Cloud Networking

Cloud-Foundations-Infrastructure Fundamentals

[Pick the date]

[Type the company name]

Chhaya Nikam

# Cloud Networking

## OSI model (Open Systems Interconnection)

OSI (Open Systems Interconnection) is a reference model for how applications communicate over a network. This model focuses on providing a visual design of how each communications layer is built on top of the other, starting with the physical cabling, all the way to the application that's trying to communicate with other devices on a network.

A reference model is a conceptual framework for understanding relationships. The purpose of the OSI reference model is to guide technology vendors and developers so the digital communications products and software programs they create can interoperate and to promote a clear framework that describes the functions of a networking or telecommunications system that's in use.

### 7 layers of the OSI model

What is the function of each layer of the OSI model? The seven Open Systems Interconnection layers are the following.

#### Layer 7. The application layer

The application layer enables the user -- human or software -- to interact with the application or network whenever the user elects to read messages, transfer files or perform other network-related tasks. Web browsers and other internet-connected apps, such as Outlook and Skype, use Layer 7 application protocols.

#### Layer 6. The presentation layer

The presentation layer translates or formats data for the application layer based on the semantics or syntax the application accepts. This layer also handles the encryption and decryption that the application layer requires.

#### Layer 5. The session layer

The session layer sets up, coordinates and terminates conversations between applications. Its services include authentication and reconnection after an interruption. This layer determines how long a system will wait for another application to respond. Examples of session layer protocols include [X.225](https://www.techtarget.com/whatis/definition/ITU-X225) and Zone Information Protocol (ZIP).

#### Layer 4. The transport layer

The transport layer is responsible for transferring data across a network and provides error-checking mechanisms and data flow controls. It determines how much data to send, where it gets sent and at what rate. TCP within the TCP/IP suite is the best-known example of the transport layer. This is where the communications select TCP port numbers to categorize and organize data transmissions across a network.

#### Layer 3. The network layer

The primary function of the network layer is to move data into and through other networks. Network layer protocols accomplish this by packaging data with correct network address information, selecting the appropriate network routes and forwarding the packaged data up the stack to the transport layer. From a TCP/IP perspective, this is where IP addresses are applied for routing purposes.

#### Layer 2. The data-link layer

The data-link, or protocol layer, in a program handles moving data into and out of a physical link in a network. This layer handles problems that occur as a result of bit transmission errors. It ensures that the pace of the data flow doesn't overwhelm the sending and receiving devices. This layer also permits the transmission of data to Layer 3, the network layer, where it's addressed and routed.

The data-link layer can be further divided into two sublayers. The higher layer, which is called logical link control (LLC), is responsible for multiplexing, flow control, acknowledgement and notifying upper layers if transmit/receive (TX/RX) errors occur.

The media access control sublayer is responsible for tracking data frames using MAC addresses of the sending and receiving hardware. It's also responsible for organizing each frame, marking the starting and ending bits and organizing timing regarding when each frame can be sent along the physical layer medium.

#### Layer 1. The physical layer

The physical layer transports data using electrical, mechanical or procedural interfaces. This layer is responsible for sending computer bits from one device to another along the network. It determines how physical connections to the network are set up and how bits are represented into predictable signals as they're transmitted either electrically, optically or via radio waves.

## TCP/IP Model aka Department of defence model

It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

we will be talking on the behalf of the receiver.

### 1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.  
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

### 2. Internet Layer –

This layer parallels the functions of OSI’s Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:  
   IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

### 3. Host-to-Host Layer –

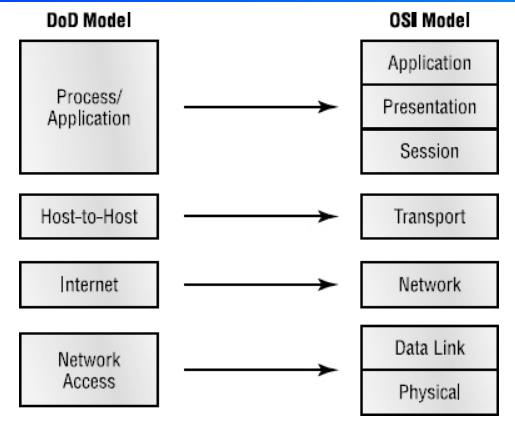
This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

### 4. Application Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

* + 1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
    2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
    3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.



## Virtual networking in Cloud

**Virtual networking** enables communication between multiple computers, virtual machines (VMs), virtual servers, or other devices across different office and data center locations. While physical networking connects computers through cabling and other hardware, virtual networking extends these capabilities by using software management to connect computers and servers over the Internet. It uses virtualized versions of traditional network tools, like switches and network adapters, allowing for more efficient routing and easier network configuration changes.

## What is a region?

The simplest explanation is that a “cloud region” describes the actual, real-life geographic location where your public cloud resources are located.

When you choose a cloud provider, you’re also choosing a “region,” which is where your data centers physically exist. However, while providers all define what a region is in a similar way, they differ in implementation.

