Chapter 6 - Fundamentals of TCP/IP Transport, Applications and Security

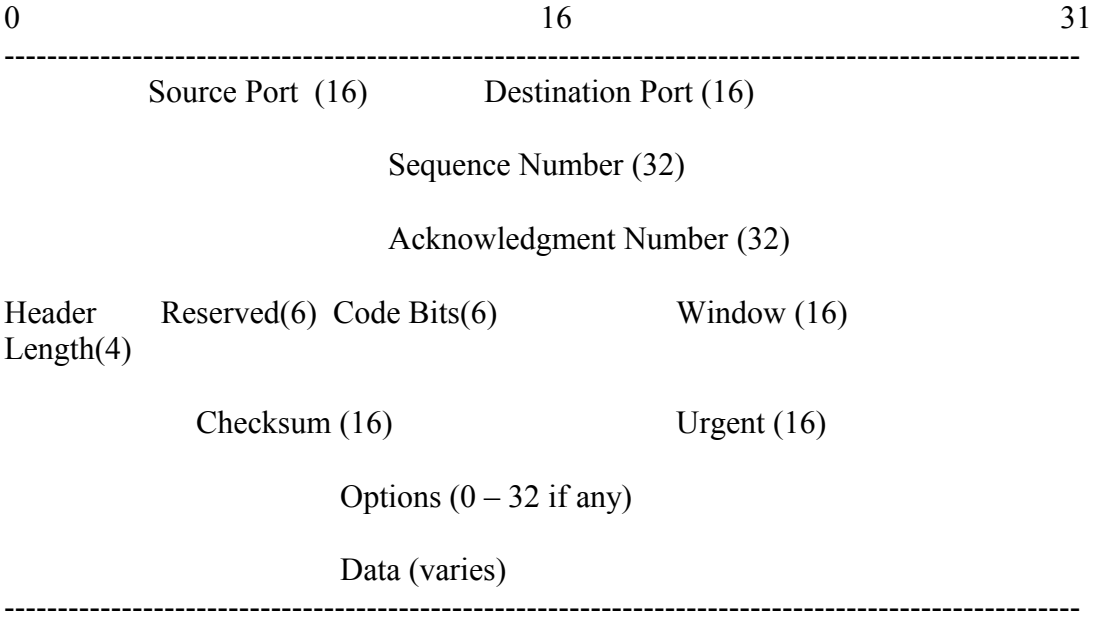
Major functions of Layer 4 – Transport layer protocol are error recovery and flow control. Most data link protocols notice errors a process called error detection, but then discard frames that have errors. TCP provides for re-transmission (error recovery) and helps to avoid congestion (flow control).

TCP/IP Transport Layer Features, only the first item is supported by UDP

Function	**Description**
Multiplexing using ports	Functions that allows the receiving hosts to choose the correct application for which the data is destined, based on the port number.
Error recovery (reliability)	Process of numbering and acknowledging data with sequence and acknowledgement header fields.
Flow control using windowing	Process that uses window sizes to protect buffer space and routing devices.
Connection establishment and termination	Process used to initialize port number, sequence and acknowledgement header fields
Ordered data transfer and data segmentation	Continuous stream of bytes from an upper layer process that is 'segmented' for transmission and delivered to upper layer process at the receiving device, with the bytes in the same order.

TCP provides error recovery but to do so it consumes more bandwidth and use more processing cycles. UDP does not perform error recovery but it takes less bandwidth and uses fewer processing cycles.

TCP Header Fields



Multiplexing using TCP port Numbers

TCP and UDP multiplexing enables the receiving computer to know which application to give the data to.

