Unit 6: The Application Layer

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

Functions of Application Layer:

- **Network virtual terminal.** A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
- **File transfer, access, and management.** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **Mail services.** This application provides the basis for e-mail forwarding and storage.
- **Directory services**. This application provides distributed database sources and access for global information about various objects and services.

Application Layer Protocols:

Domain Naming System (DNS):

The domain name system (DNS) is a naming database in which internet domain names are located and translated into internet protocol (IP) addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate a website. For example, if someone types example.com into a web browser, a server behind the scenes will map that name to the corresponding IP address. Facebook.com will be mapped to 66.220.144.0. Web browsing and most other internet activities rely on DNS to quickly provide the information necessary to connect users to remote hosts.

Although it's possible to enter an IP address into a web browser into order to get to a website, it's a lot easier to enter its domain name instead. However, computers, servers and other devices are unable to make heads or tails of domain names - they strictly rely on binary identifiers. The DNS's job, then, is to take domain names and translate them into the IP addresses that allow machines to communicate with one another. Every domain name has at least one IP address associated with it.

Figure 25.8 *DNS used in the Internet*

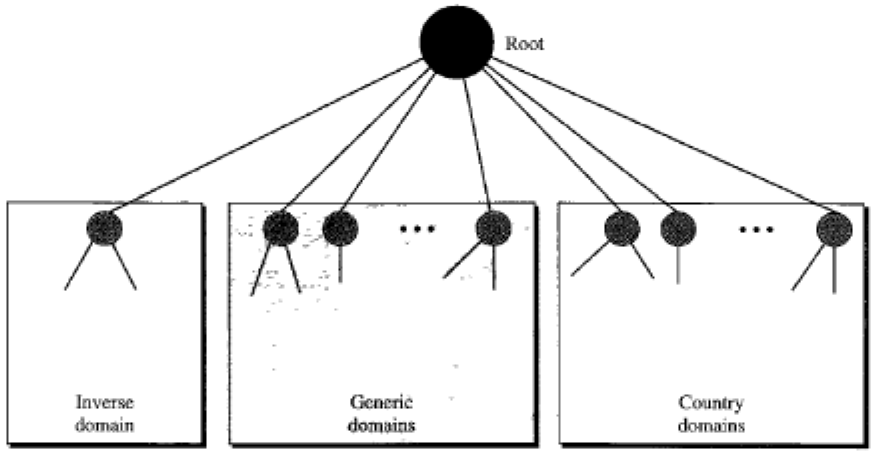
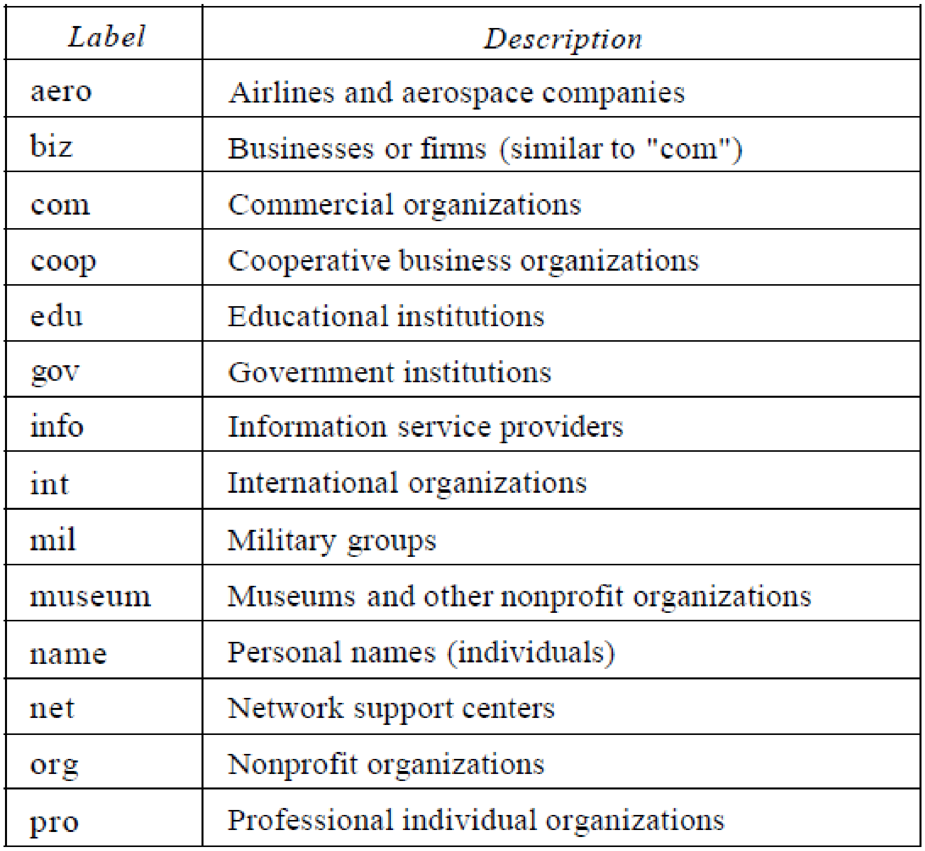
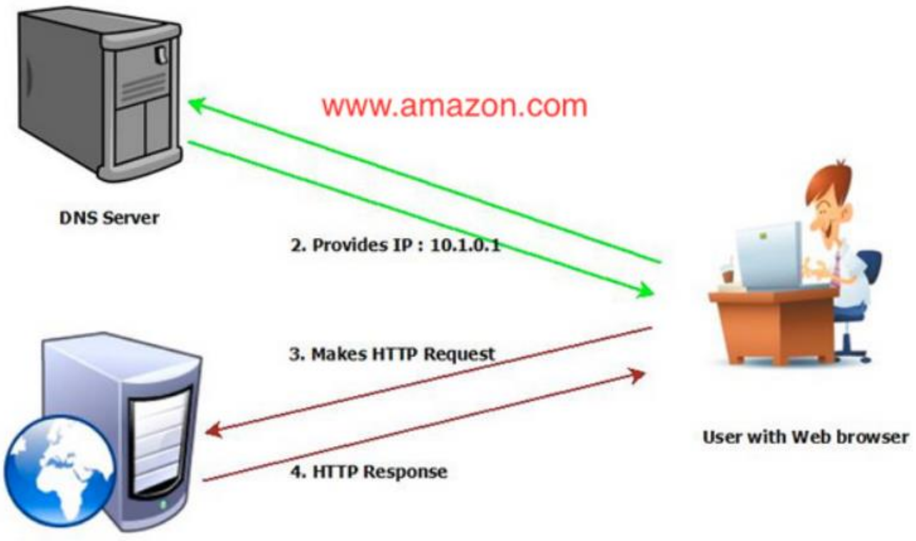


