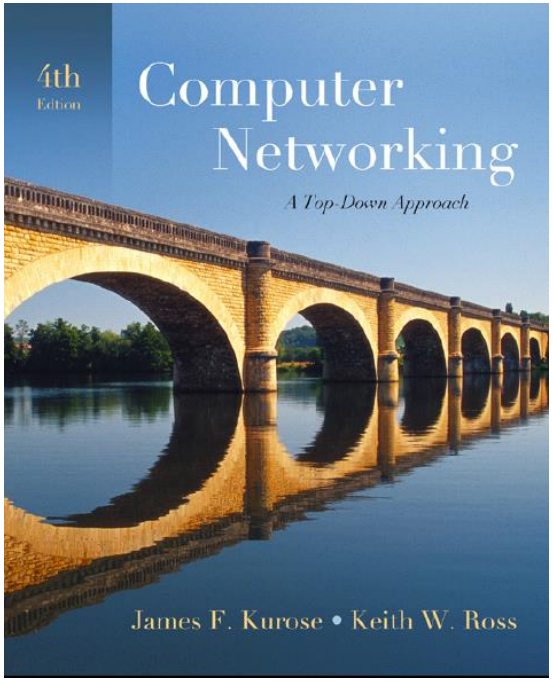
Chapter 6
Application Layer



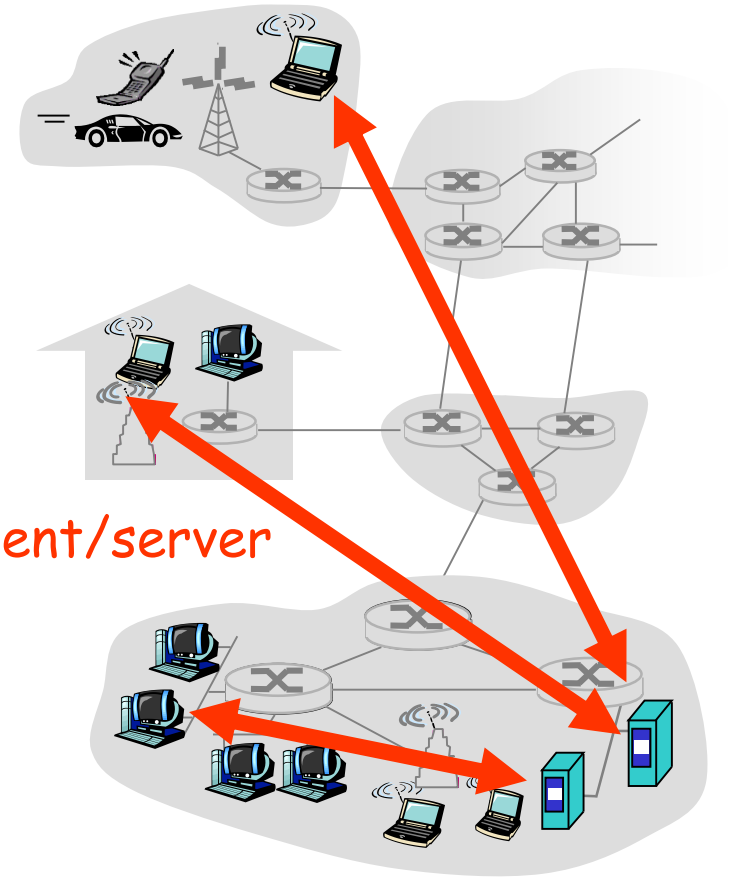
Functions of the application layer

- Transferring and accessing files
- Sending emails and engaging in other communication types
- Facilitating remote hosting
- Accessing networks and directories
- File Transfer, Access, and Management (FTAM)
- Mail Services
- Determining resource availability

Application architectures

- Client-server
- Peer-to-peer (P2P)
- Hybrid of client-server and P2P

Client-server architecture



server:

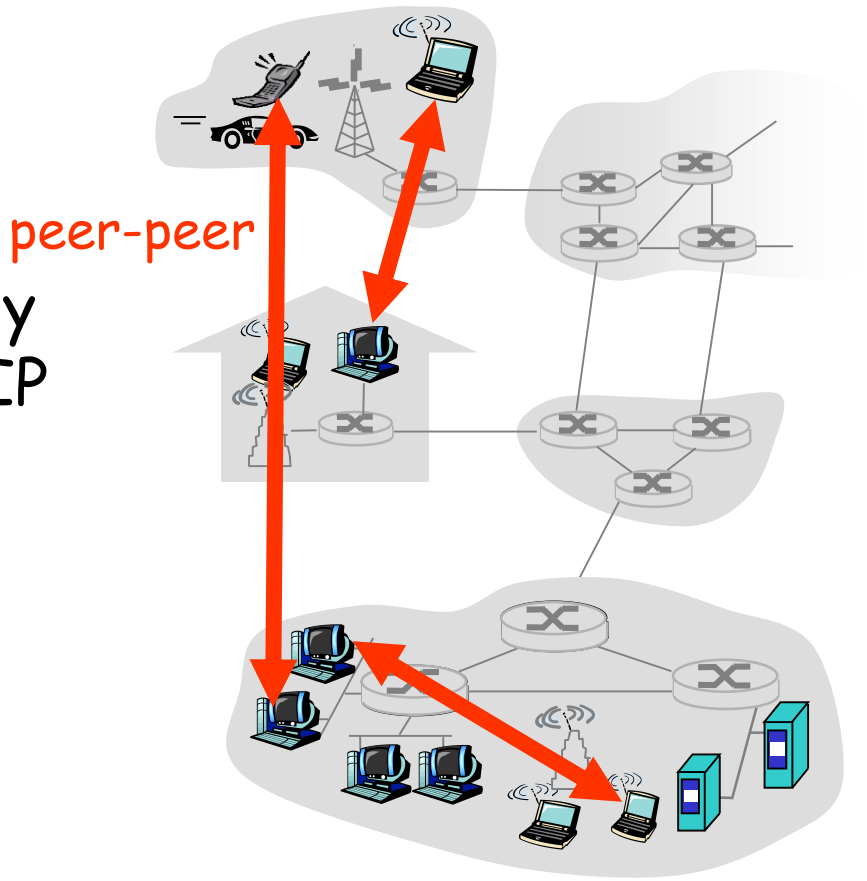
- always-on host
- permanent IP address
- server farms for scaling

clients:

- communicate with server
- may be intermittently connected
- may have dynamic IP addresses
- do not communicate directly with each other

Pure P2P architecture

- *no* always-on server
- arbitrary end systems directly communicate
- peers are intermittently connected and change IP addresses



