ORACLE

Oracle Cloud Infrastructure

Oracle Public Cloud Network

Agenda

- **OCI Networking Core Components**
- **WAN Connectivity on-prem / OCI (VPN, FastConnect)**
- **Intra-OCI region Azure Interconnect**
- **Your network requirements**
- **(optional) Advanced network configurations**

Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.
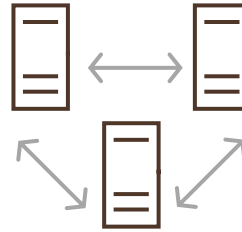
The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.
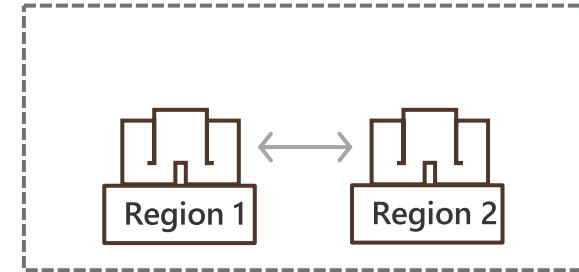
OCI Core Components
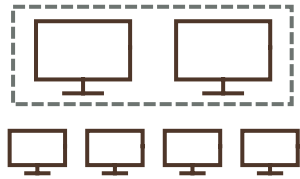
Fault Domains

Protection against failures within datacenters

Availability Domains

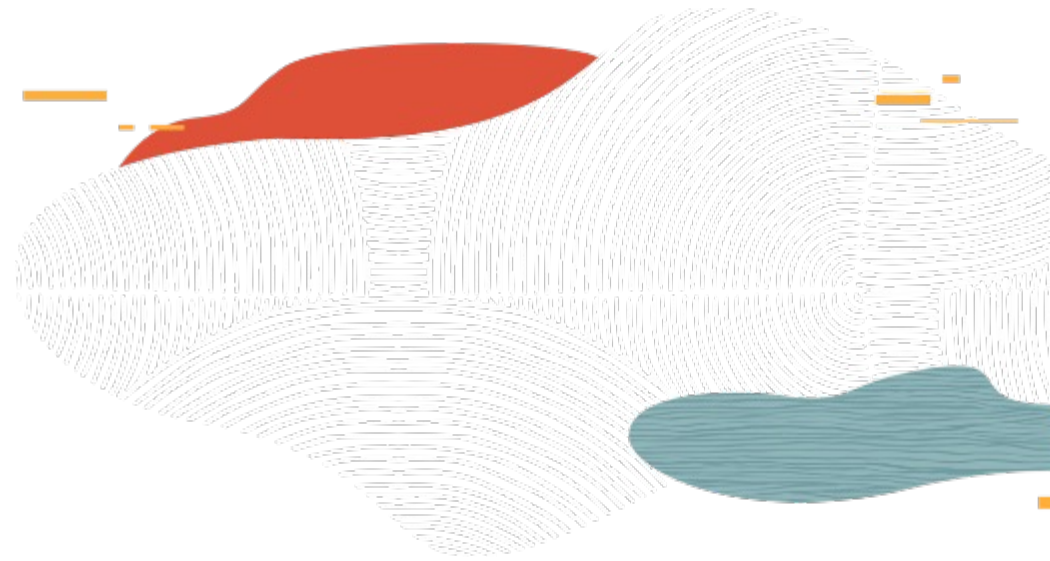Protection from entire datacenter failures

Regions

Protection from disaster with Data Residency compliance

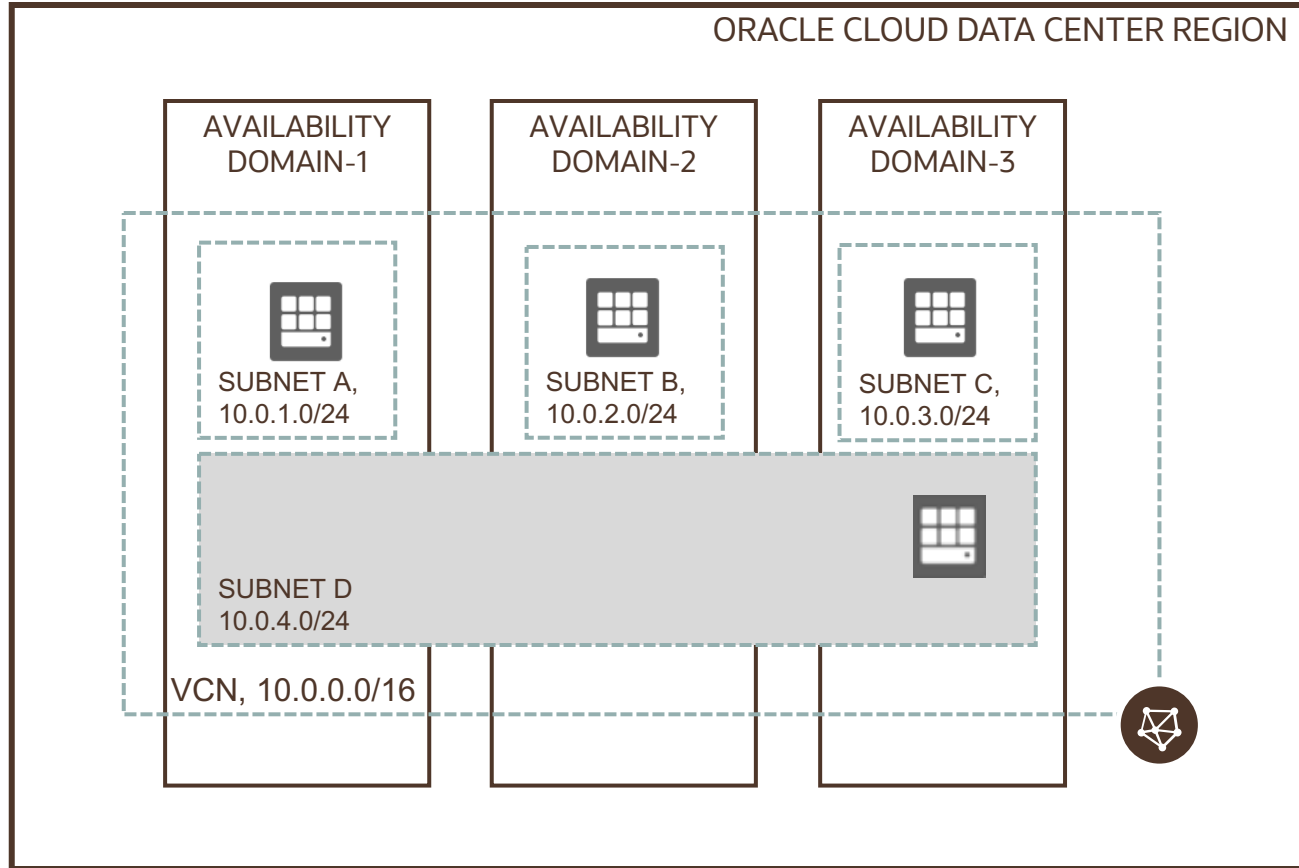SLAs on Performance, Management and Availability

ORACLE

Virtual Cloud Network

Virtual Cloud Network (VCN)

- A private network that you set up in the Oracle data centers, with firewall rules and specific types of communication gateways that you can choose to use

