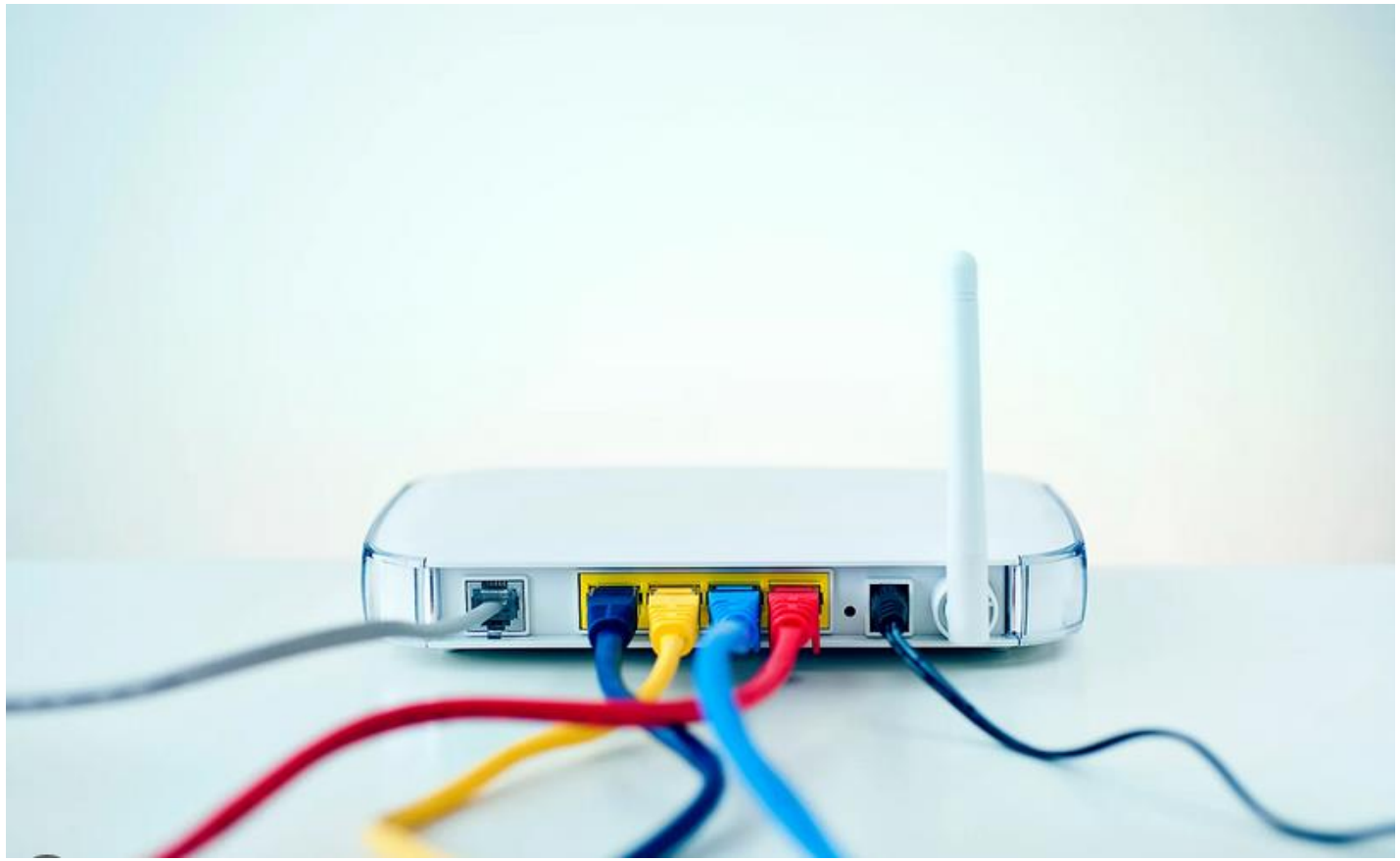
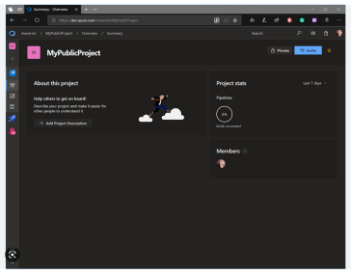
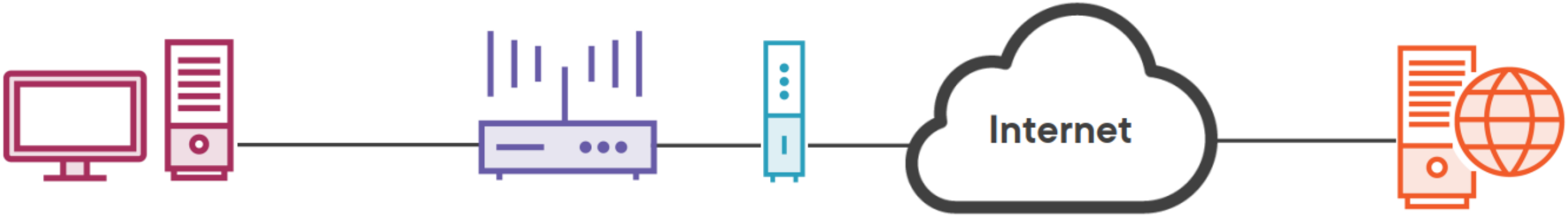
Networking – open discussion - how does it work?



