T.C.

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

Bilgisayar Ağları

Ders Notu

Murat ÖZALP

BİLECİK

3 Ocak 2023

İÇİNDEKİLER

ŞEKİL LİSTESİ

TABLO LİSTESİ

TEŞEKKÜR

Bu çalışma, 2022 yılında BŞEÜ Bilgisayar Mühendisliği 4. sınıf öğrencilerinin önerisi üzerine başlatılmıştır. El yazısı ile yazılmış ve eski kalmış olan ders notlarının kolay güncellenmesi ve güncel tutulması amacını taşımaktadır.

Katkıda bulunanlar:

- Ibrahim Khalil Atteib Yacoub
- Aleyna Çelik
- Burhan Hoşlan
- Mahamat kabir Souleymane

1 GİRİŞ

...

2 OSI MODELİ (OSI KATMANLARI)

Bir bilgisayardan gönderilen bir bilginin diğer bilgisayara nasıl ulaştığını anlatmak için tasarlanmıştır. İletişimi 7 katmanlı mimarı ile tanımlar. Ağ elemanlarının nasıl çalıştığını ve verinin iletimi sırasında hangi işlemlerden gectiğini kavramak için kullanılan rehberdir. OSI Katmanlarının mantığını anlamak ağları planlamak, ağ üzerinden çalışan program yazmak ve ağ sorunlarını çözmek için önemlidir.

2.1 Katmanlar

1. Fiziksel (Physical)
2. Veri Bağı (Data link)
3. Ağ (IP)
4. Taşıma (Transport)
5. Oturum (Session)
6. Sunum (Presentation)
7. Uygulama (Application)

2.1.1 Fiziksel Katmanlar

Haberleşme kanalının elektriksel ve mekanik olarak tanımlandığı katmandır. Bir uçtan gönderilen sinyalin karşı uca iletilmesinden sorumludur. Sayısal haberleşmede en küçük birim bit olduğundan bu katmanın hızı **(bps) (b/s) bit/saniye** cinsindendir. Birinci katman donanımları:

1. Bakır ve fiber optik kablolar
2. RF (Antenler)
3. Sinyali(işareti) elektrik olarak yükselten ve çoklayan HUB cihazları
4. Kablosuz iletişimde kullanılan hava

2.1.2 Veri Bağı Katmanı

Verinin fiziksel ortamdan güvenli bir şekilde taşınmasından sorumlu olan katmandır. Kaynaktan çıkan verilerin(bitler) hedefe ulaşan verilerle aynı olup olmadığını sınayan sistemler kullanılır. En çok kullanılan hata bulma algoritmaları **eşlik biti (parity check)** ve **CRC algoritmasıdır**. Verinin doğru olup olmadığına bakmaz, sadece sağlamlığını kontrol eder. Bu katmanda üst katmandan gelen veriler çerçeve (frame) adı verilen paketleme işlemini tabi tutulur. Kapsülleme de denir. Birbirine doğrudan bağlı ağ cihazlarının aynı kapsülleme yöntemini (ikinci katman protokolünü) kullanması gerekir.

Kaynak	Veri	Hata Denetimi

Tablo 1: Kapsülleme

Günümüzde en yaygın ikinci katman protokolleri

Yerel ağda (LAN) : Ethernet

Uzak ağlarda (WAN) : AIM, PPP, Frame, Relay, Metroethernet

Anahtarlama

- **Devre Anahtarlama**: Veri aktarımı, fiziksel değişiklikle yapılır.
- **Paket Anahtarlama**: Veri aktarımı, her bir veri paketi için hesaplanarak, yazılımsal olarak yapılır.

Ethernet protokolünde kaynak ve hedef adresleri olarak MAC adresi (fiziksel adresi) kullanılır. Çakışmaları engellemek için aynı ağda iki MAC adresi olmamalıdır.

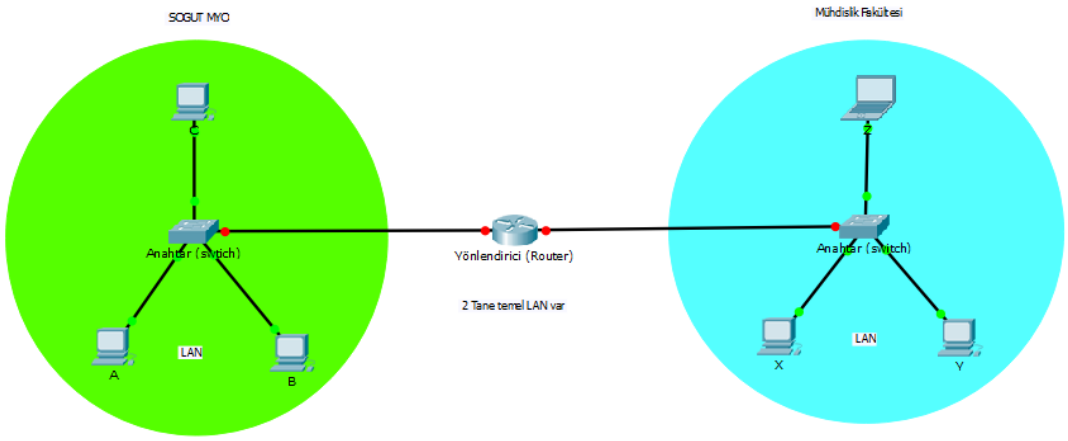
Anahtarlar (switch) bu katmanda çalışır. Anahtarlar portlarına bağlı olan cihazların MAC adreslerini bilmek zorundadır (otomatik öğrenir). Bu şekilde iki farklı portu arasındaki trafiği diğer cihazlar görmeden aktarabilirler. **HUB'lardan en önemli farkı budur**.

2.1.3 AĞ Katmanı (IP)

İnternet dünyanın farklı yerlerindeki ağlar üzerinden erişebilir kiler katman budur. Kaynak ve hedef olarak IP[1] adresi kullanılır. IP yönlendirilebilir bir protokol olduğundan her türlü veri aağı

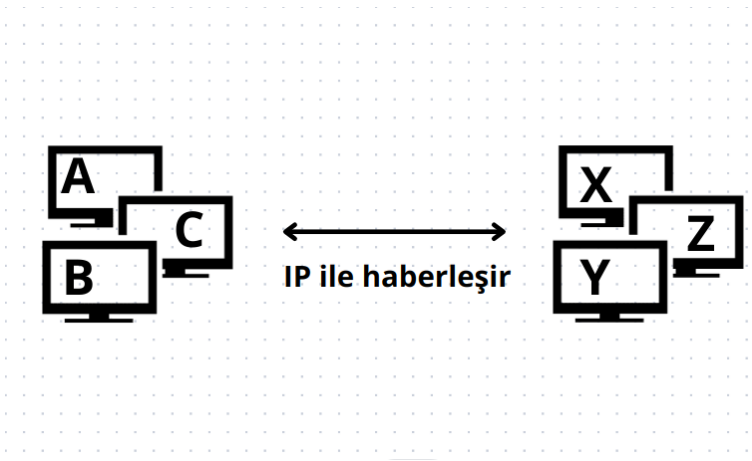
[1] IP => Internet Protocol

üzerinden haberleşmeye olarak sağlanır. Bu katman en önemli görevi yönlendirme işlemidir. Yönlendirme işlemi birden fazla ağ arayüzüne (network interface) sahip olan yönlendirici(router) adı verilen cihazlar tarafından yapılır. IP internetin temel protokolüdür. Yani bir PC internete bağlanacaksa IP'yi mutlaka biliyor olmalıdır. Bazı anahtarlar üçüncü katmanda da çalışabilmektedir.



Şekil 1: AĞ Katmanı

- **A,B,C** aynı ağdadır. Birbirleriyle MAC adresleriyle haberleşir (2. katman).
- **X,Y,Z** aynı ağdadır. Birbirleriyle MAC adresleriyle haberleşir (2. katman).



! **En küçük birimine paketleme denir.**

2.1.4 Taşıma Katmanı

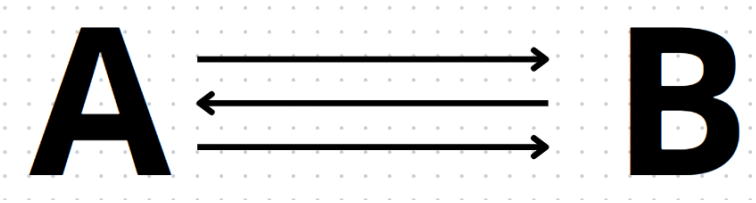
İnternette IP üzerinde kullanılan 2 tane 4. katman protokolü vardır. Bunlar **TCP** ve **UDP** dir. Bu katman uygulama programları için seri iletişim kanalları kuran katmandır. Bu kanallar port

adı verilen servis numaralarıyla kurulur.

TCP[2]: Bağlantı temelli bir protokoldür. Trafik başlamadan önce karşıdaki uca müsait olup olmadığı sorulur. Bu yönüyle telefon görüşmesine benzer.

UDP[3]: Bağlantı temelli değildir. Trafik doğrudan başlatıldığı için paketlerin iletimi garanti edilmez. SMS gönderimine benzetilebilir. Özellikle gerçek zamanlı görüntü ve ses taşıma uygulamalarında elverişlidir. **TCP**'ye göre daha **hızlıdır**.

Örnek: 3 way handshaking - 3 aşamalı el sıkışma Oturum açıldıktan sonra ilk olacak - Veri kaç



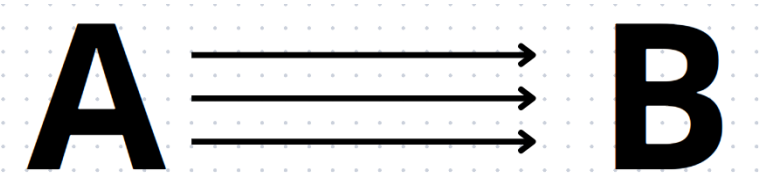
Şekil 2: TCP Protokolü

parçada gönderilecek

1GB filmi

80 segmentte ⇒ (1180 2180 .... 80/80) bunlar paketlenir.

TCP'de sadece yavaşlama olacak görürüz. En önemli avantajı budur.



Şekil 3: UDP Protokolü

UDP'nin avantajı hızlı **TCP**'ye göre. Dezavantajı ise güvensiz.

Örneğin: İnternetten radyo dinleyeceğiz bunu **UDP** ile dinlemek zorundayız, çünkü GB belli değil. **TCP**'de önemlidir.

Dördüncü katmanın bir başka görevi de üst katmanlardan gelen veriyi bölümleyerek daha küçük parçalara ayırmaktır. Bu parçalara **segment** denir.

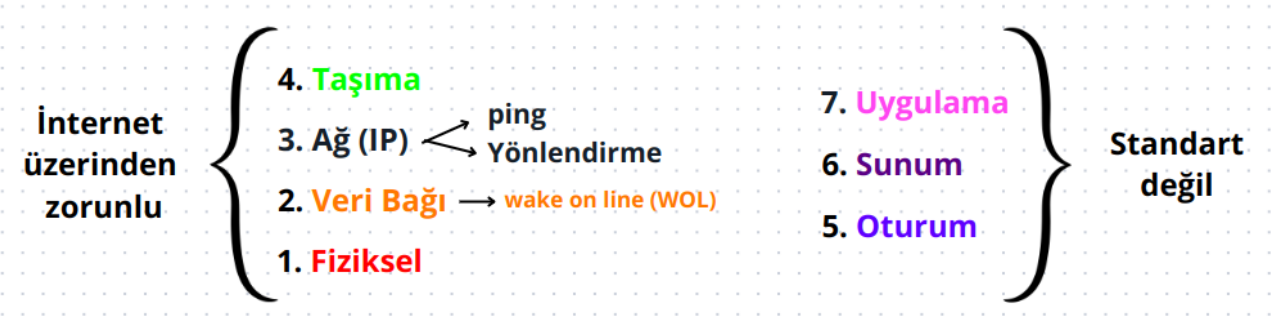
[2]TCP => Transmission Control Protocol
[3]UDP => User Datagram Protocol

TCP	UDP
Güvenli (oturum temelli)	Oturum yok
Yavaş	Hızlı

Tablo 2: TCP vs UDP

2.1.5 Uygulama Seviyesi Katmanlar

Aslında uygulama seviyesi sadece 7. katmandır. Ancak 5 ve 6 yaygın kullanılmadığından ve farklı uygulamalar arasında standart olmadığından bu derste üçüncu tek başlkta inceliyoruz. Uy-



gulama programları genellikle 7. katmanda ulaşmakta ve genellikle doğruden 4. katman ile iletişime geçmektedir.

