantı durumu istek paketleri gönderirler. Bunlara bağlantı durumu güncellemeleri ile yanıt verilir.
- **Tam Eşleşme:** Bu durumdaki iki yönlendirici arasında tam olarak eşleşme sağlanmıştır. Tüm yönlendirme bilgileri ve LSA paketleri gönderilmiş ve yönlendiriclerin topoloji veri tabanları tam olarak senkronize olmuşlardır.

  Tam eşleşme durumu, bir OSPF yönlendiricisinin normal durumudur. Eğer yönlendirici diğer durumlardan birinde takılı kalmışsa komşuluk kurulmasında sorunlar olduğu anlaşılmalıdır. Bunun tek istisnası, 2-yol durumudur. Broadcast ve NBMA şebekelerde bir yönlendirici sadece atanmış yönlendirici ve yedek atanmış yönlendirici ile tam eşleşme durumuna geçer. Diğer yönlendiriciler ile 2-Yol durumunda kalır.

4.4.5. OSPF'in Ek Özellikleri

Ek OSPF özellikleri, eşit metriklere sahip yollara yük dağılımı ve üst katmanların servis tipi (TOS – Type of Service) isteklerine dayanan yönlendirme yapabilmesidir. TOS'a dayanan yönlendirme, belirli bir servis tipi seçebilen üst katman protokollerini destekler. Örneğin, bir uygulama belirli veri paketlerinin acil olduğunu belirtebilir. Eğer OSPF'in kullanabileceği yüksek öncelikli bağlantılar varsa, acil olan veri paketini iletmek için bu bağlantılar kullanılabilir.

OSPF bir veya birden fazla metrik değerini kullanabilir. Eğer tek metrik değeri kullanılıyorsa, bu keyfi olarak değerlendirilir ve TOS desteklenmez. Birden fazla metrik değeri kullanılıyorsa, üç IP TOS biti ile belirlenebilecek 8 farklı kombinasyon için farklı metrikler (dolayısıyla farklı yönlendirme tabloları) kullanılabilir.

Alt şebeke maskeleri duyurulan her hedef şebeke için gönderilir, bu da OSPF'e VLSM desteği sağlar. Bu şekilde bir IP şebekesi çeşitli büyüklüklerdeki pek çok alt şebekeye ayrılabilir ve şebeke yöneticilerine tasarımda esneklik sağlanır [2]

4.5. IS-IS

Başlangıçta OSI CLNS şebekelerini desteklemek için geliştirilen IS-IS, daha sonra sınıfsız IP şebekeleri üzerinde yönlendirme sağlayabilecek şekilde genişletilmiştir. Bu genişletilmiş IS-IS sürümüne Entegre IS-IS (Integrated IS-IS) veya bazı kaynaklarda Çift IS-IS (Dual IS-IS) adı verilir.

Kullanılan şebeke ne tür olursa olsun, IS-IS bir bağlantı durumu yönlendirme protokolüdür. Bu yüzden OSPF'in uzaklık vektörlerine karşı sağladığı pek çok avantajı paylaşır.

IS-IS, çabuk öğrenme ve şebekedeki topoloji değişikliklerinin hızlı duyurulmasını sağlar. OSPF gibi alanların kullanılmasıyla hiyerarşik bir şebeke tasarımını destekler, bu da esneklik ve ölçeklenebilirlik sağlar. IS-IS'in esnekliğini arttıran başka bir özelliği de MPLS trafik mühendisliğini destekleyen bir iç yönlendirme protokolü olarak kullanılabilmesidir.

