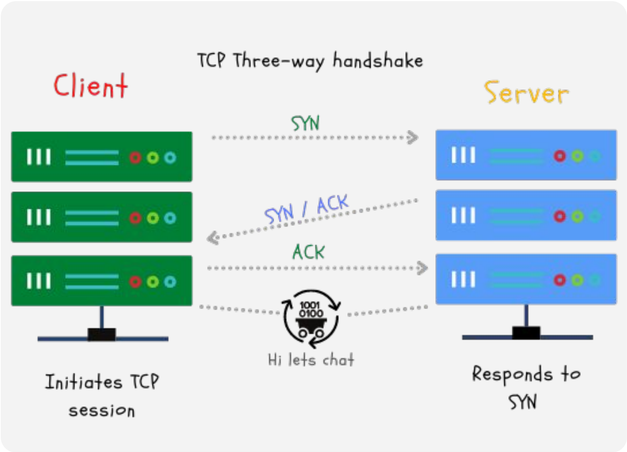
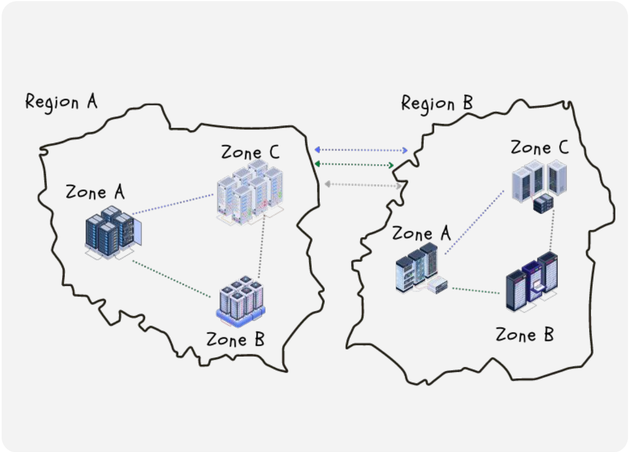
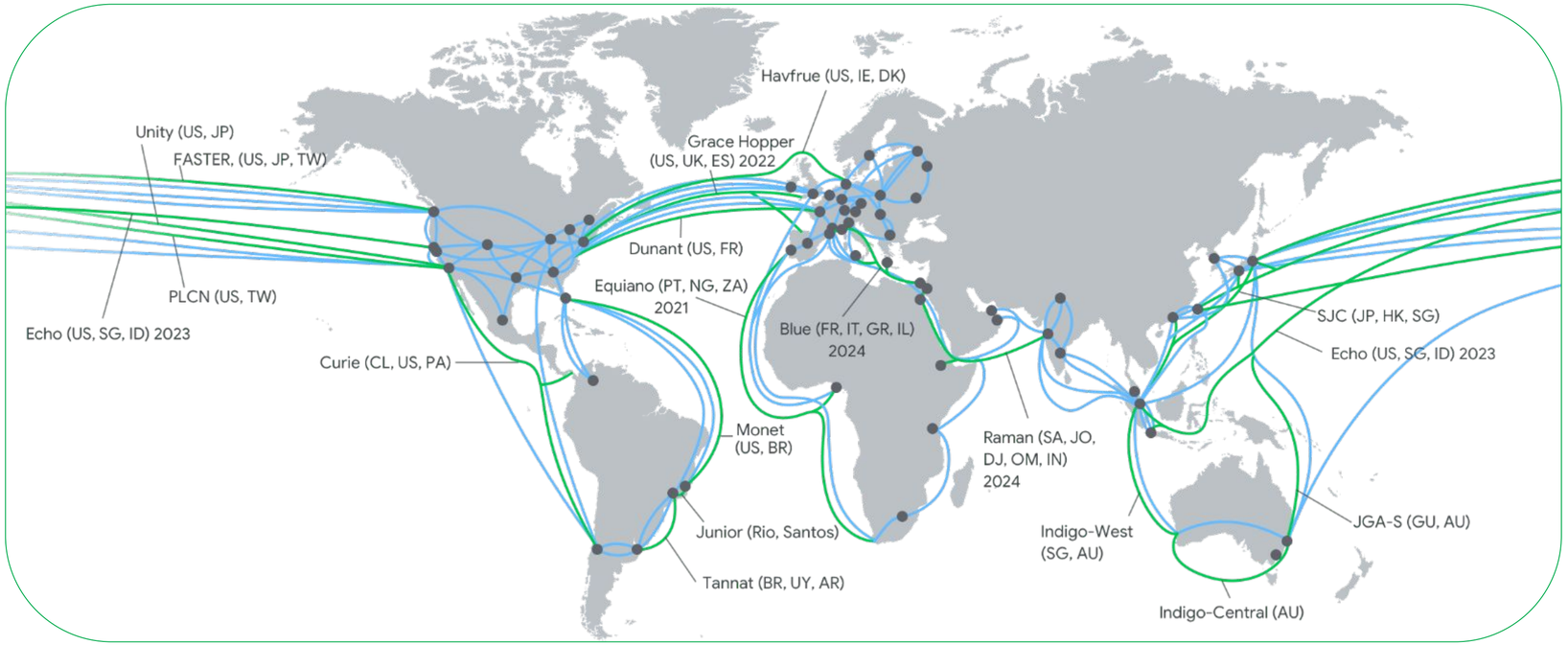




Google Cloud

Networking 101 sheet .!!!

