Network Fundamentals for Cloud

BITS Pilani
Pilani Campus

Nishit Narang
WILPD-CSIS

innovate achieve lead

BITS Pilani
Pilani Campus

CC ZG503: Network Fundamentals for Cloud

Lecture No. 13: Multi-DC Networking

Need for Multi-DC Networks

- Distributed Redundancy
- Load Sharing
- Nearest service for users in different locations, improving user experience

For one or more of above reasons, service subsystems are deployed across DCs

Multi-DC Service Scenarios

- Service scenarios of multiple DCs include:
  - cross-DC service deployment
  - geo-redundancy
  - network-level DR, and
  - distributed cloudification

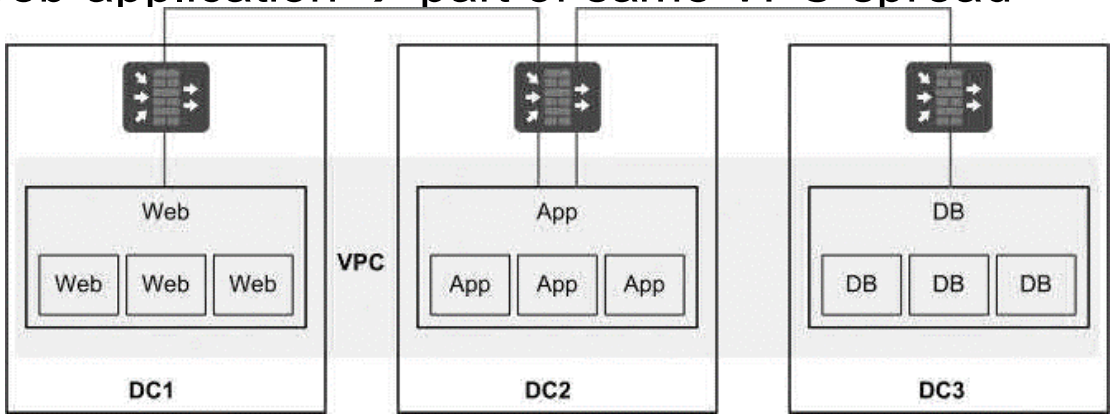
  These are discussed in subsequent slides

Source: Lei Zhang, Le Chen. Cloud Data Center Network Architectures and Technologies, CRC Press 2021

Cross-DC Service Deployment

- Modern applications need to be implemented by multiple or even hundreds of subsystems
- At times, the scale of a single DC is limited => one DC cannot accommodate all subsystems
- In such cases, different subsystems of the applications are deployed in different DCs
- Example: the three-tiers of a web-application → part of same VPC spread across DCs

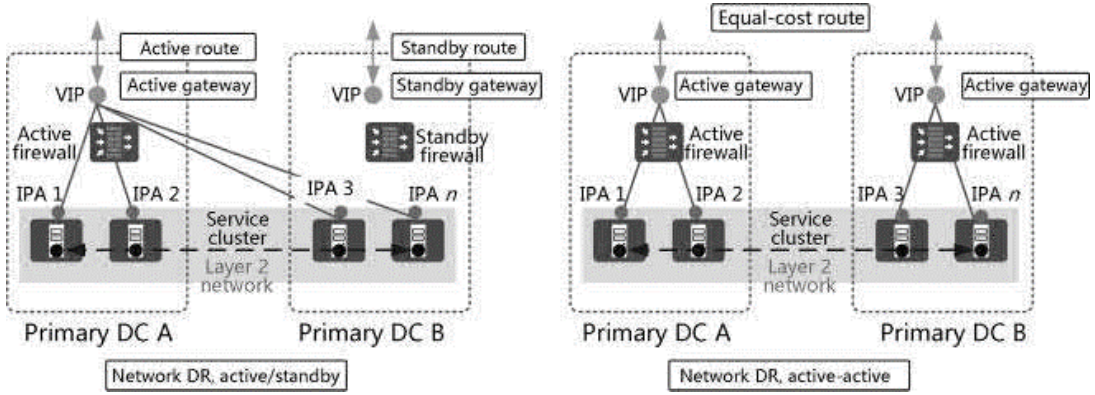
In this case, the network needs to provide interworking capabilities between DCs to ensure smooth interaction at the service layer



Source: Lei Zhang, Le Chen. Cloud Data Center Network Architectures and Technologies, CRC Press 2021

Network-level DR

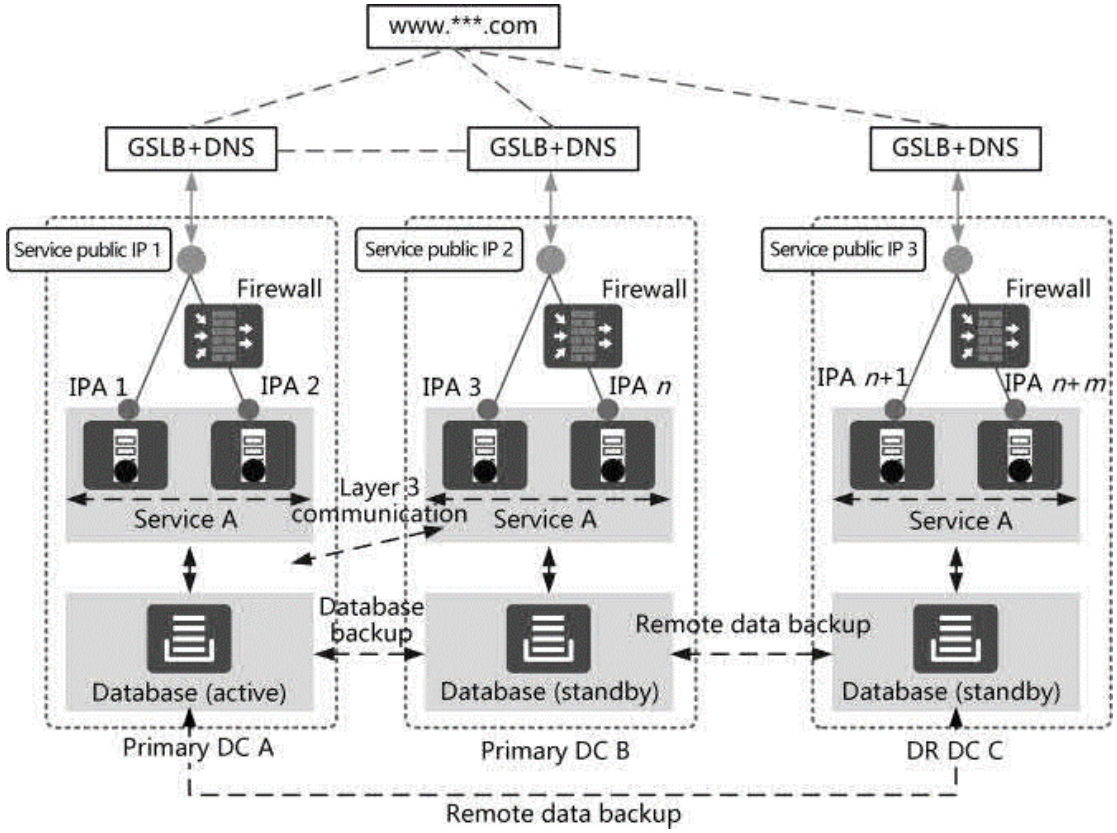
- Some modern applications need to be implemented using cluster software
- Multiple servers on a network are associated by the cluster software and appear as a logical server to the rest of the network, using a virtual IP address (VIP)
- Server clusters can be spread across DCs
- Cluster software of most vendors requires Layer 2 interconnection between servers; therefore, deployment of server clusters across DCs requires the network to provide large Layer 2 network capabilities across DCs.