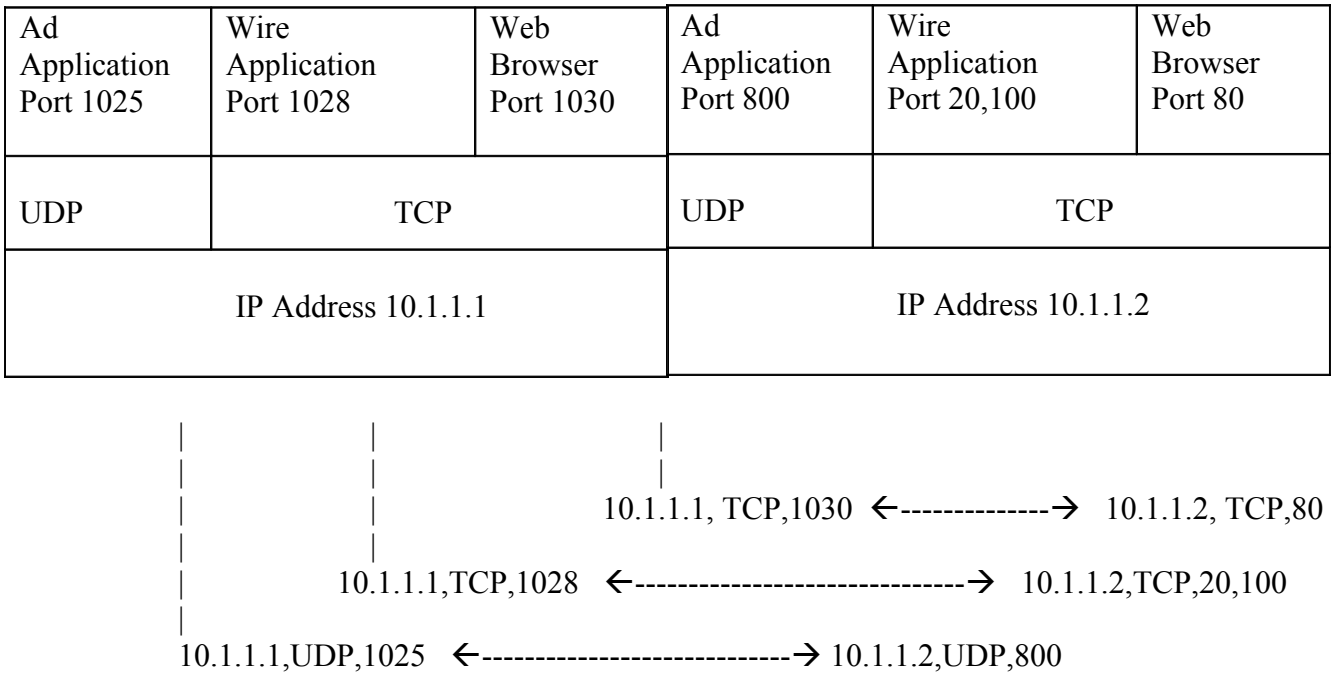
When two computers communicate between different applications, TCP and UDP segments use different destination port numbers so that the receiving computer knows which application to give the data to.

Multiplexing relies on a concept called **sockets.** A socket consists of three things:

- An IP Address
- A transport protocol
- A port number

For a webserver application the socket would be (10.1.1.2, TCP, Port 80) because, by default web servers use the well know port 80. When a client web browser connects to a web server it also uses a socket possibly like (10.1.1.1., TCP, Port 1030), client hosts typically allocate a unique **'dynamic port numbers'** starting at 1024 because port number below 1024 are reserved for well known applications such as web server.

Multiplexing based on socket ensures that data is delivered to the correct application. Applications that provide services such as FTP, Telnet and web servers. Open a socket using well-known port and listen for connection requests.



Connection between Sockets

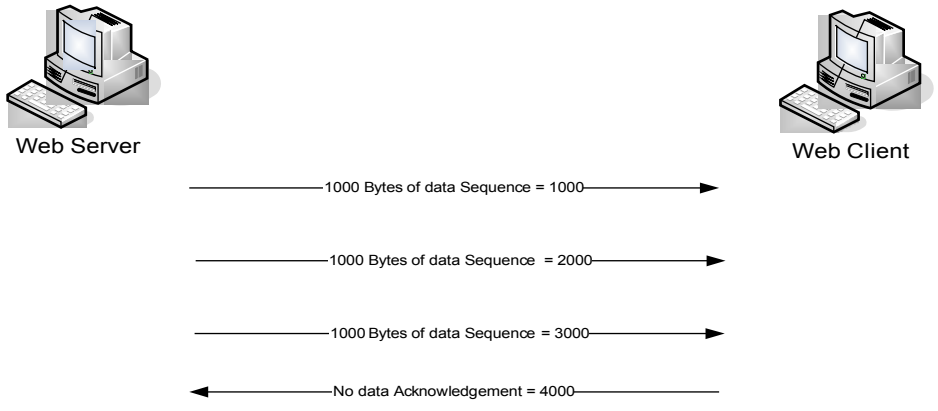
Popular applications and their well know ports