## Why are regions important?

Regions allow you to locate your cloud resources close to your customers, both internal or external. The closer your customers are to the region where your cloud resources are located, the faster and better their experience will be. For example, if your customers are located in Germany, it makes sense to choose a European region for your cloud region, even if your office is in Delaware.

Regions are also commonly used as part of disaster recovery (DR) strategy. While many public cloud users depend on the reliability and redundancy of inter-region resources for DR, some use multiple regions to achieve the same result. Sometimes this is required for regulatory or compliance reasons, but sometimes it’s simply company policy.

## How to choose a region

### Latency

If you’re a gamer, you know how vital latency is. If you have a low latency connection, when you pull the trigger in your game, there’s little to no lag. But if you have a high latency connection, when you pull the trigger, other people in the game with faster connections have killed your character before you’ve even had a chance to reload.

If your data center is in Thailand and your customers are in Arizona, they’re going to experience latency simply due to distance. So, the first thing you need to do is determine where most of your customers are and choose a region that’s closest to them.

## Cost

It costs money to run data centers, and depending on real estate costs, energy costs, and taxes, a cloud region can cost more money in some areas than in others. For instance, a cloud region in the Bay Area may cost more than a cloud region in Ohio because all those tech companies are competing for a small area of real estate. On the other hand, there’s plenty of open land in Ohio, so the cloud region is less expensive. The costs to maintain data centers are passed on to you, so a more expensive region will equal higher costs on your end.

## Compliance and security

Every company has different security requirements based on its industry, location, etc. It’s also important to know what the compliance laws are in your country so that you aren’t fined and so you don’t lose the trust of your customers. As you look into different options, stick to a cloud region that makes it easier for your company to adhere to those standards.

## Compute and processor features

What’s inside the data center matters as much as where the center is located. If you require the latest, most up-to-date compute and processing, you may not want to choose a cloud provider that relies on hardware that’s five years old. For instance, some may use Ivy Bridge microarchitecture, which could be fine for your business. But if you really want cutting-edge speed and power, you may need to look for a provider that uses Haswell processors.

## Services and features

Services vary region by region. For instance, check out [this chart](https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/) from AWS. You’ll notice the difference in features varies widely. If having Alexa for Business is vital to your company, your only option is choosing a Northern Virginia region. Jot down the features and services that are non-negotiable for you as you begin your cloud provider hunt so you know what to look for.

### Disaster recovery

Having a down network could cost your business millions, so redundancy is important. Some companies have redundant data centers in the same region, and the two data centers may only be separated by a few miles. That means if a tsunami hits, both centers are likely to be affected. When you’re searching for a cloud region, see where the backup cloud is located.

## Information about top cloud providers

Here’s the cheat sheet summary to regions: When researching cloud regions, look at the closest regions first, determine if you can afford those regions, and then look at security and redundancy features.

To help out, we’ve gathered useful info about some of the top cloud providers.

### Amazon Web Services

**Region:** Amazon defines its region as a geographic location, though it’s somewhat arbitrary.

**Local regions:** A single data center, in close proximity to a region, but not part of that region.

**Availability zone:** Multiple availability zones (AZs) per region are physically separated and connected with private low latency, high throughput, and redundant network connections.

The first AWS regions were launched with two AZs, except Singapore, which launched with a single AZ. New regions typically launch with three or more AZs. AWS currently has 18 regions composed of 55 AZs, one local region in Osaka, and plans for five more regions and 15 more AZs.

**Additional resources:**  
[aws.amazon.com/about-aws/global-infrastructure](https://aws.amazon.com/about-aws/global-infrastructure/)

### Google Cloud Platform

**Regions:** Regions are built of zones, usually close to each other, within P95 RT latencies less than 1MS and generally less than 5MS.

**Zones:** Zones should be considered independent failure domain within the region. Zones don't always map to a single data center.

Google currently has 18 regions and 55 zones. All regions have three or more zones, and one zone is in development.

**Additional resources:**  
[cloud.google.com/about/locations](https://cloud.google.com/about/locations/)  
[cloud.google.com/docs/geography-and-regions](https://cloud.google.com/docs/geography-and-regions)

### Microsoft Azure

**Region:** A region is a set of data centers connected within a latency perimeter.

Microsoft has 42 regions. 12 more regions are planned, 5 current regions have availability zones, and two have AZs in preview.

**Geography:** Azure defines a “geography” to contain multiple regions to help maintain data residency and compliance.

**Availability zones:** These are one or more data centers built on independent infrastructure with a minimum of three AZs in regions that support it.