V2 - 2023



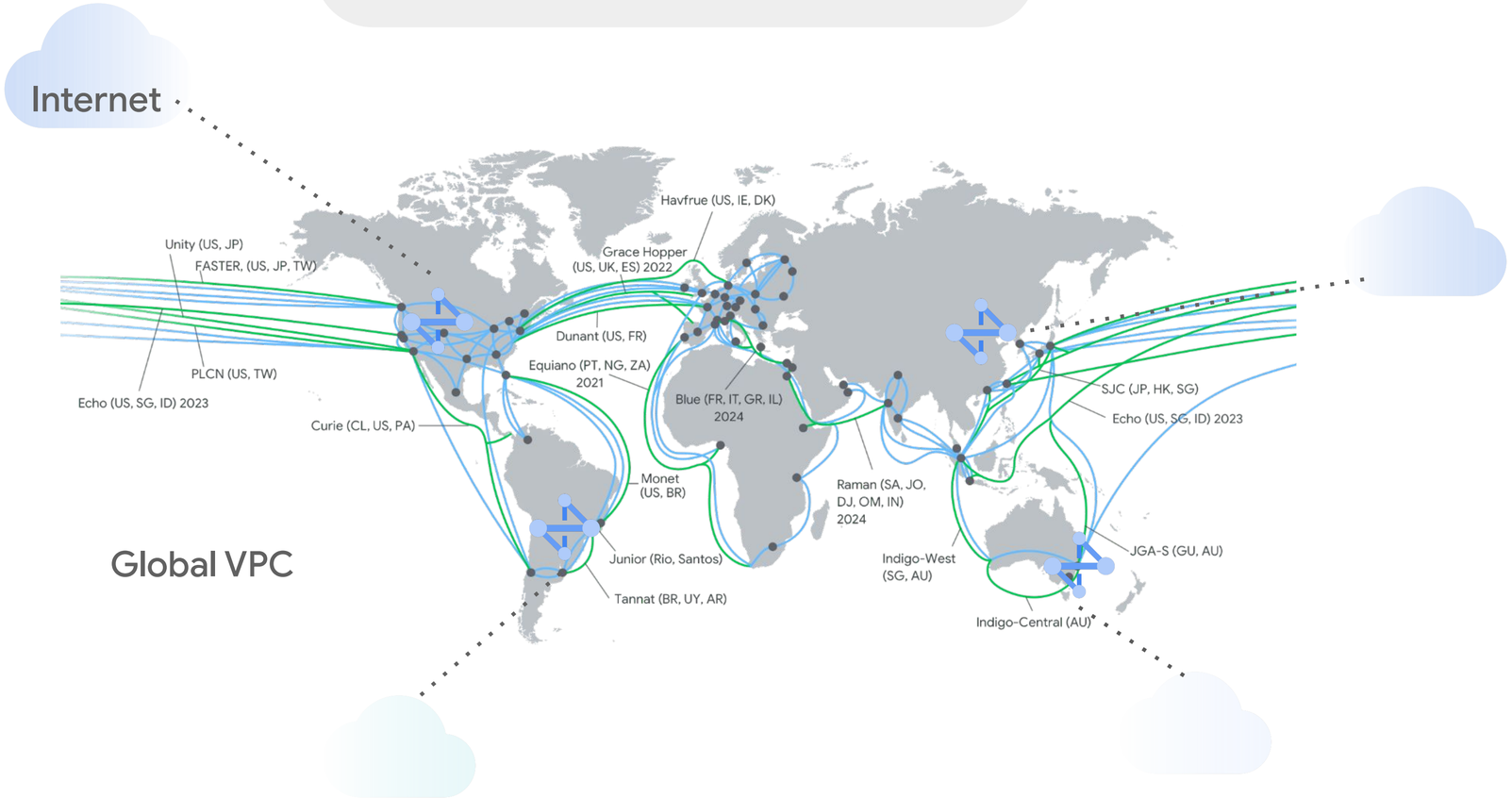
Ammett

Global Network I

Network	Is a collection of connected devices for the purpose of communication. This can be a physical or logical connection
Fiber Optic Cable	Cable made up of optical pairs that transmit data using light
Internet	Public network of networks which exchanges routes through BGP

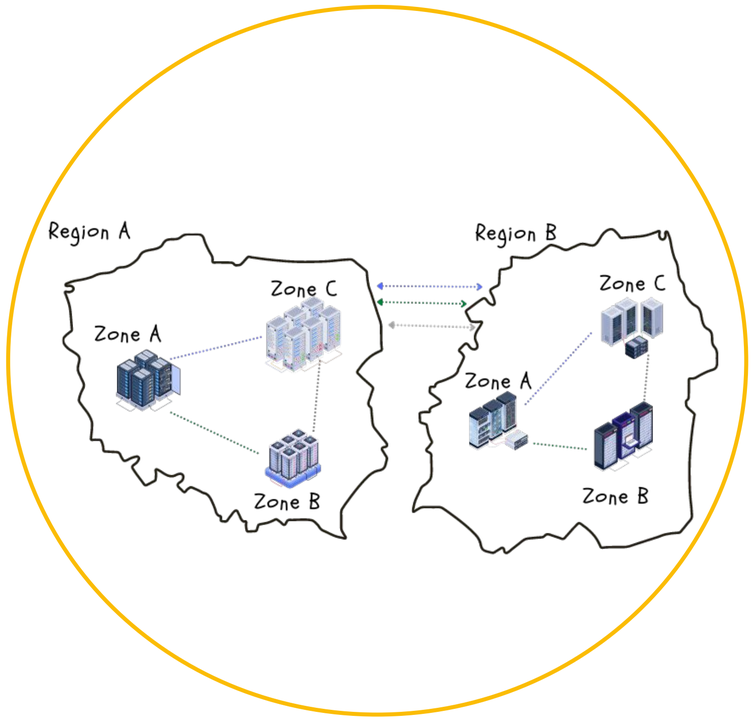
Networking 101 sheet .!!!

What are the economic advantages of using the Google Cloud network?
- Check blog **here**
- Download report **here**



Global Network II

Region	A Google Cloud geographic compute location (Made up of minimum 3 zones)
Zone	Google Cloud compute facility within a region
Point of presence (PoP)	A connection point from the internet to Google's network
On-prem	Data center belonging to an enterprise
Local Area Network (LAN)	This is a network that shares same communication lines in a distinct geographic area
Virtual LAN (VLAN)	A logical method to allow communication between systems that are located on different LAN segments



Networking 101 sheet .!!!

How much regions, zone and PoP exist in Google Cloud?
- Check current count **here**

Who controls networking on-prem?
- 100% controlled by the enterprise

Where are the regions located?
- Check list **here**

How is Google global network designed?
- Check list **here**

VPCs and IP addressing

Virtual Private Cloud (VPC)	VPC is a Logical representation of an on-prem network. This is a global construct in GCP
VPC modes	There are two modes in GCP. **Auto mode** and **custom mode**
VPC subnets	In GCP these are regional and assigned to an IP address range
IP address	A unique address used to identity host on network. Made up of network and host portions
Subnet mask	This segments and IP address into network and host portions. It determines how must host are available on the network. This can be manipulated to form **CIDR** blocks
IPV4	This is a 32 bit, 4 octet address. Written in binary or dotted decimal format. E.g. **192.168.10.20** or **11000000.10101000.00001010.00010100**
IPV6	This is a 128 bit, hexadecimal address. 2001:DB8:7654:3210:FEDC:BA98:764:3203
Private IP (RFC1918)	A special range that can be used internally by anyone. These are non internet routable
Public IP	IP address that is routable on the internet
DHCP	Dynamic Host Control protocol. A method to automatically assign an IP address to a client
Static IP	An IP that does not change after being assigned
Ephemeral IP	Temporary IP that is not reserved

Bring Your Own IP (BYOIP)	Use external IP addresses that you own in Google Cloud
Alias IP	Additional addresses that can be assigned to your VM, these can be taken from the primary or secondary address range
Secondary IP	Secondary range of IP address that can be assigned to your VM
Restricted.googleapis.com IP	Access external GCP APIs via google private network. 199.36.153.4/30. Used when **VPC service controls** are enabled and you need to access only VPC service control supported APIs
Private.googleapis.com IP	Access external GCP APIs via google private network. 199.36.153.8/30
Network Time Protocol (NTP)	Is used to synchronize systems timer across a network. This is used on both internal and external networks.

