

Protocol nedir?

İnternet nedir?

İnterneti oluşturan ana ve ara elemanlar

Bilgisayar ağlarının temel kavramları

Bilgisayar ağı güvenliği

İnternet nedir?

Ağların ağı

İnterneti oluşturan şey?

Ağa bağlı uç cihazlar

Bu cihazları diğer uçtaki cihazlara bağlayan ara cihazlar

Bunları birleştiren ağı ortamı (kablolar,kablosuz sistemler,dalgalar)

Ara cihazlar > router,switches (yönlendiriciler,anahtarlar)

Yönlendiriciler: İnternete gönderdiğimiz verileri yönlendiren

Ahmet'in verisini Google'a

Google'ın verisini Ahmet'e ve Mehmet'e göndermesini sağlayan yazılımlar yada donanımlardır.

Protokol nedir?

*** Protokoller, ağlar arasında gönderilen ve alınan mesajların biçimini, sırasını ve mesaj iletimi, alımında gerçekleştirilen eylemleri tanımlar.

Haberleşme sağlayan taraflar arasındaki anlaşmadır.

HTTP (Web), streaming video, Skype, TCP, IP, WiFi, 4G, Ethernet

Host nedir?

Konak

Host terimi, farklı anlamları olan çeşitli bağlamlarda ve alanlarda kullanılır. **İnternet Protokolü (TCP/IP)** belirtiminde, **İnternet aracılığıyla** diğer iki yönlü bilgisayarlar tam erişime sahip herhangi bir bilgisayarı ifade eder.

Bir yerel ağda kullanılan tüm bilgisayarlar arasında kullandığımız bilgisayar ile veri iletişimi yaptığımız iş istasyonu arasında, sizin bilgisayarınız Host olacaktır.

Şirketlerin websitelerini barındırdığı bilgisayar ya da bireysel kullanıcıların Web Server (Web Sunucusu) olarak kullandığı bilgisayarlar bir Host olarak adlandırılır.

Paket switch?

Veriyi gönderirken paketleyip göndermektir.

Bant genişliği nedir?

İnternet bağlantılı herhangi bir cihazın, belli bir zaman dilimi içerisinde alabileceği veri miktarıdır. Başka bir deyişle; bir kanalla aktarılacak olan maksimum verinin iletilmesi ve taşınmasıdır.

Network edge (Uç cihaz) > İnternete bağlanabilen herhangi bir cihaz

Access networks (ara cihaz) > paketleri taşıyan cihazları birbirine bağlayan kablolu yada kablossuz bağlantılardır

Network core (Ağ ortamı)> Bunları birbirine bağlayan sistemdir

Uç cihazlar bir routera nasıl bağlanır?

Evden internete nasıl bağlanırsınız?

Bir access pointe bağlanıyoruz

acc point ISP'ye bağlanıyor

ISP de sunucuya bağlanıyor

Servis nedir?

Uygulamalara hizmet sağlar

Posta hizmetine benzer hizmet seçenekleri sunar

Web, streaming video, multimedia teleconferencing, email, games, e-commerce, social media, inter-connected appliances, ...

TDM-FDM farkı? ***ÇIKACAK*******

TDM (time divison multiplexing): zamanı bölme (ders vb)

Belirli zaman slotlarında belirli data taşımaktır.

Birim zaman daha fazla veri iletmek istiyorsak TDM kullanırız

Esnektir.

Tüm frekanslar kullanılır.

Örnek:DSL,ADSL

FDM(frequency divison multiplexing):Radyo frekans

Aynı veri üzerinde birden fazla frekansta data taşımaktır

Sürekli kesintisiz yayın yapmak istiyorsak ama çok da gönderecek verimiz yoksa FDM kullanırız

-
1. FDM, daha fazla kullanıcıyı barındıracak şekilde kanalın çoklu ama daha küçük frekans aralıklarına bölünmesine karşın, TDM her kanala belirli bir süre ayırarak bir kanalı böler.
 2. TDM, FDM'ye kıyasla çok daha iyi esneklik sağlar.
 3. FDM, TDM'ye kıyasla çok daha iyi gecikme olduğunu kanıtlıyor.
 - 4.TDM'de birim zamanda daha çok veri gönderilir

*****BENZERİ ÇIKACAK*****

"Havaalanı güvenliği 14:00 dan itibaren telsizlerinde 3. Kanala geçsinler"

TDM mi FDM mi?

Cevap:FDM

Çünkü eş zamanlı bir iş yapılıyor.

FDM> Sürekli iletim.Aynı kanaldan.

Frekans Bölmeli Çoğullama (FDM), paylaşılan bir iletişim ortamı yoluyla eşzamanlı iletim için birden fazla veri sinyalinin birleştirildiği bir ağ oluşturma tekniğidir. FDM, her veri akışı için ayrı bir frekansta bir taşıyıcı sinyal kullanır ve daha sonra modüle edilmiş birçok sinyali birleştirir.

*****BENZERİ ÇIKACAK*****

"Çamlık minibüsleri saatbaşı Saltak üzerinden,yarım saatlerde ise İstiklal'den gitmektedir. "

TDM mi FDM mi?

