NETWORK BASICS-3

Friday, June 28, 2024 9:12 AM

Table of Contents

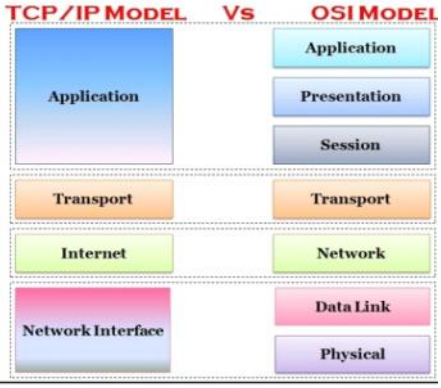
A Brief History of TCP/IP

- TCP/IP *(Transmission Control Protocol/Internet Protocol)* is a set of network protocols *(Protocol Suite)* that enable communication between computers
- TCP first came on the scene in 1974
- Divided into two distinct protocols, TCP and IP in 1978
- Became the officials means of data transport for ARPANet in 1983
- Mostly developed in UC Berkeley simultaneously with Berkeley version of UNIX (BSD)

2 TCP/IP and the DoD Model

TCP/IP (DoD) and the OSI Model

- The DoD *(Department of Defense)* created TCP/IP to ensure and preserve data integrity
- The DoD model is a condensed version of the OSI model



CLARUSWAY©

TCP/IP and the DoD Model

Process/Application layer

- Enables applications to communicate with each other.
- Provides access to the services that operate at the lower layers of the DoD model.
- It contains a protocol that implements user-level functions such as mail delivery, file transfer, and remote login.
- Includes all higher-level protocols: DNS, HTTP, Telnet, SSH, FTP, SNMP, DHCP, etc.

DNS: Domain Name Service
HTTP: Hyper-text Transfer Protocol
SSH: Secure Shell
FTP: File Transfer Protocol
SNMP: Simple Network Management Protocol
DHCP: Dynamic Host Configuration Protocol

CLARUSWAY©

TCP/IP and the DoD Model

Host-to-Host Layer (Transport Layer)

- Permits devices on the source and destination to carry on a conversation
- Defines the level of service and status of the connection used when transporting data
- Main protocols are TCP and UDP

CLARUSWAY©

TCP: Transmission Control Protocol
UDP: User Datagram Protocol

TCP/IP and the DoD Model

Internet Layer

- Packs data into data packets known as IP datagrams
- Responsible for routing of IP datagrams
- Main protocols are IP, ICMP, ARP, RARP, and IGMP

IP: Internet Protocol
ICMP: Internet Control Message Protocol
ARP: Address Resolution Protocol
RARP: Reverse Address Resolution Protocol
IGMP: Internet Group Message Protocol

CLARUSWAY©

TCP/IP and the DoD Model

Network Access Layer

- Defines details of how data is physically sent through the network
- Main protocols are Ethernet, Token Ring, FDDI, X.25, and Frame Relay

FDDI: Fiber Distributed Data Interface

CLARUSWAY©

Bizim hic duymadigimiz protokollerde mevcut cunku hersey icin bir protokol belirlenmek zorunda. Ona gore istenilen seyin devaminda eger birseyler uretilecekse ona gore bir kurali olmasi gerekiyor.
Ana protokoller burada goruldugu gibi ethernet, token ring, fddi, x.25 ve frame relay.

3 The Process/Application Layer Protocols

The Process/Application Layer Protocols

Telnet (TCP 23): Allows a user on a remote client machine to access the resources of another machine.

SSH (TCP 22): Secure Shell Protocol sets up a secure session that's similar to Telnet over a standard TCP/IP connection and is employed for doing things like logging into systems, running programs on remote systems and moving file from one system to another system.

CLARUSWAY©

Telnet, SSH vs application layerda ama TCP-UDP transport layerda.
Bizim sectigimiz ust protokol asagida transfer sirasinda nasil bir segmentasyin yapacagimizi gosteriyor.
Mesela HTTP kullaniyosan mecbur TSP kullanacak gibi.
Telnet ve SSH TCP ile segmente ediliyorlar 23 ve 22 portlarinda.
Port numarasi: MAC ve IP adresine bakilarak paket ulasmasi gereken cihaza ulasir. Fakat her cihazda bircok process isliyor eszamanli olarak. Cihazimizin hangi isleme paketi yonlendirecegini bulmasi portlar sayesinde mumkundur. Isletim sistemlerimizdeki kernel o paketlere giderken gelirken bir port numarasi veriyor. Bizlerde programlari ayarlarken hangi portta gidecek ya da hangi porttan alacak kismini belirliyoruz.
Ssh kutuphane, kafe vs gibi ortak baglanti yapilan yerlerde baglanti yapmasina izin vermez. Cunku guvenilir bulmaz. Bu durumda telefonuzmuzun internetine baglanip oradan ssh a baglanmak arti bir cozum olabilir.

