Network Security

Network protocol security flaws

Ieaun Roberts

2016035461

Table of Contents

[Introduction 3](#_Toc26289448)

[Protocols investigated 3](#_Toc26289449)

[IP 5](#_Toc26289450)

[Flaws 7](#_Toc26289451)

[TCP 9](#_Toc26289452)

[Flaws 10](#_Toc26289453)

[UDP 11](#_Toc26289454)

[Flaws 12](#_Toc26289455)

[Mitigation 12](#_Toc26289456)

[SIP 13](#_Toc26289457)

[Flaws 14](#_Toc26289458)

[RTP 15](#_Toc26289459)

[Flaws 16](#_Toc26289460)

[VoIP 17](#_Toc26289461)

[Flaws 17](#_Toc26289462)

[Conclusion 19](#_Toc26289463)

[References 20](#_Toc26289464)

[Appendix 23](#_Toc26289465)

[UDP 23](#_Toc26289466)

[1.1) OSI model 23](#_Toc26289467)

[1.2) 3-way-handshake 23](#_Toc26289468)

[1.3) TCP VS UDP 24](#_Toc26289469)

# Introduction

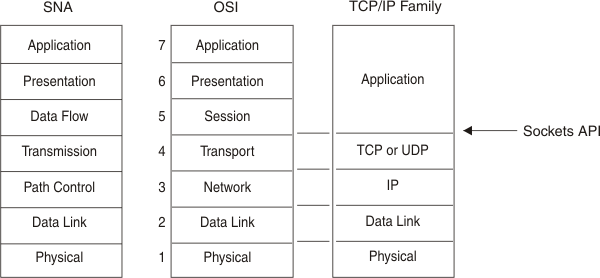
The ability to communicate with someone across the globe is a service that once had a very heavy price tag attached to it. As an individual who grew up in Africa with much of my family across the planet in the Europe, the transition from traditional telephony systems making use of circuit switching to allocate channels for each call, to the disruptive technology making use of Voice over Internet Protocol (VoIP) is one that I was able to fully utilize and immediately benefit from once implemented in the mainstream.

This report covers the main protocols used in any traditional VoIP system along with the vulnerabilities and possible mitigation techniques that may be used to secure a system implementing said protocols.

Report Structure

This report is laid out in a bottom up approach according to the OSI model, starting with the network layer protocol IP, discussing 2 Transport layer protocols (UDP and TCP) and finally ending with 2 interconnected protocols that are needed for VoIP operations along with the VoIP protocol itself.

This approach allows the reader to get a general understanding of the material from a higher level of abstraction before delving deeper into the main protocol of the report, VoIP.



(IBM, n.d.) *SNA /OSI/IP Models*

What types of attacks are touched within this report?

* IP Spoofing
* Dos Attacks
* Brute Force Attacks
* Man-in-the-Middle
* Sequence Manipulation
* Tear drop attack
* SYN, UDP and SIP flood attacks

## Protocols investigated

1. IP
2. TCP
3. UDP
4. RTP
5. SIP
6. VoIP

## IP

What is it?

The Internet Protocol (IP) is the core protocol concerned with delivery of packets of data (also called datagrams) between 2 interconnected systems from source to destination across network boundaries. It provides a means of **universally addressing** different machines on a network, data encapsulation of other protocols (TCP/IP and UDP/IP), **packet fragmentation** and reassembly.

IP is referred to as a connectionless protocol as it is only interested in sending a datagram from machine A to Machine B (setup and send).(Rey, 1981)(Kozeirok, 2005)

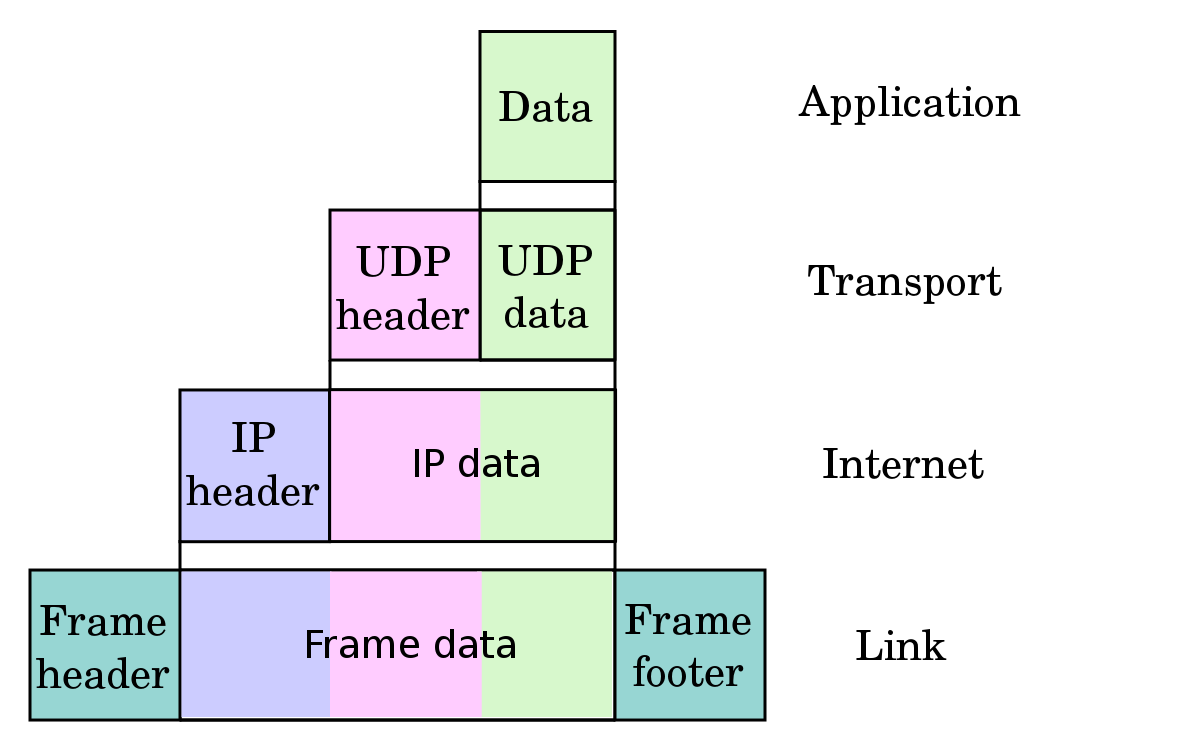
Other protocols discussed later extend the functionality of the IP packets to be connection oriented, relying on a Machine B to confirm a connection has been made before Machine A can start sending data and have means of error checking and packet ordering.(cloudflare, n.d.)

Goal: *“Delivery of datagrams from one device to another over an internetwork”*

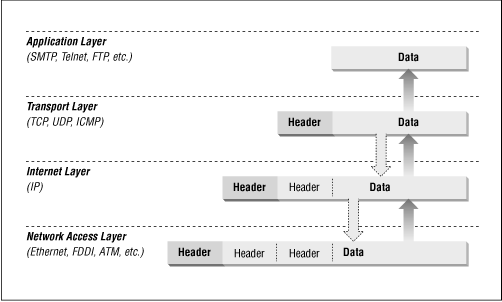
IP is an internet layer protocol. *[Appendix 1.1].*

How does it work?

* Addressing – contains a mechanism for uniquely addressing devices over a large network.
* Fragmentation and reassembly – Splits larger packets to meet network needs and reassembles them on arrival.
* Encapsulation – IP accepts UDP or TCP data and reformats it prior to transmission.