Table 25.1 *Generic domain labels*



Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other nonprofit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations



There are three types of queries in the DNS system:

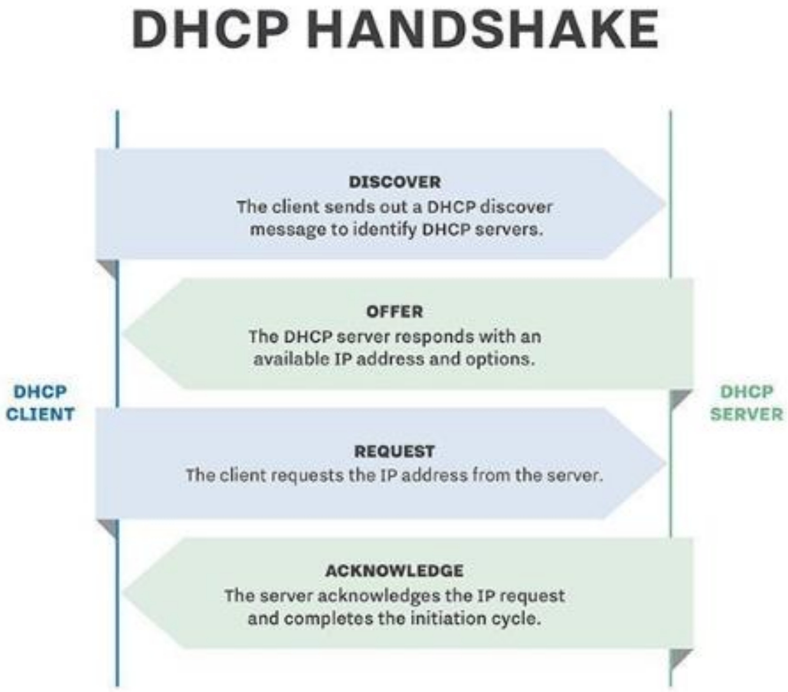
- **Recursive Query**
  In a recursive query, a DNS client provides a hostname, and the DNS Resolver “must” provide an answer—it responds with either a relevant resource record, or an error message if it can't be found. The resolver starts a recursive query process, starting from the DNS Root Server, until it

finds the Authoritative Name Server that holds the IP address and other information for the requested hostname.

- **Iterative Query**
  In an iterative query, a DNS client provides a hostname, and the DNS Resolver returns the best answer it can. If the DNS resolver has the relevant DNS records in its cache, it returns them. If not, it refers the DNS client to the Root Server, or another Authoritative Name Server which is nearest to the required DNS zone. The DNS client must then repeat the query directly against the DNS server it was referred to.
- **Non-Recursive Query**
  A non-recursive query is a query in which the DNS Resolver already knows the answer. It either immediately returns a DNS record because it already stores it in local cache, or queries a DNS Name Server which is authoritative for the record, meaning it definitely holds the correct IP for that hostname. In both cases, there is no need for additional rounds of queries (like in recursive or iterative queries). Rather, a response is immediately returned to the client.

Dynamic Host Configuration Protocol (DHCP):

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on UDP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider (ISP), reducing the need for a network administrator or a user to manually assign IP addresses to all network devices. In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address.


DHCP HANDSHAKE
DISCOVER
The client sends out a DHCP discover message to identify DHCP servers.
OFFER
The DHCP server responds with an available IP address and options.
DHCP CLIENT
DHCP SERVER
REQUEST
The client requests the IP address from the server.
ACKNOWLEDGE
The server acknowledges the IP request and completes the initiation cycle.

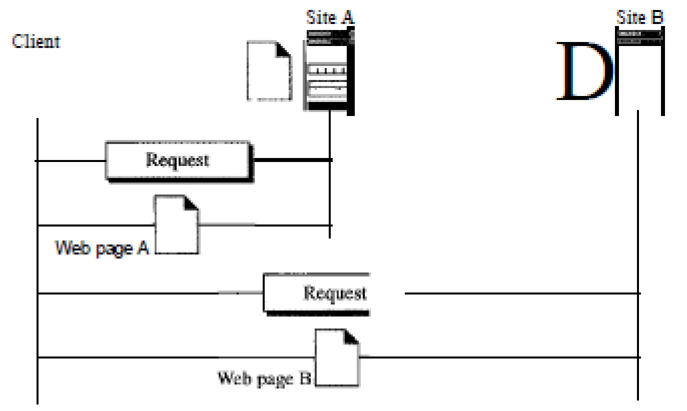
World Wide Web (WWW):

Web services are information exchange systems that use the Internet for direct application-to-application interaction. These systems can include programs, objects, messages, or documents. A web service is a collection of open protocols and standards used for exchanging data between applications or systems.