Ports are classified into 3 main categories..

- Well Known Ports (Port numbers 0 – 1023)
- Registered Ports (Port numbers1024 – 49151)
- Private or Dynamic Ports (Port numbers 49152 – 65535)

Biz herhangi bir paketimizi well known port uzerinden yayinlayamayiz. Yasak. 1023 e kadarki portlar dunyaca bilinen belirli processler icin ayrilmistir. Harici bir durum icin kullanilamaz.
Registered portlar ise dunyaca yine uzerinde islem yapabilecegimizi dusundugumuz portlardir. Zoom, whatsapp, skype vs.

The Process/Application Layer Protocols

FTP (TCP 20, 21): File Transfer Protocol lets us transfer files between any two machines. FTP functions are limited to listing and manipulating directories, typing file contents, and copying files between hosts.

SFTP (TCP 22): Same as FTP but Secure FTP uses an encrypted connection through an SSH session, which encrypts the connection.

TFTP (UDP 69): Trivial FTP is the stripped-down, stock version of FTP. TFTP is fast and so easy to use. It can only send and receive files.

CLARUSWAY©

Ftp bir dosya transfer edilecegi asamada kullanilan protokoldur.
Sftp ise ftp nin secure hali. Cunku ssh uzerinden connect sagliyor.
Tftp ise daha hizli ama udp de calisiyor. Yani tcp kadar guvenilir degil.

The Process/Application Layer Protocols

POP (TCP 110): Post Office Protocol gives us a storage facility for incoming mail (the latest version is POP3). A newer standard, IMAP, is being used more and more in place of POP3.

IMAP (TCP 143): Internet Message Access Protocol makes it so you get control over how you download your mail, with it, you also gain some much-needed security. It has some serious authentication features. IMAP4 is the current version.

Pop en guncel ornegi pop3 dir. 2004ten beri pop4e gcilme konusuluyor fakat hala bir degisim yok.
Pop email uzerinden paket gonderimlerinde kullanilir.
Imap ise internette mesajlara maillere gonderim/alim saglayan portumuz.
Bu portlar yazilim zamani belirlenmis portlar.

The Process/Application Layer Protocols

RDP (TCP 3389): Remote Desktop Protocol is a proprietary protocol developed by Microsoft. It allows you to connect to another computer and run programs. Windows, and Macs now come with a preinstalled RDP client.

TLS/SSL (TCP 995/465): Both Transport Layer Security and its forerunner, Secure Sockets Layer, are cryptographic protocols that are useful for enabling secure online data-transfer activities like browsing the Web, instant messaging, Internet faxing, and so on.

CLARUSWAY©

Windpws mac isletim sistemlerine baglanabilmemiz icin bizim rdp kullanmamiz gerekiyor.
3389 uncu portta calisiyor bir arayuz gorebilmemiz adina.
Linuxte bir arayuze ihtiyac duymadigimiz icin mesela buna gerek duymuyoruz.
Windows isletim sistemi uzerinden remote bir bilgisayara baglanmak istedigimizde rdp uzerinden baglanacagiz.

Tls/ssl duydugumuzda aklimiza kendi telefon gorusmelerimiz gelebilir.
Eger https gorursek bir yerde bileecegiz ki bu tls veya ssl ile sifrelenmistir.
Tls/ssl devops tarafinda ve sinav zamaninda cok karsilasacagimiz konu.
Bunu duydugumuz an aklimiza data transfer sirasinda sifreleme gelecek.

The Process/Application Layer Protocols

SIP (VoIP) (TCP or UDP 5060/TCP 5061): Session Initiation Protocol is a hugely popular protocol used to construct and deconstruct multimedia communication sessions for many things like voice and video calls, video conferencing, streaming multimedia distribution, instant messaging, presence information, and online games over the Internet.

RTP (VoIP) (UDP 5004/TCP 5005): Real-time Transport Protocol describes a packet-formatting standard for delivering audio and video over the Internet.

VOIP IP uzerinden ses iletmek uzere acilmis bir port kanali. Video konferasnlarinda, gorusmelerinde vs kullanilir ses iletebilmek icin.
Rtp protokolleri bizim ici gercek zamanli yollayabilmek noktasinda cok onemli hale geldi.
Mesela canli yayinlar vs aninda iletim isteyen durumlar.