TELNET: Ağlarda yönetim ve kontrol amaclı kullanılır. Ağ cihazlarının genellikle tamamı **telnet** ile yönetimi destekler. 2 cihaz arasında 4. katmanda bağlantı (erişebilirlik) kontrolü yapmak için **telnet** kullanılır.

** **Port tarama uygulamaları**

4. katmanda açık olan **TCP/UDP** portlarını tarar.

nmap: **TCP** yada **UDP**'ye kadar **0-65536**'ye kadar port taraması yapar.

OBS	**Uzak masaüstu**	**nmap -> OS dedikten**
Port tarama	TCP 3389	obs.bilecik.edu.tr
79.123.244.212 -> IP	79.123.244.212 start IP	cevaplar
TCP 80 open	79.123.244.212 end IP	tahmin

Tablo 3: Örnek

2.1.6 Aktarım Verimliliği

! Veri bloğu ne kadar büyürse, verim o kadar artar.

$$\text{Aktarım Verimliliği} = \frac{\text{Veri}}{\text{Veri + TCP/UDP + IP başlığı + Ethernet başlığı}}$$

MTU[4]: Maksimum veri miktarını belirler. Ethernet bağlarında MTU değeri varsayılan olarak **1500 byts/kapsül**

PPL[5]: Paketlerin Ağda sonsuz kadar dolaşmaması için geçen süredir.

PPL değeri genellikle **128**'dir.

! Paket noktalar arasında her aktarıldığında **PPL değeri azalır**.

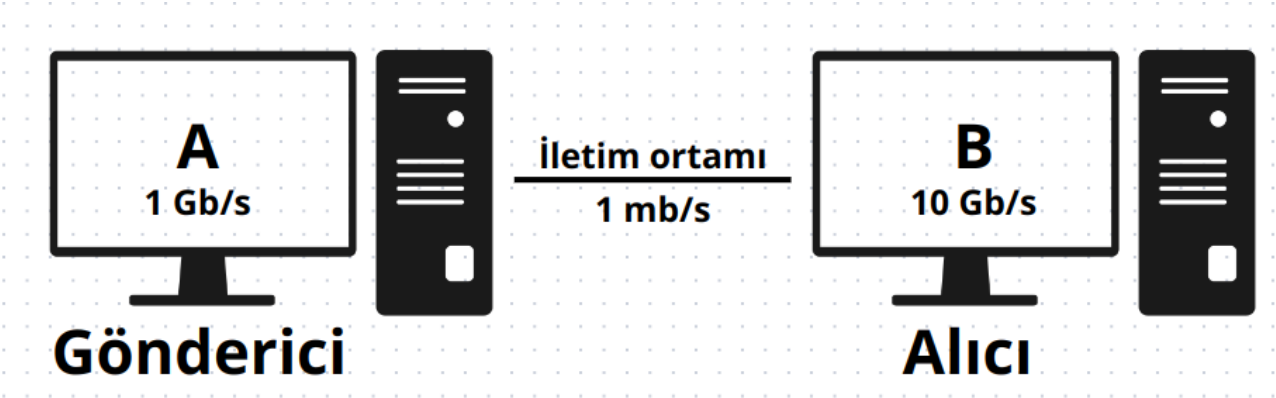
[4]MTU => Maximum Transmission Unit
[5]PPL => Time to Live (Yaşam süresi)

3 TEMEL KAVRAMLAR

3.1 Band Genişliği (Bandwidth)

Haberleşme kanalının veya iletim ortamının kapasitesini ifade etmek için kullanılır. Analog sinayallerde birini **hertz (hz)** iken digital sistemlerde **bps (b/s)**.
bir haberleşme sistemi, gönderirici, alıcı ve iletim ortamından oluşur. İletim kapasitesi en büyük olan bütün sistemin bant genişliği belirler.

Örnek:



Şekil 4: Bant Genişliği

Soru

1. 240 mb büyüklüğündeki bir MP3 dosyası bir sistemde 4dk'da aktarılıyor. Bu sistemin aktarım kapasitesini (bant genişliğini) bulunuz.
2. MP3 yerine MPG olsaydı ne olurdu?

Çözüm

Bw=?

1. 4dk 240 mb => saniyede 1mb = 8mb/s
2. Değişim olmaz...

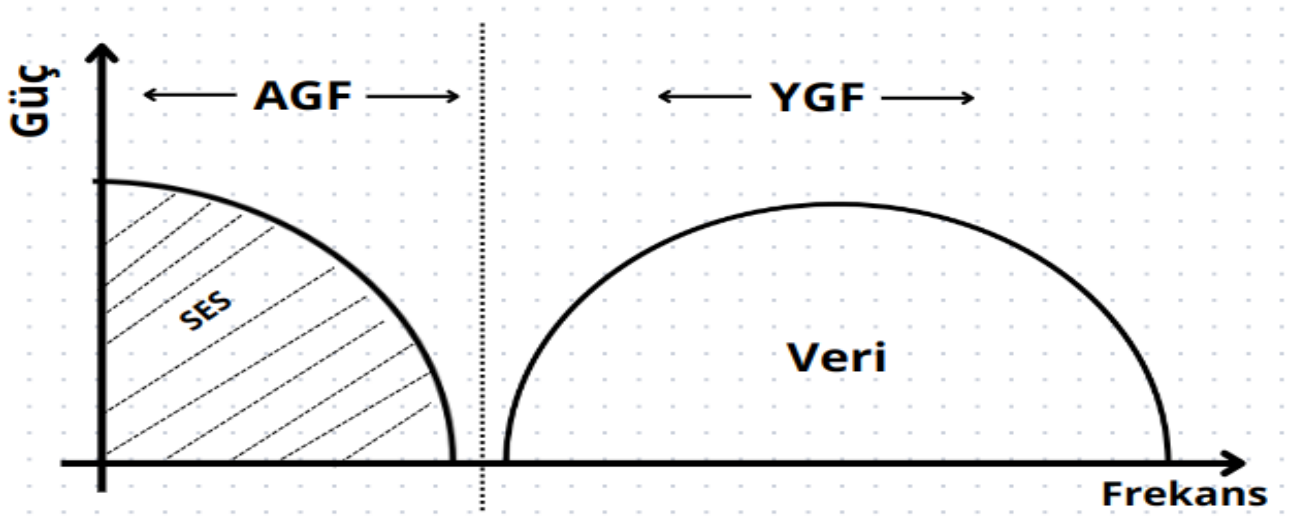
3.2 Temel Band (Base Band)

İletim ortamında tek bir frekans bandı kullanılır. Böylece teorik olarak iletim ortamının tüm kapasitesi tek bir kanal için kullanılır.

Örneğin: Ethernette bu band kullanır.

3.3 Geniş Band (Brood Band)

İletim ortamında birden fazla frekans bandı kullanılır. bulunur. Basit bir frekans band filtresi sayesinde kanallar ayrıştırılabilir. Telefon hattından aynı anda ses verinin taşınması buna örnektir.



3.4 Paralel ve Seri İletişim

Paralel iletişimde byte düzenyinde iletişim sağlanır. İki uç arasında en az 8 tane fiziksel iletim ortamı olmalıdır. Band genişliği teorik olarak 8 hat daha fazla olduğu düşünülebilir. Ancak hem maliyet hem protokol tercihi hem de kullanılan topoloji gibi ektenler bu konuda etkilidir.

3.5 Haberleşme Kanalı Modlari

a) **Simplex Kanal**: Televizyon ve radyo gibi yayının tek taraflı olarak yapıldığı kanallardır.

b) **Half-dubleks Kanal**: Çıft yönlu iletişim vardır. Ancak aynı anda sadece bir taraf veri gönderebilir. Örnek olarak **telsiz**.

c) **Full-dubleks Kanal**: İki uc arasında iki tane simplex kanal vardır. Böylece aynı anda iki taraf veri gönderebilir ve alabilir. Örnek telefon görüşmeleri.

! Günümüzde tüm bilgisayar ağları **Full-dubleks**'dir.

4 İLETİM ORTAMLARI

Temelde atmosfer ve kablo olmak üzere iki farklı iletim ortamı mevcuttur. Atmosferde RF (radyo frekans) dalgalarını kullanarak iletişim gerçekleşir. Kablolarda ise genellikle fiberoptik ve bakır kablo kullanılmaktadır.

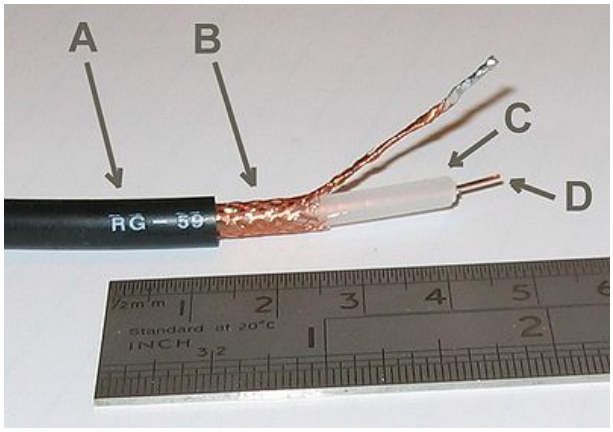
4.1 İKİ TELLİ BAKIR TELEFON HATTI

Telefon iletişimini sağlamak için tasarlanmıştır. Temel bant ve geniş bant internet hizmeti verilmektedir. Analog modülasyon teknikleriyle en fazla 56 k b/s'lik band genişliği sağlar. xDSL teknolojileriyle 25 Mb/s'lik bant genişliğine ulaşmaktadır.

Şekil 5: İki telli Bakir Kablo

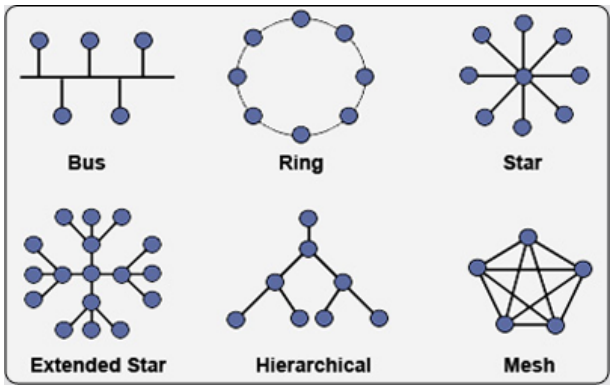
4.2 KOAKSİYEL (COAXIAL) KABLO

Genellikle elektriksel gürültünün yoğun olduğu şartlarda kullanılırdı.Yalıtkan bir tüpün içerisinde giden bir tel ve tüpün dışına sarılmış kafes şeklinde teller vardır. Yerel ağlarda (LAN) 180m'de(max) 10M b/s bant genişliği sağlar. Bu kullanımı 10 Base 2 olarak bilinir. Daha sonra 500 m mesafede çalıştırılacak hale getirilir. 10 Base 2 ismiyle standartlaştırılmıştır. 50 ohm'luk direnç değeri vardır. BNC tarzında konnektörler kullanılır. Günümüzde LAN'da hiç kullanılmamaktadır. Sebebi hem 10 Mb/s hızının çok düşük olması, hem de UTP kablolar kadar ekonomik ve işlevsel olmamasıdır. Bilgisayar ağlarında doğrusal (bus) topolojilerde kullanılmıştır.



Şekil 6: Koaksiyel Kablo

AĞ TOPOLOJİLERİ

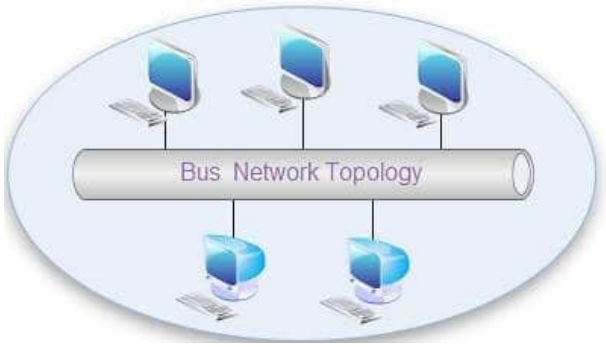


Şekil 7: Topolojiler

Ağ topolojileri nedir sorusunun en net cevabı, "bir ağı oluşturan cihazların fiziksel ve mantıksal yerleşimidir". Network Topology (Ağ Topolojisi) Yerel Ağ Alanı (LAN) içerisinde bulunan bilgisayarların fiziksel ve mantıksal yerleşimini ifade eder. Fiziksel Topoloji ağ içerisinde bulunan tüm cihazların birbirlerine nasıl bağlanacağını ve bağlantı için ne tür kablo kullanacağını belirtirken Mantıksal Topoloji bu cihazların nasıl haberleşeceğini belirtir ve bu cihazları ortak bir protokol altında birleştirir. Kullanılmak istenen Ağ Teknolojisine göre farklı ağ topolojileri kullanılmaktadır. Fiziksel Topolojinin 6 farklı çeşidi vardır. Bunlar Bus(Yol), Ring(Halka), Yıldız(Star), Ext Star(Gelişmiş Yıldız), Mesh(Örgü) ve Tree(Ağaç) topolojileridir. Broadcast(Yayın) ve Token Passing(İz) mantıksal topolojilere birer örnektir.

