TCP/IP

(Transmission Control Protocol/Internet Protocol)

防火牆(port)

dos 相關指令：ipconfig

127.0.0.1 特殊位址

What is a network protocol

A protocol is the special set of rules that end points in a telecommunication connection use when they communicate.

- specify interactions between the communicating entities.
- exist at several levels in a telecommunication connection.
- each protocol has its own method of how data is formatted when sent and what to do with it once received, how that data is compressed or how to check for errors in data.

Connectionless/Stateless Protocols

communication between two network endpoints in which a message can be sent from one end point to another without prior arrangement.

The device at one end of the communication transmits data to the other, without first ensuring that the recipient is available and ready to receive the data.

The device sending a message simply sends it addressed to the intended recipient.

If there are problems with the transmission, it may be necessary to resend the data several times

IP is a connectionless protocol.With IP(actually TCP), messages (or other data) are broken up into small independent "packets" and sent between computers via the Internet. IP is responsible for "routing" each packet to the correct destination.

TCP/IP protocol family

- IP : Internet Protocol
  - UDP : User Datagram Protocol
    - RTP, traceroute
  - TCP : Transmission Control Protocol
    - HTTP, FTP, ssh

TCP/IP

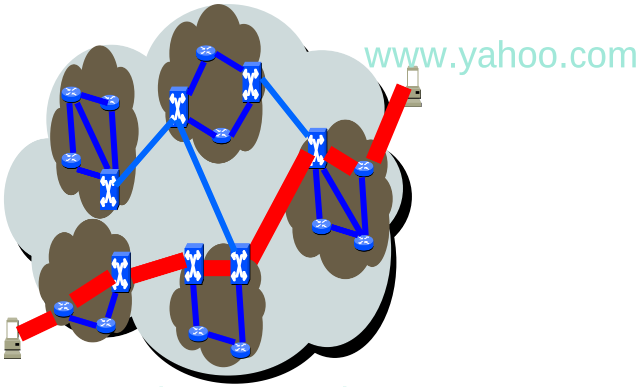
TCP - Transmission Control Protocol

TCP is responsible for breaking data down into small packets before they can be sent over a network, and for assembling the packets again when they arrived to the destination.

IP - Internet Protocol

IP takes care of the communication between computers. It is responsible for addressing, sending and receiving the data packets over the Internet.

TCP characteristics



- Connection oriented protocol

client and server must establish a connection before data transferring

- Provides reliability
  - ○ data acknowledgement(資料順序)
  - ○ 3 way handshake（三方握手）
  - ○ checksums on both header and contents（資料正確）
- Implements flow control(流量控制)
  - ○ sender cannot overwhelm receiver with data

連結導向(Connection-oriented)
□ 在發送資料前會建立一個連結，並使用錯誤檢查等方式確保資料能夠正確無誤的傳送，如果發生錯誤會自動嘗試重傳資料
□ 電話是一種連結導向的通訊方式，使用者必須先確定電話號碼，然後撥電話，若是無人接聽料無法建立連結，若是接聽則發話與受話端可藉由交談來確認資料正確傳遞

IP characteristics

無連結導向(Connectionless-oriented)
□ 在資料傳送前，並不透過事先的連線協調及建立連線才傳送資料；在資料送達對方時亦不送回確認資訊，所以效率較高，但錯誤率相對也較高□ 廣告郵件是一種無連結傳送，廠商將廣告傳單加上地址交由郵局寄送，但不能確定地址與收件人是否正確，也不能確定收件人是否能正確收到資料。
□ 無連結傳送也可用來建立連結導向的傳送，在上面廣告郵件的例子中，可使用回函的方式來確認消費者是否接收到廣告郵件

- Connectionless protocol
- Unreliable protocol
  - Cannot tell if packets were lost or out of order

TCP/IP key features

Logical addressing

Routability

Name resolution

Multiplexing

Interoperability

Logical addressing

big networks into smaller networks using devices such as routers to reduce network traffic.A network can be again subdivided into smaller subnets so that a message can travel efficiently from its source to the destination.(IP address)

Routability

TCP/IP data packets can be moved from one network segment to another.

Name resolution

TCP/IP allows to use human-friendly names, which are very easy to remember . Name Resolutions servers (DNS Servers) are used to resolve a human readable name (also known as Fully Qualified Domain Names (FQDN)) to an IP address and vice versa.