The Process/Application Layer Protocols

MGCP (Multimedia) (TCP 2427/2727): Media Gateway Control Protocol is a standard protocol for handling the signaling and session management needed during a multimedia conference.

H.323 (Video) (TCP 1720): H.323 is a protocol that provides a standard for video on an IP network that defines how real-time audio, video, and data information is transmitted.

Her multimedia konferansi icin mgcp protokolu kullanilir.

En farkli protokol adi h.323 protokoludur isim olarak.
Tcp tabanli gercek zamanli bir protokoldur. Yani aninda ses, goruntu ve data gonderim yapmakla mukelleftir.
Netten film izleme vs icin kullanilan codec diye ifade edilen terim budur.

The Process/Application Layer Protocols

SNMP (UDP 161/TCP 25): Simple Network Management Protocol collects and manipulates valuable network information. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information. This protocol can also stand as a watchdog over the network, quickly notifying managers of any sudden turn of events. Besides, SNMP can help simplify the process of setting up a network as well as the administration of your entire internetwork.

Troubleshooting yaparken kullanmak amaciyla olusturulmus bir porttur.
Mesela bir tool kullaniyor ve onun amaci troubleshooting yapmak. Networkle ilgili bir hata bulmak mesela. Iste bu toollarda kullandigimiz protokol SNMP protokoludur genel manada.
Hem tcp hem udp kullanir.

The Process/Application Layer Protocols

HTTP (TCP 80): Hypertext Transfer Protocol is used to manage communications between web browsers and web servers.

HTTPS (TCP 443): HTTP Secure uses the Secure Socket Layer (SSL). It is the secure version of the HTTP.

NTP (UDP 123): Network Time Protocol is used to synchronize the clocks on our computer to one standard time source. This protocol works by synchronizing devices to ensure that all the computers on a given network agree on the time.

CLARUSWAY©

Httpler bizim web browserlarimizin web serverlarla iletisime girip, karsilanmayi gerceklestirdigi protokollerdir. Https secure modda gerceklesir.

Ntp ise mesela pclerimizde default olarak saat ve tarih ayari yapilir. Iste bu ntp protokolu ile gerceklestirilir. Biz region degistirince saatlerde default olarak atanir. Bu su sekilde olur: bizim dunyadaki tum saatleri icinde barindiran serverimiz var. Bizim region degistirmemiz halinde bilgisayarimiz bu time serverla iletisime gecip hemen saati bize donduruyor.

The Process/Application Layer Protocols

LDAP (TCP 389): Lightweight Directory Access Protocol standardizes how you access directories.

IGMP: Internet Group Management Protocol is the TCP/IP protocol used for managing IP multicast sessions. It accomplishes this by sending out unique IGMP messages over the network to reveal the multicast-group landscape and to find out which hosts belong to which multicast group. IGMP works at the Network layer and doesn't use port numbers.

Ldap bizim bir standartlastirilmis klasorumuzden (yani mesela bir kafede servera bagli tum bilgisayarlar icin uygulayacagim baglanti isini tuttugum klasoru)diger klasorlere uyguladigim protokol.

Igmp onemli degil. Onu atladik.

The Process/Application Layer Protocols

DHCP (UDP 67/68): Dynamic Host Configuration Protocol assigns IP Address to hosts. It allows for easier administration and works well in small to very large network environments. Many types of hardware can be used as a DHCP Server, including a Cisco Router. There is a lot of information a DHCP server can provide to a host when the host is requesting an IP address from DHCP Server like

- IP Address
- Subnet Mask
- Domain Name
- Default Gateways
- DNS Server Address

Bu protokol bizler icin cok onemli.
Bizim cihazlarimizin networkte dolasabilmesi icin iki tane adrese ihtiyaci vardi (MAC, IP)
Dhcp server bizim routerimiz.
Her cihazdan unik ip adresi almasi adina uyguladigi kurallar butunudur.
Routerimiz oldugu gibi bir network cihazimin kendisi de olabilir.
Ip adresi, subneti, domain name, gatewayleri ve dns derver adresleri icerir.

4 The Transport Layer Protocols

Segmentasyonun basladigi layerdaki protokolleri ogrenecegiz burada.

