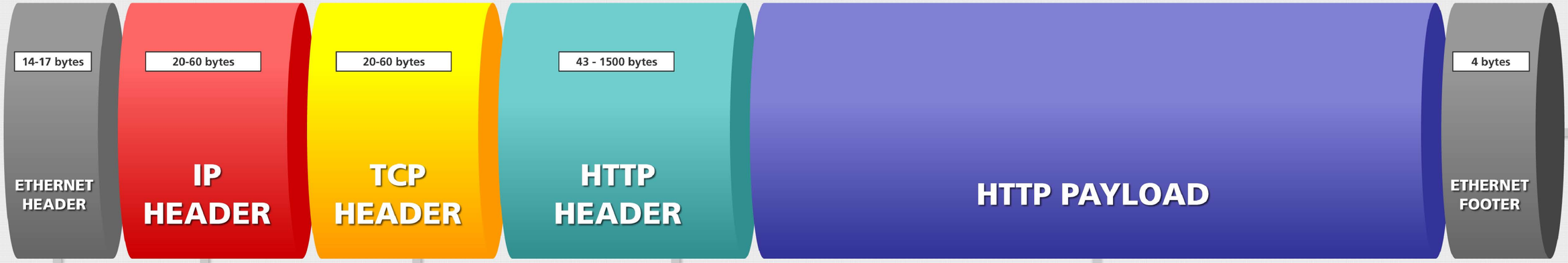
netmonstore.com
Toll Free: 1-877-444-3335

PACKET DECONSTRUCTED:
HyperText Transfer Protocol (HTTP)



Ethernet Header Reference

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Destination MAC Address	
Destination MAC Address cont'd	Source MAC Address
Source MAC Address cont'd	
Protocol Type	

Source & Destination MAC Address 48 bits + 48 bits

Contains the MAC address of the source host (48 bits) and MAC address of the destination host (48 bits).

Protocol Type 16 bits

A 2 byte value representing the lower layer protocol. Also known as the Ethernet Frame Type.

Ethernet header configuration can vary based on the underlying network architecture. For example, an Ethernet II frame looks slightly different than an 802.11g frame. However, all Ethernet frames carry at least the source and destination MAC addresses, along with a frame footer for accuracy checking.

IP Header Reference

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Version	IHL	Type Of Service (TOS)	Packet Length (bytes)
Packet Fragment Identifier		Flags	Fragment Offset
Time To Live (TTL)	Protocol		Checksum
Source IP Address			
Destination IP Address			
Options			Padding

Version 4 bits

Designates the IP version in use. The vast majority of IP traffic on modern networks is IPv4. IPv6 is a newer standard which has still not yet seen widespread adoption.

Internet Header Length (IHL) 4 bits

Indicates the total number of 4- byte words in the IP header.

Type of Service (TOS) 8 bits

Provides a method to specify quality of service parameters. In practice, only the first 3 bits are used. Each of these bits can emphasize delay(100), throughput(010) or reliability(001). These flags may be ignored by some routers.

Packet Length 16 bits

Indicates the length of the IP packet, including header. Therefore, the maximum length for an IP packet is 65,535 bytes.

Fragment Identifier 16 bits

A unique 16 bit identifier assigned to the packet by the originating host. If packets become fragmented in transit, this field is used to reassemble them at the destination host. Packet fragments all carry the same 16 bit value.

Flags 3 bits

[001] Unused
[010] Do Not Fragment Bit - Instructs routing devices with a smaller MTU to drop the packet rather than fragment it.
[001] More Fragments Bit - Indentifies this packet as a fragment of a larger packet.

Fragment Offset 13 bits

Used in fragmented packets, this field contains the number of bytes offset from the start of the original packet.

Time to Live (TTL) 8 bits

Represents the maximum number of hops a packet can take before being dropped. Valid values are 0 through 255.

Protocol 8 bits

Identifies the higher layer protocol carried in the IP datagram (i.e. this value could represent TCP or UDP packets).

Checksum 16 bits

A checksum based on the contents of the IP packet. This checksum is used to ensure that data hasn't been corrupted.

