NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Networking Communication Protocols

Cloud Infrastructure Engineering

Nanyang Technological University & Skills Union - 2022/2023

Course Content

- Quick Check-In
- Dive into the basics of Network Communications
    - Network Communication Protocols
    - Network Management Protocols
    - Network Security Protocols
- Differentiate how the communication works
- Call an Open API using Postman to better understand about HTTP/HTTPS as part of network communications

Time	What	How or Why
7:10pm - 7:30pm	Part 1 - Presentation	Network Communication Protocol + Activity
7:30pm - 7:50pm	Part 2 - Presentation	Network Management Protocol + Activity
7:50pm - 8:00pm	Review	Learners to review topics 1 and 2
8:00pm - 8:05pm	Break	
8:05pm - 8:25pm	Part 3 - Presentation	Network Security Protocol + Activity
8:25pm - 8:45pm	Postman API Activity	Learners explore hands-on open API
8:45pm - 8:55pm	Break	
8:55pm - 9:00pm	Assignment Briefing	
9:00pm - 9:50pm	Learners self attempt on assignments	
9:50pm - 10:00pm	Instructors assist learners to push changes to remote repository	

Recap

- Networking hardware
  - Router, Hub, Switch
- Types of Network
  - PAN, LAN, WLAN, MAN, WAN
- Unique Identifiers of Networking
  - IP, DNS, Sockets
- Goals of Networking

Self Study Check-In

Q1) What does HTTP stand for?

A) Hypertext Transfer Protocol
B) Hypertransfer Text Protocol
C) Hypertransmition Text Protocol
D) Hypertransport Transfer Protocol

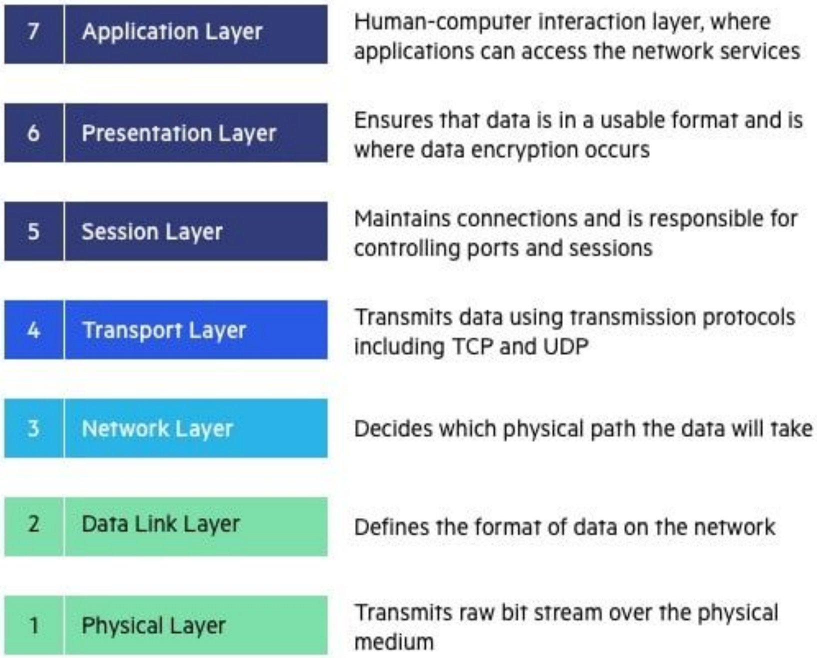
Q2) All browsers are strongly encouraging users to trust only websites implementing HTTPS because this is the single measure that can help them mitigate a variety of threats and attacks.

A) True

B) False

Network Communication Protocol

OSI (Open Systems Interconnection) Model



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

What is Network Communication?

Network communication, or internetworking, **defines a set of protocols** (that is, rules and standards) that **allow application programs to talk with each other** without regard to the hardware and operating systems where they are run.

Internetworking allows application programs to communicate independently of their physical network connections.

What is Network Communication?

What is Network Communication?

Communication protocols also **handle authentication and error detection**, as well as the syntax, synchronization, and semantics, that both analog and digital communications must abide to function.

Key Network Communication Protocols

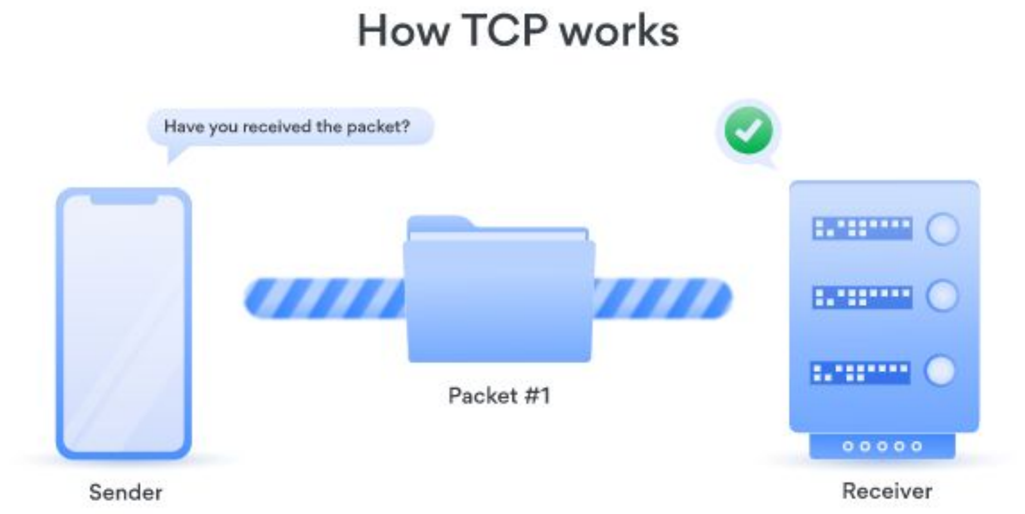
- TCP
- UDP
- HTTP
- FTP

TCP (Transmission Control Protocol)

Enables application programs and computing devices to **exchange messages over a network**.