- A VCN covers contiguous IPv4 CIDR blocks of your choice

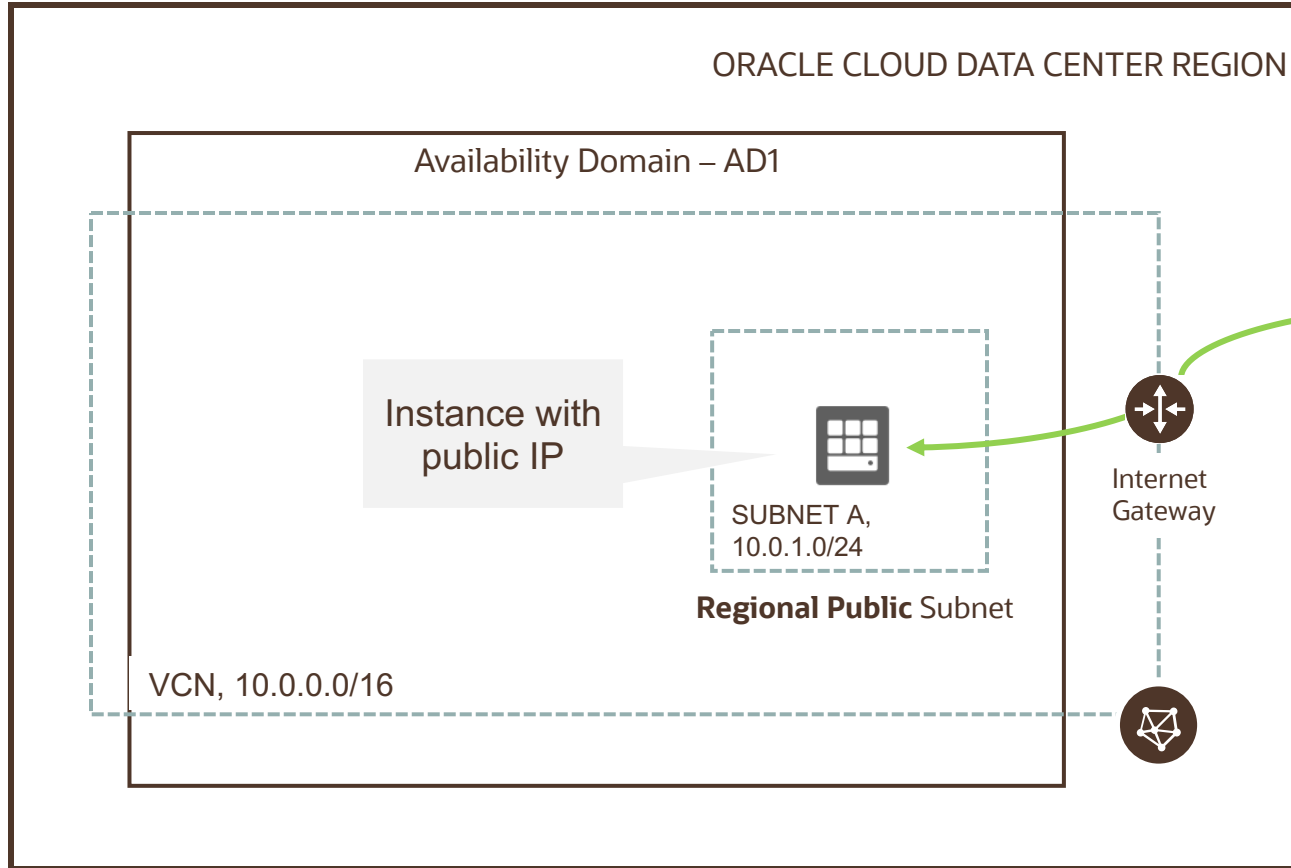- A VCN resides within a single region

Subnet

Each VCN network is subdivided into subnets

- Each subnet can be AD-specific or **Regional (recommended)**
  - AD specific subnet is contained within a single AD in a multi-AD region
  - Regional subnet spans all three ADs in a multi-AD region
- Each subnet has a contiguous range of IPs, described in CIDR notation. Subnet IP ranges cannot overlap
- Instances are placed in subnets and draw their internal IP address and network configuration from their subnet
- Subnets can be designated as either
  - **Private** (instances contain private IP addresses assigned to VNICs)
  - **Public** (contain both private and public IP addresses assigned to VNICs)
- VNIC is a component that enables a compute instance to connect to a VCN. The VNIC determines how the instance connects with endpoints inside and outside the VCN

ORACLE CLOUD DATA CENTER REGION

AVAILABILITY DOMAIN-1

AVAILABILITY DOMAIN-2

AVAILABILITY DOMAIN-3

SUBNET A, 10.0.1.0/24

SUBNET B, 10.0.2.0/24

SUBNET C, 10.0.3.0/24

SUBNET D 10.0.4.0/24

VCN, 10.0.0.0/16

Internet Gateway

ORACLE CLOUD DATA CENTER REGION

Availability Domain – AD1

Instance with public IP

SUBNET A, 10.0.1.0/24

Regional Public Subnet

VCN, 10.0.0.0/16
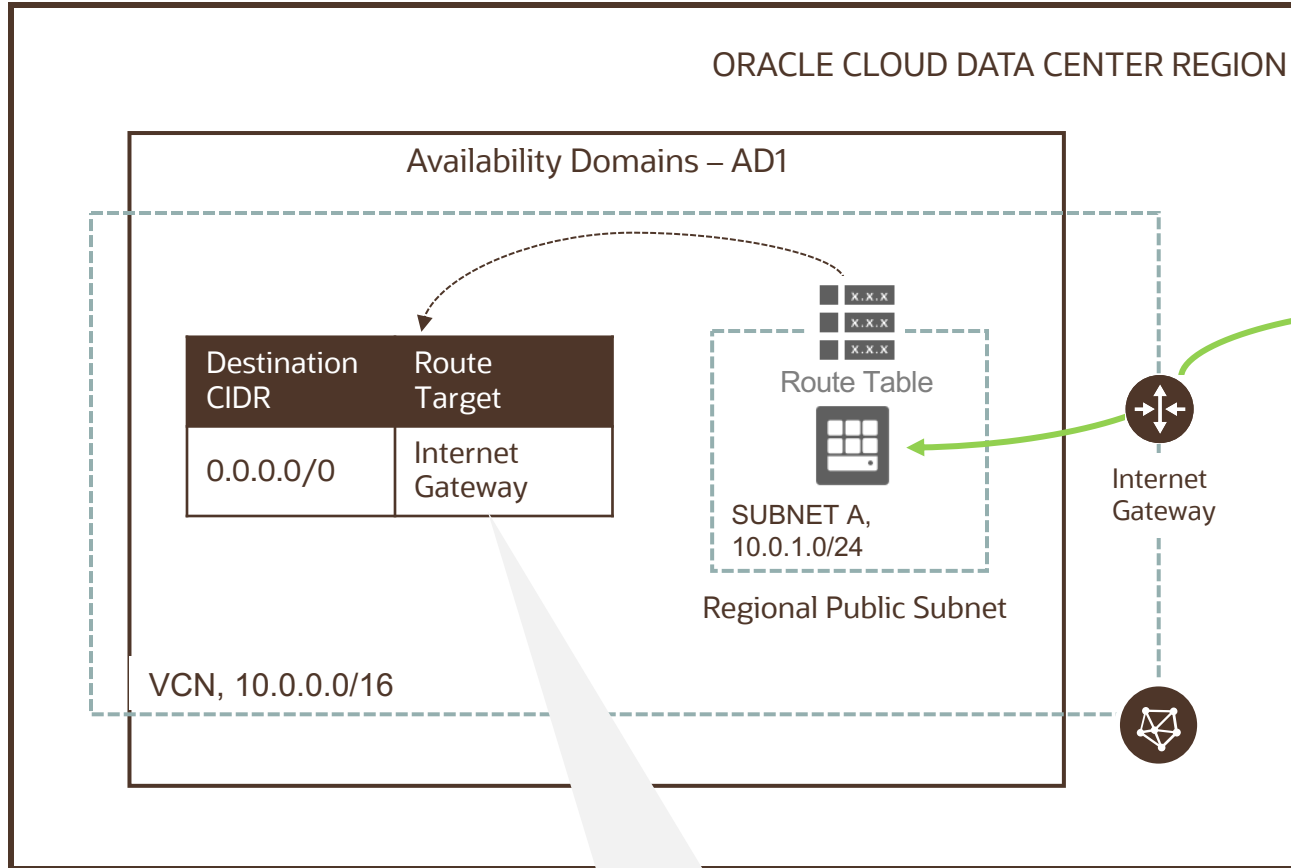
Internet Gateway

Internet

Internet gateway provides a path for network traffic between your VCN and the internet

You can have only one internet gateway for a VCN

After creating an internet gateway, you must add a route for the gateway in the VCN's Route Table to enable traffic flow