Cevap:TDM

Çünkü: "*Zaman Bölmeli Çoğullama (TDM), farklı zaman dilimlerinde ortak bir kanaldan geçmek için bir dizi sinyalin yapıldığı bir tekniktir.*"

Flow control nedir? **ÇIKACAK*******

Taraflarla ilgilidir.

Alicının kapasitesine uygun veri aktarımıdır.

Sunucu datayı çok hızlı gönderebilir.Ama karşı taraf bunu alamıyorsa.Karşı tarafın alabileceği şekilde değişiklik yapılır.

Congestion control (tıkanklık kontrolü) nedir?

Yolla ilgili.

Datanın bir kısmı kayboluyorsa data küçültülebilir.

Tıkanklığı dikkate alarak gönderebileceğimiz kadar veri göndeririz.

Hızı artırır.Paket kaybı varsa azaltır.Sonra tekrar artırır.

Connection oriented nedir?

Baştan bağlantı kurar.

Bu da zaman alır

Handshake nedir?

Ağa bağlanan her cihaz için Handshake bize kimlik doğrulaması yapar. Doğrulama yapıldıktan sonra cihaz ağa bağlanır. Eğer Handshake olmaz ise kimlik doğrulanmaz bu da demek oluyor ki Handshake olmadığı sürece ağa bağlanamayız.

-Anahtarlama(forwarding) yerelde yapılır

-Store and forward ISP'de yapılmaz.Switch,router ya da modemde yapılır.

IMAP: Email yedeđi sunucuda kalır.

mailimi istemcime aldim, sunucudan silinsin istemiyorsam, yedeklensin istiyorsam kullanırım. Imap kullanırsam bütün cihazlardan maile ulaşırım.

POP3: Email yedeđi sunucudan silinir.

mailimi istemcime aldim, sunucudan silinsin istiyorsam kullanırım.

Pop3 kullanırsam başka bir cihazdan maile ulaşamam.

Paket kaybı

TCP iletim katmanı paket kaybını farkedir ve ister.

UDP ise paket kaybını uygulamada çözer.

Devre anahtarlama:

paket belli bir yoldan gider(sadece bizim datamız gider, **daha güvenilir**dir)

Hangisi kalabalık bir grup için daha uygundur

Devre anahtarı mı? Paket anahtarı mı ?

Paket anahtarı daha uygundur

Paket anahtarlama çok fazla yönetim planlama gerektirir. Kaybedilen paketlerle ilgilenmek gerekir.

Store and forward?

Cihaz üzerinde gerçekleşir. Paket gönderilir önce depolanır sonra yollarır

Packet switching?

Paketi aldım sakladım ve ilettim.

Cihaz üzerinde gerçekleşir. Paketi diğer elemana iletmeyi sağlar.

Neden saklar?

Paketin nereye gideceđini bilmiyordur

Başka paketleri bekliyor olabilir

Bu paketleri göndermeden önce göndereceđi başka paket olabilir

Kuyruklar

A'nın iletim hızı B'den büyük ise

B kuyruđına 1 paket sokarken A 3 paket sokacaktır

Paket kaybı neden olur?

Kuyruđı giremeyen paketlerde düşme yada kayıp gerçekleşebilir

Yüksek hızdan düşük hıza iletim varsa kayıp olabilir

Paket işelenmediyse, bozulduysa, yaşam süresi dolduysa, kuyruk doluysa, iletişim adresi yoksa düşebilir.

Gecikme nerede oluşur?

Her yerde

Cihazda (paketi oluşturması uzun sürebilir)

Yolda gecikme (işlemciye giderken)

Kuyruksa gecikme

İletim gecikmesi (transmission : cihazın bir noktasından birip diğer noktasından çıkma)

Hedefe giderken gecikme (yolu uzatabilir)

Dnodal (toplam gecikme)?

İşlem gecikmesi

Kuyruk gecikmesi

İletim gecikmesi

Diğer cihaza geçiş gecikmesi

ISP? İnternet Servis Sağlayıcı

Ana bilgisayarlar ISP'ler aracılığıyla internete bağlanır

İsp aracılığıyla herhangi iki ana bilgisayar birbirine paket gönderebilir

Throughput nedir?

Bir cihazın kullanabileceği maksimum data miktarıdır.

Anlık throughput > İsp bize saniyede 100 megabit verdi. Ben 0 kullanıyorum bu benim anlık throughputum

***Throughput > bizim anladığımız

***Bandwidth > hocanın anlattığı

Client-Server (İstemci-Sunucu)Paradigm

Server

İsteklere cevap veren kısım

Sunucu daima açık olmalı

Kalıcı (statik) IP adresi vardır

Client

İstekte bulunan kısım

Aralıklarla bağlanır. Her zaman açık değildir.

Dinamik IP adresi vardır.

Birbirleriyle direkt iletişimleri yoktur.