The World Wide Web (WWW) is a repository of information linked together from points all over the world. The WWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet.

The World Wide Web (WWW), commonly known as the Web, is an information system where documents and other web resources are identified by Uniform Resource Locators (URLs, such as https://www.example.com/), which may be interlinked by hypertext, and are accessible over the Internet. The resources of the WWW may be accessed by users by a software application called a web browser. The World Wide Web is what most people think of as the Internet. It is all the Web pages, pictures, videos and other online content that can be accessed via a Web browser. The Internet, in contrast, is the underlying network connection that allows us to send email and access the World Wide Web.

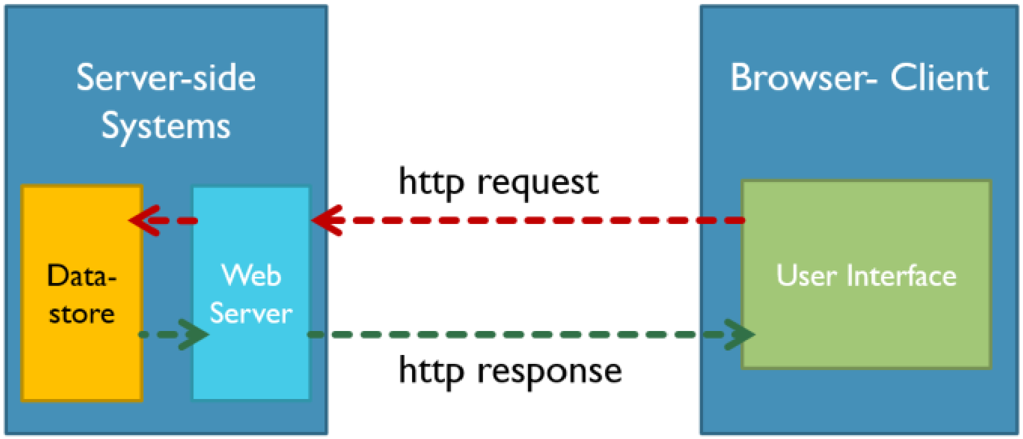
Architecture ofWWW

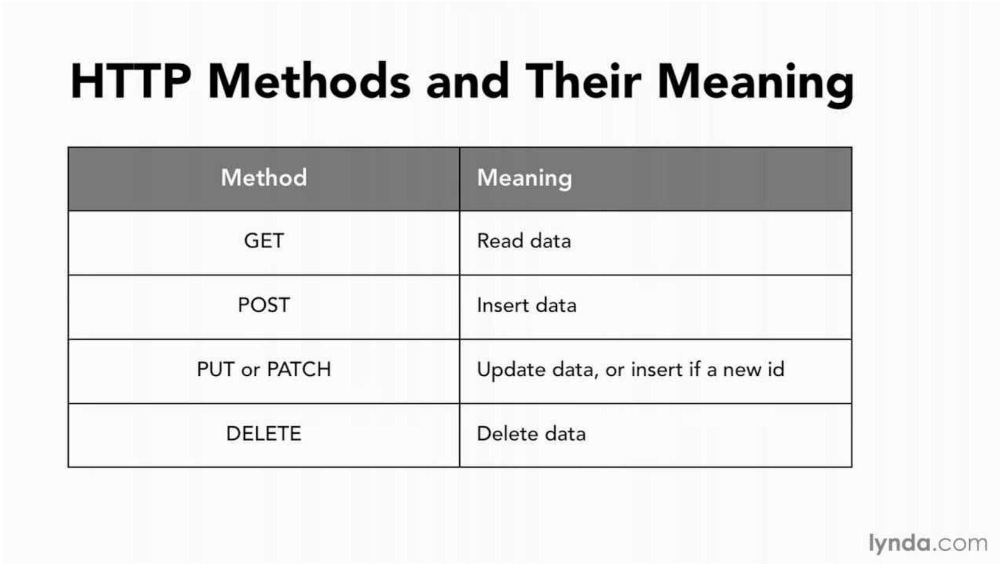


HTTP:

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

An HTTP session is a sequence of network request-response transactions. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a server (typically port 80, occasionally port 8080). An HTTP server listening on that port waits for a client's request message. Upon receiving the request, the server sends back a status and a message of its own. The body of this message is typically the requested resource, although an error message or other information may also be returned. HTTP is also called stateless protocol because the sessions between the HTTP browser and HTTP client are not saved for later reference. The session is information is only valid until the session exists.





HTTP Methods and Their Meaning

Method	Meaning
GET	Read data
POST	Insert data
PUT or PATCH	Update data, or insert if a new id
DELETE	Delete data

lynda.com

HTTPS:

Hypertext Transfer Protocol Secure (HTTPS) is a variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in transit through a secure socket layer (SSL) or transport layer security (TLS) protocol connection.

HTTPS enables encrypted communication and secure connection between a remote user and the primary web server. HTTPS is primarily designed to provide enhanced security layer over the unsecured HTTP protocol for sensitive data and transactions such as billing details, credit card transactions and user login etc. HTTPS encrypts every data packet in transition using SSL or TLS encryption technique to avoid intermediary hackers and attackers to extract the content of the data; even if the connection is compromised.

HTTPS is configured and supported by default in most web browsers and initiates a secure connection automatically if the accessed web server requests secure connection. HTTPS works in collaboration with certificate authorities that evaluates the security certificate of the accessed website.