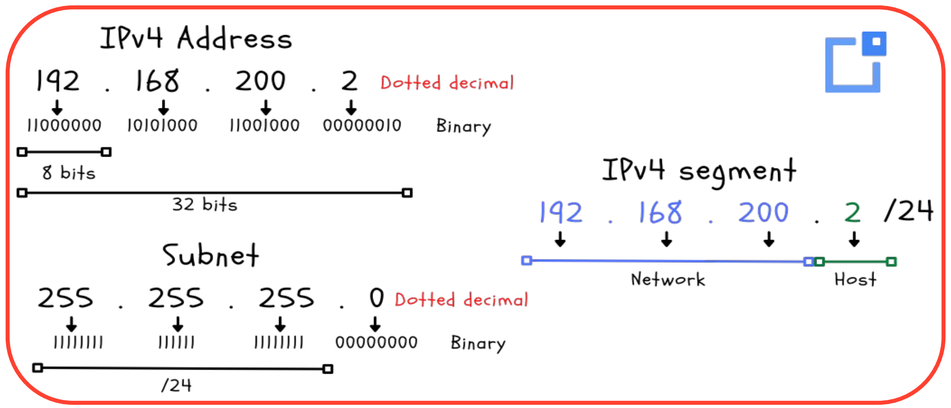
Networking 101 sheet .!!!

What is the amount of reserved IP's in GCP subnet?
- Count 4

What is the smallest GCP private subnet?
- /29 with 4 host.
  Formular 2^n - 4

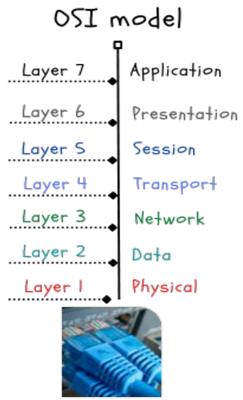
Can IPV6 be used?
- Yes, see **here**

Can I set private and public static IP's in my VPC?
- Yes, see below:
  - **External static**
  - **Internal static**



OSI model and Internet Model

What is the OSI Model	A 7 layer conceptual model that provides interoperability of the TCP stack
Application Layer (Layer 7)	User interface and application. Protocols examples HTTP, HTML
Presentation Layer (Layer 6)	Formats data to be presented. Protocols examples JPEG, ASCII, GIF
Session Layer (Layer 5)	Creates, tracks, ends the sessions between different systems
Transport layer (Layer 4)	Handles message delivery using connection and connectionless protocols. Protocol examples TCP, UDP
Network layer (Layer 3)	Focuses on subnets, route path selection. Protocols examples IP, ICMP,. Router work here
Data layer (Layer 2)	Focuses of transferring data frames over physical layer. Protocol, ARP, PPP, VLANS. Switches work here
Physical layer (Layer 1)	Transmission of raw bits over physical mediums. Examples network cables, wireless



GCP Services operating at different OSI layers

Layer 7	HTTPS Load balances, Cloud Armor
Layer 4	Load balancers
Layer 3	Interconnect
Layer 2	Interconnect VLANs

Networking 101 sheet .!!!

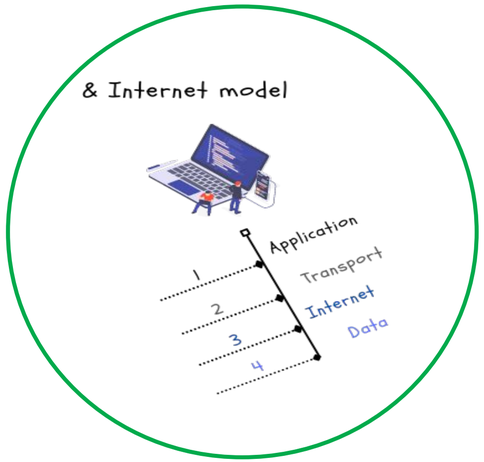
What is interoperability?

- The ability to communicate between different communication devices in a standard way.

Does a physical layer exist in the cloud?

- Yes, there are hardware devices located in **Google Data Centers**. These are 100% managed by Google.

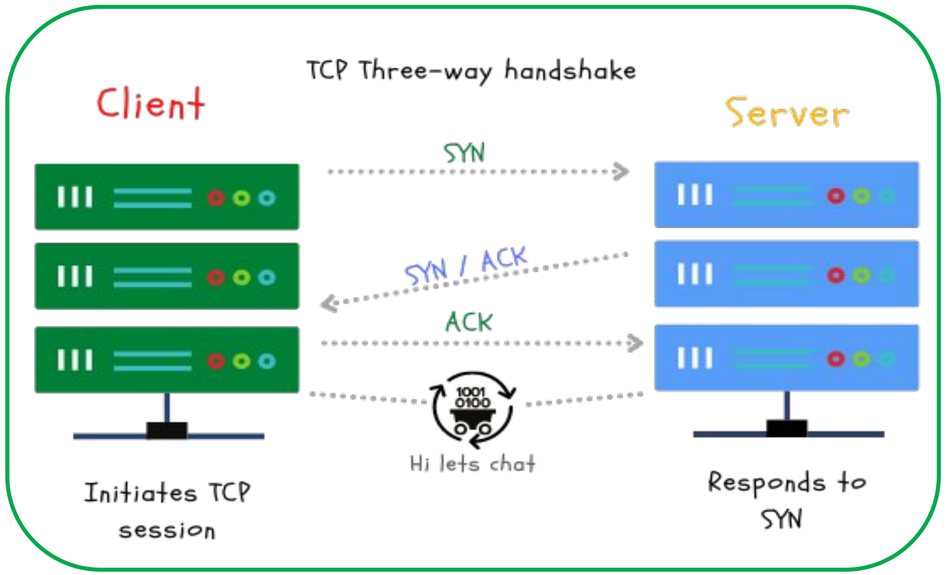
What is the Internet Model	A 4 layer model conceptual model of the TCP/IP stack
Application Layer	User interface and application.
Transport layer	Responsible for end to end data handling of data streams
Internet layer	Responsible for routing packets through networks
Link layer	From a device it interacts with physical network



TCP, Three-way handshake, UDP, QUIC

Transmission Control Protocol (TCP)	This is a connection oriented protocol that handles reliability, flow and congestion control of packets. It establishes a connection before sending a packet
Transmission Control Block (TCB)	Contains all the information about the connection and implements the sliding window
Sliding window	Determines the amount of bytes that one system can send to the other. Once the agreed bytes are received and processed, the sender sends another set of bytes to the receiver until all data is sent
Three-way handshake	This is the sequence to form a TCP connection. It involve the SYN, SYN/ACK, ACK flag exchange between client/server
Flag	These indicate the state of the connection
SYN	The SYN or **synchronize** flag is sent to start the TCP connection process
ACK	The ACK or the acknowledgement flag. This confirms that data was received
FIN	A flag sent to request termination of connection
User Datagram Protocol (UDP)	This is a best effort delivery protocol

Quick UDP Internet Connections(QUIC)	A Google made transport layer protocol. This is built on top of UDP
Transport Layer Security (TLS)	A protocol that provides cryptography by using certificates



Networking 101 sheet .!!!