Peer-Peer Architecture

-Client-Server(İstemci-Sunucu) mimarisine alternatif bir yapıdır

-Her zaman ayakta değildir

-Her istemci aynı zamanda sunucudur, her sunucu aynı zamanda istemcidir

-İstemciler doğrudan birbirleriyle haberleşebilir

-Peerlerin sürekli açık kalmasına gerek yoktur

-Peerlerden birisi sistemden çıksa bile sistem çalışmaya devam eder

-Statik bir IP adresi yoktur.

-Değişen adresler için peer'lerin listesi (tracker) tutulur.

-Self scalability (Kendi kendine ölçeklenebilirlik) vardır

-Peerler sürekli dinlemek zorundadır(port sürekli açıktır)

Örnek : Torrent indirme işlemleri BitTorrent P2P protokolü kullanılarak yapılır

Process Communicating

Uygulamaların üzerinde çalışacağı şeyler processlerdir.

process:ağ uygulaması düşünüldüğünde processler **host** üzerinden haberleşecektir.

Sockets:Uygulama katmanı ile iletim katmanı arasındaki ara birimdir.

Processlere ayri veriler gelir. Processlere ozel gelen verileri **soketler aracılığıyla** processlere dagitiriz

Adressing Processes

Mesaj alabilmek için processssler tanımlayıcıya ihtiyaç duyarlar (identifier)

Sunucu cihazlar 32 bitlik IP adresine sahiptir.

Port adresi?

İletim katmanında verinin iletileceği yere geldiğinde hangi protokol yada process tarafından kullanılacağını belirten adrestir.

IP adresi (mantıksal adres)?

Ağ katmanında iletişimi sağlayacak adrestir.

Mac adresi (Fiziksel adres)?

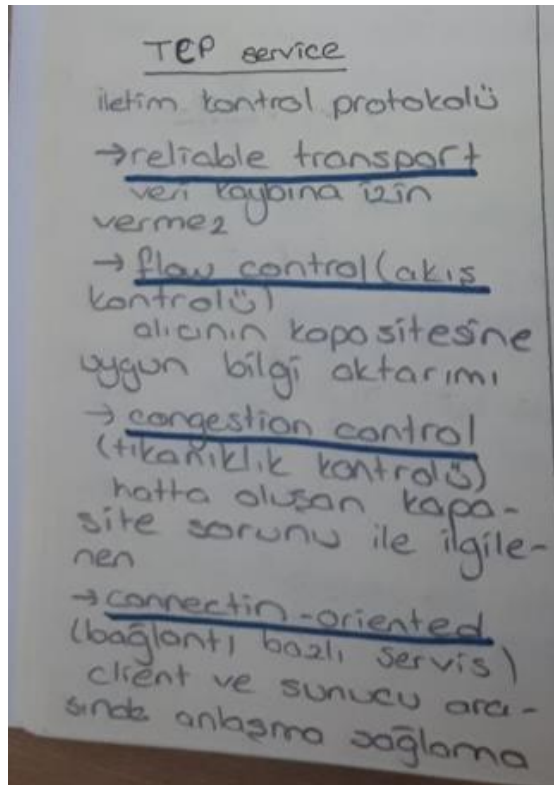
İki kablo ucundaki kartların adresidir.Tektir ve değişmez.Ağ üzerindeki cihazların birbirini tanımasını,router gibi aygıtların doğru bağlantıları sağlaması işleminde kullanılır.

hedef mac adresi ne zaman değişir?

$x > x > x > x > x > x > \text{hedef}$

cihazlar paketleri birbirine iletirken her aşamada değişir

Tcp vs Udp



→ doesn't provide
• güvenlik sağlamaz
• throughput u garanti etmez.
• zamanlama sağlamaz
→ tıkanıklık ve akış kontrolünü sağlar.
→ sıralı iletim

UDP service
kullanıcı datagram protokolü
→ unreliable data transfer
veri kaybına göz yumar
→ timing zamanlama sağlar.
→ doesn't provide
• security
• flow control
• reliability
→ sırasız iletim

Datanın gitmesi önemli ise **TCP**
Zaman önemli ise **UDP** kullanılır
UDP veri kaybına göz yumar.

TCP'yi güvenli hale getirme

Transport Layer Security (TLS) >

Şifetlenmiş TCP bütünlüğü sağlar

Data bütünlüğü

Kimlik doğrulama (handshake)

TCP- UDP farkı? *****ÇIKACAK*****

TCP

-Reliable transport (güvenilir iletim) (veri kaybına izin vermez)

-Data kesinlikle gönderilecek. Veri kaybına tahammülü yok.

-Data gitmezse tekrar gönderilir.

-Veri alındı mı emin olunur. Alındı bilgisi alınır.

Gönderdiğim-gönder-gönderiyorum-alındı mı-alındı

-Handshake var (kimlik doğrulama)

Flow control (akış kontrol) ve tıkanıklık kontrolünü sağlar.

*File transferde TCP kullanılır. Çünkü TCP'de veri kaybına tahammül yoktur. UDP ise veri kaybına göz yumar.

emailde tcp kullanılır

UDP

-DNS örneği

-Data'nın kaybolması önemli değil. Veri kaybına göz yumar. (Video ve ses gönderiminde, online oyunlarda, realtime görüşmelerde kullanılır)

-Hızlı

-Veri küçük

-Veriyi gönderdi bıraktı-sen alırsan alırsın

-Veriyi zaten tekrar gönderebilirim

HTTP

Server-client modelinde sayfanın iletilmesini sağlayacaktır

HTTP TCP'yi kullanır

Client TCP bağlantı isteğinde bulunur.