Route Table

ORACLE CLOUD DATA CENTER REGION

Availability Domains – AD1

Destination CIDR	Route Target
0.0.0.0/0	Internet Gateway

Route Table

SUBNET A, 10.0.1.0/24

Regional Public Subnet

Internet Gateway

Internet

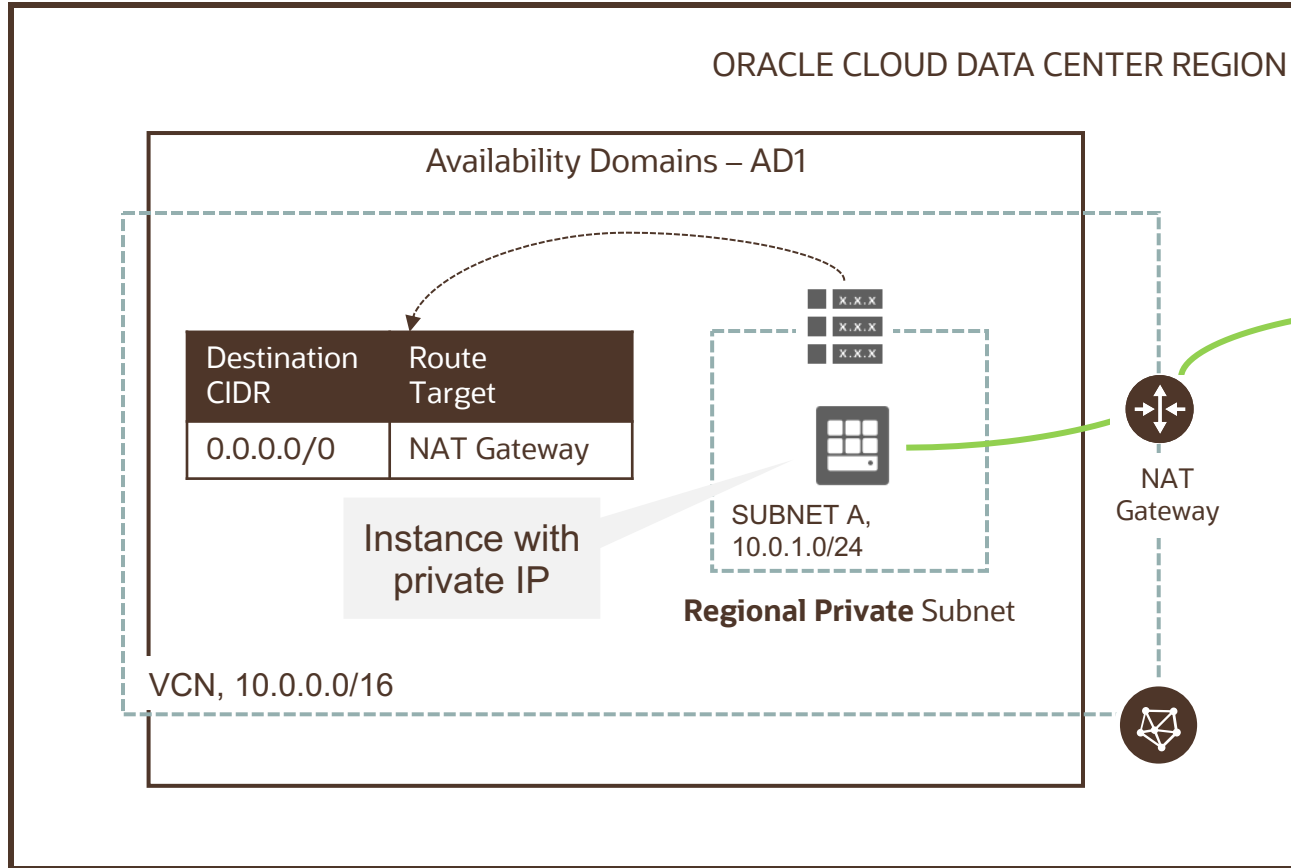VCN, 10.0.0.0/16

All traffic destined for Internet Gateway

Route Table is used to send traffic out of the VCN

Consists of a set of route rules; each rule specifies
- Destination CIDR block
- Route Target (the next hop) for the traffic that matches that CIDR

NAT Gateway

ORACLE CLOUD DATA CENTER REGION

Availability Domains – AD1

Destination CIDR	Route Target
0.0.0.0/0	NAT Gateway

Instance with private IP

SUBNET A, 10.0.1.0/24

Regional Private Subnet

NAT Gateway

VCN, 10.0.0.0/16

Internet

NAT gateway gives an entire private network access to the internet without assigning each host a public IP address

Hosts can initiate outbound connections to the internet and receive responses, but not receive inbound connections initiated from the internet. Use case: updates, patches)

You can have more than one NAT gateway on a VCN, though a given subnet can route traffic to only a single NAT gateway
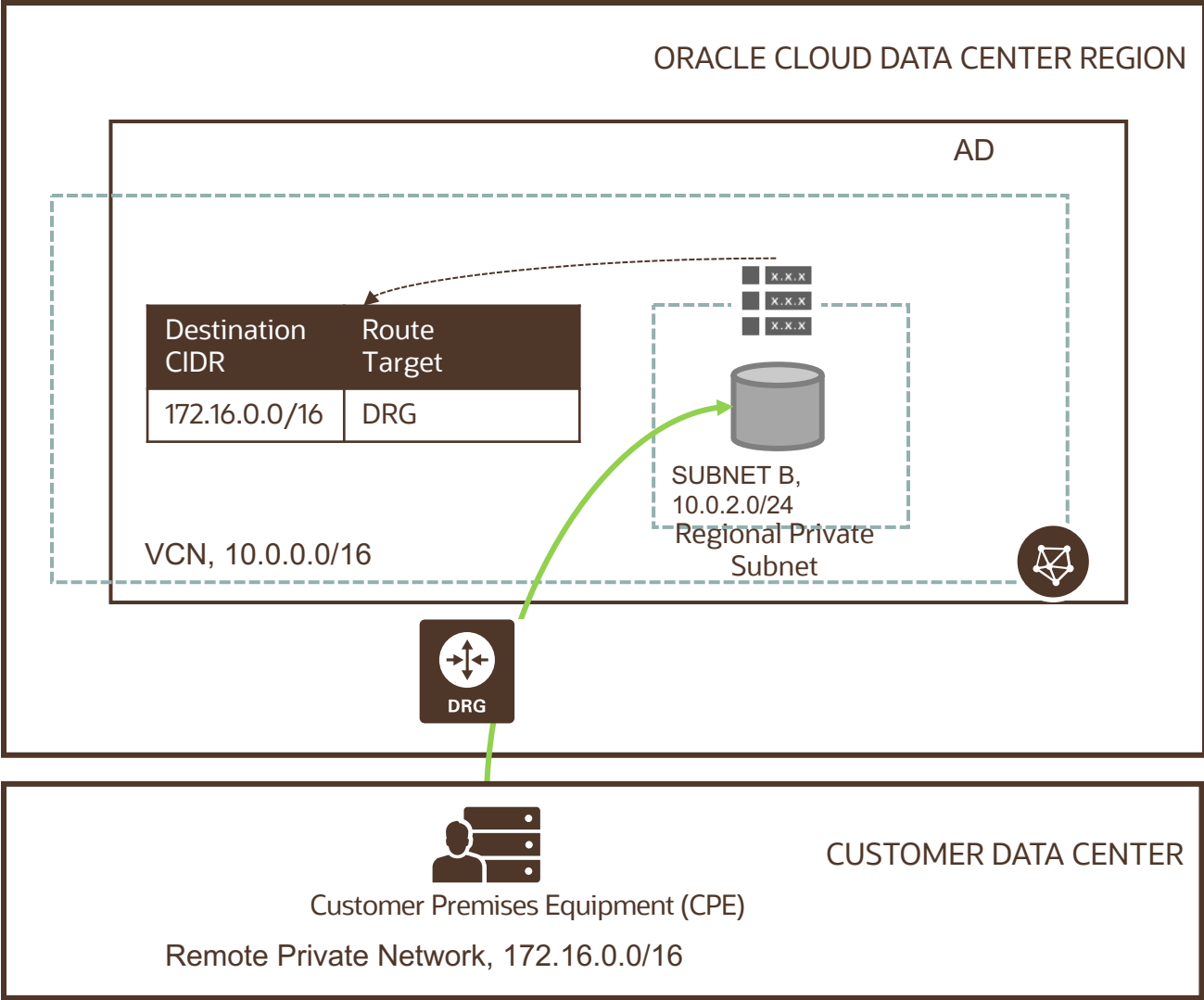
Service Gateway
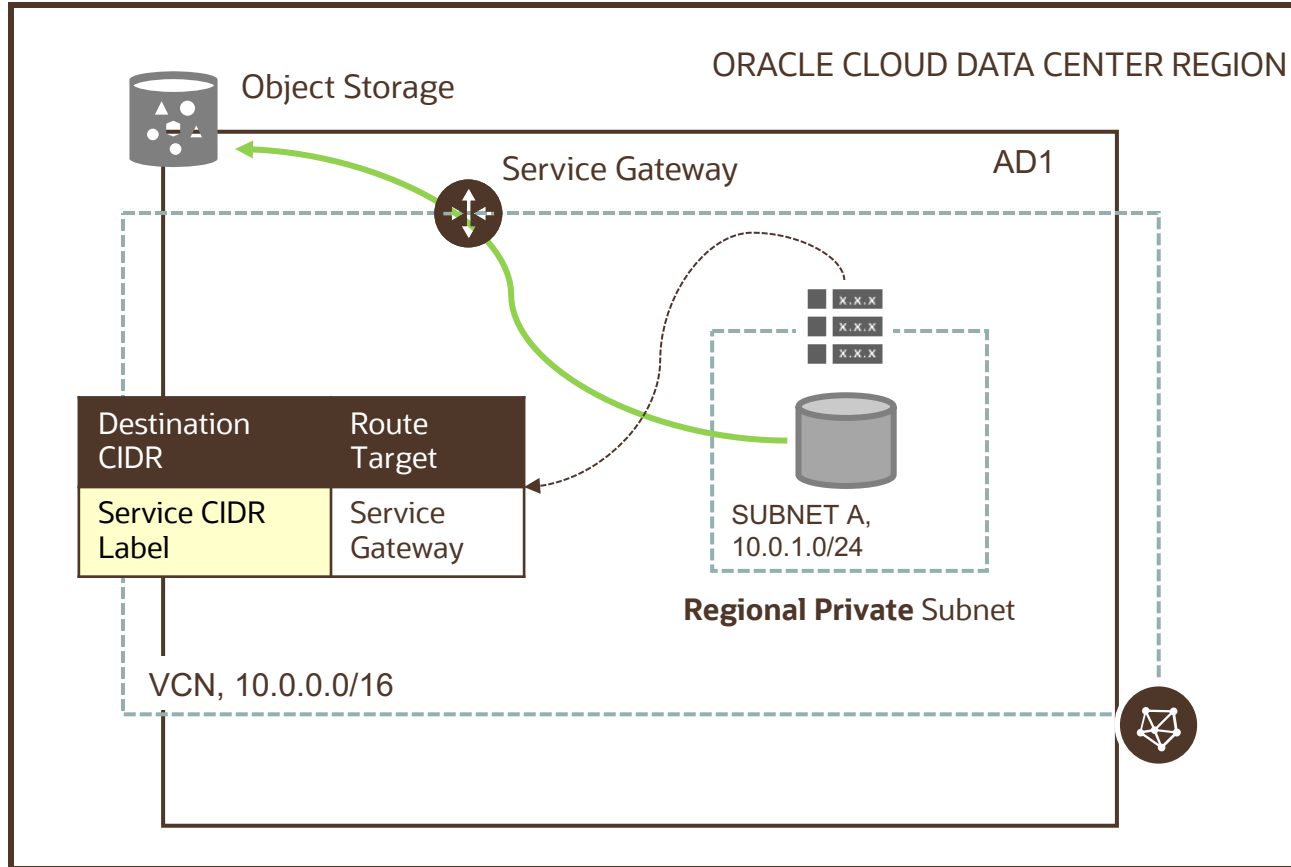
Service gateway lets resources in VCN access public OCI services, exposed on the Oracle Services Network, such as Object Storage, but without using either Internet or NAT gateway