DOĞRUSAL (BUS) TOPOLOJİ

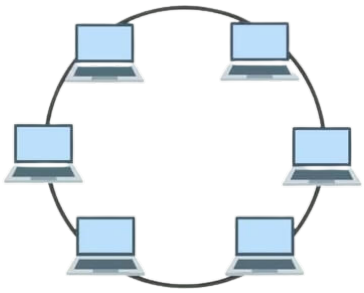
Doğrusal bir hat üzerinde bilgisayarların T konnektörlerle bağlanması şeklinde kurulur. Hattın her iki ucunda sonlandırıcı kullanmak zorunludur. Koaksiyel kablo kullanılır. Ağın herhangi bir noktasında arıza olması durumunda ağın tamamı çöker.Ağdaki veri trafiği tüm uçlara gider. Herkes herkesin trafiğini görebilir. Bu yüzden çok fazla **çakışma (colision)** olur.



Şekil 8: Bus Topolojisi

HALKA (RING) TOPOLOJİ

Doğrusal topolojiye benzer. Sonlandırıcı kullanılmaz. Hattın iki ucu birleşiktir. Hatta sanal bir jeton dolaşır(token).Jeton sırası gelen bilgisayar, jeton boş ise göndereceği veriyi hatta yerleştirir. Bilgisayarlar sırayla veri gönderdiklerinden çakışma daha azdır.Günümüzde hiç kullanılmamaktadır. Herkes herkesin verisini kullanabilmektedir.

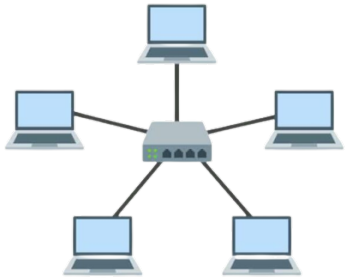


Şekil 9: Halka-Ring Topolojisi

YILDIZ (STAR) TOPOLOJİ

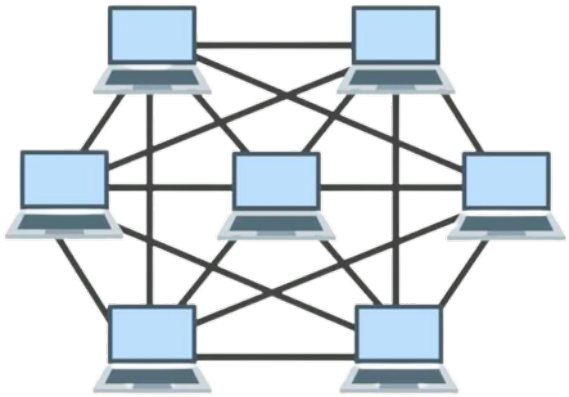
Merkezde dağıtıcı bir cihaz olur. Buradan tüm bilgisayarlara birer kablo gider. Ağın bir noktasındaki arıza sadece ilgili bilgisayarın ağ bağlantısına zarar verir. Genellikle (bükümlü çift (twisted

pair,xtp)) kullanılır. Trafiğin herkese mi gönderileceği ya da sadece ilgili uca mı gideceği dağıtıcıya bağlıdır. Dağıtıcının performansı ve kabiliyeti ağı doğrudan etkiler. Günümüzde en yaygın topolojidir.



Şekil 10: Yildiz-StarTopolojisi

ÖRGÜ (MESH)TOPOLOJİ

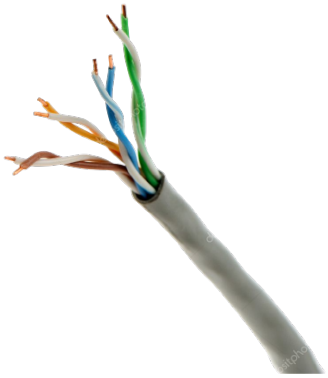


Şekil 11: Örgü-Mesh Topolojisi

Uçları arasında birden fazla rota üzerinde haberleşme imkanı olan yapılardır. Günümüzde genellikle farklı yıldız ağlar arasında yedekleme amacı olarak kullanılır.

4.3 BÜKÜMLÜ ÇİFT KABLO

İçerisinde 4 çift bakır kablo bulunur.Kabloların birbirleri üzerindeki direnç elektromanyetik etkisini azaltmak için ikişerli olarak sarılı durumundadırlar. Örneğin: UTP,CAT5,Ethernet Kablosu



Şekil 12: Bükümlü çift kablodan bir kesit

4.3.1 UTP (UNSHILDED TWISTED PAIR) Korumasız Bükümlü Çift

8 iletkenin her biri ince bir yalıtkan ile kaplanmıştır. En dışında tamamını kaplayan bir yalıtkan vardır.

4.3.2 STP(SHİLDED TWİSTED PAİR)

Her çiftin altında koruma (topraklama) vardır.

4.3.3 FTP(FOİLED TWİSTED PAİR)

4 çiftin tamamının etrafında folyo koruma vardır.

4.3.4 S/FTP

İkisinin de özelliğini taşımaktadır.

4.4 FREKANSLARINA GÖRE BÜKÜMLÜ ÇİFT KABLO

CAT:

CAT1-CAT3

Telefon hatlarında bulunur.

CAT5

En yaygın kullanılan ağ kablosudur. Azami 100m mesafe ve 10Mb/s destekler.

CAT6

100 m mesafede 1G b/s destekler.

10 BASE T Ethernet(Eth)

100 BASE T Fast Ethernet(Fa,Fe)

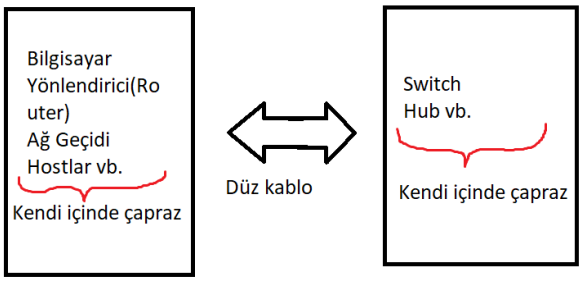
1000 BASE T Gigabit Ethernet(G,GE)

Bükümlü çift CAT5 VE CAT6 Kabloları sonlandırmak için RJ-45 adı verilen konnektörler kullanılır. Bu kablolar iki farklı iki şekilde sonlandırılabilir.**568-A,568-B**

Kablonun iki ucunun aynı standartlarla sonlandırılmasına **düz (Straight kablo)** denir. İki ucunda iki farklı standartta sonlandırılma yapılırsa **çapraz(cross-over)kablo** adı verilir.

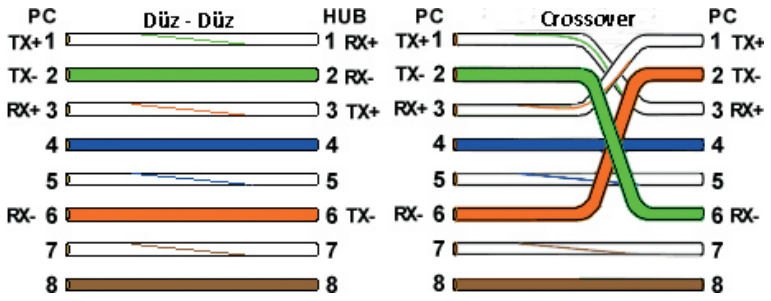
4.5 ÇAPRAZ VE DÜZ KABLO

Düz kablo, bir bilgisayarı yönlendirici gibi bir ağ hub'ına bağlamak için yerel alan ağlarında kullanılan bir tür bükümlü çift kablodur. Bu tür kablolara bazen yama kablosu da denir ve bir veya daha fazla bilgisayarın kablosuz bir sinyal yoluyla bir yönlendiriciye eriştiği kablosuz bağlantılara bir alternatiftir. Aynı türden iki cihazı bağlamak için genellikle bir çapraz kablo kullanılır. Düz kablo ve çapraz kablo tasarımları aynı standartların ve kuralların çoğunu kullanır.



Şekil 13: kablolar

Yeni ağ cihazlarının tamamı MDI/MDIX adı verilen teknoloji sayesinde karşıdaki cihazın ne tarz bir cihaz olduğunu anlar ve hangi iletkenin ne amaçla kullanılacağını buna göre düzenler. Diğerleri enerji göndermek için kullanılır.



Şekil 14: kablolar-örnek

FİBER OPTİK KABLOLAR

Fiber optik kablolar, veri göndermek için ışık sinyallerini kullanmaktadır. Bu kablolar elektrik kablolarına benzer. Ancak elektrik kablolarından farklı olarak ışığı taşımak için kullanılan minimum bir adet fiber optik içeren bir kablo çeşididir.

Fiber optik kablolar çeşitli özelliklere ve avantajlara sahiptirler. Fiber optik kablonun farklı alanlarda bu kadar sık tercih edilmesinin nedenleri kabloların bulundurduğu özellikler ve sunduğu bu avantajlardır.

Fiber Optik Avantajları

Elektrik parazitlerinden etkilenmez.

Sıcaklık değişimleri ve neme karşı dayanıklıdır.

Metalik kablolardan daha hafif ve daha küçüktürler.

Sinyal kaybı yok denecek kadar azdır ve sinyal güçlendirici ihtiyacını azaltır.

Sıcaklık değişimleri, su baskınları, şiddetli hava ve nem gibi çevresel parametrelere karşı dayanıklıdır.

Bu kablolarda iletim için ışığın yansımasını kullanılır. Böylelikle bu kablolar çok daha uzun mesafelere veri iletimi yapılabilirler. Elektromanyetik enerji sızması meydana gelmediği için bilgi güvenliği sağlanmış olur.

Bu kablolar ile bilginin ekonomik, verimli ve hızlı bir şekilde ulaştırılması sağlanır.

Fiber Optik Dezavantajları

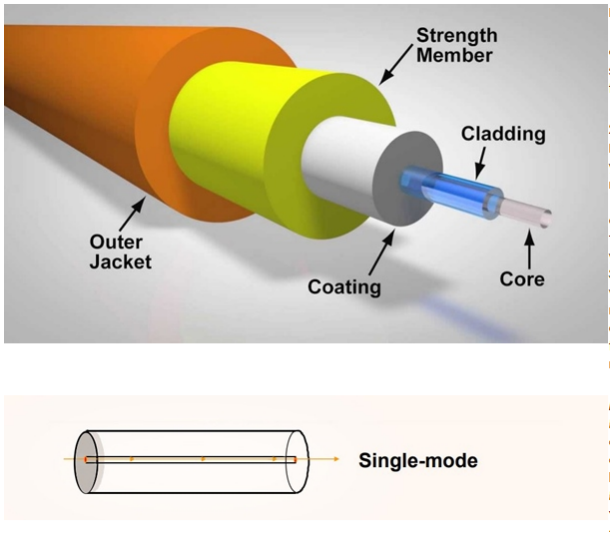
Sınırlı Uygulama — Fiber optik kablo sadece zeminde kullanılabilir ve zemini terk edemez veya mobil iletişim ile çalışamaz.

Düşük Güç — Işık yayan kaynaklar, düşük güçle sınırlıdır. Güç kaynağını iyileştirmek için yüksek güç yayıcıları bulunmasına rağmen, ek maliyet ekleyecektir.

Kırılganlık - Fiber optik, bakır tellere kıyasla daha kırılgandır ve hasara karşı daha hassastır. Fiber

optik kabloları bükmemeli veya bükmemelisiniz.

Mesafe — Verici ve alıcı arasındaki mesafe kısa olmalı veya sinyali arttırmak için tekrarlayıcılara ihtiyaç duyulmalıdır.