Source: Lei Zhang, Le Chen. Cloud Data Center Network Architectures and Technologies, CRC Press 2021

Geo-Redundancy DC Solution

- A remote DR DC is added to synchronize data with two active-active (primary) DCs in the same city
- Active-Active DCs in same city:
  - Traffic is routed to application servers in different DCs through load balancing
  - provide services for users, doubling service capabilities and performing DR in real time
  - Subsystems in different DCs need to communicate with each other at Layer 2 and Layer 3 (DCI network requirements)
- The remote DR DC is the backup of the two active-active DCs. It is used to back up the data, configurations, and services of the two active-active DCs.
- If a fault occurs in the two active-active DCs due to natural disasters, the remote DR DC can quickly recover data and applications to ensure normal service operation and reduce loss

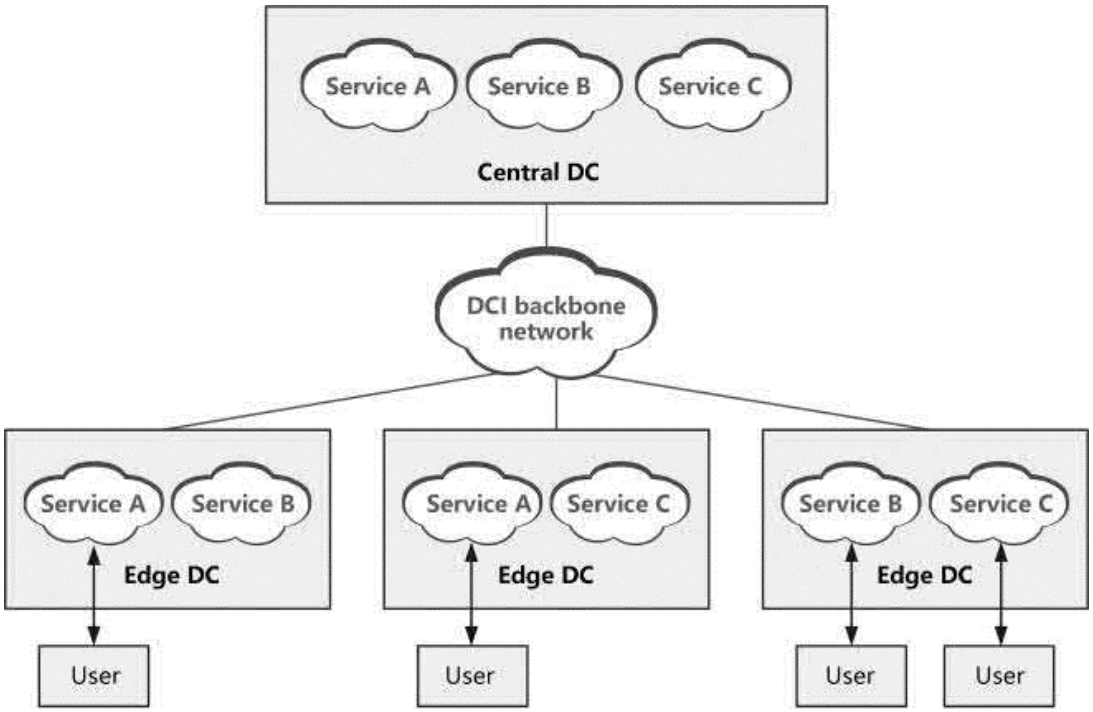


* GSLB = Global Server Load Balance

Source: Lei Zhang, Le Chen. Cloud Data Center Network Architectures and Technologies, CRC Press 2021

Distributed Cloudification Architecture

- Multiple sites work in active-active mode, and edge DCs provide services close to users, ensuring a short latency and good user experience
- Multiple DCs are interconnected through the DCI backbone network
- The central DC is the main source of data and pushes the content to edge DCs through the backbone network
- The edge DCs send the content to users
- During this process, multiple DCs need to communicate with each other at both Layer 2 and Layer 3