Interoperability

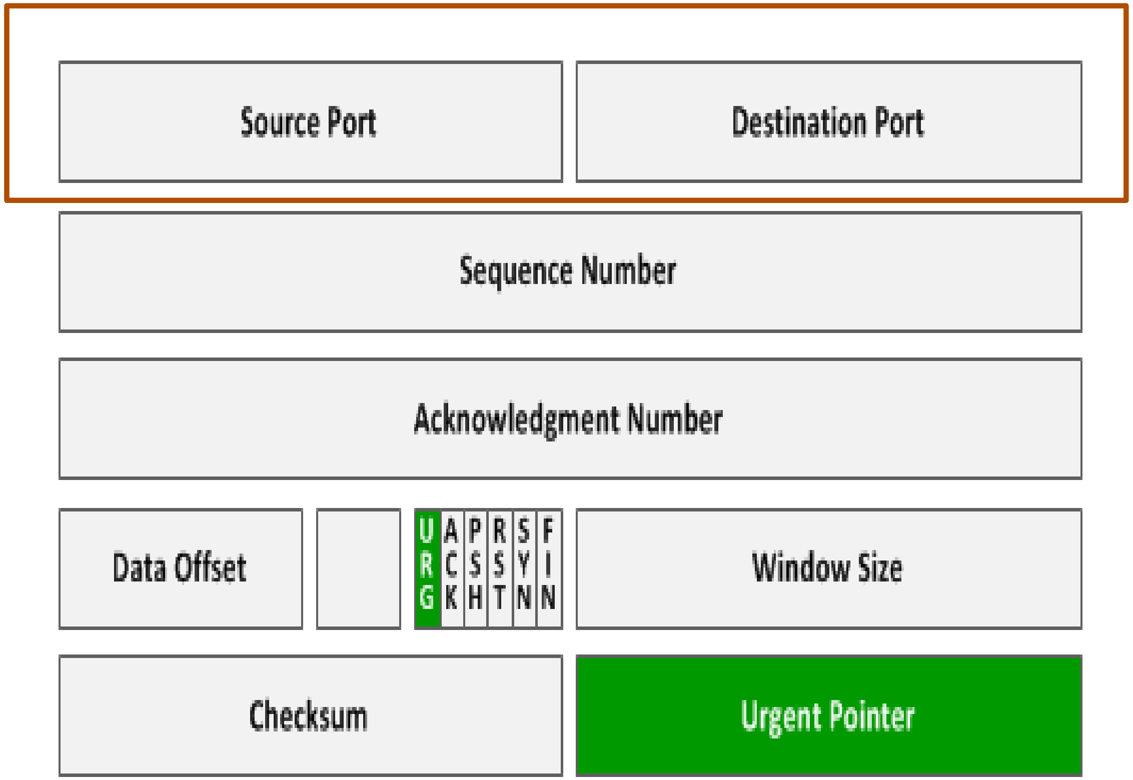
can work in a heterogeneous network.TCP/IP eliminates the cross-platform boundaries.

Multiplexing

accepting data from different applications and directing that data to different applications listening on different receiving computers

TCP packet header

The Internet Protocol header carries several information fields, including the source and destination host addresses . A TCP header follows the internet header, supplying information specific to the TCP protocol.