Port Number	Protocol	Application	
20	TCP	FTP data	
21	TCP	FTP control	
22	TCP	SSH	
23	TCP	Telnet	
25	TCP	SMTP	
53	UDP,TCP	DNS	
67,68	UDP	DHCP	
69	UDP	TFPT	
80	TCP	HTTP(WWW)	
110	TCP	POP3	
161	UDP	SNMP	
443	TCP	SSL	
16,384 - 32,767	UDP	RTP based Voice (VoIP) and Video	

Error Recovery (Reliability)

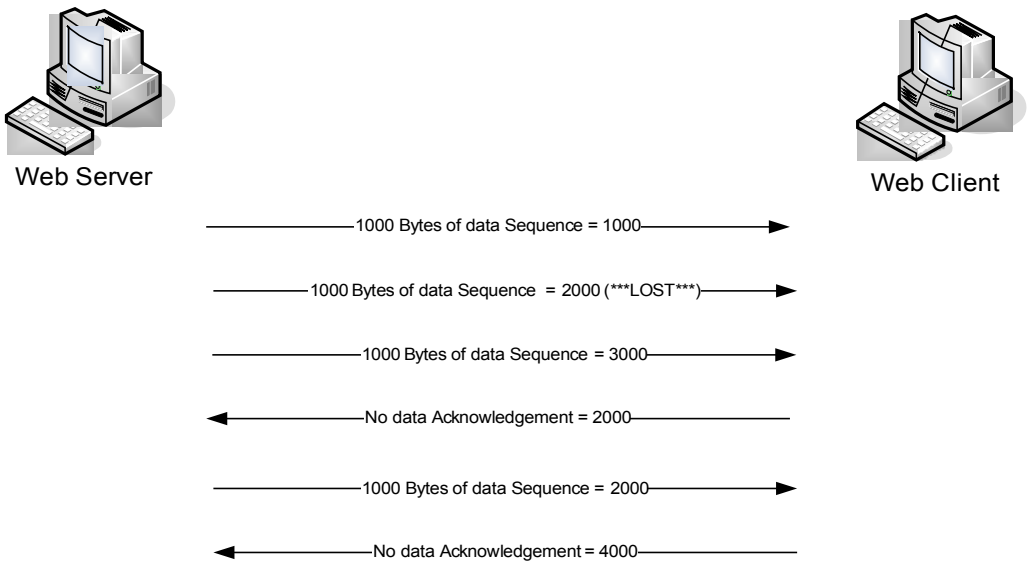
To accomplish reliability, TCP numbers data bytes using sequence and acknowledge fields in the TCP header. TCP achieves reliability in both directions, using sequence number field of one direction combined with the acknowledgement field in the opposite direction.

TCP Acknowledgement without errors



The acknowledgement field in the TCP header sent by the web client (4000) implies the next byte to be received, this is called ***forward acknowledgment***. The sequence number reflects the number of first byte in the segment. In this case each TCP segment is 1000 bytes long.

