

# HTTP AND DHCP

## Hypertext Transfer Protocol HTTP

A standard Internet protocol that specifies the client/server interaction processes between Web browsers such as Mozilla Firefox and Web servers such as Apache. Its the network protocol used to deliver virtually all files and other data(collectively called resources) on the World-Wide-Web, whether they are HTML files, image files, query results or anything else. Usually HTTP takes place though TCP/IP Sockets.

A Browser is an HTTP client because it sends requests to an HTTP server (Web Sever), which then sends response back to the client. The standard and default port for the HTTP servers to listen is 80, though they can use any port.

### **What are Resources?**

HTTP is used to transmit resources not just files. A resource is some chunk of information that can be identified by a URL (its R in URL). The most common kind of resource is a file, but a resource may also be a dynamically generated query, the output of a CGI script, a document that is available in several language or anything else.

The original Hypertext Transfer Protocol (HTTP) 1.0 protocol is a **stateless protocol** whereby a Web browser forms a connection with a Web server, downloads the appropriate file, and then terminates the connection. The browser usually requests a file using an HTTP GET method request on TCP port 80, which consists of a series of HTTP request headers that define the transaction method (GET, POST, HEAD, and so on) and indicates to the server the capabilities of the client. The server responds with a series of HTTP response headers that indicate whether the transaction is successful, the type of data being sent, the type of server, and finally the requested data.

IIS 4 supports a new version of this protocol called HTTP 1.1, which has new features that make it more efficient. These new features include the following:

- **Persistent connections:**

An HTTP 1.1 server can keep TCP connections open after a file has been transferred, eliminating the need for a connection to be opened and closed each time a file is transferred, as is the case with HTTP 1.0.

- **Pipelining:**

This is a process whereby an HTTP 1.1 client can send multiple Internet Protocol (IP) packets to the server without waiting for the server to respond to each packet.

- **Buffering:**

This process allows several HTTP requests by the client to be buffered into a single packet and sent to the server, which results in faster transfer times because fewer and larger packets are used.

- **Host headers:**

This feature enables an HTTP 1.1-compliant Web server to host multiple Web sites using a single IP address.

- **Http put and http delete commands:**

These commands enable Web browsers to upload and delete files from Web servers using HTTP.

# HTTPS VS HTTP.

As opposed to HTTP URLs that begin with "http://" and use port 80 by default, HTTPS URLs begin with "https://" and use port 443 by default. HTTP is unsecured and is subject to man-in-the-middle and eavesdropping attacks, which can let attackers gain access to website accounts and sensitive information. HTTPS is designed to withstand such attacks and is considered secure against such attacks. HTTP operates at the highest layer of the OSI Model, the Application layer; but the security protocol operates at a lower sublayer, encrypting an HTTP message prior to transmission and decrypting a message upon arrival. Strictly speaking, HTTPS is not a separate protocol, but refers to use of ordinary HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. Everything in the HTTP message is encrypted, including the headers, and the request/response load.

# DHCP(Dynamic Host Configuration Protocol)

A standard Internet protocol that enables the dynamic configuration of hosts on an Internet Protocol (IP) internetwork. Dynamic Host Configuration Protocol (DHCP) is an extension of the bootstrap protocol (BOOTP).

### How It Works

DHCP is a client-server protocol that uses DHCP servers and DHCP clients. A DHCP server is a machine that runs a service that can lease out IP addresses and other TCP/IP information to any client that requests them. For example, on Linux System example Ubuntu you can install the DHCP Server service to perform this function. The DHCP server typically has a pool of IP addresses that it is allowed to distribute to clients, and these clients lease an IP address from the pool for a specific period of time, usually several days. Once the lease is ready to expire, the client contacts the server to arrange for renewal.

DHCP clients are client machines that run special DHCP client software enabling them to communicate with DHCP servers. All versions of Linux and Windows include DHCP client software, which is installed when the TCP/IP protocol stack is installed on the machine.

DHCP clients obtain a DHCP lease for an IP address, a subnet mask, and various DHCP options from DHCP servers in a four-step process:

**1. DHCPDISCOVER:**

The client broadcasts a request for a DHCP server.

**2. DHCPOFFER:**

DHCP servers on the network offer an address to the client.

**3. DHCPREQUEST:**

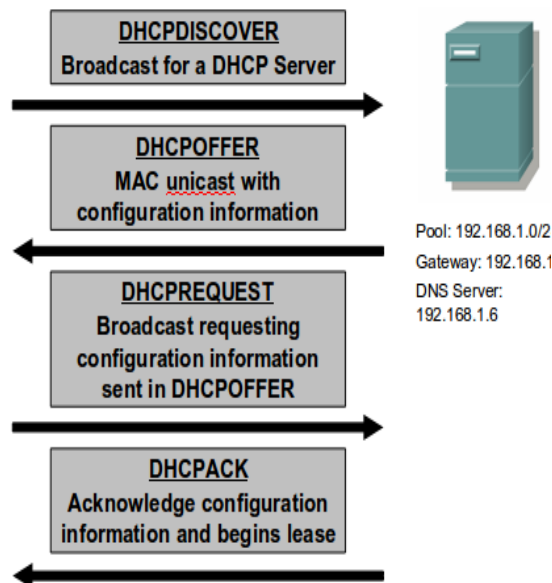
The client broadcasts a request to lease an address from one of the offering DHCP servers.

**4. DHCPACK:**

The DHCP server that the client responds to acknowledges the client, assigns it any configured DHCP options, and updates its DHCP database. The client then initializes and binds its TCP/IP protocol stack and can begin network communication.



Client IP: ??  
Gateway: ??  
DNS: ??  
Client IP: 192.168.1.10/24  
Gateway: 192.168.1.1  
DNS: 192.168.1.6





Ethernet Frame	IP	UDP	DHCP Request	
SRC MAC: MAC A	IP SRC: ?	UDP	CIADDR: ?	GIADDR: ?
DST MAC: FF:FF:FF:FF:FF:FF	IP DST: 255.255.255.255	67	Mask: ?	CHADDR: MAC A

MAC: Media Access Control Address  
 CIADDR: Client IP Address  
 GIADDR: Gateway IP Address  
 CHADDR: Client Hardware Address



Ethernet Frame	IP	UDP	DHCP Reply	
SRC MAC: MAC Serv	IP SRC: 192.168.1.254	UDP	CIADDR: 192.168.1.10	GIADDR: ?
DST MAC: MAC A	IP DST: 192.168.1.10	68	Mask: 255.255.255.0	CHADDR: MAC A

MAC: Media Access Control Address  
 CIADDR: Client IP Address  
 GIADDR: Gateway IP Address  
 CHADDR: Client Hardware Address

Source : <http://dayaramb.files.wordpress.com/2011/03/computer-network-notes-pu.pdf>