OSI Referans Modeli

Bilgisayar ağları kullanılmaya başlandığı ilk zamanlarda sadece aynı üreticinin ürettiği cihazlar birbirleriyle iletişim kurabiliyordu. Bu da şirketleri tüm cihazlarını sadece bir üreticiden almalarını zorunlu kılıyordu. 1970'lerin sonlarına doğru ISO (International Organization for Standardization) tarafında, OSI (Open System Interconnection) modeli tanımlanarak bu kısıtlamanın önüne geçildi. Böylece farklı üreticilerden alınan cihazlar aynı ağ ortamında birbirleriyle haberleşebileceklerdi.

OSI Referans Modeli 7 katman (layer)'dan oluşmuştur. Bu katmanlar sırasıyla;

Application
Presentation
Session
Transport
Network
Data Link
Physical

Şimdi bu katmanları teker teker ayrıntılı bir şekilde inceleyelim.

a) Application Layer (Uygulama Katmanı): Kullanıcı tarafından çalıştırılan tüm uygulamalar bu katmanda tanımlıdırlar. Bu katmanda çalışan uygulamalara örnek olarak, FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol), e-mail uygulamalarını verebiliriz.

b) Presentation Layer (Sunuş Katmanı): Bu katman adını amacından almıştır. Yani bu katman verileri uygulama katmanına sunarken veri üzerinde bir kodlama ve dönüştürme işlemlerini yapar. Ayrıca bu katmanda veriyi sıkıştırma/açma, şifreleme/şifre çözme, EBCDIC'dan ASCII'ye veya tam tersi yönde bir dönüşüm işlemlerini de yerine getirir. Bu katmanda tanımlanan bazı standartlar ise şunlardır;PICT ,TIFF ,JPEG ,MIDI ,MPEG.

c) Session Layer (Oturum Katmanı): İletişimde bulunacak iki nokta arasındaki oturumun kurulması, yönetilmesi ve sonlandırılmasını sağlar. Bu katmanda çalışan protokollere örnek olarak NFS (Network File System), SQL (Structured Query Language), RPC (Revate Procedure Call), ASP (AppleTalk Session Protocol) ,DNA SCP (Digital Network Arcitecture Session Control Protocol) ve X Window verilebilir.

d) Transport Layer (İletişim Katmanı): Bu katman iki düğüm arasında mantıksal bir bağlantının kurulmasını sağlar. Ayrıca üst katmandan aldığı verileri segment'lere bölerek bir alt katmana iletir ve bir üst katmana bu segment'leri birleştirerek sunar. Bu katman aynı zamanda akış kontrolü (flow control) kullanarak karşı tarafa gönderilen verinin yerine ulaşıp ulaşmadığını kontrol eder. Karşı tarafa gönderilen segment'lerin karşı tarafta gönderenin gönderdiği sırayla birleştirilmesi işinden de bu katman sorumludur.

e) Network Layer (Ağ Katmanı) : Bu katman , veri paketlerinin ağ adreslerini kullanarak bu paketleri uygun ağlara yönlendirme işini yapar. Yönlendiriciler (Router) bu katmanda tanımlıdırlar. Bu katmanda iletilen veri blokları paket olarak adlandırılır. Bu katmanda tanımlanan protokollere örnek olarak IP ve IPX verilebilir. Bu katmandaki yönlendirme işlemleri ise yönlendirme protokolleri kullanılarak gerçekleştirilir. Yönlendirme protokollerine örnek olarak RIP,IGRP,OSPF ve EIGRP verilebilir. Burada dikkat edilmesi gereken önemli bir nokta da yönlendirme protokolleri ile yönlendirilebilir protokollerin farklı şeyler olduğudur. Bu katmanda kullanılan yönlendirme protokollerinin görevi

,yönlendirilecek paketin hedef'e ulaşabilmesi için geçmesi gereken yolun hangisinin en uygun olduğunu belirlemektir. Yönlendirme işlemi yukarıda bahsettiğimiz yönlendirme protokollerini kullanarak dinamik bir şekilde yapılabileceği gibi ,yönlendiricilerin üzerinde bulunan yönlendirme tablolarına statik olarak kayıt girilerek de paketlerin yönlendirilmesi gerçekleştirilebilir.

f) Data Link Layer (Veri Bağı Katmanı) : Network katmanından aldığı veri paketlerine hata kontrol bitlerini ekleyerek çerçeve (frame) halinde fiziksel katmana iletme işinden sorumludur. Ayrıca iletilen çerçevenin doğru mu yoksa yanlış mı iletildiğini kontrol eder ,eğer çerçeve hatalı iletilmişse çerçevenin yeniden gönderilmesini sağlamak da bu katmanın sorumluluğundadır. Bu katmanda ,iletilen çerçevenin hatalı olup olmadığını anlamak için **CRC (Cyclic Redundancy Check)** yöntemi kullanılır. Switch'ler ve Bridge'ler bu katmanda tanımlıdırlar.

g) Physical Layer (Fiziksel Katman): Verilerin fiziksel olarak gönderilmesi ve alınmasından sorumlu katmandır. Hub'lar fiziksel katmanda tanımlıdırlar.Bu katmanda tanımlanan standartlar taşınan verinin içeriğiyle ilgilenmezler. Daha çok işaretin şekli ,fiziksel katmanda kullanılacak konnektör türü , kablo türü gibi elektiriksel ve mekanik özelliklerle ilgilenir. Örneğin V.24 ,V.35, RJ45 ,RS-422A standartları fiziksel katmanda tanımlıdırlar.

Data Encapsulation

Veriler ,ağ üzerindeki cihazlar arasında iletilirken OS'nin her bir katmanında enkapsülasyona uğrar.OSI 'nın her katmanı iletişim kurulan diğer cihazdaki aynı katmanla iletişim kurar.OSI modelindeki her katman iletişim kurmak ve bilgi alışverişi için **PDU (Protocol Data Units)** 'ları kulllanırlar. Aşağıdaki tabloda herbir katmanın kullandığı PDU gösterilmiştir.

Katman	PDU (Protocol Data Units)
Transport Layer	**Segment**
Network Layer	**Packet**
Data-Link	**Frame**
Physical	**Bit**

Ethernet Agları

Ethernet ,kolay kurulumu ,bakımı ve yeni teknolojilere adapte olabilme özellikleriyle günümüzde en çok kullanılan ağ teknolojilerinin başında yer alır. Ethernet ağlarda yola erişim yöntemi olarak **CSMA/CD (Carrier Sense Multiple Access with Collision Detect)** kullanılır. Bu yöntemde aynı anda birden fazla cihazın aynı yol üzerinden veri göndermesi engellenmiş olur. Veri gönderecek cihaz ilk önce yolu dinler ve eğer yolda herhangi bir veri yoksa kendi verisini yola çıkarır. Eğer iki cihaz aynı anda yola veri çikarmaya çalışırlarsa bu durumda **collision(çakışma)** olur ve bu iki cihazda hatı bırakır. Ardından yeniden hatta çıkmak için restgele hesaplanan bir süre beklerler. Bu süreyi hesaplamak için kulllanılan algoritmalar "**back-off**" algoritmaları olarak adlandırılır.

Ethernet ağlarda adresleme için **MAC (Media Access Control)** adresleri kullanılır. MAC adresleri herbir NIC(Network Interface Card) 'in içine donanım olarak kazınmıştır ve 48 bitlik bir sayıdır. Bu 48 bitin ilk 24 bit'i bu kartı üreten firmayı tanımlayan koddur. Geriye kalan 24 bit ise o karta ait tanımlayıcı bir koddur. Bir ethernet ağda aynı MAC adresine sahip iki cihaz olamaz. Zaten MAC adresleride dünyada bulunan herbir NIC için tekdir. Örnek bir MAC adresi A0-CC-AC-03-55-B9 şeklindedir.

Aşağıdaki tabloda Ethernet ağlarda tanımlanmış standartları bulabilirsiniz.

Standart	Band Genişliği	Maksimum Mesafe	Kullanılan Kablo
10Base-2 (Thinnet)	10 Mbps	185 metre	50 μηο'luk sonlandırıcı ile sonlandırılmış ince koaksiyel kablo.
10Base-5 (Thicknet)	10 Mbps	500 metre	50 μηο'luk sonlandırıcı ile sonlandırılmış kalın koaksiyel kablo.
10Base-T	10 Mbps	100 metre	Cat 3, Cat 4 ,Cat 5 UTP kablo.
10Base-F	10 Mbps	2 Km	Fiber Optik
100Base-TX	100 Mbps	100 metre	Cat 5 UTP veya Type 1 STP
100Base-T4	100 Mbps	100 metre	Cat 3,Cat 4,Cat 5 UTP
100Base-FX	100 Mbps	450 metre-2 Km	Fiber Optik
1000Base-LX	1000 Mbps	440 metre-3 Km	Single Mod veya Multi Mod Fiber Optik kablo.
1000Base-SX	1000 Mbps	260 –550 metre	Multi Mod Fiber Optik kablo.
1000Base-CX	1000 Mbps	25 metre	Bakır kablo.
1000Base-T	1000 Mbps	100 metre	Cat 5 UTP

Önemli bir nokta da aslında birbirinden farklı olan Ethernet ile IEEE'nin 802.3 standartının birbirleriyle karıştırılmasıdır.Aslında bu iki teknoloji birbirlerine çok benzerler ve bu yüzden karıştırılırlar. Ethernet DEC ,Intel ve Xerox firmaları tarafından 1980 yılıda duyurulmuştur.

Ethernet standartlarında kullanılan dört farklı tipte çerçeve (frame) mevcuttur. Bunlar;

- **Ethernet_II**
- **Ethernet_802.3 (Novell Uyumlu)**
- **IEEE 802.3**
- **IEEE 802.3 SNAP (SubNetwork Access Protocol)**

Yukarıdaki dört çerçeve tipi de Ethernet ağlarda kullanılabilir. Fakat bu çerçeve

tipleri birbirleriyle uyumlu değillerdir. Yani aynı ağda farklı çerçeve tiplerini kullanan iki cihaz haberleşemezler. Bu iki cihazın birbirleriyle haberleşebilmeleri için enkapsülasyon (encapsulation)işleminin yapılması gerekir. Yani çerçeve tiplerinin birbirlerine dönüştürülmesi gerekir. Şimdi sırasıyla bu çerçeve tiplerini inceleyelim.

1. **Ethernet_II** :

Preamle	DA	SA	EType	Üst katman verisi	CRC

Bu çerçevedeki Preamle kısmı 64 bit uzunlupunda olup senkronizasyon için kullanılır. DA(Destination Address) ,hedef adresi gösterir ve 6 byte uzunluğundadır. SA(Source Address) kısmında ise gönderenin 6 Byte uzunlupundaki MAC adresi bulunur. EType (Ether-type) kısmında ise 2 Byte'lık bir değer bulunur ve bu değer taşınan verinin hangi protokole ait olduğunu belirtir. Örneğin IP için bu değer 0800 'dür. Üst kasman verisi kısmında ise bir üst katmandan alınan veri bulunur. Çerçevenin sonunda bulunan 4 Byte 'lık CRC ise hata sezme algoritmaları kullanılarak hesaplanmış bir değerdir ve karşı taraf bu değere bakarak çerçevenin doğru iletilip iletilmediğini anlar.

2. **Ethernet_802.3** :

Preamle	DA	SA	Length	FFFF(Üst Katman verisi)	CRC

Bu çerçeve tipi yukarıda anlatılan Ethernet_II tipine çok benzer . Tek farkı bu çerçevede üst katman'dan alınan verinin başında 2 Byte uzunluğunda bir null-checksum bulunur.

3. **IEEE 802.3**

Preamle	DA	SA	Length	DSAP	SSAP	Control	Üst Katman verisi	CRC

Endüstride Ethernet_802.2 ve Cisco'nun adlandırmasıyla SAP ,802.2 başlık bilgisi

ile DSAP(Destination SAP) ve SSAP(Source SAP) bilgisini içerir. Buradaki DSAP kısmı 1 Byte uzunluğunda olup hedef servis erişim noktasının değeridir. SSAP ise yine 1 Byte uzunluğunda olup kaynak servis erişim noktasını gösterir. Control kısmı ise 1 veya 2 Byte uzunlupunda bir değer olup LLc katmanındaki bağlantının connection-oriented mi yoksa connectionless mi olduğunu gösterir.

4. **IEEE 802.3 (SNAP)** :

Preamle	DA	SA	Length	DSAP	SSAP	Control	Vendor Code	Type	Üst Katman verisi	CRC

Endüstride Ethernet_SNAP olarak bilinen bu çerçeve formatında 802.2 çerçeve başlığına 5 Byte uzunluğunda SNAP bilgisi eklenmiştir. Bu çerçevedeki Vendor Code kısmında 3 Byte uzunluğunda bir değer bulunur ve bu kod üreticiyi tanımlayan bir koddur.Type kısmında ise 2 Byte'lık bir değer bulunur ve çerçevede taşınan verinin ait olduğu protokolu belirtir.

Connection-Oriented ve Connectionless Protokoller

- Connection -Oriented (Bağlantı - Temelli) Protokoller : Bu protokoller iki uç nokta arasındaki veri iletimini güvenli ve garantili bir şekilde sağlar. Yani verinin gidip gitmediğini ,gitdiyse verinin doğru gidip gitmediğini

kontrol eder. Eğer veri yanlış iletilmişse karşı taraftan verinin doğrusunu istemekte bu protokollerin görevidir. Bu protokollerin genel karakteristik özellikleri ise şöyledir.

- **Session Setup :**İki uç sistem arasında iletişime başlamadan önce sanal bir devre kurulur.

Acknowledgements : Gönderen tarafa verinin iletildiğine dair bir mesaj yollanır.

- **Sequencing :** Gönderilen çerçevelerin iletim ortamında kaybolup kaybolmadığı kontrol edilir.
- **Flow Control :** Veri gönderim hızını kontrol eder. Bir uçtaki sistem diğer uçtaki sisteme veri gönderim hızını yavaşlatmasını söyleyebilir.

Keepalives :Veri iletiminin olmadığı zamanlarda bağlantının kopmamasını sağlar.

- **Session Teardown :** Uç sistemlerden gelen bağlantı kesme istekleri doğrultusunda aradaki sanal devreyi koparır.
- **Connectionless (Bağlantısız) Protokoller :** Bu protokoller veriyi gönderir fakat gönderilen verinin doğru yere gidip gitmediğini ,doğru gidip gitmediğini kontrol etmezler. Peki bu protolkolleri kullanmanın bize ne faydası var? En önemli faydası gönderilen verilere kontrol bitlerini eklemedikleri ve verinin doğru gidip gitmediğini kontrol etmedikleri için hızlıdırlar.

