T.C.

FIRAT ÜNIVERSITESI

MÜHENDISLIK FAKÜLTESI

ELEKTRIK – ELEKTRONIK MÜHENDISLIGI BÖLÜMÜ

C I S C O

A G A K A D E M I S I

SÖMESTR – 2

BITIRME ÖDEVI

YÖNETEN

Yrd.Doç.Dr. Hasan H. BALIK

HAZIRLAYAN

Hasim DOGAN

ELAZIG – 2005

TESEKKÜR

Bu çalisma Elazig Firat Üniversitesi , Mühendislik Fakültesi , Elektrik – Elektronik Mühendisliginde bitime ödevi olarak hazrilanmistir.

Beni bu bitirme ödevini hazirlamaya yönlendiren ve çalismalarimizin her asamasinda yardimlarini bizden esirgemeyen degerli hocam Yrd.Doç.Dr. Hasan H. BALIK' a , ögretim hayatim boyunca maddi ve manevi desteklerini esirgemeyen , tüm kosullarda arkamda bulunan babama , anneme , nisanlima , desteklerini ve yardimlarini esirgemeyen arkadaslarim Saib ATAY , M.Ali AKDENIZ ve Burak Kartal'a sonsuz tesekkürlerimi borç bilirim. Ayrica bu ödevin hazirlanmasinda çeviri islerinde bana bikmadan eleinden gelen tüm çabayi sarfeden ve manevi destek veren degerli kuzenim Av.Baki SAKALLI'ya en içten dileklerimle tesekkür ederim.

Hasim DOGAN

ÖNSÖZ

Insanoglu asirlardir birbirleri ile haberlesmektedir. Birbirleri ile olan iletisimde haberlesmek için bir çok yöntem gelistirmislerdir. Gelisen teknoloji haberlesmenin daha kaliteli daha hizli ve daha güvenilir olmasini saglamaktadir. Artik insanlarin haberlesmek için kaybedecek zamanlari yoktur. Günümüz sartlari ve teknolojinin gelismesi insan hayatina bilgisari sokmustur. Bilisim çaginda insanlarin haberlesmesi için iletisim aglari kurulmustur. Bu aglar ile tv yayini , telekominikasyon , veri iletisimi gibi ihtiyaçlar karsilanmaktadir. Ister birey ister kamu yararina olan bu hizmet beraberinde standartlari getirmistir. Hayatimizda sagliktan egimitime kadar bir standart varsa ag haberlesmesininde bir standarti vardir. Ag haberlesmesinde buna CISCO nun öncü oldugunu görmekteyiz.

Cisco bilgisayarlarin ve daha birçok haberlesme ihtiyaci duyan cihazlarin birbirleri ile olan iletisimi bir standarta oturtmak isteyen firmalardan birisidir. Kendi gelistirdigi cihazlar , iletisim prtotoklleri sayisiz faydalar saglamistir. Cshazlar arasinda kullanilan ag haberlesmesinin belirli kurallari standartlari vardir. Bu çalismada Cisco nun dört bölümde anlattigi ag haberlesmesinin ikinci bölümünden bahsedilmektedir. Bu bölümde aglarin temelini olusturan aglarin can damarlari sayilan routerlar hakkinda bilgi verecegim. Bir router dedigimiz cihazlarin elektronik iç yapisi , donanimi gibi özelliklerden bahsedecegim. Zaman zaman konularda yeri geldikçe resimli örneklerle uygulamalar yaparak akillarda ag iletisiminin daha kalici bir sekilde yer etmesini saglayacagiz.

IÇINDEKILER

BÖLÜM 8:

BÖLÜM 9:

BÖLÜM 10:

BÖLÜM 11:

BÖLÜM - 1

Giris

WAN büyük bir cografig alani olan mesafelerin oldugu bir veri iletisim agidir. WAN ni, LAN lardan ayiran önemli birkaç karakteristik özelligi vardir. Bu modülde ilk olarak WAN teknolojileri ve protokolleri görülecek. WAN larin ve LAN larin nasil farkli oldugunu açiklayarak hangi yollarin benzer oldugu gösterilecektir.

Bu bölümü tamamlayan kimseler asagidakileri yapabilmelidirler:

- WAN standartlari için organizasyon kimliklerini tanimak
- WAN ve LAN adreslerinin ve tiplerinin arasindaki farklari ve kullanimlari açiklanacak
- WAN lardaki routerlarin rolü tanimlanacak
- Routerlarin iç parçalarini taninacak ve onlarin fonksiyonu tanimlanacak
- Routerin fiziksek karakteristigi tanimlanacak
- Routerda genel portlar tanimlanacak
- Ethernet , seri WAN ve konsol portlar uygun biçimde baglanacak

1.1 WAN'lar

1.1.1 WAN' lara Giris

WAN lar , genis cografyalardaki illerdeki yada ülkerde ki aglarin data haberlesmesini saglar. WAN lar ,ortak tasiyici tarafindan çogunlukla iletim yetenegini sartini kullanirlar. Örnegin bir cihazdan diger cihaza LAN aginda 100m mesafe uygun görülürken ülkeler arasi WAN teknolojisinde 100km mesafe sinir vardir. Sekil-1

Distance Between Devices	Location of Hosts	Name
10m	Room	Local-area Network Classroom
100m	Building	Local-area Network School
1000m = 1km	Campus	Local-area Network University
10,000m = 10km	City	Metropolitan-area Network
100,000m = 100km	Country	Wide-area Network Cisco System, Inc.
1,000,000m = 1,000km	Continent	Wide-area Network Africa
10,000,000m = 10,000km	Planet	Wide-area Network Internet
100,000,000m = 100,000km	Earth-Moon Systems	Wide-area Network Earth and Artificial Satellites

Asagidaki maddeler WAN larin öneli özelliklerindendir:

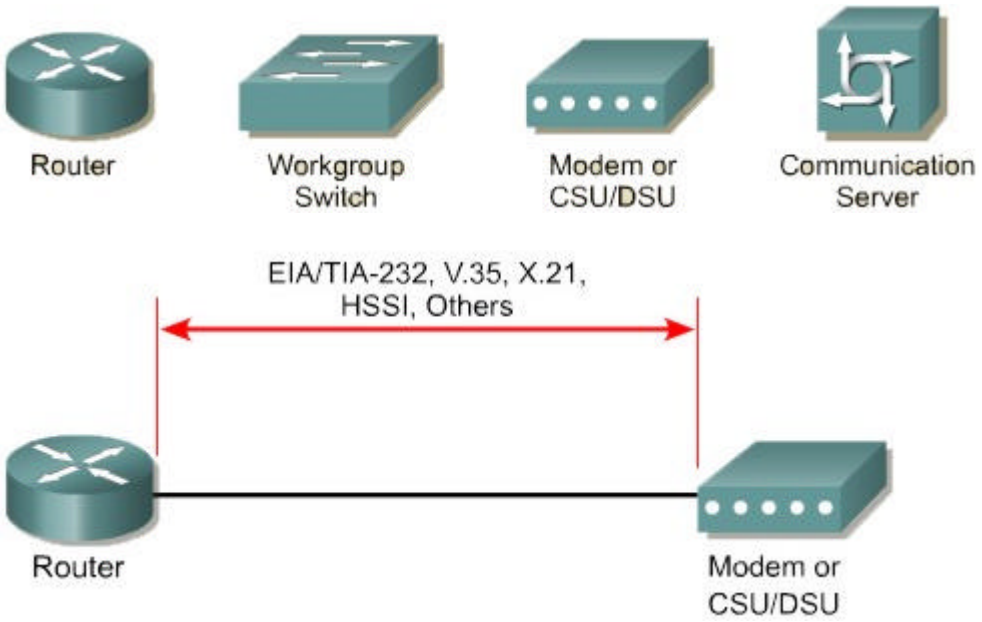
- WAN lar genis cografi alanlar tarafindan bölünmüs olan araçlari baglarlar.
- WAN lar , Regional Bell Operating Companies (RBOCs), Sprint, MCI, VPM Internet Services, Inc., ve Altantes.net gibi tasiyicilarin servislerini kullanirlar
- WAN lar cografik alanlarda çesitli tiplerde bantgenisligi erisiminde seri baglantilari kullanirlar

WAN lar bazi yollarda LAN lardan farlidirlar. Örnegin ; Farkli LAN lar ismerkezi baglantilari , çevresel terminaller, ve tek bina içerisinde yada diger küçük cografik alanlardaki diger araçlar, WAN , büyük cografik alanlari karsidan karsiya data baglantisi ile baglar. Sirketler wan lari kullanarak sirket sitelerine baglanarak uzak ofisler arasinda bilgi degistirebilirler.

WANlar OSI referans modeline göre fiziksel katmanda ve data iletim katmaninda çalisirlar. Çogunluklar genis cografyalar arasinda ayrilmis LAN lari birbirlerine baglarlar. Diger routerlar , switchler ve bagli oldugu LAN lari arasinda data paketlerinin ve çerçevelerinin degistirilmesini saglarlar.

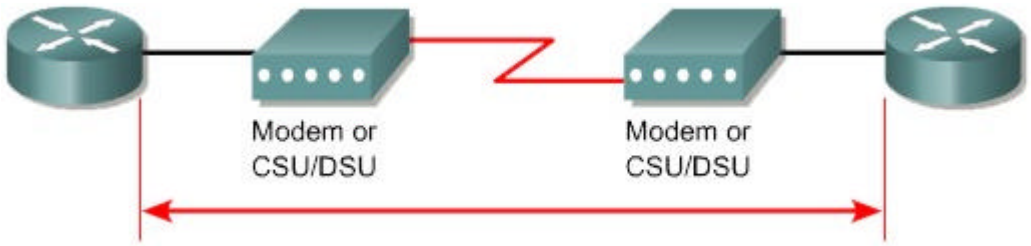
WAN larda asagidaki sekillerde gösterilen araçlar kullanilirlar:

- Routerlar yerlestirildigi internet agina ve WAN arayüz portlarina birçok servis sunarlar
- Switchler WAN larda ses , veri ve video iletisimi için baglanti saglarlar
- Modemler ses ayirici kanal servis , dijital servis ünitelerine (CSU/DSU) , T1/E1 tipi hat servislerine ve ISDN servislerinin arayüzlerine yerlestirilirler
- Iletisim sunuculari bir aradaki dial-in ve dial-out baglantilari kullanirlar.



Tek data iletimde WAN diger sistemlere tasinirken data iletim protokollerinin çerçevelerini tanimlar. Frame-Relay gibi çoklu erisim swicth servislerine , birebir baglantilarina , çoklu noktalara dizayn edilmis protokollerini yerlestirirler. Wan standartlari tanimlanir ve idare edilip takip eden aracilara yerlestirirler:

- Birlesmis Uluslararasi Telekomünikasyon-Telekomünikasyon Standartlari Bölgesi (ITU-T), önceden uluslararasi telgraf ve telefon için tavsiyede bulunabilen komite (CCITT)
- Standardizasyon için uluslararasi organizasyon (ISO).
- Internet mühendislik özel kuvveti (IETF).
- Elektronik sanayiler ortakligi (EIA).



1.1 WAN'lar

1.1.2 WAN' larda Yönlendirmeye Giris

Bir router, bilgisayarin özel bir tipidir. Bir masa üstü PC standartlarinda olarak aynen temel parçalari vardir. Bir islemci, hafiza, bir sistem veriyolu, ve çesitli giris/ çikti arayüzleri vardir. Yinede routerlar , bilgisayarlarda tipik olarak olmayan bazi özel özellikleri ile dizayn edilir. Örnegin router baglantilari ve izin verilen iki ag ile olan baglantilar ve bagli sebekelerden yolculuk yapmasi için veri için en iyi yolu kararlastirir.

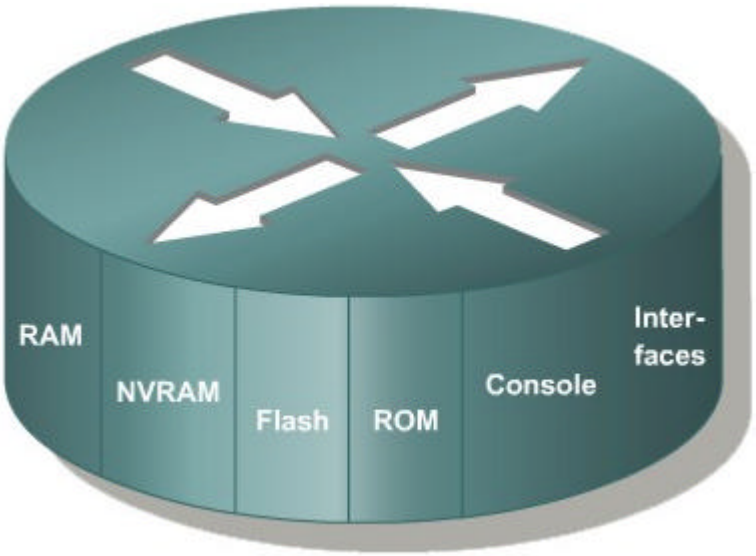
Sadece software uygulamalari çalistirmak için sistemleri çalistirirken bilgisayarlara ihtiyaç oldugu gibi, routerlar IOS adi verilen konfigürasyon dosyalarini çalistirmaya ihtiyaç duyarlar.

Bu biçim dosyalari, routerlarin içinde ve disinda trafigin akisini kontrol eden bilgiler ve parametreleri içerir. Özellikle routerlar yönlendirme protokolü kullanarak paketler için en iyi yol hakkinda kararlar yaparlar. Routerda , router protokolleri ,yönlendirme ve dogru ayar ve kullanim seçiminde tüm özel bilgiler konfigürasyonunda mevcuttur.

Bu bölümde routera IOS komutlarindan performans için gerekli ag fonksiyonlarinin konfigirasyonunun nasil yapildigi gösterilecek. Router biçim dosyasi ilk bakista, komplekste gözükebilir. Fakat egitimin sonunda nekadar basit oldugu görülecektir.

Bir routerin ana iç bilesenleri asagida görülmektedir ;

1-RAM 2-NVRAM 3-Flash Memory 4-ROM 5-Arabirim



RAM in izledigi karakteristikler ve fonksiyonlari:

- Yönlendirme tablosunun kayitlarini tutar
- ARP bellegini tutar
- Hizli anahtarlama bellegini tutar
- Paketleri tamponda tutar (paylasilmis RAM)
- Durmus paketleri sürdürür
- Açilista konfigürasyon dosyalari için geçici hafiza saplar
- Routerin enerjisi kesildiginde yada tekrar baslatildiginda içerigini kaybeder

NVRAM in izledigi karakteristikler ve fonksiyonlari:

- Baslangiç konfigürasyon dosyalari için hafiza saglar
- Routerin enerjisi kesildiginde ya da yeniden basladiginda bilgileri içinde tutar

Flash hafizanin izledigi karakteristikler ve fonksiyonlari:

- Tutulmus sistem dosyalarini (IOS) yürütür
- Izin verilmis güncellestirilmis programlari islemcideki ciplere koymadan yada geri silmeden çalistirir.
- Routerin enerjisi kesildiginde ya da yeniden basladiginda bilgileri içinde tutar
- IOS programinda ikili versiyonlari saklayabilir
- Yapisi elektronik olarak silinebilir programlanabilir ROM un tipindedir.

Sadece Okunabilir Hafiza (ROM) izledigi karakteristikler ve fonksiyonlari:

- Enerjide kendini test için talimatlari yürütür.
- Yürütülen ana sistem programlarini baslangiç programina yükler.
- Program güncellemeleri için anakartta çipler istenildiginde çikarilabilecek sekilde yerlestirilir.

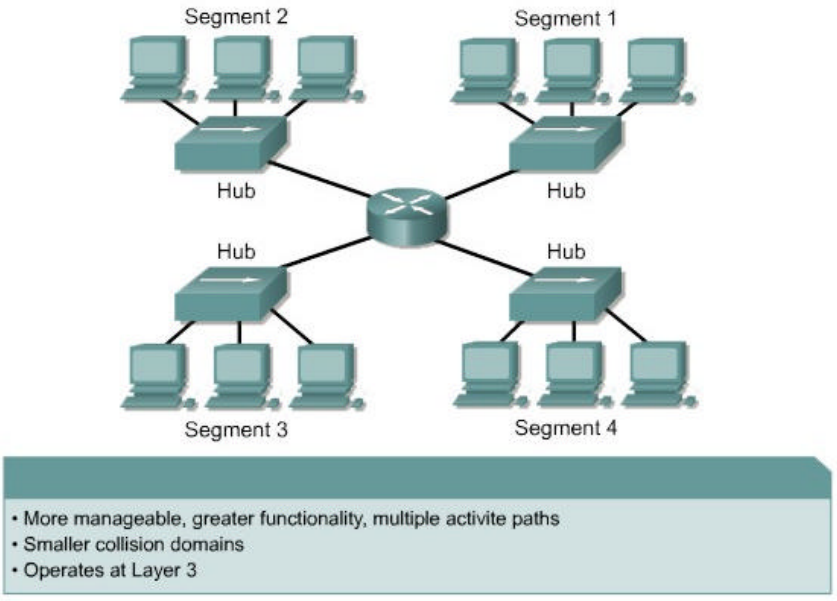
Arayüzlerin izledigi karakteristikler ve fonksiyonlari:

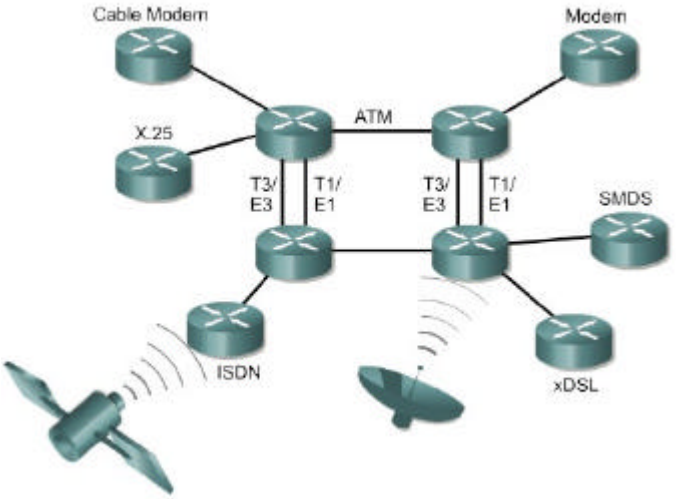
- Çerçeve giris çikislari için aga routerlari baglar
- Modül bölmelerinde yada anakartlarda olabilirler.

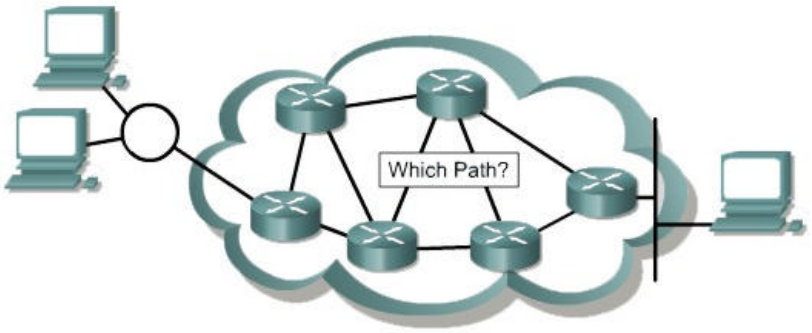
1.1 WAN' lar

1.1.3 WAN ve LAN ' larin Routeri

Routerlar LAN parçalarinda kullanirlar. WAN araçlari gibi önemli yerlerde kullanilirlar. Routerlar LAN ve WAN arayüzlerinde baslangiçlarinda olmak zorundadirlar. Gerçekte WAN teknolojileri diger WAN teknolojileri ile baglantilarini siksik routerlarla kurarlar. Routerlar internetin ve genis aglarin omurga araçlaridir. OSI referans modelinin üçüncü katmaninda çalisirlar. Ag adreslerinde temel kararlari verirler. Iki ana özellikleri vardir. Birincisi en iyi yolu seçmek , ikincisi uygun arabirime paketlerin anahtarlamasini saglamak. Routerlar diger routerlar ile ag bilgilerinin degisikligini , yönlendirme tablolarinin yapisini basariyla birbirlerine ulastirirlar.







Anayönetitici, statik yönlendirme konfigürasyonunu yönlendirme tablolari ile sürdürebilir. Fakat genellikle yönlendirme , tablolari diger routerlar ile ag topolojisi bilgilerinin degisikliklerini dinamik yönlendirme yoluyla saglanir.

Örnek verecek olursak ; dünyada x bilgisayari diger y bilgisayari ile yakininda baglantiya ihtiyaç duymaktadir. Z bilgisayari ise uzak bir yerdedir. bilgi akisi için yönlendirme yapilirken yönlendirme için güvenebilirlilik , en iyi ve en genis yol gereklidir. Birçok ag dizayninin kararinda ve teknolojilerinde x,y ve z bilgisayarlarinin baglantilari için izlenebilir olmasi istenir.

Dogru konfigürasyonla yapilmis çalisma asagidaki özelliklerle saglanmaktadir ;

- Adresin sondan sona kararliligi
- Adresler uygulandigi ag topolojisini temsil etmelidir.
- En iyi yol seçimi
- Dinamik yada statik yönlendirme
- Anahtarlama

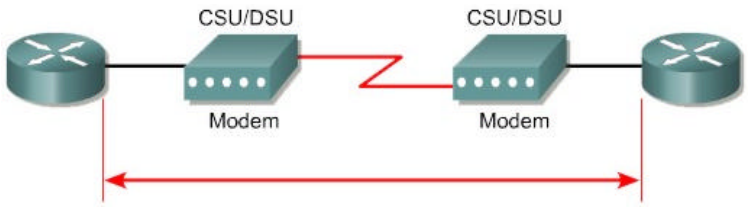
1.1 WAN' lar

1.1.4 WAN lardaki Routerin Rolü

WAN , data iletim katmaninda ve fiziksel katmanda islem görür. Bu WAN da OSI referans modelinin diger bes katmaninin olmadigi manasina gelmesin. Sadece ifade edilmek istenilen kisim WAN ni LAN da bulunan Data iletim katmanind a ve fiziksel iletim katmanindaki tipik özelliklerin frakliliklarini göstermektir. WAN nin birinci ve ikinci katmani , LAN daki kullanilan katmanlara göre diger özellikler , standartlar ve protokoller kullanilir.

WAN fiziksel katmanda data sonlandirma gereçleri (DTE) ve data devre sonlandirma gereçlerini (DCE) tanimlarlar.diger arayüzleri tanimlar. Genellikle DCE servis sunucuda , DTE ise bitisigindeki araçta bulunur. Bu modelde servisler, DTE ye mevcut araçlar modem vb. araçlar sunarlar. (Sekil 1)

Routerin baslica fonksiyonu yönlendirmedir. Yönlendirme ag katmaninda meydana gelir. Yani katman 3 te gerçeklesir. Fakat WAN operasyonlari katman 1 ve katman 2 de olur. Durum böyle ise Router bir WAN aracimidir yoksa LAN aracimidir? Cevap verecek olursak ag çalismalarinda sik sik bu soru ile karsilasilir. Bazen Router sadece LAN aracida , WAN aracida olabilir. Bazen de WAN ve LAN sinirlari arasinda veya bazi zamanlarda LAN ve WAN araci olabilir.



Katman 3 te paketleri WAN yönlendirilirken routerin bir rolü olur. Fakat bu ayni zamanda Lan da da routerin rolüdür. Bu nedenle yönlendirme router in WAN daki tam bir rolü degildir. Router fiziksel ve data iletim katmanindaki standartlar ve protokolleri kullandigi zaman WAN ile birlestirir. WAN araçlari gibi islem görür. Ilk olarak routerin WAN daki rolü bu nedenle yönlendirme degildir. Fakat WAN lar arasinda fiziksel ve data iletim katman standartlarini ve baglantilarini saglarlar. Örnek verecek olursak ; router, ISDN arayüzünde PPP seri arayüz T1 hatti sonlandirmasinda Frame Relay sikistirmasini kullanmak zorundadir. Router servisin tipine göre bitlerin akisini saglayabilmedir. Degisik data sikistirmalarindan digerlerine yada ISDN den T1 e akiskanligi saglayabilmelidir.

WAN nin katman 1 ve katman 2 protokollerinin birkaç detayi ilerleyen kisimlarda gözlemlenecektir. Fakat referans için WAN protokol ve standartlari bazilari örnek olarak verilebilir.

WAN fiziksel katman standartlari ve protokolleri:

- EIA/TIA-232
- EIA/TIA-449
- V.24
- V.35
- X.21
- G.703
- EIA-530
- ISDN
- T1, T3, E1, ve E3
- xDSL
- SONET (OC-3, OC-12, OC-48, OC-192)

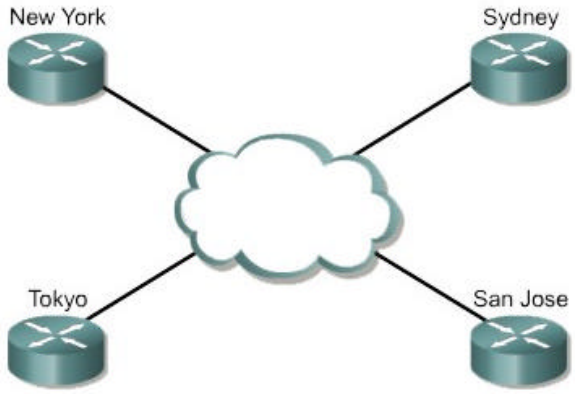
WAN data iletim standartlari ve protokolleri:

- High-level data link control (HDLC)
- Frame Relay
- Point-to-Point Protocol (PPP)
- Synchronous Data Link Control (SDLC)
- Serial Line Internet Protocol (SLIP)
- X.25
- ATM
- LAPB
- LAPD
- LAPF

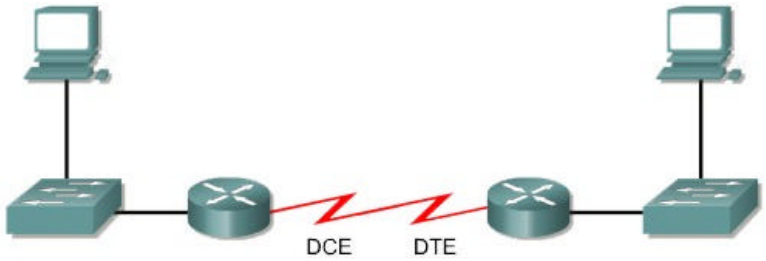
1.1 WAN' lar

1.1.5 Laboratuarlara Akademik Yaklasim

Egitim esnasinda tüm aglarin baglantilari seri yada Ethernet kablolari ile olacak ve egitim görenler tüm donanimlara dokunabilirler ve görebilirler. Egitim uygulamalarina benzemeyen , gerçek hayatta seri kablolar arkadan arkaya baglanmazlar. Gerçek dünyada bir router bir eyalette bulunurken diger router öbür uçtaki bir ülkede olabilir. Ankara daki yönetici WAN bulutundaki Ankara daki routerin arizasini düzeltmek için router baglanmak zorunda olacaktir.



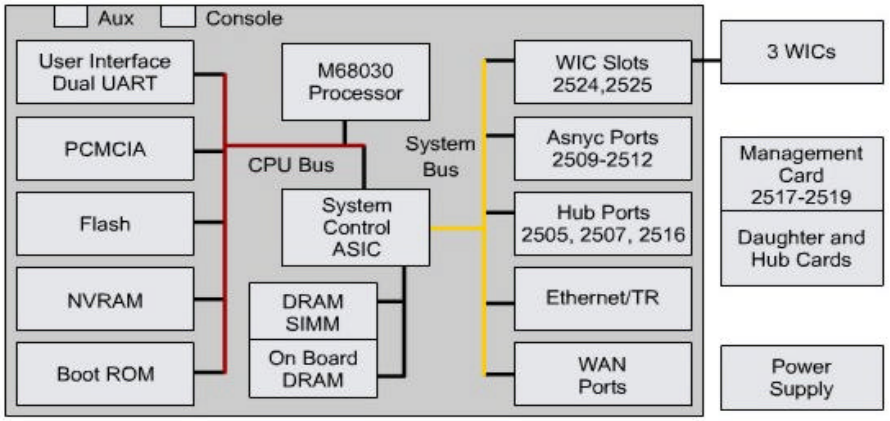
Egitimde , Araçlar WAN simülasyonu için baglanti DTE-DCE kablolari ile arkadan arkaya baglanacaktir. Baglantilar bir routerin arayüz S0/0 indan diger router arayüzüne S0/1 baglanarak baglanti olusturulacaktir. Baglanti yapilirken kablonun DCE ucu ilk routera DTE ucu ise diger router in seri arayüzüne baglanacaktir.

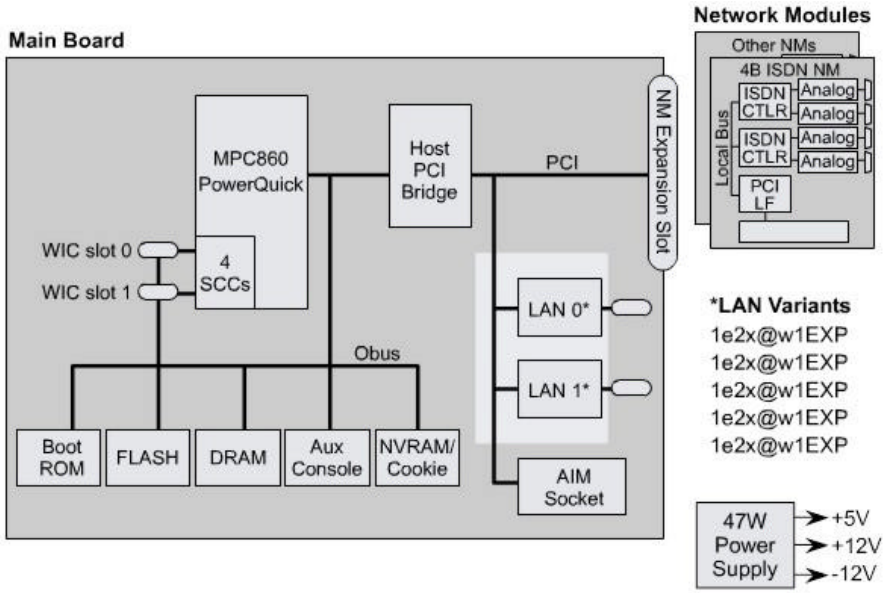


1.2 Routerlar

1.2.1 Router Iç Bilesenleri

Süre içerisinde router modelleri arasinda mimari farkliliklar olustugu görülmektedir. Bu bölümde önemli iç parçalari tanitilacaktir. Sekil1 ve 2 de CISCO router in iç yapisi gösterilmistir.





CPU – Merkezi Islem Birimi sistem islemlerini yürütür. Fonksiyonlar arasinda yönlendirme fonksiyonlari ve ag arayüz kontrolünü yönetir.CPU bir mikroislemcidir. Büyük routerlarda çift islemci bulunur.

RAM – Rastgele erisimli Hafizadir. Yönlendirme tablolari için kullanilirlar. Önbellek anahtarlamalari hizlidir. Konfigürasyonlari çalistirirlar. Paketleri siralarlar. Encok routerlarda ana islemci hafizasi ve paylasilmis giris/çikis hafizasidir. Paylasilmis I/O hafiza paketlerin arayüzler rasinda geçici olarak kaydedildigi alandir. Içerikleri enerji kesildigi zaman geri gider. RAM genellikle DRAM dir ve DIMM modülleri tarafindan eklenerek çogaltilabilirler.

Flash – Flash hafiza tüm Cisco IOS program bilgilerinin kayitlari için kullanilir. Router normalde standart IOS bilgisini flash bellekten çalistirir. Yeni bilgiler flashta yüklenip güncellenebilir. ISO sikistirilmis yada sikistirilmamis biçimde olabilir. Çogu Routerlar ISO un rame açilis islemlerini islemesi için transfer ettigi islemleri tabloya kopyalarlar. Diger routerlar ise IOS bilgilerini direkt olarak flash bellekten çalistirirlar. Eklemeli yada geri çikarmali flaslar SIMM yada PCMCIA kartlarla flash yükseltilebilir.

NVRAM – Degisken olmayan rastgele-giris hafizasi olarak tanimlanir. Baslangiç ayarlari kayitlarina kullanilirlar. NVRAM , bazi araçlarda EEROMlari kullanarak islevlerini yerine getirir. Diger araçlar baslangiç kodlari yüklenmis flaslari kullanarak yerlerine getirirler. Her iki özellikte de enerji kesildigi zaman bilgiyi hafizalarinda tutarlar.

Buses – Çogu router sistem veri yolu ve CPU veri yolu içerir. Sistem veri yolu CPU ve arayüzler arasinda baglanti için kullanilirlar.Bu veriyolu arayüzler arasinda paketleri tasirlar. CPU veriyolu router kayitlarindan parçalara erisim için CPU tarafindan kullanilir.Bu veriyolu özel hafiza adreslerinden verileri yada talimatlari tasirlar.

ROM – Sürekli olarak baslangiçta tanimlanmis kod için kullanilirlar. Ana görevleri Ram a flashtan ISO bilgilerini yüklemek ve routerin sürekli çalismasi esnasinda donanim bilgilerini açilisa yüklemektir.Bazi routerlar ana kodlarinin alternatifi olarak indirilen dosya ile karsilastirirlar.ROM lar silinemezler. Sadece soketlerde chipler çikarilip yerine yenisi takilarak güncellenebilirler.

Interfaces – Arayüz olarak tanimlanirlar. Dis hatlara router baglantilari olarak islev görürler. Arayüzün üç tipi mevcuttur. Bunlar LAN , WAN ve Konsol/AUX tipi arayüzdür.

LAN arayüzü genellikle Ethernet yada Jeton Halka standardinin bir arayüzüdür. Arayüzler medyaya sistem baglantilari için chip kontrollerinin mantigini saglamak zorundadirlar. LAN arayüzü tutturulmus bir biçim veya modüler olabilir.

WAN arayüzü , ISDN ve CSU içerir. LAN arayüzleri ile WAN arayüzleri özel çip kontrolü saglamak zorundadirlar. WAN arayüzleri tutturulmus bir biçim veya modüler olabilir.

Konsol/AUX portlari, routerin iç komutlari için ilk olarak seri portlari kullanirlar. Bu portlar ag baglantilarinda kullanilan bildigimiz portlar degildir. Bilgisayarda yada modemdeki iletisim portlarindan terminal sunumlari için kullanilirlar.

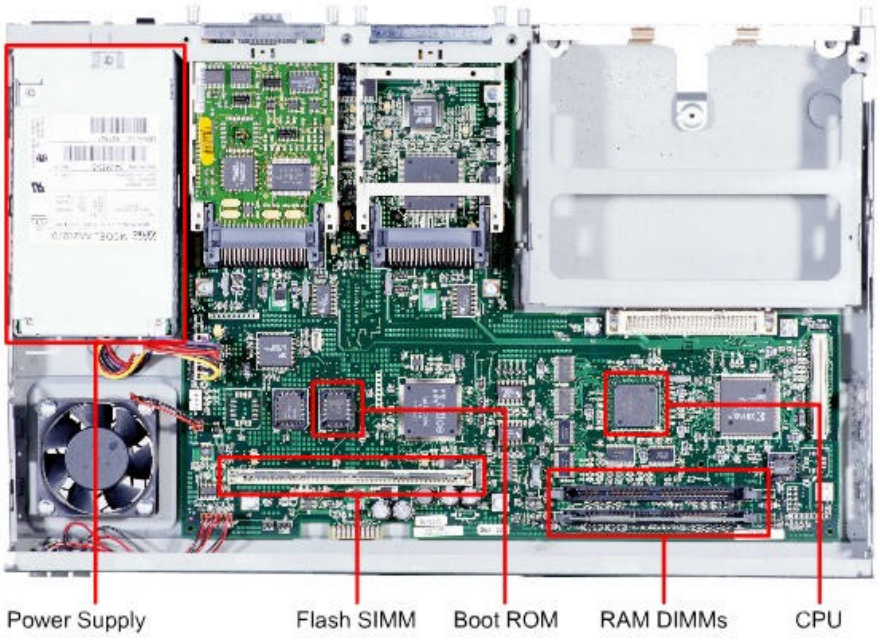
Power Supply – Enerji saglayici manasindadir. Iç parçalarin çalismalari için gerekli olan enerjiyi saglarlar. Büyük routerlar , modüler güç saglayicilari yada çift olarak kullanirlar. Bazi küçük routerlarda routera enerji beslemesi disaridan saglanmaktadir.

1.2 Routerlar

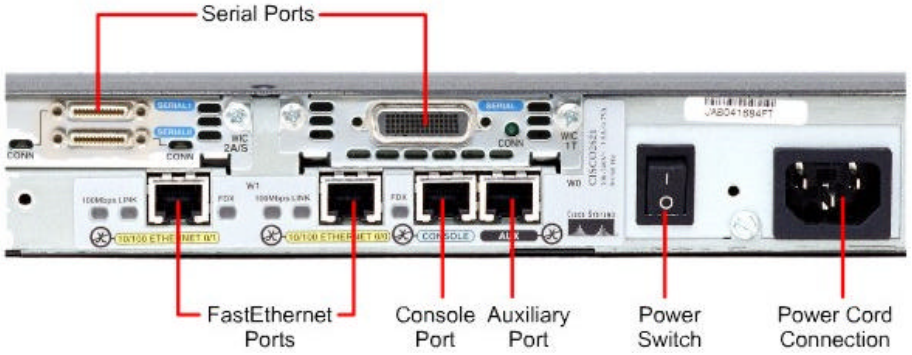
1.2.2 Routerin Fiziksel Karakteristigi

Routeri kullanmanin nasil oldugunu anlamak için routerin içinde fiziksel bilesenlerinin yerini bilmek kritik degildir. Yine de birkaç yerde , böyle hafizaya eklemek olarak, çok yardimci olabilir

Dogru parçalar kullanilir ve konumlari router modelleri arasinda degisebilir. Sekilde 2600 router in iç yapisi görülmektedir.

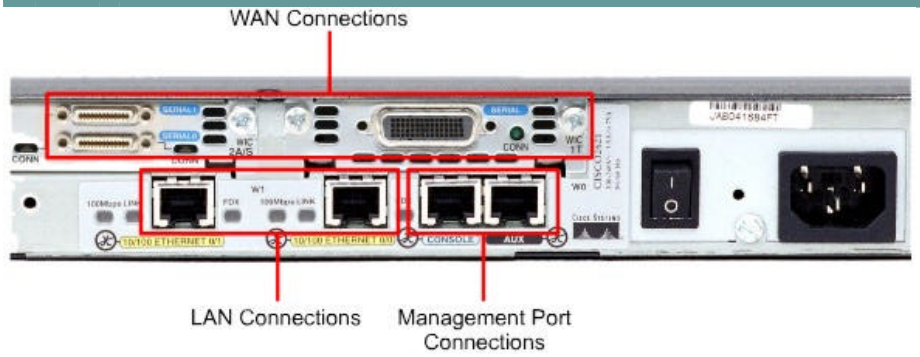


Asagidaki sekilde ise 2600 Router in disaridan arka görüntüsü görülmektedir.



1.2 Routerlar

1.2.3 Router Dis Baglantilari



Routerin arayüz baglantilarinda üç tip mevcuttur. Bunlar LAN arayüzü , WAN arayüzü ve yönetim portlaridir.
LAN arayüzü yerel alan agina olan baglantilari saglar. Bu genellikle Ethernet teknolojisinde kullanilir. Bununla birlikte Jeton Halka yada ATM gibi baglanti tiplerinde LAN teknolojileri kullanilir.

Genis alan aglarli baglantilarinda internete yada uzak sitelere servis saglayicilardan baglanti sunarlar. Diger WAN arayüzlerinde seri baglanti yada bir numara ile olabilir. WAN arayüzünün baglanti tipleri ile servis saglayicilarin lokal baglatilarina router baglantilarina harici araçla baglanabilir. Diger WAN baglanti tiplerinde servis sunucusunun baglantisi direkt olabilir.

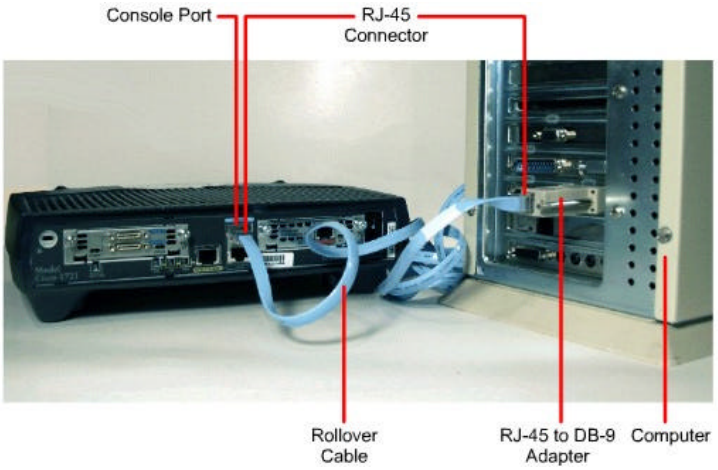
Port yönetiminin fonsiyonlari diger baglantilardan farklidir. LAN ve WAN baglatilarinda hangi paket dosyasinin geçecegi ag baglantilarini sunarlar. Routerin konfigürasyon ve aksakliklarin giderilmesi için port yönetimleri yazi ve temel baglanti sunarlar. Genel yönetim arayüzleri konsol ve yardimci portlardir.Seri portlar EIA-232 standardini kullanirlar. Bilgisayarda iletisim portlarina baglanirlar. Bilgisayar router ile yazi-temel oturum sunumlarini çalistirabilmek için terminal programlari çalistirir. Bu oturumda ag yöneticileri araçlari yönetebilirler.

1.2 Routerlar

1.2.4 Port Baglantilarinin Yönetimi

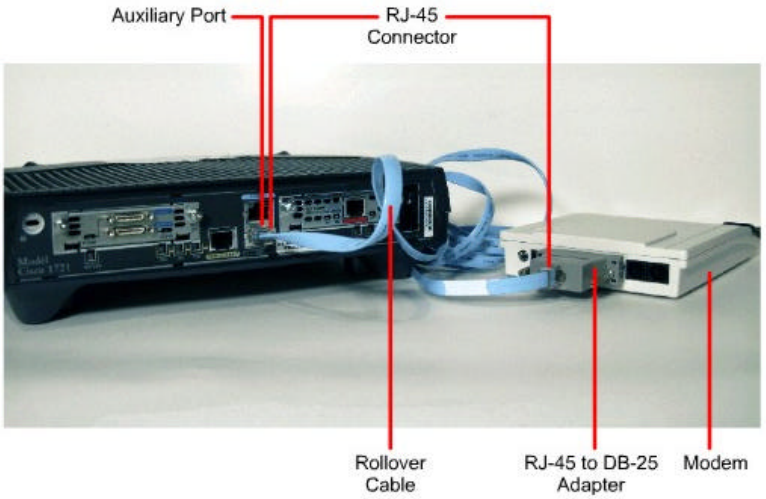
Konsol portu ve AUX portu yönetimsel portlardir. Bu senkron olmayan portlar ag iletisim portlari olarak dizayn edilmezler. Routerin iç konfigürasyonu için bu iki port gereklidir. Konsol portu , iç konfigürasyon için tavsiye edilir. Tüm routerlarda AUX portu bulunmayabilir.

Routerlar yerlerine yerlestirildigi zaman ag parametreleri ayarlari mevcut halde olmaz. Buyüzden router hiçbir ag ile haberlesemez. Konfigürasyon ve baslangiç ayarlari hazirlamak için RS-232 portu ile bilgisayardan sistem konsol portuna baglanti yapilir. Baglanti sekli asagidaki sekildeki gibi yapilir. Bu durumda konfigürasyon komutlari girilerek router ayarlanabilir.



Bu içsel konfigürasyon bilgileri , konsol veya AUX portundan routera port girildigi andan itibaren , router düzeltmek yada görüntülemek için aga baglanabilir.

Routerin , istenirse uzak bir yerden modem baglantisi kontrolü ile istenirse konsol baglantisi ile yada yardimci porttan ayarlari yapilabilir. Bu durum asagidaki sekilde daha iyi görülmektedir.

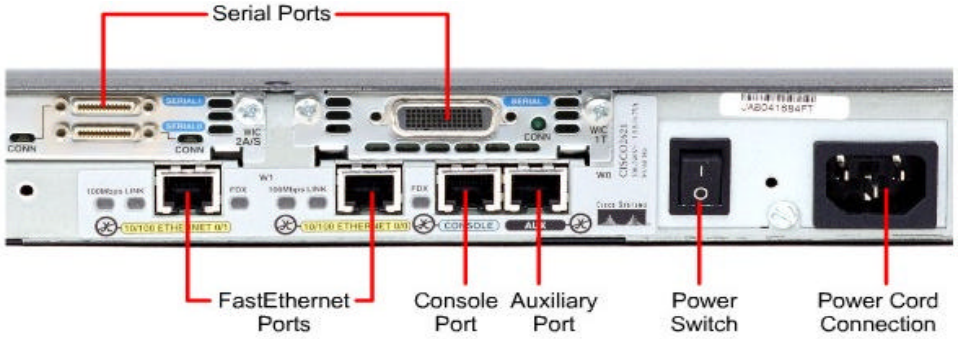


Konsol portu ayarlar için yardimci porta göre daha çok tercih edilir. Çünkü routerin baslangiç bilgileri , hata mesajlari , ayarlari görülebilir. Konsol portu , ag servislerine olan baglanti kopuklugunda baslangiç gerçeklesmedigi durumlarda kullanilabilir. Buyüzden konsol portu sifre degisikligi ve hasarlar için kullanilir.

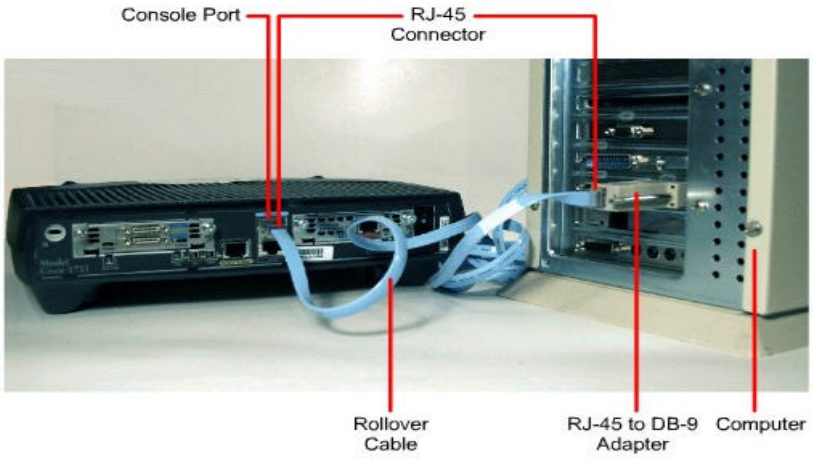
1.2 Routerlar

1.2.5 Arayüzlerin Konsol Baglantilari

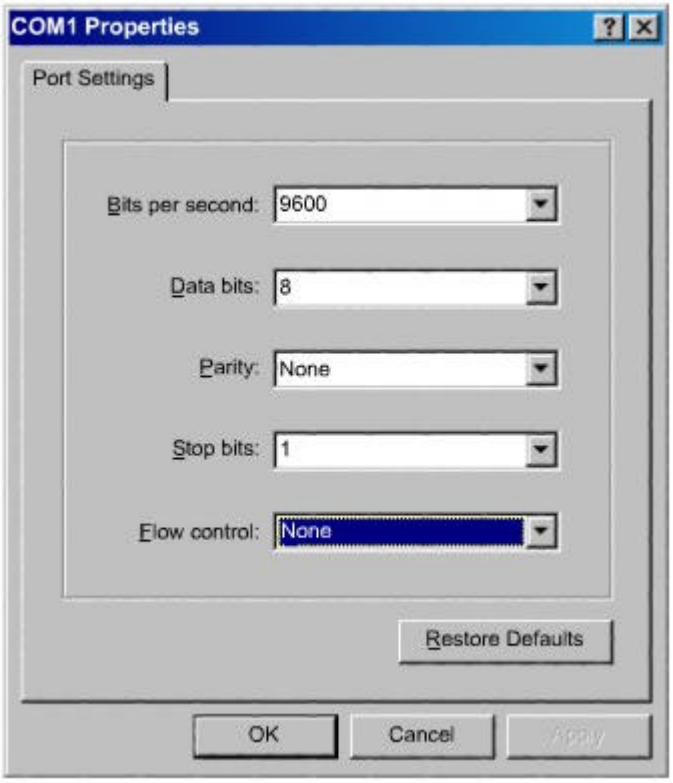
Konsol portu , routera disaridan erisim için kullanilan yönetim portudur. Routerin , gözlemleme ve hasar düzeltme prosedürleri, iç konfigürasyon için kullanilir. Asagidaki sekilde görülmektedir.



Konsol porta baglanti , rollover kablo ve RJ-45 ile DB-9 adaptör kullanilarak bilgisayara baglanir. Cisco araçlarinda konsol porta baglantida adaptör zorunludur.



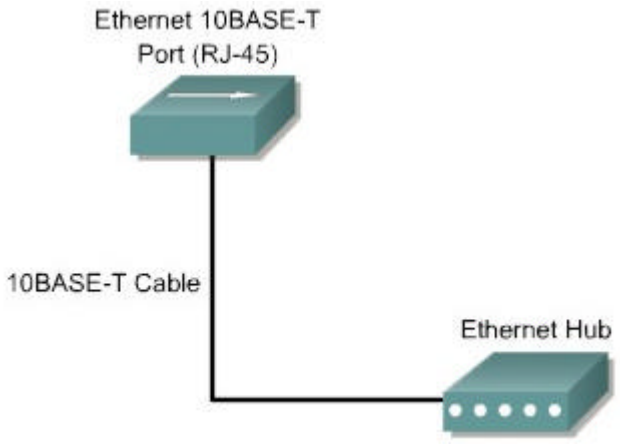
bilgisayar yada terminal , VT100 terminal emulasyonunu desteklemelidir. Terminal emülasyon yazilimi olarak Hyper Terminal programini kullanir.



1.2 Routerlar

1.2.6 LAN Arayüz Baglantilari

LAN ortamlarinin çogunda roter LAN a Ethernet veya hizli Ethernet arabirimi kullanarak baglanir. Router hub yada bir switch araciligiyla LAN la iletisim kuran bir sunucudur.bu baglanti için düz kablo kullanilir. 10/100 base TX router arabirimi cat-5 veya daha iyisini yada router tipinde mutlaka UTP kablo gerektirir.



Bazi durumlarda router in Ethernet baglantisi dogrudan bilgisayara veya diger router a olur.bu tip baglanti için crossover kablo gerekir.dogru arabirim kullanilmalidir.eger yanlis arabirim baglandiysa router yada diger network aygitlarina zarar verebilir.birçok farkli baglanti tipleri benzer konvektör stillerini kullanir.Örnegin Ethernet, ISDN BRI, konsol, AUX, entegre CSU/DSU, ve Token Ring arabirimleri,benzer sekiz pinli konnektör RJ-45, RJ-48, veya RJ-49 kullanir.

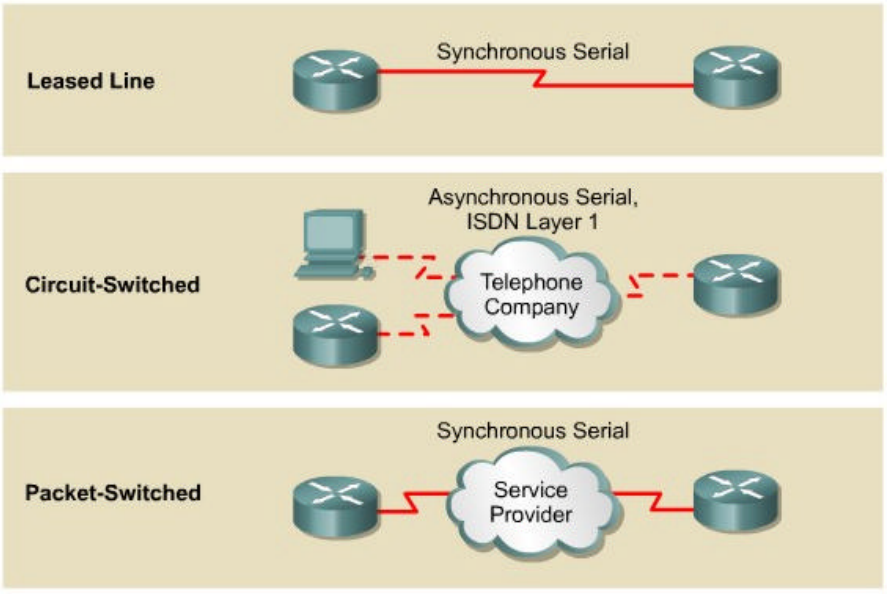
Router daki baglantilari ayirt edebilmek için, cisco, konnektör kullanimini tanimlamak için renkli kod projesini uygular.

1.2 Routerlar

1.2.7 WAN Arayüzlerine Baglanti

WAN baglantilari birçok sekilde alinabilir.WAN birçok farkli teknoloji tipleri kullanarak,genis cografi alanlarda
data baglantilari yapar.Bu WAN servisleri genellikle servis saglayicilarindan kiralanabilir.bu WAN baglantilarindan birkaçi; leased line,circuit-switched ve packet-switched tipleridir.

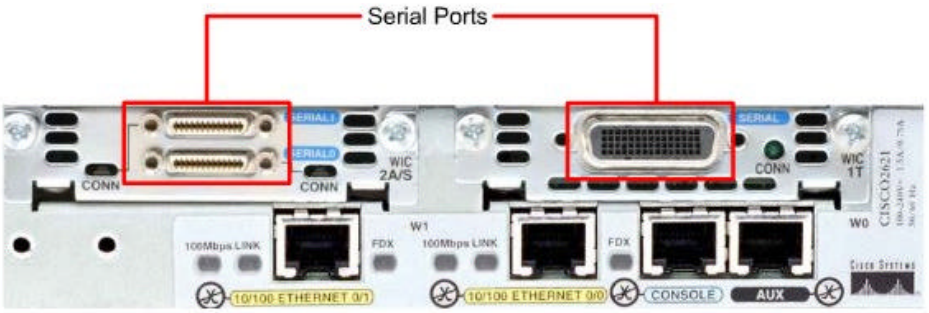
1



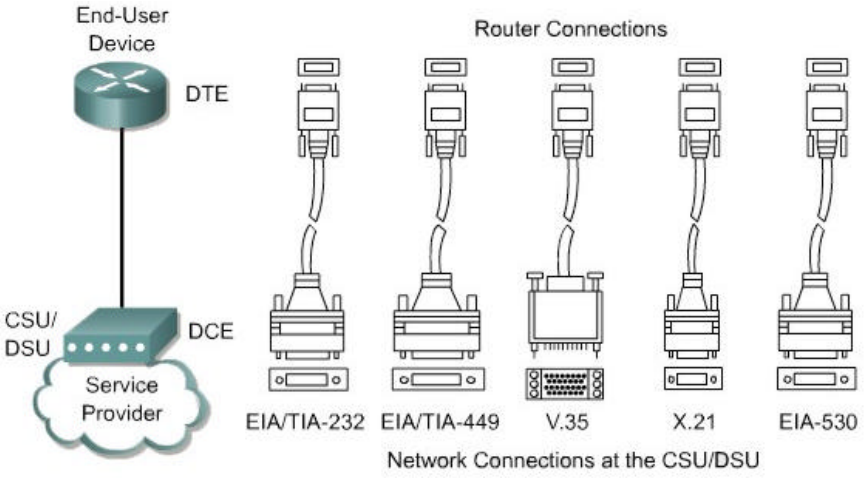
her bir WAN servis tipi için CPE,siklikla router data terminal ekipmanidir(DTE).Bu ise , DCE aygiti, genellikle bir modem veya kanal servis ünitesi/data servis ünitesi(CSU/DSU) kullanarak servis saglayicisina baglanir.bu aygit datayi DTE den WAN servis saglayicisi için uygun sekle çevirmede kullanilir.WAN servisleri için en çok kullanilan router arabirimi seri arabirimi olabilir.

Uygun seri kablo seçimi su dört sorunun cevabini vermekle kolaylasir:

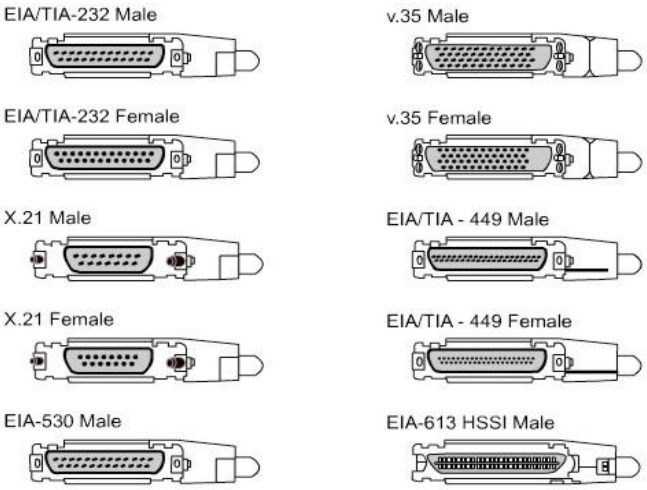
- Cisco aygitina olan baglanti tipi nedir?Cisco routerlari seri arabirimler için farkli konnektörler kullanabilir.(sekilde görülmektedir)
- soldaki arabirim smart seri arabirimdir sagdaki ise DB-60 baglantisidir.
- Bu network sistemini seri araçlara baglamak için seri kablo seçimini yapar bu ise WAN kurulumunun kritik bir kismidir.



- Network sistemi DTE veya DCE aygitina baglanmismidir?
- Iletisim için kullanilan aygitlardan DTE ve DCE seri arabirimin iki tipidir.
- Bu ikisi arasindaki kilit fark; DCE araçlari anaveri yolundaki iletisim için saat sinyali verir.aygitin kullanma klavuzu kablonun DTE veya DCE olup olmadigini açikça belirtmelidir.
- Aygit nasil bir sinyal verme standardina ihtiyaç duyar?
- Her farkli aygit için,farkli seri standardi kullanilabilir.
- Her standart kablodaki sinyalleri tanimlar ve kablo sonundaki konnektörü belirtir.
- Sinyal verme standardi için her zaman kullanma kilavuzuna bakilmalidir.



- Kabloda erkek konnektör mü,disi konnektör mü gereklidir?
- konnektörün görünür pinleri varsa erkek gereklidir.eger pinler için soketleri varsa disi gerekir.



ÖZET

Asagidaki kilit noktalarinin anlasilmis olmasi saglanmalidir.

- WAN ve LAN kavramlari
- WAN ve LAN lardaki router in rolü
- WAN protokolleri
- Enkapsülasyon konfigüresi
- Routerin dahili parçalarinin tanimlanmasi ve açiklanmasi
- Routerin fiziksel karakteristikleri
- Routerin gene portlari
- Router konsolu,LAN ve WAN portlari nasil baglanir

BÖLÜM - 2

Genel Bakis

Cisco teknolojisi, internet çalisma aygitlarinin gönderim ve degisim fonksiyonlarini kontrol eden yazilim olan internet isletim sistemi (IOS) etrafinda yapilandirilmistir.bir network yöneticisi için IOS nin çok iyi anlasilmasi
gereklidir.Bu modül IOS nin esaslarini tanitici bir sunum yapacak ve IOS nin özelliklerini pratikte inceleme olanagi saglayacaktir.En temelinden en kompleksine tüm network konfigürasyon görevleri ROUTER konfigürasyonu içinde çok güçlü bir temele ihtiyaç duymaktadir.modül bu kurs boyunca kullanilacak olan ROUTER konfigürasyonu için gerekli araç ve tekniklerini temin edecektir.

Bu bölümü tamamlayan kimseler asagidakileri yapabilmelidirler:

- IOS nin amacini tanimlayabilmelidir.
- IOS nin temel isletimini tanimlayabilmelidir.
- Çesitli IOS özelliklerini isimlendirebilmelidir
- ROUTER lar birlikte bir arabirim komut-serisi(dizini)oturumunu kuracak metotlari tanimlayabilmelidir.
- Kullanici komutuyla,yönetici ve ayricalikli EXEC modlari arasinda hareket edebilmelidir.
- ROUTER üzerinde bir hiper-terminal oturumu kurabilmelidir.
- ROUTER de belli bir mesafe kat edebilmis olmalidir.
- (CLI)daki yardim özelligini kullanabilmelidir.
- Komut hatalarini giderebilmelidir.

Cisco IOS yazilimi geleneksel CONSOLE çevresi olarak CLI kullanir.IOS, bir çok Cisco ürün yelpazesinde ana teknoloji olarak süregelmektedir.uygulamasindaki detaylar farkli internet çalisma yöntemlerine göre degisme gösterir.
Çesitli metotlarla çevreye ulasilabilir.CLI ye girmenin bir yolu CONSOLE oturumundan geçer.

CONSOLE, bilgisayardan veya terminalden, router üzerindeki CONSOLE baglantisina dogrudan düsük hizli seri baglanti kullanir.CLI oturumuna girmenin diger bir yolu da modem kullanarak dial-up baglantisiyla veya router AUX portuna bagli siradan modem kullanimidir.Bu metotlarin hiçbirisi routerin konfigüre edilmis network servislerine sahip olmasina ihtiyaç duymaz.diger bir metot ise router i TELNET lemekdir.routere telnet oturumu kurmak için en az bir tane arabirimin IP adresiyle konfigüre edilmesi ve sanal terminal oturumlari sifreler için düzenlenmelidir.

2.1 Cisco IOS Yaziliminin Isletimi

2.1.1 Cisco IOS Yaziliminin Amaci

Bilgisayarla birlikte isletim sistemi olmadan bir router veya anahtar çalisamaz.Cisco kendi isletim sistemini Cisco IOS.bu cisco routerlerinin ve catalyst anahtarlarinin içine yerlestirilmis yazilim mimarisidir.Isletim sistemi olmadan donanim hiçbir kabiliyeti haiz degildir.Cisco asagidaki network servislerini saglamaktadir:

- Temel yönlendirme ve anahtarlama fonksiyonlari
- Ag kaynaklarina güvenilir ve saglam erisim
- Network SCALABILITY

2.1 Cisco IOS Yaziliminin Isletimi

2.1.2 Routerlarda Arayüz Kullanimi

Cisco IOS yazilimi geleneksel CONSOLE çevresi olarak CLI kullanir.IOS, bir çok Cisco ürün yelpazesinde ana teknoloji olarak süregelmektedir.uygulamasindaki detaylar farkli internet çalisma yöntemlerine göre degisme gösterir.

Çesitli metodlarla çevreye ulasilabilir.CLI ye girmenin bir yolu CONSOLE oturumundan geçer.

CONSOLE, bilgisayardan veya terminalden, router üzerindeki CONSOLE baglantisina dogrudan düsük hizli seri baglanti kullanir.CLI oturumuna girmenin diger bir yoluda modem kullanarak dial-up baglantisiyla veya router AUX portuna bagli siradan modem kullanimidir.Bu metodlarin hiçbirisi routerin konfigüre edilmis network servislerine sahib olmasina ihtiyaç duymaz.diger bir metod ise router i TELNETlemekdir.routere telnet oturumu kurmak için en az bir tane arabirimin IP adresiyle konfigüre edilmesi ve sanal terminal oturumlari sifreler için düzenlenmelidir.

2.1 Cisco IOS Yaziliminin Isletimi

2.1.3 Router Kullanici Arayüz Modlari

Cisco komut-dizisi arabirimi hiyerarsik bir yapi kullanir.bu yapi özel görevleri yerine getirebilmek için farkli modlara girise gerek duymaktadir.Örnegin,bir router arabirimini konfigüre etmek için kullanici arabirim konfigürasyon moduna giris yapmak zorundadir.bunu takiben tüm konfigürasyonlar bu özel arabirime giris yapacaklardir.her bir konfigürasyon modu kendine özgü bir isaretle gösterilecek ve sadece bu mod için uygun olan komutlara izin verecektir.

IOS, “EXEC” olarak bilinen bir komut çeviri servisi saglamaktadir.her bir komut girildikten sonra, EXEC komutu onaylar ve uygular.Bir güvenlik özelligi olarak Cisco IOS yazilimi EXEC oturumlarini iki giris bölümüne ayirir. Bu bölümler kullanici ve ayricalikli EXEC modlaridir.ayricalikli EXEC modu ,enable modu
olarak da bilinir.Asagida bu iki modun özelliklerine yer verilmistir:

- Kullanici EXEC modu yalnizca kisitli sayida ki temel izleme komutlarina izin verir.bundan genellikle

“yalnizca görüs”modu olarak bahsedilir.Kullanici EXEC modu router konfigürasyonunu degistirebilecek
hiçbir komuta müsaade etmez.kullanici EXEC modu “>” imgesiyle ifade edilir.

-

EXEC Mode	Prompt	Typical Use
User	GAD>	check the router status
Privileged	GAD#	accessing the router configuration modes

Ayricalikli EXEC modu tüm router komutlarini kullanabilir.bu moda giristen önce sifre gerektirecek sekilde düzenlenebilir. Daha fazla koruma için kullanici ID si isteyecek sekilde de düzenlenebilir.Bu yalnizca routere girmeye yetkili kullanicilara imkan tanir.konfigürasyon ve yönetici komutlari ayricalikli EXEC bölümünde bulunan network yöneticisine ihtiyaç duyar.Global konfigürasyon modlara ve diger tüm spesifik modlara bu bölümden erisilebilir ve bu mod “#” ile tanimlanir.Kullanici bölümünden,ayricalikli bölüme geçis için “>” promptundaki **enable** komutuna girilir. Sifre koyulursa router bunu sorgular.Güvenlik nedeniyle girilen sifre görünmez.Dogru sifre girildiginde,router imgesi kullanicinin artik ayricalikli moda geçtigini gösteren “#” imgesine dönüsür. Ayricalikli bölümde “(?)” isaretinin girilmesi kullanici bölümündekilerden çok daha fazla komut seçeneklerini gösterecektir.

.

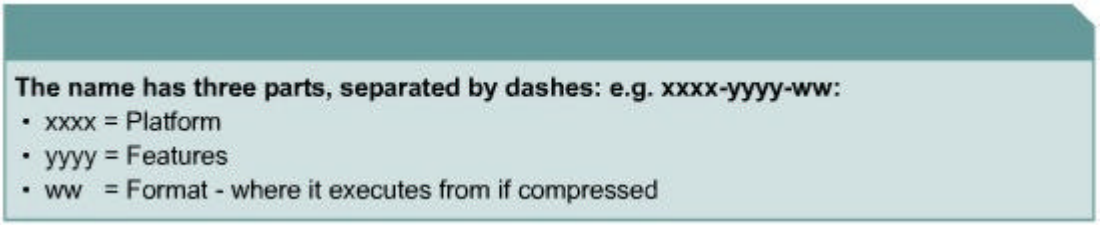
2.1 Cisco IOS Yaziliminin Isletilmesi

2.1.4 Cisco IOS yazlim özellikleri

Cisco network ürün platformlarinin genis bir bölümünü kapsayan aygitlar için imajlar saglamaktadir.Bu çesitli platformlarin gerek duydugu Cisco,IOS yazilim imajlarini en iyi biçimde kullanmak için birçok farkli Cisco yazilim imajlari gelistirmeye çalisiyor.Her bir imaj çesitli aygit platformlarina,mevcut hafiza kaynaklarina ve müsteri gereksinimlerine hizmet eden farkli özellik gruplari sunar.Farkli Cisco aygit modelleri ve özellik gruplari için sayisiz IOS imajlari olmasina ragmen temel konfigürasyon komut yapisi aynidir.Ürünlerin genis bir bölümünde uygulanan her hangi bir aygit, konfigürasyon ve hata düzeltim kabiliyetlerine sahiptir

Farkli IOS yazilimlari için konvansiyon isimlendirmesi üç bölümü içerir.

- imajin çalistigi platform
- imajda desteklenen özel nitelikler
- imajin sikistirilmis olup olmadigi ve çalistigi yer



spesifik IOS özellikleri ,Cisco yazilim danismani kullanilarak seçilebilir.Cisco yazilim danismani,en fazla mevcut veri saglayan ve network ihtiyaçlarini karsilayan opsiyon seçimlerine olanak veren interaktif bir araçtir.

Yeni bir IOS imaj seçilirken temel etmenlerden biri router flash ve RAM bellegiyle uyumlu olmasidir.genelde,sagladigi fazla özellikler ve yenilikler için daha fazla hafizaya ihtiyaç duyar.kullanilabilir flash ve mevcut imaji kontrol etmek için Cisco aygitindaki **show version** komutunu kullanmak gerekir.Cisco destek sitesi ,her bir imaj için gerekli flash ve ram miktarini belirlemeye yardim eden aygitlara sahiptir.Router üzerine yeni bir Cisco IOS yazilim imajini kurmadan önce,routerin o imaj için gereken hafizayi karsilayip karsilamadigini kontrol ediniz.Ram miktarini görmek için **show version** komutunu kullaniniz.

… <*output omitted*>… cisco 1721 (68380) processor (revision C) with 3584K/512K bytes of memory.