Any traffic from VCN that is destined for one of the supported OCI public services uses the instance's private IP address for routing, travels over OCI network fabric, and never traverses the internet. Use case: back up DB Systems in VCN to Object Storage)

Service CIDR labels represent all the public CIDRs for a given Oracle service or a group of Oracle services. E.g.
- OCI <region> Object Storage
- All <region> Services

Dynamic Routing Gateway

ORACLE CLOUD DATA CENTER REGION

AD

Destination CIDR	Route Target
172.16.0.0/16	DRG

SUBNET B, 10.0.2.0/24
Regional Private Subnet

VCN, 10.0.0.0/16

DRG

CUSTOMER DATA CENTER

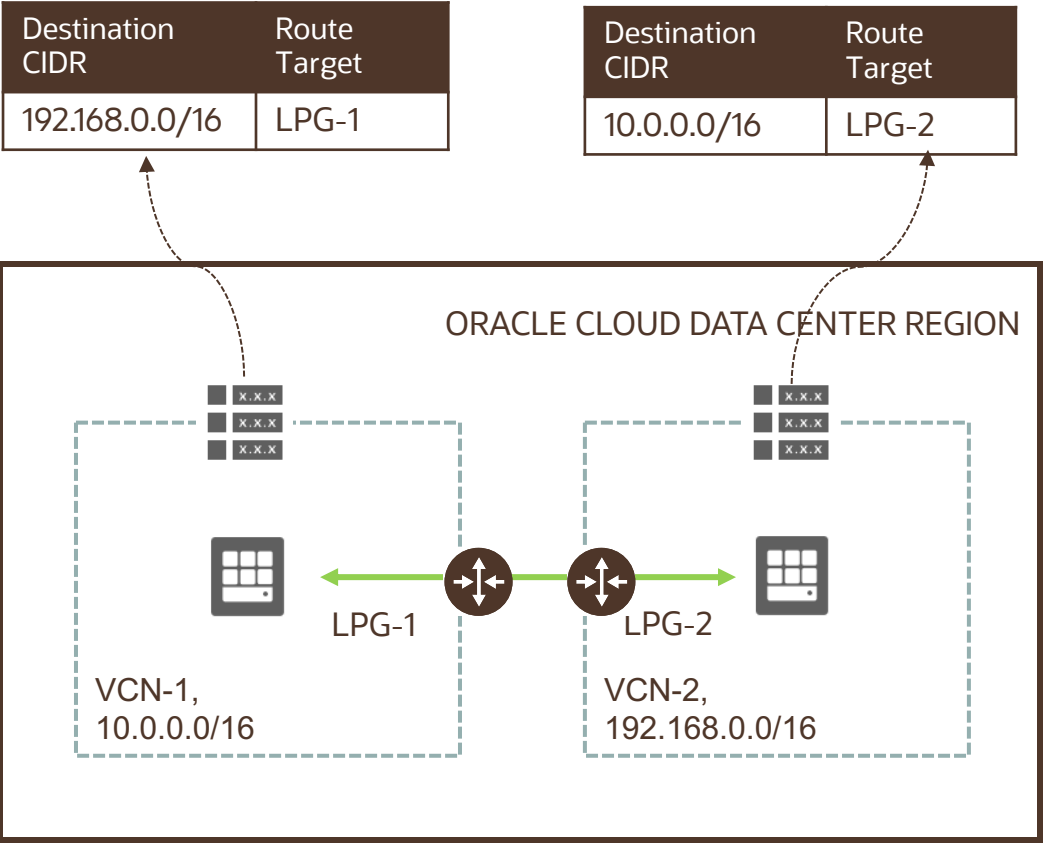Customer Premises Equipment (CPE)

Remote Private Network, 172.16.0.0/16

A virtual router that provides a path for private traffic between your VCN and destinations other than the internet

You can use it to establish a connection with your on-premises network via IPsec VPN or FastConnect (private, dedicated connectivity)

After attaching a DRG, you must add a route for the DRG in the VCN's route table to enable traffic flow

DRG is a standalone object. You must attach it to a VCN. VCN and DRG have n:1 relationship