The Transport Layer Protocols

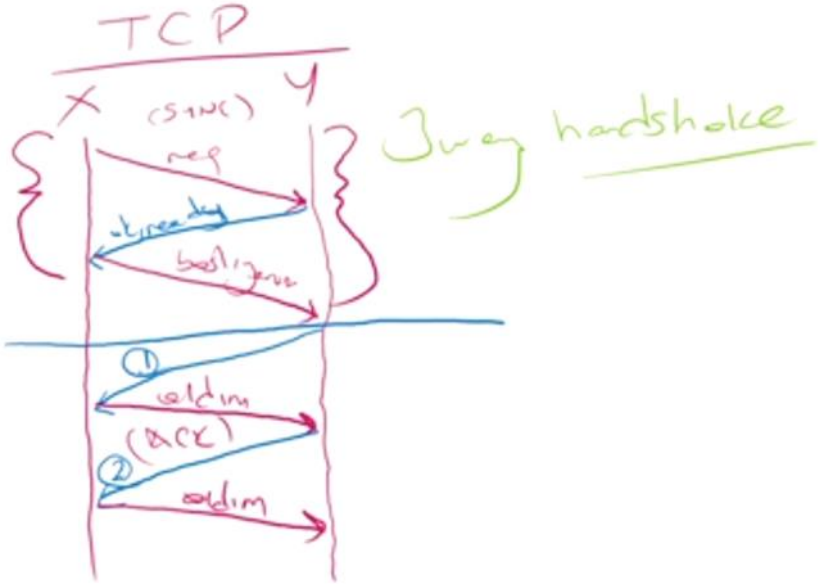
- **TCP** and **UDP** are the main protocols for Transport Layer
- **TCP** is full-duplex, connection-oriented, reliable and accurate protocol
- In order to send information, TCP establishes a connection with the receiving host *(connection-oriented)*
- **TCP** takes information and breaks it into segments
- **TCP** sends this segments in the order that application intended
- After segments are sent **TCP** waits for the acknowledgement for each segment
- Retransmits the segments that aren't acknowledged *(reliable)*

Tcp gonderimin her asamasini takkip eder. Eger gonderilmeyen bir ileti varsa onu acknowledgement yapiyor yani iletinin, segmentasyon asamasinin takibini kontrolluce takip ediyor.
Guveilir demek oluyor bu da
Sirali bir gonderim yapar.

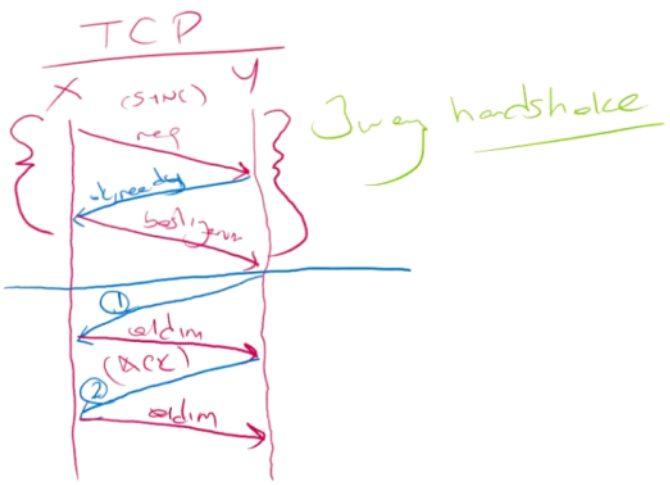
The Transport Layer Protocols

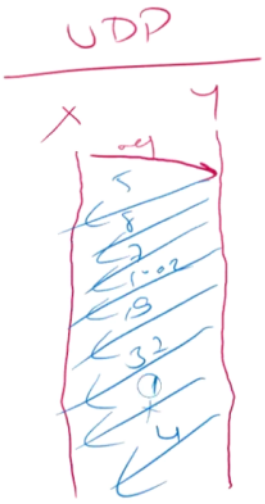
- **UDP** uses less bandwidth compared to **TCP**
- **UDP** transports data much faster than **TCP**
- **UDP** doesn't care the order of the segments
- **UDP** doesn't care if the segment is received by the recipient (no acknowledgement) *(not reliable)*
- **UDP** doesn't establish a connection with the receiver *(connectionless protocol)*
- Mostly used while speed is more important than reliability (like video teleconferencing or SNMP)

Udp ise tcp gibi degil.
Guveilir olmayan kargo. Gonderme ilemi yapacagini soyler ama adres bulamazsa ya da iletimde bi hata olursa bunun takibini yapmaz.
Guvenilmez kargocu gibi.
Unacknowledgement



Her paket sonrasi aldim geri donutnu vermesi guvenilir kismi.