Bu satir nekadar ana ve paylasilmis hafizanin kuruldugunu gösterir.bazi platformlar paylasilmis hafiza olarak DRAM in küçük bir kismini kullanir.hafiza gereksinimleri bunu hesaba alir bunun için routerdeki kurulmus dram miktarini bulmak için her iki numara birlikte toplanmak zorundadir.flash memory miktarini ögrenmek için **show flash** komutunu giriniz:

GAD#**show flash**
… <*output omitted*>…
15998976 bytes total (10889728 bytes free)

2.1 Cisco IOS Yaziliminin Isletilmesi

2.1.5 Cisco IOS Yaziliminin Çalistirilmasi

Cisco IOS aygitlari üç tane özel moda sahiptir:

1

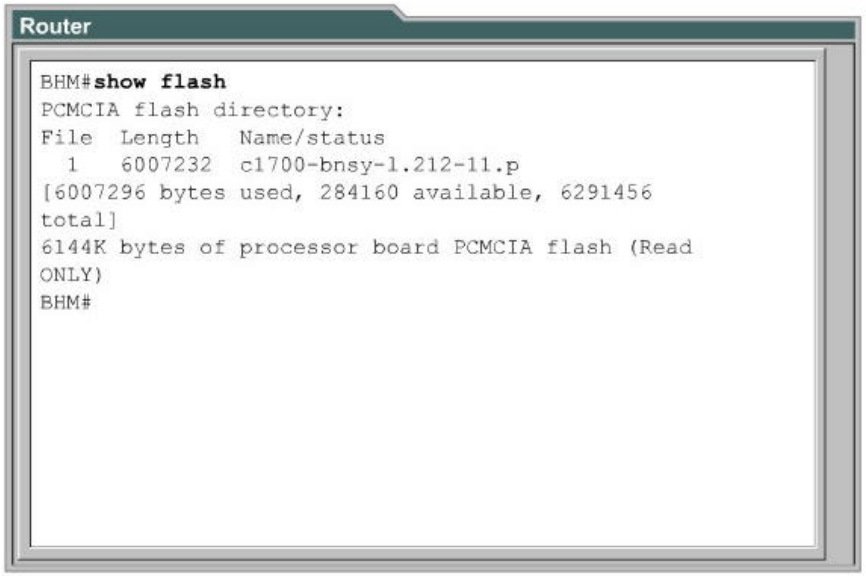
- ROM monitörü
- Boot ROM
- Cisco IOS

Operating Environment	Prompt	Usage
ROM monitor	> or ROMMON>	Failure or password recovery
Boot ROM	Router(boot)>	Flash image upgrade
Cisco IOS	Router>	Normal operation

Routerin açilis asamasi normal olarak RAM içine yüklenir ve bu isletim modlarindan birini uygular.router için varsayilan açilis modunu kontrol etmek için konfigürasyonun kaydettigi ayar sistem yöneticisi tarafindan kullanilabilir.ROM monitörü bootstrap asamasini yürütür ve düsük seviyede fonksiyonalite ve belirginlik saglar.sistem hatalarini düzeltmede ve kayip sifreleri yeniden elde etmede kullanilir.ROM monitörü herhangi bir network arabirimi tarafindan kullanilamaz sadece konsol portundan fiziksel ve direkt baglantiyla kullanilabilir.

Router boot ROM modunda çalistiginda sadece Cisco IOS özelliklerinin kisitli ikincil ayarlari kullanilabilir.Boot ROM yazili islemlere izin verir ve her seyden önce flash da depolanan Cisco imajinin yerine yenisini koymak için kullanilir.Cisco IOS imaji,TFTP sunucusunda depolanmis bir IOS imajini routerin flash sunucusunda hafizasina kopyalayan, **copy tftp flash** komutu kullanilarak boot Rom içinde modifiye edilebilir.routerin olagan bir islemi flashda depolanmis Cisco IOS imajinin tam kullanimina ihtiyaç duyar.bazilarinda ise,IOS flash tan direkt olarak yürütülür.bununla birlikte birçok Cisco routeri RAM e yüklenmek ve de RAM den yürütülmesi için IOS nin bir kopyasina ihtiyaç duyar.bazi IOS imajlari flashta sikistirilmis halde depolanir ve RAM e kopyalanirken açilmalari lazimdir.

Çalisan IOS imajini ve versiyonunu görmek için konfigürasyon kayit ayarlarini da gösteren **show version** komutunu kullarininiz. **show flash** komutu yeni bir Cisco IOS imajini yüklemek için sistemin yeterli bellege sahip olup olmadigini dogrulamak için kullanilir. 2



2.2 Routerlarin Baslatilmasi

2.2.1 Cisco Routerlarin Baslangici

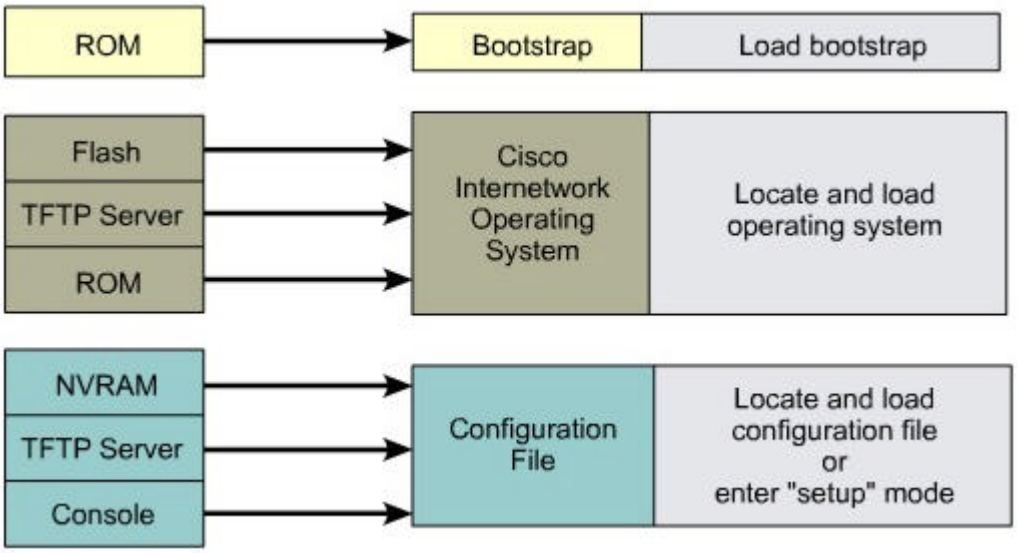
Router baslangiçta konfigürasyon bilgilerini , isletim sistemini baslangica yükler. Eger router, konfigürasyon dosyalarini bulamazsa ayar moduna girer. NVRAM de saklanmis olan konfigürasyon bilgilerinin yedegini ayar modundan kopyalar.

Cisco IOS programi için her zamanki baslangiçtaki amaç router a operasyonlari baslatabilmektir. Bunun için asagidaki görevleri baslangiçta tamamlamalidir.

- Router donaniminin testi ve fonksiyonlari kesinlikle yapilmalidir.
- Cisco IOS programi bulunup yüklenmeli
- Baslangiç ayarlari bulunup uygulanmali yada ayar moduna girilmelidir

Cisco Router çalistigi zaman kendisini test eder. Kendini test süresince , tüm donanim modüllerinde ROM dan tanimlayarak yürütür. Ag arayüz portlari , hafiza , ve islemcide temel operasyonlar yaparak testi sürdürür. Donanimin dogrulugunu tamamladiktan sonra , router baslangiç programini yürütür.

Donanim test edildikten sonra Router asagidaki akisli izlemektedir: 1



Adim 1 ROM dan genel baslangiç adimlarini yükler. Örnegin baslangiç adimlarinda operasyon için donanimin testi ve IOS bilgilerinin yürütülmesi saglanir.

Adim 2 IOS birkaç yerde bulunabilir. IOS yüklenirken baslangiç kisminda konfigürasyon kayitlari belirlenir. Eger baslangiç , agdan yada flas bellekten yüklendiyse sistem komutlari belirtilen yer ve isimdeki dosyadan okunur.

Adim 4 Konfigürasyon dosyasi NVRAM den kayit edildiginde ana hafizaya ve tek hatta birken yüklenir. Konfigürasyon komutlari yönlendirme islemlerini baslatir. Arayüzler için adres saglar. Routerdaki diger operasyonlari tanimlar.

Adim 5 Eger NVRAM deki konfigürasyon dosyasi kayipsa , mevcut TFTP sunucudan aratilir. Eger sunucuda bulunmussa yüklenilir.

Ayarlar , routerdaki karisik protokol girisleri için tasarlanmamistir. Ayar modundaki amaç yöneticiye verilmis izinler dogrultusunda router için minimum ayarlari yüklemektir. Diger kaynaklardan ayarlarin yerini ögrenmek mümkün degildir.

Ayar modunda, standart cevaplar asagidaki sorularda parantez içindeki alanda gözükmektedir. Enter tusuna basilir. Ayar islemleri süresince , **Ctrl+C** ile isleme son verilebilir. Ctrl+C ayarlar

Router

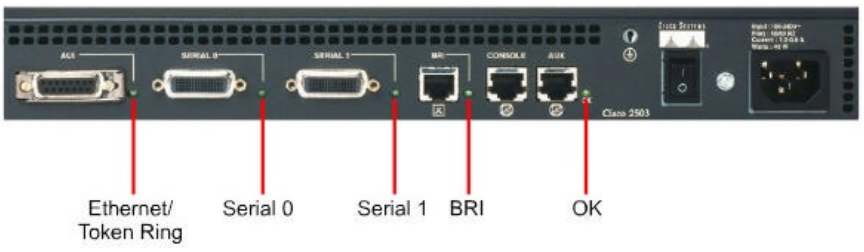
```
#setup

--System Configuration Dialog--
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Continue with configuration dialog? [yes].

First, would you like to see the current interface summary?
[yes]

Interface    IP-Address    OK?   Method    Status   Protocol
TokenRing0   unassigned    NO    not set     down     down
Ethernet0    unassigned    NO    not set     down     down
Serial0      unassigned    NO    not set     down     down
Fddi0        unassigned    NO    not set     down     down
```

2.2 Routerlarin Baslatilmasi

2.2.2 Router LED Göstergeleri

Cisco Router lar bilgileri göstermeli için isikli göstergeler kullanirlar. Cisco router modellerinde buna ihtiyaç duyulur. Isikli göstergeler çesitli renklerde olabilirler.

Arayüz lambalari , arayüz üzerinde görülebilecek yerde islem görürler. eger arayüz aktif ve dogru baglanti yapildigi zaman LED yanmaz ise bir problem var demektir. Eger arayüz çok mesgulse LED sürekli yanacaktir. AUX portun isigi yesil isil yaniyorsa sistem dogru çalisiyordur. Sistem dogru baslatilabilir.



2.2 Routerlarin Baslatilmasi

2.2.3 Router Açilisinin Incelenmesi

Ekranlarda görüntülenen grafik sadece referans içindir ve konsoldaki görüntüyü tam olarak yansitmazlar.

" Geçersiz NVRAM, yazi geçersiz oldugundan silinmistir " mesaji geliyorsa router henüz konfigüre edilmemistir yada NVRAM silinmis olabilir. Router konfigüre edilmelidir. Konfigürasyon dosyasi NVRAM e yüklenir. Ondan sonra konfigürasyon dosyasi NVRAM' de kullanilarak konfigüre edilir. Konfigürasyon kayitlari için fabrika ayari 0x2102 dir. Flash hafizadan Cisco IOs dosyasi routera yüklenir.

Kullanici önyükleme versiyonunu ve IOS versiyonunu tanimlayabilir. Router kullanilarak router modeli , islemci ve routerdaki hafiza miktari ögrenilebilir. Diger bilgiler grafiklerde listelenir:

- Arayüzün numarasi
- Arayüzün Tipi
- NVRAM miktari
- Flash Hafiza Miktari

Kullanici ayar moduna girerek seçmek zorundadir. Ayar modunda yöneticiye sadece minimum konfigürasyonu yükleyebilmesi müsaade edildigi hatirlanmalidir.

2.2 Routerlarin Baslatilmasi

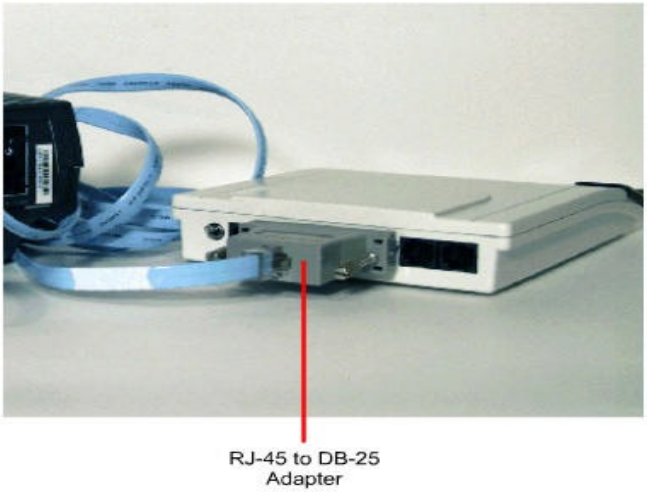
2.2.4 HyperTerminal Oturumunun Kurulmasi

Tüm Cisco routerlarda TIA/EIA-232 eszamansiz seri konsol portu (RJ-45) mevcuttur. Kablolar ve adaptörler konsol portuna terminal konsol baglantisina ihtiyaç duyarlar. Konsol terminali ASCII terminal yada bilgisayardan çalistirilan HyperTerminal emülatör yazilimidir. Bilgisayar kullanilarak konsol portu olusturulabilir. RJ-45 ve RJ-45 kablosu ile disi RJ-45 kullanilir.

Konsol portu için varsayilan parametreler 9600 bps , 8 veri biti, esitlik yok, 1 tane durdurma biti ve akis kontrolü olmayacaktir. Konsol portunun akis denetimi için donanim destegi yoktur.

Routerda konsol portuna terminalle baglanmak için su adimlar uygulanir.

1. RJ-45 ve RJ45 kablosu yada DB-9 ve DB-25 adaptör kullanilarak terminal baglantisi yapilir.
2. 9600 bps , 8 veri biti, esitlik yok, 1 tane durdurma biti ve akis kontrolü olmadan terminal konfigüre edilir.



PC Operating System	Software
Windows 95, Windows 98, Windows NT, Windows 2000	HyperTerminal (included with Windows software), ProComm Plus
Windows 3.1	Terminal (included with Windows software)
Macintosh	ProComm, VersaTerm, ZTerm (supplied separately)
Unix/Linux	Minicom

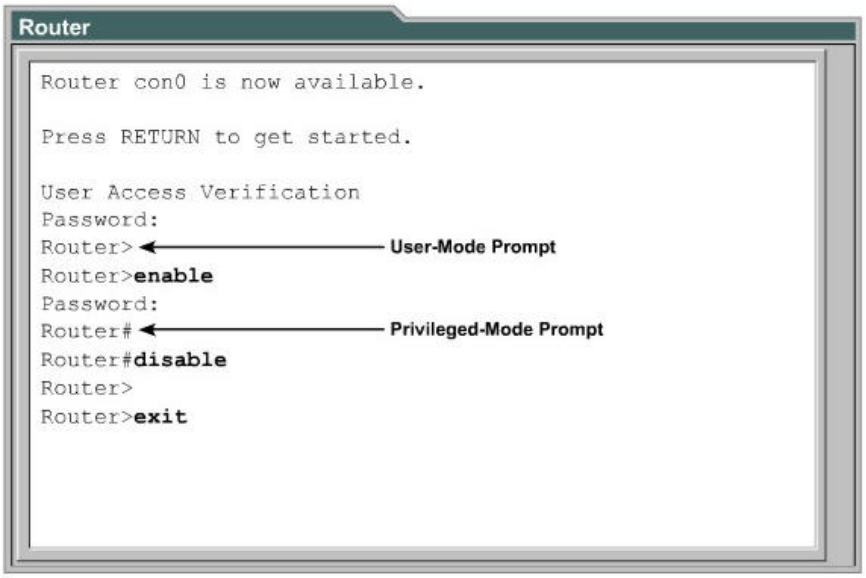
2.2 Routerlarin Baslatilmasi

2.2.5 Routerda Günlük Tutulmasi

Cisco routerlarinin konfigürasyonunda , router kullanicisi uzaktan erisimle yada terminale erisim yapabilir.routera erisim yapildigi zaman komutlar girilmeden önce routera giris yapilmalidir.

Güvenlik için , router komutlarina erisim iki kisimdan olusur:

- **Kullanici Modu** – bu moda router konfigürasyonunda degisiklik yapilamaz. Routerin görevlerini kontrol eden tipik görevlerdir.
- **Yönetici Modu** – Router konfigürasyonunda degisikliklerin yapildigi moddur.



Kullanici modunda kullanilan komutlar yönetici modda kullanilan komutlarin alt komutlaridir. Roter konfigürasyonundaki degisikliklerin dalindaki bilgilerin görüntülendigi komutlardir.

Komutlarin tamamina erisebilmek için yönetici moda girin. ">" yerindeyken **enable** komutunu yazin. **Password *sifre*** ile sifreyi girin. Sifreyi girdikten sonra **enable secret** komutunu kullanin. Bu iki komutu kullanarak yönetici moda girebilirsiniz. Eger bu komutlari girerseniz **enable secret** komutu öncelik alacaktir. "#" isareti görülüyorsa yönetici moda girilmis demektir. Global konfigürasyon moduna sadece yönetici modayken ulasilabilir. Global konfigürasyon modundayken asagidaki kisimlara erisilebilir.

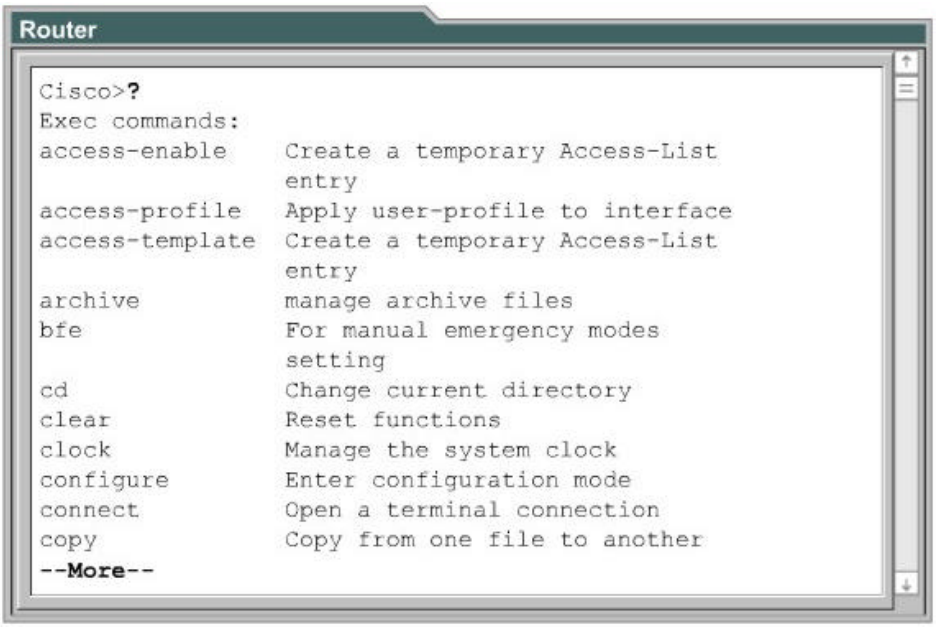
- Arayüze
- Altarayüze
- Hatta
- Routera
- Router haritasina

Kullanici moduna geri dönmek için yönetici modayken **disable** yada **exit** komutunu girin. Böylece global konfigürasyon modundan yönetici moduna gri dönülecektir. Tekrar **exit** yada **Ctrl-Z** komutlari girilerek kullanici moda geri dönebilirsiniz.

2.2 Routerlarin Baslatilmasi

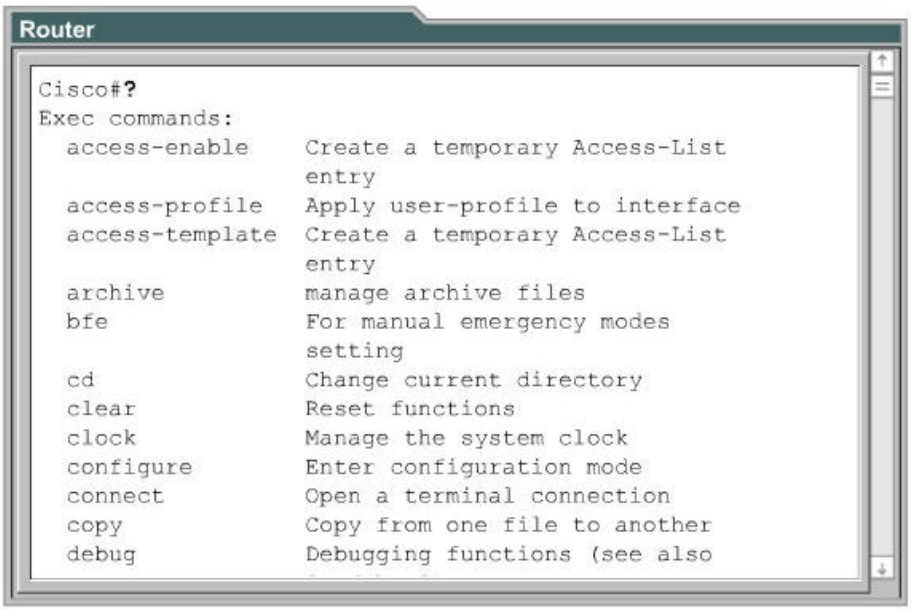
2.2.6 Routerda Klavye Yardimlari

Kullanici yada yönetici moda soru isareti kullanilarak komut listesi görüntülenebilir. Asagidaki sekilde örnek olarak gösterilmistir.



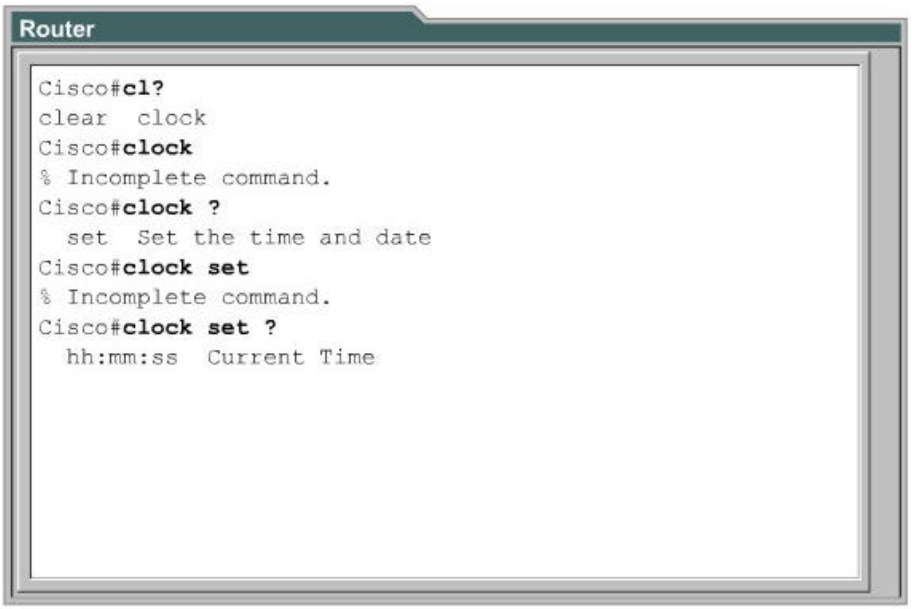
Not: "**--More--**" görüntünün asagida devam ettigini göstermektedir. Ekran görüntüsü birkaç satirdan ibarettir. MORE komutu ile çikis birden fazla sayfada gösterilir. Her more komutu gözüktügü zaman bir sonraki ekranin görüntülenmesi için bosluk tusuna basilir.
Return yada enter tusu ile de gelecek satirlara gidilebilir. Diger tuslarla da ilerlenebilir.

Yönetici moda "**enable**" yada "**ena**" yazilarak erisilenebilinir. Bunun nedeni router . Soru isareti , yönetici moda komutlarin uzun ve açiklayici bir sekilde ekranda görüntülenmesini saglar.



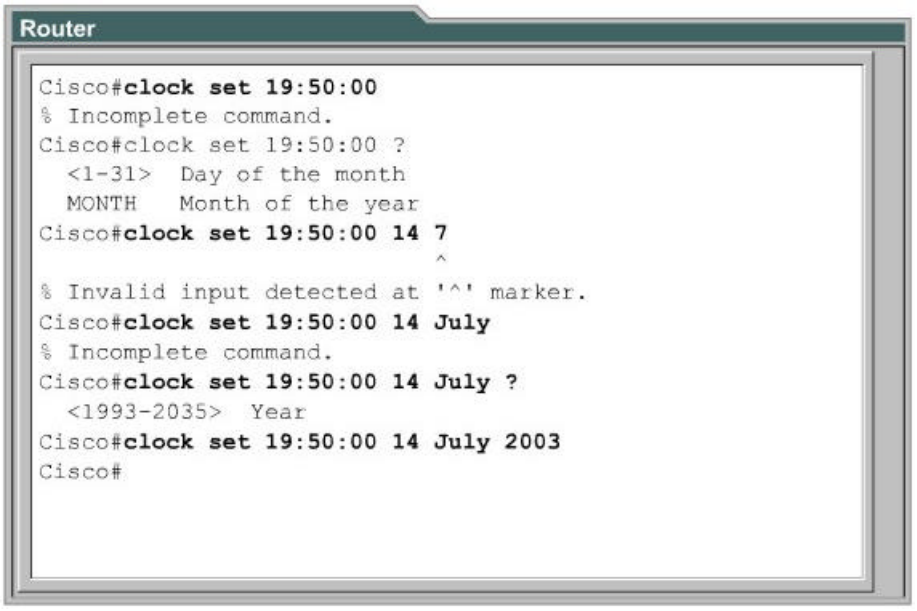
Degisik ekran çikislari Cisco IOS programinda yada router ayarlarina göre degisir.

Eger kullanici router saatini ayarlamak isterse fakat gerekli komutu bilemezse , dogru komut için yardim fonksiyonlarini kullanabilir. Asagidaki örnekle yardim fonksiyonlarinin nasil kullanilacagi gösterilmistir..



amacimiz routerin saatini ayarlamaktir. Komutu bilmedigimizi varsayiyoruz. Asagidaki adimlari uygulayacagiz.:

1. saat ayari için kullanilacak komut ? isareti ile bulunur. Yardim mönüsünden clock komutunun gerekli oldugu görülür
2. zaman degisiklikleri için sözdizim kontrol edilir.
3. sekilden gösterildigi gibi kullanilan zaman saat,dakika ,saniye olarak girilir. Asagidaki sekilde görülmektedir.



4. Ihtiyaç duyulan sistem ek bilgileri tamamlanir
5. **Ctrl-P** yada yukari tusu ile otomatik olarak komut tekrarlanir. Soru isareti kullanarak gerekli eklemeler yapilarak komut tamamlanir.
6. (^) iasreti ve yardim hatasi gösterilir. Problemin nerede oldugu gösterilir ve dogru sözdizim girilir.
7. Yil girilirken dogru sözdizim kullanirken Return ve Enter ile komutlar girilebilir.

2.2 Routerlarin Baslatilmasi

2.2.7 Gelistirilmis Düzenleme Komutlari

Kullanici arayüzüne “çogaltilmis düzenleme modu” yerlestirilmistir. Tus fonksiyonlarinin düzenlenmesi ayarlarini gerçeklestirirler. Kullanici komut satirinda düzenleme yaparlar. Tus düzenleri asagidaki sekilde gösterilmektedir. Komut satirinda düzeltmeler ve degisiklikler için kullanilirlar. Geçerli program ile otomatik olarak önceden düzenlenmislerdir. Kapalida olabilirler. Eger baslangiçta kapali ise yazilardaki etkilesim ile engellemelerle karsilasilabilir. Kapali ise bu moda düzenleme yapilamaz.

Command	Description
Ctrl-A	Moves to the beginning of the command line
Esc-B	Moves back one word
Ctrl-B (or right arow)	Moves back one character
Ctrl-E	Moves to the end of the command line
Ctrl-F(or left arrow)	Moves forward one character
Esc-F	Moves forward one word

Düzenleme komutlari , ekranda tek satira yayilmis komutlar için düzenlemeyi saglarlar. Kursor sag kenara gittigi zaman komut satiri on tane bosluk kadar sol tarafa gider. Ilk on karakter görünmeyebilir. Fakat kullanici geriye dogru ve komutun basina dogru ilerleyebilir. Geriye dönüs islemi **Ctrl-B** yada sol ok tusu ile yapilir. **Ctrl+A** kullaniciyi dogrudan hattin basina götürecektir.

Ekran çikis degisiklikleri , router ayarlarinda ve Cisco IOS programinda bulunur.

Ctrl+Z komutu ayarlar modunda geri gitmek için kullanilir. Kullanici yönetici moduna dönecektir.

2.2 Routerlarin Baslatilmasi

2.2.8 Router Komut Geçmisi

Kullanici arayüz geçmis bilgilerini sunmayi yada komutlarin kayitlarini girmek zorundadir. Bu özellik , özellikle karisik yada uzun komutlarin tekrar çagirilmasinda kullanilir. Komut geçmisi ile asagidaki görevleri yapabiliriz.

- Komut geçmisi alaninin büyüklügü ayarlanir.
- Komutlar yeniden çagrilir.
- Komut geçmisi özelligi kapatilabilir.

Komut geçmisi normalde açiktir ve sistem kayitlarindan on tane komut satirini geçmis hafizasinda bulundurabilir. Terminal oturumunda sistem kayitlari esnasinda komut satirindaki numaralar degiskendir. "**terminal history** size yada **history size** "komutu kullanilir. Komutlarda en fazla numaralandirma 256 ya kadardir.

Geri çagirma komutlari geçmis hafiza alaninda en son kullanilan komut ile baslarlar. **Ctrl-P** tusuna yada yukari ok tusuna sik sik basilarak birbirini izleyen eski komutlar tekrar çagrilir. Geçmis hafiza alaninda son kullanilan komutlar geri çagrilir. **Ctrl+P** ile yada yukari ok ile komutlar çagrildiktan sonra **Ctrl+N** e yada asagi tusuna basilarak bir sonraki yada bir önceki komutlar çagrilir.

Komutlar girilirken, kisaltmalar , tekil karakterler komut için girilebilir. **Tab** tusu ve arayüze giris tamamlanacaktir. Tab tusunun kolayligi görsel olarak taninmistir. Routerlar özel komutlarla tasalanirlar.

Bilgisayarlarda kopyalanabilir fonksiyonlar ve ek seçenekler mevcuttur. Hazirlanmis olan komut dizisi kopyalanmis veya güncel komut girisleri yerlestirilmis olabilir.

2.2 Routerlarin Baslatilmasi

2.2.9 Komut Satiri Hatalarinin Giderilmesi

Yapilan yanlislardan önce komut satiri hatalari meydana gelir. Eger komut kelimeleri dogru girilirse kullanici arabiminde hata göstergesi (^) yardimiyla hatalar önlenir. "^" sembolü , dogru komutlarin , kelimelerin komut sirasinin nasil oldugunu gösterir. Hata yeri gözlemleyici ve görsel yardim sistemleri saglayarak kullanicilara dogru hatasiz ve kolay bulucu bir yardim saglar.

Örnek:

Router#**clock set 13:32:00 23 February 93**
^

% Geçersiz giris tespit edildi .

(^) sembolü ve yardim yanitlari 93 de hata gösterdi. Dogru sözdizimi listelemek için, komut satirinda hatali olan yere soru isareti girilip enter tusuna basilir.

Router#**clock set 13:32:00 23 February ?**
<1993-2035> Year
Router#**clock set 13:32:00 23 February**

Yilin girilmesi ile dogru sözdizim yazilarak tekrar komut girilir.

Router#**clock set 13:32:00 23 February 1993**

Eger komut satirina dogru girildiyse ve dogru tusa basildiysa , yukari ok son komutu tekrar gösterebilir. Sagi ve solu kullanarak yanlisin nerede oldugu konusunda bilgi verilir. Eger ihtiyaç olan bazi komutlar silinme ihtiyaci duyulursa backspace tusuna basilir.

2.2 Routerlarin Baslatilmasi

2.2.10 show version Komutu

Show version komutu Cisco IOS programinin versiyonu hakkinda bilgileri görüntüler. Routerda çalistirilan geçerli bir komuttur. Ana çalisma ayarlarinda ve konfigürasyon kayitlarina eklenmis bir komuttur.

Asagida Show versiyon komutlarinin bazi özellikleri gösterilmistir:

- IOS versiyonu ve tanimlayici bilgileri
- ROM versiyon kayitlari
- Router çalisma zamani
- Geri baslatma metotlari
- Sistemin kalip dosyasi ve yeri
- Router platformu
- Konfigürasyon kayitlarin ayarlari

ÖZET

Asagidaki kilit noktalarinin anlasilmis olmasi saglanmalidir.

- IOS un amaçlari
- IOS un temel islemleri
- Çesitli IOS özeliklerinin belirtilmesi
- Router ile CLI oturumu için gerekli metotlarin belirtilmesi
- Kullanici ve yönetici modlarin birbirleri arasindaki farkliliklar
- Hyper Terminal oturumunu kurmak
- Router in içine erismek
- Komut arayüzünde yardim komutlarini kullanmak
- Komutlari kullanmayi çogaltmak
- Kayit komutlarini kullanmak
- Komut hatalarini düzeltmek
- Show version komutlarini kullanmak

BÖLÜM - 3

Genel Bakis

Ayarlari yapilan router karisik ag çalismalarinda görevlerini yerine getirirken zorluklarla karsilasabilir. Router ayarlari için baslatilan uygulamalarin hepsi zor degildir. Prosedürleri ve adimlari gerçeklestirmek için routerda pratikler yapilmalidir. Daha karisik konfigürasyonlarla karsilasildiginda daha az korkutucu olacaktir. Bu modülde routerin temel ayarlari yapilacaktir. Ayrica basit ayarlarla pratiklik kazanilacaktir.

Temiz , kolay anlasilabilir router ayarlari tüm ag yönetimlerinde amaç olarak belirlenmistir. Cisco IOS ayarlar dosyasina bilgi eklemek için yönetim araçlari saglar. Sadece becerikli programcilar her bir program adimi için dokümantasyon sunarlar. Ag yöneticileri imkanlari oldugu sürece agda baska insanlar benzer sorunlarla karsilastigi zaman zorlanmamalari için gerekli bilgileri sunarlar.

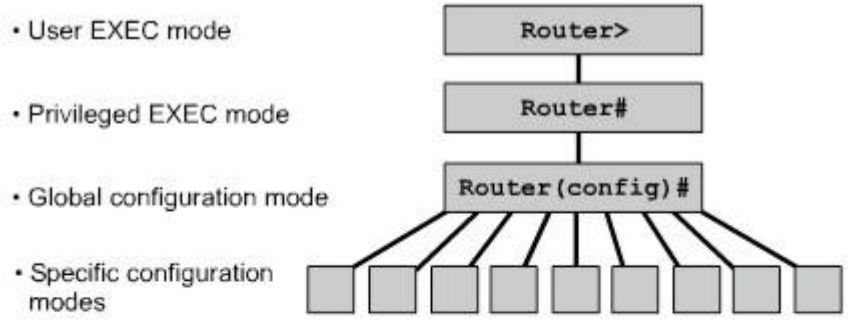
Bu modül tamamlandiginda asagidaki özellikler ögrenilecektir:

- Routerin ismi
- Sifreleri ayarlamayi
- Gösterilen komutlar gözden geçirilecek
- Seri arayüz konfigürasyonu
- Ethernet arayüz konfigürasyonu
- Routera degisiklikleri uygulamak
- Routera degisikliklerin kayit edilmesi
- Arayüz tanimlamalarinin konfigürasyonu
- Günlük mesajlarin ayarlari
- Kullanici tablo ayarlari
- Yedeklemenin ve dokümantasyonun anlam ve önemi

3.1 Router Konfigürasyonu

3.1.1 CLI Komut Modlari

Tüm arayüz komut satir ayarlarinin degisikligi Cisco routerlarda global modayken yapilir. Diger özel modlar üzerinde konfigürasyon degisiklikleri gereklidir. Fakat o özel modlarin hepsi global moda ayarlama yaparlar. Asagidaki sekilde global mod komutlarindan bazilari görülmektedir.



Configuration Mode	Prompt
Interface	`Router(config-if)#`
Subinterface	`Router(config-subif)#`
Controller	`Router(config-controller)#`
Map-list	`Router(config-map-list)#`
Map-class	`Router(config-map-class)#`
Line	`Router(config-line)#`
Router	`Router(config-router)#`
IPX-router	`Router(config-ipx-router)#`
Route-map	`Router(config-route-map)#`

global ayar mod komutlari routerda kullanilir. Yapilan ayarlamalarla tüm sisteme etki ederler. Belirtilen komutlar global moda girilir. Ve terminalden komutlar giris yapilir.

Router#**configure terminal**
Router(config)#

Global mod , global config olarak kisaltilmis olarak kullanilabilir. Global moddan birkaç moda geçis yapilabilir.

- Arayüz modu (Interface mode)
- Hat modu (Line mode)
- Router modu (Router mode)
- Ana arayüz modu (Subinterface mode)
- Kontrol modu (Controller mode)

Özel modlar kullanildigi zaman router geçerli router konfigürasyon modunda degisiklikler meydana gelecektir. Belirli modlardan islemler korunur yada bazi degisiklikler sadece arayüzlere yapilacaktir.

"**exit**" ile özel bir konfigürasyon modundan global moda geri dönülebilir. **Ctrl+Z** tusuna basildigi zaman bulunulan konfigürasyon modundan ayrilir ve yönetici moda geri döner.

3.1 Router Konfigürasyonu

3.1.2 Router Isminin Konfigürasyonu

Konfigürasyon yapilirken ilk olarak routera bir isim girilmelidir. Bunu yapmak için global moddayken asagidaki komut girilmelidir.

Router(config)#**hostname Firat**
Firat(config)#

Enter tusuna bakildiktan sonra varsayilan sunucu isminde degisiklik olur. Girilen isim sunucunun ismi olur. Örnek olarak biz routerin ismini Firat yaptik.

3.1 Router Konfigürasyonu

3.1.3 Roter Sifrelerinin Konfigürasyonu

Sifreler routerlara olan erisimi sinirlandirirlar. Sifreler, konsol hat ve sanal terminaller için konfigürasyonda daima olmalidirlar. Yönetici moda erisimlerde kullanilirlar. Konfigürasyon dosyasina yapilacak degisiklileri sadece sifreyi bilen kullanicilar müdahale edebilirler.

Asagidaki örnekteki komutlar kullanilarak ayarlama yapilabilir fakat konsol hattinda sifrelendirme yapilmasi önemli tavsiye edilir.

Router(config)#**line console 0**
Router(config-line)#**password** <*sifre*>
Router(config-line)#**login**

Uzaktan erisim lerde yönlendirme telnet ile yapilir. Tipik Cisco routerlar , numaralandirilmis bes tane sanal terminal baglantisina izin verirler. Diger donanim platformlari , VTY baglantilarinda diger numaralara bakarlar. Tüm baglanti hatlari için sik sik ayni sifre kullanilirlar. Fakat bazen bir hat , eger diger dört hat baglantilari kullaniliyorsa geri düsebilir. VTY hatlarda asagidaki komutlar kullanilarak sifre ayarlanmis olur.

Router(config)#**line vty 0 4**
Router(config-line)#**password** <*sifre*>
Router(config-line)#**login**

Açik sifre ve açik gizlilik kullanilarak yönetici moda erisimleri sinirlandirir. Açilmis sifre sadece gizlilik açilmadigi zaman kullanilir. Açik gizliligin daima ayarlanmasi ve kullanilmasi tavsiye edilir. Asagida sifreyi açmak ile ilgili örnekler görülmektedir.

Router(config)#**enable password** <*sifre*>
Router(config)#**enable secret** <*sifre*>

Bazen sifreler için istenmeyebilir. **show running-config** yada **show startup-config** komutlarindan çikis görülebilir. Bu komut konfigürasyon çikisinda sifrelerin özel olarak paketlenmesinde kullanilir.

Router(config)#**service password-encryption**

"service password-encryption" komutu sifrelerin geri çözümlenmesinde çözümlemeyi etkisiz kilar. "**enable secret <password>** " komutu çözümleme için güçlü MD% algoritmasini kullanir.

Console Password

```
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password cisco
```

Virtual Terminal Password

```
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password cisco
```

Enable Password

```
Router(config)#enable password san-fran
```

Perform Password Encryption

```
Router(config)#service password-encryption
(set passwords here)
Router(config)#no service password-encryption
```

3.1 Router Konfigürasyonu

3.1.4 show Komutlarinin Incelenmesi

Show komutlari aksakliklari gidermek için ve routerda dosyalari gözden geçirmek için kullanilir. Yönetici ve kullanici modlarda "**show ?**" komutu girildiginde show komutlari listelenir. Kullanici moda göre yönetici moda daha fazla show komutu listelenir.

- **show interfaces** – Routerda tüm arayüzler için tüm istatistikleri görüntüler. "show interface" komutu girildigi zaman arayüzleri ve port numaralari izlenir. Örnegin:

Router#**show interfaces serial 0/1**

- **show controllers serial** – Arayüz donaniminin özel bilgilerini görüntüler
- **show clock** – Routerin zaman ayarlarini gösterir
- **show hosts** – Sunucu isinlerinin ve adreslerinin kayitlarini listeler
- **show users** – Router a hangi kullanicilarin baglandigini listeler
- **show history** – Girilen komutlarin geçmisini görüntüler

- **show flash**– Flash hafiza hakkindaki bilgileri vehangi ISO dosyasinin kayitli oldugunu gösterir
- **show version** – Router hakkindaki bilgileri ve RAM de çalisan ISO hakkindaki bilgileri görüntüler
- **show ARP** – Router daki ARP tablosunu görüntüler
- **show protocol** – Üçüncü katman konfigürasyonunun arayüzünü görüntüler
- **show startup-configuration** – NVRAM deki konfigürasyonun nerede kayitli oldugunu gösterir
- **show running-configuration** – RAM deki geçerli ayarlari görüntüler.

3.1 Router Konfigürasyonu

3.1.5 Seri Arayüz Konfigürasyonu

Seri arayüz , sanal terminal hat araciligi ile yada konsoldan ayarlanabilir. Ayarlarin yapilabilmesi için asagidaki adimlarin uygulanmasi gerekir

1. Global moda girilir
2. Arayüz moda girilir
3. Subnet makesi ve arayüz adresi girilir
4. Eger DCE kablo ile baglanti yapildiysa saat hizi (clock rate) ayarlanir. Eger DTE kablo ile yapildiysa bu adim atlanir.
5. Arayüze dönülür

Her seri arayüz baglantisinda IP adres ve subnet makesi olmalidir. Ancak bu sayede arayüz IP paketlerini yönlendirebilir. Asagidaki komut kullanilarak IP adresi konfigüre edilir.

Router(config)#**interface serial 0/0**
Router(config-if)#**ip address** <*ip adres*> <*netmaskesi*>

Seri arayüz , baglantilarda zamanlama kontroünü saat sinyali ile yapar. En çok DCE araci CSU gibi saat sinyali sunacaktir. Normalde Cisco routerlar DTE araçlaridir. Fakat onlar ayarlanabilir DCE araçlaridir.

Seri linkte diret olarak yapilan baglantidir. Laboratuar ortaminda DCE nin yanimizda oldugunu farz edelim DCE saat sinyali sunmaktadir. Saatin açilmasi ve hizi "**clock rate**" komutu ile yapilir. Mevcut saat hizi saniyedeki bit sayisidir. Saat hizi oranlari standart olarak sunlardir:1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, yada 4000000. Bazi bit hizlari seri arayüzlerde mevcut olmayabilir.

Normalde arayüzler kapalidirlar. Arayüzleri açmak için "**no shutdown"** komutu girilmelidir. Arayüz bakim nedeniyle yönetimsel olarak kapanabilir yada **shutdown** komutu ile arayüz önceden kapatilmis olabilir. Laboratuar ortaminda saat hizi 5600 bit/sn olarak ayarlanip kullanilacaktir. Saat hizinin ayarlanmasi ve seri arayüzün açilmasi ile ilgili komut asagidaki örnekte gösterilmistir.

Router(config)#**interface serial 0/0**
Router(config-if)#**clock rate 56000**
Router(config-if)#**no shutdown**

In the following commands, the *type* argument includes serial, ethernet, fastethernet, token ring, and others:

```
Router(config)#interface type port
Router(config)#interface type slot/port
```

The following command is used to administratively turn off the interface:

```
Router(config-if)#shutdown
```

The following command is used to turn on an interface that has been shut down:

```
Router(config-if)#no shutdown
```

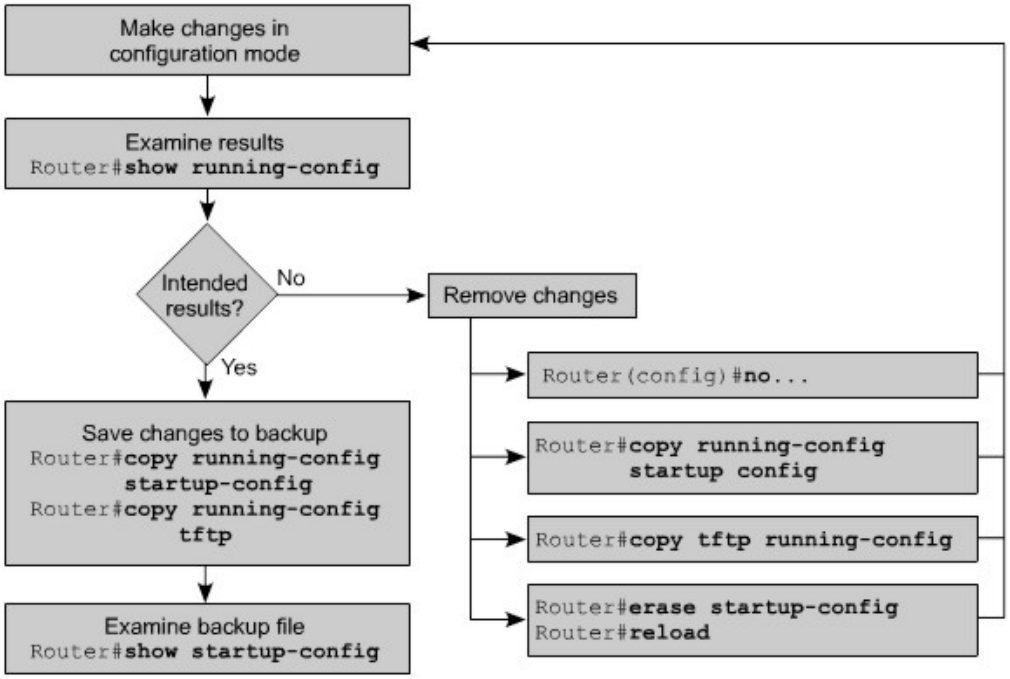
The following command is used to quit the current interface configuration mode:

```
Router(config-if)#exit
```

3.1 Router Konfigürasyonu

3.1.6 Eklemelerin Tasimalarin Degistirmelerin Yapilmasi

Eger konfigürasyon tekrar bir ayarlama istiyorsa uygun moda gidilir dogru komutlar girilir. Örnek verecek olursak, eger arayüz açilmak isteniyorsa global moda girilir. Oradan arayüz moda (interface mode) girilir. Burada ise **no shutdown** komutu girilir.



Degisiklikleri dogrulamak için **show running-config** komutu kullanilir. Bu komut geçerli olan konfigürasyonu gösterecektir. Eger istedigimiz degisiklik görüntülenmiyorsa asagidaki adimlar izlenir:

- Konfigürasyon komutu tarafindan yayinlanmamis olabilir.
- NVRAM den orijinal konfigürasyon dosyasini sistemden tekrar çagrilir
- TFTP servisinden konfigürasyon dosyasi arsive kopyalanir.
- **erase startup-config** komutu ile konfigürasyon dosyasi baslangiçtan kaldirilir. Router tekrar baslatilir. Ayar (setup) moda girilir.

NVRAM den baslangiç konfigürasyon dosyasina geçerli ayarlar kaydedilir. Yönetici moda girilip asagidaki komut çalistirilir.

Router#**copy running-config startup-config**

3.1 Router Konfigürasyonu

3.1.7 Ethernet Arayüzünün Konfigürasyonu

Ethernet arayüzü , konsoldan yada sanal terminalden ayarlanabilir.

Her Ethernet arayüzü bir ip adresine ve subnet maskesine sahip olmalidir. Böylece ip paketlerinin yönlendirilmesi saglanabilir.

Ethernet Arayüzünün konfigürasyonu için su adimlar izlenmelidir:

1. Global moda girilir (global configuration mode)
2. Arayüz konfigürasyon moduna girilir (interface configuration mode)
3. Ip adres i ve subnet maskesi girilir
4. Arayüz aktif hale getirilir.

Normalde arayüzler kapalidirlar yada pasif haldedirler. **no shutdown** komutu ile geri açilirlar yada aktif hale getirilirler. Eger arayüz yönetimsel olarak kapatilmak isteniyorsa **shutdown** komutu kullanilarak arayüz kapatilmis olur.

3.2 Konfigürasyonun Tamamlanmasi

3.2.1 Konfigürasyonu Standartlarinin Önemi

Organizasyon içerisinde konfigürasyon dosyalari için standartlari yükseltmek önemlidir. Bunun için konfigürasyonun numaralarla kontrol edilmesi gerekir. Dosyalar nasil kayit edilecek? Nerede kayitlar tutulacak. Bu gibi sorularin halledilmesi gerekir.

Standart, kurallarin yada prosedürlerin gerçeklestirilmesidir. Her ikisi de genis landa kullanilir. yada en basinda belirlenir. Organizasyonda standartlar olmazsa olmazlardandir. Standartlarin bulunmadigi serviste agda karsiligin olmasi kaçinilmazdir.

Ag yönetim düzenlemesi yapilirken standart destekli olmalidir. Konfigürasyon , güvenlik , performans ve ag için uygun adreslemeler yapilmalidir. Aglarda olusabilecek karisikliklara en uygun sekilde yardim edebilmesi için standartlar olusturulmustur. Planlanmamis kesilmelerin miktari ve ag performansinin çakismalara maruz kalmasi gibi sorunlarin giderilmesinde standartlara basvurulmustur.

3.2 Konfigürasyonun Tamamlanmasi

3.2.2 Arayüz Tanimlamalari

Özel ag parçasi , devre numarasi yada uzaktaki router a ait önemli bilgi kimlikleri bira arayüz tanimlamasinda kullanilir. Arayüzdeki tanimlamalar , agdaki kullanicilarin arayüz hakkinda özel bilgileri hatirlamalarinda yardimci olabilir. Ne tip bir arayüz servisi kullanildigi hakkinda bilgiye sahip olunmus olur


```
Tokyo(config)#interface e 0

Tokyo(config-if)#description Engineering LAN, Bldg. 18
```

Tanimlama arayüz hakkinda yorumlarin yapildigi yerdir. Router hafizasinda bulunan konfigürasyon dosyasinda bulunur. Tanimlama , routerin operasyonuna etki yapmaz. Her arayüze standart olarak eklenirler. Devre kimlikleri , arayüzlere olan baglantilar yada diger araçlarin yerleri hakkindaki bilgilerin tutulmasi amaçlanmistir. Problemlerin çözümünün daha hizli olmasi için ve arayüz problemlerinin anlatilmasinda personelin daha iyi anlamasi için tanimlamalar kullanilir.

3.2 Konfigürasyonun Tamamlanmasi

3.2.3 Arayüz Konfigürasyonunun Tanimlanmasi

Arayüz tanimlamasinin konfigürasyonu global moda girilerek yapilir. Global konfigürasyon moddayken arayüz konfigürasyon moda girilir. Tanimlamalar için asagidaki adimlar gerçeklestirilir.

Prosedür adimlari:

1. Global konfigürasyon moda girilir ve **configure terminal** komutu girilir.
2. Özel arayüz moduna girilir. (Örnegin : **interface ethernet 0**)
3. Tanimlama bilgileri girilir. (Örnegin: Firat 13)
4. Ctrl+Z komutu kullanilarak yönetici moda geri dönülür.
5. **copy running-config startup-config** komutu kullanilarak NVRAM e konfigürasyon degisiklikleri kayit edilir.

Asagida bir arayüzün nasil tanimlanmasi gerektigine dair örnek görülmektedir:

interface Ethernet 0
description LAN Muhendislik, Bilg.2
interface serial 0
description FIRAT network 1, Circuit 1

3.2 Konfigürasyonun Tamamlanmasi

3.2.4 Karsilama Mesajlari

Tüm ag kullanicilarinin mesajlari görebilmeleri için giris mesaj bölümü görüntülenir.
Giris mesajlari herhangi birisi tarafindan görülebilir. Buyüzden giris mesajlari dikkatli seçilir. Kisiye özel mesajlar degildirler. Routera herhangi birisi için karsilama olarak " hos geldiniz " mesaji girilmesi muhtemelen uygun degildir.

Açilis mesaji , yetkisi olmayan kisilerin sisteme girmeye çalismamali için uyari nitelikli mesaj olmalidir. " Bu güvenli bir sistemdir sadece yetkililer girebilir " gibi bir mesaj istenmeyen ziyaretçilere yada geçersiz kullanicilara sunulabilir.

3.2 Konfigürasyonun Tamamlanmasi

3.2.5 Günlük Mesajlarin Konfigürasyonu

Tüm terminal baglantilarinda günün mesaji görüntülenebilir.

Günün mesajini ayarlamak için global ayarlar moduna girilmelidir. Burada " **banner motd "** komutu kullanilir. Daha sonra # isareti basta ve sonda olmak üzere araya mesaj yazilir.

Asagidaki adimlarda günün mesajinin nasil görüntülenecegi ve nasil yapilacagi gösterilmektedir.

1. Global ayar moduna , **configure terminal** komutu kullanilarak girilir.
2. **banner motd # Günün mesaji yazilir #** komutu ile günün mesaji girilmis olur.
3. Degisiklikleri kaydetmek için **copy running-config startup-config** komutu girilir.

3.2 Konfigürasyonun Tamamlanmasi

3.2.6 Host Isim Çözümlemesi

Bir bilgisayar sisteminde sunucu ismi ile ip adresleri verilirken sunucu isim çözümlemesi gerçeklestirilir.

Diger IP ve ag araçlari ile baglantilarda sunucu isimleri kullanilir. Router lar ip adresleri ile sunucu isimlerini iliskilendirebilmelidirler. Sunucu isimlerini listelerler ve onlari ip adresleri ile iliskilendirerek sunucu tablosuna kayit ederler.

Asagidaki örnekte ip adresleri ve bunlarla iliskilendirilen host isimlerinin nasil yapilacagi gösterilmektedir.

The following is an example of the configuration of a host table on a router:

```
Router(config)#ip host Auckland 172.16.32.1
Router(config)#ip host Beirut 192.168.53.1
Router(config)#ip host Capetown 192.168.89.1
Router(config)#ip host Denver 10.202.8.1
```

Ag organizasyonlarinda tüm araçlara sunucu tablosu yerlestirilebilir. Her bir tekil ip adresi kullanici ismi ile iliskilendirilir. Cisco IOS programinda komutlarda kullanabilmek için sunucu isimlerini ve adreslerini haritalarini önbellekte korur. Isimleri adreslere çevirirken bu önbellekte hizlica yapar.

Sunucu isimleri , DNS isimlerinden farkli olarak sadece konfigürasyon edilmis routerlarda belirtilirler. Sunucu tablosu ag yöneticilerine izin verilmistir. Sunucuya uzaktan baglanirken yada Telnet e sunucunun ismi yada ip adresinden birisi yazilarak ag yöneticisinin ag tablosuna erismesine izin verilmistir.

3.2 Konfigürasyonun Tamamlanmasi

3.2.7 Host Tablolarinin Konfigürasyonu

Adreslere isim atarken ilk olarak global konfigürasyon moduna girilir. **ip host** komutu ile hedeflenen isim ve bu isimlerin ip adresleri girilir. Bu haritalarda arayüz ip adreslerin her birinin isimleri bulunur. Sunucuya ulasirken telnet yada ping konutlari router in ismi yada ip adresi kullanilarak girilir.

Asagida bir sunucu tablosunun hazirlanma adimlari görülmektedir.

1. Routerda global konfigürasyon moduna girilir.
2. ip host “router ismi yada ip adresi” her bir routerda arayüz ile girilir.
3. agdaki routerlarin hepsi girilerek devam edilir.
4. NVRAM e konfigürasyon kayit edilir.
5.

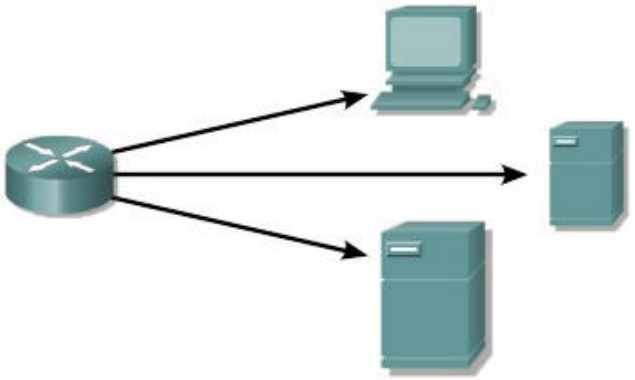
3.2 Konfigürasyonun Tamamlanmasi

3.2.8 Yedekleme ve Dokümantasyon Konfigürasyonu

Agin nasil davranacagi, network araçlarinda konfigürasyonda belirlenir. Araç konfigürasyonunda gerçeklestirilen yönetim asagidaki özellikleri kapsamaktadir.

- Çalisan araçlarda konfigürasyon dosyalarinin listelenmesi ve karsilastirilmasi
- Ag sunucularindaki konfigürasyon dosyalarinin kayit edilmesi
- Program yüklemelerinin ayarlanmasi ve güncellenmesi

Konfigürasyon dosyalari problem gerçeklestigi zaman yedek dosyalardan yüklenebilir olmalidirlar. Ag sunucularinda , TFTP sunucuda yada güvenli disk ortaminda saklanabilirler. Dokümantasyon



Save configuration files to a:
- TFTP Server
- Network Server
- Disk in a safe place

3.2 Konfigürasyonun Tamamlanmasi

3.2.9 Kopyala , Yapistir, Düzenle Konfigürasyonu

Konfigürasyonun güncel kopyasi TFTP sunucuda saklanabilir. **copy running-config tftp** komutu kullanilarak kayit islemi gerçeklestirilir. Asagidaki adimlarda TFTP sunucuya nasil kayit yapilacagi gösterilmektedir.

Adim 1 **copy running-config tftp** komutu girilir.

Adim 2 Hosta konfigürasyon dosyasinin kayit edilecegi yerin ip adresi girilir.

Adim 3 Konfigürasyon dosyasina bir isim verilir.

Adim 4 Her seferinde seçileri evet ile onayla

Bir ag sunucusuna ruoter in o anki kullandigi ayarlar kayit edilebilir. Bunu yapmak için asagidaki adimlar gerçeklestirilir:

1. Konfigürasyon moddayken **copy tftp running-config** komutu girilir.
2. Sistem konsolunda ag konfigürasyon dosyasi yada host seçilir. Dosya , agdaki terminal sunuculara ve tüm routerlara komutlarla eklenir. Sistem konsolunda dosyanin yüklenecegi yerin ip adresi girilir. Örnek verecek olursak 131.108.2.155 adresindeki TFTP sunucudan router ayarlanir.
3. sistem konsolunda dosyaya ya bir isim girilir yada varsayilan isim uygulanir. Varsayilan dosya ismi genelde ag konfigürasyonu için **host ismi**-config veya **network-config** tir. DOS ortaminda , dosya isimleri sekiz karakter isim ve üç karakter dosya uzantisi ile sinirlidirlar. Örnegin **router.cfg**. dosya ve TFTP sunucu adresleri sitem kaynaklarinda mevcuttur.

Router ayarlari routerda yazilar kopyalanarak diske kayit edilebilir. Daha sonra bir harddiske yada cd ye kayit yapilabilir. Eger dosyanin routera geri kopyalanmasi ihtiyaç hissedilirse terminal emülatör programinin edit kismina kopyala yapistir yöntemi ile roture yüklenir.

Özet

Bu bölüm de route konfigürasyonu kisaca özetlenmistir.

Router in sahip oldugu modlar:

- Kullanici modu (User EXEC mode)
- Yönetici modu (Privileged EXEC mode)
- Global konfigürasyon modu (Global configuration mode)
- Diger konfigürasyon modlari

Arayüz komut satirinda konfigürasyonda degisiklik yapmak için kullanilan komutlar:

- Host ismi ayarlari
- Sifre ayarlari
- Arayüz ayarlari
- Konfigürasyonun düzenlenmesi
- Konfigürasyonlarin gösterilmesi

Asagidaki gösterilen konular anlasilmistir.

- Bir organizasyonda verimli bir ag olusturmak için gerekli konfigürasyon standartlari gerektigi
- Arayüz tanimlamalari aga yardim etmek için önemli bilgileri içerebilirler.
- Karsilama mesajlari ve günlük mesajlari routera karsilama bilgileri ile kullanicilara sunulur.
- Host isim çözümlemeleri , adresleri isimlere çevirerek router a daha hizli erisimi saglar.
- Konfigürasyon kayitlari ve dokümanlari ag operasyonlarina müdahalede son derece önemlidir.

BÖLÜM - 4

Genel Bakis

Bazen ag yöneticileri ag dokümantasyonunda bazi yerlerin tamamlanmadigini yada yanlis yaptigini karsilastirirlar. Cisco Discovery Protokolü (CDP) bu gibi sorunlarda yararli olabilir. Çünkü agda temel resimlerle yardim edebilirler. CDP , medya ve protokolden bagimsizdir. Cisco komsu kesifler için tescilli protokol kullanir CDP sadece yakinlardaki direkt baglanti bilgilerini gösterecektir. Fakat yinede güçlü bir araçtir.

Çogu durumda router baslangiçta konfigüre edilir. Zordur yada ag yönetimi için konfigürasyon degisiklikleri yada diger aktiviteler için routera yapilacak direkt baglantilarda rahatsiz edicidir. Telnet , TCP/IP yarsinda bir uygulamadir. Konfigürasyon için router komut hatti arayüzüne uzaktan yönetim için kullanilirlar. Profesyonel aglar için zorunlu bir araçtir.

Bu bölüm tamamlandigi zaman asagidaki konular tamamlanacaktir:

- CDP yi açmayi kapamayi
- **show cdp neighbors** komutunu kullanmayi
- yakinlardaki hangi araçlarin hangi yerel arayüze baglanacaginin tanimlanmasi
- Yakinlardaki araçlarin CDP kullanarak toplu ag adreslerinin hakkindaki bilgilerini
- Tenet baglanti kurmayi
- Telnet baglantilarini dogrulamayi
- Telnet oturumundan çikmayi
- Telnet oturumunu askiya almayi
- Alternatif baglantilarin testleri
- Aksakliklari uzaktan terminal baglantilar ile düzeltme

4.1 Yakindaki Cihazlarin bulunmasi ve Baglanilmasi

4.1.1 CDP ye Giris

Cisco Discovery Protocol ü ikinci katmanda düsük medya özellikli baglantilari olan ve üst ag katman protokolüdür. CDP , yakinlardaki bilgisayarlar hakkinda elde edilmis bilgileri kullanir. Cihazlarin baglanti tipleri , router arayüzleri , onlara olan baglantilar gibi bilgileri, baglanti yapmak için kullanilan arayüzler ve cihazlarin model numaralari gibi bilgileri bulundururlar.

CDP , medyadan ve protokolden bagimsizdir. Tüm Cisco araçlarinda çalisirlar.

CDP versiyon 2, protokolün en son kismidir.

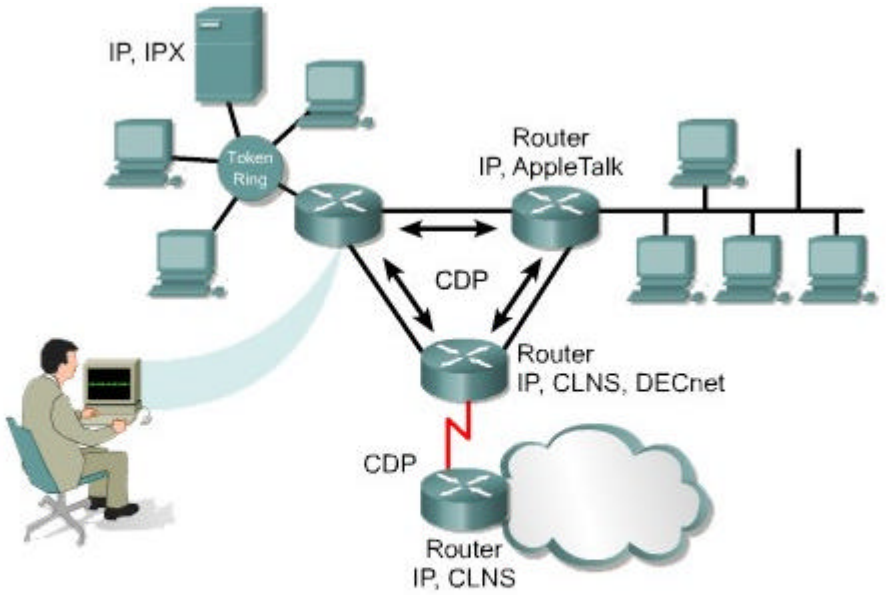
Cisco cihazlari açilis yaparken , CDP otomatik olarak çalisir. CDP nin çalismasi ile yakinlardaki cihazlar hemen taranir. CDP data iletim (data link) katmaninda çalisirlar. Diger sistemler hakkindaki bilgileri ögrenirler. Bezende diger ag katman protokollerini kullanabilirler.

Ikili routerlara , CDP periyodik mesajlari göndermek her bir cihaz ayri ayri konfigüre edilir. Her bir cihaz , SNMP mesajlarini dönüstürürken en az bir adres bildirirler. Ayrilma zamani yada bekleme zamani gibi bilgileri atmadan önce CDP bilgilerinde cihazla tarafindan çevrilerek tutulurlar. Ek olarak her bir cihaz , yakindaki cihazlar hakkinda periyodik olarak gönderilen CDP mesajlarini dinlerler.

4.1 Yakindaki Cihazlarin bulunmasi ve Baglanilmasi

4.1.2 CDP ile Bilgilerin Elde Edilmesi

Yerel ag cihazlarina direkt baglantida , tüm Cisco cihazlarini bulmak için ilk olarak CDP kullanilir. **show cdp neighbors** komutu kullanilarak yerel cihazdaki CDP güncellemeleri görüntülenir.



Single command summarizes protocols and addresses on target (for example, neighboring Cisco router)

Yukaridaki sekilde ag yöneticisine bilgilerin CDP ile nasil toplandigi gösterilmektedir. Her bir router CDP yi çalistirarak yakinindaki router ile protokol bilgilerini degis tokus ederler. Ag yöneticisi yerel routera konsol araciligi ile baglanarak degis tokus edilmis CDP bilgilerini görüntüleyebilir.

Yönetici , **show cdp neighbors** komutunu kullanarak routera direkt baglanarak ag hakkindaki bilgileri görüntüler. CDP yakinlarindaki cihazlarin hakkindaki bilgileri TLVs e ileterek sunarlar.

TLVs cihazi , **show cdp neighbors** komutu ile asagidakileri görüntüleyebilir:

- Cihazini kimligi
- Yerel arayüzü
- Durma zamani
- Yetenegi
- Platformu
- Port kimligi
- VTP Alan Ismi Yönetimi (CDPv2 only)
- Yerel VLAN (CDPv2 only)
- Full/Half-Duplex (CDPv2 only)

Not: eski routerlarda yöneticilerin routera konsoldan direkt olarak baglanmasi mümkün olmayabilir. Bu cihazlar hakkindaki CDP bilgilerine , ag yöneticisi routera telnet araciligi ile direkt olarak baglanabilir.

4.1 Yakindaki Cihazlarin bulunmasi ve Baglanilmasi

4.1.3 CDP nin Bakimi Izlenmesi Yürütülmesi

Asagidaki komutlari kullanarak VDP bilgileri görüntülenebilir.

- **cdp run**
- **cdp enable**
- **clear cdp counters**
- **show cdp**
- **show cdp entry {*|*device-name*[*][protocol | version]}**
- **show cdp interface [type number]**
- **show cdp neighbors [type number] [detail]**

cdp run komutunu kullanarak routerda CDP açilir. Normalde CDP açik varsayilir. CDP enable komutu , belirli arayüzdeki CDP yi açar. Cisco IOS 10.3 ve daha üst versiyonda tüm arayüzlerde CDP bilgilerinin gönderilmesi çevrilmesi açik halde gelir.

4.1 Yakindaki Cihazlarin bulunmasi ve Baglanilmasi

4.1.4 Çevrenin Ag Haritasinin Olusturulmasi

CDP çerçeveleri küçük olabilir. Yakinlardaki Cisco cihazlari hakkindaki bilgilere erisirken ugrasabilir.

Bu bilgiler cihaz baglantilarinin ag haritasini olusturarak kullanabilir. Cihazlar yakinlarindaki diger cihazlari telnet baglanti kullanarak kesfetmek için **show cdp neighbors** komutunu kullanirlar.

4.1 Yakindaki Cihazlarin bulunmasi ve Baglanilmasi

4.1.5 CDP nin Kapatilmasi

CDP yi kapatmak istedigimizde , global moddayken **no CDP run** komutunu girmek yeterlidir. Eger CDP kapaliysa arayüzler CDP için açilamiyacaktir.

Asagidaki örnekte CDP komutlarinin nasi kullanilacagi konusunda ufak bir örnek görülmektedir.

Rt1

```
Rt1#show cdp
Global CDP information
   Sending CDP packets every 60 seconds
   Sending a holdtime value of 180 seconds
   Sending CDPv2 advertisements is enabled
Rt1#configure terminal
Enter configuration commands, one per line. End with
 CNTL/Z
Rt1(config)#no cdp run
Rt1(config)#^Z
Rt1#show cdp
%CDP is not enabled
Rt1#configure terminal
Enter configuration commands, one per line. End with
 CNTL/Z
Rt1(config)#cdp run
Rt1(config)#^Z
```

Cisco IOS 10.3 ve yukarisi versiyonlarda CDP bilgilerinin çevrilmesi ve gönderilmesinde tüm arayüzlerde normalde açiktir. Bazen eszamanli olmayan arayüzlerde CDP kapali olarak gelebilir. Eger kapaliysa arayüz konfigürasyon modundayken **CDP enable** komutu ile açilir. Özel bir arayüzde açildiktan sonra CDP kapatilmak isteniyorsa **no CDP enable** komutu kullanilir. Bunun için yine arayüz konfigürasyon modunda olunacagi unutulmamalidir.