Local Peering

Destination CIDR	Route Target
192.168.0.0/16	LPG-1

Destination CIDR	Route Target
10.0.0.0/16	LPG-2

ORACLE CLOUD DATA CENTER REGION

LPG-1
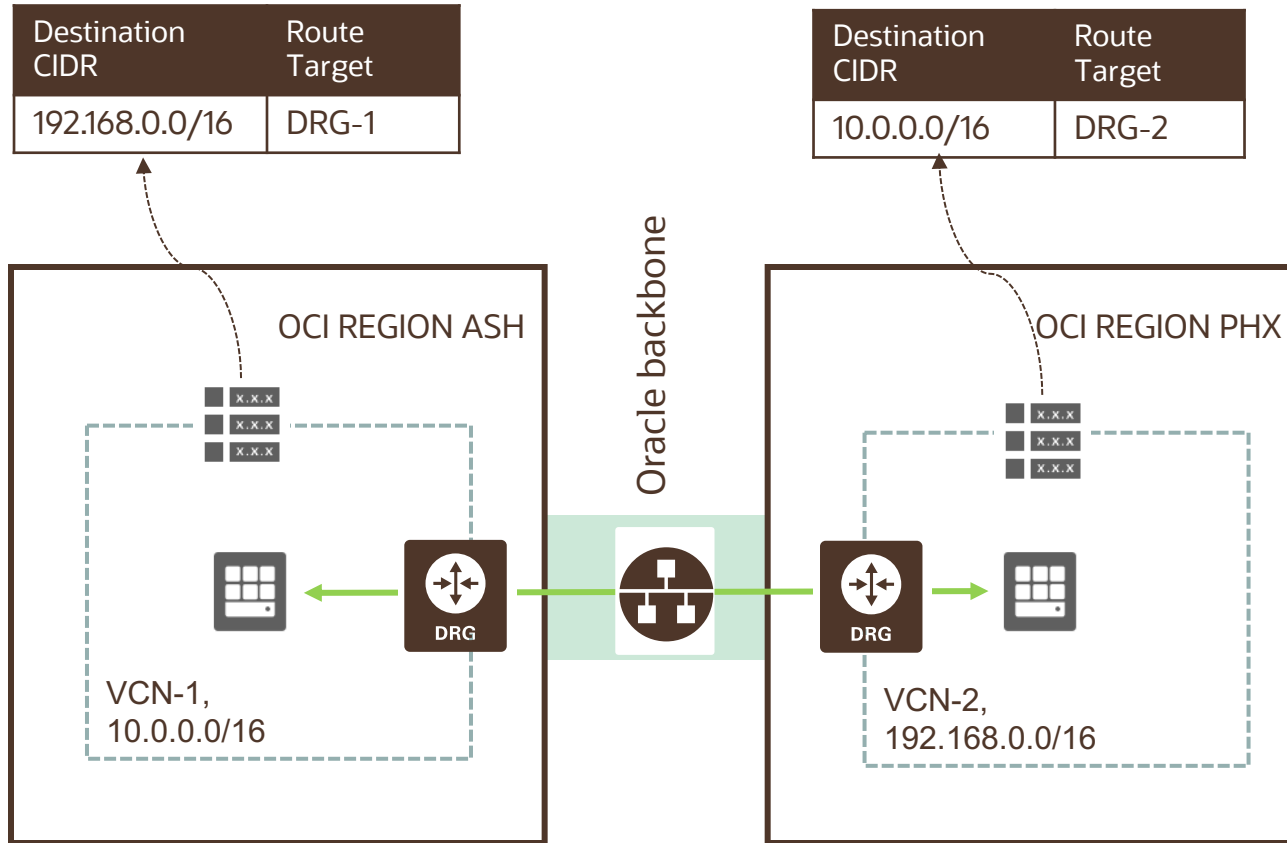LPG-2

VCN-1,
10.0.0.0/16
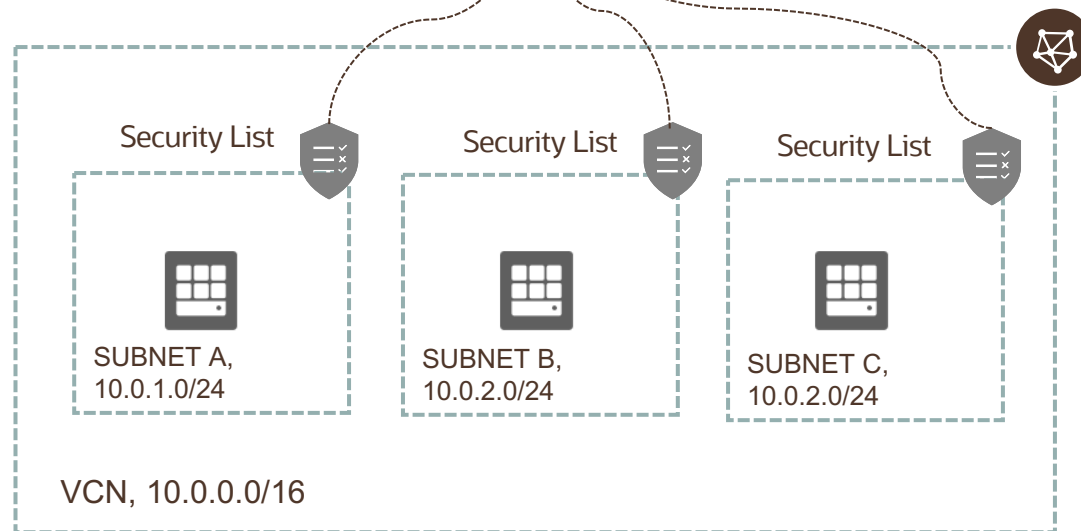
VCN-2,
192.168.0.0/16

VCN peering is the process of connecting multiple VCNs

Local VCN peering is the process of connecting two VCNs in the **same region** so that their resources can communicate using private IP addresses

A local peering gateway (LPG) is a component on a VCN for routing traffic to a locally peered VCN

The two VCNs in the peering relationship shouldn't have overlapping CIDRs

Remote Peering

Destination CIDR	Route Target
192.168.0.0/16	DRG-1

Destination CIDR	Route Target
10.0.0.0/16	DRG-2

OCI REGION ASH

OCI REGION PHX

Oracle backbone

VCN-1, 10.0.0.0/16

VCN-2, 192.168.0.0/16

DRG

DRG

Remote VCN peering is the process of connecting two VCNs in **different regions or in the same region** so that their resources can communicate using private IP addresses

Requires a remote peering connection (RPC) to be created on the DRGs. RPC's job is to act as a connection point for a remotely peered VCN

The two VCNs in the peering relationship must not have overlapping CIDRs

Security List (SL)

	Direction	CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	0.0.0.0/0	TCP	All	80
Stateful	Egress	10.0.2.0/24	TCP	All	1521

Security List

Security List

Security List

SUBNET A, 10.0.1.0/24

SUBNET B, 10.0.2.0/24

SUBNET C, 10.0.2.0/24

VCN, 10.0.0.0/16

A common set of firewall rules associated with a subnet and applied to all instances launched inside the subnet

- Security list consists of rules that specify the types of traffic allowed in and out of the subnet
- To use a given security list with a particular subnet, you associate the security list with the subnet either during subnet creation or later.
- Security list apply to a given instance whether it's talking with another instance in the VCN or a host outside the VCN
- You can choose whether a given rule is stateful or stateless
  - **Stateful Rules** enable a Connection Tracking mechanism. When an instance receives traffic matching the stateful ingress rule, the response is tracked and automatically allowed regardless of any egress rules; similarly for sending traffic from the host
  - **Stateless rules**: response traffic is not automatically allowed. To ow the response traffic for a stateless ingress rule, you must create a corresponding stateless egress rule

Network Security Group (NSG)

		Direction	CIDR	Protocol	Source Port	Dest Port
NSG-A	Stateful	Ingress	0.0.0.0/0	TCP	All	80
NSG-B	Stateful	Ingress	0.0.0.0/0	TCP	All	22

NSG-A   NSG-B

NSG-A

SUBNET A, 10.0.1.0/24

SUBNET B, 10.0.1.0/24

VCN, 10.0.0.0/16
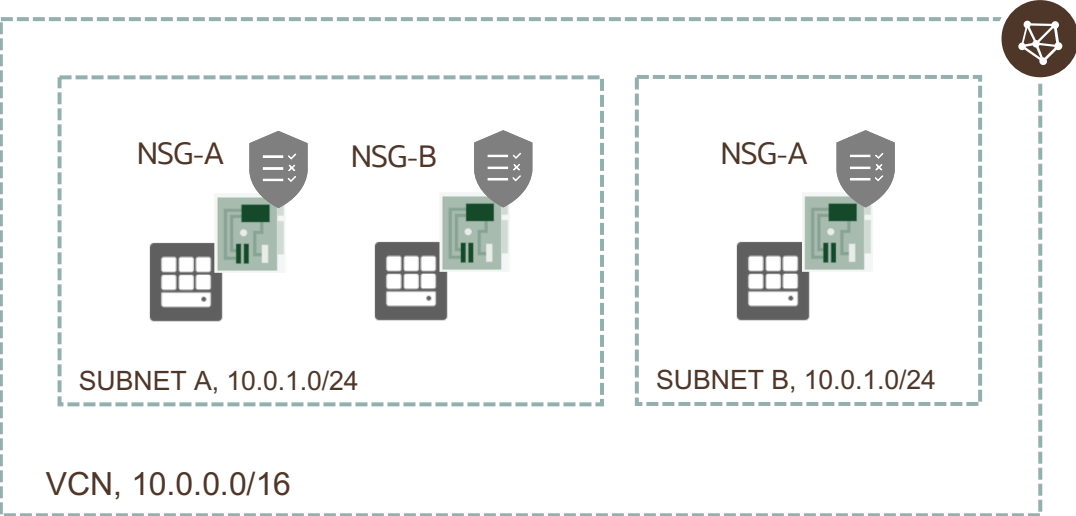
A network security group (NSG) provides a virtual firewall for a set of cloud resources that all have the same security posture

