Subject: DHCP Server Implementation

Introduction

動態主機設定協定（Dynamic Host Configuration Protocol，縮寫為DHCP）是一種網路協定，用於自動分配IP位址和其他網路配置參數給連接到網路的設備。DHCP的目的是簡化網路管理的工作，讓網路設備能夠更容易地獲取有效的IP位址和相關的網路設定。

在傳統的網路環境中，網路管理員必須手動為每個設備分配IP位址和配置相應的網路參數，這樣的工作非常繁瑣和耗時。而有了DHCP協定，網路管理員只需要設置一個或多個DHCP伺服器，這些伺服器會自動接收設備的請求並分配IP位址和相關的網路設定。

使用DHCP的設備在加入網路時，會向網路上的DHCP伺服器發送一個「DHCPDISCOVER」訊息，該訊息是一個廣播訊息，它告訴網路上的DHCP伺服器該設備需要獲取IP位址和其他網路參數。DHCP伺服器接收到這個請求後，根據自己的設定和資源來源，為該設備分配一個可用的IP位址，同時還可能提供子網遮罩、預設閘道、DNS伺服器和其他網路設定。

使用DHCP協定有許多優點。首先，它簡化了網路管理的流程，減少了網路管理員的工作量，同時也減少了人為錯誤的可能性。其次，它提高了網路的靈活性和可擴展性，因為設備可以輕鬆地加入或退出網路，而不需要手動配置網路參數。此外，DHCP還支援租約的功能，可以控制IP位址的使用時間，使網路資源得到更有效的利用。

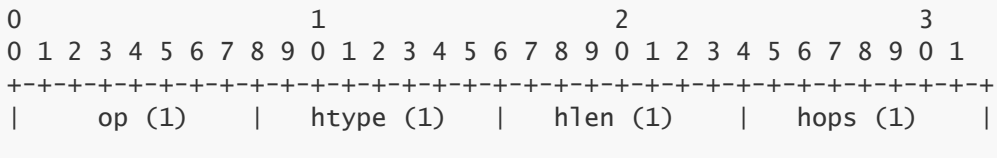
本次 Project 將實作 DHCP Server ，以深入了解 DHCP 運作原理。