IEEE Data Link Altkatmanları

IEEE ,OSI'nin Data Link katmanını **LLC(Logical Link Control)** ve **MAC (Media Access Control)** olmak üzere iki alt katmana ayırmıştır. Böylece aynı network kartı ve kablosu üzerinden birden fazla protokol ve çerçeve tipi iletişim kurabilir. Şimdi kısaca bu katmanları inceleyelim.

1. **LLC (Logical Link Control) Katmanı**:Network katmanı ile donanım arasında transparan bir arayüz sağlar. Bu katmanda protokoller çerçeve içindeki bir byte'lık SAP(Service Access Point) numarasıyla adreslenir. Örneğin SNA 'nın SAP numarası 04,NETBIOS 'un Sap numarası F0 'dır. Bunun haricinde LLC üst katman protokollerine connection-oriented veya connectionless servis verebilir. Bu servisler type 1,type 2 ve type 3 kategorileri olarak adlandırılırlar.

2. **MAC (Media Access Control) Katmanı** :NIC kartlarını kontrol eden sürücüler (driver) bu katmanda tanımlıdırlar. Bu sürücüler protokollerden bağımsız çalışırlar ve taşınan çerçevede hangi protokolun olduğunu dikkate almazlar.

Half-Duplex ve Full-Duplex Haberleşme

Half –Duplex iletişimde ,iletişimin yapıldığı iki sistem arasında aynı anda sadece bir tanesi iletim yapabilir. Diğer sistem bu sırada karşı sistemden gönderilen verileri almakla meşguldür.

Full-Duplex iletişimde ise her iki sistem de aynı anda veri alıp gönderebilirler.

Üç Katmanlı Hiyerarşi

Cisco , ağ planlaması sırasında ve donanımların yerlerinin belirlenmesi sırasında kendisinin sunduğu üç katmanlı yapıyı gözönünde bulundurmayı tavsiye eder. Bu yapı aşağıdaki üç katmandan oluşur;

- **Core Layer**
- **Distribution Layer**
- **Access Layer**

Bu modelde ,herbir katmanda çalışacak ağ cihazlarının özellikleri ve fonksiyonları açıklanmıştır.

Şimdi kısaca bu katmanlara bir göz atalım;

1. **Core Layer** : Bu katmandaki ağ cihazları network'ün omurgasında kullanılmalıve yüksek hızlara sahip olmalıdır.

2. **Distribution Layer** : Bu katmandaki ağ cihazları core katmanındaki cihazlara bağlantı için kullanılır. Ayrıca bu cihazlar broadcast ve multicast trafiğini kontrol ederler.

3. **Access Layer** : Bu katmandaki ağ cihazları ağa bağlanacak kullanıcılar için bir bağlantı noktasıdır. Bu katmanda kullanılabilecek ağ cihazlarına örnek olarak switch,bridge ve hub verilebilir.

Layer-2 Switching

Layer-2 Switching ,donanım tabanlı bir filtreleme yöntemidir ve bu yöntemde trafiği filtrelemek için NIC kartlarının MAC adresleri kullanılır. Layer-2 switching ,filetreleme için Network katmanı bilgilerinin yerine çerçevelerdeki MAC adreslerini kullandığı için hızlı bir yöntemdir. Layer-2 switching kullanmanın en önemli amacı ,ağı **collision domain**'lere bölmektir. Böylece ağ ortamı daha verimli kullanılmış olur. Switch kullanarak ağ ortamını segmentlere bölebilirsiniz. Böylece ağdaki **collision domain** sayısını arttırarak **collision**'u azaltmış olursunuz. Fakat switch kullanılarak yapılan segmantasyon işleminden sonra bile mevcut ağ tek bir broadcast domain olarak kalır. Yani yapılan tüm broadcast mesajlar ağın tamamını etkiler. Eğer ağı birden fazla broadcast domain'e bölmek istiyorsanız o zaman segmentasyon işlemi için router kullanmalısınız.

Layer-2 switching `in başlıca üç fonksiyonu vardır. Bunlar ;

- Adres Öğrenme :Layer –2 swicth ve bridge'ler ,herbir arayüzlerinden aldıkları çerçevelerin kaynak adreslerini öğrenerek bu adresleri kendi MAC veritabanlarına kayıt ederler.

- İletme/Filtreleme Kararı :Switch , arayüzlerinden aldığı herbir çerçevenin hedef adresine bakar ve bünyesinde bulundurduğu MAC veritabanına bakarak bu çerçevenin hangi arayüzünden çıkarılacağına karar verir.

- Döngüden Kaçınma :Eğer ağdaki switch'ler arasında birden fazla bağlantı varsa ,bu switchler arasında bir dönğü ağı oluşabilir. Bu durumu önlemek için **STP (Spanning Tree Protocol)** protokolu kullanılır

STP (Spanning Tree Protocol)

STP protokolü birden fazla link üzerinden birbirine bağlanmış switch'ler arasında bir ağ döngüsü olmasını engeller. Bunun için , kullanılan yedek linkleri kapatır. Yani STP ağdaki tüm likleri bularak bu linklerin yedek olanlarını kapatıp döngü oluşmasını engeller. Bunu gerçekleştirmek için ağ üzerindeki switch'lerden bir tanesi "**root bridge**" olarak seçilir. Bu switch'in portları da "**designated port"** olarak adlandırılır. Bu portlar üzerinden trafik alış verişi olur.Ağdaki

diğer switch'ler ise "**nonroot bridge**" olarak adlandırılır.Root switch , ağ üzerinde daha düşük öncelikli ID'ye ve MAC adresine sahip olan switch olur.Root switch'in dışındaki switch'ler kendileri ile root switch arasındaki en düşük cost değerine sahip yolu seçerler. Bu yolun haricindeki diğer yollar yedek olarak kalır ve birinci yol aktif olduğu müddetçe bu yollar kullanılmaz. STP protokolü , **BPDU (Bridge Protocol Data Unit)** tipinde çerçeveler kullanır.

LAN Switch Tipleri

LAN'larda kullanılabilecek üç tip anahtarlama modeli vardır. Bunlar;

- **Store and forward**

- **Cut-through**

- **Fregment Free**

Store and forward modelinde bir çerçevenin tamamı tampon belleğe alınır. CRC'si kontrol edilir ve daha sonra MAC tablosuna bakılarak iletilmesi gereken arayüze gönderilir. Cut-through modelinde ise alınan çerçevelerin tamamının tampon belleğe gelmesi beklenmeden sadece çerçevedeki hedef adrese bakılır ve MAC tablosundaki karşılığına bakılarak uygun arayüzden çıkartılır. Fregment Free modelinde ise çerçevenin ilk 64 byte'ına bakılır ve daha sonra MAC tablosundaki karşılık gelen arayüzden çıkarılır.

TCP/IP ve DoD Modeli

TCP/IP protokol kümesi Department of Defense (DoD) tarafından geliştirilmiştir. DoD modeli daha önce açıkladığımız OSI modelinin özetlenmiş hali gibi düşünülebilir. Bu modelde 4 katman mevcuttur. Bu katmanlar şunlardır;

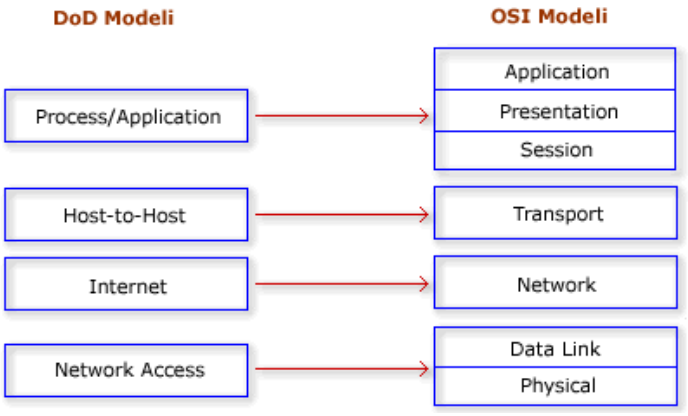
- **Process/Application katmanı**

- **Host-to-Host katmanı**

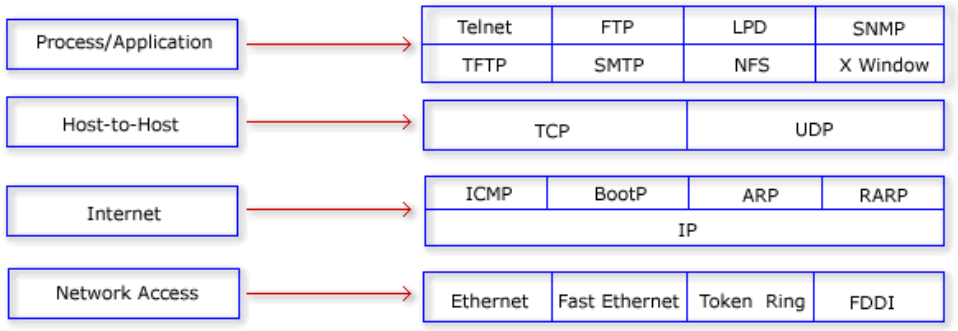
- **Internet katmanı**

- **Network Access katmanı**

Bu modelle OSI modelini karşılaştırırsak, bu modeldeki hangi katmanın OSI modelindeki hangi katmana denk düştüğünü aşağıdaki şekilden görebilirsiniz.



Şimdi de DoD modelinde her bir katmanda tanımlı olan protokolleri inceleyelim.



a) Process/Application Katmanı Protokolleri

Telnet : Telnet bir terminal emülasyon protokolüdür. Bu protokol, kullanıcıların telmet istemci programlarını kullanarak Telnet sunuculara bağlanmalarını sağlar. Böylece telnet sunucuları uzaktan yönetilebilir.

FTP (File Transfer Protocol) : İki bilgisayar arasında dosya alıp vermeyi sağlayan bir protokoldür.

TFTP (Trivial File Transfer Protocol) : Ftp protokolünün bazı özellikleri çıkartılmış halidir. Mesela bu protokolde FTP protokolünde bulunan klasör-gözatma (directory-browsing) ve kullanıcı doğrulama (authentication) yoktur. Genellikle küçük boyutlu dosyaların lokal ağlarda aktarılması için kullanılır.

NFS (Network File System) : Bu protokol farklı tipte iki dosya sisteminin bir arada çalışmasını sağlar.

SMTP (Simple Mail Transfer Protocol) : Bu protokol mail göndermek için kullanılır.

LPD (Line Printer Deamon) : Bu protokol yazıcı paylaşımını gerçekleştirmek için kullanılır.

X Window : Grakfiksel kullanıcı arayüzü tabanlı istemci sunucu uygulamaları geliştirmek için tanımlanmış bir protokoldür.

SNMP (Simple Network Management Protocol) : Bu protokol network cihazlarının göndermiş olduğu bilgileri toplar ve bu bilgileri işler. Bu özelliğe sahip cihazlar SNMP yönetim programları kullanılarak uzaktan izlenip yönetilebilir.

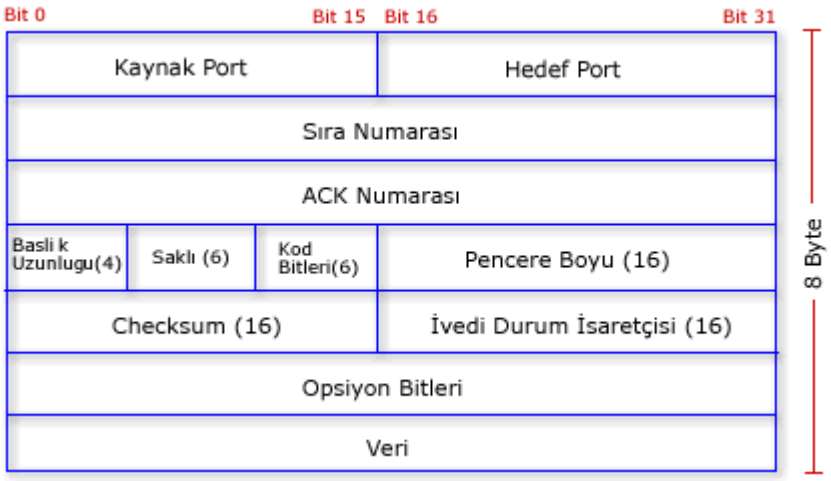
DNS (Domain Name Service) : Bu protokol internet isimlerinin (örneğin www.geocities.com gibi) IP adreslerine dönüştürülmesini sağlar.

BootP (Bootstrap Protocol) : Bu protokol disket sürücüsü olmayan bilgisayarların IP adres almalarını sağlar. Şöyleki network'e bağlı disket sürücüsüz bir bilgisayar ilk açıldığında ağa bir Boot P istediğini broadcast yapar. Ağdaki BootP sunucu bu isteği duyar ve gönderenin MAC adresini kendi tabanında arar. Eğer veritabanında bu istemci için bir kayıt bulursa bu istemciye bir IP adresini TFTP protokolünü kullanarak yollar. Ayrıca yine TFTP protokolünü kullanarak istemciye boot edebilmesi için gereken dosyayı yollar.

DHCP (Dynamic Host Configuration Protocol) : Bu protokol ağ üzerindeki istemcilere dinamik olarak IP adresi dağıtma işlemini yapar. Istemcilere IP adresinin yanısıra alt ağ maskesi (subnet mask), DNS sunucusunun IP adresi, ağ geçici adresi, WINS sunucunun adresi gibi bilgilerde dağıtılabilir.

b) Host-to-Host Katmanı Protokolleri

TCP (Transmission Control Protocol) : TCP protokolü uygulamalardan aldığı verileri daha küçük parçalara (segment) bölerek ağ üzerinden iletilmesini sağlar. Iki cihaz arasında TCP iletişimi başlamadan önce bir oturumun kurulması gerekir. Yani TCP connection-oriented türünde bir protokoldür. Bunun yanında TCP full-duplex ve güvenilir bir protokoldür. Yani gönderilen datanın ulaşıp ulaşmadığını, ulaştıysa doğru iletilip iletilmediğini kontrol eder. Bir TCP segmentinin formatı ise aşağıdaki şekildedir.



TCP başlığı 20 byte uzunluğundadır. Şimdi bu başlıktaki alanları teker teker inceleyelim. Kaynak port kısmında paketin ait olduğu uygulamanın kullanıldığı portun numarası bulunur. Hedef port kısmında ise alıcı uygulamanın port numarası bulunur. Sıra numarası kısmındaki sayı TCP'nin parçalara verdiği sayı numarasıdır. Paketler bu numaraya göre karşı tarafa gönderilir ve karşı tarafta paketleri bu sırayla birleştirir. ACK kısmındaki sayı ise TCP'nin özelliği olan güvenilirliğin bir sonucudur ve karşı tarafın gönderen tarafa hangi sıra numarasına sahip paketi yollaması gerektiğini belirtir. Yani karşı taraf birinci paketi aldığında gönderen tarafa ACK'sı 2 olan bir paket yollar. HLEN ise başlık uzunluğunu ifade eder. Saklı alanındaki bitler ise daha sonra kullanılmak üzere saklı bırakılmışlardır ve hepsi 0'dır. Kod bitleri kısmındaki değer ise bağlantının kurulması ve sonlandırılmasını sağlayan fonksiyonlar tarafından kullanılır. Pencere kısmındaki değer ise karşı tarafın kabul edeceği pencere boyutunu ifade eder. Checksum kısmındali değer CRC değeridir ve TCP tarafından hesaplanır. İvedi-durum işaretçisi eğer paketin içinde öncelikle değerlendirilmesi gereken bir veri varsa onun paket içindeki başlangıç noktasını işaret eder.