4.5.1. IS-IS Yönlendirme Mimarisi

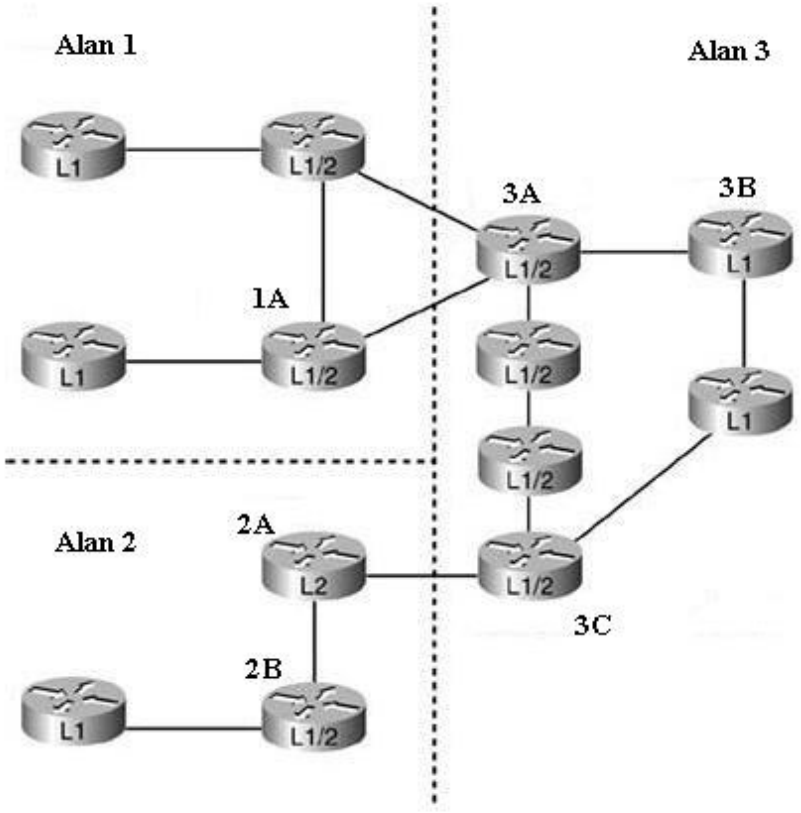
IS-IS hiyerarşik yönlendirme yapısını alanları kullanarak gerçekleştirir. OSPF'te yapıldığı gibi, büyük bir şebeke daha küçük alanlara bölünür. Bu, bağlantı durumu protokollerinin gerektirdiği yüksek işlemci ve hafıza gereksinimi sonucu ortaya cıkan ve yönlendiricilerin üzerindeki yükü azaltan bir çözümdür.

IS-IS alanları ve hiyerarşik yapıyı kullanması ile OSPF'e benzese de arada bazı farklılıklar vardır. Bunlardan biri, IS-IS'de adreslerin ve alanların bir yönlendiricinin tamamına atanmasıdır. OSPF'te ise bu atama arabirim bazında yapılabilir. Bu tanımdan görebileceğimiz gibi bir OSPF yönlendircisi birden fazla alana dahil olabilirken, bir IS-IS yönlendiricisi sadece bir alana dahil olabilir[2].

Tamamen bir alan içinde yönlendirme yapan yönlendiriciler birinci düzey yönlendirici adını, farklı alanlar arasında yönlendirme yapan yönlendiriciler ikinci düzey yönlendirici adını alırlar.

IS-IS omurgası, OSPF omurgası gibi ayrı bir alan değildir. Birbirine bağlı ikinci düzey yönlendircilerden oluşur. Her ikinci düzey yönlendirici tek bir alan içinde yer alır ancak başka alanlardaki diğer ikinci düzey yönlendiricilerle bağlantıları olabilir. Görüldüğü gibi, OSPF'ten farklı olarak, alanın sınırı ikinci düzey yönlendirici değil,

ikinci düzey yönlendiriciler arasındaki bağlantılardır. Şekil 4.13 bir IS-IS hiyerarşisini göstermektedir.



Şekil 4.13: IS-IS Hiyerarşik yapısı

Genelde, birinci düzey yönlendirciler sadece kendi alanlarındaki yönlendirme bilgisine sahiptirler. Eğer kendi alanlarının yönlendirme bilgisi ile yönlendiremeyecekleri bir paket alırlarsa, bu paketi en yakın ikinci düzey yönlendiriciye gönderirler. Paket buradan uygun alana yönlendirildikten sonra o alanın içindeki birinci düzey yönlendiriciler tarafından hedefe gönderilir.

Bir 1-2 düzeyi yönlendirici farklı bir alana bağlandığında, kendi alanı içindeki birinci düzey yönlendiricileri duyuru paketlerindeki işaret bitini ayarlayarak uyarır. Birinci düzey yönlendiriciler bunu algıladıklarında 1-2 düzeyi yönlendiricinin diğer alanlara ulaşmak için kullanılabileceğine karar verirler. Entegre IS-IS'te 1-2 düzeyi yönlendiriciler kendi alanları içine varsayılan yol duyurusu yaparlar. Örnek şekildeki 3A ve 3C yönlendiricileri, Alan 3 içindeki diğer yönlendiricilere varsayılan yol duyurmaktadırlar.

İkinci düzey yönlendiriciler sadece alanlar arası yönlendirme bilgilerini bilirler, kendi alanlarına ait yönlendirme bilgisine sahip değillerdir. Bir OSI-şebekesinde yönlendiriciler sadece ikinci düzey yönetici olarak ayarlanmamalıdır, çünkü tüm OSI yönlendiricilerinin kendi alanlarının topolojisini bilmesi zorunludur. Yönlendirici 1-2 düzeyi olarak ayarlanabilir ve bu durumda hem kendi alanının yönlendirme bilgisini hem de alanlar arası yönlendirme bilgisini öğrenmesi sağlanır. Entegre IS-IS'te 1-2 düzeyi yönlendirici birinci düzey bilgiyi ikinci düzeye sızdırır ve bu sırada özetleme yapılabilir.