Networking – practical example



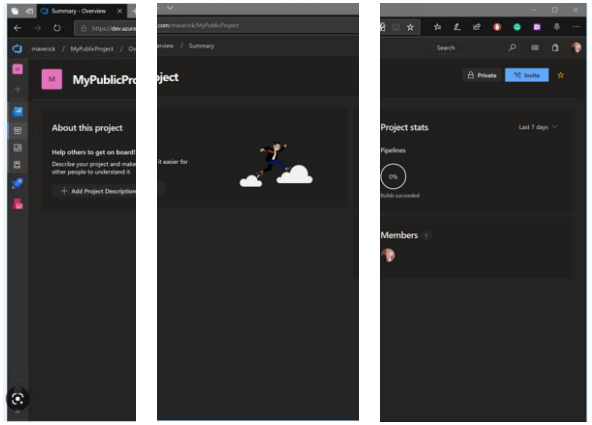


Open Systems Interconnection (OSI) model

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		GATEWAY Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

https://blogs.cisco.com/cloud/an-osi-model-for-cloud



(OSI) model example

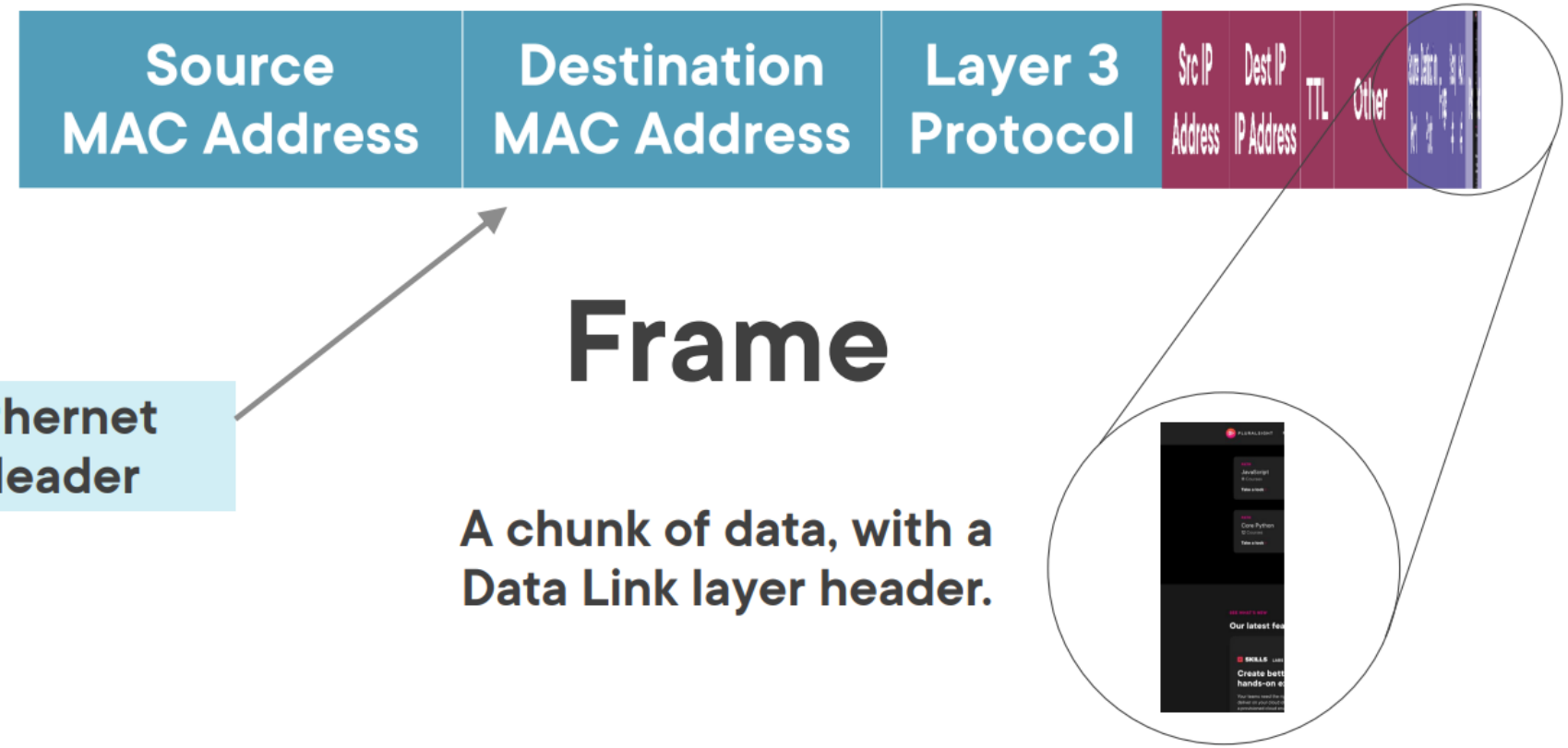
- **7 – Application layer** : using HTTPS protocol we fetch the website, but because of the size it has to be divided into smaller chunks

