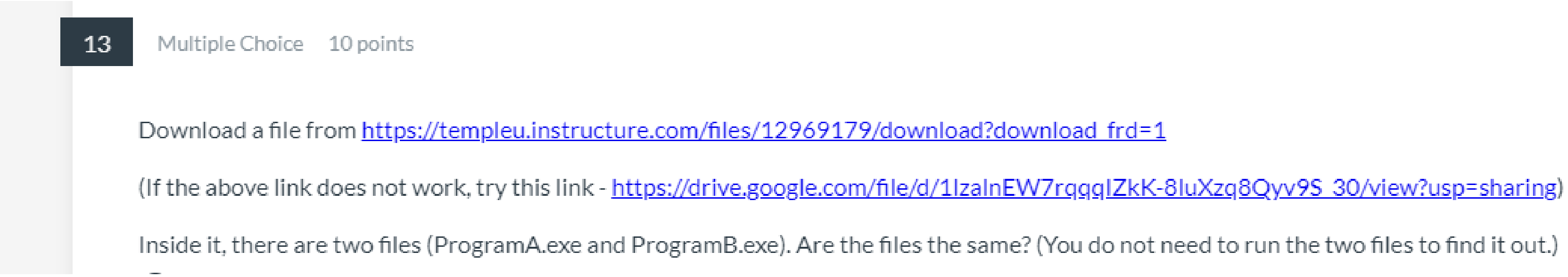
Managing Enterprise Cybersecurity MIS 4596

Unit #13

Agenda

- Mid-term question 13
- OSI Reference Model
- Linux commands for working with:
  - Domain names
  - Network availability of computers
  - Mapping paths data packets take

Midterm Question 13



Download a file from https://templeu.instructure.com/files/12969179/download?download_frd=1

(If the above link does not work, try this link - https://drive.google.com/file/d/1lzalnEW7rqqqIZkK-8luXzq8Qyv9S_30/view?usp=sharing)

Inside it, there are two files (ProgramA.exe and ProgramB.exe). Are the files the same? (You do not need to run the two files to find it out.)

- People with MacOS cannot directly open the files
  - *When I finally get the files downloaded onto my computer and try to open them a message pops up saying, "You can’t open the application “ProgramA.exe” because Microsoft Windows applications are not supported on macOS."*

They are Windows programs, however, you should be able to solve the problem anyway without running the programs themselves. I did the work for you in a class that analyzed the same to programs. Look through the class lectures and you will find what you need to know.

Telecommunication Models

Electromagnetic transmission of data among systems

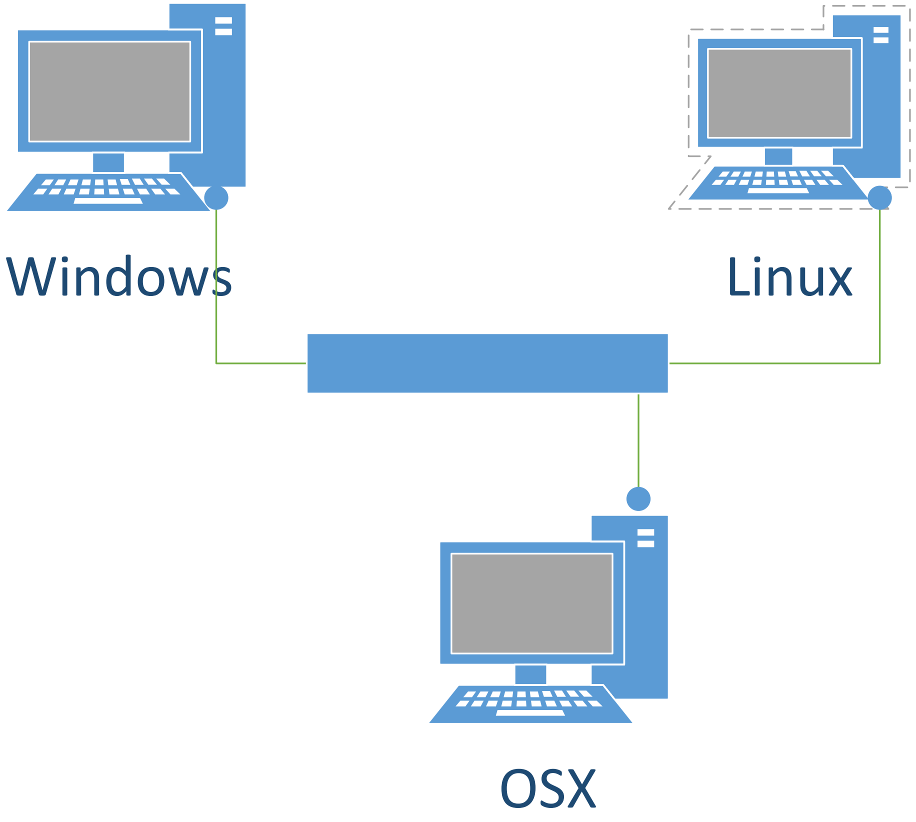
  - Through digital, wireless and analog transmission types

- **Models** and standards of the following organizations have shaped our IT communication technology today
  - International Telecommunication Union (ITU)
  - International Standards Organization (ISO)

Information and Communications Technologies (ICT)

Network protocol

- Standard set of rules that determines how systems communicate across networks
- Different systems can use the same protocol to communicate and understand each other despite their differences



Open Systems Interconnection(OSI) Reference Model

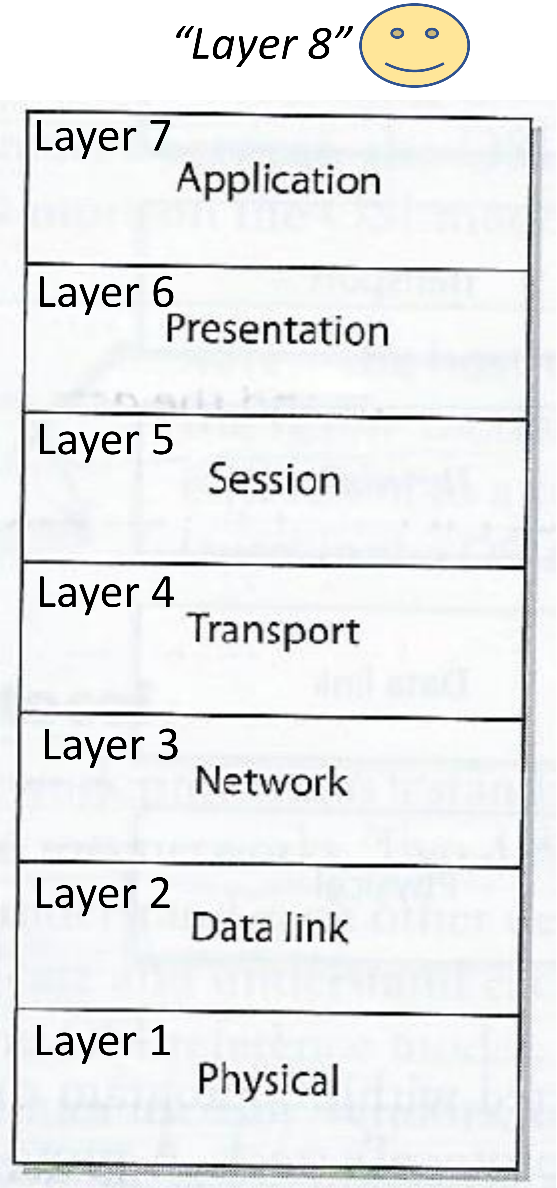
OSI Model

- Guidelines used by vendors, engineers, developers to develop products that enable computer systems to interoperate
- **Open network architecture is**
  - Not owned by vendors and not proprietary
  - Can easily integrate various technologies and vendor implementation of those technologies

Open Systems Interconnection(OSI) Reference Model – ISO Standard 7498-1

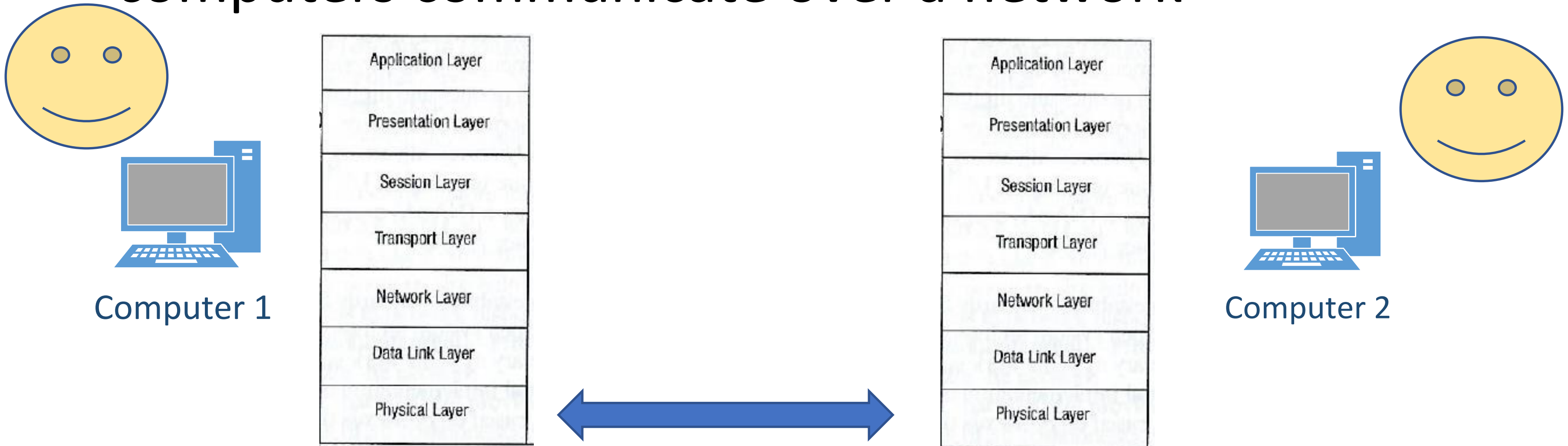
OSI Model

- Guidelines used by vendors, engineers, developers to enable their systems to interoperate
- Layers networking tasks, protocols and services into different layers
- Each layer has its own responsibilities regarding how two computers communicate over a network



“Layer 8”

Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data link
Layer 1	Physical



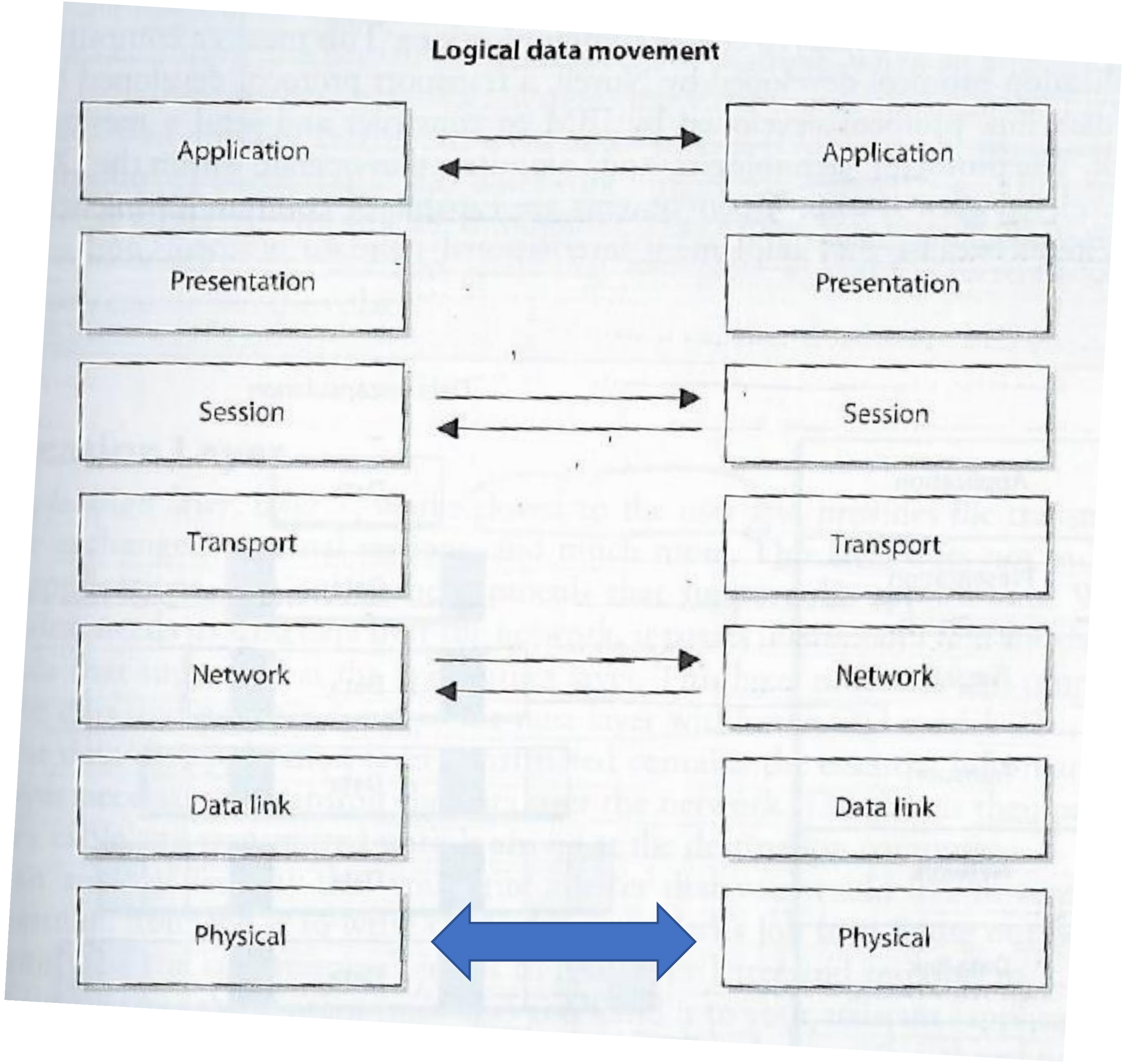
Computer 1	Computer 2
Application Layer	Application Layer
Presentation Layer	Presentation Layer
Session Layer	Session Layer
Transport Layer	Transport Layer
Network Layer	Network Layer
Data Link Layer	Data Link Layer
Physical Layer	Physical Layer

Computers communicate via network

- Protocols function in specific OSI layers
- Each protocol on one computer communicates with the same corresponding protocol within the same OSI layer on another computer

- Via logical channels

- At the physical layer electronic/light signals are passed from one computer over a wire/fiber optic cable to the other computer



