Transmission control protocol internet protocol (tcp ip) essay

TCP/IP has evolved to become the standard protocol used for interoperability among many different types of computers. This interoperability is a primary advantage of TCP/IP. Most networks support TCP/IP as a protocol, which serves as an internetworking protocol for routing.

Designed to be routable, robust and functionally efficient, TCP/IP was designed by the United States Department of Defense as a set of wide area network protocols. Its purpose was to maintain communication links between sites in different parts of the United States.

Benefits of using TCP/IP are vast and they include its recognition as an open protocol de facto standard for the Internet, connectivity for a range of dissimilar operating systems and a scalable, cross-platform client server architecture to meet future trends.

TCP/IP: An Introduction

The birth of Transmission Control Protocol/Internet Protocol (TCP/IP) came about when there was a need for multi networks to communicate together. This was vital due to the fact that the US Army was at war at that time and that information was an important asset in ensuring the success of missions. The Advance Research Projects Agency (ARPA) of the Department Of Defense (DOD) was the one responsible in developing this widely used protocol in which we know today as TCP/IP. It was developed under the leading eye of Vincent Cerf and Robert Khan. They were both in charge in leading the team into developing a protocol that could not only transmit messages between vast networks but also a protocol that ensures the delivery of those messages. Their main goal basically was to connect a

number of different networks together. In other words, make them talk to each other.

As we know today, TCP/IP has been widely used by the Internet community to transmit data between them. One of the reasons for this huge success is its ability to deliver basic services such as file transfer, e-mail and remote logons across networks. This helps the Internet community by offering the freedom of these options to communicate efficiently and effectively. Besides the growth of the Internet, large corporation are using the TCP/IP protocol to connect their huge Local Area Networks together to ensure the integrity of data transmission and ability to communicate between inter-departments. TCP-IP protocols are also use in Wide Area Networks (WAN) and Metropolitan Area Networks (MAN) too. Daily business activities relies on this protocol to ensure that important information is sent to the receiver only and not to anyone else. With the TCP/IP protocol at use, it is hard for intruders to obtain the whole message because it has been sent over the network through the form of packets. It wouldn’t be of any use to the intruders if they would to obtain only partial of the packets. The only way to get the whole message is through the receiver’s side.

The name TCP/IP was basically taken from two of the fundamentals protocols, Internet Protocol (IP) and Transmission Control Protocol (TCP). These protocols work together to provide a basic networking framework that is used by many different applications protocol, each tuned to achieving a particular goal. The reason why we need TCP and IP is basically to provide Internet users with basic operations on the network. In the past, TCP/IP was robust enough in maintaining communication throughout battlefields. This is

possible because it has the functionality to recover any node or phone failure. For example, the US networks is a combination of many different nodes. With the ability for it to stay up and running allows them to route sent information to the intended receiver on the network, but what if one of those nodes would to be shut down. This wouldn’t be a problem, with TCP there is no dedicate route on the network that the packets must run on. If one node is down, the packets will find other means to routes itself it to its destination. Additional to that, TCP and IP has the extra ability to allow expansion and growth of large networks. This is an additional plus in the advancement in technology. Because of the flexibility of this protocol, nodes can be added on to expand the size of the network. In this case, each node can be another option as router for packets to pass through. The more nodes there are, the bigger the network and the more options there are for faster transmission of packets.

TCP/IP: An Overview

TCP/IP is in essence, a suite of standard protocols designed for wide area networks. TCP/IP protocols map to a four layer model, Network Interface, Internet, Transport and Application.

Figure 1, TCP/IP model

At the base of the model is the network interface layer. This layer is responsible for putting frames on the wire and pulling frames off the wire. I will explain later how this layer works in detail. The next layer is the Internet layer. This layer is where packets are addressed and packaged for routing. In this layer, we can find 3 protocols:

* Internet Protocol (IP) – primarily responsible for addressing and routing packets between hosts and networks.

* Address Resolution Protocol (ARP) – used to obtain hardware addresses of hosts located on the same physical network.

* Internet Control Message Protocol (ICMP) – sends messages and reports errors regarding the delivery of a packet.