UDP (User Datagram Protocol) : Bu protokol TCP'nin aksine connectionless ve güvensiz bir iletişim sunar. Yani iletime başlamadan önce iki uç sistem arasında herhangi bir oturum kurulmaz. Ayrıca UDP'de gönderilen verinin yerine ulaşıp ulaşmadığı kontrol edilmez. Buna karşılık UDP TCP'den daha hızlıdır. Aşağıda bir UDP segmentinin formatı gösterilmiştir. Buradaki alanların işlevleri TCP segmentindeki alanlarla aynıdır.

c) Internet Katmanı Protokolleri

IP (Internet Protocol) : IP protokolü internet katmanının temel protokolüdür. Bu katmanda tanımlı olan diğer protokoller IP protokolünün üzerine inşa edilmişlerdir. Bu protokolde ağ üzerindeki her bir cihaza bir IP adresi tanımlanır. Bu katmanda çalışan ağ cihazları (örneğin router) kendisine gelen paketlerdeki IP adres kısmına bakarak bu paketin hangi ağa yönlendirilmesi gerektiğine kara verir.

ICMP (Internet Control Message Protocol) : Bu protokol IP tarafından değişik servisler için kullanılır. ICMP bir yönetim protokolüdür ve IP için mesaj servisi sağlar. Bu protokolü kullanan servislere örnek olarak ping, traceroute verilebilir.

ARP (Address Resolution Protocol) : Bu protokol ağ üzerinde IP adresi bilinen bir cihazın MAC adresinibulmak için kullanılır.

RARP (Reverse Address Resolution Protocol) : Bu protocol ise ARP'nin tam tersini yapar. Yani MAC adresi bilinen bir cihazın IP adresini öğrenmek için kullanılır.

IP adresi sayısal bir değer olup IP ağlardaki her bir cihazın sahip olması gerekir. IP adresleri MAC adreslerinin tersine donanımsal bir adres değil sadece yazılımsal bir değerdir. Yani istenildiği zaman değiştirilebilir. IP adresleri iki kısımdan oluşur. Birinci kısım Network ID olarak bilinir ve cihazın ait olduğu ağı belirtir. İkinci kısım ise Host ID olarak adlandırılır ve IP ağındaki cihazın adresini belirtir. Her bir cihaz için IP adresi tüm ağda tek olmalıdır.

IP Adresleri

IP adresleri 32 bit uzunluğundadır ve birbirinden nokta ile ayrılmış dört oktetden oluşur. Bu sayılar 0 ile 255 arasında bir değer olabilir. Örnek bir IP adresi 192.168.10.101'dir. Peki network'teki cihaz hangi ağa sahip olduğunu nasıl anlar? Bunu anlamak için subnet mask (alt ağ maskesi) denilen değeri kullanır. IP adresi ile subnet mask değerini lojik AND işlemine tabii tutarak kendi Network ID'sini bulur. Her bir IP adres sınıfı için bu subnet mask değeri farklıdır. Burada yeni bir kavram karşımıza çıktı. IP Adres Sınıfları. Şimdi bu IP adres sınıflarını inceleyelim.

1.) **A Sınıfı Adresler**: IP adresindeki ilk oktet 0 ile 127 arasındadır ve varsayılan subnet mask ise 255.0.0.0 'dır. A sınıfı IP adreslerinde ilk oktet network ID'yi diğer üç oktet ise host ID'yi gösterir. Burada ilk oktet'in 0 ve 127 olma durumları özel durumlardır ve network'te kullanılmazlar. Örneğin 127.0.0.1 yerel loopback adresidir. Dolayısıyla A sınıfı IP adresi kullanılabilecek ağ sayısı 126'dır. A sınıfı IP adresine sahip bir ağda tanımlanabilecek host sayısı ise şu formülle hesaplanır; $2^{24} - 2$. Bu işlemin sonucu olarakta 16.777.214 adet host olabilir. Peki burada kullandığımız 24 nereden geldi? A sınıfı adreste host'u tanımlamak için son üç oktet (sekizli) kullanılıyordu. Yani toplam 24 bit'i host tanımlamak için kullanabiliyoruz. Bu bitler ya 0 ya da 1 olmak zorunda. Bu yüzden birbirinden farklı kaç kombinasyon olacağını 2^{24} ile bulabiliriz. Bu sayıdan 2 çıkarmamızın nedeni ise bu 24 bit'in hepsinin 0 veya 1 olmasının özel bir anlamı olduğu ve herhangi bir

host'a IP adresi olarak verilemediği içindir. Örnek bir A sınıfı IP adresi 49.19.22.156 olarak verilebilir. Burada 49 bu IP adresinin ait olduğu ağın ID'sini 19.22.56 ise bu IP adresine sahip host'un host ID'sini gösterir.

2.) **B Sınıfı Adresler**: IP adresindeki ilk oktet 128 ile 191 arasındadır ve kullanılan subnet mask ise 255.255.0.0 'dır. Bu da demektir ki bu tür bir IP adresinde ilk iki oklet Network ID'sini, diğer iki oklet ise Host ID'yi gösterir. B sınıfı IP adresinin kullanılabileceği ağ sayısı 16.384 ve her bir ağda kullanılabilecek host sayısı ise 65.534'dür. Örnek bir B sınıfı IP adresi 160.75.10.110.olarak verilebilir.

3.) **C Sınıfı Adresler**: IP adresindeki ilk oktet'in değeri 192 ile 223 arasında olabilir ve varsayılan subnet mask değeri ise 255.255.255.0 'dır. Yani bu tür bir IP adresinde ilk üç oktet Network ID'yi son oktet ise Host ID'yi belirtir. Örneğin 192.168.10.101 IP adresini inceleyelim. Bu IP adresi C sınıfı bir IP adresidir. Bunu ilk oktetin değerine bakarak anladık. Bu IP adresinin ait olduğu ağın ID'si ise 192.168.10'dur. Bu IP adresine sahip cihazın host numarası ise 101'dir. C sınıfı IP adreslerinin kullanılabileceği ağ sayısı 2.097.152 ve bu ağların herbirinde tanımlanabilecek host sayısı ise 254'dür.

Bu üç IP sınıfının haricinde D ve E sınıfı IP adresleride mevcuttur. D sınıfı IP adresleri multicast yayınlar için kullanılır. E sınıfı adresler ise bilimsel çalışmalar için saklı tutulmuştur.

Subnetting

Subnetting kavramı nedir? Bu sorunun cevabını şöyle verelim. Farzedelim ki elimizde bir tane ağ adresiniz var fakat trafik olarak birbirinden bağımsız 4 tane ağ kurmak istiyorsunuz. Mesela şirketinizde bulunan muhasebe departmanı ile satış departmanlarının ağlarının birbirini etkilememesini istiyorsunuz ve elinizde bir tane ağ adresi var. Bu gibi durumlarda subnetting yani alt ağlara bölme işlemi yapılır. Bunun için IP adresindeki host'lar için ayrılmış kısımdaki bitlerden ihtiyaç olduğu kadarını subnet yapmak için alırız. Bu bitleri alırken gözönünde bulundurmamız gereken birkaç önemli nokta var. Bu noktalardan birincisi; kaç tane alt ağa ihtiyacımızın olacağını belirlememiz ayrıca her bir alt ağda kaç tane host bulunacağınıda gözönünde bulundurmamız gerekiyor. Alt ağ sayısını hesaplarken bu alt ağlar arasındaki bağlantılarıda bir alt ağ olarak hesaba katmalıyız. Host sayısını hesaplarken ise bu alt ağlar arası bağlantının sağlandığı arayüzleri de ayrı birer host gibi düşünüp hesaba katmalıyız.

Aşağıdaki tablolarda A, B ve C sınıfı IP adreslerinde kullanılabilecek alt ağ maskeleri ile bu alt ağ maskelerine denk düşen alt ağ sayısı ve her bir alt ağdaki host sayısını bulabilirsiniz. Biz burada bu alt ağ sayısı ve host ihtiyacına göre bu subnetmask'ların nasıl hesaplandığını göstermeyeceğiz. Bu konu hakkında kitaplardan yardım alınabilir

A Sınıfı IP Adreslerinde Subnetting

Subnet Mask	Alt ağ Sayısı	Host Sayısı	Kullanılabilecek Toplam Host Sayısı
255.192.00	2	4194302	8388604
255.224.0.0	6	2097150	12582900
255.240.0.0	14	1048574	14680036
255.248.0.0	30	524286	15728580
255.252.0.0	62	262142	16252804
255.254.0.0	126	131070	16514820
255.255.0.0	254	65534	16645636

255.255.128.0	510	32766	16710660
255.255.192.0	1022	16382	16742404
255.255.224.0	2046	8190	16756740
255.255.240.0	4094	4094	16760836
255.255.248.0	8190	2046	16756740
255.255.252.0	16382	1022	16742404
255.255.254.0	32766	510	16710660
255.255.255.0	65534	254	16645636
255.255.255.128	131070	126	16514820
255.255.255.192	262142	62	16252804
255.255.255.224	524286	30	15728580
255.255.255.240	1048574	14	14680036
255.255.255.248	2097150	6	12582900
255.255.255.252	4194302	2	8388604

B Sınıfı Adreslerde Subnetting

Subnet Mask	Alt ağ Sayısı	Host Sayısı	Kullanılabilecek Toplam Host Sayısı
255.255.192.0	2	16382	32764
255.255.224.0	6	8190	49140
255.255.240.0	14	4094	57316
255.255.248.0	30	2046	61380
255.255.252.0	62	1022	63364
255.255.254.0	126	510	64260
255.255.255.0	254	254	64516
255.255.255.128	510	126	64260
255.255.255.192	1022	62	63364
255.255.255.224	2046	30	61380
255.255.255.240	4094	14	57316
255.255.255.248	8190	6	49140
255.255.255.252	16382	2	32764

C Sınıfı IP Adreslerinde Subnetting

Subnet Mask	Altağ Sayısı	Host Sayısı	Kullanılabilecek Toplam Host Sayısı
255.255.255.192	2	62	124
255.255.255.224	6	30	180
255.255.255.240	14	14	196
255.255.255.248	30	6	180
255.255.255.252	62	2	124

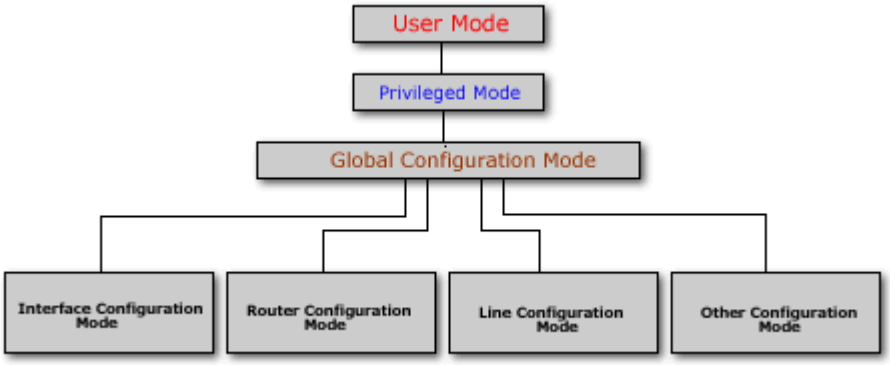
Router Temelleri

Cisco deyince birçoklarımızın aklına router gelir. Şimdi biraz router'ların temel yapısını inceleyelim. Router'ların üzerinde **IOS (Internetwork Operating System)** işletim sistemi çalışır. Bu işletim sisteminde temel olarak iki farklı komut modu vardır.

- **User exec**

- **Privileged exec**

Bu modların haricinde başka modlarda vardır. Modlar'ın hiyerarşik yapısı aşağıdaki şekildedir.



Router'a bağlanıp ,yönetmek için değişik seçenekler mevcuttur. Birincisi router'a direk konsol portundan bağlantı yapabilirsiniz. İkincisi uzaktan modem yoluyla router'in auxiliary portuna bağlanabilirsiniz. Üçüncü seçenek ise Router aktif olan LAN veya WAN portunda telnet aracılığı ile bağlanabilirsiniz. Fakat telnet ile bağlantı kurulacak Router'in bazı öncelikli ayarlarının yapılması (örneğin interface'lerin up duruma getirilip adreslerinin atanmış olması) gerekir.

Router'a ilk logon olduğunuzda user exec moda düşersiniz. Bu modda sadece bilgi görüntülüyebilirsiniz. Yani herhangi bir konfigürasyon değişikliği yapamazsınız. Herhangi bir değişiklik yapmak istiyorsanız privileged exec moda geçmeniz gerekiyor. User exec moddan privileged moda geçmek için **enable** komutu kullanılır. Bu komutu yazıp enter'a basarsanız router sizden şifre girmenizi isteyecektir. Doğru şifreyi girdikten sonra Router üzerinde istediğiniz ayarları gerçekleştirebilirsiniz.

Router'ın temel bileşenlerini

Router'ın temel bileşenlerini ve bu bileşenlerin işlevlerini bilmek Router'ın nasıl çalıştığı hakkında bir fikir sahibi olmamızı sağlayacaktır. Router'ların başlıca bileşenleri RAM, ROM, Flash ve NVRAM olarak sıralanabilir. Şimdi bu bileşenleri ve temel işlemlerini teker teker inceleyelim;

a. **ROM (Read Only Memory)**: Bootstrap yazılımı ,test ve bakım amaçlı kullanılan temel seviyede bir işletim sistemi olan ROM Monitor, POST (Power On Self Test) rutin'leri ve RXBoot olarak adlandırılan mini bir IOS ROM'da tutulur.

b. **Flash**: Silinebilir, yeniden programlanabilir (EPROM) olan bu yongada Cisco'nun IOS işletim sisteminin imajları tutulur. Bir flash'ta birden fazla IOS imajı bulunabilir. Router kapatıldığında flash'daki veri korunur.

c. **NVRAM (Non Volatile RAM)**: Router'ın konfigürasyon dosya veya dosyalarının tutulduğu yeniden yazılabilir bir yongadır. Router kapatıldığında NVRAM'daki veri korunur.

d. **RAM**: Çalışan IOS konfigürasyonlarını tutar. Ayrıca kaşelere (caching) ve paket depolama sağlar. Router kapatıldığında RAM'deki tüm veri kaybolur.

