A Multidisciplinary Indexed International Research Journal

ISSN : 2320-3714
Volume : XIV
Journal : 63012
Impact Factor : 0.75 to 3.19

ADHYAYAN
INTERNATIONAL
RESEARCH
ORGANISATION

Airo International Research Journal

Volume XIV, ISSN: 2320-3714
January, 2018

UGC Approval Number 63012

SIGNIFICANCE OF HAND-SHAKING METHOD IN DATA TRANSMISSION

Divya Shree

Assistant Professor (Resource Person),

Department of computer science and engineering,

UIET, MDU, Rohtak

ABSTRACT

Handshaking is an automated process of negotiation that dynamically sets parameters of a communications channel established between two entities before normal communication over the channel begins. It follows the physical establishment of the channel and precedes normal information transfer.

The handshaking process usually takes place in order to establish rules for communication when a computer sets about communicating with a foreign device. When a computer communicates with another device like a modem, printer, or network server, it needs to handshake with it to establish a connection.

KEYWORDS: *Handshaking, Connection, Communication, Information*

INTRODUCTION

Handshaking can negotiate parameters that are acceptable to equipment and systems at both ends of the communication channel, including information transfer rate, coding alphabet, parity, interrupt procedure, and other protocol or hardware features.

Handshaking is a technique of communication between two entities.

However, within TCP/IP RFCs, the term "handshake" is most commonly used to reference the TCP three-way handshake. For

example, the term "handshake" is not present in RFCs covering FTP or SMTP. One exception is Transport Layer Security, TLS, setup, FTP RFC 4217. In place of the term "handshake", FTP RFC 3659 substitutes the term "conversation" for the passing of commands.

A simple handshaking protocol might only involve the receiver sending a message meaning "I received your last message and I am ready for you to send me another one." A more complex handshaking protocol might allow the sender to ask the receiver if it is ready to receive or for the receiver to reply with a negative acknowledgement meaning "I did not receive your last message correctly, please resend it" (e.g., if the data was corrupted en route).

Handshaking facilitates connecting relatively heterogeneous systems or equipment over a communication channel without the need for human intervention to set parameters.

A Realtek RTL8019 10Base-T interface chip provides a 10 Mbps Ethernet connection. This chip is used on many Ethernet-enabled Z-World boards. The corresponding port can be connected directly to an Ethernet network. By using hubs and routers, a network can include a large number of computers. A network might include all the computers in a particular building. A local network can be connected to the Internet by means of a gateway. The gateway is a computer that is connected both to the local network and to the Internet. Data that must be sent out over the Internet are sent to the local network interface of the gateway, and then the gateway sends them on to the Internet for routing to some other computer in the world. Data coming in from the Internet are directed to the gateway, which then sends them to the correct recipient on the local network.

Ethernet cables are similar to U.S. telephone plug cables, except they have eight connectors. For our purposes, there are two types of cables—crossover and straight-through. In most instances, the straight-through cables are used. It is necessary to use a crossover cable when two computers are connected directly without a hub (for example, if you want to connect your PC's Ethernet directly to the Rabbit Semiconductor TCP/IP Development Board.) Some hubs have one input that can accept either a straight-through or crossover cable depending on the position of a switch.

In this case make sure that the switch position and cable type agree.

TCP THREE-WAY HANDSHAKE

Establishing a normal TCP connection requires three separate steps:

1. The first host (Alice) sends the second host (Bob) a "synchronize" (SYN) message with its own sequence number , which Bob receives.
2. Bob replies with a synchronize-acknowledgment (SYN-ACK) message with its own sequence number and acknowledgement number , which Alice receives.
3. Alice replies with an acknowledgment (ACK) message with acknowledgement number, which Bob receives and to which he doesn't need to reply.

In this setup, the synchronize messages act as service requests from one server to the other, while the acknowledgement messages return to the requesting server to let it know the message was received.

One of the most important factors of three-way handshake is that, in order to exchange the starting sequence number the two sides plan to use, the client first sends a segment with its own initial sequence number , then the server responds by sending a segment with its own sequence number and the acknowledgement number and finally the client responds by sending a segment with acknowledgement number .

The reason for the client and server not using the default sequence number such as 0 for establishing connection is to protect against two incarnations of the same connection reusing the same sequence number too soon, which means a segment from an earlier incarnation of a connection might interfere with a later incarnation of the connection.

When a Transport Layer Security (SSL or TLS) connection starts, the record encapsulates a "control" protocol—the handshake messaging protocol (content type 22). This protocol is used to exchange all the information required by both sides for the exchange of the actual application data by TLS. It defines the messages formatting or containing this information and the order of their exchange. These may vary according to the demands of the client and server—i.e., there are several possible procedures to set

up the connection. This initial exchange results in a successful TLS connection (both parties ready to transfer application data with TLS) or an alert message.