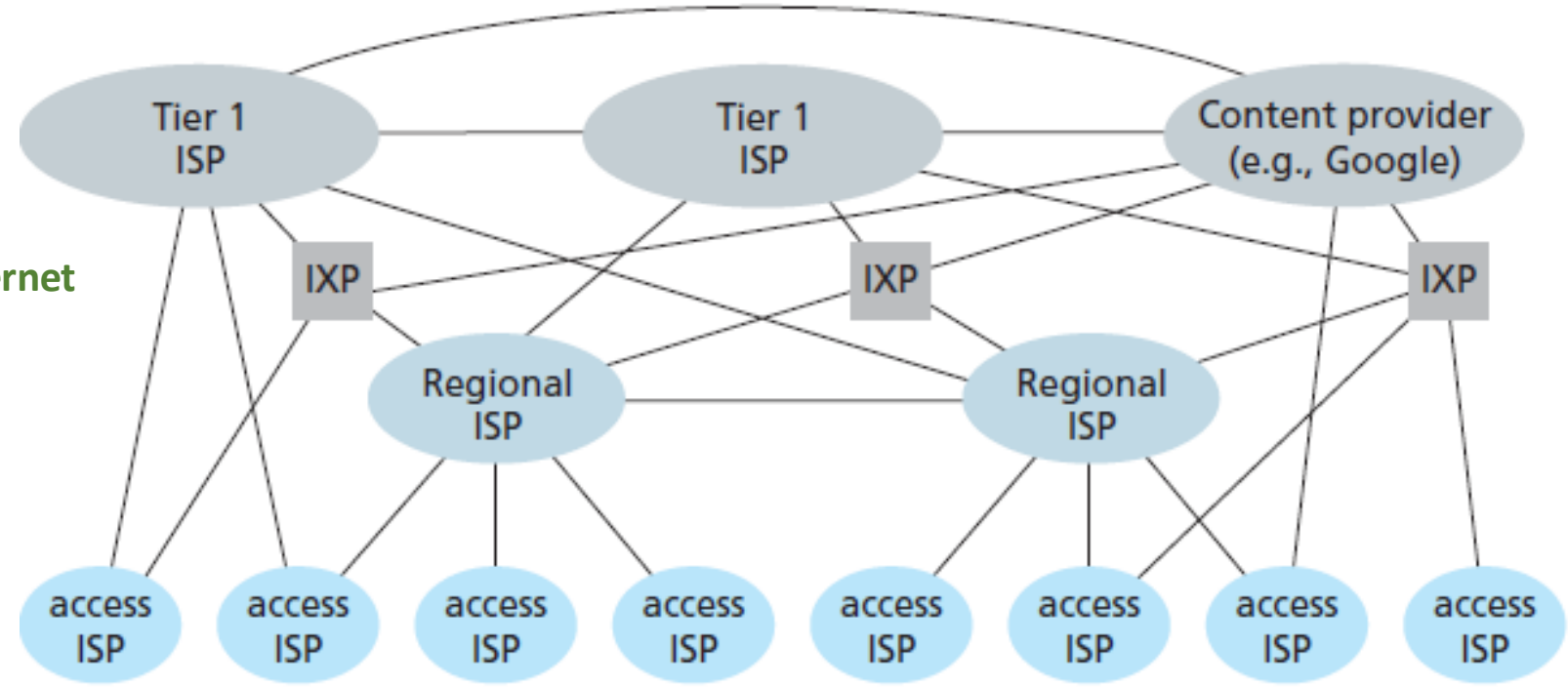
Source: Lei Zhang, Le Chen. Cloud Data Center Network Architectures and Technologies, CRC Press 2021

Multi-DC Service Example: Content Delivery Networks

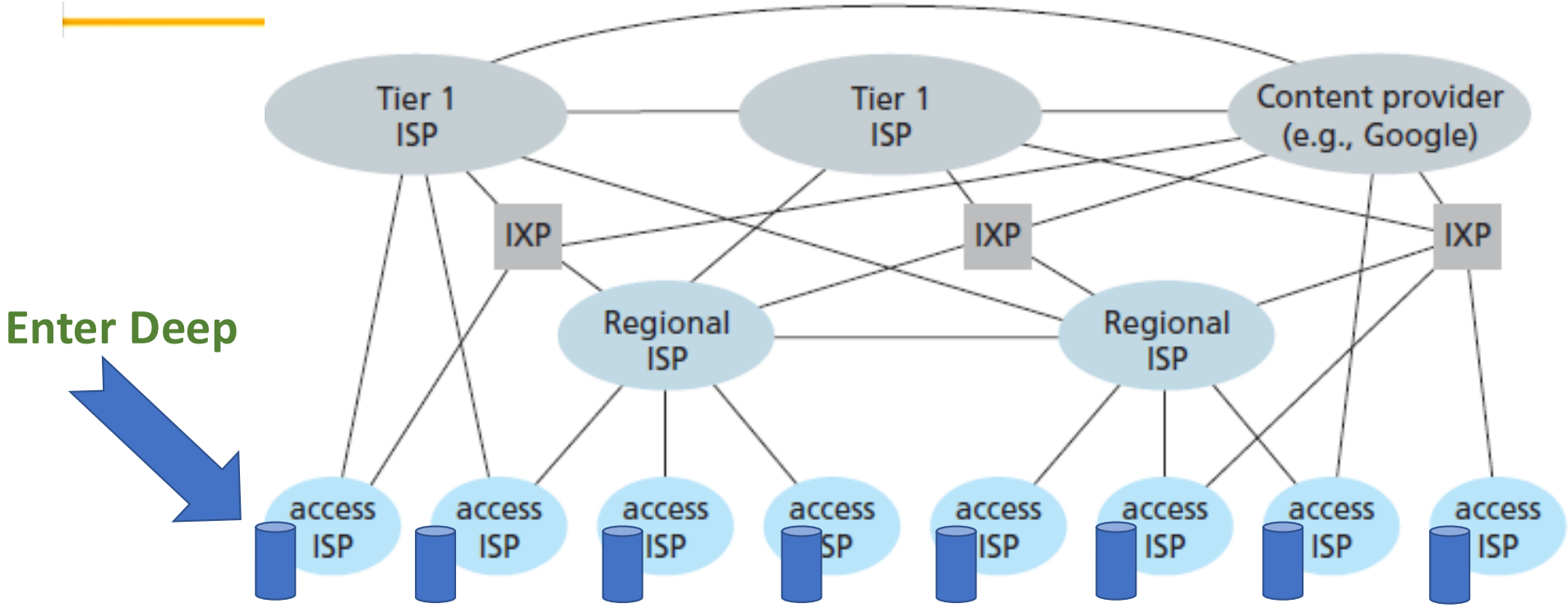
- Special types of Networks focused towards Content Delivery
  - E.g. You Tube Videos
- A simple CDN can be implemented as a special type of DCN
  - Challenges with a single massive data center
    - Single Point of Failure
    - Higher delays to certain locations
- Distributed Approaches
  - Mirror Sites
  - Proxy Caches
  - Content Delivery Networks
    - Manage servers in multiple geographically distributed locations
    - Distribute content from the “best” server to maximize user experience