4.1 Yakindaki Cihazlarin bulunmasi ve Baglanilmasi

4.1.6 CDP Komutlari

Asagidaki komutlar kullanilarak versiyon gösterme, güncelleme bilgileri , tablolar , ve trafik gibi islemler gerçeklestirilebilir:

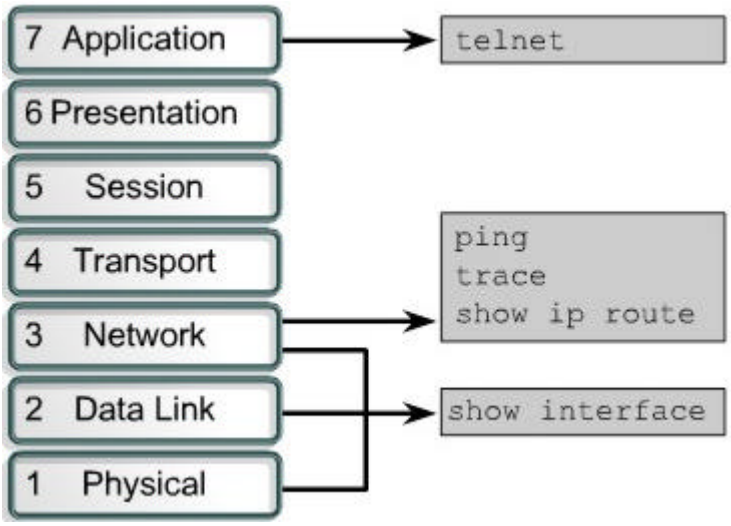
- **clear cdp table** : Yakindakiler hakkinda bilgilerin tutuldugu CDP tablosunu siler
- **clear cdp counters** : Trafik sayaçlarini sifirlar
- **show cdp traffic :** Trafik sayaçlarini, gelen giden kaybolan paket sayilarini gösterir
- **show debugging :** Ayiklanmis türlerin bilgilerini görüntüler
- **debug cdp adjacency :**Yakindakilerin CDP bilgileri
- **debug cdp events** : CDP olaylarini gösterir
- **debug cdp ip** : CDP IP bilgilerini
- **debug cdp packets** : CDP paketleri ile ilgili bilgileri
- **cdp timer :** Cisco IOS programina yollanan CDP güncellemeleri
- **cdp holdtime** : güncelleme paketlerinin gönderim süresi
- **show cdp** : Zaman ve bekleme sürelerini gösterir

4.2 Uzaktaki Cihazlar Hakkinda Bilgi Elde Etmek

4.2.1 Telnet

Telnet , TCP/IP protokolünü kullanan sanal bir terminal protokolüdür. Uzaktaki hostlara baglanti yapmak için kullanilirlar. Telnet sunucularinin ag terminallerine yada uzaktan erisim yapabilme yetenekleri vardir. Telnet , IOS EXEC komutunu kullanarak uygulama katmaninda kaynak ve hedef arasini dogrular.

Telnet OSI modelinin uygulama katmaninda çalisir. Data istemcileri yada sunucularda dogru ve düzgün bir teslimi TCP de garantili bir sekilde gerçeklestirir.



Routerlar , telnet oturumlarini çoklu olarak ayni anda gerçeklestirebilirler. Sifirdan dörde kadar olmak üzere bes tane VTY yada telnet hatti kullanirlar. Gelen bes oturumu ayni zamanda alabilir.

Uygulama katman baglantilari telnette dogrulanir. Ag cihazlarina uzaktan baglanti için genelde telnet kullanilir. telnet basit ve evrensel bir programdir.

4.2 Uzaktaki Cihazlar Hakkinda Bilgi Elde Etmek

4.2.2 Telnet Baglantisini Kurmak ve Dogrulamak

Telnet komutu ile bir Cisco cihazindan digerine telnet baglanti gerçeklestirilebilir. **connect** yada **telnet** komutunun girilmesi gerekli degildir. Uzaktaki routerin host isminin yada ip adresinin girilmesi yeterlidir. Telnet oturumunu sonlandirmak için **exit** yada **logout** komutlari girilir.

Initiate a session

```
Denver>telnet paris
```

End a session

```
Paris>exit
```

Suspend a session

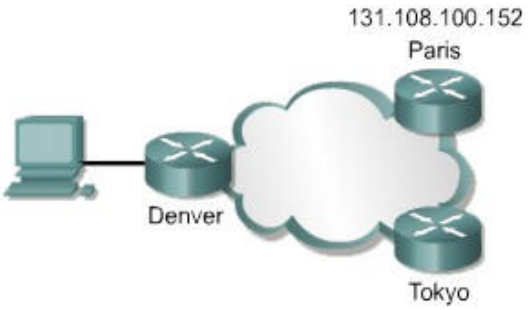
```
Paris><Ctrl><Shift><6><x>
Denver>
```

Resume a session

```
Denver><Return>
```

Disconnect a session

```
Denver>disconnect paris
```



Display Session

```
Denver#show sessions
 Conn    Host    Address            Idle    Conn Name
 1       Paris   131.108.100.152    0       Paris
 2       Tokyo   126.102.57.63      0       Tokyo
```

Telnet oturumunu birkaç sekilde baslatmak mümkündür. Asagidaki örnekteki gibi programi çalistirabiliriz.

Denver>**connect paris**
Denver>**paris**
Denver>**131.108.100.152**
Denver>**telnet paris**

Telnet in bir yere isimle baglanabilmesi için DNS e erisiminin tada host isimleri tablosuna sahip olmasi gerekir. Aksi halde uzaktaki routerin ip adresi girilmelidir. Eger telnet araciligi ile bir routerdan diger bir routera baglanabiliyorsa ag baglantisinin ana testleri basarilidir. Bu islem kullanici yada yönetici moddayken geçeklestirilebilir.

Eger bir roterdan diger bir router erismek için TCP/IP uygulamasi ile uzaktaki routera ulasilabilir. Üst katman uygulamalari basariyla yapilabiliyorsa basarili bir telnet baglantisi yapilmistir demektir.

Bir router a telnet baglantisi yapilirken baska routera yapilamiyorsa muhtemelen adreslemesinde , isimlendirmede yada erisim izinleri nedeniyle baglanti gerçeklesemiyordur. Böyle durumlarin olmasi olagandir. Oldugunda bir sonraki adim olarak tekrar **ping** atilir. Ping ag katmaninda uçtan uca baglantilari test etmek amaçli kullanilir.

telnet tamamlandiktan sonra host tan çikilir. Telnet baglantisi , exit komutu girildigi zaman yada birkaç dakika kullanilmadigi zaman otomatikman sonlandirilir.

4.2 Uzaktaki Cihazlar Hakkinda Bilgi Elde Etmek

4.2.3 Telnet Oturumunun Sonlandirilmasi veya Askiya Alinmasi

Bir önemli özellik telnet komutlarindan askiya alma özelligidir. Bununla beraber potansiyel bir problem oldugu zaman telnet oturumu askiya alinir ve **enter** tusuna basilir. Cisco IOS programinin yeniden için telnet baglantisinin askiya alinmis olmasi gerekir. Enter tusuna siklikla basilir. telnet oturumunun askiya alinmasi ile diger routerlara tekrar baglanti mümkündür. EXEC komutlari kullanildiginda yada konfigürasyonda degisiklik yapildigi zaman tehlikeli olabilir. Daima uygulamada telnet askiya alindigi zaman uyarilar dikkate alinmalidir.

Zaman asimi dolayisiyla oturum askiya alinir. telnet oturumunu devam ettirmek için **Enter** tusuna basilir. Telnet oturumunun nerede kaldigi **show sessions** komutu ile gösterilecektir.

Telnet oturumunun nasil sonlandirilmasi gerektigi asagidaki adimlarda gösterilmektedir.

- **disconnect** komutu girilir.
- Komutla beraber routerin ismi yada ip adresi girilir.

  Ankara>**disconnect sivas**

Telnet oturumunu askiya almak için ise asagidaki adimlar gerçeklestirilir:

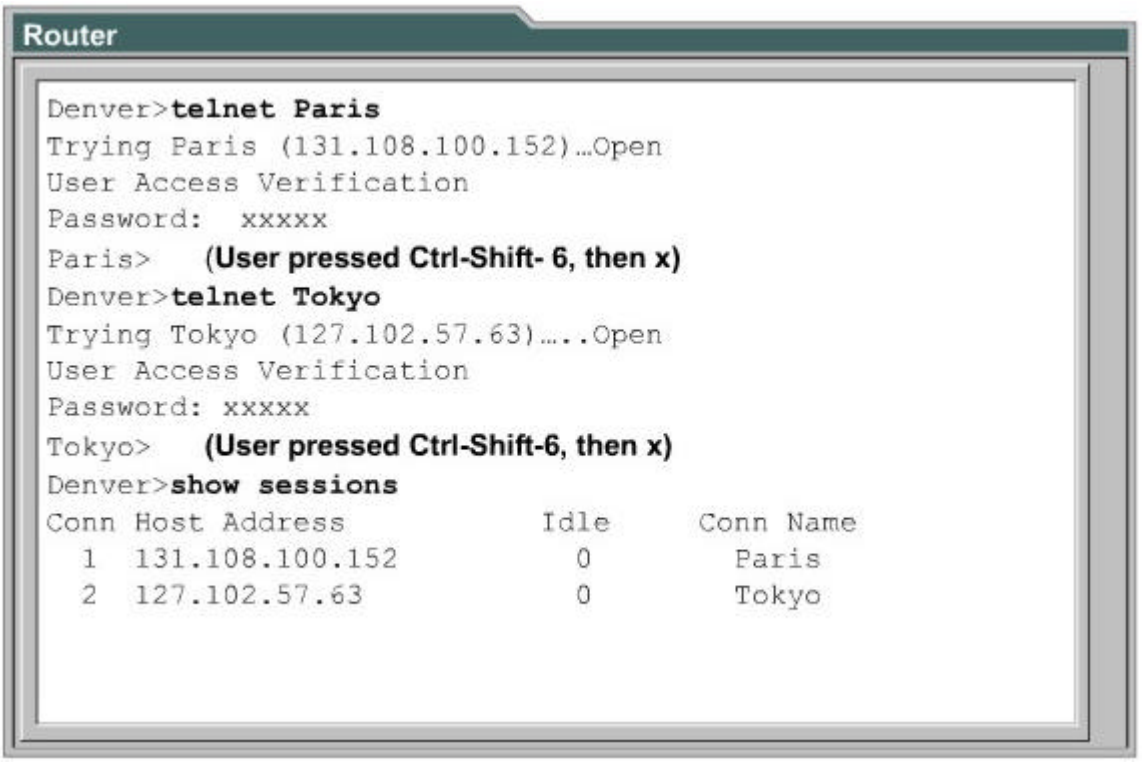
- **Ctrl-Shift-6** ya sonrada **x** e basilir.
- Routerin ismi yada ip adresi girilir.

4.2 Uzaktaki Cihazlar Hakkinda Bilgi Elde Etmek

4.2.4 Gelismis Telnet operasyonlari

Telnet oturumlari çesitli sekillerde açilirlar. **session limit** komutu ile açik oturumlarin numaralari bir defaya mahsuz tanimlanir.

Bir oturumdan çikilmasi kaldigi yerden devam ettirilmesi gibi kullanilan komutlar asagidaki sekilde gösterilmistir.



Cisco 2500 serisi routerlarda ayni anda sadece bes tane oturumla sinirlandirilmistir.

Çoklu telnet oturumlari kullanirken **Ctrl-Shift-6** komutu ve ardindan **x** e basilir. Eger oturum askiya alinmissa devam ettirmek için enter tusuna basilir. Enter a basildigi zaman tekrar baglantiya geçilir. Eger "**resume**" komutu baglanti kullanildiginda baglanti kimligi gerekebilir. Baglanti kimligi, **show sessions** komutu kullanilarak görüntülenebilir.

4.2 Uzaktaki Cihazlar Hakkinda Bilgi Elde Etmek

4.2.5 Alternatif Baglanabilirlilik Testleri

Temel ag baglantilarinda yardim için , birkaç ag protokolü yanki protokollerinde desteklenmistir. Yanki protokolleri , paketler yönlendirilirken testleri kullanirlar. Ping komutu ile hedeflenen hosta paket yollarlar. O hosttan paketlerin geri dönmesini beklerler. Bu yanki protokolünden hosta giden yolun güvene bilinirligi hakkinda yardim ettigi sonucu çikarilir. Yoldaki gecikmeler , hostun cevap verip vermedigi , ada çalisip çalismadigi hakkinda bilgi verirler.bu temel bir test mekanizmasidir. Kullanici yada yönetici moddayken uygulanabilir.

Ping komutu ile paketler gönderildikten sonra her gelen basarili yankida (!) isareti gösterilir. Eger bir yada daha fazla periyotta router zaman asimina ugradiysa ünlem isareti yerine (.) isareti görüntülenir.

traceroute komutu agda gönderilen veri paketinin nereye gönderildiginin bulunmasinda kullanilir. Ping komutuna benzer bir komuttur. Yine ayni sekilde uçtan uca baglantinin test edildigi bir komuttur. Her bir yolun uzunlugunu test eder. Bu uygulama ping gibi kullanici ve yönetici moddayken kullanilabilir.

show ip route komutu hedef ag için önceden olusturulmus yönlendirme tablosuna göre mevcut yönlendirmeyi gösterir. Bu komut ileriki konularda detayli olarak görülecektir.

Ping komutunun nasil kullanilmasinda asagidaki adimlar uygulanir.

- **ping** IP adres yada hedeflenen routerin ismi
- **Enter** tusuna basilir.

traceroute komutunun nasil kullanilmasinda asagidaki adimlar uygulanir:

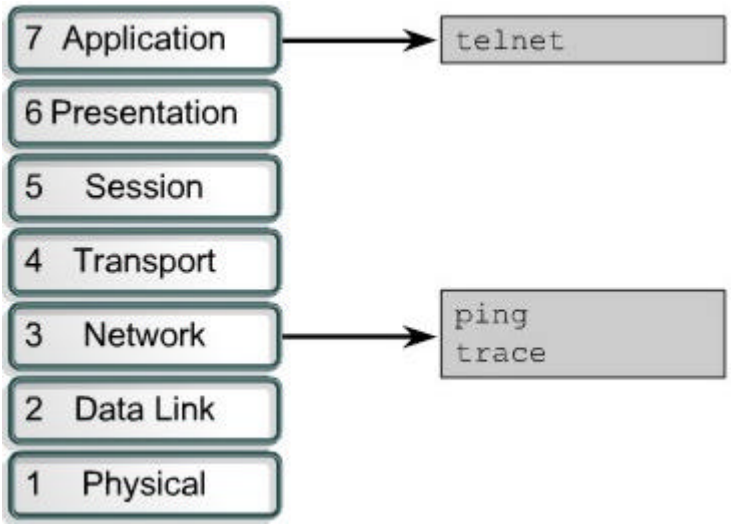
- **traceroute** IP adres yada hedeflenen routerin ismi
- **Enter** tusuna basilir

4.2 Uzaktaki Cihazlar Hakkinda Bilgi Elde Etmek

4.2.6 IP Adreslendirmedeki Sorunlarin Giderilmesi

Adreslemedeki problemler , ip aglarinda ortaya çikan ortak bir sorundur. Asagidaki komutlari kullanarak adreslemede çikacak sorunlar giderilebilir.

- Ag katmanin ip adresleri ve donanim baglantilarindaki ICMP protokolünde **ping** kullanilir. Bu temel bir test mekanizmasidir.
- Bir kaynaktan hedefe uygulama katmaninda program olarak **Telnet** kullanilir. Bu test mekanizmalarinin tamamlanmasinda olmasi gereken bir programdir.
- Kaytan hedefe olan yolda olusabilecek basarisizliklarin yeri konumu hakkinda bilgi vermesi için **traceroute** komutu kullanilir.



ÖZET

Asagidaki kilit noktalarinin anlasilmis olmasi saglanmalidir.

.

- CDP nin açilmasi ve kapanmasi
- **show cdp neighbors** komutunun kullanilmasi
- Hangi yerel arayüze yakinlardaki hangi cihazin baglanacaginin belirlenmesi
- CDP kullanarak yakinlardaki cihazlar hakkindaki bilgilerin ag adreslerinde toplanmasi
- Telnet baglantisi kurmayi
- Telnet baglantisi dogrulamasi
- Telnet oturumundan ayrilma
- Telnet baglantisinin askiya alinmasi
- Alternatif baglantilarin testleri
- Uzaktaki terminal baglantilarinin sorunlarinin giderilmesi

BÖLÜM - 5

Giris

Cisco routerlar Cisco IOS olmadan islem yapamazlar. Her routerda sitemin çalismasi, islem siranin gerçeklesmesi ve ISO un yüklenmesi için sitem açilisinin önceden belirlenmis olmasi gerekir. Bu bölümde açilisin yapilmasi esnasinda gerçeklestirilmesi geren prosedürlerin evreleri ver önemi hakkinda bilgi verilecektir.

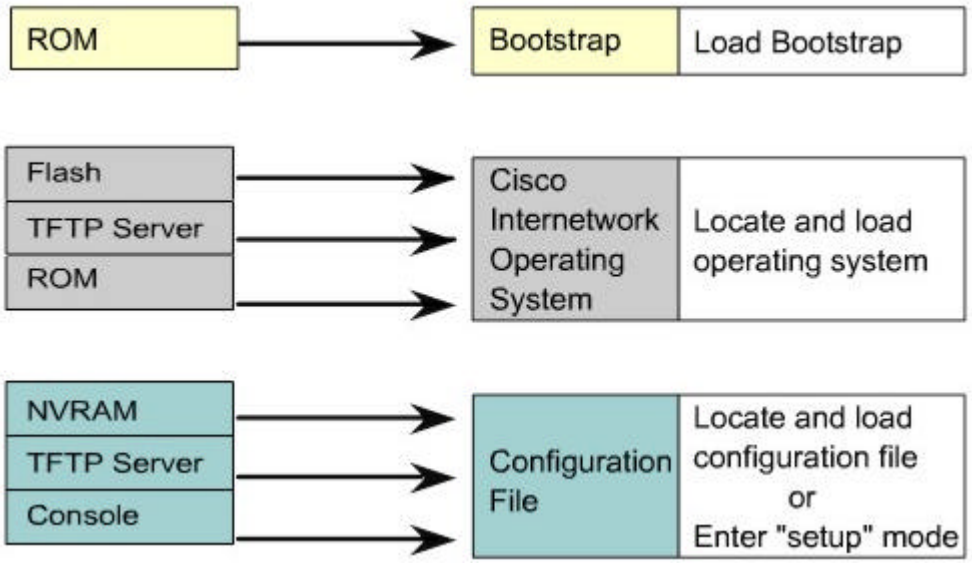
Cisco internet cihazlari birkaç farkli dosyayi kullanarak islem görürler. Bu is için içlerine yerlestirilen IOS dosyasini ve konfigürasyon dosyalarini kullanirlar. Ag yöneticileri uygun versiyonlari kullanirlar ve gerekli yedeklemeleri alirlar. Bu bölümde Cisco sistem dosyasi ve araçlarin etkilibir sekilde yönetilmesi sunulacaktir.

Bu modül tamamlandiginda asagidaki konular hakkinda daha genis fikir edinilecektir.

- Router açilis sirasinin bölümlerinin belirtilesi
- Cisco IOS un cihazlarda bulunmasi ve nasil yükleneceginin belirlenmesi
- Çikis sistem komutlarinin kullanilmasi
- Konfigürasyon kayit bilgilerinin belirlenmesi
- Cisco Ios un ve fonksiyonlarinin nasil kullanilacaginin kisaca tanimlanmasi
- Konfigürasyon dosyalarinin TFTP kullanarak ve kopyala yapistir yöntemiyle kayit edilip düzenlenmesi
- Diger dosya tiplerinin routerdaki yerlerinin listelenmesi
- IOS isminin kisimlarinin kisaca belirtilmesi
- TFTP kullanarak IOS dosyasinin yüklenmesi
- XMODEM kullanarak IOS dosyasinin yüklenmesi
- Sistem dosyalarini kullanarak komutlarin gösterilmesi

5.1 Routerin Açilisinin Siralanmasi ve Dogrulanmasi

5.1.1 Routerin Enerjilendigindeki Açilis Kisimlari



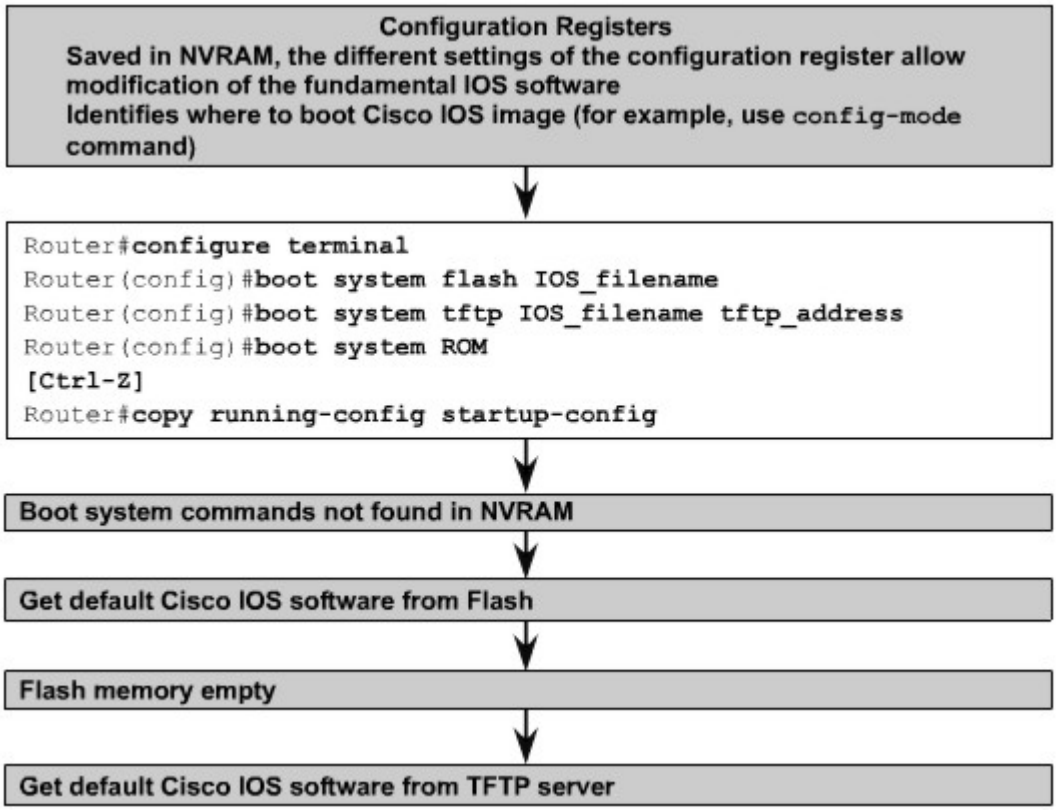
Cisco IOS programi alilista rutin bir sekilde router operasyonlarini baslatir. Router , ayarlandigi aga baglanirken islerini performansli bir sekilde yerine getirmelidir. Router açilirken standart olarak sunlari yapar:

- Donanimini test eder
- Cisco Ios programini bulur ve yükler
- Konfigürasyon tanimlamalarini , yerlestirilmis protokollerin fonksiyonlarini ve arayüzlerin adreslerini bulur ve uygular.

5.1 Routerin Açilisinin Siralanmasi ve Dogrulanmasi

5.1.2 Cisco Cihazlari ISO u Nasil Bulur ve Yükler

Normalde donanim platformunda Cisco IOS programinin oldugu kabul edilir. Fakat genelde routerlar NVRAM de sakladiklari açilis sistem komutlarina bakarlar. Cisco IOS programi alternatif durumlarda kullanilir. Diger kaynaklar program için özellestirilmis olabilir.



Ayarlar konfigürasyon kayitlarinda asagidaki durumlara göre açiktir:

- Global konfigürasyon modu açilis sistem komutlari router için özel olarak girilirler. Router yeniden baslatildiginda duyulan ihtiyaca göre sirasi ile bu komutlar kullanilir.
- Eger NVRAM de açilis sistem komutlari yoksa router Flash hafizada bulunan Cisco IOS programinda bulunan varsayilan sistemi kullanir.
- Eger flash hafiza bossa router , TFTP sunucuyu kullanir. Buradan Ios dosyasini agdan yükler. Ag sunucusunda açilis için varsayilan sistem dosyasindan , dosya isminden konfigürasyon kayir degerlerini kullanirlar.

5.1 Routerin Açilisinin Siralanmasi ve Dogrulanmasi

5.1.3 Açilis Sistem Komutlarinin Kullanilmasi

Asagida Cisco IOS program dosyasinin ilk olarak flash hafizadan sonra ag sunucusundan sonrada Rom dan nasil yüklendigi anlatilacaktir:

- **Flash Hafiza** – Sistem dosyasi flash hafizadan yüklenir. Flash hafizada bilginin kayitli olmasi bir avantajdir. TFTP sunucudan sistem dosyasi yüklenirken agda olasabilecek basarisizliklara göre flash hafiza çok avantajlidir.

- **Ag Sunucusu** – flash hafizada dosya yoksa yada bozulmussa Sistem dosyasi TFTP sunudan yüklenebilir.
- **ROM** – Flash hafiza bozuk ve ag sunucusundan dosyanin yüklenmesi basarisizlikla sonuçlanmissa ROM dan açilis yapilir. Ancak sistem dosyasi ROM da Cisco IOS un muhtemelen alt kisimlarindadir. Ayni zamanda router satin alindiginda güncellenmesi gerekebilir. Rom da eski sistem dosyalari kayir edilmis olabilir.

"copy running-config startup-config" komutu ile NVRAM e kayit edilir.Router böylece açilis sistem komutlarini çalistirabilecektir.

5.1 Routerin Açilisinin Siralanmasi ve Dogrulanmasi

5.1.4 Konfigürasyonun Kayit edilmesi

Açilis ayarlarinda sistem önyükleme bilgileri için routerlar konfigürasyon kadilarina bakarlar. Varsayilan konfigürasyon kayit ayarlari , global konfigürasyon modunda **config-register** komutu kullanilarak degistirilir. Bu komut için hekzadesimal numaralar kullanilir.

Konfigürasyon kayitlari NVRAM de 16-bitlik kayitlardir. Boot alanindan en düsük 4 bit kayitlarindir. Diger 12-bit degistirilemez. **show version** komutu kullanilarak varsayilan degerlere erisilebilir. **config-register** komutu kullanilarak sayilarda degisiklik yapilabilir.

Value	Description
0xnnn0	Use ROM monitor mode (manually boot using the **b** command)
0xnnn1	Automatically boot from ROM (default if router has no Flash)
0xnnn2 to 0xnnnF	Examine NVRAM for boot system commands (0xnnn2 is the default if the router has Flash)

- ROM monitör moduna girilir. Konfigürasyon kayitlari 0x*nnn*0 degerine ayarlanir. "nnn" yazan kisma açilis alaninin numaralari girilir. Açilis için 0000 bitleri ayarlanmistir. ROM monitörden operasyon sisteminin açilisi **b** komutu kullanilarak el ile olarak yapilabilmektedir.
- Sistem konfigürasyonu ROM dan otomatik olarak baslatilir. Konfigürasyon kayitçisi 0x*nnn*1 degerine ayarlanir. "nnn" ile gösterilen kisma 0001 bitleri ayarlanir.
- Sistem konfigürasyonu NVRAM deki açilis sistem dosyalarini kullanir. Kayitçi , 0x*nnn*2 den 0x*nnn*F e kadar ayarlanir. "nnn" 0010 ile 1111 arasinda bir deger alir. Açilis sistem komutlari kullanilirken NVRAM de oldugu varsayilir.

5.1 Routerin Açilisinin Siralanmasi ve Dogrulanmasi

5.1.5 IOS Açilis Kayiplarinin Düzeltilmesi

Ruter açilis islemini tam anlamiyla yerine getiremedigi zaman yanlis bir seyler var demektir:

- Konfigürasyon dosyasi kayip yada yanlis bir açilis sistemidir.
- Konfigürasyon kayitçisi yanlis bir degerde olabilir
- Flash dosyasi bozulmus olabilir
- Donanim arizalanmis olabilir

Router açilirken açilis sistemi için konfigürasyon dosyasina bakar. Açilis sistemi , flash taki IOS un diger dosyasindan açilabilir. Açilis dosyasinin kayit bilgileri **show version** komutu girilerek görülür.

show running-config komutu ile konfigürasyonun açilis sistem bilgilerine bakilir. Eger açilis sistemi yanlis bir ISO dosyasi ise silme islemi kullanilir.

Dogru olmayan konfigürasyon kayitçi ayarlari flas tan yüklenirken engellenecektir. IOS dosyasinin nerede oldugunu routera söyleyecektir. Kayitçi için son satirda bakmak ve ayarlamak için **show version** komut kullanilir. Dogru degerler donanim platformundan donanim platformuna göre degisir. **show version** nun çikisi dokümantasyona bir yazicidan kopyalanir. Eger dokümantasyon mevcut degilse Cisco döküman cd si yada sitesinden dogru konfigürasyon kayitçilari temin edilir. Sonra konfigürasyona kayit edilir yeniden baslatilir.

Eger hala problem devam ediyorsa router flash dosyasi bozulmus olabilir. Açilista asagidaki gibi hata mesajlari görüntülenir.

- open: read error...requested 0x4 bytes, got 0x0
- trouble reading device magic number
- boot: cannot open "flash:"
- boot: cannot determine first file name on device "flash:"ú

Eger flash dosyasi bozulmussa routera yeni ISO yüklenmelidir.

Eger görünürde problem yoksa routerin donaniminda bir sorun var demektir. Teknik destek kismi ile irtibata geçilmelidir.

Not: konfigürasyon kayitçisi görüntülenmiyorsa **show running-config** yada **show startup-config** komutlari kullanilir.

5.2 Cisco Dosya Sisteminin Yönetimi

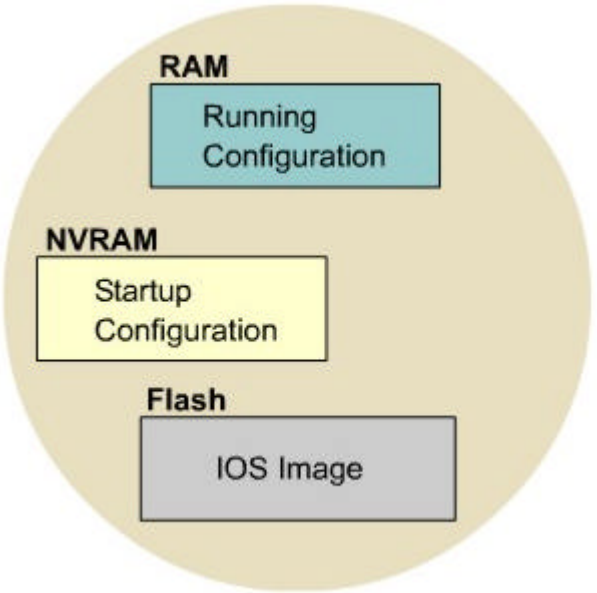
5.2.1 IOS Dosya Sistemine Giris

Routerlar ve switc'ler operasyonlari için bir yazilima baglidirlar. Iki tip yazilim mevcuttur. Operasyon sistemi ve konfigürasyon yazilimidir.

Isletim sistemi hemen hemen tüm Cisco cihazlarinda kullanilir. Cisco IOS , donanima router ve switch fonksiyonlarina izin veren bir yazilimdir. Çesitli megabyte larda olabilir.

Yazilim, router yada switch lerde kullanilan konfigürasyon yada konfigürasyon dosyasidir. Cihazin router yada Switch modunda çalismasi konfigürasyonda tanimlanir. Ag yöneticileri Cisco cihazlarindan istedikleri islevi tanimladiklari konfigürasyonu olustururlar. Fonksiyonlar , arayüzlerin ip adresleri , yönlendirme protokolleri, belirtilmis aglarin konfigürasyonu olabilir. Konfigürasyon dosyasi tipik olarak birkaç yüz yada bin byte olabilir.

Her bir yazilimin bilesenleri hafizada ayri bir dosya olarak saklanir. Dosyalar ayni zamanda farkli hafiza tiplerinde de saklanabilir.



IOS , flash hafiza alaninda saklanir. Flash hafiza , açilista isletim sisteminde kullanilan IOS dosyasini kaybolmayan bir bellege saklar. Flash , IOS dosyasini çift kayit edilebilir yada güncellenebilme imkani saglar. Bazi routerlarin yapisinda IOS, RAM den kopyalanabilir ve çalistirilabilir.

Konfigürasyon dosyasinin kopyasi NVRAM de kayitlidir. Konfigürasyon baslangiç sirasinda NVRAM den kullanilabilir. Bu kisim baslangiç ayarlarinda (startup config) bölümünde belirtilecektir. Baslangiç konfigürasyonu açilis sirasinda RAM e kopyalanir. Ram de router i çalistirmak için kullanilir. Bu kisim açilis ayarlarinda (running config) kisminda anlatilacaktir.

IOS , versiyon 12 ile baslamistir. Tüm dosya sistemlerine tek arayüzde router kullanimini saglamistir. Cisco IOS dosya sistemi konusunda bahsedilecektir. Tüm sistem dosya yönetimleri routerlarda kullanilirken bir tek metotla gerçeklestirilir. Bunlarin flash hafizada ,

ag dosya sisteminde (TFTP sunucu yada FTP) , okunur yazilabilir hafizada (NVRAM yada ROM) olmasi istenir. IOS dosya sitemi cihazlarda belirtilen dosya sisteminde ortak olarak kullanilir.

Prefix	Description
bootflash:	Bootflash memory
flash:	Flash memory. This prefix is available on all platforms. For platforms that do not have a device named flash, the prefix flash: is aliased to slot0:. Therefore, the prefix flash: can be used to refer to the main flash memory storage area on all platforms.
flh:	Flash load helper log files
ftp:	File Transfer Protocol (FTP) network server
nvram:	NVRAM
rcp:	Remote copy protocol (rcp) network server
Slot0:	First Personal Computer Memory Card International Association (PCMCIA) flash memory card
Slot1:	Second PCMCIA flash memory card
system:	Contains the system memory, including the running configuration
Tftp:	TFTP network server

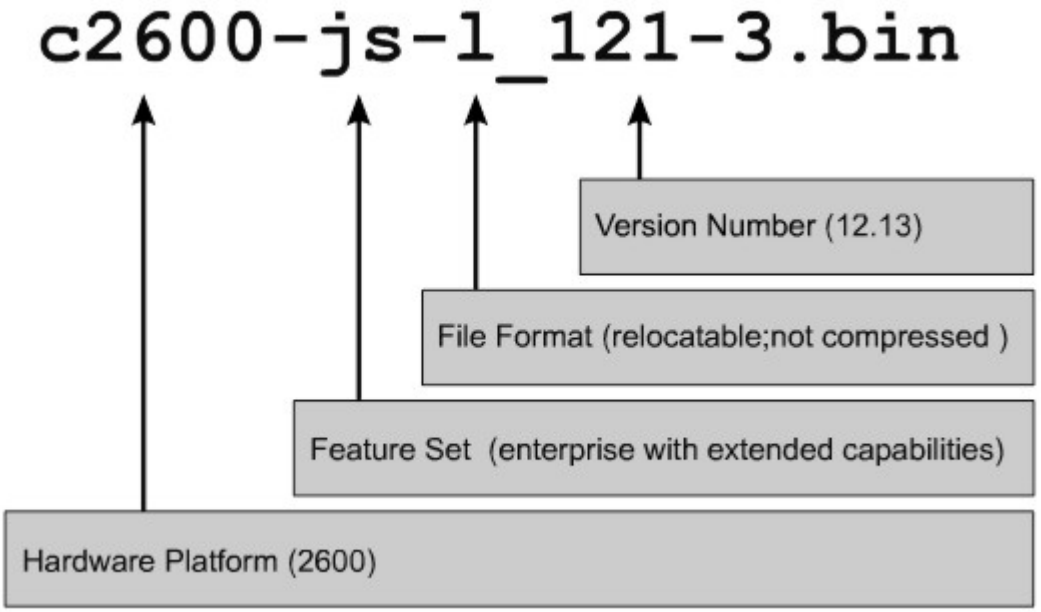
Ios dosya sistemi ag cihazlarinda ve agda , belirtilen dosyalara URL yöntemini kullanirlar. Konfigürasyon dosyasina URL ile ulasilmak istenildiginde kolona: [[//konum]/dizin]/dosya ismi] olacak sekilde yazilir. Ios dosya sistemi ayni zamanda FTP dosya transferini saglar.

5.2 Cisco Dosya Sisteminin Yönetimi

5.2.2 IOS Isimlendirmenin Egilimleri

Cisco , IOS un birçok farkli versiyonu gelistirmistir. IOS , çesitli donanim platformlari ve özellikleri sunarlar. Cisco, IOS un yeni versiyonlarini sürekli olarak gelistirmektedir.

Diger versiyonlari kimliklendirirken IOS dosyalari için standart isimlendirme yapilmak zorundadir. Isimlendirmedeki standartlar diger isimlendirmelerde de kullanilir. Isimlendirmede donanim platform kimligi, özellik kayit kimligi, dosya formati ve versiyon numaralari bulunur..



Dosya isimlendirmenin ilk kisimda dosyanin hangi donanim platformu için olusturuldugu yerin kimligi girilir.

Dosya isimlendirmenin ikinci kisimda o dosyanin kapsadigi çesitli özelikler bulunur. Birçok farkli özellik vardir. Yazilim dosyalarinda paketlenmis özellikler bulunur. Her bir özellik , IOS un alt bir özelligidir. Bu alt kategorilere örnek verecek olursak:

- **Basic** – Donanim platformu için temel özellik ayarlaridir. Örnegin IP ve IP/FW
- **Plus** – IP Plus, IP/FW Plus, ve Enterprise Plus eklentilerinin temel özellikleri
- **Encryption** – temel yada + özelliklere 56 bitlik veri sifreleme saglarlar. Örnegin Cisco IOS Release 12.2 ve ilerisi versiyonlarda IP/ATM PLUS IPSEC 56 yada Enterprise Plus 56 özellikleri kendinden k8/k9 sifreleme algoritmasi kullanirlar.

    - **k8** – 12.2 ve yukarisi versiyonlarda 64 bit veya altini sifrelemeye esittir.
    - **k9** – 64-bit ten yukari sifreleme (12.2 ve üzeri versiyonlarda)

Üçüncü kisimda dosya formati belirtilir. Flashtaki sikistirilmis format IOS a kayit edilir yoksa bile yerlestirilebilir. Eger dosya sikistirilmis ise IOS dosyayi RAM a kopyalayarak açilista açabilmelidir. Flash ram den kopyalanip çalistirilabilir. Eger mümkün degilse direkt olarak flash tan çalistirilir.

Dördüncü kisimda IOS un versiyon numarasi bulunur. Cisco , IOS un versiyonlarinin gelistirirken versiyonlari numaralandirir.

5.2 Cisco Dosya Sisteminin Yönetimi

5.2.3 Konfigürasyon Dosyalarinin Yönetilmesinde TFTP nin Kullanilmasi

Cisco router yada switchlerde konfigürasyon aktivasyonu ramde dir. NVRAM de baslangiç konfigürasyonunun oldugu varsayilir. Konfigürasyon kayboldugu zaman buradan baslatilir. Bir kopyasi TFTP sunucudan kayit edilebilir. **copy running-config tftp** komutu bu is için kullanilir. Bu islemi yapmak için gerekli adimlar asagida listelenmistir:

- **copy running-config tftp** komutu girilir.
- Dosyanin kayitli oldugu TFTP sunucunun ip adresi girilir.
- Dosyanin ismini yada varsayilan ismi onaylanir
- Dogrulamak için her seferinde **yes** yazilir.

TFTP sunucudan yedeklenmis dosya yüklenirken router router konfigüre edilebilir. Bu islem için ise asagidaki adimlar uygulanmalidir:

- **copy tftp running-config** komutu girilir.
- Host yada ag konfigürasyon dosyasinin adi seçilir.
- Dosyanin kayitli oldugu TFTP sunucusunun ip adresi girilir.
- Dosyanin ismi girilir yada varsayilan isim kabuledilir.
- Dosya ismi ve sunucu adresi sistem kaynaklarinca dogrulanir

5.2 Cisco Dosya Sisteminin Yönetimi

5.2.4 Konfigürasyon Dosyasinin Kopyala Yapistir ile Kullanilmasi

Konfigürasyon dosyasinin yedegini kopyalanmadaki bir baska yol **show running-config** komutunu kullanarak çikisi yakalamaktir. Bu çikisi , terminal oturumundan yaziyi metin dosyasina kayit ederek kopyala-yapistir yöntemi ile yapmakta mümkündür. Bu dosya , routera yüklenip kullanilmadan önce düzenlenme ihtiyaci duyabilir.

Hyper Terminal programinin ekraninda konfigürasyonda görüntülenen yaziyi yakalayip yazi dosyasina söyle aktarilir:

1. **Transfer** seçilir
2. **Capture Text** seçilir
3. kopyalanacak konfigürasyonun metin dosyasi için isim girilir
4. **Start** a basilarak yazi yakalanir
5. **show running-config** komutu girilerek ekranda konfigürasyon görüntülenir
6. Ekran doldugu zaman kaldigi yerden devam ettirmek için **space bar** tusuna basilir.

Konfigürasyon görüntülendigi zaman yakalamayi durdurmak için:

1. **Transfer** seçilir
2. **Capture Text** seçilir
3. **Stop** seçilir

Yakalama tamamlandiktan sonra konfigürasyon dosyasi geri düzenlenme ihtiyaci duyabilir. Routera geri yapistirma yapmadan önce gereksiz bilgilerin yakalanan bilgilerden geri alinmasi gerekir. Açiklamalara ! isareti ile baslangiç satirina eklenirler.

Konfigürasyon dosyasi , Notepad metin editörü ile düzenlenebilir. Düzenleme yapmak için Notepad deyken **File** > **Open** bulunup seçilir.

Satirlar da asagida gösterilen yazilarin silinmesi gerekir:

- show running-config
- Building configuration...
- Current configuration:
- - More -
- Any lines that appear after the word "End"

no shutdown komutu her bir arayüz bölümlerinin sonuna eklenir. Bunun için **File** > **Save ile** konfigürasyonun temiz versiyonu kayit edilecektir.

Yedeklenen ayarlar , Hyper Terminal oturumu tarafindan tekrar geri yüklenebilir. Geri yüklemen önce routerdan konfigürasyonun kaldirilmasi gerekir. Bunun için yönetici modayken **erase startup-config** komutu routera girilir. Daha sonra **reload** komutu kullanilarak router yeniden baslatilir.

HyperTerminal konfigürasyonu yeniden yüklemek için kullanilir. Konfigürayonun temiz bir yedegi routera asagidaki gibi yüklenir:

- Global Konfigürasyon moduna girilir
- Hyper Terminalden **Transfer > Send Text File** tiklanir
- Yedek konfigürasyonu yüklemek için dosya ismi girilir
- Eger yaziliysa dosya satira girilir.
- Hatalar gözlenir
- Sonra konfigürasyon girilir ve
- **Ctrl-Z** tusuna basilarak global modan çikilir.
- **copy running-config startup-config** ile baslangiç konfigürasyonu kayitedilir.

5.2 Cisco Dosya Sisteminin Yönetimi

5.2.5 TFTP Kullanarak IOS Dosyalarinin Yönetimi

Routerlarda ISO´un güncellenmesi yada yeniden yüklenmesi gerekir. Router ilk alindigi zaman IOS dosyasida gelir. Bu dosya kalibi diger IOS kaliplari ile merkezi sunucudan kayit edilebilir. Dosya kaliplari , ag çalismalarinda routerlar ve switchlerde IOS´un güncellenmesinde ve kayit edilmesinde kullanilir.

Bu sunucu TFTF servisini çalistirmak zorundadir. Yedeklenmis IOS **copy flash tftp** komutu ile yönetici modayken kopyalanabilir.

Routera , kullanici TFTP sunucunun ip adresini girecektir. Sunucuda IOS dosya kalibinin isimi için girildigi zaman router flashin silinmesini saglayacaktir. Bu yeni yüklenecek dosya için flashta yeterli alan olmayabilir. Flashtan dosya silinir.

Her bir IOS dosyasinin indirilmesinde ! isareti görüntülenir. Bu IOS dosyasi birkaç megabyte olabilir ve biraz zaman alabilir.

Yeni flash dosyasi indirildikten sonra dogrulanacaktir. Router artik yeni dosyayi yükleyip kullanmaya hazirdir.

5.2 Cisco Dosya Sisteminin Yönetimi

5.2.6 Xmodem Kullanarak IOS Dosyalarinin Yönetimi

Eger IOS dosyasi flashtayken silinmis yada bozulmussa , ROM monitör modundan tekrar yükleme ihtiyaci duyacaktir. Cisco donanim mimarisinde ROM monitör modu "**rommon 1 > prompt"** olarak belirtilmistir.

Bu ilk adimda "IOS dosyasi flashtan neden yüklenememistir?" sorgusu yapilir. Burada dosya bozulmus yada kaybolmus olabilir. **dir flash** komutu ile flash kontrol edilecektir.

Eger dosyanin yeri ögrenilmisse o dosyadan açilis yapmasi denenir. Bunun için **boot flash** komutu kullanilir. Örnegin buldugumuz dosyanin ismi c2600-is-mz.121-5 olsun. Bunu çalistirmak için rommon modundayken asagidaki komut yazilir:

rommon 1>**boot flash:c2600-is-mz.121-5**

eger router uygun bir sekilde açilis yaparsa flashtan IOS kullanilan dosyanin neden açilis yapmadigi arastirilir. **show version** komutu kullanilarak konfigürasyon kayitlari kontrol edilir. Varsayilan açilis sirasi için konfigüra edilir. Eger konfigürasyon kayitlari dogru ise **show startup-config** komutu kullanilir. Bununla ROM monitörde router IOS´u kullanirken bulunan açilis sistem komutlari görünür.

Eger router dosyadan uygun bir sekilde açilis yapmiyorsa yada ISO dosyasi yoksa yeni bir IOS indirilmesi gerekmektedir. IOs dosyasi konsoldan Xmodem kullanarak yada ROMmon modundayken TFTP yi kullanarak dosyayi indirip yeniden yükler.

ROMmon dan Xmodemi kullanarak dosyanin indirilmesi: konsoldan IOS yüklerken IOS dosyasinin kopyalanmasi için bir bilgisayar olmak zorundadir. Hyper Terminal programinin çalistirilmasi ve düzenleme yapmak için bu bir gereksinimdir. IOS ta düzenleme yaparken varsayilan konsol baglanti hizi **9600bps** dir. Saniyedeki bit hizi (baud rate) 115200bps e kadar degistirilebilir. Konsol hizi , **confreg** komutu kullanilarak ROMmon modundayken degistirilebilir. **confreg** komutu girildikten sonra routerdaki parametreler degistirilebilecektir.

“change console baud rate? y/n [n]:” sorusu soruldugu zaman “y “ tusuna basilarak yeni hiz girilir. ROMmon moda konsol hizi degistirildikten sonra router yeniden baslatilir. Terminal oturumu 9600bps te sonlandirilir. Yeni oturum 115200 bps konsol hizina eslestirilir.

Xmodem komutu bilgisayardan IOS yazilim dosyasinin düzenlenmesini ROmmon moda yapmak için kullanilir. Komutun yazim formati söyledir: **xmodem -c dosya adi .** örnek verecek olursak : dosya adi “c2600-is-mz.122-10a.bin” olsun. Buna göre yazacagimiz komut asagidaki gibidir:

xmodem -c c2600-is-mz.122-10a.bin

“-c” komut eklentisi Xmodem kullandigimizda dosyayi indirme esnasinda dönüssel artiklik denetimi (CRC) ni kullanarak hata denetimi yapmaktir.

Router transfer baslamadigi zaman uyari mesaji verecektir. Uyari mesaj bilgileri dogrulari sorar ve silinebilirdir. Islem devam ettigi zaman router transferi baslatacaktir.

Xmodem transferi terminal emülatöründen baslayacaktir. Hyper Terminal den **Transfer** > **Dosya Gönder** kisimi seçilir. Dosya gönder de dosya ismi / yeri , Xmodem protokolünde seçilir ve transfer baslatilir. Transfer esnasinda dosya gönderimi transferin durumu görüntülenecektir.

Transfer tamamlandiginda mesaj gelir ve flash silinir. “Indirme Tamamlandi!” mesaji gelir. Routr yeniden baslatilmadan önce konsol hizinin 9600bps e ayarlanmasi gerekir. Konfigürasyon kayitlari 0x2102 ye dönmelidir. Yönetici moddayken **config-register 0x2102** komutu girilir.

Router yeniden baslatilirken 115200 bps baglanti hizli oturum sonlanacak 9600bps lik baglanti hizi ile oturum baslatilacaktir.

5.2 Cisco Dosya Sisteminin Yönetimi

5.2.7 Çevre Degiskenleri

IOS , TFTP oturumundan da geri yüklenebilir. Routera IOS dosyasi geri yüklemenin en hizli yolu ROMmon ile TFTP yi kullanarak indirmektir. Bunun için **tftpdnld** komutu kullanilarak ayarlar yapilir.

ROMmon´ün fonksiyonlari çok kisitlidir. Açilis sirasinda konfigürasyon dosyasi yüklenemez. Router bu yüzden ip adresine yada arayüz konfigürasyonuna sahip degildir. Çevresel degiskenler IOS un TFTP için izin verilen minimum konfigürasyonu sunarlar.ROMmon TFTP çalismalari sadece ilk LAN portunda olur. Bu arayüz için basit ip parametreleri ayarlanir. ROMmon çevre degiskenleri ayarlanirken , çevre isimleri yazilir. Isim ile ip adresi arasina "=" isareti konulur. Örnegin: 10.0.0.1 adresi ROMmon da Degisken_Ismi=10.0.0.1 yazilir.

Not:tüm degisken isimleri büyük küçük harfe karsi duyarlidir.

tftpdnld kullanarak enaz asagidaki tanimlamalar yapilabilir

- **IP_ADDRESS** – LAN arayüzündeki ip adresleri
- **IP_SUBNET_MASK** – – LAN arayüzü için alt ag maskesi
- **DEFAULT_GATEWAY** – The LAN arayüzü için varsayilan geçit
- **TFTP_SERVER** – TFTP sunucunun ip adresi
- **TFTP_FILE** – Sunucudaki IOS dosyasinin ismi

set komutu kullanilarak ROMmon´nun ortam degiskenleri kontrol edilir.

IOS için degiskenler ayarlanirken **tftpdnld** komut girilerek bagimsiz olmayan degiskenlerle girilir. ROMmon degisimleri yansitacaktir ve flashi silme uyarisi görüntülenecektir.

IOS taki dher dogrulama paketi çevrilerek ! isareti ile görüntülenecektir. IOS dosyasinin çevrilmesi tamamlandigi zaman flash silinecektir ve yeni IOs dosyasi yazilacaktir. Islem tamamlandiginda uygun mesaj görüntülenecektir.

Flash a yeni dosya yazildigi zaman ve ROMmon da görüntülendiginde router yeniden baslayacaktir. Router artik flashtan yeni dosya ile açilis yapar.

5.2 Cisco Dosya Sisteminin Yönetimi

5.2.8 Dosya Sistemi Dogrulamasi

Router dosya sistemi dogrulanirken birkaç komut kullanilabilir. Bunun için **show version** komutu kullanilir. **show version** komutu flashtaki toplam miktari ve mevcut dosyayi kontrol etmekte kullanilir. Bununla beraber IOs yüklenirken iki farkli görevi vardir. IOS dosyasinin kaynagini görüntüler ve routerin açilista kullandigi konfigürasyon kayitlarini görüntüler. Router IOS dosyasini nereden yükleyecegini konfigürasyon kayitlarinda inceler ve karar verir. Eger kabul etmezse bozukluk vardir ya flshtaki dosya kayiptir yada baslangiç konfigürasyonundaki sistem açilis komutlari kaybolmus olabilir.

show flash komutu dosya sistemini dogrulamada kullanilir. Bu komut flashta kullanilan IOS dosyasinin kimliklendirilmesinde kullanilir. Bu komut ayni zamanda yeni IOS dosyasinin kayit edilmesinde gerekli olan bosluk miktarini da gösterir.

Konfigürasyon dosyasi açilis sistem komutlarini içerebilir. Bu komutlar istene IOS açilis dosyasinin kaynaklarinin belirtilmesinde kullanilabilir. Çoklu sistem sistem açilis komutlari , onlarin konfigürasyon dosyasinda görüntülenmesi islemini görür

Özet

Asagidaki kilit noktalarinin anlasilmis olmasi saglanmalidir.

- Router açilis sirasinin kisimlarinin tanitilmasi
- Cisco cihazlarina IOS un yerlestirilmesi ve nasil yükleneceginin belirtilmesi
- Açilis Sistem komutlarinin kullanilmasi
- Problemlerin giderilmesi
- Kullanilan IOS un dosyalarinin tanitilmasi ve fonksiyonlari
- Routerdaki farkli dosya tiplerinin yerlerinin belirtilmesi
- IOS isimlendirmenin kisimlari
- Konfigürasyon dosyalarinda kullanilan TFTP nin yönetilmesi
- Konfigürasyon dosyalarini kullanirken kopyala-yapistirin kullanilmasi
- TFTP ile IOS dosya kaliplarinin yapilmasi
- Xmodem ile IOS dosya kaliplarinin yapilmasi
- Gösteri komutlarini kullanarak dosya sisteminin dogrulanmasi

BÖLÜM - 6

Genel Bakis

Bir agdan diger bir aga gitmek için yönlendirme yapilir. Yönlendirmeler bir routerdan diger bir routera dinamik bir sekilde olabilir. Yöneticiler tarafindan routera statik olarak atanabilirler.

Bu bölümde dinamik yönlendirme protokollerinin siniflarinin kavramlari incelenip her bir sinifin protokolü ile ilgili örnekler verilecektir.

Ag yöneticileri dinamik yönlendirme protokolünü temel olarak düsünürler. Agin büyüklügü , kullanilan hattin band genisligi, ag routerlarinin güç islemleri, agdaki routerlarin modelleri ve markalari ve agda kullanilan protokoller , yönlendirme protokolünün seçiminde hesaba katilmasi gereken tüm faktörlerdir. Bu bölüm yönlendirmedeki farkliliklar hakkinda ag

Bu modülü tamamlayan kimseler sunlari yapabiliyor olmalilar:

- Statik yönlendirmenin anlamini açiklamayi
- Statik ve varolan yönlendirme konfigürasyonu
- Statik ve varolan yönlendirmedeki sorunlar ve dogrulamalar
- Yönlendirme protokollerinin siniflarinin belirtilmesi
- Hat-durum (link-state) yönlendirme protokollerinin belirtilmesi
- Ortak yönlendirme protokollerinin temel karakteristiklerinin tanimlanmasi
- Iç ag geçidi protokollerinin tanimlanmasi
- Dis ag geçidi protokollerinin tanimlanmasi
- Routerdaki yönlendirme bilgi protokolünün (RIP) açilmasi

6.1 Statik Yönlendirmeye Giris

6.1.1 Yönlendirmenin Tanitimi

Routerlar paketleri hedefteki aga iletirken yönlendirme islemini kullanirlar. Routerlar paketlerdeki hedefin ip adresine göre karar verirler. Tüm cihazlar yol boyunca paketin noktaya dogru yönlendirilmesinde hedef ip adresini kullanirlar. Böylece paket hedefe ulastirilir. Dogru karar vermek için routerlar uzaktaki aglara olan yönlendirmeleri ögrenirler. Dinamik yönlendirme kullanildigi zaman bu bilgiler diger roterlardan ögrenilir. Statik yönlendirme kullanildigi zaman ag yöneticileri uzaktaki routerlar hakkindaki bilgileri el ile girilerek ögrenirler.

Statik yönlendirmede konfigürasyon elle yapilmaktadir. Ag topolojisindeki her bir degisiklikte ag yöneticileri degisiklikler için statik olarak yönlendirmeleri silerler ve eklerler. Genis aglarda , yönetim zamaninin çok büyük bir miktari yönlendirme tablolarinin el ile yapilan bakimda harcanir. Küçük aglarda birkaç degisiklikle statik yönlendirme çok kisa bir sürede yapilir. Çünkü ekstra yönetimsel sartlar ortaya çikar. Statik yönlendirme dinamik yönlendirme ile kiyaslanamaz. Genis aglarda yapilan statik yönlendirme , dinamik yönlendirme protokolleri ile çogu zaman özel amaçlar için kullanilirlar.

6.1 Statik Yönlendirmeye Giris

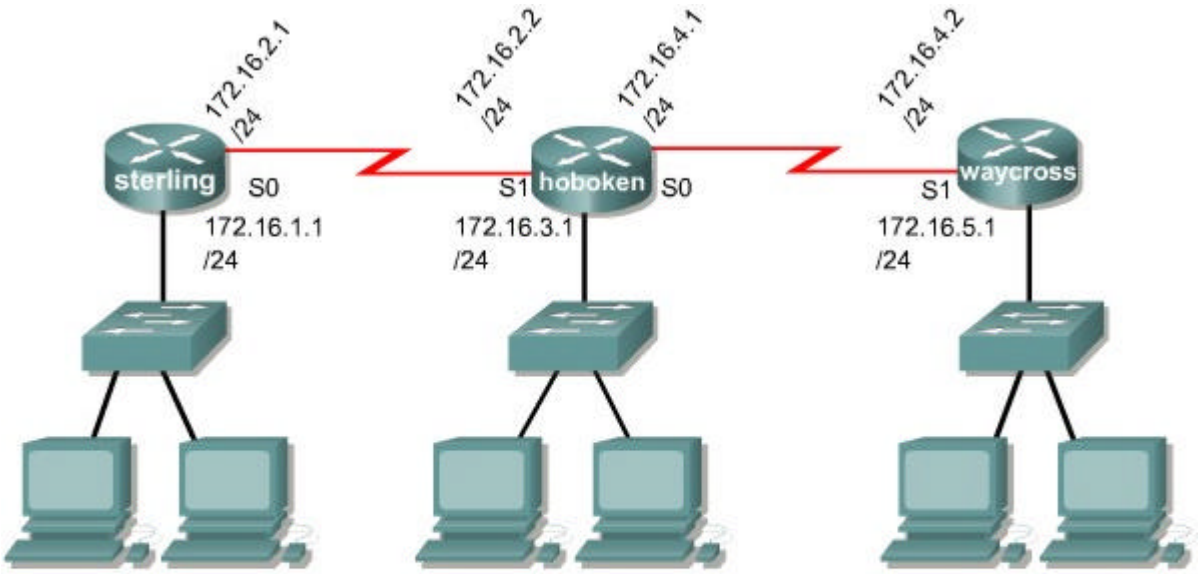
6.1.2 Statik Yönlendirme Islemi

Statik yönlendirme islemi üç kisima bölünebilir:

- Ag yöneticisi yollari ayarlarlar
- Routerlar , yönlendirme tablosuna yolu yüklerler
- Paketler statik yönlendirmede kullanilan yollardir.

Statik yönlendirme el ile konfigüre edilmek istendigi zaman , yönetici **ip route** komutunu routerda kullanarak statik yönlendirmeyi ayarlarlar. **ip route** komutunun kullanimi için dogru dizim asagidaki sekilde gösterilmistir.

Asagidaki sekilde ise , ag yöneticisi Hoboken routerinin diger routerlarla haberlesmesi için statik yönlendirme yaparak 172.16.1.0/24 ve 172.16.5.0/24 iplerini girmistir. Yönetici bu ögeleri tamamlamak için iki komut olarakta girebilir. Asagidaki sekilde bitisik routerin ip adresi tanimlanmistir. Hoboken routerinin yönlendirme tablosuna yönlendirme komutlari ile statik yönlendirme yapilmistir. Tek fark yönlendirme tablosunda routerdan routera uzaklik tanimlari yönetimsel olarak iki tanedir.




```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 s1
                   command destination  sub mask    gateway
                           network
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 s0
                   command destination  sub mask    gateway
                           network
```

```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
                   command destination  sub mask    gateway
                           network
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 172.16.4.2
                   command destination  sub mask    gateway
                           network
```

Yönetimsel uzaklik routerin güvenebilirliginin ölçüsünü veren opsiyonel parametrelerdir. Yönetimsel uzaklik için kisa degerler güvenilir bir yönlendirme sayilir. Böylece kisa yönetimsel uzaklik , özdes daha uzun uzaklik ile yönlendirilmeden önce yüklenebilir. Varsayilan uzaklik kullanildigi zaman gelecek adres 1 ile ifade edilir. Giden bir arayüz kullanildigi zaman 0 kullanilir. Eger uzaklik , varsayilan adrese yönlenmis ise 0-255 arasinda bir deger alir.

waycross(config)#**ip route 172.16.3.0 255.255.255.0 172.16.4.1 130**

Eger router , yönlendirmede kullanilan arayüze ulasamiyorsa , tablodaki yönlendirme yüklemesi yanlis olacaktir. Bu arayüzün düsmesi demektir. Yönlendirme tablosuna yerlesemicektir.

Bazen statik yönlendirme yedekleme amaci için kullanilir. Statik yönlendirme routerde ayarlanabilir. Sadece bu kullanildigi zaman dinamik yön ögrenme basarisiz olacaktir. Statik yönlendirmenin usulü dinamik yönlendirme protokolü kullaniminda çok uzun hatlarin basitçe ayarlanmasinda kullanilir.

6.1 Statik Yönlendirmeye Giris

6.1.3 Statik Yönlendirme Konfigürasyonu

Bu bölümde statik yönlendirme konfigürasyonu için gerekli adimlar listelenecek ve basit örnekler verilecektir.

Statik yönlendirmede su adimlar kullanilacaktir:

1. Istenen tüm hedef aglarin , alt ag maskelerinin , alt ag geçitlerinin tanimlanmasi yapilacaktir. Alt ag geçidi , diger arayüzler yada bir sonraki tanimlanmis adres olabilir.
2. Global konfigürasyon moduna girilir.
3. **ip route** komutu ile alt ag geçidine iliskin hedef adres ve alt ag maskesi izlenir. Istege bagli olarak yönetimsel uzaklik eklenir.
4. Üçüncü adim diger hedef aglarin tanimlanmasi için tekrarlanir.
5. Global konfigürasyon modundan çikilir.
6. **copy running-config startup-config** komutu kullanilarak NVRAM e aktif konfigürasyon kayit edilir.

Örnegin: Agimiz üç adet routerin basit konfigürasyonundan olussun. Hoboken routeri konfigürasyon sonucunda 172.16.1.0 ve 172.16.5.0 agina ulasabilsin. Bu aglarin alt ag maskeleri 255.255.255.0 olsun.

Paketler hedef ag olarak 172.16.1.0 a yönlendirilsin ve paketler 172.16.5.0 in hedef adresi olsun. Statik yönlendirme ile bu islem gerçeklestirilir.

Statik yönlendirmede ilk olarak yerel arayüzlerin diger aglara olan alt ag geçidinin konfigürasyonu gerçeklestirilir. Yönetimsel uzakliklar belirtilmemistir.. Yönlendirme tablosu yüklendigi zaman 0 oldugu varsayilir. Yönetimsel uzaklik direkt ag baglantilarinda 0 olur.

Iki statik yönlendirmede gelecek adreslere onlarin alt ag geçidi kullanilarak konfigürasyon yapilir. Ilk yönlendirme olan 172.16.1.0 agina 172.16.2.1 nin alt ag geçid adresi girilir. Ikinci yönlendirmede ise 172.16.5.0 agina 172.16.4.2 nin alt ag geçidir. Uzaklik tanimlanmamissa 1 oldugu varsayilir.

6.1 Statik Yönlendirmeye Giris

6.1.4 Varsayilan Yönlendirme Iletiminin Konfigürasyonu

Varsayilan yönlendirmede hedef ile yönlendirme paketleri kullanilirken yönlendirme tablosundaki diger yönlendirmeler eslestirilemez. Internette tüm aglara yapilan yönlendirmeler çogu zaman lüzumsuz ve elverissizdir.internet trafigi için routerlar tipik olara konfigüre edilirler.

Statik yönlendirmede varsayilan yönlendirme formati asagidaki gibidir

ip route 0.0.0.0 0.0.0.0 [*bir sonraki adres* | *giden arayüz*]

0.0.0.0 maskesi yönlendirilen paketlerin hedef ip adreslerini lojik "ve" islemine tabi tutar. Eger paket yönlendirme tablosundaki yönlendirmelerle eslesmiyorsa 0.0.0.0 agina yönlenecektir.

Varsayilan yönlendirme konfigürasyonunda asagidaki adimlar izlenir:

1. Global konfigürasyon moduna girilir.
2. **ip route** komutu yazilarak hedef ag için 0.0.0.0 ve alt ag için 0.0.0.0 adresleri girilir. Bir sonraki routerin ip adresi yada dis aga olan baglantilara yerel routerdan varsayilan bir yönlendirme yapmak için alt ag geçidi girilir.
3. Global konfigürasyon modundan çikilir.
4. **copy running-config startup-config** komutu kullanilarak NVRAM e aktif konfigürasyon kayit edilir.

Statik yönlendirme bölümünde , Hoboken routerindan Sterling teki 172.16.1.0 agina ,Sterling routerindan Waycross daki 172.16.5.0 agina erisimin konfigürasyonu yapilmisti. Hoboken dan diger aglara paketlerin yönlendirilmesi mümkündür. Yinede hiç biri Sterling nede Waycross direkt olmayan ag baglantilarina paketlerin nasil geri dönecegini bilmeyecektir. Statik yönlendirmede direkt olmayan hedef agin her biri için Sterlingte ve Waycrossta konfigürasyon yapilmalidir. Büyük aglarda ölçeklendirilebilir bir çözüm yoktur.

Sterling baglatilari seri-0 arayüzü ile direkt olmayan baglantilara baglanir. Waycross direkt olmayan tüm aglara sadece bir baglanti ile baglanacaktir. Bunu seri-1 arayüzü ile gerçeklestirir. Sterling ve Waycross da varsayilan yönlendirme direkt olmayan baglantilar için yönlendirme saglayacaktir.

6.1 Statik Yönlendirmeye Giris

6.1.5 Statik Yönlendirme Konfigürasyonunun Dogrulanmasi

Statik yönlendirme konfigüre edildikten sonra yönlendirme tablosunda bulunanlarin dogrulanmasi önemlidir. Bunun için **show running-config** komutu kullanilir. RAM deki statik yönlendirmenin dogru girildigini dogrulamak için aktif konfigürasyon gözden geçirilir. **show ip route** komutu kullanilarak yönlendirme tablosunun içindeki statik yönlendirmenin yapildigindan emin olunur.

Statik yönlendirme konfigürasyonu için asagidaki adimlar izlenir:

- Yönetici moddayken aktif konfigürasyon **show running-config** komutu ile incelenir.
- Statik yönlendirmenin dogru girildigi dogrulanir. Eger dogru degilse global konfigürasyon moduna geri dönülür yanlis yönlendirme geri düzeltilir.
- **show ip route** komutu girilir
- yönlendirme tablosundaki yönlendirme konfigürasyonu dogrulanir.

6.1 Statik Yönlendirmeye Giris

6.1.6 Statik Yönlendirme Konfigürasyonundaki Sorunlarin Giderilmesi

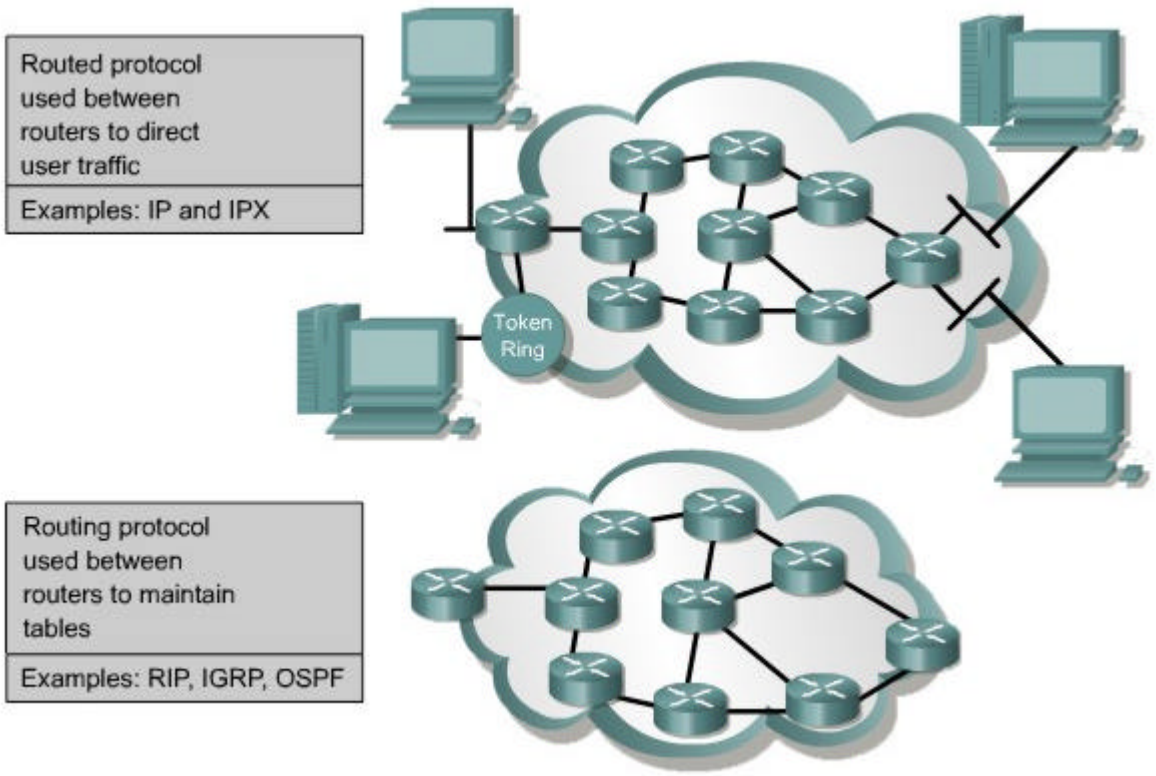
Statik yönlendirme konfiügrasyonunda , Hoboken routerindan Sterling teki 172.16.1.0 agina ve Waycross daki 172.16.5.0 agina statik yönlendirme konfigürasyonu ile erisilebilir. Bu konfigürasyonu kullanirken dügüm Sterlingin 172.16.1.0 agindan 172.16.5.0 a ulasamayabilir. 172.16.5.0 agindayken ping atilirsa basarisiz olur. a **traceroute** komutu ile Sterlingten ayni adreslere ping atilir. **Traceroute** nerede kaybolmustur. ICMP paketleri Hoboken den geri dönmüs. Fakat Waycross dan dönmemis. Routerlarin birinde problem vardir. Hoboken roterina telnet yapilir. Tekrar 172.16.5.0 agina baglanir Waycross a ping atilir. Bunun basarilmis olmasi gerekir. Çünkü Hoboken direkt olarak Waycross a baglidir.