Server TCP bağlantısını kabul eder.

Server isteği döndürür

TCP bağlantısı kopar

HTTP stateless yani durumsuzdur

Ben bir web isteği gönderdim ilk defa beni görmüş gibi davranacak

Sunucu istemcinin geçmişi hakkında bilgi tutmaz.

HTTP'nin amacı bağlantıyı kurmak, veriyi aktarmaktır

Kullanıcı bilgileri cookie ve cache'te tutulur.

HTTP connections

non persistens HTTP (kalıcı olmayan)

Tek bir nesne gönderilir.TCP bağlantısı açıldı
***Her obje için bir kez bağlantı kurup bitiriyorum.

Persistent HTTP (kalıcı)

TCP bağlantısı açıldı
***Çoklu objeleri tek bir TCP bağlantısında gönderir
TCP bağlantısı kapanıyor

Non persistent HTTP

RTT (Round trip time) : Küçük bir paketin clienttan servera gidip dönmesi sırasında geçen süredir.

Persistent HTTP:

Obje için 2 tane RTT ister

http request message

request,response

ACII tipinde mesaj ister

request line (get,post,head) >

Get > sayfayı almak için

Post > veri gönderme

Head > veri neler içeriyor, karşı taraf nasıl kontrol edecek, veri nasıl gelecek

Push > veri gönderme

Pull > veri çekme

Maintaining user / server state : cookies

Kullanıcı bir web sayfasına ulaştığında kullanıcı için cookie belirlenir.O id ile kullanıcının bilgileri verilir.Giriş yapıldıktan sonra ise geçmiş bilgilerine erişebilirsiniz

Cookie özellikleri >

Sunucudan istemciye gönderilen mesajdır

Cookie **istemci**de tutulur

Sunucuda yapılan işlemler ise sunucuda tutulur

Cookie ne için kullanılabilir?

Kimlik doğrulamanın zayıflatılmış versiyonu,yetkilendirme için kullanılır

sepete ulaşım (alışverişte)

önerilerde bulunabilir

mail taslağı kayıt edebilir

gizlilikle ilgili sorunları vardır.

Cache

Amaç veriyi daha yakın taşıyarak gecikmeyi azaltmak.

Örnek:Yüzüklerin Efendisi'ni kampüste izlemek (CDN).Normalde kaynak sunucu ABD'de.

Veriyi Pamukkale kampüsündeki bir local sunucuya çekiyoruz.Verilocal sunucudan istemciye geliyor.

Veriyi yereldeki sunucuya çekiyoruz

Amac veriyi istemciye yaklastirip gecikmeyi ve sunucuya yakin (sunucu-cache) trafigi azaltmak

Aradaki baglantiyi iyilestirmektense web cache(sunucu) daha ucuz.

Amaç:kaynak sunucuyu dahil etmeden müşteri isteklerini karşılamak

Kullanıcı tarayıcıyı local bir web önbelliğini gösterecek şekilde yapılandırır

Browser tüm HTTP requestlerini cache'e gönderir

If >>>Nesne cache'de ise : cache nesneyi client'a döndürür

Else > Nesne orijinal serverda ise : cache kaynak sunucudan nesne ister.nesneyi cache'e alır.ardından nesneyi istemciye döndürür.

Web cache'leri proxy server gibi çalışır

Web cacheleri Neden kullanılır?

Client'a yakındır.Daha hızlı çalışır.

Dışardaki bağlantı trafiğini azaltır.

Miss'i değil hit'i çok olan şeyler cachelenmelidir.

IXP, ISPleri birbirine bağlayarak ag olustururlar.

Icerik saglayici aglar IXPlerden bagimsiz ag baglantilari kurarlar

IMAP: Email yedeği sunucuda kalır.

mailimi istemcime aldim, sunucudan silinsin istemiyorsam, yedeklensin istiyorsam kullanirim.Imap kullanırsam bütün cihazlardan maile ulaşırım.

POP3:Email yedeği sunucudan silinir.

mailimi istemcime aldim, sunucudan silinsin istiyorsam kullanirim.

Pop3 kullanırsam başka bir cihazdan maile ulaşamam.

Bring home:Veriyi kendi güçlü olduğu yere taşımak.

HTTP client pull ile çalışır

SMTP client push ile çalışır.

HTTP bir nesneyi bağımsız gönderebilir.

SMT hepsini tek seferde gönderir.