TCP Acknowledgement with errors

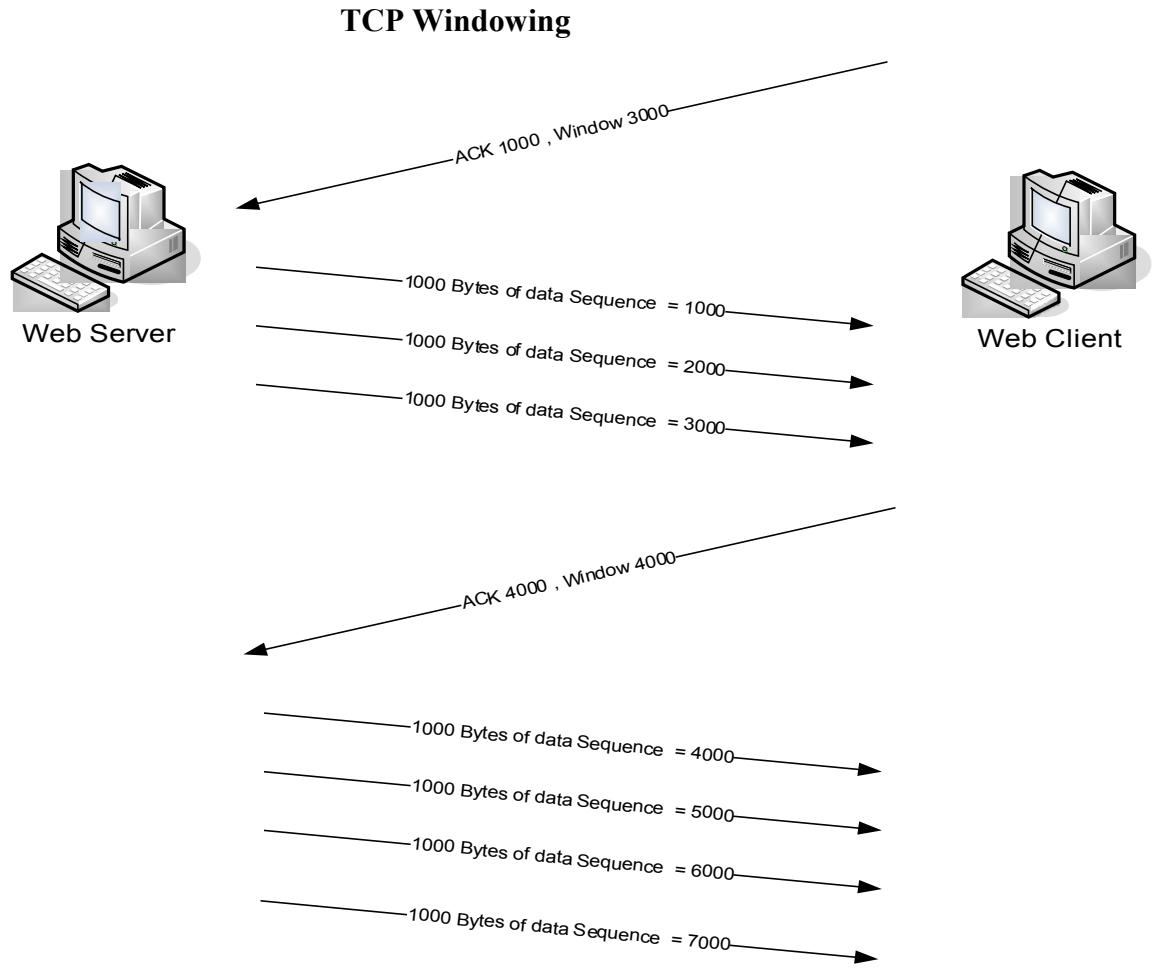


The second TCP segment was lost or is in error, web client's reply has an acknowledgement field = 2000, implying that the web client is expecting byte 2000 next, TCP functions at the web server re-sends the second segment and waits for an ACK=4000.

Flow Control using Windowing

TCP implements flow control by taking advantage of Sequence and Acknowledgment fields in the TCP header, along with another field called the Window field. Window field implies the maximum number unacknowledged bytes that are allowed at any point in time. The window starts small and grows until error occurs, additionally actual Sequence and Acknowledgments numbers also grows, so it is called dynamic window, or sliding window. When the window is full, the sender does not send, and thereby controls the flow of data.

Receiver grants window to the sender, sender send until the window is full, waits for the acknowledgement, if no errors occurred, the receiver grants larger window.



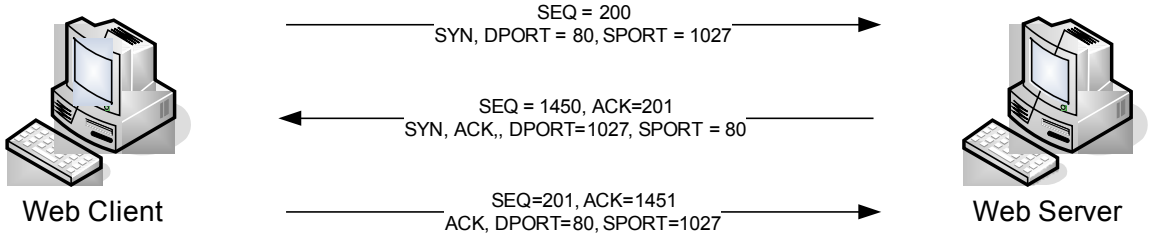
Windowing does not require that sender stops sending in all cases. If an acknowledgement is received before the window is exhausted, a new window begins and sender continues sending data until the current window is exhausted. The term Positive Acknowledgement and Re-transmission [PAR] is sometimes used to describe error recovery and windowing process that TCP uses.