TELNET:

TELNET is a client/server application program. TELNET is an abbreviation for TErminaL NETwork. It is the standard TCP/IP protocol for virtual terminal service as proposed by the International Organization for Standards (ISO). TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.

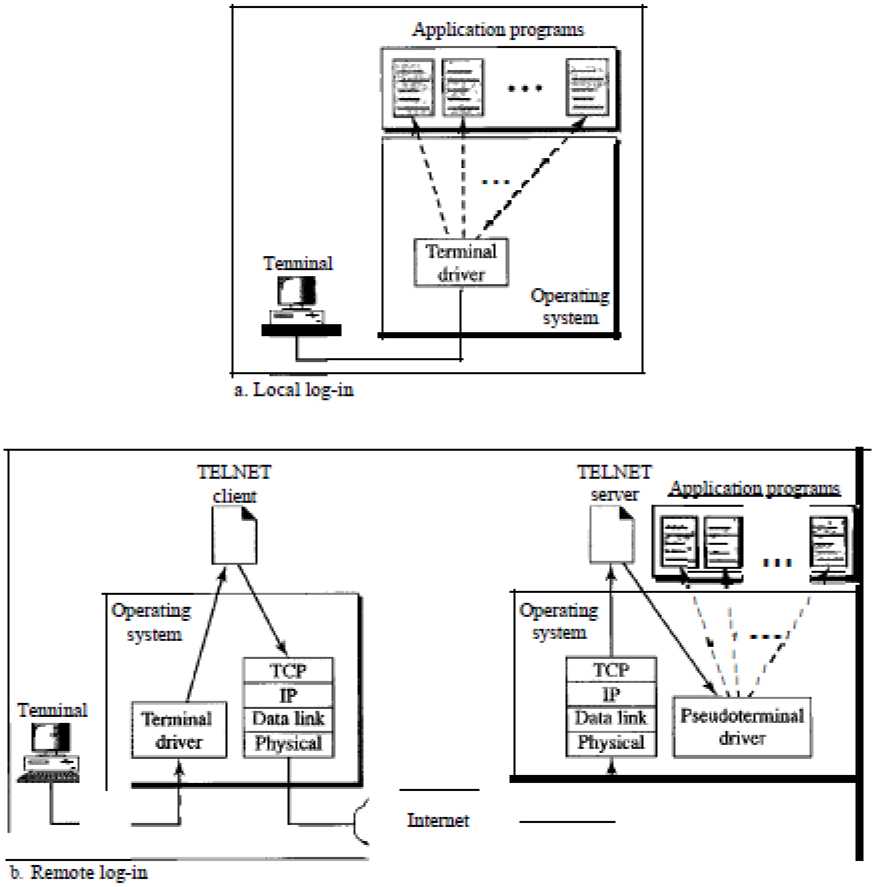
Timesharing Environment

TELNET was designed at a time when most operating systems, such as UNIX, were operating in a timesharing environment. In such an environment, a large computer supports multiple users. The interaction between a user and the computer occurs through a terminal, which is usually a combination of keyboard, monitor, and mouse. Even a microcomputer can simulate a terminal with a terminal emulator.

Logging

In a timesharing environment, users are part of the system with some right to access resources. Each authorized user has an identification and probably a password. The user identification defines the user as part of the system. To access the system, the user logs into the system with a user id or log-in name. The system also includes password checking to prevent an unauthorized user from accessing the resources.

Figure 26.1 *Local and remote log-in*



a. Local log-in

b. Remote log-in

When a user logs into a local timesharing system, it is called local log-in. As a user types at a terminal or at a workstation running a terminal emulator, the keystrokes are accepted by the terminal driver. The terminal driver passes the characters to the operating system. The operating system, in turn, interprets the combination of characters and invokes the desired application program or utility.

When a user wants to access an application program or utility located on a remote machine, he/she performs remote log-in. Here the TELNET client and server programs come into use. The user sends the keystrokes to the terminal driver, where the local operating system accepts the characters but does not interpret them. The characters are sent to the TELNET client, which transforms the characters to a universal character set called network virtual terminal (NVT) characters and delivers them to the local TCP/IP protocol stack.

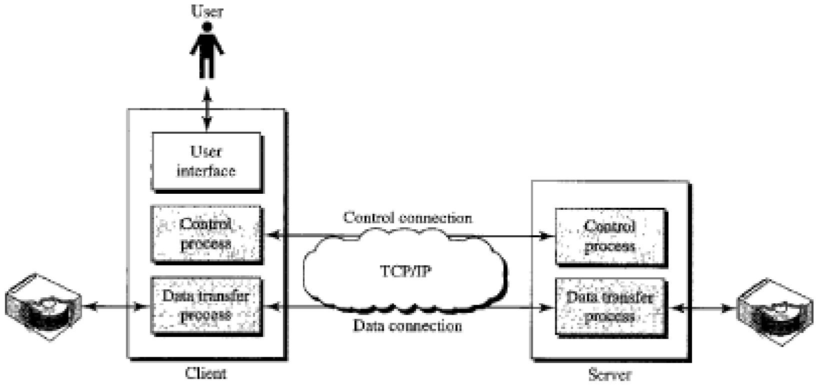
The commands or text, in NVT form, travel through the Internet and arrive at the TCP/IP stack at the remote machine. Here the characters are delivered to the operating system and passed to the TELNET server, which changes the characters to the corresponding characters understandable by the remote computer. However, the characters cannot be passed directly to the operating system because the remote operating system is not designed to receive characters from a TELNET server: It is designed to receive characters from a terminal driver. The solution is to add a piece of software called a pseudoterminal driver which pretends that the characters are coming from a terminal. The operating system then passes the characters to the appropriate application program.