CDN Server Placement Strategies

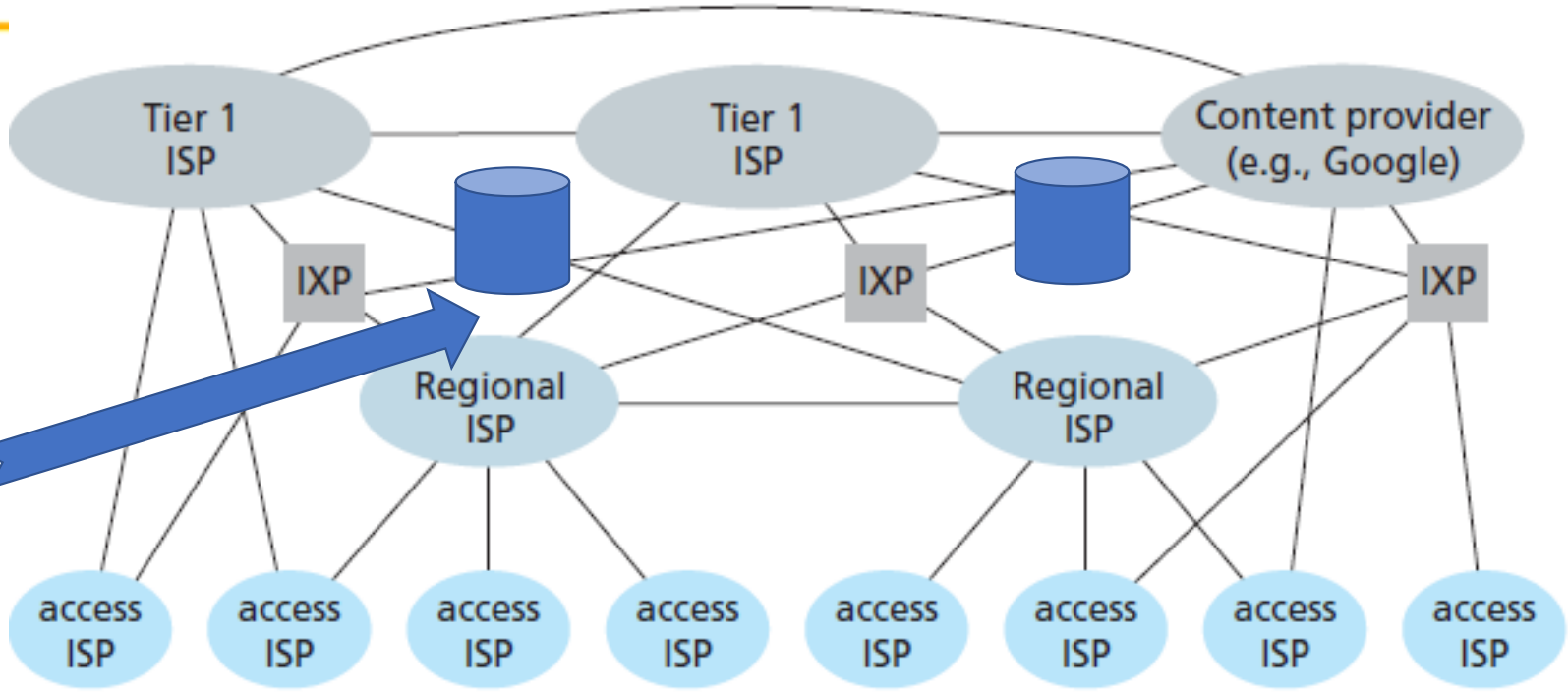
Multi-Tier Internet Architecture



CDN Server Placement Strategy #1



CDN Server Placement Strategy #2



Bring Home

CDN Server Selection Strategy

- Geographical proximity to the client
  - Makes use of geographic location mapping of Local DNS server IP addresses
- Current traffic conditions
  - Periodic real-time measurements of delay and loss performance between clusters and clients
- IP anycast
  - Routers in the Internet route the client's packets to the "closest" cluster, as determined by BGP
  - CDN company assigns the same IP address to each of its clusters
  - Uses standard BGP to advertise this IP address from each of the different cluster locations

Multi-DC Networking Requirements

- **REQ#1:** L2 Networking across DCs:
  - Example: Cross-DC Service Deployment → an independent VPC that crosses multiple fabric networks for a large website.
    - VMs within the VPC communicate at Layer 2.
- **REQ#2:** L3 Networking across DCs:
  - Example: Service Interworking → customers can allocate different services to different VPCs that may be deployed on different fabric networks.
    - To implement service interworking, the VPCs need to communicate with each other across fabric networks at Layer 3.
    - Layer 3 communication is typically used between VPCs.
- **REQ#3:** Data synchronization and backup → storage interconnection

Source: Lei Zhang, Le Chen. Cloud Data Center Network Architectures and Technologies, CRC Press 2021

Multi-DC Networking Technologies

- **REQ#3:** Data synchronization and backup → storage interconnection
  - Storage interconnection is implemented through Dense Wavelength Division Multiplexing (or DWDM) devices or bare optical fibers
  - DWDM or bare optical fibers provide direct physical links
  - The advantage of this interconnection mode is that exclusive channels can fully meet requirements for high bandwidth and low latency for traffic interaction between DCs.
  - In addition, the channels can carry data transmission of multiple protocols and provide flexible SAN/IP service access.
  - This mode supports traffic transmission of both the IP SAN and FC SAN

Source: Lei Zhang, Le Chen. Cloud Data Center Network Architectures and Technologies, CRC Press 2021

Multi-DC Networking Technologies (Contd.)

- **REQ#1:** L2 Networking across DCs
  - Option 1: Virtual Private LAN Service (VPLS)
    - a type of L2VPN technology based on MPLS and Ethernet technologies
    - connects multiple Ethernet networks across a public network to enable the Ethernet networks to function as a single LAN
    - Disadvantage: deployment is complex, and the MPLS network needs to be leased from a carrier or built by yourself
  - Option 2: Use of VXLAN [PREFERRED OPTION]
    - provides L2VPN services on the IP core network through VXLAN tunnels
    - can provide Layer 2 interconnection for scattered physical sites based on the Internet
    - is low cost and enables long-distance connections and easy expansion
    - Disadvantage: network quality is restricted by the IP network

Source: Lei Zhang, Le Chen. Cloud Data Center Network Architectures and Technologies, CRC Press 2021