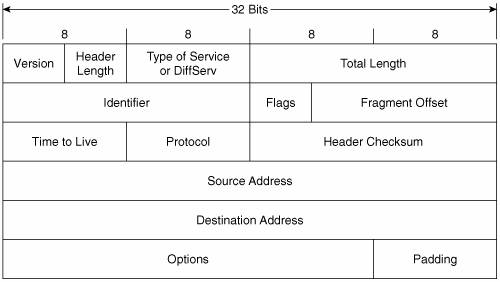


(WikiPedia, 2019)



(Associates., 1999)

Packet structure?



(Jeff Doyle, 2005) *IP packet structure*

Packet headers

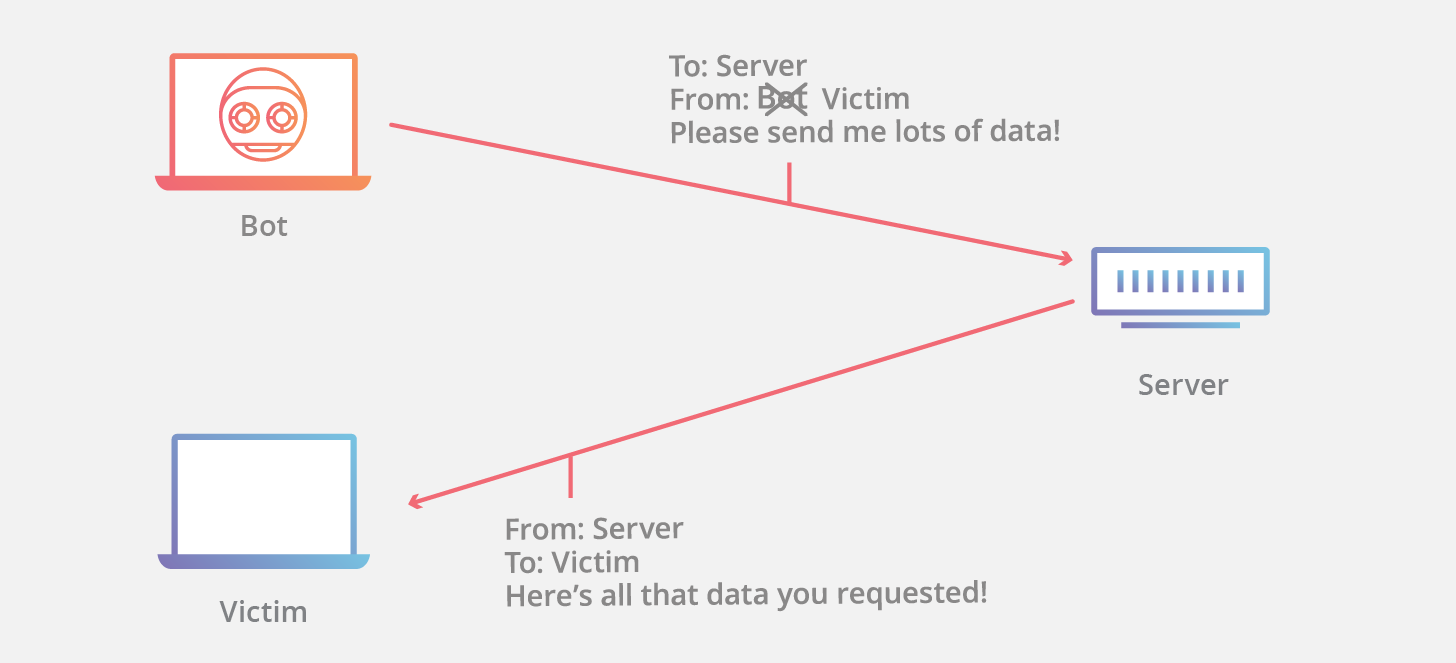
As packets are transferred across different layers *[appendix 1.1]* theytake with them headers that each contain different data to perform protocol specific tasks. One of the main focal points of the IP packet would be the Source and Destination IP addresses (e.g 192.0. 2.1) which determines where we send a packet.

### Flaws

Common attacks:

IP spoofing

A cyber security attack in which the attacker impersonates another trusted system using a modified IP packet within which the original source address has been altered to a trick another computer system to transmit data to a victim. (cloudflare, n.d.)(kaspersky, n.d.)

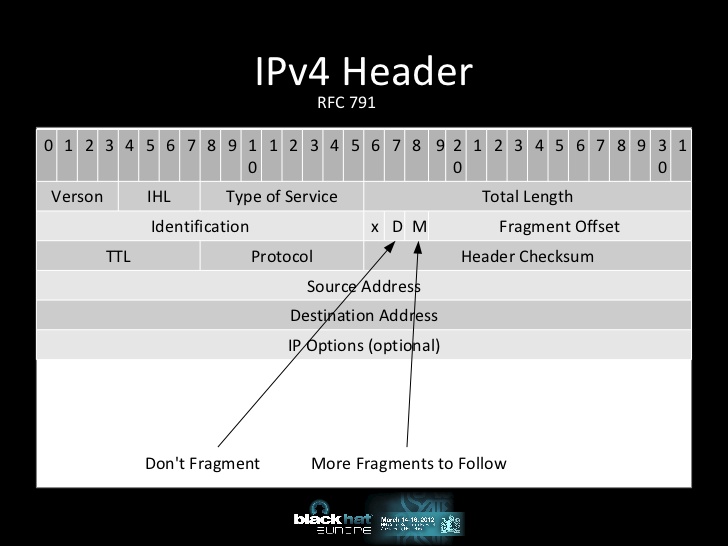


(cloudflare, n.d.)

Dos Attacks

IP spoofing is most common in Dos (**Denial of service**) attacks where attackers attempt to overwhelm a victim and render their machine unusable with as many packets a possible in a short amount of time. With packets coming from multiple sources, it is nearly impossible to block hosts at the scale these types of attackers use and challenging to identify perpetrators of these types of attacks.

(Tanase, 2003)(kaspersky, n.d.)



(Atlasis, 2012)

Vulnerabilities

1. As discussed, IP packets have a mechanism to split larger datasets up into smaller datagrams when the size of the packet is larger than the maximum transmission unit (MTU) of the route. Whether or not a packet is fragmented, and its fragment ID number is stored in the header *[Appendix ??].* Attackers abuse the mechanism in place to transmit fraudulent packets (unordered, overlapping, incomplete, too small) that the machine will not be able to reassemble to consume resources in an attempt to disrupt and disable. This is a form of DoS attack.(Atlasis, 2012) (imperva, n.d.)(NordVPN Black, 2019)

Mitigation

1. The most common methods for mitigation against these type of DOS attacks include, taking measures to ensure that malicious packets never reach the target machine by inspecting incoming packets and ensuring they do not violate fragmentation rules. This can be implemented within a secure proxy server (an intermediary for client and server interactions). Users should also make use of black/white listing to filter traffic based on IP and patterns (imperva, n.d.)(NordVPN Black, 2019)
   1. Make sure your OS is up to date
   2. Make use of firewalls and intrusion detection systems.
   3. IPv6 removed the “don’t fragment” and “more fragments to follow” fields from its header.

## TCP

What is it?