- NSG consists of set of rules that apply only to a set of VNICs of your choice in a single VCN

- Currently, compute instances, load balancers and DB instances support NSG

- When writing rules for an NSG, you can specify an NSG as the source or destination. Contrast this with SL rules, where you specify a CIDR as the source or destination

- Oracle recommends using NSGs instead of SLs because NSGs let you separate the VCN's subnet architecture from your application security requirements

Network Visualizer v2.0

Network Visualizer v2.0

Network Visualizer v2.0

Network Visualizer v2.0

Load Balancer

Network Load Balancer

It can be public or private and regional scoped

It's an always Free Service

Every Load balancer configuration limits:
- One IP address
- 50 backend sets
- 512 backend servers per backend set
- 1024 backend servers total
- 50 listeners
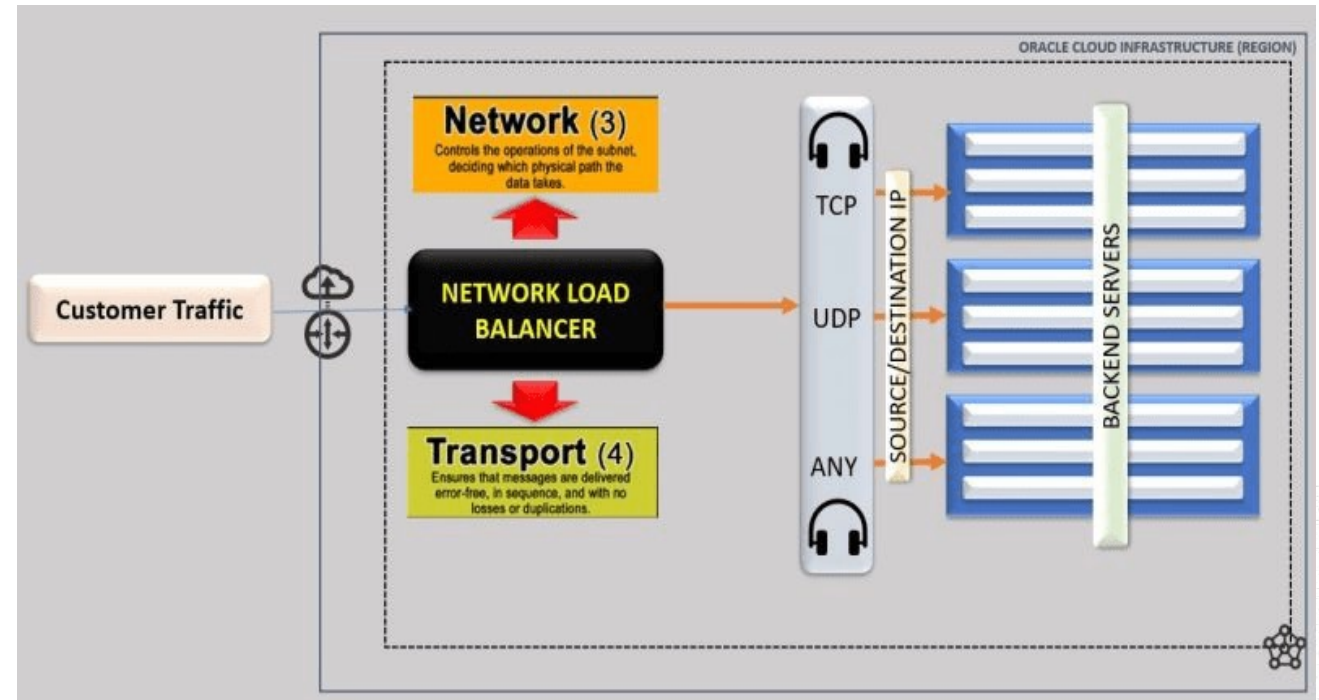
VPN Basics

VPN – using a public network to make end to end connection between two private networks in a secure fashion

Tunnel   VPN Connection

Private
Network 1

Private
Network 2

Internet

VPN
Router

VPN
Router
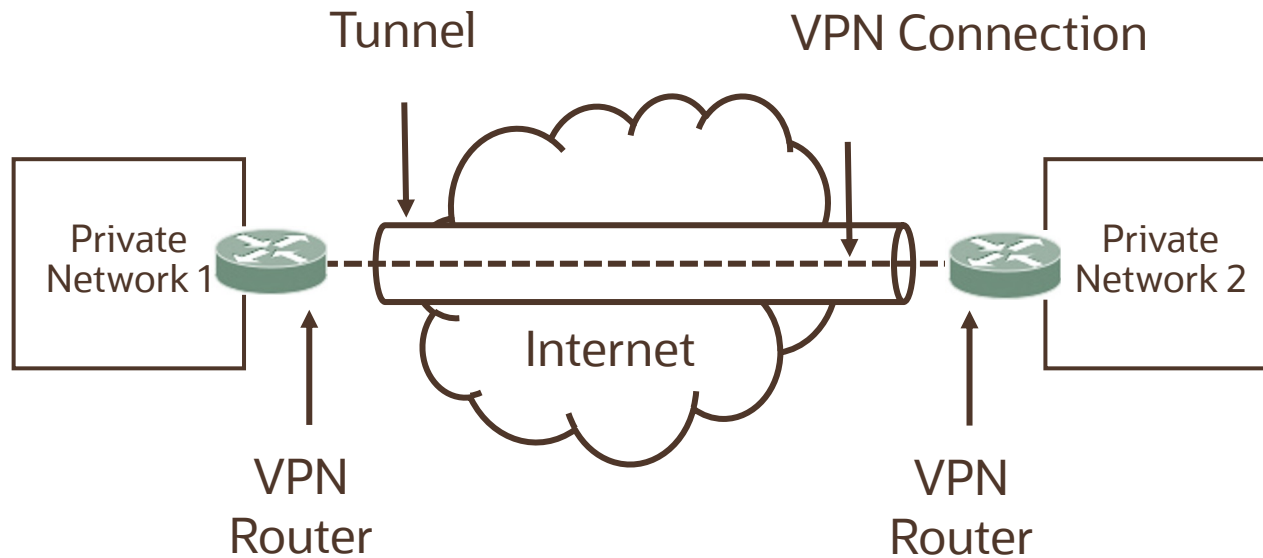
- **Tunnel** – a way to deliver packets through the internet to private RFC 1918 addresses
- **Authentication** – provides a mechanism to authenticate who you are
- **Encryption** – packets need to be encrypted, so they cannot be sniffed over the public internet
- **Static routing**: configure a router to send traffic for particular destinations in preconfigured directions
- **Dynamic routing**: use a routing protocol such as BGP to figure out what paths traffic should take

VPN Connect (IPSec)