Logical data movement

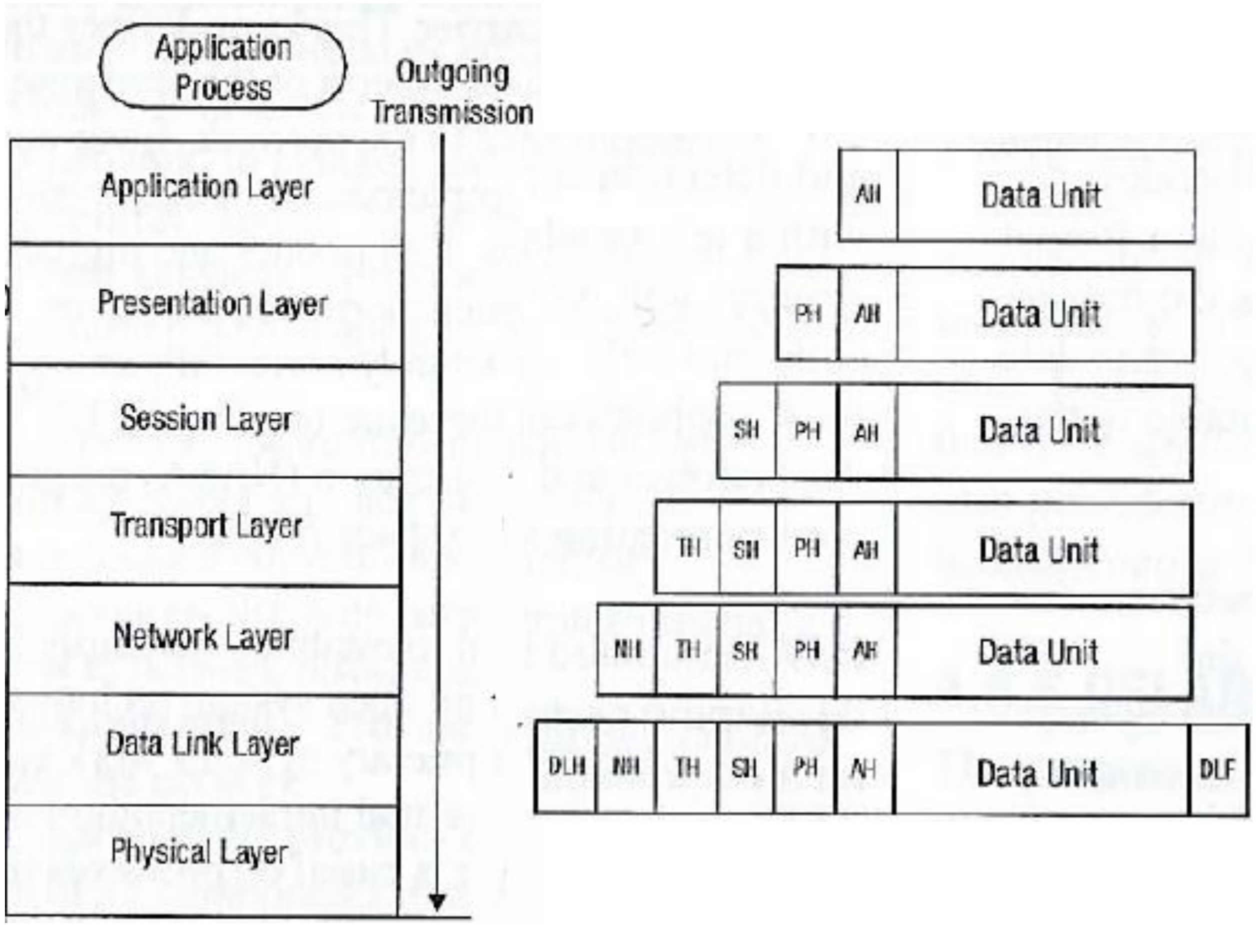
Application	Application
Presentation	Presentation
Session	Session
Transport	Transport
Network	Network
Data link	Data link
Physical	Physical

Encapsulation

- Process by which a protocol is used to enable two computers to communicate with each other within a specific OSI layer on each

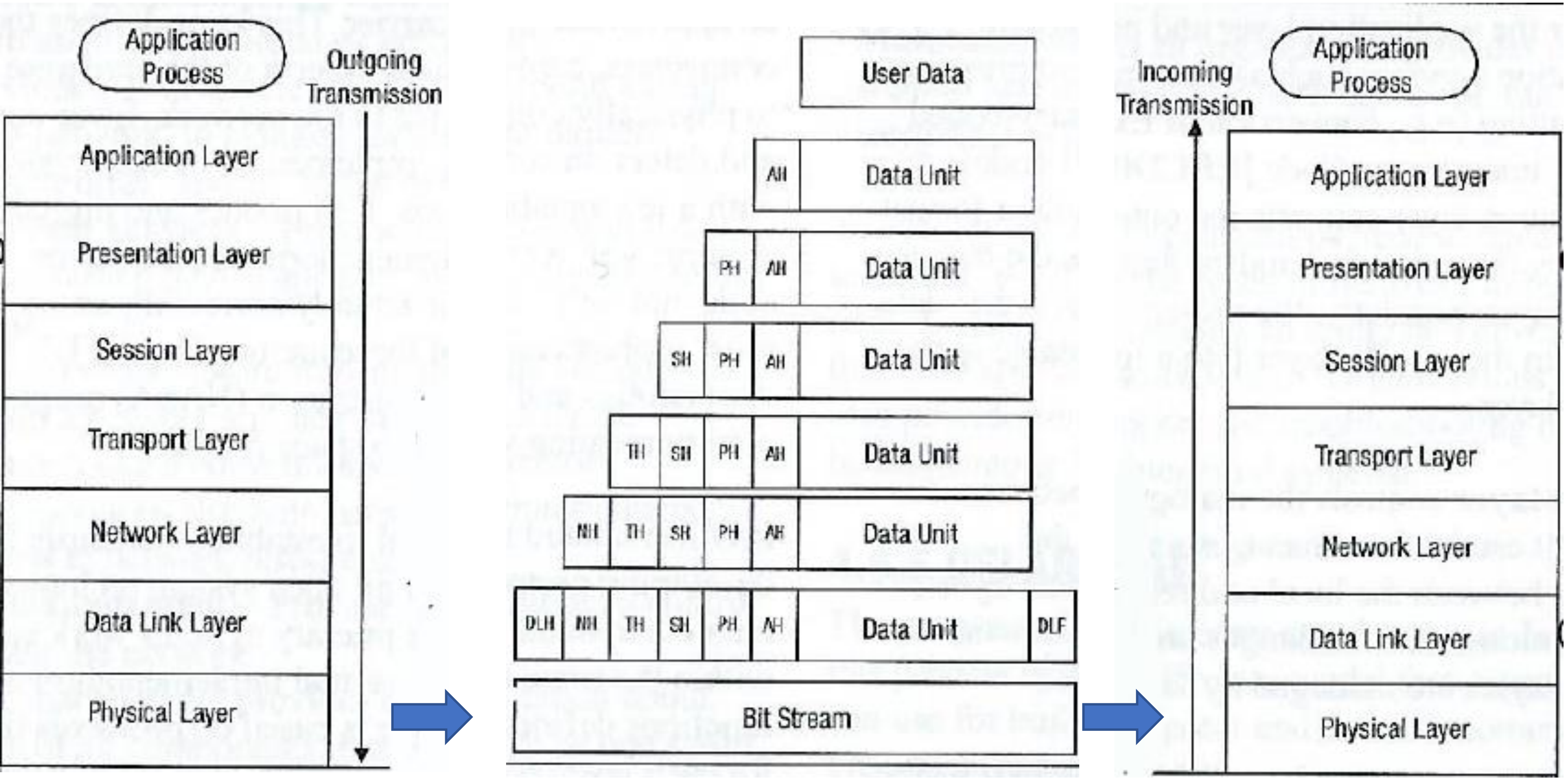
1. A message is constructed within a program on one computer and passed down through the network protocol's stack…

   A protocol at each layer adds its own information to the message, and the message grows in size as it does down the protocol stack



Encapsulation

2. At the physical layer of the network the message is passed by the sending computer as bits via electronic or light pulses (on/off) across the network to the destination computer

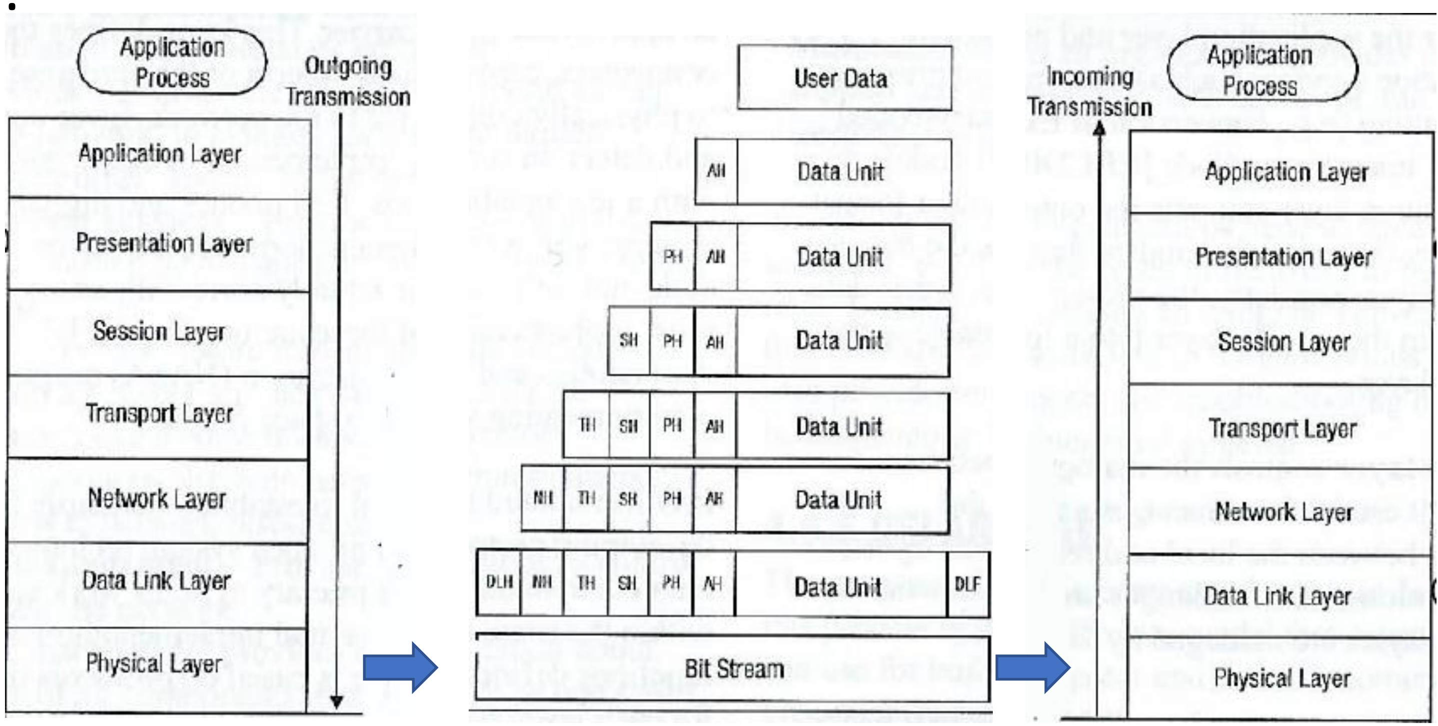


3. At the destination computer the encapsulation is reversed taking the message apart via the protocols of each layer until the data is ready for the application processing

OSI Network Model

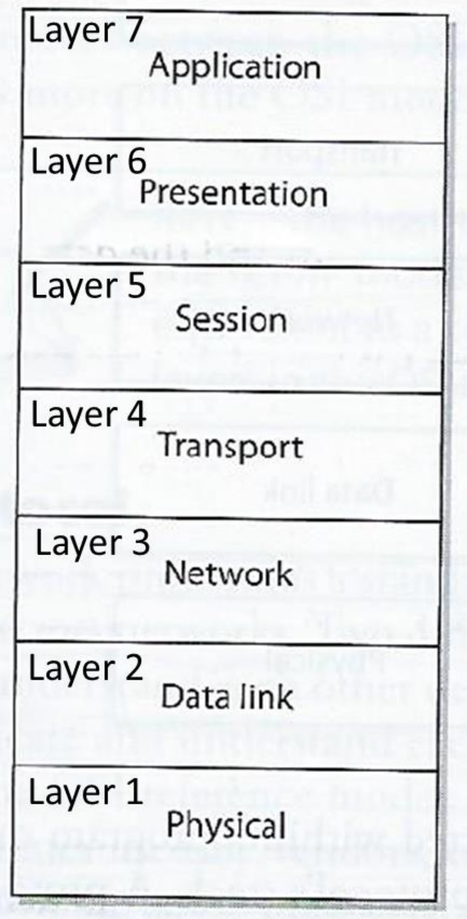
- A protocol at each layer expects the data in a particular format (“syntax”) and performs specific control functions on the data
- Data for control functions are added by the protocols at each layer in the form of headers and trailers of the datagram/packet/frame
- Each layer has a connection point (“interface”) that allows it to communicate with 3 other layers, communications with:

1. Interface of the layer above
2. Interface of the layer below it
3. Communications with the same layer in the interface of the destination computer



OSI Layers

- Specifications for each layer's interface is very structured
- Implementing international standard protocols and interfaces within different vendors' technologies makes them part of an "open system" in which computers can communicate with one another
- Being part of an open system of protocols makes the different layers of a common network stack vulnerable and targets of attack



Layer 7 Application

Layer 6 Presentation

Layer 5 Session

Layer 4 Transport

Layer 3 Network

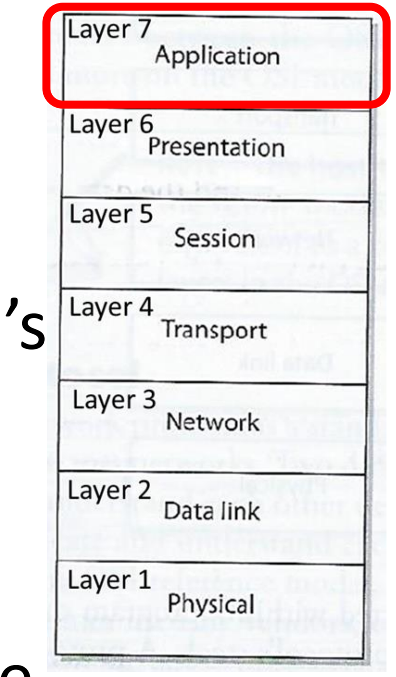
Layer 2 Data link

Layer 1 Physical

A network can be:

1. Used as a <u>channel of an attack</u> – i.e. as a resource for an attacker
   - For example: *Attacker sends a virus via a network channel from one system to another*
2. The <u>target of an attack</u>
   - For example: *Attacker carries out a denial-of-service (DoS) attack which sends a large volume of badly formed protocol message traffic over a network link to bog it down*