The Transport layer is responsible for providing communication between 2 hosts. Here we can find:

* Transmission Control Protocol (TCP) – provides a connection oriented reliable communications for applications that typically transfer large amounts of data at one time, or that require an acknowledgement for data received.

* User Datagram Protocol (UDP) – provides connectionless communications and does not guarantee that packets will be delivered. Applications that use UDP typically transfer small amounts of data at one time. Reliability is the responsibility of the application.

At the top of the model is the Application layer. This layer is where applications gain access to the network.

Next, we'll examine how data is transmitted over a network. When an application sends data to another host, each layer adds its own information to a header that is encapsulated as data by the protocol in the layer below. When the data is received at the destination host, the corresponding layer

strips of the header and treats the remaining packet as data. The packet is then passed up the stack to the appropriate protocol.

The network interface layer is responsible for merging outgoing frames onto the wire and for pulling incoming frames off the wire. When the network interface receives a packet from the layer above, it adds a preamble and Cyclic Redundancy Check (CRC). The preamble is a sequence of bytes that identifies the beginning of a frame. The CRC is a mathematical computation that is added to ensure that the frame is not corrupted. When the frame is received at the destination host, the preamble is discarded and the CRC value is calculated. If the CRC values match, the frame is passed to the layer above. If the CRC values do not match, the frame is discarded.

Now we take a look at the next layer on the stack. The Internet layer is where packets are addressed and packaged for routing. IP provides a connectionless delivery service, meaning a session is not required with another host before a packet can be delivered. The delivery service of IP is not guaranteed. Packets can arrive out of order, or be lost during routing. Reliability is the responsibility of the higher layer protocols and the applications. When a packet is passed down from the transport layer, IP adds its own header to the packet. The IP header includes:

* the source IP address where the packet originates

* destination IP address where the packet is going

* the transport protocol initiating the request. The protocol informs IP at the destination host whether to pass the packet up to TCP or UDP.

* A checksum value, which is a simple mathematical computation used to verify that the packet arrived intact

* Time to live (TTL), a value which determines how long the packet lives on the wire before it’s discarded. This prevents it from looping endlessly around the network.

If the destination address is identified as a local address, IP transmits the packet directly to the host. If the destination address is identified as a remote address, IP checks the local routing table for a route to the remote host.

When IP routes packets, it needs to obtain the destination hardware address. IP relies on ARP to obtain hardware addresses of TCP/IP hosts on broadcast based networks such as Ethernet and Token Ring. When IP needs a hardware address, ARP first consults the ARP cache for the hardware address that corresponds to the destination IP address. If the mapping is not in cache, ARP builds an ARP request frame for the destination hosts hardware address. To make future connections easier, the IP address and hardware address mapping of the source host is also included in the request frame. The frame is then merged onto the wire broadcast on the network. All hosts receive the request and the frame is passed up to ARP. If the receiving hosts IP address matches the requested IP address, an ARP reply is formulated with the requested hardware address and sent directly to the source host. When the hardware address is received, both the IP address and hardware address are stored as an entry in the local ARP cache. The IP packet can now be delivered using the destination hardware address.

If problems are encountered during routing, the ICMP sends messages and reports errors to the source host. ICMP messages:

* Source quench – when traffic becomes congested at a router

* Redirect – when a preferred route is detected

* Destination unreachable – when there is no route available such as when a line goes down

The ICMP message is packaged in an IP datagram and routed to the source host.

The next layer in our model is the Transport layer. The transport layer provides end points as means to communicate between two hosts. In UDP and TCP, the end points are called ports. UDP is typically used to transfer small amounts of data. UDP has 2 main characteristics:

* Connectionless delivery – it is connectionless, meaning that a session is not established between two hosts before exchanging data. Instead, UDP messages can be broadcast so that many hosts receive the message.

* Delivery not guaranteed – UDP does not guarantee delivery of messages. Packets may arrive out of order or be duplicated. Reliable delivery is the responsibility of the application.

When UDP wants to send data to another host, UDP builds a header that includes:

* source port

* destination port – which provides an address for delivering messages

* checksum – a checksum value for the data and header

At the destination host, the packet is passed up to UDP and delivered to the destination port.