How does TCP differ from UDP?

- TCP is connection oriented, UDP is best effort.

What layer of the OSI is TCP and UDP found?

- These exist at layer 4, transport layer.

Packet, Frame, MTU

Data messages types	These are frames, packets, datagrams. They may exist at different layers of the OSI model
Maximum transfer unit (MTU)	The size of the largest unit of data that can be transmitted over the network
Time to Live (TTL)	This indicates the life of the packet usually has a max of 255 hops. This ensures packets don't exist forever in a network
Unicast message	These are sent on a 1 to 1 basis on a network
Multicast message	These are sent to subscribed groups on a network
Broadcast message	These are sent to every device on a network.

Networking 101 sheet .!!!

How do the different message types work?

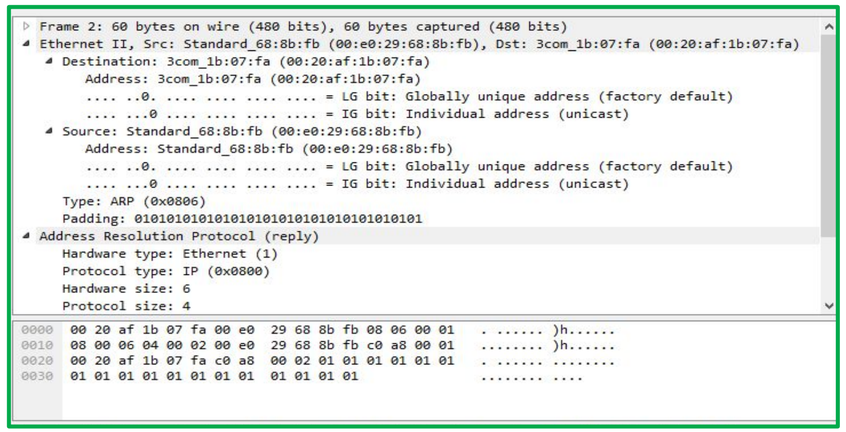
- See **guide**

What MTU option do you have in Google Cloud?

- Currently, 1440, 1460, 1500, 8896 **See options doc**

Does multicast and broadcast works natively work in Google Cloud?

- Currently no.

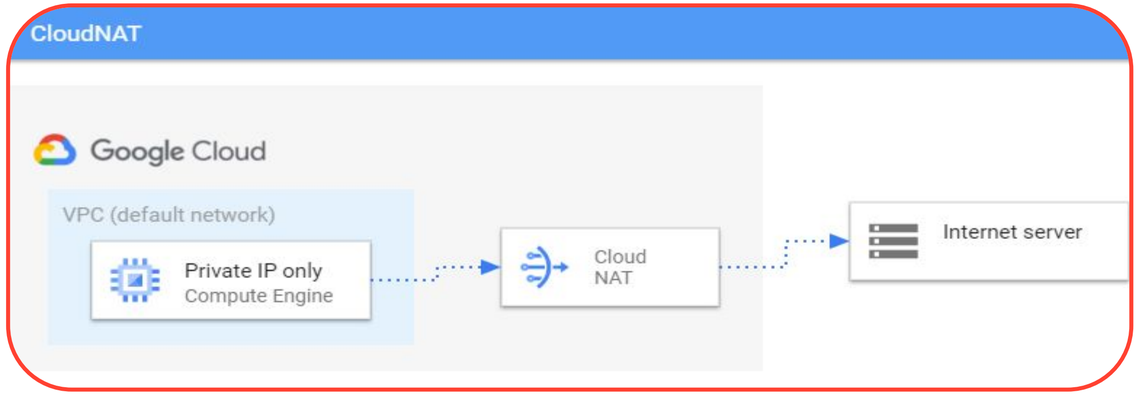


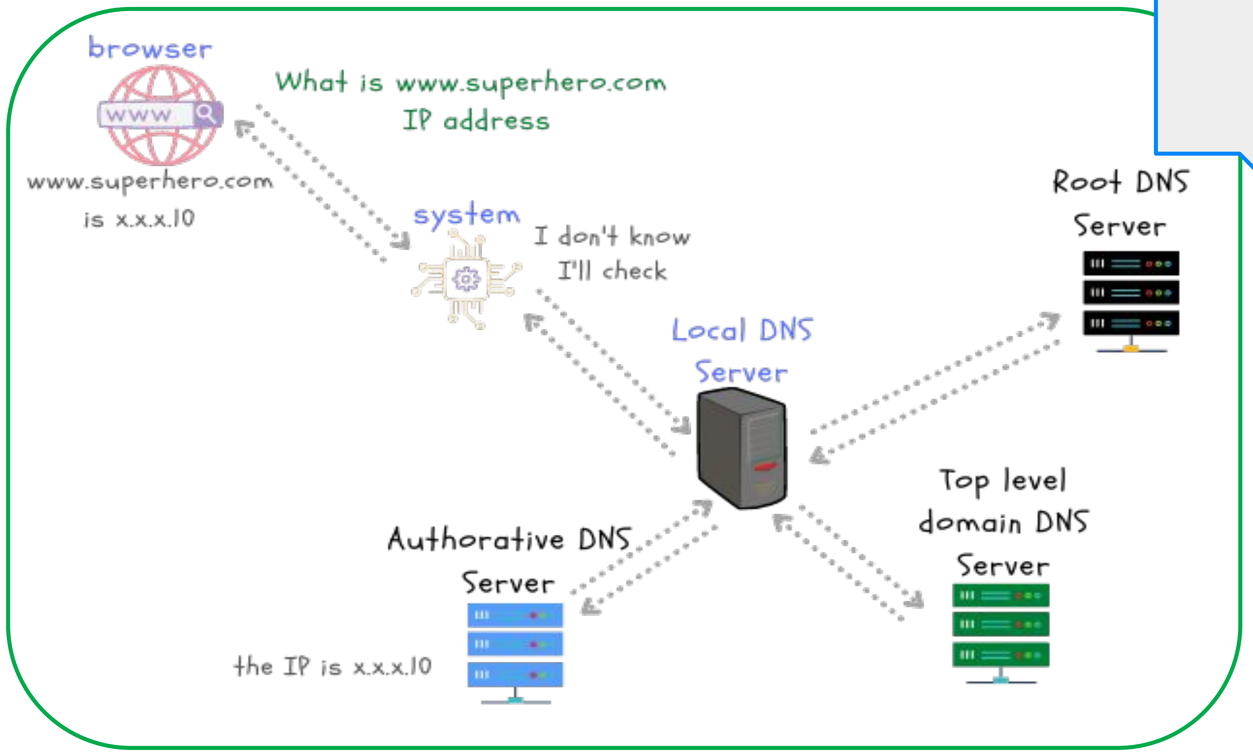
```
▷ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
◢ Ethernet II, Src: Standard_68:8b:fb (00:e0:29:68:8b:fb), Dst: 3com_1b:07:fa (00:20:af:1b:07:fa)
  ◢ Destination: 3com_1b:07:fa (00:20:af:1b:07:fa)
      Address: 3com_1b:07:fa (00:20:af:1b:07:fa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ◢ Source: Standard_68:8b:fb (00:e0:29:68:8b:fb)
      Address: Standard_68:8b:fb (00:e0:29:68:8b:fb)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 0101010101010101010101010101010101
◢ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4

0000  00 20 af 1b 07 fa 00 e0  29 68 8b fb 08 06 00 01   . ...... )h......
0010  08 00 06 04 00 02 00 e0  29 68 8b fb c0 a8 00 01   ........ )h......
0020  00 20 af 1b 07 fa c0 a8  00 02 01 01 01 01 01 01   . ...... ........
0030  01 01 01 01 01 01 01 01  01 01 01 01               ........ ....
```