4 - Transport Layer

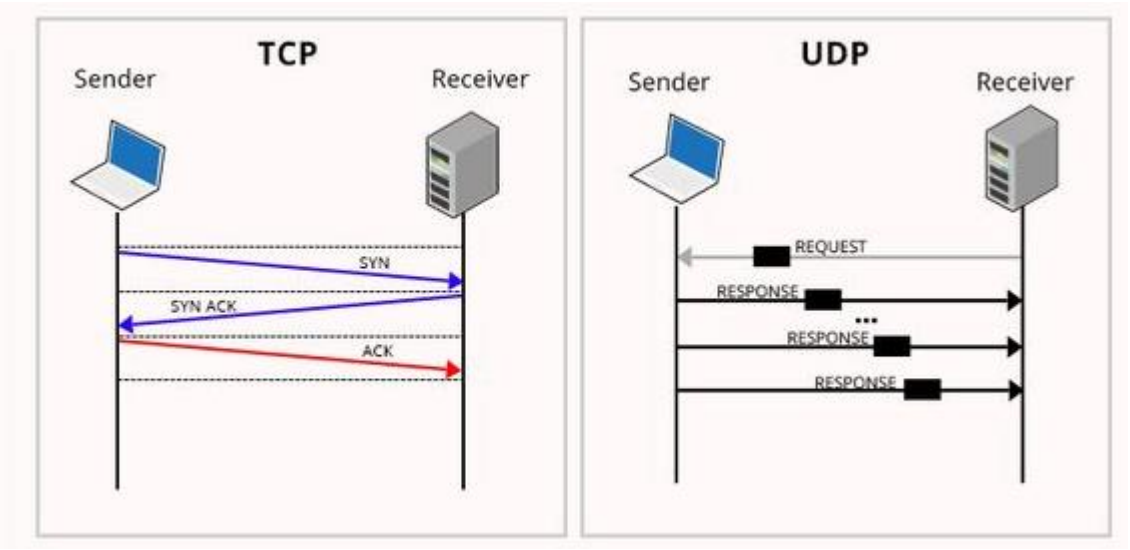
3 – Network Layer

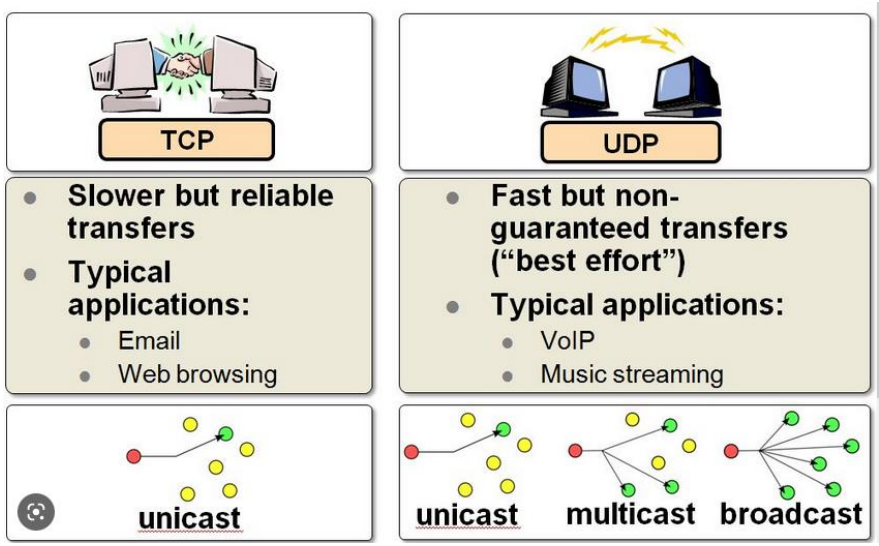
2 – Data Link Layer

2 – Data Link Layer



TCP vs UPD in Transport Layer





TCP vs UDP

TCP	UDP
Connected	Connectionless
State Memory	Stateless
Byte Stream	Packet/Datagram
Ordered Data Delivery	No Sequence Guarantee
Reliable	Lossy
Error Free	Error Packets Discarded
Handshake	No Handshake
Flow Control	No Flow Control
Relatively Slow	Relatively Fast
Point to Point	Supports Multicast
Security: SSL/TLS	Security: DTLS

Ports Numbers

Well Known
0 – 1023

Registered
1,024 – 49,151

Application Protocol	Port Number
HTTP	80
HTTPs	443
FTP	20 , 21
SSH	22
Telnet	23

Custom Applications
“Official and Unofficial”

Subnet Mask

superuser

Home

PUBLIC

Questions

Tags

What is a subnet mask, and the difference between a subnet mask of 255.255.255.0 and 255.0.0.0?

Asked 13 years, 5 months ago Modified 3 years, 11 months ago Viewed 176k times

Ask Question

6 Answers Sorted by: Highest score (default)

29

The zero in the subnet mask will correspond to the `xxx` of your IP address. If you need more than 255 different addresses, you'll have to change the DHCP IP's to 10.0.xxx.xxx (broadcast IP of 10.0.255.255) and the subnet mask to 255.255.0.0.

Theoretically, 255.0.0.0 is a valid subnet mask for 10.0.0.0 to 10.255.255.255 addresses. This wikipedia article shows the valid addresses for private networks.