It is designed to send **packets** across the internet and ensure the successful delivery of data and messages over networks.

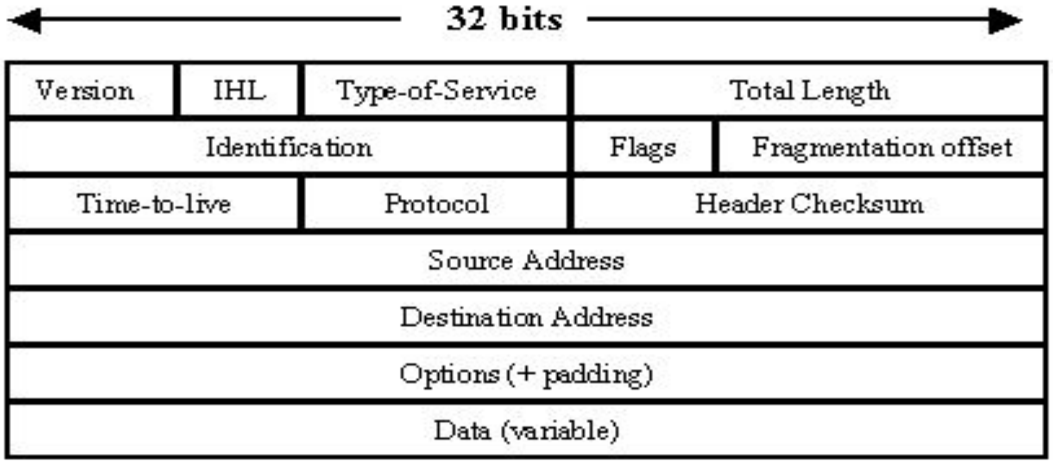
TCP (Transmission Control Protocol)



Recap: What is a Packet?

In networking, a packet is a **small segment of a larger message**. Data sent over computer networks*, such as the Internet, is divided into packets. These packets are then recombined by the computer or device that receives them.

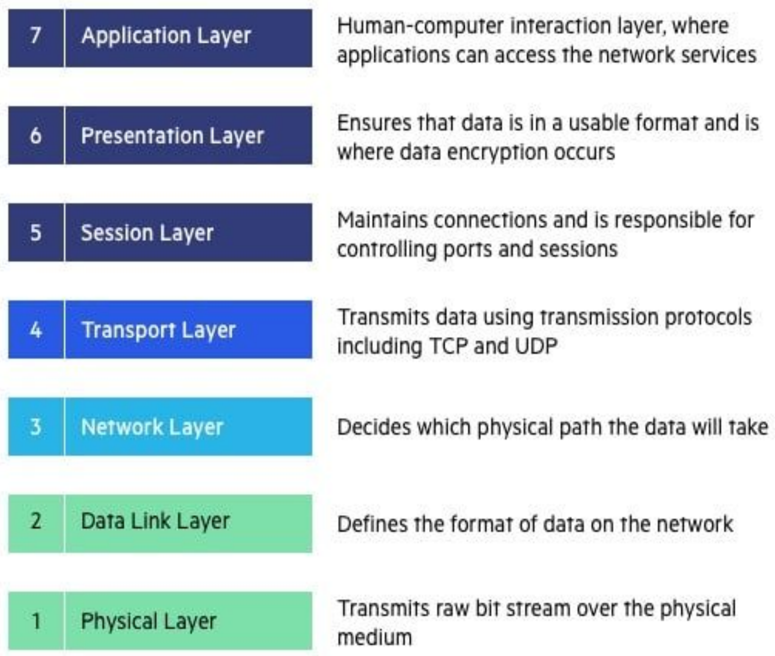
Recap: What is a Packet?



32 bits

<table>
<tr><td>Version</td><td>IHL</td><td>Type-of-Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragmentation offset</td></tr>
<tr><td colspan="2">Time-to-live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">Options (+ padding)</td></tr>
<tr><td colspan="5">Data (variable)</td></tr>
</table>

OSI (Open Systems Interconnection) Model



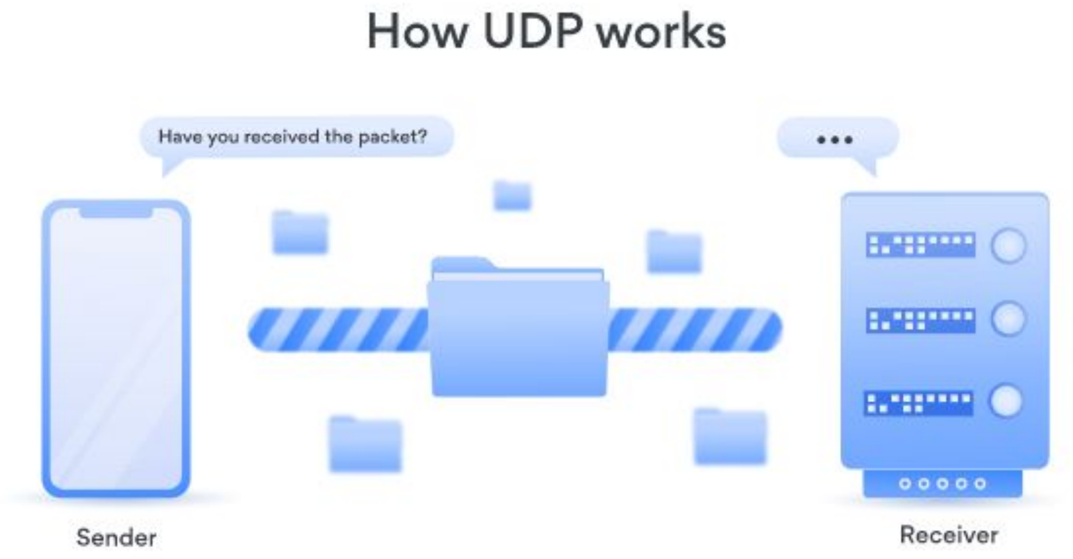
7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

UDP (User Datagram Protocol)