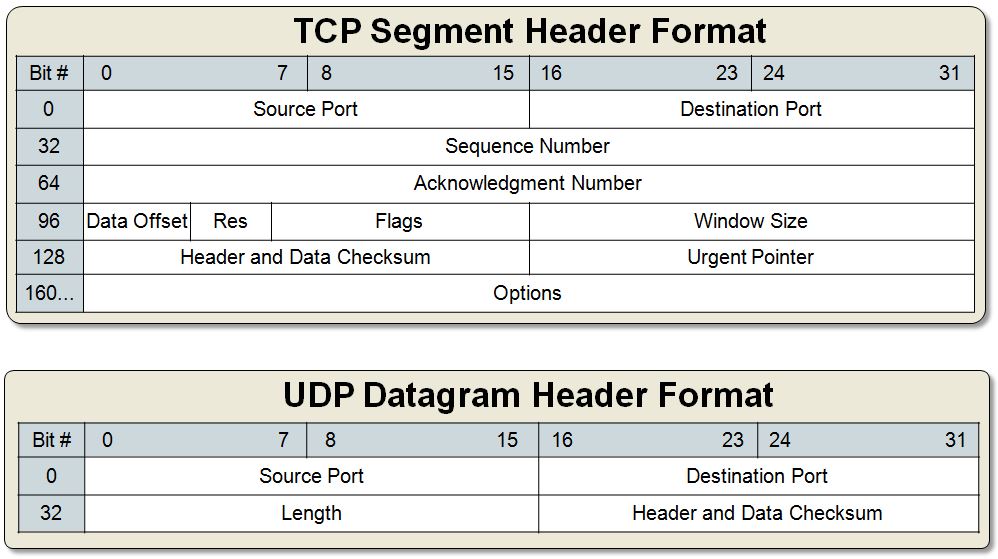
Transmission Control Protocol along with UDP (discussed next) are the main protocols in the IP suite. TCP is a connection-oriented protocol that allows devices to facilitate communication through an established end-to-end channel.

TCP introduces mechanisms to number the packets it is sending to another device, mechanisms to acknowledge the recipient has received a packet and mechanisms to specify a port (endpoint in recipients’ machine). (cloudflare, n.d.)(Rouse, n.d.)

TCP is a transport layer protocol. *[Appendix 1.1].*

Goal: “Allow computers to reliably communicate over networks”

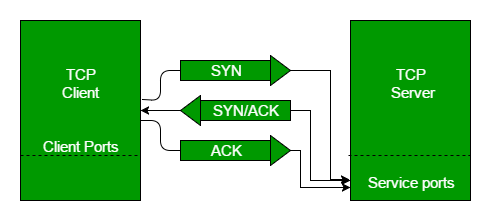
Packet structure?



(skminhaj, 2016)

How does it work?

Connection – The client starts by sending a TCP packet to the server (device we want to connect to). This packet has a value in the “flags” field of the header (see above) to inform the recipient that it wants to perform a SYN (Synchronize sequence number) and will likely want to start a communication channel. The server then returns an SYN +ACK (flag value) to acknowledge that it has received the SYN as well as what the initial sequence number is going to be. One final ACK is sent to the serve to acknowledge that the SYN + ACK was received and a connection is opened to start the data transfer(geeksforgeeks, n.d.). (cloudflare, n.d.)

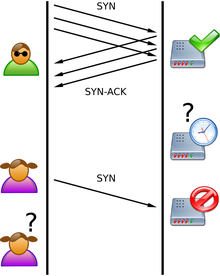
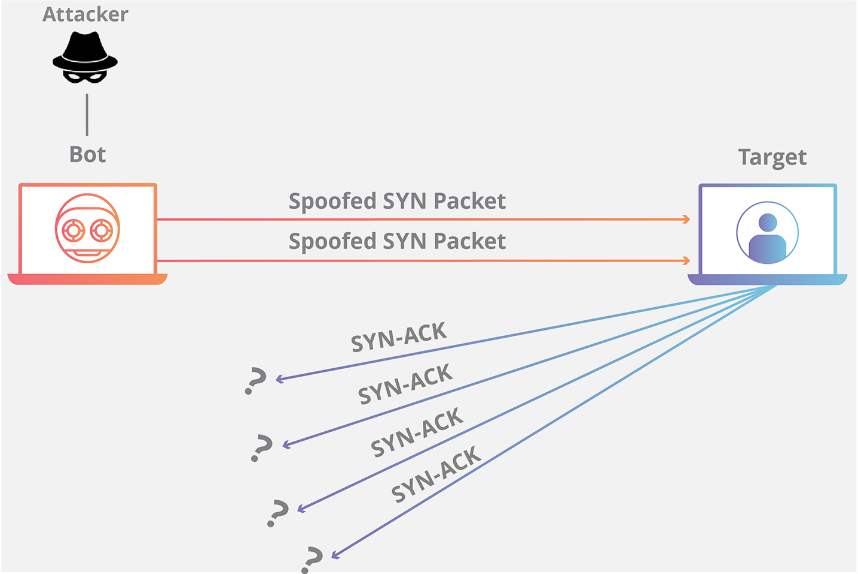


(geeksforgeeks, n.d.)

### Flaws

Vulnerabilities

1. TCP is vulnerable to a special type of fragmentation attack known as the **Teardrop Attack**. In this attack (which is a form of DOS attack) perpetrators send a machine incomplete packets that it cannot reassemble with intentionally altered fragmentation offsets which slowly accumulate, overlapping each other and consuming vast amounts of resources. (Shekhar, 2016)
2. Due to the mechanism that increases the sequence number used in TCP packets at a constant rate, it is possible for attackers to forge packets and step into the communication stream posing as the original sender of the packet. Attacks that make use of this vulnerability are known as **Sequence manipulation** / prediction attacks.
3. The 3-way handshake mechanism used in TCP can be abused in a **SYN Flooding** attack. When a client requests a connection to be set up as described on the previous page, the server it is communicating with is required to respond to them and then listen for an ack. This requirement is abused in this form of DOS attack which makes use of multiple false addresses to request connection setup to a target machine to deplete the machines resources and possibly lock out any connection requests from legitimate users of the system being attacked.(finjan, n.d.)



(Anon., 2019)

Mitigation

1. Make use of up to date networking devices that are able to detect incomplete packets and drop problem packets.
2. It is possible to guard against sequence manipulation attacks by setting the initial sequence number increment value to a generated random number.
3. RFC 4987 lists numerous counter measures to **SYN flooding** attacks most notably implementing a recycling system which overwrites the oldest “half open” connection after a certain point to ensure resources don’t reach a point where it could impact the quality of the service. Using this method, connections can be established faster than resources can be consumed by SYN flooding (cloudflare, n.d.)
   1. The use of a proxy server (server in between sender and recipient) is another favorable method that can be used to mitigate SYN Attacks by outsourcing this flaw to a system with more resources to handle it effectively.

## UDP

What is it?

User Datagram Protocol is a relatively quick, connectionless, minimalist transport layer protocol *[Appendix 1.1]* used to transmit data from one point to another, often used as an alternative to TCP when transmission speed is mission critical.(IBM, n.d.)

UDP is a transport layer protocol. *[Appendix 1.1].*

Goal: “Allow computers to quickly communicate over networks”

How does it work?

Encapsulated within IP datagrams, UDP sends packets as quickly as possible without regarding the order of packets sent, duplicate packets or packets being lost from one source to another. Data that is sent include source and destination ports.

UDP is connectionless because it does not require another host to signal that it is listening before it starts to send its data.

Sender - Data is sent to a port without any regard to whether the recipient has received it.

Recipient – Listens for any incoming data on a port.

