Assignment No.11

Title:

Study and Analyze the performance of HTTP, HTTPS and FTP protocol using Packet tracer tool.

Theory:

File Transfer Protocol (FTP)

File Transfer Protocol(FTP) is an application layer protocol which moves files between local and remote file systems. It runs on the top of TCP, like HTTP. To transfer a file, 2 TCP connections are used by FTP in parallel: control connection and data connection.

FTP Session :

When a FTP session is started between a client and a server, the client initiates a control TCP connection with the server side. The client sends control information over this. When the server receives this, it initiates a data connection to the client side. Only one file can be sent over one data connection. But the control connection remains active throughout the user session. As we know HTTP is stateless i.e. it does not have to keep track of any user state. But FTP needs to maintain a state about its user throughout the session.

Data Structures : FTP allows three types of data structures :

1. **File Structure –** In file-structure there is no internal structure and the file is considered to be a continuous sequence of data bytes.
2. **Record Structure –** In record-structure the file is made up of sequential records.
3. **Page Structure –** In page-structure the file is made up of independent indexed pages.
4.

Hypertext Transfer Protocol (HTTP)

The Hypertext Transfer Protocol (HTTP) is an application-level protocol that uses TCP as an underlying transport and typically runs on port 80. HTTP is a stateless protocol i.e. server maintains no information about past client requests.

HTTP was invented alongside HTML to create the first interactive, text-based web browser: the original World Wide Web. Today, the protocol remains one of the primary means of using the Internet.

As a request-response protocol, HTTP gives users a way to interact with web resources such as HTML files by transmitting hypertext messages between clients and servers. HTTP clients generally use Transmission Control Protocol (TCP) connections to communicate with servers.

HTTP utilizes specific request methods in order to perform various tasks. All HTTP servers use the GET and HEAD methods, but not all support the rest of these request methods:

- GET requests a specific resource in its entirety
- HEAD requests a specific resource without the body content
- POST adds content, messages, or data to a new page under an existing web resource
- PUT directly modifies an existing web resource or creates a new URI if need be

- DELETE gets rid of a specified resource
- TRACE shows users any changes or additions made to a web resource
- OPTIONS shows users which HTTP methods are available for a specific URL
- CONNECT converts the request connection to a transparent TCP/IP tunnel
- PATCH partially modifies a web resource

HTTP Connections

1. Non-Persistent
2. Persistent

HTTPS (HTTP over SSL or HTTP Secure)

HTTPS is an abbreviation of **Hypertext Transfer Protocol Secure**. It is a secure extension or version of HTTP. This protocol is mainly used for providing security to the data sent between a website and the web browser. It is widely used on the internet and used for secure communications. This protocol uses the 443 port number for communicating the data.

This protocol is also called **HTTP over SSL** because the HTTPS communication protocols are encrypted using the SSL (Secure Socket Layer).

By default, it is supported by various web browsers.

Those websites which need login credentials should use the HTTPS protocol for sending the data.

Difference between HTTP and HTTPS

HTTP	HTTPS
1. It is an abbreviation of Hypertext Transfer Protocol	1. It is an abbreviation of Hypertext Transfer Protocol Secure.
2. This protocol operates at the application layer.	2. This protocol operates at the transport layer.
3. The data which is transferred in HTTP is plain text.	3. The data which is transferred in HTTPS is encrypted, i.e., ciphertext.
4. By default, this protocol operates on port number 80.	4. By default, this protocol operates on port number 443.
5. The URL (Uniform Resource Locator) of HTTP start with http://	5. The URL (Uniform Resource Locator) of HTTPS start with https://
6. This protocol does not need any certificate.	6. But, this protocol requires an SSL (Secure Socket Layer) certificate.
7. Encryption technique is absent in HTTP.	7. Encryption technique is available or present in HTTPS.
8. The speed of HTTP is fast as compared to HTTPS.	8. The speed of HTTPS is slow as compared to HTTP.

9. It is un-secure.	9. It is highly secure.
10. Examples of HTTP websites are Educational Sites, Internet Forums, etc.	10. Examples of HTTPS websites are shopping websites, banking websites, etc.

Analyzing Site Traffic

To show you the traffic level for a given site over a selected period of time: Step 1 Choose Analyze > Traffic > Site. Step 2 To change the data to see the top application traffic coming into a specific site, out of a specific site, or all traffic within, coming in and moving out of that site, use the traffic selector buttons. Step 3 To see site conversations about the conversation between sites to pinpoint specific applications or sites, select the Site Conversations button and choose filters from the Interactive Report to further pinpoint an application, data source, or time frame in question. Step 4 To view top applications transmitting and receiving traffic for the selected time period and drill down to collect more data utilizing capture data, real-time graphs, and application group detail), left click the Top N Application dashboard. Step 5 To see the criteria by which the Packet Analyzer classifies the amount of application traffic on this site over this period of time, use the view Application Distribution graph. Hover over graph parts to view detailed information on speed and percentages or left-click a graph element for other menu options.

Analyzing Application Traffic

To show you the traffic level for a given application over a selected period of time: Step 1 Choose Analyze > Traffic > Application. Step 2 To see data for a different time interval (when No data for select time interval displays), click Filter on the Interactive Report, and expand the time range to allow more data to be viewed. Step 3 To focus in on a spike or area of interest, use the slider under the Application Traffic graph. Hover over the data points to see specific traffic details. Step 4 To see top application traffic details, click Top Application Traffic and choose filters from the Interactive Report to further pinpoint a data source, encapsulation method, or time frame in question. Step 5 To view top hosts transmitting and receiving traffic for the selected time period and drill down to collect more data utilizing capture data, real-time graphs, and application group detail), left-click a Top N Hosts graph element and select a specific task. Step 6 For example, select Hosts Detail to see the All Hosts window and the detailed information about all hosts. Table D-45 describes the fields in this window. Step 7 To show the criteria by which the Packet Analyzer classifies packets as that application, select one of the options under the Application Configuration. This is typically a list of TCP and/or UDP ports that identify the application. Some applications are identified by heuristic or other state-based algorithms. You can select Configure Application to configure specific applications in your network

Analyzing Host Traffic

The Host Traffic Analysis window will show you at a quick glance the input and output of a particular host over a specified time range. It is available under the menu option Analyze > Traffic > Host. It will show you: • Input and output traffic for the host • Top N application activity of the host over the selected interval • Total application usage distribution for the host • Host Conversations—Shows detailed lists of all the conversations for a particular host.

Using the Packet Analyzer Application Programming Interface Packet Analyzer provides an Application Programming Interface (API) that allows you to configure and retrieve data from the Packet Analyzer. The API follows the commonly used Representational State Transfer (REST)

style of providing services over HTTP or HTTPS. The Packet Analyzer REST API is also referred to as the Northbound Interface (NBI).

Conclusion:

Hence we have studied and analyzed the performance of HTTP, HTTPS and FTP protocol using Packet tracer tool.