Şekil 15: fiberkablo

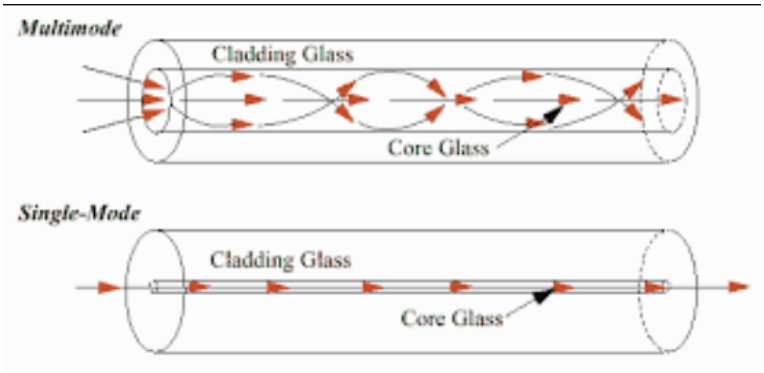
Veri optik dalgalar arıcılığı ile ışığın yansıma kurallarına göre elde edilir. Elektriksel sinyallerine göre mesafeye bağı zayıflama sinyalleri çok azdır. Bakır kablolarda olduğu gibi gerilim farkından kaynaklanan topraklama ihtiyacı yoktur. Fiberoptik kabloların yerel ağa bağlanmasında elektriksel sinyal ile optik dalgalar arasında çevrilmesi gerekir.Verici tarafından ışık kaynağı olarak lazer diyod(led),alıcı tarafında ise fotodiyod ya da foto transistör kullanılır.

4.6 FİBER OPTİK KABLO TÜRLERİ

Single mod(SM) ve Multi mod(MM) olmak üzere ikiye ayrılır

Multi-Mode

Bina ya da kampüs içi kısa mesafelerde tercih edilir.Optik dalga üretmek için Led kullanılır.Verici ve alıcı maliyetleri single moduna göre yarı yarıya azdır. **Single-Mode** Hem daha uzun mesafelerde hem de daha yüksek band genişliğine imkan sağlar. Optik dalga üretmek için LazerDiyod kullanılır.Bu nedenle verici ve alıcı donanım maliyetleri daha fazladır.



Şekil 16: single-multimode

FİBER OPTİK ÇEVİRİCİLER

*F/O CONVERTOR

*F/O TRANSREİVER (ALICI/VERİCİ)

*GBIC (Switch modülü halindedir)

*STP (Switch modülü halindedir)

YEREL AĞLAR (LAN)

Kablo çekebileceğimiz (bize ait olan) yerler yerel ağlardır. Ağlarda band genişliği ,protokol,topoloji gibi altarnetifler isteğe göre özelleştirilebilir. Günümüz yerel ağlarında ethernet harici protokol kullanılmamamktadır.

ETHERNET PROTOKOLÜ

İlk kez "INTEL VE XEROX" tarafından geliştirilmiştir.Daha sonra IEEE(Institue of Electrical and Electronical Enginner) tarafından 809.3 ismi ile standartlaştırılmıştır.

10 M b/s Ethernet Portları

10 Base 2 : 10 sayısı 10 m b/s'yi ifade eder.Base sözcüğü temel bandı ifade eder.En sondaki kablo türüdür.2 olduğunda ince (thin) kooksiyel kablodur.

10 Base 5 : Sondaki 5 Kalın(thick) kooksiyel kablo olduğunu belirtir.

10 Base T :Bükümlü çift kablo olduğunu ifade eder.

100 M b/s ETHERNET PORTLARI

100 Base Tx : Fast Ethernet Cat-5 kablo kullanılır.

100 Base Fx :F harfi Fiberoptik Kablo kullanıldığını belirtir.

1000 M b/s ETHERNET PORTLARI

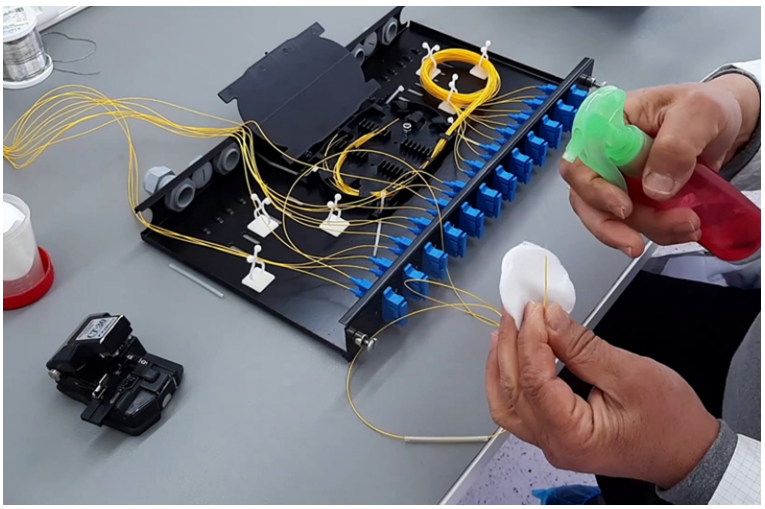
1000 Base-T : Cat5 ve Cat6 kablolar kullanılır.Ancak Cat6 tercih edilir.

1000 Base-Lx : L long kısaltmasıdır.SM,MM,FO kblolar kullanılır.Uzak mesafelerde tercih edilir.En önemli dezavantajı maliyetlerin SX'e göre fazla olmasıdır.

1000 Base-SX : Yalnızca mm FO kablolar kullanılır.Kısa mesafeleri destekler.Ekipmanları daha ucuzdur.

FİBEROPTİK SONLANDIRMA ŞEKİLLERİ

LC,SC,ST,FC sonlandırma mevcuttur.Günümüzde en yagın olan "LC" tipi sonlandırma şeklidir.



Şekil 17: fibersonlandırma

*F/O eki füzyon cihazı ile yapılır.2 tane cam tüpleri kaynatarak birbirine ekler.

İşlemler mikron seviyesinde yapıldığından kendi mikroskopu olan ve hassasiyeti yüksek olan cihazlar kullanılır.
F/O kablo testleri "OTDR" isimli cihaz ile yapılır.

MAC ADRESİ VE ADRES ÇÖZÜMLEME

Yerel ağlarda haberleşmeyi sağlayan ethernet çerçevesinde(frame) 48 bitlik adres kullanılır. MAC adresi 16'lık sayı sisteminde 12 tane karakter ile gösterilir.

16 bit $\rightarrow 2^4$ 0000
48 $\rightarrow$ 16 tane 2^4

İlk 6 karakterlik ilk 24 bit üretici kodunun son 6 karakter ise seri numarasını belirtir.Bir üretici aynı MAC adresiini birden fazla karar vermez.Dolyısıyla MAC adresleri dünyada tektir. * Birden fazla aynı MAC adresi aynı ağ üzerinde(LAN,VLAN vb) olmamalıdır.

Windows $\rightarrow$ CMD
$\rightarrow$ ipconfig
$\rightarrow$ getmac
Linux $\rightarrow$ ifconfig

Adres Çözümleme Ağdaki Bilgisayarlar başlangıçta diğer bilgisayarların mac adreslerini bilemez. MAC adreslerini öğrenmek için;

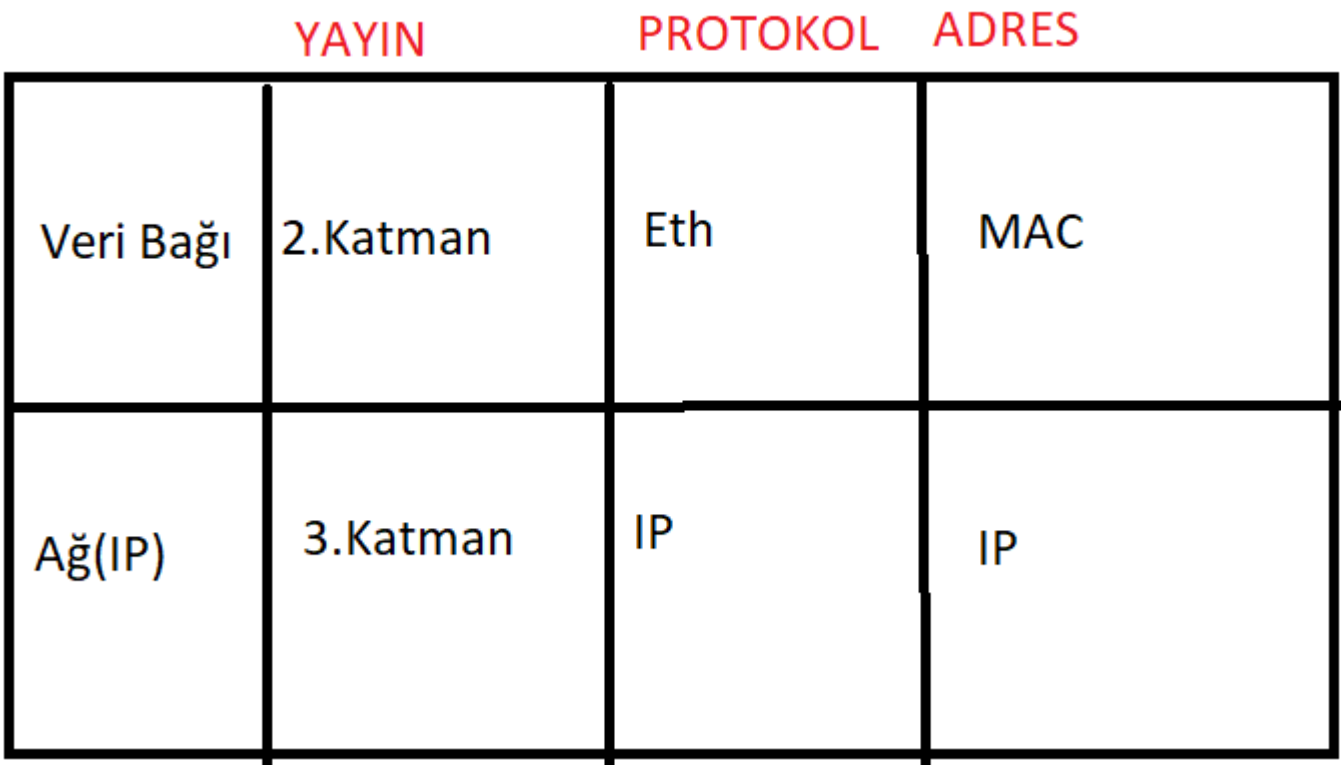
ARP(Adress Resulotion Protocol) (Adres Cözümleme Protokolü)

Bu protokol ikinci katmanda çalışır.Ağdaki Bilgisayarların MAC adreslerini öğrenmek ve bu cihazdaki ARP tablosunu güncellemek en temel görevdir.

SORU** ARP tablosunda;statik kayıt ne işe yarar? 1970 de bilgisayar ağları tasarlanırken gelişimi hakkında kesin bilgi olmadığında statik(önü açık) bırakılmıştır.

YAYIN ADRESİ(BROADCAST ADDRESS)

Tüm yerel ağı temsil eden tek bir adrestir .Bu adrese gönderilen paket ağdaki tüm cihalara aynı anda uaştırılır.İkinci veya üçüncü katmanda yayın mesajı gelir.Yayın mesajlarında ne gibi fark vardır?



Şekil 18: fibersonlandırma

İkinci katmanda yayın adresi göndermek için çerçevedeki hedef mac adresindeki kısmında tüm bitler 1 yapılır. Dolayısıyla hedef adresi FF:FF:FF:FF:FF:FF yapılır.Ağa yeni bağlanan her cihaz kendi mac ve IP adreslerini içeren bir yayın mesajı gönderir. Her bilgisayarda ve anahtarda aynı ağdaki cihazlarla tutulan IP ve MAC adreslerinin tablosuna "ARP TABLOSU" denir. ARP Tablosu dinamik olarak güncellenir,ancak istenirse elle düzenleme ya da statik kayıt işlemi yapılabilir.