Source Port

Destination Port

Sequence Number

Acknowledgment Number

Data Offset

URG

ACK

PSH

RST

SYN

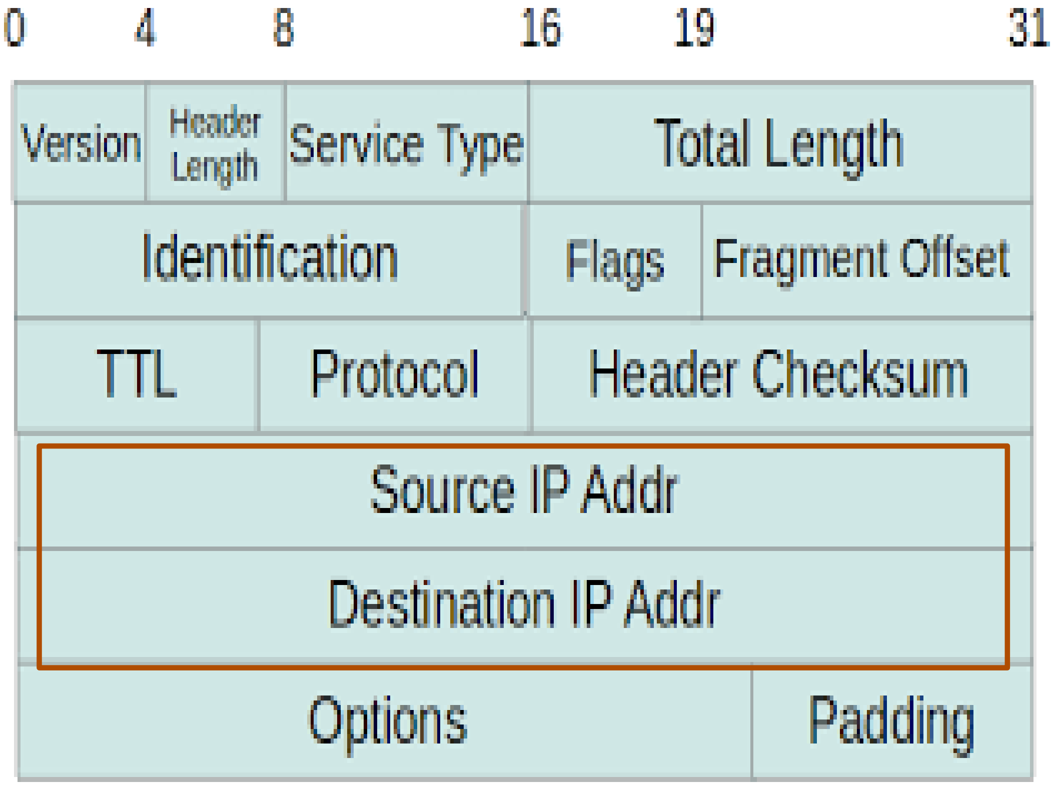
FIN

Window Size

Checksum

Urgent Pointer

IP packet header



0	4	8	16	19	31
Version	Header Length	Service Type	Total Length		
Identification			Flags	Fragment Offset	
TTL		Protocol	Header Checksum		
Source IP Addr					
Destination IP Addr					
Options				Padding	

What is a port..

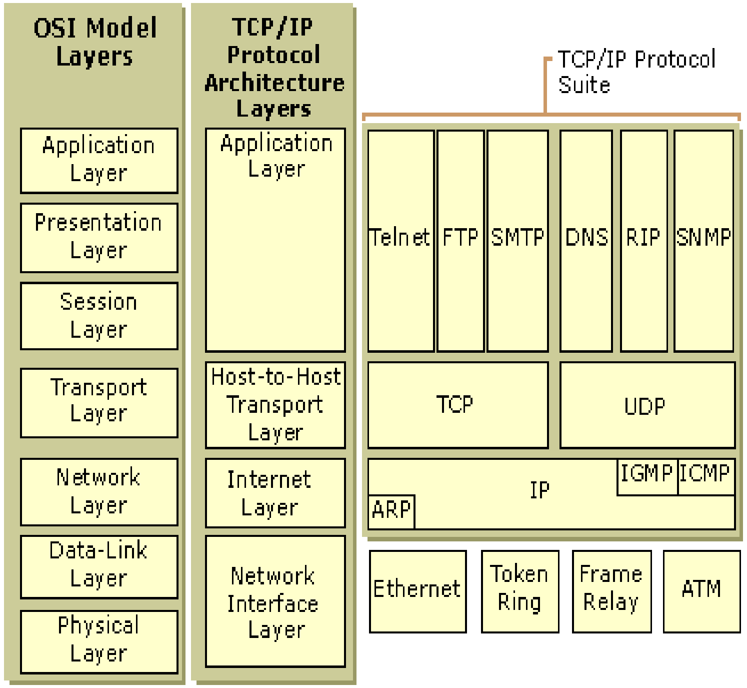
a **port** is an endpoint of communication in an operating system.

A port is always associated with an IP address of a host and the protocol type of the communication, and thus completes the destination or origination address of a communication session. A port is identified for each address and protocol by a 16-bit number, commonly known as the **port number**.

Default port number for TCP is 1.