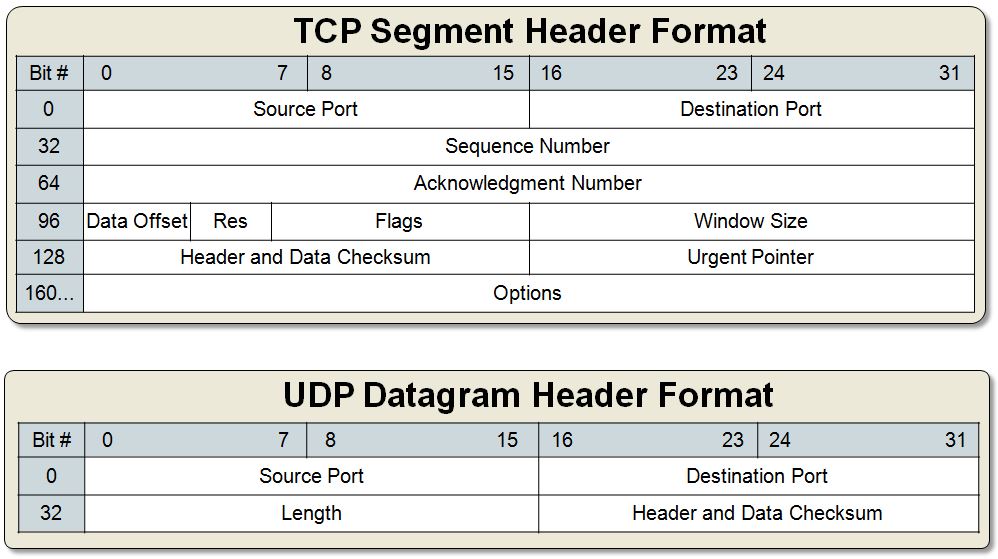
(RFC 768, 28 August 1980)(Rouse, n.d.)

Compared to TCP?

Both UDP and TCP make use of the Internet Protocol (IP) within which they are encapsulated. UDP is considered simpler. UDP manages to improve on speed by forgoing the end-to-end connection used by TCP, characterized by 3-way-handshakes to set up connections *[Appendix 1.2]* and acknowledgements of packets received. UDP is ideal in real-time application scenarios where latency is a higher priority than any individual packets data. For more difference see *[Appendix 1.3].*

Packet structure?

In the figure below visualizing the UDP datagram, note the absence of the fields for “Sequence number” and “Acknowledgement Number”.



(skminhaj, 2016)

In the figure above it is evident that UDP packets have less overhead when considering the amount of metadata used to further describe the TCP packet. This smaller size decreases the amount of bandwidth needed for each packet.

### Flaws

Many of the prominent flaws of UDP are related to its very design. Any application running over UDP would need to deal directly with communication issues that a connection-oriented protocol like TCP would have handled such as retransmission and reassembly of packets.(RFC 1122, 1989)

Vulnerabilities

1. Abusing the fact that recipients of UDP blindly accept packets on a given port with nothing in terms of IP address validation built in to the protocol, attackers can send packets that appear to be originating from a trustworthy address that the recipient is listening for, this is known as **IP spoofing** which often goes hand in hand with a **DoS attack**. (David, 2018)
2. Due to the connectionless nature of UDP communication, it is vulnerable to an attack that when used effectively, receives small sized packets and sends out exponentially larger sized responses (attacker sends 1-byte request, victim responds with 100-byte response/ attacker sends 1 packet, victim responds with 5). This is known as **UDP amplification**.Coupled with multiple device participating in the attack, this type of attack can be used to severely impact bandwidth. This is specifically prevalent in the UDP protocol as there is no verification if the sender of a packet has any malicious intent before sending a response, resulting in blind responses. This coupled with **IP spoofing** can be used to reflect large amounts of data to a victim’s system in a DoS attack and **DDoS** (Distribute Dos, making use of multiple sources to overwhelm a system). *(Hart, 2016)* (RFC 768, 1980)(secplicity, 2018)

Mitigation

1. A considerable mitigation method would be the implementation at an Internet Service Provider (ISP) level rejection of any identifiably spoofed IP addresses, methods on how to go about doing this include filtering network traffic and rejecting packets who’s addresses are not reachable by following the actual packets path. This type of filtering is known as **ingress filtering**. (Sunhux, 2014)

## SIP

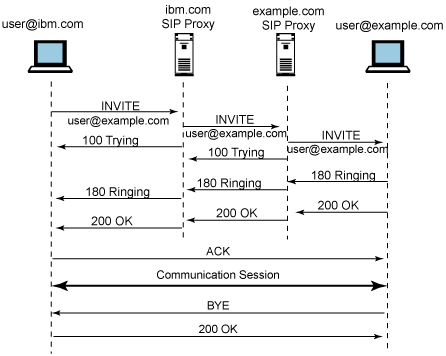
What is it?

Session initiation protocol is a peer-to-peer signaling protocol used to control communication sessions. It does this by initiating, maintaining, modifying (change IP/Port/Stream) and terminating sessions that typically make use of voice or video calls over the internet. SIP is expandable and is not restricted to any specific media type. (Voip-Mechanic, n.d.)(Metaswitch, n.d.)

SIP is an application layer protocol. *[Appendix 1.1].*

Goal: “The job of SIP is to set up an interactive communication session and terminate it when it’s over” (Harris, 2016)

How does it work?



(DavideCisco, 2013)

Basic messages used within the session initiation protocol include:

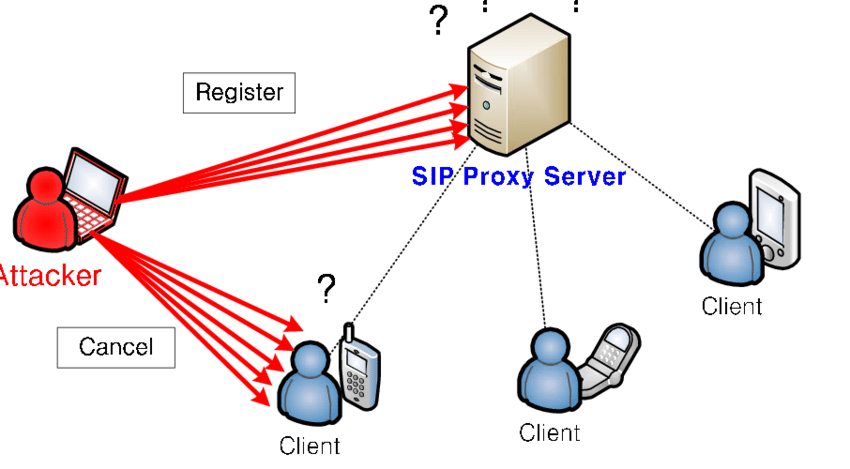
* Invite – Session establishment request
* ACK – Acknowledge the device has received SIP INVITE response
* BYE – Terminate session
* CANCEL – Terminate a requested INVITE that has yet to receive an answer

SIP Packets are typically carried by UDP, however as with RTP, TCP variants do exist.

### Flaws

Vulnerabilities

1. Whether SIP is transmitted using UDP or TCP, the traffic related to the protocol which contains sensitive data regarding an RTP stream is often in plain / clear text within the UDP or TCP packet.(Jordan, 2017)
2. As a SIP communication session starts with a similar pattern as a TCP 3-way handshake it can be abused in the same manner with multiple false half opened invites consuming system resources, this is referred to as **SIP Register Flooding.** *(Fadi El-moussa, 2010)*



*(Lee, 2009)*

Mitigation

1. Encrypt as much of the SIP traffic as possible to mitigate the risk of malicious attackers intercepting sensitive data and ensure secure transmission.

## RTP

What is it?