Router'ın Çalışması

Aynen PC'ler gibi Router'larda ilk açıldıklarında POST işlemini gerçekleştirir. Yani CPU, hafıza, interface devreleri gibi sistem donanımlarını kontrol eder. Tüm donanımın sağlam çalıştığından emin olduktan sonra POST işlemi ROM'da tutulan bootstrap yazılımını çalıştırır. Bootstrap programı Flash'da bulunan IOS'u bulur, sıkıştırmasını açar (decompress) ve bu IOS'u Flash'dan RAM'e yükler. Bazı router'lar yeterli hafızaya sahip olmadıkları için IOS'u RAM'e yüklemeden direkt Flash'dan çalıştırırlar. Eğer router herhangi bir geçerli IOS bulamazsa RAM'daki RXBoot olarak adlandırılan mini IOS'u yükler. Eğer bu işlemde başarısız olursa ROM Monitor (ROMMON) moduna düşer. IOS yüklendikten sonra NVRAM'da bulunan başlangıç konfigürasyonlarını (startup configuration) yükler. Eğer herhangi bir sebepten ötürü konfigürasyon dosyası bulamazsa IOS, "NVRAM invalid" mesajını verir ve IOS otomatik olarak "setup dialog" olarak adlandırılan konfigürasyon işlemini başlatır.

Konfigürasyon Register

Tüm cisco router'lar 16 bitlik bir software register'a sahiptirler ve bu register NVRAM'da tutulur. Bu registerin varsayılan değeri hex olarak 0X2102'dir ve route'a IOS'u Flash'tan ve konfigurasyon dosyasını da NVRAM'dan alarak başlamasını söyler. Bu register değerini değiştirerek router'ın nasıl boot edeceğine karar verebilirsiniz. Şöyle ki bu register'ın değerini 2142 yaparsanız Router'a NVRAM'ın içeriğine bakmadan başlamasını sağlarsınız. Böylece privileged mod şifresini unuttuğunuz bir router'ı bu yolla çalıştırıp şifreyi geçersiz yapabilirsiniz. Bu register'ın değerini 2100 yaparsanız Router ROM monitor modunda açılır. Konfigürasyon register'inin değerini öğrenmek için "**show version**" komutunu kullanabilirsiniz. Bu register'ın değerini değiştirmek için ise "**config-register**" komutunu kullanmalısınız.

RouterA(config)#config-register 0X0101

Temel arayüzleri

Şimdi de bir Router'da bulunan temel arayüzleri ve nerede kullanıldıklarına bir göz atalım.

- **AUI (Attachment Unit Interface)**: 15 pin'lik bir arayüzdür ve bir harici transceiver ile Enhernet ağlara bağlanabilir.

- **Seri Arayüzler**: Senkron WAN bağlantıları için kullanılırlar. 2400 Kbps ile 1.544 Mbps arasında bir veri hızına destek verirler. Serial 0, serial 1 gibi isimlerle isimlendirilirler..

- **BRI Portları**: Basic Rate ISDN portu, uzak bağlantılarda ISDN network'ünü kullanmamıza imkan verir. Genellikle asıl bağlantının yanında yedek bir bağlantı olarak kullanılır. Ayrıca Dial on Demond (DOR) özelliği ile eğer asıl link'in yükü çok artarsa bu bağlantıya yardımcı olmak için devreye girebilir.

- **Konsol Portu**: Router'a yerel olarak bağlanıp konfigüre etmek için kullanılan porttur. Varsayılan veri iletim hızı 9600 bps'dir. Bu portu kullanmak için **rollover kablo** kullanılır. Bu kablonun her iki ucunda RJ 45 konnektor bağlanmıştır.

Daha sonra bu konnektörlerin bir tanesi PC'nin seri portlarına bağlanabilmesi için RJ45 - 9 pin seri veya RJ45-25 pin seri dönüştürücüsüne takılarak PC'nin seri portlarından birisine takılır. Kullanılan rollover kablonun her iki uçtaki konnektörlere bağlantı şekli ise şöyle olmalıdır; Bir uçtaki konnektördeki kablo sırası 1-8 ise diğer uçtaki konnektöre bağlantı sırası ise 8-1 olmalıdır.

- **AUX Portu**: Router'ı konfigüre etmek için her zaman router'ın yanına gitmek zahmetli bir iştir. Router'ı uzaktan konfigüre etmek için bir modem aracılığıyla Router'ın bu portuna bağlantı kurulup gerekli işlemler yapılabilir.

DTE ve DCE

DTE ve DCE kavramları network'teki cihazları işlevsel olarak sınıflandırmamızı sağlar. DTE cihazları genellikle end-user cihazlardır. Örneğin PC'ler, yazıcılar ve router'lar, DTE cihazlardır. DCE cihazları ise DTE'lerin servis sağlayıcıların ağlarına ulaşabilmek için kullandıkları modem, multiplexer gibi cihazlardır. DCE'ler DTE'lere clock işaretini sağlarlar.

Cisco Router'ların seri interface'leri DTE veya DCE olarak konfigüre edilebilir. Bu özellik kullanılarak WAN bağlantıları simüle edilebilir. Bunun için birbirine bağlı Router'ların interface'lerinden bir tanesini DCE diğer Router'ın interface'sini ise DTE olarak kabul ediyoruz. Ardından DCE olarak kabul ettiğimiz interface'in DTE olan interface clock sağlaması gerekiyor. DCE olarak kullanabileceğimiz interface'de "**clock rate**" komutunu kullanarak bir değer atamamız gerekiyor. Aksi halde bağlantı çalışmayacaktır. Örneğin;

RouterA(conf-if)#clock rate 64000

Ayrıca clock rate parametresinin yanında "**bandwidth**" parametresininde girilmesi gerekiyor. DCE ve DTE olarak konfigüre edilecek interface'lerde tanımlanan "bandwidth" değerinin aynı olması gerekiyor. Eğer bandwidth değerini belirtmezseniz varsayılan değeri olarak 1,544 Mbps alınır. Bandwidth'e atadığınız değer sadece yönlendirme protokolü tarafından yol seçimi için kullanılır. Örnegin;

RouterA(conf-if)#bandwidth 64

Hyperterminal

Router'ı konfigüre etmek için kullanılan bir terminal emülasyon yazılımıdır. Bu yazılım Win 95/98 ve Win NT ile birlikte geldiği için en çok kullanılan terminal emülasyon programıdır. Şimdi bu programı kullanarak Router'a nasıl bağlantı kurulacağını anlatalım. PC'nin herhangi bir seri portuna taktığımız (COM1 veya COM2) DB-9-RJ45 dönüştürücüye rollover kabloyu takıyoruz. Ardından hyperterminal programını (hypertrm.exe) Start-Programlar-Donatılar'dan çalıştırıyoruz. Karşımıza çıkan "Connection Description" başlıklı pencerede kuracağımız bağlantıya bir isim veriyoruz. Ardından karşımıza çıkan "Connect to" penceresinde ise bağlantının kurulacağı seri port seçiliyor. Bağlantıyı kuracağımız seri portu seçtikten sonra bu portun özelliklerinin belirlendiği bir pencere ile karşılaşıyoruz. Uygun değerleri girdikten sonra hyper terminal penceresindeki "Call" butonuna basıp Router'a bağlantıyı sağlamış oluyoruz.

Router' ın Kurulması

Router'ın açılması sırasında router konfigürasyon dosyasını arar. Eğer herhangi bir konfigürasyon dosyası bulamazsa sistem konfigürasyon işlemi başlar. Bu işlem sırasında aşağıdaki sorulara "Yes" diye cevap verirseniz Router'ı soru temelli konfigüre edebilirsiniz.

- **Continue with configuration dialog? [yes/no]**

- **Would you like to see the current interface summary? [yes/no]**

Bu konfigürasyon türünde router size bir takım sorular sorar ve sizden bu soruların cevaplarını ister. Sorulan soruların varsayılan cevapları soru sonundaki köşeli parantezlerin ([]) içinde verilmiştir. Varsayılan cevapları kabul ediyorsanız yapmanız gereken tek şey Enter'a basmaktır. Eğer soru cevap tabanlı konfigürasyondan herhangi bir zamanda çıkmak istiyorsanız o zaman **Ctrl+C** tuşlarına basmanız yeterlidir.

Eğer yukarıda sorulan sorulara "No" diye cevap verirseniz Router'ı konfigüre edeceksiniz demektir. Bu durumda komut satırı aşağıdaki şekildedir.

Router>

Yani ilk düştüğünüz mod "user exec" moddur. Varsayılan olarak konfigüre edilmemiş tüm Router'ların adı Router'dır ve "privileged exec" moda geçmek için herhangi bir şifre tanımlanmamıştır. Router üzerinde herhangi bir konfigürasyon değişikliği yapmak istiyorsak privileged moda geçmemiz gerekiyor. Bunun için komut satırına aşağıdaki komutu yazalım.

Router>enable

Komutu yazdıktan sonra Enter'a basarsanız privileged moda geçersiniz. Bu sırada komut satırının şeklinin değiştiğine dikkat edin. Komut satırı şu şekli almıştır;

Router#

Privileged exec moddan, user exec moda geri dönmek için ise "disable" komutunu kullanabilirsiniz. Router'da tamamen bağlantıyı koparmak için ise "logout", "exit" veya "quit" komutlarını kullanabilirsiniz.

Router Komut Satırı İşlemleri

Cisco IOS'lar kullanıcılara birçok bakımdan kolaylıklar sunarlar. Örneğin Cisco IOS'lar komut kullanımı sırasında kullanıcılara geniş bir yardım seçeneği sunar. Mesela komut satırındayken **?** karakterine basarsanız bulunduğunuz modda kullanabileceğiniz tüm komutlar bir liste halinde karşınıza çıkacaktır. Eğer sıralanan komutlar ekrana sığmıyorsa ekranın alt kısmında **–More-** diye bir ifade belirecektir. Burada space tuşuna basarsanız sonraki komutları bir ekrana sığacak şekilde görebilirsiniz. Yok eğer varolan komutları teker teker görmek istiyorsanız Enter tuşuna basmanız gerekir.

Bunun haricinde Cisco IOS'lar komut bazında da yardım sağlıyor. Şöyleki; farzedelimki siz sh harfleriyle başlayan komutları listelemek istiyorsunuz. Bunun için komut satırına sh? yazarsanız sh ile başlayan tüm komutlar listelenecektir. Ayrıca kullandığınız komutun parametreleri hakkında bilgi almak içinde komutu yazdıktan sonra bir boşluk bırakıp ? karakterine basın. Örneğin show komutuyla birlikte kullanılabilecek parametreleri görmek için show ? ifadesini yazmalısınız.

Cisco IOS'un kullanıcılara sağladığı diğer önemli bir kolaylık ise komutların syntax'ını tam yazmaya gerek kalmadan komutu anlayarak zaman kazandırmasıdır. Örneğin show komutunu kısaltılmış hali sh'dir. Yani siz komut satırından sh girerseniz IOS bunun show komutu olduğunu anlayacaktır. Komutların kısaltılmış halini belirleyen kural ise o komutun komut listesinde tek (unique) olarak tanımlayabilecek karakter dizisini belirlemektir. Ayrıca komutun kısaltılmış halini yazdıktan sonra Tab tuşuna basarsanız IOS bu komutu, kısaltılmamış haline tamamlayacaktır. Örnegin show komutunu yazmak için sh yazıp Tab tuşuna basarsanız IOS bu komutu show şeklinde tamamlayacaktır. Ayrıca IOS

varsayılan olarak yazdığınız son 10 komutu hafızasında tutar. Bu sayıyı "history size" komutunu kullanarak 256'ya kadar arttırabilirsiniz.

Komut yazımı sırasında karşılaşabileceğiniz hata mesajları ve açıklamaları aşağıdaki tabloda verilmiştir.

Hata Mesajı	Açıklama
%Incomplete command	Yazdığımız komutun tamamlanmadığını ,eksik parametre girildiğini belirtir.
%Invalid input	Bu hata mesajıyla birlikte ^ karakteri kullanılır ve bu karekter yanlış girilen omutun neresinde yanlış yapıldığını gösterir.
%Ambiguous command	Girilen komut için gerekli karakterlerin tamamının girilmediğini belirtir. Kullanmak istediğiniz komutu **?** karakterini kullanarak tekrar inceleyin.

Aşağıgaki tabloda ise komut satırında kullanılabilecek kısayol tuşları ve fonksiyonlarını bulabilirsiniz.

Kısayol	İşlevi
Ctrl+A	İmleç'i komut satırının başına taşır.
Ctrl+E	İmleç'i komut satırının sonuna taşır.
Ctrl+N veya (↓)	Router'a son girdiğiniz komutlar arasında gezinmemizi sağlar.
Ctrl+F veya (→)	İmleç'i komut satırında bir karakter sağa götürür.
Ctrl+B veya (←)	İmleç'i komut satırında bir karakter sola götürür.
Ctrl+Z	Konfigürasyon modundan çıkartıp exec moda geri döndürür.
Ctrl+P veya (↑)	Router'a girdiğiniz son komutu gösterir.

Router Configurasyon Komutları

Router üzerinde yapmış olduğunuz değişikliklerin kalıcı olması için bu değişikliklerin konfigürasyon dosyasına yazılması gerekir. Aşağıdaki tabloda Router üzerindeki konfigürasyon ayarlarını görmek, kaydetmek veya silmek için kullanılabilecek komutları bulabilirsiniz.

IOS 10.3 ve öncesi	IOS 11.3 ve öncesi	IOS 12.0	Açıklama
Write terminal	Show running-config	More system: startup-config	Router üzerinde çalışan konfigürasyonu gösterir.
Show configuration	Show startup-config	More NVRAM: startup-config	NVRAM'da bulunan ve Router boot ederken kullanılan konfigürasyonu gösterir.
Write erase	Erase startup-config	Erase NVRAM	NVRAM'de bulunan ve Router boot ederken kullanılan konfigürasyon dosyasını siler.
Write memory	Copy runnig-config startup-config	Copy system: running–config	Router üzerinde yapmış olduğumuz konfigürasyon ayarlarının kalıcı olması için NVRAM'daki konfigürasyon dosyasını yazar.
Write network	Copy running-config TFTP	Copy system: running-config FTP; TFTP	Çalışan konfigürasyonunu FTP veya TFTP server'a kaydetmek için kullanılır.

IOS'un Yedeklenmesi ve Geri Yüklenmesi

Cisco IOS'ların yedeklenmesi ve yedekten geri yüklenmesi için kullanılan komutlar aşağıdaki tabloda listelenmiştir.

Komut	Açıklama
Copy flash tftp	Router'ın flash'ındaki IOS'un yedeğini TFTP server'a kopyalar.
Copy tftp flash	TFTP server'da bulunan bir IOS imajını flash'a kopyalamak için kullanılır.
Copy running-config tftp	Router üzerinde çalışan konfigürasyonu TFTP sunucuna kopyalar.
Copy tftp running-config	TFTP sunucunda bulunan bir konfigürasyon dosyasını router'a yükler.