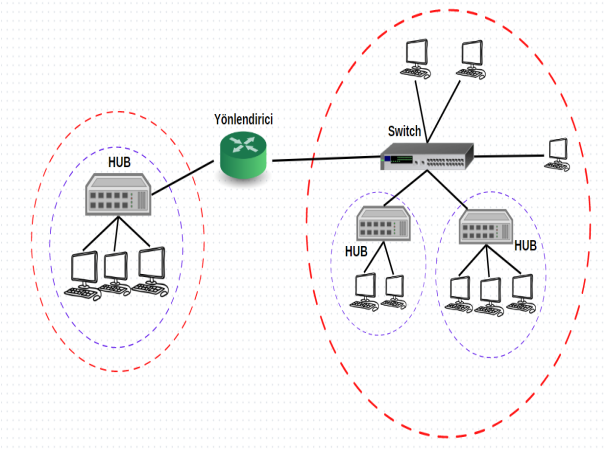
YAYIN ALANI

Bilgisayarların doğrudan mac adresleriyle haberleştikleri alandır.Bir yayın paketi gönderildiğinde bunu alabilen tüm cihazlar aynı yayın alanındadır. Bir bilgisayr kendi yayın alanında olmayan başka bir bilgisayarla haberleşmek için "ağ geçidinden" geçmek zorundadır.

ÇARPIŞMA ALANI

Bir yayın alanı içerisinde bir veya birden fazla çarpışma alanı bulunur.Aynı çarpışma alanındaki bilgisayarlar birbirine gelen her paketi görürler,ancak sadece kendi mac adreslerine gelen her paketi görürler. Çarpışma alanı aynı anda bir pc tarafından kullanılabilir.

İki PC aynı anda paket göndermek isterse çarpışma(collision) oluşur.Adını burdan alır.



Şekil 19: Soru1

1)Kaç tane yayın alanı vardır? 2

2)Kaç tane çarpışma alanı vardır? 3

3)Her çarpışma alanında kaç tane bilgisayar vardır?

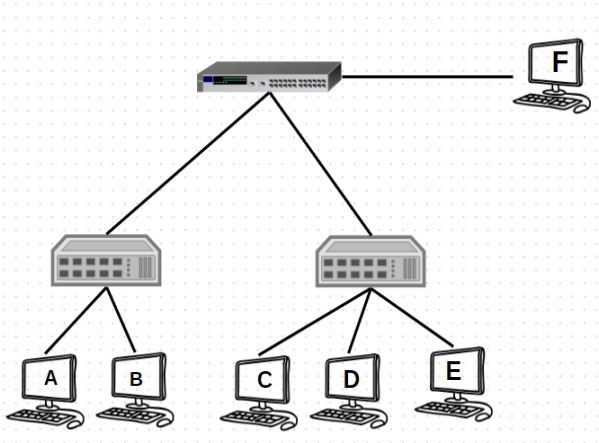
4)Her yayın alanında kaç tane bilgisayar vardır?

Birinci yayın alanında 3 tane

İkinci yayın alanında 8 tane

*YAYIN ALANI:mecburen ağ geçidi kullanılır.

*ÇARPIŞMA ALANI:Birbirlerinin verisini görecekler.



Şekil 20: Soru2

A ile B aynı anda paket gönderebilir mi? Yaçarpışma olur ya da sıra

B ile C aynı anda paket gönderebilir mi?

B ile C aynı Pc gönderirse olur,ancak farklı olursa aralarındaki topolojileri bilmediğimiz için bilemeyiz.

C yayın mesajı gönderdiğinde tüm pc'lere gider mi?

Evet tüm Pclere gider.

B ile C aynı arasındaki trafiği F görür mü?

Normal zamanda göremez.Ancak örneğin aynalama gibi işlemerde görebilir.

Anahtar üzerinde pc'lerin haricinde dış dünya ile iletişim kurmak için bağlantı yapılan porta "upink" poru denir. Anahtarın bilgisayara bağlanan normal portlarına(bakır portlara 45 port) "giriş portu" denir.Genel olarak 100mb/s-1000mb/s olurken "uplink portları" genellikle daha kapasiteli olur. Anahtarları birbirinden ayıran bir diğer özellikte "demir gücü kapasitesi"anahtarın aynı anda çevirebileceği trafik miktarına "switchfabric" ya da "through put"denir.

AĞ GEÇİTLERİ(GATEWAY)

Önceden bahsedildği gibi anahtarlar çarpışma alanına geçemezler.Bu nedenle kablolara göre daha fazla tercih edilir. Ancak anahtarlar da yayın trafiğini geçebilirer.Bünyesinde çok fazla anahtar bulunan yerel ağlar,yayın paketlerin çokluğu ağı hantallaştırır.Bu nedenle LAN'ları birbirinden çok alt ağa bölmek performansı arttıracaktır. **Örnek Yayın Mesajları**

*IPV4 İIPV6 mesajları

*Komşuluk mesajları

*Donanım keşif mesajları

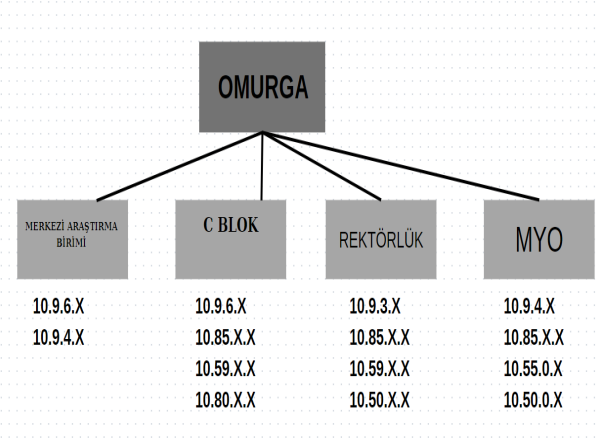
*Ip alma (DHCP)mesajları

*Virüs gibi kötü yazılımlar

Alt Ağa Bölmenin temel olarak iki yolu vardır

Klasik Yöntem (Fiziksel Ağ Geçidi Kullanma)

Klasik yöntemde herbir ağ için bir ağ geçidi kullanılması zorunludr.Dolayısıyla ciihazların,bağlantıları ve topolojilerin sınırları en önemli kısıtlardır.Bir vlan yapısında ise fiziksel bir müdahale olmadan hatta uzaktan bağlanarak ağ istenilen şekilde özelleştirilebilir. **Sanal Ağlar(VLAN)**
yönlendirici,Kablosuz Ap,Güvenlik Duvarı,PC vb.



Şekil 21: VLAN

Aynı ağ her yerde kullanılabiliyor.
Geleneksel yapıda ağları birbirinden ayrılması için ağ geçidi kullanılır
Bir anahtarda çok sayıda ağ(VLAN) kullanabiliyoruz.

SANAL AĞ(VLAN)KULLANMANIN AVANTAJLARI

a) **Ağları Bölerek**: Her bir ağdaki pc sayısını azaltarak yayın alanını daraltmak ve performansı azaltmak

b) **Esneklik**: Farklı coğrafyadaki bilgisayarlar aynı vlanda oabilir ya da aynı anahtar üzerinde birden fazla farklı vlan olabilir.

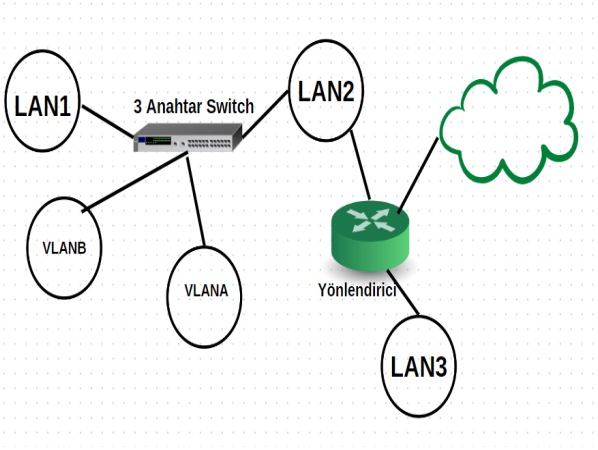
c) **Güvenlik**: Birbirine erişimi kısıtlamaması gereken ağlar arasında erişim denetim listeleri(Access Control List(ACL)) oluşturularak erişim kısıtlanabilir.

d) **İşletme Kolaylığı**: Ağlar küçük olduğunda sorunu çözmek kolaylaşır.Yani ağ eklemek ve mevcut ağları düzenlemek kolaylaşır.Ağ isimleri,IP grupları ve kullanım yerleri eşleştirilerek hiye-

rarşik sistemler oluşturulabilir.

Ağ geçidi tanımı yönlendirme,prptokol çevirme veya güvenlik uygulaması gibi işlemleri yapan tüm cihazları kapsar.Sıradan bir PC ,3.katman(L3) anahtar,yönlendirici veya özel üretilmiş donanım olabilir.

Ağ geçitleri üzerindeki ağ arayüzüne(interface) bağlı olarak ethernet,Frame Relay,ATM,PPPoE gibi protokollerin hepsinin kullanılabilme özelliğine sahip olduğundan bazı kaynaklardan protokol çevirici olarak adlandırılır.



Şekil 22: LAN-VLAN

VLAN ANAHTARLAR

Üzerinde sanal ağlar tanımlanabilen anahtarlardır.Sıradan anahtarlarda üstün olmasının en önemli sebebi ayarlanabilir olmasıdır. Bu nedenle yönetilebilir anahtarlar da denmektedir.Vlan anahtarın üzerindeki portlar gruplandırılarak birden çok sanal ağ oluşturulabilir.Her bir sanal anahtar ayrı bir ağ gibi çalıştırılabilir.Bu sanal ağlara "VLAN" denir.Her bir vlan'ın kendine özel Vlan Id isminde bir tanımlayıcı numarası olur. Anahtarları fizikse portları Vlan ID'leri ile eşleştirilerek ağlar düzenlenir.Aynı vlan numrasına sahip portlar aynı sanal ağa aittir.

Bazı durumlarda VLAN yapılandırılması portlardan ve fiziksel bağlantılardan bağımsız olarak yapılabilir.Örneğin pc'nin MAC adreslerine göre ya da kullanıcı kimlik doğrulama yöntemine göre (parola,parmak izi) Vlan ataması yapılabilir.

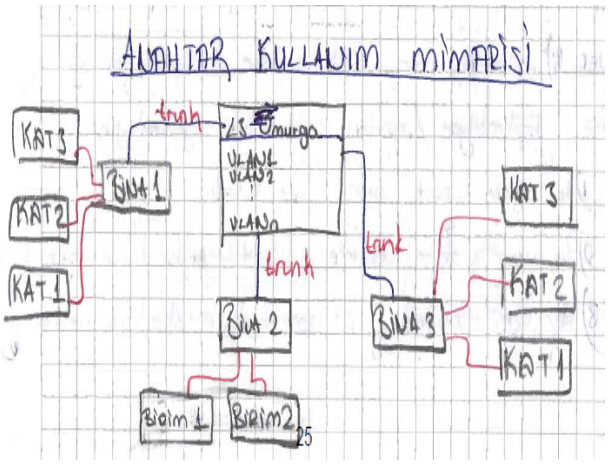
Vlan anahtarlar kullanıldığında birden fazla sanal ağı oluştururusa bu alt ağlar arasında trafiğin yönlendirilmesi gerekmektedr.Bu yönlendirme işlemi anhtarın kendi üzerinde veya ayrı bir yönlendirici

cihazla yapmak mümkündür.

Anahtar üzerinde yönlendirme yapılacaksa 3 katmanda(L3) çakıştırılacak bir anahtar kullanılmalıdır.

trunk: Anahtarın herhangi bir portundan birden fazla VLAN taşınması gerekiyorsa o port trunk olarak yapılandırılmalı.Bu bağlantıya da "trunk" denir.

ANAHTAR KULLANIM MİMARİSİ



Şekil 23: Anahtar-Kullanım-Mimarisi

1)OMURGA(CORE)

Üçüncü katman veya daha üstü anahtar kullanılır.Genellikle tüm Vlanlar burda oluşturulur.Ağın tüm yönlendirme yükü bunun üzerindedir.Bu nedenle genellikle yedekli kullanıır.Performansı çok fazladır.Binalar arası bağlantıyı sağlamak için kullanılır.Bu nedenle çok sayıda fiberoptik port sergiler.Modüler yapıdadırlar,yani port sayıları ve türleri modüler halinde takılıp çıkartılabilir.Modülerin takıldığı yere "şase" denir.Fiziksel olarak çok yer kaplarlar ve pahalıdırlar.

2)Dağıtım(Distrubution)Katmanı

Omurga anahtarında bağlı olan ve binaların içerisinde küçük bir omurga gibi düşünebileceğimiz anahtarlardır.Omurga anahtarına göre daha ucuzdur.L2 veya L3 olabilir.