6.2 Dinamik Yönlendirmeye Genel Bakis

6.2.1 Yönlendirme Protokollerine Giris

Yönlendirme protokolleri baslangiç fonksiyonlari ve görevlerince yönlendirmeden farklidir.

Yönlendirme protokolleri diger roterlarda kullanilan bir iletisimdir. Buna izin verilen bir router dagdaki diger routerlarla bilgilerini paylasarak diger routerlara olan yakinligi hakkindaki bilgileri bilir. Routera bilgileri diger roterlardan getirilir. Bunun için yönlendirme protokolleri kullanilir. Bunlari kullanarak yönlendirme tablolari olusturulur ve korunur.



Yönlendirme protokolleri ne iliskin örnekler:

- Yönlendirme Bilgi Protokolü (RIP)
- Içsel Alt Ag Geçidi Yönlendirme Protokolü (IGRP)
- Gelismis Içsel Alt Ag Geçidi Yönlendirme Protokolü (EIGRP)
- Açik Ilk Yol Testi (OSPF)

Yönlendirme protokolü direkt kullanici trafigini kullanir. Yönlendirme protokolü yeterli bilgileri planlanmis adreslemede bir hosttan digerine paket yollarken ag katman adreslerini sunarlar.

Yönlendirme protokolüne örnek verecek olursak:

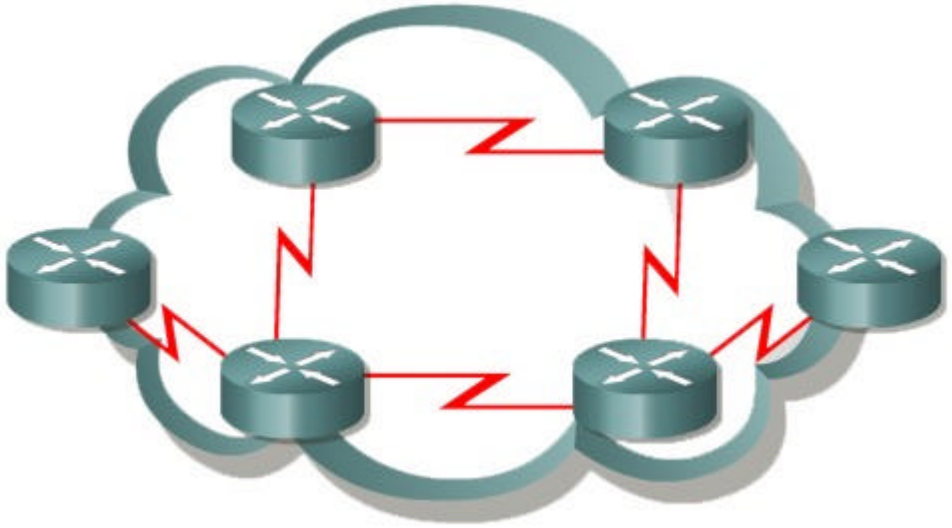
- Internet Protokolü (IP)
- Internetwork Paket Degisimi (IPX)

6.2 Dinamik Yönlendirmeye Genel Bakis

6.2.2 Özerk Sistemler

Özerk sistem (AS), yönetim stratejileri ve yönetim biçimleri bir olan bir ag altinda toplanmis bütünlüge denilir. Dis dünyada özerk sistemler tekbir bütün olarak gözden geçirilirler. Özerk sistemler bir yada birçok operatör tarafindan çalistirilirlar.

Internet Numaralarinin Amerikan Kayitçisi (ARIN) , servis sunucular yada yöneticiler her özerk sisteme bir kimlik numarasi atarlar. Bu özerk sistem numaralari 16bitlik numaralardir. Yönlendirme protokolleri , mesela Cisco nun IGRP için özerk sistem atanmasini ister.



6.2 Dinamik Yönlendirmeye Genel Bakis

6.2.3 Yönlendirme Protokollerinin ve Özerk Sistemlerin Amaçlari

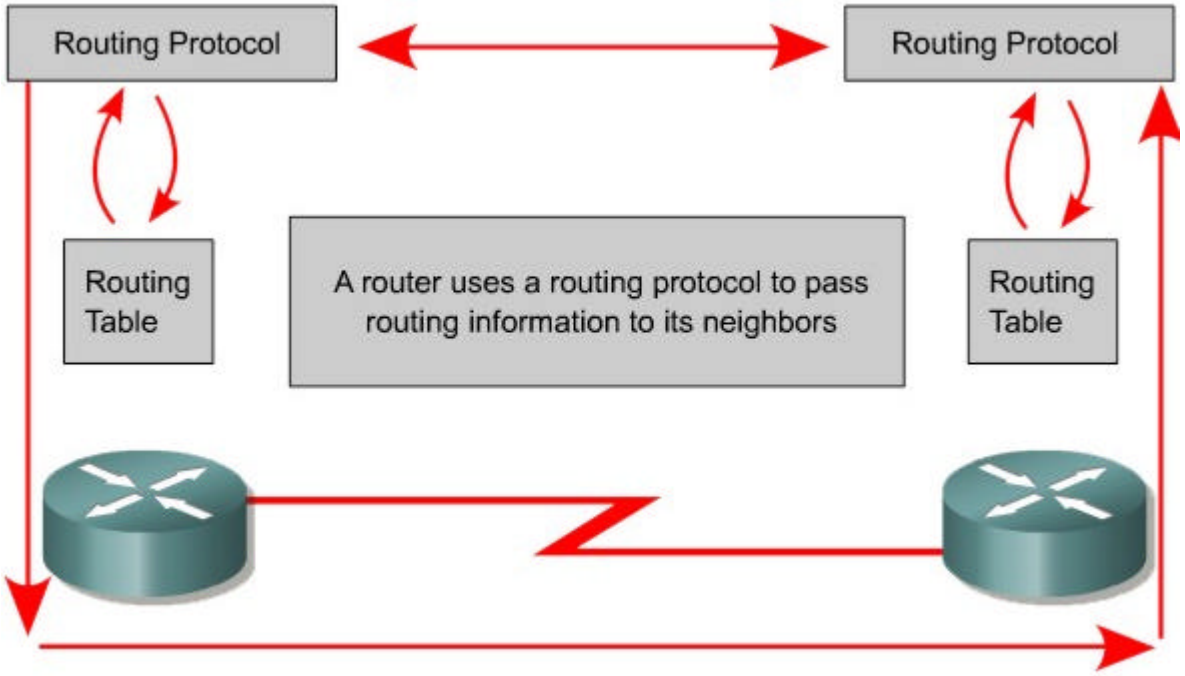
Yönlendirme protokollerinin hedefi yönlendirme tablolarini olusturmak ve korumaktir. Bu tablo , aglar için gerekli olan ögrendikleri aglar ve beraberindeki portlari içerir.routerlar diger routerlardan kendi arayüzlerinin konfigürasyonundan bilgileri ögrenerek yönetim bilgilerini çevirirken yönlendirme protokollerini kullanirlar.

Yönlendirme protokolleri tüm mevcut routerlari ögrenirler. Tabloda en iyi yönleri yerlestirirler ve geçerliliklerini kaybettikleri zaman geri alirlar. Router yönlendirilmis protokol paketlerini iletirken yönlendirme tablolarindaki bilgileri kullanirlar.

Yönlendirme algoritmasi dinamik yönlendirmenin temelidir. Her zaman degisken aglarin topolojisidir. Çünkü büyüme , yeniden konfigürasyon yada kayiplarda agin veritabani degisebilir. Ag veritabani yeni topolojilerin yanlissiz tutarliligi yansitmalarini ister.

Routerlarin hepsi ag islerinde bazi bilgilerle islem görürler. Ag ortami bir noktada birlestilirilmek zorundadir. Hizli yakinsama arzu edilir. Çünkü routerlar yönlendirmede dogru karar verip uygulama yaparken zamanin periyotlarinda is görürler.

Özerk sistemler , genel ag çalisma ortamlarinin bölümlerini saglarlar. Küçük ve yönetilebilir aglardir. Her özerk sistem kurallari, ilkeleri ve özerk sistem numarasini kendisi ayarlar. Böylece dünyadaki diger özerk sistemlerden ayirt edilebilir ve tekil olacaktir.



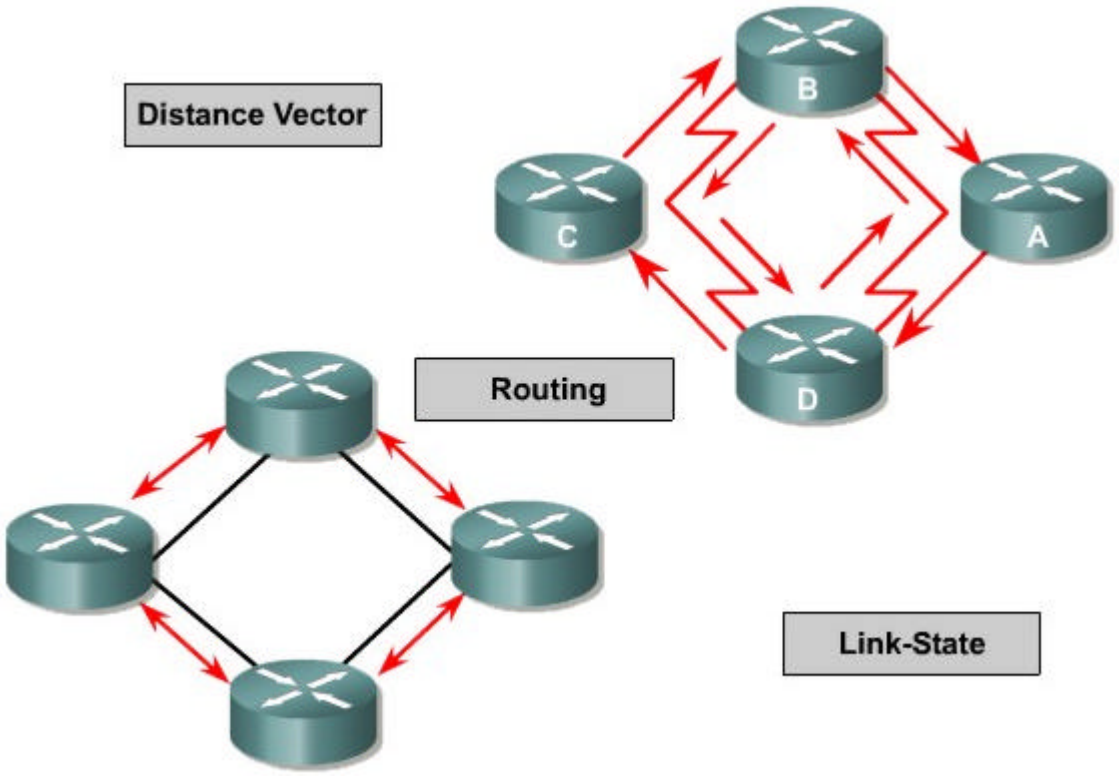
6.2 Dinamik Yönlendirmeye Genel Bakis

6.2.4 Yönlendirme Protokollerinin Siniflarinin Belirtilmesi

Yönlendirme protokolleri iki kategori olarak tek bir sinif altinda olabilirler:

- Uzaklik vektörü
- Baglanti - durum

Uzaklik vektörü vektör yaklasimlarina ve ag toplulugundaki baglantilara olan uzakliga göre yönlendirme yapar.

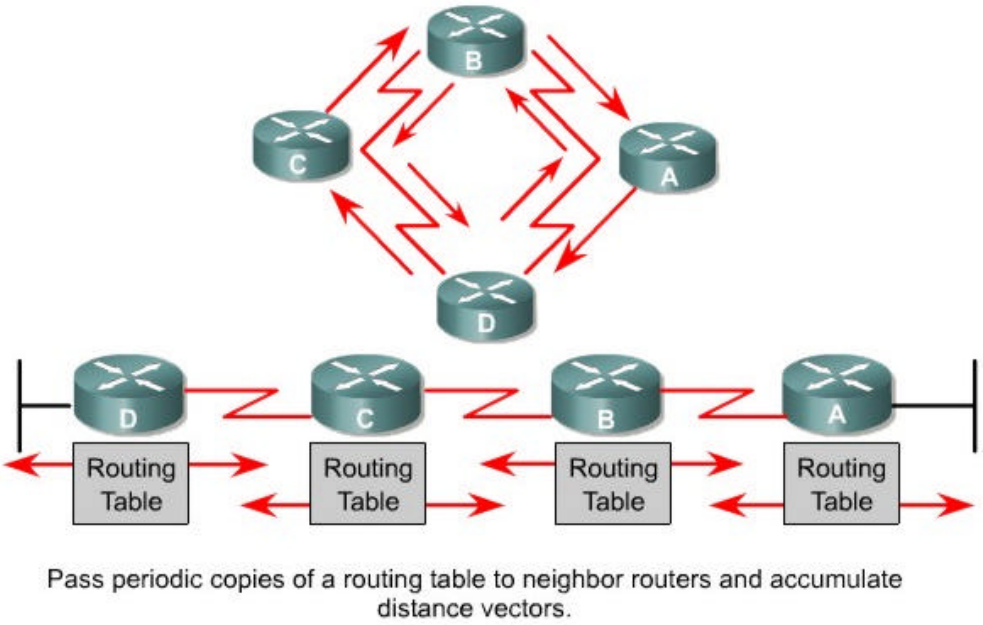


6.2 Dinamik Yönlendirmeye Genel Bakis

6.2.5 Uzaklik Vektör Yönlendirme Protokolünün Özellikleri

Uzaklik vektör yönlendirme algoritmalari, bir routerdan diger bir routera yönlendirme tablolarinin kopyalarini periyodik olarak gönderirler. Düzenli olarak yapilan güncellemelerle routerlar arasinda topoloji degisiklikleri haberlesilir. Uzaklik vektörünün temel yönlendirme algoritmasi Bellman-Ford algoritmalari olarak ta bilinirler.

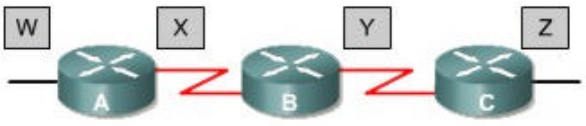
Her router yakinlarindaki direkt olarak baglandigi routerdan yönlendirme tablolarini alirlar. Mesela B-routeri bilgileri A-routerindan bilgileri alsin. A-routeri B´ye uzaklik vektör numaralarini ekler. B-routerina gelen yeni yönlendirme tablosu yakinlardaki diger C-routerina gönderilir. Yakinlardaki diger routerlara olan tüm yönler adim adim islenir.

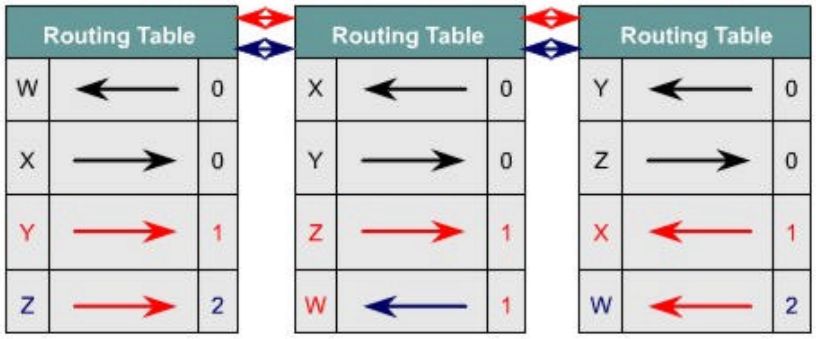


Pass periodic copies of a routing table to neighbor routers and accumulate distance vectors.

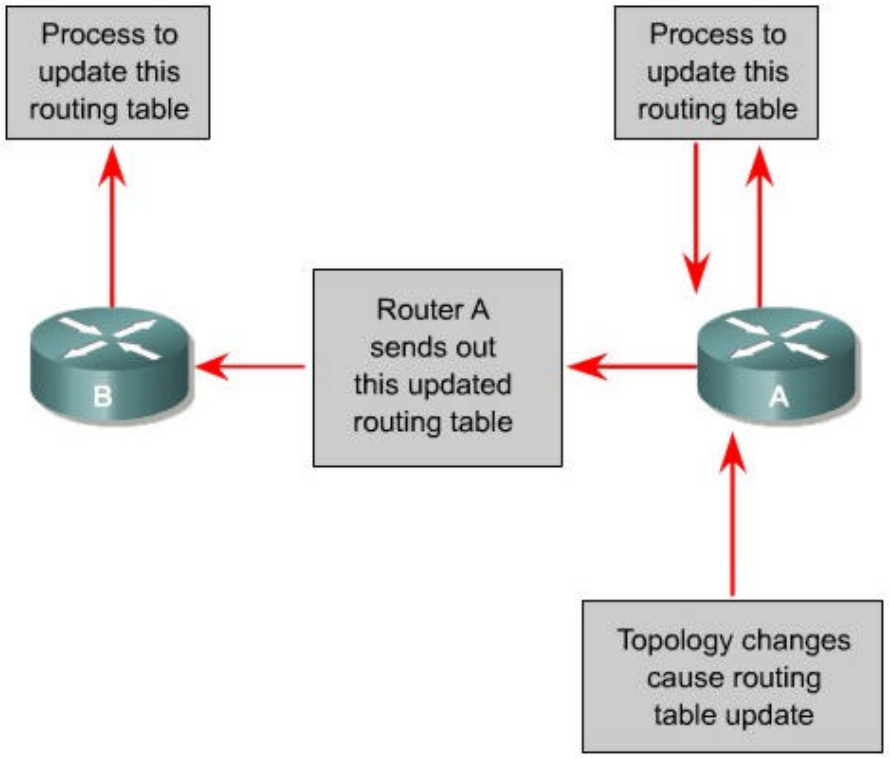
Algoritma sonunda , ag topolojisinin bilgilerinin veritabani da korunmasi için uzaklik vektörleri biriktirilir. Yine de uzaklik vektör algoritmasi , her router sadece yakinindaki routeri görsün diye ag çalisma ortaminin tam topolojisini bilmesine izin vermez.

Her router uzaklik vektörünü kullaranak kendi yakinindaki belirtirler. Arayüzlerin iletiminde , her bir direkt bagli agin uzakligi 0 ile gösterilir. Routerlar yakinlarindakilerin bilgilerini çevirirken hedefteki aglara olan en iyi yolu kesfederler. A-Routeri B routerindan aldigi bilgileri çevirerek diger aglarin yapisini ögrenir. Her bir agin digerine olan gidisi , çok uzaklardaki agarla nasil gidilecegi yönlendirme tablosunda uzaklik vektörlerinin biriktirilmesi ile mümkündür.

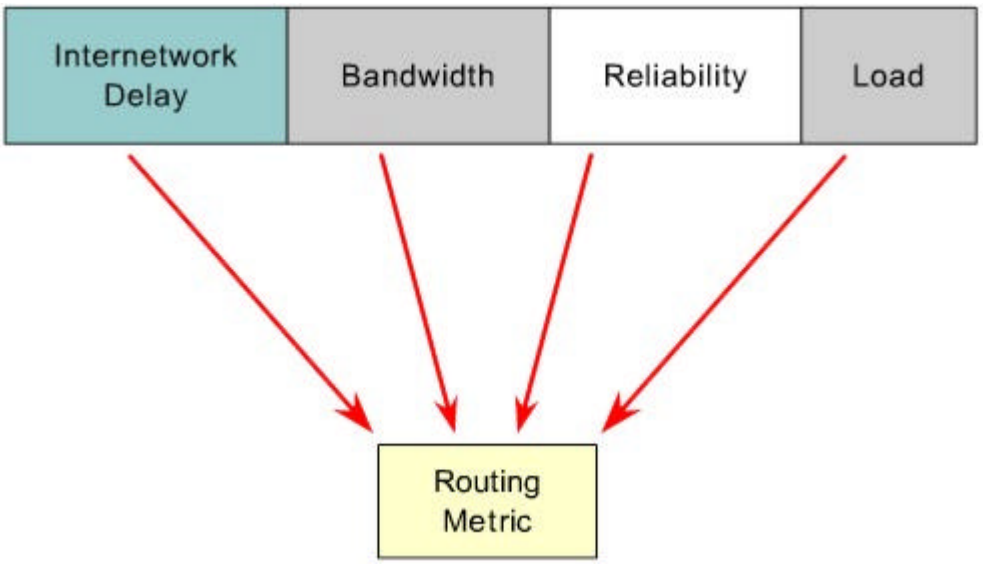




Yönlendirme tablosu güncellemeleri topolojide bir degisiklik oldugu zaman yapilir. Ag kesif islemleri gibi topoloji degisiklikleri bir routerdan diger bir routera adim adim islenir.



Uzaklik vektörü algoritmalari her router için bitisiklerindeki her bir routerin gönderdigi yönlendirme tablosunu çagirirlar. Yönlendirme tablolari metrik olarak tanimlanmis tüm yollar hakkindaki bilgileri muhafaza ederler. Ayrica tabloda , ilk roterdan yolu üzerindeki her bir routerin lojik adreslerini içerirler.



Uzaklik vektörünün analojisinde anayollarin kesismesinde bulunan sinyallerde olabilir. Sinyal noktalarina dogru hedef ve hedefe olan uzaklik gösterilir. Daha uzaklardaki anayol düstügünde , diger sinyal noktalari hedefe dogrudur. Fakat uzaklik kisalmistir. **Uzaklik artsada azalsada trafik en iyi yolu izler.**

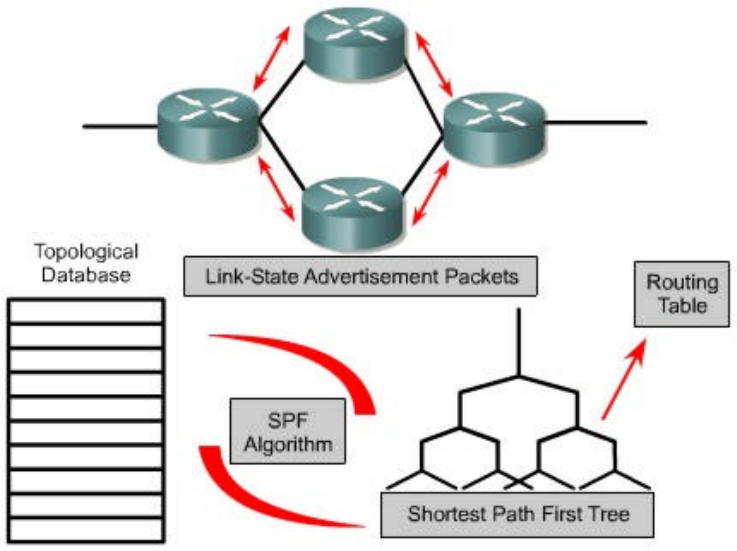
6.2 Dinamik Yönlendirmeye Genel Bakis

6.2.6 Baglanti-Durum Yönlendirme Protokolünün Özellikleri

Ikinci temel algoritma olarak yönlendirme için baglanti-durum algoritmasi kullanilir. Bu algoritma Dijkstras algoritmasi yada enkisa yol ilk yoldur (SPF) algoritmasi olarak ta bilinir. Baglanti-Durum yönlendirme algoritmalari topoloji bilgilerinin karisik veri yapisini korurlar. Uzaklik vektör algoritmasinda uzak aglar hakkindaki bilgiler kesin degildi. Uzaktaki routerlarin bilgileri bilinmiyordu. Baglanti-Durum yönlendirme algoritmasi uzaktaki routerlarin birbirine nasil baglandiginin hakkindaki tüm bilgileri bulundururlar.

Baglanti-Durum yönlendirmede kullanilanlar:

- **Baglanti-Durum reklamlari (LSAs) –** Diger routerlara gönderilen yönlendirme bilgilerinin oldugu küçük paketlerdir.
- **Topoloji Veritabani –** Topoloji Veritabani , Baglanti-Durum reklamlarindan toplanilan bilgilerin saklandigi yerdir.
- **SPF Algoritmasi –** Enkisa Yol Eniyi yoldur algoritmasi veritabanindaki sonuçlara göre performansi hesaplarlar.
- **Yönlendirme Tablolari –** arayüzleri ve bilinen yollari listeler

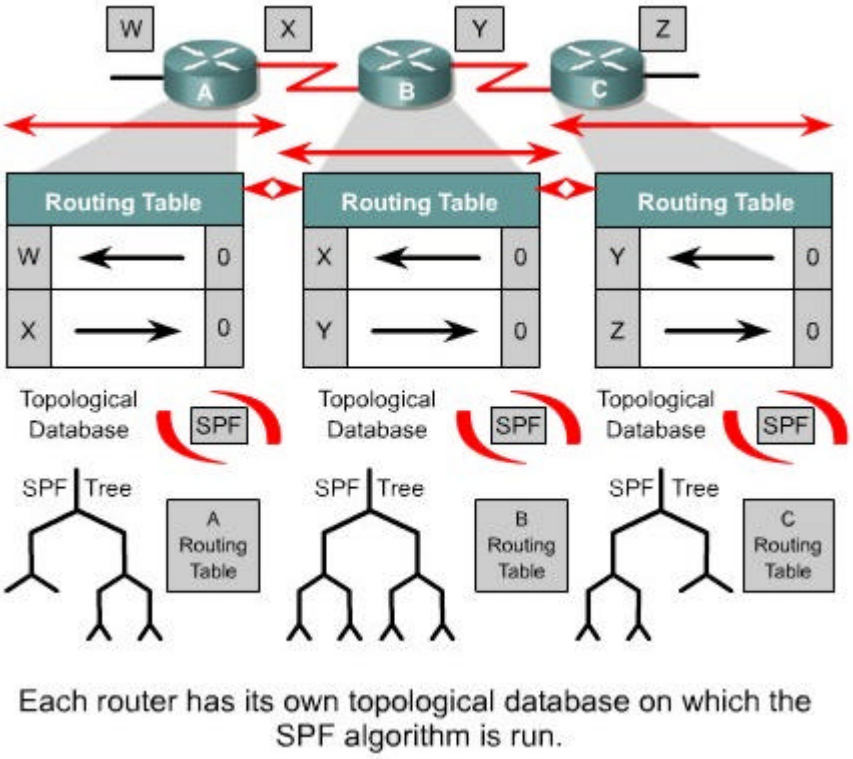


Routers send LSAs to their neighbors. The LSAs are used to build a topological database. The SPF algorithm is used to calculate the shortest path first tree in which the root is the individual router and then a routing table is created.

Baglanti-Durum yönlendirme ile ag kesfetme islemleri:

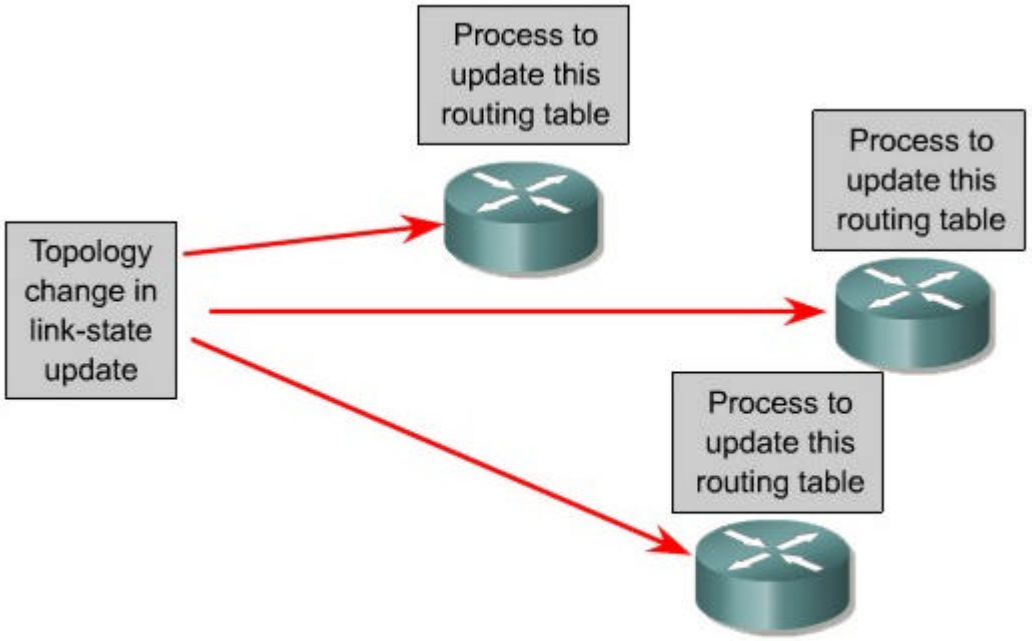
Bilgilere direkt sahip olmak için aglara direkt baglanti baslatildiginda routerlar arasinda bu algoritmalar degistirilir. Her router paralelindeki diger router ile degistirilen tüm baglanti-durum algoritmalarini veritabaninda olustururlar.

Enkisa Eniyi Yoldur algoritmasi aga ulasilabilirligini hesaplar. Router bu agin lojik agacini olusturur. Ag ortamindaki baglanti-durum protokolünde her bir aga mümkün yollarin olusunu köke ekler. Router en iyi yolu listeler ve yönlendirme tablosuna arayüzlerin uzaktaki aga olan uzakliklarini listeler. Topolojinin durum detaylarini ve elemanlarini diger veritabanlarinda dahi korunur.



Each router has its own topological database on which the SPF algorithm is run.

Router , baglanti-durum topolojisindeki gönderilen degistirilmis bilgilerden ilk olarak haberdar olur. Ag ortamindaki tüm routerlara ortak yönlendirme bilgilerini gönderir. Yakinsama arsivlerine her bir router yakinlarindaki routerlarin isimleri, arayüz durumlari ve yakinlarindaki hattin degerleri hakkindaki bilgileri yakalarlar. Router , baglanti-durum algoritmasi paketleri ile yakinlardaki yenilikler ile hatlardaki degisiklik bilgilerinin listelerini olustururlar. Paketler diger routerlarin hepsi çevirsin diger disari gönderilir.



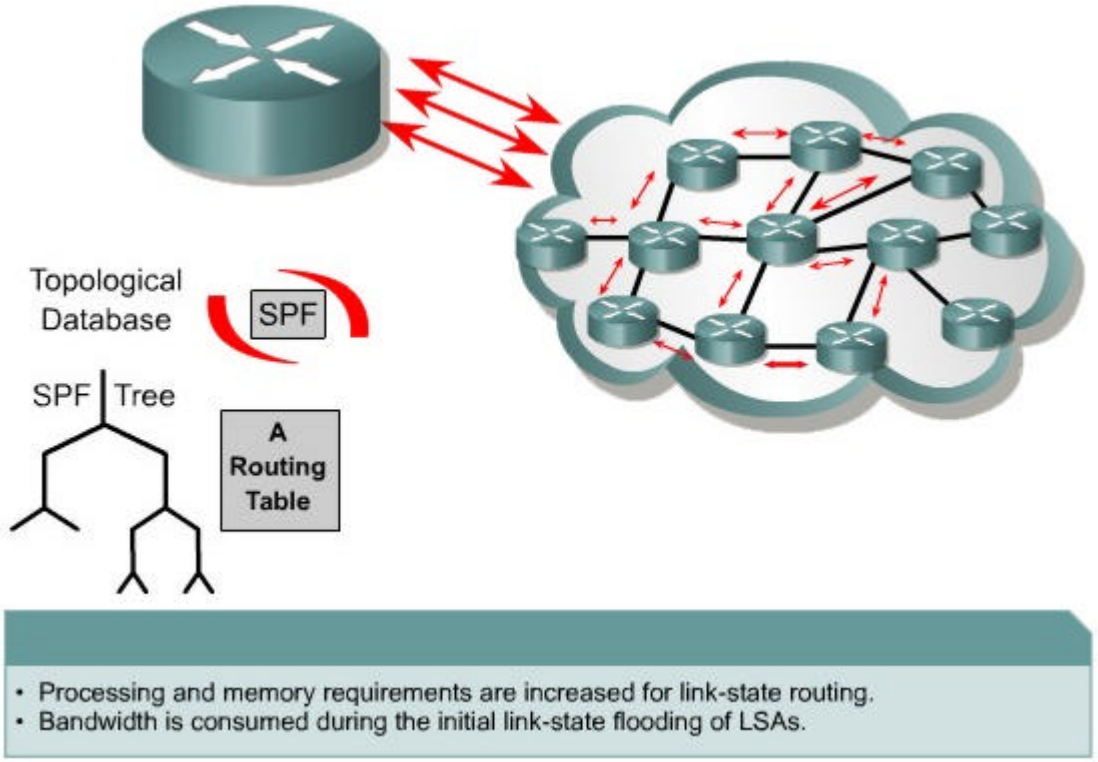
Each router has its own topological database on which the SPF algorithm is run.

Router paketleri çevirdigi zaman veri tabani , en son gelen bilgileri ve enkisa yol eniyi yol algoritmasi kullanan diger aglara yol hesaplari ve ag ortaminda kullanilan biriktirilmis verinin haritasini günceller.

Baglanti- durum ilgileri:

- Islemci ek yükü
- Hafiza gereksinimleri
- Bantgenisligi tüketimi

Routerlar baglanti-durum algoritmasini kullanirlarken uzaklik vektör yönlendirme protokolünden daha çok hafiza ve islem gücüne gereksinim duyarlar. Routerlarin hafizalari çesitli veritabanlarindan tüm bilgileri alabilmek için topoloji agaci ve yönlendirme tablosu olusturmak için yeterli olmak zorundadir. Baglanti durum paketleri baslangiçta bant genisligini tüketirler. Kesif islemleri süresince tüm routerlar diger routerlara paketleri göndermek için bu yönlendirme protokolünü kullanirlar. Yönlendirme trafigi kullanici verilerini tasimak için geçici olarak bant genisligini kullanirlar ve agda tasma olusur. Baslangiçtaki bu taskinlik , bu protokolün genellikle en ufak bant genisligine ihtiyaç duyar.



- Processing and memory requirements are increased for link-state routing.
- Bandwidth is consumed during the initial link-state flooding of LSAs.

6.3 Yönlendirme Protokollerine Genel Bakis

6.3.1 Yol Belirleme

Router bir data hattindan digerine paketlerin yoluna karar verirken iki temek fonksiyon kullanir:

- Yol belirleme fonksiyonu
- Anahtarlama fonksiyonu

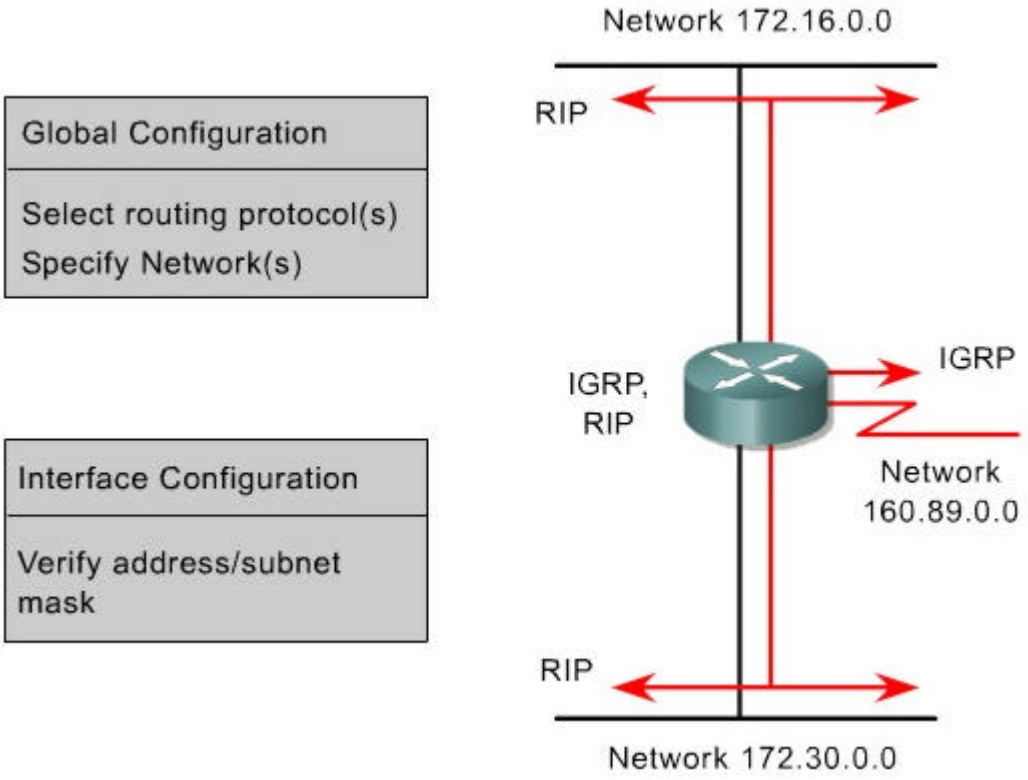
Yol belirleme fonksiyonu ag katmaninda meydana gelir. Bu fonksiyon , paketin tercihli olarak islenmesini olusturmak ve yol tayin etmek için routerlarda açiktir. Routerlar, paket iletiminde anahtarlama fonksiyonunu kullanmak istediklerinde en iyi yolu seçmek için yönlendirme tablolarini kullanirlar.

Anahtarlama fonksiyonu , özdes routerlarda ikinci arayüze iletimde ve bir arayüzde paket kabulü için islem gören içsel bir fonksiyondur. Sonraki veri hatti için uygun çerçeve tipinde routerin paketleri olusturmasinda bu fonksiyon kullanilir.

6.3 Yönlendirme Protokollerine Genel Bakis

6.3.2 Yönlendirme Konfigürasyonu

Genel açilis ve yönlendirme parametrelerin routerda ayarlarini yapmak için IP yönlendirme protokol açilir. Genel görevler seçilen yönlendirme protokolüne yerlestirilmistir. RIP, IGRP,EIGRP yada OSPf örnek olarak verilebilir. Asil görev yönlendirme konfigürasyon modundaki IP ag numaralarinin gösterilmesidir. Dinamik yönlendirme , diger routerlar ile haberlesmede yayinlar ve çoklu yayinlari kullanirlar. Metrik yönlendirme routerlarin her bir aga en iyi yolu bulmasinda yardimci olurlar.



router komutu yönlendirme islemlerini baslatir.

network komutu gereklidir. Çünkü yönlendirme islemlerini açarak yönlendirme güncellemelerinin çevrilmesi ve gönderilmesinde hangi arayüze katilacagina karar verir.

Yönlendirme konfigürasyonuna örnek verecek olursak:

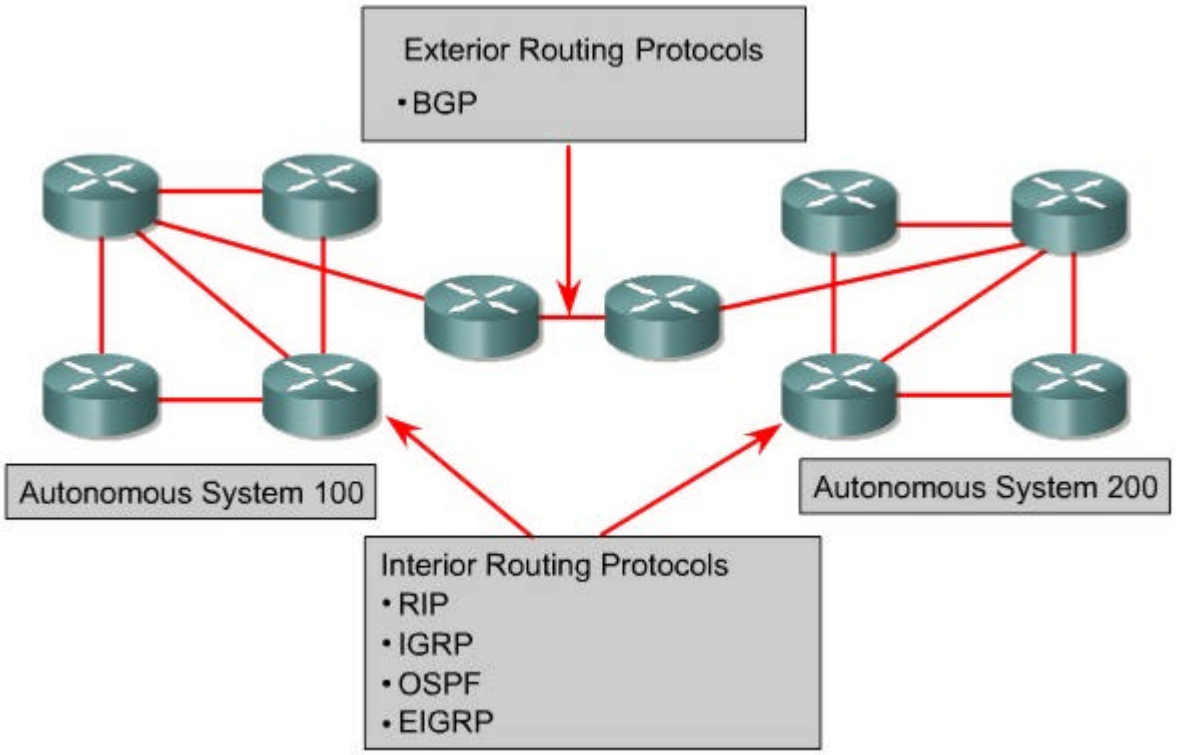
GAD(config)#**router rip**
GAD(config-router)#**network 172.16.0.0**

Ag numaralari , ag sinif adreslerinin temelidir. Alt ag adresileri yada bireysel host adresleri degildirler. Esas ag adresleri A-Sinifi , B-Sinifi, C-Sinifi numaralari ile sinirlidir.

6.3 Yönlendirme Protokollerine Genel Bakis

6.3.3 Yönlendirme Protokolleri

Internet katmaninda TCP/IP nin protokollerinde router IP yönlendirme protokolünü belirli yönlendirme protokollerin yönlendirme sayesinde gerçeklestirmek için kullanabilirler. Yönlendirme protokollerin kapsamlarina örnek verecek olursak:



- **RIP** – Uzaklik vektörü içerisindeki yönlendirme protokolü
- **IGRP** – Cisco nun uzaklik vektörü içerisindeki yönlendirme protokolü
- **OSPF** – Baglanti-Durum içerisindeki yönlendirme protokolü
- **EIGRP** – Cisco nun gelismis uzaklik vektörü içerisindeki yönlendirme protokolü
- **BGP** – Uzaklik vektörü disindaki yönlendirme protokolü

Yönlendirme Bilgi Protokolü , RFC 1058 in içinde orijinal olarak belirlidir. Içerdigi anahtar özellikleri asagida gösterilmistir:

- Uzaklik vektörü yönlendirme protokolü
- Atlama sayisi yol seçimi için metre gibi kullanilir.
- Eger atlama sayisi 15 den daha büyük olursa paket atilir.
- Yönlendirme güncellemelerinin her 30 saniyede yayinlandigi varsayilir.

IGRP protokolü Cisco tarafindan gelistirilmistir. IGRP de dizayninda asagidaki karakteristik özellikler vurgulanmistir:

- Uzaklik vektörü yönlendirme protokolüdür.
- Bantgenisligi , yükleme , gecikme ve güvenebilirlik birlesik metrik olusturulurken kullanilir.
- Yönlendirme güncellemelerinin her 90 saniye yayinlandigi varsayilir.

OSPF, baglanti-durum yönlendirme protokolüne özel bir protokoldür. Anahtar karakteristikleri asagida belirtilmistir:

- Baglanti – durum yönlendirme protokolüdür.
- RFC 2328´de tanimlanmis açik standart yönlendirme protokolüdür
- Hedefe düsük maliyeti hesaplayan SPF algoritmasini kullanir.
- Yönlendirme güncellestirmeleri topolojide bir degisiklik ortaya çikinca yayinlanir. .

EIGRP , Cisco´nün gelistirdigi uzaklik vektörü yönlendirme protokolüdür. Anahtar karakteristikleri asagidaki gibidir.

- Gelismis bir uzaklik vektör yönlendirme protokolüdür.
- Dengeleyici yük kullanirlar
- Uzaklik vektörü ve baglanti-durum özelliklerinin kombinasyonunu kullanir.
- Yayilim Güncelleme Algoritmasi(DUAL) kullanarak en kisa yolu hesaplarlar
- Yönlendirme güncellemeleri her 90 saniyede yayinlanir yada topoloji degistiginde tetiklenir

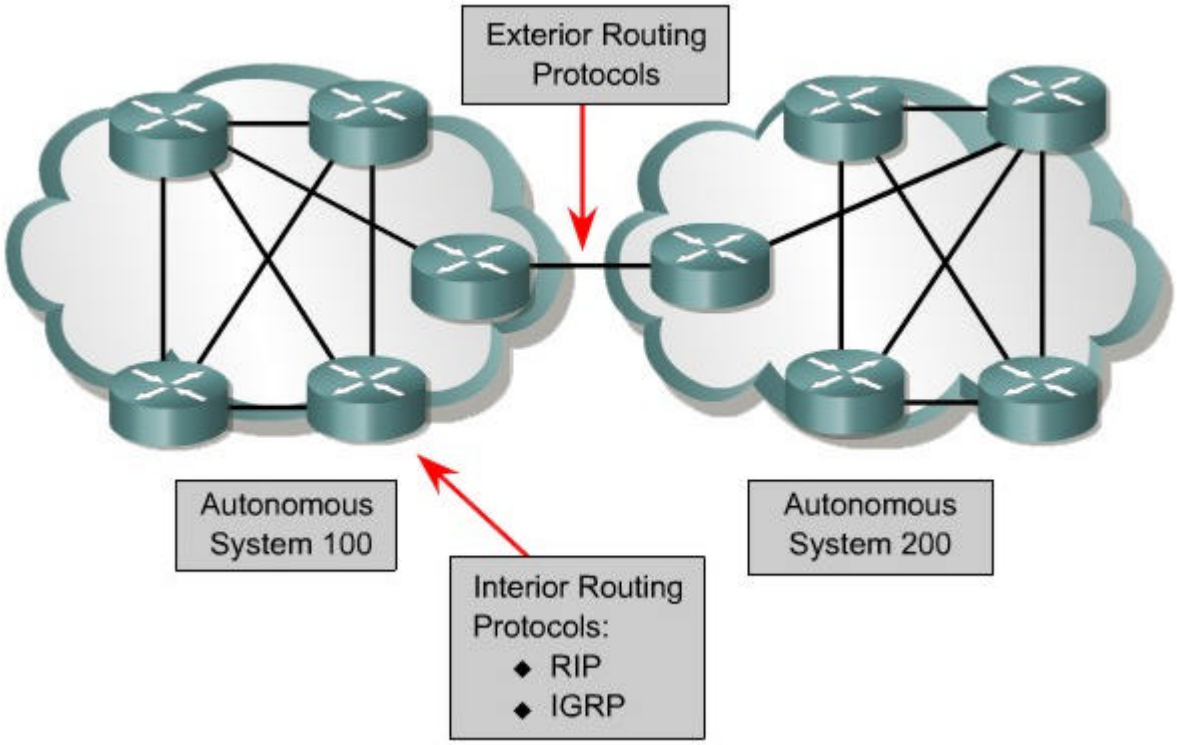
Sinirli Alt Ag Geçidi Protokolü (BGP) bir dis yönlendirme protokolüdür. Anahtar karakteristikleri asagidaki gibidir:

- Uzaklik vektörü bir yönlendirme protokolüdür
- Internet Servis saglayici ve kullanicilari arasinda kullanilirlar
- Özerk sistemler arasinda internet trafigini yönlendirmede kullanilirlar

6.3 Yönlendirme Protokollerine Genel Bakis

6.3.4 Özerk Sistemler ve IGP´ye Karsi EGP

Içsel yönlendirme protokolleri agda bir organizasyonun yollarinin kimin kontrolü altinda oldugunu kullanmak için dizayn edilirler. Içsel yönlendirme protokollerinin agdaki en iyi yolun bulunmasi için dizayn bir kriterdir. Diger bir deyisle, metrik ve metrigin nasil kullanilacagi içsel yönlendirme protokollerinde önemli bir elemandir.



Dis yönlendirme protokolleri iki farkli organizasyonun kontrolü altindaki diger iki ag arasinda kullanmak için dizayn edilmistir. Tipik olarak farkli internet servis saglayicilarda yada isletme ve servis saglayici arasinda kullanilir. Örnegin; isletme BGP protokolünü çalistirsin. Bu bir dis yönlendirme protokolüdür. Bir routerdan diger router arasinda ISP olsun. IP dis alt ag geçidi protokolü yönlendirme baslamadan önce üç tane bilginin ayarlanmasini ister:

- Yakinlardaki hangi routerin dis yönlendirme bilgileri listelenecek
- Aglarin tanitimi listelenecek
- Yerel routerdaki özerk sistem numaralari

Dis yönlendirme protokolleri özerk sistemleri yalitabilmelidir. Hatirlanirsa , özerk sistemler diger yöneticiler tarafindan yönetilmekteydi. Aglar farkli sistemler arasinda baglatilarda protokollere sahip olmalilar.

Özerk sistemler numaralarla isimlendirilmek zorundadirlar. Uluslar arasi ARIN yada sunuculardan saglanir. Özerk sistem numaralari 16bitliktir. Yönlendirme protokolleri cisco nun IGRP ve EIGRP gibi tekildirler.

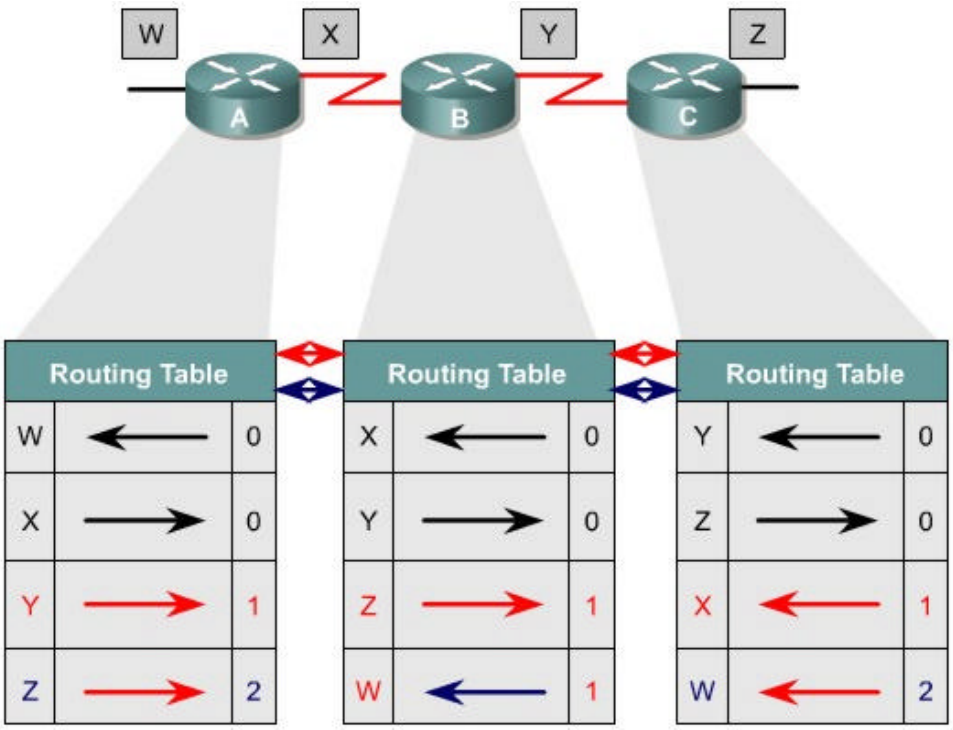
6.3 Yönlendirme Protokollerine Genel Bakis

6.3.5 Uzaklik Vektörü

Uzaklik vektörü algoritmasi (Bellman-Ford algoritmasi olarakta bilinir) her bir router için hepsine çagri yapar ya da sadece yakindakilerine yönlendirme yönlendirme tablolarini paylastirir. Uzaklik vektör algoritmasi yakinlardaki routerlarin temel bilgilerini sunarak yönlendirme karari verirler.

Bu protokol sistem kaynaklarini daha az kullanir. Fakat yavas yakinsamadan katlanilabilir. Genis sistemlere metrik kullanarak ölçeklenemez. Protokolün temeli uzaklik bulmak (atlamanin sayisi) ve çalisma alanindaki her bir baglantiya olan vektördür. Algoritmalar periyotlarda bir routerdan diger bir routera yönlendirmenin tamamlanmasinda kopyalarin geçmesini ihtiva ederler.

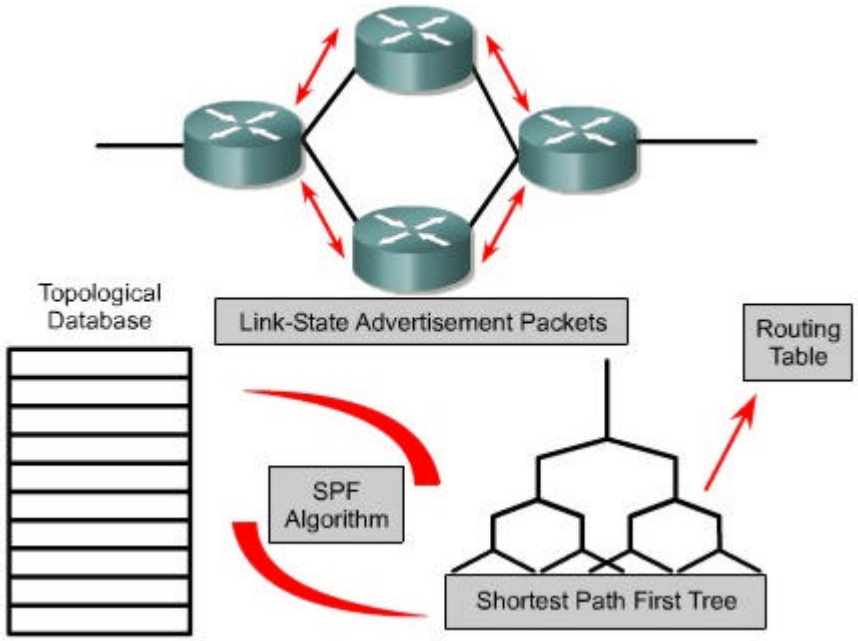
Bu tip yönlendirme protokollerinin , yönlendirme tablolari ile yakinlardaki her bir routera basit bir sekilde ulasmak ister. Her bir ag yolu için yakinlarindaki düsük maliyetli tanitimlari çevirirler. RIP ve IGRP ortak bir uzaklik yönlendirme protokolüdür.



6.3 Yönlendirme Protokollerine Genel Bakis

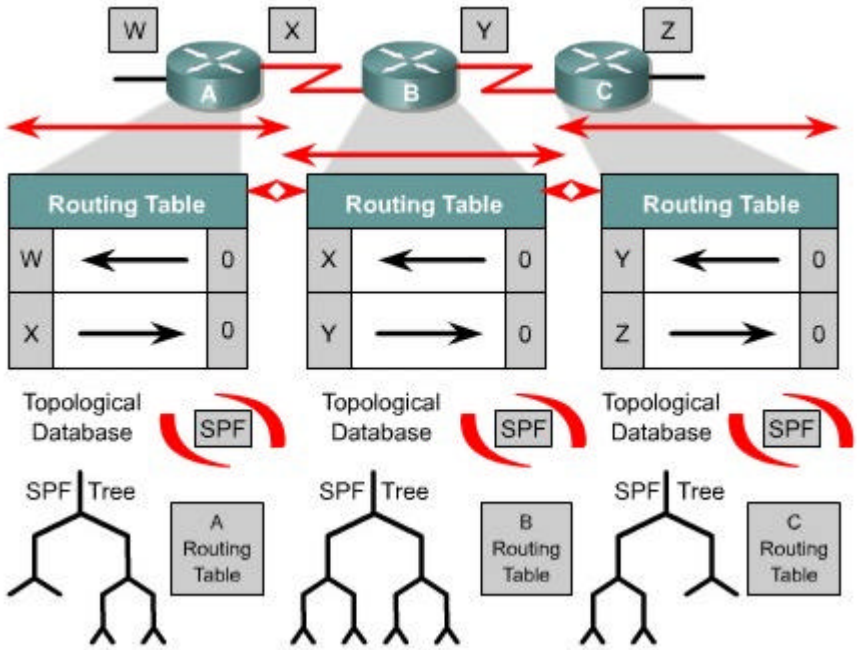
6.3.6 Baglanti-Durum

Baglanti-Durum algoritmasi (En kisa yol en iyi yoldur algoritmasi olarak ta bilinir) tüm agin çalisma agi ortamindaki haritasini olusturarak bilgileri yönlendirir. Her bir router yakinlarindaki her routera paketleri gönderirler. Paketler aglara baglantili routerlari yada agin tanimlamalarini içerirler. Routerlar , agda bilinen site yollarini en kisa sürede ulasmayi hesaplayan ag topolojinin içerigini tamamlayarak hepsini bilgiye çevirirler. Ondan sonra agda her bir tanimlama için en iyi yolun gösterildigi yönlendirme tablosu üretilir. Bir kez yakinsadiginda baglanti-durum protokolü küçük güncelleme paketleri kullanir. Ondan sonra yönlendirme tablosunun tamami kopyalanir. Güncelleme paketleri güncelleme oldukça boydan boya geçirilirler. Böylece yakinsama hizlanmis olur.



Çünkü onlar uzaklik vektör protokollerinden daha hizli bir sekilde yakinsarlar. Baglanti-durum algoritmalarinin yönlendirme döngüleri daha azdir. Bu protokollerin yönlendirme hatalari da azdir. Fakat onlar sistem kaynaklarini kullanirlar. Bu yüzden uygulamalari ve desteklemeleri daha pahalidir. Yinede uzaklik vektöründen genellikle daha çok ölçeklendirilebilirler.

Hat durumunda bir degisiklik oldugu zaman aga bastan basa bildirim yaparlar. Tüm routerlar degisiklileri not ederler. Bundan dolayi yönlerini yeniden ayarlarlar.



Özet

Asagidaki kilit noktalarinin anlasilmis olmasi saglanmalidir:

- Router hedef aga yönlendirmesiz paket gönderemez.
- Ag yöneticileri statik yönlendirmeyi el ile konfigüre ederler.
- Varsayilan yönlendirme alt ag geçitleri ile özel yönlendirmeler routerlara saglanir.
- Statik ve varsayilan yönlendirmeler **ip route** komutunu kullanirlar.
- Statik ve varsayilan yönlendirme konfigürasyonu **show ip route**, **ping**, ve **traceroute** komutlari ile dogrulanir
- Statik ve varsayilan yönlendirmenin sorunlarinin giderilmesi ve dogrulanmasi
- Yönlendirme protokolleri
- Özerk sistemler
- Yönlendirme protokollerinin ve Özerk sistemlerin amaçlari
- Uzaklik vektör yönlendirme protokolünün özellikleri ve örnekleri
- Yönlendirme protokollerinin siniflari
- Durum - uzaklik protokolünün özellikleri ve örnekleri
- Yön belirleme
- Yönlendirme protokolleri (RIP, IGRP, OSPF, EIGRP, BGP)
- Özerk sistemler ve IGP ye karsi EGP
- Uzaklik vektör yönlendirmesi
- Baglanti-durum yönlendirmesi

BÖLÜM - 7

Genel Bakis

Dinamik yönlendirme protokolleri ag yöneticisinin islerini kolaylastirmaya yardimci olabilir. Dinamik yönlendirme, statik yollarin konfigüre edilmesi islemini tamamlar ve zaman tasarrufu saglar. Dinamik yönlendirme ayni zamanda, ag yöneticisinin müdahalesi olmaksizin routerlarin agdaki degisikliklere tepki göstermesine ve yol tablolarinin dogru bir sekilde ayarlanmasina imkan verir. Bununla birlikte sorunlara da yol açabilir. Bu bölümde, protokol tasarimcilarinin ortaya koydugu bazi çözüm asamalarini da alarak dinamik mesafe yönü yol protokolleriyle ortaya çikan bazi sorun ele alinacaktir.

Yönlendirme Bilgisi Protokolü (RIP) (***Routing Information Protocol***), dünyadaki binlerce agda kullanilmakta olan bir mesafe yönlendirme vektörü protokolüdür. Açik standartlara dayali olmasi ve uygulanabilirliginin çok basit olmasi yönüyle bazi ag yöneticilerince çekici bulunmasina karsin RIP, daha gelismis gönderim protokollerinin özelliklerinden ve gücünden yoksundur. Basit olusundan dolayi ag konusunda kendini gelistirmek isteyen kimseler için iyi bir baslangiç protokolüdür. Bu bölümde yine ayrica RIP yapilandirilmasi ve sorun giderme konulari gösterilecektir.

RIP gibi , Dahili Altaggeçidi Yönlendirme Protokolü (IGRP) (***Interieur Gateway Routing Protocol***) de bir mesafe vektörü yönlendirme protokolüdür. IGRP´ den farkli olarak standart temelli bir protokol olmaktan çok Cisco'nun özel bir protokolüdür. Uygulanma kolayligi açisindan IGRP, RIP´e göre daha karmasik bir protokoldür ve bir agin varis adresine ulasmada en iyi yolu saptamak için faktör numaralari kullanir. Bu bölümde IGRP yapilanmasi ve sorun giderme konulari ele alinacaktir

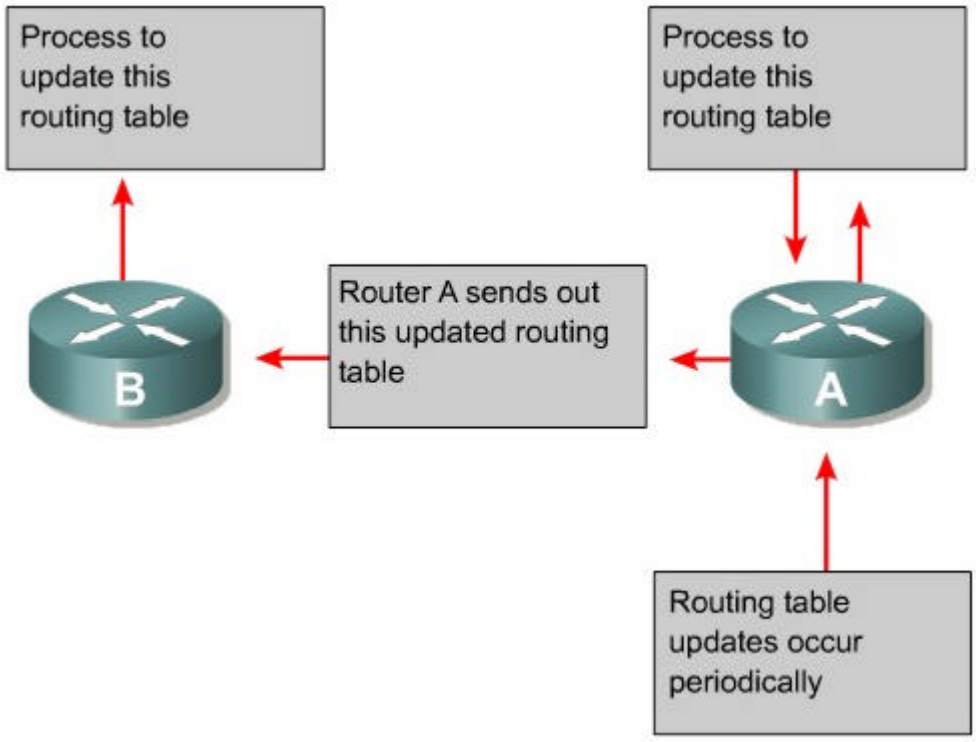
Bu modülü tamamlayan kimseler su konulari yapabiliyor olmalilar:

- Uzaklik vektör yönlendirmesinde yönlendirme döngülerinin nasil gerçeklesecegini açiklayabilmeli.
- Gönderim bilgisinin kesin dogrulugunu temin için, mesafe yönü yönlendirme protokollerince kullanilan farkli yöntemleri açiklayabilmeli.
- RIP' yi konfigüre edebilmeli
- **ip classless** komutunu kullanmali.
- RIP sorunlarini giderebilmeli
- Yük dengelemesinde RIP i konfigüre edebilmeli
- RIP için statik yollar konfigüre edebilmeli
- RIP i dogrulamali
- IGRP' yi konfigüre edebilmeli
- IGRP islemini dogrulayabilmeli
- IGRP sorunlarini giderebilmeli.

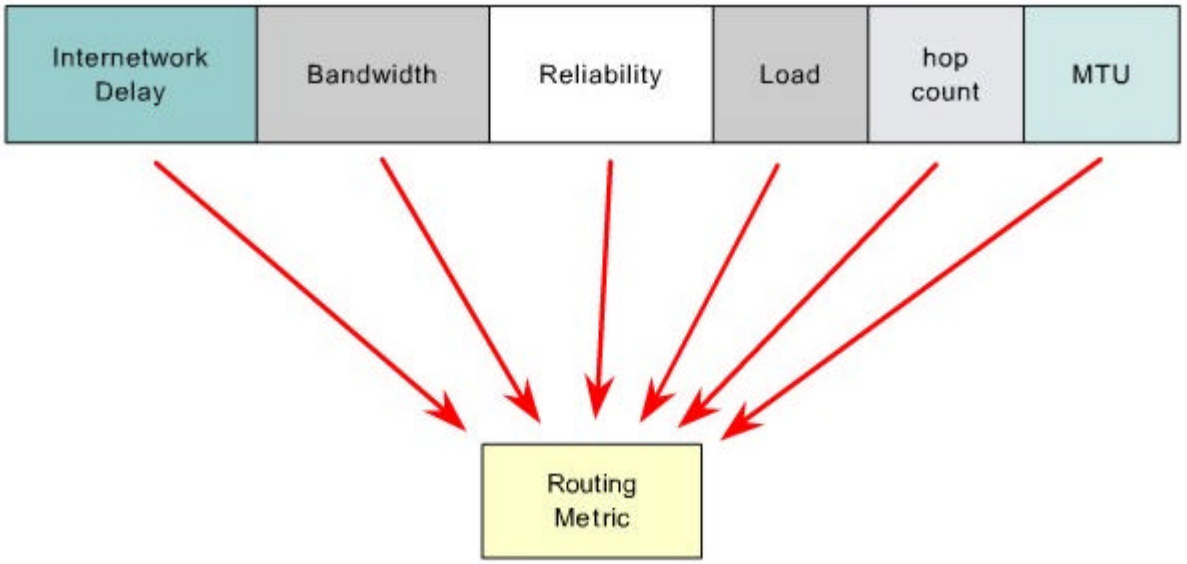
7.1 Uzaklik Vektörü Yönlendirmesi

7.1.1 Uzaklik Vektörü Yönlendirmesi Güncellemeleri

Yönlendirme tablosu güncellemeleri, periyodik olarak ya da mesafe yönü ag protokolündeki topoloji degismelerinde gerçeklesir. Bir yönlendirme protokolünün yönlendirme tablosunun güncellenmesinde etkin olmasi önemlidir. Ag konusundaki yeni buluslar, topoloji degismeleri , routerdan router a sistematik olarak güncellemeyi gerektirir.