OSI 7 KATMAN

*****ÇIKACAK*****

- 7-Uygulama – app (HTTP,IMAP,SMTP,DNS)
- 6-Sunum – presentation
- 5-Oturum – session
- 4-İletim - transport (process-process data transferi,TCP,UDP) (segment)
- 3-Ağ – network (IP,routing protocols) (paket)
- 2-Bağlantı – MAC
- 1-Fiziksel – donanım

Bu katmanlar şöyle sıralanmaktadır:

- 1- Fiziksel Katman (Physical Layer)
- 2- Veri Bağı Katmanı (DataLink Layer)
- 3- Ağ Katmanı (Network Layer)
- 4- İletim Katmanı (Transport Layer)
- 5- Oturum Katmanı (Session Layer)
- 6- Sunum Katmanı (Presentation Layer)
- 7- Uygulama Katmanı (Application Layer)

OSI (Open Systems Interconnections) Katmanları

İletişim protokolü, ağ üzerindeki cihazlar arasındaki iletişimi sağlanmasında, standart olarak kabul edilen düzendir.

1.Physical Layer (Fiziksel Katman)

Donanım katmanı ve ilk katmandır. Bu katmanda, verilerin kablo üzerinden gelen bilgiyi **bit olarak** (0 ve 1 olarak) iletilmesini sağlar. Verileri gönderen tarafta 1 ve 0 'ı elektrik sinyallerine dönüştürürken, alıcı tarafta kablodan gelen bu sinyalleri tekrar 1 ve 0'a dönüştürür.

Fiziksel Katmanın İletişim Kuralları; DSL, ISDN, RS-232,802.11a/b/g/n

2.Data Link Layer(Veri Bağlantı Katmanı) (MAC)

Veri bağlantı katmanı, verinin donanım katmanına ulaşmasını ve kuralların oluşturulmasını sağlar. Ethernet, token ring gibi erişim yöntemleri bu katmanda çalışır. Veriyi, erişim yöntemleri kendi protokollerine uygun bir şekilde iletir. Ağ katmandan gelen veriyi fiziksel katmana iletir. Burada veriler bölünerek frame'ler (çatılar) oluşturur. Frame'ler, verileri kontrol ederek gönderilmesini sağlar. Bu işlemlerin büyük çoğunluğu ağ kartı üzerinde olur. Data Link katmanı iki alt bölüme ayrılır. Bunlar; MAC (Media Access Control) ve LLC (Logical Link Control)

MAC; Fiziksel katmanla iletişim kurulmasını sağlar. Fiziksel/donanım adresi olarak da isimlendirilir. Her bir ağıttın kendisine özel bir MAC adresi vardır.

LLC; Mantıksal bir arabirim kullanarak bir üst katmanla iletişimi ve bozulmuş paketlerin tekrar gönderilmesi sağlar. Flow Control, alıcının işleyebileceğinden fazla gelen veriyi kontrol eder engellenmesini sağlar. Akış kontrolünü sağlar.

Veri Bağlantısı Katmanının İletişim Kuralları; Ethernet, Token Ring, FDDI, PPP, ATM, HDCL

3.Network Layer (Ağ Katmanı) (IP)

Network katmanı verilerin ağ içerisindeki iletişimini sağlar. Adres bilgisi eklenir ve verilerin iletilmesin en uygun rota çizilir. **IP protokolü** bu katmanda çalışır. Verilerin kaynak, hedef IP'si, yaşam süresi eklenerek **paket oluşturulur**. Oluşturulan paketler en uygun rotaya göre gönderilir.

Ağ Katmanının İletişim Kuralları; IP, ICMP, IPsec, ARP, RIP, BGP, IPX

4.Transport Layer (İletim Katmanı)

Alt katmanlar ve üst katmanlar arasında mantıksal bir bağlantının kurulmasını sağlar. Üst katmandan gelen veriyi **segmente** bölerek bir alt katmana iletilmesini sağlar. Alt katmandan gelen veriyi de birleştirip bir üst katmana iletir. TCP ve UDP protokolleri bu katmanda çalışır.

Taşıma Katmanının İletişim Kuralları; DCCP, SCTP, SPX,TCP, UDP

5.Session Layer (Oturum Katmanı)

Oturum katmanı, birden fazla bilgisayarın aynı anda iletişimin kurduğunda , doğru bilgisayarın ile iletişim kurmasını sağlar. Uygulamalar arasındaki bağlantının kurulması, yönetilmesi ve sonlandırılması bu katmanda olur.

Oturum Katmanının İletişim Kuralları; NetBIOS, SIP, SAP, LDP

6.Presentation Layer (Sunum Katmanı)

Gönderilen verinin, karşı taraf bilgisayar tarafından anlaşılmasını sağlar.
Uygulama katmanına verileri gönderir, verinin yapısında düzenleme yapar.
Verinin formatı bu katmanda belirlenir.

Sunum Katmanının İletişim Kuralları; ASCII, MIDI, EBCDIC, MPEG

7.Application Layer (Uygulama Katmanı)

Osi katmanlarından uygulama katmanı, son kullanıcıya en yakın olan katmandır.
Doğrudan kullanıcıdan bilgi alır ve gelen verileri kullanıcıya götürür. Bu katmanda kullanıcıların gereksinimleri karşılanır. Uygulamaların ağ üzerinde çalışmasını sağlar.

