Internet Protocol: Connectionless Datagram Delivery (IPv4, IPv6)

- This chapter focuses on connectionless delivery and the Internet Protocol (IP).
- IP is one of the major protocols in internetworking (TCP being the other).
- We'll explore IPv4 and IPv6 packet formats and their role in internet communication.

A Virtual Network

- Internet presents the abstraction of a single virtual network connecting all hosts.
- Focus on abstraction, not underlying interconnection technology.
- Internet is an abstraction of a large physical network.
- Higher-level internet software and applications add rich functionality.

Internet Architecture And Philosophy

- TCP/IP internet provides three sets of services.
- Conceptual levels: Connectionless Packet Delivery, Reliable Transport Service, Application Services.

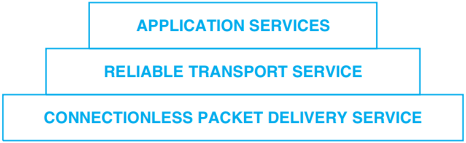

Figure 7.1 The three conceptual levels of internet services.

Figure 1: The three conceptual levels of internet services.

Principles Behind The Structure

- Internet protocols are designed around three conceptual levels.
- Connectionless service at the lowest level matches underlying hardware.
- Reliable transport service provides service to applications.
- The design has been robust and adaptable.

Connectionless Delivery System Characteristics

- Fundamental Internet service: Unreliable, best-effort, connectionless packet delivery.
- Similar to most network hardware.
- Unreliable means no guaranteed delivery.
- Connectionless treats each packet independently.
- Best-effort means earnest attempt to deliver packets.

Purpose And Importance Of The Internet Protocol

- Internet Protocol (IP) defines unreliable, connectionless delivery.
- IP specifies packet format, forwarding, and rules for unreliable delivery.
- IP is fundamental to the design of the Internet.

Next Topics

- IPv4 packet format.
- IPv6 packet format.
- Packet forwarding and error handling.

The IP Datagram

- On a physical network, the unit of transfer is a frame containing a header and data.
- In the Internet, it's called an Internet datagram (IP datagram).
- An IP datagram is divided into a header and payload, similar to a network frame.
- The header contains metadata like source and destination addresses.

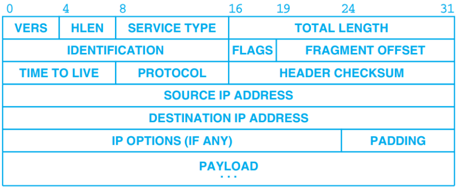

Figure 7.3 Format of an IPv4 datagram, the basic unit of transfer in a TCP/IP internet.

IPv4 Datagram Format

- IPv4 datagram structure is discussed in detail.
- IPv4 version is indicated in the datagram.
- Header length (HLEN) indicates the length of the header in 32-bit words.
- TOTAL LENGTH field specifies the length of the entire datagram (header + payload).
- PROTOCOL field indicates the format of the PAYLOAD area.
- HEADER CHECKSUM ensures header integrity.

IPv4 Datagram Format (Contd.)

- SOURCE IP ADDRESS and DESTINATION IP ADDRESS contain sender and recipient IP addresses.
- Checksums apply to header values but not payload.
- Fields allow for flexibility and reduce processing time in routers.
- The source and destination addresses remain constant throughout forwarding.

IPv4 Datagram Format (Contd.)

- PAYLOAD field carries the data and is variable in length.
- IP OPTIONS field is variable in length, discussed below.
- PADDING is used to ensure the header length is a multiple of 32 bits.

IPv4 Datagram Format (Contd.)

- The source and destination addresses in a datagram are consistent throughout forwarding.
- Header checksum ensures integrity.
- Payload length depends on the data being sent.
- Options and padding vary, affecting header length.

Conclusion

- We've explored the fundamental concepts of Internet Protocol (IP).
- IPv4 datagram format has been discussed in detail.
- Later chapters will cover packet forwarding and error handling.

IPv6 Datagram Format

- IPv6 introduces a new datagram format.
- Base header followed by optional extension headers.
- NEXT HEADER field specifies the type of the header that follows.
- Extension headers can be processed sequentially.

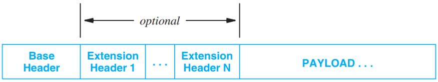

Figure 7.4 The general form of an IPv6 datagram with a base header followed by optional extension headers.

Figure 3: General form of an IPv6 datagram with base and extension headers.

IPv6 Base Header Format

- Each IPv6 datagram starts with a 40-octet base header.
- It contains less information than IPv4 headers as some details are moved to extension headers.
- IPv6 uses a 64-bit alignment.

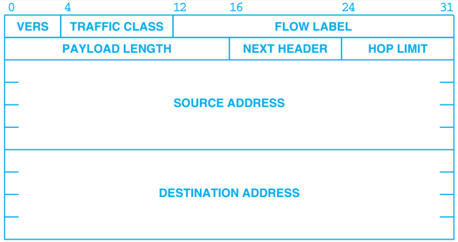

Figure 7.6 The IPv6 base header format; the size is fixed at 40 octets.

Figure 4: The IPv6 base header format.

IPv6 Base Header Format (Contd.)

- VERS field specifies IPv6 (version 6).
- TRAFFIC CLASS is analogous to IPv4's TYPE OF SERVICE.
- FLOW LABEL supports resource reservation in some technologies.
- PAYLOAD LENGTH refers only to data, excluding headers.

IPv6 Base Header Format (Contd.)