FTP:

File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.

FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for control information (commands and responses) and a data channel for transmitting file content. Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, rename, move and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, also known as anonymous FTP. FTP uses two well-known TCP ports: Port 21 for control connection and Port 20 for the data connection.

Figure 26.21 *FTP*



The control connection remains connected during the entire interactive FTP session. The data connection is opened and then closed for each file transfer. It opens each time commands that involve transferring files are used, and it closes when the file is transferred. In other words, when a user starts an FTP session, the control connection opens. While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred.

SFTP:

SFTP, which stands for SSH File Transfer Protocol, or Secure File Transfer Protocol, is a separate protocol packaged with SSH that works in a similar way but over a secure connection. The advantage is the ability to leverage a secure connection to transfer files and traverse the filesystem on both the local and remote system.

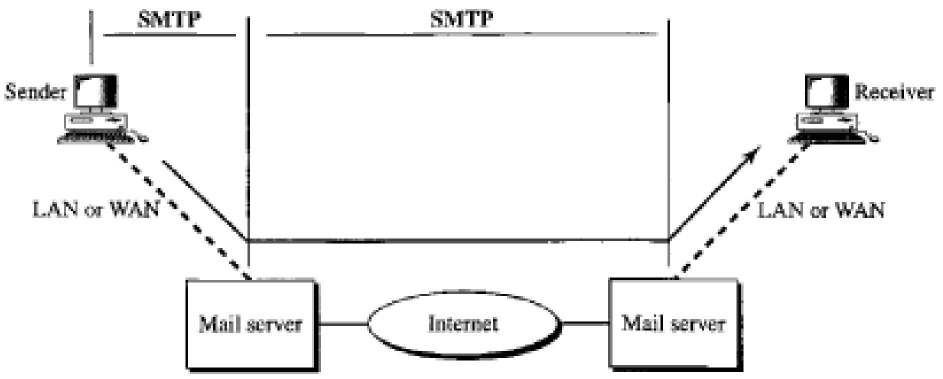
In almost all cases, SFTP is preferable to FTP because of its underlying security features and ability to rely on an SSH connection. FTP is an insecure protocol that should only be used in limited cases or on networks you trust.

SSH or Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH.

Simple Mail Transfer Protocol (SMTP):

It is a standard protocol used for sending e-mail efficiently and reliably over the internet. The SMTP protocol focuses specifically on how the underlying mail delivery system passes messages across an internet from one machine to another. It does not specify how the mail system accepts mail from a user or how the user interface presents the user with incoming mail. Also, SMTP does not specify how mail is stored or how frequently the mail system attempts to send messages.

Figure 26.16 *SMTP range*



Key Points:

- SMTP is application-level protocol.
- SMTP is connection-oriented protocol.
- SMTP is text-based protocol.
- It handles exchange of messages between e-mail servers over TCP/IP network.
- Apart from transferring e-mail, SMTP also provides notification regarding incoming mail.
- When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
- In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.

S.N.	Command Description
1	**HELLO** This command initiates the SMTP conversation.
2	**EHELLO** This is an alternative command to initiate the conversation. ESMTP indicates that the sender server wants to use extended SMTP protocol.
3	**MAIL FROM** This indicates the sender's address.
4	**RCPT TO** It identifies the recipient of the mail. In order to deliver similar message to multiple users this command can be repeated multiple times.
5	**SIZE** This command let the server know the size of attached message in bytes.
6	**DATA** The **DATA** command signifies that a stream of data will follow. Here stream of data refers to the body of the message.
7	**QUIT** This command is used to terminate the SMTP connection.

8	**VERFY** This command is used by the receiving server in order to verify whether the given username is valid or not.
9	**EXPN** It is same as VRFY, except it will list all the users name when it used with a distribution list.

IMAP:

IMAP stands for Internet Message Access Protocol. It is a standard protocol for accessing e-mail from the local server. IMAP is a client/server protocol in which e-mail is received and held by the Internet server. As this requires only a small data transfer, this works well even over a slow connection. Only if we request to read a specific email, message will it be downloaded from the server. We can also create and manipulate folders or mailboxes on the server, delete messages etc.

Version 4 of the Internet Message Access Protocol (IMAP4) is an alternative to POP3 that uses the same general paradigm. Like POP3, IMAP4 defines an abstraction known as a mailbox; mailboxes are located on the same computer as a server. Also, like POP3, a user runs an MAP4 client that contacts the server to retrieve messages. Unlike POP3, however, MAP4 allows a user to dynamically create, delete, or rename mailboxes.

Key Points:

- IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.
- The e-mail is hold and maintained by the remote server.
- It enables us to take any action such as downloading, delete the mail without reading the mail. It enables us to create, manipulate and delete remote message folders called mail boxes.
- IMAP enables the users to search the e-mails.
- It allows concurrent access to multiple mailboxes on multiple mail servers.

POP:

POP stands for Post Office Protocol. It is generally used to support a single client. There are several versions of POP but the POP 3 is the current standard.

The most popular protocol used to transfer e-mail messages from a permanent mailbox to a local computer is known as version 3 of the Post Ofice Protocol (POP3). The user invokes a POP3 client, which creates a TCP connection to a POP3 server on the mailbox computer. The user first sends a login and a password to authenticate the session. Once authentication has been accepted, the user client sends commands to retrieve a copy of one or more messages and to delete the message from the permanent mailbox.

Key Points

- POP is an application layer internet standard protocol.