Layer 7: Application Layer



Layer 7 Application

Layer 6 Presentation

Layer 5 Session

Layer 4 Transport

Layer 3 Network

Layer 2 Data link

Layer 1 Physical

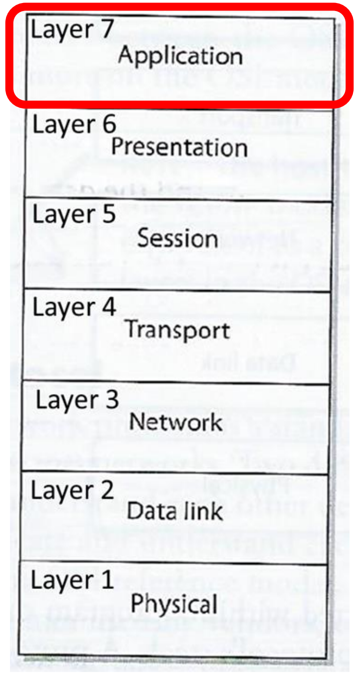
Works closest to the user – providing protocols that support the user's applications

For example: File transmissions, message exchanges, terminal sessions…

- When an application needs to send data over the network, it passes instructions and the data through the protocols that support it at the application layer

Application layer properly formats the data and sends it down to the presentation layer… (after data makes it through all the layers it has all the information needed to transmit it over the network)

Layer 7: Application Layer

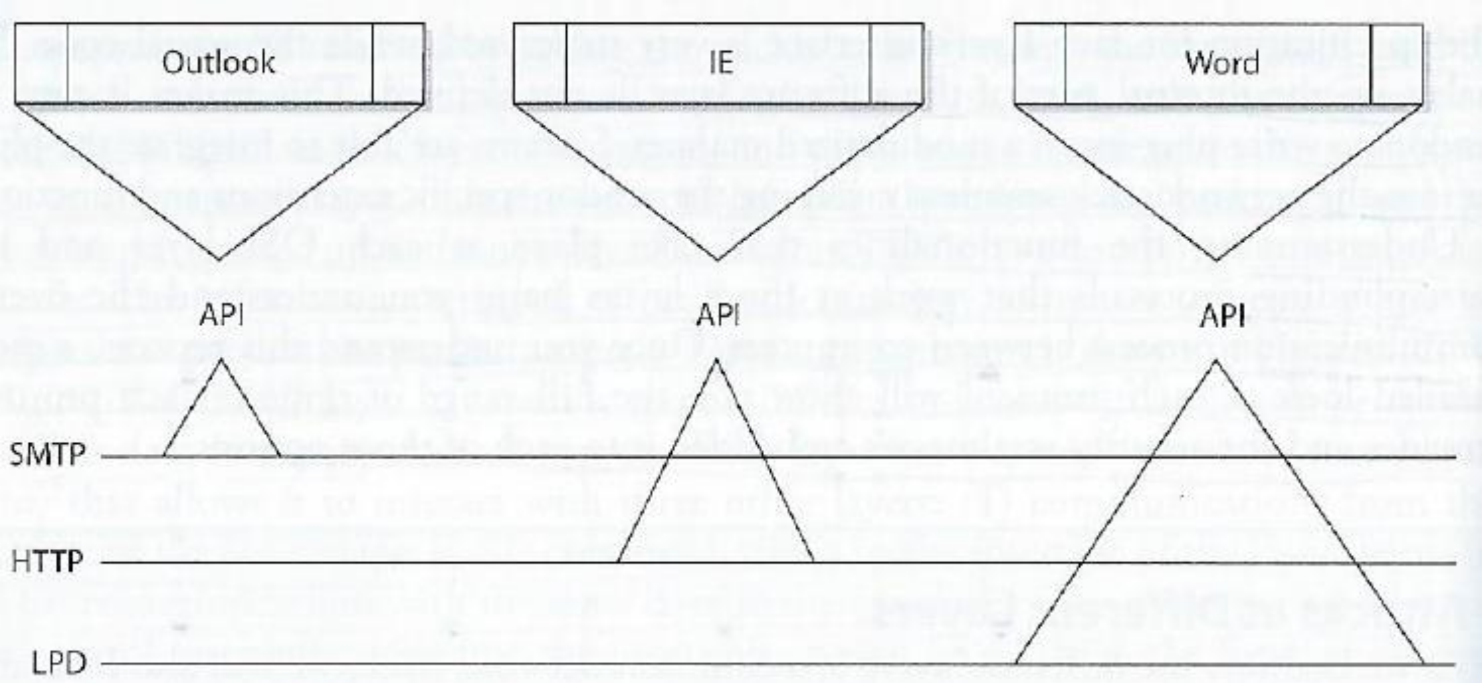


Protocols functioning at this layer communicate include:

- SMTP – Simple Mail Transfer Protocol
- HTTP – Hyper Text Transfer Protocol
- DNS – Domain Name System
- IRC – Internet Relay Chat
- LPD – Line Printer Daemon

Applications communicate with Layer 7 protocols by sending requests using Application Program Interface (API) libraries

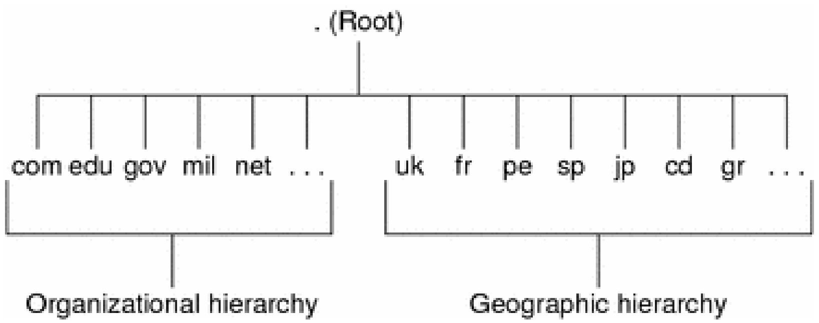
E.g. Outlook user clicks send, and the email client sends this information to SMTP which adds information to the user's message and passes it down to the Presentation Layer



Domain Name System (DNS)

- Basically, it is the internet directory
- Consists of a tree of domain names
- Example:

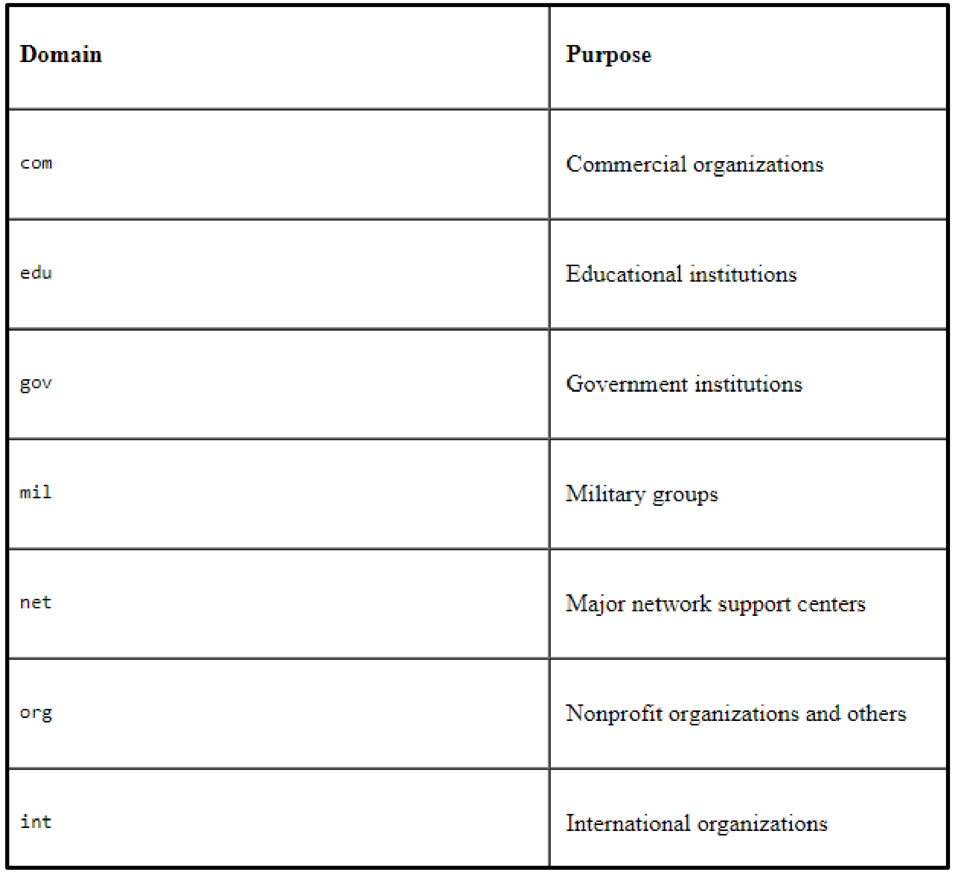
  Root -> .edu -> temple.edu



The root directory, which is represented as a dot (.), and two top level domain hierarchies:

- one organizational
- one geographical

Organizational Domains



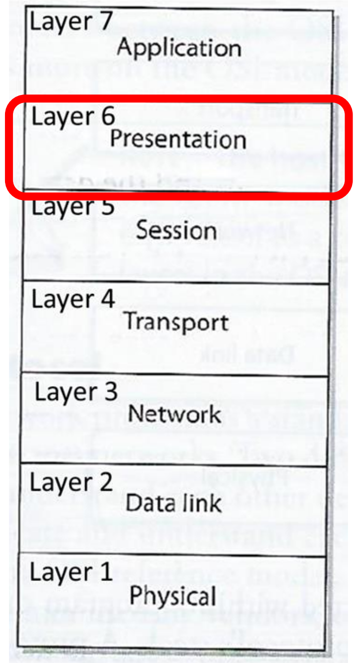
Domain	Purpose
com	Commercial organizations
edu	Educational institutions
gov	Government institutions
mil	Military groups
net	Major network support centers
org	Nonprofit organizations and others
int	International organizations

The geographic hierarchy assigns each country in the world a two or three-letter identifier

The hierarchy also provides official names for the geographic regions within each country, for example:

- domains in Britain are subdomains of the uk top-level domain, Japanese domains are subdomains of jp, and so on

Layer 6: Presentation Layer



Receives data from the application layer protocol and puts it in a standard format with annotation that enables understanding by the processes operating at Layer 6 on destination computer

Presentation layer

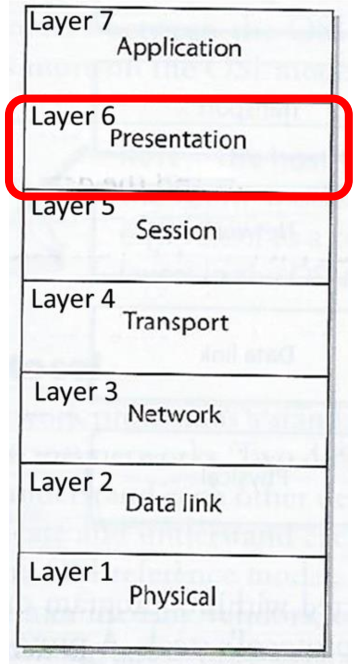
1. Translates the format of data an application is using into a standard format used for passing messages over a network
2. Adds file type data to tell destination computer the file type and how to process and present it
3. Handles compression and encryption requests and adds data that enables the receiving computer to know how to decompress and decrypt the data

Application layer properly formats the data and sends it down to the presentation layer… (after data makes it through all the layers it has all the information needed to transmit it over the network)

Layer 6: Presentation Layer

Protocols functioning at this layer communicate include:

- MIME – Multipurpose Internet Main Extensions standards
- TIFF - Tagged Image File Format
- GIF – Graphic Interchange Format
- JPEG – Joint Photographic Experts Group



Layer 7 Application

Layer 6 Presentation

Layer 5 Session

Layer 4 Transport

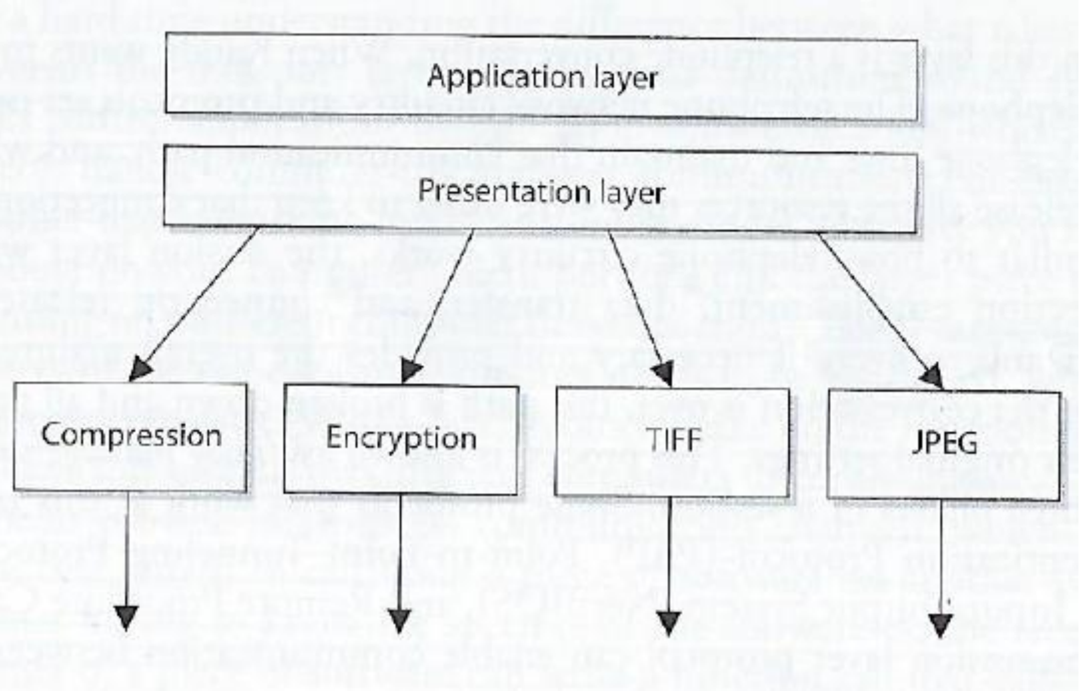
Layer 3 Network

Layer 2 Data link

Layer 1 Physical

For example,

1. *User compresses file(s) on a Windows computer, sends it to someone on Linux computer*
2. *Linux computer receives the file, it looks at the file header, interprets the header's MIME type (Content-Type: application/zip) and knows what application can decompress the file*
3. *If systems does not have a program that understands the compression/decompression instructions, the file is displayed to the user with an unassociated icon*



Application layer

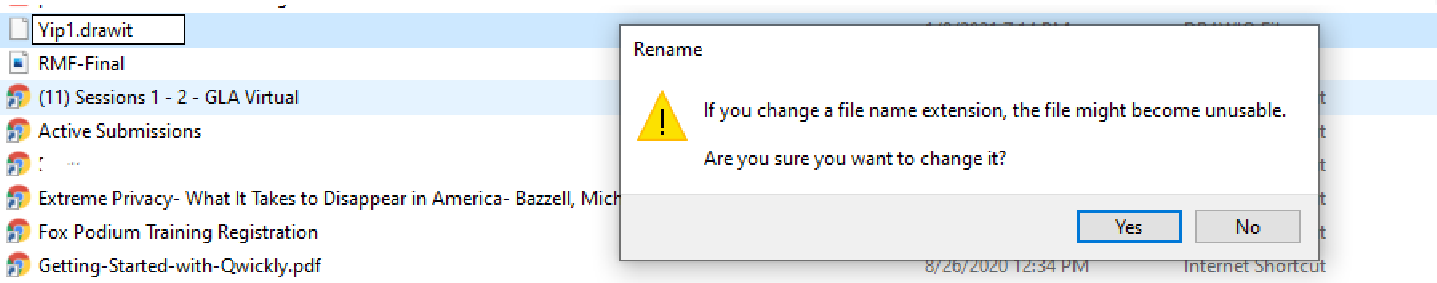
Presentation layer

Compression

Encryption

TIFF

JPEG



Yip1.drawit

RMF-Final

(11) Sessions 1 - 2 - GLA Virtual

Active Submissions

Extreme Privacy- What It Takes to Disappear in America- Bazzell, Mich

Fox Podium Training Registration

Getting-Started-with-Qwickly.pdf

8/26/2020 12:34 PM

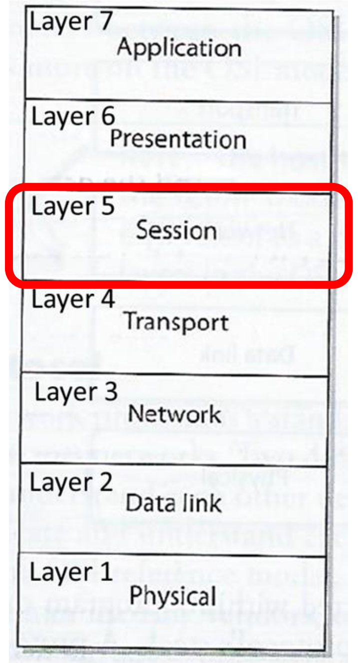
Internet Shortcut

Rename

If you change a file name extension, the file might become unusable.