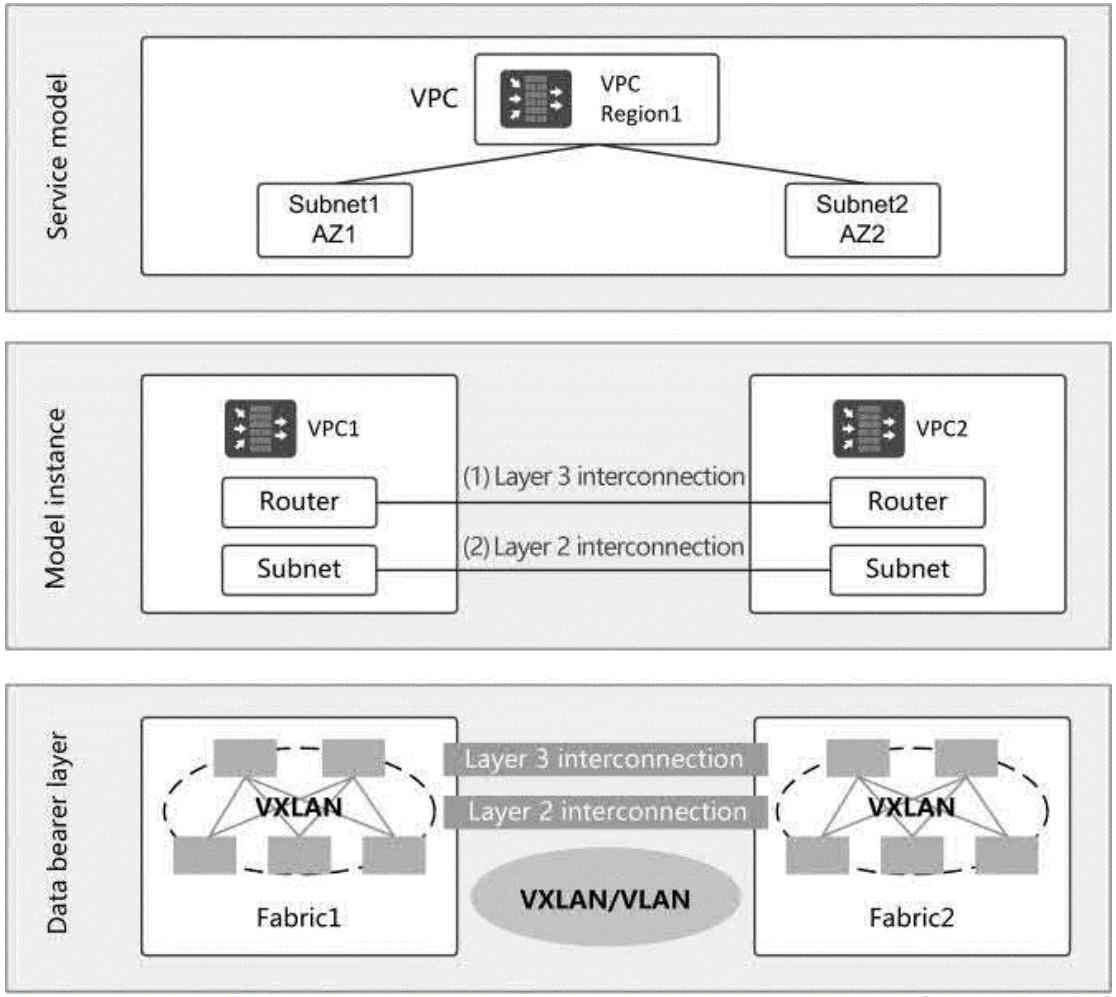
Multi-DC Networking Technologies (Contd.)

- **REQ#2:** L3 Networking across DCs
  - Option 1: MPLS L3VPN:
    - a virtual L3VPN constructed on the MPLS network
    - enables devices on service network segments in different DCs to communicate with each other at Layer 3
    - has the same advantages and disadvantages as VPLS
  - Option 2: VXLAN based L3VPN services:
    - VXLAN tunnels are established on the IP network to provide L3VPN services

VXLAN technology is still most widely used in the DCI solution and is the most recommended / used DCI technology

Source: Lei Zhang, Le Chen. Cloud Data Center Network Architectures and Technologies, CRC Press 2021

Multi-DC Service Model



Service Model of Multi-site scenario

Source: Lei Zhang, Le Chen. Cloud Data Center Network Architectures and Technologies, CRC Press 2021

VPCs and Subnets: AWS Example

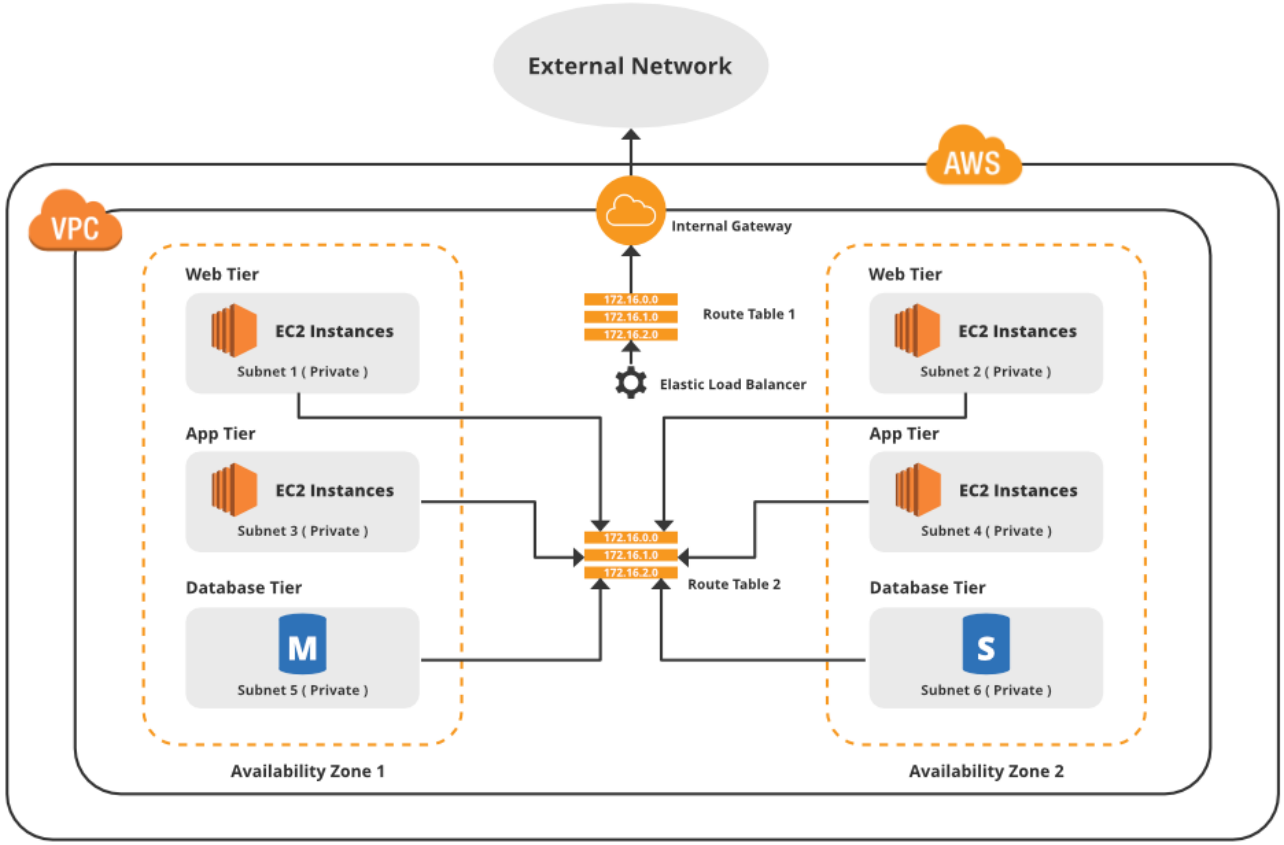
- A *virtual private cloud* (VPC) is a virtual network dedicated to your AWS account.
  - It is logically isolated from other virtual networks in the AWS Cloud.
  - You can specify an IP address range for the VPC, add subnets, add gateways, and associate security groups.
- A *subnet* is a range of IP addresses in your VPC.
  - You launch AWS resources, such as Amazon EC2 instances, into your subnets.
  - You can connect a subnet to the internet, other VPCs, and your own data centers, and route traffic to and from your subnets using route tables.