- Since POP supports offline access to the messages, thus requires less internet usage time.
- POP does not allow search facility.
- In order to access the messages, it is necessary to download them.
- It allows only one mailbox to be created on server.
- It is not suitable for accessing non-mail data.

Network Traffic Analysis:

Network traffic analysis (NTA) is the process of intercepting, recording and analyzing network traffic communication patterns in order to detect and respond to security threats. In other words, Network traffic analysis is the process of recording, reviewing and analyzing network traffic for the purpose of performance, security and/or general network operations and management.

Network traffic analysis is primarily done to get in-depth insight into what type of traffic/network packets or data is flowing through a network. Typically, network traffic analysis is done through a network monitoring or network bandwidth monitoring software/application. The traffic statistics from network traffic analysis helps in:

- Understanding and evaluating the network utilization
- Download/upload speeds
- Type, size, origin and destination and content/data of packets

Network security staff uses network traffic analysis to identify any malicious or suspicious packets within the traffic. Similarly, network administrations seek to monitor download/upload speeds, throughput, content, etc. to understand network operations.

Network traffic analysis is also used by attackers/intruders to analyze network traffic patterns and identify any vulnerabilities or means to break in or retrieve sensitive data.

Simple Network Management Protocol (SNMP):

We can define network management as monitoring, testing, configuring, and troubleshooting network components to meet a set of requirements defined by an organization. These requirements include the smooth, efficient operation of the network that provides the predefined quality of service for users.

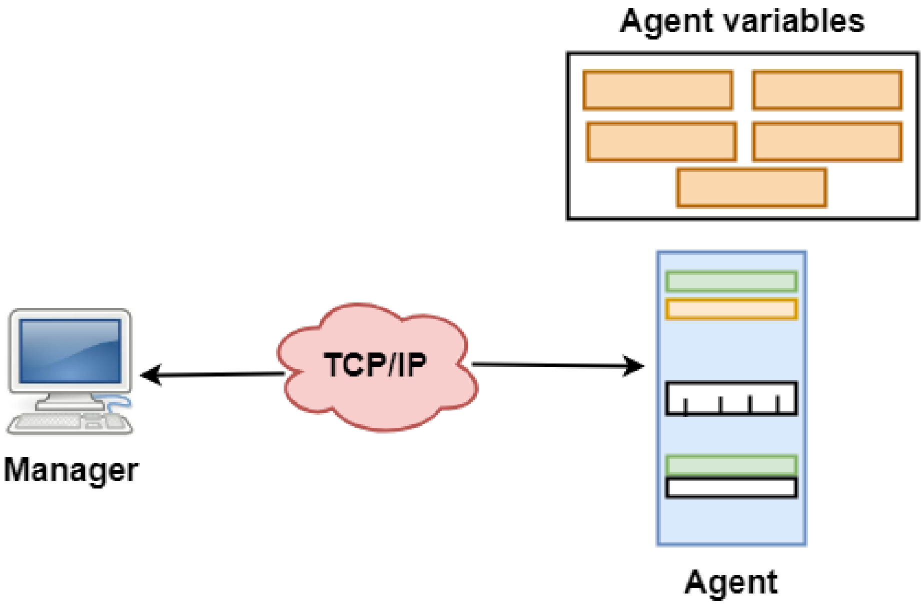
Network Management Functions:

- **Performance management** deals with monitoring and managing the various parameters that measure the performance of the network. Performance management is an essential function that enables a service provider to provide quality-of-service guarantees to their clients and to ensure that clients comply with the requirements imposed by the service provider.
- **Fault management** is the function responsible for detecting failures when they happen and isolating the failed component. The network also needs to restore traffic that may be disrupted due to the failure, but this is usually considered a separate function.
- **Configuration management** deals with the set of functions associated with managing orderly changes in a network. The basic function of managing the equipment in the network, connection management, network adaptation belongs to this category.

- **Security management** includes administrative functions such as authenticating users and setting attributes such as read and write permissions on a per-user basis

Simple Network Management Protocol (SNMP) is the application layer protocol that is used to perform the above-mentioned network management functions.

SNMP uses the concept of manager and agent. That is, a manager, usually a host, controls and monitors a set of agents, usually routers. A few manager stations control a set of agents. The protocol is designed at the application level so that it can monitor devices made by different manufacturers and installed on different physical networks.



Managers and Agents:

- A manager is a host that runs the SNMP client program while the agent is a router that runs the SNMP server program.
- Management of the internet is achieved through simple interaction between a manager and agent.
- The agent is used to keep the information in a database while the manager is used to access the values in the database. For example, a router can store the appropriate variables such as a number of packets received and forwarded while the manager can compare these variables to determine whether the router is congested or not.
- Agents can also contribute to the management process. A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manage.

Multi Router Traffic Grapher (MRTG):

The Multi Router Traffic Grapher (MRTG) is free software for monitoring and measuring the traffic load on network links. It allows the user to see traffic load on a network over time in graphical form.

MRTG is being used to graph all sorts of network devices as well as everything else from weather data to vending machines. MRTG is written in PERL and works on Unix/Linux as well as Windows systems. MRTG is free licensed software/tool being used by network administrators. It supports SNMP to collecting data to visually graph points and charts within the interface via their routines and algorithms that are programmed in C.

