CCNA R&S: Introduction to Networks

Chapter 10:

The Application Layer

Frank Schneemann
Upon completion of this chapter you will be able to:

- Explain how the functions of the application layer, session layer, and presentation layer work together to provide network services to end user applications.
- Describe how common application layer protocols interact with end user applications.
- Describe, at a high level, common application layer protocols that provide Internet services to end-users, including WWW services and email.
- Describe application layer protocols that provide IP addressing services, including: DNS and DHCP.
- Describe the features and operation of well-known application layer protocols that allow for file sharing services, including: FTP, File Sharing Services, SMB protocol.
- Explain how data is moved across the network, from opening an application, to receiving data.
Network applications…
- make communication in the workplace easier
- affect the amount of work completed on a daily basis
- reduce data communications time and costs
The application layer is the top layer of both the OSI and TCP/IP models.

The TCP/IP application layer includes a number of protocols that provide specific functionality to a variety of end-user applications.

The functionality of the TCP/IP application layer protocols fit roughly into the framework of the top three layers of the OSI model: application, presentation and session layers.

The OSI model Layers 5, 6, and 7 are used as references for application software developers and vendors to produce products, such as web browsers that need to access networks.
10.1.1.2 Application Layer

Application layer protocols are used to exchange data between programs running on the source and destination hosts.
10.1.1.3 Presentation and Session Layers

The presentation layer has three primary functions:

- **Formats**, or presents, data from the source device into a compatible form for receipt by the destination device.
- **Compression** of the data in a way that can be decompressed by the destination device.
- **Encryption** of the data for transmission and the decryption of data upon receipt by the destination.
10.1.1.4 TCP/IP Application Layer Protocols

- **Name System**
  - DNS
  - DHCP

- **Host Config**
  - BOOTP

- **Email**
  - SMTP
  - POP
  - IMAP

- **File Transfer**
  - FTP
  - TFTP

- **Web**
  - HTTP
10.1.1.5 Activity – Application Protocols and Standards

OSI Model

7 Application
- HTTP
- IMAP
- DNS
- POP
- TFTP
- DHCP

6 Presentation
- HTML
- JPEG
- MPEG

5 Session

TCP/IP Model

Application
- HTML
- POP
- IMAP

- HTTP
- TFTP
- JPEG

- MPEG
- DNS
- DHCP
10.1.2.1 Peer-to-Peer Networks

Peer-to-Peer Networking

I have files on my hard drive that are being shared for Peer2. I also have a page that I need to print through Peer2.

I need to access a file from the hard drive on Peer1. I also need to print a file that I received from Peer1, with a print request.

Peer1
Print client
File server

Peer2
Print server
File client

Printer
Directly connected printer
A peer-to-peer (P2P) application allows a device to act as both a client and a server within the same communication, as shown in the figure.
With P2P applications, each computer in the network running the application can act as a client or a server for the other computers in the network running the application. Common P2P applications include:

- eDonkey
- eMule
- Shareaza
- BitTorrent
- Bitcoin
- LionShare

Some P2P applications are based on the **Gnutella protocol**. They enable people to share files on their hard disks with others. As shown in the figure,
In this lab, you will complete the following objectives:

- Part 1: Identify P2P Networks, File Sharing Protocols, and Applications
- Part 2: Research P2P File Sharing Issues
- Part 3: Research P2P Copyright Litigations
10.1.2.5 Client-Server Model

Client/Server Model

Files are downloaded from the server to the client.

Resources are stored on the server.

A client is a hardware/software combination that people use directly.
Three application layer protocols that are involved in everyday work or play are:

- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol (POP)
10.2.1.2 Hypertext Transfer Protocol and Hypertext Markup Language

HTTP Protocol Step 2

HTTP/1.1 200 OK
Date: Mon, 23 May 2005 22:38:34 GMT
Server: Apache/1.3.27 (unix) (Red-Hat/Linux)
Etag: "3f80f-1b6-3elcb03b"
Accept-Ranges: bytes
Content-Length: 438
Connection: close
content-Type: text/html; charset=UTF-8

<html>
<head>
<title>Cisco Systems Inc, Home Page</title>
</head>
<body>
...CONTENTS OF HTML PAGE...
</body>
10.2.1.3 HTTP and HTTPS