TCP is typically used by applications to transfer large amounts of data. TCP has 3 main characteristics:

* Connection oriented delivery – TCP is connection oriented, which means that TCP first establishes a session between 2 hosts before any data is exchanged

* Reliable delivery – TCP assures reliability by using sequence numbers and acknowledgements. Sequence numbers allow TCP segments to be split into multiple packets and then reassembled into the original segment. Acknowledgements verify that the data was received.

* Byte-stream communications – TCP uses byte stream communications which means that the data is treated as a sequence of bytes with no message boundaries.

The next 2 sections of this report will go into more detail the 2 fundamental building blocks of TCP/IP.

TCP/IP: Transmission Control Protocol

Now what is TCP? TCP, or Transfer Control Protocol, is in charge of establishing a connection between two hosts to enable the exchange of data.

It basically guarantees the delivery of those data from one place to the other. These are all possible by using the TCP protocol to break down the data into smaller packets. This packet will then be sent over the network, with the help of the IP protocol, to the other host. At that host, the TCP's job is to reassemble those packets back into its original state to form the send data. You can say that TCP controls the break down of data into smaller packets and the reassembly of them at their destination. Once all packets have been sent, the TCP's job is to destroy the current connection via the exchange of management packets.

One huge advantage with TCP is that it is reliable and it has the ability to offer a higher degree of protection against data loss, data corruption, packet reordering and data duplication. Data loss for example is when data is cancelled half way through its routing process. This happens all the time when a router is down. Data corruption on the other hand is when the data sent is corrupted. It is generally received but the state of it wasn't the same as before it was sent. Packet reordering and data duplication are all faults of data transmission. It happens frequently when the network is congested. These are all fault factors that requires the need for data protection and TCP offers that functionality. Without these options, the Internet would not have been this successful. The protection capabilities from the TCP protocol are possible with the use of checksums and sequence numbers. Checksums and sequence numbers are added to a transmitted packet to ensure the delivery of it. Once this packet reaches the receiver, an acknowledgement will be sent back to the sender to tell him that the packet has been sent successfully. However, if the packet is lost, there will be no

acknowledgement sent back and the sender would have to resend that data packet again. Besides offering the advantages of data protection, TCP was also given the role to make as much use of the network by packing as much data into an IP packet. This helps in decreasing the time that takes to transfer a packet from one end to the other. It also helps in increasing the amount of data that can be sent to the receiver. Additional to that, TCP has a multi stage flow control mechanism that can help in adjusting the sender's rate.

Figure 2, Packet transmission

The diagram above basically shows the processes involve in ensuring the transmission of data packets. This all starts when a sender wishes to send data to a receiver. What TCP does is to first break that data down into smaller packets. These packets can best be resembled by the color circles in the diagram. This process happens in step 1 of the diagram. The IP protocol on the other hand will assign the IP address to each and every one of those packets. The addresses will tell them where to go in the network.

In step 2. Packets, also known as datagrams, will travel through different routes over the internet. One thing is for sure, all of them will end up at the same destination due to the help of the IP protocol. These packets act as an independent body that knows its destination. So it does not matter which route it takes at the end because they would all eventually end up at the same destination.

As shown in step 3, the job of the TCP protocol is to reassemble those receiver packets into the state it was in before. In this case, packets do not

have to arrive in order. Those packets that arrive first will be arranged to fit the original state.

Overall, TCP plays an important role in the networking industry. It has helped us to communicate through the Internet by ensuring us that its full proof services can be dependent on. However, TCP can still under perform our judgments by providing transmission errors. These errors are rare but it does happen. The only to overcome this is to resend those data again and reconfirm their delivery with the receiver.

TCP/IP: Internet Protocol

The Internet Protocol (IP), defined by IETF RFC791, is the routing layer datagram service of the TCP/IP suite. IP is a standardized protocol that executes hosts and routers to interconnect a number of independent networks (Stallings, 2001). IP belongs to the network layer (layer 3) in the OSI model. There are a few roles that the IP undertakes; one of these roles is that IP transmits data from a higher-level protocol, such as TCP, UDP in IP datagrams, across networks (from one host to the other). IP also routes datagrams through gateways and uses IP addresses to identify individual networks. Lastly IP oversees the fragmenting and reassembling of datagrams. This is based on the MTU of the underlying network.