But in your case (10.0.0.xxx), you should use 255.255.255.0.

Share Improve this answer Follow

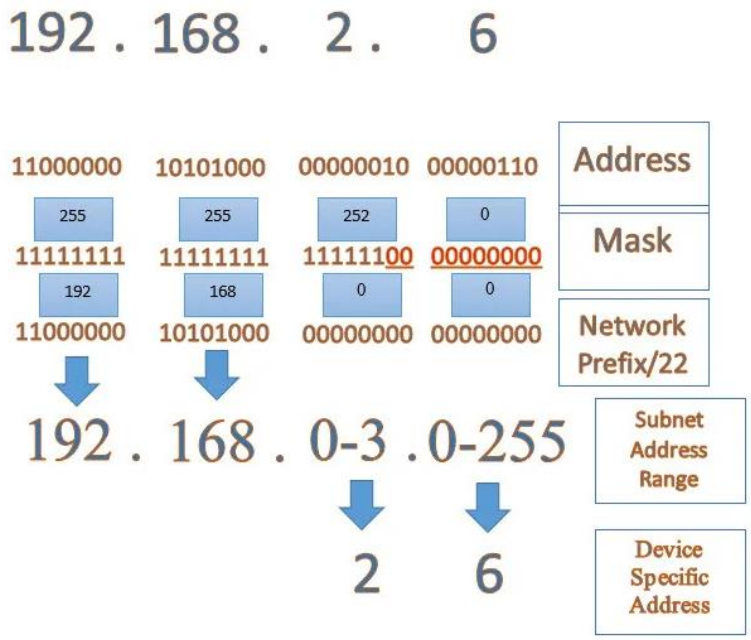
edited Nov 6, 2009 at 10:42

answered Oct 13, 2009 at 13:52

djeidot

1,468 ● 1 ● 13 ● 14

Add a comment



What are ICMP PING responses?
What is TELNET?

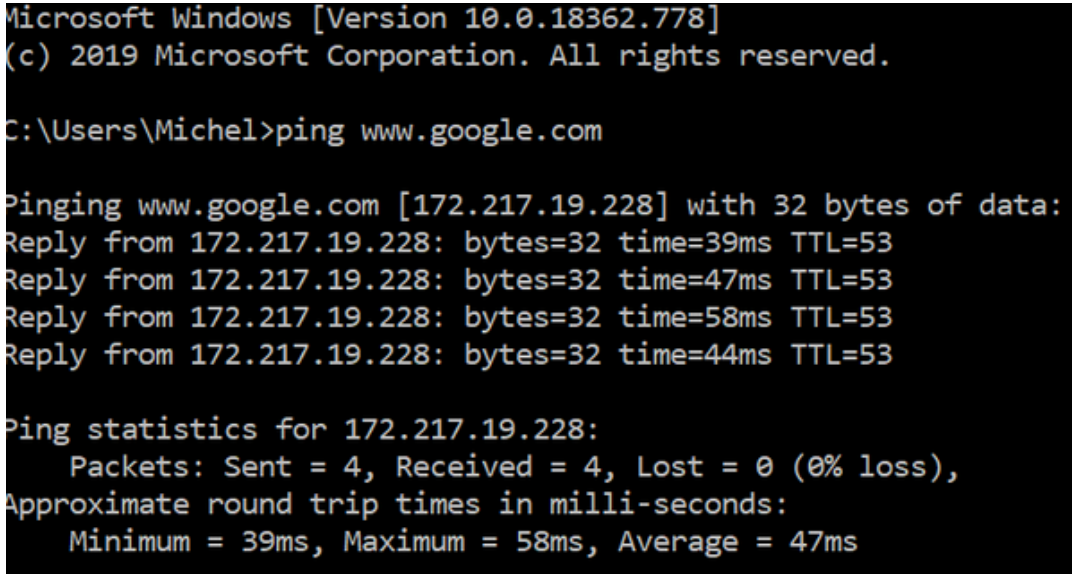
Internet Control Message Protocol (ICMP) is one of the protocols of the TCP/IP suite.