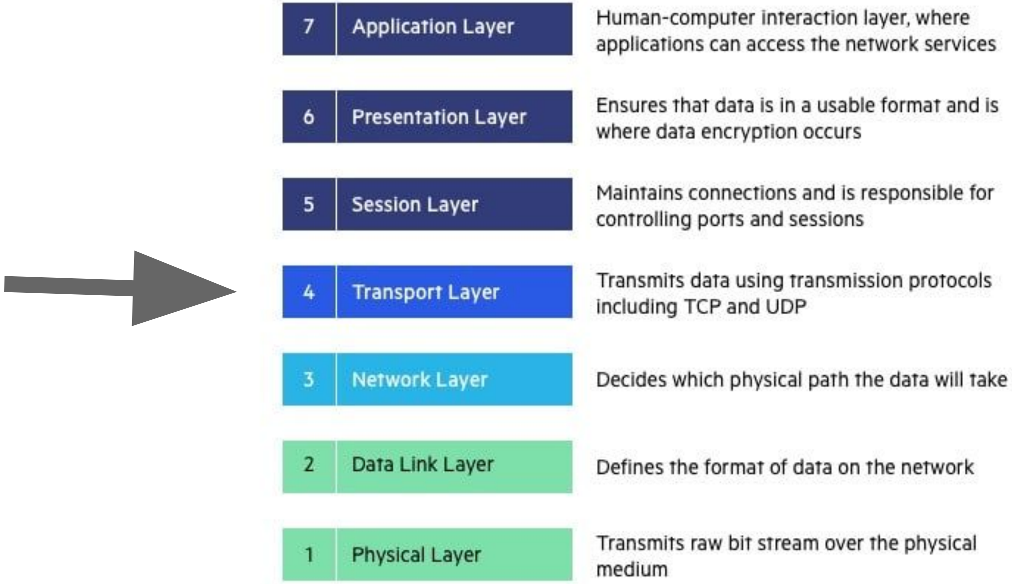
Compared to TCP, the UDP network protocol is **less reliable, but faster and more straightforward**.

UDP is **connectionless**, so it doesn’t establish a prior connection between two parties. It has the potential to lose data along the way, but in return you’ll have much higher speeds.

UDP (User Datagram Protocol)



OSI (Open Systems Interconnection) Model



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

HTTP (HyperText Transfer Protocol)

Serves as a set of rules and guidelines that **help web servers provide your browser** with everything they need to faithfully display websites on your screen.

HTTP (HyperText Transfer Protocol)

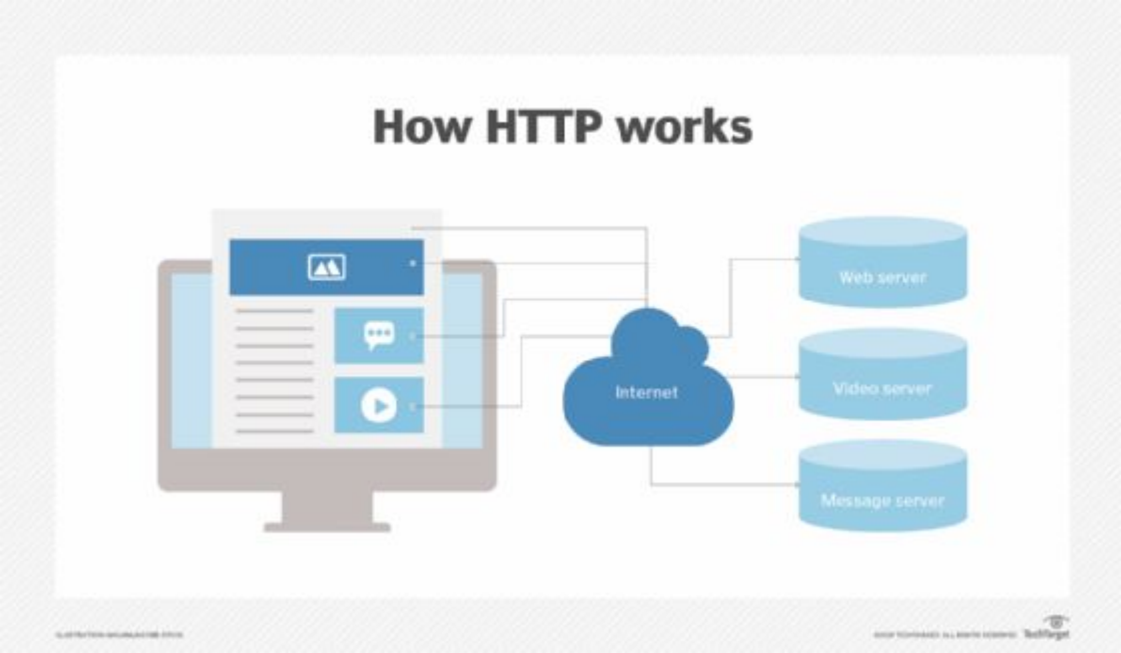
HyperText

Any type of media – text, images, video and audio – that can contain connections to other types of media

Transfer Protocol

Network protocol - Governs the transfer of information between devices on the application layer

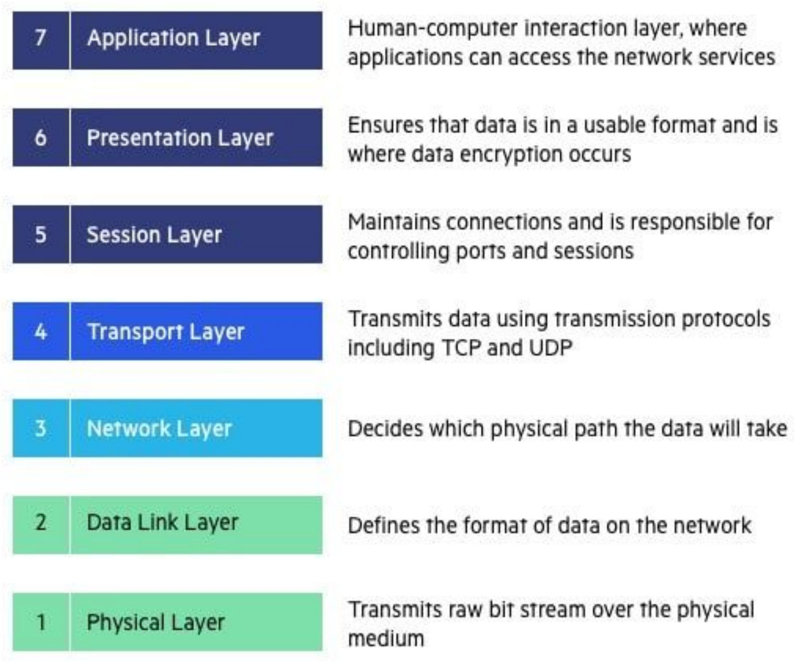
HTTP (HyperText Transfer Protocol)