ftp:21, telnet:20, http80

TCP/IP layered architecture



OSI Model Layers

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data-Link Layer

Physical Layer

TCP/IP Protocol Architecture Layers

Application Layer

Host-to-Host Transport Layer

Internet Layer

Network Interface Layer

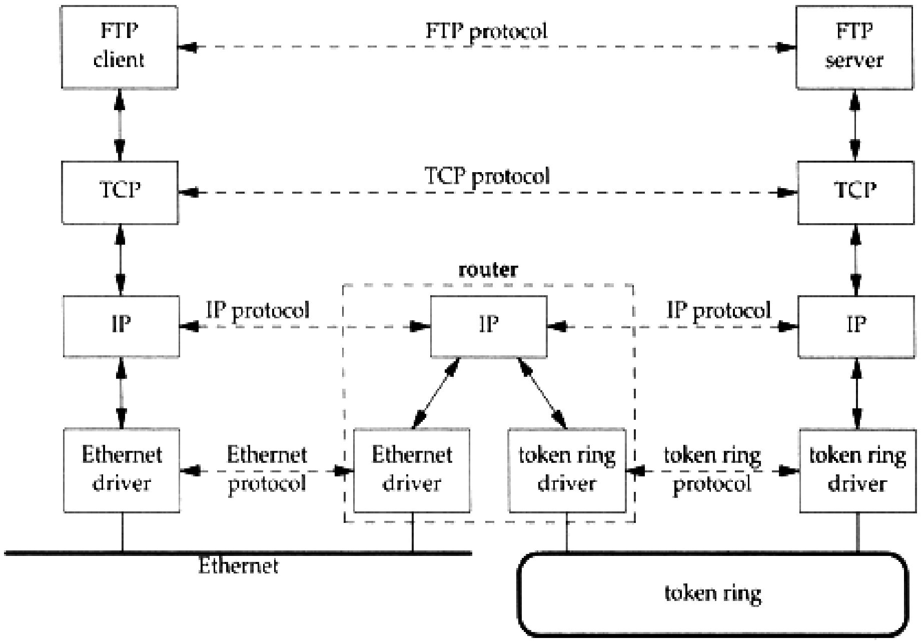
TCP/IP Protocol Suite

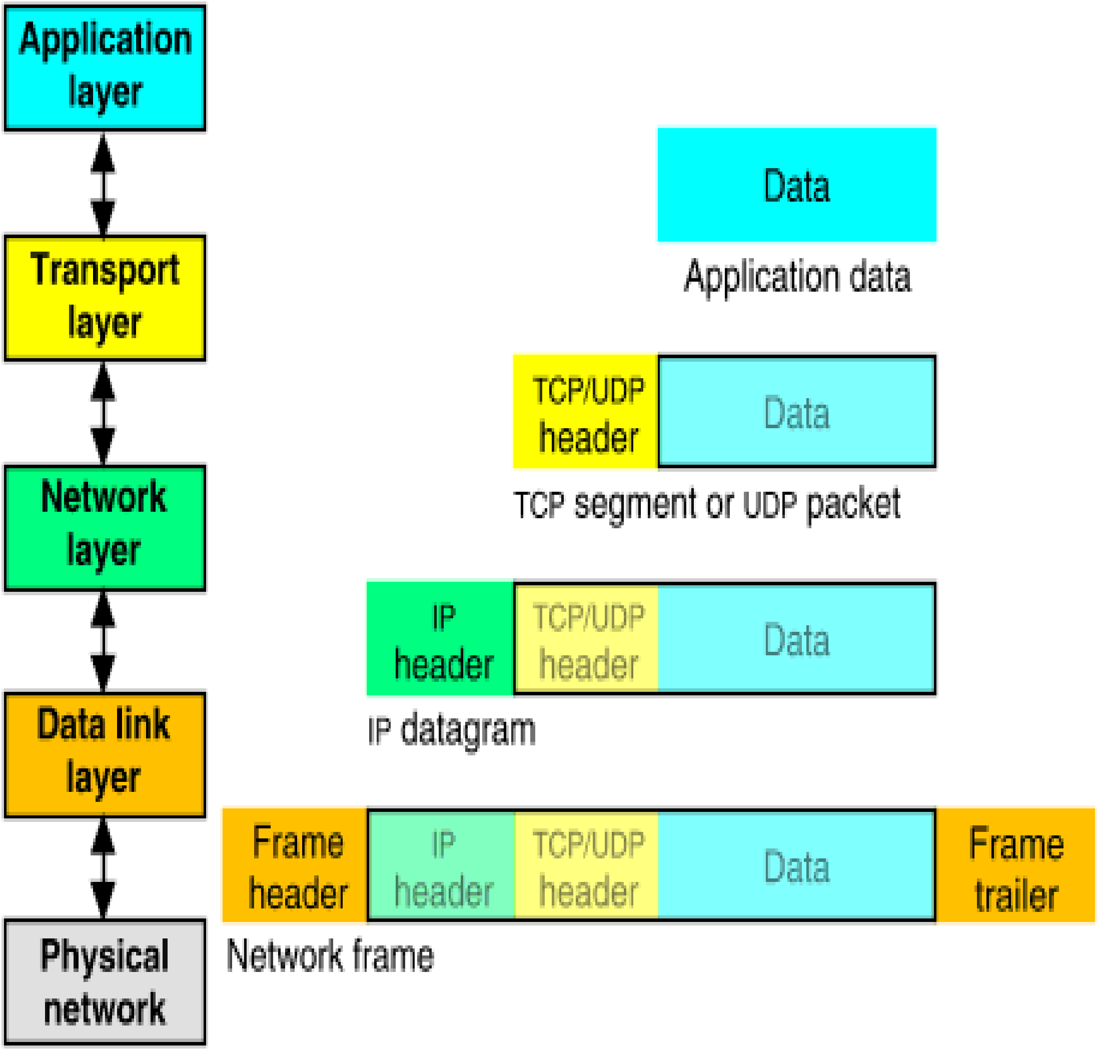
Telnet, FTP, SMTP, DNS, RIP, SNMP

TCP, UDP

IP, IGMP, ICMP, ARP

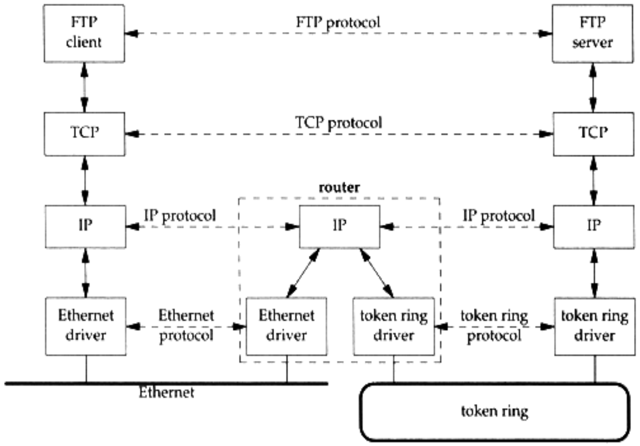
Ethernet, Token Ring, Frame Relay, ATM




Application layer
Transport layer
Network layer
Data link layer
Physical network
Data
Application data
TCP/UDP header
Data
TCP segment or UDP packet
IP header
TCP/UDP header
Data
IP datagram
Frame header
IP header
TCP/UDP header
Data
Frame trailer
Network frame

Network interface layer

The Network Interface layer is responsible for placing TCP/IP packets on the network medium and receiving TCP/IP packets off the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. In this way, TCP/IP can be used to connect different network types.