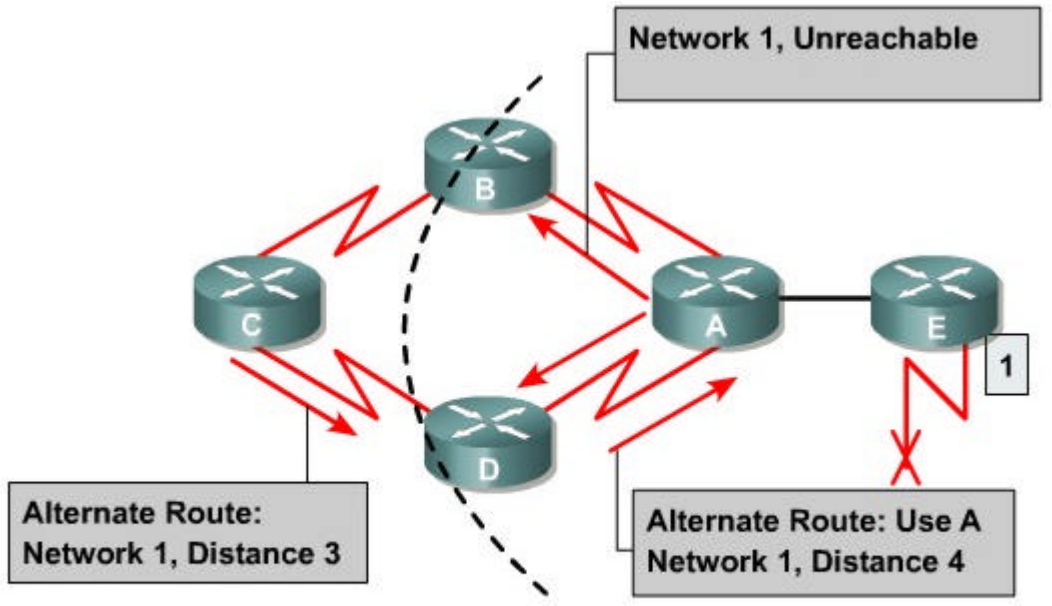
Mesafe yönü algoritmalari, her routeri kendi içindeki gönderim tablosunu yakinindakilerden herbirine göndermeye yönlendirir. Yönlendirme tablolari, metrik olarak tanimlanan toplam yol tutari ve tabloda yer alan her ag için yoldaki ilk router in mantiksal adresini içerir



7.1 Uzaklik Vektörü Yönlendirmesi

7.1.2 Uzaklik Vektörü Yönlendirme Döngüsünün Baslatilmasi

Yönlendirme döngüsü, bir ag degisikliginde agirlasan yakinlasmadan kaynaklanan çeliskili yönlendirme tablolarinin güncellenmedigi zaman meydana gelebilir



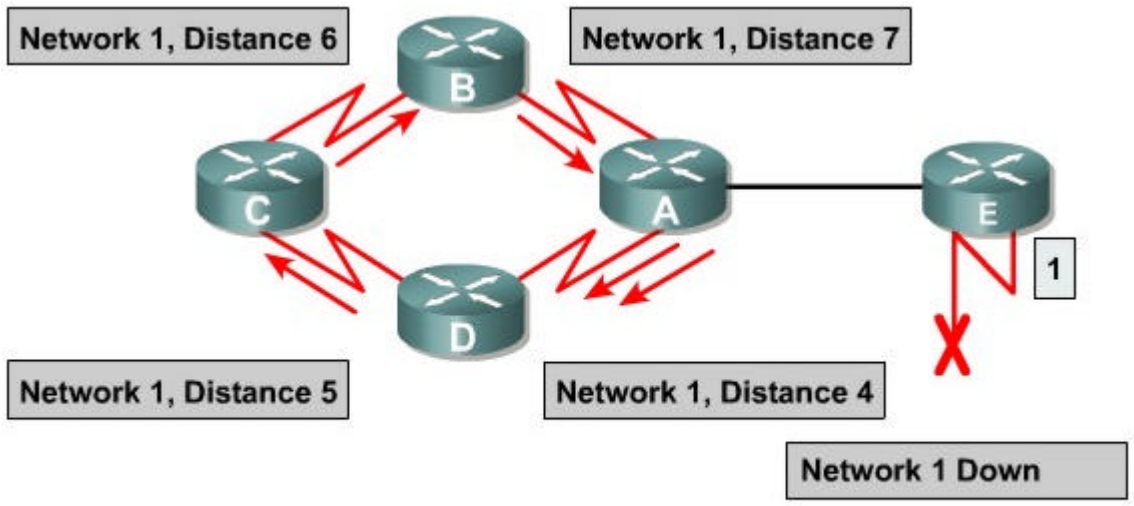
Alternate routes, slow convergence, inconsistent routing

1. 1.Ag bozulmadan önce tüm routerlar dogru yönlendirme tablolarina ve düzgün bilgilere sahiptir. Ag yakinlastirilmis demektir. Bu örnekten çikartilacak sey, 1.Ag yolunu tercih eden C router inin B router i yoluyla oldugu ve C routerindan 1.Ag'a olan mesafe 3 tür.
2. 1.Ag bozuldugu zaman E router 2 A routerina bir güncelleme yollar. A routeri 1.Ag'a paket gönderimini durdurur, fakat B, C ve D roterlari göndermeye devam eder. Çünkü onlar henüz arizadan haberdar edilmemislerdir. A routeri disariya güncelleme yolladiginda B ve D routerlari 1.Ag'a yönelimi durdurur. Bununla birlikte, C routeri henüz bir güncelleme almamistir. 1.Ag hala C routerina B routeri üzerinden baglidir.
3. Simdi C routeri, D routerina , B routeri vasitasiyla 1.Ag'in yolunu gösteren periodik güncellemeler yollar. D routeri kendi gönderim tablosunu degistirir. Fakat bu yanlis bilgidir ve bilgiyi A routerina bildirir. A routeri da bu bilgiyi B ve E routerlarina iletir. 1.Ag'a gidecek her paket simdi C routerindan B' ye A' ya ve D' ye döngü baslatacaktir ve sonra tekar C' ye gelecektir.

7.1 Uzaklik Vektörü Yönlendirmesi

7.1.3 Maksimum Saymanin Tanimlanmasi

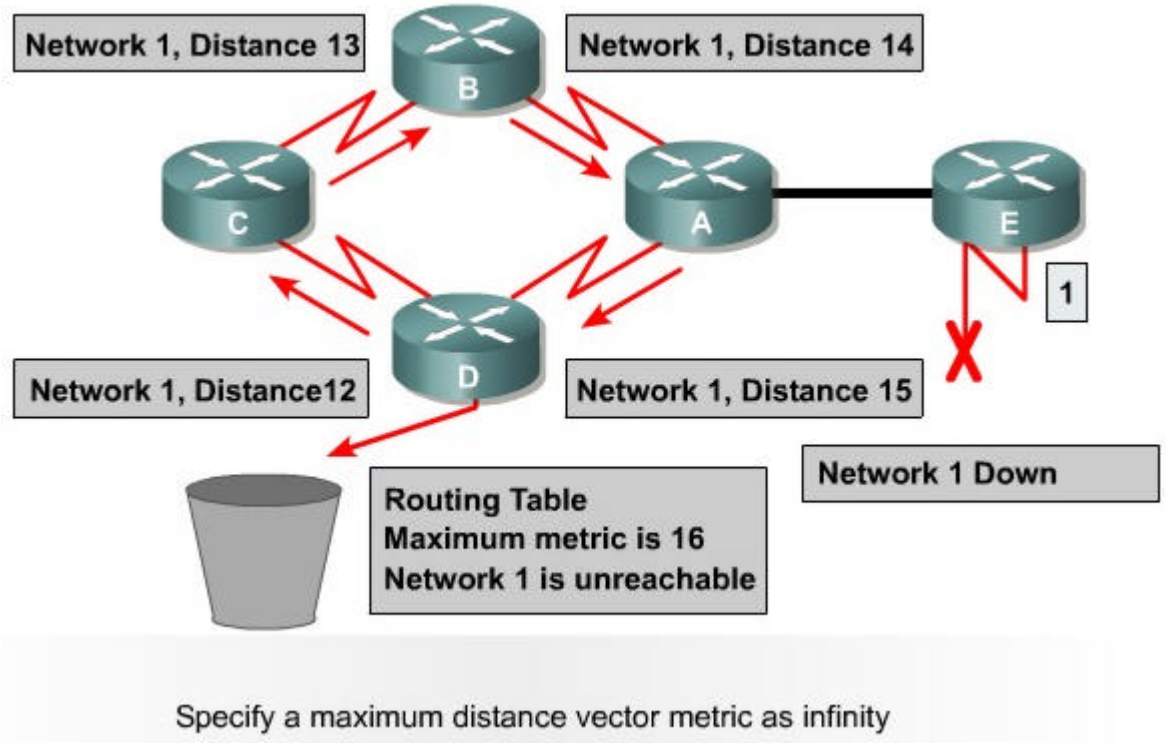
1.Ag'in geçersiz güncellemesi, baska diger islemler kesene kadar döngünün devam etmesine yol açacaktir. Sonsuzun hesaplanmasi olarak adlandirilan bu durum, hedef agin yani 1.Ag 'in arizali oldugu gerçegine ragmen paketlerin sürekli olarak ag etrafinda dönmesine yol açar. Routerlar sonsuzu hesaplamaya çalisirken geçersiz bilgi bir kisir döngüye girer.



Routing loops increment the distance vector

Sonsuzu hesaplama islemini durdurmak için önlem almaksizin, hesap artisindaki büyümenin metrik mesafe vektörü her defasinda paketi bir sonraki router geçirir. Yönlendirme tablosundaki yanlis bilgiden dolayi paketler ag içinde dönüp durur.

Mesafe yönü yönlendirme vektörü algoritmalari kendi kendini düzeltme özelliklidir. Fakat gönderim döngüsü sorunu sinirsiz döngüyü gerektirebilir. Sorunun uzamasini engellemek için mesafe yönü protokolü sonsuzu maksimum düzeyli özel bir sayi olarak tanimlamalidir. Bu sayi, döngüden kurtulmayi saglayacak metrik bir gönderime tekabul eder.



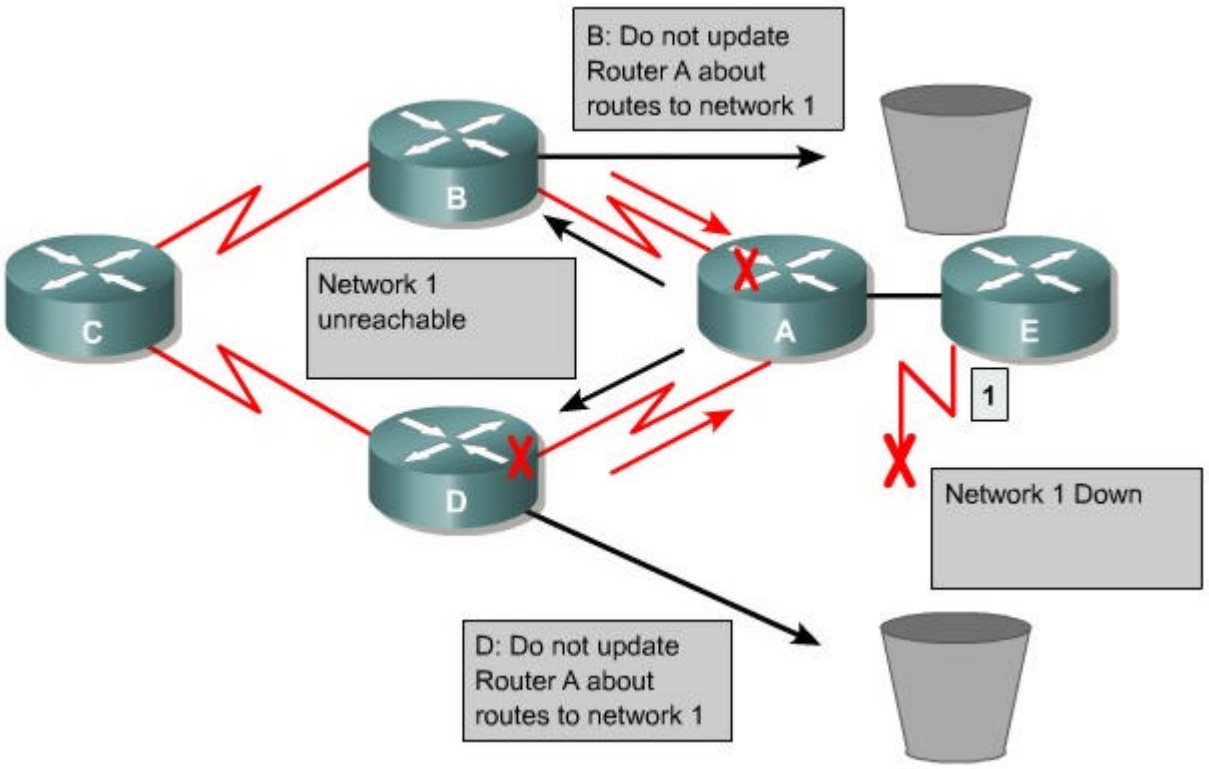
Specify a maximum distance vector metric as infinity

Bu yaklasimda, yönlendirme protokolü, yönlendirme döngüsünün izin verilen maksimum metrik degere ulasana kadar devam edecektir. Grafik, metrik degeri 16 atlama olarak göstermektedir. Mesafe vektöründeki default 15 atlamanin tasmasidir bu ve dolayisiyla paketler router tarafindan reddedilir. Metrik degerin maksimum degeri geçmesi gibi bir durumda 1.Ag´a ulasilamaz olacaktir.

7.1 Uzaklik Vektörü Yönlendirmesi

7.1.4 Yönlendirme Döngüsünün Kesisim Noktasinda Elenmesi

Yönlendirme döngüsüne yol açan muhtemel bir sebep ise bir router a gönderilen yanlis bilginin routerdaki dogru bilgiyle çatismasindir. Bu sorunun nasil olustugu asagida gösterilmistir



1. Router A, B ve D routerlarina 1.Ag'in arizali oldugunu bildiren bir güncelleme yollar. Ama bu arada router B' ye 1.Ag'In router D vasitasiyla 4 lük bir mesafede kullanilabilecegini belirten bir güncelleme iletir. Bu durum, kesisim noktasi kurallarina aykiri degildir.
2. Router B, 1.Ag.'a ulasmak için Router C' nin hala geçerli bir yol oldugu sonucuna varir. Router B, router A' ya 1.Ag'in yeni yolunun router A oldugunu hatirlatan bir güncelleme yollar.
3. Router A o anda onu Router B üzerinden 1.Ag'a gönderebilecegini saptar. Router B ise router C üzerinden gönderebilecegini, ve Routrer C de router D üzerinden gönderebilecegini saptar.Bu ortama giren her paket roterlar arasinda dönüp durur.
4. Kesisim noktasi bu durumdan sakinmaya çalisir. Eger Ag 1 ile ilgili bir gönderim güncellemesi router A' ya ulasirsa, router B veya router D Ag 1 ile ilgili bilgiyi router A'

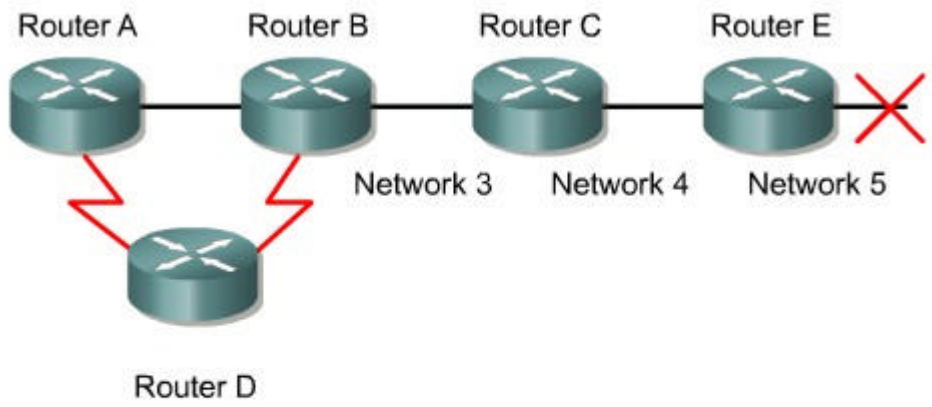
ya geri gönderemez(1). Böylelikle kesisim noktasi, hatali gönderim bilgisini ve gönderim yükünü azaltir.

7.1 Uzaklik Vektörü Yönlendirmesi

7.1.5 Yönlendirmenin Mantiksal Hesabi

Mantiksal yol hesabi , degisik mesafe yönü protokollerince büyük ölçekli gönderim döngülerini giderebilmek ve ag ya da alt agin islem yapamaz oldugu durumlarda kesin bilgi verebilmek amaciyla kullanilir. Bu genellikle atlamanin makimumdan bir fazla ayarlanmasiyla yapilir.

Çeliskili güncellemelerden kaçinmanin bir yolu mantiksal yol hesabidir. Ag 5 devre disi kalirken Router E 16 da oldugu gibi Ag 5 içinbir tablo girisi yaparak mantiksal yol hesabini baslatir. Ag 5' in bu yol hesabindan dolayi, router C Ag hakkindaki yanlis güncellemelere duyarli degildir. Router C, router E' den bir yol hesabi aldiginda tekrar router E' ye geri hesaplama adi verilen bir güncelleme yollar. Bu , segment üzerindeki tüm yollarin hesaplanmis yol bilgisini almis oldugunu kesinlestirir.



When Network 5 goes down, Router E initiates route poisoning by entering a table entry metric of 16 (unreachable).

Mantiksal yol hesabi, baslatilmis güncellemelerle kullanildiginda , komsu routerlar hesaplamanin bildirilmesinden önce 30 saniye beklemek zorunda olmadiklari için zamansal yakinlasma hizina ulasacaktir.

Mantiksal yol hesabi, hatali bir yol için gönderim protokolünün sonsuz-metrik yollar bildirmesine yol açar. Mantiksal yol hesabi, kesisim noktasi kurallarina ters düsmez.tersine hesaplamali kesisim noktasi aslinda mantiksal yol hesaplamasidir fakat akis için gönderim

bilgisine normal olarak izin vermeyen kesisim noktalarindaki linklere özellikle yerlestirilmislerdir. Diger türlü, bu hatali yollar sonsuz metrik olarak iletilecektir.

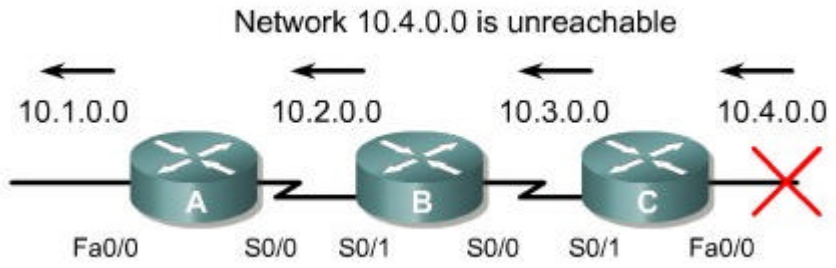
7.1 Uzaklik Vektörü Yönlendirmesi

7.1.6 Güncellemelerin Baslatilmasiyla Yönlendirme Döngülerinden Kaçinmak

Yeni yönlendirme tablolari komsu routerlara düzenli kurallar dogrultusunda gönderilir. Örnegin GBP güncellemeleri her 30 saniyede olur. Bununla birlikte, baslatilmis bir güncelleme yönlendirme tablosundaki bazi degisiklikleri bildirmesi için aninda gönderilir. Topoloji degisikligi tespit eden bir router hemen yakinindaki diger routerlara bir güncelleme mesaji gönderir. Bir yol yanlis oldugunda, güncelleme süresinin dolmasini beklemek yerine derhal bir güncelleme yollanir. Baslatilmis güncellemeler, süre sinirlamalari dolmadan önce tüm routerlarin hatali yollari bilmelerini saglamak için mantiksal yol hesabi ile birlikte kullanilirlar.

Baslatilmis güncellemeler ve güncellemeyi yollar. Çünkü degismis gönderim bilgisi artik sürenin dolmasini bekliyordur. Router sürenin dolmasini beklemektense diger arabirimlere yeni bir gönderim güncellemesi yollar. Bu ise degismis olan yol durumu hakkindaki bilginin iletilmesine ve komsu routerlarda süre sinirlayicisin daha hizli baslamasina yol açar. Güncelleme dalgasi ag üzerinde hizla yayilir.

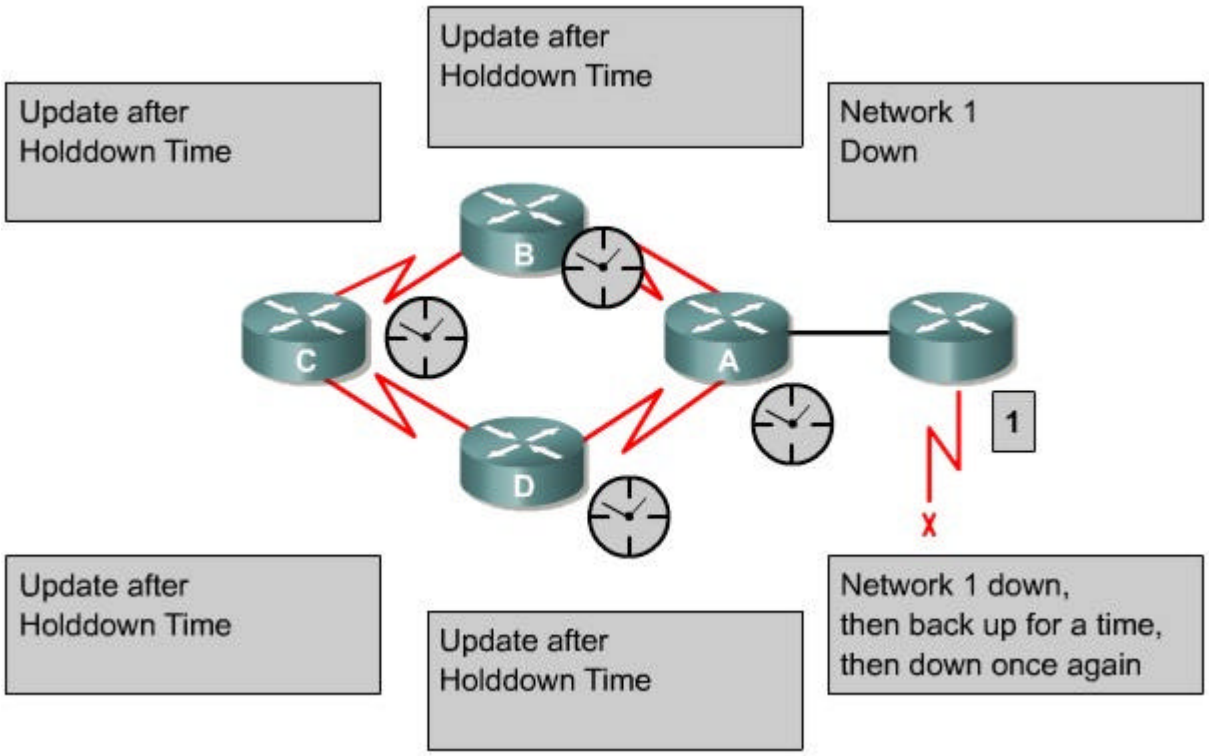
C routerindan çikan baslatilmis güncelleme 10.4.0.0 aginin ulasilamaz oldugunu bildirir. Bu bilginin alinmasi üzerine, B routeri S0/1 arabirimi üzerinden 10.4.0.0 aginin arizali oldugunu bildirir. Ardindan, A routeri Fa0/0 çikis arabirimine bir güncelleme yollar.



7.1 Uzaklik Vektörü Yönlendirmesi

7.1.7 Süre Sinirlayicilari ile Gönderim Döngülerini Engellemek

Sonsuzu hesaplama sorunu süre sinirlayicisi kullanmak suretiyle halledilebilir



- Bir router komsu routerdan bir önceki erisilebilir agin simdi erisilemez olduguna iliskin bir güncelleme alirsa router, yolu erisilemez olarak isaretler ve bir süre sayaci baslatir. Eger süre dolmadan ayni komsu routerdan agin tekrar erisilebilir durumda olduguna iliskin bir güncelleme alirsa, router agi erisilebilir olarak isaretler ve sayaci kaldirir.
- Eger farkli bir komsu routerdan agdaki orijinal kayitli olandan daha metrik bir güncelleme gelirse, router agi erisilebilir olarak isaretler ve sayaci kaldirir.
- Eger sayaç süresi dolmadan farkli bir komsu routerdan zayif metrik güncelleme gelirse bu durumda güncelleme geçersiz sayilir.

7.2 RIP

7.2.1 RIP Yönlendirme Islemi

Bazen IP RIP olarak da gösterilen GPP' nin bu açik standardi biçimsel olarak iki farkli dokümanda ayrintilandirilmistir. Ilki RFC 1058 olarak, digeri de STD 56 olarak bilinir

The key characteristics of RIP include the following:

- It is a distance vector routing protocol.
- Hop count is used as the metric for path selection.
- If the hop count is greater than 15, the packet will be discarded.
- By default, routing updates are broadcast every 30 seconds.

Yönlendirme bilgi protokolü (RIP) yillardir, RIPv1' den RIPv2' ye kadar sürekli gelistirilmistir. RIP v2' nin artilar sunlardir:

- Ilave yönlendirme paketi bilgisi tasiyabilme
- Tablo güncellemelerinin güvenligi için yetkilendirme mekanizmasi
- Degisik uzunlukta alt maskeleme destegi

RIP , kaynaktan alici adresine giden yolda izin verilen atlama sayilarindaki sinirin dolmasiyla sürekli devam eden gönderim döngüsünü engeller. Bir yolda maksimum atlama sayisi 15 tir. Bir router, yeni veya degismis bir giris içeren gönderim güncellemesi aldiginda metrik deger, yol üzerinde bir atlama olarak kendi hesabina 1 artirilir. Eger bu, metrigin 15 üzerinde artirilmasina yol açiyorsa bu durumda sonsuzluk gibi düsünülür ve ag adresi ulasilamaz olarak kabul edilir. RIP, diger gönderim protokollerinde de ortak olan özellikleri içerir. Örnegin RIP gönderilen yanlis gönderim bilgisini önlemek için kesisim noktasi ve süre sinirlayicisini kullanir.

7.2 RIP

7.2.2 RIP Konfigürasyonu

Router rip komutu RIP i bir gönderim protokolü gibi yetkin kilar. Ardindan, routera RIP' nin hangi arabirim üzerinde çalisacagini söyleyen **network** komutu kullanilir. Gönderim islemi daha sonra özel arabirimleri bir araya toplar ve bu arabirimler üzerinden RIP güncellemelerini göndermeye ve almaya baslar.

RIP, yönlendirme-güncellemesi mesajlarini düzenli araliklarla yollar. Bir router, bir giris degisikligi içeren yönlendirme güncellemesi aldiginda yönlendirme tablosunu yeni bir yola yönlendirmek üzere günceller. Yol için alinan metrik deger 1 artirilir ve güncelleme arabirim kaynagi yönlendirme tablosundaki bir sonraki atlama gibi belirtilir. RIP routerlari, bir alici adresi için en zahmetli fakat en iyi yolu saglarlar.

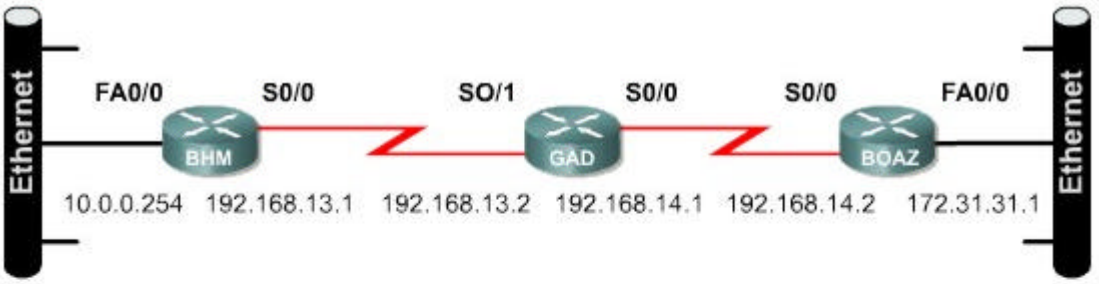
RIP çalistiran bir router, ag topolojisi degistiginde **ip rip triggered** komutunu kullanarak baslatilmis güncelleme göndermek için konfigüre edilebilir. Bu komut, routerda (config-if)# iletisiyle sadece seri arabirim üzerinden girilebilir. Konfigürasyon degisikligine bagli olarak yönlendirme tablosunun kendisini güncellemesinden sonra router hemen yönlendirme güncellemelerini diger aglara bildirmek için baslatir.GBP routerin dagittigi baslatilmis güncelleller adi verilen bu güncellemeler düzenli olarak gönderilir. Örnegin, BHM routerini konfigüre etmek için gerekli komut tanimlari asagida verilmistir:

- BHM(config)#**router-rip** – yönlendirme protokolü olarak RIP i seçer
- BHM(config-router)#**network 10.0.0.0** Dogrudan bagli bir agi belirtir
- BHM(config-router)#**network 192.168.13.0** Dogrudan bagli bir agi belirtir

192.168.13.0 ve 10.0.0.0 aglarina bagli Cisco router arabirimleri GBP güncellemelerini gönderir ve alir. Bu gönderin güncellemeleri, routera komsu ag routerlarinin topolojilerini tanima ve ayni zamanda GBP' yi çalistirma olanagi verir.

- Metriklerin gönderimi için offsetler kullanmak
- Süre sayaci ayarlamak
- Bir RIP versiyonu belirtmek
- RIP yetkilendirmesini aktiflestirmek
- Arabirim üzerinde yol özeti konfigüre etmek
- IP yol özetini dogrulamak
- Otomatik yol özetini pasiflestirmek
- IGRP ve RIP i basarili sekilde çalistirmak
- IP adreslerinin kaynaklarinin geçerliligini pasiflestirmek
- Kesisme noktasini aktif ya da pasif yapmak
- RIP' i WAN' a baglamak

GBP' yi aktiflestirmek için asagidaki komutlari global konfigürasyon modunda baslayarak kullanin




```
BHM(config)#router rip
BHM(config-router)#network 10.0.0.0
BHM(config-router)#network 192.168.13.0
```

```
GAD(config)#router rip
GAD(config-router)#network 192.168.14.0
GAD(config-router)#network 192.168.13.0
```

```
BOAZ(config)#router rip
BOAZ(config-router)#network 192.168.14.0
BOAZ(config-router)#network 172.31.0.0
```

- Roter(config)#**router rip** – RIP yönlendirme islemini aktiflestirir.
- Roter(config-router)#**network** ag numarasi – Bir agi RIP yönlendirme islemiyle birlestirir

7.2 RIP

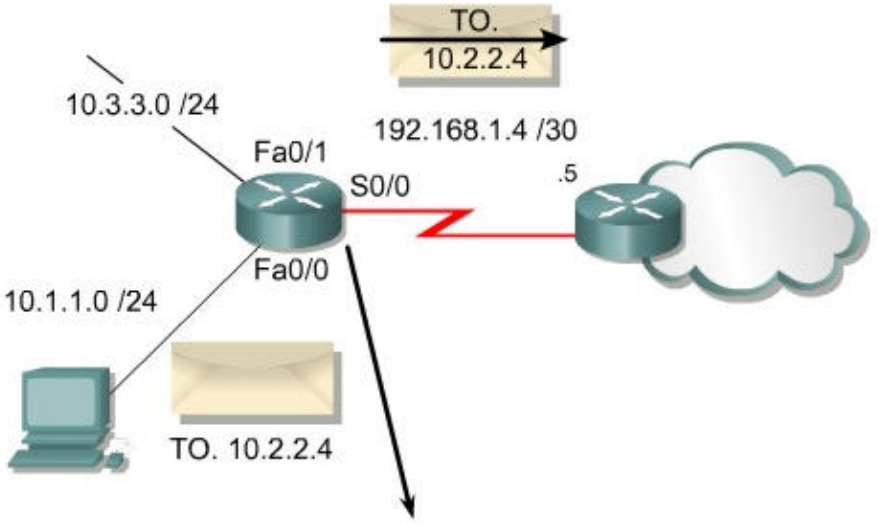
7.2.3 ip classless Komutunun Kullanilmasi

Bazen router dogrudan alt ag bagli bir agin bilinmeyen alt agina gönderilmek üzere paketler alir. Cisco nun IOS yazilimi için bu paketleri mümkün olan en uygun supernet yola yönlendirmek için ip classles global konfigürasyon komutunu kullanin. Supernet yolu, çok genis bir alt ag dizgesini tek bir girisle kaplayan bir yoldur. Örnegin, bir isletme tümden 10.10.0.0/16 alt agini kullanir ve bu durumda 10.10.10.0/24 için supernet yolu 10.10.0.0/16 olabilir. **ip classless** komutu CISCO'nun IOS yaziliminin 11.3 ve daha sonraki versiyonlarinda default olarak aktiftir.Bu özelligi pasiflestirmek için bu komutun **no** biçimini kullanin.

Bu özellik pasiflestirildiginde,router alt aga göndermek üzere almis oldugu paketleri yok ayar.

IP classles, sadece IOS da gönderme sürecine etki eder. Ip siniflari yerlesik yönlendirme tablosunun yolunu etkilemez. Bu siniflandirilmamis gönderimin temelidir. Eger ana ag biliniyor. Fakat bu ana ag içinde paketlerin gönderildigi alt ag bilinmiyorsa paket gönderimden düser.

Bu kuralin en kafa karistiran yani, yönlendirme tablosunda eger ana agin varis adresi yoksa routerin sadece varsayilan yolu kullanmasidir. Yönlendirme tablosunda , dogrudan bagli agin tüm alt aglari tarafindan varsayilan olarak kabul edilen router yönlendirme tablosunda yer almalidir. Aga dogrudan bagli olan belirsiz bir alt agdan adresi belli olmayan bir paket alindiginda router o alt agin olmadigi sonucunu çikaracaktir. Dolayisiyla router varsayilan bir yol olsa bile paketi düsürecektir. Router üzerinde **ip classles in konfigüre edilmesibu sorunu ,** yönlendirme tablosu içerisinde agin siniflandirilmamis sinirlari yok saymasina izin vererek ve basitçe varsayilan yola yönelerek bu sorunu çözecektir.



Destination Network	Outbound Interface
10.1.1.0	Fa 0/0
10.3.3.0	Fa 0/1
0.0.0.0	S 0/0

7.2 RIP

7.2.4 Genel RIP Konfigürasyonu Sorunlari

RIP routerlari ilk elde taninmayan ag bilgileri konusunda komsu routerlara güvenmelidir. Bu islevi tanimlamaya yönelik kullanilan ortak terim Rumor tarafindan yönlendirmedir. (Routing By Rumor). RIP , uzaklik vektör yönlendirme algoritmasi kullanir. Tüm mesafe vektör yönlendirme protokolleri ilk olarak agir yakinsama tarafindan olusturulmus olan çikarimlara sahiptir. Yakinsama tüm routerlarin ayni iç ag üzerinde ayni yol bilgisine sahip oldugu zaman mevcuttur.

Bunlarin arasinda çikarimlar, yönlendirme döngüsü ve sonsuzun hesaplanmasidir. Bunlar, iç ag etrafindaki yayilmis olan yol tarihinin geçersiz olmasi ile yönlendirme güncelleme mesajlarina yönelik uyusmazliklara yol açar.
Yönlendirme döngüsünü ve sonsuzu hesaplamayi azaltmak için RIP asagidaki teknikleri kullanir:

- Sonsuzun hesaplanmasi
- Kesisim noktasi
- Ters mantik yürütme
- Sayaç tutucular
- Baslatilmis güncellemeler

Bu yöntemlerden bazilari belli konfigürasyon gerektirirken bazilari hiç gerektirmez bazilari da nadiren gerektirir.

RIP, 15 lik bir atlama miktarina izin verir. 15 atlamadan daha büyük herhangi bir alici adresi ulasilamaz olarak imlenir. RIP' in maksimum hesap atlamasi kendisinin ag içinde kendi kullanimini büyük ölçüde sinirlar ama ag gönderim döngüsünde çikissizliga yol açan " **sonsuzu hesaplama** " adiyla bilinen sorunu engeller.

Kesisme noktasi, bir yol hakkinda geri adresine bilgi gönderilmesinin gerekli olmadigi teorisine dayanir.

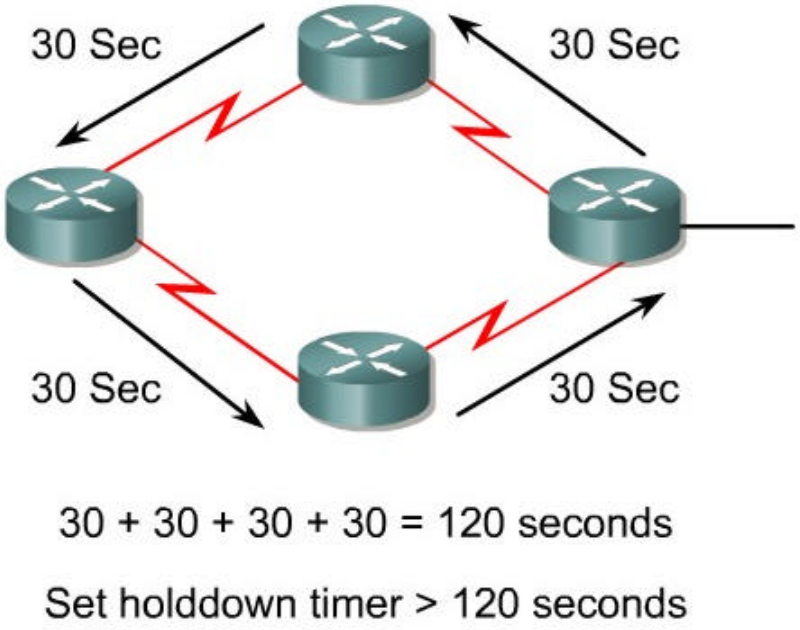
Bazi ag konfigürasyonlarinda kesisme noktasini pasiflestirmek gerekebilir

Kesisme noktasini pasiflestirmek için, asagidaki komut kullanilir:

GAD(config-if)#**no ip split-horizon**

Süre tutucu, bazi degisiklikler gerektiren bir diger mekanizmadir. Süre tutucular, sonsuzu hesaplama islemini engellemeye yardimci olur fakat zaman yakinsamasini artirir. GBP ler için süre tutucu default degeri 180 saniyedir. Bu, güncellenmekte olan herhangi bir iç yolu engelleyebilecegi gibi daha önceden kurulmus olan geçerli alternatif bir yolu da engelleyecektir. Yakinsama hizini artirmak için, süre tutucunun süre siniri azaltilabilir ama bu

dikkatlice yapilmalidir. Ideal bir ayarlama, iç ag güncellemesi için gerekli olan en uzun sürenin ayarlanmasidir. Resimdeki örnekte 4 adet routerin döngüsü yer almaktadir. Eger her bir router 30 saniyelik güncelleme zamanina sahipse en uzun döngü 120 saniye sürecektir. Dolayisiyla süre tutucular birazcik 120 saniyenin üzerine ayarlanmalidir.



Süre tutucuyu degistirmek için :

Router(config-router)#**timers basic**

Konfigüre edilebilirligi ve yakinsama zamanini etkileyen ek bir konu da araliklarla güncellemedir. RIP'nin Cisco IOS da aralikla güncelleme varsayilan degeri 30 saniyedir. Bant genisligini muhafaza etmek için bu süre daha uzun araliklarla ayarlanabilir ya da yakinsama zamanini azaltmak için aralik süresi daha bir daraltilabilir.

Dahili güncellemeyi degistirmek için:

GAD(config-router)#**update-timer** saniye

Yönlendirme protokollerinden çikan bir sonuç da gönderim güncellemelerinin istenmeyen bildirimlerini belli bir arabirimden disari atmasidir. Bir **network** komutu belli bir ag için verildiginde, RIP derhal özel bir ag adres araligindan tüm arabirimlere bildirimler göndermeye baslayacak.

Yönlendirme güncellemelerini degistirmeye yönelik arabirimleri ayarlamayi kontrol için ag yöneticisi
Passive-interface komutunu kullanarak belli bir arabirim üzerinden güncelleme bildirimi yollamayi pasiflestirebilir

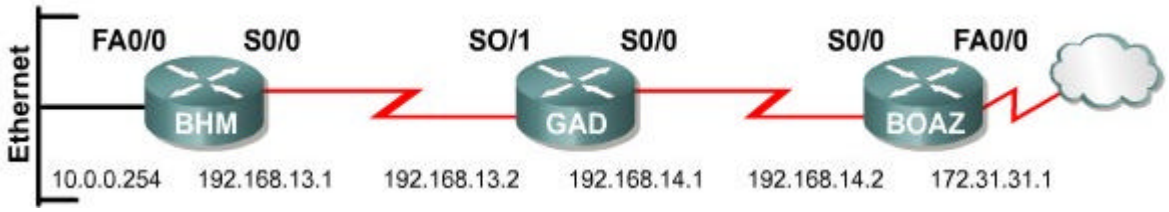
RIP in bir dagitim protokolü olmasindan dolayi , ag yöneticileri Frame relay gibi dagitimsal olmayan bir agda yönlendirme bilgisini degistirmek için GBP' yi konfigüre etmek zorunda kalabilir. Bu tip agda, GBP nin diger komsu RIP router larda tutulmasi gerekir. Bunu yapmak için, sekil 4 de gösterilen komutu kullanin.

Default olarak, Cisco IOS yazilimi GBP nin versiyon1 ve versiyon2 paketlerini alir fakat sadece versiyon1 paketlerini yollar. Ag yöneticisi, routeri sadece versiyon1 paketlerini gönderebilecek ve alabilecek sekilde ya da sadece sadece versiyon2 paketlerini gönderebilecek sekilde konfigüre edebilir. Paketleri sadece bir versiyondan göndermek ve almak için sekilde gösterilen komutu kullanin.

7.2 RIP

7.2.5 RIP Konfigürasyonunun Incelenmesi

RIP in düzgün yapilandirilmis olup olmadigini dogrulamak için kullanilan degisik komutlar vardir. Bunlarin en yaygin olanlarindan ikisi **show ip route** komutu ve **show ip protocols** komutlaridir



Show ip protocols komutu router üzerinde IP trafigini hangi gönderim protokollerinin tasidigini gösterir. En yaygin konfigürasyon dogrulama basliklari sunlardir:

- RIP gönderimi konfigüre edilmistir.
- RIP güncellemelerini dogru arabirimler alir ve gönderir
- Router dogru aglari bildirir

Show ip route komutu, yönlendirme tablosunda yer alan komsu RIPlerce alinan yollari dogrulamak için kullanilabilir. Komut çiktisini inceleyin ve " R " ile gösterilen RIP yollarini arayin. Yakinsama için agin biraz zaman alacagini ve dolayisiyla aninda görülmeyecegini unutmayalim.

RIP konfigürasyonunu kontrol etmek için ilave komutlar sunlardir:

- **Show interface** arabirim
- **Show ip interface** arabirim
- **Show running-config**

7.2 RIP

7.2.6 RIP Güncelleme Sorunlarinin Giderilmesi

RIP konfigürasyon hatalarinin çogu hatali bir ag, düzensiz alt aglar ya da hedef çakismasi içerir. RIP güncelleme sonuçlarini bulma için en etkin komut **debug ip rip** komutudur.

debug ip rip komutu, RIP yönlendirme güncellemelerini gönderip aldigi gibi görüntüleyebilir. Bir RIP güncellemesi aldiktan sonra **debug ip rip** komutu kullanilarak routerdan çikisi gösterir. Güncellemeleri aldiktan ve isledikten sonra router , iki RIP arabirimine güncellenmis bilgiyi yeniden yollar. Çikis, routerin RIP versiyon1 i ve güncelleme dagitimini kullandigini gösterir. (dagitim adresi 255.255.255.255 tir). Parantez içindeki rakamlar, RIP güncellemesinin IP basliginda yer alan kaynak adresleri temsil eder.

debug ip rip komutunun çiktisinda aranacak degisik anahtar göstergeler vardir. Düzensiz alt ag isi ya da tekrarlanmis aglar gibi sorunlar bu komutla gözden geçirilebilir. Bu sonuçlarin bir belirtisi bir router in ag için aldigi metrikten daha küçük bir metrikle yol bildirimi yapmasidir

GBP sorunlarini gidermede kullanilacak diger komutlar sunlardir:

- **show ip rip database**
- **show ip protocols {summary}**
- **show ip route**
- **debug ip rip {events}**
- **show ip interface brief**

7.2 RIP

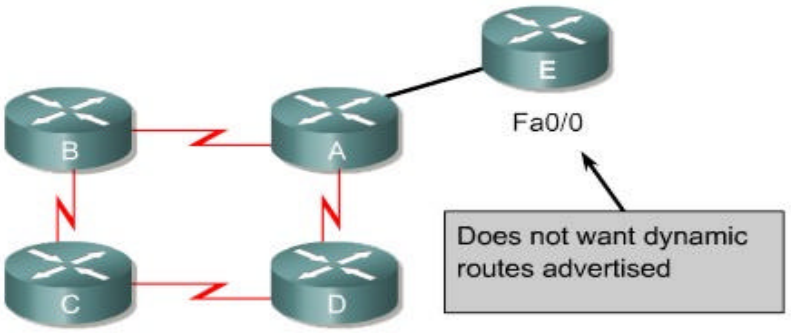
7.2.7 Arayüz Içerisindeki Yönlendirme Güncellemelerinin Önlenmesi

Yol filtrelemesi içeri giren ya da disari çikan yol tablolarini duyuran yollari düzenleme dogrultusunda çalisir. Bunlar, yönlendirme protokolleri durum linkleri üzerinde mesafe yönlendirme protokololllerinden daha farkli etkiye sahiptirler. Mesafe yönü protokolünü çalistiran bir router, yol tablosunda yer alan yollari duyurur. Sonuç itibariyla router i yönlendiren yol filtresi komsu routerlara da bunu bildirir.

Öte yandan link durum protokollerini çalistiran routerlar , komsu router in bildirdigi yol girislerinden ziyade link durum veritabanindaki bilgilere dayali olarak yolu tespit eder. Yol

filtrelerinin link durum bildirimleri ya da link durum veritabani üzerinde bir etkisi yoktur. Bu nedenle, tipki RIP ve IGRP de oldugu gibi bu dokümandaki bilgiler sadece mesafe yönü IP yönlendirme protokolüne uygulanir

Passive interface komutu routerlari, router arabiriminden gönderilen yönlendirme güncellemelerinden alikoyar. Bir router arabirimi üzerinden gönderilen yönlendirme güncelleme mesajlarini yakalamak ag üzerindeki diger sistemlerin yolu dinamik olarak ögrenmesini engeller. E-router i gönderilen güncellemeleri yakalamak için komut kullanir.




```
RouterE(config-router)#passive-interface Fa0/0
```

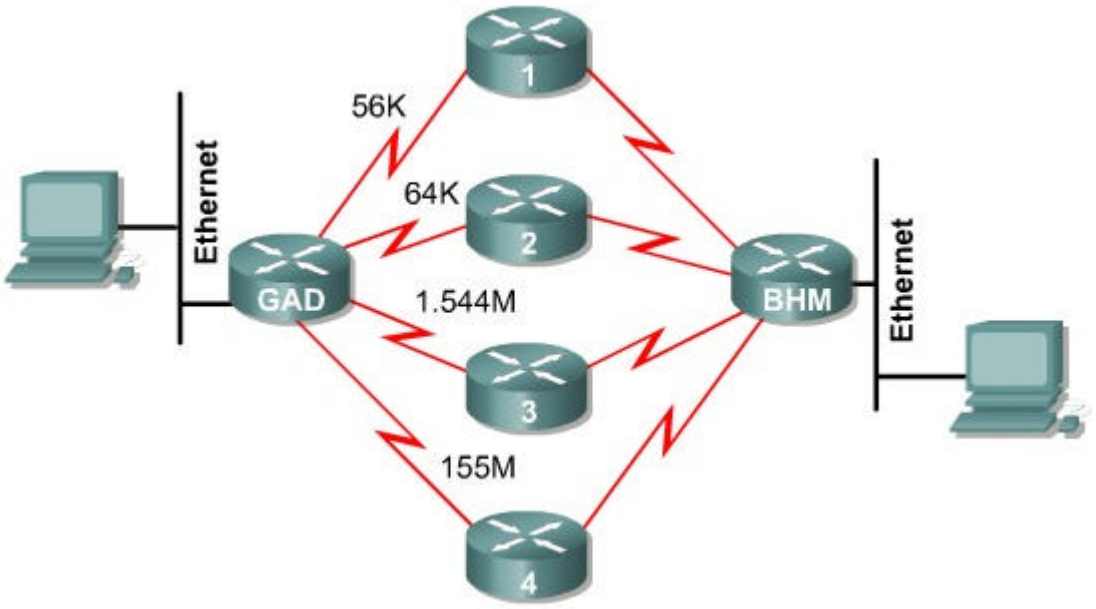
RIP ve IGRP için **passive interface** komutu routerin komsu bir routera güncellemeler göndermesini durdurur. Fakat router yönlendirme güncellemelerini dinlemeyi sürdürür. Bir router arabirimi üzerinden gönderilen yönlendirme güncelleme mesajlarini yakalamak ag üzerindeki diger sistemlerin yolu dinamik olarak ögrenmesini engeller.

7.2 RIP

7.2.8 RIP ile Yük Dengeleme

Yük dengelemesi, routerin belirli bir adres için birden fazla iyi yol avantajina izin veren bir düsüncedir. Bu yolar ya yönetici tarafindan statik olarak ya da GBP gibi dinamik yönlendirme tarafindan hesaplanmistir

RIP , dörtü varsayilan yol ile alti tane kadar ayni zorlukta yük dengelemesi yetenegine sahiptir



1.1.1 Yukaridaki resim, esit ölçekli dört adet RIP yolu göstermektedir. Router, router 1'e bagli olan arabirime bir arabirim pointerla baslayacaktir. Daha sonra, arabirim pointeri arabirim içinde ve 1-2-3-4-1-2-3-4-1 gibi belirlenmis bir tarzdaki yollar üzerinde çevrim baslatacaktir. RIP biçim metrigin hesap atlamasi olmasindan dolayi linklerin hizina yönelik görüs belirtilmemistir. Bu yüzden, 56Kbps lik bir yol 155 mbps lik bir yoldaki gibi ayni tercihi verecektir.

Esit ölçekli yollar, **show ip route** komutu kullanilarak bulunabilir. Resim 2 , **show ip route** komutunun çogul yollarla belli bir alt aga çikisini göstermektedir.

```
RouterC#show ip route 192.168.2.0
Routing entry for 192.168.2.0/24
 Known via "rip", distance 120, metric 1
 Redistributing via rip
 Last update from 192.168.4.2 on FastEthernet0/0,
00:00:18 ago
 Routing Descriptor Blocks:
 192.168.4.1, from 192.168.4.1, 00:02:45 ago, via
FastEthernet0/0
 Route metric is 1, traffic share count is 1
 * 192.168.4.2, from 192.168.4.2, 00:00:18 ago,
via FastEthernet0/0
 Route metric is 1, traffic share count is 1
```

NOT: Iki tane gönderim tanimlayicisi olduguna dikkat edin. Her blok bir yoldur. Ayni zamanda blok girislerinin bitisigindeki yolda yildiz vardir

7.2 RIP

7.2.9 Çoklu Çarpa Yollarda Yük Dengelemesi

Yük dengelemesi, routerin bir IP adresine paketleri birden fazla yolla gönderebilme yetenegini ifade eder. Yük dengelemesi, routerin belirli bir adres için birden fazla iyi yol avantajina izin veren bir düsüncedir. Bu yollar, RIP, EIGRP ve IGRP gibi statik ya da dinamik protokollerden kaynaklanir.

Bir router, belirgin bir ag yönelik çogul yol ögrendiginde, yol yönlendirme tablosuna yerlestirilir. Bazen router, ayni yönetim mesafesiyle ayni yönlendirme islemi sayesinde bilgi edinerek pekçok yol arasindan birini seçmek zorunda kalabilir. Bu durumda router varis adresine en düsük metrik ya da ölçüye sahip olan yolu seçer. Her yönlendirme islemi onun boyutunu farkli hesaplar ve boyutlar yük dengesini saglamak amaciyla manuel olarak ayarlanmayi gerektirebilir.

Administrative Distance Route Source	Default Distance
Connected interface	0
Static route	1
Enhanced IGRP summary route	5
External BGP	20
Internal Enhanced IGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP external route	170
Internal BGP	200
Unknown	255

Eger router ayni yönetim mesafesine ve adrese boyutuna sahip çogul yollar alir ve kurarsa yük dengesi ortaya çikabilir. Orada alti esit yol büyüklügü olabilir (yönlendirme tablosunda Cisco' nun impoze ettigi bir limit vardir) fakat bazi iç ag geçidi protokolleri (IGP) ler kendi sinirlarina sahiptirler. EIGRP dört esit büyüklükte yola izin verir.

Varsayilan olarak, çogu IP yönlendirme protokolü bir yönlendirme tablosuna maksimum 4 paralel yol kurar. Istisnai olarak RIP bir varis adresine varsayilan olarak olarak sadece bir yol kurar.

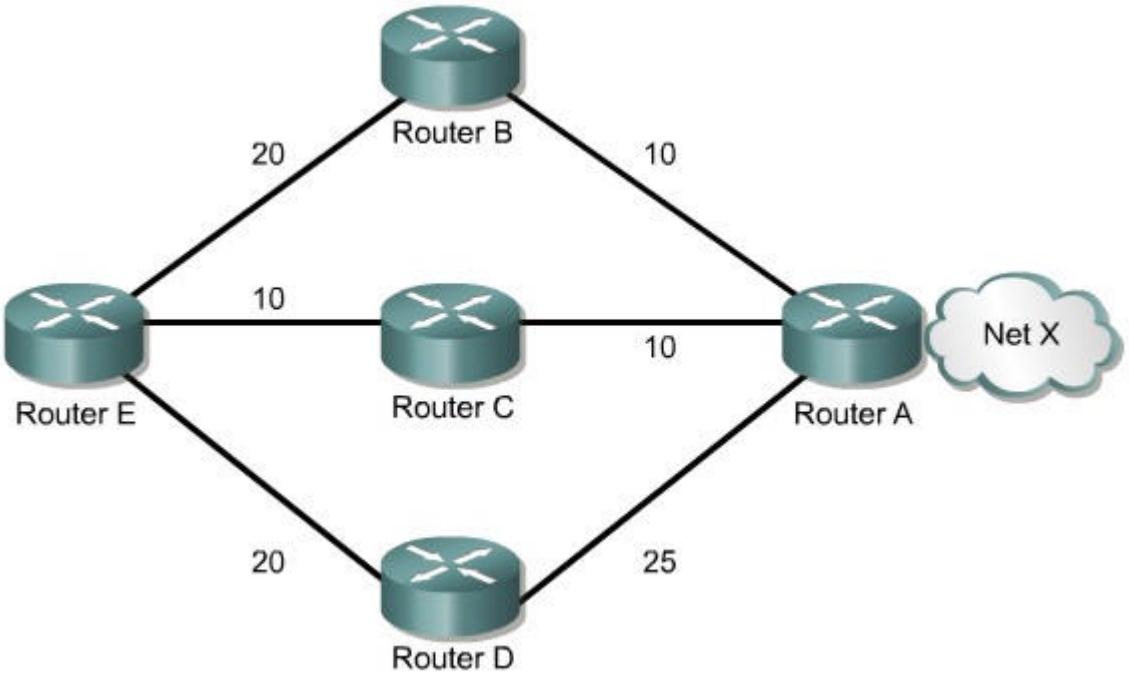
Maksimum yol adedi birden altiya kadardir. Birbirini izleyen paralel yollarin maksimum sayisini artirmak için routerda konfigürasyon modunda asagidaki komutu kullanmak gerekir

Router(config-router)#**maximum-paths** [*numara*]

IGRP esit olmayan alti adede kadar dengeyi saglayabilir. RIP aglari yük dengesi için ayni atlama miktarina sahip olmalidir. Oysa IGRP yük dengesinin nasil oldugunu saptamak için bant genisligini kullanir.

X agina ulasmak için üç yol vardir:

- 30 metrik ile E' den B' ye B' den A' ya
- 20 metrik ile E' den C' ye , C' den A' ya
- 45 metrik ile E' den D' ye, D' den A' ya



E routeri , E-C-A üzerinde 30 ve 45 den daha küçük olarak 20 metrik degerinde ikinci bir yol seçer.

Gönderim esnasinda Cisco IOS, yük dengesi için iki yöntem sunar: pakete göre ve erisim adresine göre. Eger islem anahtari açik ise, router yollari paket tabanli olarak degistirecektir. Eger hizli anahtarlama açik ise degisen yollardan sadece birisi varis adresi için muhafaza edilecek, dolayisiyla her paket ayni yola sevkedilecektir. Paketlerin ayni agdan farkli hostlara atlamasi bir yol degisikligine ve trafigin alici adresi temelinde dengelemesine yol açacaktir.

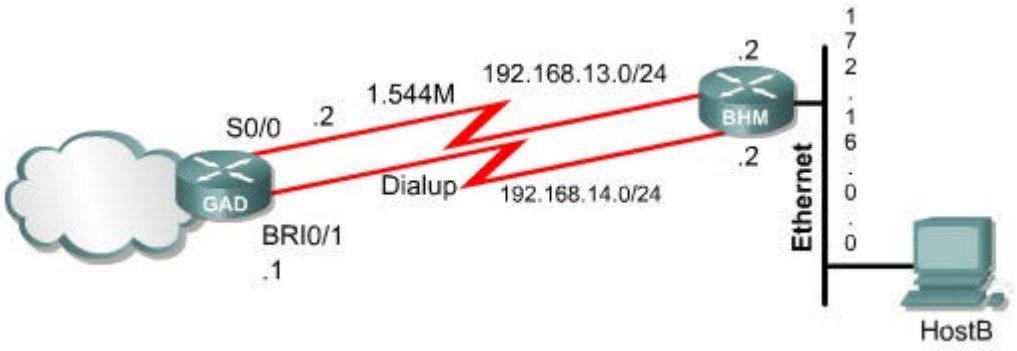
7.2 RIP

7.2.10 RIP ile Statik Yollarin Entegrasyonu

Statik yollar, paketleri özel bir yol almak amaciyla kaynakla alici adresi arasinda harekete zorlayan kullanici-tanimli yollardir. Cisco IOS yazilimi belirgin bir adres yol edinemiyorsa statik yollar çok önemli hale gelir. Ayni zamanda onlar varsayilan yol olarak basvurulan "son çare ag yolu " belirtmek için de faydalidir. Eger bir paket, yönlendirme tablosunda listelenmeyen bir alt aga yönelmisse paket varsayilan yola yönderilir.

RIP'i çalistiran bir router , RIP çalistiran diger bir router vasitasiyla gelen varsayilan bir yol alabilir. Router için diger bir seçenek kendi varsayilan yolunu olusturmasidir.

Statik yollar, **no ip route** global konfigürasyon komutu kulanilarak silinebilir. Yönetici idari mesafe degerini ayarlamak suretiyle statik yolu gönderim bilgisiyle degis tirebilir. Her dinamik yönlendirme protokolü varsayilan bir idari mesafe degerine sahiptir. Statik bir yol, dinamik olarak ögrenilen bir yoldan daha az tercih edilen bir yol olarak tanimlanabilir.



Bir arabirimi gösteren statik yollar, kendi statik yolu olan routerlarca bildirilir ve bu bildirim tüm agda yayilir. Bunun sebebi, bir arabirimi gösteren statik yollarin yönlendirme tablosunda bagli olabileceginin ve dolayisiyla güncellemede kendi statik dogalarini kaybedecenin düsünülmesidir. Eger statik bir yol , **network** komutuyla RIP isleminde tanimli olmayan bir bir arabirime atanirsa, RIP **redistribute static** komutu RIP isleminde belirtilmedikçe yol bildirimi olmayacaktir.

Bir arabirim sistemden düstügünde bu arabirimi gösteren tüm statik yollar Ip yönlendirme tablosundan çikartilacaktir. Keza yazilim statik yolda belirtilmis adres için geçerli birileri atlamayi uzunca süre bulamadiginda statik yol IP yönlendirme tablosundan çikartilacaktir.

Sekil 2' de RIP yönlendirme isleminin basarisizliga ugramasi durumunda RIP yolunun yerini alan GAD routeri üzerinde statik yolun konfigüre edilisi gösterilmistir. Bu degisken statik bir yoldur. Degisken statik yol, RIP'in varsayilan idari mesafesinden (AD- IM) daha büyük statik bir yol üzerinde (130) tanimli biridari mesafenin tanimlanmasiyla konfigüre edilmistir. BHM routeri da varsayilan bir yol ile tanimlanmayi gerektirir.

Statik bir yolu konfigüre etmek için sekildeki komutu global konfigürasyon modunda kullanin.

7.3 IGRP

7.3.1 IGRP' nin Özellikleri

IGRP bir iç ag geçidi mesafe yönü protokolüdür. Mesafe yönü protokolleri matematiksel olarak mesafeleri ölçmek suretiyle yolu hesaplar. Bu ölçüm mesafe yönü olarak bilinir. Mesafe yönü protokolü kullanan routerlar komsu routerlarin her birine düzenli araliklarla bir yönlendirme mesaji içinde kendi yönlendirme tablolarinin tamamini ya da bir kismini göndermek zorundadirlar. Ag içinde yayilan yönlendirme bilgisi olarak routerlar su asagidaki islemleri gerçeklestirirler:

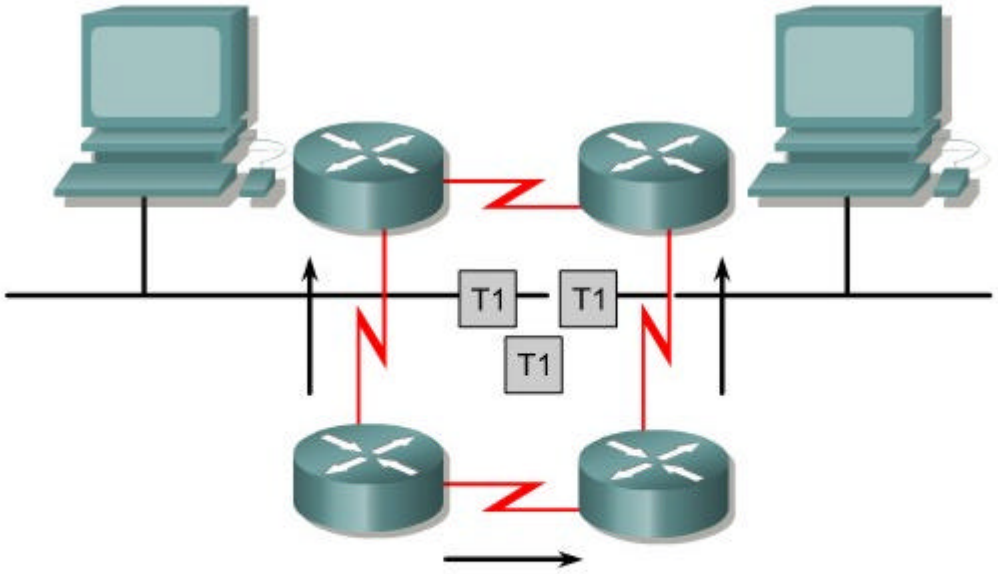
- Yeni alici adresleri tanimlamak
- Hatalari ögrenmek

IGRP Cisco tarafindan gelistirilmis bir mesafe yönü yönlendirme protokolüdür. IGRP , aglari bilgilendirerek 90 saniye araliklarla belli özerk bir sistem için yönlendirme güncellemeleri yollar. IGRP' nin tasarimindaki karakteristik noktalar sunlardir:

- Tanimsiz ve karmasik topolojileri yönetmek için çok yönlülük
- Farkli bant genisligi ve gecikme özellikleri için gereken esneklik
- Çok genis bir ag üzerinde çalisma ölçegi

Varsayilan olarak IGRP yönlendirme protiokolleri metrik olarak bant genisligi ve gecikmeyi kullanirlar. Ilave olarak, IGRP bilesik metrikleri saptamak için degiskenler bileskesinin kullaniminda konfigüre edilebilir. Bu degiskenler sunlardir:

- Bant genisligi
- Gecikme
- Yük
- Güvenilirlik
-



- Composite metric selects the path
- Speed is the primary consideration

7.3 IGRP

7.3.2 IGRP Metrikleri

Show ip protocol komutu ,router üzerinde kullanimda olan yönlendirme protokollerine iliskin ag bilgisi, filtreler ve parametreleri görüntüler. IGRP için metrik gönderimi hesaplamada kullanilan algoritma grafikte gösterilmistir. Bu, K1-K5 metrik degerlerini tanimlar ve maksimum atlama miktarina yönelik bilgi saglar. K1 metrigi bant genisligini ve K3 metrigi gecikmeyi temsil eder. Varsayilan olarak K2, K4 ve K5' in metrik degerleri 0 olarak ayarlanmisken K1 ve K3 1 olarak ayarlanmistir.

Bu tümlesik metrik RIP'in bir alici adresi yolu seçimi esnasinda kullandigi metrik atlamadan daha bir kesin dogruluktadir. En küçük metrik degere sahip olan yol en iyi yoldur.

IGRP nin kullandigi metrikler sunlardir:

- **Bandwith –** yoldaki en düsük bant genisligi
- **Delay** – yol boyunca olan toplam arabirim gecikmesi
- **Reliability** – alici adreslerine yönelik linklerdeki güvenilirlik
- **Load** – Alici adresine yönelik saniyede gönderilen bit sayisi tabanli yük
- **MTU** - yolun maksimum aktarim birim degeri

IGRP tümlesik metrik kullanir. Bu metrik, band genisligi, gecikme, yük ve güvenirligin bir fonksiyonu olarak hesaplanir. Varsayilan olarak, sadece bant genislligi ve gecikme gözönünde bulundurulur. Diger parametrelerin sadece konfigürasyon dogrultusunda aktiflestirilecegi ya da aktiflestirilmeyecegi dügsünülür.

Gecikme ve bant genisligi degerlerle ölçülmez, fakat gecikme ve bant genisligi arabirim komutlarina yerlestirilmislerdir. Yüksek bant genisligine sahip bir link daha düsük bir metrige sahip olacak daha düsük toplam gecikme de daha küçük bir metrige sahip olacaktir.

7.3 IGRP

7.3.3 IGRP Yollari

IGRP üç tip yol bildirir:

- Iç
- Sistem
- Dis

Iç

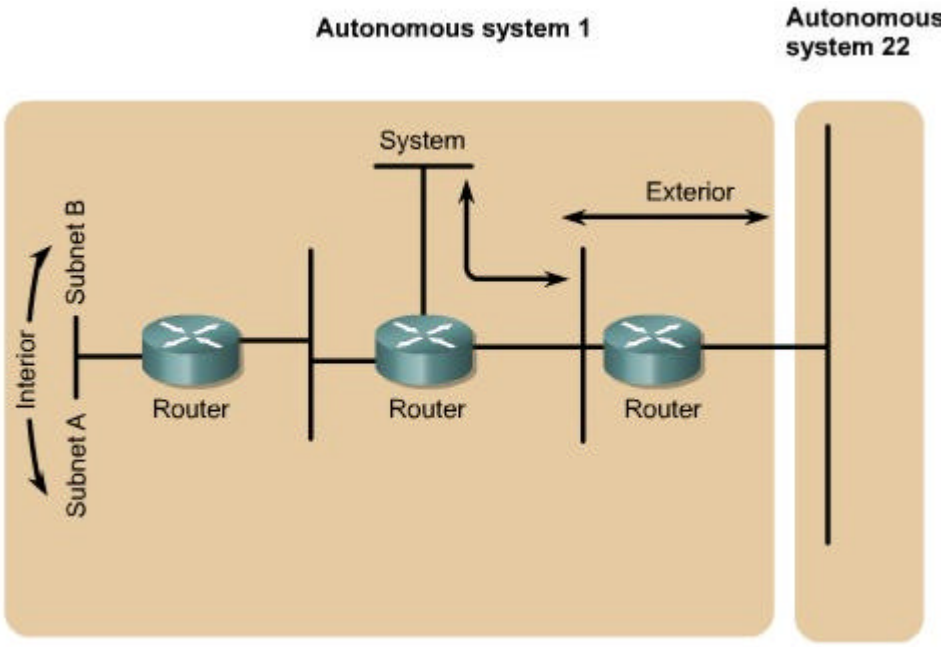
Iç yollar, bir router arabirimine bagli olan agin ile o agin alt agi arasindaki yollardir. Eger bir routera bagli ag alt ag yapilmamis ise IGRP iç yollara bildirimde bulunmaz.

Sistem

Sistem yollari, özerk sistemin içinde kalan ag yollaridir. Cisco IOS yazilimi sistem yolarini dogrudan bagli olan arabiriminden alir ve sistem yol bilgisi diger bir IGRP rafaindan saglanir. Sistem yollari alt ag bilgilerini içermez.

Dis

Dis yollar, özerk sistemin disinda kalan ag yollaridir. ve son nokta ag geçidi tanimlamasi yapilirken göz önüne alinir. Cisco IOS yazilimi, IGRP' nin saglamis oldugu dis yollar listesinden bir son nokta ag geçidi seçer. Yazilim, eger daha iyi bir yol bulunmaz ise varis adresi bagli degilse son nokta ag geçidini kullanir. Eger özerk sistemler dis aga birden fazla baglantiya sahipse farkli routerlar son nokta ag geçidi olarak farkli routerlari seçebilirler.



7.3 IGRP

7.3.4 IGRP Dayaniklilik Özellikleri

IGRP dayanikliligini sürdürmek için pekçok özellige sahiptir. Bunlar:

- Tutucular
- Kesisme noktalari
- Mantiksal çikarim güncellemeri

1.2 Tutucular

Tutucular, uygun olmayan yollardan gelen düzenli günceleme mesajlarini engellemek için kullanilirlar. Bir router devre disi kaldiginda komsu routerlar bunu düzenli gelen günc elleme mesajlarinin olmayisi ile tespit ederler.

1.3 Kesisme noktalari

Kesisme noktalari, bir bilginin geldigi yönde geri routera gönderilmesini belirtmeninyararli olmadigi düsüncesinden kaynaklanir. Kesisme noktasi, gönderim döngüsünü engeller.

1.4 Mantiksal çikarim güncellemeri

Kesisme noktalari, komsu routerlarla olabilecek gönderim döngülerini engellerler fakat mantiksal çikarim güncellemeleri büyük ölçekli gönderim döngülerini bertaraf etmek için gereklidir. Genel ifadesiyle gönderim metriklerindeki artis gönderim döngüsünü gösterir. Mantiksal çikarim güncellemeleri daha sonra silinmek üzere yola gönderilir ve tutuculara

yerlestirilir. IGRP ile mantiksal çikarim güncellemeleri sadece metrik yolda 1.1 ya da daha fazla bir artis var ise gönderilir.

IGRP ayni zamanda pekçok süre tutucu ve zaman araligi içeren degiskenler saglar. Bunlar: zamanlayici güncellemesi, geçersizlik zamanlayicisi, zaman tutucu ve bosaltma zamanlayicidir.

Zamanlayici güncellemesi, gönderim güncelleme mesajlarinin hangi siklikta gönderildigini belirler. Bu degisken için IGRP''in default degeri 90 saniyedir.

Geçersizlik zamanlayicisi, bir routerin daha önceden geçersizligi belirtilmemis özel bir yolda gönderim günceleme mesajlarinin olmadigi durumda ne kadar bekleyecegini belirtir. Bu degisken için IGRP nin default degeri üç defa güncelleme periyodudur.

Zaman tutucular, zayifligindan dolayi yok sayilan yollarla ilgili toplam zaman bilgisini tutarlar. Bu degisken için IGRP nin default degeri 10 saniyenin üzeri için üç defa dir

Son olarak, bosaltma zamanlayicilari , bir yolun gönderim tablosundan çikarilmasindan önce ne kadar zamanin geçmesi gerektigini belirler. Varsayilan degeri yedi defadir.

Günümüzde IGRP artik yaslanmis durumdadir. Alt ag maskelemesi ve degisken uzunlugu konusunda eksikleri vardir. Cisco, bu sorunu gidermek için IGRP' nin 2. Versiyonunu çikarmak yerine IGPR' nin basaryla gelistirilmis seklini yapti.

7.3 IGRP

7.3.5 IGRP Konfigürasyonu

IGRP gönderim islemini konfigüre etmek için, **router igrp** komutunu kullanin. IGRP gönderim islemini sona erdirmek için bu komutun **no** biçimini kullanin

RouterA(config)# **router igpr** sayi
RouterA(config)# **no router igpr** sayi

IGRP islemini tanimlayan özerk sistem numarasi birdir. Ayni zamanda gönderim bilgisini etiketlemekte de kullanilir

IGRP gönderim isleminde ag listesini belirtmek için **network** router konfigürasyon komutunu kullanin. Bir girisi silmek için komutun **no** biçimini kullanin.