Uygulama Katmanının İletişim Kuralları; HTTP, SMTP, POP, SNMP, FTP, Telnet

Cmd komutları

MAC adresi benzersiz olmalıdır

Yerelde cihazların MAC'i farklı olmalıdır

Bir cihazın birden fazla MAC'i olabilir

Whoami veya hostname > cihaz bilgisini verir

Net user > ağa bağlanan kullanıcıları gösterir

Getmac > mac adresini verir

Ipconfig > IP adresini verir

Ipconfig /release IP adresini sıfırlar

ipconfig /renew IP adresini yeniler

Netstat -c > aktif internet bağlantılarını gösterir

Netstat -s> her İletişim Kuralları İçin İstatistikleri Gösterir.

ping –

Uzak konak erişim kontrolü, zaman ölçümü

– ICMP (Internet Control Message Protocol) paketi

ICMP protokolü nedir nasıl çalışır?

Icmp,ağ içinde hata kontrolü yapar.

ICMP (Internet Control Message **Protocol**-İnternet Kontrol Mesaj **Protokolü**), İnternet Katmanında IP paketinin veri bölümünde çalışıp, sorunları haberleşen birimlere bildirerek bir geri besleme mekanizması oluşturur.

Tracert-

TCP/IP sayesinde kullanabildiğimiz bir komuttur. Bu komut, yazdığımız ip adresi ve ya domaine gönderilmek istenen veri paketinin, oraya ulaşana kadar geçtiği ağ geçitlerini tek tek listeler.

Pathping Nedir ;

Veri paketlerinin hedef sunucuya giderken geçtiği tüm routerleri küçük veri paketleri ile denetleyerek daha ayrıntılı bir raporlama sağlamaktadır.

Sunucuda Bir sıkıntı olduğunda bu komutu kullanarak hangi veri alış verişin hangi noktada sıkıntı olduğunu bulabiliriz. Pathping aynı Tracert komutu gibi verilerin nereden geçtiğini de listeler.

ARP komutu ne işe yarar?

ARP(Address Resolution Protocol) Adres Çözümleme Protokolü bir yerel ağda IP adresi bilinen cihazın MAC adresini bulmak için kullanılır. Yerel ağda cihazlar birbirleri ile MAC adreslerini kullanarak iletişim kurarlar.

Nslookup Komutu Nedir?

Dns Serverin Düzgün çalışıp çalışmadığı kontrol etmek için kullanılır.

>route print 10.*

Komut yardımıyla 10. ile başlayan route'ları görürüz.

>route add 0.0.0.0 mask 0.0.0.0 192.168.1.1

Komut yardımıyla gelen bütün paketleri 192.168.1.1 ip adresine yönlendirilir.

>route delete 10.54.0.0 mask 255.255.0.0

Komut yardımıyla 10.54.0.0 route'unu siliyoruz.

DHCP:

IP adresini

alt ağ maskesini

varsayılan ağ geçidini verir

DNS > domaini IP adresine çevirir

UDP checksum ÇIKACAK*****

Slayt: https://w3.gazi.edu.tr/~akcayol/files/CNL7_TransportLayer.pdf

UDP checksum

- ▶ UDP checksum ile **uçtan-uca** (iki transport layer arasında) **hata denetimi sağlar.**
- ▶ UDP gönderici segment'teki **16-bit blokları toplar** ve **1 tümleyen alır.**
- ▶ Toplama işleminden taşan bitler sağ tarafa eklenerek tekrar toplanır.
- ▶ Elde edilen **sonuç UDP segment'indeki checksum alanına yazılır.**
- ▶ UDP, **link-by-link** veya **in-memory hatalarına bakmaz.**
- ▶ **UDP, uçtan uca hata denetimi yapar (end-end principle).**

26

UDP checksum

- ▶ Örnek: Üç 16-bit için checksum hesaplanarak segment'e yazılır.

```
0110011001100000
0101010101010101
1000111100001100
```

- ▶ İlk ikisinin toplamı aşağıdadır.

```
0110011001100000
0101010101010101
1011101110110101
```

- ▶ Üçüncünün eklenmesiyle aşağıdaki değer elde edilir.

```
1011101110110101
1000111100001100
10100101011000010
```

- ▶ Sonuç 1 tümleyen alınarak hesaplanır.

```
1011010100111101
```

- ▶ Alıcı segment ile checksum'ı toplar ve 1 tümleyeni hesaplar.
- ▶ **Sonuç 0 ise hatasız** olarak kabul edilir (**hatalı olabilir mi?**).

27

Checksum videosu > <https://www.youtube.com/watch?v=pJt36ekvom4>

Go back N and selective repeat *****ÇIKACAK*****

https://w3.gazi.edu.tr/~akcayol/files/CNL8_ReliableDataTransfer.pdf

<https://www.youtube.com/watch?v=bTC6rSE6eKY>

<https://www.youtube.com/watch?v=CkEQ0sJ6uJw>

<http://www.engincode.com/selective-repeat-arq-algoritmasi>

<https://tr.gadget-info.com/difference-between-go-back-n>

Animasyon:

https://wps.pearsoned.com/ecs_kurose_compnetw_6/216/55463/14198702.cw/index.html

Go Back N Control

- Paketler eşzamanlı gönderilir.
- Pencere için zaman tutulur.
- Hata oluşursa gönderilen paketler tekrar gönderilir.
- Daha fazla paket göndermemiz gerekebilir.
- Tek zaman tutulur

Selective Repeat Control

- Paketler eşzamanlı gönderilir.
- Gönderilen her bir paket için zaman tutulur.
- Hata oluşursa gönderilenler tekrar gönderilmez.Hatadan dolayı gönderilemeyen paketler gönderilir.
- Her pakete özel zaman tutulur.