HTTP Methods

HTTP Method	**CRUD Action**
GET	Read
POST	Create
PUT	Update or Replace
PATCH	Update or Modify
DELETE	Remove

OSI (Open Systems Interconnection) Model



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

Activity Time

In this activity, **break into groups of 3 and discuss the use cases for each network communication protocol**

- **TCP**
- **UDP**
- **HTTP**

Once done, take a break!

Where is TCP is used?

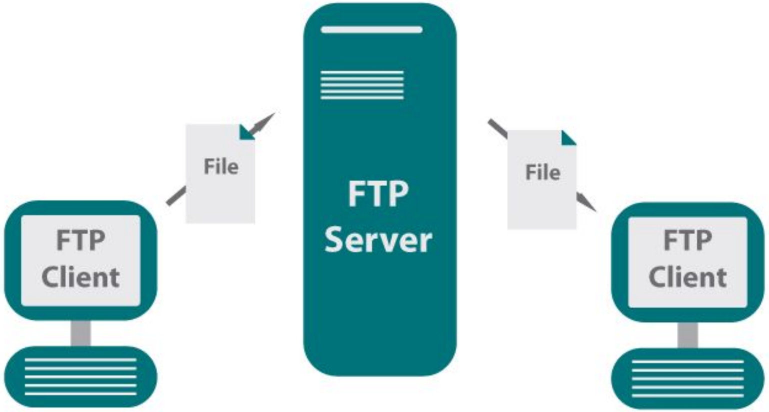
- Text Messaging
- SSH, FTP, telnet
- SMTP, sending mail
- IMAP/POP, receiving mail

Where is UDP is used?

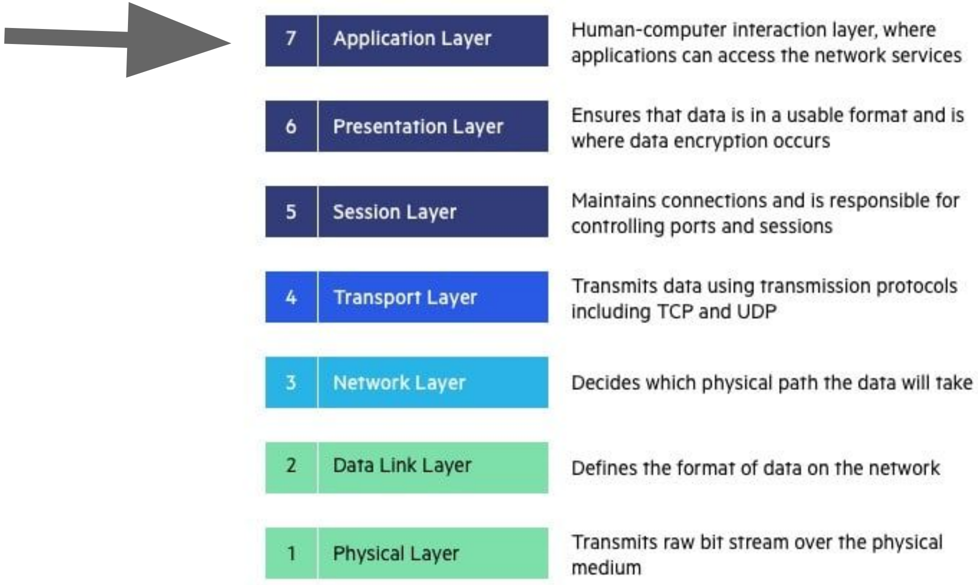
- Video Streaming
- Online Gaming
- Tunneling/VPN (lost packets are ok - the tunneled protocol takes care of it)

FTP (File Transfer Protocol)

Client/server protocol that is used for **moving files to or from a host computer**. It allows users to download files, programs, web pages, and other things that are available on other services.