Şebeke tasarımına bağlı olarak, en yakın ikinci düzey yönlendirici bir şebekeye ulaşmak için en iyi yol olmayabilir; ancak birinci düzey yönlendiriciler bunu bilmezler çünkü sadece kendi alanlarının yönlendirme bilgisine sahiptirler. Örneğin şekildeki 3B yönlendiricisi 3A yönlendiricisini kendisine en yakın ikinci düzey yönlendirici seçer. Eğer göndereceği paket alan 2'ye gitmesi gereken bir paketse, 3A üzerinden uzun bir yoldan dolaşarak hedef alana ulaşabilecektir.

Bu sorunu çözmek amacıyla, ikinci düzey yönlendiriciler seçilen yol bilgilerini birinci düzey alanına sızdırmak için ayarlanabilirler. Bu şekilde birinci düzey yönlendiricilerin daha akıllıca karar vermeleri sağlanabilse de; yönlendirme bilgisinin artması, esas IS-IS yönlendirme yapısının ölçeklenebilirliğini azaltır.

IS-IS yönlendiricileri, komşularını merhaba paketleri yollayarak otomatik olarak bulurlar. Noktadan noktaya bağlantılarda doğrudan eşlilik oluşturarak yönlendirme bilgilerini Bağlantı Durumu Paketleri (LSP – Link State Packets) gönderirler. Bu paketlerdeki bilgiler, Bağlantı Durumu Veri Tabanı (LSDB – Link State DataBase) oluşturulmasında kullanılır. Veri tabanı oluşturulduktan sonra SPF ağacı oluşturularak yönlendirme tablosu doldurulur[7].

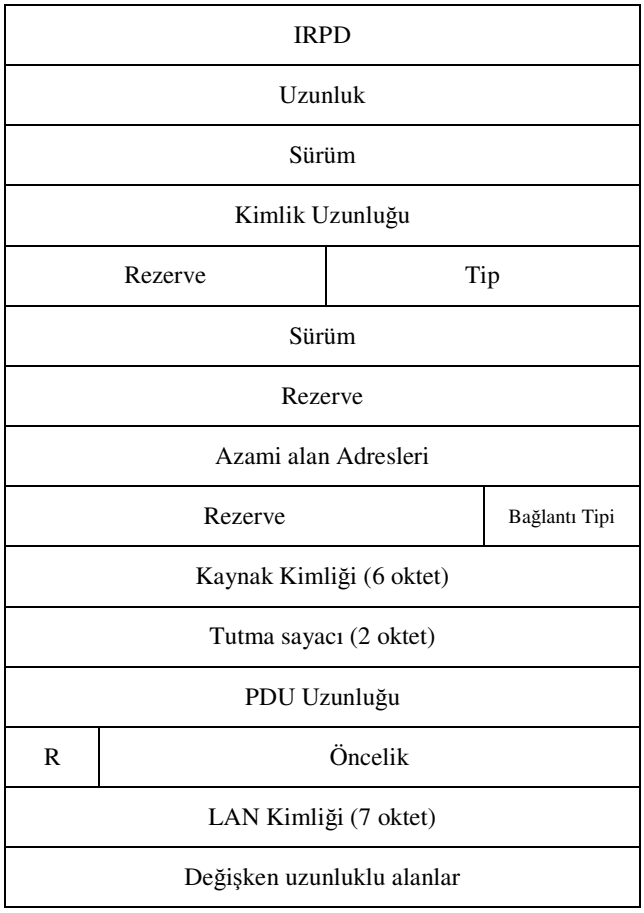
Broadcast şebekelerde merhaba paketleri bilinen multicast MAC adreslerine gönderilir. Bir yönlendirici atanmış orta sistem olarak seçilir ve bu yönlendirici, alandaki diğer yönlendiriciler yerine LSP'leri dağıtır.

4.5.2. IS-IS Metriği

IS-IS tarafından dört metrik değeri belirlenmiştir. Bunlar maliyet, gecikme, masraf ve hata miktarıdır. Sadece maliyetin kullanılması zorunludur. Varsayılan maliyet değeri sabit olarak 10'dur. Bir yolun metrik değerinin azami 1023 olabilmesi, yönlendirme tasarımını sınırlamaktadır.

4.5.3. IS-IS Paket Yapısı

Daha önce belirtildiği gibi, IS-IS komşuluk ilişkisi kurmak için merhaba paketleri gönderir. Şekil 4.14'te birinci ve ikinci düzey merhaba paketlerinin yapısı görülmektedir.