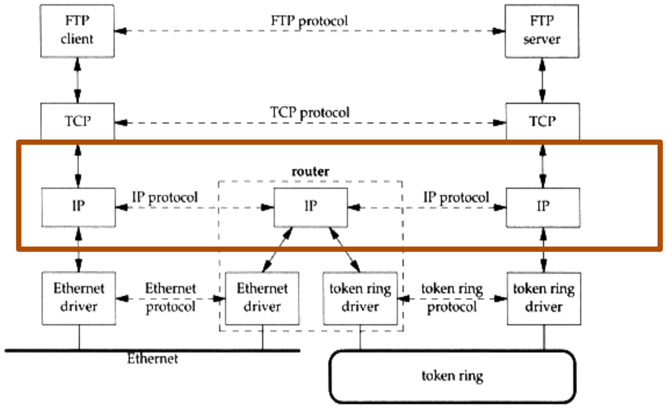


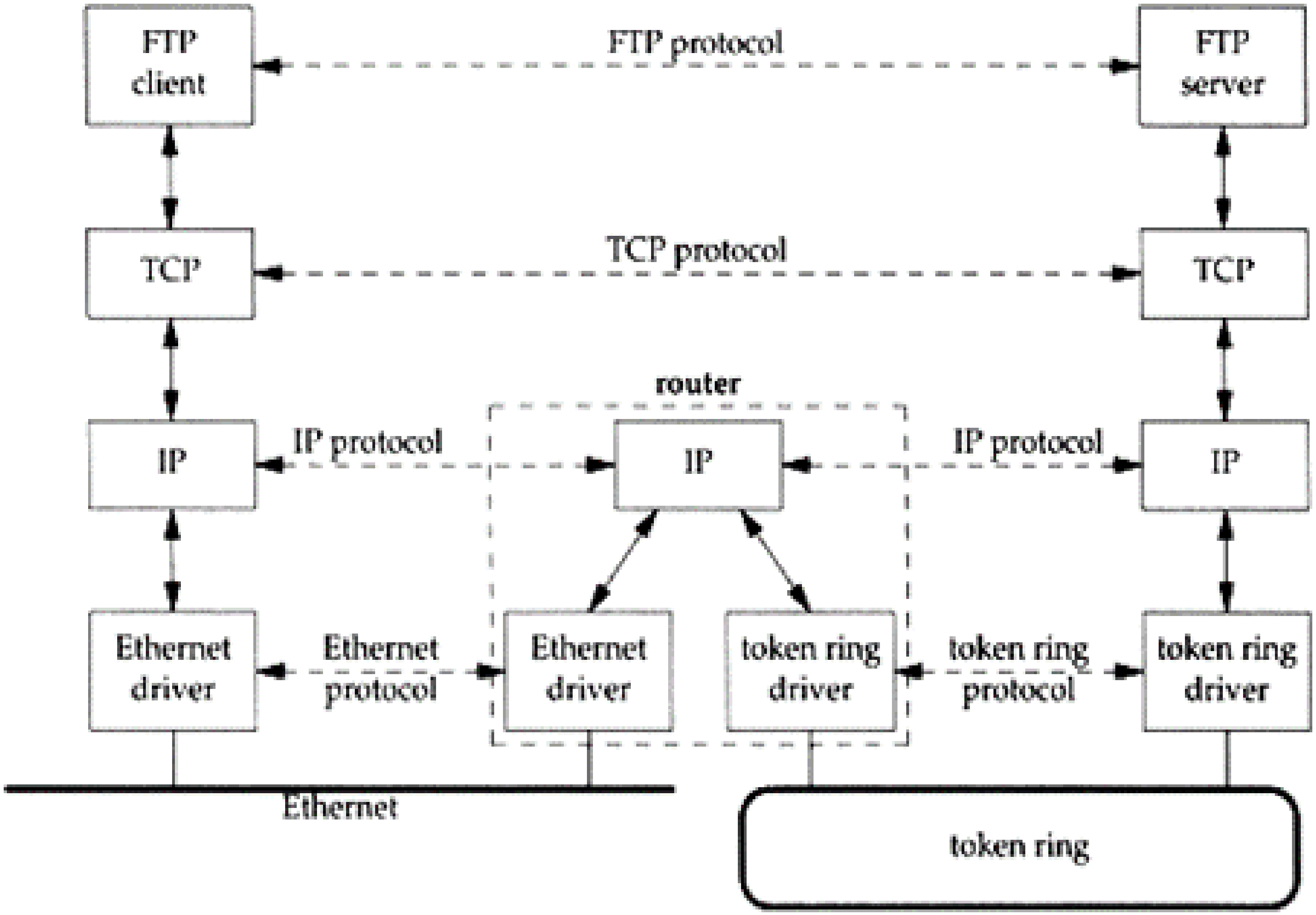
Internet layer

The Internet layer is responsible for addressing, packaging, and routing functions. The core protocols of the Internet layer are IP, ARP, ICMP, and IGMP.

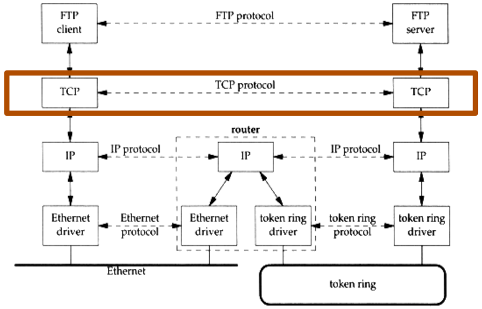
The *Internet Protocol* (IP) is a routable protocol responsible for IP addressing, routing, and the fragmentation and reassembly of packets.

The *Address Resolution Protocol* (ARP) is responsible for the resolution of the Internet layer address to the Network Interface layer address such as a hardware address.




FTP client
FTP protocol
FTP server
TCP
TCP protocol
TCP
router
IP
IP protocol
IP
IP protocol
IP
Ethernet driver
Ethernet protocol
Ethernet driver
token ring driver
token ring protocol
token ring driver
Ethernet
token ring

Transport layer

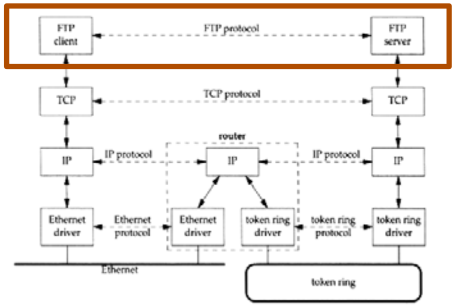


The Transport layer is responsible for providing the Application layer with session and datagram communication services. The core protocols of the Transport layer are *Transmission Control Protocol* (TCP) and the *User Datagram Protocol* (UDP).

TCP provides a one-to-one, connection-oriented, reliable communications service. TCP is responsible for the establishment of a TCP connection, the sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission.

UDP provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when the overhead of establishing a TCP connection is not desired or when the applications or upper layer protocols provide reliable delivery.

Application layer



The Application layer provides applications the ability to access the services of the other layers and defines the protocols that applications use to exchange data. There are many Application layer protocols and new protocols are always being developed.