To understand how IP works, 3 main areas would be covered, the description of the IP packet form, the addressing system used by IP and how packets are routed from source to destination.

Once the higher-level protocol such as TCP or UDP receives a datagram(s), headers are inserted to the datagram(s) and this is passes to the Internet Protocol (IP). An IP datagram can be defined as a piece of information used by the IP layer to exchange data between two hosts. It consists of an IP header and data. As mentioned earlier, the main job of the IP is to find a suitable path and method to transport the datagrams to the destination servers. The IP itself does not perform any kind of error checking.

The IP adds its own header to the datagram. This is to allow or other intermediate systems to forward datagrams. Routing information and control information associated with datagram delivery are stored in the IP frame header. The main headers are the source and destination address, (32-bit addresses, like 120. 1. 1. 333), the protocol number and the header checksum. The source address is the IP address of the source host sending the IP datagram. The destination address is the IP address of the destination host to which the IP datagram must be delivered. The protocol indicates to which upper-layer protocol layer the datagram would be sent too. The header checksum allows the IP at the other end (the receiving machine) to verify that the header wasn’t damaged during the transit. Both the TCP and IP have a different checksum.

The IP header structure consists of other headers as well. The Version indicates the format of the Internet header. Internet Header Length is the length of the IP header in multiples of 32 words. Type of Services indicates the quality of service requested for this delivery. Total length is the total length of the datagram measured in bytes. Identification refers to the value that is assigned to the sender. This is done to help in the assembling of

datagram fragments. Options are used to add timestamps, security, source routing and so on. The Data consist of the IP data or a higher layer protocol header. Flags and fragment offset are used to keep track of the datagram pieces when it is split up. Time to Live refers to the maximum time a datagram can live in the network.

The first three classes, A to C, contains addresses that can be assigned to hosts. However, some addresses are reserved; therefore not all possibilities are allowed. A host ID with value zero does not specify a host, but the location of the specific network ID of the host in the network A host ID with the highest possible value for its class (all one bits in binary format), is the broadcast address for a certain network. IP datagrams that are sent to the address are delivers to all hosts on that network. In the cast where the network ID of an address is zero, it specifies the local network. This is used for initialisation procedures, when the local network ID is unknown. 0. 0. 0. 0 and 255. 255. 255. 255 are the rest of the reserved addresses. The first specifies the local host on the local network and is used for initialisation procedures. The second are limited broadcast addresses.

Class D specifies a multicast address. Multicasting allows data to be sent to a group of hosts. When an IP datagram is sent to the multicast address, the datagram is sent to all hosts in the corresponding multicast group. Class E is meant for future enhancement and use.

Now we go into how packets are routed from source to destination using IP. Data is transmitted using the link layer and the data can only be delivered to hosts that are connected to the same medium. The destination IP address is

firstly examined by the internet layer of the sending host when it’s transmitting a datagram. This is done because the internet layer has to tell the link layer which machine the data has to be delivered. The internet layer examines the routing table if an address does not specify a host on the local network. These entries can be vied as pairs of a destination address (address of a host or a network) and a router address.

The internet layer then compares the destination address of the datagram with the destination in the routing network when it starts searching for a router to deliver the datagram. In the case that no matches are found, the internet layer checks for matching network entries. If this fails too, a default entry is used. The Internet layer would use corresponding router address and instruct the link layer to deliver the datagram to the particular address if an entry is found.

The datagram is passed from the link layer to the internet layer when it reaches the router. An almost identical search procedure is used to search for a destination machine to forward the datagram to. The difference is that the router is connected to several networks and a suitable interface to transmit the data has to be selected. The procedure will be repeated until the datagram reaches its destination.

There are alternatives, proposal and enhancements to the current IP. IP version 6 (IPv6) is a newer IP that is based on IP version 4. The main difference in IPv6 is that it has a larger amount of IP address size, from 32 bits to 128 bits. This provides additional support to the level of hierarchy, a larger number of addressable nodes and a much more simplistic auto-

configuration of addresses. IPv6 provides multicast address as well. Other then this IPv6 provides improves support for extensions and options. In IPv6 the options are placed in separated headers that are between the IPv6 header and the transport layer header. These changes allow more efficient forwarding, les stringent limits on the length of option and greater flexibility for future options enhancements. Hop-by-Hop Option, Routing (Type 0), Fragment, Destination Option, Authentication, Encapsulation Payload are the extension headers. IPv6 allows flow labeling capability as well. Newer capabilities are added to enable the handling of packets to particular traffic flows for which the sender requests special handling. These are Quality of Service or real-time service.