Real-Time Transport Protocol defines how devices transmit media (such as audio and video) in real time over IP networks and is heavy used in streaming entertainment systems. The protocol includes within it means to detect packet loss and out of order delivery with the inclusion of a sequence number and timestamp field in the header. The protocol is implemented with a concatenation over integrity of data ethos and can be thought of as an add-in to enable UDP to gain more information about transmitted and received packets (sequence number and timestamps).

RTP is often connectionless and is encapsulated within UDP packets due to their fast delivery and the protocols real time priority, however variants of the protocol do exist that make use of TCP. It is worth noting that multiplexing (combining data into one channel, often needed when resources are scarce) is a feature of UDP that makes it more desirable in an RTP context to TCP.(extrahop, n.d.)(RFC, 2003)

RTP is an application layer protocol.

Goal: “Ensure a uniform way to transmit multimedia data subject to real-time constraints”

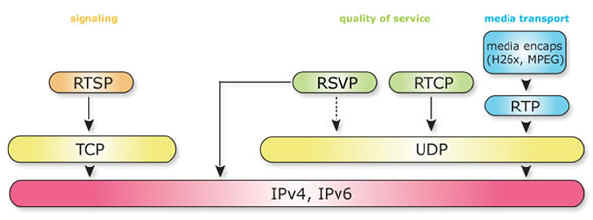
How does it work?

To achieve the end goal of streaming media from one end point to another, RTP must be used in conjunction with other signaling protocols such as SIP or **RTSP** that perform tasks such as signaling (establish connections and initiate sessions) and Real-time transport control protocol (**RTCP**) that oversees the quality of the RTP stream flow by counting the amount of packets sent and packet size.

In operation, RTP transmits media streams between two end points in a full duplex manner (bother directions simultaneously).

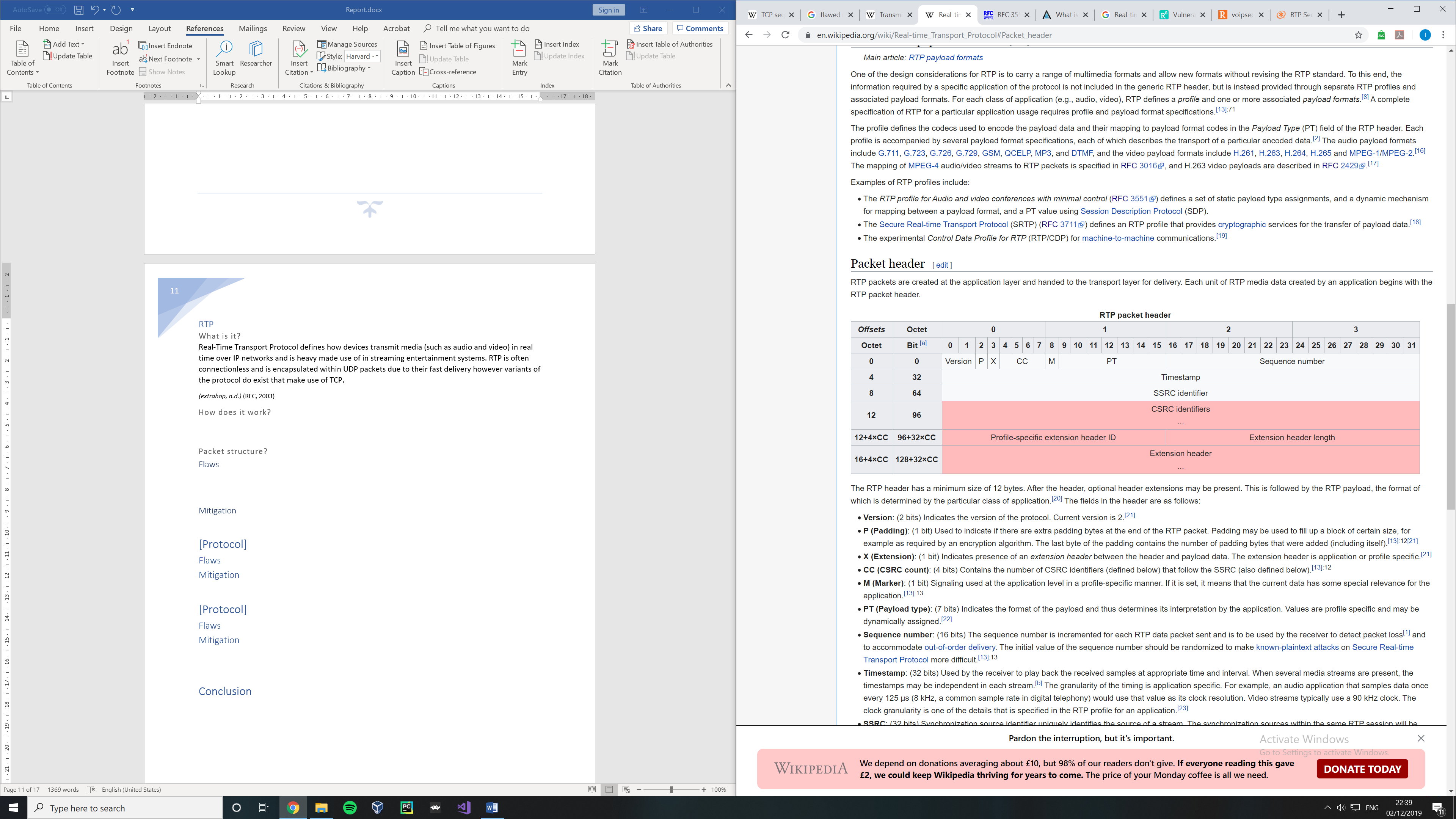
A sender encodes the media data they wish to transmit with each iteration increasing the sequence and timestamp values.

A receiver notes any missing packets and decodes the data according to the encoding method used (e.g. Jpeg, H264 …) and presents the stream to the user. Multiple receivers can view a stream from a single sender.(Hartpence, n.d.)(RFC, 2003)



(Mousavi, 2019)

Packet structure?



(wikipedia, 2019)

The RTP packet contains fields specifying the codec (PT – Payload type), source identifier which uniquely identifies the source of the stream (SSRC) and the data itself.

### Flaws

Vulnerabilities

1. Real-Time Transport Protocol does not on its own have any form of **authentication** procedures, so verification that a packet is coming from the intended source is not possible.(Jordan, 2017)
2. RTCP is built into RTP and reports statistics about the current session, this includes data such as number of participants and their identities. This data (in plain text) is compressed within the packet.
3. Protocols making use of compression techniques could be exposed to DOS attacks exploiting the fact that each packet payload will require computational resources to decompress, overloading the recipient.

Mitigation

1. The RFC recommends any device making use of RTP to also keep track of who has sent the packets. In the case that suddenly, **received packets are coming from a new source, then** **do not accept** them until the source can be validated somehow depending on the application.
   1. Drop packets that are not the same as the original source IP/ Port.
      1. 1 connection, 1 stream.(Jordan, 2017)
2. Encrypt confidential data after compression.