3)KENAR Son kullanıcı cihazlarının bağlandığı anahtarlardır.Bu nedenle özel görevleri olabilir.

İhtiyaca göre :

802.1x(Kimlik Doğrulama)

PoE(802.3aaf) Enerji göndermek için kullanılır.

Captive Portal

Örnek:20 portlu bir VLAN anahtar 4 portlu bir ağ geçidine bağlanabiliyorAşağıdaki durumları yorumlayınız.

1)Her portun port sayısı 5'er tanedir.

Böyle bir zorunluluk yoktu.

2)Bir valan anahtar üzerine doğrudan bağlanacak PC sayısı 16'dır

16 tane de olabilir daha fazla da olabilir.

3)Her vlana atanmış portlar ardışık olmak zorundadır

Öyle bir şey yok.Esneklik özelliği vardır .

5 IP ADRESİ VE HESAPLAMALARI

32 bit uzunluğa sahip olan IP adresi 2 temel bileşene sahiptir.

1. Ağ tanımlayıcı
2. Host tanımlayıcı

NOT : Bir ağ içerisinde IP atanabilen ve kendisinin ağa bağlanma ihtiyacı olan bilgisayar, yönlendirici, güvenlik duvarı vb. cihazların tümüne host denir.

IP adresinin bu iki bileşeni hesaplanırken alt ağ maskesine ihtiyaç duyulur. Temel olarak alt ağ maskesi IP adresinin sınıfına göre belirlenir. IP adresleri 32 bitin sekizerli olarak gruplandırılması ve decimal olarak gösterilmesi şeklinde olur. Bu 8 bitlik grupların her birine oktet denir. Her oktet birbirinden nokta ile ayrılır.

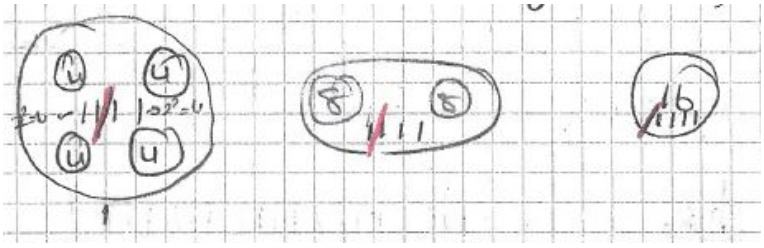
ÖRNEK :

00001010.	00000000.	00000001.	10000000
10.	0.	1.	128
Her sekizerli			
grup bir oktet			

Bir IP adresinin bağlı olduğu sınıf ilk oktetinden anlaşılır.

00001010.00000000.00000001.	10000000
ağ tanımlayıcısı	host tanımlayıcısı
24 bit ile 2^{24} tane ağ tanımlanabilir	8 bit ile $2^8 = 256$ tane ağ tanımlanabilir

ÖRNEK : 16 tane IP adresini bölüyoruz. (2^4 bit)



NOT : Ağlardaki bilgisayar sayıları(kullanılabilecek ip sayıları) belirlenirken maksimum kapasite 2'nin kuvveti 2^n alınarak belirlenir.

ÖRNEK : Bir şirketin iki farklı şubesinde 120 ve 280 adet bilgisayar kullanılmaktadır. Bu şirketler için optimal ağ büyüklüklerini hesaplayınız.

$120 => 2^n = 2^7 => 128$

$280 => 2^n = 2^9 => 512$

NOT : Host tanımlayıcısı kısmında belirtilen bitlerde elde edilebilecek en büyük sayı o ağda kullanılabilecek IP adresi sayısıdır. Her ağın ilk IP adresi "ağ adresi" ve son IP adresi "yayın adresi" olarak kullanıldığından her ağda kullanılabilecek host sayısı IP sayısından 2 eksiktir.

Host bitleri : n tane

Ağdaki IP adresi : 2^n tane

Ağda kullanılabilecek host sayısı $2^n - 2$

ÖRNEK : 10.9.8.0 IP adresinin 30. bitten sonrasının bulunduğunu varsayalım. Alt ağ IP adresinin kullanım amacına göre yazalım.

....

30 bit 2bit

IP sayısı $2^2 = 4$ tane Host sayısı $2^2 - 2 = 2$ tane

1.IP adresi 10.9.8.0 -> Ağ adresi

2. ve 3. IP adresi 10.9.8.1 ve 10.9.8.2 -> Hostlar için kullanılabilir

4. IP adresi 10.9.8.3 -> Yayın adresi

NOT :

Ağ sayısı	Host sayısı	Toplam host sayısı
1	16	14
2	8	$2(8-2) = 12$
4	4	$4(4-2) = 8$

5.1 IP Sınıfları

IP'nin ilk tasarlandığı sıralarda ortaya çıkmış bir kavramdır. Kurumlarda IP adresleri tahsis edilirken ihtiyaca göre optimal sayıda verebilmek için tasarlanmıştır. En büyük IP sınıfı A sınıfı, en küçük IP sınıfı C sınıfıdır.

A sınıfı : İlk biti(MSB) 0 olan IP adresleridir.

01111111.11111111.11111111.11111111

127 255 255 255

İlk oktet 0-127 arasında olur. Varsayılan ap maskesi 255.0.0.0'dır. A sınıfı bir IP adresinde 2^{24} tane IP oluşturulabilir.

B sınıfı İlk iki biti 1.0 şeklindedir. Ondalık formda ilk okteti 128 ve 191 arasındaki adreslerdir. Varsayılan alt ağ maskesi 255.255.0.0'dır. B sınıfı bir IP adresinde 2^{16} tane IP oluşturulabilir.

C sınıfı İlk üç biti 1.1.0 şeklindedir. Ondalık formda ilk okteti 192 ve 223 arasındaki adreslerdir. Varsayılan alt ağ maskesi 255.255.255.0'dır. B sınıfı bir IP adresinde 2^8 tane IP oluşturulabilir.

D sınıfı İlk dört biti 1.1.1.0'dır. Ondalık formda ilk okteti 224-239 arasındadır. Multicast(Çoklu yayın) olarak bilinir. Normalde hostlarda kullanılmaz.

E sınıfı 240-248 ile başlar. Deneysel amaçlar için rezerve edilmiştir. Normalde hostlarda ve ağlarda kullanılmaz.

A sınıfı	0-127	
B sınıfı	128-191	
C sınıfı	192-223	
D sınıfı	224.0.0.0	Kullanmıyoruz
E sınıfı	255.0.0.0	Kullanmıyoruz

Peki neden böyle bir sınıflandırma yapıldı?

Ağ biti	Host bitleri	Her ağdaki IP sayısı
8	24->A sınıfı	2^{24} tane IP
16	16->B sınıfı	2^{16} tane IP
24	8->C sınıfı	2^8 tane IP

ÖRNEK : 132.x.x.x IP adresi B sınıfıdır. 132.45.x.x IP adresinin ilk iki okteti ağ tanımlayıcısı son iki oktet host tanımlayıcısıdır. 2^16 tane IP alabilir.

112.x.x.x IP adresi A sınıfıdır. 2^{24} tane IP alabilir.

193.140.253.x IP adresi C sınıfıdır. 2^8 tane IP alabilir.

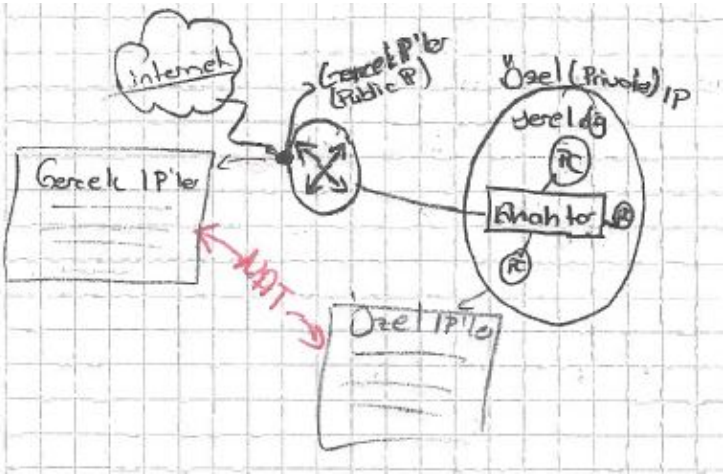
5.2 Özel IP Adresleri(Private IP Blocks)

İnternette kullanılmayan IP adresleridir. İnternet üzerinde hiçbir yönlendirici tarafından yönlendirilmeyen IP adresleridir. Bu adreslerin kullanım amacı test uygulamaları ve NAT uygulamaları gibi durumlardır. IP adresleri tükendiğinden kurumlarda kullanılan bilgisayarların tamamına yetmemektedir. Bu nedenle günümüzde kurumların iç ağlarında özel IP adresleri istenilen sayıda kullanılabilir.

- 10.0.0.0/8 ->2^{24} IP adresi

- 172.16.0.0 ->2^{20} IP adresi
- 192.168.0.0 ->2^{16} IP adresi

NAT(Network Address Translation)



5.3 Ağ Maskesi(Netmask)

IP adreslerinin bitlerden oluştuğunu ve iki bileşeni olduğunu biliyoruz. Bu iki bileşenin hangi bitten ayrılacağını bulmak için ağ maskesi kullanılır. Ağ maskesi herhangi bir IP adresi ile ikilik sistemde çarpılırsa(ve işlemi) çıkan sonuç ağın adresini verir.

ÖRNEK :

IP : 192.168.1.75

Ağ maskesi : 255.255.255.0

11000000.10101000.00000001.01001011

11111111.11111111.11111111.00000000

11000000.10101000.00000001.00000000

Ağ adresi 192.168.1.0

5.4 CIDR Notasyonu

Elimizde sadece IP adresleri olduğunda ağla ilgili yeterli bilgiye ulaşamadığımızı, ilave olarak IP adresinin hangi bitten bölündüğünü bilmemiz gerektiğini biliyoruz. Bunun için ağ maskesine alternatif olarak CIDR Notasyonu kullanılmaktadır. Bu gösterim şeklinde IP adresinin sağına "/" işareti konulup bölünen bit numarası yazılır.

ÖRNEK :

192.168.1.75 IP adresli ve 255.255.255.0 ağ maskesine sahip bir cihazın CIDR notasyonu 192.168.1.75/24 şeklindedir.

10.1.0.0 ve 255.0.0.0 ise 10.1.0.0/8 olarak gösterilir.

10.9.8.0 ve 255.255.255.128 ise 10.9.8.0/25 şeklinde gösterilir. (128 ikilik tabanda 10000000 şeklinde gösterildiğinden soldan 25 tane 0 vardır.)

5.5 Alt Ağa Bölme

IP adresi ve ağı temsil eden bit sayısı belirli olan bir ağ birden fazla küçük ağlara bölünebilir. Alt ağa bölme işlemi alt ağ maskesinde bir bit kaydırılarak yapılır. Bu şekilde 2^n tane alt ağ bölme işlemi yapılabilir.

ÖRNEK :

a) 10.0.0.0/24 ağını iki ayrı ağa bölünüz.

b)Yeni oluşturulan ağlar için 10.0.0.100 ve 10.0.0.150 IP adreslerinin aynı ağda olup olmadıklarını hesaplayın. (İpucu : Ağ adresi = IP x Ağ maskesi)

c)128 IP'li ağların her birini ikiye bölünüz.

Çözüm :

a)

Ağ : 10.0.0.0/24

Ağ maskesi : 255.255.255.0 (24 tane 1, 8 tane 0 var. 2^8 tane IP var)

Ağ maskesi : 11111111.11111111.11111111.00000000 ağ maskesinde 1 bit sağa kaydırdığımızda 25 tane 1, 7 tane 0 olacaktır. $2^7 = 128$ tane IP elde edilir.

1 bit kayarsa $2^1 = 2$ alt ağ, 2 bit kayarsa $2^2 = 4$ alt ağ, . . . ,n bit kayarsa 2^n alt ağ elde edilebilir.

10.0.0.0/25 notasyonuna sahip bir ağda 1.alt ağ 10.0.0.0 IP adresiyle başlar. 128 adet IP tanımlanır. Son IP 10.0.0.127 olur. 2. alt ağ ise 10.0.0.128 IP adresinden 10.0.0.255 IP adresine kadar 128 adet IP alabilir.