Defining a VPC in AWS

- How Amazon VPC Works
  - Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined
  - This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of the scalable infrastructure of AWS.
  - A VPC allows its users to launch their virtual machines in a protected as well as isolated virtual environment
  - VPC enables us to select the virtual address of our private cloud and define all the sub-constituents of the VPC like subnet, subnet mask, availability zone, etc.

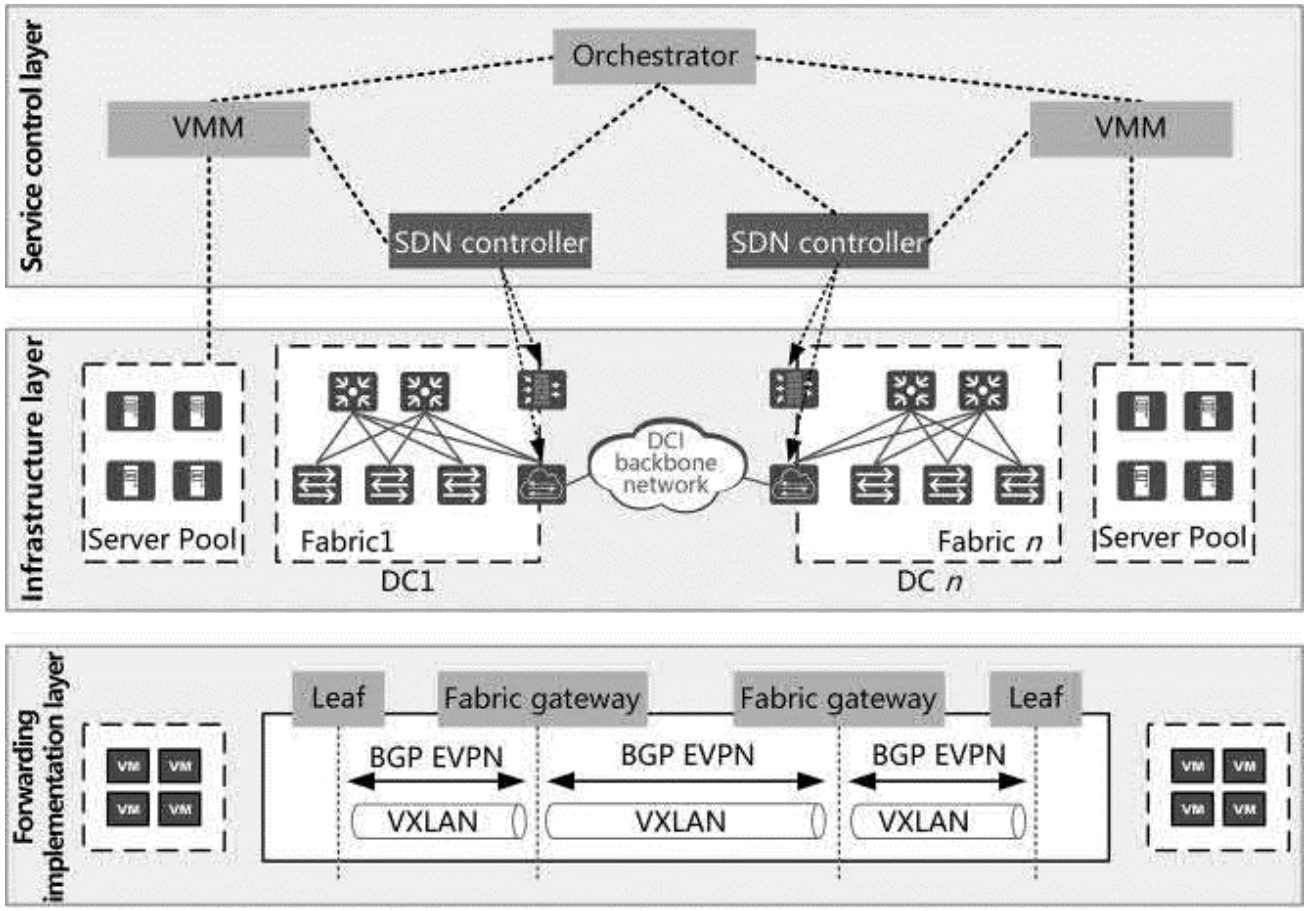
Amazon VPC Architecture

- VPC Consists of:
  - Subnets
  - Route Tables
  - Internet Gateway
  - Availability Zones
  - Load balancers etc
- Security policies / checks are associated with VPCs at multiple levels