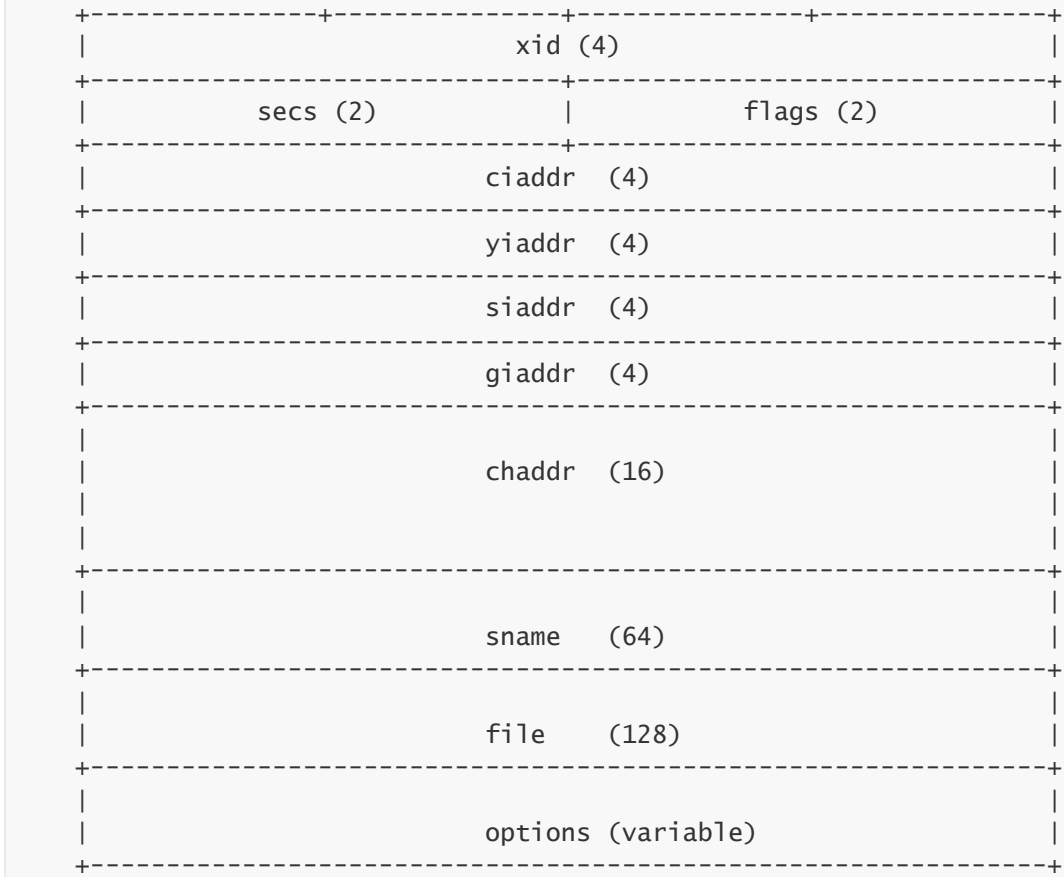
Expected Functionality

1. DHCP 請求接收：伺服器能夠監聽並接收來自客戶端的 DHCP 請求封包。
2. 動態 IP 位址分配：伺服器能夠從可用的 IP 位址池中選擇並分配一個可用的 IP 位址給客戶端。伺服器需要管理位址池，跟蹤已分配和可用的位址。
3. 靜態 IP 位址分配：伺服器能夠支援靜態 IP 位址分配，允許管理員指定特定設備使用特定的 IP 位址。
4. 網路配置回應：伺服器能夠回應客戶端的請求，提供適當的網路配置參數，如子網遮罩、預設閘道、DNS 伺服器等。
5. 租約管理：伺服器能夠管理 IP 位址的租約時間。當租約到期時，伺服器將釋放位址並重新分配給其他設備。
6. 客戶端註冊：伺服器能夠註冊已知的客戶端，使其在每次請求時保持相同的 IP 位址。
7. 錯誤處理：伺服器能夠處理可能出現的錯誤情況，如重複的 IP 位址分配、無法回應請求等。
8. 設定管理：伺服器應該提供管理界面或命令行介面，以便管理員能夠配置伺服器的參數和選項。
9. 日誌記錄：伺服器能夠記錄重要的事件和活動，以便進行故障排除和監視。

Details

DHCP packet format:





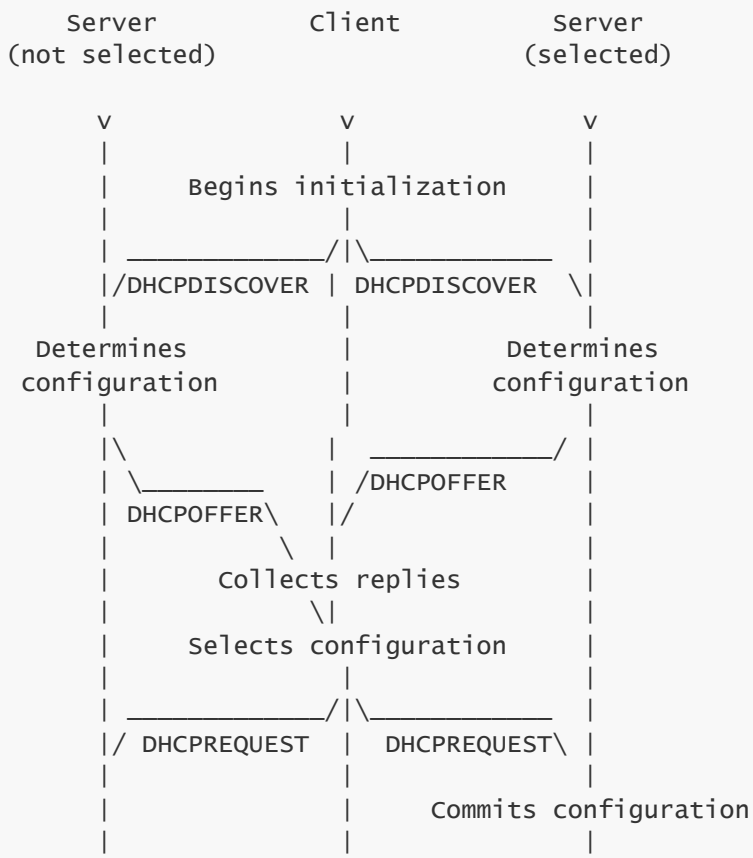
參數意義對照表：

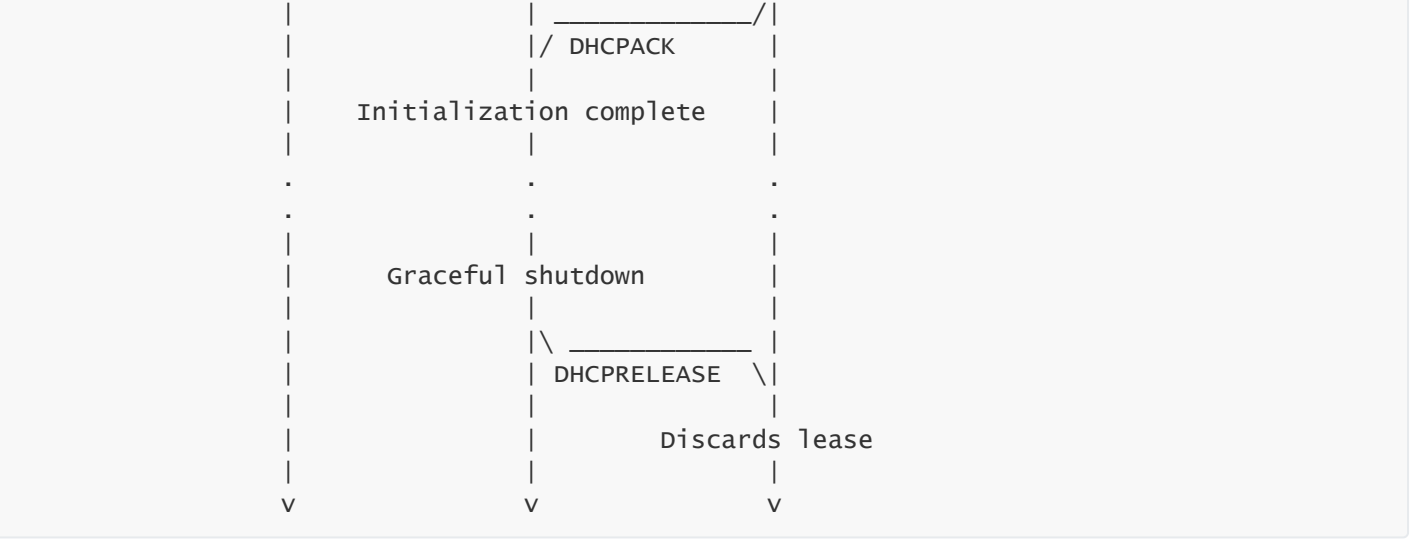
```
FIELD      OCTETS       DESCRIPTION
   -----      ------       -----------

   op            1  Message op code / message type.
                    1 = BOOTREQUEST, 2 = BOOTREPLY
   htype         1  Hardware address type, see ARP section in "Assigned
                    Numbers" RFC; e.g., '1' = 10mb ethernet.
   hlen          1  Hardware address length (e.g.  '6' for 10mb
                    ethernet).
   hops          1  Client sets to zero, optionally used by relay agents
                    when booting via a relay agent.
   xid           4  Transaction ID, a random number chosen by the
                    client, used by the client and server to associate
                    messages and responses between a client and a
                    server.
   secs          2  Filled in by client, seconds elapsed since client
                    began address acquisition or renewal process.
   flags         2  Flags (see figure 2).
   ciaddr        4  Client IP address; only filled in if client is in
                    BOUND, RENEW or REBINDING state and can respond
                    to ARP requests.
   yiaddr        4  'your' (client) IP address.
   siaddr        4  IP address of next server to use in bootstrap;
                    returned in DHCPOFFER, DHCPACK by server.
   giaddr        4  Relay agent IP address, used in booting via a
                    relay agent.
   chaddr       16  Client hardware address.
   sname        64  Optional server host name, null terminated string.
   file        128  Boot file name, null terminated string; "generic"
                    name or null in DHCPDISCOVER, fully qualified
                    directory-path name in DHCPOFFER.
   options     var  Optional parameters field.  See the options
                    documents for a list of defined options.
```

DHCP messages type:

```
Message         Use
  -------         ---

  DHCPDISCOVER -  Client broadcast to locate available servers.

  DHCPOFFER    -  Server to client in response to DHCPDISCOVER with
                  offer of configuration parameters.

  DHCPREQUEST  -  Client message to servers either (a) requesting
                  offered parameters from one server and implicitly
                  declining offers from all others, (b) confirming
                  correctness of previously allocated address after,
                  e.g., system reboot, or (c) extending the lease on a
                  particular network address.

  DHCPACK      -  Server to client with configuration parameters,
                  including committed network address.

  DHCPNAK      -  Server to client indicating client's notion of network
                  address is incorrect (e.g., client has moved to new
                  subnet) or client's lease as expired

  DHCPDECLINE  -  Client to server indicating network address is already
                  in use.

  DHCPRELEASE  -  Client to server relinquishing network address and
                  cancelling remaining lease.

  DHCPINFORM   -  Client to server, asking only for local configuration
                  parameters; client already has externally configured
                  network address.
```