Connection establishment and termination

TCP connection establishment refers to the process of initialling sequence and acknowledgement fields and agreeing on the port numbers used.

TCP header has no single socket field, of the three parts of the socket, IP address is implied by the source and destination ip address in the ip header, TCP is implied by the protocol type field in the ip header and also because TCP header is in use. Only part of the socket that needs to be encoded in the TCP header are the port numbers.

TCP connection establishment – Three way connection establishment flow must be complete before data transfer can begin.

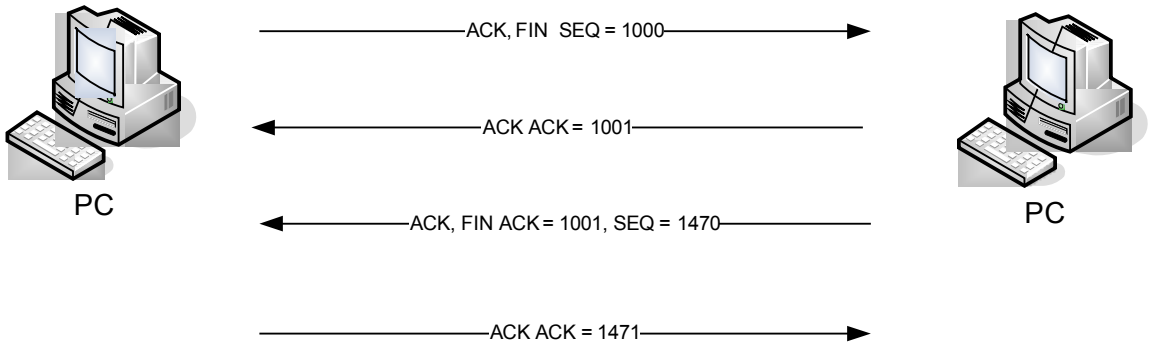


TCP signals connection establishment using two bits inside the flag field of the TCP header, called SYN and ACK flags.

SYN : Synchronize the Sequence numbers
ACK : Acknowledgment field is valid in this header

Acknowledgement field cannot be useful until the sequence field is initialized and continues to be set until the connection is terminated.

TCP Connection Termination : Four way termination flow uses an additional field called FIN bit (Finished), before sending the third TCP segment, PC on right notifies the application connection is coming down, it then waits for an acknowledge from the application before sending the third segment in the flow, in case the application takes some time to respond the second flow in the figure is send, acknowledging the PC on the left that it can take the connection down, otherwise the it will send the first segment repeatedly.



TCP establishes and terminates connection between end-points whereas UDP does not.

Connection Oriented Protocol: A protocol that require exchange of messages before data transfer begins or that has a required pre-established correlation between two end-points.

Connectionless Protocol : A protocol that does not require exchange of messages before data transfer beings and that does not require a pre-established correlation between two end-points.

Data Segmentation and Ordered Data Transfer

MTU – Maximum Transmission Unit – maximum data (Layer 3 (IP) Packet) that can be sent inside a data link frame, mostly including Ethernet it is 1500 bytes.

TCP segments large amounts of application data into segments, typically into 1460 byte chunks (TCP and IP header are each 20 bytes).

TCP receiver does the **ordered data transfer** by reassembling the data into the original order.

UDP – User Datagram Protocol

UDP support data transfer and multiplexing using ports numbers, and has fewer bytes of overhead and less processing is required compared to TCP.

UDP is used by application such as VoIP , DNS, NFS etc, applications where loss of data is tolerant (VoIP) or they have some application mechanism to recover the lost data (DNS).

TCP and UDP headers

Source Port	Dest-Port	Seq Number	Ack Number	Offset	Reserved	Flags	Window Size	Check Sum	Urgent	Options	PAD
2	2		4	4	4bits	6bits	2	2	2	3	1

TCP Header

Source Port	Dest-Port	Length	Checksum
2	2	2	2

UDP Header

Notice no Sequence and Acknowledge fields in the UDP header. UDP does not require waiting on acknowledgments or holding the data in memory until it is acknowledged, this means UDP applications are not artificially slowed by the acknowledgment process, and memory is freed more quickly.

TCP Applications

VoIP : An application protocol passes voice traffic over data networks inside IP Packets. A generic Voice Adaptor (VA) converts analog voice signals from the normal telephone to an IP Packets and sends it over the internet from a home dsl line.