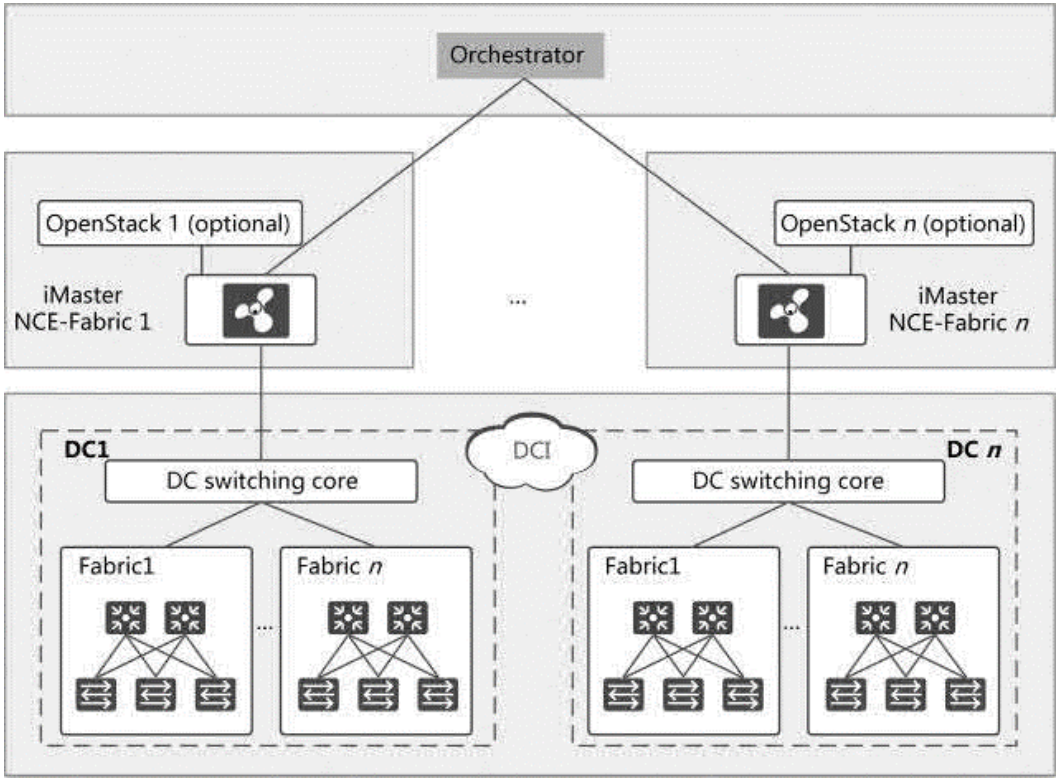
Source: Amazon VPC - Introduction to Amazon Virtual Cloud - GeeksforGeeks

Multi-DC Networking Architecture



Source: Lei Zhang, Le Chen. Cloud Data Center Network Architectures and Technologies, CRC Press 2021

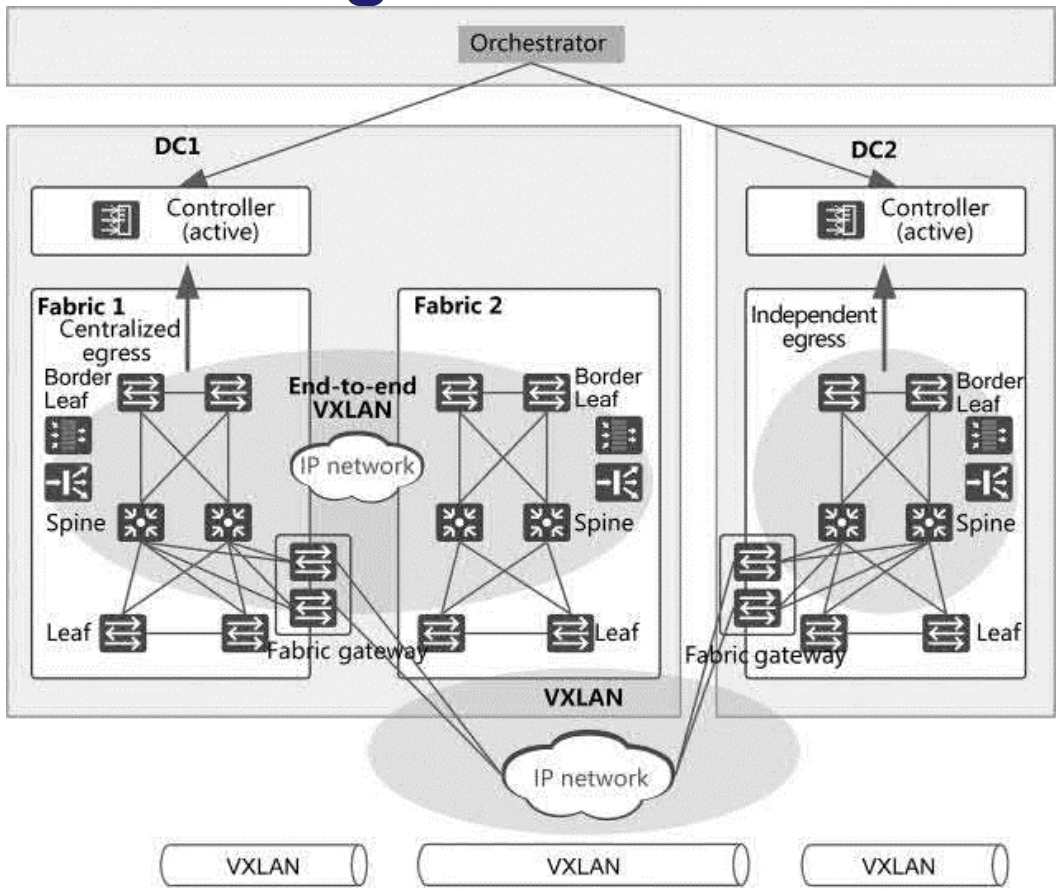
Multi-DC Networking Architecture



Hierarchical Switching Planes in Multi-site DCs

Source: Lei Zhang, Le Chen. Cloud Data Center Network Architectures and Technologies, CRC Press 2021