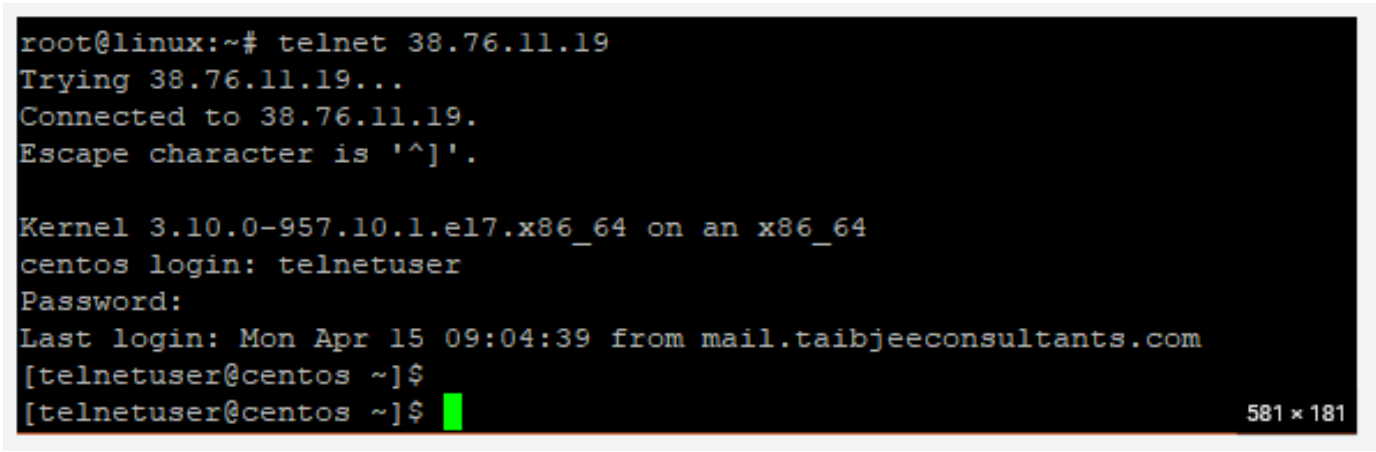
Ping

- troubleshooting tool to manually test for connectivity between network devices
- test for network delay and packet loss
- Ping reply can be blocked to prevent unauthorized network discovery