Source & Destination IP Address 32 + 32 bits

Contains the IP address of the source host (32 bits) and IP address of the destination host (32 bits)

Options 16 bits

Contains flags for various IP-level functions, such as special routing instructions. This field is rarely used.

TCP Header Reference

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Source Port		Destination Port	
Sequence Number			
Acknowledgment Number			
Data Offset	Reserved	Flags	Window
Checksum			Urgent Pointer
Options			Padding

Source & Destination Port 16 bits + 16 bits

Contains a source port number (0 thru 65,535) and a destination port number (0 thru 65,535) for the TCP packet.

Sequence Number 32 bits

TCP is a connection-oriented protocol. Sequence numbers allow packets to be reassembled properly at the destination.

Acknowledgement Number 32 bits

Acknowledgement Numbers work closely with Sequence Numbers. This field contains the sequence number of the last packet properly received, plus one (1).

Data Offset 4 bits

Indicates the number of words in the TCP header, identifying where the data portion of the packet begins. TCP headers are always an even multiple of 32 bits.

Flags 6 bits

[100000] URG - Packet is Urgent.
[010000] ACK - Indicates that the acknowledgement number in the TCP header is valid.
[001000] PSH - Indicates that the packet should be forwarded to the receiving process as soon as possible.
[000100] RST - Tells the receiving host that the connection should be reset.
[000010] SYN - This flag tells the receiving host that this packet is part of a TCP connection handshake.
[000001] FIN - This flag tells the receiving host that the sender has no more data to send.

Window 16 bits

Indicates the number of bytes that the receiving host is willing to accept in its window. Used for traffic throttling. Either host can modify this value.

Checksum 16 bits

A value computed to ensure the integrity of the packet header and contents.

Urgent Pointer 16 bits

This field is only used when the URG flag is set. Indicates the last sequence number of last urgent data block.

Options Variable

The most common usage of this field is to indicate a maximum segment size. Remaining bits are padded to 32.