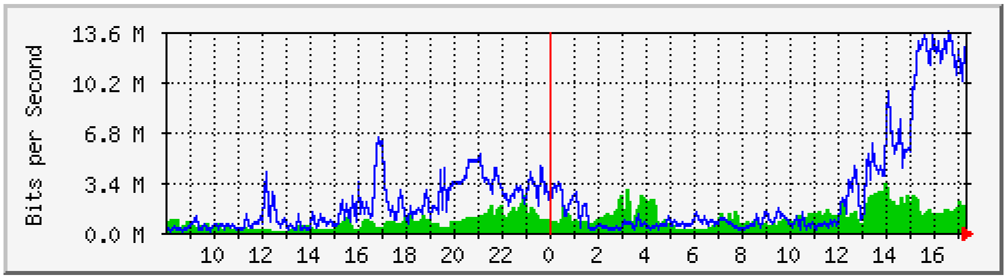


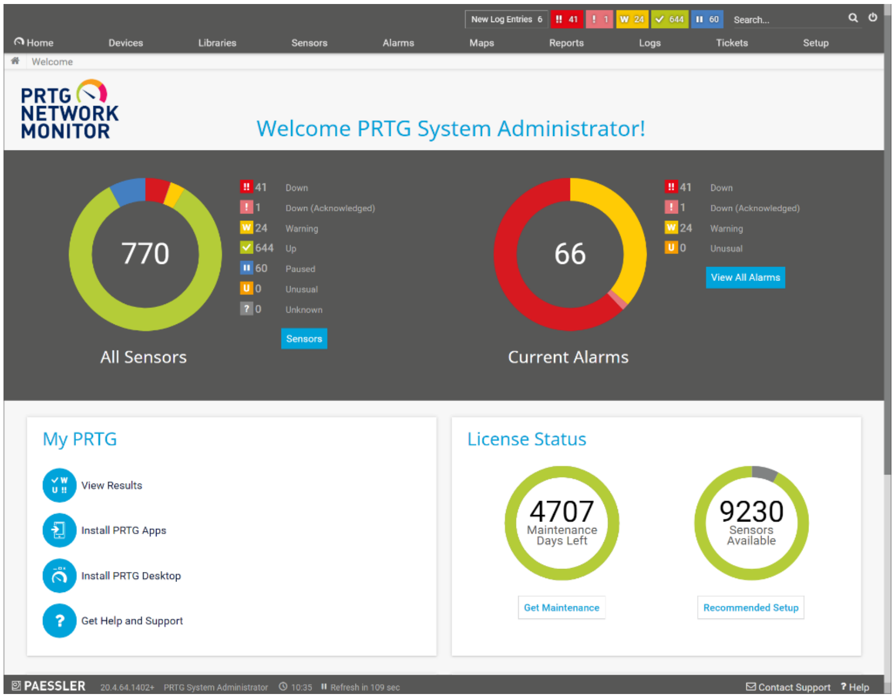
Fig: A sample MRTG bandwidth graph

Paessler Router Traffic Grapher (PRTG):

PRTG Network Monitor (Paessler Router Traffic Grapher) is a network monitoring software. It can monitor and classify system conditions like bandwidth usage or uptime and collect statistics from miscellaneous hosts as switches, routers, servers and other devices and applications. It is a paid network monitoring tool that provides strong network monitoring features for enterprises.

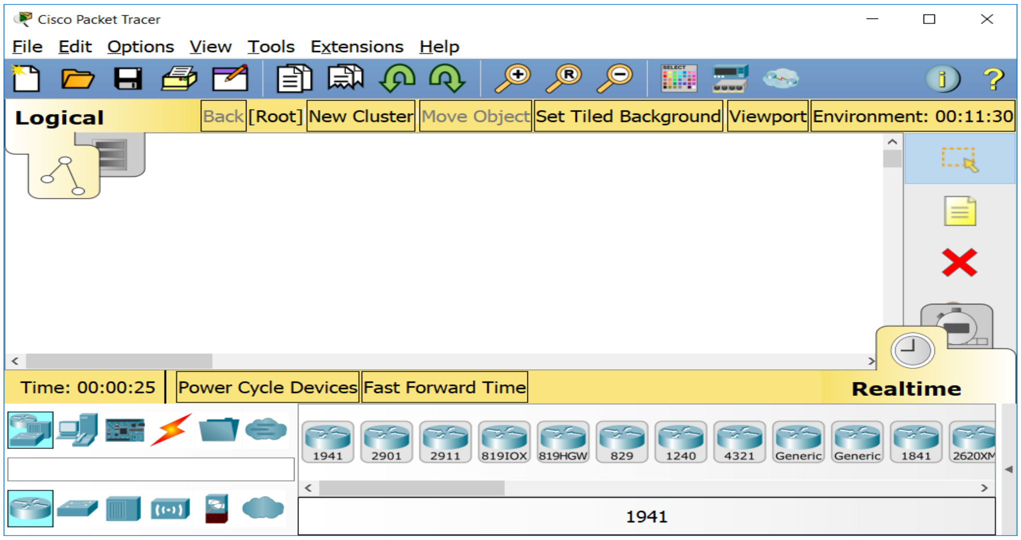
PRTG Network Monitor has an auto-discovery mode that scans predefined areas of an enterprise network and creates a device list from this data. PRTG offers a full array of features that can be summed up as comprehensive, some of which include:

- Monitor Server Uptime/Downtime
- Network Devices (Switches, Firewalls, Routers, Wifi, etc) Monitoring features
- Virtual Servers and Machine Monitoring
- Email Server & Backup monitoring
- Automatic Network Discovery and Inventory
- Bandwidth and Traffic Analysis including sorting by Source/Destination and Content
- QOS & VOIP Monitoring
- Hardware (CPU Loads, HDD Disk Space, Memory, etc) Monitoring
- Temperature & Humidity Monitoring with paired with the Right Sensors/Equipment
- Cloud (AWS, Azure, etc) Monitoring
- DB Performance Monitoring
- Easy to Use Web Interface
- SSL Encryption for Accessing Dashboard
- Extension Alerting Options including SMS Text Messages, Push Notifications, Email, Syslog, SNMP traps, HTTP requests, Execute Scripts or Programs, etc.
- Create Reports based on Schedules