Highly scalable but difficult to manage

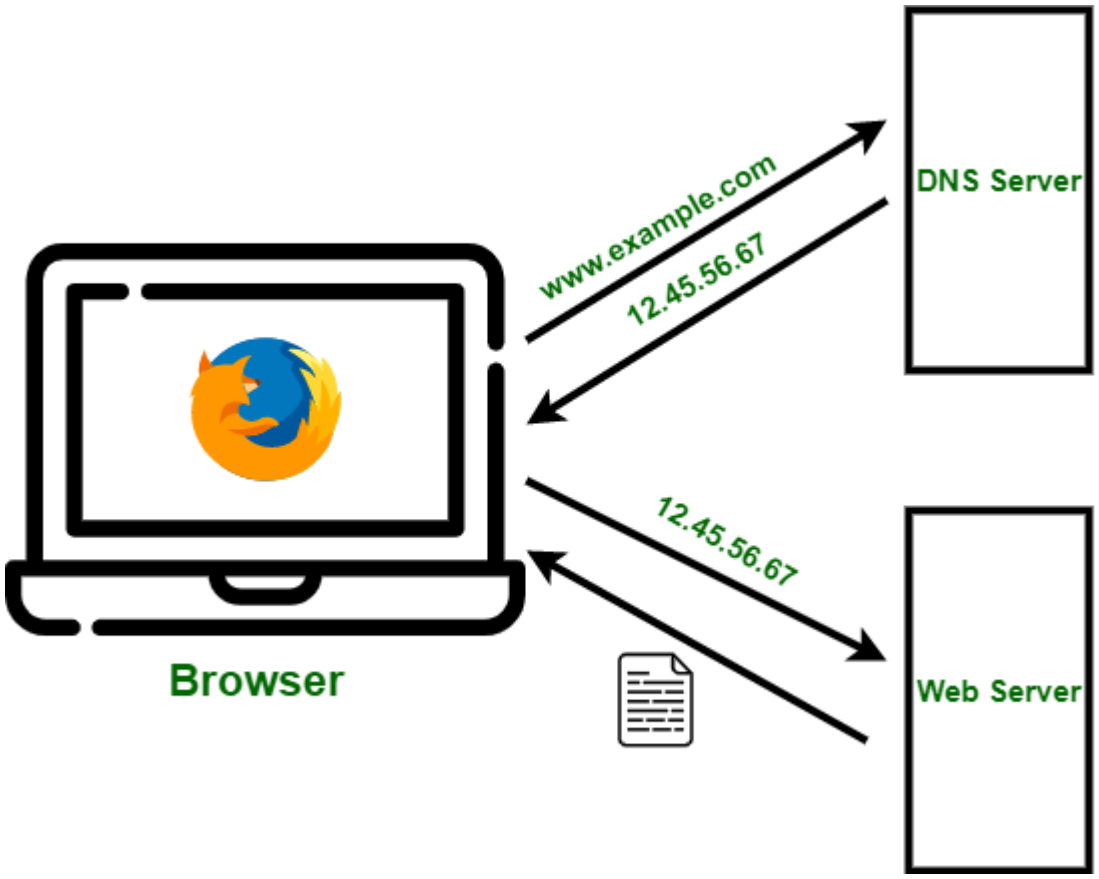
Hybrid of client-server and P2P

Skype

- voice-over-IP P2P application
- centralized server: finding address of remote party:
- client-client connection: direct (not through server)

Instant messaging

- chatting between two users is P2P
- centralized service: client presence detection/location
  - user registers its IP address with central server when it comes online
  - user contacts central server to find IP addresses of buddies


DNS Server
www.example.com
12.45.56.67
12.45.56.67
Web Server
Browser

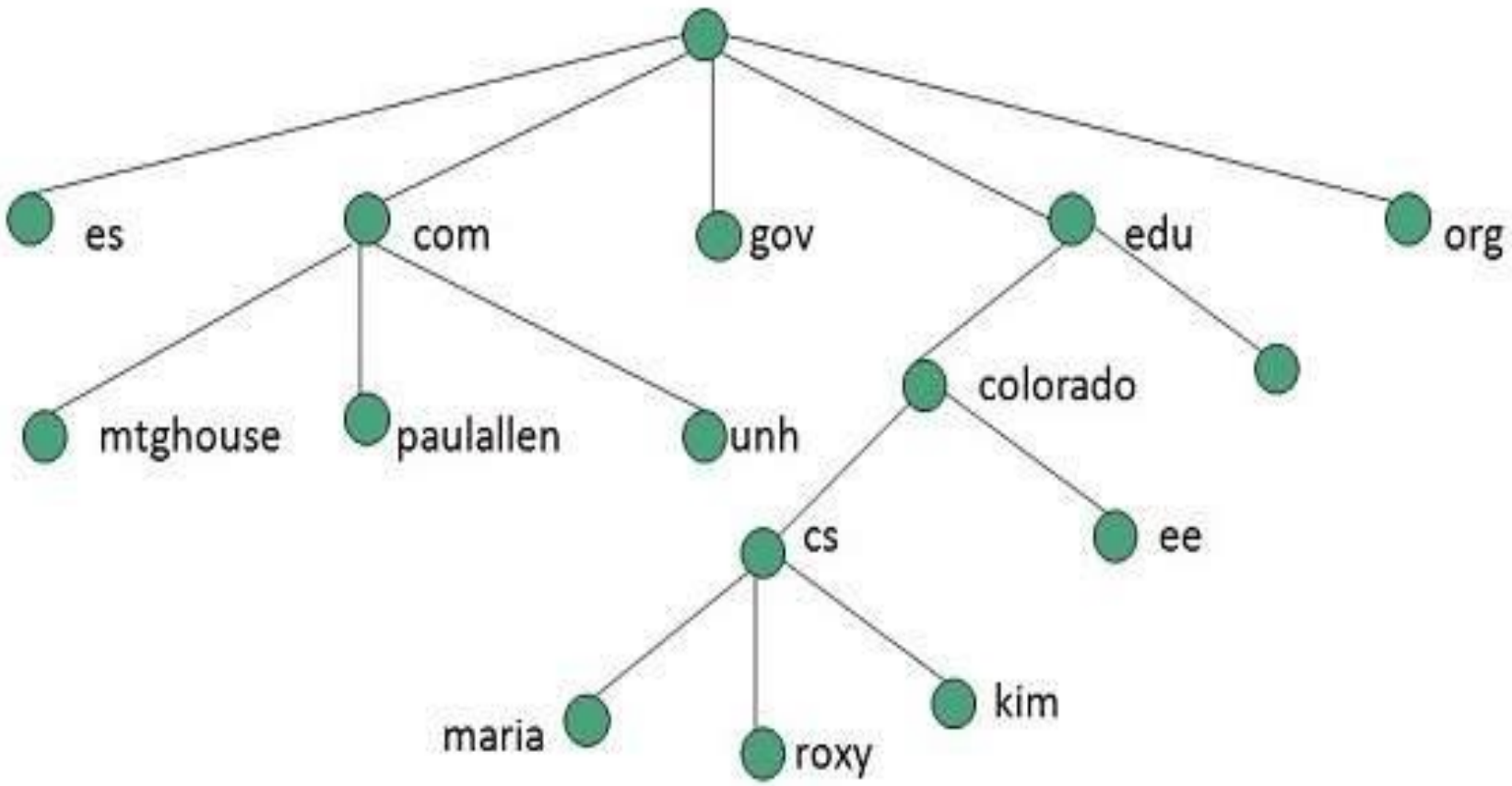
What is DNS?

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

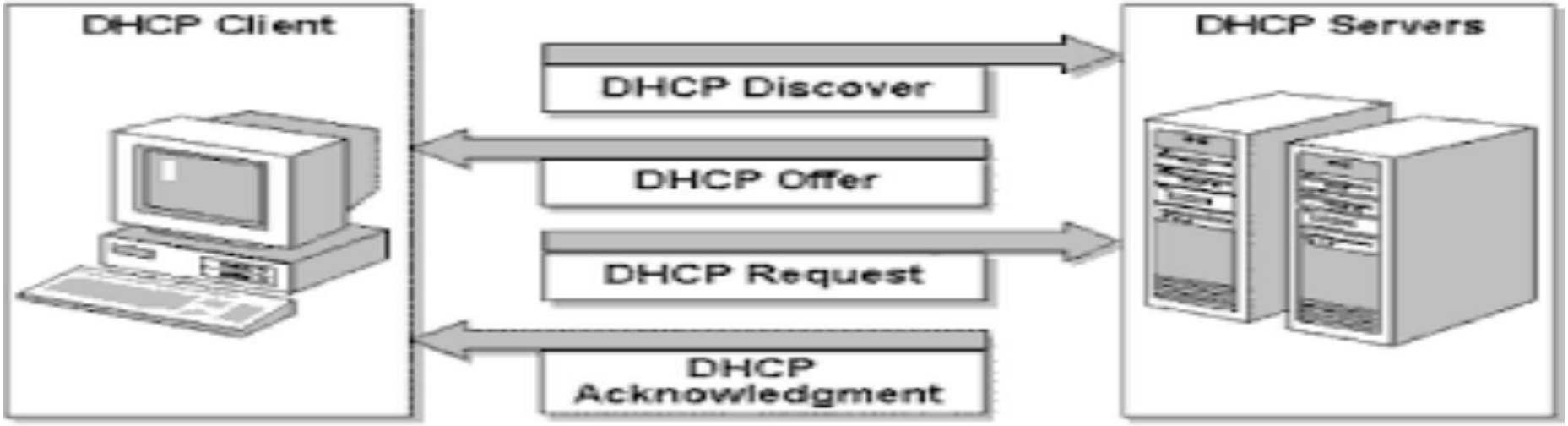
How does DNS work?