Are you sure you want to change it?

Layer 5: Session Layer



When two applications need to communicate or transfer data between themselves, Layer 5 is responsible for:

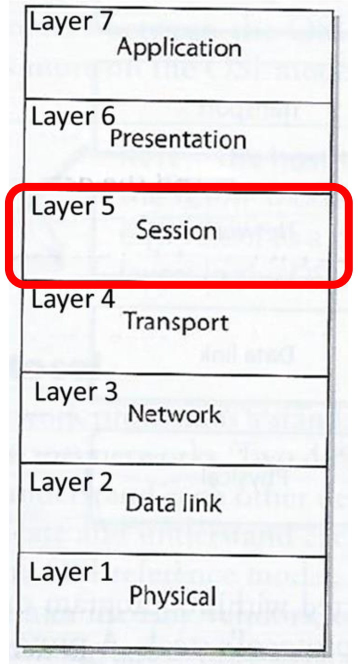
1. Establishing a connection between two applications
2. Dialog management to maintain the connection during the transfer of data
   - *Restarts and recovers the session to maintain the connection if needed*
3. Controlling release of the connection

- Provides inter-process communication channels, enables one software module on a local system to call a second software module running on a remote system. The results of the second module are retuned to the first system over the same session protocol channel

The session layer protocol enables 3 different modes of communications between 2 applications running on different computers across the network:

1. ***Simplex:** Communication takes place in one direction (very seldom used)*
2. ***Half-duplex:** Communication takes place in both directions, but only one application can send information at a time*
3. ***Full-duplex:** Communication takes place in both directions , and both applications can send information at the same time*

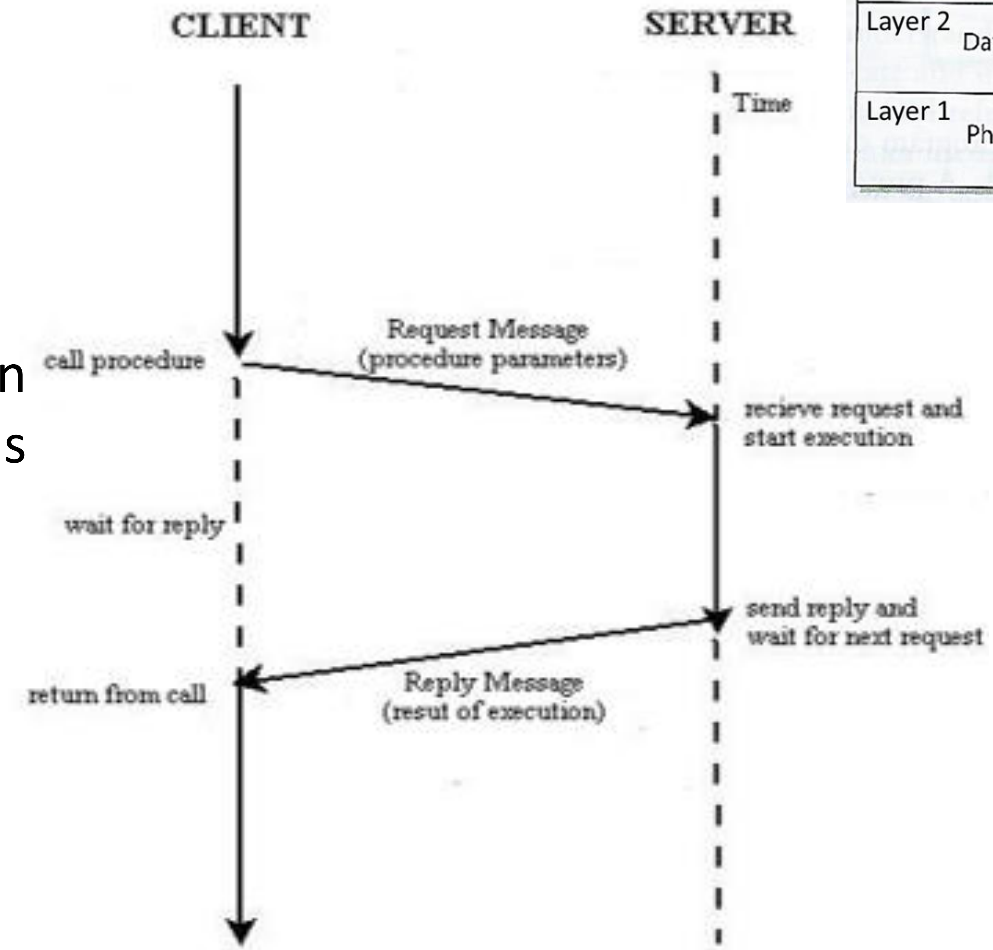
Layer 5: Session Layer



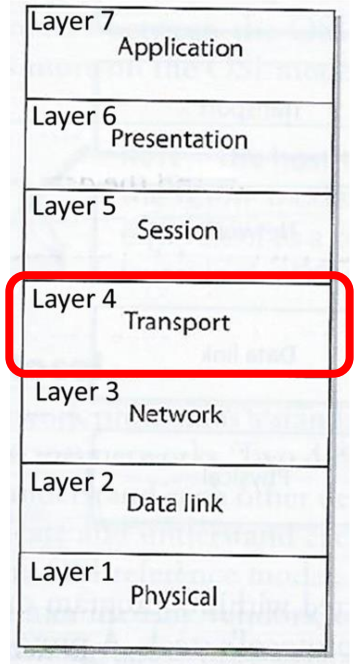
Provides inter-process communication channels, enables one software module on a local system to call a second software module running on a remote system. The results of the second module are retuned to the first system over the same session protocol channel

Session layer protocols provide the middleware functionality that connects and maintains the connection between software applications on different computers as they communicate (i.e. application to application communication)

- Client-server model
- Service oriented architecture (SOA)



Layer 4: Transport Layer

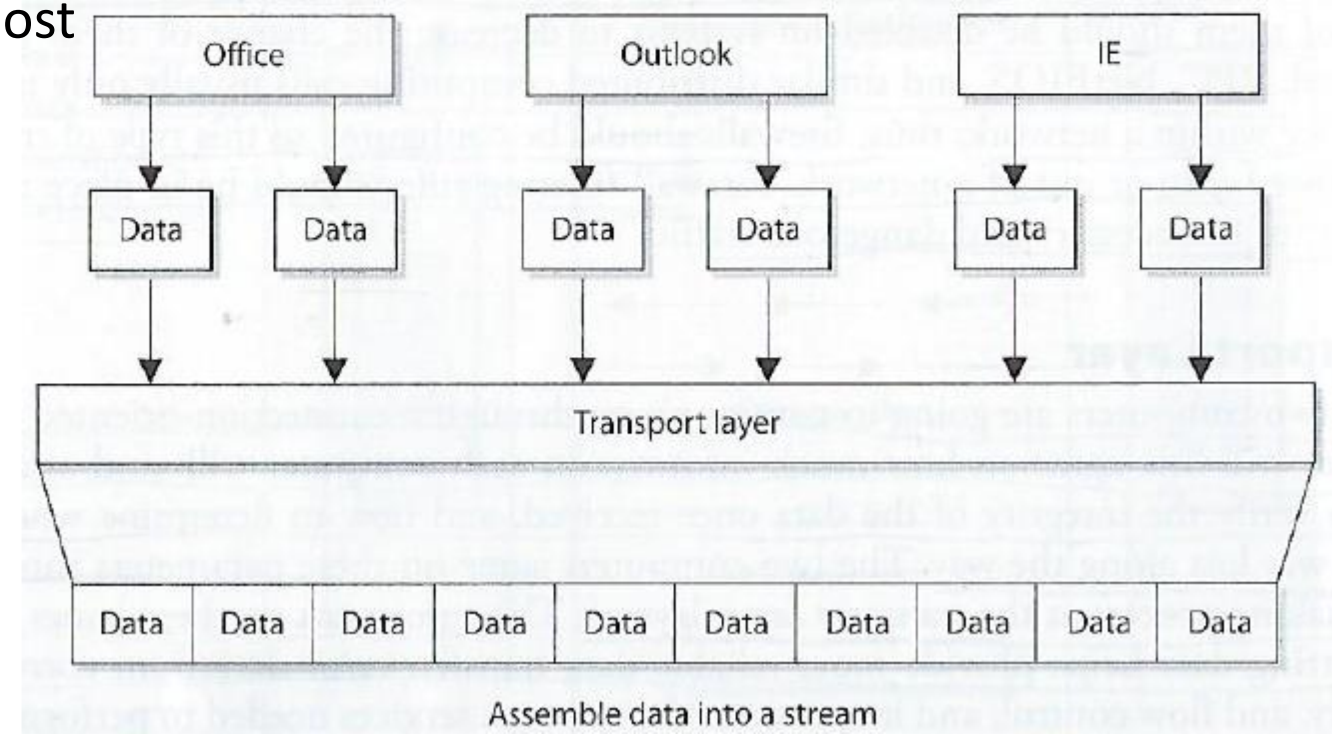


Establishes a logical connection between two computer systems and provides end-to-end data transport services

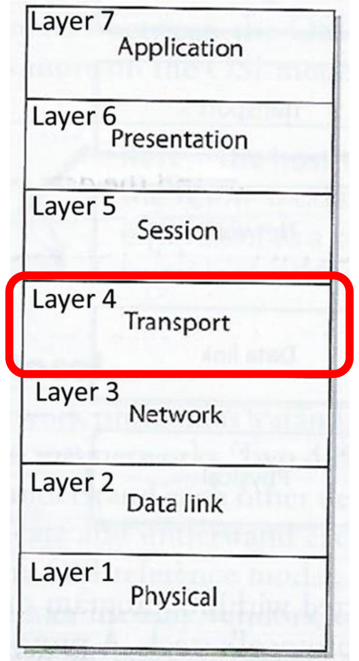
Provides connection level protocols for two computers to engage in a "handshaking process" and agree on parameters for:

1. How much data each computer will send at a time
2. How to verify data integrity once received
3. How to determine if a data packet was lost

Receives data from different applications and assembles their data into a stream for transmission over the network



Layer 4: Transport Layer



Transport layer protocol controls data flow across computer to computer connections without tracking connections between individual pairs of applications communicating across the network

Protocols:

- TCP – Transmission Control Protocol

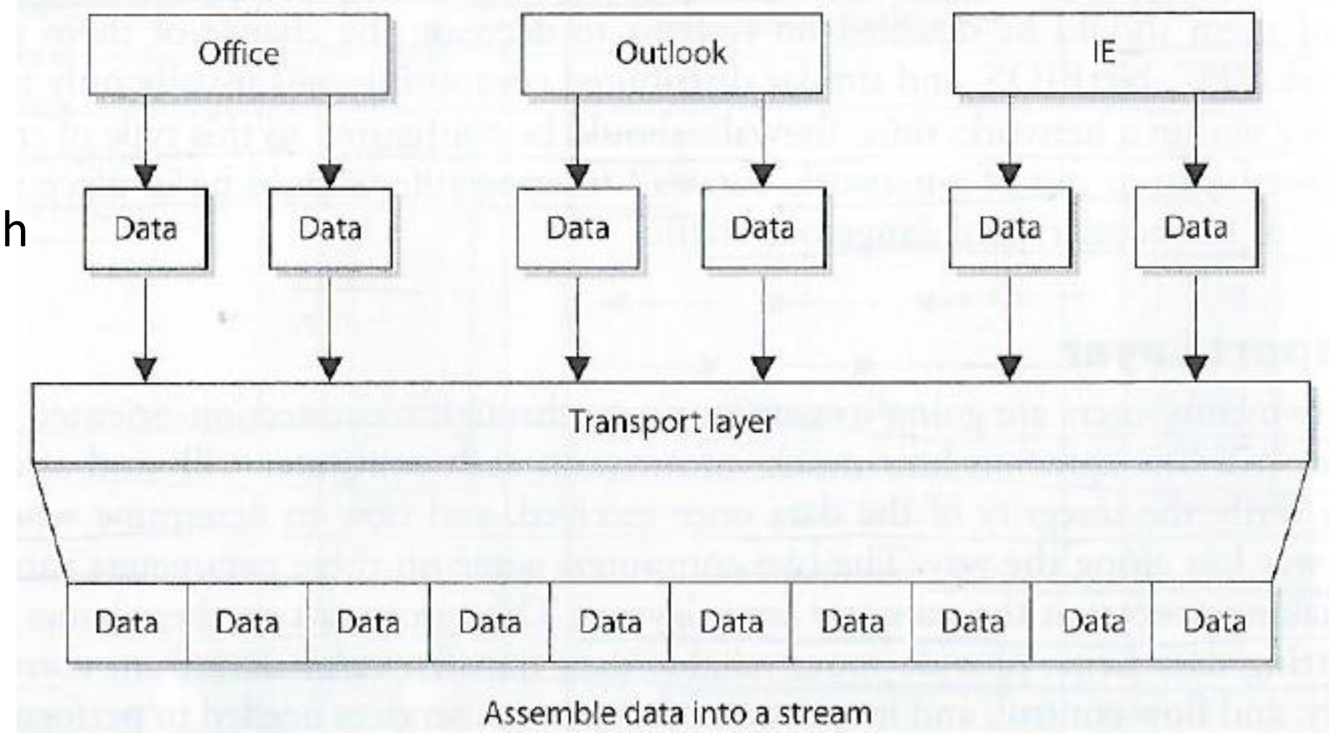
  Connection-oriented provides reliable data transmission