There are four proposals for a new version of IP, Simple Internet Protocol (SIP), PIP, TUBA and TP/IX. The SIP proposed that IP uses a 64 bit address and a different header format. PIP proposed to have a larger, variable length and a hierarchical address with a different header format. TUBA (TCP and UDP with Bigger Address) proposed to have much larger addresses, and variable lengths up to 20 bytes. TP/IX proposed to use 64 bit address, changes to be made on the TCP and UDP headers, 32 bit port numbers, 64 bit sequences numbers, 64 bit acknowledgment numbers and 32 bit windows for TCP.

Related essay: “ Values and Standards of the British Army”

Even though IP is the standard and most commonly protocol used for transmission and delivery of data, it is still an unreliable protocol. This is because IP does not guarantee the delivery of a datagram to its destination. It depends on upper layer protocols such as TCP and UDP for reliability. Flow

control, retransmission, acknowledgement and error recovery are not provided by IP. IP can be considered as a best-effort protocol as it tries its best (make every effort) to always transmit a datagram and ensure that it’s not discarded. Delivery of the datagram to the destination in the network is not guaranteed. Overall, IP performs what it was meant to do and the industry will continue to use it as there are no better protocols compared to it at this time.

Glossary of Terms

Address Resolution Protocol (ARP) – used to obtain hardware addresses of hosts located on the same physical network.

Cyclic Redundancy Check (CRC) – mathematical computation that is added to ensure that the frame is not corrupted.

Internet Control Message Protocol (ICMP) – sends messages and reports errors regarding the delivery of a packet.

Internet Protocol (IP) – primarily responsible for addressing and routing packets between hosts and networks.

Maximum Transmission Unit (MTU) – the largest physical packet size, measured in bytes, which a network can transmit.

Multicast – To act of transmitting a single message to a select group of recipients

Transmission Control Protocol (TCP) – provides a connection oriented reliable communications for applications that typically transfer large amounts of data at one time, or that require an acknowledgement for data received.

User Datagram Protocol (UDP) – provides connectionless communications and does not guarantee that packets will be delivered. Applications that use UDP typically transfer small amounts of data at one time. Reliability is the responsibility of the application.

Bibliography

1. Microsoft Press, 2000, Chapter 6: Defining Network Protocols in Networking Essentials Plus 3rd Edition, Microsoft Press, Washington, pp. 245 – 251

2. William Stallings. Business Data Communications. 4th Edition. Prentice Hall.

3. http://www. yale. edu/pclt/COMM/TCPIP. HTM

Introduction to TCP/IP

4. http://www. private. org. il/tcpip_rl. html

Uri’s TCP/IP Resources List

FAQs, tutorials, guides, web pages ; sites, and books about TCP/IP

By Uri Raz

5. http://www. sangoma. com/fguide. htm

TCP/IP and IPX routing Tutorial

6. http://www. itprc. com/tcpipfaq/default. htm

TCP/IP Frequently Asked Questions

7. http://www. webopedia. com/TERM/T/TCP_IP. html

www. webopedia. com

8. http://www. protocols. com/pbook/tcpip. htm

Protocol Dictionary

TCP/IP Suite

9. http://www. msln. maine. edu/msln/support/archive/tcptut/tcptut-2. htm

Intro to IP – Chap 2

Maine School and Library Network

10. http://www. astalavista. com/library/protocols/tcp-ip/tcp-ip_for_newbies. shtml

TCPIP: A Mammoth Description

Ankit Fadia

11. http://www. freesoft. org/CIE/Topics/79. htm

IP Protocol Overview

Freesoft. org

12. http://www. protocols. com/pbook/tcpip. htm

Protocol Directory – TCP/IP

Protocols. com

13. http://www. geocities. com/SiliconValley/Vista/8672/network/ip. html

Internet Protocol: Questions ; Answers

Yegappan Lakshmanan