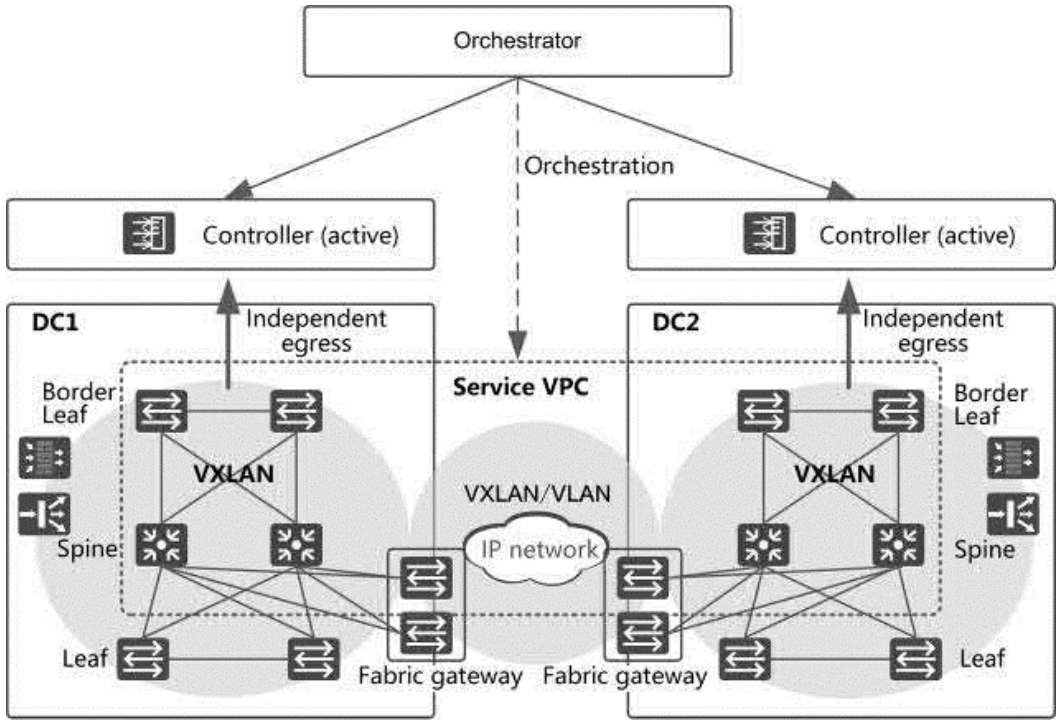
Multi-DC Networking Architecture



Networking of Hierarchical Multi-site DCs

Source: Lei Zhang, Le Chen. Cloud Data Center Network Architectures and Technologies, CRC Press 2021

Multi-DC Networking Architecture



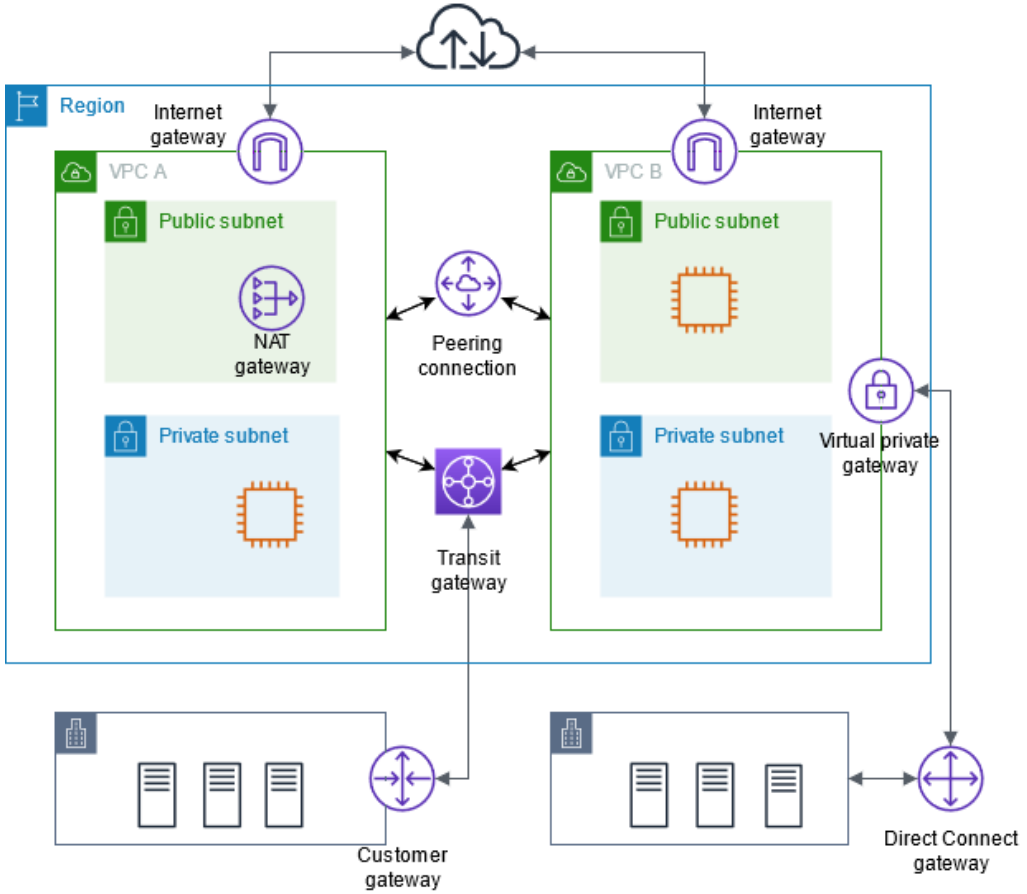
Cross-DC Deployment of a Large VPC

Source: Lei Zhang, Le Chen. Cloud Data Center Network Architectures and Technologies, CRC Press 2021

External Network Connections for a VPC: AWS Example

- You can optionally connect your VPC to your own corporate data center using an IPsec AWS Site-to-Site VPN connection, making the AWSCloud an extension of your data center.
  - A Site-to-Site VPN connection consists of VPN tunnels between a virtual private gateway or transit gateway on the AWS side, and a customer gateway device located in your data center.
- You can create a *VPC peering connection* between two VPCs that enables you to route traffic between them privately.
  - Instances in either VPC can communicate with each other as if they are within the same network.
- You can also create a *transit gateway* and use it to interconnect your VPCs and on-premises networks

Amazon VPC Networking



Thank You!