OSI (Open Systems Interconnection) Model



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

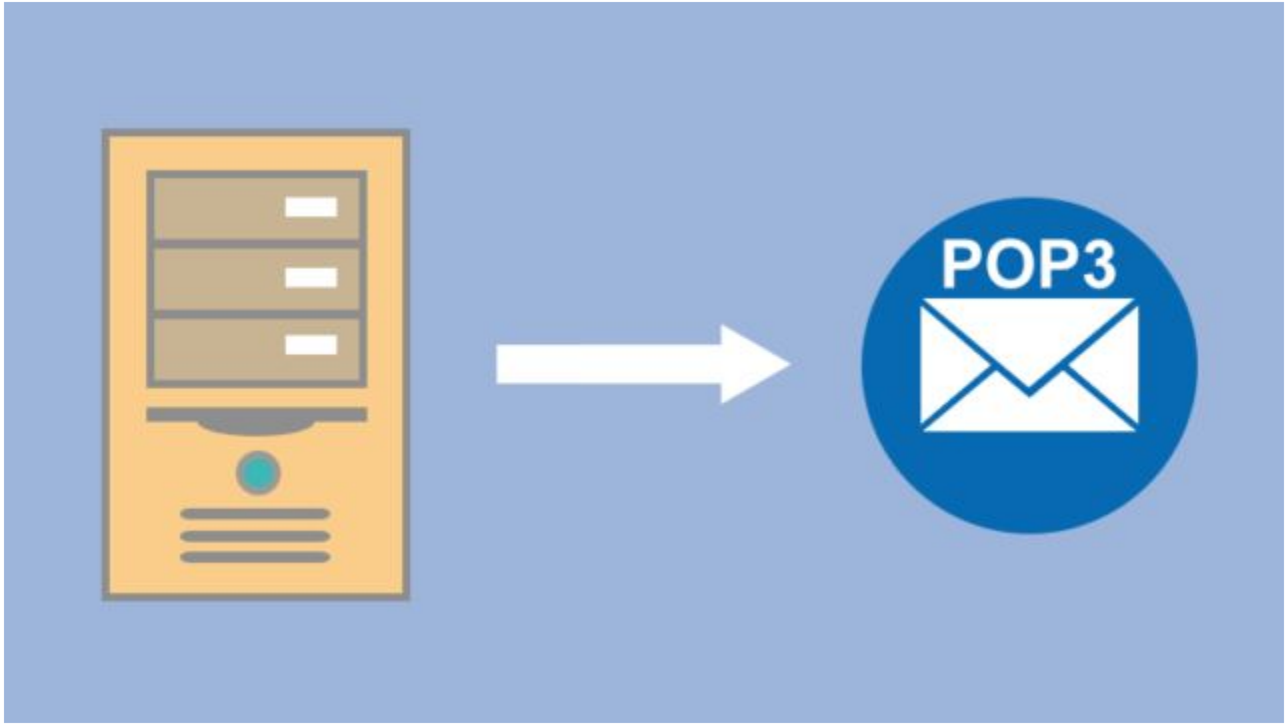
POP3 (Post Office Protocol)

Used by local mail clients to **get email messages** from a remote email server over a TCP/IP connection.

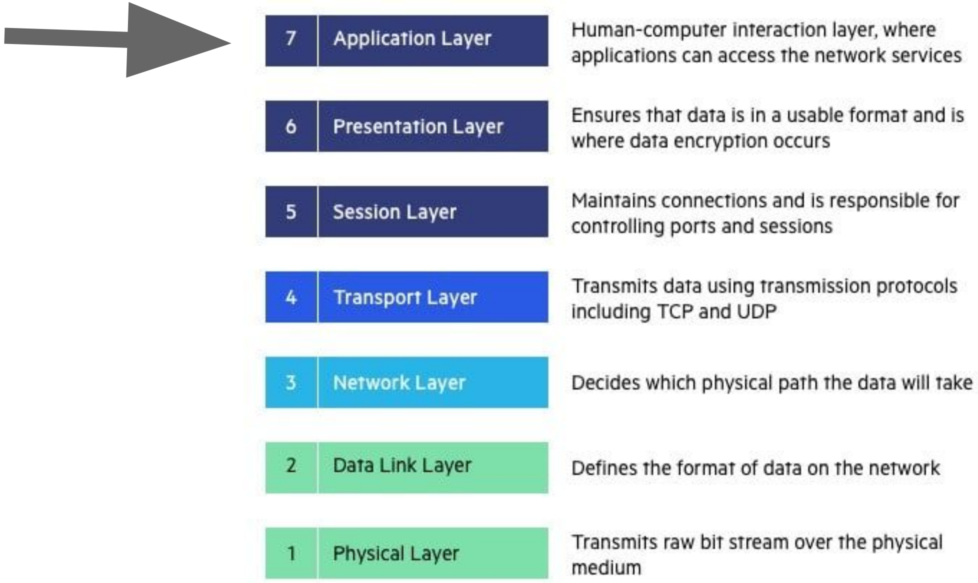
Email servers hosted by ISPs also use the POP3 protocol t**o hold and receive emails intended for their users.**

After the email client downloads the emails, they are generally deleted from the servers.

POP3 (Post Office Protocol)



OSI (Open Systems Interconnection) Model



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

Network Management Protocol

What is Network Management Protocol?

Network management protocols are designed for **maintaining and governing the network**.

Specifically, they determine the policies and procedures required for monitoring, managing, and maintaining a computer network.

This allows for **stable network communication and performance**.

Why are Network Management Protocols important?

A network management protocol provides a network operator with a host’s availability, packet/data loss, overall status, and information about the **health of the connection**.

A network operator can use this information to **effectively troubleshoot connections between host and client devices.**

The policies managed by management protocols can be **applied to all devices on the network, including computers, switches, routers and even servers.**

2 Types

- SNMP (Simple Network Management Protocol)
- ICMP (Internet Control Message Protocol)

SNMP (Simple Network Management Protocol)