VoIP Packet

IP	UDP	RTP	Digital Voice Bits

A single VoIP call that passes over a WAN typically takes less than 30 kbps of bandwidth, but it has several other QoS demands on the network before the VoIP traffic will sound good…

Low Delay : VoIP requires a very low delay between sending phone and the receiving phone – typically less than 200 milliseconds (.2 seconds). This is much lower delay than what is required by a typical data application.

Lower Jitter : Jitter is the variation in delay. VoIP requires very low jitter as well, where as data applications can tolerate much higher jitter. For example the jitter for consecutive VoIP packets should not exceed 30 milliseconds (.03 seconds), or the quality degrades.

Loss : If a VoIP packet is lost during transmission, no attempt is made to recover the packet, as it will be useless by the time it is recovered because of the Delay and Jitter issues. Lost packets can sound like a break in the sound of the VoIP call.

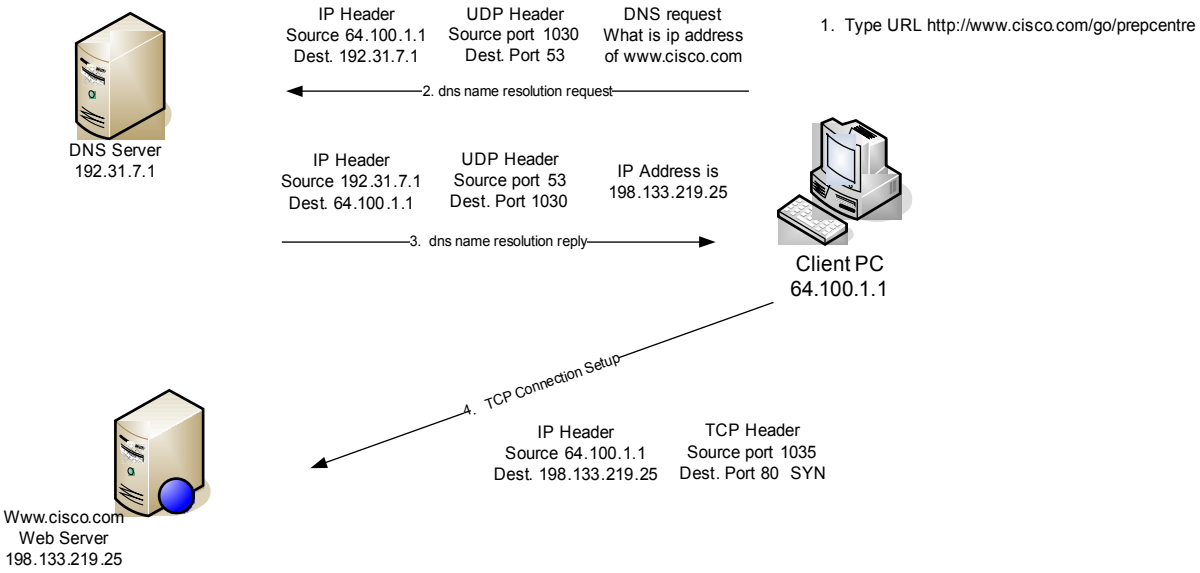
Video over IP requires a lot more bandwidth in the range of 300-400 kbps to 3-10 Mbps per video.

Type of Applcation	Bandwidth	Delay	Jitter	Loss
VoIP	Low	Low	Low	Low
Two-way Video over IP (such as videoconfernceing)	Medium/High	Low	Low	Low
One-way Video over IP (security camera)	Medium	Medium	Medium	Low
Interactive Mission Critical data (web based payroll)	Medium	Medium	High	High
Interactive Business Data (online chat with a co-worker)	Low/medium	Medium	High	High
File Transfer (Backing up disk drive)	High	High	High	High
Non Business (Browsing)	Medium	High	High	High