	Ağ adresi	Yayın adresi	Ağ maskesi	IP sayısı	Host sayısı
1.ağ	10.0.0.0/25	10.0.0.127	255.255.255.128	128	126
2.ağ	10.0.0.128/25	10.0.0.255	255.255.255.128	128	126

b)

	00001001.00000000.00000000.01100100	=	10.0.0.100
ağ maskesi:	11111111.11111111.11111111.00000000	=	10.0.0.128
	00001001.00000000.00000000.10010110	=	10.0.0.150

Son oktetleri farklı olacağından aynı ağda değillerdir.

c)

1.ağ	2.ağ
10.0.0.0/25	10.0.0.128/25

Ağ maskesi 255.255.255.128

1111111.11111111.11111111.10000000

Yeni oluşan ağ maskesi 255.255.255.192

1.ağ	10.0.0.0 ->ağ	
	10.0.0.63 ->yayın	
2.ağ	10.0.0.64 ->ağ	
	10.0.0.127 ->yayın	
3.ağ	10.0.0.128 ->ağ	
	10.0.0.191 ->yayın	
4.ağ	10.0.0.192 ->ağ	
	10.0.0.255 ->yayın	

SORU : 10.9.6.0/25 ağını 4 ayrı ağa bölünüz.

Ağ maskesi 255.255.255.0 11111111.11111111.11111111.0

Yeni ağ maskesi : 11111111.11111111.11111111.11100000 ($2^5 = 32$ IP var.)

: 255.255.255.224

10.0.0.0	10.0.0.64
10.0.0.31	10.0.0.127

10.0.0.32	10.0.0.128
10.0.0.63	10.0.0.191

ÖRNEK : 10.0.0.0/22'yi 4 alt ağa bölünüz.

11111111.11111111.11111100.00000000 $2^{10} = 1024$ tane IP var.

Ağ maskesi : 255.255.252.0

Yeni alt ağ maskesi : 255.255.255.0(2 bit kaydı.$2^8 = 256$ IP var.)

Yeni CIDR gösterimi -> 10.0.0.0/24 olmalıdır.

10.0.0.0 -> 10.0.0.255

10.0.1.0 -> 10.0.1.255

10.0.2.0 -> 10.0.2.255

10.0.3.0 -> 10.0.3.255

ÖRNEK : /17 şeklinde gösterilen ağın maskesi nedir?

11111111.11111111.10000000.00000000 = 255.255.128.0 şeklindedir.

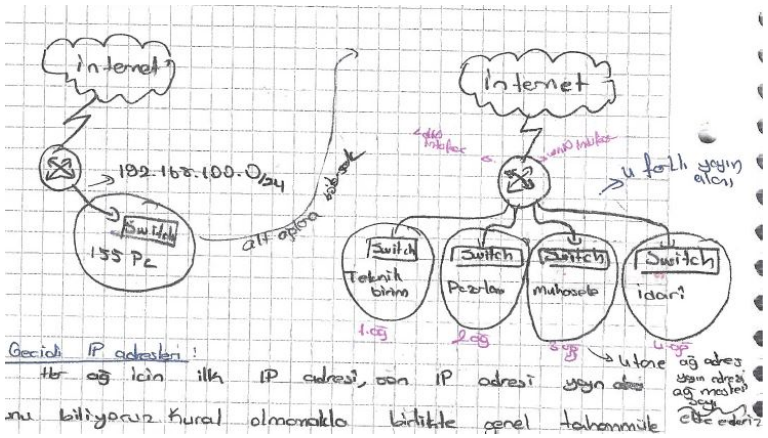
ÖRNEK : 10.10.0.0 ve 255.255.0.0 şeklindeki ağda kaç host olabilir?

$2^{16} - 2$ adet host olabilir.

NOT : Özel IP ile ??? 127 ile başlayan IP ler kullanılamazlar. Localhost : 127.0.0.1 bilgisayarın kendisini temsil eder.

169.254.0.0 Windows işletim sisteminin IP alınamadığında kendi IP bloğundan otomatik olarak verdiği IP adresidir.

ÖRNEK : Bir şirkete 192.168.100.0/24 şeklinde IP aralığı tahsis edilmiştir. Şekilde sistem yöneticisi ağdaki aşırı yayın trafiğinin sorun çıkardığını düşünerek ağı alt ağlara bölmek istiyor. Birimlerin PC sayısı aşağıdaki gibidir. Teknik birim=70, Pazarlama=40, Muhasebe=20, İdari birim=25



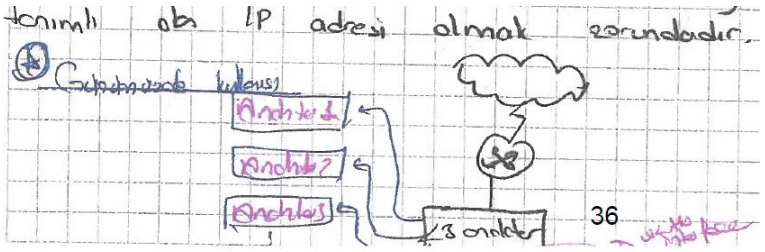
5.6 Ağ Geçidi IP Adresleri

Her ağ için ilk IP adresi ağ adresi, son IP adresi yayın adresi olduğunu biliyoruz. Kural olmamakla birlikte genel teamüllere göre ağ adresinden sonraki ilk IP adresi(kullanılabilecek ilk host adresi) ağ geçidi olarak belirlenir. Herhangi bir host adresi ağ geçidi olarak belirlensede hiçbir problem olmaz.

NOT : IP adresinin ve ağın son IP adresi değiştirilemez.

NOT : Ağ geçidi IP adresi herbir ağın doğrudan bağlı olduğu yönlendirici arayüzünde(interface, ara birim, ethernet kartı, NIC(Network Interface Card)) tanımlı olan IP adresi olmak zorundadır.

Günümüzde kullanılışı :



Soruya gelirsek :

128 Teknik Birim	64 Pazarlama	
	32 Muhasebe	32 İdari birim

Ağ adresi : 192.168.0.0

Yayın adresi : 192.168.100.127

Teknik	192.168.100.0(Ağ adresi) 192.168.100.127(Yayın adresi)
Pazarlama	192.168.100.128 192.168.100.191
Muhasebe	192.168.100.192 192.168.100.223
İdari birim	192.168.100.224 192.168.100.255

Alt ağ maskesi ise teknik:255.255.255.0,

pazarlama:255.255.255.192,

muhasebe:255.255.255.224,

idari:255.255.255.255 ??? şeklindedir.

ÖRNEK : 10.50.100.200/25 şeklinde IP adresi tahsis edilmiş bir bilgisayarın ağ adresi ve yayın

adresi nedir?

32-25=7 olduğundan $2^7 = 128$ tane IP var.

	10.50.100.200	
x	255.255.255.128	
	10.50.100.128	ağ adresi
	10.50.100.255	yayın adresi

ÖRNEK : Aşağıdaki bilgisayarlardan hangileri ağ geçidine ihtiyaç duymadan haberleşirler.

		Ağ adresi	
a)	10.0.0.120/25	10.0.0.0	-128
b)	10.0.0.121/24	10.0.0.0	-256
c)	10.0.0.254/24	10.0.0.0	-256
d)	10.0.0.1/24	10.0.0.0	-256
e)	10.0.0.253/25	10.0.0.0	-128

NOT : X'in Y ile aynı ağda olup olmadığını anlamak için X bilgisayarı Y nin IP adresiyle kendi ağ maskesini çarpar. Kendi ağ adresiyle karşılaştırır.

A'nın B ile haberleşmesi :

B'nin IP adresi		10.0.0.121
A'nın ağ maskesi	x	10.0.0.128
		10.0.0.0

Çıkan sonuç A'nın ağ adresiyle aynı olduğundan haberleşirler.

A'nın C ile haberleşmesi :

C'nin IP adresi		10.0.0.254
A'nın ağ maskesi	x	10.0.0.128
		10.0.0.128

Çıkan sonuç A'nın ağ adresiyle aynı olmadığından haberleşemezler.

6 IP YÖNLENDİRME

...

7 BİLGİSAYAR AĞLARI MODELLEME

Bu başlıkta simülatör ve emülatör kavramları açıklanmaya çalışılıp örnek uygulamalar verilecektir.

7.1 Simülatör & Emülatör

Bilgisayar üzerinde bir ağı modellemek için; simülatör ve emülatör şeklinde iki tür program kullanılmaktadır:

Simülatör: Gerçek ortamdaki sistemler ile (çok benzese de) birebir aynı şekilde çalışmaz. Uçuş simülatörleri buna örnek gösterilebilir. Gerçek sistemlerde kullanılan donanımların üzerindeki yazılımlar bunda kullanılmaz, simülatörlerde kullanılan sanal cihazlarda özel geliştirilmiş ve kısıtlı yazılımlar çalışır. Ayrık zamanda çalışır: gerçek hayatta binlerce saat sürecek bir işlem 1 saniyede yapılabilir; gerçek hayatta 1ms içerisinde biten bir eylem saniyelerce sürecek şekilde yavaşlatılabilir.

Emülatör: Gerçek cihazlarda kullanılan yazılımlar doğrudan burada da çalıştırılır. Virtualbox üzerinde Windows çalıştırmak için, gerçek Windows kurulumu yaptığımızı hatırlayın. Donanımlar sanallaştırılır ama donanımlar üzerinde gerçek yazılımlar (işletim sistemleri) kullanılır. Gerçek zamanda çalışır.

Simülatör ve emülatör kavramlarını bilgisayar ağları konusu özelinde özetlemeye çalışalım.

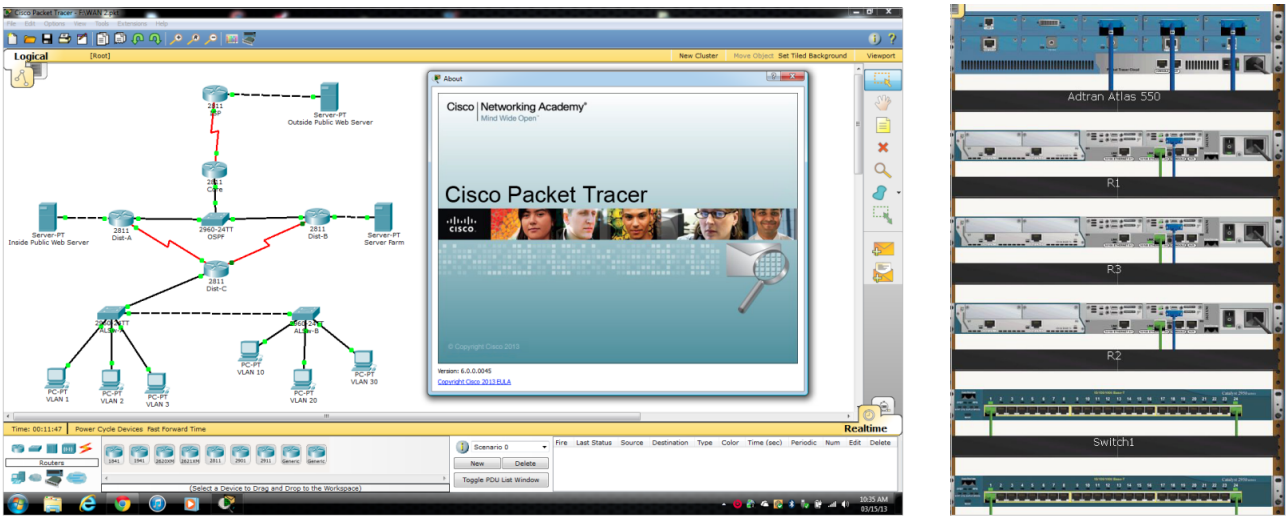
İnternet'in ortak dilinin IP olması gibi, bilgisayar ağlarında ortak donanım da Cisco firmasının ürünleridir. Pazara erken girmiş olması, ürünlerinin kaliteli olması, geniş ürün yelpazesi olması, bol miktarda dokümanı olması, kullanıcı sayısının çok olması, vb. nedenlerle bilgisayar ağları çalışan hemen herkes Cisco cihazlara hakim olmaktadır. Bu nedenle, ağ modelleme programlarında öncelikle Cisco cihazlara (yönlendirici, anahtar, vb.) destek sağlanmaktadır.

Emülatör uygulamalarında, *-simülatörlerden farklı olarak-* gerçek Cisco işletim sistemi kullanılması gerekmektedir. Gerçek işletim sistemi kullanıldığı için, gerçek cihazlarla yapılan fiziksel ağ uygulamalarına çok yakın bir çalışma ortamı sağlamaktadır. Bunun en büyük dezavantajı ise Cisco işletim sistemleri ücretli olduğu için ilave maliyet çıkarmasıdır. Diğer taraftan; bu işletim sistemlerinin İnternet'in yeraltı dünyasında yaygınlaşması gibi illegal durumlara da sebebiyet vermektedir.