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.


es
com
gov
edu
org
mtghouse
paulallen
unh
colorado
cs
ee
maria
roxy
kim

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

How DHCP Works



WWW stands for **World Wide Web.** A technical definition of the World Wide Web is : all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP).

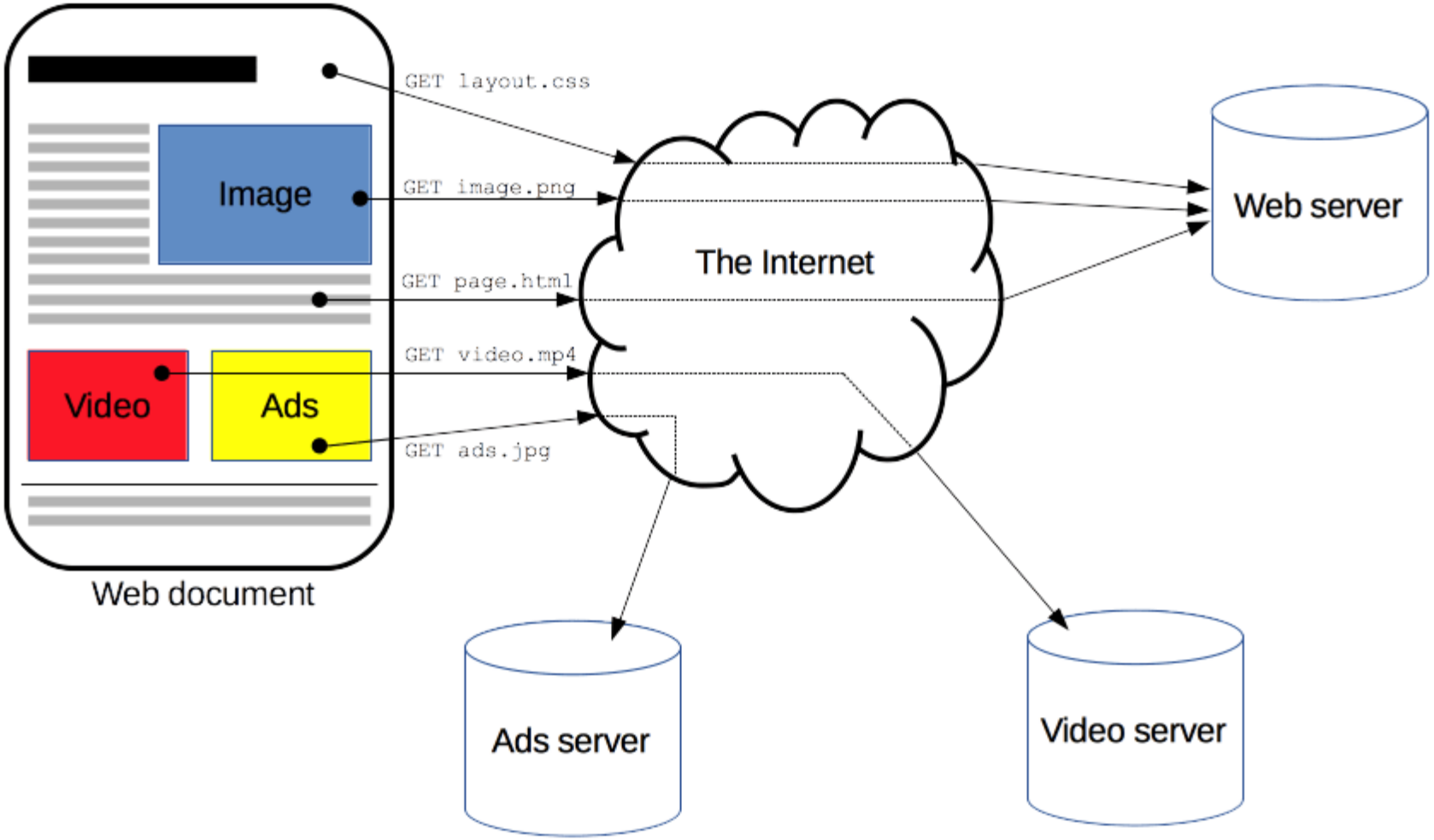
The World Wide Web is the universe of network-accessible information, an embodiment of human knowledge.

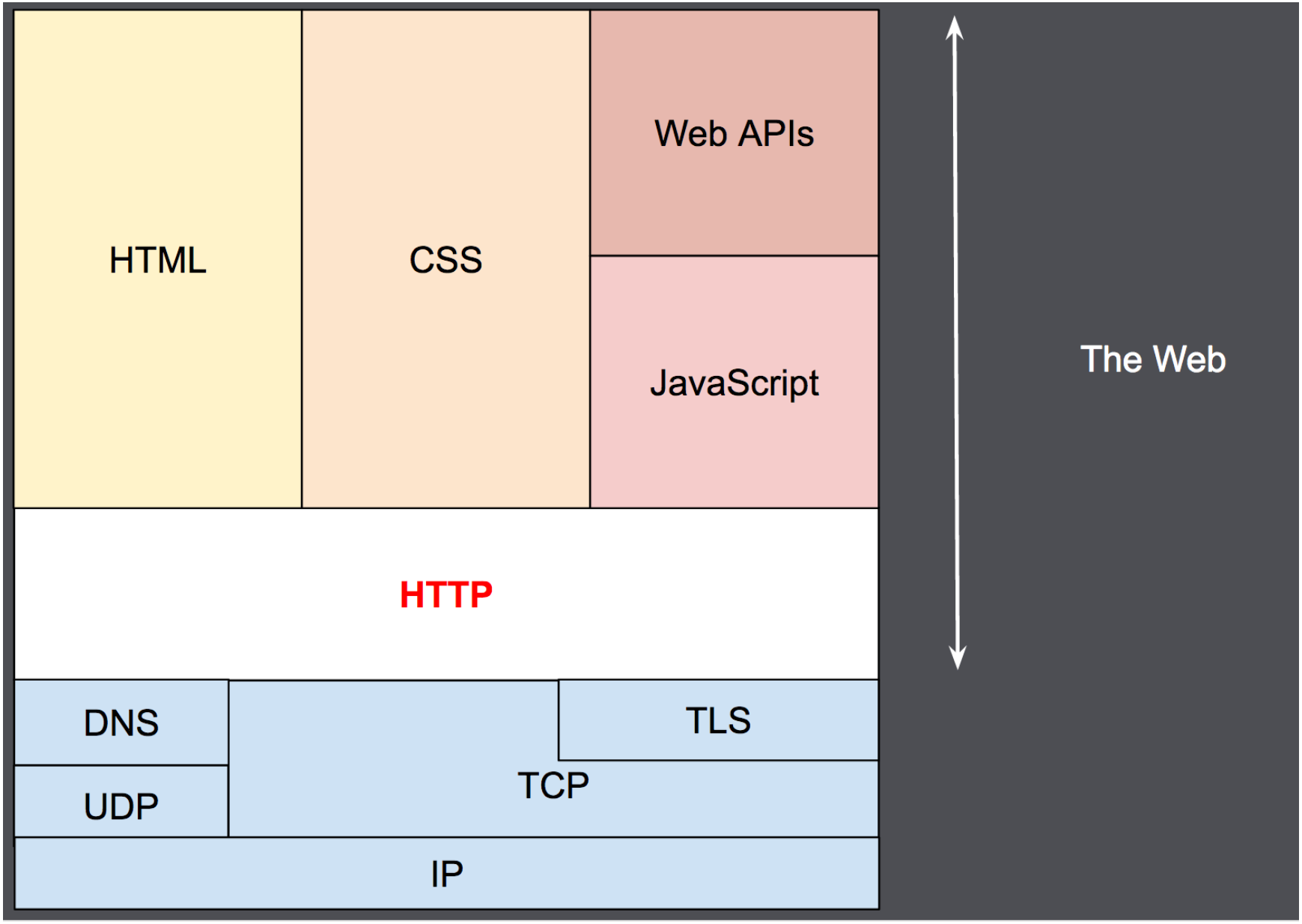
In simple terms, The World Wide Web is a way of exchanging information between computers on the Internet, tying them together into a vast collection of interactive multimedia resources.