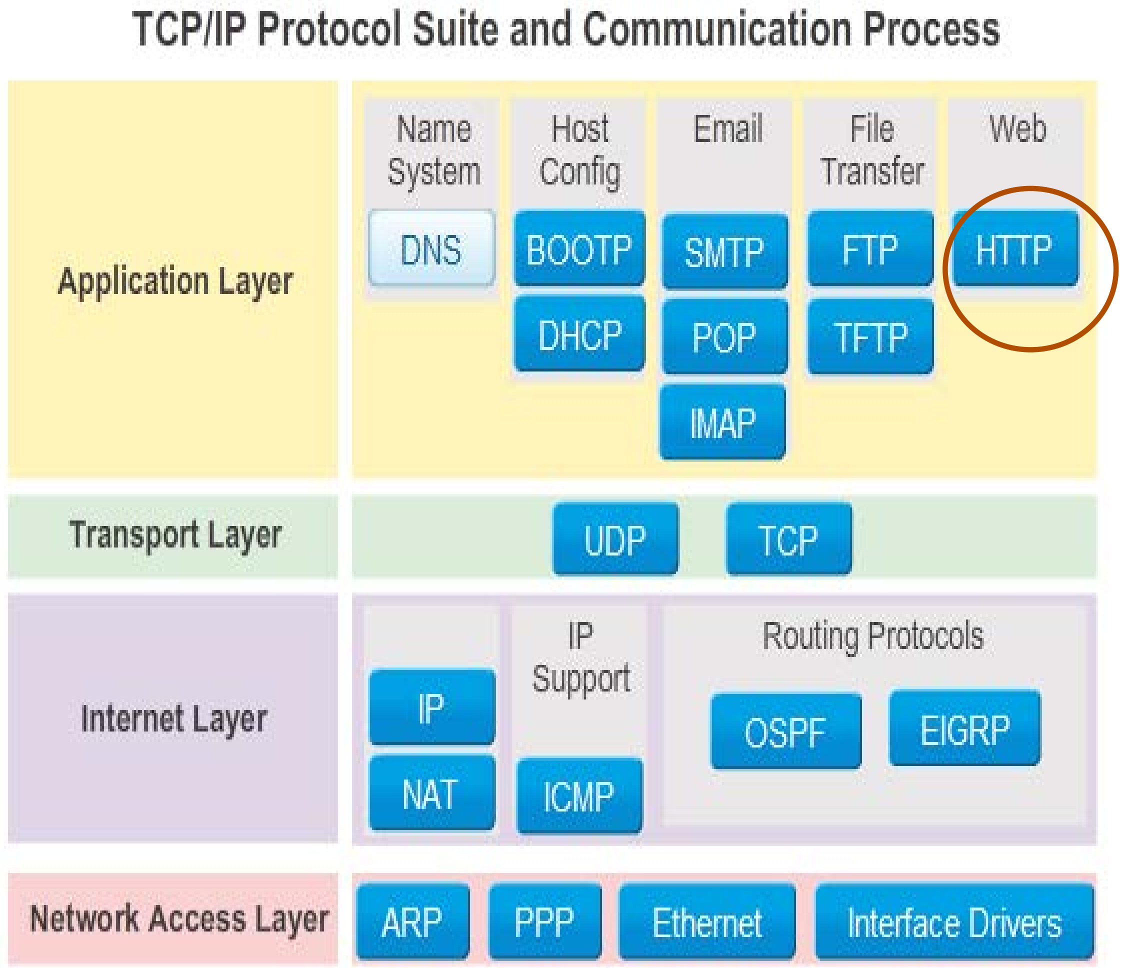
following Application layer protocols help facilitate the use and management of TCP/IP networks:

The Domain Name System (DNS) is used to resolve a hostname to an IP address.

The Routing Information Protocol (RIP) is a routing protocol that routers use to exchange routing information on an IP internetwork.

The Simple Network Management Protocol (SNMP) is used between a network management console and network devices (routers, bridges, intelligent hubs) to collect and exchange network management information.

TCP/IP protocol Suite



位址解析協定（Address Resolution Protocol,ARP)

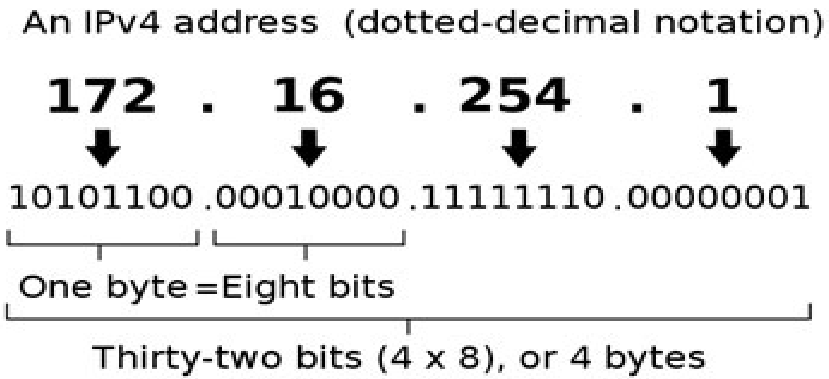
IP routers

When an IP packet is sent from a computer, it arrives at an IP router.

The IP router is responsible for "routing" the packet to the correct destination, directly or via another router.

The path the packet will follow might be different from other packets of the same communication. The router is responsible for the right addressing, depending on traffic volume, errors in the network, or other parameters.

IP Addresses


An IPv4 address (dotted-decimal notation)
172 . 16 . 254 . 1
10101100.00010000.11111110.00000001
One byte=Eight bits
Thirty-two bits (4 x 8), or 4 bytes

An IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination.