Router Configurasyonu II

Şimdi sıra geldi şimdiye kadar teorisiyle ilgilendiğimiz Router'ı konfigüre edip basitçe yönlendirme yapabilecek duruma getirmeye. Bunun için ilk önce Router'a login oluyoruz. Ardından privileged exec mode geçmeniz gerekiyor. "**enable**" yazıp bu mode giriyoruz. Ardından router'a onu konfigüre edeceğimizi belirten "**configure terminal**" komutunu veriyoruz. (Bu komutun kısa yazılışı ise "config t"dir.) Şimdi gönül rahatlığı içinde Router'ı konfigüre etmeye başlayabiliriz. İlk önce Router'ımıza bir isim vererek başlayalım. Bunun için "**hostname**" komutunu aşağı şekilde giriyoruz. (Router'ın komut satırının nasıl değiştiğine dikkat edin!)

Router(config)#hostname RouterA

Bu komutu girdikten sonra komut satırı aşağıdaki gibi olacaktır.

RouterA(config)#

Router'ımıza bağlanan kullanıcılara bir banner mesajı göstermek isteyebiliriz. Bunu gerçekleştirmek için "**banner motd**" komutunu aşağıdaki şekilde kullanmalıyız.

RouterA(config)#banner motd#turkmcse.com Router'ına hoşgeldiniz#

Burada komuttan sonra kullandığımız # karakterlerinin arasına mesajımızı yazıyoruz.Bunun haricinde tanımlanabilecek bannerlar ise şunlardır;**Exec banner**,**Incoming banner** ve **Login banner.**

Sıra geldi Router'ımıza bağlantı sırasında kullanıcılara sorulacak şifreleri belirlemeye. Cisco Router'larda beş farklı şifre bulunur. Bunlardan ikisi privileged mod'a erişim için tanımlanırken, bir tanesi konsol portu, bir tanesi AUX portu ve diğeride Telnet bağlantıları için tanımlanır. Bu şifrelerden "**enable secret**" ve "**enable password**", privileged mod'a geçmek için kullanılırlar ve aralarındaki fark "enable secret""in şifrelenmiş bir şekilde saklanmasıdır. Yani konfigürasyon dosyasına baktığınızda "enable secret" şifresinin yerinde şifrelenmiş halini görürsünüz. Ama aynı dosyada "enable password""u ise açık bir şekilde şifreleme yapılmadan saklandığını görürsünüz. Bu da sizin konfigürasyon dosyanızı ele geçiren birisinin "enable password" şifresini kolayca okuyabileceğini ama "enable secret" şifresinden bir şey anlamayacağı anlamına gelir. "Enable password" şifresi ise "enable secret" şifresi tanımlanmamışsa veya kullanılan IOS eski ise kullanılır. "Enable secret" şifresinin konfigürasyon dosyasına yazılırken kullanılan şifrelemenin derecesini ise "**service password-encryption**" komutu ile belirleyebilirsiniz. Şimdi sırasıyla bu beş şifrenin nasıl tanımlandığını anlatalım; "Enable secret" ve "enable password" şifreleri aşağıdaki şekilde tanımlanır.

RouterA(config)#enable password cisco

RouterA(config)#enable secret istanbul

Burada turkmcse ve istanbul bizim koyduğumuz şifrelerdir.

Eğer Router'ın konsol portuna şifre koymak istiyorsanız

RouterA(config)#line console 0

RouterA(config-line)#login

RouterA(config-line)#password cisco

Router'ın AUX portuna şifre koymak için:

RouterA(config)#line aux 0

RouterA(config-line)#login

RouterA(config-line)#password istanbul

Router'ın Telnet bağlantılarında soracağı şifreyi ise şöyle belirleyebilirsiniz:

RouterA(config)#line vty 0 4

RouterA(config-line)#login

RouterA(config-line)#password turkiye

Burada telnet portlarının tamamına aynı şifre verilmiştir. Bu portların herbirisine farklı şifreler atanabilir. Fakat router'a yapılan her telnet isteğine router, o zaman kullanımda olmayan bir port'u atadığı için bağlantıyı kuran kişinin tüm bu telnet portlarına atanmış şifreleri bilmesi gerekir. Bu yüzden telnet portlarına ayrı ayrı şifre atamak iyi bir yaklaşım değildir.

Bunun haricinde Router'a yapılan konsol bağlantılarının, kullanıcı herhangi bir işlem yapmadan ne kadar süre aktif kalacağını da "**exec-timecut**" komutuyla belirleyebiliriz

Router Arayüzleri

Router'ların interface'lerini konfigüre etmek için her bir interface'e ait interface konfigürasyon moduna girilmelidir. Bu modda o interface'in aktif (up)'mi yoksa pasif mi (down) olacağını, IP adreslerini vb. konfigürasyon ayarları yapılır. Örneğin Router'ımızın 1 Ethernet ,2 tane de seri interface'inin olduğunu düşünelim. Ethernet interface'ini konfigüre etmek için aşağıdaki komutu global konfigürasyon modundayken girmeliyiz.

RouterA(config)#int e0

Bu komutu yazıp Enter'a basarsanız interface konfigürasyon moduna geçersiniz(Burada IOS'un bize sunmuş olduğu kolaylıkları kullanması da ihmal etmiyoruz tabiki ☺). Şimdi bu interface'in IP adresini belirleyelim. Bunun için aşağıdaki komut kullanılır;

RouterA(config-if)#ip address 10.3.9.1 255.255.255.0

Eğer bu interface için bir açıklama eklemek istiyorsanız bunu aşağıdaki gibi "**description**" komutunu kullanarak yapabilirsiniz.

RouterA(config-if)#description Pazarlama Grubunun LAN bağlantısı

Konfigüre ettiğiniz interface'in işlevselliğini yerine getirebilmesi için aktif (up) olması gerekiyor. Varsayılan olarak bütün interface'ler pasif **(administratively disabled)**'dir. Bunun için ise aşağıdaki komutu kullanmalısınız.

RouterA(config-if)#no shutdown

Ayrıca Cisco'nun 7000 veya 7500 serisi router'larında VIP(Versatile Interface Processor) kartları varsa bunun için aşağıdaki formatta bir komut kullanarak interface tanımlamalısınız;

Interface tip slot/port adaptör/port numarası

Örneğin;

RouterA(config)#interface ethernet 2/0/0

Debug İşlemi

Router üzerinde hata ayıklamak için kullanılabilecek komutlar mevcuttur. Bu komutların başında "**debug**" komutu gelir.

RouterA#debug all

Unutulmaması gereken bir nokta da debug işleminin Router'ın kaynaklarını bir hayli fazla kullandığıdır. Bu yüzden debug işlemi bitirildikten sonra "**undebug all**" veya "**no debug all**" komutlarından bir tanesi kullanılarak Router'a debug yapmaması gerektiği bildirilmelidir.

CDP (Cisco Discovery Protocol)

Data Link katmanında çalışan bu protokol Cisco tarafından geliştirilmiştir ve fiziksel olarak birbirine bağlı tüm Cisco cihazlarının birbirleri hakkında bilgi sahibi olmalarını sağlar. IOS 10.3 veya daha yukarı versiyon çalıştıran Router'larda CDP default olarak aktifdir ve otomatik olarak komşu Router ve switch'ler hakkında bilgi toplar. Bu bilgiler arasında cihaz ID'si ve cihaz tipi gibi bilgilerde bulunur. CDP kullanılarak öğrenilen bilgileri privileged mod'da "**show cdp neighbors**" komutunu kullanarak görebilirsiniz. Bu komutu kullandığınızda fiziksel olarak bağlı olduğunuz cihazların isimlerini, portlarını, cihaz tiplerini(router,switch vs.) ,sizin router'ınıza hangi interface'inin bağlı olduğunu,bu cihazların

hangi platforma ait olduğunu,holdtime değerini interface isimlerini görebilirsiniz. CDP ile toplanmış bilgileri daha ayrıntılı bir şekilde görmek istiyorsanız "**show cvp neighbor detail**" komutunu kullanmalısınız. Bu komutun çıktısında ise show cdp neighbors komutunun çıktısında bulunan bilgilere ek olarak cihazda kullanılan IOS versiyonu, IP adresleri gibi bilgileri bulabilirsiniz.

Eğer CDP protokolünün Router üzerinde çalışmasını istiyorsanız o zaman global konfigürasyon modunda iken "**no CDP run**" komutunu girmelisiniz. Ayrıca CDP'yi interface bazında da pasif yapabilirsiniz. Bunun için interface konfigürasyon modunda iken "**no CDP enable**" komutunu girmelisiniz.

Telnet Kullanarak Router'ı Yönetmek

Tüm Cisco Router ve switch'ler Telnet isteklerine cevap verecek şekilde, üzerlerinde Telnet server servisi çalışır vaziyette gelirler. Bunun yanında tüm Cisco Router'ları ve bazı switch'ler Telnet istemci programı ile birlikte gelir ve ağ yöneticilerinin Router'ları uzaktan yönetmesini sağlar. Privileged modda iken herhangi bir Router'a bağlanmak için "**telnet**" veya "**connect**" komutlarını kullanabilirsiniz. Bu komutlar parametre olarak bağlantının kurulacağı Router'ın IP adresini veya host ismini alır. Eğer parametre olarak host ismi kullanılmışsa Router'da DNS ayarlarının yapılması gerekir. Ya da Router'daki host tablosuna "**ip host**" komutunu kullanarak bu host'a ait kayıt girilmelidir. Örneğin aşağıdaki komutla adı RouterB ve IP adresi 10.3.10.1 olan router'ın kaydı host tablosuna girilmektedir.

RouterA(config)#ip host RouterB 10.3.10.1

Eğer router'ın isim çözümleme işini host tablosuyla değilde DNS sunucu ile halletmek istiyorsanız o zaman Router'a DNS sunucunun adresini "**ip name-server**" komutunu kullanarak belirtmelisiniz.

RouterA(config)#ip name-server 10.3.9.2

Router'ın komut satırında herhangi bir şeyi örneğin bir komutu yanlış veya eksik yazarsanız router bunun bir isim olduğunu farzedip DNS sunucuyu arayacak ve bu ismi çözmeye çalışacaktır. Bu işlemde bir hayli zaman alacaktır. Böyle bir durumda beklememek için **Ctrl+Shift+6** tuş kombinasyonuna bastıktan sonra **X** tuşuna basıp bu işlemi sonlandırabilirsiniz. Bunun haricinde bu tuş kombinasyonu uzak sistemlere yapılan telnet bağlantısını askıya alıp kendi router'ınıza geri dönmek içinde kullanılır.

Bir telnet otrumunu kapatmak için "**disconnect**", "**exit**", "**quit**" veya "**logout**" komutlarını kullanabilirsiniz. Eğer birden fazla Router'a Telnet ile bağlanmışsanız bu bağlantıları "**show session**" komutunu kullanarak görebilirsiniz.

Yönlendirme Temelleri

Router'ların temel işlevi yönlendirme yapmaktır. Peki kendilerine ulaşan bu paketleri hangi interface'lerinden çıkaracaklarını nasıl biliyorlar? Bunun için statik ,dinamik veya default yönlendirmeyi kullanırlar. Statik yönlendirmeler sistem yöneticisi tarafından elle girilir ve hedef ağ ile bu paketi hedefine taşıyacak bir sonraki router'ın adresi bilinmelidir. Statik yönlendirme tanımlamak için router'da global konfigürasyon modunda iken "**ip route**" komutunu kullanmalıyız. Aşağıda bu komut parametreleriyle birlikte açıklanmıştır.

Router(config)#ip route [hedef adres][subnet mask][Bir sonraki ağda bulunan Router'ın IP adresi veya yerel interface][distance]permanent

Yukarıdaki komutta "distance" parametresi seçimlik olup yönlendirmede kullanılan yönetimsel mesafeyi ifade eder ve 1 ile 255 arasında bir değer alabilir. Permanent ifadesi ise girilen kayıdın yönlendirme tablosunda, ilişkili olduğu interface pasif olduğu zamanda bile kalmasını sağlar. Aşağıdaki örnekte 10.3.11.0 network'üne gelen paketlerin router'ın s0 interface'inden çıkacağını söylüyoruz.

RouterA(config)#ip route 10.3.11.0 255.255.255.0 s0

Statik yönlendirme küçük network'ler için ideal bir çözüm olabilir fakat büyükçe bir ağı yönetecekseniz statik yönlendirmede hata yapma olasılığınız çok olacaktır.

Ayrıca router'lar üzerinde statik olarak tanımlanan default(varsayılan) yönlendirmeler ise hedef adresi bilinmeyen paketlerin hangi interface'den çıkarılacağını belirler. Default yönlendirmeyi aşağıdaki örnekte inceleyelim;

RouterA(config)#ip route 0.0.0.0 0.0.0.0 10.3.10.1

Burada router'a hedef adresi belli olmayan paketleri 10.3.10.1 adresine sahip interface'inden çıkarmasını söylüyoruz.

Router'da tanımlanmış statik kayıtları görmek için privileged modda iken "**show IP route**" komutunu kullanmalıyız. Karşımıza çıkan listedeki kayıtların başında bulunan **C** harfi fiziksel olarak birbirine bağlı ağlara olan yönlendirmeyi, **S** harfi yönlendirmenin statik olduğunu **S*** işareti ise kaydın default yönlendirme olduğunu gösterir.

Default yönlendirmenin router'larda çalışabilmesi için "**ip classless**" komutunun girilmesi gerekir. Ayrıca statik bir kaydı yönlendirme tablosunda silmek için "**no ip route**" komutunu parametreleriyle birlikte kullanmanız gerekir.

Dinamik yönlendirmede ise router üzerindeki yönlendirme tablosu administrator tarafından elle girilmez. Bu işi router üzerinde koşan yönlendirme algaritmaları yapar. Dinamik yönlendirmenin iki temel fonksiyonu vardır. Birincisi yönlendirme tablosunu oluşturmak, ikincisi ise oluşturulan bu yönlendirme tablolarının router'lar arasında paylaşılması yani router'ların yönlendirme tablolarındaki güncellemeleri diğer router'lara haber etmesi. Dinamik yönlendirme protokolleri hedef ağa ulaşan en iyi yolu belirlemek için metric değerlerini kullanırlar. Bir kısım protokol metric değerini hesaplarken hedef ağa ulaşma sırasında atladığı router sayısını metric değerine eşit tutar. Bu tür protokoller Uzaklık Vektor protokoller olarak adlandırılır(Distance Vector).Bu protokollere örnek olarak RIP ve IGRP verilebilir. Diğer bir grup dinamik yönlendirme protkolleri ise Bağlantı Durumu (Link State) protokolleri olarak adlandırılırlar ve metric değerini hesaplarken sadece geçilen router sayısına değil yoldaki trafik durumunu, bağlantının hızı gibi daha karışık değerleri de hesaba katar. Bu protokollere ise OSPF örnek olarak gösterilebilir. Ayrıca bu iki grubun haricide Hybrid protokoller de vardır ve bu protokoller Distance Vector protokolleri ile Link State protokollerinin birleşiminden oluşmuştur. Örneğin EIGRP bu sınıf bir protokoldür.