SORU CEVAP

1-İnternette uç cihazlar sadece bilgisayarlardır.

Yanlış.İnternete bağlanabilen tüm cihazlar uç cihazdır.

2-Yönlendirici ve anahatlar internetteki ara cihazlardır

Doğru.Router(yönlendirici) ve switchler(anahtarlar) ara cihazlardır.

3-Mobil internet sağlayıcılarının temel görevi mobil cihaz satmaktır.

Yanlış.Temel görevi ağdaki paketlerin taşınmasıdır.

4-ASP.net bir internet protokolüdür?

Yanlış.

5-HTTP bir protokoldür?

Doğru

6-Protokol biçim sıra ve alınan aksiyonlardan oluşur.

Doğru.

7-TDM zamanın bölümlendiği modulasıyondur.(Örnek.TV programları)?

Doğru. Time division multiplexing.

8-Anahtarlama yerelde paket iletimi yapılır?

Doğru.

9-Store and forward ISP’de yapılır?

Yanlış.Store and forward (gelen paketi sakla ve ilet) switch,router ya da modemde yapılır.

10-FDM frekansın bölümlendiği fonksiyondur?

Doğru.

11-Devre anahtarlama paket anahtarlama dan daha güvenlidir?

Doğru.Düşürölme ya da gecikmeye uğramaz.Ama daha pahalıdır.Bu yüzden paket anahtarlama daha çok tercih edilir.

12-Yönlendirme (routing) ile yerelde paket iletimi yapılır?

Yanlış.Globalde yapılır.

13-Paket anahtarlama devre anahtarlama dan daha yaygındır?

Doğru.

14-IXP,ISP’leri birbirine bağlayarak ağ oluşturur?

Doğru.

15-İçerik sağlayıcılar IXP’den bağımsız ağ bağlantıları kurarlar?

Doğru.İçerik sağlayıcılar Netflix,Youtube,Amazon gibi sistemlerdir.

Google IXP’den bağımsız ağ kurar (hız ve bant genişliği için)

1-Hangisi ağ katmanının görevidir?

A-Mantıksal Ağ oluşturur

B-Uygulamaları birbirine bağlar

C-Verileri bitler şeklinde gönderir

D-Hepsi

2-Hangisi ile iletim katmanı ilgilenir?

A-Bitler

B-Paketler

C-Frameler

D-Segmentler

3-Hangisi ile ağ katmanı ilgilenir?

A-Bitler

B-Paketler

C-Frameler

D-Segmentler

4-Hangisi ağ katmanındaki bir protokoldür?

A-HTTP

B-UDP

C-IP

D-Hepsi

5-Hangisi iletim katmanındaki bir protokoldür?

A-icmp

B-TCP

C-IP

D-Hiçbiri

6-Hangisi icmp'nin kullanım amaçlarındandır?

A-Ağ içinde hata kontrolü

B-Adresleme

C-Paket iletimi

D-Hiçbiri

7-Çamlık minibüsleri saatbaşı Saltak'tan,yarım saatlerde ise İstiklal'den gitmektedir ifadesi için ne söylenebilir?

A-TDM için bir örnektir

B-FDM için bir örnektir

8-Havaalanı güvenlikleri 14.00'dan itibaren 3.kanala geçsinler?

A-TDM için bir örnektir

B-FDM için bir örnektir

9-Hangisi katman2 adresidir?

A-127.0.0.1

B-8080

C-10:08:B1:BF:95:1B

D-www.google.com

Hangisi katman3 adresidir?

A-IP

B-Port

C-MAC

D-Socket

Hangisi katman2 adresidir?

A-IP

B-Port

C-Mac

D-Gateway

Hangisi yanlıştır?