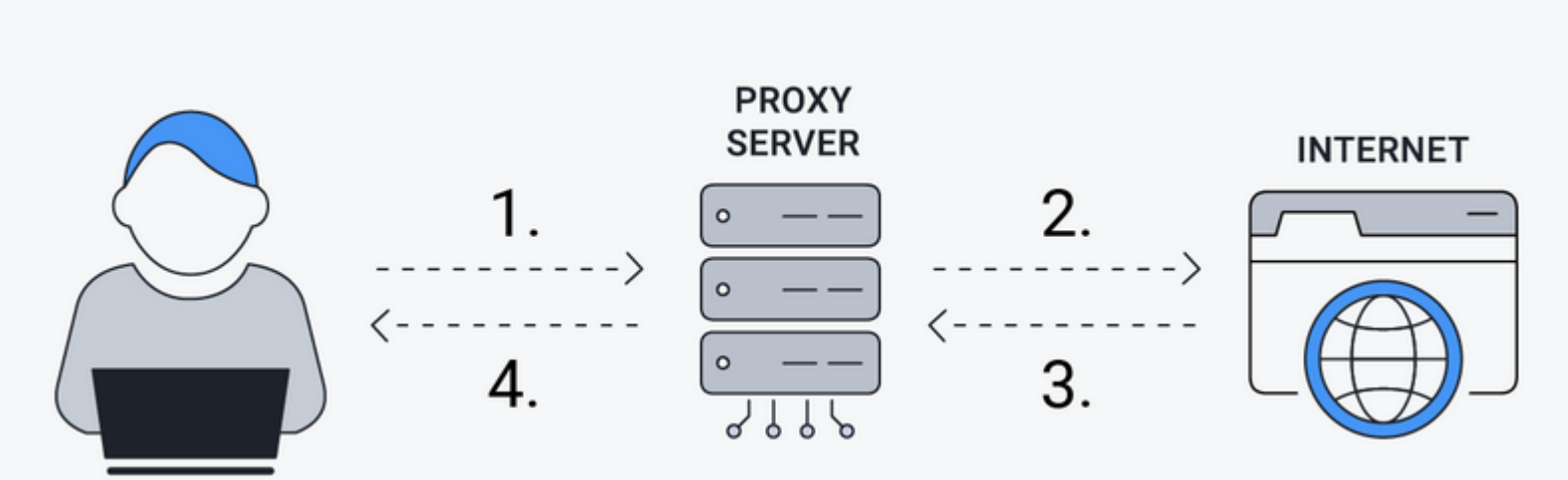
Telnet

- Tests the connectivity between two network parties.
- Sends data over Unencrypted and it has no authentication mechanism
- It's an old version of SSH and it uses by default port 23