ARP, RARP, DNS & NAT

Domain Name Service (DNS)	Resolves names to IP addresses
Cloud DNS	Google Cloud DNS offering
Internal DNS	Used internally within a private network
DNS Security Extensions (DNSSEC)	Uses digital signature to secure DNS information
Hybrid DNS	**DNS configured between** cloud and on-prem or external networks
Address resolution Protocol (ARP)	Protocol used to resolve IP address to a MAC/link layer address. Maintained in the ARP table.
Reverse ARP (RARP)	This is the inverse of ARP. Used to resolve MAC to IP addresses.
Media Access Control address(MAC)	Unique hexadecimal identifier assigned to a network interface controller (NIC) card. Usually a 12 digit hexadecimal number.
Network Address Translation (NAT)	Allows private IP ranges to communicate with the internet. Maintains a NAT table of private to public address & port mappings for communications.
Cloud NAT	Google Cloud managed NAT service





Networking 101 sheet .!!!

How can I configure Hybrid DNS?

- See, docs.

How is cloud NAT configured?

- See docs.

Can you use ARP inside a subnet in GCP?

- No, all communication between VMs only happens through the virtual gateway - no ARP between VMs is supported.

Routing, Cloud Router, Dynamic Routing, BGP, MPLS

Routing	Selecting a path for traffic to flow within internal networks or between different networks
Router	Allows communication between different networks
Cloud Router	Google Cloud router that allows you to dynamically exchange routes between your VPC and on-prem using BGP
Routing table	A repository of all the routing information within a network
Routing modes	These are static or dynamic
Static routing	These routes are fixed an don't update. They usually have to be manually adjusted
Dynamic routing	These routes update to reflect current state
Route summarization	Used to reduce the number of route advertised to neighbours. See **example**
next-hop	The address of the next router in the transit route of a packet
Software Defined Networking (SDN)	A software based networking approach that uses application programming interfaces (API) to communicate with underlying infrastructure to control the network traffic

Border Gateway Protocol (BGP)	Is the path vector protocol of the internet. Made up of Autonomous systems (AS) and uses TCP port 179
Autonomous System (AS)	Is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators
Autonomous System Number (ASN)	The number used to identify an AS. This can be 16 bit or 32 bit
External BGP (eBGP)	BGP connection formed between different AS's
Internal BGP (iBGP)	Connection formed within the same AS
Multiple Exit Discriminator (MED)	This a one of several BGP attributes used to influence path selection. This is non transitive and the lower metric wins
AS-path-prepend	This is one of several BGP attributes used to influence path selection. This is a mandatory attribute. The **shorter path** should be preferred
Multiprotocol label switching (MPLS)	This is a switching method that uses labels instead of IP information to transmit packets across the backbone core at high speed
Bidirectional Forwarding Detection (BFD)	This is a protocol that detects failure quickly on links when enabled. In GCP you can use this feature with Cloud router

Networking 101 sheet .!!!

What is Google Cloud Platform's network virtualization stack called?

- **Andromeda**

Max amount of BGP routes advertised to Cloud router?

- Presently 250. **See current limit here**

How can you control path selection using BGP attributes in GCP?

- **MED** is supported.

What is the ASN number used in GCP for partner interconnect?

- Presently **ASN 16550** is automatically assigned.

Data Center Networking

optical circuit switching	Maps optical input to output ports to form a connection
wave division multiplexing	WDM technology allows you to combine multiple optical signal onto a single optical fiber
Clos topology	A non blocking, multistage switching network, used in data center switching fabrics
Merchant switch silicon	Chip made by 3Ps that are sold to any consumers to design a product based on it
Data Center Fabric	This is a Data Center design comprised of leaf and spine switches that allows low latency and scalable data center operations.
Top-of-Rack switches	These switches are place in the same rack as other equipment to connect all equipment in the rack and to connect to other TOR switches in the DC
OpenFlow	OpenFlow is a communications protocol that allows network controllers to directly program the network forwarding plane
Leaf and Spine	A two layer full mesh topology. Has leaf switches and spine switches
East West traffic	Communication traffic flow between devices in a Data center
North South Traffic	In and out communication traffic flow between Data center and outside networks
Colocation	3P Data Center facilities where multiple tenants can house their data center equipment

Networking 101 sheet .!!!

How can I learn more about Google data centers?

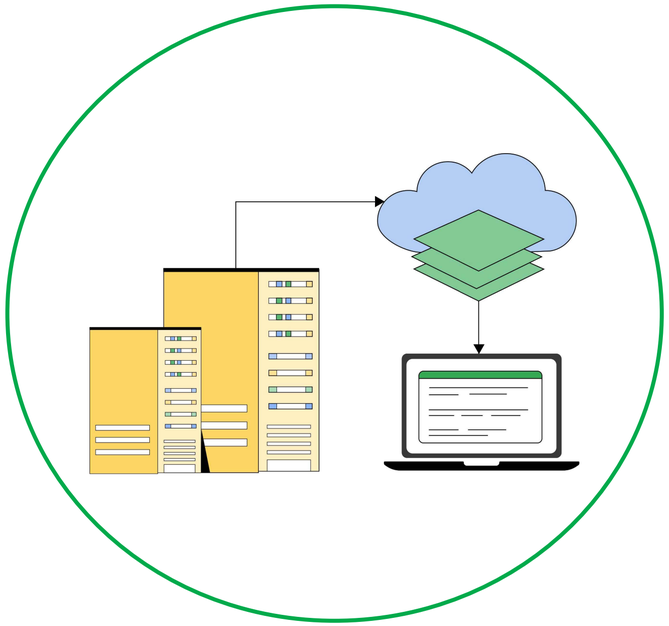
- **Check out Discovering Data Centers**

Where are the data Centers located?

- **Locations**

Are there any interesting publications?