ORACLE CLOUD DATA CENTER REGION

AVAILABILITY DOMAIN-2

Custom Route Table

SUBNET B, 10.0.2.0/24

VCN, 10.0.0.0/16

DRG

CUSTOMER DATA CENTER

Customer Premises Equipment
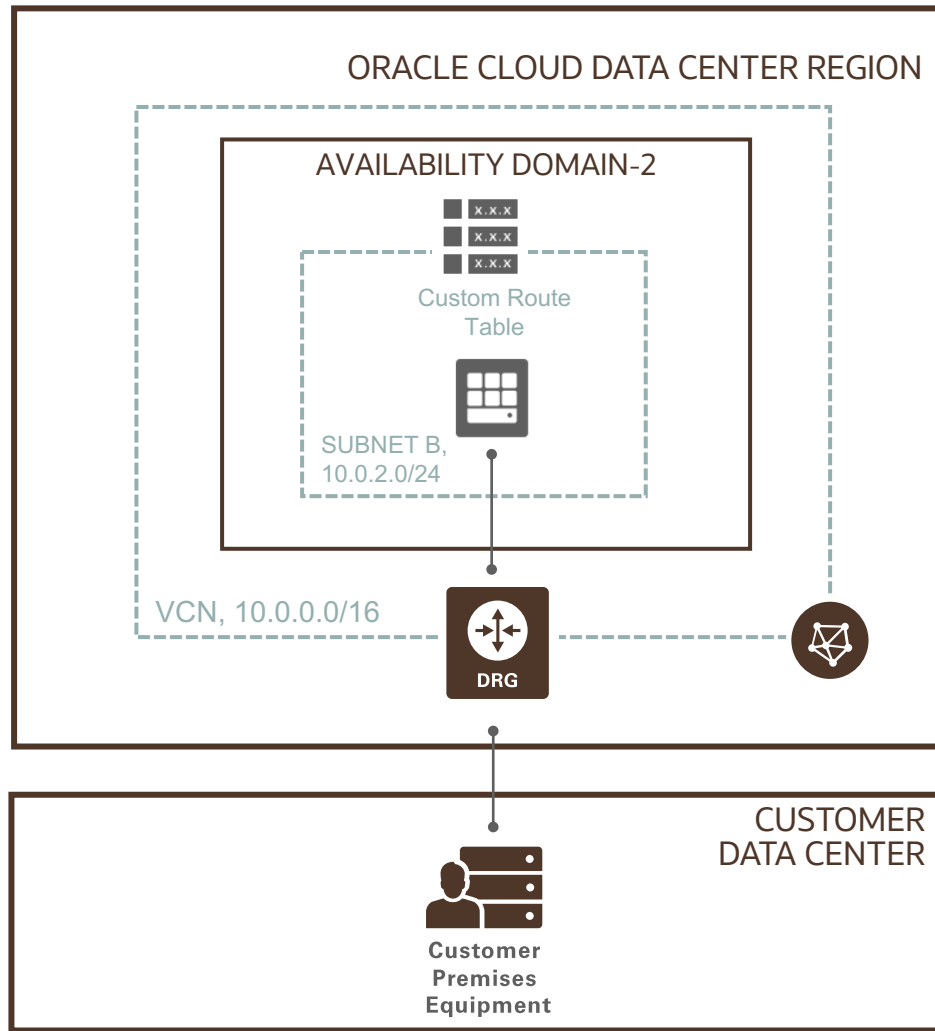
- VPN Connect is a managed VPN service which securely connects on-premises network to OCI VCN through an **IPSec VPN connection**

- VPN Connect ensures secure remote connectivity via industry standard IPSec encryption

- Bandwidth is dependent on the customer's access to the Internet and general Internet congestion (Typically less than 250 Mbps – but your mileage may vary)

- **VPN Connect is offered for free**

- Customer Proof of Concepts usually start as a VPN and then morph into FastConnect designs

- OCI provisions redundant VPN tunnels located on physically and logically isolate tunnel endpoints

VPN Connect (IPSec) - Workflow

On-Premises Network

10.0.0.0/16

CPE, 142.32.45.56

Static Route or Dynamic Routing (BGP)

Internet

Route Table
10.0.0.0/16 → DRG

OCI REGION

DRG

x.x.x
x.x.x
x.x.x

SUBNET, 172.16.1.0/24

VCN, 172.16.0.0/16
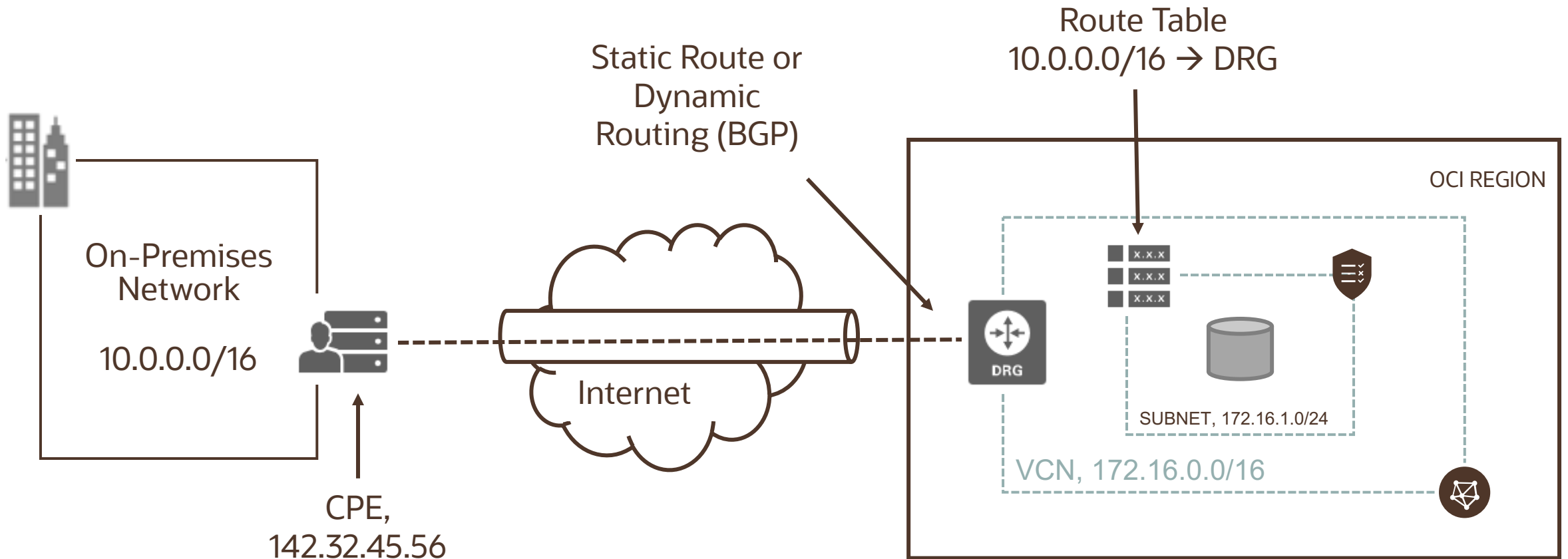
VPN Connect workflow

1. Create a Virtual Cloud Network (VCN)

2. Create a Dynamic Routing Gateway (DRG)

3. Attach DRG to your VCN

4. Update VCN Router to route traffic to DRG

5. Create a CPE Object and add on-premises router Public IP address

6. From DRG, Create an IPsec Connection between CPE and DRG and provide a Static Route or use BGP routing

7. Configure on-premises CPE Router
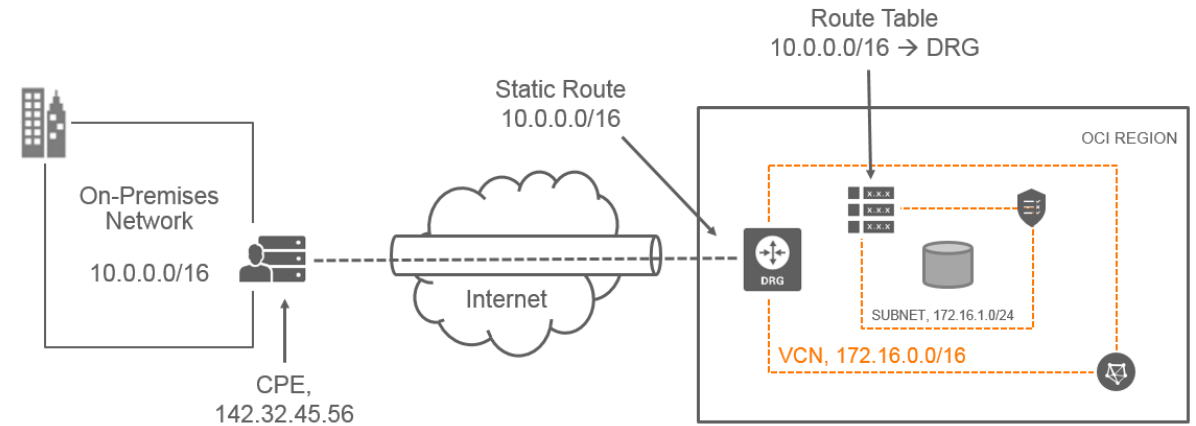
FastConnect

Dedicated, private, secure network connectivity to connect customer locations to OCI.

