

# Lecture 22: Application Layer

Adam Hawley

April 9, 2019

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Dynamic Host Configuration Protocol</b>	<b>2</b>
<b>3</b>	<b>Domain Name System</b>	<b>2</b>
3.1	Name Servers . . . . .	3
3.2	Hierarchy of Name Servers . . . . .	3
<b>4</b>	<b>World Wide Web</b>	<b>3</b>
4.1	Hyper Text Transfer Protocol (HTTP) . . . . .	4
4.2	Persistent TCP Connections . . . . .	4

## 1 Introduction

Applications, ranging from browsers to videoconferencing tools that run on computer networks are part:

- **Network protocols**, since they exchange messages with their peers on other hosts.
- **Traditional application programs** that interact with a host's window and file systems as well as with the user.

We will discuss three main examples:

**DHCP (Dynamic Host Configuration Protocol)** Dynamically assigns IP addresses to devices (over UDP).

**DNS (Domain Name System)** Translates host names into IP addresses (over UDP, TCP for zone transfers between servers).

**WWW (World Wide Web)** (Over TCP)

## **2 Dynamic Host Configuration Protocol**

DHCP assigns an IP address to a host. This cannot be done by the host manufacturer as hosts on the same network must have the same network IP address. IP addresses need to be re-configurable, in case hosts are moved between networks or if network topologies change. This avoids placing the burden onto a system administrator to assign IP addresses uniquely and correctly.

Within each collision domain there should be a DHCP server so that the IP can be given to the host even though the host does not have a full address yet. Because this is not very practical, often DHCP relays are used (see slide 6 for diagram of DHCP connections).

Four step handshake:

1. Client sends broadcast (Ethernet and IP) discovery packet (claims IP source = 0.0.0.0)
2. DHCP server or relay receives and responds to discovery packet over broadcast (IP) of that collision domain and sender's MAC address for Ethernet. Payload includes:
  - Offered IP address
  - Subnet mask
  - Gateway IP address
  - Lease time
  - DNS servers
3. Client sends request to the DHCP server (this stage means that if there is more than one DHCP server within the collision domain then the client will only respond to one).
4. DHCP server sends acknowledgement to the IP offered.

## **3 Domain Name System**

DNS is a naming system that allows one to assign names (variable length, mnemonic but providing almost no routing information) to nodes. A name service translates between user-friendly names and router-friendly addresses.

Name spaces can be flat but are often hierarchical (cf. the name `www.cs.york.ac.uk`). DNS maintains a collection of bindings of names to values (usually addresses). A **name server** implements a **resolution mechanism** for mapping names to values, that can be queried on a network. The Internet's naming system is called **Domain Name System**, is based on hierarchical names and distributes the **binding table** throughout the Internet.

### 3.1 Name Servers

Name servers store **resource records**:

- <Name, Value, Type, Class, TTL>
  - Name, Value: As expected
  - Type: States how to interpret Value (e.g. IPv4 or IPv6 or Name Server which is a server which does know how to deal with a given name).
  - Class: Only the Internet class ("IN") is in use today.
  - TTL (time-to-live): Used for sensibly caching resource records.

### 3.2 Hierarchy of Name Servers

The domain name hierarchy is implemented by partitioning the domain name tree into **zones**. Each zone operates a name server (and a backup server) which is accessible via the Internet. In order to ease the load on networks and servers, **name servers cache resource records** until the TTL field for each record under consideration expires.

## 4 World Wide Web

The WWW is the main driver for making the Internet accessible. It consists of sets of cooperating clients and servers. It is important to distinguish between application programs and protocols:

- The Hyper Text Transfer Protocol (HTTP) is used for retrieving web pages from remote servers over the Internet.
- Web clients (such as Firefox and IE) are **browser** programs with different looks and feels but all employ HTTP.

Steps that occur when a link is selected:

1. Browser determines URL
2. Browser asks DNS for the IP address of the server
3. DNS replies
4. The browser makes a TCP connection
5. Sends HTTP request for the page
6. Server sends the page as HTTP response
7. Browser fetches other URLs as needed
8. The browser displays the page
9. The TCP connections are released

#### 4.1 Hyper Text Transfer Protocol (HTTP)

When a user asks a web client to open a web page specified by a **uniform resource locator (URL)**, the browser fetches the HTML file from the web server and then displays the encoded page. HTTP is a **text-oriented protocol** where messages are of the form:

```
START_LINE <CRLF>
MESSAGE_HEADER <CRLF>
<CRLF>
MESSAGE_BODY <CRLF>
```

See slides 21 and 22 for examples of HTTP requests and responses.

#### 4.2 Persistent TCP Connections

HTTP/1.1 uses **persistent TCP connections**, i.e. client and server can exchange multiple messages over the same TCP connection. Advantages include:

- Eliminates the **connection setup overhead** (reduce the load on the server and on the network).
- Allows TCPs **congestion window mechanism** to work properly.

Disadvantage:

- Who decides when a connection should be closed?

- Server times out and tears down its part of the TCP connection if a client does not use the server for some time.
- Client has to watch out for such behaviour and tear down its direction of the TCP connection too.