- **Check out Jupiter Evolving**



Connectivity, Hybrid Connectivity

Dedicated Interconnect — Dedicated connection between Google and your private network. Available from 10 GBit/s to 100 GBit/s. Has high availability configurations and you can use multiple links

Partner Interconnect — Highly available connection between Google and your network provisioned through a Service provider. Available from 50 MBit/s to 10 GBit/s. Has high availability configuration and you can use multiple links

Virtual private network (VPN) — This offers a secure connection between two locations over a secure IPSEC tunnel

Cloud VPN — Google Cloud VPN service

Carrier Peering — Google Cloud service that enables you to access Google Workspace and other Google apps via service provider connection

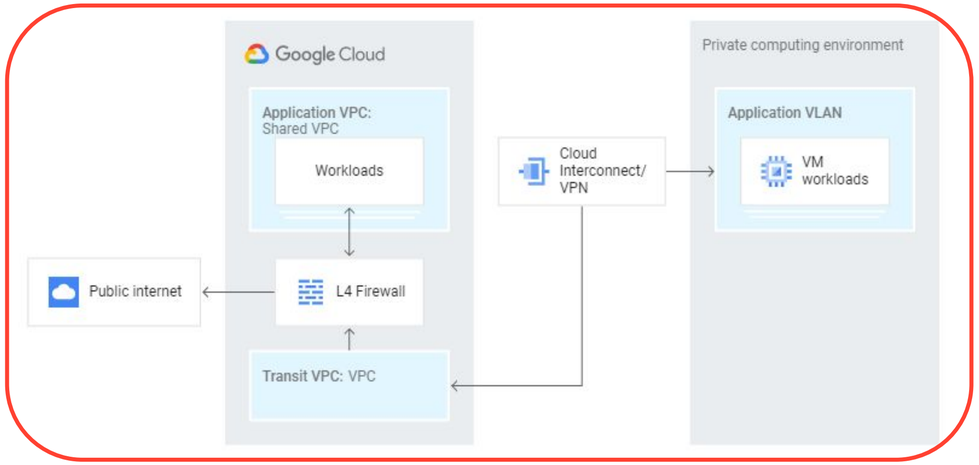
Direct Peering — Google Cloud service that enables you to access google Workspace and other Google apps via direct connection to Google edge

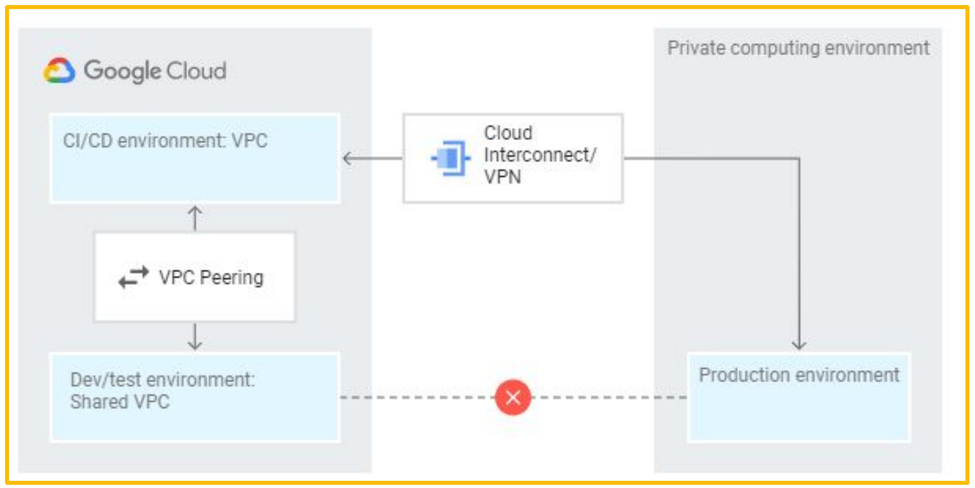
Shared VPC — GCP service that allow you to provision and connect host projects, and service projects

VPC Network Peering — GCP service that allow you to connect between different VPC's in the same or separate project and organizations. 1-to-1 peering that is not transitive. Max peering per VPC is 25 connections

Traffic Director — Google Cloud service that offers a fully managed traffic control plane for service mesh

Cross Cloud Interconnect — Dedicated connection between Google and your Cloud providers network. Available from 10 Gbps to 100 Gbps. Has high availability configurations and you can use multiple links





Networking 101 sheet .!!!

Shared VPC or **VPC** network peering?

- The best **practices VPC design document** will be helpful.

Are VPNs redundant?

- You have **high availability configuration options.**

Dedicated or Partner Interconnect?

- Depends on several **factors**.

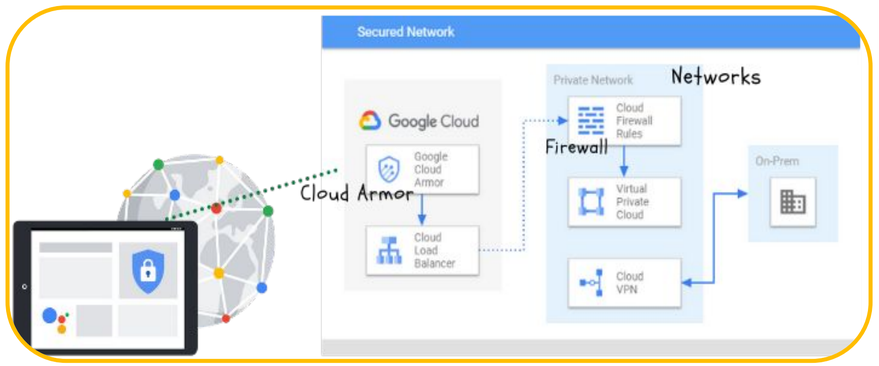
Can I connect to other cloud providers?

- Yes check out **Cross-Cloud Interconnect**.

Where can I find GCP Networking reference Architectures?

- **Cloud Architecture Centre**
- **Designing networking docs**

Network Security



Firewalls	Allow, deny & filter traffic based on rules. Affect ingress and egress traffic
Firewalls rules	Criteria used to deny, allow access in Google Cloud. e.g. IP, source, tag, service account
Distributed denial of service (**DDoS**)	This is a type of attack that affect availability of service by overloading the systems
Cloud Armor	Google Cloud service that provides filtering at OSI layer 7 to 4
VPC service controls	Google Cloud service that allows you the ability to create perimeters that protect resources and data
Cloud Identity-Aware Proxy (IAP)	Google Cloud service that controls access to your application and restricts it to only authorized users
Security Command Center	Google Cloud service that has asset discovery, threat detection, and threat prevention components
Beyond Corp	Google Cloud **zero trust model**
Cloud IDS	Google Cloud's Intrusion Detection System. Detect and logs potential threats

Networking 101 sheet .!!!

Tell me about Google Cloud Firewall?
- **Cloud Firewall doc.**

What can help with **DDoS attacks?**
- Cloud Armor, Autoscaling, Load balancing.