What is HTTP protocol?

Hypertext Transfer Protocol (HTTP) is **an application-layer protocol for transmitting hypermedia documents, such as HTML**. It was designed for communication between web browsers and web servers, but it can also be used for other purposes.

HTTP is a protocol for fetching resources such as HTML documents. It is the foundation of any data exchange on the Web and it is a client-server protocol, which means requests are initiated by the recipient, usually the Web browser. A complete document is reconstructed from the different sub-documents fetched, for instance, text, layout description, images, videos, scripts, and more.


GET layout.css
Image
GET image.png
GET page.html
GET video.mp4
Video
Ads
GET ads.jpg
Web document
The Internet
Web server
Ads server
Video server

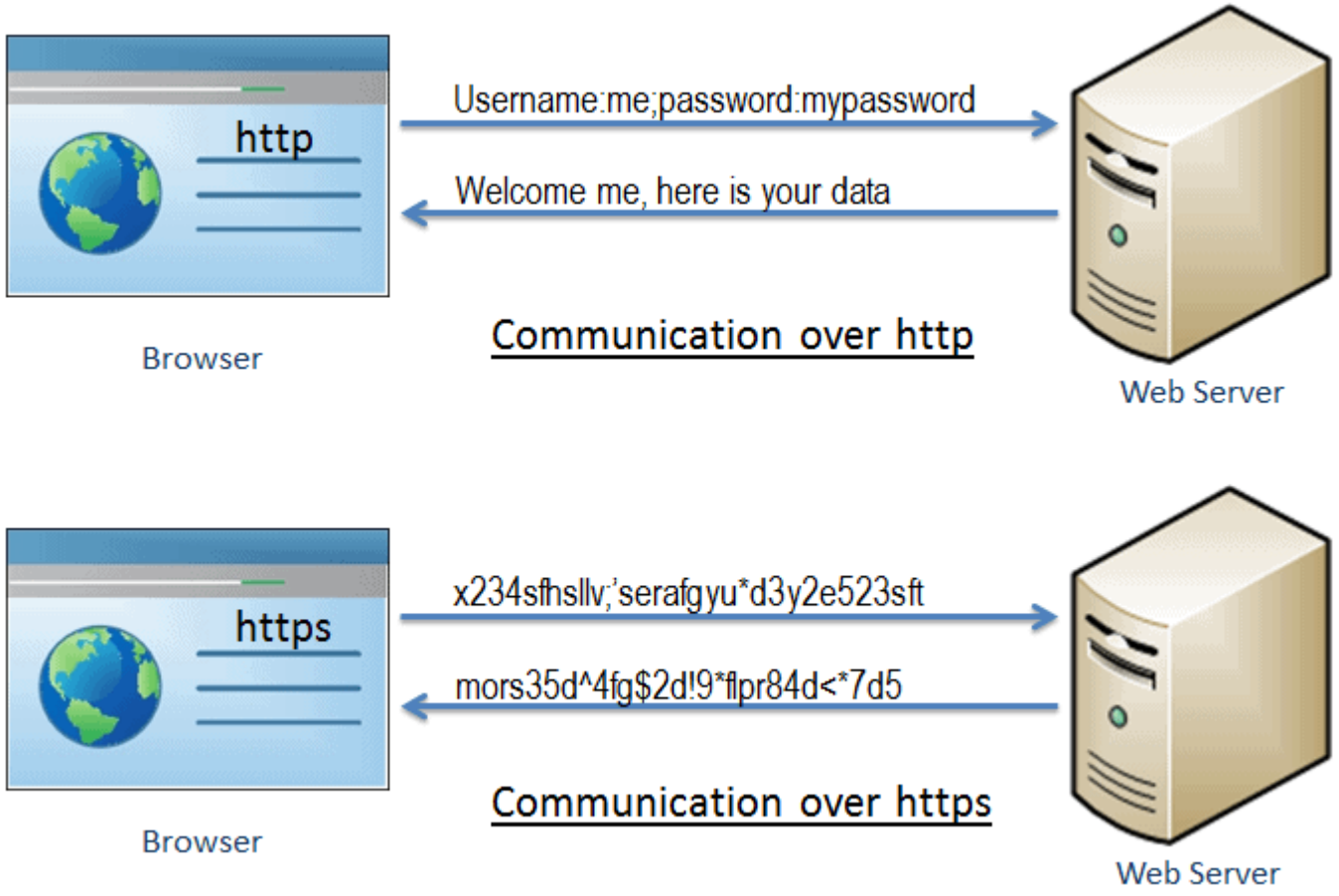

HTML
CSS
Web APIs
JavaScript
The Web
HTTP
DNS
TLS
UDP
TCP
IP

Hypertext Transfer Protocol Secure (HTTPS)

Hypertext Transfer Protocol Secure (HTTPS) is a protocol that secures communication and data transfer between a user's web browser and a website. HTTPS is the secure version of HTTP.

The protocol protects users against eavesdroppers and man-in-the-middle attacks. It also protects legitimate domains from domain name system (DNS) spoofing attacks.

HTTPS plays a significant role in securing websites that handle or transfer sensitive data, including data handled by online banking services, email providers, online retailers, healthcare providers and more. Simply put, any website that requires login credentials or involves financial transactions should use HTTPS to ensure the security of users, transactions and data.


http
Username:me;password:mypassword
Welcome me, here is your data
Communication over http
Browser
Web Server
https
x234sfhsllv;'serafgyu*d3y2e523sft
mors35d^4fg$2d!9*flpr84d<*7d5
Communication over https
Browser
Web Server

Web and HTTP

First some jargon

- Web page consists of objects
- Object can be HTML file, JPEG image, Java applet, audio file,…
- Web page consists of base HTML-file which includes several referenced objects
- Each object is addressable by a URL
- Example URL:

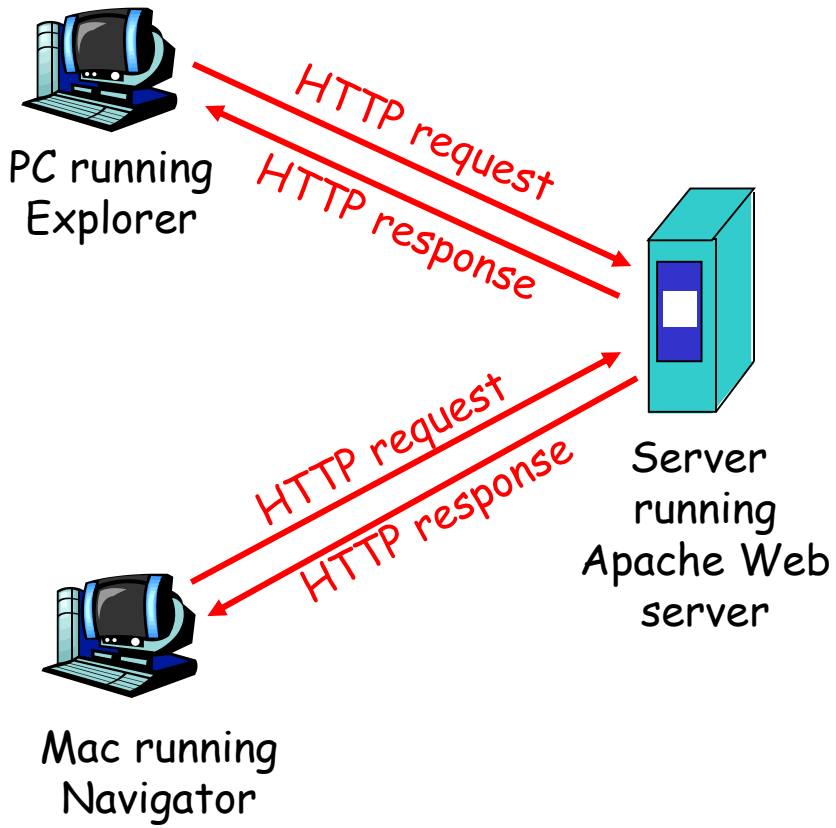
`www.someschool.edu/someDept/pic.gif`

host name | path name

HTTP overview

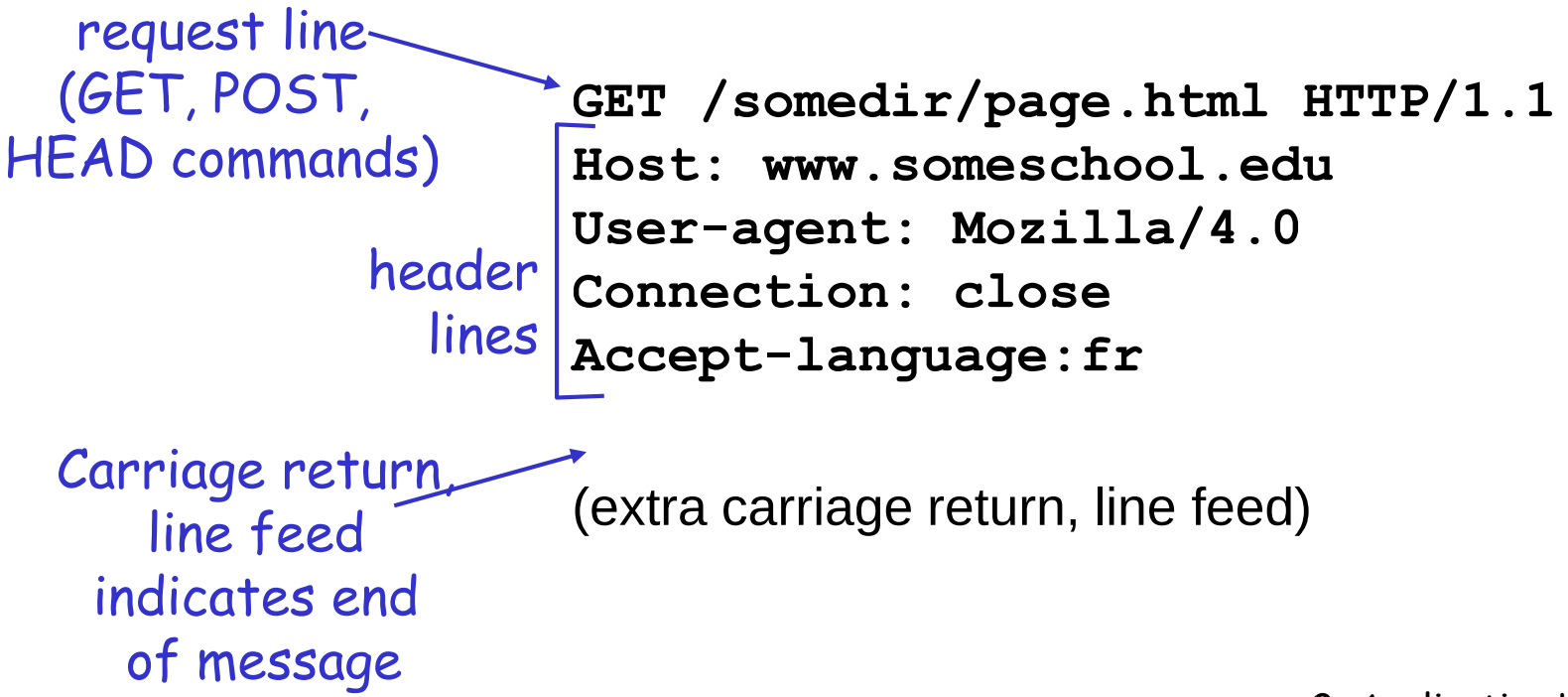
HTTP: hypertext transfer protocol

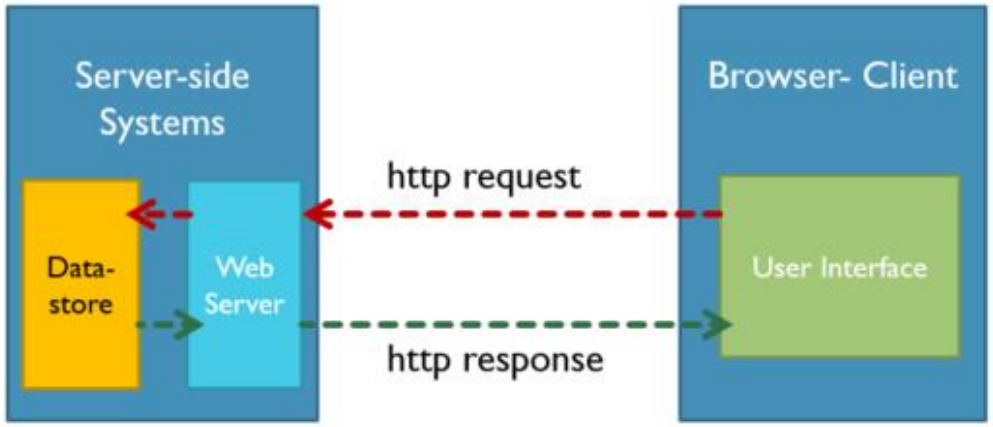
- Web's application layer protocol
- client/server model
  - *client:* browser that requests, receives, "displays" Web objects
  - *server:* Web server sends objects in response to requests



HTTP request message

- two types of HTTP messages: *request, response*
- HTTP request message:
  - ASCII (human-readable format)





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

Method types

HTTP/1.0

- GET
- POST
- HEAD
  - asks server to leave requested object out of response

HTTP/1.1

- GET, POST, HEAD
- PUT
  - uploads file in entity body to path specified in URL field
- DELETE
  - deletes file specified in the URL field

HTTP response status codes

In first line in server->client response message.

A few sample codes:

200 OK

- request succeeded, requested object later in this message

301 Moved Permanently

- requested object moved, new location specified later in this message (Location:)