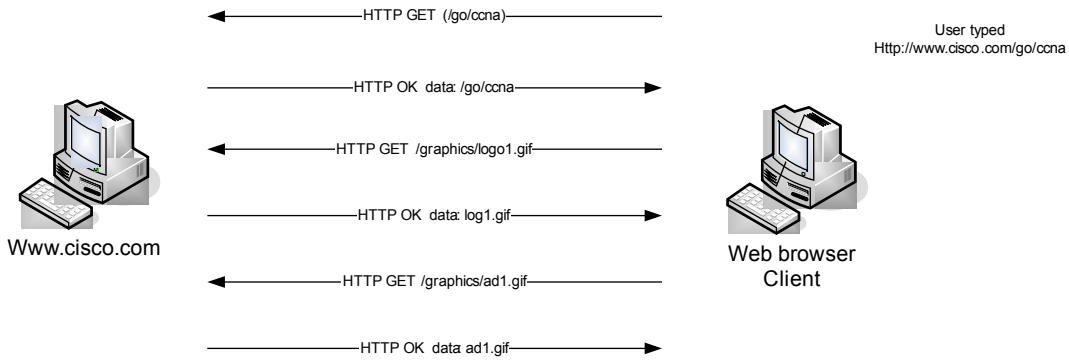
To support QoS requirements of various applications, routers and switches can be configured with a wide variety of QoS tools.

The World Wide Web, HTTP and SSL.

DNS resolution and requesting a web page



Multiple HTTP get requests/responses



Network Security

Firewalls : Firewalls are mainly the best known security appliances, sitting between enterprise network and the dark cold internet. The firewall mainly looks at the transport layer port numbers and the application layer headers to prevent certain port and applications from getting packets into the enterprise.

Kind of security attacks…

Denial of service attacks : An attack whose purpose is to break things DoS attacks called ***Destroyers*** try to harm the hosts, erasing data and software. DoS attacks called ***Crashers*** cause harm by causing hosts to fail or causing the machine to no longer be able to connect to the network. Also DoS attacks called ***Flooders*** , flood the network with packets making the network unusable, preventing any useful communication with the server.

Reconnaissance attacks : This kind of attack may be disruptive as a side effect, but its goal is gathering information to perform an access attack. An example is learning IP address and then try to discover servers, that does not appear to require encryption to connect to the server.

Access Attacks : An attempt to steal data, typically for financial advantage, for a competitive advantage with another company, or even for international espionage.

Computer Viruses are just one tool that can be used to carry out any of these attacks.
Virus Signature : Characteristics of viruses

Common Security Issues in an Enterprise

Access from the Wireless LAN : Wireless radio signals might leave the building, so an unsecured wireless LAN allows the user across the street in a coffee shop to access the enterprise network and rest of the devices in the enterprise network.

Infected Mobile Laptops : An employee connected an infected (from home) laptop to the enterprise network, causing the virus to spread to other vulnerable PCs.

Disgruntled Employees : An employee (who is planning to move to a new company) stealing the information from the network into portable devices.

Cisco uses the term **Security in Depth** to refer to a security design that includes security tools throughout the network, including features in routers and switches. Cisco also uses the term **"Self Defending Network"** to refer to automation in which network devices automatically react to network problems.

Network Admission Control (NAC) is a security tool, it prevents a computer from connecting to LAN until its virus definitions are updated, and with a requirement for a recent full virus scan, it also requires username and password before being able to send data in the LAN.

Tools used for an attack other than Viruses.

Scanners : sends connection requests to different TCP and UPD ports for different applications

Spyware : a virus that looks for private and sensitive information

Worm : A self propagating program that can replicate itself often casing DoS attacks on server and enterprise networks

Keystroke Logger : a virus that logs all keystrokes, or possibly just keystrokes from when secured sites are accessed.

Phishing : attackers sets up illegitimate website that looks like a bank or credit card company website, sends out emails with URL can tries to get sensitive information from the users.

Malware : refers to broad class of malicious viruses, including spyware.

Tools for In depth Security

Firewalls and Cisco Adaptive Security Appliance (ASA)

Firewall determines the allowed traffic versus the disallowed traffic based on their destination and source IP address, TCP and UDP port numbers, and application layer headers.

Demilitarized Zone (DMZ) LAN is a place to put devices that needs to be accessible from internet in an enterprise network.

Two allowed and one disallowed traffic in a network with a firewall….

1. A web client in side the network sending packets to a web server out side (internet)
2. Allow web client outside (internet) send packets to web server in the DMZ
3. Disallow web client outside sending packets to web server in side the secured network

Cisco Firewall were generally called PIX firewalls, but the newer models are called ASA.

Anti-x : The term Anti-x refers to the whole class of security tools to prevent various security problems, including the following…

Anti-virus, Anti-spyware, Anti-spam, Anti-phishing, URL filtering and EMAIL filtering.