Udp daha hizli ama guvensiz
Bunu hiz ihtiyaci olanlar kullanir
Mesela mac seyredenler canli udp kullanir

The Transport Layer Protocols

TCP	UDP
Secure	Unsecure
Connection-oriented	Connectionless
Slow	Fast
Guaranteed transmission	No guarantee
Flow control	No flow control
Reliable	Unreliable
Virtual circuit	No virtual circuit
Acknowledgement	No acknowledgement
20 bytes header	8 bytes header

5 The Internet Layer Protocols

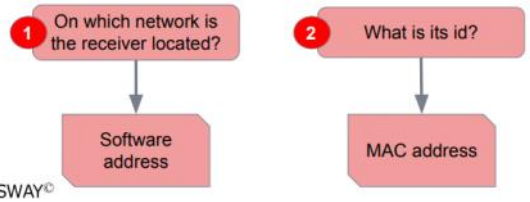
The Internet Layer Protocols

- Main functions: routing and providing a single network interface to upper layers
- Main protocols:
  - Internet Protocol (IP)
  - Internet Control Message Protocol (ICMP)
  - Address Resolution Protocol (ARP)
  - Reverse Address Resolution Protocol (RARP)

Ip adressimizin calistigi layer burasidir.
Ana mesele yonlendirmek ve bir ust layera single network saglamak
Ip haricinde baska protokoller de burada calisir

The Internet Layer Protocols

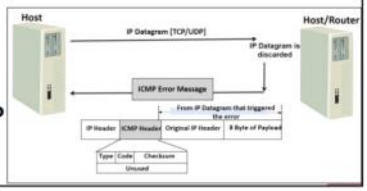
- **Internet Protocol (IP)** looks at each packet's destination address, then, using a routing table, it decides where a packet is to be sent next, choosing the best path.
- To find the receiver host, sender has to find out:



CLARUSWAY©

The Internet Layer Protocols

- **Internet Control Message Protocol (ICMP)** is a management protocol and messaging service provider for IP
- **ICMP** messages are sent as IP packets
- Common events that **ICMP** relates to:
  - Destination unreachable
  - Buffer full
  - Hops
- **Ping** and **Traceroute** use **ICMP**

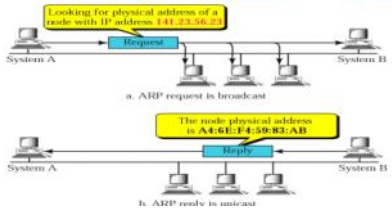


CLARUSWAY©

Biz bir message gonderdigimizde mesela bilgisayaramizdan ciktigi an bizim artik onun uzerinde bir yetkimiz yok. Burada devreye ICMP giriyor.
Ip paketleri halinde iletim sagliyor.
Gidilmesi en hizli yolu bululp paketleri iletiyor.
Ping bir pong gonderdigimizde yani bi ileti gonderdigimizde karsilik olarak aldigimiz cevap hizi.
Ping bu protokolu kullanarak calisiyor.

The Internet Layer Protocols

- **Address Resolution Protocol (ARP)** is a procedure for mapping a dynamic **IP address** to a permanent physical machine address in a LAN
- Essentially matches IPv4 Address 32-bit ⟷ MAC Address 48-bit

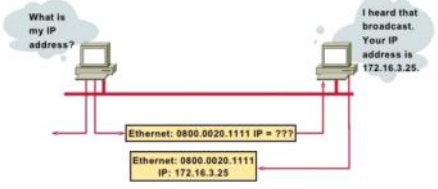


CLARUSWAY©

Arp bizim icin onemli. Hepimizin cihazinda bir arp tablosu bulunur. Router baglantisinda en son router baglantisininyani iletim yapilacak MAC adresinin roterinin kendi LAN adresini bulana kadar bu protokol isler. Ve gonderim yapmak istedigimiz IP adresinin LANini bulana kadar router connecti devam eder ve en sonunda LANa ulasir.

The Internet Layer Protocols

- Host machines that don't know their own IP address can use the **Reverse ARP (RARP)** protocol for discovery



- ARP is replaced by **Neighbor Discovery Protocol** with the use of IPv6

CLARUSWAY©

DCP IP adresini bulamadiginda ulasamadiginda, bu protokol devreye girer.
Komsulardan IP adresini ogrenmeye calismakla yukumludur.
Sadece dcp ile iletisim kuramadigi durumlarda gecerlidir. Aksi takdirde zaten arp ip adresini bilir.