What Happens When We Type GOOGLE.com and Hit Enter

IN NETWORK LAYER

A Comprehensive Analysis Based on the TCP/IP Model

Submitted By:
Aayush Adhikari,
Roshan Tiwari,
Shishir Sharma Rijal,
Sudip Acharya

July 22, 2024

1 Introduction

When a user types "google.com" into a web browser and presses Enter, the Network Layer (Layer 3) of the OSI model plays a crucial role in routing the data packets from the user's device to Google's servers. This document provides a detailed analysis of the processes occurring at the Network Layer during this interaction.

2 Network Layer Overview

Network Layer Functions

The Network Layer is responsible for packet forwarding including routing through intermediate routers. Its primary functions include:

- Logical addressing
- Routing
- Path determination
- Packet forwarding
- Fragmentation and reassembly

3 Detailed Network Layer Processes

3.1 IP Address Resolution

IP Address Resolution Process

1. **DNS Resolution Completion:**
   - Receives resolved IP address for google.com from upper layers
   - Typically resolves to multiple IP addresses for load balancing
2. **ARP (Address Resolution Protocol) Process:**
   - Translates IP addresses to MAC addresses for local network communication
   - Broadcasts ARP request if destination MAC is unknown
   - Caches results for future use

3.2 IP Packet Formation

Packet Formation Process

1. **Packet Header Creation:**
   - Constructs IPv4 or IPv6 header
   - Sets source IP (your device) and destination IP (Google server)
2. **Header Fields Population:**
   - Version: Set to 4 (IPv4) or 6 (IPv6)
   - IHL (Internet Header Length): Typically 5 for IPv4 (20 bytes)
   - DSCP (Differentiated Services Code Point): Set for QoS if applicable
   - ECN (Explicit Congestion Notification): If supported and enabled
   - Total Length: Sum of header and payload lengths
   - Identification: Unique identifier for packet fragments
   - Flags: Sets DF (Don't Fragment) for IPv4 if path MTU discovery is active
   - Fragment Offset: 0 for unfragmented packet
   - TTL (Time To Live): Typically starts at 64 or 128
   - Protocol: Set to 6 for TCP
   - Header Checksum: Calculated over the header
3. **Options and Padding:**
   - Rarely used in modern networks
   - Ensures header is multiple of 32 bits

3.3 Routing Decision

Routing Decision Process

1. **Destination IP Analysis:**
    - Compares destination IP with local subnet mask
2. **Routing Table Lookup:**
    - Consults local routing table for next hop
    - Determines if packet should be sent to default gateway
3. **Policy-Based Routing:**
    - Applies any configured routing policies
    - May route based on source IP, protocol, or other criteria

3.4 Path Determination

Path Determination Process

1. **Metric Calculation:**
    - Considers factors like hop count, bandwidth, delay
    - Uses routing protocol's metric system (e.g., OSPF cost, BGP attributes)
2. **Best Path Selection:**
    - Chooses optimal path based on calculated metrics
    - Considers redundant paths for fault tolerance
3. **Equal Cost Multi-Path (ECMP):**
    - Distributes traffic across multiple equal-cost paths if available

3.5 Packet Forwarding

Packet Forwarding Process

1. **Next Hop Determination:**
   - Identifies next router in the path to Google's servers
2. **TTL Decrement:**
   - Decreases TTL value by 1
   - Drops packet and sends ICMP Time Exceeded if TTL reaches 0
3. **Checksum Recalculation:**
   - Recalculates header checksum after TTL modification

3.6 Fragmentation and Reassembly

Fragmentation and Reassembly Process

1. **MTU Consideration:**
   - Compares packet size with outgoing interface's MTU
2. **Fragmentation Process (if necessary):**
   - Splits packet into smaller fragments if larger than MTU
   - Sets fragmentation flags and offsets in IP header
3. **Path MTU Discovery:**
   - Uses ICMP to determine smallest MTU along the path
   - Adjusts packet size to avoid fragmentation

4 Additional Considerations

4.1 Quality of Service (QoS)

QoS Implementation

- **Traffic Classification:**
  - Identifies packet type (e.g., HTTP traffic to google.com)
- **Policy Application:**
  - Applies QoS policies based on classification
  - May prioritize or rate-limit based on configured rules
- **DSCP Marking:**
  - Sets appropriate DSCP value in IP header for end-to-end QoS

4.2 Network Address Translation (NAT)

NAT Process

- **Source NAT:**
  - Replaces private source IP with public IP if behind NAT
  - Updates IP header and recalculates checksum
- **Port Address Translation:**
  - Modifies source port if using PAT (Port Address Translation)
  - Maintains NAT translation table

5 Conclusion

The Network Layer plays a crucial role in routing packets from your device to Google's servers. It handles complex tasks such as IP addressing, routing decisions, and potential fragmentation, ensuring that your request reaches its destination efficiently and reliably. Understanding these processes is essential for network engineers to design, troubleshoot, and optimize network communications.