7.3 IGRP

7.3.6 RIP' in IGRP' ye Tasinmasi

IGRP' nin 1980 li yillarin basinda olusturulmasiyla Cisco sistemleri iç routerlar arasinda datagram gönderme konusunda RIP kullanimiyla ortaya çikan sorunlari çözen ilk firma idi. IGRP, roterlar arasindaki ag gecikmesi ve bant genisligini inceleyerk dahili agda en iyi yolu tespit eder. IGRP bir sonraki olacak gönderim atlamasi üzerindeki anlasmazliktan kaynaklanan yönlendirme döngülerinden kaçinmak için RIP den daha hizli yakinlasir. Dahasi, IGRP RIP' in atlama miktari sinirini paylasmaz. Bunun ve RIP üzerindeki diger gelistirmelerin neticesi olarak IGRP çok yaygin, kompleks ve topoloji itibariyla çok yayginlik kazandi.

2 **RIP' i IGRP' ye dönüstürme asamalari sunlardir:**
3 1- Dönüstürülecek router üzerindeki mevcut RIP leri dogrulayin
4 2- IGRP' yi router A ve router B üzerinde konfigüre edin
3- Router A ve router B üzerinde **show ip protocols** girin
4- Router A ve router B üzerinde **show ip route** girin

```
Entered on Router A

RouterA#configure terminal
RouterA(config)#router igrp 101
RouterA(config-router)#network 192.168.1.0
RouterA(config-router)#network 192.168.2.0


Entered on Router B

RouterB#configure terminal
RouterB(config)#router igrp 101
RouterB(config-router)#network 192.168.2.0
RouterB(config-router)#network 192.168.3.0
```

7.3 IGRP

7.3.7 IGRP Konfigürasyonunun Incelenmesi

IGRP' nin düzgün bir sekilde yapilandirildigini kontrol etmek için **show ip route** komutunu girin ve " I " ile gösterilen IGRP yolunu arayin
IGRP konfigürasyonunu kontrol eden diger ilave komutlar sunlardir:

- **Show interface** arabirim
- **Show running-config**
- **Show running-config interface**
- **Show running-config begin interface**

- **Show running-config begin igrp**
- **Show ip prtocols**

Ethernet arabiriminin düzgün yapilandirilip yapilandirilmadigini dogrulamak için **show interface fa0/0** komutunu girin resim 1 çikisi göstermektedir

IGRP' nin router üzerinde aktif olup olmadigini görmek için **show ip prot**ocols komutunu girin..

7.3 IGRP

7.3.8 IGRP Sorunlarinin Giderilmesi

Çogu IGRP konfigürasyon hatasi yanlis yazilmis ag bildirimlerini , bitisik olmayan alt aglari, ya da yanlis özerk sistem numaralarini içerir..

Asagidaki komutlar IGRP sorunlarini gidermekte yararlidir:

- **Show ip protocols**
- **Show ip routes**
- **Debug ip igrp events**
- **Debug ip igrp transaction**
- **Ping**
- **Traceroute**

ÖZET

Asagidaki kilit noktalarinin anlasilmis olmasi saglanmalidir.

- Yönlendirme Bilgileri uzaklik vektörü protokolü içerisinende nasil korunur.
- Yönlendirme döngüleri uzaklik vektöründe nasil ortaya çikar
- Sayicinin sonsuza gitmemesinin tanimlanmasi
- Yönlendirme döngülerinin elenmesi
- Güncelleme teriklemeleri ile yönlendirme döngülerinin sakinilmasi
- Durdurma zamani ile yönlendirme döngülerinin engellenmesi
- Arayüz içerisindeki yönlendirme güncellemelerinin önlenmesi
- Çoklu yollarla yük dengelenmesi
- RIP islemleri
- RIP konfigürasyonu
- **ip classless** komutunun kullanilmasi
- Genel RIP sorunlari
- RIP ile yük dengelenmesi
- RIP ile statik yönlendirme

- RIP konfigürasyonunun tanimlanmasi
- IGRP özellikleri
- IGRP metrikleri
- IGRP yönleri
- IGRP denge özelligi
- IGRP konfigürasyonu
- RIP’ in IGRP ye dahil edilmesi
- IGRP konfigürasyonunun tanimlanmasi
- IGRP sorunlarinin giderilmesi
- Configuring IGRP
- Migrating RIP to IGRP
- Verifying IGRP configuration
- Troubleshooting IGRP

BÖLÜM – 8

Genel Bakis

IP ler sistemlere dagitimi zor oldugu icin sinirlidir. Network uzerinde bir problem olustuguna bakmadan , verinin ulastigindan emin olan bir mekanizma yoktur. Donanim hatasi , uygunsuz konfigurasyon , yada yanlis yonlendirme bilgileri gibi çesitli nedenlerle veri hedefine ulasmamis olabilir. Bu hatalari tesbit etmek icin , verinin ulasmasinda bir hata oldugunu gondericiye bildiren ICMP protokolu kullanilir. Bu bolum ICMP hata mesajlarini ve bu mesajlarin kullanilma yollarini aciklar.

Çünkü Ip, iletim hatasi veya control mesaji iletmek icini bir mekanizmaya sahip degildir. IP kullanicilara hata ve control mesaji gonderip almak icin ICMP protokolunu kullanir. Bu bolum kullanicilar icin konfigurasyon parametreleri ve bilgiler iceren control mesaji ile ilgilenir. ICMP control mesajlari bilgisi bilgisi network kurtarimi icin onemli bir bolumdur , ayrica Ip networklerini tamamen anlamak icin bir anahtardir.

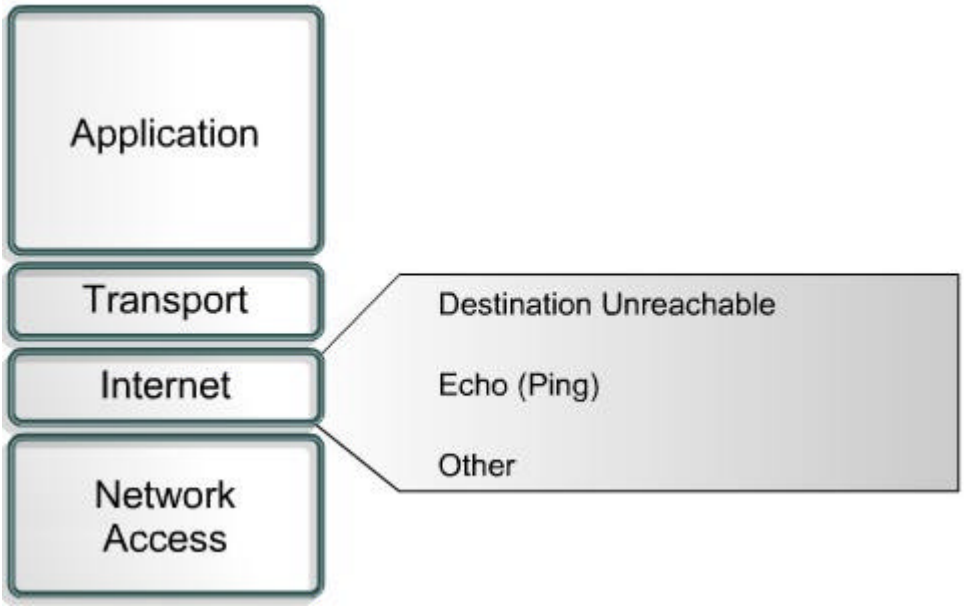
Ögrenciler bu bolumu bitirdiginde yapabilecekleri ;

- ICMP nin tanimlanmasi
- ICMP mesaj formatlarinin tanimlanmasi
- ICMP hata mesaj tiplerinin taninmasi
- Potansiye ICMP hata mesajlarinin tanimlanmasi
- ICMP control mesajlarinin taimlanmasi
- Bir çesit ICMP control mesajini bugunk u networklerde kullanimi

8.1 TCP/IP Hata Mesajlarina Genel Bakis

8.1.1 Internet Mesaj Kontrol Protokolü (ICMP)

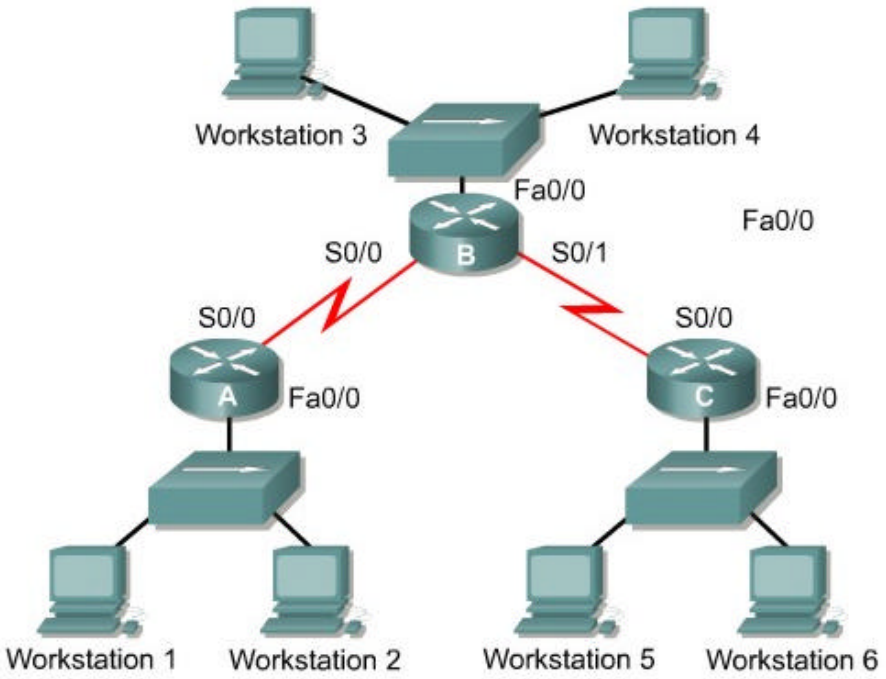
Verinin iletilmesi icin Ip guvensiz bir metoddur.IP network haberlesmesinde bir problem olustugunda, verinin ulastigindan emin olunan bir mekanizmaya sahip degildir. Router gibi araci bir cihaz aksar ise veya hedef aygitin network baglantisi kesilirse veri hedefe ulasamaz. Ek olarak Ip nin temel dizayninda verinin iletilmesinin aksadigini bildirecek bir uygulama yoktur. ICMP IP nin bu guvensizligini gidermez, guvenilirlik ihtiyac duyuldugunda bir ust katmanda bulunmalidir



8.1 TCP/IP Hata Mesajlarina Genel Bakis

8.1.2 Hatalarin Raporlanmasi ve Hata Düzeltilmesi

ICMP, IP icin bir raporlama protokoludur. Bir hata olustugunda , ICMP datagram in kaynagina hata mesajini raporlamak icin kullanilir. Ornek olarak resimdeki Workstation1 Workstation6 ya bir veri gonderiyor , fakat router C deki Fa0/0 arayuzu kapali durumda , o zaman Router C WorkStation1 e verinin ulasmadigini gosteren bir mesaj gondermek icin ICMP protokulunu kullanir. ICMP karsilasilan network problemini duzeltmez sadece hata mesajini raporlar



Rotuer C Workstation 1 den bir datagram aldiginda , Sadece datagramin kaynak ve hedef Ip adreslerini bilir. Verinin Router C ye nasil geldigi hakkinda hic bir sey bilmez. Bu yuzden Router C sadece hatanin Workstation1 den kaynaklandigini bildirir ve herhangi bir ICMP mesaji Router A ve Router B ye gonderilmez. ICMP sadece mesaj kaynaginin durumunu raporlar.

8.1 TCP/IP Hata Mesajlarina Genel Bakis

8.1.3 ICMP Mesaj Teslimi

ICMP mesaji herhangi bir verinin datagram icerisine yerlestirilmesi gibi yerlestirilir. Resim 1 bir ICMP mesajinin IP datagrami icerisine nasil yerlestirildigini gosterilir.

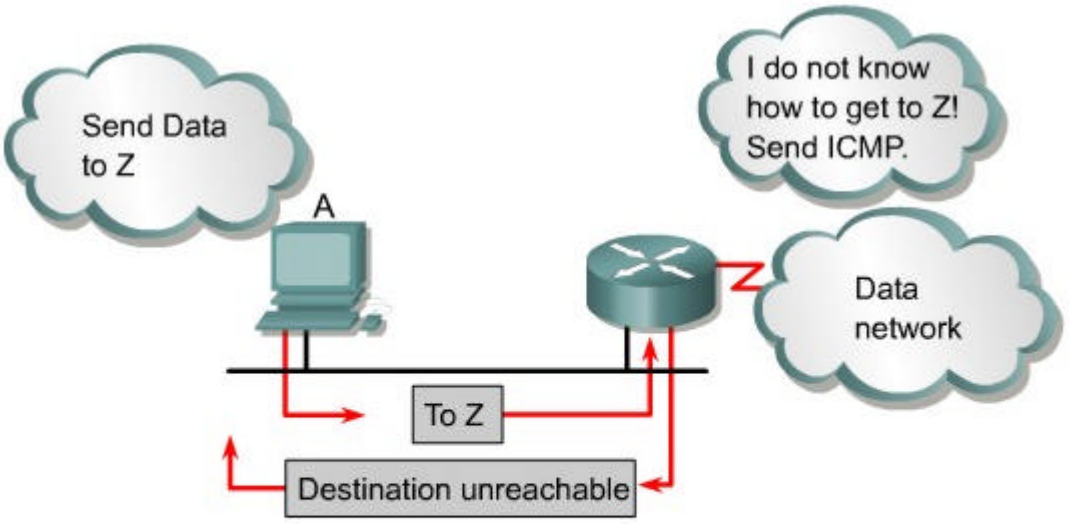
ICMP mesaji diger veriler gibi iletildikten sonra ayni veriler gibi ulastirilamayabilir. Bu bir hata mesajinin hata ile karsilasmasi sonucu daha fazla hata mesajinin gonderilmesi ile sonuclanir. Bu yuzden hata ile karsilasan bir ICMP hata mesaji kendi ICMP mesajini uretmez.

8.1 TCP/IP Hata Mesajlarina Genel Bakis

8.1.4 Ulasilamayan Aglar

Network haberlesmesi karsilikli degis tokus esasina dayanir. Ilk olarak gonderme ve alma aygitlari uygun bir sekilde kanfigure edilmis TCP/IP stoguna sahip olmalidir. Bu sart TCP/IP protokollerinin yuklenmesini , ve IP adres ve subnet Mask larinin uygun bir sekilde konfigure edilmesini icerir.Eger datagramlar local network disinda bir yere gonderilecekse bir default gateeway de konfigure edilmeli. Ikinci olarak araci aygitlar datagramlari kaynak aygittan hedef aygita yonlendimek icin yerlestirilmeli. Routerlar bu fonksiyonu saglar. Ve yine routerlar kendi arayuzlerinde uygun bir sekilde konfigure edilmis TCP/IP protokollerine sahip olmalidir , ve yine uygun yonlendirme protokolunu kullanmalidir.

Eger bu sartlar saglanmaz ise , network haberlesmesi isleyemez. Ornek olarak , gonderici aygit datagrama olmayan bir IP adresi verebilir , veya hedef aygit networkte offline olmus olabilir. Routerlar kapali bir arayuze baglanabilir , veya hedef networke ulasmak icin gerekli olan bilgilere sahip olmayabilir. Eger hedef network e ulasilamiyorsa , hedef erisilemez network olarak tanimlanir.



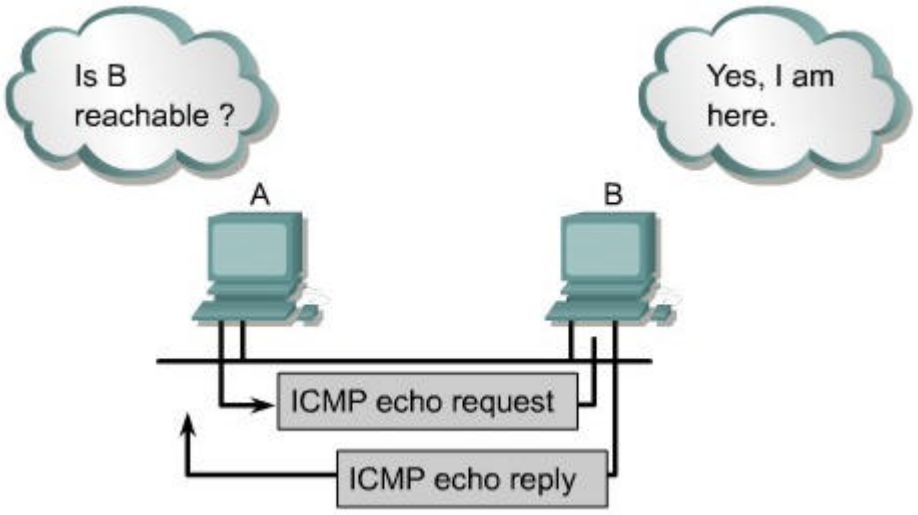
An ICMP destination unreachable meassage is sent if:

- Host or port unreachable
- Network unreachable

8.1 TCP/IP Hata Mesajlarina Genel Bakis

8.1.5 Ping Kullanarak Hedefe Ulasilabilinirligin Testedilmesi

ICMP protokolu hedefin varligini test etmek icin kullanilabilir. Sekil 1 ICMP nin echo mesaji icin kullanimini gosteriri.Eger hedef aygit ICMP echo istegi alirsa , echo istegi gonderen kaynaga echo cevap mesaji duzenler. Eger gonderici echo cevap mesajini alirsa , bu hedef aygitin Ip protokolu ile erisebildigini gosterir.



Echo istek mesaji tipik olarak sekil 2 de gosterildigi gibi ping komutu gibi baslar. Bu ornekte komut hedef aygitin IP adresi ile kullaniliyor. Komut sekil 3 de gosterildigi sekilde de hedef aygitin IP adresini kullanarak isletilebilir. Bu ornekte ping komutu 4 echo istek ve alimini ,4 echo cevabini ve iki aygit arasinda IP kullanarak kurulan baglantiyi gosteriyor.

8.1 TCP/IP Hata Mesajlarina Genel Bakis

8.1.6 Çok Uzaklardaki Yönlerin Bulunmasi

Datagramin daire seklinde yolculuk ettigi, hedefe asla ulasamadigi network haberlesmesi gibi durumlar ortaya cikabilir. Bu iki rotuer in datagrami surekli olarak bir grup arasinda birbirlerine gondermesi ile olusabilir. Bu bir sonraki hob un hedef oldugu düsünüldügü icin olusur. Bu yonlendirme bilgilerinin yanlis oldugunu gosteren bir ornektir.

Yonlendirme protokulunun sinirlandirmalari hedefin ulasilamaz olmasinin sounucu olabilir. Ornekte RIP datagramlarin yolculuk mesafelerini sinirlandiran bir limite sahiptir. RIP in hop limiti 15 dir. Bu paketlerin en fazla 15 routerdan gecebilecegi anlamina gelir.

Bu olaylarin her birinde asiri olarak uzun bir yol vardir.

Paketler en fazla atlama sayisi kadar iletilebilir. Bu ayni zamanda ulasma süresi TTL kadardir. Çünkü TTL , yönlendirme protokolleri tarafindan tanimlanmis en fazla atlama sayisi ile eslestirilmistir. Her gönderilen dogrulama paketi TTL degerlerinde tanimlanmistir. Her bir router dogrulama paketini isleyebilir. TTL de dogrulama paketi sifir olarak ulasirsa paket atilir.

8.1 TCP/IP Hata Mesajlarina Genel Bakis

8.1.7 Yanki Mesajlari

Herhangi bir pakette oldugu gibi ICMP mesajlarida ozel formatlara sahiptir. Sekil 1 de her bir ICMP mesaji kendine has karakteristige sahiptir. Fakat butun ICMP mesaj formatlari ayni 3 alanla baslar.

- Tip
- Kod
- Saglama alani (Cheksum)

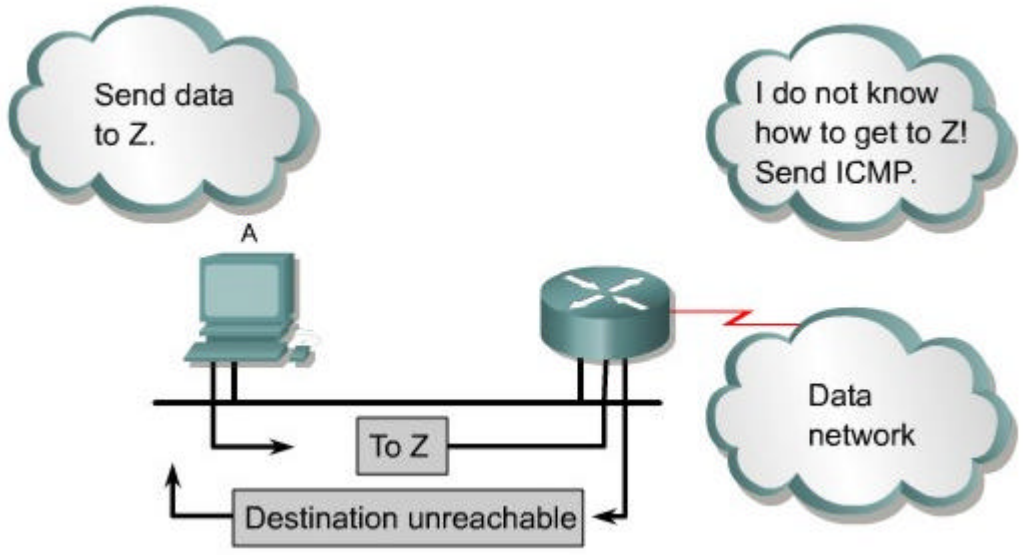
Tip gonderilen ICMP mesajinin tipini gosterir. Kod alani mesaj tipine ait ozel bilgileri icerir. Checksum alani ise diger paket tiplerinde oldugu gibi verinin butunlugunu kontrol etmek icin kullanilir

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

ICMP echo istek ve cevap mesaj formatlarini gosterir. Anlamli tip ve kod numaralari her bir mesaj icin gosterilmistir. Kimlik ve sira numarasi alanlari her bir cevap ve istek echo mesajlari icin tek tir. Kimlik ve sira numarasi alanlari echo cevabini dogru echo istegine eslestirmek icin kullanilir. Data alani echo istek veya cevap mesajinin bir bolumu olan ek bilgiler icerebilir.

8.1 TCP/IP Hata Mesajlarina Genel Bakis

8.1.8 Hedefe Ulasamayan Mesajlar



Datagram lar her zaman hedeflerine gonderilemezler. Donanim hatalari , yanlis protokol kanfigurasyonlari , kapanmis arayuzler ve yanlis yonlendirme bilgileri datagramlarin basarili bir sekilde ulasmasini engelleyen nedenlerdir. Bu durumlarda ICMP gondericiye datagramin dogru sekilde gonderilemedigini gosteren bir “hedef ulasilamaz” mesaji gonderir.

Sekil de bir “ICMP hedef ulasilamaz” mesaj basligini gosterir. Tip alanindaki 3 degeri mesajin “hedef ulasilamaz” mesaji oldugunu gosterir. Kod degeri paketin ulasamamasinin nedenini gosterir. Sekil 3 deki kod degeri networkun ulasilamadigini gosteren 0 degerine sahiptir. Sekil 4 mumkun olan “hedef ulasilamaz” mesajlarina ait kodlarin anlamlarini verir.

Bir “hedef ulasilamaz” mesaji paket gondermek icin parcalanma istendigi zaman gonderilebilir. Parçalanma genelde datagram Token-Ring networkden Ethernet networkune gonderilecegi zaman gereklidir. Eger datagram parçalanmaya izin vermezse paket gonderilemez. Bu yüzden “hedef ulasilamaz” mesaji gonderilecektir. Yine “hedef ulasilamaz” mesaji FTP veya Web servis gibi IP tabanli servisler kullanilamaz oldugu zaman da gonderilebilir. Etkin olarak bir IP networkunu kurtarmak icin “ICMP hedef ulasilamaz” mesaj cesitlerini anlamak gerekir.

.

8.1 TCP/IP Hata Mesajlarina Genel Bakis

8.1.9 Çesitli Hata Raporlari

Datagramlari isleyen aygitlar basliginda bazi hata tiplerini içeren datagramlari gondermeyebilir. Bu hata hedef bilgisayarin veya networkun durumu ile ilgili degildir fakat datagramin islenmesi ve ulastirilmasi engellenir. Bu durumda bir ICMP tip 12 parametreli problem mesaji datagramin kaynagina gonderilir. Sekil 1 parametre problem mesaj basligini gosterir.

Parametre problem mesaj basligi bir gosterici alan icerir. Kod degeri 0 oldugu zaman, gosterici alan hata ureten datagrami gosterir.

The parameter problem message includes the pointer field in the header. When the code value is 0, the pointer field indicates the octet of the datagram that produced the error.

8.2 TCP/IP Takim Kontrol Mesajlari

8.2.1 Kontrol Mesajlarina Giris

Internet kontrol mesaj protokolu(ICMP) TCP/IP protokol takiminin onemli bir parcasidir. Gercekte butun IP uygulamalari ICMP destegini icermelidir. Bunun sebepleri basittir. Ilk olarak IP verinin ulasmasini garanti etmedigi icin , hata meydana geldigi zaman dogal olarak kullaniciyi bilgilendirmeyecektir. Üstelik IP bilgilendirme veya kontrol amacli mesajlar icermemektedir. ICMP bu fonksiyonlari IP icin yerine getirir.

Hata mesajlarindan farkli olarak , kontrol mesajlari kayip paketlerin veya paket iletilmesinde olusan hatalarin sonucu degildir. Kontrol mesajlari kullaniciya uzak network icin daha iyi bir gateway veya network deki tikanikligi bildirmek icin kullanilir. Bütün ICMP mesajlari gibi , ICMP kontrol mesaji da bir IP datagrami ile sarmalanir.

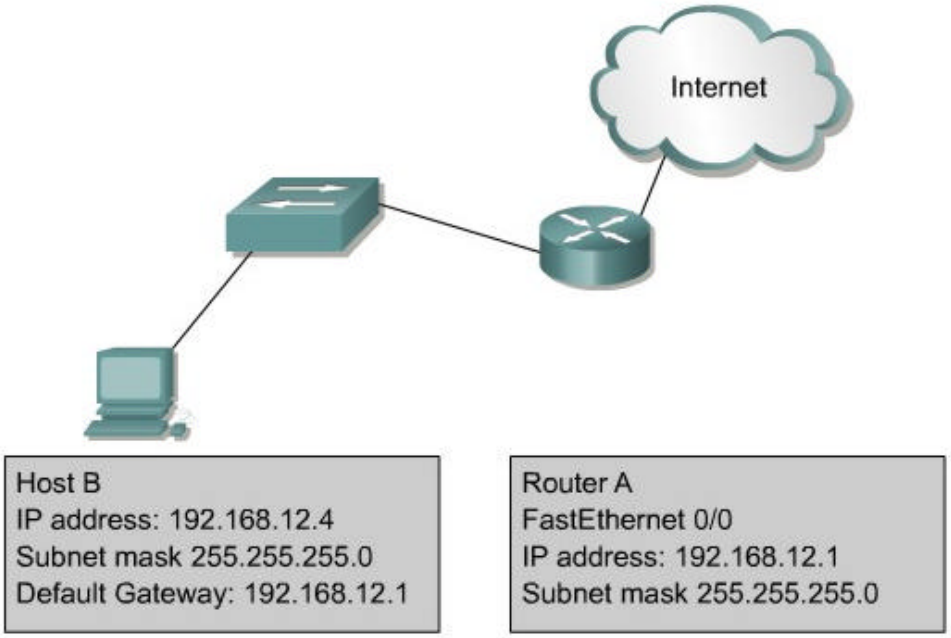
Çoklu kontrol mesaj tipleri ICMP tarafindan kullanilir. Cok yayginlarindan bazilari sekil 2 de gosterilmistir. Bunlarin cogu bu bolumde gosterilmistir

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

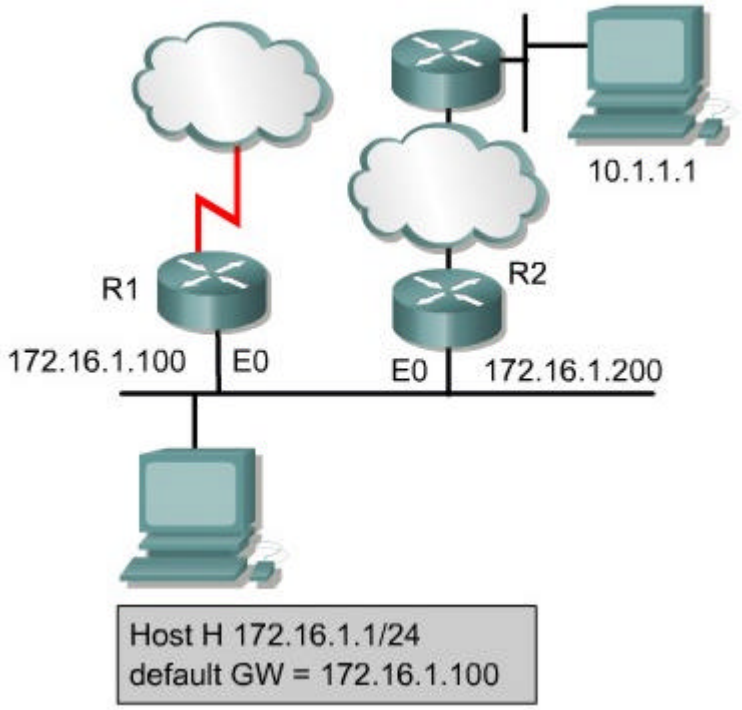
8.2 TCP/IP Takim Kontrol Mesajlari

8.2.2 ICMP Yeniden Gönder/Degistir Talepleri

Siradan bir ICMP kontrol mesaji da ICMP degistirme istegidir. Bu tip mesajlar sadece bir çogu zaman bir router tanimlanarak olusturulan gateway tarafindan baslatilabilir. Butun coklu networklere erisen kullanicilar bir default gateway konfigure etmelidir. Bu default gateway kullanici ile ayni network e baglanmis bir routerin port adresidir.



Sekilde internete erisebilen bir router a baglanmis kullaniciyi gosteriyor. Default gateway i Fa 0/0 in adresi olarak konfigure edilmistir. Kullanici B kendisine direk bagli olmayan bir networke erismek icin bu IP adresini kullanir. Normal olarak kullanici B sadece tek bir gatewat e baglidir. Hernasilsa bazi durumlarda , kullanici birden fazla roter a bagli bir segment e baglanir. Bu durumda kullanicinin default gateway i sozu gecen network hakkinda en iyi yolu kullaniciya bildirmesi icin ICMP degistirme istegine ihtiyac duyar.



Sekil 2 ICMP degistirilmesinin kullanildigi bir network gosterir. Network 10.0.0.0/8 de Kullanici B kullanici C ye bir paket gonderir. Host B ayni ayni networke direkt bagli olmadigindan , paketi once kendi defaule gateway ine gonderir. Router A kendi yonlendirme tablosuna bakarak 10.0.0.0/8 icin dogru yonlendirme yi bulur. Paketi gonderir ve kullanici B

ye network 10.0.0.0/8 e erismek icin default gateway inin Router B olmasi gerektigini soyleyen bir ICMP degistirme istegi gonderir.

Default gateway sadece asagidaki sartlar yerine gelirse ICMP degistirme istegi gonderir.

- Router da paketin geldigi arayuz paketin disari gonderildigi arayuzle ayni olacak
- Kaynak IP adresinin subnet/network adresi yonlendirilen paketin IP adresinin subnet/network adresi ile ayni olacak.
- Datagram kaynaga yonlendirilmeyecek.
- Degistirme istegi icin yonlendirme baska bir ICMP degistirme istegi olmayacak.
- Router yonlendirme isteklerini gondermek icin konfigure edilmis olacak. (default olarak , Cisco routerlari ICMP degistirme isteklerini gonderir. Arayuz alt komutu olan **no ip redirects** ICMP degistirme istegini disable edecektir.

ICMP degistirme istegi sekil 2 te gosterilen formati kullanir ve ICMP 5 koduna sahiptir. Ek olarak 0,1,2 ve 3 kod degerlerine sahiptir.

ICMP degistirme deki Yonlendirme internet adres alani moduler bir network icin default gateway gibi kullanilabilir. Sekil 2 deki ornekte Router A Router internet adresi 172.16.1.200 olan kullanici B ye bir ICMP degistirme mesaji gonderiyor.

8.2 TCP/IP Takim Kontrol Mesajlari

8.2.3 Saat Eslemesi ve Gemis Zamaninin Kestirilmesi

TCP/IP protokol takimi sistemlere cok uzak mesafelerdeki coklu aglarda bulunan diger bir sisteme baglanmasina musade eder. Bu networkleri her biri kendi yollarinda saat senkronizasyonunu icerir. Bunun sonucunda farkli aglarda saat senkronizasyonu isteyen yazilimlar kullanan kullanicilar bazen problem ile karsilasabilir. ICMP timestamp mesaj tipi bu problemi gidermek icin dizayn edilmistir.

ICMP timestamp istegi uzak kullaniciya saat ayarini sormaya musaade eder. Uzak kullanici ICMP timestamp cevap mesajini kullanarak istege cevap verir.

ICMP timestamp mesajinda tip alani 13 veya 14 olabilir. Kod alani her zaman 0 dir cunku ek olarak eklenebilecek parametre yoktur

All ICMP timestamp reply messages contain the originate, receive and transmit timestamps. Using these three timestamps, the host can estimate transit time across the network by subtracting the originate time from the transit time. It is only an estimate however, as true transit time can vary widely based on traffic and congestion on the network. The host that originated the timestamp request can also estimate the local time on the remote computer.

ICMP timestamp mesaji toplam network iletim zamanini ve uzak kullanicidaki zamani hesaplamak icin basit bir yol icerir. bu bilgileri bulmak icin en iyi yol degildir. TCP/IP

protokol takiminin daha bir ust katmaninda olan network time protocol (NTP) daha guvenilir bir protokoldur.

8.2 TCP/IP Takim Kontrol Mesajlari

8.2.4 Sorgulama Bilgileri ve Mesaj Formati Yanitlari

ICMP bilgi istegi ve cevap mesaji kullaniciya kendi network numarasini bulmaya musade eder. Sekil 1 ICMP bilgi istek ve cevap mesajinin formatini gosterir.

Bu mesajlarda iki tip kod mevcuttur. Tip 15 bir bilgi istek mesaji oldugunu , tip 16 ise bilgi cevap mesaji oldugunu gosterir. Bu ICMP mesajlari eski olarak sayilir. BOOTP ve DHCP gibi protokoller kullaniciya kendi network numaralarini bulmaya izin verir.

8.2 TCP/IP Takim Kontrol Mesajlari

8.2.5 Adres Maskelemenin Gereksinimi

Bir network yoneticisi ana IP adresini coklu aglara bolmek icin subnetting islemini kullandiginda yeni alt ag maskesi olusturulur. bu yeni alt ag maskesi IP adresi icerisinde kac bitin ag, kac bitin kullanici adresi oldugunu tanimlar. Eger bir kullanici alt ag maskesini bilmiyor ise router bir adres maskesi istegi gonderebilir. Eger router in adresi biliniyor ise bu istek direk olarak router a gonderilir. Diger turlu istek yayin seklinde yapilir. Router istek mesajini aldiginda adres maskesi cevabini gonderecektir. Ornek olarak , kullanicinin Sinif B networkunde oldugunu ve IP adresinin 172.16.5.2 oldugunu varsayalim. Bu kullanici alt ag maskesini bilmiyor,
Bu yuzden bir alt ag maskesi istegi yayinliyor:

Kaynak Adres:	172.16.5.2
Hedef Adres:	255.255.255.255
Protokol:	ICMP = 1
Tip:	Address Mask Request = AM1
Kod:	0
Maske:	255.255.255.0

Bu yayin 172.16.5.1 yerel yonlendirici tarafindan alinir. Yonlendirici adresleri cevap olarak gonderir:

Kaynak Adres:	172.16.5.1
Hedef Adres:	172.16.5.2
Protokol:	ICMP = 1
Tip:	Address Mask Reply = AM2
Kod:	0
Maske:	255.255.255.0

Adres maskesi istegi ve cevap mesajinin cerceve formati sekil 1 de gosterildigi gibidir. Sekil 2 adres maskesi istek mesajinda tanimlanan her bir alanin tanimlamalarini gosterir. Bu formatlar hem istek mesajinda hemde cevap mesajinda kullanilir. ICMP tip 17 istek icin kullanilir , 18 ise cevap icin kullanilir.

8.2 TCP/IP Takim Kontrol Mesajlari

8.2.6 Router Kesif Mesajlari

Networkdeki Bir kullanici boot edildiginde ve kullanici manuel olarak default gateway konfigure edilmediginde router bulma islemi ile onu bulabilir. Bu islem kullanicinin butun yonlendiricilere yayin yapmasi ile baslar. Sekil 1 ICMP kesif mesajini gosterir. Eger kesif mesaji kendisini desteklemeyen bir router a gonderilmis ise cevaplanmayacaktir.

Kesif islemini destekleyen bir router kesif mesaji aldiginda router tanitim mesaji geri döner.

8.2 TCP/IP Takim Kontrol Mesajlari

8.2.7 Router Rica Mesajlari

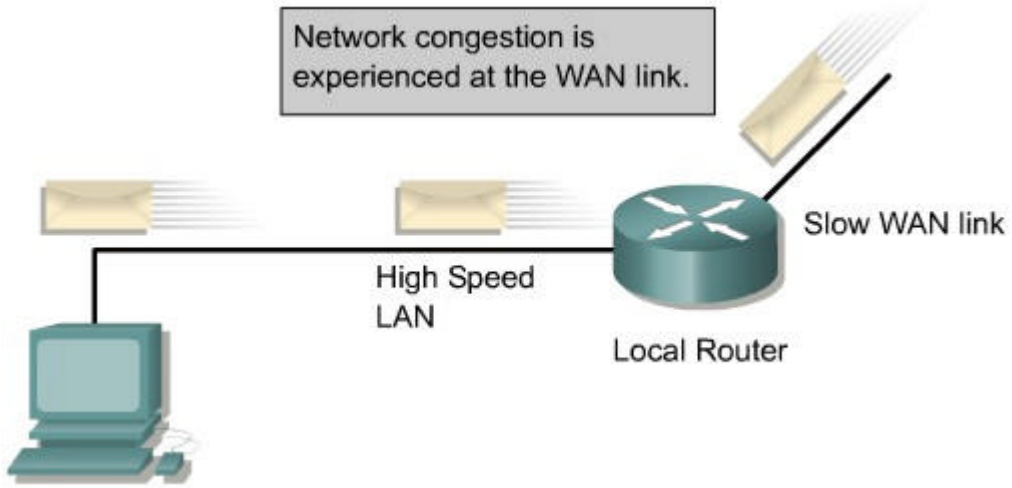
Kullanici bir ICMP router istek mesajini default gatewayi belirlemek icin gonderir. Bu mesajin ilk adimi router kesif islemidir. Bir lokal yonlendirici lokal kullanici icin default gateway i kendi yonlendirici kimlik bilgisi ile tanimli olan bir cevap mesaji gonderecektir.

8.2 TCP/IP Takim Kontrol Mesajlari

8.2.8 Tikaniklik ve Akis Kontrol Mesajlari

Iki bilgisayar ayni kaynaga ayni anda ulasmak istedigi zaman , kaynak bilgisayar trafik yogunlugundan bunalir. Tikaniklik eger trafik yuksek hizli LAN dan düsük hizli LAN a dogru ise gerçeklesir. Eger hatta cok fazla tikaniklik var ise paketler bailacaktir. ICMP source-quench mesaji veri kaybini azaltmak icin kullanilir. source-quench mesaji gondericiye verilerin bit oranini indirmesini soyler. Bircok durumda tikaniklik kisa bir sure sonunda giderilir ve kaynak yavasca transfer oranini eskisine gore azaltir. Bir cok Cisco router lari default olarak source-quench mesajlari gondermez. Cunku source-quench mesajinin kendisi de ag trafigini yogunlastirir.

Küçük ev aglari (SOHO) , ICMP kaynak söndürme mesajlarinin etkin bir sekilde kullanilabilmesini gösteren bir örnektir. Küçük bir ev agi dört adet bilgisayar çalisma grubunun CAT-5 kablosu kullanilarak 56K modem ile internet baglantisinin paylasildigini düsünelim. Ev aginda 10Mbps lik hizli bir baglanti görülür. WAN baglantisinin ise 56K mevcut yavas badgenisligi vardir. Bu nedenle veri kayiplari ve gönderememe sorunlari ortaya çikar. ICMP mesajlari ile sunucu alt ag geçidi yapar. Diger sunucularin sorgusunu azaltmak için iletim hizi düzenlenebilir. Böylece veri kayiplari önlenebilir.



ÖZET

Asagidaki kilit noktalarinin anlasilmis olmasi saglanmalidir:

- IP , ICMP mesaj uyarilari göndererek kullanarak hedefe olan veririn ulasilamama sorunlarinda en iyi çaba sarfedilir.
- ICMP yanki sorgulari ve yanki tekrarlayici mesajlari ag yöneticilerinin islem sorunlarinin giderilmesinde IP baglatantisnin test edilebilmesine olanak saglar.
- ICMP mesajlari iletisimde IP protokolü kullanilarak teslim güvenilmezligini ortadan kaldirir
- ICMP paketleri bulundurduklari baslik bilgilerini tip ve kod alanlari ile baslatirlar.
- Özel ICMP hata mesajlarinin potansiyel nedenlerinin belirtilmesi
- ICMP Ł-kontrol mesajlarinin fonksiyonlari
- ICMP geridönderme/deistirme sorgu mesajlari
- ICMP eszamanli saat ve iletim zamaninin kestirim mesajlari
- ICMP bilgi sorgulari ve yanit mesajlari
- ICMP adres maskeleme ve yanit mesajlari
- ICMP router kesfetme mesajlari
- ICMP router istek mesajlari
- ICMP tikaniklik ve akis kontrol mesajlari

BÖLÜM - 9

Genel Bakis

Router,dinamik yönlendirme protokolünü kullanarak veya el ile olarak kurulmus statik yönlendirmelerle ag için izlenecek yollari ögrenir. Router yollari bulmak için genellikle dinamik ve statik yönlendirme kombinasyonunu kullanir. Kullanilan metot ne olursa olsun , router bir yolun gidilecek yer için en iyi yol oldugunu belirlerse kendi içindeki yönlendirme tablosuna onu yükler. Bu bölümde , yönlendirme tablosunun içeriginin çevrimi ve tetkiki için gerekli metotlari tanimlayacaktir.

Ag testi ve hata düzeltimi muhtemelen tüm ag yöneticilerinin islerinin büyük kismini olustururlar. Etkili test ve hata düzelti minin mantiksal , sirali ve iyi belgelendirilmis biçimde yapilmasi gerekir. Aksi halde ayni problemler yeniden ortaya çikabilir ve ag yöneticisi asla agi tam manasiyla anlayamaz. Bu bölüm agda hata düzeltimi için kalipsal bir yaklasimi açiklar ve hata düzeltimi islemi için bazi araçlar saglar.

Yönlendirme sorunlari ag yöneticileri için teshisi en zor ve en yaygin olanlaridir. Yönlendirme problemlerini tanimlamak ve çözmek kolay olmayabilir. Fakat bu isi kolaylastirabilecek birçok aygit mevcuttur. Bu bölümde bu aygitlarin en önemli birkaçini tanitilacak ve kullaniminda pratiklik saglanacaktir.

Bu bölümü tamamlayan kimseler asagidakileri yapabilmelidirler:

- **Show ip route** komutunu kullanarak routerde kurulu yollar hakkinda detayli bilgi edinmek
- Varsayilan bir yolu veya agi konfigüre etmek
- Routerin 2. ve 3. Katmani kullanarak agdan veriyi nasil tasidigini anlamak
- **Ping** komutunu kullanarak temel ag baglanti testleri yapmak
- **telnet komutunu** kullanarak kaynak ve hedef uç birimleri arasindaki uygulama katmani yazilimini dogrulamak
- OSI asamalarinin ardisik olarak testi ile hata düzeltimi
- **Show interfaces** komutunu kullanarak 1. ve 2. Katman problemlerini dogrulatmak
- **Show ip route ve show ip protocol komutlarini** kullanarak yönlendirme meselelerini tanimlamak
- **Show cdp** komutunu kullanarak 2. Katman baglantisini onaylamak
- **Traceroute** komutunu kullanarak aglar arasinda alinan paket yollarini tanimlamak
- **Show controllers serial** komutunu kullanarak uygun kablonun bagli oldugunu garantiye almak
- Temel **debug** komutlarini kullanarak router aktivitelerini gözlemlemek

9.1 Yönlendirme Tablosunun Incelenmesi

9.1.1 show ip route komutu

Routerin öncelikli fonksiyonlarindan biri verilen hedef için en iyi yolu tayin etmektir. Router,bir yöneticinin konfigürasyonundan veya diger router lar dan yönlendirme protokolleri yoluyla yollari ögrenir. Routerlar bu yönlendirme bilgisini yönlendirme cetvellerinde saklarlar ve dinamik hafizada (DRAM) kullanirlar. Bir yönlendirme cetveli en iyi yollarin bir listesini içerir. Routerler bu cetveli ileri paket kararlari yapmakta kullanirlar.

Show ip route komutu IP yönlendirme cetvelinin içerigini gösterir. Bu cetvel bilinen tüm aglara ve alt birimlerine girisleri, bu bilginin nasil ögrenildigini belirten bir Kod kadar içerir.

Asagidakiler **show ip route** komutuyla birlikte kullanilabilen bazi ek komutlardir:

- **show ip route *connected***
- **show ip route *network***
- **show ip route *rip***
- **show ip route *igrp***
- **show ip route *static***

Bir yönlendirme tablosu haritalari önekleri sinir disi arabirime baglar. RTA 192.168.4.46 için gönderilen bir paket aldiginda bu cetvelde 192.168.4.0/24 olarak görülür. Bu halde router paketi yönlendirme tablosu girisinde kurulmus arabirime gönderir. RTA eger 10.3.21.5 e gönderilmis bir paket alirsa bu paketi seri 0/0 disina yollar. Örnek yönlendirme tablosu dogrudan bagli aglar için 4 yol gösterir. Bu yollardan “C” etiketli olanlar dogrudan(direkt) bagli aglar için geçerlidir. RTA ag için gönderilmis ve cetvelde listelenmemis herhangi bir paketi atar. RTA için gerekli tablo , diger istasyonlara ilerlemesi için daha fazla yol içermek zorunda kalacaktir. Bu yeni yollar su iki metottan birinin kullanimiyla eklenebilir:

- **Statik Yönlendirme** – bir yönetici el ile , bir veya daha fazla hedef aglara yönlendirmeyi tanimlar
- **Dinamik Yönlendirme** – Routerler, yönlendirme bilgisini ve bagimsizca seçilmis en iyi yolu degis tokus etmek için yönlendirme protokolünde belirlenmis kurallari izler.

Yönetimselsel olarak tanimlanan yollarin statik oldugu söylenmektedir. Çünkü ag yöneticisi degisiklikleri el ile programlayana kadar degisiklik yapmazlar. Diger routerler tarafindan ögrenen routerlar dinamiktir. Çünkü komsu routerler kendilerini yeni bilgilerle güncellediklerinde otomatik olarak degistirebilirler. Her metot temel bazi avantaj ve dezavantajlara sahiptir.

.

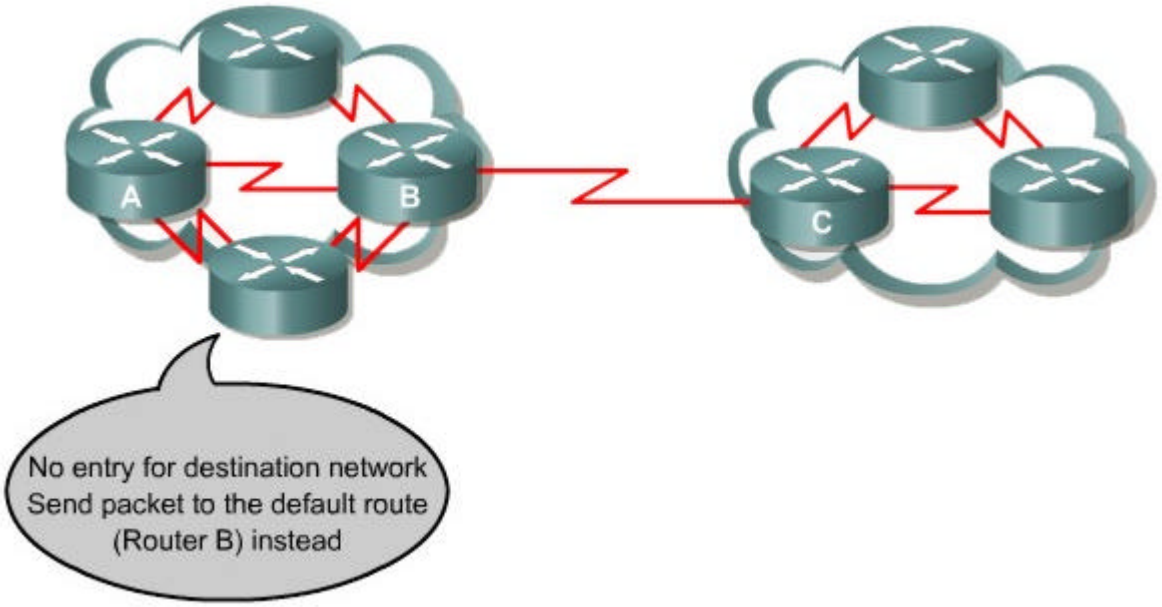
Static Routing Advantages	Static Routing Disadvantages
Low processor overhead. Routers do not spend valuable CPU cycles calculating the best path. This requires less processing power and less memory (and therefore, a less expensive router).	*High maintenance configuration*. Administrators must configure all static routes manually. Complex networks may require constant reconfiguration.
No bandwidth utilization. Routers do not take up bandwidth updating each other about static routes.	*No adaptability*. Statically configured routes can not adapt to changes in link status.
Secure operation. Routers that do not send updates will not inadvertently advertise network information to an untrusted source. Routers that do not accept routing updates are less vulnerable to attack.	
Predictability. Static routes enable an administrator to precisely control a router's path selection. Dynamic routing sometimes yields unexpected results, even in small networks.	

Dynamic Routing Advantages	Dynamic Routing Disadvantages
High degree of adaptability. Routers can alert each other about links that are down or about newly discovered path. Routers automatically "learn" a network's topology and select optimum paths.	*Increased processor overhead and memory utilization*. Dynamic routing processes can require a significant amount of CPU time and system memory.
Low maintenance configuration. After the basic parameters for a routing protocol are set correctly, administrative intervention is not required.	*High bandwidth utilization*. Routers use bandwidth to send and receive routing updates, which can detrimentally affect perfomance on slow WAN links.

9.1 Yönlendirme Tablosunun Incelenmesi

9.1.2 Alt Ag Geçidinin Son Kaldigi Yerin Belirlenmesi

Bir router için tüm muhtemel istasyonlara yollari sürdürmek (devam ettirmek) olanakli olmamakla birlikte arzu edilecek bir durumda degildir. Bunun yerine routerler kullanilmayan bir yolu veya son kalinan yerin girisini bulundurlar. Kullanilmayan yollar ,router, tablodaki daha spesifik bir giris ile ag istasyonunu esleyemedigi durumlarda kullanilir. Router bu kullanilmayan yolu son kalinan yerin girisine erismek için kullanir.



Ölçeklenebilir özelligi kullanilmayan yollarin, yönlendirme tablolarini olabildigince zayif tutmasidir. Bunlar routerler için, tüm internet aginda tablo bulundurma zorunlulugu olmadan, herhangi bir internet sunucusuna belirlenmis paketleri yollamayi olanakli kilmaktadir. Bu yollara, bir yönetici tarafindan statik olarak girilebilir veya yönlendirme protokolü kullanilarak dinamik olarak ögrenilebilir.

Yönlendirmenin yöneticiyle basladigi varsayilir. Routerlar bilgi alisverisinde bulunmadan önce yönetici varsayilan bir yolla bir router i konfigüre etmek zorundadir. Elde edilmek istenen sonuçlara göre, yönetici varsayilan yolu statik olarak konfigüre etmek için asagidaki iki komuttan birini kullanabilir.

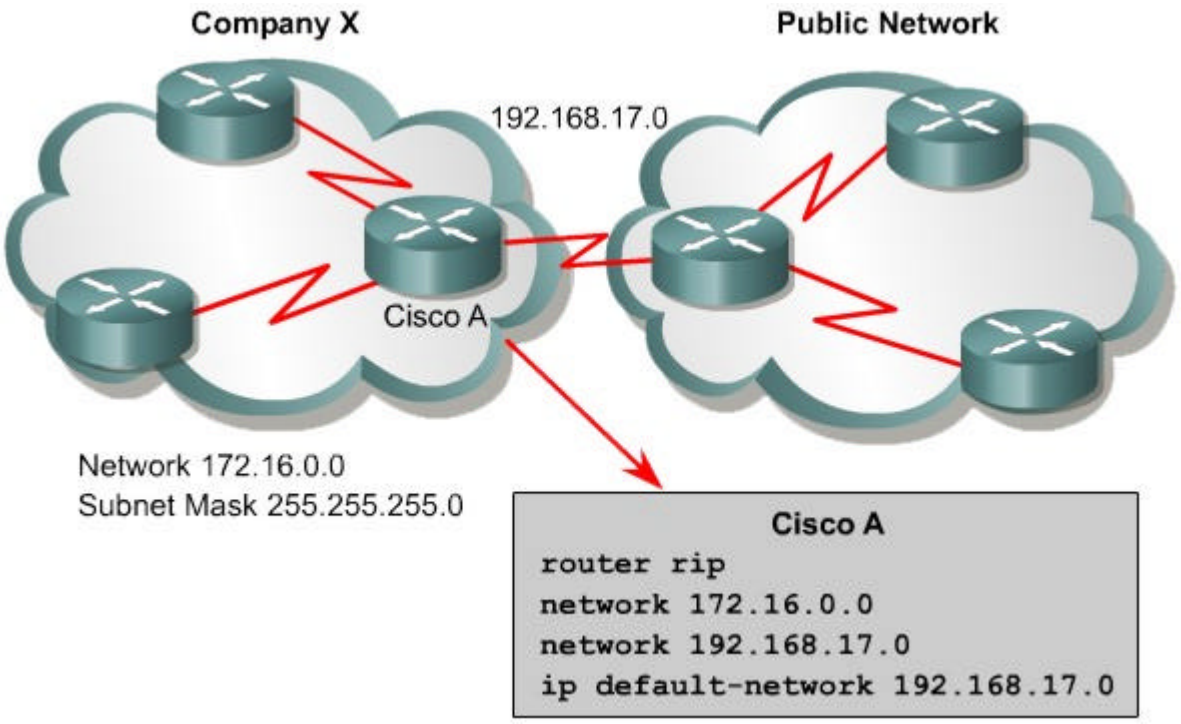
Command
`Router(config)#ip default-network [network number]`

ip default-network
yada
ip route 0.0.0.0 0.0.0.0

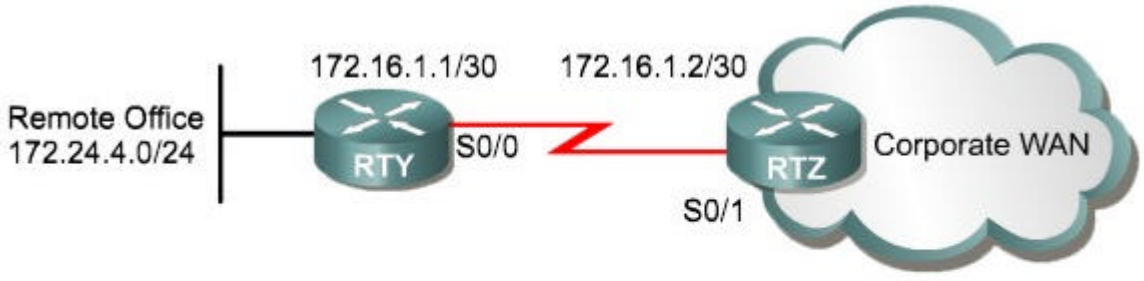
ip default-network komutu dinamik yönlendirme protokolleri kullanarak ag da varsayilan yolu kurabilir.

ip default network Command	Description
`network-number`	The candidate default IP network or subnetwork number.

ip default-network 192.168.17.0 genel komutu C sinifi aglarda tanimlanmistir. 192.168.17.0 yi , yönlendirme tablosu girisleri olamayan paketler için hedef yol belirler. **ip default-network** ile kurulmus aglar için; eger bir router aga giden bir yola sahipse, o yolun varsayilan bir yol olma adayligi zayiflar.



Bir 0.0.0.0/0' a **ip route** olusturmak yeni bir yol kurmanin baska bir yöntemidir




```
RTY(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2
```

Router(config)#**ip route 0.0.0.0 0.0.0.0 [next-hop-ip-address | exit-interface]**

Yeni bir yol veya ag olusturduktan sonra **show ip route** komutu asagidakileri gösterecektir.

Gateway of last resort is 172.16.1.2 to network 0.0.0.0

9.1 Yönlendirme Tablosunun Incelenmesi

9.1.3 Kaynak ve Hedef Yolun Tanimlanmasi

Bir ag kümesindeki trafige girmek için, ag katmaninda ag tanimlamasi gerçeklesir. Yol tayini islemi, varis yeri için uygulanabilir yönlerin degerlendirilmesini ve tercih edilmis isleyen bir paketin kurulmasini mümkün kilar. Yönlendirme servisleri ag topoloji bilgilerini ag yollari belirlenecegi zaman kullanirlar. Bu bilgi ag yöneticisi tarafindan veya agdaki dinamik islemlerden toplanilabilir.

Ag katmani,birbirine bagli aglar arasindaki paket ulasimini bastan basa ve en iyi çabayi gösterir. Ag katmani, kaynak agdan varis agina paket gönderirken IP yönlendirme cetvelini kullanir. Router hangi yolun kullanilacagini belirledikten sonra, paketi bir arabirimden digerine veya paketin varacagi en iyi yolu gösteren porta yollar.

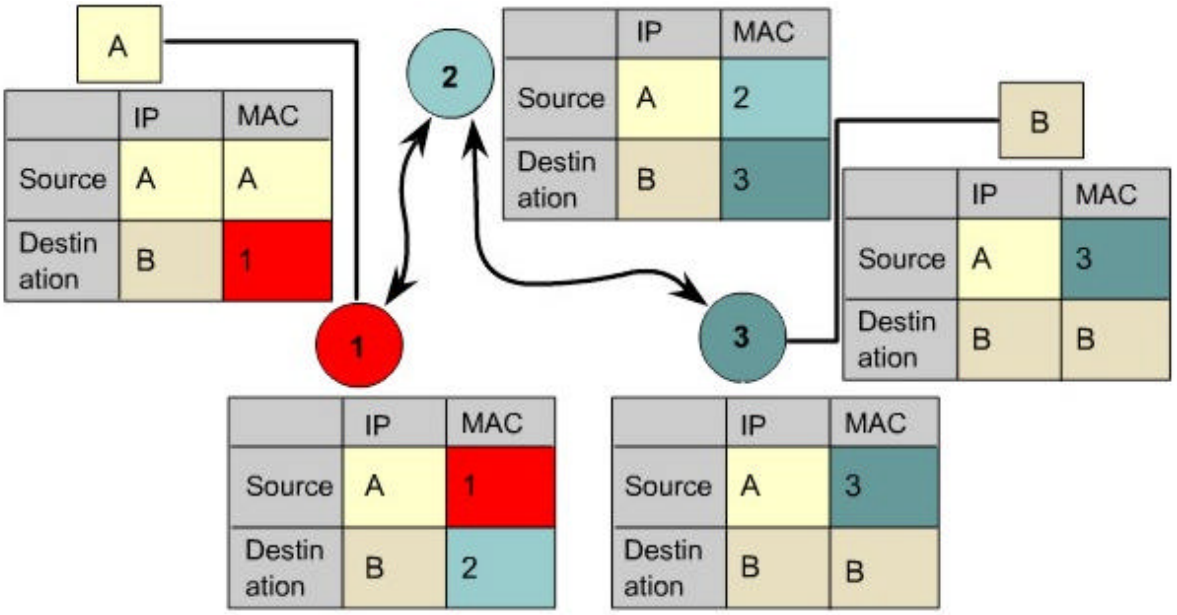
Ag tabakasi adresleri paketleri kaynaktan varis yerine götürmede kullanilirken anlasilmasi gereken önemli bir nokta bir routerden sonrakine paketleri tasimak için farkli bir adres çesidinin kullanilacagidir. Paket tasinim için 2. ve 3. katman adresleri kullanilir. Her arabirimde, paket ag boyunca hareket ettikçe, yönlendirme tablosu incelenir ve router bir sonraki adimi belirler. Sonra paket sonraki adimin MAC adresi kullanilarak iletilir. IP kaynagi ve varis yeri hiçbir zaman degismez.

3. Katman adresi paketi kaynaktan varisa yönlendirmede kullanilir. Kaynak ve hedef IP adresleri ayni kalir .MAC adresi her asamada veya routerde degisir. Veri iletim katmani adresi gereklidir. Çünkü ag içindeki iletim 2.katmandaki adres tarafindan belirlenir

9.1 Yönlendirme Tablosunun Incelenmesi

9.1.4 L2 ve L3 Adreslerinin Tanimlanmasi

Ag katmani adresleri kaynaktan hedefe paketlerin gönderilmesinde kullanilirlar. Bir routerdan digerine paket gönderiminde kullanilan farkli adres tipleri unutulmamalidir. Kaynaktan hedefe gidecek paket için 2.ve 3. katman adresleri ayni zamanda kullanilacaktir. Asagidaki sekilde her bir ara yüzdeki paketlerin agda nasil ilerleyecegi , yönlendirme tablosuna bakilir ve bir sonraki router tanimlanir. Paket MAC adreslerini kullanarak bir sonraki yere iletilir. Kaynak ve hedef IP basliklari degismez.



At each interface, as the packet moves across the network, the routing table is examined and the router determines the next hop. The packet is then forwarded using the MAC address of the next hop. The IP source and destination headers do not change, at any time.

3. katman adresleri kaynak agdan hedef aga paketlerin yönlendirilmesinde kullanilir. Kaynak ve hedef IP adresleri ayni kalirlar. MAC adresleri her atlamada yada router da degisirler. Veri iletim katman adresleri gereklidir. Çünkü adreste 2.katmanin basligi tanimlidir. 3. katman paket basligi degildir.

9.1 Yönlendirme Tablosunun Incelenmesi

9.1.5 Yönetimsel Uzaklik Yolunu Tanimlama

Bir router dinamik yönlendirme protokollerini kullanarak yolu kesfeder yada routerlar yönetici tarafindan el ile girilerek konfigüre edilirler. Yollari kullanarak yeni yollar kesfedebilirler. Yollar kesfedildikten veya kurulduktan sonra router verilen aglar için en iyi olan yollari seçer.

Yönetimsel uzaklik mesafesi routerin özel varis yerine olan en iyi rotayi belirlemesi için anahtar bilgidir. Yönetimsel uzaklik , yol bilgisinin kaynaginin güvenilirligini ölçen bir numaradir. Mesafe azaldikça kaynagin güvenilirligi artar.

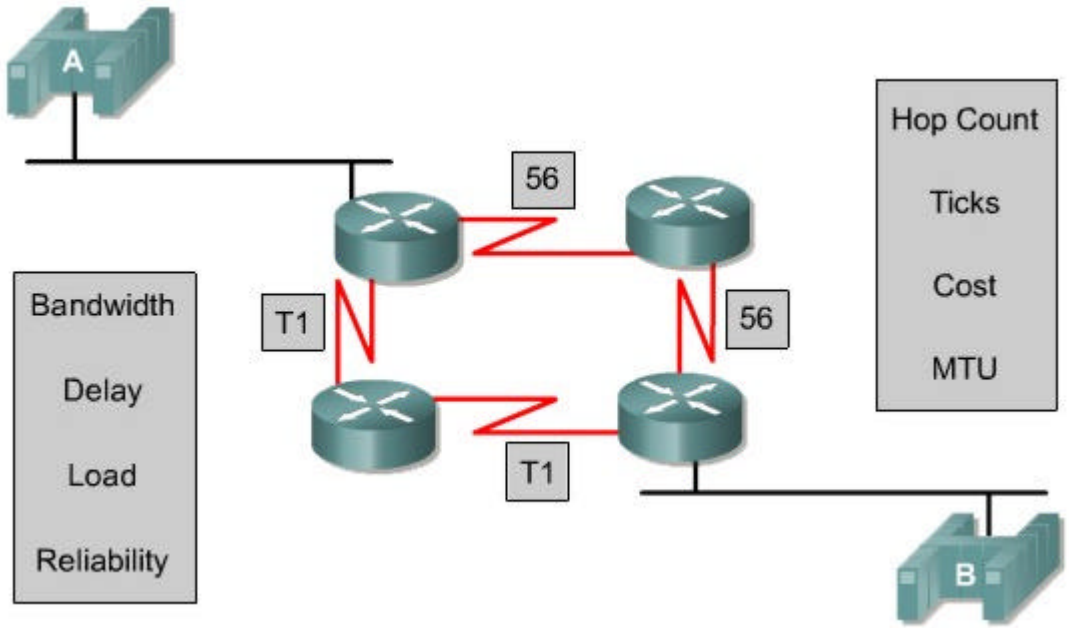
Farkli yönlendirme protokolleri farkli yönetimsel mesafelere sahiptir. Eger bir yol en düsük mesafeye sahipse yol yönlendirme tablosunda kurulmus vaziyettedir. Eger bir diger kaynaktan olan mesafe daha düsük ise yol cetvelde kurulu degildir.

Protocols	Default Administrative Distances
Connected	0
Static	1
EIGRP summary route	5
eBGP	20
EIGRP (Internal)	90
IGRP	100
OSPF	110
IS	115
RIP	120
EIGRP (External)	170
iBGP (external)	200

9.1 Yönlendirme Tablosunun Incelenmesi

9.1.6 Metrik Yol Tanimlamasi

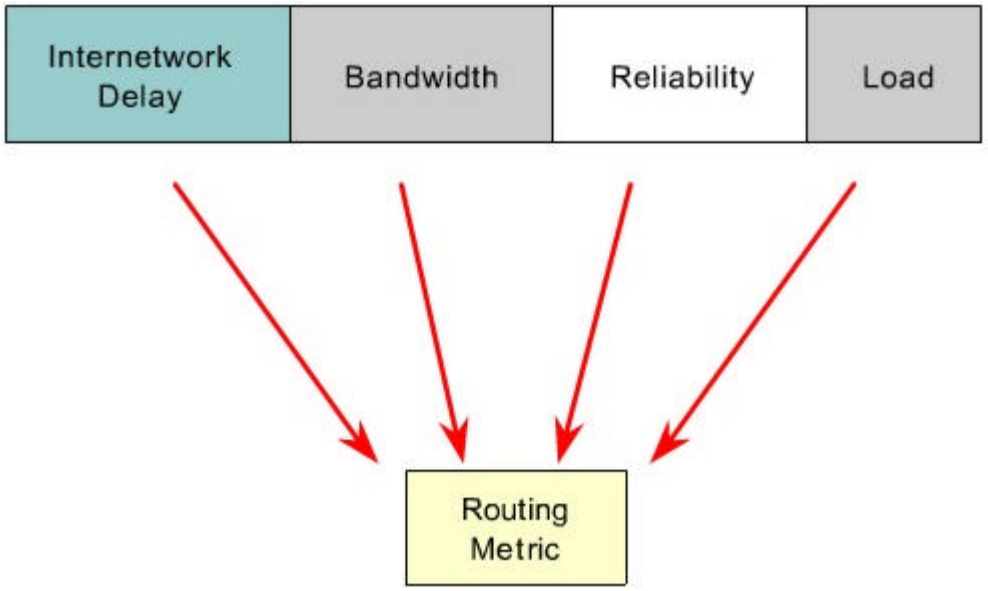
Yönlendirme protokolleri varisa olan en iyi yolu belirlemek için metrikleri kullanirlar. Metrik , yola ulasilabilirligi ölçen bir degerdir. Bazi protokoller metrigi hesaplamada yalnizca bir etkeni kullanirlar. Örnegin RIP versiyon 1 , sekme sayma yolunu metrigini hesaplamada tek etken olarak kullanir. Diger protokoller metriklerini temellendirirken, bandgenisligi, gecikme , yükleme , güvenilirlik , saniye gecikmesi ,maksimum iletim ünitesi (MTU) ve fiyati baz alirlar.



Her yönlendirme algoritmasi kendi içinde en iyi yolun hangisi oldugunu anlatir. Algoritma agdaki her bir yol için metrik degerde denen bir numara olusturur. Genelde metrik numara küçüldükçe yol iyilesir.

Bandgenisligi ve gecikme gibi faktörler statiktir. Çünkü her bir router yeniden kurulana veya her bir ag yeniden dizayn edilene kadar ayni kalir. Yükleme ve güvenilirlik gibi faktörler dinamiktir. Her bir arabirim için router tarafindan o zaman da hesaplanir

Metric	Description
Hop Count	The number of routers that must be traversed to reach a destination. The path with the lowest hop count is preferred.
Bandwidth	The link speed. The path with the greatest bandwidth is preferred.
Delay	The amount of time it takes for a packet to travel a link. The path with the least delay is preferred.
Load	The amount of activity on a link. On Cisco routers, the value can typically range anywhere between 1 and 255, where 1 represents a link with the less load, and 255 a link with the most load. Paths with the smallest load are preferred.
Reliability	The error rate on a link. On Cisco routers, the value can typically range anywhere between 1 and 255, with 255 representing a link with the highest reliability. Paths with the greatest reliability are preferred.