- UDP – User Datagram Protocol

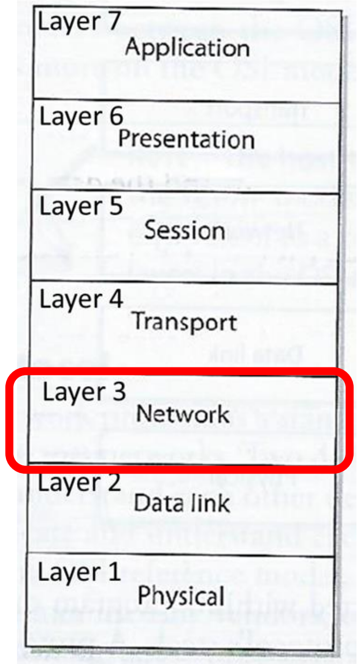
  Connectionless

TLS – Transport Layer Security protocol, straddles both Session and Transport layers

After the Transport Layer appends it's information to the data message, it is called either a TCP "segment" or a UDP "Packet"



Layer 3: Network Layer's



Routing protocols

- Build and maintain routing tables

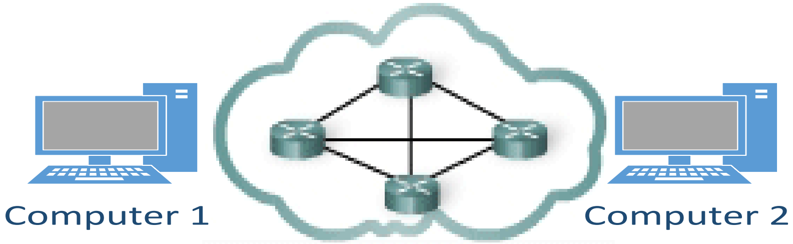
  Routing tables are maps of the network

- Determine best route (via "hops") to send packet from source computer to destination computer
- Inserts information into the data packet's header consisting of addresses (source and destination) and routes to their destination
- Do not guarantee delivery of packets

  Transport layer protocols catch problems and resend packets as needed (TCP not UDP)

Routers operate on OSI Layer 3

After the Network Layer appends it's information to the data message, it converts it to binary format and the unit of data is called a "packet"



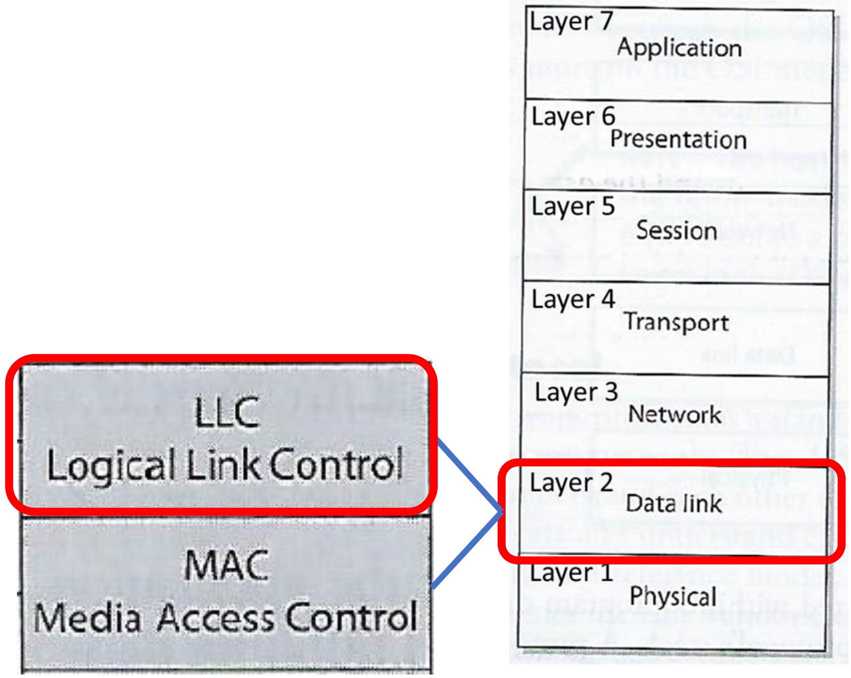
Layer 2: Data Link Layer

Translates the data packet with header/footer information accumulated from layers above into

- LAN (Local Area Network) or WAN (Wide Area Network) binary format for transmission over the network transmission line

After the network layer adds its routing information into the data packet, it passes the packet to the Data Link Layer's LCC sublayer

- LCC sublayer takes care of flow of control and error checking and passes it to the MAC sublayer

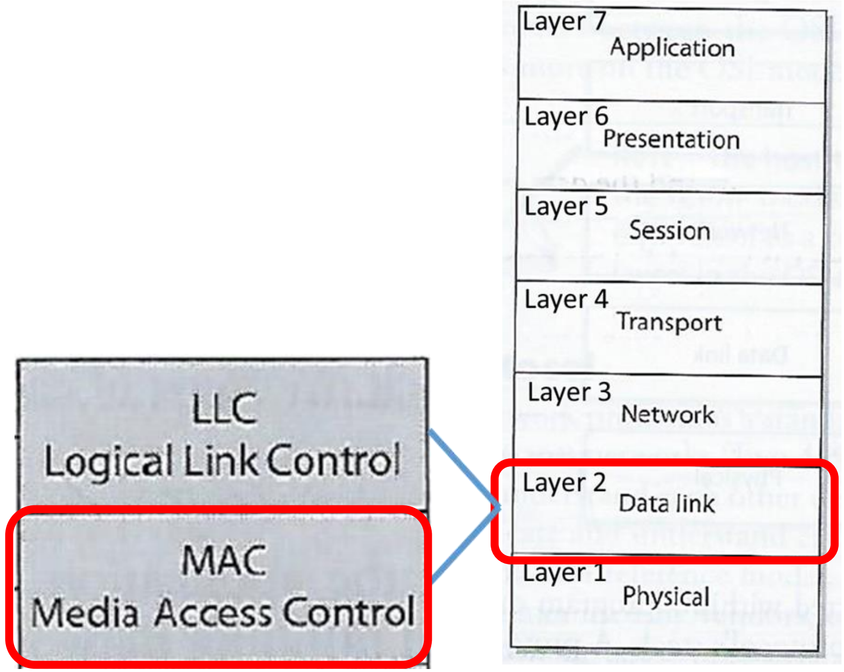


Switches operation on OSI Layer 2

Layer 2: Data Link Layer

The MAC sublayer determines if the data will be transmitted over a LAN or WAN, the network type and protocols and puts the last header and trailer on the packet before it is “put on the wire” and transmitted

- Each network type uses different protocols, NICs (network interface cards), cables, and transmission methods
- The MAC sublayer determines the format of the data frame for transmission over the particular type network the computer’s NIC is attached to

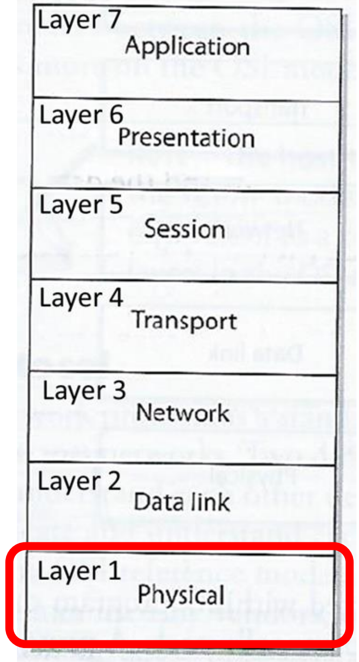


The computer’s network card bridges the data link and physical layers, takes data passed down from the user’s application through the 6 layers above and its network card driver encodes the bits at the data link layer

Each component has a different:

- *Header data format structure*
- *Protocol for physical transmission across the network type (coaxial, twisted pair, fiber optic cable; or wireless)*

Layer 1: Physical Layer



Layer 7 Application

Layer 6 Presentation

Layer 5 Session

Layer 4 Transport

Layer 3 Network

Layer 2 Data link

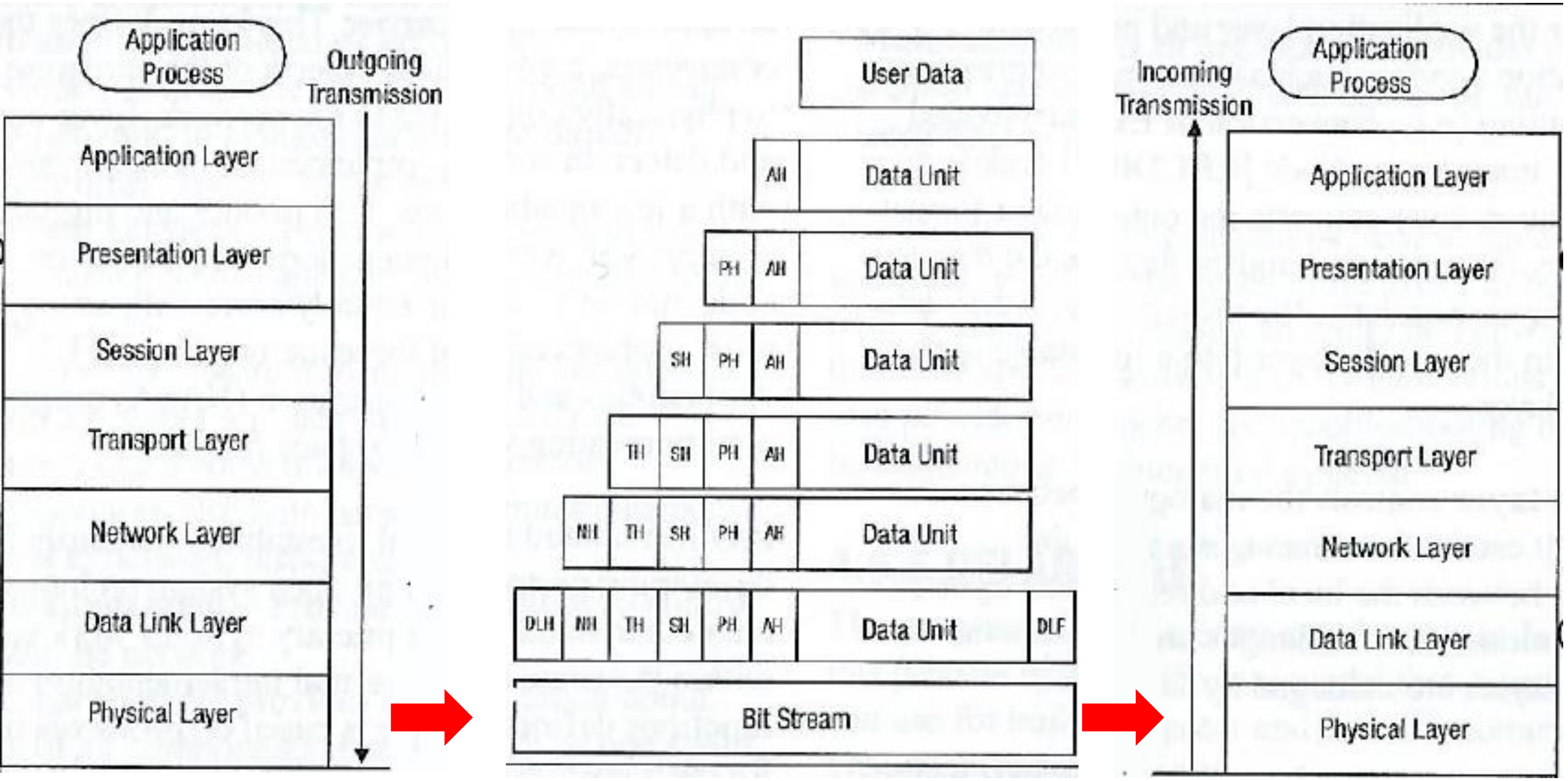
Layer 1 Physical

The Network Interface Card (NIC)

- Produces and interprets electromagnetic signals
- Converts bits into signals or voltages suitable for transmission across the LAN or WAN technology it is connected
- Determines synchronization, data transfer rates, line noise and transmission techniques based on the physical connection to electrical, optical or mechanical equipment

E.g. A ‘1’ bit transmitted via Ethernet would be translated by the NIC to +0.5-volt electric signal, and ‘0’ bit would be transmitted as 0-volts