7.2 Ağ Modelleme Platformları (Ücretsiz Olanlar)

7.2.1 Cisco Packet Tracer

Cisco firması tarafından geliştirilmektedir. Cisco'nun Networking Academy adı altında vermiş olduğu eğitimlerde katılımcılara verilmektedir. Bunun haricinde satışı bulunmamaktadır. Simülatör tarzında bir uygulamadır.



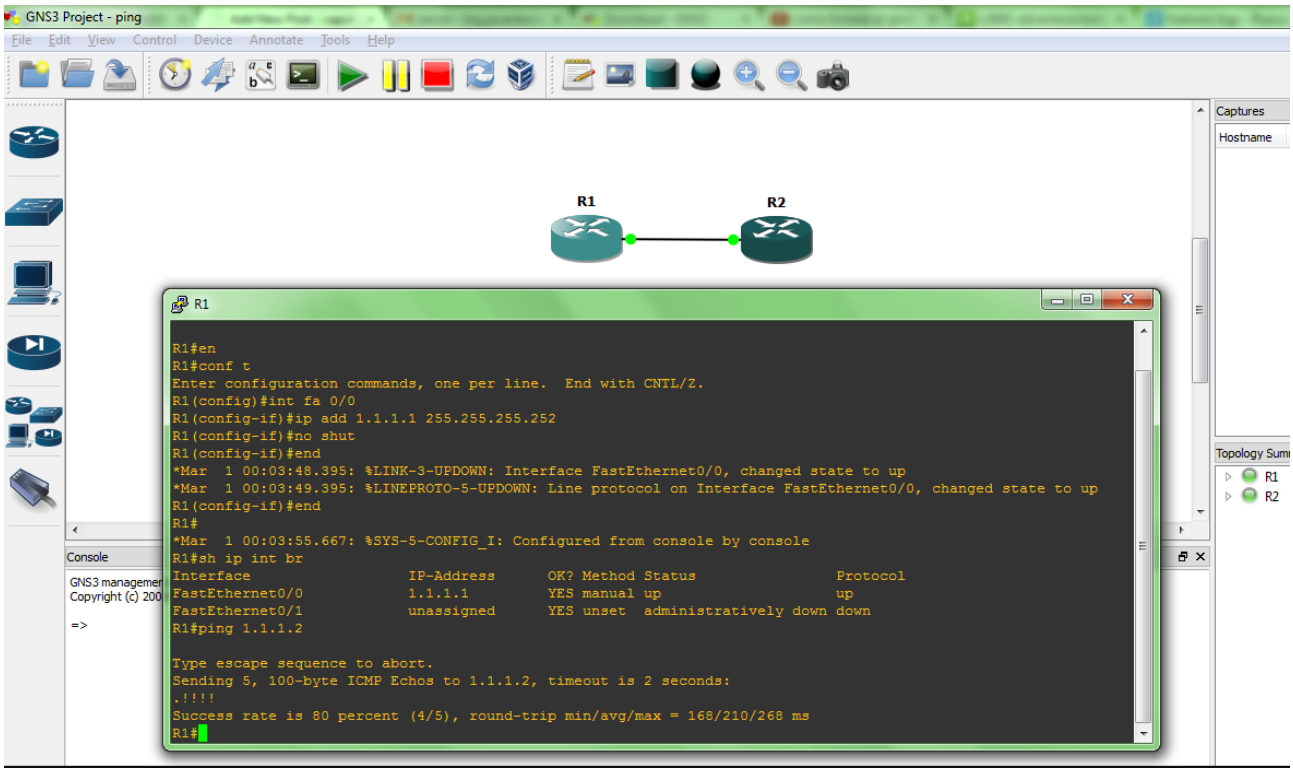
Şekil 24: Cisco Packet Tracer arayüzü. Sol tarafta "mantıksal", sağ tarafta "fiziksel" görünüm

Kataloğunda Sadece Cisco firmasına ait ürünler bulunmaktadır. Yönlendirici, anahtar, kablosuz erişim noktası, IP telefon sistemler, vb. farklı türde ürünler kullanılabilmektedir. Linux ve Windows sürümleri bulunmaktadır. Program kurulduğunda, ilave bir işlem yapmaya gerek kalmadan tüm özellikleri ile aktif halde olmaktadır. Program içerisinde oluşturulan sanal cihazların gerçek hayat ile bağlantısı yapılamamaktadır. Sadece klasik bilgisayar ağları değil, üst katmanlarda da uygulama gerçekleştirilebilmektedir. Sanal sunucu cihazı üzerinden HTTP, DNS, e-posta sunucuları gibi servisler de simüle edilebilmektedir.

7.2.2 GNS3 (Graphical Network Simulator 3)

Cisco'nun kendi cihazları için tasarladığı IOS isimli işletim sistemlerini kullanır. Bu IOS'lerden GNS3 içerisine en az 1 tane dahil edilmelidir. Bu IOS'leri elde etmek için yasal bir yol malesef bulunmamaktadır. Cisco müşterisi olanlar WEB üzerinden indirebilmektedir. Bunun haricinde satışı bulunmamaktadır. VirtualBox PC'leri bunun içine dahil edilebilmektedir. Gerçek yönlendirici imajları ve gerçek sanal bilgisayarlar kullandığından oldukça gerçekçi bir çalışma ortamı sağlamaktadır. Cisco

sertifikasyon sınavlarına hazırlananlar için de kullanışlıdır. Programın önemli bir özelliği de sanal ağda kullanılan sanal makinaların Host-PC (fiziksel bilgisayar) üzerinden internet'e çıkabilmesidir.

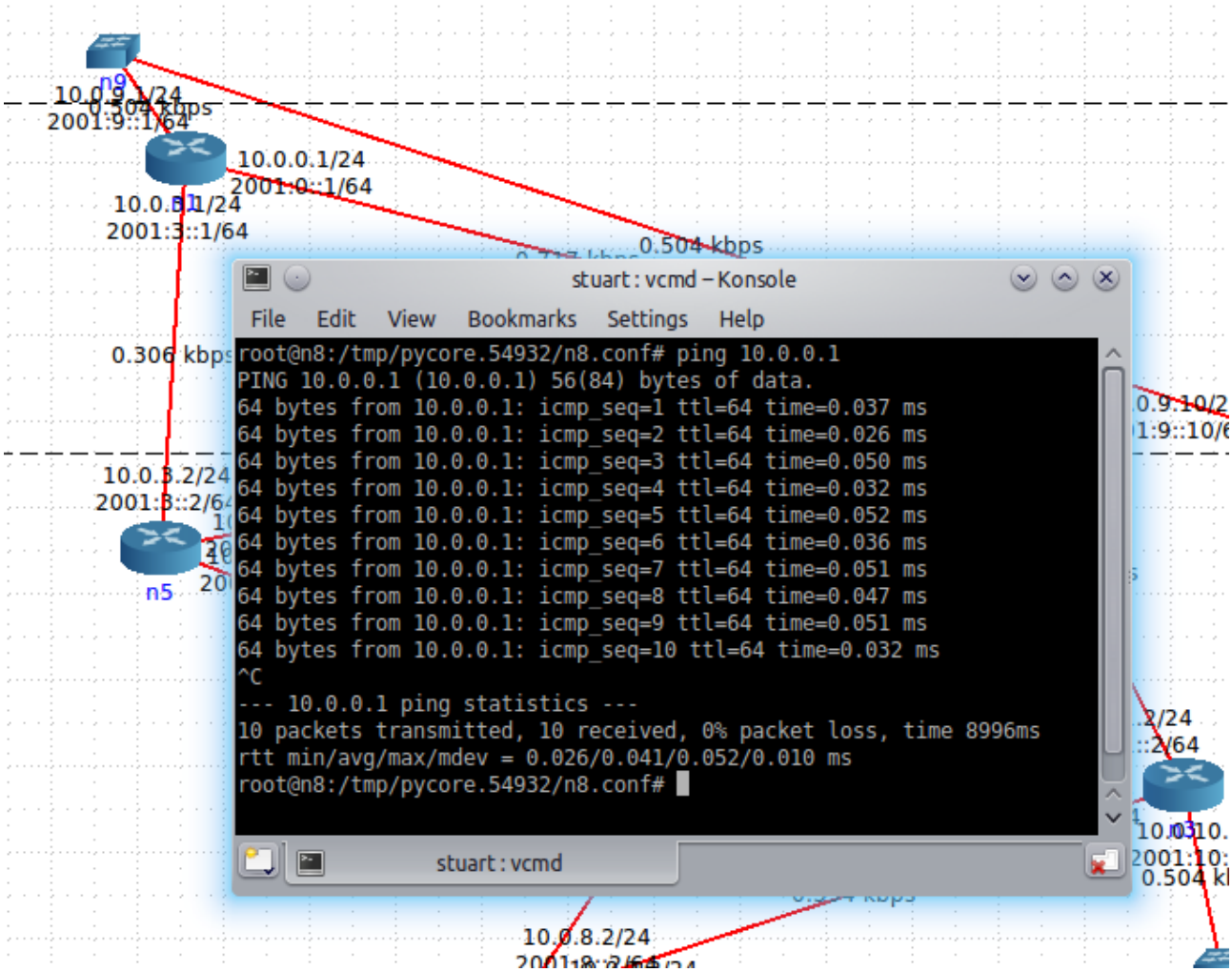


Şekil 25: GNS3 arayüzü içindeki yönlendiricinin konsolu

7.2.3 CORE (Common Open Resource Emulator)

Linux ve BSD üzerinde çalışıyor. Windows üzerinde sanal bilgisayarda çalıştırılabiliyor. Hatta kendi sitesinde, VmWare Player için hazır imajları da var. CORE içindeki her bir sanal PC'de Linux çalışıyor. Sanal ağ üzerinde lazım olan tüm işlevleri bu Linux'lar vasıtasıyla gerçekleştirilebiliyor. DHCP sunucusu, yönlendirici hizmeti, WEB sunucusu, vb. tüm işlevler Linux platformları üzerinden sağlanabiliyor. Yönlendirici olarak Cisco kullanma alışkanlığı olanlar, bir sanal Linux üzerine Quagga kurarak, onu sahte Cisco yönlendiriciye çevirebilirler.

Sanal ağı, gerçek ağa bağlayarak internet'e çıkarma özelliği bulunmaktadır. Büyük projelerde kullanmak üzere dağıtık hesaplama desteği de bulunmaktadır. Örneğin; elinizde 3 tane fiziksel PC varsa ve 200 tane node'dan oluşan sanal bir ağ kullanmak istiyorsanız, node'ları iki fiziksel PC'ye paylaştırabilir, 1 PC'yi de GUI amacı ile kullanabilirsiniz. Phyton ile script yazılabildiğini de belirtelim.



Şekil 26: CORE ekran görüntüsü

7.2.4 Diğerleri

- **NS2:** `http://www.isi.edu/nsnam/ns/`
- **NS3:** `https://www.nsnam.org/` (NS2'nin devamı olarak yapılmasına rağmen geriye doğru uyumluluğu olmadığından ayrı bir yazılım olarak değerlendiriliyor)
- **Cloonix**: http://clownix.net Açık kaynaklı. KVM sanal makine desteği var.
- **IMUNES**: http://www.imunes.net Açık kaynaklı. FreeBSD üzerinde çalışıyor. Sanal makinede çalıştırılabilir.
- **OMNeT++**: `http://www.omnetpp.org/`
- **Marionnet**: `http://www.marionnet.org/EN/`

- **Mininet**: http://www.mininet.org
- **Netkit:** http://wiki.netkit.org
- **Psimulator2:** http://code.google.com/p/psimulator/
- **Virtualsquare:** http://wiki.virtualsquare.org/wiki/index.php/Main_Page
- **VNX and VNUML:** http://www.dit.upm.es/vnx
- **OPNET (Ücretli):** http://www.riverbed.com/products/performance-management-co opnet.html

8 Kaynaklar

1. http://www.brianlinkletter.com/open-source-network-simulators/
2. http://www.finmars.co.uk/blog/4-evaluating-network-simulation-tools
3. http://nil.uniza.sk/network-simulation-and-modelling/network-simulators

9 SONUÇLAR VE ÖNERİLER

10 EKLER