HTTPS uses the same client request-server response process as HTTP, but the data stream is encrypted with Secure Socket Layer (SSL) before being transported across the network. HTTPS creates additional load and processing time on the server due to the encryption and decryption of traffic.
Email is a store-and-forward method of sending, storing, and retrieving electronic messages across a network. Email messages are stored in databases on mail servers. ISPs often maintain mail servers that support many different customer accounts.
Simple Mail Transfer Protocol (SMTP) transfers mail reliably and efficiently. For SMTP applications to work properly, the mail message must be formatted properly and SMTP processes must be running on both the client and server.

SMTP message formats require a message **header** and a message **body**. While the message body can contain any amount of text, the message header must have a properly formatted recipient email address and a sender address. Any other header information is optional.
Post Office Protocol (POP) enables a workstation to retrieve mail from a mail server. With POP, mail is downloaded from the server to the client and then deleted on the server.

The server starts the POP service by passively listening on TCP port 110 for client connection requests. When a client wants to make use of the service, it sends a request to establish a TCP connection with the server. When the connection is established, the POP server sends a greeting. The client and POP server then exchange commands and responses until the connection is closed or aborted.
Internet Message Access Protocol (IMAP) is another protocol that describes a method to retrieve email messages. However, unlike POP, when the user connects to an IMAP-capable server, copies of the messages are downloaded to the client application. The original messages are kept on the server until manually deleted. Users view copies of the messages in their email client software.

Users can create a file hierarchy on the server to organize and store mail. That file structure is duplicated on the email client as well. When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.
In this activity, you will configure HTTP and email services using the simulated server in Packet Tracer. You will then configure clients to access the HTTP and email services.
10.2.2.1 Domain Name Service

Resolving DNS Addresses Step 2

The DNS server matches the domain name with numeric address. The devices use numbers.
The DNS server stores different types of resource records used to resolve names. These records contain the name, address, and type of record. Some of these record types are:

- **A** - An end device address
- **NS** - An authoritative name server
- **CNAME** - The canonical name (or Fully Qualified Domain Name) for an alias; used when multiple services have the single network address, but each service has its own entry in DNS
- **MX** - Mail exchange record; maps a domain name to a list of mail exchange servers for that domain

When a client makes a query, the server’s BIND process first looks at its own records to resolve the name. If it is unable to resolve the name using its stored records, it contacts other servers to resolve the name.
10.2.2.3 DNS Hierarchy

• The naming structure is broken down into small, manageable zones.
• Each DNS server maintains a specific database file and is only responsible for managing name-to-IP mappings for that small portion of the entire DNS structure.
• When a DNS server receives a request for a name translation that is not within its DNS zone, the DNS server forwards the request to another DNS server within the proper zone for translation.
Computer operating systems also have a utility called `nslookup` that allows the user to manually query the name servers to resolve a given hostname. This utility can also be used to troubleshoot name resolution issues and to verify the current status of the name servers.

In the figure, when the `nslookup` command is issued, the default DNS server configured for your host is displayed. In this example, the DNS server is `dns-sj.cisco.com` which has an address of 171.70.168.183.
10.2.2.5 Syntax Checker - DNS CLI Commands in Windows and UNIX

**Using the `nslookup` Command**

Enter the `nslookup` command to begin a manual query of the name servers.

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
c: \>

c: \> nslookup
Default Server: UnKnown
Address: 10.10.10.1

The output lists the name and IP address of the closest name server. In this case, the user is in a home network behind a router firewall. The address is the router.