Packet Tracer:

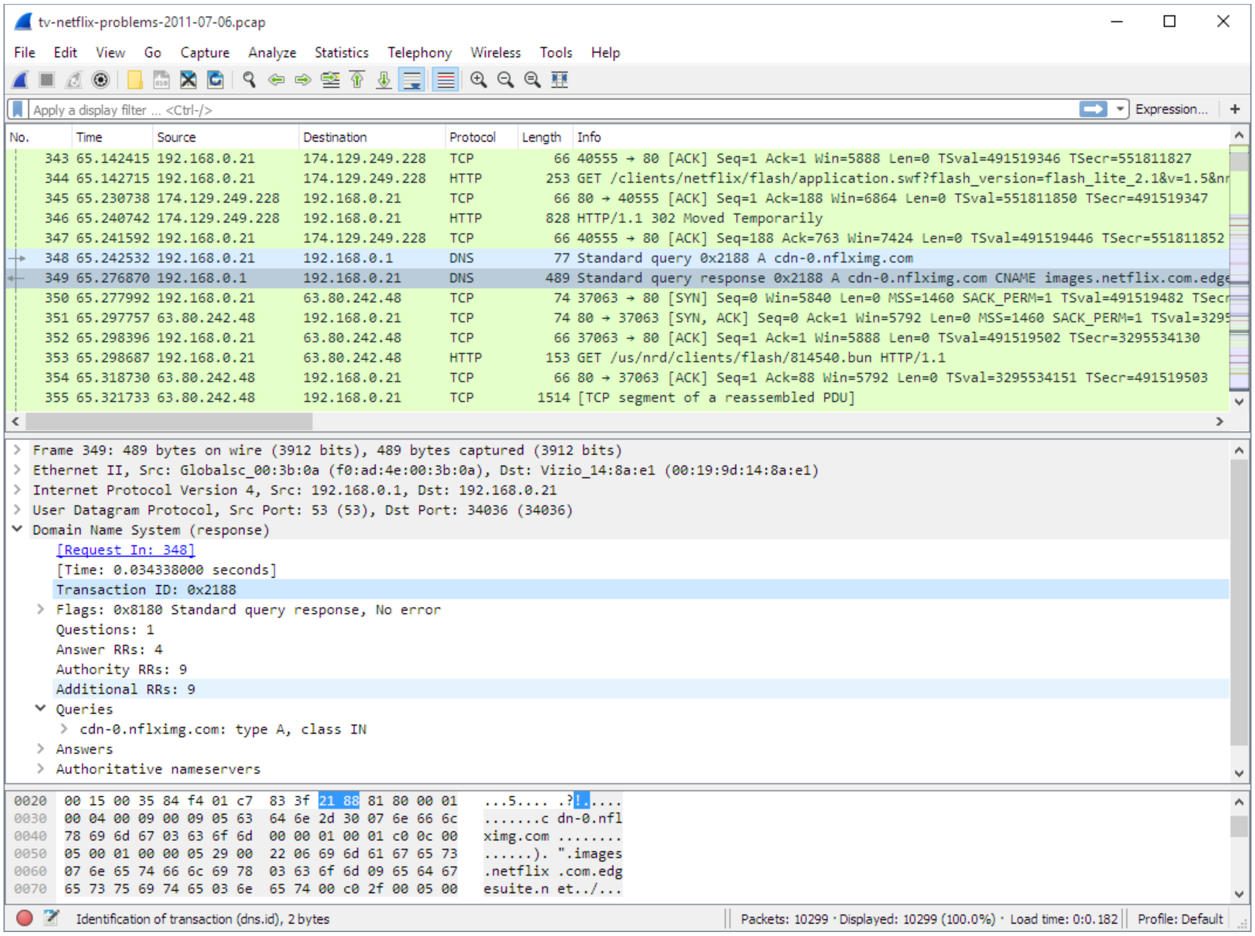
Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.



Wireshark:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

It captures network traffic on the local network and stores that data for offline analysis. Wireshark captures network traffic from Ethernet, Bluetooth, Wireless (IEEE. 802.11), Token Ring, Frame Relay connections, and more.


tv-netflix-problems-2011-07-06.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time      Source          Destination     Protocol  Length Info
  343 65.142415 192.168.0.21    174.129.249.228 TCP         66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
  344 65.142715 192.168.0.21    174.129.249.228 HTTP       253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
  345 65.230738 174.129.249.228 192.168.0.21    TCP         66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
  346 65.240742 174.129.249.228 192.168.0.21    HTTP       828 HTTP/1.1 302 Moved Temporarily
  347 65.241592 192.168.0.21    174.129.249.228 TCP         66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
  348 65.242532 192.168.0.21    192.168.0.1     DNS         77 Standard query 0x2188 A cdn-0.nflximg.com
  349 65.276870 192.168.0.1     192.168.0.21    DNS        489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
  350 65.277992 192.168.0.21    63.80.242.48    TCP         74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
  351 65.297757 63.80.242.48    192.168.0.21    TCP         74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
  352 65.298396 192.168.0.21    63.80.242.48    TCP         66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
  353 65.298687 192.168.0.21    63.80.242.48    HTTP       153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
  354 65.318730 63.80.242.48    192.168.0.21    TCP         66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
  355 65.321733 63.80.242.48    192.168.0.21    TCP       1514 [TCP segment of a reassembled PDU]
```

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Identification of transaction (dns.id), 2 bytes | Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default