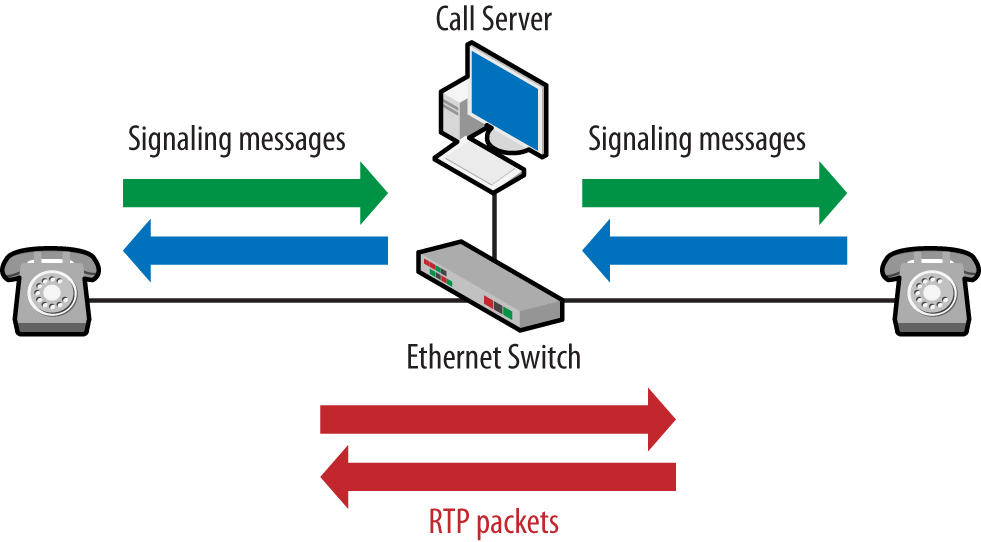
## VoIP

What is it?

Voice over internet protocol (VoIP) is used to transmit audio and video over internet protocol (IP) based networks*.*

(oreilly, n.d.)(Voip-Mechanic, n.d.)

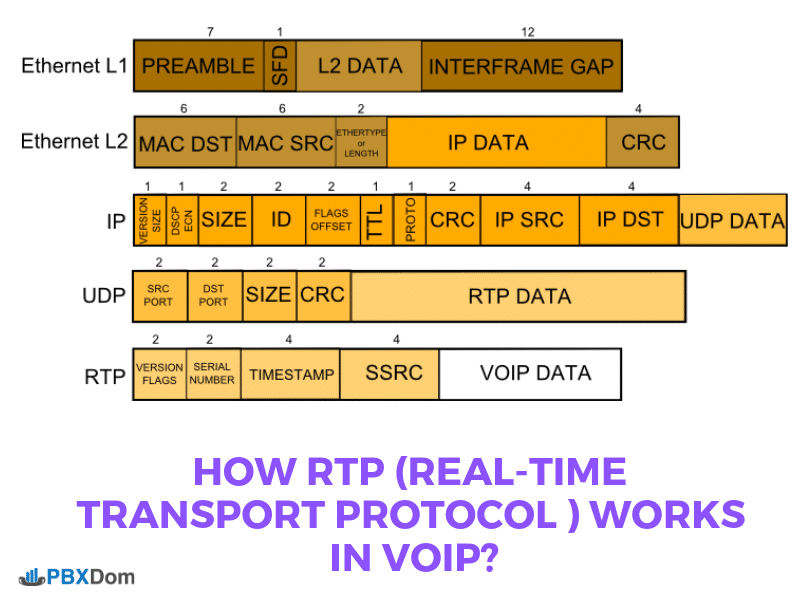
How does it work?



(oreilly, n.d.)

VoIP makes use of each of the protocols mentioned earlier in the report to facilitate its operation. Although other means exist RTP is the most widely accepted means of transporting multimedia packets in this context.

Packet structure?



(Mousavi, 2019)

### Flaws

Vulnerabilities

Mitigation

# Conclusion

* Do not transmit sensitive data that can be used to identify any individual machine or entity in clear or plain text. This data is very easily intercepted by low level attackers.
* Try to use methods of authenticating packets whenever possible.
* Use proxy servers to put a layer of protection in between any possible attackers and mission critical devices.

# References

Anon., 2019. *Wikipedia.* [Online]   
Available at: https://en.wikipedia.org/wiki/SYN\_flood#:~:targetText=A%20SYN%20flood%20is%20a,system%20unresponsive%20to%20legitimate%20traffic.  
[Accessed 2019].

Associates., O. &., 1999. *http://web.deu.edu.tr.* [Online]   
Available at: http://web.deu.edu.tr/doc/oreily/networking/firewall/ch06\_03.htm  
[Accessed 2019].

Atlasis, A., 2012. *Blackhat europe.* Amsterdam, Blackhat .

blackmagicboxes, N/A. *https://www.blackmagicboxes.com.* [Online]   
Available at: https://www.blackmagicboxes.com/wp-content/uploads/2016/12/Network-Protocols-Map-Poster.jpg  
[Accessed 2019].

Cisco, 2006. *https://www.cisco.com.* [Online]   
Available at: https://www.cisco.com/c/en/us/support/docs/security-vpn/kerberos/16087-1.html#whatisit  
[Accessed 2019].

cloudflare, n.d. *https://www.cloudflare.com.* [Online]   
Available at: https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/  
[Accessed 2019].

cloudflare, n.d. *https://www.cloudflare.com.* [Online]   
Available at: https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/  
[Accessed 2019].

cloudflare, n.d. *https://www.cloudflare.com.* [Online]   
Available at: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/  
[Accessed 2019].

cloudflare, n.d. *www.cloudflare.com.* [Online]   
Available at: https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/  
[Accessed 2019].

David, 2018. *https://www.cryptologie.net.* [Online]   
Available at: https://www.cryptologie.net/article/449/problems-that-udp-and-only-udp-has/  
[Accessed 2019].

DavideCisco, 2013. *http://davidecisco.blogspot.com.* [Online]   
Available at: http://davidecisco.blogspot.com/2013/06/session-initiation-protocol-sip.html  
[Accessed 2019].

extrahop, n.d. *https://www.extrahop.com.* [Online]   
Available at: https://www.extrahop.com/resources/protocols/rtp/  
[Accessed 2019].

finjan, n.d. *https://blog.finjan.com.* [Online]   
Available at: https://blog.finjan.com/tcpip-vulnerabilities/  
[Accessed 2019].

geeksforgeeks, n.d. *https://www.geeksforgeeks.org.* [Online]   
Available at: https://www.geeksforgeeks.org/tcp-3-way-handshake-process/  
[Accessed 2019].

Harris, D., 2016. *https://www.softwareadvice.com.* [Online]   
Available at: https://www.softwareadvice.com/resources/what-is-sip/  
[Accessed 2019].

Hartpence, B., n.d. *https://www.oreilly.com.* [Online]   
Available at: https://www.oreilly.com/library/view/packet-guide-to/9781449339661/ch04.html  
[Accessed 2019].

IBM, n.d. *https://www.ibm.com.* [Online]   
Available at: https://www.ibm.com/support/knowledgecenter/en/SSLTBW\_2.2.0/com.ibm.zos.v2r2.halc001/ipcicint\_protocol.htm  
[Accessed 22 11 2019].

imperva, n.d. *https://www.imperva.com.* [Online]   
Available at: https://www.imperva.com/learn/application-security/ip-fragmentation-attack-teardrop/#:~:targetText=IP%20fragmentation%20attacks%20are%20a,by%20exploiting%20datagram%20fragmentation%20mechanisms.&targetText=If%20a%20datagram%20is%20being,order%20to%20be%20  
[Accessed 2019].

Jeff Doyle, J. C., 2005. *Routing TCP/IP, Volume 1 (2nd Edition).* s.l.:s.n.

Jordan, M., 2017. *https://blogs.asterisk.org.* [Online]   
Available at: https://blogs.asterisk.org/2017/09/27/rtp-security-vulnerabilities/  
[Accessed 2019].

kaspersky, n.d. *usa.kaspersky.com.* [Online]   
Available at: https://usa.kaspersky.com/resource-center/threats/ip-spoofing  
[Accessed 2019].