- NEXT HEADER field specifies the type of the next header.
- HOP LIMIT defines the maximum number of networks the datagram can traverse.
- SOURCE ADDRESS and DESTINATION ADDRESS contain sender and recipient IPv6 addresses.

Conclusion

- IPv6 introduces a new datagram format.
- Base header and extension headers offer flexibility.
- Base header contains essential information, with specifics moved to extensions.

Datagram Type of Service and Differentiated Services

- SERVICE TYPE (IPv4) and TRAFFIC CLASS (IPv6) fields specify datagram handling.
- Originally, SERVICE TYPE had subfields for precedence and path characteristics.
- Re-defined for Differentiated Services (DiffServ).

Figure 7.7 The differentiated services (DiffServ) interpretation of bits in the IPv4 *SERVICE TYPE* and IPv6 *TRAFFIC CLASS* header fields.

Figure 5: DiffServ interpretation of IPv4 SERVICE TYPE and IPv6 TRAFFIC CLASS fields.

Differentiated Services (DiffServ)

- The first six bits form a codepoint (DSCP), and the last two bits are unused.
- Codepoint maps to service definitions.
- Supports up to 64 separate services.

Pool	Codepoint	Assigned By
1	xxxxx0	Standards organization
2	xxxx11	Local or experimental
3	xxxx01	Local or experimental

Figure 7.8 The three administrative pools of DiffServ codepoint values.

Figure 6: Codepoint division into administrative pools for DiffServ.

Differentiated Services (DiffServ) Pools

- Three administrative pools of codepoint values.
- Pool 1: Assigned by standards organizations.
- Pools 2 and 3: Available for local or experimental use.

Service Type as a Hint

- Specifying service type in a datagram is a hint to the forwarding algorithm.
- Helps choose among available paths based on local policies and hardware.
- No guarantee of a particular service level.

Datagram Encapsulation

- Datagram size is not constrained by hardware but by protocol design (IPv4 allows up to 65,535 octets).
- Datagram encapsulation is used to efficiently transport datagrams by mapping them to network frames.
- Encapsulation means the entire datagram, including header, is treated as data by the underlying network hardware.

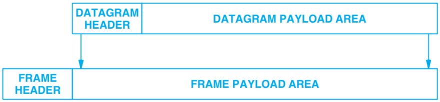

Figure 7.9 The encapsulation of an IP datagram in a frame. The underlying network treats the entire datagram, including the header, as data.

Figure 7: Encapsulation of an IP datagram in a network frame.

Identifying Encapsulated Datagrams

- Receivers identify encapsulated datagrams by the type field in the frame header.
- For example, Ethernet uses type values like 0x0800 for IPv4 and 0x86DD for IPv6.

Datagram Size and Fragmentation

- Datagram size should ideally fit within one physical network frame for efficient transmission.
- Networks have varying Maximum Transfer Units (MTU), which limit the amount of data transferred in one frame.
- Internet design principles: accommodate diverse network hardware and applications.
- The compromise: allow applications to choose datagram size, and if it exceeds the MTU, perform fragmentation.
- Fragmentation divides a datagram into smaller pieces that fit within the MTU.
- Path MTU is the minimum MTU along the path of a datagram.

IPv4 vs. IPv6 Fragmentation

- IPv4 allows any router along the path to perform fragmentation.
- IPv6 requires the original source to determine the path MTU and perform fragmentation, while routers cannot fragment.

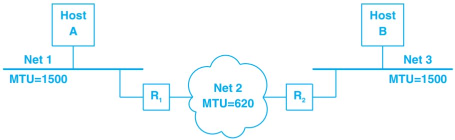

Figure 7.10 An illustration of IPv4 fragmentation. Each router may need to fragment datagrams before sending across network 2.

Figure 8: An illustration of fragmentation in IPv4 networks.

IPv4 Datagram Fragmentation

- IPv4 fragmentation occurs when a datagram is too large for a network's MTU along its path.
- Hosts ensure datagrams fit within the first network's MTU; routers handle fragmentation along the path.
- Fragmentation divides a datagram into smaller pieces, each fitting the MTU.
- Each fragment retains the same IPv4 datagram format but with flags and offset fields adjusted.
- Fragment size must be a multiple of eight octets.

IPv4 Datagram Fragmentation

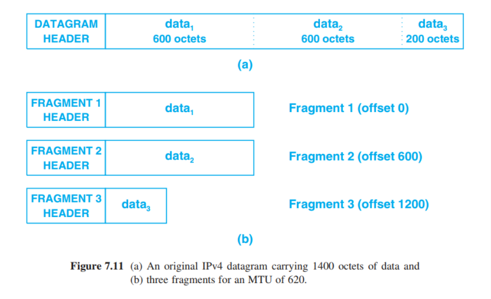

Figure 9: IPv4 fragmentation process.

IPv6 Fragmentation and Path MTU Discovery (PMTUD)

- IPv6 uses early binding, requiring the source host to find the path MTU and fragment accordingly.
- IPv6 routers cannot fragment datagrams; they send error messages if the datagram doesn't fit.
- Path MTU Discovery (PMTUD) is used to find the path's minimum MTU by probing with datagrams.
- PMTUD specifies periodic probing for possible changes in the path MTU.
- IPv6 uses Fragment Extension Headers for datagram fragmentation, containing flags and offset fields.

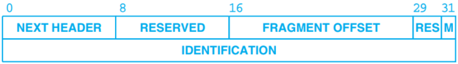

Figure 7.12 The format of an IPv6 *Fragmentation Extension Header.*

Figure 10: IPv6 fragmentation using Fragment Extension Header.