Layer 1: Physical Layer



Data/file requests and terminals

Standard formats, encryption, compression

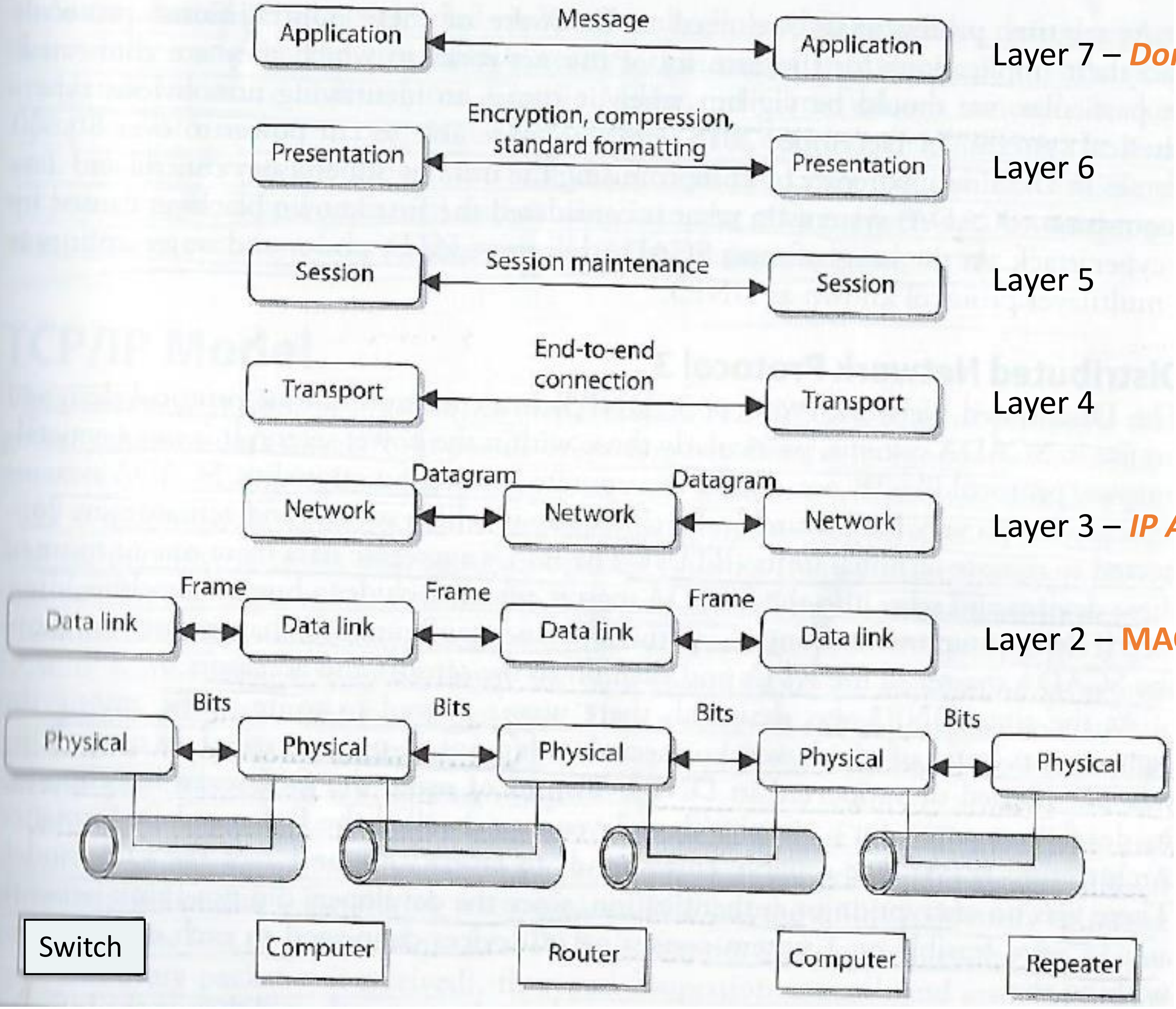
Applications communicating data

Computers communicating

Routing packets formed

Data frames ready for transfer

Signal processing



Layer 7 – ***Domain Name e.g. temple.edu***

Layer 6

Layer 5

Layer 4

Layer 3 – ***IP Address e.g. 155.247.166.60***

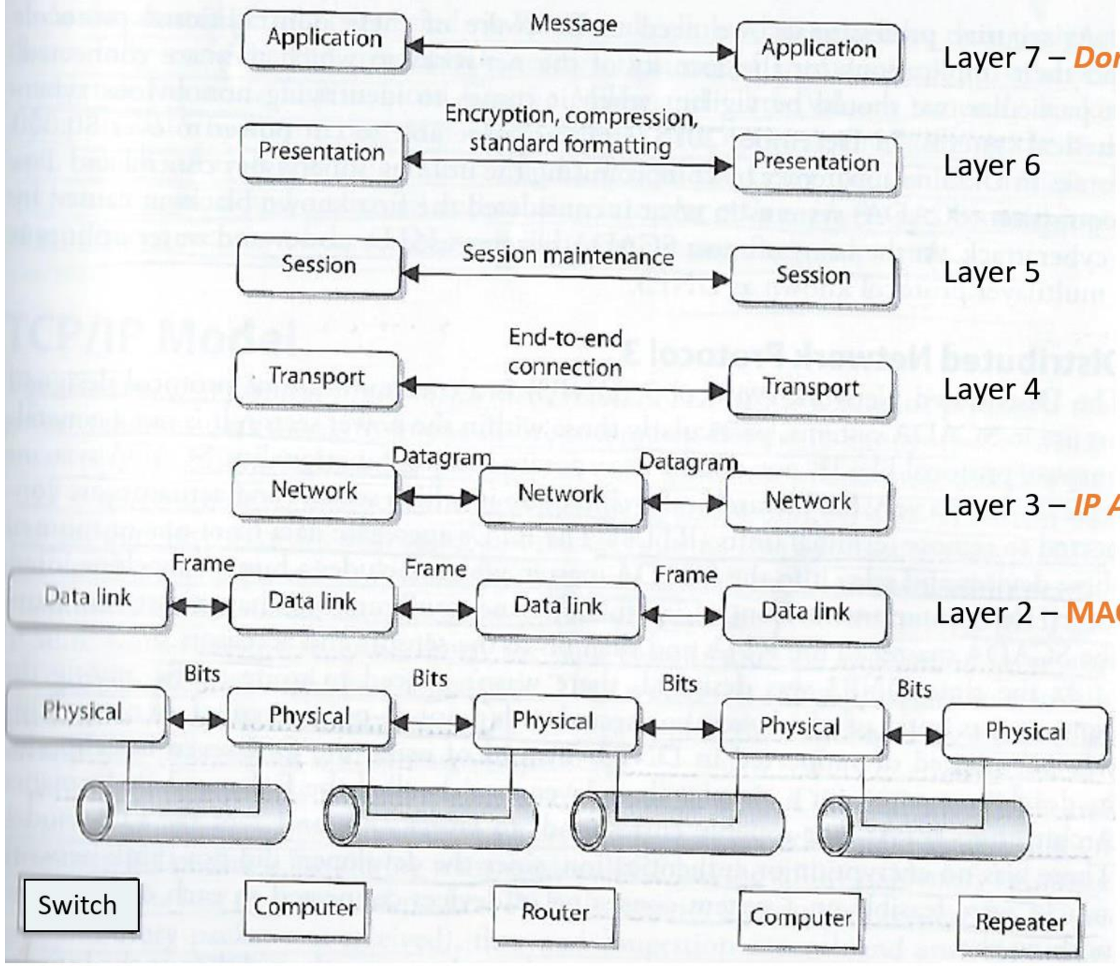
Layer 2 – **MAC (Media Access Control) Address**

Layer 1

Note: Synonyms for host computer across the OSI Model

Linux commands for working with:

- Domain names
- Network availability of computers
- Mapping paths data packets take
- Scanning computer ports



Layer 7 – ***Domain Name** e.g. temple.edu*

Layer 6

Layer 5

Layer 4

Layer 3 – ***IP Address** e.g. 155.247.166.60*

Layer 2 – **MAC (Media Access Control) Address**

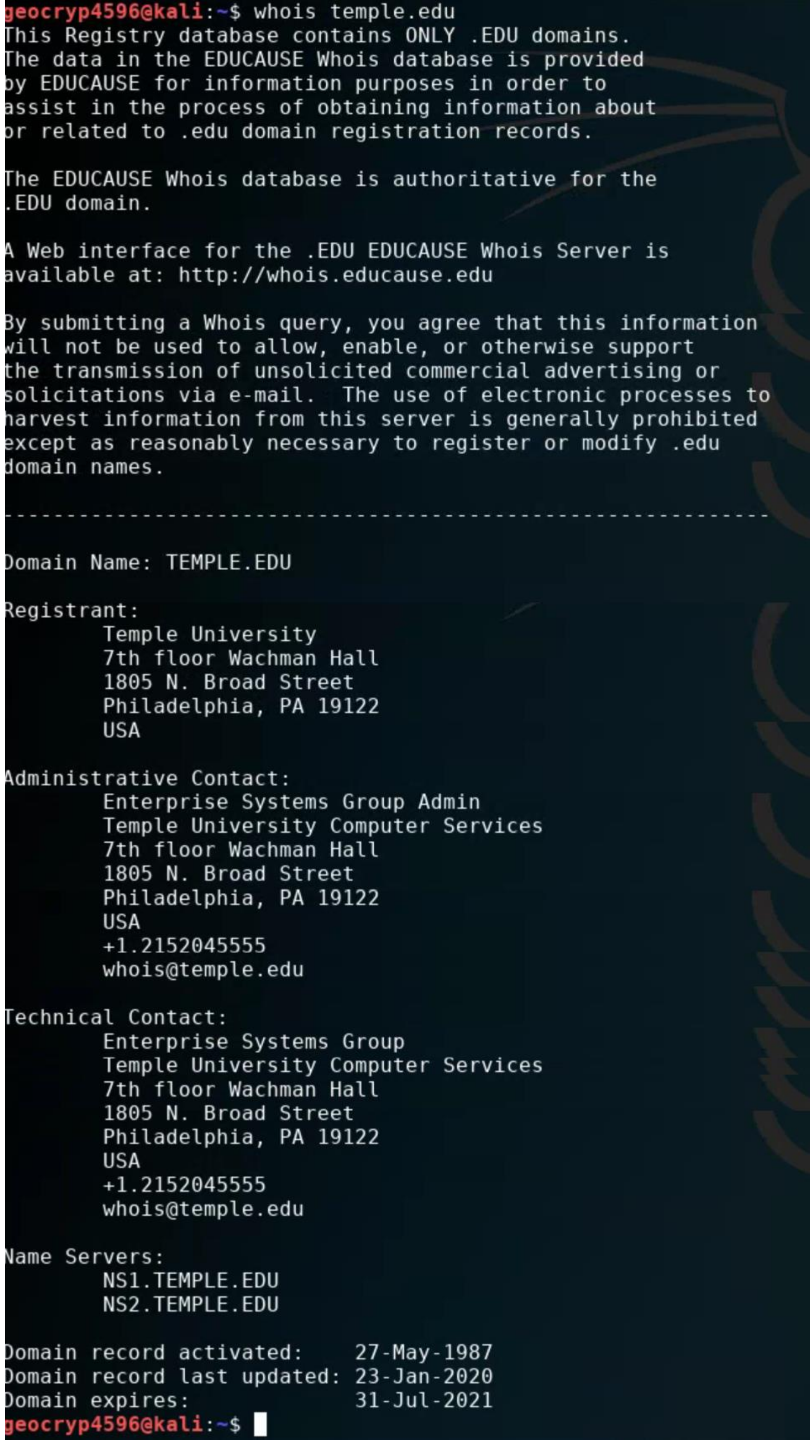
Layer 1

Note: Synonyms for host computer across the OSI Model

whois

- Database to lookup domain name, IP address, and who registered the address
- Web-based or Command line
  - whois temple.edu

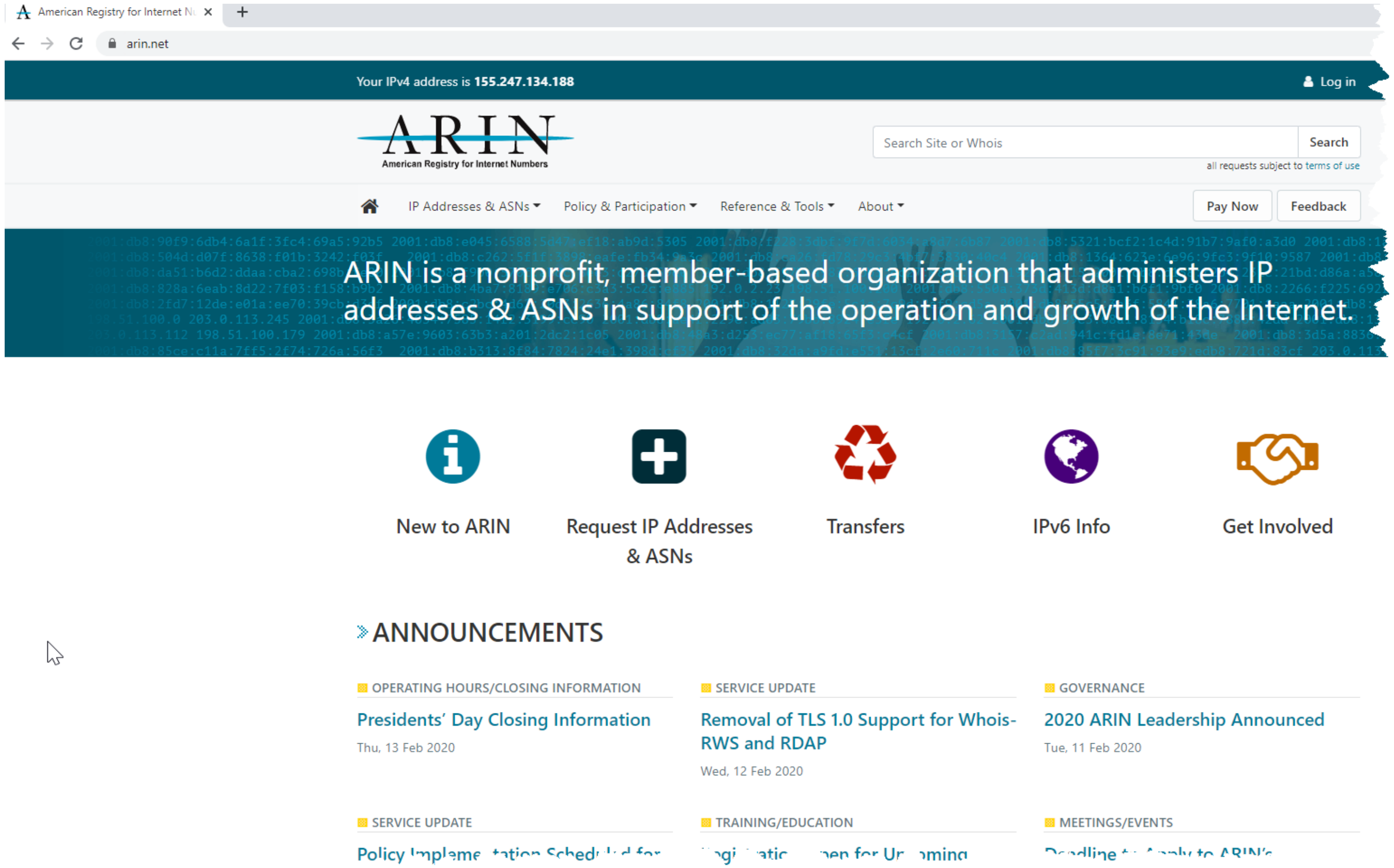
http://www.networksolutions.com/whois/index.jsp



```
geocryp4596@kali:~$ whois temple.edu
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.edu

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail.  The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

-------------------------------------------------------------

Domain Name: TEMPLE.EDU

Registrant:
        Temple University
        7th floor Wachman Hall
        1805 N. Broad Street
        Philadelphia, PA 19122
        USA

Administrative Contact:
        Enterprise Systems Group Admin
        Temple University Computer Services
        7th floor Wachman Hall
        1805 N. Broad Street
        Philadelphia, PA 19122
        USA
        +1.2152045555
        whois@temple.edu

Technical Contact:
        Enterprise Systems Group
        Temple University Computer Services
        7th floor Wachman Hall
        1805 N. Broad Street
        Philadelphia, PA 19122
        USA
        +1.2152045555
        whois@temple.edu

Name Servers:
        NS1.TEMPLE.EDU
        NS2.TEMPLE.EDU

Domain record activated:    27-May-1987
Domain record last updated: 23-Jan-2020
Domain expires:             31-Jul-2021
geocryp4596@kali:~$
```

ARIN

- American Registry for Internet Numbers
- Regional Internet Registry for US, Canada, and many Caribbean islands
- ARIN is one of five regional registries
- Provides services related to the technical coordination and management of Internet number resources



Your IPv4 address is 155.247.134.188

ARIN is a nonprofit, member-based organization that administers IP addresses & ASNs in support of the operation and growth of the Internet.