400 Bad Request

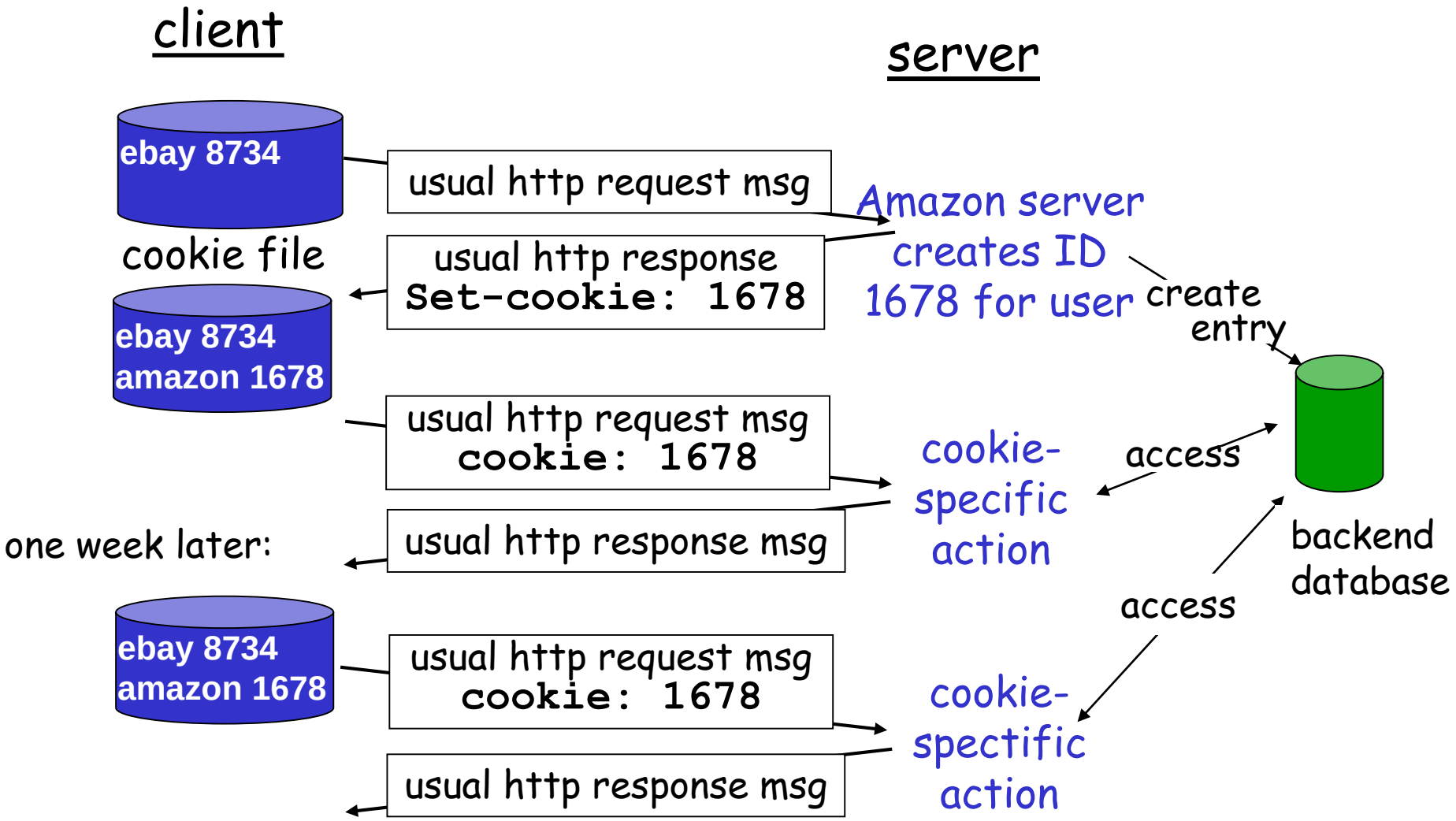
- request message not understood by server

404 Not Found

- requested document not found on this server

505 HTTP Version Not Supported

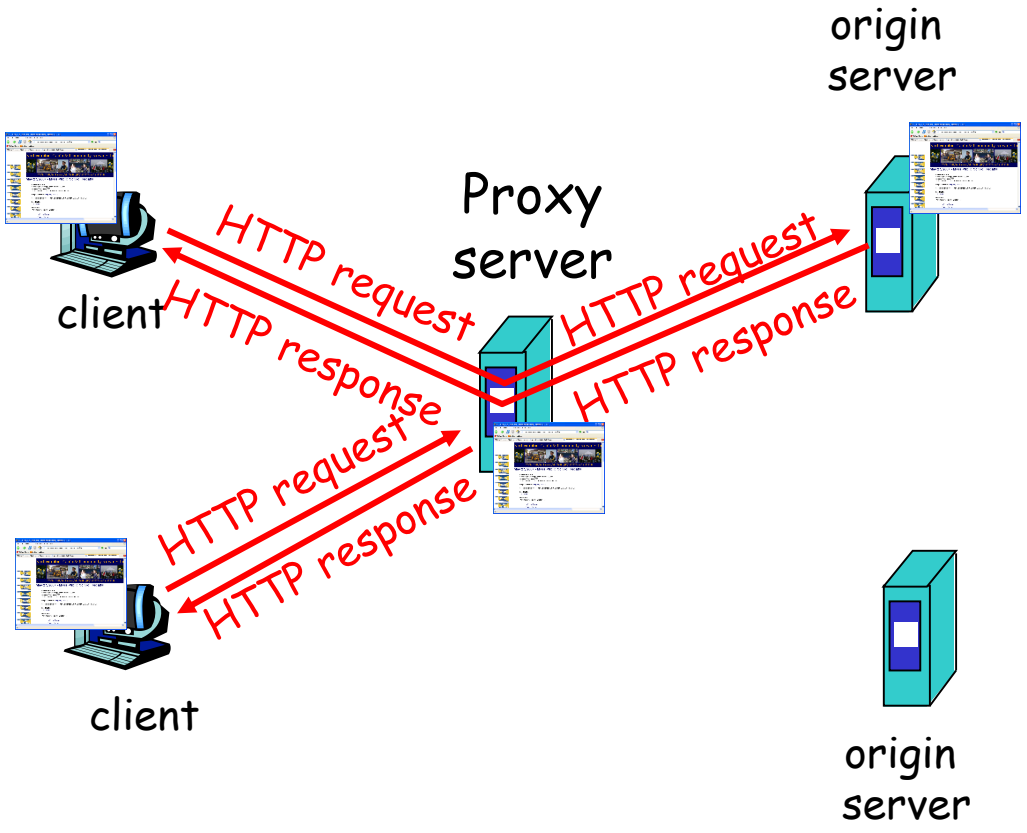
Cookies: keeping "state" (cont.)



Web caches (proxy server)

Goal: satisfy client request without involving origin server

- user sets browser: Web accesses via cache
- browser sends all HTTP requests to cache
  - object in cache: cache returns object
  - else cache requests object from origin server, then returns object to client



TELNET stands for **Tel**etype **Net**work. It is a type of protocol that enables one computer to connect to local computer. It is a used as a standard **TCP/IP protocol** for virtual terminal service which is given by **ISO**. Computer which starts connection known as the **local computer**. Computer which is being connected to i.e. which accepts the connection known as **remote computer**. When the connection is established between local and remote computer. During telnet operation whatever that is being performed on the remote computer will be displayed by local computer. Telnet operates on client/server principle. Local computer uses telnet client program and the remote computers uses telnet server program.

FTP

•FTP stands for File transfer protocol.

•FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.

•It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.

•It is also used for downloading the files to computer from other servers.

Objectives of FTP

•It provides the sharing of files.

•It is used to encourage the use of remote computers.

•It transfers the data more reliably and efficiently.

SMTP

•SMTP stands for Simple Mail Transfer Protocol.

•SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called **Simple Mail Transfer Protocol**.