Kozeirok, C. M., 2005. *http://www.tcpipguide.com/.* [Online]   
Available at: http://www.tcpipguide.com/free/t\_IPOverviewandKeyOperationalCharacteristics.htm  
[Accessed 2019].

Masetic, Z., 2017. *https://www.researchgate.net.* [Online]   
Available at: https://www.researchgate.net/figure/TCP-three-way-handshake\_fig3\_321698222  
[Accessed 2019].

Metaswitch, n.d. *https://www.metaswitch.com/knowledge-center/reference/what-is-session-initiation-protocol-sip.* [Online]   
Available at: https://www.metaswitch.com/knowledge-center/reference/what-is-session-initiation-protocol-sip  
[Accessed 2019].

MIT, 2019. *http://web.mit.edu/kerberos/.* [Online]   
Available at: http://web.mit.edu/kerberos/  
[Accessed 2019].

Mousavi, R., 2019. *https://www.pbxdom.com.* [Online]   
Available at: https://www.pbxdom.com/how-rtp-real-time-transport-protocol-works-in-voips  
[Accessed 2019].

NordVPN Black, P., 2019. *https://nordvpn.com.* [Online]   
Available at: https://nordvpn.com/blog/ip-fragmentation-attack/  
[Accessed 2019].

oreilly, n.d. *https://www.oreilly.com.* [Online]   
Available at: https://www.oreilly.com/library/view/packet-guide-to/9781449339661/ch01.html  
[Accessed 2019].

Rey, M. d., 1981. DARPA INTERNET PROGRAM. *RFC 791,* Issue 791, p. 45.

RFC 1122, R., 1989. *http://www.networksorcery.com/enp/rfc/rfc1122.txt.* [Online]   
Available at: http://www.networksorcery.com/enp/rfc/rfc1122.txt

RFC 768, P. J., 28 August 1980. *RFC 768,* s.l.: ISI.

RFC, H. S., 2003. *https://tools.ietf.org.* [Online]   
Available at: https://tools.ietf.org/html/rfc3550  
[Accessed 2019].

Rouse, M., n.d. *https://searchnetworking.techtarget.com.* [Online]   
Available at: https://searchnetworking.techtarget.com/definition/UDP-User-Datagram-Protocol#:~:targetText=UDP%20(User%20Datagram%20Protocol)%20is,between%20applications%20on%20the%20internet.

Shekhar, A., 2016. *https://fossbytes.com.* [Online]   
Available at: https://fossbytes.com/what-is-teardrop-attack-working/  
[Accessed 2019].

skminhaj, 2016. *https://skminhaj.wordpress.com.* [Online]   
Available at: https://skminhaj.wordpress.com/2016/02/15/tcp-segment-vs-udp-datagram-header-format/  
[Accessed 2019].

Sunhux, 2014. *https://www.experts-exchange.com/questions/28360739/UDP-protocols'-vulnerabilities.html.* [Online]   
Available at: https://www.experts-exchange.com/questions/28360739/UDP-protocols'-vulnerabilities.html  
[Accessed 2019].

Tanase, M., 2003. *https://www.symantec.com.* [Online]   
Available at: https://www.symantec.com/connect/articles/ip-spoofing-introduction  
[Accessed Novemeber 2019].

Voip-Mechanic, n.d. *https://www.voipmechanic.com.* [Online]   
Available at: https://www.voipmechanic.com/sip-basics.htm  
[Accessed 2019].

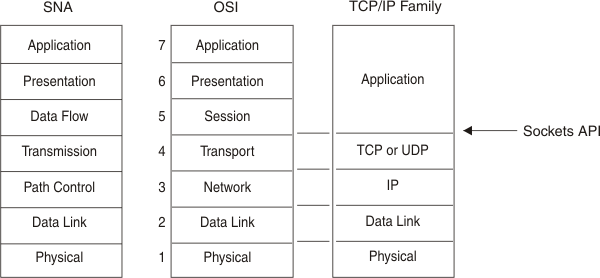
wikipedia, 2019. *https://en.wikipedia.org.* [Online]   
Available at: https://en.wikipedia.org/wiki/Real-time\_Transport\_Protocol#Packet\_header  
[Accessed 2019].

WikiPedia, 2019. *https://en.wikipedia.org.* [Online]   
Available at: https://en.wikipedia.org/wiki/Internet\_Protocol  
[Accessed 2019].

# Appendix

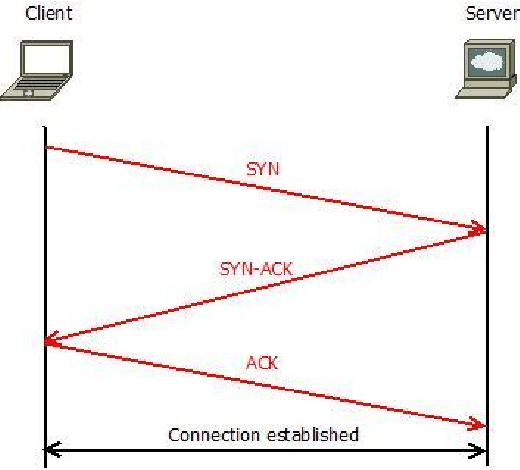
## UDP

### OSI model



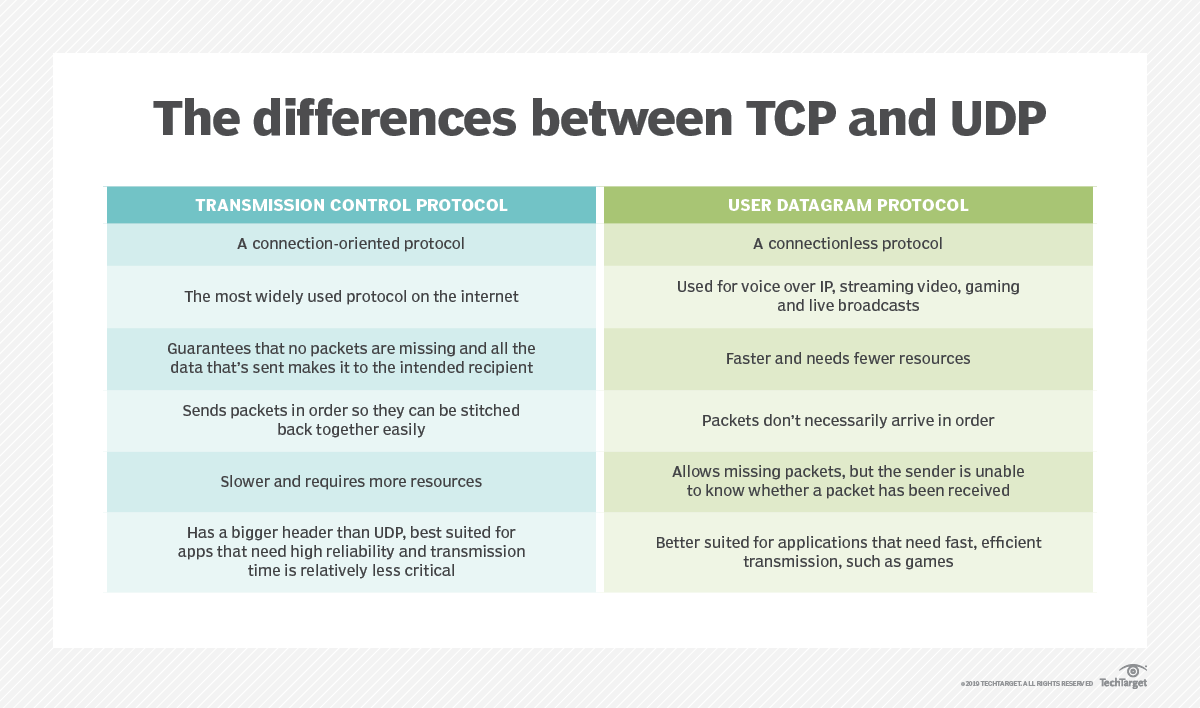
(IBM, n.d.)