DISCUSSION

IP defines an addressing scheme that is independent of the underlying physical address (e.g, 48-bit MAC address). IP specifies a unique 32-bit number for each host on a network. This number is known as the Internet Protocol Address, the IP Address or the Internet Address. These terms are interchangeable. Each packet sent across the internet contains the IP address of the source of the packet and the IP address of its destination. For routing efficiency, the IP address is considered in two parts: the prefix which identifies the physical network, and the suffix which identifies a computer on the network. A unique prefix is needed for each network in an internet. For the global Internet, network numbers are obtained from Internet Service Providers (ISPs). ISPs coordinate with a central organization called the Internet Assigned Number Authority (IANA).

Netmasks are used to identify which part of the address is the Network ID and which part is the Host ID. This is done by a logical bitwise-AND of the IP address and the netmask. For class A networks the netmask is always 255.0.0.0; for class B networks it is 255.255.0.0 and for class C networks the netmask is 255.255.255.0.

All hosts are required to support subnet addressing. While the IP address classes are the convention, IP addresses are typically subnetted to smaller address sets that do not match the class system. The suffix bits are divided into a subnet ID and a host ID. This makes sense for class A and B networks, since no one attaches as many hosts to these networks as is allowed. Whether to subnet and how many bits to use for the subnet ID is determined by the local network administrator of each network. If subnetting is used, then the netmask will have to reflect this fact. On a class B network with subnetting, the netmask would not be 255.255.0.0. The bits of the Host ID that were used for the subnet would need to be set in the netmask.

Each IP datagram travels from its source to its destination by means of routers. All hosts and routers on an internet contain IP protocol software and use a routing table to determine where to send a packet next. The destination IP address in the IP header

contains the ultimate destination of the IP datagram, but it might go through several other IP addresses (routers) before reaching that destination.

Routing table entries are created when TCP/IP initializes. The entries can be updated manually by a network administrator or automatically by employing a routing protocol such as Routing Information Protocol (RIP). Routing table entries provide needed information to each local host regarding how to communicate with remote networks and hosts. When IP receives a packet from a higher-level protocol, like TCP or UDP, the routing table is searched for the route that is the closest match to the destination IP address.

The Address Resolution Protocol is used to translate virtual addresses to physical ones. The network hardware does not understand the software-maintained IP addresses. IP uses ARP to translate the 32-bit IP address to a physical address that matches the addressing scheme of the underlying hardware (for Ethernet, the 48-bit MAC address).

TCP/IP can use any of the three. ARP employs the third strategy, message exchange. ARP defines a request and a response. A request message is placed in a hardware frame (e.g., an Ethernet frame), and broadcast to all computers on the network. Only the computer whose IP address matches the request sends a response.

TCP can detect errors or lost data and can trigger retransmission until the data is received, complete and without errors.

Sequence Number - This 32-bit number contains either the sequence number of the first byte of data in this particular segment or the Initial Sequence Number (ISN) that identifies the first byte of data that will be sent for this particular connection. The ISN is sent during the connection setup phase by setting the SYN control bit. An ISN is chosen by both client and server. The first byte of data sent by either side will be identified by the sequence number ISN + 1 because the SYN control bit consumes a sequence number. The following figure illustrates the three-way handshake.

Internet Control Message Protocol is a set of messages that communicate errors and other conditions that require attention. ICMP messages, delivered in IP datagrams, are usually acted on by either IP, TCP or UDP. Some ICMP messages are returned to

application protocols. A common use of ICMP is “pinging” a host. The Ping command (Packet INternet Groper) is a utility that determines whether a specific IP address is accessible. It sends an ICMP echo request and waits for a reply. Ping can be used to transmit a series of packets to measure average roundtrip times and packet loss percentages.

CONCLUSION

One classic example of handshaking is that of dial-up modems, which typically negotiate communication parameters for a brief period when a connection is first established, and thereafter use those parameters to provide optimal information transfer over the channel as a function of its quality and capacity. The "squealing" (which is actually a sound that changes in pitch 100 times every second) noises made by some modems with speaker output immediately after a connection is established are in fact the sounds of modems at both ends engaging in a handshaking procedure; once the procedure is completed, the speaker might be silenced, depending on the settings of operating system or the application controlling the modem.

REFERENCES

1. *"Router". Oxford English Dictionary (3rd ed.). Oxford University Press. September 2005.* (Subscription or UK public library membership required.)
2. *"Overview Of Key Routing Protocol Concepts: Architectures, Protocol Types, Algorithms and Metrics". Tcpipguide.com. Retrieved 15 January 2011.*
3. F. Baker (June 1995). *Requirements for IPv4 Routers*. RFC 1812.
4. *"Cisco Networking Academy's Introduction to Routing Dynamically". Cisco. Retrieved August 1, 2015.*
5. H. Khosravi& T. Anderson (November 2003). *Requirements for Separation of IP Control and Forwarding*. RFC 3654.
6. *"Setting uoNetflow on Cisco Routers". MY-Technet.com date unknown. Retrieved 15 January 2011.*
7. *"Windows Home Server: Router Setup". Microsoft Technet 14 Aug 2010. Retrieved 15 January 2011.*

8. *Oppenheimer, Pr (2004). Top-Down Network Design. Indianapolis: Cisco Press. ISBN 1-58705-152-4.*

9. *"Windows Small Business Server 2008: Router Setup". Microsoft Technet Nov 2010. Retrieved 15 January 2011.*