Şekil 4.14: IS-IS Merhaba Paketi

Şekilde her satır bir okteti (8 bit) göstermektedir. Alanların anlamları aşağıdadır:

- **IRPD:** IS-IS için şebeke katmanı belirleyicisidir. (0x83)
- **Uzunluk:** Bayt cinsinden başlık uzunluğudur.
- **Sürüm:** 1 değerini alır.
- **Kimlik Uzunluğu:** Kaynak kimliği alanının uzunluğunu belirtir. 0 değeri, 6 oktetlik varsayılan uzunluk değerini gösterir.
- **Tip:** Merhaba paketinin tipini gösterir. 15 değeri birinci düzey, 16 değeri ikinci düzey, 17 değeri ise noktadan noktaya merhaba paketlerini gösterir.

- **Azami Alan Adresleri:** İlgili alan içinde izin verilen adreslerin sayısını belirtir. 1 ile 254 arasında değer alır.
- **Bağlantı Tipi:** 00 değeri rezervedir, 01 birinci düzey, 10 ikinci düzey, 11 birinci ve ikinci düzey anlamına gelir.
- **Kaynak Kimliği:** Kaynak yönlendiricinin kimlik bilgisini içerir.
- **Tutma sayacı:** 16 bitlik tutma sayacı değeridir.
- **PDU Uzunluğu:** Paket (PDU - Protocol Data Unit) başlığı ve değişken uzunluklu alanlarla beraber PDU uzunluğunu gösterir.
- **Öncelik:** Atanmış Orta Sistem seçimindeki önceliği belirtir.
- **LAN kimliği:** Atanmış Orta Sistemin kimliği ve ek bir bayt
- **Değişken Uzunluklu Alanlar:** TLV'leri içerir.

IS-IS yönlendiricileri komşuları ile yönlendirme bilgilerini LSP'leri kullanarak paylaşırlar. Duyurulan esas şebeke adresleri LSP'nin sonunda bulunan TVLlerde saklanırlar. Şekil 4.15 bir LSP paket yapısını göstermektedir.

<table>
<tr><td colspan="4">IRPD</td></tr>
<tr><td colspan="4">Uzunluk</td></tr>
<tr><td colspan="4">Sürüm</td></tr>
<tr><td colspan="4">Kimlik Uzunluğu</td></tr>
<tr><td colspan="2">Rezerve</td><td colspan="2">Tip</td></tr>
<tr><td colspan="4">Sürüm</td></tr>
<tr><td colspan="4">Rezerve</td></tr>
<tr><td colspan="4">Azami Alan Adresleri</td></tr>
<tr><td colspan="4">PDU Uzunluğu (2 oktet)</td></tr>
<tr><td colspan="4">Kalan Yaşama Zamanı (2 oktet)</td></tr>
<tr><td colspan="4">LSP Kimliği (Kimlik Uzunluğu + 2 oktet)</td></tr>
<tr><td colspan="4">Sıra Numarası (4 oktet)</td></tr>
<tr><td colspan="4">Kontrol Toplamı (2 oktet)</td></tr>
<tr><td>P</td><td>ATT</td><td>L</td><td>IS Tipi</td></tr>
<tr><td colspan="4">TLVler</td></tr>
</table>

Şekil 4.15: IS-IS LSP yapısı

Şekilde her satır bir okteti (8 bit) göstermektedir. Merhaba paketinden farklı alanların anlamları aşağıdadır:

- **Kalan Yaşama Zamanı:** LSP'nin atılmasından önce geçmesi gereken zamanı sn olarak belirtir.
- **LSP Kimliği:** LSP kimlik bilgisini belirtir.
- **Sıra Numarası:** Gönderilen paketin sıra numarasıdır.
- **Kontrol Toplamı:** Paketin iletimde zarar görüp görmediğinin kontrolü içindir.
- **P:** 1 değeri kaynağın parça tamiri desteklediğini gösterir.
- **ATT:** Kullanılan yönlendirme metriğini gösterir.
- **L:** 1 değeri göndericinin çok yüklendiğini ve SPF ağacı hesaplamalarında dikkate alınmaması gerektiğini belirtir.
- **IS Tipi:** Birinci veya ikinci düzey anlamına gelir.

5. SONUÇ

Günümüzde haberleşme mühendislerinin önemli işleri arasında şebekelerin tasarlanması, yönetimi ve verimli şekilde veri akışının sağlanması da bulunmaktadır. Artık IP şebekelerinde sadece veri değil, gerçek zamanlı ses ve görüntü de aktarıldığından; şebeke yöneticilerinin ve trafik mühendislerinin yönlendirme konusunu çok iyi anlamış olması gerekmektedir.