ANNOUNCEMENTS

OPERATING HOURS/CLOSING INFORMATION
Presidents' Day Closing Information
Thu, 13 Feb 2020

SERVICE UPDATE
Removal of TLS 1.0 Support for Whois-RWS and RDAP
Wed, 12 Feb 2020

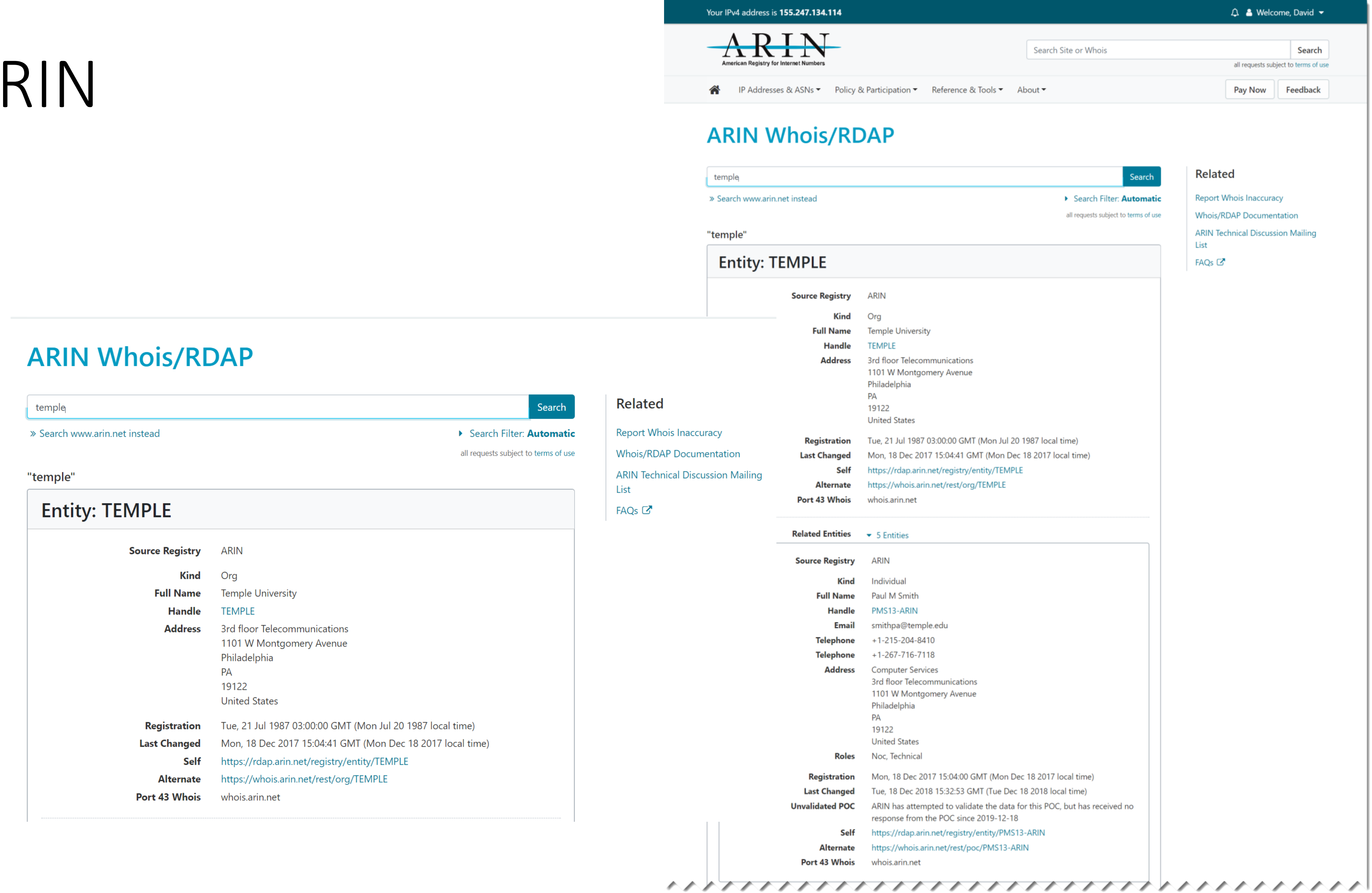
GOVERNANCE
2020 ARIN Leadership Announced
Tue, 11 Feb 2020

SERVICE UPDATE
Policy Implementation Schedule for

TRAINING/EDUCATION
Registration Open for Upcoming

MEETINGS/EVENTS
Deadline to Apply to ARIN's

ARIN



Your IPv4 address is **155.247.134.114**

all requests subject to terms of use

ARIN Whois/RDAP

all requests subject to terms of use

"temple"

Entity: TEMPLE

Source Registry	ARIN
Kind	Org
Full Name	Temple University
Handle	TEMPLE
Address	3rd floor Telecommunications 1101 W Montgomery Avenue Philadelphia PA 19122 United States
Registration	Tue, 21 Jul 1987 03:00:00 GMT (Mon Jul 20 1987 local time)
Last Changed	Mon, 18 Dec 2017 15:04:41 GMT (Mon Dec 18 2017 local time)
Self	https://rdap.arin.net/registry/entity/TEMPLE
Alternate	https://whois.arin.net/rest/org/TEMPLE
Port 43 Whois	whois.arin.net

Related Entities ▾ 5 Entities

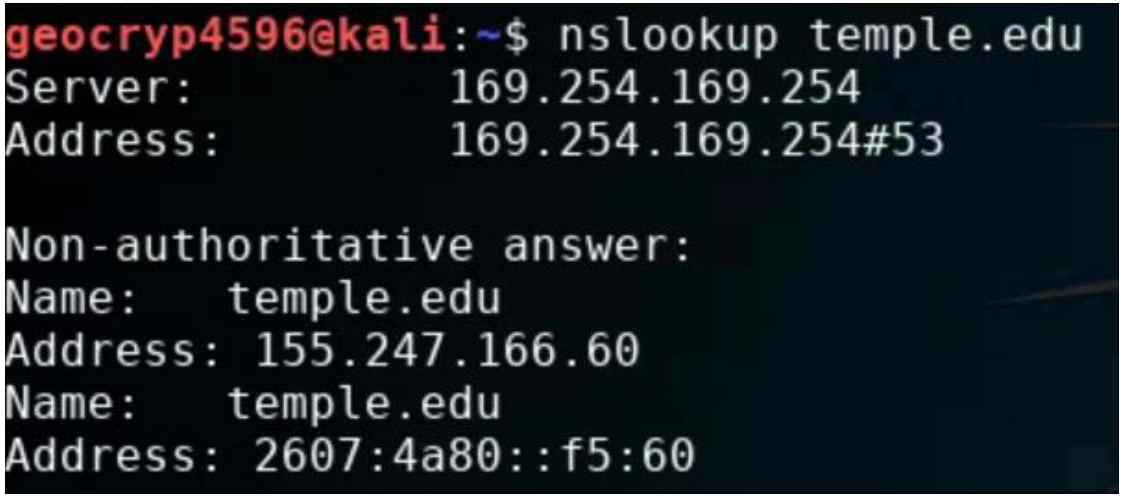
Source Registry	ARIN
Kind	Individual
Full Name	Paul M Smith
Handle	PMS13-ARIN
Email	smithpa@temple.edu
Telephone	+1-215-204-8410
Telephone	+1-267-716-7118
Address	Computer Services 3rd floor Telecommunications 1101 W Montgomery Avenue Philadelphia PA 19122 United States
Roles	Noc, Technical
Registration	Mon, 18 Dec 2017 15:04:00 GMT (Mon Dec 18 2017 local time)
Last Changed	Tue, 18 Dec 2018 15:32:53 GMT (Tue Dec 18 2018 local time)
Unvalidated POC	ARIN has attempted to validate the data for this POC, but has received no response from the POC since 2019-12-18
Self	https://rdap.arin.net/registry/entity/PMS13-ARIN
Alternate	https://whois.arin.net/rest/poc/PMS13-ARIN
Port 43 Whois	whois.arin.net

Related

- Report Whois Inaccuracy
- Whois/RDAP Documentation
- ARIN Technical Discussion Mailing List
- FAQs

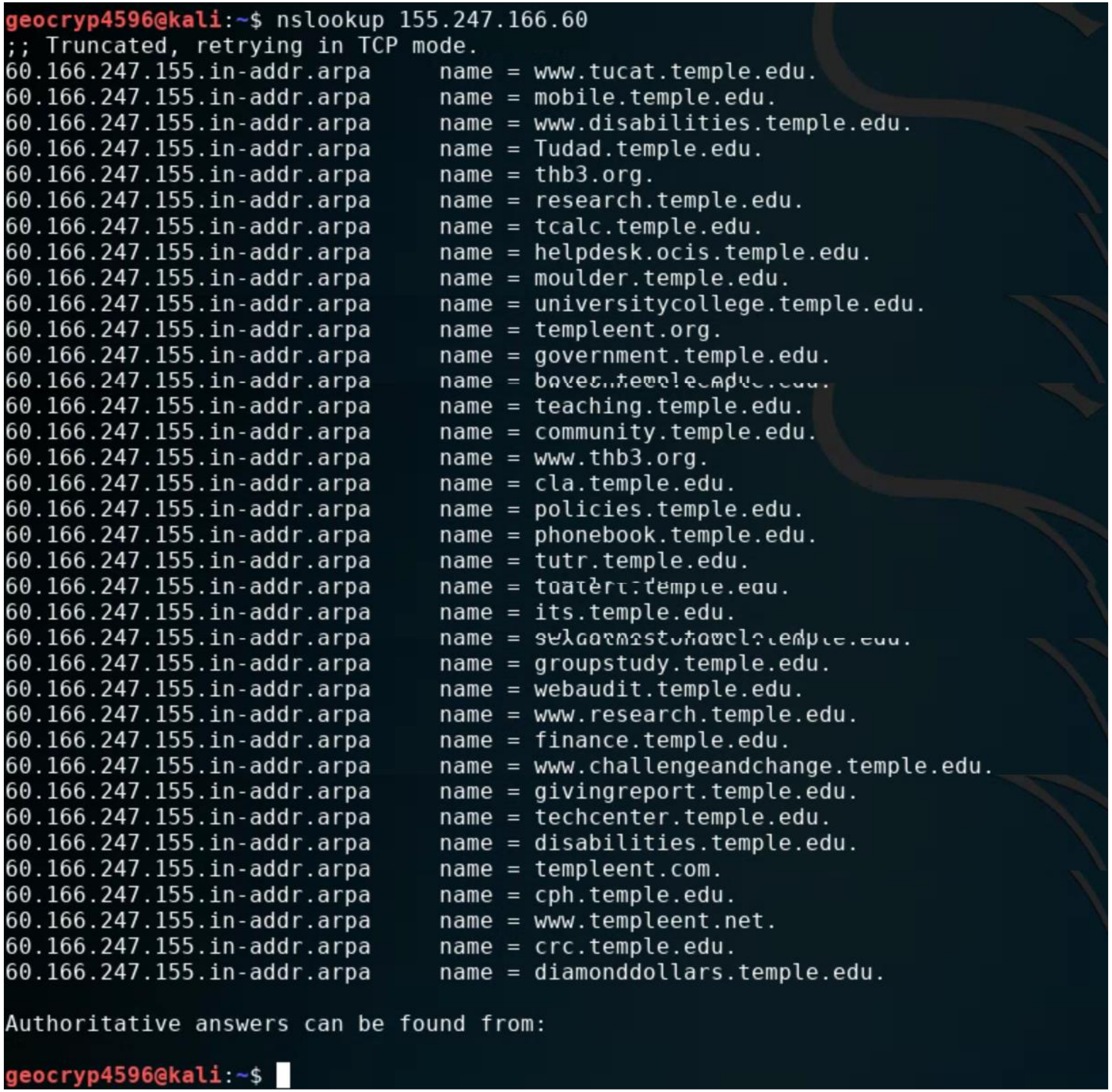
DNS

- nslookup – for querying DNS server
  - Example
    - By domain name: nslookup temple.edu
    - By IP address: nslookup 169.254.169.254

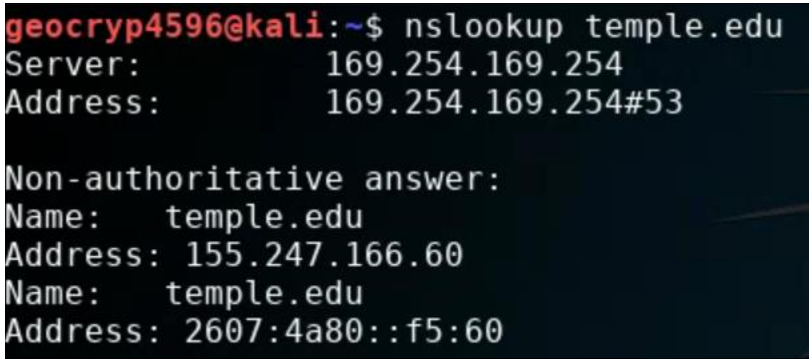


```
geocryp4596@kali:~$ nslookup temple.edu
Server:         169.254.169.254
Address:        169.254.169.254#53

Non-authoritative answer:
Name:   temple.edu
Address: 155.247.166.60
Name:   temple.edu
Address: 2607:4a80::f5:60
```