What are some Google Cloud security services**?**
- **Security and Identity products**

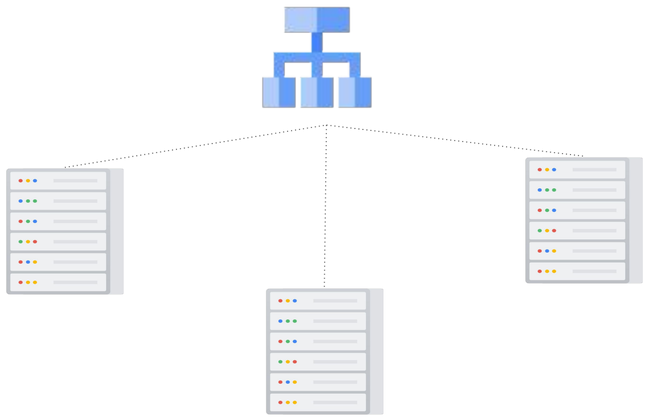
How are firewall rules read?
- From lowest 0 to highest 65535.

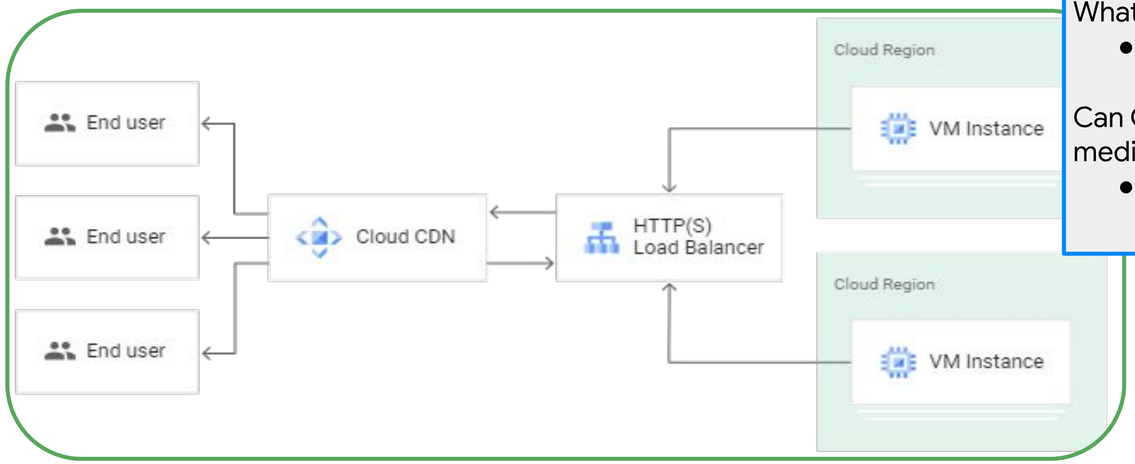
How does Cloud firewall handle connect state?
- These are stateful firewalls.

Traffic handling, Load balancing, Content Delivery

HTTP(S) LB	Global load balancer for HTTP(S) traffic
SSL proxy	Global load balancer for SSL traffic
TCP proxy	Global load balancer for TCP traffic
Network LB	Regional LB used to load balance TCP traffic (available internally and externally)
Internal LB	Regional LB used with a VPC
NEG	Network Endpoint Group are used to attach a backend pool to a load balancing service in Google Kubernetes Engine
Ingress	Allows HTTP(S) traffic connections to a kubernetes cluster
Content Delivery Network (CDN)	Caches content at a distribution endpoint closest to customer.
Cloud CDN	Google Cloud's standard web acceleration CDN offering.
Media CDN	Google Cloud's media delivery solution. Can handle high throughput media like streaming.

Hypertext Transfer Protocol (HTTP)	Protocol used for transmitting hypermedia documents. This is a standard on the internet, more commonly in it secure form HTTP(S)
HTTPS	Secure version of HTTP enabled by using TLS on the connection





Networking 101 sheet .!!!

What is a Global LB?
- Operates globally and can load balance and spill over traffic between regions.

What is a regional LB?
- Operate in the region it is created.

What type of LB exist in Google Cloud?
- See summary of LB

How does CDN reduce latency?
- By returning traffic to the user from the closest networking point.

What is Google LB software called.
- It's called Maglev

Can Google Cloud support streaming media?
- Yes, Media CDN supports this

Troubleshooting & Monitoring

ping	This tool checks the availability of host by using Internet Control Message Protocol
Traceroute or tracert	Shows the hops between source and destination
nslookup	Allows you to resolve IP from host name
Domain information groper (dig)	Performs DNS lookup and displays the answers of the query
ipconfig or ifconfig	Show the IP address, subnet and gateway information of a system
Flow logs	This GCP service tells you about the traffic flow in your VPC
Network Intelligence Center	GCP service that provides you with a few tools to gain visibility into your network
Cloud Audit Logs	Google Cloud logs that provide information on activities in your cloud. A few are; Admin Activity, Data Access, system events and Policy denied, audit logs
Cloud Operations	Google Cloud tool that allows you to monitor, log and trace application and systems in your environments
Packet Mirroring	Packet Mirroring clones the traffic on the network and forwards it for examination. See more here
My Traceroute (MTR)	Is an application that combines the functions of the traceroute and ping programs in one network diagnostic tool

Service Directory	A GCP managed service that gives you a single place to publish, discover, and connect services
Tcpdump & wireshark	tcpdump is a command-line packet analyzer. Wireshark is a packet inspector.

```
C:\Users\[redacted]>nslookup google.com
Server:  mynetwork
Address:  192.168.2.1

Non-authoritative answer:
Name:    google.com
Addresses:  2607:f8b0:400b:803::200e
          142.251.41.78
```

```
Pinging www.google.com [142.251.32.68] with 32 bytes of data:
Reply from 142.251.32.68: bytes=32 time=3ms TTL=115
Reply from 142.251.32.68: bytes=32 time=5ms TTL=115
Reply from 142.251.32.68: bytes=32 time=5ms TTL=115
Reply from 142.251.32.68: bytes=32 time=3ms TTL=115
```

Networking 101 sheet .!!!

What protocol does ping use?