Şebeke genişlediğinde, yönlendirmenin kararlı ve hızlı şekilde yapılmasını sağlamak, daha şebeke tasarımı sırasında dikkat edilmesi gereken hususlardan biridir. Şebekelerin büyüklüğü ile orantılı olarak daha yüksek kapasiteli yönlendiriciler ve bağlantılar kullanmak, oluşabilecek sorunları gidermeye yetmeyebilir. Şebeke tasarımı sırasında yönlendirilecek üçüncü katman protokolünün ne olduğu, bunu yönlendirmek için kullanılacak yönlendirme protokolü, şebekenin topolojisi, bağlantıların tipi gibi hususlara özellikle dikkat edilmeli, şebekenin gelecekteki genişleme potansiyeli ve halihazırdaki topolojide kullanılacak uygulamalar da tasarım kararlarına dahil edilmelidir.

Bir şebekede kullanılacak yönlendirme protokolü seçiminde, öncelikle yönlendirilecek üçüncü katman protokolü etkili olur. Kullanılacak protokolü yönlendirebilecek yönlendirme protokolleri belirlendikten sonra, şebekenin fiziksel tasarımına ve uygulamalara göre en elverişli yönlendirme protokolü seçilmelidir. Örneğin cihazlar OSPF kullanımını desteklese de Apple Talk protokolünü yönlendirmek için OSPF kullanılamaz.

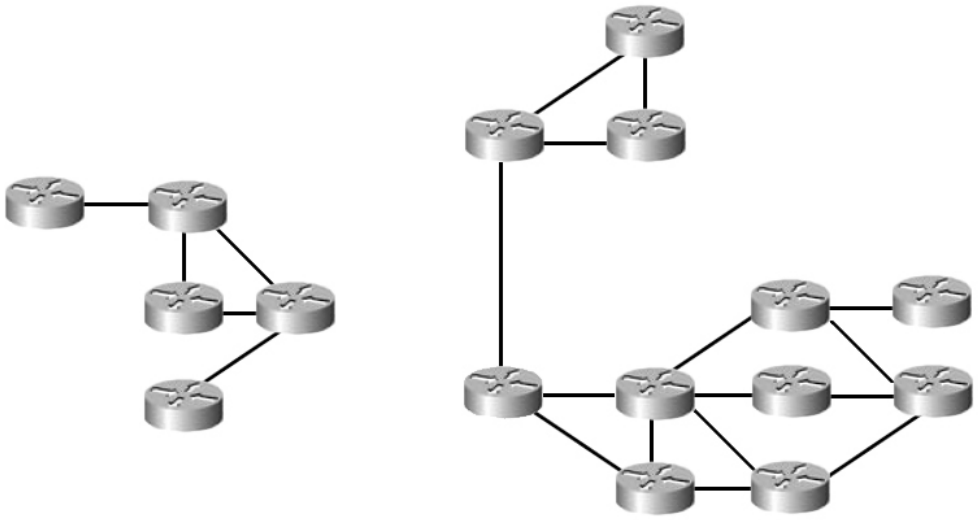
Yönlendirme protokolünü etkileyen diğer bir faktör de kullanılan yönlendiricilerdir. Yönlendirici özellikleri IGRP ve EIGRP gibi marka bağımlı protokollerin kullanımını etkileyebileceği gibi, yönlendiricilerin işlemci ve hafıza gibi özellikleri de cihazın üzerinde çalıştırılabilecek yönlendirme protokolünü etkileyebilir. Şebeke yöneticisinin kullanabileceği yönlendiricilerin hepsi Cisco değilse, şebekenin tamamında IGRP veya EIGRP kullanmak mümkün olmayacaktır. Aynı şekilde, düşük işlemci gücü ve hafızaya sahip yönlendiriciler üzerinde bir bağlantı durumu yönlendirme protokolü çalıştırmak verimli bir yönlendirme sağlamayacaktır.

Şebekenin topolojik büyüklüğü ve bağlantıların yapısı da yönlendirme protokolünün seçimini etkiler. RIP, küçük ölçekli ağlarda kurulumu ve yönetiminin kolaylığı ve düşük kapasiteli yönlendiricilerde de rahatlıkla kullanılabilmesi ile öne çıkarken, şebeke topolojisi büyüdüğünde veya bağlantıların özellikleri farklılaştığında yetersiz kalmaktadır. Aynı şekilde IGRP de kullandığı metrik ve farklı metrik değerlerine sahip bağlantılar üzerinde yük dağılımı yapabilmesi ile öne çıkarken, VLSM desteklememesi şebeke tasarımınında yeterli esnekliğin sağlanmasını engelleyebilir.

Görüldüğü gibi her yönlendirme protokolünün öne çıktığı veya eksik kaldığı yerler bulunmaktadır. Şebeke yöneticisine düşen, bu protokolleri tanıyıp, temel özelliklerini anlayarak amaca uygun şebeke tasarımını en verimli şekilde yönlendirebilecek olan protokolü seçmektir.