Metrigi olusturan faktörler arttikça ag islemlerinin spesifik ihtiyaçlari karsilamaktaki esnekligi artar. Bunun yaninda IGRP metrik deger hesabinda bandgenisligi ve gecikme gibi statik faktörleri kullanir. Bu iki faktör el ile kurulabilir ve routerin hangi yollari seçtigi üzerinde tam bir kontrole izin verir. IGRP dinamik faktörleri (güvenlik ve yükleme) içermesi için metrik hesaplamada kurulabilir. Dinamik faktörleri kullanarak IGRP routerleri yaygin kosullara bagli olarak kararlar alabilir. Bir baglanti çok yüklü hale gelirse veya güvenilir olmaktan çikarsa, IGRP o baglantiyi kullanarak yollarin metrigini arttirir. Degiserek olusan yollar derecesi indirilmis yoldan daha az metrik sunabilir ve bunun yerine kullanilabilirdi.

IGRP, aga olan baglantinin farkli karakterlerinin avantajli degerlerini sorgulayip toplayarak metrigi hesaplar. Takip eden örnekte oldugu gibi ;bandgenisligi, bunu bölen yükleme, ve gecikme degerleri K1 K2 ve K3 sabit katsayilari ile agirlastirilir.

Metric=K1 *Bandgenisligi + (K2 * Bandgenisligi)/256-load) + K3 * gecikme

varsayilan sabit degerleri K1=K3=1 and K2=K4=K5=0 olunca:

Metrik=Bandgenisligi + gecikme

9.1 Yönlendirme Tablosunun Incelenmesi

9.1.7 Sonraki Atlama Yolunun Tanimlanmasi

Yönlendirme algoritmalari yönlendirme tablolarini çesitli bilgilerle doldururlar. Varis yeri/sonraki adim bileskesi, router a belli bir varis yerine, özel bir routere paket göndererek ulasilabilecegini söyler. Bu router son hedefe giden yol üzerindeki bir sonraki adimi temsil eder.

Router gelen bir paketi aldigi zaman varis adresini kontrol eder ve bu adresi sonraki sekmeyle birlestirmeye çalisir.

9.1 Yönlendirme Tablosunun Incelenmesi

9.1.8 Son Yönlendirme Güncellemesinin Incelenmesi

Asgidaki komutlar son yönlendirme güncellemesini bulmak için kullanilir:

- **show ip route** 1
- **show ip route** *network* 1
- **show ip protocols** 2
- **show ip rip database**

9.1 Yönlendirme Tablosunun Incelenmesi

9.1.9 Varis Yerine Olan Çesitli Yollari incelemek

Bazi yönlendirme protokolleri ayni hedefe giden çesitli yollari destekler. Tekil yol algoritmalardan farkli olarak bu çogul-yol algoritmalari çoklu hatlardaki iletime izin verir ve daha güvenilirdirler. Örnegin Rt1 192.168.30.0 agina giden iki yola sahiptir.192.168.30.0 agina olan her iki yolunda kullanimini garantiye almak için karsit komut Rt1 de olusturulur.

show ip route komutunun çiktisini karsiti olusturulmadan evvel Rt1 tarafindan gösterir. Serial 0/0 192.168.30.0.' a olan tek yoldur.

show ip route komutunun çiktisini karsiti olusturulduktan sonra gösterir.

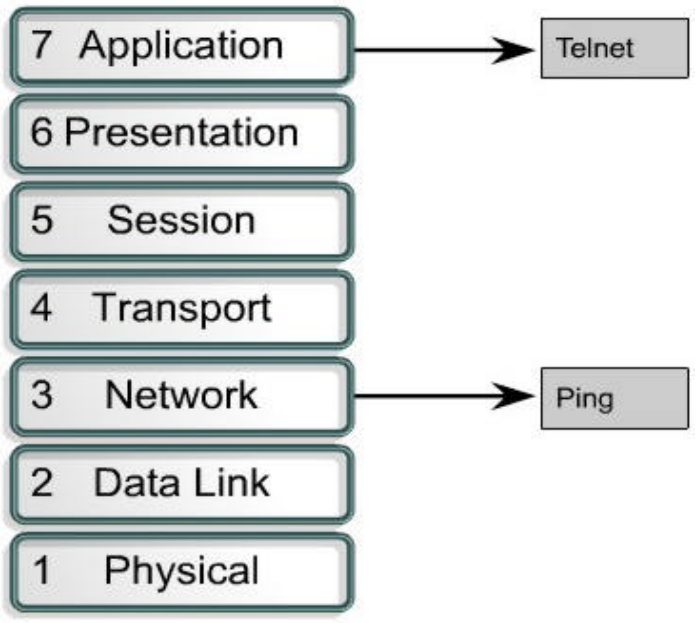
Tercih edilen arabirim hizli eternet 0/0 dir fakat Serial 0/0 da kullanilabilir.yükleme dengesini dogrulamak için **ping** 192.168.30.1

9.2 AG Testi

9.2.1 Ag Testine Giris

Bir agin temel testi , OSI referans model asamasindan bir sonrakine ardil olarak ilerlemelidir. 1. Katman ile baslayip gerektiginde 7. Katmana dogru çalismak en iyisidir. Katman 1 ile baslamak duvardaki güç kablolari gibi basit problemleri arastirir. IP sebekesinde olusan ortak problemlerin birçogu adreslendirme planindaki hatalardan kaynaklanir. Bu yüzden daha fazla konfigürasyon asamalari kaydetmeden adres kurulumunu kontrol etmek önemlidir

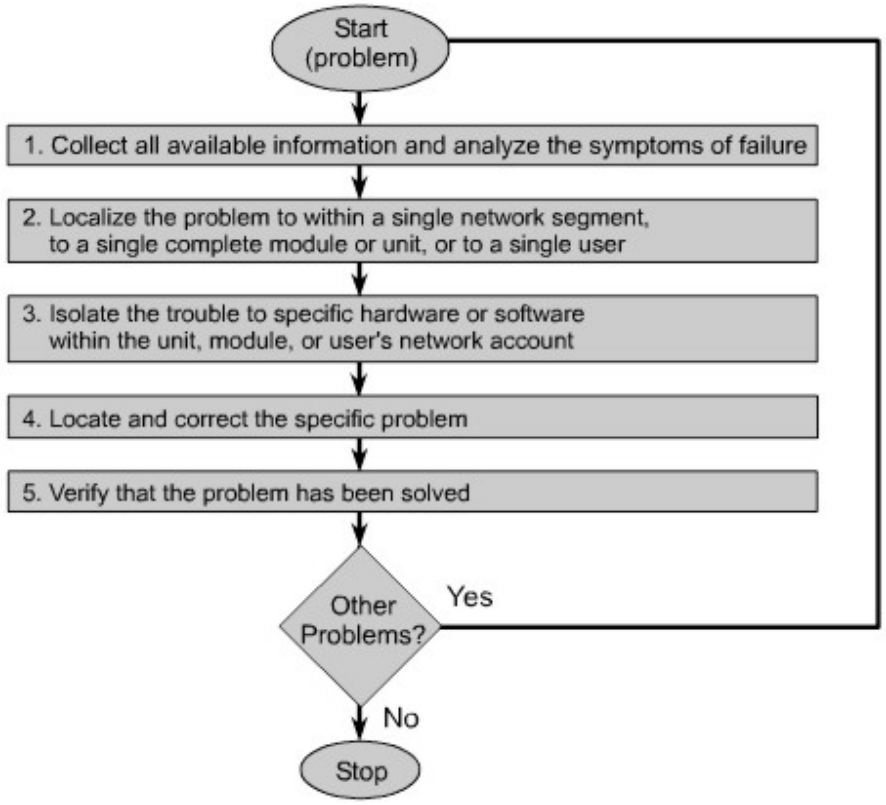
Bu kisimda sunulan her test OSI modelinin özel kademesindeki sebeke islemlerinde yogunlasir. **Telnet** ve **ping** sebeke testi için gerekli iki önemli komuttur.



9.2 AG Testi

9.2.2 Yapisal Yaklasim Kullanarak Sorunlarin Giderilmesi

Hata giderimi kullaniciya sebekedeki problemleri bulmaya olanak taniyan bir islemdir. Yönetim tarafindan gelistirilmis isletim sistemi standartlarina dayali düzenli bir sorun çözme islemi olmalidir. Dokümantasyon hata giderimi isleminin önemli bir bölümüdür.



Bu modeldeki asamalar sunlardir:

1. Bütün uygun bilgileri toplamak ve hatanin bulgularini analiz etmek
2. Tekil sebeke veya tekil tam modül veya ünite içinde problemin yerini belirle
3. Problemi ünite içindeki yazilim veya spesifik donanimdan,modülden veya kullanici ag hesabindan izole etmek
4. Sorunu belirleyip , düzeltmek
5. Problemin çözüldügünü dogrulamak

Hata giderimi için baska bir yöntem gösterir. Bu konseptler hata giderimi için tek yol degildirler. Bununla beraber agin kolay ve sorunsuz çalismasi için en önemli sey düzenli bir islem sürecidir.

Hata düzeltimi için kalipsal bir yol kullanmak, sebeke destek takiminin her üyesi, takimin bütün üyelerinin problemi çözmek için hangi adimlari tamamladigini bilir. Çesitli hata giderimi fikirleri, organize veya belgelendirme olmadan problem çözümünde etkili degildir.

Eger problem kalipsal olmayan bir yolla çözülürse gelecekti. Benzer problemler için o çözümün uygulanmasi imkansiz hale gelir.

9.2 AG Tesri

9.2.3 OSI Katmanlari Tarafindan Test

Test OSI modelinin 1.Katmanindan 7.Katmanina dogru olmalidir.

Katman 1 hatalari sunlardir:

- Kirik kablolar
- Bagli olmayan kablolar
- Yanlis porta baglanmis kablolar
- Gidip gelen(aralikli)kablo baglantisi
- Eldeki is için yanlis is kullanimi
- Alici problemleri
- DCE kablo problemleri
- DTE kablo problemleri

Katman 2 hatalari sunlardir:

- Yanlis kurulmus ethernet arabirimleri
- Yanlis kurulmus seri arabirimler
- Yanlis kapsülleme islemi
- Seri arabirimde uygun olmayan zaman ayarlari
- (NIC) Ag arabirim Kart problemleri
-

Katman 3 hatalari sunlardir:

- Yönlendirme protokolü kullanimda olmaz
- Yanlis yönlendirme protokolü aktiftir
- Yanlis IP adresleri
- Yanlis alt ag maskeleri

Eger agda hatalar görülürse, OSI asamalarindaki test etme islemi baslamalidir. Ping komutu baglantiyi kontrol etmek için 3. katmanda kullanilir. 7.kanmandaki telnet komutu kaynak ve varis istasyonlari arasindaki uygulama asamasini dogrulamak için kullanilir. Bu iki komut ilerleyen bölümde detayli olarak incelenecektir.

9.2 AG Testi

9.2.4 1. Katman Göstergelerini Kullanarak Sorun Giderme

Gösterge isiklari hata giderimi için kullanilir. Çogu arabirim yada NIC ler geçerli bir baglanti olup olmadigini gösteren gösterge isiklara sahiptir. Bunlara baglanti isigida denir. Arabirim trafigin iletildigini veya alindigini gösteren isiklara sahiptir. Eger arabirim gösterge isigi geçerli olmayan bir baglantiyi gösteriyor ise aygiti kapatip ve arabirim kartini yeniden yerlestirin. Kablo dogru olmayan bir biçimde baglanirsa, baglanti isigi, kötü baglanti yada baglanti yok sinyali verebilir.

Emin olmak için tüm kablolarin uygun porta bagli olup olmadigini kontrol edin. Uygun metot ve kablolar kullanilarak çapraz baglantilarin dogru yerlere yapildigindan emin olun.

Bütün anahtar veya merkez portlarin dogru VLAN içinde oldugunu veya ayri bir alanda oldugunu, ve ayirma agaci ve diger elemanlar için dogru seçenekleri tatbik edin. Uygun kablonun kullanildigini dogrulayin. Merkez ve anahtar arasinda veya bilgisayar gibi sunucular ve routerler arasindaki baglantilar için crossover kablo kullanimi gerekebilir.

Kaynak arabirimden gelen kablonun iyi kosullarda oldugundan ve dogru baglandigindan emin olun. Baglantinin iyi oldugu konusunda süphe varsa kabloyu yeniden takip baglantinin güvenligini garantiye alin. Kabloyu çalisan diger bir kabloyla degistirmeyi deneyin. Eger bu kablo duvara montajli ise kablo test aleti kullanarak kontrol edin.

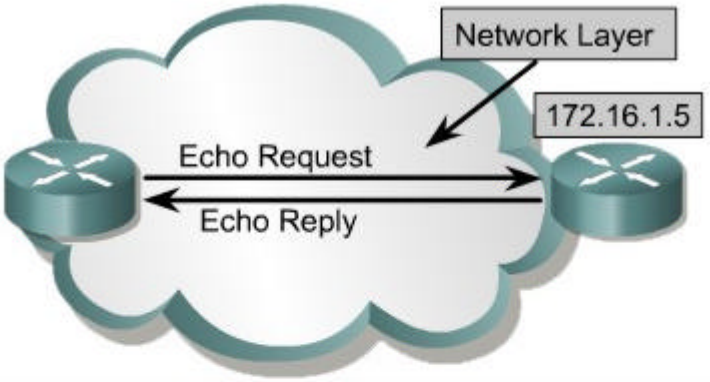
Kullanimda olan alici verici tipin, kurulumun, ve baglantinin dogrulugunu garanti etmek için kontrol edin. Kablolari degistirmek sorunu çözmezse ve eger kullaniliyor ise alici vericiyi degistirin.

Aygitin açik oldugundan emin olmak için her zaman kontrol edin. Hata teshisi ve giderilmesinden önce her zaman temel seyleri kontrol edin.

9.2 AG Testi

9.2.5 3.Katmanda Ping Kullanarak Sorunlarin Giderilmesi

Ping komutunun yarari Ag baglantilarini test ederken ortaya çikar. Yardim olarak ,temel ag baglantisini tespit etmek için birçok ag protokolü yanki protokolünü destekler. Yanki protokolleri dagitilmakta olan protokol paketlerinin test edilmesinde kullanilirlar. Ping komutu varis yeri sunucusuna bir paket gönderir ve cevap bekler. Buna bagli olarak; yanki protokolü sunucuya olan yolun degerlendirmesini yapabilir. Yolu ve ulasilabilirse veya kullanimdaysa sunucuyu erteleyebilir. Ping çiktisi , bir ping paketinin özgün bir sistem bulup geri dönmek için minimum ortalama veya maksimum zaman aldigini gösterir. Ping komutu donanim baglantisini ve sebeke adreslerinin uygunlugunu dogrulamak için ICMP kullanir. (Internet Control Message Protocol) . Sekil çesitli ICMP mesaj tiplerini içeren bir çizelgedir. Bu ag baglantisi için bayagi temel bir test mekanizmasidir. Örnekte ping hedefi 172.16.1.5 gönderilmis bes datagramin hepsini basariyla karsilar. Ünlem isareti (!) her basarili yankiya isarettir.




```
Router>ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent,
round-trip min/avg/max = 1/3/4 ms
Router>
```

Komut	**Amaçlar**
Router#**ping** [protokol] {sunucu|adres}	Baglanti testi için tespitsel bir araca basvurmak

Ping komutu ag baglantilarini test için hedef bir sunucuya ICMP yanki teklifinde bulunur ve bunu zamanla tekrarlar. Ping gönderilmis ve alinmis paket numaralarini ve kayip paketlerin yüzdelik oranini izler. Ayni zamanda paketlerin varisi ve gönderilmis olanlarin alinisi için gecen zaman miktarinda izler. Bu bilgi çalisma istasyonlari ve diger sunucular arasindaki baglantinin onayina ve bilginin kaybolup olmadigina iliskin bilgiyi içerir.

Ping komutuna kullanici ve yönetici modundan ulasilabilir. Ping komutu APPLE talk üzerinden temel ag baglantisinin onayinda kullanilir. Gelismis ping komutu kullanimi, routeri daha fazla test opsiyonu uygulamaya yönlendirir. Bunun için “ping” yazin ve ip adresi girmeden enter tusuna basin enter tusuna her basildiginda promptlar belirecektir. Agda hata giderimi oldugunda, ona karsi karsilastirma olsun diye, komutun normal sartlar altinda nasil çalistigini görmek için ag devredeyken ping komutunu kullanmak iyi bir fikirdir.

9.2 AG Testi

9.2.6 7.Katmanda Telnet Kullanarak Sorunlarin Giderilmesi

Telnet araçlari TCP/IP protokol takiminin parçasi olan sanal bir terminal protokolüdür. Kaynak ve hedef yerler arasindaki uygulama katmani yaziliminin dogrulugunu ispat etmeye olanak tanir. Bu mümkün olan en komplike test mekanizmasidir. Telnet normal olarak uzak aygitlara baglanti, bilgi toplamak ve programlari çalistirmak için kullanilir.

Telnet uygulamasi router larda TCP/IP yi çalistirirken baglanti için sanal bir terminal olusturur. Hata giderimi amaçlari için bir baglantinin telnet kullanilarak yapilabilecegini söylemek yerindedir. Bu en az bir TCP/IP uygulamasinin bastan sona baglanabilecegini gösterir. Telnet baglantisi üst kademe uygulamasi ve alt kademe servislerinin düzgün isledigini gösterir.

Eger bir yönetici router lardan birine telnet yapip digerine yapmiyor ise alt kademe baglantisini sorgulayin. Sorgulanip hata çikmadiysa sorun muhtemelen özel adreslemeden isimlemeden veya giris izni probleminden kaynaklanir. Bu problemler yöneticinin veya telnetin hedef routerinda ortaya çikabilir.

Eger telnet bir sunucudan belirli bir sunucuya basarisiz olursa router dan veya diger bazi aygitlardan deneyin.**Telneti denerken giris basarilamadiysa sunlari deneyin:**

- Birçok telnet servisleri DNS girisi olamayan ip adreslerinden olan baglantiya izin vermeyecektir. Yöneticinin DHCP havuzlarina DNS eklememesi, DHCP adresleri için genel bir problemdir.
- Telnet uygulamasi uygun seçenekleri tartismayabilir ve bu yüzden baglanamaz.Cisco routeri üzerinde bu sorgulama "**debug telnet**" komutuyla görülebilir.
- Telnet kapali olabilir veya hedef sunucudaki 23. porttan hariç bir porta yönlenmis olabilir

9.3 Router Sorunlarinin Giderilmesine Genel Bakis

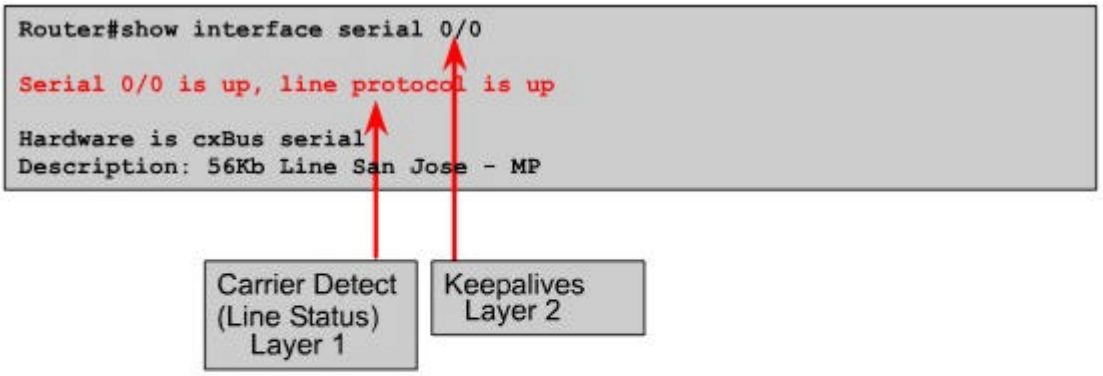
9.3.1 1.Katmandaki "show interfaces" Komutunu Kullanarak Sorun Giderme

Cisco IOS hata giderimi için zengin bir komutlar kümesi içerir. Bunlar içinde daha çok kullanilanlari **show** komutlaridir. Routerdaki tüm olaylar **show** komutlarinin bir veya fazlasi kullanilarak görülebilir. Arabirimlerin konum ve istatistiklerini kontrol etmekte kullanilan gösterge komutu "**show interfaces**" komutudur. Bu komutun degisik farkli tipleri arabirimlerin konumunu kontrolde kullanilir. Hizli ethernet arabirimlerini görüntülemek için "**show interfaces FastEthernet**" komutunu kullanin. Bu komut ayni zaman da özel bir arabirimin konumunu görmek içinde kullanilir. Serial 0/0 konumunu görmek için **show interfaces serial 0/0** komutunu kullaniniz.

Arabirimlerin iki önemli kismi **show interfaces** komutuyla gösterilebilir. Bu kisimlar fiziksel (donanim) kisim ve mantiksal (yazilim) kismidir. Bunlar 1.Katman ve 2.Katman fonksiyonlariyla ilgilidirler.

Donanim aygitlari arasindaki fiziki baglantinin durumunu gösteren kablolar , konnektörler ve arabirimleri içerir. Yazilim durumu kontrol ve kullanici bilgileri gibi yakin aygitlar arasinda geçen mesajlari gösterir. Bu , bagli iki router arasinda geçen asamaya iliskindir.

Show interfaces serial komutunun bu önemli elemanlari, hat olarak ve veri-baglanti protokolü olarak görülür.



Serial 0/0 is up, line protocol is up	Operational.
Serial 0/0 is up, line protocol is down	Connection Problem
Serial 0/0 is down, line protocol is down	Interface Problem
Serial 0/0 is administratively down, line protocol is down	Disabled

Birinci parametre yazilim asamasina yöneliktir ve arabirimin baglantinin diger basindan Tasiyici Algilayici (CD) sinyali alip almadigini özellikle gösterir. Hat düsmüs ise kablolamayla ilgili problem olabilir. Devrede bir yerde aygit çalismiyor olabilir veya yanlis çalisiyor olabilir veya bir taraf yönetimsel olarak düsmüs olabilir. Eger arabirim yönetimsel olarak düsmüs ise kurulumda el ile ayarlanarak saf disi birakilmistir.

show interfaces serial komutu , pek te kolay olmayan diger 1.Katman sorunlarini teshis için bilgi saglar. Seri baglantida artan sayida görülen hatali geçis su sorunlara neden olabilir:

- Hat kesintileri servis saglayici sebeke içinde problemlere neden olabilir.
- Kusurlu anahtarlama , DSU veya router yazilimi

.

Eger **show interfaces serial** komutu çikisinda artan sayida girdi hatalari olursa bu problemlerin bazi nedenleri vardir.

Bunlardan bazilari 1.Katman problemlerine iliskindir:

- Hatali telefon sirketi araçlari
- Gürültülü (yogun) seri hat
- Yanlis kablo veya kablo uzunlugu
- Hasarli kablo veya baglanti
- Hatali CSU veya DSU
- Hatali router donanimi

Incelenecek diger bir alanda arayüzlerin yeniden baslatilmasinin sayisindaki artistir. Asagidaki 1.Katman problemleri arabirimin resetlenmesi sonucu olusabilir:

- Kötü hat sorunlu geçise neden olur.
- CSU,DSU veya anahtardaki muhtemel donanim problemi

Eger tasiyici geçisleri ve arabirim resetleri artiyorsa veya giris hatalari arabirim resetleri artarak yükseliyorsa problem kötü baglanti ya hatali CSU ya da DSU ya iliskin olabilir.

Hatalarin sayisi routerin yürüttügü trafigin yogunlugu ve istatistiklerin tutuldugu zamanin miktariyla açiklanmalidir. Router arabirim hakkinda bilgi saglayan istatistikleri izler. Istatistikler islemin basladigi veya numaratörlerin sifirlandigi en son zamandan itibaren router islemini yansitir.

Eger **show interfaces** komutu numaratörlerin en son ne zaman sifirlandigini göstermiyor ise routerin ne zamandir fonksiyonda oldugunu bulmak için "**show version**" komutunu kullanin

clear counters komutunu numaratörleri sifirlamak için kullanin. Bu sayicilar bir arabirimin sorunu giderildikten sonra daima sifirlanmalidir. Sifirdan baslamak , agin hali hazirdaki konumunun iyi bir resmini veriri ve meselenin gerçekten halledildigini gösterir.

9.3 Router Sorunlarinin Giderilmesine Genel Bakis

9.3.2 2.Katmanda show interfaces Komutu ile Sorunlarin Giderilmesi

show interfaces komutu routerin 1.Katman ve 2.Katman problemlerini bulmak için beklide en önemli araçtir. Birinci parametre (hat) fiziksel katmanla iliskindir. Ikinci parametre (protokol) hat protokolünü kontrol eden IOS islemlerinin arabirimi kullanilir yapip yapmadigini gösterir. Bu tasiyicilarin basariyla alinip alinmadigi yönünden belirlenir. Tasiyicilar bir ag aygitindan diger bir aygita, bu ikisi arasindaki sanal devrenin halen aktif oldugu yönünde bilgilendirmesi için gönderilen mesajlar olarak tanimlanir. Arabirim ardisik 3 tasiyiciyi kaçirirsa, hat protokolü düstü diye isaretlenir.

Hat düstügünde, protokol her zaman düser. Çünkü 2. Katman protokolü için kullanilir. Iletim araci kalmaz. Arabirim bir donanim problemine iliskin olarak düstügünde veya yönetimsel olarak düstügünde bu dogru olabilir.

Eger arabirim bagliyken hat protokolü düsük ise 2.Katmanda problem vardir ve muhtemel nedenleri sunlar olabilir:

- Tasiyicilar yoktur
- Zaman oraninin olmamasi
- Özetleme isinde yanlis esleme

show interfaces serial komutu degisiklikleri ve arabirimin islevsel oldugunu dogrulamak için bir seri arabirim kurulduktan sonra kullanilmalidir.

9.3 Router Sorunlarinin Giderilmesine Genel Bakis

9.3.3 show cdp Kullanarak Sorunlarin Giderilmesi

Cisco Kesif Protokolü (CDP) , dogrudan komsularina, MAC ve IP adreslerini içeren aygit bilgisini ilan eder.

show cdp neighbors komutu dogrudan bagli olan komsular hakkindaki bilgiyi görüntüler. Bu bilgi baglantiyla ilgili meseleler için kullanilmalidir. Eger kablolama probleminden süphe ediliyorsa **no shutdown** komutuyla arabirimi etkin kilin, sonra herhangi diger bir kurulumdan önce ”**show cdp neghbors detail**” komutunu yürütün.bu komut aktif arabirimler , ID portu ve aygit gibi özel detaylari görüntüler. Cisco IOS versiyonu da görülür.

Eger fiziksel tabaka düzgün çalisiyor ise o halde diger tüm dogrudan bagli Cisco aygitlari görüntülenmelidir. Eger bilinmeyen bir aygit belirirse 1.Katman problemini andirir.

CDP ile ilgili diger bir ilgi alani güvenliktir. CDP nin sagladigi bilgi okadar fazladir ki bu potansiyel bir güvenlik açigi olusturabilir. Güvenlik nedeniyle CDP yalnizca Cisco aygitlari arasindaki baglantilarda kurulmali ve kullanici portlarinda veya yerel olarak yönetilmeyen baglantilarda kapatilmalidir.

9.3 Router Sorunlarinin Giderilmesine Genel Bakis

9.3.4 Traceroute Kullanarak Sorunlarin Giderilmesi

Traceroute komutu paketler hedeflerine giderken izledigi yolu bulmak için kullanilir. Ayrica bu komut, asama asama temellendirilmis ag tabakasinin test edilmesine ve performans kistaslarinin bulunmasina da yardimci olur.

Traceroute komutunun çikisi , basarili bir sekilde tamamlanan , hedefine ulastirilan siçramalarinin genel bir listesini sunar. Data istenilen hedefe sorunsuz olarak ulastiginda ‘çikis’ datagram’in geçtigi her yolu gösterir. Bu çikis kaydedilebilir ve daha sonra internet aginda sorun çiktiginda kullanilabilir.

Traceroute komutu ayni zamanda sorunun oldugu noktayi tam olarak gösterir. Hattaki her yol için, terminalde verinin girdigi ara birimin IP adresini gösteren bir çikis listesi olusturulur. Yildiz (*) varsa paket basarisizdir. Traceroute çikisinin son basarili islemi bulunup, bunu ag çalisma ortaminin diyagramiyla karsilastirdigimizda sorunlu bölge ayrilabilir.

Traceroute, baglantilarin ortak performanslarini gösteren bilgiyi de içerir. Gidis dönüs zamani bir yanki paketi gönderdikten sonra cevabi gelinceye kadar geçen süredir. Bu baglantidaki gecikme hakkinda fikir verme açisindan faydali bir islemdir. Bu göstergeler figürler tam bir performans gelisimi için kaydedilebilir ve ileride ag çalisma ortaminda bir sorun çikarsa kullanilabilir.

```
Arab#traceroute 192.168.6.1

Type escape sequence to abort.
Trace the route to Eva (192.168.6.1)

1 Boaz (192.168.10.1)          72 msec  72 msec 88 msec
2 Centre (192.168.12.1)        80 msec 128 msec 80
3 Decatur (192.168.75.1)       540 msec 88 msec 84 msec
4 Eva (192.168.6.1)            96 msec     *    96 msec
```

Traceroute i alan aygitin ayni zamanda traceroute´in kaynagina nasil geri cevap gönderecegini bilmesi gerektigine dikkat edin. Traceroute'nin ya da ping datanin , yollar arasinda gel-git yapmasi için iki yöndeki yolunda bilinmesi gerek. Basarisiz bir cevap her zaman bir sorun oldugunu göstermez. Çünkü ICMP mesaji islemin yapildigi yerde sinirlandirilabilir veya filtre edilebilir. Bu özellikle internet için dogrudur.

Traceroute, router'dan geçersiz bir adrese Kullanici Datagram Protokolü dogrulama paketi dizisi yollar. Gönderilen ilk üç dogrulama paketi dizisi için, Time-to-Live, bir'e ayarlar. Bu datagram yoldaki ilk router'a gidis zamani ölçer. Bu router'da dogrulama paketinin tamamlandigini gösteren ICMP zaman sinirli mesajla yanit verir.

Simdi üç tane daha UDP mesaji yollanir, bu kez TTL, ikiye ayarlanir. Bu ikinci routerin ICMP Zaman Asim Mesaji (TEM) na dönmesini saglar. Bu islem paketler diger hedeflere varana kadar devam eder.

Bu dogrulama paketleri hedefteki geçersiz porta geçmeye çalistiklarindan, ICMP zaman sinirli mesajlar yerine ICMP porta ulasilamaz mesajlar gönderilir. Bu ulasilamaz portu gösterir ve islemi aksatan traceroute programini belli eder.

9.3 Router Sorunlarinin Giderilmesine Genel Bakis

9.3.5 Yönlendirme Sorunlarinin Giderilmesi

"**show ip protocols**" ve "**show ip route**" komutlari yönlendirme protokolü ve yönlendirme tablosunu hakkinda bilgi verir. Bu komutlarin çikislari yol gösterici protokol konfigürasyonunu dogrulamak için kullanilabilinir.

"**show ip route**" komutu, sorun giderici yönlendirme konularinda beklide en önemli komuttur. Bu komut IP yönlendirme tablosunu gösterir. "**show ip route**" komut çiktilari bilinen bütün aglarin ve alt aglarin girislerini gösterir.

Sayet belirli bir sebekeye ulasmada sorun yasanirsa "**show ip route** " komutu kullanilir.

"**show ip route** " beklenilen bilgiyi vermiyorsa, sorun büyük ihtimalle yol gösteren bilginin degis-tokus edilememesidir. Bu durumda yönlendirme protokolü konfigürasyonu hatasini bulmak için "**show ip protocols**" kullanin.

show ip protocols" komutu bütün router'daki IP yönlendirme bilgisi hakkindaki seyleri gösterir. Bu komut hangi protokoller düzenledigini , hangi aglar tanitildigini, hangi arabirimlerin güncelleme yolladigini ve bunlarin kaynaklarini dogrulamak için kullanilir. "**show ip protocols**" çiktisi zamanlayicilari, filtreleri, yol özetini, yolun yeniden dagilimini ve router'daki her yönlendirme protokolüyle alakali parametreleri gösterir. Bir fazla protokol düzenlendiginde, bunlar hakkindaki bilgiler ayri bir bölümde gösterilir.

"**show ip protocols**" çikisi, kötü router bilgisi gönderdigi düsünülen router'in tespiti dahil, birçok konunun belirlenmesini saglar. Beklenilen protokolleri, tanitilan aglari ve kullanimdaki komsulari dogrulamak için de kullanilabilir. Her sorun giderme isleminde oldugu gibi, bilgi olmazsa sorunu tespit çok zor olabilir.

9.3 Router Sorunlarinin Giderilmesine Genel Bakis

9.3.6 show controllers serial Komutu kullanarak Sorunlarin Giderilmesi

Router baglantilarinin tespitinin mümkün olmadigi zamanlarda, router'daki düzen ve sorun giderme uzaktan komutlarla yapilir. "**show controllers serial**" komutu kabloyu incelemeden onun türünü , tipini belirlemede kullanilabilinir.

show controllers serial komutunun çiktisiyla kontrolörün belirledigi türler tespit edilebilir. Bu da kablosuz , yanlis kabloyu yada bozuk kablolu arabirimleri bulamada faydalidir.

show controllers serial komutu, seri arabirimleri kontrol eden devreyi arastirir ve arabirimler hakkindaki bilgileri gösterir. Bu çikti kontrolör devresine göre degisir. Bir router'in için farkli devreler kullanilabilir.

Kontrolör çipine bakmaksizin "**show controllers serial** " çok sayida çikti üretir. Kablo türünden baska, bu çiktinin büyük bölümü çipin durumu hakkinda bilgi veren detaylari içerir. Devre hakkinda bilgi sahibi olmadan bu bir ise yaramaz.

9.3 Router Sorunlarinin Giderilmesine Genel Bakis

9.3.7 Hata Ayiklamaya Giris

"**Debug (hata gider)**" komutu protokol ve sistem sorunlarini ayirmada yardimci olur. "**Debug**" çalisir durumdaki bilgiyi ve olaylari gösterir. **show** komutlari yalnizca duragan bilgiyi gösterdiginden, router isleminin geçmisini gösterir. "**Debug**" daha ayrintili bilgi verir. Bunlar, arabirimlerdeki trafik, sebekedeki dügümlerce olusturulan hata mesajlari, protokole özel paketler ve diger faydali sorun çözme bilgileri olabilir. "**Debug**" komutunun kullanimdaki çiktisi normal router islerini kesintiye ugratabilecek yüksek islemler üreten bir performans araliginda gelir. Bundan ötürü "**Debug**" sakinilarak kullanilir. Birkaç nedene indirgenmis sorunlardan sonra ve özel yogun tespitinde "**Debug**" kullanin. "**Debug**" sorunlari gösterme degil, gidermede kullanilir.

UYARI: Router islemini kesebileceginden ötürü **debug all** komutu nadiren kullanilmali.

Düzeltirken router "**Debug**" çiktisini ve sistem mesajlarini konsola gönderir, sayet router'i incelemek için bir bir telnet sistemi kullaniliyorsa, "**debug**" çiktisi ve sistem çiktisi uzaktaki terminale yeniden yönlendirilebilinir. Bu "**terminal monitor**" komutuyla telnet bölümü araciligi ile yapilir. Telnet 'ten **debug** kullanirken ekstra tedbirler alinmalidir. "**Debug**" komutunun yol açtigi yogunlugu, artirici baska bir islem yapilmamali. Eger yapilirsa, telnet yogunluk ile olan bagi sonuna kadar kullanacak ve router bir yada daha çok kaynagi tüketecektir. Bunu engellemek için en iyi kural :"**Oturumun kuruldugu yerde hiçbir zaman "debug" kullanma!"**

Farkli "**debug**" komutlarinin çiktilari çesitlilik gösterir. Bazilari her birkaç dakika bir yolda iki bag üretirken, bazilari da birçok üretebilir.

"**Debug**" çiktisinin kullanisliligini saglayan, baska bir IOS software serisini de **"timestamps**" komutudur.

Bu komut bir "**debug**" mesajinin üzerine "**timestamp**" koyar. Bu, **debug**'in oldugu zamani, islemler arasinda geçen zamani gösterir. Bir sonraki komut çiktinin saati, dakikasi ve saniyesini, router'in en son güçlendirilmesinden bu yana geçen zamanin ve yeniden yükle komutunun ne zaman uygulandigini gösteren bir "**timestamp**" düzenler.

GAD(config)#**service timestamps debug uptime**

"**no debug all**" komutu bulunmus tüm çiktilari kapatir. Belli bir "**debug**" komutunu etkisiz hale getirebilmek için, komutun basina "**no**" ekleyin. Örnegin; RIP' i "**debug**" komutu kullanarak "**debug ip rip**" seklinde yaptiysak, bu isle "**no debug ip rip**" ile sonlandirilir. Su anda "**debug**" komutu kullanilarak neyin arastirildigini görmek için "**show debugging**" kullanin.

ÖZET

Asagidaki anahtar noktalar anlasilmalidir:

- **show ip route** komutu.
- Son alt ag geçidi girisinin belirlenmesi.
- Yönlendirme kaynaginin ve adresin belirlenmesi
- Yönlendirme mesafenin belirlemesi
- Yönlendirme metrigin belirlemesi
- Bir sonraki yönlendirmenin belirlenmesi.
- Son yönlendirme güncellemesinin belirlenmesi.
- Hedefe giden diger yollari gözlemleme.
- Sorun çözmede yapici bir yöntem izleme.
- OSI katmanlariyla test.
- Göstergeleri kullanarak 1.Katmandaki sorun giderimi.
- Ping'i kullanarak 3. Katmandaki sorun giderimi.
- Telnet'i kullanarak 7.Katmandaki sorun giderimi.
- "**show interfaces**" i kullanarak 1.Katman sorunlarinin giderilmesi
- "**show interfaces**" i kullanarak 2.Katman sorunlarinin giderilmesi
- "**CDP**'yi göster"i kullanarak sorun giderme.
- **traceroute** kullanarak sorun giderme.
- **show ip route show ip protocols**'i kullanarak sorun giderme.
- **show controllers serial** i kullanarak sorun giderme.
- **Debug** komutunu kullanarak sorun giderme.

BÖLÜM - 10

Genel Bakis

Routerlar , IP paket basliklarinda tanimli Internet Protokolü (IP) adres bilgilerini kullanirlar. Arayüz paketlerinin hedefe ulastirilmasinda anahtardirlar. Çünkü hiçbir servise yardim amaçli paketin karsiya kesin ulastigina dair bilgi saglamaz. Güvenilmez olarak tanimlanabilir. Teslimde eni iyi çabayi gösterirler. Eger ip paketleri yolda düstüyse yanlis bir sira ile ulasirlar. Yada hizli bir sekilde iletimden sonra çeviri islemi yapilirken IP tek basina problemleri düzeltemez. Problem adreslerdedir. IP , Iletim Kontrol Protokolü (TCP) üzerine kurulmustur. Bu bölümde TCP ve fonksiyonlari ve UDP tanimlamasi ile 4.Katman protokollerinin diger önemleri tanimlanacaktir.

OSI ag olusturma modelindeki her katman çesitli fonksiyonlara sahiptir. Bu fonksiyonlar diger katmanlardan bagimsizdir. Her katman altindaki katmanin servislerini çevirebilme yetenegine sahiptir. Uygulama , sunum ve oturum katmanlari OSI modelinin içerisindedir. TCP/IP modeli uygulama katmaninda tüm dikkatleri üzerine toplamistir. Bu bölümde portlarin genel kavramlari tanitilip veri agi olusumunda port numaralarinin ve portlarin kritik özellikleri açiklanacaktir.

Bu modülü tamamlayan kimseler sunlari yapabiliyor olmalilar :

- TCP ve fonksiyonlarini tanimlamak
- TCP senkronizasyonu ve akis kontrolünü tanimlamak
- UDP operasyonlarini ve islemlerini tanimlamak
- Port numaralarinin isimlendirilmesi
- Sunucular arasindaki çoklu diyalogun tanimlanmasi
- Servisler ve istemciler için kullanilan portlarin tanimlanmasi
- MAC adres, IP adres ve port numaralari arasindaki iliski ve farkliliklarin anlasilmasi

10.1 TCP Isletimi

10.1.1 TCP Isletimi

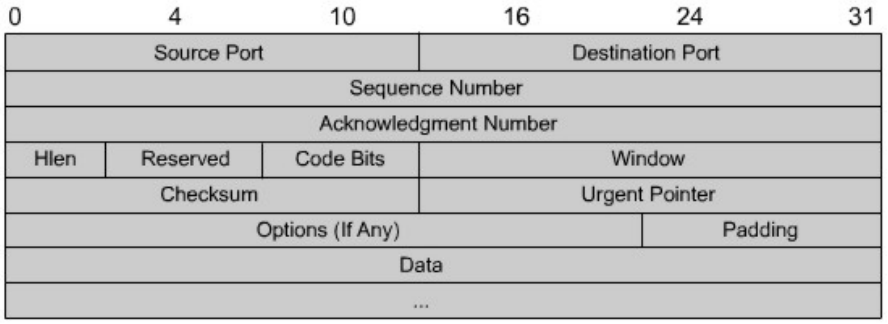
IP adresleri aglar arasinda paketlerin yönlendirilmesi için izin verirler. Halbuki IP` nin teslimiyet guvencesi yotur. Tasima katmani kaynaktan hedefe veri akisinin güvenli bir sekilde tasinmasi düzenlenmesinden sorumludur. Bu , senkronizasyon islemi ile ardarda numaralari siralayarak pencereleri kaydirmayi kullanarak sonuçlandirir.

Guvenilirligi saglamak ve akis kontrolünü anlamak için bir yillik yabani dil egitimi yapan ögrenciyi dikkate alalim. Simdi ögrencinin o dilin kullanildigi ülkeyi ziyaret ettigini düsünelim. Diyalokta ögrenci kisilere kelimeleri tekarlamalarini (güvenilirlik icin) ve yavas konusmalarini söylemeli, böylece ögrenci kelimeleri anlayabilir (akis kontolu). Iletim Katmani, OSI modelinin 4.katmanidir, TCP yoluyla 5. katmana ulasmayi saglar

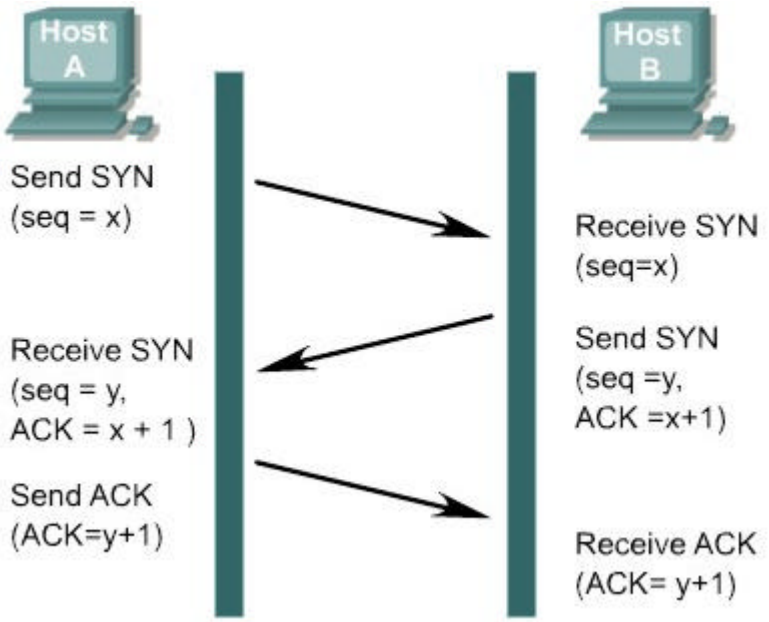
10.1 TCP Isletimi

10.1.2 Senkronizasyon yada 3-Yol Anlasmasi

TCP yölü iletisim protokolüdür. Bilgi transferinden önce iki iletisim sunucusu sanal baglanti gerçeklestirmek için senkronizasyon islemi yaparlar. Bu senkronizasyon islemi iki tarafinda bilgi transferi çin hazir olmasini saglar ve aygitin gerekli dizi numaralari saklamasina izin verir. Bu islem 3-yollu anlasma olarak bilinir. Bu üç adim islemi iki aygit arasinda sanal bir baglanti saglar.



- Ilk olarak bir sunucu senkronizasyon paketi göndererek iletisime baslar. Baglanti istegini göstermek için önceden ayarlanmis baslik biti ile x´in sira numarasi paketle beraber gönderilir. Bu bit TPC basligindaki onay numarasinda ayarlanmistir.
- Ikincisi,diger sunucu paketi alir, x`in sira numarasini kaydeder, (x+1) bilgisiyle cevap verir ve kendi baslangicina y sira numarasini ekler. X+1 in manasi , sunucunun tüm sekiz bitlik herseyi x dahil aldigini gösterir ve bir sonraki x+1 `i bekler.
- Son olarak , baslangictaki sunucu y+1 (sunucu b `nin sira numarasi +1) bilgisiyle cevap verir. Baglanti islemini sonlandirmak için önceki onay gösterilir.

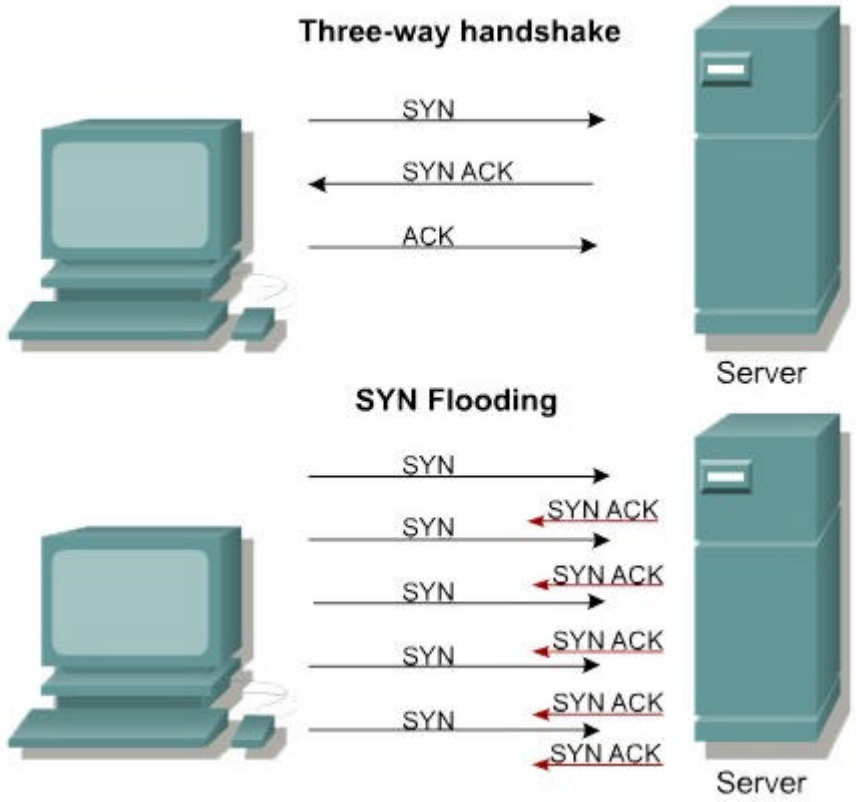


Önemli olan sira numaralarinin iki aygit arasindaki iletisimi baslatmanin bir parçasi oldugunu anlamaktir. Iki aygit arasinda baslangiç referans numaralari gibi hareket ediyorlar. Sira numaralari her onayda herbir sunucuya yol verir. Senkronizasyon olmasi için , uygun baglanti istegine yanit gönderir.

10.1 TCP TCP Isletimi

10.1.3 Servis Hareketlerinin Reddedilmesi

Servis hareketlerini reddedilmesi (DoS), sunucularin iletisim kurma çabalarini reddetmek için dizayn edilmistir. DoS hareketlerinin genel yöntemi Hacker larin sistem cevaplarindan yararlanmaktir. DoS un bir tipide senkronizasyon tasmasi olarakta bilinir. Senkronizasyon tasmasi normal üç-yol anlasmasinin sömürülmesinden ve cihaza olan hedeflerden dolayi yada onay kaynak adresilerinin anlasmayi tamamlayamamasindan kaynaklanir.
Üç-yol anlasmasi , sunucu senkronizasyon yolladigi zaman baslar. Senkronizasyon paketi kaynak ip adresini ve hedef ip adreslerini barindirir. Bu kaynak ve hedef adres bilgileri alici tarafindan senkronizasyon/onay paketini gönderen sunucuya geri gönderirken kullanilir.



DoS saldirilarinda , saldirgan senkronizasyonu baslatir. Fakat kaynak adresini kandirirlar. Kandirmalar, alim süresince kullanilarak, mevcut olmayan cihaz yanitlari , ulasilamayan IP adresleri gibi sorunlar olusturur. Ondan sonra olayi baslatan kimsenin onay çerililerinin bitmesi için durum-bekle politikasi uygulanir. Gerçek olmayan aygitin birseye cevap verdigi dönemdir, ulasilamayan bir adrestir. Baslaticidan en son onaylamayi almayi beklerken bekleme durumunda konumlanir. Bekleme istegi kuyruk baglantisinda veya hafizadaki tutma bölgesinde konumlanir. Bu bekleme durumu aygitin hafiza gibi sistem kaynaklarina saldirmasini saglar. Bglanti siresi bitene kadar bekleme islemine devam eder. Saldirganlar sahte senkronizasyon ile sunucuya saldirilari baslatacaktir. Tekrar kaynaklara baglanarak sahte baglantilar için beklerler.

Bu saldirilara karsi korunmak için sistem yöneticileri zaman disi iletisim sürecini arttirabilirler ve iletisim kuyruk büyüklügünü arttirabilirler. Ayrica bu tip saldirilardan korunmak için ve savunmaya yönelik ölçümü baslatmak için yazilim mevcuttur.

10.1 TCP Isletimi

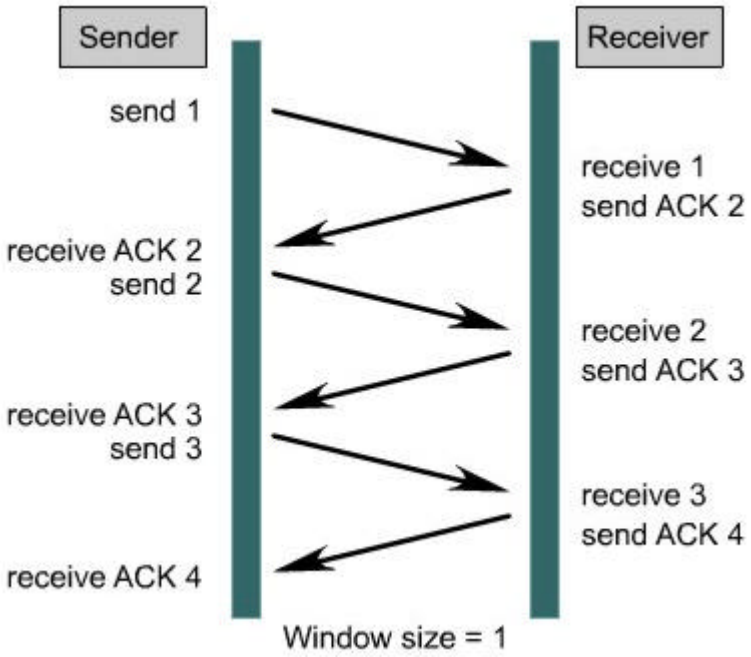
10.1.4 Pencereleme ve Pencere Büyüklügü

Gönderimesi gereken bilgi miktari basit bilgi parcalari göndermeye açiktir. Bu durumda bilgi, bilgi transferini saglayabilmek için ufak parcalara ayrilmalidir. TCP, bilgileri parçalara ayirmakla görevlidir. Bu çocugu beslemeye benzer. Çocuklar büyük parçalari tam olarak yiyemedikleri için, insan çocugu yedirirken yiyecegi çocugun agiz kapasitesinin alabilecegi ufak parçalar halinde kesmelidir. Ek olarak, alici makineler, bilgiyi kaynagin gönderebildigi

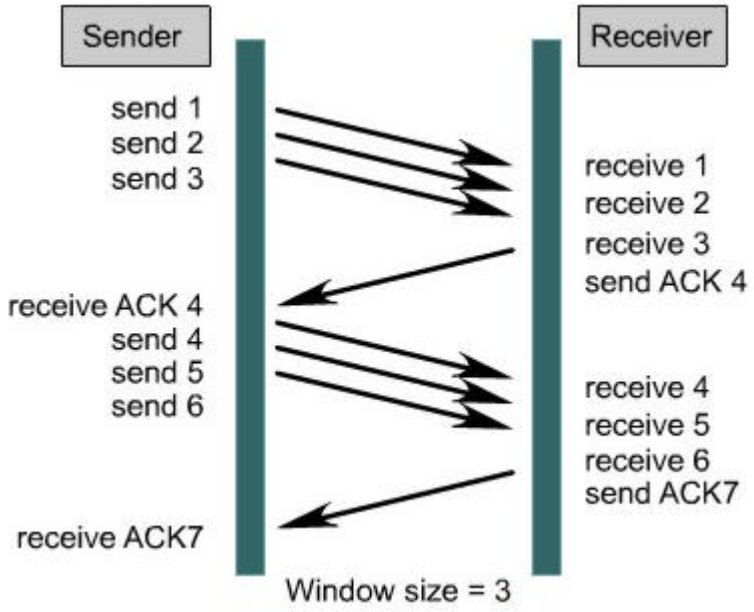
kadar hizli almayabilirler. Çünkü alici aygit diger sekillerle meskuldür veya belki gönderici daha güçlü bir aygitta olabilir.

Bilgi kisimlara ayrildiginda, alici aygita gönderilmelidir. TCP tarafindan saglanan servislerden biri akis kontrolüdür, bu iletisim asamasi süresince nekadar bilgi gönderildigini düzene koyar. Akis kontrol süreci pencerelendirme olarak bilinir.

Pencere büyüklügü bir devrede alici tarafindan bilginin alimindan önce gönderilebilen bilgi miktarini belirler. Sunucu birimleri pencere büyüklügünden numaralarla ilettiken sonra, bilginin daha fazla haber göndermeden önce haberi almalidir. Mesela,1 büyüklügündeki pencerede parçalarin bütün içerikleri bir sonraki parçaya bilgi gönderilmeden önce bilgilendirilmelidirler.



TCP iletisim büyüklügünü belirlerken pencereyi kaydirir. Kaydirilan pencere basit bir iletisim sirasinda bir bayttan daha büyük gönderilmesini saglar. Ayrica kaydirilan bu pencere, gönderilen bilgi miktarinin arttirilmasi veya azaltilmasi gerektiginde alici aygitin kaynagi belirlemesini saglar. Çünkü çok bilgi, alim sirasinda basarisiz olabilir.



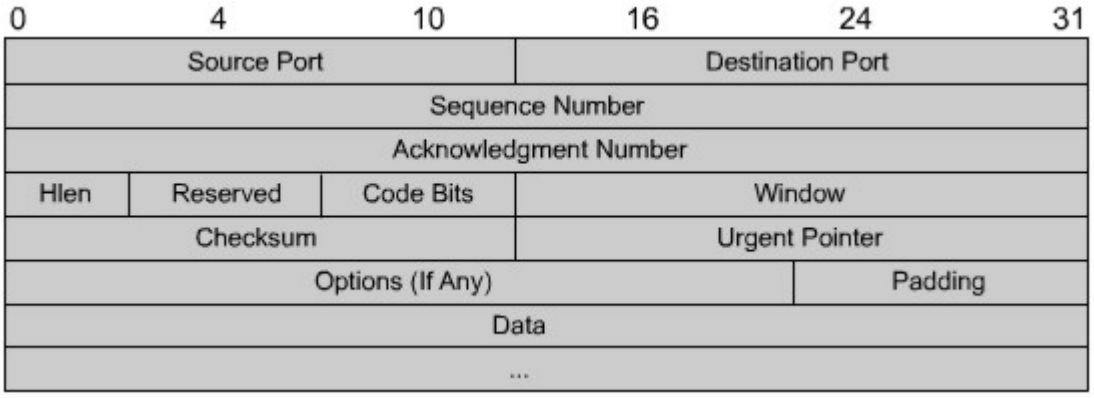
10.1 TCP Isletimi

10.1.5 Siralama Numaralari

TCP bilgiyi parçalara ayirir. Sonradan bilgi parçalari göndericiden aliciya iletilir, daha sonra senkronizasyon islemi takip edilir ve her zaman iletilebilen birim sayilarini gösteren pencere gelir. Iletilen bilgi parçalari bütün bilgi ulasmadan önce yeniden monte edilmis olmalidir. Bilginin iletilen emirler dahilinde ulasip ulasmayacagi konusunda garanti yoktur. TCP bilgi parcalarina sira numaralari saglar. Böylece alicida düzenli olarak parçalari orjinal bir sekilde yeniden monte edebilir. Eger TCP parçalari hizmet disi olursa, parçalar dogru bir sekilde toplanamicaktir Sira numaralari çeviri islemi oldugu zaman hedef cihaza hangi baytin nereye dogru bir sekilde konulacagini gösterir.

Bu sira numaralari ayrica alicinin bilgiyi çevirebilmesinde referans numaralari olarakta bilinirler. Bunlar ayrica kayip bbilgi parçalarinida belirler. Böylece kayip bilgi yeniden gönderilebilir. Bu göndericinin bütün bir bilgi yerine, sadece ihtiyaç olan gönderilmesi gereken kayip kismin tekrar gönderilmesini saglar.

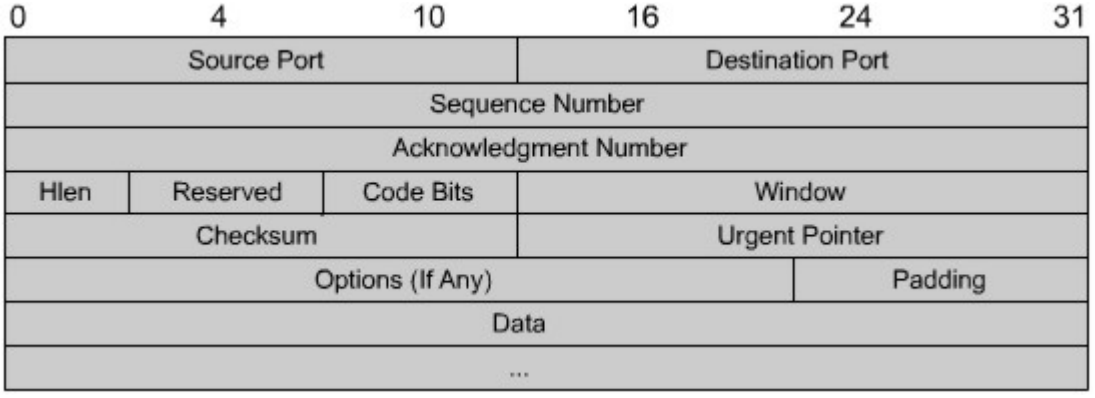
Herbir TCP parçasi göndermeden önce numaralandirilmistir. Dikkat edilmeli ki, parça biçiminde hedefin portu numara sirasinda bulunmaktadir. Alim durumunda , TCP mesaji tamamlamak için parçalarin tekrar birlestirilmesinde sira numaralarini kullanirlar. Eger numara sirasi seride kaybolmussa, bu parça yeniden gönderilir.



10.1 TCP Isletimi

10.1.6 Pozitif Alindi Bildirimi

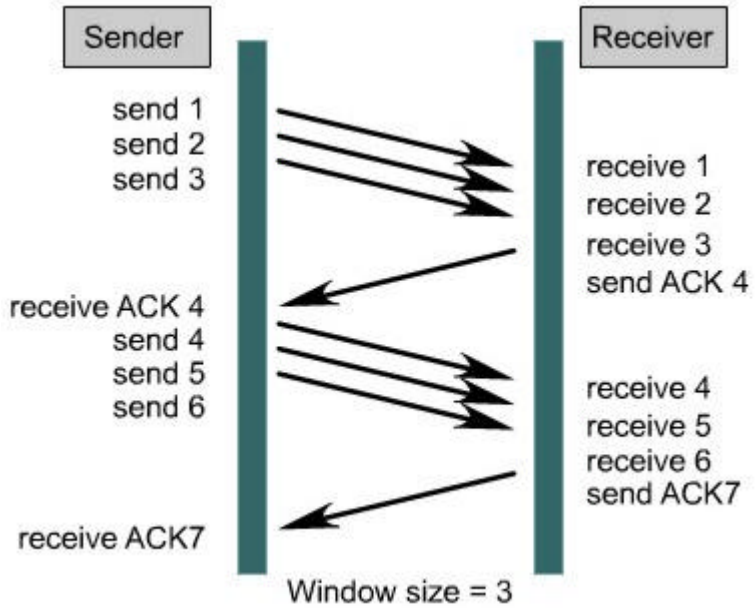
Alindi bildirimi genel olarak senkronizasyon isleminde pencerelerin kaydirilmasi ve datanin siralanmasi isleminin oldugu bir adimidir. TCP parçasinda, numara sirasi alani alindi bildirimi numara alani tarafindan takip edilir. Bu bolge bilginin veya nereye alindigini yada alindiklarini gösterir.



Gerçek olmayan IP protokolünün ,bilgi parçalarinin gerçekte gidecegi yere ulastiginin tespit edilememesi bir problemdir. Bu yuzden bilgi parçalari bilgisiz olarak alinir yada alinmayabilirler. TCP pozitif bilgilendirme ve yeniden gonderme ile verinin izlenmesi ve teslimi kontrol edilebilir.

Positif alindi bilgisi ve yeniden gönderme (PAR) birçok protokolün güvenilirligini saglamak için kullandigi genel bir tekniktir. Pozitif alindi bilgisi ile kaynak paketi gönderilir, zaman baslar, ve bir sonraki paketi göndermeden öce bilgiyi bekler. Eger kaynak alindi bilgisini almadan önce zaman biterse , kaynak paketi yeniden gönderilir ve zaman yeniden baslar. TCP

Pencereleme akis denetimi konrol mekanizmasidir ki, kaynagin bilgiyi gidecegi yerden kesin bilgi aldiktan sonra göndermesini saglar. Üç pencere büyüklügüyle kaynak uyarilari gidecegi yere gönderebiliyor. Daha sonra bilgiler için beklemesi gerekiyor. Eger üç sekizliyi çevirde , kaynak cihaza alindi bilgisini gönderir. O eger bir nedenden dolayi üç sekizliyi alamazsa ,tampon tasmil olabilir. Böylece alindi bilgisai yollanmayacaktir. Çünkü kaynak alindi bilgisini çeviremeyecek ve üç sekizliyi yeniden göndermesi gerektigini bilecektir. Busefer hizi yavaslatacaktir.

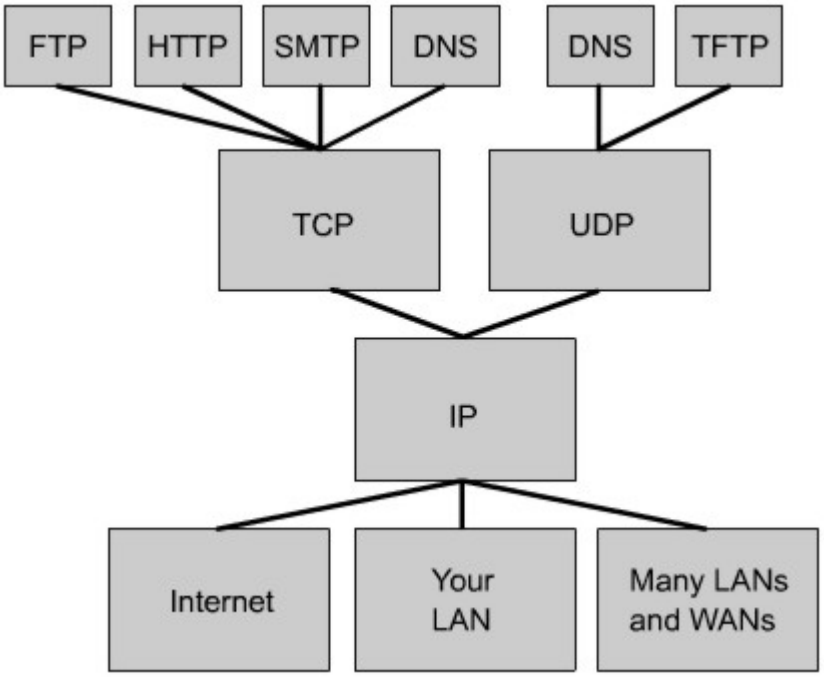


10.1 TCP Isletimi

10.1.7 UDP Isletimi

TCP/IP protokol kümesi bir çok degisik protokolü içerir. Bunlar kesin taslagi olusturmak için dizayn edilmislerdir. IP saglayicilari üçüncü katman baglantilarini ag çallisma ortamlari arasinda iletimi saglar. TCP de yönlü baglanti açiktir. Paketlerin güvenilir bir sekilde iletilmesi OSI modelinin dördüncü katmanda yapilir. UDP baglantisi , OSI modelinin dördüncü katmaninda paketlerinin garantisiz iletimini saglar

TCP ve UDP baslangiçta IP kullanmislardir. Üçüncü katman protokolü temelleridir. Ayrica TCP ve UDP , çesitli uygulama katmani protokolleri kullanirlar. TCP uygulamalar için servisler saglar. Örnek verecek olursak ; FTP, HTTP, SMTP, ve DNS olabilir. UDP bu örnekler tarafindan iletim katmani protokolü kullanir.



TCP , paketin ulasip ulasmadigina dair garantiye ihtiyaç duyuldugunda kullanilmalidir. Bazen TCP kullanildiginda paketin teslimini saglamak bazen problem olur. Uygulamalarin hepsinde veri paketinin garantili teslimine ihtiyaç duyulmaz.. Bundan dolayi hizli kullanilirlar. UDP tarafindan daha az baglanti mekanizmasi meydana getirir. UDP protokolü standart olarak RFC 768 olarak tarif edilir. Basit bir protokoldür. Garantili teslim yada alindi bilgisi olmadan parçalarin degistirildigi basit bir protokoldür.

# of Bits	16	16	16	16	16
	Source Port	Destination Port	Length	Check Sum	Data...

UDP pencereleme ve alindi bilgisini kullanmaz.Bu yüzden uygulama katman protokolleri hata yakalama saglamalidirlar.Kaynak portu sadece bilginin gönderilen yere dönmesi gerektiginde kullanilan bir bölgedir. Hedef router yönlendirme güncellemesi yaptigi zaman kaynak router hiçbir istekte bulunmaz. Bilgide yada veride bir degisiklik yok demektir. Hedef port alani , UDP nin geçirmesi gereken protokoller için gerekli uygulamalari belirler. DNS , DNS sunucudaki 53 numarali hefed porta sahip olabilmek için hosttan istekte bulunur. UdP port numarasi DNS içindir. UDP parçasinda sekiz bitlik olarak numaralandirilir. UDP bilginin iletim surecinde tahrip olmamasini saglamak icin kullanilmalidir. Agda diger tarafa tasinmasi için ,UDP IP paketlerinin içerinine paketler.

UDP parçalari , IP adresindeki yere ulastiginda mekanizma, alici ve sahibinin kesin olarak ulasacak bilgiyi belirlemesine izin veren sistemi olusturmalidir. Hedef port bu amaç için kullanilir. Eger sunucu açilista TFTP ve DNS servislerini çalistiriyorsa , UDP parçalarinin ihitiyaçlarini saglayan servise karar vermelidir. Hedef port alani UDP basliginda belirlenir.

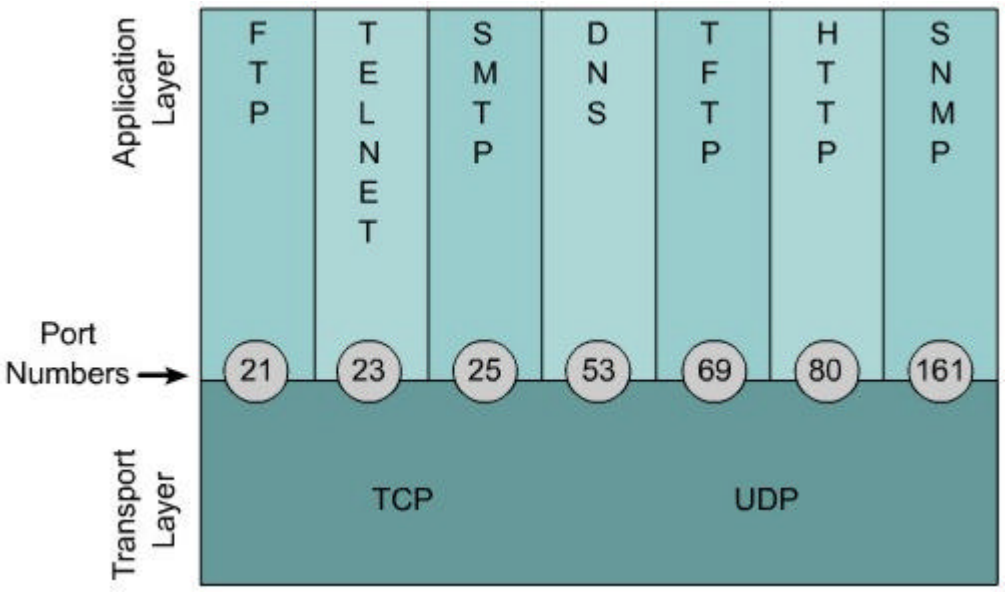
10.2 Iletim Katmani Portlarina Genel Bakis

10.2.1 Sunucular Arasinda Çoklu Multiple Diyalog

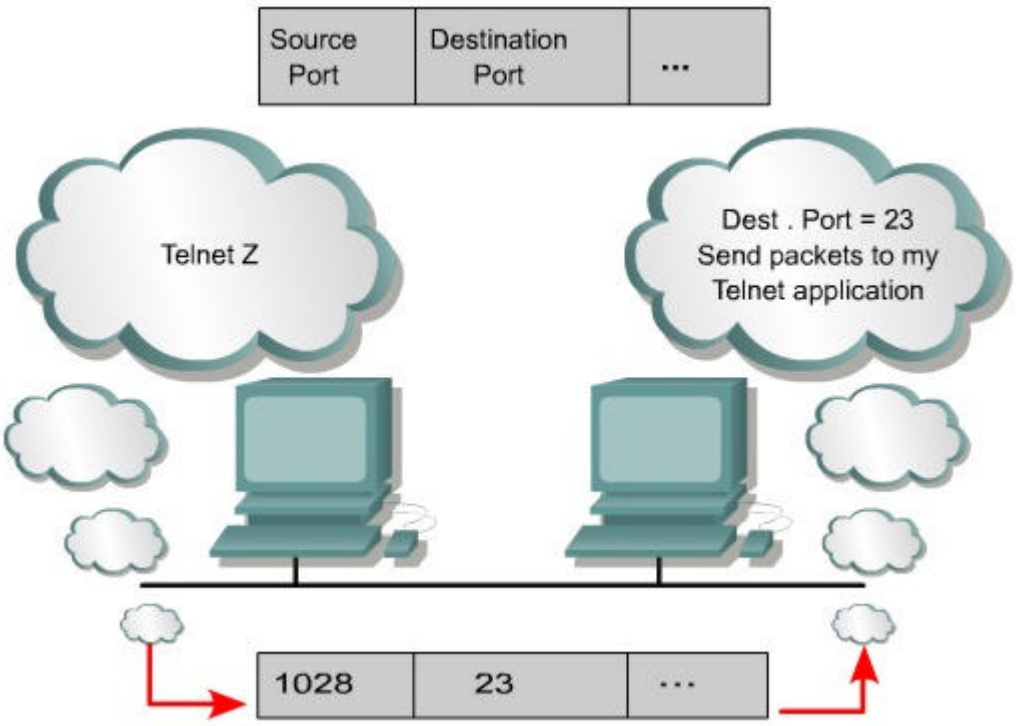
Modern aglarda her bir dakikada binlerce paket yüzlerce farkli servise tasinmaktadir. Çogu zaman sunucular , paketlerin adreslenmesi için adreslerde çok az problem yaratan çapraz servisler kullanirlar. Eger sunucu SMTP ve WWW nin her ikisini çalistiriyorsa , o servisin istedigi bölgeyi belirlemede kullanilir. Sadece sunucu ip adresleri için paket olusturulamaz. Çünkü hedef, servisin ne oldugunu bilemez. Port numaralari, sunucular arasindaki diyalog ile iliskilendirilmis olmali. Sunucuda uygun servislerde paket ulastirilabilir. Farkli diyaloglar ayarinda yollar ayirtedilemez. Istemcinin e-mail, web sayfalarini gözlemleme gibi islemleri kisa bir sürede bir sunucu kullanarak yapmaya gücü yetmez. Iletim katmani diyaloglari için ayrilmis metotlar kullanilmalidir.