Bunun haricinde network'teki topoloji değişikliklerine adaptasyon otomatik olarak gerçekleşir. Fakat bu dinamik yönlendirme protokollerinin ağ topolojilerini öğrenip yönlendirme tablolarını ona göre oluşturmaları ve bu tablolardaki güncellemeleri diğer router'lara bildirmeleri başta yönlendirme çevrimleri (routing loops) gibi problemlere yol açabilir. Bu gibi problemlerin önüne geçmek için bazı teknikler kullanılır. Bunların başlıcaları;

- **Split Horizon**: Split horizon, router'ın ağ üzerinde herhangi bir değişiklik olduğunu anladığında bu değişikliği, öğrendiği interface haricindeki interface'lerden yayınlamasını sağlar. Böylece router'lar değişikliği sadece bir yönde yayınlarlar.

- **Maximum Hop Count**:Yönlendirilen paketlerin en fazla kaç hop atlayabileceği belirlenerek belli bir değeri aşan paketlerin yok edilmesini sağlar. Örneğin RIP için bu değer 15 dir ve bri paket için 16. Hop erişilemez olarak değerlendirilir ve paket yönlendirilmeden yok edilir.

- **Poison Reverse**: Router'ların yönlendirme tablosuna hop count değer 16 olarak yazılan bir yönlendirmedir ve hedef adresin erişilemez olduğunun router'lar arasında bilinmesini sağlar.

- **Hold-Down Timer**: Bu teknikte hold-down sayıcılar router'ın komşusundan aldığı ulaşılamaz bir ağa ait güncelleme ile başlar. Eğer aynı komşudan aynı ağa ait daha iyi bir metric değerine sahip bir güncelleme bilgisi alırsa hold-down kaldırılır. Fakat hold-down değeri dolmadan aynı komşudan daha düşük bir metric değerine sahip bir güncelleme gelirse bu kabul edilmez.

Administrative distance

Administrative distance, router'lar tarafından mevcut yönlendirmeler arasındaki önceliği belirler. Aşağıdaki tabloda yönlendirme kaynakları ve bu kaynakların sahip olduğu AD listelenmiştir. Düşük AD'ye sahip yönlendirmenin önceliği en fazladır.

Yönlendirme Kaynağı	Varsayılan AD Değeri
Direkt fiziksel bağlantı	0
Statik yönlendirme	1
RIP	120
IGRP	100
EIGRP yönlendirme özeti	5
Internal EIGRP	90
External EIGRP	170
OSPF	110
Bilinmeyen yönlendirme	255

RIP

RIP, uzaklık-vektör tabanlı bir yönlendirme protokolüdür. Bu protokolü çalıştıran router'lar kendi yönlendirme tablolarının tamamını 30 saniye aralıklarla bütün interface'lerinden komşu router'lara gönderirler. Ayrıca en iyi yolu seçerken sadece hop count değerini baz alır ve en fazla müsaade edilebilir hop count değeri 15'dir. Yani hop count değeri 16 ağlar erişilemez (unreachable) olarak değerlendirilir. RIP versiyon 1 sadece classful yönlendirmeyi kullanır. Yani bu versiyon da ağdaki tüm cihazlar aynı subnet mask'ı kullanmak zorundadır. RIP veriyon 2 ise prefix yönlendirme olarak adlandırılır ve yönlendirme güncellemeleri sırasında subnet mask değeride gönderilir. Bu yönlendirmenin diğer bir adıda classless yönlendirmedir.

RIP üç farklı sayaç (timer) kullanarak performansını ayarlar. Bu sayaçlar şunlardır;

- **Route Update timer**: Router'ın komşularına, yönlendirme tablosunun tümünü göndermesi için beklediği zaman aralığı. Tipik olarak 30 sn.'dir.

- Route invalid timer: Bir yönlendirmenin, yönlendirme tablosunda geçersiz olarak kabul edilmesi için geçmesi gereken zaman aralığı. 90 sn.'lik bu zaman aralığında yönlendirme tablosundaki bir yönlendirme kaydıyla alakalı bir güncelleme olmazsa o kayıt geçersiz olarak işaretlenir. Ardından komşu router'lara bu yönlendirmenin geçersiz olduğu bildirilir.

- Route flush timer: Bir yönlendirmenin geçersiz olması ve yönlendirme tablosundan kaldırılması için gereken zaman aralığı(240 sn.).

RIP'ı router üzerinde çalıştırmak için global konfigürasyon modunda "**router rip**" komutunu girmeliyiz.

RouterA(config)#router rip

Ardından router'a hangi network'e ait olduğunu bildiren "network" komutunu girmeliyiz.

RouterA(config-router)#network 172.16.0.0

RIP kullanılarak öğrenilen yönlendirme kayıtlarını "**show ip route**" komutunu kullanarak görebilirsiniz. Karşımıza çıkan yönlendirme tablosunda kayıtların başında R harfi bulunanlar RIP tarafında yönlendirme tablosuna girilmiş kayıtlardır. Ayrıca RIP çalıştıran bir router'ın tüm interface'lerinden RIP anonslarını yayması gerekmeyebilir. Örneğin router'ın ethetnet interface'inden RIP anonslarının yayılması herhangi bir işimize yaramaz. Bu yüzden bu interface'i RIP için pasif bir interface olarak tanımlamalıyız. Bunu gerçekleştirmek için aşağıdaki komutları kullanmalıyız.

RouterA(config)#router rip

RouterA(config-router)#network 172.16.0.0

RouterA(config-router)#passive-interface e0

IGRP

IGRP Cisco tarafından geliştirilmiş bir uzaklık-vektör algoritmasıdır. Bu yüzden network'te IGRP çalıştırmak için tüm router'ların Cisco olması gerekir. IGRP'de maksimum hop count değeri 255 dir ve RIP'te tanımlanabilecek maksimum hop count olan 15'den çok daha büyük bir değerdir. Bunun haricinde IGRP, RIP'ten farklı olarak en iyi yolu seçerken kullanılan metric değeri için varsayılan olarak, hattın gecikmesi (**delay**) ve band genişliğini (**bandwidth**) kullanır. Bunun haricinde güvenilirlik (**reliability**), yük (**load**) ve MTU(**Maximum Transmission Unit**) değerleri de metric hesabında kullanılabilir.

IGRP performans kontrolü için aşağıdaki sayaçları kullanır.

- Update timer: Hangi sıklıkla yönlendirme güncelleme mesajlarının gönderileceğini belirler. Varsayılan olarak 90 sn.'dir.

- Invalid timer: Router'ın herhangi bir yönlendirme kaydını geçersiz olarak işaretlemesi için ne kadar beklemesi gerektiğini belirtir. Varsayılan olarak update timer değerinin üç katıdır.

- Holddown timer: Holddown periyodunu belirtir ve varsayılan olarak update timer değeri artı 10 sn.'dir.

- **Flush timer**: Bir yönlendirmenin, yönlendirme tablosundan ne zaman süre sonra kaldırılacağını belirtir. Varsayılan değer ise update timer değerinin yedi katıdır.

IGRP'nin konfigürasyonu RIP'inkine çok benzese de önemli bir fark vardır. O da autonomous system (AS) numarasıdır. Aynı autonomous sistem de bulunan tüm router'lar aynı AS numarasına sahip olmalıdırlar. Router üzerinde IGRP'yi çalıştırmak için aşağıdaki komutu girmeniz gerekiyor.

RouterA(config)#router igrp 10

RouterA(config-router)#network 172.16.0.0

Yukarıdaki komutta router'a autonomous system (AS) numarasının 10 olduğunu ve bağlı bulunduğu ağın IP numarası bildiriliyor.

IGRP kullanılarak öğrenilen yönlendirme kayıtları "**show ip route**" komutunu yazdıktan sonra karşımıza çıkan yönlendirme tablosunda başında **I** harfi olan kayıtlardır

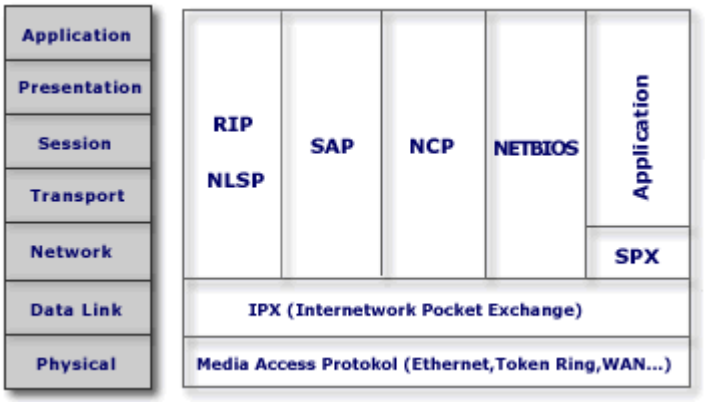
Konfigürasyonların Doğrulanması

Router üzerinde yapılan konfigürasyonu görüntülemek için kullanabileceğimiz bazı komutlar aşağıda listelenmiştir.

Komut	Açıklama
Show protocol	Her bir interface'in Network katmanı adresini ve interface'lerin aktif (up) mi yoksa pasif(down) mi olduğunu gösterir.
Show ip protocol	Router'da çalışan yönlendirme protokolleri hakkında özet bilgi verir.
Debup ip rip	Router tarafından gönderilen ve alınan yönlendirme güncellemelerinin konsol portuna da yollanmasını sağlar. Böylece yönlendirme işlemlerini izleyebilirsiniz. Eğer telnet ile router'a bağlıysanız bu güncellemeleri izleyebilmek için "**terminal monitor**" komutunu kullanmalısınız.
Debug ip igrp (events/transactions)	Eğer events parametresi ile kullanılırsa ağ üzerindeki IGRP yönlendirme bilgileri hakkında özet bilgi sunar. Transactions parametresi ile birlikte kullanılırsa komşu router'lara yapılan güncelleme istekleri ile broadcast mesajları hakkında bilgi verir.

IPX/SPX Protokol Ailesi

Novell tarafından geliştirilen bir protokol kümesidir. Novell'in çıkarmış olduğu ağ işletim sistemlerinde Netware 5 hariç varsayılan protokol kümesi olarak gelir. Novell Netware 5 ile birlikte varsayılan protokol ailesini TCP/IP olarak değiştirmiştir. IPX ile OSI modeli arasındaki ilişki aşağıdaki şekilde gösterilmiştir.



IPX : IPX bağlantısız (connectionless) bir protokol olup üst katman protokolleri ile haberleşirken socket'leri kullanır.

SPX (Sequenced Packet Exchange): Bağlatı temelli (connection-oriented) bir protokoldür. Bağlantı kurulan iki uç sistem arasında güvenilir bir iletişimi garanti eder.

RIP (Routing Information Protocol): Uzaklık-vektör temelli bir yönlendirme protokolu olan RIP,IPX üzerinde de çalışır.

SAP (Service Advertising Protocol): Servis duyurmak ve servis istemek için kullanılır. Sunucular istemcilere bunu kullanarak bir servisi teklif eder ve istemcilerde bunu kullanarak network servislerinin yerine bellirlerler.

NLSP (Netware Link Services Protocol): Novell tarafından geliştirilen bağlantı durumu (link-state) temelli bir yönlendirme protokolüdür.

NCP (Netware Core Protocol): İstemcilerin sunucu kaynaklarına erişmelerini sağlar. NCP'nin başlıca fonksiyonlarının başında file access, printing, security gelir.

Tüm Netware istemciler network üzerindeki kaynakları bulmak için sunucuya ihtiyaç duyarlar. Netware sunucularda ise SAP tabloları bulunur ve bu tabloda network'te bulunan ve haberdar oldukları kaynaklara ait bilgiler tutulur. Istemciler bu kaynaklara erişmek istediklerinde **GNS (GetNearestServer)** istediği olarak adlandırılan bir IPX broadcast yayınlarlar. Bu mesajı alan sunucular kendi SAP tablolarını kontrol ederek uygun bir cevapla GNS mesajını cevaplarlar. Bu GNS mesajında istemciye uygun sunucunun bilgisi gönderilir. Cisco router'larda da SAP tablosu oluşturulur ve istemcilerden gelen GNS isteklerine Cisco router'lar da cevap verebilir.

Netware sunucular 60 sn.'de bir SAP broadcast yayını yaparlar ve bu yayınlar sunucunun diğer sunuculardan öğrendiği tüm servisleri içerir.

IPX Adresleri

IPX adresleri 80 bit yani 10 byte uzunluğundadır. TCP/IP adreslerindeki hiyerarşik yapı IPX adreslerinde de vardır. Yani IPX adresleri de Network ve node adreslerine ayrılır. İlk 4 byte network adresini belirtir. Geriye kalan 6 byte ise node adresidir. Network adresi sistem yöneticisi tarafından atanır ve bir IPX network'ünde bu numara tek olmalıdır. Node adresi ise herbir host için otomatik olarak atanır ve bu adres host'un MAC adresidir. Örnek bir IPX adresi şöyledir;

00006603.0000.7269.32CC

Buradaki sekiz haneli (00006603) network adresini geriye kalan (0000.7269.32CC) ise nod adresidir.

IPX Network'te kullanılabilecek enkapsülasyon tipleri ise şunlardır.

- **Ethernet**
- **Token Ring**
- **FDDI**

Netware'de tanımlanabilecek Ethernet frame tipleri ise aşağıdaki tabloda listelenmiştir.

Netware Frame Tipi	Açıklama	Cisco Karşılığı
Ethernet_802.3	Netware 3.11'in varsayılan frame tipi	novel-ether
Ethernet_802.2	Netware 3.12'ye kadarki versiyonların varsayılan frame tipi	Sap
Ethernet_II	IPX ve IP desteği olan frame tipi	Arpa
Ethernet_SNAP	Apple Talk,IPX ve TCP/IP desteği olan bir frame tipi	snap

Aynı IPX network'teki host'ların birbiriyle iletişim kurabilmesi için aynı frame tiplerin kullanmaları gerekir.

:: Router'da IPX Konfigürasyonları ::

Router üzerinde IPX ayarlarını sırasıyla yapalım. Bunun için ilk önce router'ın interface'lerine hangi ipx network'ünde olduklarını bildirmemiz gerekiyor. Router'ın interface'lerine IPX network adresini atamak için "**ipx network**" komutunu interface konfigürasyon modundayken yazmamız gerekiyor. Örneğin aşağıda Router'ın seri 1 interface'i için 20 nolu ipx network'ünü tanımlayabiliriz.