**Additional resources:**  
[azure.microsoft.com/en-us/global-infrastructure/regions](https://azure.microsoft.com/en-us/global-infrastructure/regions/)  
[docs.microsoft.com/en-us/azure/availability-zones/az-overview](https://docs.microsoft.com/en-us/azure/availability-zones/az-overview)

**What is a public endpoint?**

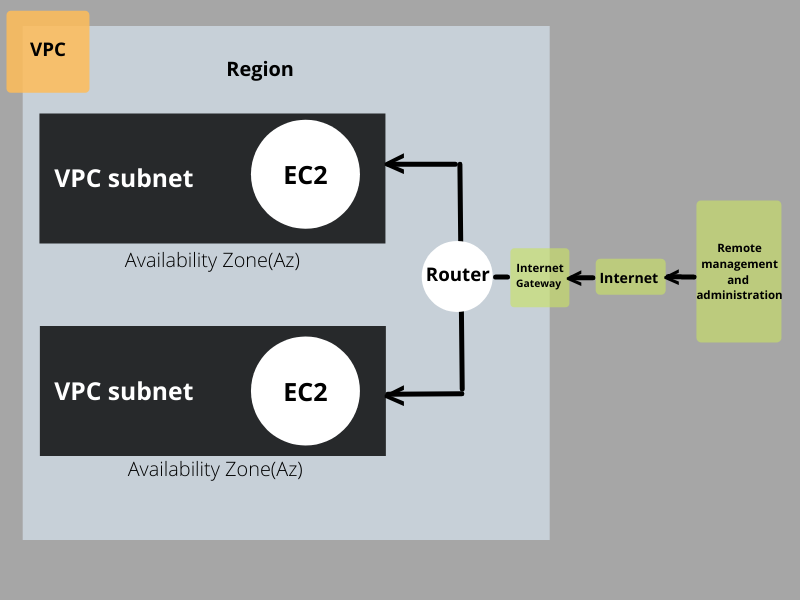
Public endpoint for a managed instance **enables data access to your managed instance from outside the virtual network**. You are able to access your managed instance from multi-tenant Azure services like Power BI, Azure App Service, or an on-premises network.

A private endpoint is **a network interface that uses a private IP address from your virtual network**. This network interface connects you privately and securely to a service that's powered by Azure Private Link. By enabling a private endpoint, you're bringing the service into your virtual network

### ****Components of Amazon VPC:****

* ***Subnet:*** It is a section of a VPC that can contain resources such as Amazon EC2 services and shares a common address component. *Public Subnet*where resources are exposed to the internet through Internet Gateway and *Private Subnet*where resources are not exposed to the outside world.
* ***Route Table:*** They are the set of rules used to decide where the network traffic has to be managed. It specifies the destination i.e, IP address and target. The target can be Internet gateway, NAT gateway, Virtual private gateway, etc.
* ***Virtual Private Gateway:*** It is the VPN(Virtual Private Network) hub on the Amazon side of the VPN connection to have a secure transaction. Users can attach it to the VPC from which they want to create the VPN connection.
* ***NAT Gateway:***Network Address Translation (NAT) Gateway is used when higher bandwidth, availability with lesser management effort is required. It updates the routing table of the private subnet such that it sends the traffic to the NAT gateway. It supports only UDP, TCP, and ICMP protocols.
* ***VPC Peering:***A VPC peering connection allows you to route traffic between two Virtual Private Clouds using IPv4 or IPv6 private addresses. Users can create a VPC peering connection between their own VPC with a VPC in another AWS account. This connection helps you to smoothly transfer the data.
* ***Security Groups:***It consists set of firewalls rules that control the traffic for your sample. You can have a single security group associated with multiple instances.
* ***Elastic IP:***It is a static IP address which is a reserved public IP address that can be assigned to any Instance in a particular region and never changes.
* ***Network Access Control Lists (NACL):***It is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. It adds an additional layer of security to your VPC.
* ***Customer Gateway:***VPN connection links your network (or data) to your Amazon VPC (virtual private cloud). A customer gateway is a presenter on your side of that connection. It can be a physical or software appliance.
* ***Network Interface:***It’s a connection between private and public networks. Network traffic is automatically shifted to the new instance if you move it from one instance to the other.
* ***VPC Endpoints:***It allows VPC to make a connection with other services of AWS without using the internet. They are of two types, Interference endpoints, and  Gateway endpoints. They are scaled, redundant, and highly available VPC components.

The below image will give you an architectural view of Amazon VPC:



### Benefits Of Using AWS Virtual Private Cloud:

Following are the benefits of using AWS VPC:

* **Efficient coordination:**VPC can scale to a vast extent and users have total control over a network size including automation resources.
* **Protection:**VPC environment is more secure and its resources contain cloud infrastructure which uses firewalls to protect the system from internet attacks.
* **Enhanced performance:**VPCs enable a hybrid cloud environment in which a VPC is used by an organization as an extension of their database instead of having to deal with the complexity of building an on-premises private cloud.
* **Low Cost:** VPCs are within a public cloud so the cost is quite economical.
* **East to use:**AWS VPC can be easily created using AWS Management Console in two ways; first by creating manually and second through Start VPC Wizard.
* **Variety of Connectivity Options:**AWS VPC can be connected to a variety of resources, such as the internet, other VPCs account, VPN connection,