### 3-way-handshake

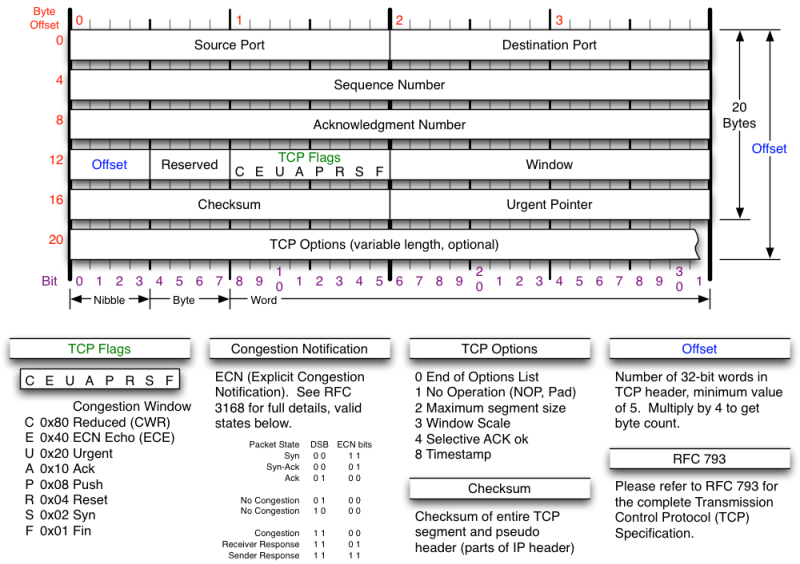


(Masetic, 2017)

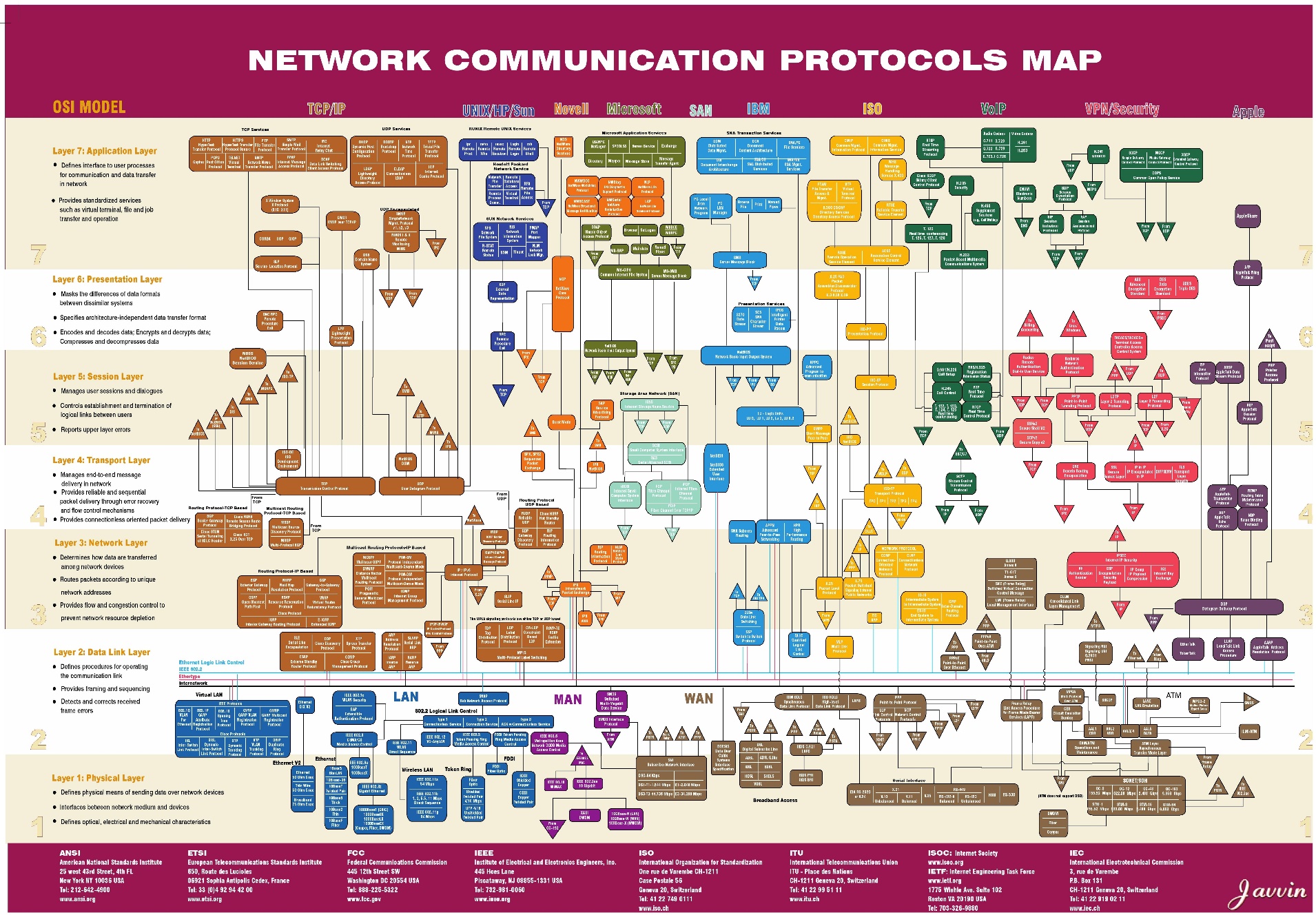
### TCP VS UDP



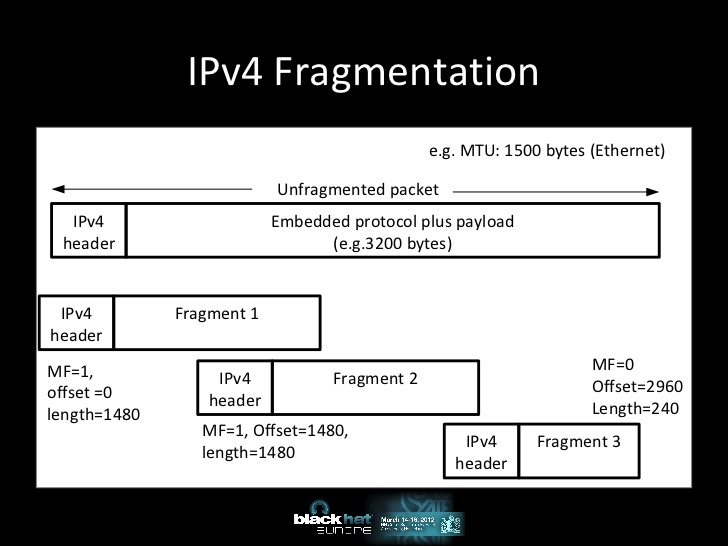
(Rouse, n.d.)



(skminhaj, 2016)



(blackmagicboxes, N/A)



(Atlasis, 2012)