DHCP Client-Server 交互流程、方法：





Server configuration file:

```
# DHCP Server Configuration

# Set the DHCP server to listen on the specified network interface
interface eth0;

# Define the IP address range to be used for DHCP leasing
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.200;
    option subnet-mask 255.255.255.0;
    option routers 192.168.1.1;
    option domain-name-servers 8.8.8.8, 8.8.4.4;
    default-lease-time 600;
    max-lease-time 7200;
}

# Specify additional DHCP options for clients
option domain-name "example.com";
option broadcast-address 192.168.1.255;
option ntp-servers 192.168.1.10;

# Configure DHCP reservations for specific clients
host client1 {
    hardware ethernet 00:11:22:33:44:55;
    fixed-address 192.168.1.50;
}

host client2 {
    hardware ethernet AA:BB:CC:DD:EE:FF;
    fixed-address 192.168.1.51;
}
```

Experimental/Development Environment

1. Programing Language: C++
2. Operation System: Linux (Ubuntu 22.04)
3. Development Tools: GCC compiler, Make build system
4. Text Editor: Vim, Visual Studio Code
5. Libraries: Standard C++ libraries for socket programming

Methodology

1. 研究 DHCP 協定：深入研究 DHCP 協定相關的標準文件，如 RFC 2131，了解 DHCP 封包的格式、協定行為和相關選項。
2. 設計伺服器架構：根據 DHCP 協定的要求，設計伺服器的架構和功能模組。確定所需的模組，如請求接收、位址分配、網路配置回應、租約管理等。
3. 實作 Socket 連接：使用 C++ TCP Socket 建立伺服器端的連接，監聽指定的 DHCP Port（預設為 67）。確保伺服器能夠接收並處理從客戶端發送的 DHCP 封包。
4. 解析 DHCP 封包：解析接收到的 DHCP 封包，檢查封包的類型、選項等。根據封包的類型和內容，進行相應的處理。
5. 動態 IP 位址分配：為客戶端分配一個可用的 IP 位址。確保 IP 位址從可用的位址池中選取，並將其標記為已分配狀態。更新位址池的狀態。
6. 靜態 IP 位址分配：實作支援靜態 IP 位址分配的機制，允許管理員指定特定的 IP 位址和網路配置參數給指定的客戶端。確保伺服器能夠識別靜態分配的請求並正確回應。
7. 網路配置回應：根據客戶端的需求和伺服器的配置，回應 DHCP 請求封包，提供相應的網路配置參數，如子網遮罩、預設閘道、DNS 伺服器等。確保回應封包中包含正確的選項和參數。
8. 租約管理：維護 IP 位址的租約時間。記錄每個分配的位址和其對應的租約到期時間。定期檢查租約的狀態，釋放過期的位址並重新分配。
9. 客戶端註冊：實作客戶端註冊機制，允許管理員將特定的 IP 位址和 MAC 地址關聯起來。確保伺服器能夠識別已註冊的客戶端並確保它們獲得相同的 IP 位址。
10. 日誌記錄：實作日誌記錄機制，記錄伺服器的活動和事件。這包括接收的 DHCP 封包、位址分配、租約更新等。透過日誌記錄，能夠追蹤和監控伺服器的運作狀態，並進行故障排除。
11. 安全性考量：考慮 DHCP 伺服器的安全性。實施適當的安全措施，例如限制伺服器的存取權限、防止未授權的設備接入、防範釣魚攻擊等。確保只有合法的客戶端能夠獲得 IP 位址和相關的網路配置。
12. 測試和驗證：進行全面的測試和驗證，確保 DHCP 伺服器的正常運作。測試各種情境下的 DHCP 請求和回應，驗證位址分配和租約管理的準確性和效能。

我們將根據 RFC 2131 和其他相關的 DHCP 協定規範來實作 DHCP 伺服器，以確保我們的實作符合標準並具有正確的功能。此外，我們還需要進行測試和調試，以驗證 DHCP 伺服器的正確性和可靠性，DHCP Server 實際運作流程如下：

1. 建立 TCP Socket 並監聽指定的 DHCP 伺服器端口。
2. 接收來自客戶端的 DHCP 封包。
3. 解析接收到的封包，檢查其中的 DHCP 請求類型和相關的選項。
4. 根據請求類型和選項，進行相應的處理和回應。這可能包括分配 IP 位址、設置子網遮罩、閘道和 DNS 伺服器等。
5. 將回應封包發送回客戶端。
6. 持續監聽和處理來自其他客戶端的 DHCP 請求。

Reference

https://datatracker.ietf.org/doc/html/rfc2131