RouterA(config)#int s1

RouterA(config-if)#ipx network 20

Bu ayarları yaptıktan sonra bu interface'in ait olduğu ipx network'ünde kullanılan frame tipini belirlemeliyiz. Herhangi bir ayarlama yapmazsak bu interface'in ait olduğu ipx network'ünde Ethernet_802_3 frame tipi kullanılır. Eğer bu frame tipini değiştirmek veya yeni bir frame tipi eklemek istiyorsak o zaman "**encapsulation**" komutunu interface konfigürasyon modundayken kullanmalıyız. Aşağıdaki örnekte Router'ın ethernet 0 interface'i 10 network'üne katılıyor ve frame tipi olarakta sap(Ethernet_802.2) kullanılacağı belirtiliyor.

RouterA(config)#int e0

RouterA(config-if)#ipx network 10 encapsulation sap

Eğer ekleyeceğiniz frame tipi ikinci bir frame tipi ise yukarıdaki komutun sonunda "**secondary**" ifadesini kullanmalısınız.

IPX yönlendirmenin çalışması için Router'ın global konfigürasyon modundayken "**ipx routing**" komutunu kullanmamız gerekiyor.

RouterA(config)#ipx routing

Bunun haricinde ,eğer router'lar arasında birden fazla IPX yolu tanımlanmışsa ,router'lar bunu default olarak ögrenemezler.Bu yüzden sadece bir yol kullanılır ve diğer yollar iptal edilir. Siz birden fazla yol tanımlı olan IPX networkünde bu yollar arasında yük dağılımı istiyorsanız o zaman "**ipx maximum-paths**" komutunu kullanarak paralel kullanılacak yol sayısını belirtebilirsiniz.

RouterA(config)#ipx maximum-paths 2

Router'da bulunan IPX yönlendirme tablosundaki kayıtları görmek için ise "**show ipx route**" komutu kullanılır. Bunun haricinde Router üzerinde IPX protokolünü izlemek için kullanılabilecek bazı komutlar aşağıdaki tabloda listelenmiştir.

Komut	Açıklama
Show ipx server	Cisco router üzerindeki SAP tablosunun içeriğini gösterir. Netware'deki "display servers" komutuna eşdeğerdir.
Show ipx traffic	Router tarafından alınan ve gönderilen IPX paketlerinin sayısı ve tipi hakkında özet bilgiler gösterir.
Show ipx interfaces	Router interface'lerindeki IPX durumunu, IPX parametrelerini gösterir.
Show protocols	Router interface'lerinin IPX adresini ve frame tipini gösterir.
Debug ipx	ipx konfigürasyon hatalarını belirlemek için kullanılır ve bu komut ile ipx ve sap güncellemelerini gösterir.

Ayrıca ping komutu kullanılarak karşı uçla olan bağlantı test edilebilir.

RouterA#ping ipx 10.0000.0B95.553c

Access list

Access list'ler sistem yöneticilerine, ağdaki trafik üzerinde geniş bir kontrol imkanı sunar. Ayrıca access list'ler router üzerinden geçen paketlere izin vermek veya reddetmek içinde kullanılır. Bunun haricinde telnet erişimleri de access list'ler kullanılarak düzenlenebilir. Oluşturulan access list'ler router'daki interface'lerin herhangi birisine giren veya çıkan trafiği kontrol edecek şekilde uygulanabilir. Eğer herhangi bir interface'e bir access list atanmışsa router bu interface'den gelen her paketi alıp inceleyecek ve access list'te belirtilen işlevi yerine getirecektir. Yani ya o paketi uygun yöne iletecek ya da paketi yönlendirmeden yok edecektir.

Router'ın interface'inden alınan bir paketin tanımlanan bir access list ile karşılaştırılma sırası şöyledir;

- Paket, access list'teki kayıtlar kayıt sırasına göre karşılaştırılır. Yani ilk önce access list'teki ilk satırla daha sonra 2,3... gibi.

- Paket, access list'de uyuşan satır bulununcaya kadar karşılaştırılır. Yani paket access list'teki 3.satırla uyuşuyorsa, bu paket access list'deki diğer satırlarla karşılaştırılmaz.

- Her access list'in sonunda "deny" satırı bulunur ve access list'deki satırlarla uyuşmayan paketlerin tamamının router tarafından imha edilmesini sağlar.

IP ve IPX ile birlikte kullanılan iki farklı türde access list vardır. Bunlar;

a) Standart access list: Bu tür access list'te IP paketlerinin sadece kaynak (source) adreslerine bakılarak filtreleme yapılır. Izin verme ya da yasaklama bütün protokol kümesi için geçerlidir. IPX paketlerinde ise kaynak(source) ve hedef(destination) adresleri kullanılarak filtreleme yapılır.

b) Extended access list: Bu tür access list'ler, IP paketlerinin hem kaynak hem de hedef adreslerini kontrol eder. Ayrıca Network katmanında tanımlanan protokol alanı ile Transport alanındaki port alanıda kontrol edilir. Böylece izin verilirken veya yasaklama yaparken protokol bazında bu işlemleri gerçekleştirmeye olanak sağlar. IPX paketlerinde ise kaynak adres, hedef adres Network katmanına ait protokol alanı ve Transport katmanındaki soket numarasıda kontrol edilir.

Access list'ler oluşturulduktan sonra sıra bu access list'leri Router'ın interface'lerine giriş veya çıkış listesi olarak atamaya geldi. Burada giriş(**inbound**) ve çıkış (**outbound**) kavramlarını açıklayalım. Inbound access list'lerin tanımlandığı interface'lerde paketler yönlendirme işlemine tabii tutulmadan access list'deki kayıtlarla karşılaştırılır. Outbound access list'lerin tanımlandığı interface'lerde ise router'a gelen paket ilk önce yönlendirme tablosuna göre yönlendirilir, ardından access list'deki satırlarla karşılaştırılır.

Bir interface için sadece bir tane inbound ve bir tane outbound access list tanımlanabilir. Aşağıdaki tabloda herbir protokole ait tanımlanabilecek access list'lerin numara aralıkları verilmiştir.

Access List Numarası	Açıklama
1-99 arası	IP standart access list
100-199 arası	IP extended access list
1000-1099 arası	IPX SAP access list
1100-1199 arası	Extended 48-bit MAC address access list
1200-1299 arası	IPX summary address access list
200-299 arası	Protocol type-code access list
300-399 arası	DECnet access list
400-499 arası	XNS standart access list
500-599 arası	XNS extended access list
600-699 arası	Appletalk access list
700-799 arası	48-bit MAC address access list
800-899 arası	IPX standart access list
900-999 arası	IPX extended acess list

Standart IP Access List

Standart IP access list'leri IP paketinin kaynak IP kısmına bakarak filtreleme gerçekleştirir. Aşağıdaki örnekte access-list numarası 15 olan ve 10.3.9.3 nolu hostdan gelecek tüm paketleri kabul etmeyecek bir access list tanımlanmıştır.

RouterA(config)#access-list 15 deny 10.3.9.3

Yukarıda oluşturulan access list ile sadece network'teki bir bilgisayardan gelecek paketlerin filtrelemesini sağlıyor. Peki biz birden fazla host'u etkileyecek bir access list'i nasıl oluşturacağız? Bunun için **wildcard**'ları kullanacağız. Wildcard'lar router'a kullanılan IP adres aralığının ne kadarının filtreleneceğini gösterir. Örneğin;

RouterA(config)#access-list 20 deny 10.3.10.1 0.0.0.0

komutundaki sıfır rakamları router'a IP adresi 10.3.10.1 olan host'a ait paketleri filtrelemesini söyler. Eğer biz 10.3.10.0 network'üne ait tüm host'lardan gelecek paketlerin filtrelenmesini istiyorsak o zaman aşağıdaki komutu kullanmalıyız.

RouterA(config)#access-list 20 deny 10.3.10.0 0.0.0.255

Eğer biz 10.0.0.0 network'üne ait tüm host'lardan gelecek paketlerin filtrelenmesini istiyorsak o zaman da aşağıdaki komutu kullanmalıyız.

RouterA(config)#access-list 20 deny 10.3.10.0 0.255.255.255

Oluşturduğumuz access list'i router'ın istediğimiz interface'ine inbound veya outbound olarak ilişkilendirmeye sıra geldi. Bunun için interface konfigürasyon moduna geçip "**ip access-group**" komutunu kullanıyoruz. Aşağıdaki örnekte 15 nolu bir standart IP access list'i oluşturulduktan sonra bu access list'e iki tane kayıt giriliyor. Ilk kayıt 10.3.10.0 network'ünden gelecek paketlerin router tarafından yönlendirilmemesini istiyor. Ardından access list'e eklenen ikinci kayıt ise tüm paketlere izin veriyor. Eğer bu son satırı girmezsek ilk satıra uymayan tüm oaketler router tarafından yok edilecektir(Zaten uyan pekatleri de yönlendirme yaptırmadığımız için router hiçbir yönlendirme işlemi yapmayacaktır). Burada bu iki kaydın access list'e yazılış sırasına dikkat edin. Bu iki kaydın yerleri değişirse uygulamaya çalıştığınız access list hiçbir işe yaramayacaktır. Bu kayıtlar girildikten sonra bu access list belirlediğimiz uygun bir arayüze outbound olarak ilişkilendirilmiştir.

RouterA(config)#access-list 15 deny 10.3.10.0 0.0.0.255

RouterA(config)#access-list 15 permit any

RouterA(config)#int e0

RouterA(config-if)#ip access-group 15 out

Extended IP Access List

Extended IP access list'ler, standart IP access list'lere oranla çok daha gelişmiş bir filtreleme imkanı sunarlar. Örneğin filtreleme yaparken paketlerde taşınan protokol bilgisini kullanabilirsiniz. Böylece bazı protokollere ait paketlerin router'ın belirlediğiniz interface'lerinden çıkmasını veya o interface'lere girmesini engelleyebilirsiniz. Örneğin router'ın e0 interface'ine bağlı server'ımıza (IP adresi 10.3.20.1) gelen telnet isteklerini kesmek isteyelim. Bunun için router üzerinde yapmamız gereken işlemler şöyledir;

RouterA(config)#access-list 121 deny tcp any host 10.3.20.1 eq 23

RouterA(config)#int e0

RouterA(config-if)#ip access-group 121 out

Burada 23 telnet'in kullandığı TCP port numarasıdır. Siz bu server'a gelen tüm tcp paketlerini engellemek isterseniz ise o zaman kullanacağımız komut;

RouterA(config)#access-list 121 deny tcp any host 10.3.20.1

şeklinde olacaktır.
Router üzerinde tanımlanmış access-list'leri görmek için "**show access-list**" komutunu kullanabilirsiniz. Eğer oluşturduğunuz access list hakkında daha geniş bilgi istiyorsanız oluşturduğunuz access list'in numarasını yukarıdaki komuta parametre olarak girmelisiniz. Örneğin;

RouterA(config)#show access-list 121

Access List Kullanarak Telnet Bağlantılarını Kontrol Etmek

Access list kullanarak telnet bağlantılarını kontrol etmek için ilk önce standart bir IP access list oluşturulur ve bu access list'te sadece istenilen host veya host grubuna izin verilir. Ardından bu access list router'ın vty portlarına "**access class**" komutu kullanılarak uygulanır. Aşağıdaki örnekte router'a sadece 10.3.9.2 adresinden telnet bağlantısı yapılabilmesi izin veriliyor.

RouterA(config)#access-list 70 permit host 10.3.9.2

RouterA(config)#line vty 0 4

RouterA(config-line)#access-class 70 in

WAN (Wide Area Network) Protokolleri

WAN bağlantı tipleri dedicated, circuit-switchet ve packet-switched olmak üzere üç çeşittir. Şimdi sırasıyla bunları inceleyelim.

- **Dedicated (Leased Line)**: İki uç sistem arasında atanmış bir bağlantı sağlar. Senkron seri hatlar kullanılır ve haberleşme hızı 45 Mbps'e kadar çıkabilir. Pahalı bir bağlantıdır. Desteklediği enkapsulasyon türleri ise PPP, SLIP ve HDLC'dir.

- **Circuit Switching (Devre Anahtarlama)**: İki uç sistem arasında iletişime başlamadan önce sanal bir devre oluşturma esasına dayanır. Paketler bu devre üzerinden gönderilip alınır. Standart telefon hatları veya ISDN üzerinde asenkron seri iletişim sağlar. Desteklediği enkapsülasyon'lar PPP, SLIP ve HDLC'dir.

- **Packet-switching (Paket Anahtarlama)**: Bu yöntemde band genişliği diğer şirketlerle paylaşılarak daha ucuz iletişim sağlanır. Desteklediği enkapsülasyon'lar X.25, ATM ve Frame Relay'dır.

Bunun yanında bilmemiz gereken bazı WAN terimleri ve açıklamaları aşağıdaki tabloda verilmiştir.

Terim	Açıklama
Costumer premises equipment (CPE)	Müşterinin sahip olduğu ve kendi binasında bulundurduğu Cihazlar için kullanılır.
Demarcation(demarc)	Servis sağlayıcı firmanın sorumluluğunun bittiği nokta.Bu nokta müşterinin CPE 'sine bağlantının sağlandığı noktadır.
Local loop	Demarc'ların ,en yakın anahtarlama ofisine bağlantılarını sağlar.
Central Office (CO)	Müşterilerin ,servis sağlayıcısının networkune katıldığı nokta.POP(Point of Presence) olarak da bilinir.
Toll network	Servis sağlayıcının networkündeki trunk hatları.

PPP (Point-to-Point Protocol)

PPP bir data-link protokolüdür ve dial-up gibi asenkron seri veya ISDN gibi senkron seri hatlarda kullanılır. LCP (Link Control Protocol)'yi kullanarak data-link bağlantısını kurar ve yönetir. PPP dört ana bileşenden oluşur. Bunlar;

- **EIA/TIA-232-C**: Seri haberleşmede kullanılan uluslararası bir fiziksel katman standardı.

- **HDLC**: Seri bağlantılar üzerinde kullanılan bir enkapsülasyon yöntemi.

- **LCP**: Point-to-point bağlantıyı kurmak, yönetmek ve sonlandırmak için kullanılan protokol.

- **NCP**: PPP'nin birden fazla Network katmanı protokolüne destek vermesini sağlayan protokol.

Link Control Protokolünün Konfigürasyon Seçenekleri

Aşağıda LCP tarafından konfigürasyon seçenekleri anlatılmıştır. Bu seçenekler router üzerinde PPP tanımlandıktan sonra interface konfigürasyon modunda iken değiştirilebilir.

- **Authentication**: Bu özellik bağlantının diğer ucundaki arayan kullanıcının kimlik doğrulaması yapmasını zorunlu koşar. İki farklı yöntem kullanılabilir; **PAP (Password Authentication Protocol)** ve **CHAP (Challenge Authentication Protocol)**.