Tablo 5.1.de IP'yi yönlendirmek için kullanılan protokollerin özellikleri karşılaştırılarak verilmiştir. Bu tablodaki bilgiler gözden geçirilerek bir şebeke için yönlendirme protokolü seçiminde ilk adım atılabilir.

Bu bilgiler ışığında, Şekil 5.1de topolojileri görülen iki firmanın birleştirilmesi senaryosuna göz atalım.



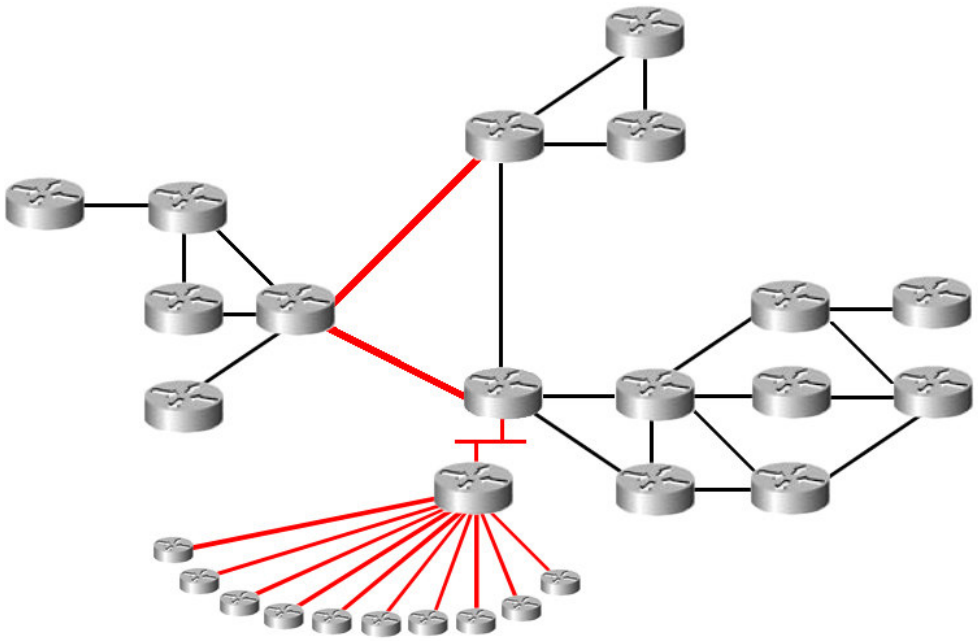
Şekil 5.1: Örnek senaryoda firma topolojileri

Tablo 5.1: IP Yönlendirme Protokolleri

	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
İşleyişine göre çeşidi	Uzaklık Vektörü	Uxaklık Vektörü	Uzaklık Vektörü	Melez	Bağlantı Durumu	Bağlantı Durumu
IP adreslerini değerledirmelerine göre çeşidi	sınıflı	sınıfsız	sınıflı	sınıfsız	sınıfsız	sınıfsız
Kullandığı algoritma	Bellman-Ford	Bellman-Ford	Bellman-Ford	DUAL	Dijkstra	Dijkstra
Şebeke boyutu	küçük	küçük	orta	geniş	geniş	geniş
Öğrenim zamanı	yavaş	yavaş	yavaş	çok hızlı	hızlı	hızlı
Metrik	adım sayısı	adım sayısı	karışık	karışık	maliyet	karışık
Güncelleme sayacı	30 sn	30 sn	90 sn	-	-	-
Tetiklenmiş Güncelleme	var	var	var	var	var	var
Güncelleme tipi	broadcast	multicast	broadcast	multicast	multicast	multicast
Yönetimsel Uzaklık	120	120	100	90	110	115
Adım Sayısı Sınırı	16	16	100	255	-	-
Eş Metrikli Yollara Yük Dağılımı	var	var	var	var	var	var
Farklı Metrikli Yollara Yük Dağılımı	yok	yok	var	var	yok	yok
Marka bağımlılık	yok	yok	var (sadece Cisco)	var (sadece Cisco)	yok	yok
TOS desteği	yok	yok	yok	yok	var	var

Görüldüğü gibi, Şekil 5.1 de Firma A daha küçük bir topolojiye sahip ve birleşmeden once RIP kullanmaktadır. RIP bu gibi küçük topolojilerde rahatlıkla kullanılabilmesine rağmen, daha büyük topolojilerde kullanıma elverişli değildir. Firma B ise daha geniş bir topolojiye sahiptir ve birleşme öncesinde EIGRP kullanmaktadır. EIGRP hem hızlı, hem de kararlı olmasına rağmen, marka bağımlı olması yüzünden sadece tüm cihazların Cisco olduğu şebekelerde kullanıma uygundur.