Sunucular, iletim katmaninda TCP/IP ile iliskilendirilmis portlari çalistirirlar. Ayni zamanda agda farkli çapraz diyalog lari yakalamak için port numaralari kullanilir. Port numaralarina , sunucu çoklu servis çalistiran sunucularla iletisime geçtigi zaman ihtiyaç duyulur. TCP ve UDP nin ikisi de port ve soket numaralarini üst katmanin bilgilerine geçmek için kullanirlar.

Uygulama yazilim gelistiricileri , RCF1700 de tanimlanmis bilinen port numaralarini kullanirlar. FTP uygulamasini standart olarak 21 numarali porttan kullanirlar.



Diyaloglar uygulamalar ile iyi bilinen port numaralarini karistirmazlar. Özel bir sira içerisinden karisik olarak seçilmislerdir. Port numaralari TCP parçasinda kaynak ve hedef adresleri kullanirlar.



Port numaralari asagidaki görev dizisindedirler:

- 255 den asagi numaralar halka açik uygulamalar için ayrilmistir.
- 255 den 1023 e kadar olan numaralar satilabilir uygulamalar için sirketlere ayrilmistir.
- 1023 den yukari düzenlenmemistir

Son sistemler uygun uygulamalarda seçilen port numaralarini kullanirlar. Kaynak port numaralari sunucu tarafindan dinamiklestirilirler. Genellikle 1023 den büyük numaralardir. Port numaralari 0-1023 arasinda ise Internet Numara Yetkilendirme Dairesi (IANA) tarafindan kontrol edilir.

Posta ofisi kutu numaralari, port numaralari için iyi bir benzesimdir. Mesajin bir kismi posta sehir koduna , sehre ve posta kutusuna gönderilebilir. Sehir kodu ve sehir , posta kutusuna mektubun dogru bir sekilde gelmesine olanak saglar. Posta kutusu mektubun adreslendigi yere ulasmasini saglarken, posta ve sehir kodu genel mesaj seklinde yollanir.

posta numaralari icin iyi bir on siralamadir. Mesajin bir kismi posta, sehir koduna gonderilebilir. Posta kutusu meilin adreslendigi yere ulasmasini saglarken, posta ve sehir kodu genel mesaj seklinde yollanir. Benzer olarak IP adresleri dogru server`a gonderilir, fakat TCP ve UDP numaralari paketlerin dogru basvuruya gectigini grantiler. Benzer olarak IP adresleri paketleri dogrudan sunucuya gönderirler. Fakat TCP yada UDP port numaralari paketlerin dogru uygulamaya garantili bir sekilde geçmesini saglarlar.

10.2 Iletim Katmani Portlarina Genel Bakis

10.2.2 Servisler Portlari

Servisler sunucularda çalisirken iletisimde bulunabilmeleri için port numaralarina sahip olmak zorundadirlar. Uzaktaki sunucuya baglanti istedikleri zaman servisler iletim katmani protokolü ve portlari kullanmak isteyeceklerdir. Bazi portlar RFC 1700 ün içinde tanimlidir. TCP ve UDP her ikisinin içerisinde saklanmis iyi bilinen portlardir.

Decimal	Keyword	Description
0		Reserved
1-4		Unassigned
5	RJE	Remote Job Entry
7	ECHO	Echo
9	DISCARD	Discard
11	USERS	Active Users
13	DAYTIME	Daytime
15	NETSTAT	Who is Up or NETSTAT
17	QUOTE	Quote of the day
19	CHARGEN	Character Generator
20	FTP-DATA	File Transfer Protocol (data)
21	FTP	File Transfer Protocol
23	TELNET	Terminal Connection
25	SMTP	Simple Mail Transfer Protocol
37	TIME	Time of Day
39	RLP	Resource Location Protocol

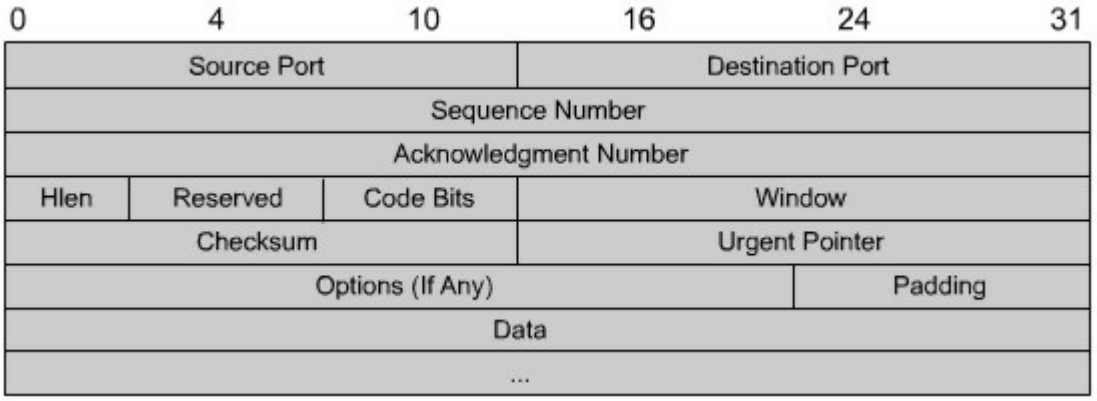
Decimal	Keyword	Description
42	NAMESERVER	Host Name Server
43	NICNAME	Who Is
53	DOMAIN	Domain Name Server
67	BOOTPS	Bootstrap ProtocoalServer
68	BOOTPC	Bootstrap Protocol Client
69	TFTP	Trivial File Transfer Protocol
75		Any Private Dial-out Service
77		Any Private RJE Service
79	FINGER	Finger
80	HTTP	HyperText Transfer Protocol
95	SUPDUP	SUPDUP Protocol
101	HOSTNAME	NIC Host Name Server
102	ISO-TSAP	ISO-TSAP
110	POP3	Post Office Prorotol for client to retrieve mails from mail server
113	AUTH	Authentication Service
117	UUCP-PATH	UUCP Path Service

Iyi bilinen portlar uygulamalarda tanimlanmistir. Iletim katmani protokollerinin üstünde çalistirilabilirler. Örnek verecek olursak; sunucular FTP servisini kullanirken TCP baglantilarini 20. portu kullanarak iletirler ve 21. porttan FTP uygulamalarini gerçeklestirirler. Yolda sunucu uzaktaki kullanicinin hangi servisi kullanmak istegine karar verir. TCP ve UDP iletimde dogru servise karar vermek için port numaralarini kullanir.

10.2 Iletim Katmani Portlarina Genel Bakis

10.2.3 Istemci Portlari

Ne zaman istemciler sunuculardaki servislere baglansalar kaynak ve hedef portlari belirtmelidirler. TCP ve UDP parçalari kaynak ve hedef portlari için alan bulundururlar. Hedef portlari yada servisin portu iyi olarak bilinen portlar kullanilarak tanimlanir. Kaynak portlari istemciler tarafindan dinamik olarak tanimlanirlar.



genelde istemciler kaynak portlari 1023 den yukari olan karisik olarak seçilmis olarak tanimlarlar. Örnek verecek olursak ; istemci iletisim yapmak istediginde web sunucu ile TCP yi kullanirken 80. portu kullanir ve kaynak portu ise 1045 dir. Paket sunucudan vardigi zaman iletim katmanindan geçmistir. Sonunda http servisi ile 80. portta islem tabi tutulur. http sunucu istemcilere 80. portu kullanarak cevap verir . hedef olarak 1045 i kullanir. Yolda sunucular ve servisler iliskilendirildikleri portlari kullanirlar.

10.2 Iletim Katmani Portlarina Genel Bakis

10.2.4 Port Numaralandirmasi ve En çok bilinen Port Numaralari

Port numaralari , TCP yada UDP parçalarin çerçevelerinde 2 bayt ile ifade edilirler. Bu 16bit degerine denk gelmektedir. Port numaralari 0 dan 65535 e kadar degismektedir. Port numaralari üç farli kategoriye bölünmüstür.

1-Iyi bilinen portlar

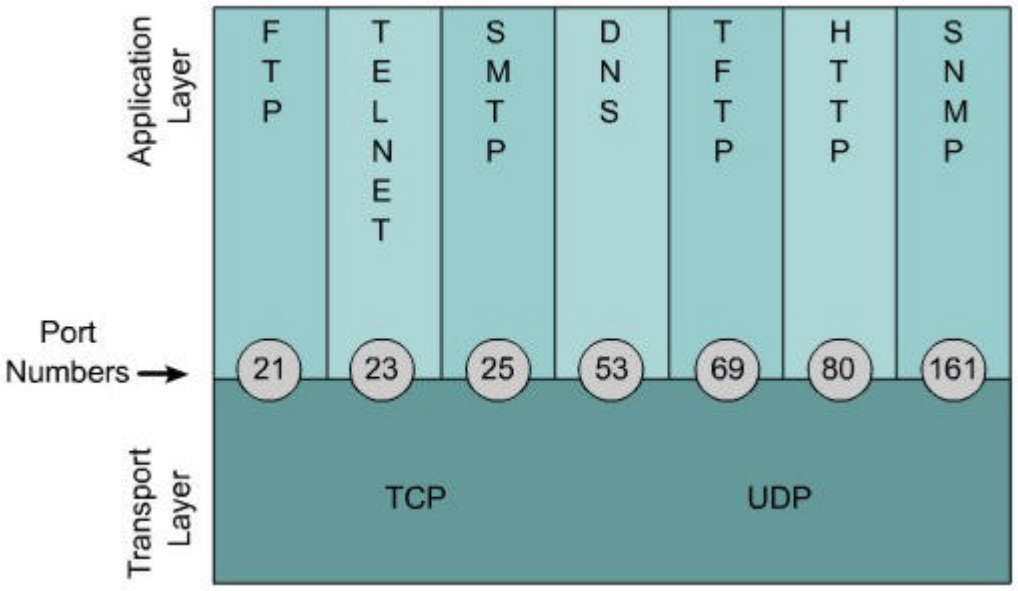
2-Kayitli portlar

3-Dinamik yada özel portlar.

Iyi bilinen portlar - Ilk 1023 port ençok bilinen portlardir. Ag servislerinde iyi bilindikleri için bu isim kullanilmistir. FTP , Telnet yada DNS gibi.

Kayirli Portlar – 1024 ten 49151 e kadar olan kayitli portlardir.

Dinamik yada Özel Portlar – 49152 ile 65535 arasindaki portlardir



10.2 Iletim Katmani Portlarina Genel Bakis

10.2.5 Sunucular Arasindaki Çoklu Oturumlara Örnek

Port numaralari sunucular arasinda çoklu oturumlar ortaya çikabildigi için kullanilirlar. Kaynak ve hedef port numaralari soketten ag adresleri ile bütünlesiktir. Soket çiftleri her sunucuda bir tanedir. Örnegin telnet baglantisi port 23 tür. Bazi zamanlar nette gezerken port 80 olabilir. Ip ve MAC adresler ayni olabilir. Çünkü paketler ayni sunucudan gelebilir. Buyüzden her diyalog kaynakta kendi port numarasina ihtiyaç duyabilir. Ve her servis yanitlarken kendi port numarasina ihtiyaç hissedebilir.

10.2 Iletim Katmani Portlarina Genel Bakis

10.2.6 MAC adreslerin , IP adreslerin ve Port Numaralarinin Karsilastirilmasi

Adreslemede üç adet metot sik sik karistirilir. Fakat bu önlenebilir. Eger adresler OSI modelindeki referanslarda açiklanmistir. Port numaralari iletim katmaninda yerlestirilmistir ve ag katmanindan servis edilirler. Ag katmaninda lojik adresler(IP adresi) atanmistir. Bunlar data iletim katmani tarafindan hizmet verirler. Burada fiziksel adresler (MAC adres) atanmistir.

Bir mektup örnegi ile benzesim yapilabilir. Mektuptaki adresler isim , sokak , sehir ve ülke yi barindirir. Ag verisi için port, MAC ve IP adresleri kullanarak kiyaslama yapabiliriz. Port numaralarina esdeger olarak isimi , sokak adresi olarak MAC adresini , sehir ve ülke adresi olarak IP adresini eslestirebiliriz. Çoklu mektuplar sokak adreslerine, sehir ve ülkeye göre gönderilebilirler. Fakat mektuplardaki alicilarin isimleri farklidir. Örnegin elimizde bir adrese

Baki SAKALLI ve Fevzi SAKALLI adina iki mektup gönderilmis olsun. Bunu farkli port numaralari ile benzestirebiliriz

ÖZET

Asagidaki kilit noktalarinin anlasilmis olmasi saglanmalidir:
:

- TCP isletiminin tanitilmasi
- Senkronizasyon Islemleri (üç-yol anlasmasi)
- Servis saldirilarinin engellenmesi
- Pencereleme ve pencere genisligi
- Numara silalari
- Pozitif alindi bilgisi
- UDP operasyonu
- Sunucular arasinda çoklu diyalog
- Servis portlari
- Istemci portlari
- Port numaralandirilmasi ve iyi bilinen portlar
- Sunucular arasindaki çoklu oturum örnegi
- MAC adresin, IP adresin ve port numaralarinin karsilastirilmasi

BÖLÜM - 11

Genel Bakis

Ag yöneticileri, dahili kullanicilarin gerekli servislere yaptigi normal giris islemlerine izin verirken istenmeyen giris islemlerini ne sekilde engelleyeceklerini göz önünde bulundurmalidir. Parolalar, geri çagirma ekipmanlari ve fiziksel güvenlik aygitlari gibi araçlar yardimci birer unsur olmakla birlikte çogu kez temel filtreleme esnekliginden ve çogu yöneticinin tercih ettigi özel kontrollerden yoksundurlar. Sözgelimi, bir ag yöneticisi kullanicilarin internet erisimine izin vermeyi isteyebilir fakat dis kullanicilarin ag içinde telnet erisimlerine izin vermeyebilir.

Router'lar , erisim kontrol listeleriyle (EKL) bir tür internet trafigini bloklama gibi temel trafik filtrelemesi yetenegi saglarlar. Bir erisim kontrol listesi (EKL) üst katman protokolleri ya da adreslere uygulanan izin ya da red durumlarinin yer aldigi ardisik bir listedir. Bu bölümde ag trafigini kontrol amaçli standart ve uzatilmis ACL' ler tanitilacak ve onlarin bir güvenlik çözümümün bir parçasi olarak nasil kullanilacagi gösterilecektir.

Ek olarak bu bölüm ipuçlari, degerlendirmeler, öneriler ve ACL' lerin nasil kullanilacagina yönelik genel kilavuzlar ile EKL olusturmada gereksinim duyulan konfigürasyon ve komutlari içermektedir. Son olarak, yine bu bölümde standart ve uzatilmis ACL örnekleri ve onlarin router arabirimine nasil uygulandigi gösterilmistir.

ACL'ler belirli bir host'dan gönderilen paketlere izin verme dogrultusunda tek bir satir kadar yalin olabilecegi gibi router erisiminin performansini etkileyen ve trafigi kesin bir sekilde tanimlamaya yönelik son derece karmasik bir kurallar ve kosullar kümesi de olabilir. Bu bölümde EKL' nin ileri düzey kullanimlarinin çogu konu disi birakilmis olup, standart ve uzatilmis EKL hakkinda ayrinti, EKL' nin düzgün yapilandirilmasi ve bazi özel uygulamalara yer verilmistir.

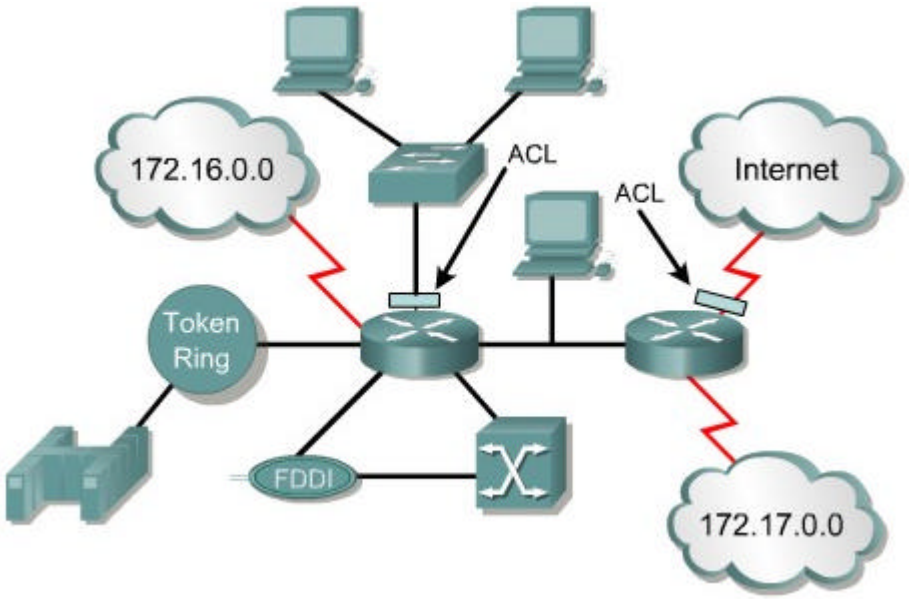
Bu modülü tamamlayan kimseler sunlari yapabiliyor olmalilar :

- Standart ve uzatilmis EKL' ler arasindaki farklari tanimlayabilmeli
- EKL' lerin yapilandirma kurallarini açiklayabilmeli
- EKL adlandirmalarini olusturabilmeli ve uygulayabilmeli
- Güvenlik duvari fonksiyonunu açiklayabilmeli
- Sanal terminal erisimlerini kisitlamada ACL' leri kullanabilmeli

11.1 Erisim Kontrol Listesinin Temelleri

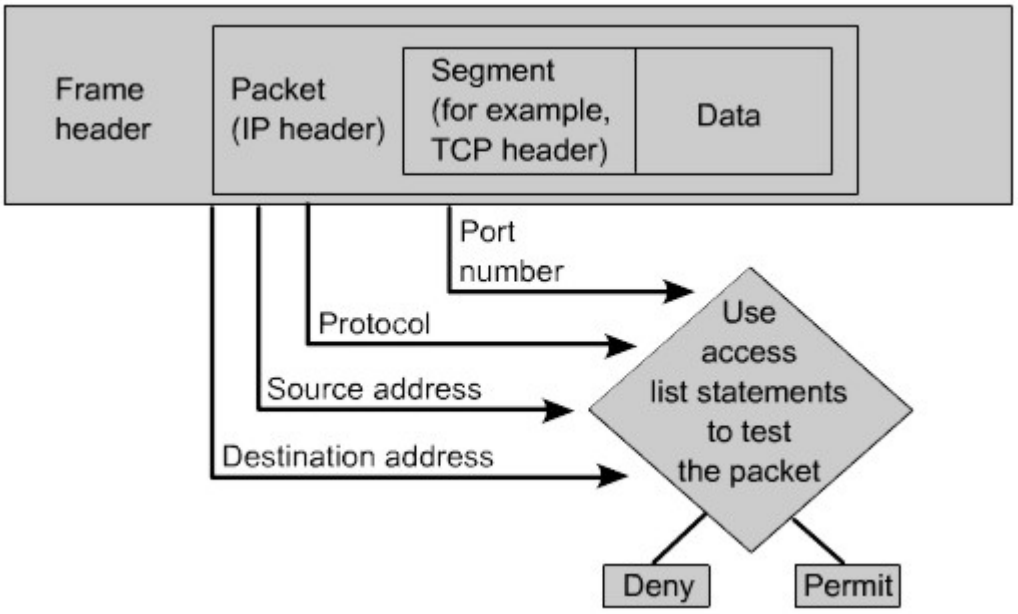
11.1.1 ACL Nedir ?

EKL (ACL)' ler bir router arabirimi üzerinde yol alan trafige uygulanacak kosullar listesidir. Bu listeler, router'a hangi tip veri paketlerinin kabul ya da red edilecegini söyler. Kabul ya da red belirlenmis kosullara baglidir. ACL'ler trafigin yönetimini mümkün kilar ve bir aga ya da agdan yapilacak erisimi güvenli kilar.



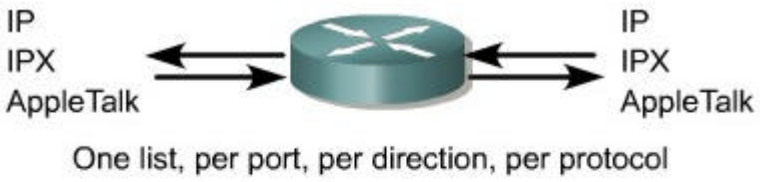
ACL'ler , Internet Protokolü (IP) ve Internet Is Paket Degisimi (IPX) gibi her tür yönlendirilmis ag protokolleri için olusturulabilir. ACL' ler bir aga ya da alt aga erisimi kontrol için router üzerinde yapilandirilirlar.

ACL' ler yönlendirilmis paketlerin gönderilmis ya da bir router arabiriminde bloke edilmis olup olmadigini kontrol etmek suretiyle ag trafigini filtreler. (2) Router, EKL' de belirtilen kosullara dayali olarak, gönderilmis mi yoksa düsmüs mü oldugunu saptama amaciyla her paketi inceler. Bazi EKL karar noktalari veri paketinin gidecegi adreslerin, protokollerin ve üst katman port numaralarinin kaynagidir.



ACL' ler protokol, yön ya da port temelli olarak tanimlanmalidir. (3) Bir arabirim üzerindeki trafik akisini kontrol etmek için arabirim üzerinde çalisir durumdaki her bir protokol için bir ACL tanimlanmalidir. ACL' ler trafigi bir arabirim üzerinde tek bir yönde ve tek zamanda kontrol ederler. Her farkli bir yön için ayri ayri bir ACL olusturulmalidir ; giris trafigi için bir tane, çikis trafigi için bir tane. Sonuç itibariyla her bir arabirim çok sayida protokole ve tanimlanmis yöne sahip olabilir. Eger router IP ve IPX için konfigüre edilmis iki arabirime sahip ise 12 farkli EKL gerekecektir. Her protokol için bir EKL, giris ve çikis dogrultusu için iki defa ve port sayisi için iki defa gerekecektir.

.



With two interfaces and three protocols running, this router could have a total of 12 separate ACLs applied.

EKL olusturmanin birincil nedeni sunlardir:

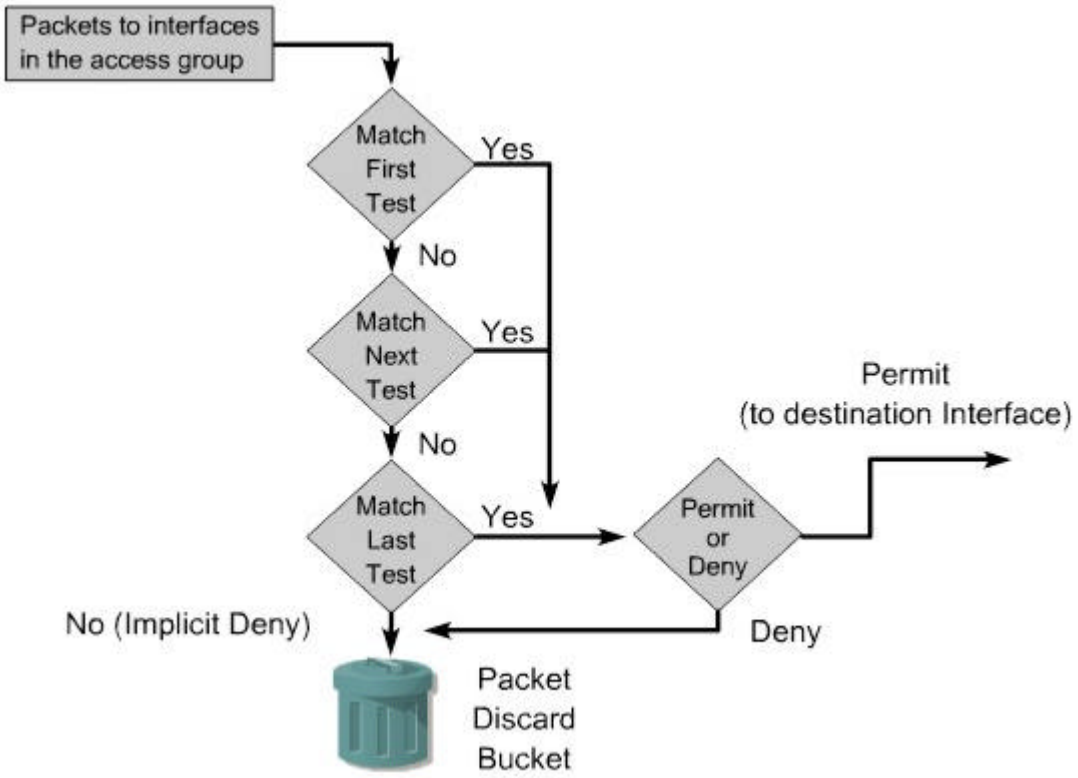
- Ag trafigini sinirlamak ve ag performansini artirmak. Örnegin ACL'ler video trafigini sinirlamak suretiyle agdaki yükü büyük ölçüde azaltir ve neticede ag performansini artirir.
- Trafik akisi kontrolünü saglamak. ACL' ler gönderi yenilemelerinin dagitimini sinirlayabilir. Eger yenilemeler ag kosullari nedeniyle gerekli degilse bana genisligi muhafaza edilir.
- Ag erisiminde temel bir güvenlik düzeyi saglamak. ACL' ler bir dost'un agin bir kismina erismesine izin verebilir ve diger bir dost'un ayni bölgeye erisimini engelleyebilir. Örnegin, höst A ' nen Insan Kaynaklari Agina erisimine izin verilirken, höst B' nine oraya erisimi engellenebilir.
- Router arabirimlerinde hangi tip trafige yol verilecegi ya da bloke edilecegine karar vermek. E-Posta trafiginin gönderime izinli olmasi ama tüm telnet trafiginin bloklu olmasi.
- Bir yöneticiye, bir istemcinin aga hangi alanda erisebilecegini kontrol etmek izni vermek.
- Agin belli bir kismina erisim izni olsun ya da olmasin bazi hostlari ekranda görüntülemek. Sadece FTP ya da HTTP gibi belli basli dosyalarda Erisim için kullanici iznini onaylamak ya da reddetmek

Eger ACL' ler router üzerinde konfigüre edilmezlerse router içinden geçen her pakete agin her yanina ulasmasi için izin verilecektir.

11.1 Erisim Kontrol Listesinin Temelleri:

11.1.2 ACL ler Nasil Çalisir

Bir EKL, bir verinin giris ve çikis arabirimi sinirlarinda kabul ya da reddedilecegini tanimlayan bildirimler grubudur. (1) Bu kararlar, bir erisim listesindeki kosul bildirimlerinin örtüstürülmesiyle gerçeklesir ve ardindan bildirimde tanimlanan kabul ya da ret eylemi uygulanir.



*** ACL' lerin hangi sirada konumlandirilacagi önemlidir. Cisco IOS yazilimi, paketleri her kosul bildirimi karsisinda en tepeden en alta kadar test eder. Listede bir eslesme oldugunda kabul ya da ret eylemi icra edilir ve diger EKL bildirimleri kontrol edilmez. Tüm trafige topyekün izin veren bir kosul bildirimi listenin en basinda yer aliyorsa asagiya eklenmis bildirimler asla kontrol edelimeyecektir.

Eger bir erisim listesinde ilaveten kosul bildirimleri gerekiyorsa, tüm EKL listesi silinmeli ve yeni kosul bildirimleriyle tekrar olusturulmalidir. Bir EKL' yi yenilemeyi kolaylastirma konusunda notepade gibi bir editör kullanmak ve EKL' yi router konfigürasyonuna yapistirmak iyi bir fikirdir.

ACL'ler kullanilsin ya da kullanilmasin, router islemlerinin baslangici aynidir. (3) Bir çerçeve gibi arabirim girer, router iki adres katmaninin eslesip eslesmedigini ya da gösterim çerçevesi olup olmadigini kontrol eder. Eger çerçeve adresi kabul edilirse çerçeve bilgisi çikartilir ve router inbound bir arabirim üzerinde EKL olup olmadigini kontrol eder. Eger mevcut bir EKL varsa, paket o anda listede yer alan bildirimler dogrultusunda test edilir. Eger paket bir bildirimle eslesirse paketi kabul ya da ret islemi gerçeklesir. Eger paket arabirimde kabul edilirse bu durumda alici arabirimin saptanmasi ve arabirime yöneltilmesi için paket gönderi tablosu girisleri dogrultusunda kontrol edilir. Sonrasinda router alici arabirimin bir EKL' si olup olmadigini kontrol eder. Eger mevcut bir EKL varsa, paket o anda listede yer alan bildirimler dogrultusunda test edilir. Eger paket bir bildirimle eslesirse paketi kabul ya da ret islemi gerçeklesir. Eger EKL yoksa ya da paket kabul edilmis ise paket ikinci yeni katman protokolüne alinir ve bir sonraki aygita gönderilmek üzere arabirim disina yönlendirilir.

Genel görünüs itibariyla EKL bildirimleri ardisik ve mantiksal bir düzende çalisir. Eger bir kosulun dogrulugu eslesiyorsa pakete izin verilir ya da tam tersi reddedilir ve EKL bildirimlerinin digerleri kontrol edilmez. Eger EKL bildirimlerinin hiçbiri esleme göstermiyorsa listenin en sonuna default bir deger olarak gizli bir " hepsi ret " bildirimi

yerlestirilir. Liste sonundaki bu bildirim, EKL' de eslesme saglamayan hiçbir paketin kabulüne olanak saglamayacaktir. " hepsi ret " degeri bir ACL' nin son satiri gibi görünür olmamasina karsin orada olacaktir ve EKL de eslesme göstermeyen hiçbir paketin kabulüne izin vermeyecektir. ACL' lerin nasil olusturulacagini ilk ögrenirken, komut satirinin dinamik varligini güçlendirmek için ACL' nin sonuna gizli bir ret eklemek iyi bir fikirdir.

11.1 Erisim Kontrol Listesinin Temelleri

11.1.3 ACL' lerin olusturulmasi

ACL'ler global konfigürasyon modunda olusturulur.(1) Standart, uzatilmis, IPX, Apple Talk, ve baska digerlerini de içeren çok farkli tiplerde ACL' ler vardir. Bir router üzerinde ACL' leri konfigüre ederken her ACL kendisine atanan bir rakamla kendine özerk tanimlanmalidir. Bu rakam, olusturulan erisim listesinin tipini tanimlar.

Protocol	Range
IP	1-99
Extended IP	100-199
AppleTalk	600-699
IPX	800-899
Extended IPX	900-999
IPX Service Advertising Protocol	1000-1099

Dogru komut moda girildikten ve liste tip numarasina karar verildikten sonra, kullanici uygun parametreleri takiben, Access-list anahtar sözcügünü kullanarak erisim listesi bildirimlerini girer. (3) Erisim listesi olusturma isi onlari router üzerinde kullanmanin ilk yarisidir. Islemin ikinci yarisi ise, onlarin dogru arabirimlere atanmasidir.

Step 1	Define the ACL by using the following command: `Router(config)#access-list access-list-number {permit | deny} {test-conditions}` A global statement identifies the ACL. Specifically, the 1-99 range is reserved for standard IP. This number refers to the type of ACL. In Cisco IOS Release 11.2 or newer, ACLs can also use an ACL name, such as education_group, rather than a number. The **permit** or **deny** term in the global ACL statement indicates how packets that meet the test conditions are handled by Cisco IOS software. **permit** usually means the packet will be allowed to use one or more interfaces that you will specify later.The final term or terms specifies the test conditions used by the ACL statement.

Step 2	Next, you need to apply ACLs to an interface by using the **access-group** command, as in this example: `Router(config-if)#{protocol} access-group access-list-number` All the ACL statements identified by *access-list-number* are associated with one or more interfaces. Any packets that pass the ACL test conditions can be permitted to use any interface in the access group of interfaces.

ACL'ler bir ya da daha fazla arabirime atanabilir ve **access-group** (erisim-küme) komutu kullanilarak giris ve çikis trafigini filtreleyebilir.

```
Router(config)#
access-list 2 deny   172.16.1.1
access-list 2 permit 172.16.1.0  0.0.0.255
access-list 2 deny   172.16.0.0  0.0.255.255
access-list 2 permit 172.0.0.0   0.255.255.255
interface ethernet 0
  ip access-group 2 in
```

Access-group komutu arabirim konfigürasyonuna iletilir. Bir giris ya da çikis arabirimine herhangi bir EKL atandiginda konumlandirma özellestirilmelidir. Filtreleme yönü içeri ya da disari giden paketleri kontrol için ayarlanabilir. ACL' nin giris trafigi mi yoksa çikis trafigine mi adreslenmis oldugunu saptarken ag yöneticisi router' in içinden gelen arabirimlere göz atma geregi duyabilir. Bu çok önemli bir düsüncedir. Bir arabirimden gelen trafik giris erisim listesince, arabirimden çikan trafik de çikis erisim listesince filtrelenir. Numaralandirilmis bir EKL olusturulduktan sonra bir arabirime atamsi yapilmalidir. (5) Numaralandirilmis EKL bildirimleri içeren bir EKL degistirilecekse, içindeki tüm bildirimler **no access-list /** liste no komutu kullanilarak silinmelidir.

```
Router(config)#no access-list 2
```

Erisim listeleri olusturulurken ve uygulanirken su temel kurallar takip edilmis olmalidir:

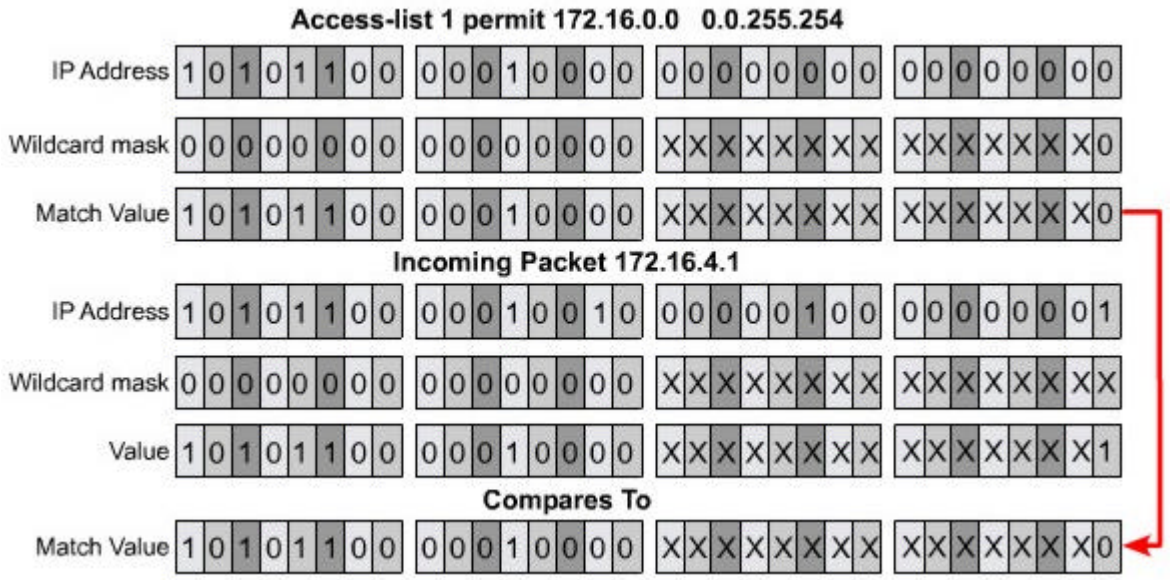
- Protokol ve yön temelli bir erisim listesi
- Standart erisim listesi alici adresine en yakin olmalidir
- Uzatilmis erisim listesi kaynaga en yakin olmalidir.
- Giris ve çikis arabirim referanslari router'in içinden sanki porta bakiyormus gibi kullanilmalidir.
- Bildirimler, bir esleme gerçeklesene kadar listenin en basindan en sona kadar ardisik olarak gerçeklesecektir ve eger eslesme olmaz ise paket reddedilecektir.
- Erisim listesinin sonunda gizli bir ret olacaktir. Bu normal olarak konfigürasyon listelemesinde ekrana görüntülenmez.
- Erisim listesi girisleri özelden genele bir sira içinde filtrelenmelidir. Özel hostlar önce reddedilmeli, ve gruplar ya da genel filtrelemeler sonra gelmelidir.
- Eslesme kosulu ilk önce incelenir. Izin ya da ret sadece eslesme dogru ise incelenir.
- Bir erisim listesi aktif olarak uygulamadayken üzerinde asla çalismayin
- Mantiksal çikis yorumlari olustururken bir metin editörü kullanin ve ardindan mantiksal kosulu icra eden bildirimleri tamamlayin
- Erisim listesinin sonuna daima yeni satirlar eklenir. **No access-list** x komutu tüm listeyi silecektir. Numaralandirilmis bir EKL' yi seçerek silme ya da ekleme mümkün degildir.
- IP erisim listesi, reddedilen paketin göndericisine , "bulunamayan ICPM mesaji" yollar ve paket göz ardi edilir.
- Bir erisim listesi silinirken dikkatli olunmalidir. Eger erisim listesi bir ürünün arabirimine uygulanir ve silinirse, IOS'un versiyonuna bagli olarak arabirime default bir red uygulanir ve dolayisiyla tüm sistem durur.
- Çikis filtrelemesi lokal routerdan kaynaklanan trafigi etkilemez.

11.1 Erisim Kontrol Listesinin Temelleri

11.1.4 (wildcard mask) Joker Maske nin islevi

Joker maske (wildcard mask) , dört sekizlige bölünmüs bir 32 bitdir. Joker maskesi bir IP adresi ile eslesir. Maskedeki sifir ve birler, Ip adres bitleriyle nasil haberlesecegini tanimlamak için kullanilir. Wildcard maskelemesi terimi tipki bir poker oyununda herhangi bir kartla eslesen joker mantiginda olup, ACL' nin mask-bit eslesmesi için bir tür takma addir (nickname). Joker maskelerinin alt ag maskeleriyle islevsel bir iliskisi yoktur. Onlar farkli amaçlar ve farkli kurallar dogrultusunda kullanilir. Alt ag maskeleri IP adresinin sol tarafindan baslar ve host alanindan ödünç bitler almak suretiyle agda genislemek için sag tarafa dogru ilerler. Joker maskeleri, adrese bagli olarak kaynaklara erisimi kabul ya da red eden bireysel veya grup ip adreslerini filtrelemek için tasarlanmistir. Joker maskelerinin alt ag maskeleriyle nasil iliskilendirilip çalistirilacagini düsünmek sadece kafa karistir. Joker maske ile alt ag maskesi arasindaki tek benzerlik her ikisinin de otuz iki bit uzunlukta olmasi ve maskelemede sifir ve birleri kullaniyor olmasidir.

Diger bir açidan, joker maskesindeki sifir ve birler, alt ag maskesin dekindekilerden çok farklidir.(2) Bu karisikligi gidermek için, grafikte joker maskesindeki 1 lerin yerine X ler konmustur. Bu maskeleme 0.0.255.255 olarak yazilabilirdi. Buradaki sifirin anlami, kontrol edilecek degerlere izin vermek, X 'lerin (yani 1 ' lerin) anlami ise karsilastirilan degerlerin bloklanmasidir.



Joker maskesi isleminde, erisim listesi bildiriminde yer alan ip adresi kendisine uygulanmis bir joker maskesine sahiptir. Bu, bir paketin EKL tarafindan isleme konup konmayacagini görmede ve karsilastirmada kullanilacak bir deger üretir ya da bir sonraki bildirimi kontrol amaciyla gönderir. EKL isleminin ikinci kismi, belli bir ACL bildirimince kontrol edilmis olan herhangi bir IP adresinin bildirim tarafindan ona uygulanacak olan joker maskesinin alinmasidir. IP adresinin ve joker maskesinin sonucu EKL' nin degerini eslemede esit olmalidir. Bu islem çizimde gösterilmistir.

ACL'lerde kullanilan iki özel anahtar sözcük vardir. Bunlar: **any** ve **host** seçenekleridir.(4) Basit sekliyle, **any** seçenegi IP adresi için 0.0.0.0 in yerini, joker maskesi için de 255.255.255.255'in yerini tutar. Bu seçenek, karsilastirilmis olan herhangi bir adresi eslestirecektir. **Host** seçenegi, 0.0.0.0 maskesinin yerini tutar. Bu maske, EKL adresinin tüm bitlerine ve paket adresinin eslesmis olmasina gerek duyar. Bu seçenek tek bir adresi eslestirecektir.

```
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255

Can be written as:
Router(config)#access-list 1 permit any

Router(config)#access-list 1 permit 172.30.16.29 0.0.0.0

Can be written as:
Router(config)#access-list 1 permit host 172.30.16.29
```

11.1 Erisim Kontrol Listesinin Temelleri

11.1.5 ACL' lerin Dogrulanmasi

Router üzerinde ACL' lerin yerlesimini ve içerigini dogrulamak için pekçok **show** komutu vardir

Show ip interface komutu, Ip arabirim bilgilerini görüntüler ve herhangi bir ACL' nin kurulu olup olmadigini belirtir(1) . **Show access-list** komutu router üzerindeki tüm ACL' lerin içerigini görüntüler.(2). Özel bir listeyi görmek için, bu komutla birlikte seçenek olarak ACL adini ya da numarasini eklemek gerekir. **Show running-config** komutu da yine router üzerindeki erisim listesini ve arabirim atama bilgilerini ortaya çikaracaktir.

```
Router#show access-lists
Standard IP access list 2
 deny   172.16.1.1
 permit 172.16.1.0, wildcard bits 0.0.0.255
 deny   172.16.0.0, wildcard bits 0.0.255.255
 permit 172.0.0.0, wildcard bits 0.255.255.255
Extended IP access list 101
 permit tcp 192.168.6.0 0.0.0.255 any eq telnet
 permit tcp 192.168.6.0 0.0.0.255 any eq ftp
 permit tcp 192.168.0.0 0.0.0.255 any eq ftp-data
Router#
```

Bu show komutlari, liste içeriklerini ve yapilanmalarini dogrulayacaktir. Erisim listesi mantigini dogrulamak için örneksel bir trafik üzerinde erisim listelerini teste yönelik olarak da bu iyi bir alistirmadir.

11.2 Erisim Kontrol Listeleri (ACL)

11.2.1 Standart ACL' ler

Standart ACL' ler yönlendirilmis IP paketlerinin kaynak adresini kontrol ederler(1). Aga, alt aga ve host adreslerine bagli olarak topyekün protokol için karsilastirma izin ya da red ile sonuçlanacaktir. Örnegin, Fa0/0 dan gelen paketler kaynak adresi ve protokolü için kontrol edilecektir. Eger izin verilmisse, paketler routera dogru bir çikis arabirimine yönlendirilecektir. Eger izin verilmemisse daha giris arabirimindeyken düseceklerdir.

Access-list global konfigürasyon komutunun standart versiyonu, standart bir ACL' nin 1 ile 99 arasi bir rakamla tanimlanmasinda kullanilir.(Yeni IOS da bu 1300' den 1999' a kadar da olabilir) (2). Ilk EKL bildiriminde Joker kart maskesi olmadigina dikkat edin. Listenin görüntülenmedigi böylesi bir durumda 0.0.0.0 olarak default maske kullanilir. Bunun anlami, tüm adreslerin eslesmek zorunda oldugu ve EKL' deki bu satirin uygulanmadigi ve routerin bir sonraki satirda esleme için kontrol yapmasi gerektigidir.

```
access-list 2 deny   172.16.1.1
access-list 2 permit 172.16.1.0  0.0.0.255
access-list 2 deny   172.16.0.0  0.0.255.255
access-list 2 permit 172.0.0.0   0.255.255.255
```

- Access list number range of 1-99
- Filter only on source IP address
- Wildcard masks
- Applied to port closest to destination

Standart EKL komutunun yazilis formati su sekildedir:

Router(config)# **access-list** erisim liste no [deny / permit] source [kaynak-jokerkart] [**log**]

Bu komutun parametresiz sekli standart bir ACL' nin silinmesinde kullanilir. Yazilis sekli söyledir:

Router(config)#**no access-list** erisim listesi no

Komut yazisilisindaki parametrelerin tanimi tabloda gösterilmektedir.

Parameter	Description
access-list-number	Number of an ACL. This is a decimal number from 1 to 99 (for a standard IP ACL).
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
source	Number of the network or host from which the packet is being sent. There are two ways to specify the *source*: ·Use a 32-bit quantity in four-part, dotted- decimal format. ·Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.55.
	(Optional) Wildcard bits to be applied to the source. There are two ways to specify the *source-wildcard*: ·Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.

11.2 Erisim Kontrol Listeleri (ACL)

11.2.2 Uzatilmis ACL' ler

Uzatilmis ACL' ler, genis bir kontrol araligi sagladigi için standart ACL' lerden daha sik kullanilirlar(1). Uzatilmis ACL' ler port numaralari ve protokolleri de kontrol edebilecegi gibi paketin kaynagini ve alici adresini kontrol eder. Bu, ACL' nin neyi kontrol edecegini tanimlama konusunda büyük bir esneklik saglar. Erisim izni ya da reddi verilen paketler, protokol tipi ve port adresinin yani sira, paketin nereden çiktigi ve nereye yollandigina dayalidir. Uzatilmis bir EKL, Fa0/0 dan özel bir S0/0 adresine yapilacak olan mail trafigine dosya transferi ve web tarayici reddi olma kosuyla izin verir. Paketler göz ardi edildiginde bazi protokoller göndericiye alici adresine ulasilamadigini bildiren bir yanki paket yollar.

Tek bir ACL için, birden çok bildirim düzenlenebilir.(2). Bu bildirimlerin her biri, bildirimi ayni ACL' ye ilintilendirmek için ayni erisim listesi numarasi içermelidir.Gerektigi ölçüde kosul bildirimlerinin sayisi artabilir, bu sayiyi sinirlayan sadece router in kullanilabilir bellegidir. Dogal olarak bildirimlerin artirilmasi ACL nin yönetimini ve anlasilmasini daha bir zorlastiracaktir.

```
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data
```

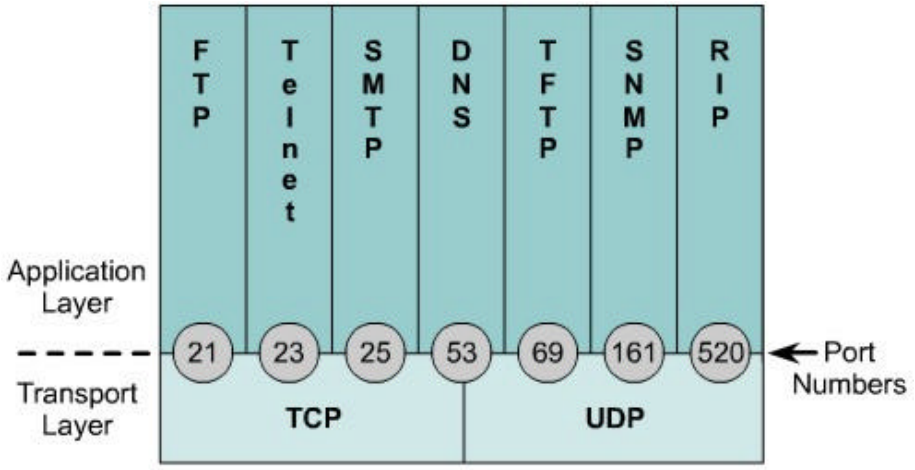
- Access list number range of 100-199
- Source destination IP address
- Layer 4 protocol number
- Applied to port closest to source host

Uzatilmis ACL bildirimleri için yazim formati oldukça uzun olabilir ve çogu kez terminal ekranini hepten kaplayabilir. Joker kartlar da komutlarda host ve anahtar sözcüklerinin kullaniminda seçenekler içerir

```
Router(config)#access-list access-list-number {permit | deny}
protocol source
[source-mask destination destination-mask operator operand]
[established]
```

Paramter	Description
access-list-number	Identifies the list using a number in the range 100 to 199.
permit | **deny**	Indicates whether this entry allows or blocks the specified address.
protocol	The protocol, such as IP, TCP, UDP, ICMP, GRE, or IGRP.
source and **destination**	Identifies source and destination addresses.
source-mask and *destination-mask*	Wildcard mask; zeros indicate positions that must match, ones indicate do not care positions.

Uzatilmis EKL bildiriminin sonunda, opsiyonel TCP ya da UDP port numaralarinin özellestigi bir alandan kazanilan ilave bir kesinlik vardir



TCP/IP için en iyi bilinen port numaralari çizimde gösterilmistir. (5). Uzatilmis ACL' nin özel protokollerde gerçeklestirecegi mantiksal islemler özellestirilebilir. Mesela, = (esittir) için (eq), not equal (esit degildir) için (neq), grater than (büyüktür) için (gt), less than (küçüktür) için (lt) gibi.... Uzatilmis ACL' ler 100 ile 199 araliginda bir erisim listesi numarasi kullanirlar. (Son dönem IOS larda bu 2000 den 2699 a kadardir)

ip access-group komutu mevcut bir EKL' yi bir arabirime baglar. Tek bir ACL' nin arabirim, yün, protokol itibariyla baglanacagini animsayin. Komutun yazilis formati söyledir(6):

Router(config-if)#**ip access-group** erisim listesi no {in/out}

11.2 Erisim Kontrol Listeleri (ACL)

11.2.3 Adlandirilmis ACL' ler

ACL' lerde verilmis IP, CISCO' nun standart ve uzatilmis ACL' lere sayi yerine isimler vermesine izin veren IOS 11.2 yazilimiyla ortaya çikti(1). Adlandirilmis bir erisim listesinin avantajlari sunlardir:

- EKL' yi karaktersel bir isim kullanarak sezgisel olarak tanimlamak
- Uzatilmis ACL' lerde 799 basitlerde 798 sinirini elimine etmek..
- Adlandirilmis ACL'ler , ACL' leri silmeksizin düzenleme ve yeniden konfigüre etme olanagi saglar. Ancak, adlandirilmis erisim listelerinin sadece liste sonuna eklenmis bildirimlerin silinmesine olanak verdigine dikkat edin. Adlandirilmis listeleri olusturmak için bir metin editörü kullanmak iyi fikirdir.(2)

Adlandirilmis ACL' leri tamamlamadan önce sunlari göz önünde bulundurun:

Adlandirilmis ACL'ler , Cisco IOS' un 11.2 sürümünden önceki sürümü ile uyumlu degildir.

Çoklu ACL'lerde ayni isim kullanilmamali. Örnegin, hem standart hem de uzatilmis ACL'nin ikisini de George olarak adlandiramazsiniz.

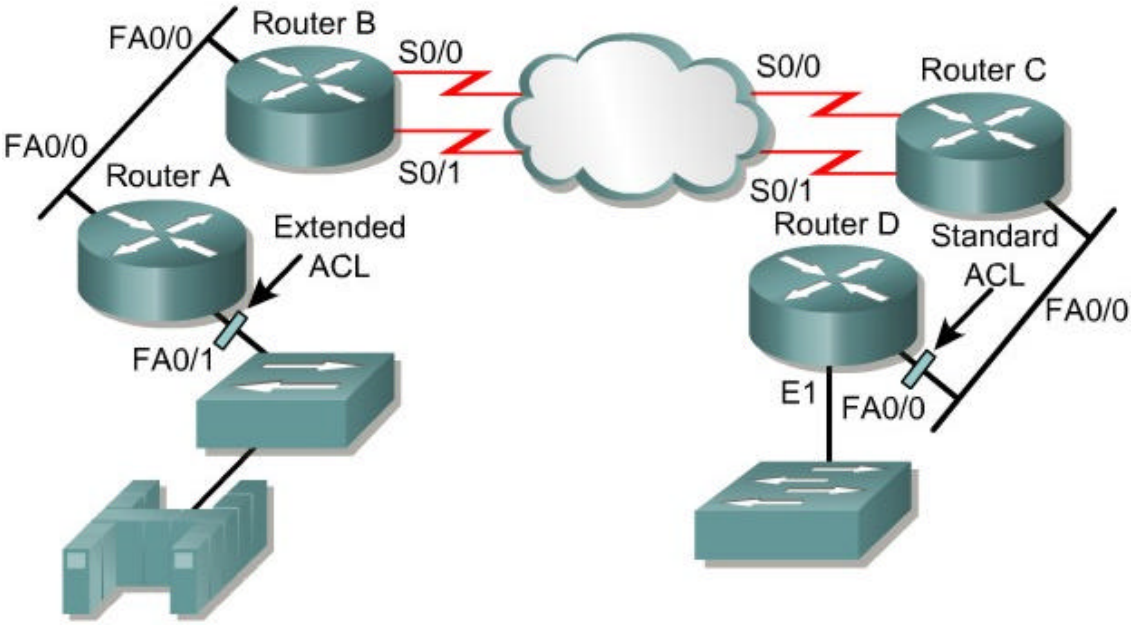
Avantajlarindan biraz önce söz edilen adlandirilmis erisim listelerinden haberdar olmak önemlidir. Adlandirilmis ACL ler gibi gelismis erisim listesi islemlerine CCNP anlatiminda yer verilecektir.

Adlandirilmis bir ACL ip **access-list** komutu ile olusturulur(3). Bu, kullaniciyi ACL içinde konfigürasyon moduna konumlandirir. ACL konfigürasyon modunda izin verilen ya da reddedilen bir ya da daha fazla kosul belirlenir(4). Bu ise, EKL bildirimlerinin eslesmesiyle paketin geççigini ya da düstügünü saptar.

Gösterilen konfigürasyon, internet filtresi adinda bir standart EKL ve " pazarlama_grubu " adinda uzatilmis bir EKL olusturur(5). Ayni zamanda gösterimde erisim listelerinin nasil adlandirilacagi ve bir arabirime nasil uygulanacagi da yer almaktadir.

11.2 Erisim Kontrol Listeleri (ACL)

11.2.4 ACL' lerin Konumlandirilmasi



ACL'ler, ag üzerindeki istenmeyen trafigi azaltmak ve paketleri filtrelemek suretiyle trafigi kontrol amaçli kullanilirlar. ACL' lerin uygulanisinda göz önünde bulundurulmasi gereken bir diger önemli nokta erisim listelerinin nerede konumlandirilacagidir. Eger erisim listeleri dogru yerde bulunursa sadece trafik filtrelenmekle kalmaz ayni zamanda tüm agin daha verimli çalismasi saglanir. Eger trafigin filtrelenmesi düsünülüyorsa, EKL ag performansinin artisinda en çok hangi noktada etki yapiyorsa oraya yerlestirilmelidir.

Isletme politikasinin amacinin D router i üzerindeki Fa/01 ag kartina bagli A router inin ag karti biriminden FTP ya da telnet trafigini engellemeye yönelik oldugunu düsünmek gerekir. Ayni zamanda diger trafige izin verilecektir. Bu politikayi farkli yaklasimlar tamamlar. Önerilen politika, hem kaynagi hem de alici adresini belirleyen uzatilmis EKL kullanilmasidir. Bu uzatilmis ACL' yi A router ine yerlestirin. Bu durumda A router inin ethernetindeki paketler kesismez, B ile C router inin seri arabirimi kesismez ve D router ina girilmez. Farkli kaynak ve alici adresi içeren trafige hala izin veriliyor olacaktir.

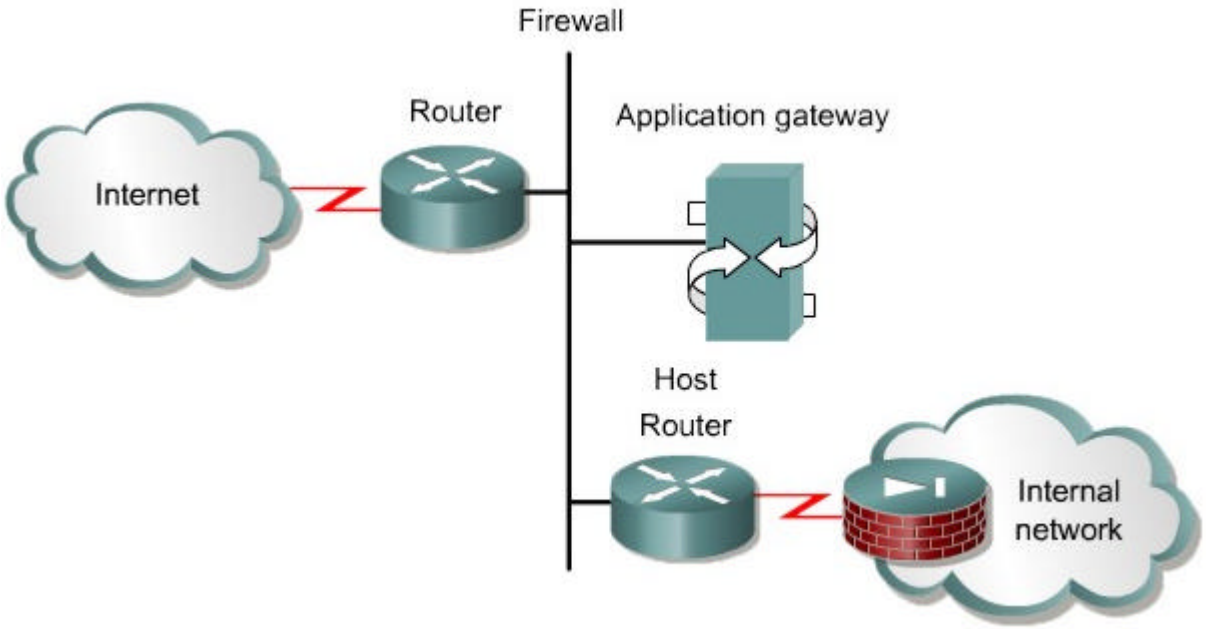
Genel kural, uzatilmis EKL' yi engellenecek trafik kaynagina mümkün oldugunca yakin yere koymaktir. Standart ACL' ler alici adresini belirlemez. Dolayisiyla mümkün oldugunca alici adresine yakin yerde olmalidir

Örnegin, A router indan gelen bir trafigi engellemek için standart bir EKL D router inin Fa0/0 i üzerinde konumlandirilmalidir.

Bir yönetici, bir aygit üzerine kontrol edebilecegi tek bir erisim listesi yerlestirebilir. Bu yüzden erisim listelerinin konumlari ag yöneticisinin kontrol yogunlugu olan noktalarda belirtilmelidir.

11.2 Erisim Kontrol Listeleri (ACL)

11.2.5 Güvenlik Duvarlari



Güvenlik duvari, kullanici ile dis dünya arasinda yer alan ve kullaniciyi davetsiz misafirlere karsi korumaya yönelik mimari bir yapidir. Çogu durumda, bu davetsiz misafirler global internetten ve uzak aglardan baglanan binlerce kisidir. Tipik olarak bir güvenlik duvari istenmeyen yasa disi girisleri engellemek için birlikte çalisan pek çok degisik makineyi içerir.

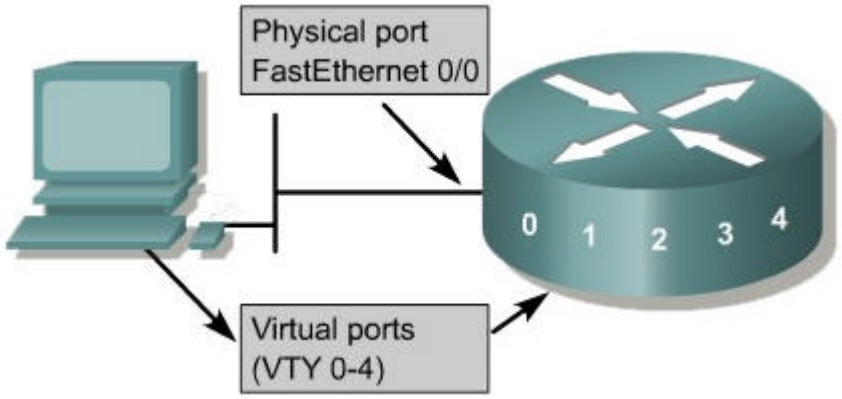
Bu mimaride, internete bagli olan router, gelen tüm trafigi ag geçidindeki uygulamaya yönlendirir. Dahili aga bagli olan router, yani iç router paketleri sadece ag geçidindeki uygulamadan kabul eder. Aslinda, ag geçidi hem gelen hem de dahili ag içindeki ag tabanli hizmetlerin dagitimini kontrol eder. Sözgelimi, sadece belli kullanicilarin internet yoluyla iletisim kurmasina izin verilir ya da iç ve dis hostlar arasinda baglantiyi kurmak için sadece belli uygulamalara izin verilir. Eger uygulama maile izin veriyor ise bu durumda sadece mail paketleri router a yollanir. Bu ise ag geçidi uygulamasini korur ve onun göz ardi ettigi paketlerle asiri yük altina girmesini engeller.

ACL' ler, internet gibi iç ag ile dis ag arasinda konumlandirilmis olan güvenlik duvari routerlarinda kullanilmalidir. Güvenlik duvari router i, bir izolasyon noktasi olusturur ve böylelikle duvarin gerisinde kalan iç ag yapisi hiç etkilenmez. ACL' ler , iç agin belli bir kismindan giren ya da çikan trafigi kontrol amaciyla agin iki kismi arasinda konumlandirilmis bir router üzerinde kullanilabilirler. Agin bitim noktasinda konumlandirilmis olan bir uç nokta router i üzerinde ACL nin yapilandirilmasi güvenlik yararlari sagmasi açisindan gereklidir. Bu, bir dis agdan ya da kontrolü düsük bir ag bölgesinden bir agin çok özel bir alanina yönelik trafikte temel bir güvenlik saglar. Bu uç nokta routerlari üzerinde, router arabiriminde konfigüre edilmis her bir ag protokolü için ACL' ler olusturulabilir.

11.2 Erisim Kontrol Listeleri (ACL)

11.2.6 Sanal Terminal Erisimlerinin Kisitlanmasi

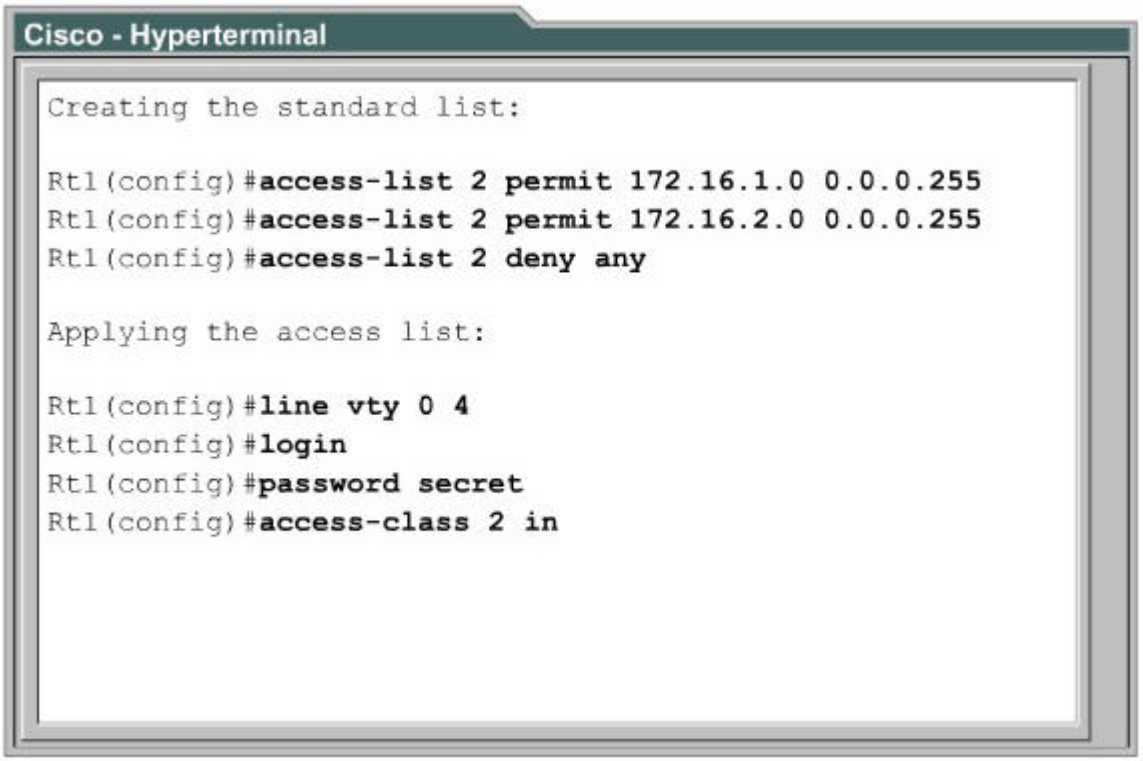
Standart ve uzatilmis erisim listeleri router da yol alan paketlere uygulanir(1). Onlar routerdan gelen paketleri bloklamak için tasarlanmamistir. Uzatilmis bir telnet çikis erisim listesi, telnet oturumunu baslatmis bir router i default olarak engellemez..



Router üzerinde Fa0/0 ve S0/0 gibi fiziksel portlar ya da arabirimler oldugu gibi sanal portlar da vardir. Bu sanal portlar vty hatlari olarak adlandirilir. Sekil 1' de gösterildigi gibi, 0 dan 4' e kadar numaralandirilan bes tür vty hatti vardir(1). Güvenlik önerisi olarak, kullanicilarin router a yönelik sanal terminal erisimlerine izin verilebilir ya da reddedilebilir, fakat routerdan alici adresine erisim reddedilmistir.

Vty erisiminin yasaklanmasi düsüncesi ag güvenligini artirir. Vty' ye erisim, router a fiziksel olmayan bir baglanti yapmak için telnet protokolünü kullanarak tamamlanir. Sonuç olarak, sadece bir vty erisim listesi tipi vardir. Kullanicinin hangi hattan baglandigini kontrol etmek mümkün olmadigindan tüm vty hatlarina tanimsal yasaklar yerlestirilmelidir.

Vty erisim listesi olusturma islemi bir arabirim için tarif edilenle aynidir. Bununla birlikte, EKL' yi bir terminal hattina baglamak **access-group** komutu yerine **access-class** komutunu gerektirir. 2



Vty hatlarinda erisim listelerini konfigüre ederken asagidakiler göz önünde bulundurulmalidir:

- Bir arabirime erisim kontrolünde isim ya da numara kullanilmis olmali.
- Sadece numaralandirilmis erisim listeleri sanal hatlara uygulanabilir.
- Sanal terminal hatlarina tanimsal yasaklar yerlestirilmeli, çünkü bir kullanici onlardan herhangi birine baglanmaya tesebbüs edebilir.

ÖZET

Asagidaki kilit noktalarinin anlasilmis olmasi saglanmalidir.

- ACL'ler router üzerinde güvenlik/ erisim islemlerini de içeren degisik fonksiyonlari yerine getirir.
- ACL' ler trafigi kontrol ve idare amaçli kullanilirlar.
- Bazi protokoller için bir arabirime iki EKL uygulanabilir: bir giris EKL ve bir çikis EKL gibi
- EKL ile paket ,eslendikten sonra routera erisim izin verilir yada reddedilir.
- Özel sembol (wildcard) maske bitleri ip adres bitlerine müdahale etmekte nasil 1 ve 0 ile kimliklendirilirler.
- Erisim listesi olustururken ve uygularken belirlenmis IOS gösterim komutlari kullanilir.
- Erisim kontrol listelerinin iki ana tipi standart ve genisletmelerdir.
- Erisim listeleri numaralari yerine isimlerin kullanilmasi için erisim kontrol listeleri isimlendirilir.
- Erisim kontrol listeleri tüm yönlendirme ag protokolleri için konfigüre edilebilir.
- Erisim kontrol listeleri , hizli verimli kontrollerin olmasi gereken yerlere yerlestirilmistir.
- ACL ler tipik olarak güvenlik routerlarinda kullanilirlar.
- Erisim listeleri routera olan sanal terminal erisimlerini sinirlandirabilirler.