Proxy

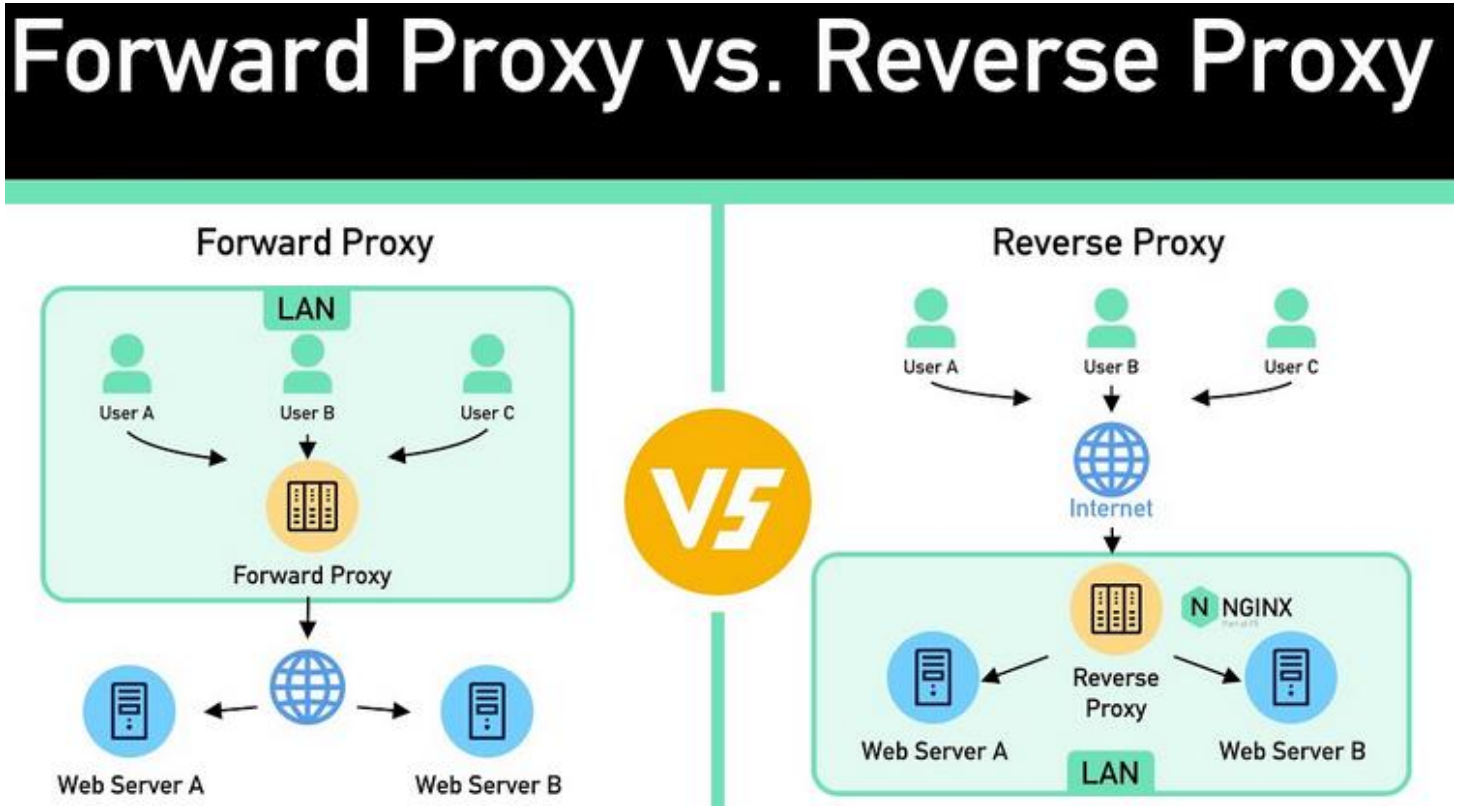


A proxy is just a middle server that captures your traffic request and forwards it as it's own

Why would you need a proxy server?

- To control internet usage of employees / students / etc
- Bandwidth savings and improved speeds (cache if all the requests are for the same website)
- Privacy , user ip address will not be visible on the internet
- Improved security: block some un-wanted website in schools/companies, etc
- Access to blocked resources: Netflix if you use an US based proxy ☺