DNS



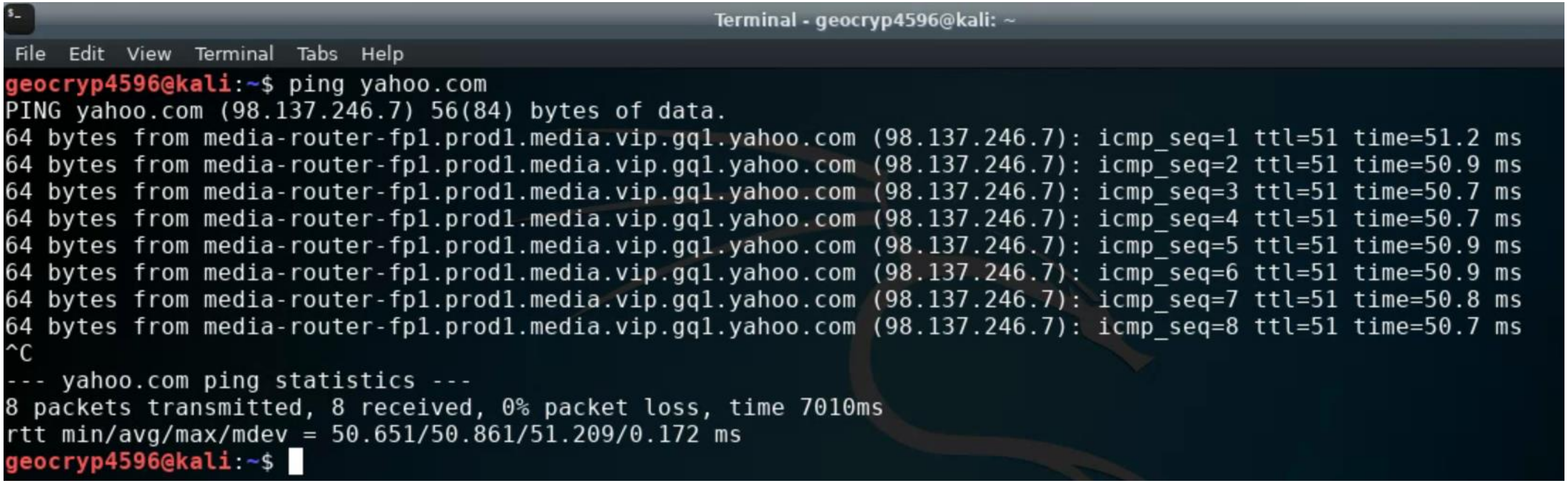
```
geocryp4596@kali:~$ nslookup 155.247.166.60
;; Truncated, retrying in TCP mode.
60.166.247.155.in-addr.arpa     name = www.tucat.temple.edu.
60.166.247.155.in-addr.arpa     name = mobile.temple.edu.
60.166.247.155.in-addr.arpa     name = www.disabilities.temple.edu.
60.166.247.155.in-addr.arpa     name = Tudad.temple.edu.
60.166.247.155.in-addr.arpa     name = thb3.org.
60.166.247.155.in-addr.arpa     name = research.temple.edu.
60.166.247.155.in-addr.arpa     name = tcalc.temple.edu.
60.166.247.155.in-addr.arpa     name = helpdesk.ocis.temple.edu.
60.166.247.155.in-addr.arpa     name = moulder.temple.edu.
60.166.247.155.in-addr.arpa     name = universitycollege.temple.edu.
60.166.247.155.in-addr.arpa     name = templeent.org.
60.166.247.155.in-addr.arpa     name = government.temple.edu.
60.166.247.155.in-addr.arpa     name = bover.temple.edu.
60.166.247.155.in-addr.arpa     name = teaching.temple.edu.
60.166.247.155.in-addr.arpa     name = community.temple.edu.
60.166.247.155.in-addr.arpa     name = www.thb3.org.
60.166.247.155.in-addr.arpa     name = cla.temple.edu.
60.166.247.155.in-addr.arpa     name = policies.temple.edu.
60.166.247.155.in-addr.arpa     name = phonebook.temple.edu.
60.166.247.155.in-addr.arpa     name = tutr.temple.edu.
60.166.247.155.in-addr.arpa     name = tuatert.temple.edu.
60.166.247.155.in-addr.arpa     name = its.temple.edu.
60.166.247.155.in-addr.arpa     name = [illegible].temple.edu.
60.166.247.155.in-addr.arpa     name = groupstudy.temple.edu.
60.166.247.155.in-addr.arpa     name = webaudit.temple.edu.
60.166.247.155.in-addr.arpa     name = www.research.temple.edu.
60.166.247.155.in-addr.arpa     name = finance.temple.edu.
60.166.247.155.in-addr.arpa     name = www.challengeandchange.temple.edu.
60.166.247.155.in-addr.arpa     name = givingreport.temple.edu.
60.166.247.155.in-addr.arpa     name = techcenter.temple.edu.
60.166.247.155.in-addr.arpa     name = disabilities.temple.edu.
60.166.247.155.in-addr.arpa     name = templeent.com.
60.166.247.155.in-addr.arpa     name = cph.temple.edu.
60.166.247.155.in-addr.arpa     name = www.templeent.net.
60.166.247.155.in-addr.arpa     name = crc.temple.edu.
60.166.247.155.in-addr.arpa     name = diamonddollars.temple.edu.

Authoritative answers can be found from:

geocryp4596@kali:~$
```



```
geocryp4596@kali:~$ nslookup temple.edu
Server:         169.254.169.254
Address:        169.254.169.254#53

Non-authoritative answer:
Name:   temple.edu
Address: 155.247.166.60
Name:   temple.edu
Address: 2607:4a80::f5:60
```

PING – Packet InterNet Groper

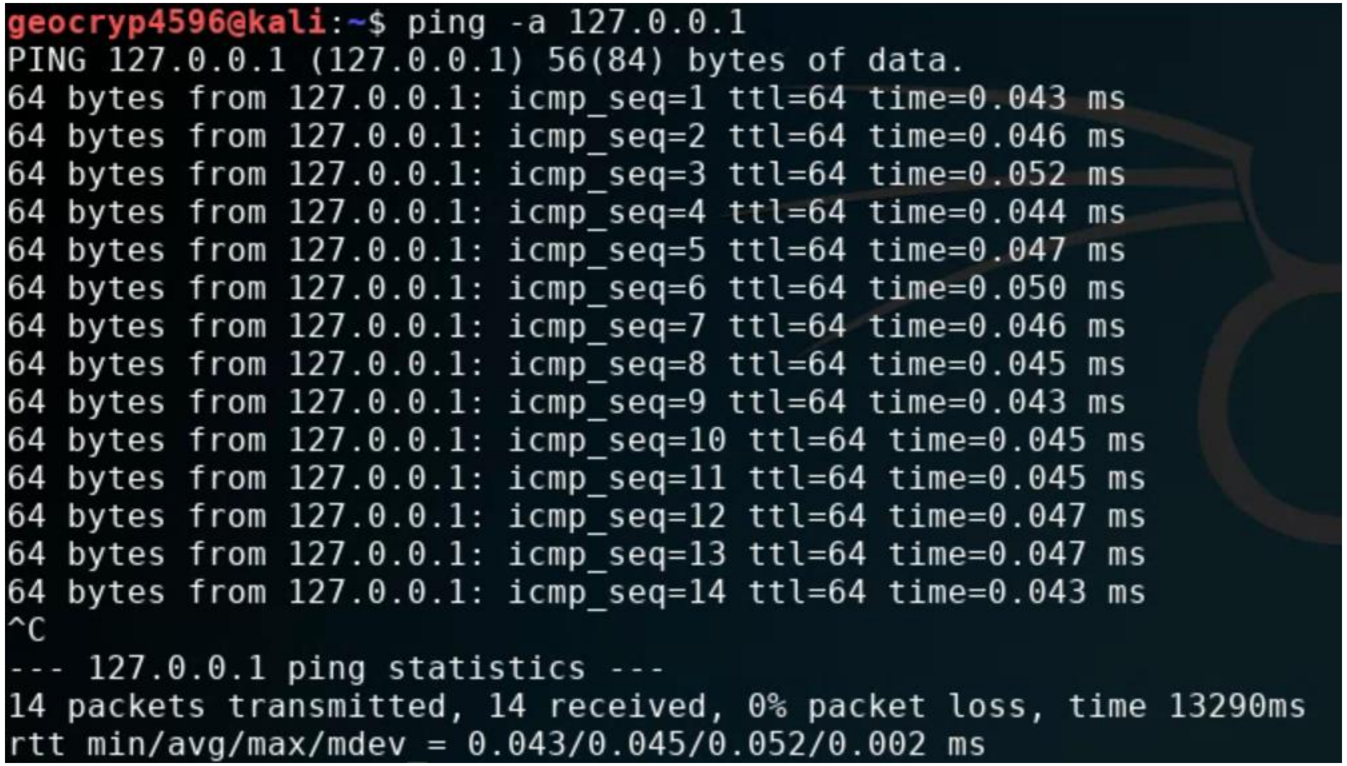
- Networking utility
- Used to test whether a host is “alive” on the Internet Protocol (IP) network
- It measures the time it takes for a message sent from one host to reach another and echo back to the original host
- Ctrl+C can stop the ping command


Terminal - geocryp4596@kali: ~
File Edit View Terminal Tabs Help

```
geocryp4596@kali:~$ ping yahoo.com
PING yahoo.com (98.137.246.7) 56(84) bytes of data.
64 bytes from media-router-fp1.prod1.media.vip.gq1.yahoo.com (98.137.246.7): icmp_seq=1 ttl=51 time=51.2 ms
64 bytes from media-router-fp1.prod1.media.vip.gq1.yahoo.com (98.137.246.7): icmp_seq=2 ttl=51 time=50.9 ms
64 bytes from media-router-fp1.prod1.media.vip.gq1.yahoo.com (98.137.246.7): icmp_seq=3 ttl=51 time=50.7 ms
64 bytes from media-router-fp1.prod1.media.vip.gq1.yahoo.com (98.137.246.7): icmp_seq=4 ttl=51 time=50.7 ms
64 bytes from media-router-fp1.prod1.media.vip.gq1.yahoo.com (98.137.246.7): icmp_seq=5 ttl=51 time=50.9 ms
64 bytes from media-router-fp1.prod1.media.vip.gq1.yahoo.com (98.137.246.7): icmp_seq=6 ttl=51 time=50.9 ms
64 bytes from media-router-fp1.prod1.media.vip.gq1.yahoo.com (98.137.246.7): icmp_seq=7 ttl=51 time=50.8 ms
64 bytes from media-router-fp1.prod1.media.vip.gq1.yahoo.com (98.137.246.7): icmp_seq=8 ttl=51 time=50.7 ms
^C
--- yahoo.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7010ms
rtt min/avg/max/mdev = 50.651/50.861/51.209/0.172 ms
geocryp4596@kali:~$
```

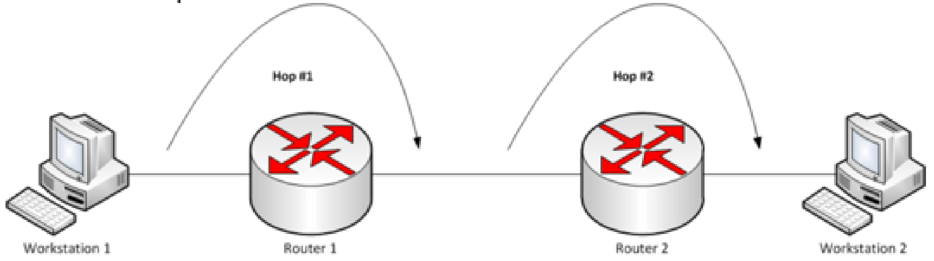
Ping – yourself via your loopback address

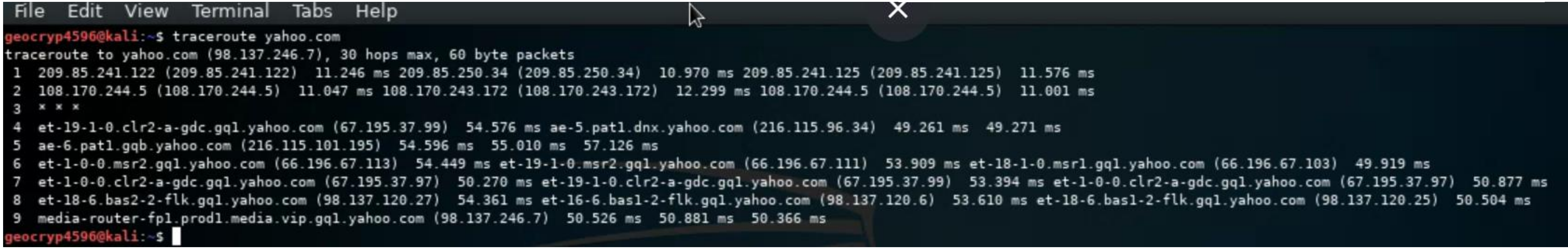
- 127.0.0.1 is a special reserved IP address, called a loopback address
- When you ping this address, you are testing your own system to make sure it is working properly
- If this IP does not return an appropriate response, the problem is with your system, not the network, nor the Internet service provider (ISP), or your target URL
- -a parameter resolves to hostname if possible



```
geocryp4596@kali:~$ ping -a 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.046 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.052 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.047 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.050 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.046 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.045 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.045 ms
64 bytes from 127.0.0.1: icmp_seq=11 ttl=64 time=0.045 ms
64 bytes from 127.0.0.1: icmp_seq=12 ttl=64 time=0.047 ms
64 bytes from 127.0.0.1: icmp_seq=13 ttl=64 time=0.047 ms
64 bytes from 127.0.0.1: icmp_seq=14 ttl=64 time=0.043 ms
^C
--- 127.0.0.1 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13290ms
rtt min/avg/max/mdev = 0.043/0.045/0.052/0.002 ms
```

Traceroute & tracert





```
geocryp4596@kali:~$ traceroute yahoo.com
traceroute to yahoo.com (98.137.246.7), 30 hops max, 60 byte packets
 1  209.85.241.122 (209.85.241.122)  11.246 ms 209.85.250.34 (209.85.250.34)  10.970 ms 209.85.241.125 (209.85.241.125)  11.576 ms
 2  108.170.244.5 (108.170.244.5)  11.047 ms 108.170.243.172 (108.170.243.172)  12.299 ms 108.170.244.5 (108.170.244.5)  11.001 ms
 3  * * *
 4  et-19-1-0.clr2-a-gdc.gq1.yahoo.com (67.195.37.99)  54.576 ms ae-5.pat1.dnx.yahoo.com (216.115.96.34)  49.261 ms  49.271 ms
 5  ae-6.pat1.gqb.yahoo.com (216.115.101.195)  54.596 ms  55.010 ms  57.126 ms
 6  et-1-0-0.msr2.gq1.yahoo.com (66.196.67.113)  54.449 ms et-19-1-0.msr2.gq1.yahoo.com (66.196.67.111)  53.909 ms et-18-1-0.msr1.gq1.yahoo.com (66.196.67.103)  49.919 ms
 7  et-1-0-0.clr2-a-gdc.gq1.yahoo.com (67.195.37.97)  50.270 ms et-19-1-0.clr2-a-gdc.gq1.yahoo.com (67.195.37.99)  53.394 ms et-1-0-0.clr2-a-gdc.gq1.yahoo.com (67.195.37.97)  50.877 ms
 8  et-18-6.bas2-2-flk.gq1.yahoo.com (98.137.120.27)  54.361 ms et-16-6.bas1-2-flk.gq1.yahoo.com (98.137.120.6)  53.610 ms et-18-6.bas1-2-flk.gq1.yahoo.com (98.137.120.25)  50.504 ms
 9  media-router-fp1.prod1.media.vip.gq1.yahoo.com (98.137.246.7)  50.526 ms  50.881 ms  50.366 ms
geocryp4596@kali:~$
```

Traceroute (Mac and Linux) and tracert (Windows) are computer network diagnostic commands for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network

- The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path); the sum of the mean times in each hop is a measure of the total time spent to establish the connection

- Traceroute proceeds unless all sent packets are lost more than twice; then the connection is considered lost and the route cannot be evaluated

Ping, on the other hand, only computes the final round-trip times from the destination point

Remainder of the class – Work on Midterm

Agenda

- ✓Mid-term question 13
- ✓OSI Reference Model
- ✓Linux commands for working with:
  - ✓Domain names
  - ✓Network availability of computers
  - ✓Mapping paths data packets take