OLD DOMINION UNIVERSITY

CYSE 301: CYBERCITY TECHNIQUES AND OPERATIONS

FALL 2017

Module I
Traffic Tracing and Analysis

Topic 2: Introduction of Network Protocols

1. Introduction

In this module, we are going to learn about the basic network structures and the way of simple network defense and countermeasures. As a network administrator, if we want to set up and maintain a simple functionality and security network, we are not only need to master the fundamental knowledge of the network but also need to operate and configure the network facility such as the switch, router and firewall in the field and track the trace of the package through the network to deeply understand how to do cyber defense from the very beginning. Also, as a network administrator, one essential ability is to capture and analyze network traffic. This can be important to identify the cause of bottleneck, determining who is responsible for certain intrusion.

2. Objective

The objective of this topic is to understand different layered network protocols in the data communication. A focus is placed on the analysis of protocols at different layers, network architectures, and networking systems performance analysis. The following subtopics will be addressed:

1. Learn the layered network protocols
2. Understand the fundamentals of wireless networks

3. Layered Network Protocols

In the last topic, we reviewed the OSI Network Model (7 Layers) and TCP/IP Model (5 Layers) and TCP/IP Model will be used in this lab instruction. And at the end of the last topic, there is a figure and a table to tell the difference between OSI Model and TCP/IP Model. Today's topic will start from there to study some most widely used protocols in the TCP/IP model.

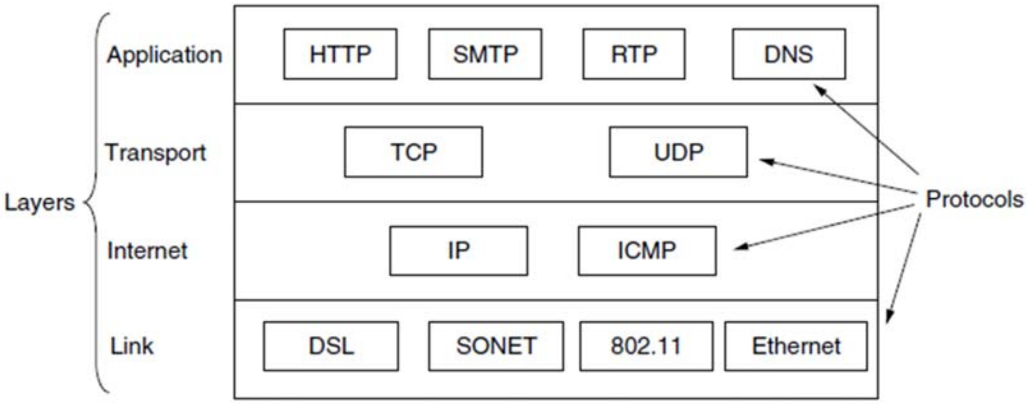

Figure 1 The TCP/IP model with some protocols we will study

3.1 The Link Layer

In the TCP/IP Model, the link layer replaces the Data link layer and Physical layer in the OSI model. The link layer describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer. It is not really a layer at all, in the normal sense of the term, but rather an interface between hosts and transmission links, which means, it varies from host to host and network to network.

Fig.1 gives some example (DSL, SONET, 802.11, Ethernet) on the protocols running on the Link layer. Each of these protocols define a different way to access the network. For example:

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands.

Ethernet is a family of computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN). It was commercially introduced in 1980 and first standardized in 1983 as IEEE 802.3 and has since been refined to support higher bit rates and longer link distances. Over time, Ethernet has largely replaced competing wired LAN technologies such as *token ring*, *FDDI* and *ARCNET*.

3.2 The Internet Layer

The ***Internet layer*** is the linchpin that holds the whole architecture together. Its job is to permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network). They may even arrive in a completely different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired.

The internet layer defines an official packet format and protocol called ***IP (Internet Protocol)***, plus a companion protocol called ***ICMP (Internet Control Message Protocol)*** that helps it function. The job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly a major issue here, as is congestion (though IP has not proven effective at avoiding congestion).

Internet Protocol: The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. No over, IP is a ***connectionless*** protocol, which means that there is no continuing connection between the end points that are communicating.

Internet Control Message Protocol: ICMP is not used regularly in end-user applications, it is used by network administrators to troubleshoot Internet connections in diagnostic utilities including *ping* and *traceroute*.

3.3 The Transport Layer

The layer above the internet layer in the TCP/IP model is now usually called the **transport layer**. It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer. Two end-to-end transport protocols have been defined here:

Transmission Control Protocol: TCP is a reliable ***connection-oriented protocol*** that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It segments the incoming byte stream into discrete messages and passes each one on to the internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

User Datagram Protocol: UDP is an unreliable, **connectionless protocol** for applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video. The relation of IP, TCP, and UDP is shown in Fig. 1. Since the model was developed, IP has been implemented on many other networks.

3.4 The Application Layer

On top of the transport layer is the **application layer**. It contains all the higher-level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP). Many other protocols have been added to these over the years. Some important ones that we will study, shown in Fig. 1 include the Domain Name System (DNS), HTTP, and RTP, the protocol for delivering real-time media such as voice or movies.

Dominion Name System: DNS are the Internet's equivalent of a phone book. They maintain a directory of domain names and translate them to Internet Protocol (IP) addresses. DNS will make people easily to remember and access a website such like " www.odu.edu " not its IP address "128.82.112.29".

HTTP is the protocol for fetching pages on the World Wide Web and it functions as a *request–response* protocol in the *client–server* computing model. A web browser, for example, may be the client and an application running on a computer hosting a website may be the server. The client submits an HTTP request message to the server. The server, which provides resources such as HTML files and other content, or performs other functions on behalf of the client, returns a response message to the client. The response contains completion status information about the request and may also contain requested content in its message body.

HTTPS (also called HTTP over Transport Layer Security (TLS), consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security, or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.