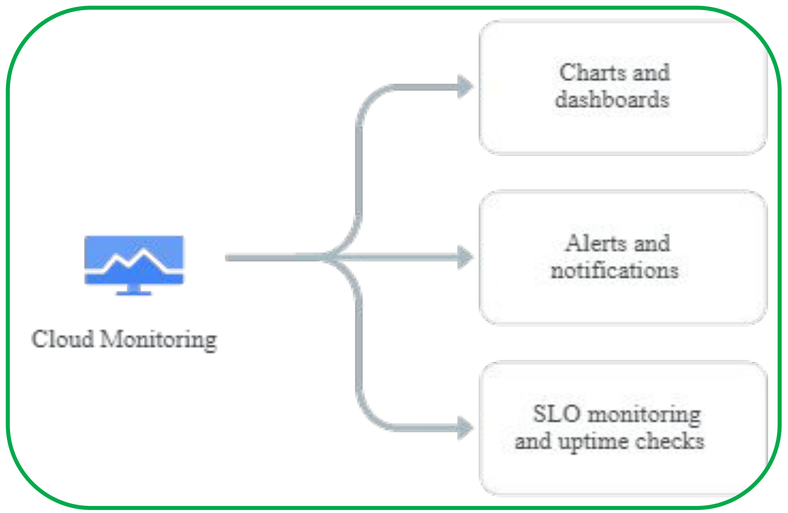
- Internet Control Message Protocol (ICMP)

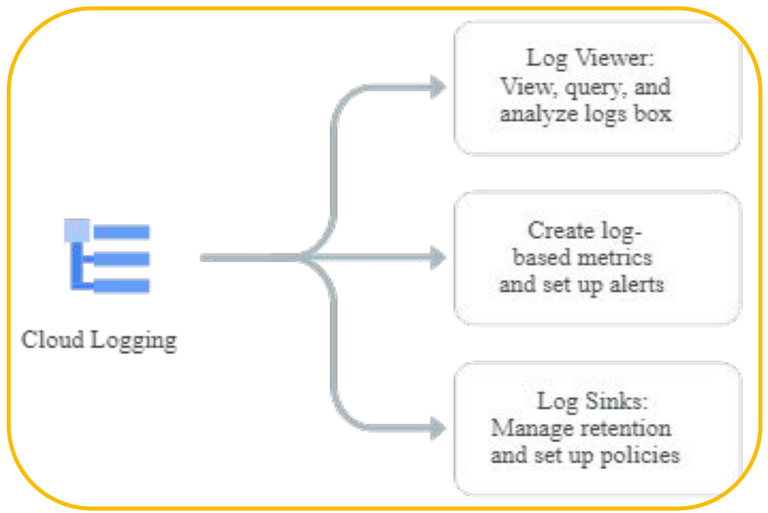
Are flow logs enabled by default on GCP?

- This has to be enabled by user

What are the component of Network Intelligence Center?

- This is made up of
  - Network Topology
  - Connectivity test
  - Performance dashboard
  - Firewall Insights





What happens when you type www.google.com in a browser

Networking 101 sheet .!!!

#1 Open browser type www.google.com

#2 Browser cache is checked to see if IP information was cached

#3 If #2 has no infor system checks host file for address information

#4 If #3 has no info, system queries local DNS

#5 If #4 has no info query sent to Service Provider (SP) DNS

#6 If SP has no info query sent to Root level DNS

#7 Root level returns the Top level DNS

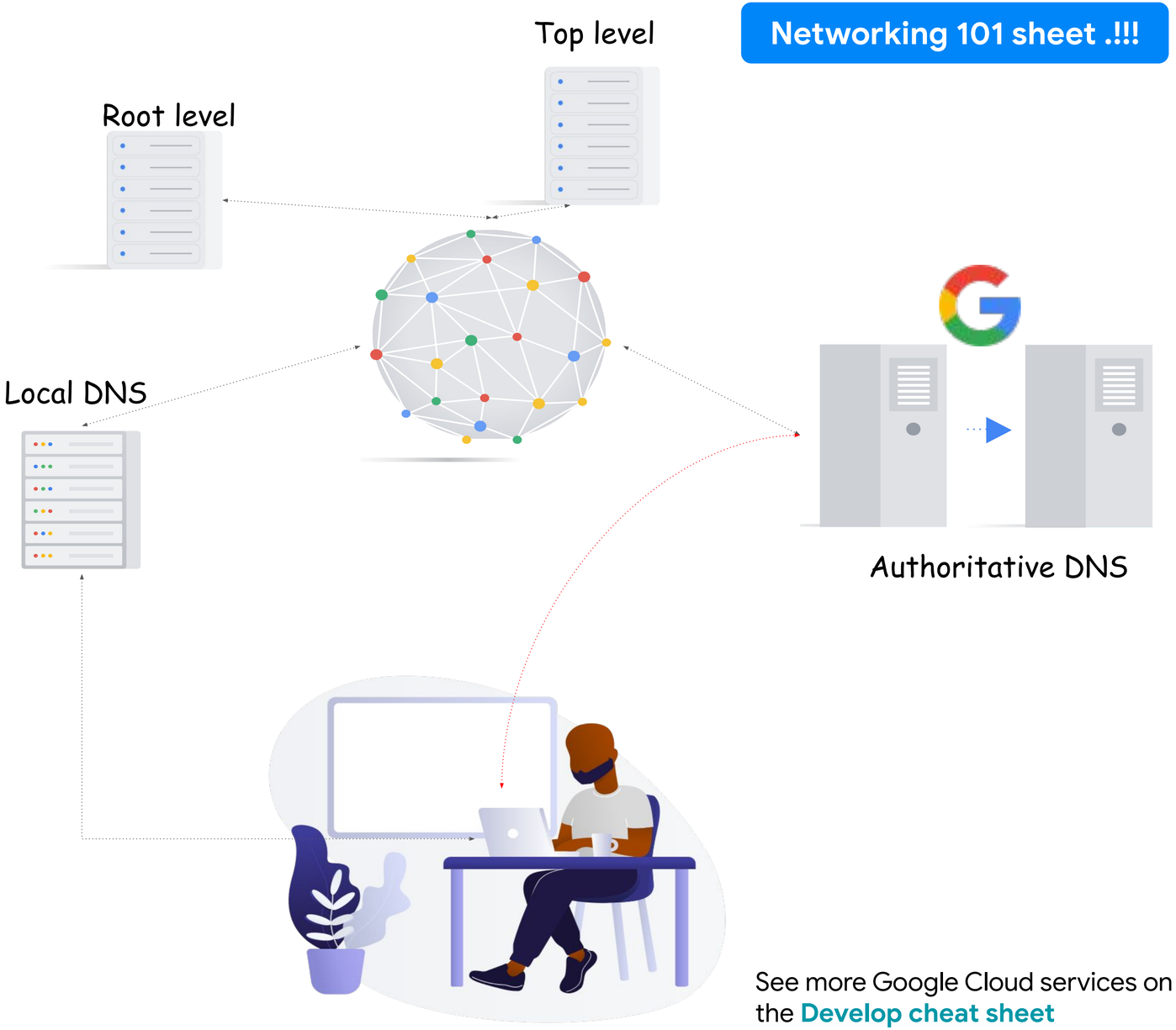
#8 Top level DNs returns the Authoritative DNS who has the record

#9 Authoritative DNS returns a DNS response with the IP address and DNS TTL information

#10 The system now has the IP address and initiates a TCP connection to the server

#11 TCP three-way handshake takes place, TLS Secure authentication process takes place and secure connection is setup.

#12 HTTP(S)/HTML process begins to return information as required



See more Google Cloud services on the **Develop cheat sheet**