Intrusion Detention System: IDS tools typically receive a copy of the packet through a monitoring port, IDS then rate and report on potential threats, and requests firewall or routers to take any preventative actions.

Intrusion Prevention System: The IPS tool often sit in the packets forwarding path, giving IPS the capability to perform the same functions as the IDS, but also to react and filter the traffic.

VPN

VPN makes the communication over the internet secure like a private leased line. VPNs authenticate VPN end points, meaning both the end points can be sure that the other end point of the VPN connection is legitimate. Additionally VPN uses encryption of the IP packets.

Two types of VPNs : Access VPN and sit-to-site intranet VPNs, Access VPNs support a home or small office user, with the remote office's PC typically encrypting the packets.

Definitions

Anti-x : A term used by Cisco to refer to a variety of security tools, that help prevent various attacks, including anti-virus, anti-phishing and anti-spam.

Connection Establishment : The process by which a connection oriented protocol creates a connection. With TCP a connection is established by a three-way transmission of TCP segments.

Denial of Service (DoS) : A type of attack whose goal is to cause problems by preventing legitimate users from being able to access network services, thereby preventing the normal operation of the computers and the network.

Error detection : The process of discovering whether or not the data link frame was changed during transmission. The process typically uses Frame Check Sequence (FCS) field in the data link trailer.

Error Recovery : is the process of noticing when some transmitted data was not successfully received, and re-sending data until it is successfully received.

Firewall : a device that forwards data packets between a less secure and more secure parts of the network, applying rules that determine which packets are allowed to pass, and which are not.

Flow Control : The process of regulating the amount of data sent by a sending computer towards a receiving computer. Several flow control mechanisms exists including TCP flow control which uses Windowing.

Forward Acknowledgment : A process that used by protocols that uses error recovery in which the number that acknowledges the data, lists the next data that should be sent, not the last data that was successfully received.

HTTP : Hypertext Transfer Protocol, a protocol. A protocol used by web browsers and web servers to transfer files, such as text and graphic files.

Intrusion Detection System (IDS) : A security function that examines more complex traffic patterns against a list of both known attack signatures, and general characteristics of how an attack may be carried out, rating each perceived threat and reporting on each threat.

Intrusion Prevention System (IPS) : A security function that examines more complex traffic patterns against a list of both known attack signatures, and general characteristics of how an attack may be carried out, rating each perceived threat and reacting to prevent the more significant threats.

Ordered Data Transfer: A networking function included in the TCP, in which the protocol defines how a sending host should number the data transmitted, defines how a receiving device should re-order the data if it arrives out of sequence, and specifies to discard the data if it cannot be delivered in order.

Port : In TCP and UDP a number that is uniquely used to identify an application process that either sent (source port) or should receive (destination port) data. In LAN switching another term for switch interface.

Positive Acknowledgment and re-transmission (PAR): A generic reference to how error recovery works in most protocols including TCP, in which the receiver must send an acknowledgement that either implies that the data was (positive) received, or send an acknowledgment that implies that some data was lost, so the sender can resend the lost data.

Segment: In TCP a term used to describe TCP header and its encapsulated data, also called L4PDU. Also in TCP the process of accepting large chunk of data from the application layer and breaking it into smaller pieces that fit into a TCP segment. In Ethernet a segment is either a single Ethernet cable, or a single collision domain.

Sliding windows: For a protocol such as TCP, that allow the receiving device to dictate the amount of data the sender can send before receiving an acknowledgment – a concept called window – a reference to the fact that mechanism to grant future window is typically just a number that grows up words slowly after each acknowledgment, sliding up word.

URL : Universal Resource Locator. A standard for referring to any piece of information retrievable via a TCP/IP network. Eg. http://www.cisco.com/univercd is a URL that defines HTTP as the protocol, host name www.cisco.com and /univercd as the web page.

Virtual Private Network (VPN): The process of securing communication between two devices whose packets pass over some unsecured public network, typically the internet. VPN encrypt the packets so that the communication is private, and authenticate the identity of the end points.

VoIP : Voice over IP, the transport of voice traffic inside IP packets over an IP network.

Web server: Software that runs on some computer, that stores web pages, and sends those web pages to web clients on request.

Please go to ……Do I know this Already –QUIZ. – Chapter 6. :- Page 130.