- **Compression**: Bu özellik verinin sıkıştırılmasını ve açılmasını sağlar. Böylece PPP bağlantısının throughput'u artmış olur. Cisco router'lar **Stacker** ve **Predictor** sıkıştırma metodlarını kullanırlar.

- **Multilink**: Bundling olarak da adlandırılan bu özellik sayesinde trafik birden fazla bağlantı üzerinden yük dağılımı esasına göre tanınır. IOS version 11.1'den itibaren tanımlanmıştır.

- **Error detection**: PPP, Quality and Magic Number seçeneğini kullanark güvenilir ve döngüsüz bir bağlantı sağlar.

Şimdi bu özellikleri biraz daha açalım. Autentication ile başlayalım. İki farklı metod kullanıldığını söylemiştik. Sırasıyla bunları inceleyelim.

- **Password Authentication Protocol (PAP)**: Bu metod'da kullanıcı adı ve şifre clear text olarak iletilir.

- **Challenge Authentication Protocol (CHAP)**: Bu metod'da, kimlik doğrulaması için karşı cihaza gönderilen kullanıcı adı ve şifre bilgileri şifrelenmiş bir şekilde iletilir.

Multilink özelliğinde ise iki farklı fiziksel bağlantının tek bir bağlantı şeklinde kullanıılması sağlanır. Örneğin elimizde iki ayrı 64K kanalına sahip bir BRI varsa biz router'ın bu iki ayrı kanalı, toplam band genişliği 128 olan tek bir kanal gibi kullanmasını sağlayabiliriz. Bu bağlantının kullanış şekli ise şöyledir. Diyelim ki kullanıcıların kullandığı toplam band genişliği 64K'nın altında. O zaman ikinci link aktif edilmeden sadece birinci bağlantı kullanılır. Ne zaman ki kullanılan band genişliği 64K'nın üstüne çıkarsa o zaman ikinci bağlantıda devreye girerek yük dağılımı sağlayacaktır.

Router'ın seri interface'lerinde PPP tanımı yapmak için "**encapsulation PPP**" komutu kullanılır.

RouterA(config)#int s0

RouterA(config-if)#encapsulation PPP

Bağlantının sağlandığı her iki uçtaki interface'lerin ikisinde de PPP aktif yapılmalıdır. Ayrıca PPP'nın authentication özelliğini kullanmak için yapılması gerekenler ise şöyledir. İlk önce router'lara "hostname" komutu kullanılarak bir isim verilmelidir. Ardından karşı tarafın bağlantı kuracağı sırada kullanacağı kullanıcı adı ve şifresinde global konfigürasyon modundayken tanımlanmalıdır. Aşağıdaki örnekte router'ın adı RouterA olarak veriliyor ve ardında PPP de kullanılacak kullanıcı adı ve şifre tanımlanıyor.

Router(config)#hostname RouterA

RouterA(config)#username cisco password 123456

Bunun haricinde birde PPP bağlantısında kullanılacak kimlik doğrulama metodu da belirlenmelidir. Bunun için "**PPP authentication**" komutunu interface konfigürasyon modunda iken kullanmalıyız. Aşağıdaki örnekte chap metodu seçiliyor.

RouterA(config-if)#ppp authentication chap

ISDN (Integrated Services Digital Network)

ISDN varolan telefon ağı üzerinden sayısal hizmet vermek için geliştirilen bir teknolojidir. ISDN üzerinden ses, görüntü ve veri eş zamanlı olarak iletilebilir. ISDN'de genellikle veri enkapsülasyonu, bağlantı kontrolü ve kimlik doğrulaması için PPP kullanılır.

ISDN ağına bağlanacak cihazlar terminal equipment (TE) ve network termination (NT) equipment olarak sınıflandırırlar. Şimdi sırasıyla bunları inceleyelim;

TE1: Bu sınıfa dahil olan cihazlar direkt olarak ISDN ağına bağlanabilirler.

TE2: Bu sınıfa dahil olan cihazlar ISDN standartlarını anlamazlar ve ISDN ağına bağlanabilmeleri için bir terminal adaptör (TA)'e ihtiyaç duyarlar.

NT1: ISDN fiziksel katman özelliklerini tanımlar ve kullanıcıların cihazlarını ISDN ağına bağlar.

NT2: Genellikle servis sağlayıcının cihazlarıdır. (Örneğin switch veta PBX)

TA: Terminal adaptör TE2 kablolamasını TE1 kablolamasına dönüştürür.

ISDN ağında tanımlanmış referans noktaları ise şunlardır;

- **R referans noktası**: ISDN olmayan cihaz ile TA arasındaki referans noktasını tanımlar.

- **S referans noktası**: Müşterinin router'ı ile NT2 arasındaki referans noktasını tanımlar.

- **T referans noktası**: NT1 ve NT2 cihazları arasındaki referans noktasını tanımlar. S ve T referans noktaları elektriksel olarak aynıdırlar ve bazen S/T referans noktası olarakda kullanılabilirler.

- **U referans noktası**: Taşıyıcı ağdaki (sadece kuzey Amerika'da kullanılır) NT1 cihazı ile line-termination equipment arasındaki referans noktasını tanımlar.

BRI (Basic Rate Interface)

ISDN BRI servisi ,2 tane 64 Kbps 'lik B kanalı ve bir tanede 16 Kbps 'lik D kanalı sunar. B kanalları veri taşımak için kullanılır. D kanalları ise kontrol ve işaretleşme bilgilerini taşır. BRI 'ı konfigüre ederken herbir B kanalı için bir tane **SPID (Service Profile Identifiers)** 'e ihtiyaç vardır. SPID 'leri kulandığımız telefon numaralarına benzetebiliriz.

ISDN'in bize sağlamış olduğu faydaları sıralarsak;

- Aynı hat üzerinden hem ses,hem video hem de veri iletimi eşzamanlı olarak yapılabilir.

- Bağlantı kurulum hızı modemlerden daha hızlıdır.

- Modem bağlantılarının sağlamış olduğu veri transfer hızından daha hızlı bir bağlantı sağlar.

Bunun haricinde Amerikada 23B+1D kanallarından ,Avrupada ise 30B+1D kanallarından oluşan PRI (Primary Rate Interface) hizmeti de mevcuttur. Burada kullanılan D kanallarının band genişliği 64 Kbps'dir.

Cisco router'ları ISDN network'üne bağlamak için ya router'ı NT1 uyumlu olarak üretilmesi veya bir ISDN modeme ihtiyaç vardır. Router'da bulunan her bir ISDN BRI interface'i için servis sağlayıcı tarafından bize verilen SPID numaralarını "**isdn spid1**" ve "**isdn spid2**" komutlarını kullanarak girmeliyiz. Ayrıca servis sağlayıcının kullandığı switch türünü de bilmemiz gerekiyor. Elimizdeki router'in ne tür switch'lere destek verdiğini görmek için "**isdn switch-type ?**" komutunu kullanabiliriz.

Aşağıda router üzerinde yapılan örnek bir ISDN BRI konfigürasyonu gösterilmiştir.

RouterA(config)#isdn switch-type basic-ne1

RouterA(config)#int bri0

RouterA(config-if)#encap ppp

RouterA(config-if)#isdn spid1 075866043112 4440321

RouterA(config-if)#isdn spid1 075866043112 4440322

Dial-on-Demand Routing(DDR)

DDR iki veya daha fazla Cisco router'ın gerektiğinde , bir ISDN dial-up bağlantı yapmasını sağlar.Genellikle PSTN (Public Switched Telephone Network) veya ISDN kullanılarak gerçekleştirilen periyodik network bağlantılarında kullanılır. Böylece siz WAN bağlantınız için dakika bazında veya alınan paket bazında bir ücret ödüyorsanız bu özellik sizin için çok kullanışlı olacaktır. Çünkü gerek duyulduğu zaman bağlantı kurulacak ve böylece ödemiş olduğunuz ücret de o oranda düşecektir.

Router aldığı paketi inceleyip, administrator tarafından tanımlanmış access-list'lerde bu pakete bir ait kayıt bulduğu anda DDR çalışmaya başlar. DDR'ı konfigüre etmek için gereken işlemleri ise şöyle sıralayabiliriz;

- Static bir yönlendirme "**ip route**" komutu kullanılarak tanımlanıp ,hengi network'e hangi interface kullnılarak ulaşılacağı belirlenir.

- Ardından "**dialer-list**" komutu kullanılarak oluşturulan liste ile hangi tür paketlerin bu bağlantıyı aktif yapacağı belirlenir.

- Daha sonra uzaktaki network bağlantısında kullanılacak arama bilgileri konfigüre edilir.

Aşağıda bir routerda DDR `ın nasıl konfigüre edildiği gösterilmiştir.

RouterA#conf t

RouterA(config)#dialer-list 1 protocol ip permit

RouterA(config)#int bri0

RouterA(config-if)#ip address 192.168.2.1 255.255.255.0

RouterA(config-if)#no shut

RouterA(config-if)#encapsulation ppp

RouterA(config-if)#dialer-group 1

RouterA(config-if)#dialer-string 4320544

Burada kullanılan "**dialer-string**" komutu bağlantı kurulumu için aranacak numarayı belirtir. Bu komutdaki numara yerine "**dialer map**" komutunu kullanarak oluşturduğuz kayıtta kullanılan ve karşı taraf için tanımladığınız ismi de kullanabilirsiniz. Örneğin;

RouterA(config-if)#dialer map ip 192.168.2.2 name RouterB 4320544

Bunun haricinde Router üzerince ISDN BRI konfigürasyonunda kullanılan iki komut daha vardır. Bunlar "**dialer load-threshold** " ve "**dialer idle-timeout**". Bu komutlardan "dialer load-threshold" komutu BRI interface'inin ikinci B kanalını ne zaman aktif hale getireceğini söyler. Bu komut paremetre olarak 1 ile 255 arasında bir değer alır ve 255 değeri kullanıldığında BRI interface'i ikinci B kanalını birinci B kanalı %100 kullanıldığında aktif hale getirir. Bu komut ikinci parametre olarak da trafik hesabında ,gelen trafiğin mi(**in**) ,giden trafiğin mi(**out**) yoksa her ikisinin birden mi (**either**) hesaplanacağını router'a bildirir. İkinci komut olan "dialer idle-timeout" komutu ise en son iletilen paketin ardından ne kadar süre sonra bağlantının koparılacağını belirtir. Varsayılan olarak 120 saniye sonra bağlantı koparılır. Örnek bir konfigürasyon aşağıda gösterilmiştir.

RouterA(config-if)#dialer load-threshold 125 either

RouterA(config-if)#dialer idle-timeout 180

Sifre Unutulursa:)))

Telefon çalar: Ring! Ring!
Madam Rommon: İyi günler ben Madam Rommon, nasıl yardımcı olabilirim?
Kullanıcı Eeee. Sorun router'ım... Bir derdi var...
Madam Rommon: Aaa, evet... Fakat önce kredi kartı numaranıza ihtiyacım var.
Kullanıcı: Tabii ki. Numarası 5XXX-XXXX-XXXX-XXXX, son kullanma tarihi 08/02. Lütfen Madam Rommon, bana yardım edebilir misiniz?
Madam Rommon: Merak etme evladım, Madam Rommon herşeyi görür ve bilir. Router'ınız kötü niyetli bir ruhun etkisi altında. Router'ınıza şeytan girmiş!
Kullanıcı: Evet! Evet! Patronuma da bunu söyledim ama bana inanmadı! Bugüne kadar herşey normaldi, bu 2620'nin konfigürasyonunu değiştirmek istedim fakat router birden şifremi kabul etmemeye başladı...

Madam Rommon: Router'ınız bir sır barındırıyor... Kötü bir sır...
Kullanıcı: Nasıl bildiniz??? Evet! "Bad Secrets" yazıyor! Aman Tanrım! Bunu bildiğinize inanamıyorum! Patronum şifre kurtarma işlemi yapmam gerektiğini söyledi ama ekranda "Bad Secrets"ı görünce bundan daha ciddi olduğunu anlamıştım. Lütfen Madam Rommon, ne yapmam gerektiğini söyleyin!
Madam Rommon: Güzel evladım, bir şeytan çıkarma ayini yapmamız gerekiyor. Router'a bazı kutsal komutlar vereceğiz. Bunlar çok özel komutlar. O kadar özel ki, kredi kartınızdan 750$ daha çekmem gerekecek. Bunu kabul ediyor musun?
Kullanıcı: Evet tabii! Patronumun Mastercard'ı elimde. Router'ı düzeltmem için ne gerekiyorsa yaparım.
Madam Rommon: Harika! Fazladan bir 1000$ karşılığında, router'ınız için bir dua okuyabilirim. Bunu kabul ediyor musunuz?
Kullanıcı: Evet, evet! Lütfen, herşeyi ödeyebilirim! Yeter ki yardım edin!
Madam Rommon: Kaygılanmayın, konsol kablonuzu router'a takın ve cihazı kapatıp açın. Router yeniden açıldığında, şeytan startup-config'i yüklemeye çalışacak. Buna engel olmaslısınız. Anlıyor musunuz?
Kullanıcı: Evet. Şeytanın config'i yüklemesiniönleyeceğim. Peki nasıl?
Madam Rommon: Router boot ederken 60 saniye içinde BREAK'e basmalısınız. Yanında router adı olmayan bir ">" işareti görürseniz anlayın ki şeytanı durdurdunuz.
Kullanıcı: Evet! ">" işaretini gördüm! Şimdi ne yapıyorum?
Madam Rommon: Pekala, işte kutsal komut, yazın: confreg 0x2142
Kullanıcı: Tamam, sırada ne var?
Madam Rommon: Şimdi router'ın yeniden boot etmesini sağlamalısınız. Bunun için kutsal harf olan "i"yi yazın
Kullanıcı: Hey! Router boot etti ve şimdi bana başlangıç konfigürasyon diyaloğunu girmek isteyip istemediğimi soruyor. Ne yapayım?
Madam Rommon: Bu şeytanın bir kandırmacası. Ondan kurtulmaya çalıştığınızı anladı. "Hayır" deyin. "Enable" yazıp şeytanı öldürdükten sonra kontrolü tekrar ele almak için "copy start run" yazın.
Kullanıcı: Anlıyorum. Router IOS'u yükledi fakat config'i yüklemesini kutsal komutlar sayesinde önledik. Sonra da config'i hafızaya yükleyerek şeytanı defettik. Şimdi ne yapıyoruz?
Madam Rommon: Son bir kez daha 500$'lık bir büyü yapacağız.
Kullanıcı: Amma da masraf ettik, neyse, haydi bakalım...
Madam Rommon: Yavrucuğum şeytan kovmak kolay mı. Şimdi "copy run start" yaz. Daha sonra "reload" yaz ki şeytan bir daha router'ına giremesin. Artık rahatsın evladım.
Kullanıcı: Madam Rommon hayatımı kurtardınız!
Madam Rommon: Ne zaman istersen evladım, lafı olmaz....