Şirketler birleştirilirken daha önce ADSL bağlantıları üzerinden internet bağlantısı sağlayan daha küçük şubeler de topolojiye dahil edilmek istenmiş, bunlar FR bağlantılar ile merkeze bağlanmıştır. Buradaki bağlantılar ve guvenlik için kurulan tüneller ayrı bir yönlendiricide sonlandırılarak, ana yönlendiricinin üzerindeki işlemci ve hafıza yükünün çok fazla olmaması amaçlanmıştır. Tüm bağlantılar sağlandıktan sonra ortaya çıkacak topoloji, Şekil 5.2de gösterilmiştir. Şekilde kırmızı ile çizilmiş bağlantılar, sonradan eklenen bağlantıları göstermektedir.



Şekil 5.2: Birleşme sonrası ortaya çıkan topoloji yapısı

Topoloji oluşturulduktan sonra, yönlendirme protokolünün seçimine gelinmiştir. Daha önce bahsedildiği gibi seçim sırasında ilk karar, yönlendirilecek üçüncü katman protokolüne göre verilir. Burada firmalar IP haberleşmesi yapacaklarından, tez kapsamında anlatılan tüm protokoller kullanılabilmektedir.

IP protokolünü yönlendirebilecek protokoller ayrıldıktan sonra, topolojiye en uygun olanın seçilmesi gerekmiştir. Günümüz ihtiyaçları göz önüne alındığında böyle bir şebekede kullanılacak protokolün VLSM kullanımını desteklemesi tercih edilir. Bu yüzden RIPv1 ve IGRP protokolleri tercih edilmemiştir.

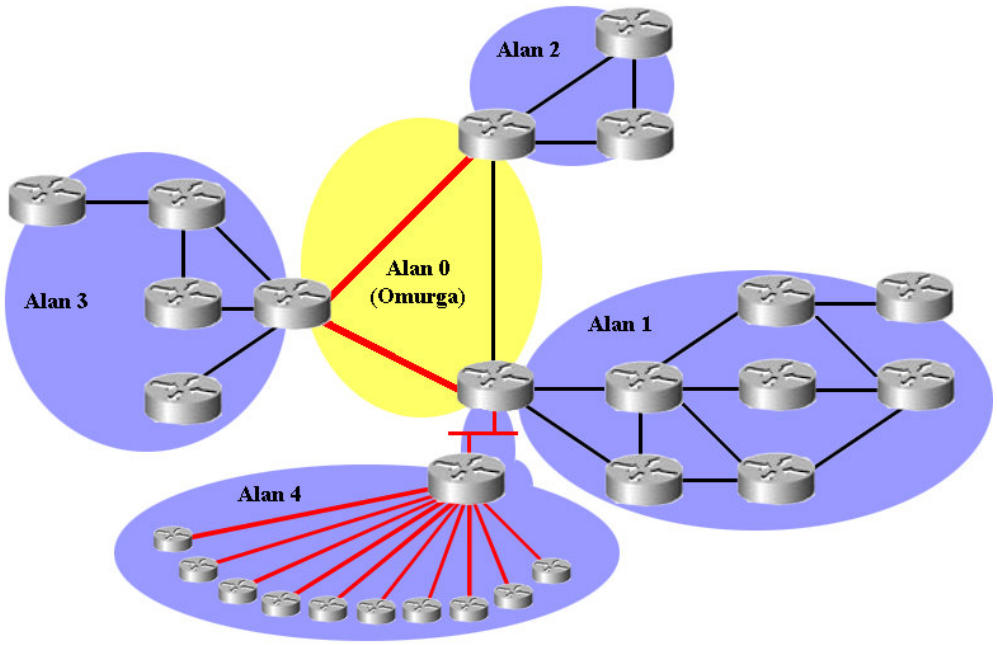
Şebekenin büyüklüğü ve ilerideki genişleme olanakları göz önüne alındığında RIPv2 protokolünün kullanımı da uygun olmayacaktır. RIP hem yavaş öğrenimi ile şebeke değişikliklerine yeterince hızlı uyum sağlayamaz; hem de metrik olarak adım sayısını kullanması, zaman zaman verilen yönlendirme kararlarının sağlıklı olmamasına yol açar.

EIGRP protokolü buradaki topolojide kullanıma uygun olmakla birlikte, Firma A yapısındaki cihazların tamamının Cisco olmaması nedeniyle, bu protokol kullanılırsa, cihazların değişimini veya topoloji üzerinde iki farklı yönlendirme protokolünün aynı anda çalıştırılmasını gerektirecektir. Bu da farklı yönlendirme protokollerinin metrikleri birbirine çevrilirken sorunlar oluşturabilmektedir.