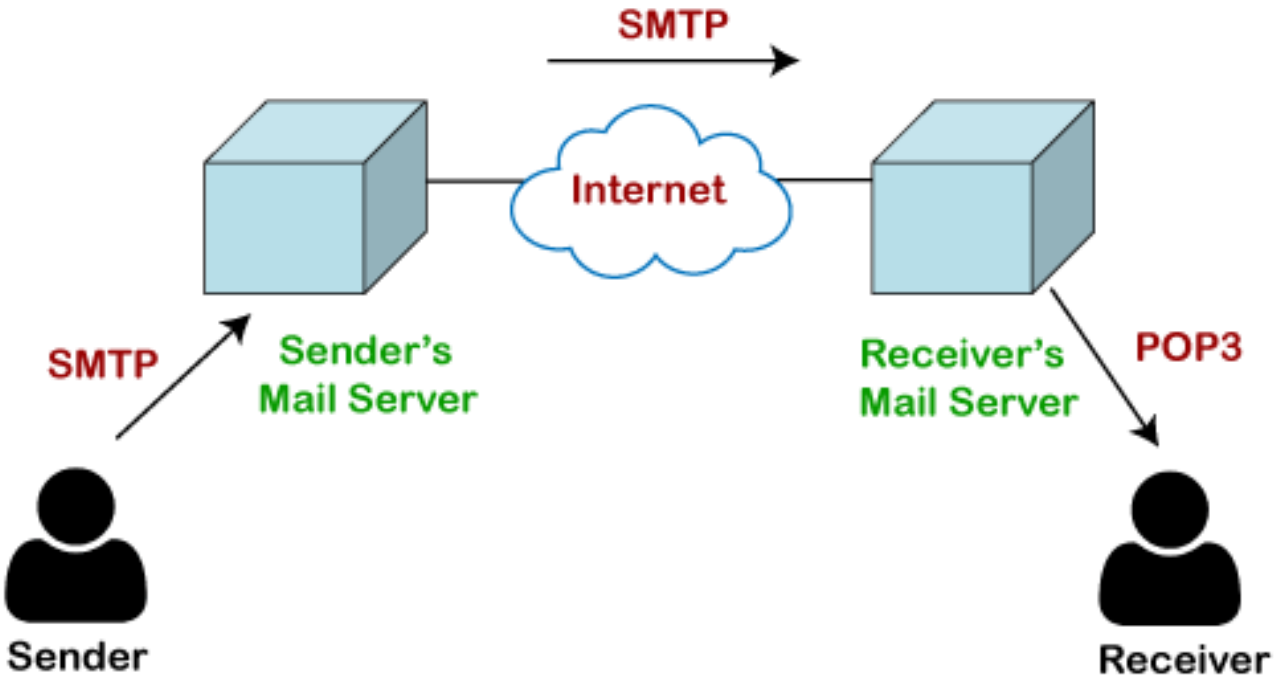
•It is a program used for sending messages to other computer users based on e-mail addresses.

•It provides a mail exchange between users on the same or different computers, and it also supports:

- It can send a single message to one or more recipients.
- Sending message can include text, voice, video or graphics.

- It can also send the messages on networks outside the internet.

•The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.


SMTP
Internet
SMTP
Sender's
Mail Server
Receiver's
Mail Server
POP3
Sender
Receiver

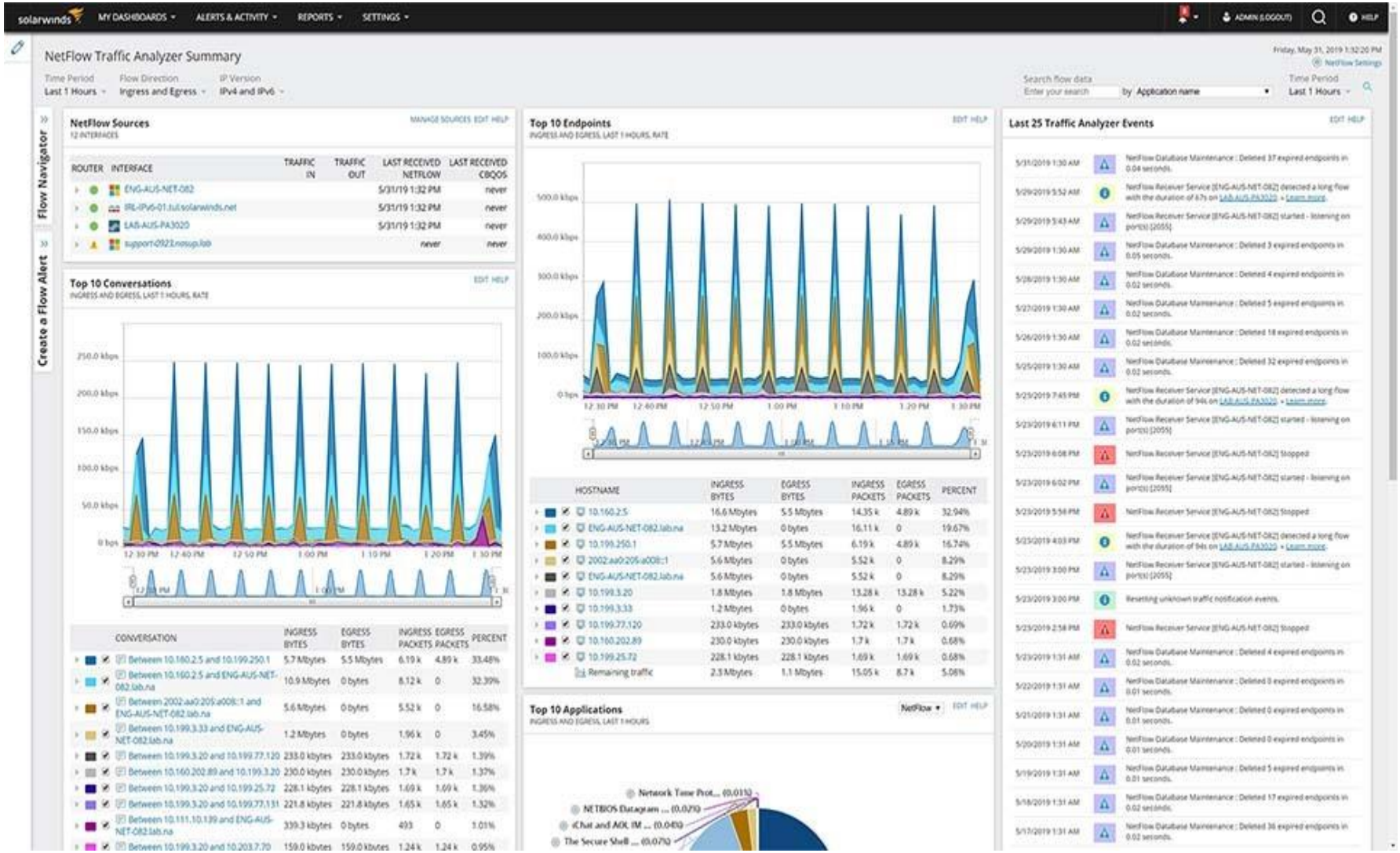
POP Protocol

The POP protocol stands for Post Office Protocol. As we know that SMTP is used as a message transfer agent. When the message is sent, then SMPT is used to deliver the message from the client to the server and then to the recipient server. But the message is sent from the recipient server to the actual server with the help of the Message Access Agent. The Message Access Agent contains two types of protocols, i.e., POP3 and IMAP.

IMAP Protocol

IMAP stands for **Internet Message Access Protocol**. It is an application layer protocol which is used to receive the emails from the mail server. It is the most commonly used protocols like POP3 for retrieving the emails.

It also follows the client/server model. On one side, we have an IMAP client, which is a process running on a computer. On the other side, we have an IMAP server, which is also a process running on another computer. Both computers are connected through a network.