A-E-posta uygulamaları zaman bağımlı olduğu için UDP kullanılır

B-E-posta sunucuları kendi aralarında SMTP kullanır

C-E-posta uygulamaları hata toleranslı olmadıkları için TCP kullanır

D-E-posta uygulamaları katman7de çalışır

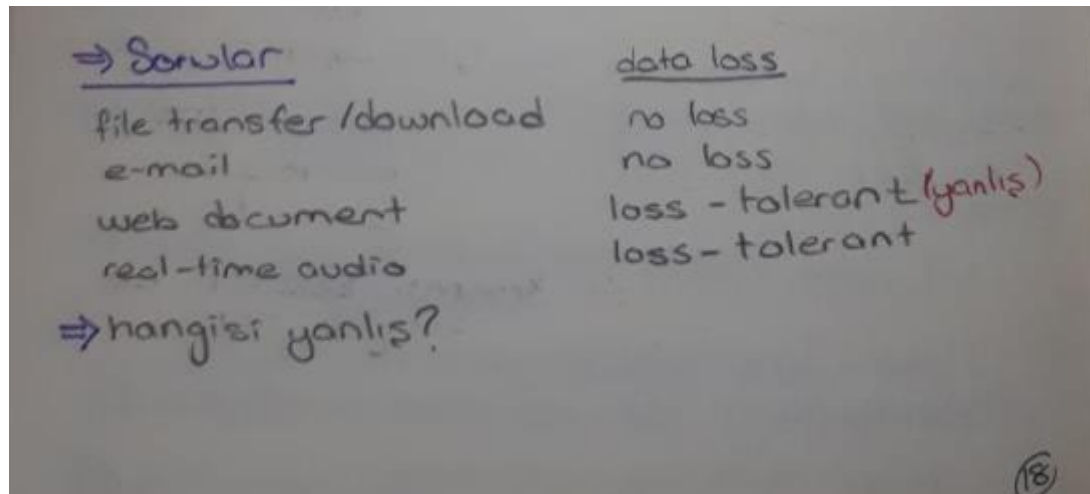
Hangisi yanlıştır?

A-Online oyunlar zaman bağımlı olduğu için UDP kullanırlar

B-TCP'de veri hata kontrolü yapılır

C-Video yayınlar(stream) geri alma ileri sarma varsa TCP kullanır

D-UDP bağlantı kurar paketin gittiğini kontrol eder



streaming video/audio	<u>data loss</u>
interactive game	no-loss (yanlış)
text messaging	loss-tolerant
⇒ hangisi yanlış	no-loss

<u>application</u>	<u>throughput</u>
file transfer / download	elastic
e-mail	elastic
web documents	elastic (yanlış)
real time audio/video	audio: 5 kbps - 1 Mbps video: 10 kbps - 5 Mbps
streaming audio/video	elastic
interactive games	Gbps (yanlış)
text messaging	elastic
<p>→ dokümanların yüklenmesine karşı browserlar den gösterir. Belirli bir değerde olmalı.</p> <p>→ Genelde kilobit seviyesindedir.</p>	

<u>application</u>	<u>time sensitive</u>
file transfer / download	no
e-mail	no
web document	yes (yanlış)
real-time audio/video	yes, 10's msec
streaming audio/video	yes, few secs
interactive games	yes, few secs (yanlış)
text messaging	yes and no
↳ bazı uygulamalarda önemli bazılarında değil (wp ve instagram gibi)	

(19)

⇒ Hangisi doğru?

<u>application</u>	<u>application layer protocols</u>			
	SIP	SNTP	HTTP	FTP
file t. / download				
e-mail		✓		✓
web documents			✓	
Internet telephony	✓			
streaming a/v			✓	
interactive games				

FTP → file transfer protokol

SMTP → Simple mail transfer protokol

SIP → Session Initiation protokol (Ölümün başlatma p.)

<u>application</u>	<u>transport protocols (TCP/UDP)</u>
file t. / d	TCP
e-mail	TCP
web document	TCP
Internet telephony	UDP / TCP
streaming a/v	TCP / UDP
interactive g.	UDP / TCP

→ hızda UDP, TCP bağlantısının kalıcı ve veri kaybı konusunda

⇒ Sanal market web sayfasını ziyaret eden bir kullanıcının az önce doldurduğu sepetinin boş olduğu görünmektedir. Kullanıcı HTTP 'yi suçlar. Kullanıcının söylediği için ne söylene bilir?

Yanlış bir ifadedir. cookies

⇒ Kullanıcının az önce baktığı uçak biletinin fiyatı artmıştır. Kullanıcı cookie'leri suçlar. Doğru mudur?

Cookie 'de tutulan değeri arttıran bir algoritma kullanılabilir. Doğrudur

⇒ HTTP davranışının hangisinde tüm nesneler tek bir bağlantı ile indirilir, Persistent HTTP

→ Çok kullanıcıli sistemde kalıcı bağlantı daha avantajlıdır.

→ Ağın through-put u düşükse geçici bağlantı daha avantajlıdır

⇒ Web cache için yararlıdır?

A) İa ağıda haberleşmeyi hızlandırır.

B) Dış ağıda trafik yoğunluğunu azaltır.

C) İstemciye yakındır.

~~X~~ Servis sağlayıcısına yakındır.

⇒ POP3 e-postayı istemciye taşır sunucudan siler?

Doğrudur. Eski zamanlarda sunucudaki yükü azaltırdı.

⇒ IMAP e-postayı istemcide tutar ve sunucudan silmez?

Ne kadar istemci dursa olsun hepsine push eder. Kendinde de bir kopyasını tutar.

21.10.2020

⇒ DNS : Domain Name Server

• google.com, google.com.tr v.b IP adresleri farklıdır.

→ DNS 256 karaktere kadar büyüyeabilen host isimlerini IP adresine çevirmek için kullanılan sistemdir.

→ Neden birden fazla DNS sunucusu var?

Herkes tek bir sunucuya istek atarsa oluşacak sorun. Aynı zamanda bazıldığı zaman domain - IP geçişleri yavaşlar.

Tek sunucu olsa nereye kurulacak.