A way of communicating to **network elements that you want to monitor**

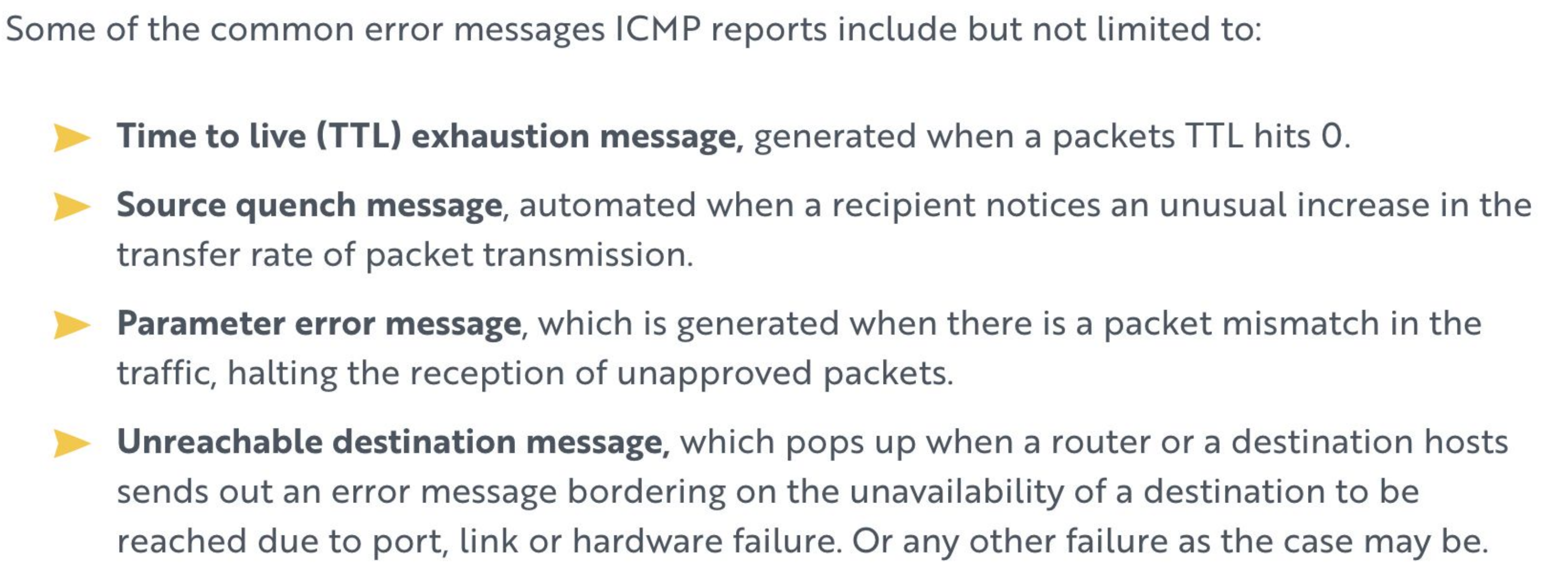
SNMP **allows devices on a network to communicate**, regardless of hardware and software. This provides network devices (routers, printers, servers, etc.) with a common language for sharing information with a network management system.

ICMP (Internet Control Message Protocol)

Designed **specifically for error reporting**

Network devices such as routers make use of ICMP to **send error messages** at situations where for example a **host/client can’t be reached or requested information is not available.**

ICMP (Internet Control Message Protocol)



Some of the common error messages ICMP reports include but not limited to:

- **Time to live (TTL) exhaustion message,** generated when a packets TTL hits 0.
- **Source quench message**, automated when a recipient notices an unusual increase in the transfer rate of packet transmission.
- **Parameter error message**, which is generated when there is a packet mismatch in the traffic, halting the reception of unapproved packets.
- **Unreachable destination message,** which pops up when a router or a destination hosts sends out an error message bordering on the unavailability of a destination to be reached due to port, link or hardware failure. Or any other failure as the case may be.

Activity Time

In this activity, **break into teams of 3 and create a diagram of how POP3 protocol works.**

Once done, take a break!

Network Security Protocols

What are Network Security Protocols?

Network security protocols are designed to ensure that **data in transit over the network's communications are safe and secure**.

These protocols also define how the network **secures data from any attempts** to review or extract said data by illegitimate means.

This helps ensure that **no unauthorized users, services, or devices access your network data,** and this works across all data types and network mediums being used.

Key Network Communication Protocols

- SSL
- TLS
- SFTP
- HTTPS

SSL (Secure Socket Layer)

Standard technology for keeping an **internet connection secure and safeguarding any sensitive data** that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details.

It does this by making sure that any **data transferred impossible to read via encryption algorithms** to scramble data in transit

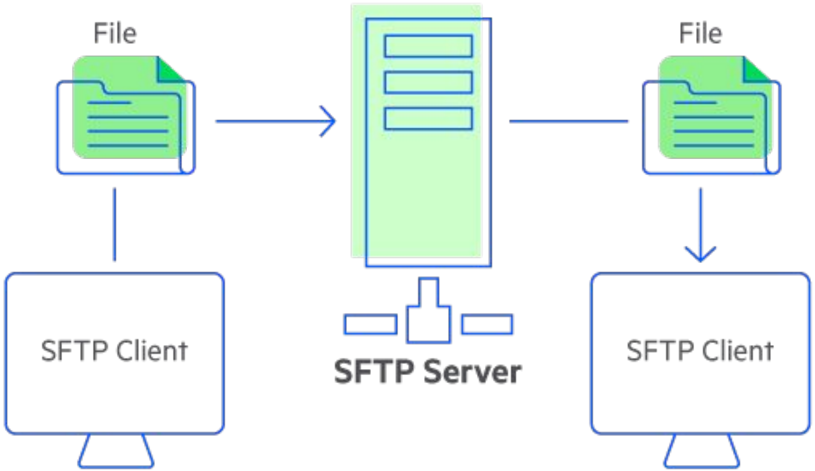
TLS (Transport Layer Security)

TLS is just an **updated, more secure, version of SSL.**

We still refer to our security certificates as SSL because it is a more commonly used term, but when you are buying SSL from DigiCert **you are actually buying the most up to date TLS certificates** with the option of ECC, RSA or DSA encryption.

SFTP (Secure File Transfer Protocol)

Used to **securely transfer files across a network**. Data is encrypted and the client and server are authenticated.