solarwinds
MY DASHBOARDS
ALERTS & ACTIVITY
REPORTS
SETTINGS
NetFlow Traffic Analyzer Summary
Time Period
Last 1 Hours
Flow Direction
Ingress and Egress
IP Version
IPv4 and IPv6
Search flow data
Enter your search
by Application name
Time Period
Last 1 Hours
Flow Navigator
Create a Flow Alert
NetFlow Sources
12 INTERFACES
ROUTER
INTERFACE
TRAFFIC IN
TRAFFIC OUT
LAST RECEIVED NETFLOW
LAST RECEIVED CBQOS
ENG-AUS-NET-082
5/31/19 1:32 PM
never
IRL-IPv6-01.tul.solarwinds.net
5/31/19 1:32 PM
never
LAB-AUS-PA3020
5/31/19 1:32 PM
never
support-0923.nosup.lab
never
never
Top 10 Conversations
INGRESS AND EGRESS, LAST 1 HOURS, RATE
250.0 kbps
200.0 kbps
150.0 kbps
100.0 kbps
50.0 kbps
0 bps
12:30 PM
12:40 PM
12:50 PM
1:00 PM
1:10 PM
1:20 PM
1:30 PM
CONVERSATION
INGRESS BYTES
EGRESS BYTES
INGRESS PACKETS
EGRESS PACKETS
PERCENT
Between 10.160.2.5 and 10.199.250.1
5.7 Mbytes
5.5 Mbytes
6.19 k
4.89 k
33.48%
Between 10.160.2.5 and ENG-AUS-NET-082.lab.na
10.9 Mbytes
0 bytes
8.12 k
0
32.39%
Between 2002:aa0:205:a008::1 and ENG-AUS-NET-082.lab.na
5.6 Mbytes
0 bytes
5.52 k
0
16.58%
Between 10.199.3.33 and ENG-AUS-NET-082.lab.na
1.2 Mbytes
0 bytes
1.96 k
0
3.45%
Between 10.199.3.20 and 10.199.77.120
233.0 kbytes
233.0 kbytes
1.72 k
1.72 k
1.39%
Between 10.160.202.89 and 10.199.3.20
230.0 kbytes
230.0 kbytes
1.7 k
1.7 k
1.37%
Between 10.199.3.20 and 10.199.25.72
228.1 kbytes
228.1 kbytes
1.69 k
1.69 k
1.36%
Between 10.199.3.20 and 10.199.77.131
221.8 kbytes
221.8 kbytes
1.65 k
1.65 k
1.32%
Between 10.111.10.139 and ENG-AUS-NET-082.lab.na
339.3 kbytes
0 bytes
493
0
1.01%
Between 10.199.3.20 and 10.203.7.70
159.0 kbytes
159.0 kbytes
1.24 k
1.24 k
0.95%
Top 10 Endpoints
INGRESS AND EGRESS, LAST 1 HOURS, RATE
500.0 kbps
400.0 kbps
300.0 kbps
200.0 kbps
100.0 kbps
0 bps
12:30 PM
12:40 PM
12:50 PM
1:00 PM
1:10 PM
1:20 PM
1:30 PM
HOSTNAME
INGRESS BYTES
EGRESS BYTES
INGRESS PACKETS
EGRESS PACKETS
PERCENT
10.160.2.5
16.6 Mbytes
5.5 Mbytes
14.35 k
4.89 k
32.94%
ENG-AUS-NET-082.lab.na
13.2 Mbytes
0 bytes
16.11 k
0
19.67%
10.199.250.1
5.7 Mbytes
5.5 Mbytes
6.19 k
4.89 k
16.74%
2002:aa0:205:a008::1
5.6 Mbytes
0 bytes
5.52 k
0
8.29%
ENG-AUS-NET-082.lab.na
5.6 Mbytes
0 bytes
5.52 k
0
8.29%
10.199.3.20
1.8 Mbytes
1.8 Mbytes
13.28 k
13.28 k
5.22%
10.199.3.33
1.2 Mbytes
0 bytes
1.96 k
0
1.73%
10.199.77.120
233.0 kbytes
233.0 kbytes
1.72 k
1.72 k
0.69%
10.160.202.89
230.0 kbytes
230.0 kbytes
1.7 k
1.7 k
0.68%
10.199.25.72
228.1 kbytes
228.1 kbytes
1.69 k
1.69 k
0.68%
Remaining traffic
2.3 Mbytes
1.1 Mbytes
15.05 k
8.7 k
5.06%
Top 10 Applications
INGRESS AND EGRESS, LAST 1 HOURS
NetFlow
Network Time Prot... (0.01%)
NETBIOS Datagram ... (0.07%)
iChat and AOL IM ... (0.04%)
The Secure Shell ... (0.07%)
Last 25 Traffic Analyzer Events
5/31/2019 1:30 AM
NetFlow Database Maintenance : Deleted 37 expired endpoints in 0.04 seconds.
5/29/2019 5:52 AM
NetFlow Receiver Service [ENG-AUS-NET-082] detected a long flow with the duration of 67s on LAB-AUS-PA3020. Learn more.
5/29/2019 5:43 AM
NetFlow Receiver Service [ENG-AUS-NET-082] started - listening on port(s) [2055]
5/29/2019 1:30 AM
NetFlow Database Maintenance : Deleted 3 expired endpoints in 0.05 seconds.
5/28/2019 1:30 AM
NetFlow Database Maintenance : Deleted 4 expired endpoints in 0.02 seconds.
5/27/2019 1:30 AM
NetFlow Database Maintenance : Deleted 5 expired endpoints in 0.02 seconds.
5/26/2019 1:30 AM
NetFlow Database Maintenance : Deleted 18 expired endpoints in 0.02 seconds.
5/25/2019 1:30 AM
NetFlow Database Maintenance : Deleted 32 expired endpoints in 0.02 seconds.
5/25/2019 7:45 PM
NetFlow Receiver Service [ENG-AUS-NET-082] detected a long flow with the duration of 94s on LAB-AUS-PA3020. Learn more.
5/23/2019 6:11 PM
NetFlow Receiver Service [ENG-AUS-NET-082] started - listening on port(s) [2055]
5/23/2019 6:08 PM
NetFlow Receiver Service [ENG-AUS-NET-082] Stopped
5/23/2019 6:02 PM
NetFlow Receiver Service [ENG-AUS-NET-082] started - listening on port(s) [2055]
5/23/2019 5:58 PM
NetFlow Receiver Service [ENG-AUS-NET-082] Stopped
5/23/2019 4:03 PM
NetFlow Receiver Service [ENG-AUS-NET-082] detected a long flow with the duration of 94s on LAB-AUS-PA3020. Learn more.
5/23/2019 3:00 PM
NetFlow Receiver Service [ENG-AUS-NET-082] started - listening on port(s) [2055]
5/23/2019 3:00 PM
Resetting unknown traffic notification events.
5/23/2019 2:58 PM
NetFlow Receiver Service [ENG-AUS-NET-082] Stopped
5/23/2019 1:31 AM
NetFlow Database Maintenance : Deleted 4 expired endpoints in 0.02 seconds.
5/22/2019 1:31 AM
NetFlow Database Maintenance : Deleted 0 expired endpoints in 0.01 seconds.
5/21/2019 1:31 AM
NetFlow Database Maintenance : Deleted 0 expired endpoints in 0.01 seconds.
5/20/2019 1:31 AM
NetFlow Database Maintenance : Deleted 0 expired endpoints in 0.01 seconds.
5/19/2019 1:31 AM
NetFlow Database Maintenance : Deleted 5 expired endpoints in 0.01 seconds.
5/18/2019 1:31 AM
NetFlow Database Maintenance : Deleted 17 expired endpoints in 0.02 seconds.
5/17/2019 1:31 AM
NetFlow Database Maintenance : Deleted 36 expired endpoints in 0.02 seconds.

What is a network analyzer?

In IT, a network analyzer is a tool that records and analyzes the traffic on your network. A network analyzer breaks down traffic by different parameters and presents data flows in form of diagrams or tables. PRTG as a network analyzer helps you to break down traffic by connection, by protocol, and by IP address to identify the top talkers in your network. This facilitates the identification and solution of problems in your IT environment.

What is MRTG?

MRTG (Multi Router Traffic Grapher) is a tool that monitors traffic on a network connections mainly using SNMP. Although useful, MRTG has its limitations, especially the complex installation on Linux systems. Many of its users have now discovered PRTG Network Monitor, an innovative and user-friendly network and bandwidth monitoring tool.

What is a protocol analyzer?

A protocol analyzer (also protocol analysis tool, network analyzer, or network analysis tool) is software that you can use to record and analyze data traffic in a network. In concrete terms, this means that the network traffic is broken down according to various parameters. The data flows are then displayed in diagrams and tables for analysis.
PRTG includes protocol analysis functionalities to track and analyze different flow protocols. Network traffic is categorized by connection, IP address, and by protocol. PRTG supports all major flow protocols such as Net Flow, slow, jFlow, and IPFIX.

Simple Network Management Protocol (**SNMP**) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behaviour. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more.

SNMP is widely used in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organized in a management information base (MIB) which describe the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications.

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998.

Wireshark has a rich feature set which includes the following:

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- The most powerful display filters in the industry
- Rich VoIP analysis