HTTP Header Reference

Accept [Request] - Specifies which Internet media types are acceptable for the response and to assign additional parameters.
Accept-Charset [Request] - Specifies which character encodings are acceptable for the response and to assign preferences to them.
Accept-Encoding [Request] - Specifies which content encodings, such as compression mechanisms, are acceptable for the response and assigns preferences.
Accept-Language [Request] - Specifies which natural languages are acceptable for the response and to assign additional parameters.
Accept-Ranges [Response] - Indicates the server's acceptance of range requests for a resource.
Age [Response] - Gives the sender's estimate of the amount of time since the response, or its revalidation, was generated at the origin server.
Allow [Entity] - Lists the set of methods supported by the resource identified by the Request-URI. The purpose is to inform the recipient of valid methods associated with the resource.
Authorization [Request] - Consists of credentials containing the authentication information of the client for the realm of the resource being requested.
Cache-Control - Specifies directives that must be obeyed by all caching mechanisms along the request/response chain.
Connection - Specifies options that are desired for the particular connection and must not be communicated by proxies over further connections.
Content-Encoding [Entity] - Used as a modifier to the media-type to indicate what additional data format transformations, such as compression, have been applied to the entity-body.
Content-Language [Entity] - Specifies the natural language(s) of the intended audience for the enclosed entity.
Content-Length [Entity] - Indicates the size (in octets) of the entity-body that is sent or that would have been sent if it has reen requested.
Content-Location [Entity] - Supplies a resource location for the entity enclosed in the message when that entity is accessible from a location separate from the requested resource's URI.
Content-MD5 [Entity] - An MD5 digest of the entity-body for the purpose of providing an end-to-end integrity check of the entity-body.
Content-Range [Entity] - Sent with a partial entity-body to specify where in the full entity-body the partial body should be applied.
Content-Type [Entity] - Specifies the media type of the entity-body that is sent or would have been sent if requested.
Date - Date and time at which the message originated.
ETag [Response] - Provides the current value of the entity tag for the requested variant, for caching purposes.
Expect [Request] - Indicates that particular server behaviors are required by the client.
Expires [Entity] - Gives the date/time after which the response is considered stale, for caching purposes.
From [Request] - The Internet e-mail address for the human user who controls the requesting browser or other client.
Host [Request] - Specifies the Internet host and port number of the resource being requested. Obligatory in all HTTP/1.1 requests.
If-Match [Request] - Used with a method to make it conditional: a client that has previously obtained entities can verify that one of those entities is current by including a list of their associated entity tags in the If-Match header field.
If-Modified-Since [Request] - Used with a method to make it conditional: if the requested variant has not been modified since the time specified in this field, the server will not return the entity but information about this fact.
If-None-Match [Request] - Used with a method to make it conditional: a client that has previously obtained entities can verify that none of those entities is current by including a list of their associated entity tags in the If-None-Match header field.
If-Range [Request] - Used together with Range to say: "if the entity is unchanged, send me the part(s) that I am missing; otherwise, send me the entire new entity".
If-Unmodified-Since [Request] - Used with a method to make it conditional: if the requested variant has been modified since the time specified in this field, the server will not perform the requested operation but information about this fact.
Last-Modified [Entity] - Indicates the date and time at which the origin server believes the variant was last modified.
Location [Response] - Redirects the recipient to a location other than the Request-URI for completion of the request or identification of a new resource.
Max-Forwards [Request] - Provides a mechanism with the TRACE and OPTIONS methods to limit the number of gateways that can forward the request to the next inbound server.
Pragma - Used to include implementation-specific directives that optionally applies to any recipient along the request/response chain.
Proxy-Authenticate [Response] - Included as part of a 407 (Proxy Authentication Required) response. The field value consists of a challenge that indicates the authentication scheme and parameters applicable to the proxy for this Request-URI.
Proxy-Authorization [Request] - Used by a client to identify itself (or its user) to a proxy which requires authentication.
Range [Request] - Restricts the request to some part(s), specified as range(s) of octets, in the resource.
Referer [Request] - Used by a client to specify, for the server's benefit, the address (URI) of the resource from which the Request-URI was obtained.
Retry-After [Response] - Indicates how long the service is expected to be unavailable to the requesting client.
Server [Response] - Contains information about the software used by the origin server to handle the request.
TE [Request] - Indicates what extension transfer-codings the client is willing to accept in the response and whether or not it is willing to accept trailer fields in a chunked transfer-coding.
Trailer - Indicates that the given set of header fields is present in the trailer of a message encoded with chunked transfer-coding.
Transfer-Encoding - Indicates the type of transformation which has been applied to the message body in order to safely transfer it between the sender and the recipient.
Upgrade - Used by a client to specify what additional communication protocols it supports and would like to use if the server finds it appropriate to switch protocols. The server uses the Upgrade header to indicate which protocol(s) are being switched.
User-Agent [Request] - Contains information about the user agent (client) originating the request.
Vary [Response] - Indicates the set of request-header fields that fully determines, while the response is fresh, whether a cache is permitted to use the response to reply to a subsequent request without revalidation.
Via - Used by gateways and proxies to indicate the intermediate protocols and recipients between the user agent and the server on requests, and between the origin server and the client on responses.
Warning - Carries additional information about the status or transformation of a message which might not be reflected in the message.
WWW-Authenticate [Response] - Used in 401 (Unauthorized) response messages. The field value consists of at least one challenge that indicates the authentication scheme(s) and parameters applicable to the Request-URI.

HTTP Payload Reference

The contents of HTTP packets can vary considerably. HTTP is a fairly flexible protocol, which is used for a huge number of different puposes, from the delivery of web pages and multimedia to interprocess communications.

HTTP servers typically listen on TCP port 80, but they can be configured to listen on virtually any port. HTTP response traffic is generally sent to an ephemeral (system-assigned) port.

Samples of many common HTTP payloads can be seen below.

Ethernet Footer Reference

A 32-bit Cyclic Redundancy Check (CRC) checksum is added at the end of the Ethernet frame. It provides error detection in the case where line errors (or transmission collisions) result in frame corruption.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

CRC Checksum