Yapısal özellikleri çok benzer olan OSPF ve IS-IS bu şebekede kullanıma uygundurlar. Bu senaryoda, yönetim kolaylığı ve alanların yönlendiricilere arabirim bazında atanabilmesi gibi özellikleri göz önüne alınarak, OSPF kullanılmasına karar verilmiştir. OSPF yapısı kurulduğunda ve alanlar belirlendiğinde oluşan yapı ise, Şekil 5.3'te gösterilmiştir.

Omurga üzerindeki yönlendiriciler daha fazla trafik yükü taşıyacaklarından aralarındaki bağlantıların kapasiteleri yüksek seçilmiş, şubeler ise daha az trafik yarattıklarından daha düşük kapasiteli FR hatlar üzerinden merkeze bağlanmışlardır.

OSPF, yeni oluşan firmanın ihtiyaçlarını en iyi şekilde karşıladığı gibi, gelecekteki gelişme olanaklarını da kısıtlamamaktadır. Şebeke üzerinde özellikle VoIP uygulamaları için trafiğin önceliklendirilmesine olanak tanıyan OSPF, firmanın kendi uygulamalarının trafiği için de istenen ayarlamaların yapılabilmesini sağlamaktadır.



Şekil 5.3: OSPF uygulamasında alanlar

Görüldüğü gibi, yönlendirme protokollerinin seçiminde pek çok husus etkili olmaktadır. IP şebekeleri tasarlanırken bu hususların tümü göz önünde bulundurulmalı, ayrıca yönlendirme protokollerindeki gelişmeler de izlenerek, en uygun yönlendirme protokolüne karar verilmelidir. Günümüzde yönlendirme protokollerinin kullandığı algoritmaların değişmesinden çok, var olan algoritma ve protokollerin yeni teknolojiler ile kullanıma uygun hale getirilmesine çalışılmaktadır. Özellikle, var olan yönlendirme protokollerinin Mobil IP, IPv6, MPLS ve Trafik mühendisliği ile trafiğin yönetilmesi teknolojilerine uygulanması üzerinde durulmaktadır.

KAYNAKLAR

[1] **Lammle, T., Odom, S. and Wallace, K.**, 2001. CCNP Routing Study Guide, Sybex Inc., Alameda USA

[2] **Gough, C.**, 2004. CCNP Self Study - CCNP BSCI Exam Certification Guide 3rd Edition, Cisco Press, Indianapolis USA

[3] Route Selection in Cisco Routers, Document ID: 8651

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094823.shtml

[4] **Hedrick, C.,** 1988. RFC 1058 – Routing Information Protocol

[5] **Lammle, T.,** 2004. CCNA: Cisco Certified Network Associate Study Guide 4th Edition, Sybex Inc., Alameda USA

[6] **Odom, W.,** 2004. CCNA ICND Exam Certification Guide, Cisco Press, Indianapolis USA

[7] **Cisco Press,** 2003. Internetworking Technologies Handbook 4th Edition, Cisco Press, Indianapolis USA

[8] **Haden, R.,** 1998-2001. IGRP, EIGRP, http://www.rhyshaden.com/igrp.htm, http://www.rhyshaden.com/eigrp.htm

[9] **Goralski, W. J.,** 2002. Juniper and Cisco Routing - Policy and Protocols forMultivendor IP Networks, Wiley Publishing, Indianapolis USA

[10] **Garett, A., Drenan, G. ve Morris, C**., 2002. Juniper Networks Field Guide and Reference, Juniper Networks, USA

[11] **Thomas, T. M., Pavlichek, D.**, 2002. Juniper Networks Reference Guide, Juniper Networks, USA

[12] **Sportack, M**., 1999. IP Routing Fundamentals, Cisco Press, Indianapolis USA

[13] **Perkins, C.E.,** 2005. IP Mobility Support for IPv4,

http://www.mip4.org/drafts/rfc3344bis/draft-ietf-mip4-rfc3344bis-02.txt

[14] **Ishiguro, K., Takada, T.,** 2006. Traffic Engineering Extensions to OSPF version 3, http://www.ietf.org/internet-drafts/draft-ietf-ospf-ospfv3-traffic-07.txt

ÖZGEÇMİŞ

Özgür Karaman 1980 yılında İstanbulda doğmuştur. İlk öğrenimini Sakıp Sabancı Yıldız İlköğretim Okulu'nda, orta ve lise öğrenimini İstanbul Özel Alman Lisesi'nde tamamlamıştır. İstanbul Teknik Üniversitesi Elektronik ve Haberleşme Bölümü'nde 1999 yılında Lisans öğrenimine başlayarak 2003 yılında mezun olmuştur. Aynı yıl içinde İstanbul Teknik Üniversitesi Telekomunikasyon Mühendisliği Bölümü'nde yüksek lisans öğrenimine başlamıştır. Halen İTÜ'de yüksek lisans öğrenimine devam etmektedir.