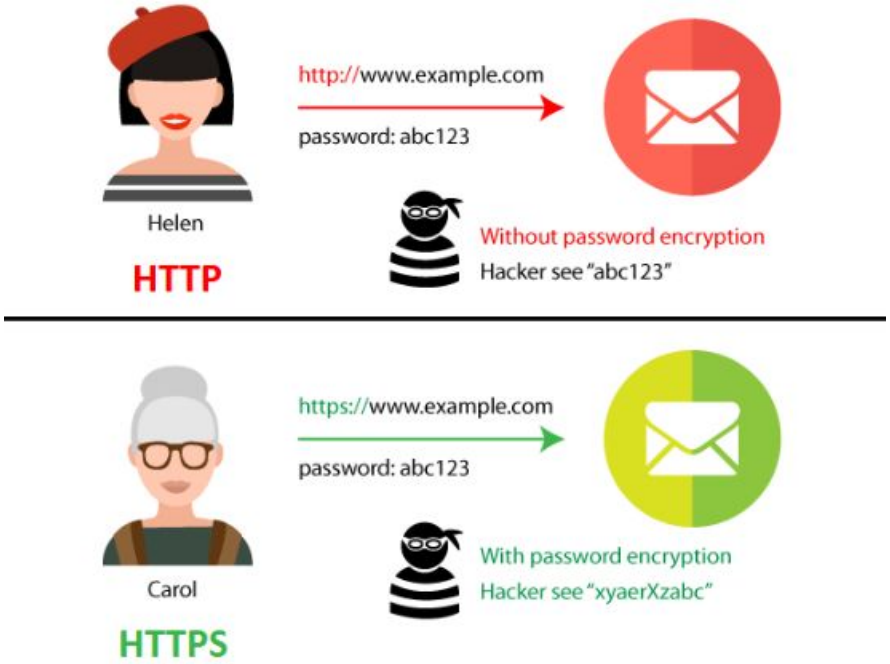


HTTPS (HTTP Secure)

Hypertext Transfer Protocol Secure is the secure version of HTTP. Data sent between the browser and server are **encrypted to ensure protection.**

You might wondering what is the difference between HTTP vs HTTPS

HTTPS (HTTP Secure)



Activity Time + Break

In this activity, **let's try the HTTPS protocol and how it's used differently.**

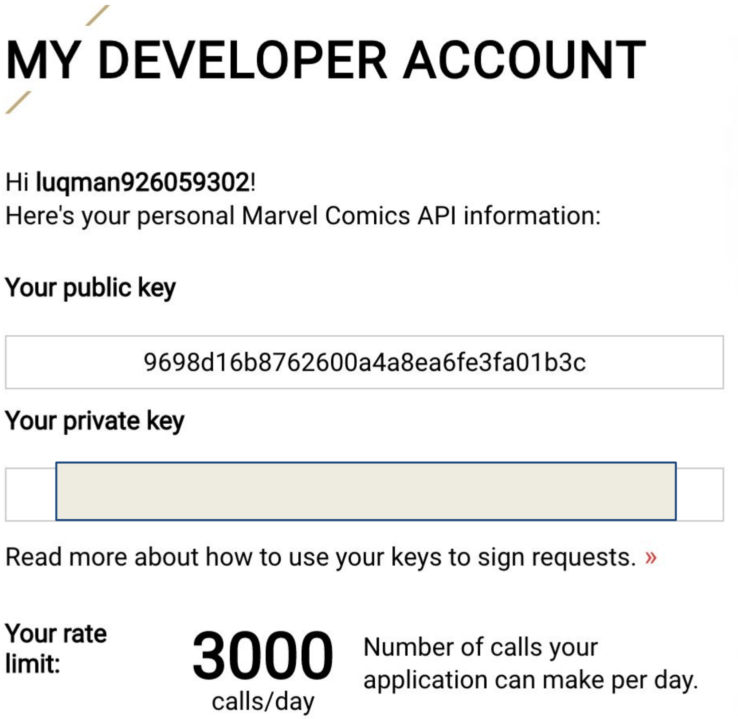
You may use tools like Postman or any similar tools:

- Install Postman: https://www.postman.com/
- Explore MARVEL API https://developer.marvel.com/documentation/getting_started
- Try Marvel API using Postman

Guide

1. Register for a MARVEL API account - https://developer.marvel.com/documentation/getting_started
2. Sign up for Postman API / any API caller tool - https://www.postman.com/

Guide



MY DEVELOPER ACCOUNT

Hi **luqman926059302**!
Here's your personal Marvel Comics API information:

Your public key

9698d16b8762600a4a8ea6fe3fa01b3c

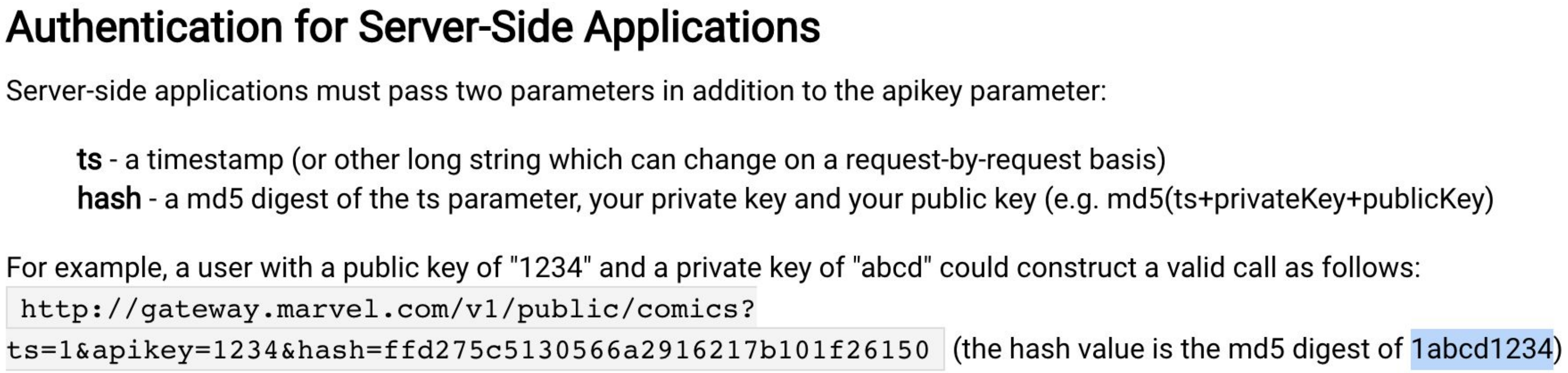
Your private key

[redacted]

Read more about how to use your keys to sign requests. »

Your rate limit: **3000** calls/day Number of calls your application can make per day.