You are now in `nslookup` mode. Enter the domain name `www.cisco.com`.
As in Windows, you can directly query the DNS servers by simply adding the domain name to the 'nslookup' command. Enter 'nslookup www.google.com'.

```
user@cisconetacad$ nslookup www.google.com
Server:     127.0.1.1
Address:    127.0.1.1#53

Non-authoritative answer:
Name:       www.google.com
Address:    74.125.225.209
Name:       www.google.com
Address:    74.125.225.210
Name:       www.google.com
Address:    74.125.225.211
Name:       www.google.com
Address:    74.125.225.212
Name:       www.google.com
Address:    74.125.225.208

user@cisconetacad$
```

You successfully used the nslookup command to verify the status of domain names.
DHCP allows a host to obtain an IP address dynamically when it connects to the network. The DHCP server is contacted and an address requested. The DHCP server chooses an address from a configured range of addresses called a pool and assigns (leases) it to the host for a set period.
When a DHCP-configured device boots up or connects to the network, the client broadcasts a DHCP discover (DHCPDISCOVER) message to identify any available DHCP servers on the network. A DHCP server replies with a DHCP offer (DHCPOFFER) message, which offers a lease to the client. The offer message contains the IP address and subnet mask to be assigned, the IP address of the DNS server, and the IP address of the default gateway. The lease offer also includes the duration of the lease.
In this activity, you will configure and verify static IP addressing and DHCP addressing. You will then configure a DNS server to map IP addresses to the website names.
In this lab, you will complete the following objectives:

- Part 1: Observe the DNS Conversion of a URL to an IP Address
- Part 2: Observe DNS Lookup Using the nslookup Command on a Web Site
- Part 3: Observe DNS Lookup Using the nslookup Command on Mail Servers
10.2.3.1 File Transfer Protocol

As the figure illustrates, to successfully transfer data, FTP requires two connections between the client and the server, one for commands and replies, the other for the actual file transfer:

• The client establishes the first connection to the server for control traffic, consisting of client commands and server replies.
• The client establishes the second connection to the server for the actual data transfer. This connection is created every time there is data to be transferred.

The data transfer can happen in either direction. The client can download (pull) data from the server or, the client can upload (push) data to the server.
In this activity, you will configure FTP services. You will then use the FTP services to transfer files between clients and the server.
In this lab, you will complete the following objectives:

- Part 1: Use FTP from a Command Prompt
- Part 2: Download an FTP File Using WS_FTP LE
- Part 3: Use FTP in a Browser
10.2.3.4 Server Message Block

SMB messages can:

- Start, authenticate, and terminate sessions
- Control file and printer access
- Allow an application to send or receive messages to or from another device

SMB is a client-server, request-response protocol. Servers can make their resources available to clients on the network.
A file may be copied from PC to PC with Windows Explorer using the SMB protocol.
10.3.1.1 The Internet of Things

Using smart-tagging and advanced connectivity to digitize unintelligent products - from bikes and bottles, to refrigerators and cars - and connect them to the Internet, will allow people and companies to interact in new and almost unimaginable ways. Objects will be able to collect, receive and send information to users and other connected objects. As shown in the figure, this new wave in Internet development is known as the Internet of Things!
When an application sends a request to a server application, the message is built by the application layer, but is then passed down through all the various layer functionalities on the client for delivery. As it moves through the stack each lower layer encapsulates the data with a header that contains the protocols of communication for that layer.
10.3.1.3 Getting the Data to the End Device

The Internet layer creates an IP datagram or packet. The packet includes the source and destination IP addresses. The packet is passed to the network access layer.
10.3.1.4 Getting the Data through the Internetwork

The network access layer frames the packet with source and destination MAC addresses, and then converts the frame to electrical signals.
As shown in the figure, recall that at the transport layer, information contained in the PDU header identifies the specific process or service running on the destination host device that will act on the data. Hosts, whether they are clients or servers on the Internet, can run multiple network applications simultaneously. People using PCs often have an email client running at the same time as a web browser, an instant messaging program, some streaming media, and perhaps even a game. All these separately running programs are examples of individual processes.
An entertaining resource to help you visualize networking concepts is the animated movie "Warriors of the Net" by TNG Media Lab.

To view the video, Warriors of the Net, go to: http://www.warriorsofthe.net

http://www.bing.com/videos/search?q=warriors%20of%20the%20net&FORM=BVLH1#view=detail&mid=46AFE91FF2936DFF2E8946AFE91FF2936DFF2E89
Network applications use protocols to facilitate data communication...

- POP
- IMAP
- HTTP
- FTP

...and the list goes on!
Multiuser - Tutorial
10.4.1.3 Packet Tracer Multiuser - Implement Services

Multiuser - Implement Services
Thanks for your attention!!