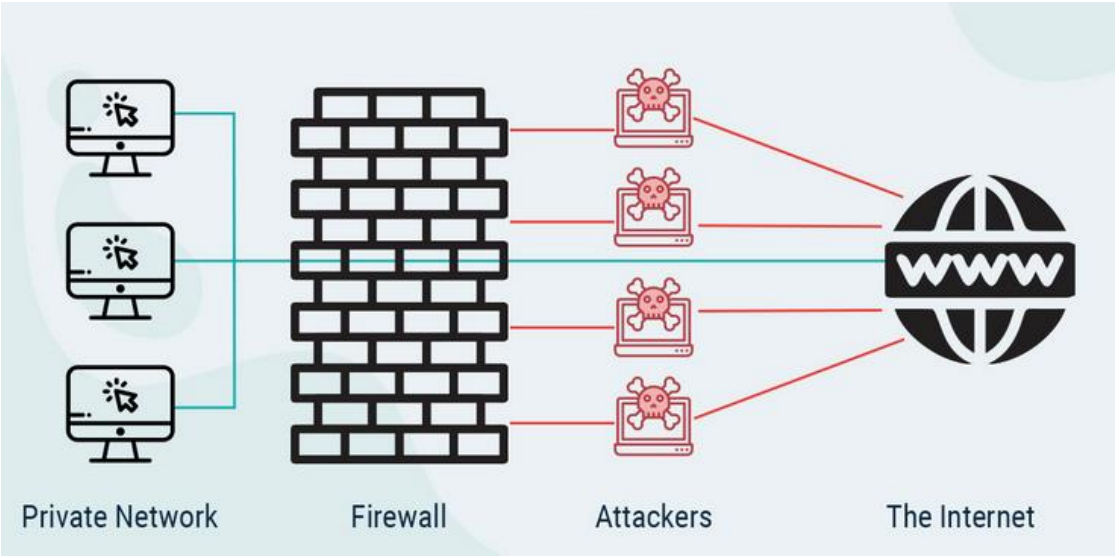
Reverse Proxy



A reverse proxy is a server that sits in front of one or more web servers, intercepting requests from clients. This is different from a forward proxy, where the proxy sits in front of the clients.
Why would you need a proxy server?

- Protects the website (another layer of abstraction between client and the WebServer)
- Load balancing (bonus : what is the difference between a Load Balancer and a Reverse Proxy?)
- Cache

Firewall



- A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.