Guide



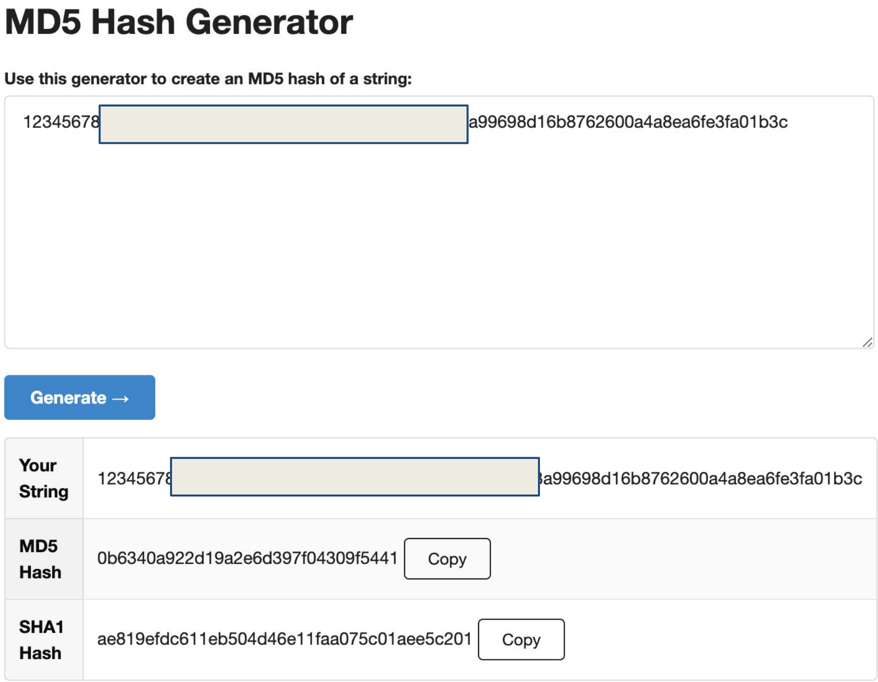
Authentication for Server-Side Applications

Server-side applications must pass two parameters in addition to the apikey parameter:

ts - a timestamp (or other long string which can change on a request-by-request basis)
hash - a md5 digest of the ts parameter, your private key and your public key (e.g. md5(ts+privateKey+publicKey)

For example, a user with a public key of "1234" and a private key of "abcd" could construct a valid call as follows: `http://gateway.marvel.com/v1/public/comics?ts=1&apikey=1234&hash=ffd275c5130566a2916217b101f26150` (the hash value is the md5 digest of 1abcd1234)

Guide



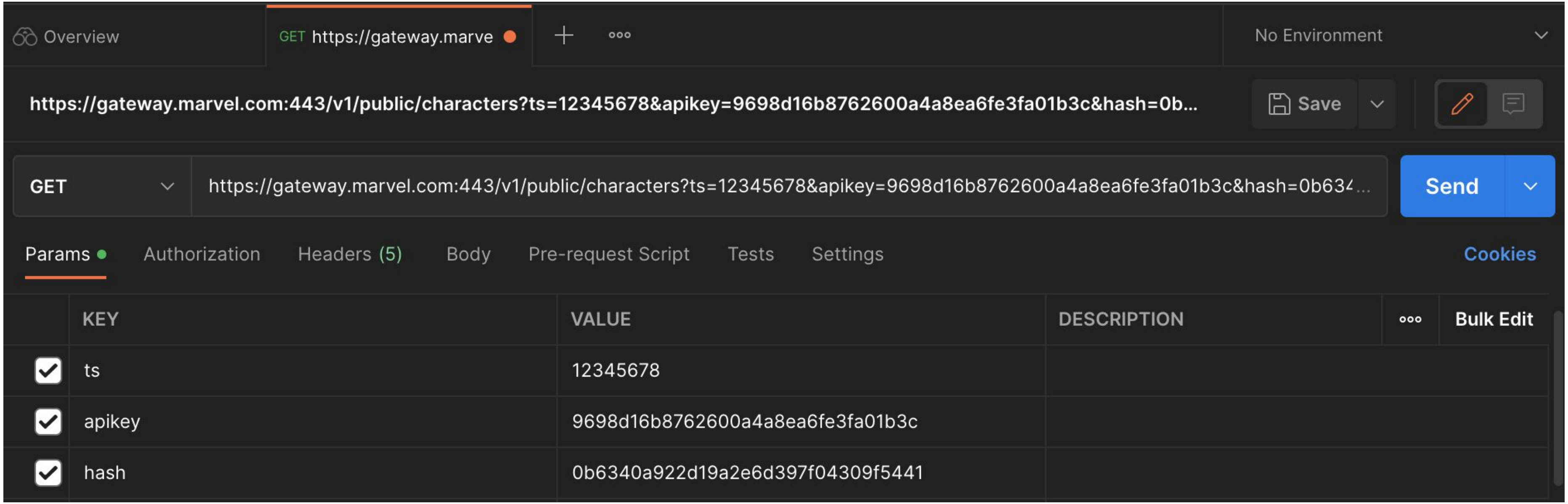
MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

12345678[redacted]a99698d16b8762600a4a8ea6fe3fa01b3c

Your String	12345678[redacted]a99698d16b8762600a4a8ea6fe3fa01b3c
MD5 Hash	0b6340a922d19a2e6d397f04309f5441 Copy
SHA1 Hash	ae819efdc611eb504d46e11faa075c01aee5c201 Copy

Guide



```
https://gateway.marvel.com:443/v1/public/characters?ts=12345678&apikey=9698d16b8762600a4a8ea6fe3fa01b3c&hash=0b...
```

GET

```
https://gateway.marvel.com:443/v1/public/characters?ts=12345678&apikey=9698d16b8762600a4a8ea6fe3fa01b3c&hash=0b634...
```

	KEY	VALUE	DESCRIPTION
☑	ts	12345678	
☑	apikey	9698d16b8762600a4a8ea6fe3fa01b3c	
☑	hash	0b6340a922d19a2e6d397f04309f5441	

What’s Next?

Useful Links

https://www.geeksforgeeks.org/layers-of-osi-model/

https://www.geeksforgeeks.org/examples-of-tcp-and-udp-in-real-life/

https://www.liveaction.com/resources/blog/types-of-network-monitoring-protocols/