IPv4 uses 32 binary bits to create a single unique address on the network. An IPv4 address is expressed by four numbers separated by dots. Each number is the decimal (base-10) representation for an eight-digit binary (base-2) number

216.27.61.137

IPv6 uses 128 binary bits to create a single unique address on the network. An IPv6 address is expressed by eight groups of hexadecimal (base-16) numbers separated by colons, as in

2001:cdba:0000:0000:0000:0000:3257:9652.

Domain names

The network software generally needs a 32-bit Internet address (IP i.e.: 192.123.12.2) in order to open a connection.

Users prefer to deal with computer names rather than numbers. Thus there is a database that allows the software to look up a name and find the corresponding number.

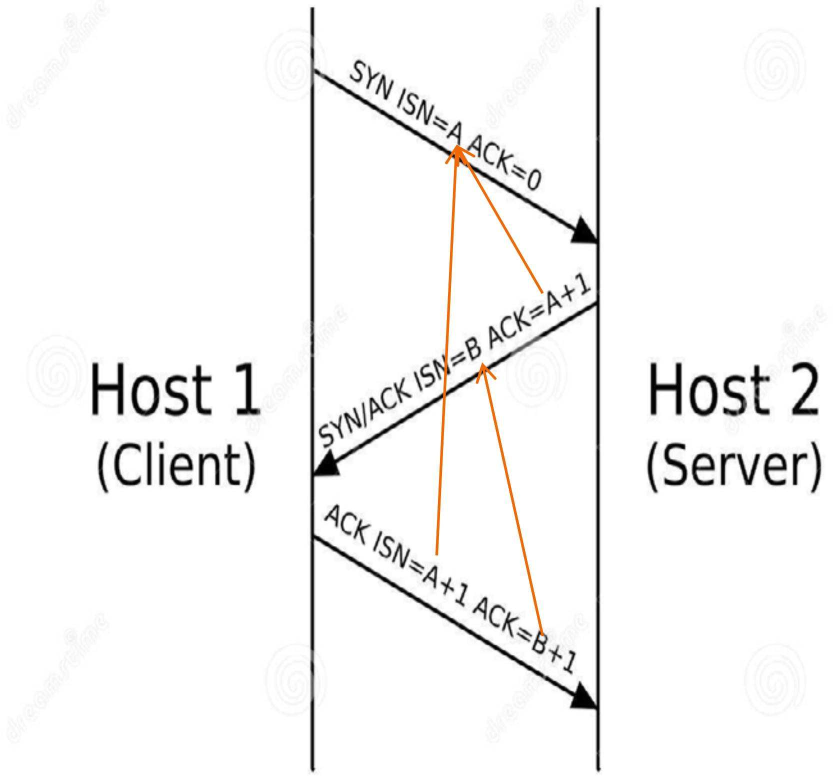
Each system would have a file that listed all of the other systems, giving both their name and number.These files have been replaced by a set of name servers that keep track of host names and the corresponding Internet addresses.

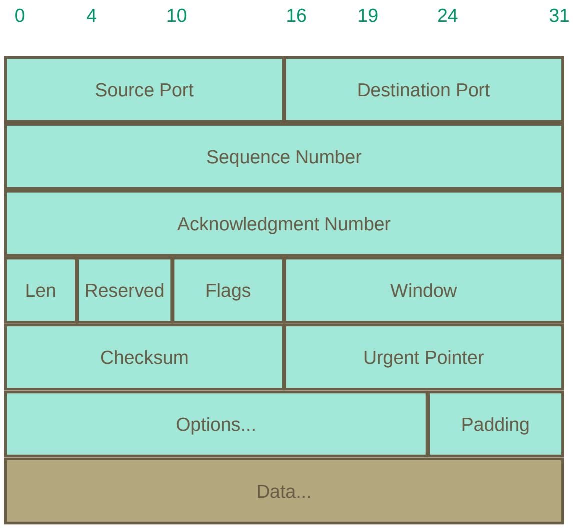
TCP communication

TCP communication mainly consists of four main tasks

- Establish a connection
- Data transmission
- Error detection/correction/acknowledgement
- Connection closure

3 way handshake





Source Port | Destination Port
Sequence Number
Acknowledgment Number
Len | Reserved | Flags | Window
Checksum | Urgent Pointer
Options... | Padding
Data...

Field	Purpose
Source Port	Identifies originating application
Destination Port	Identifies destination application
Sequence Number	Sequence number of first octet in the segment
Acknowledgment #	Sequence number of the **next** expected octet (if ACK flag set)
Len	Length of TCP header in 4 octet units
Flags	TCP flags: SYN, FIN, RST, PSH, ACK, URG
Window	Number of octets from ACK that sender will accept
Checksum	Checksum of IP pseudo-header + TCP header + data
Urgent Pointer	Pointer to end of “urgent data”
Options	Special TCP options such as MSS and Window Scale