Features
Multiple bandwidth options with FastConnect: through a Partner
1G or 10G, 100G port bandwidth options with FastConnect
Cost effective - No egress data transfer charges and lower port charges on hourly basis.
Private Peering – extends corporate network to Oracle Cloud
Public Peering – Internet alternative to connect to public Oracle Cloud resources

Customer Location — **FastConnect** — **Oracle Cloud**
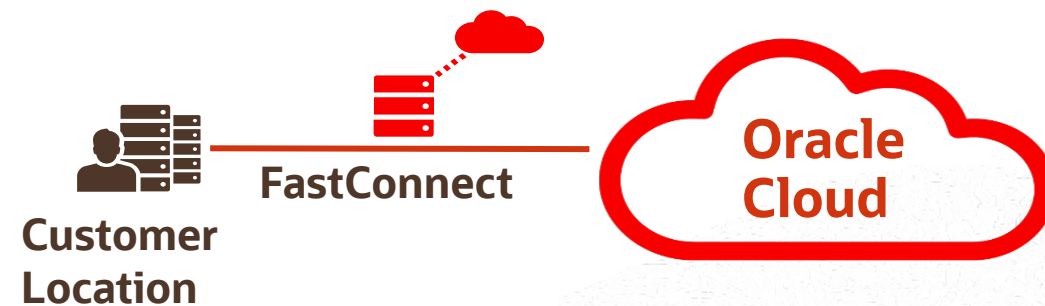
FastConnect Models

1. Oracle FastConnect Partner Network

- Direct connection between the customer and Oracle through a pre-established FastConnect partner

- The most flexible and typically least expensive to set up

2. Direct Cross-connect – Colocation

- Direct connection between the customer and Oracle when both are in the same FastConnect facility

- Good model if the customer and Oracle are already colocated

3. Direct Cross-connect – Dedicated Circuits

- Connection between the customer's network provider and Oracle using a dedicated circuit

- Least flexible and typically most expensive to set up

FastConnect: Through a Partner

Point-to-point or multi-point service

CPE

CUSTOMER DATACENTER

CPE

CUSTOMER DATACENTER

PARTNER NETWORK

FASTCONNECT LOCATION

Partner Edge

Partner Demarc

Redundant 10Gbps

FastConnect Edge

Oracle CAGE

Subnet 1

Subnet 2

Subnet 3

Regional Cloud Services

Partners
- *Network Service Providers*
- *Exchanges (e.g. Equinix, Megaport, Interxion)*
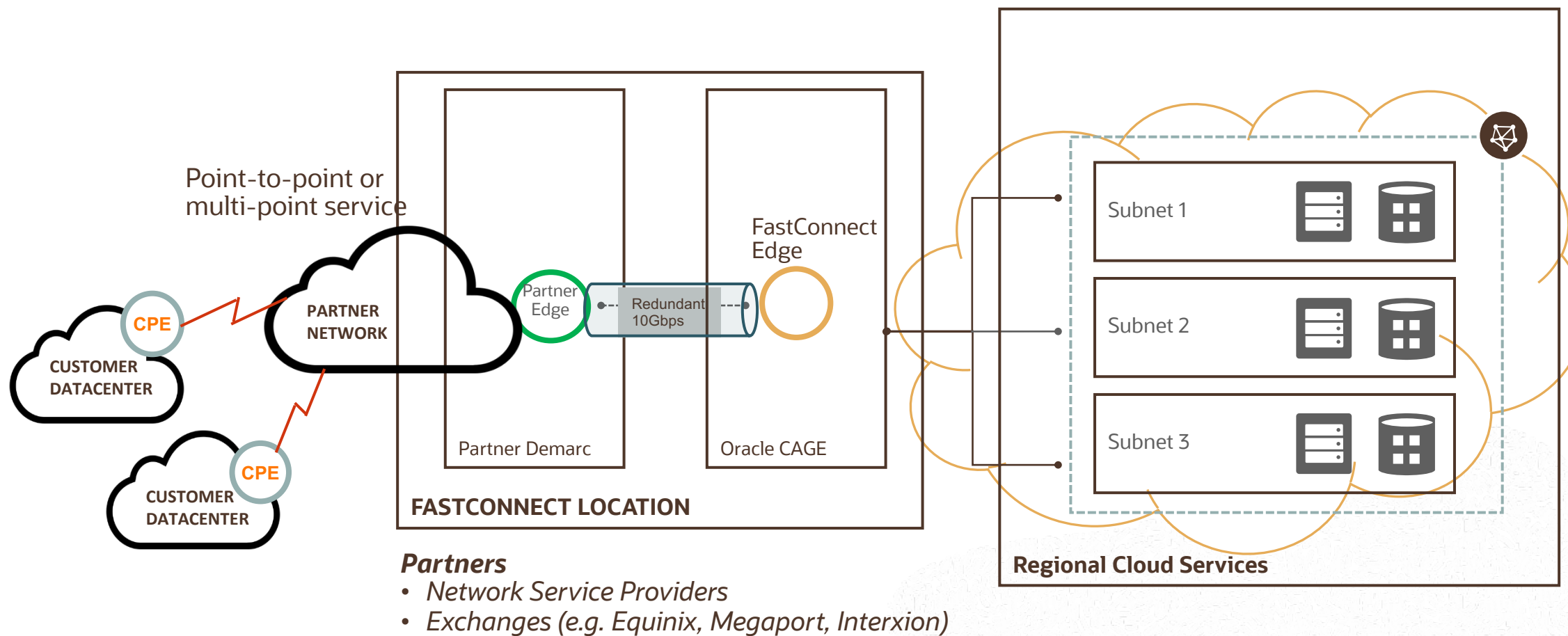
Public Peering *Internet Alternative*
Private Peering *Infrastructure Extension*

Legend: Public virtual circuit ● ‑ ‑ ‑ ‑ ●
Private virtual circuit ●━━●

Legend: Private virtual circuit ●━━●
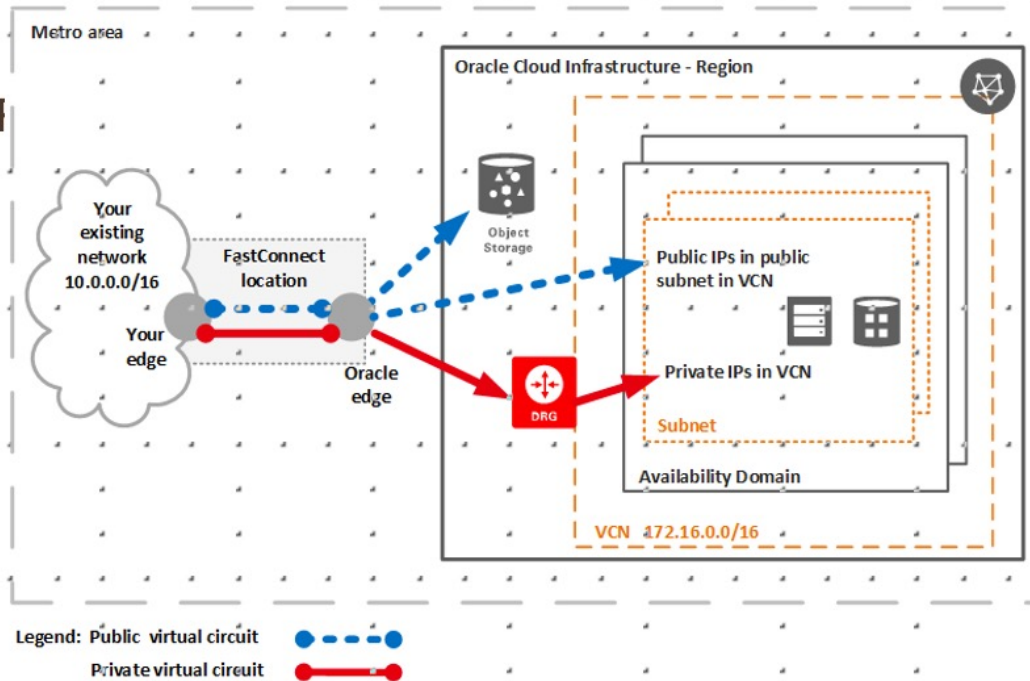
- Connect to Public services like Object Storage or Public load balancer via **FastConnect**.
- Public peering with **FastConnect** provides an alternative to public Internet access for customers to connect to their public resources in OCI.
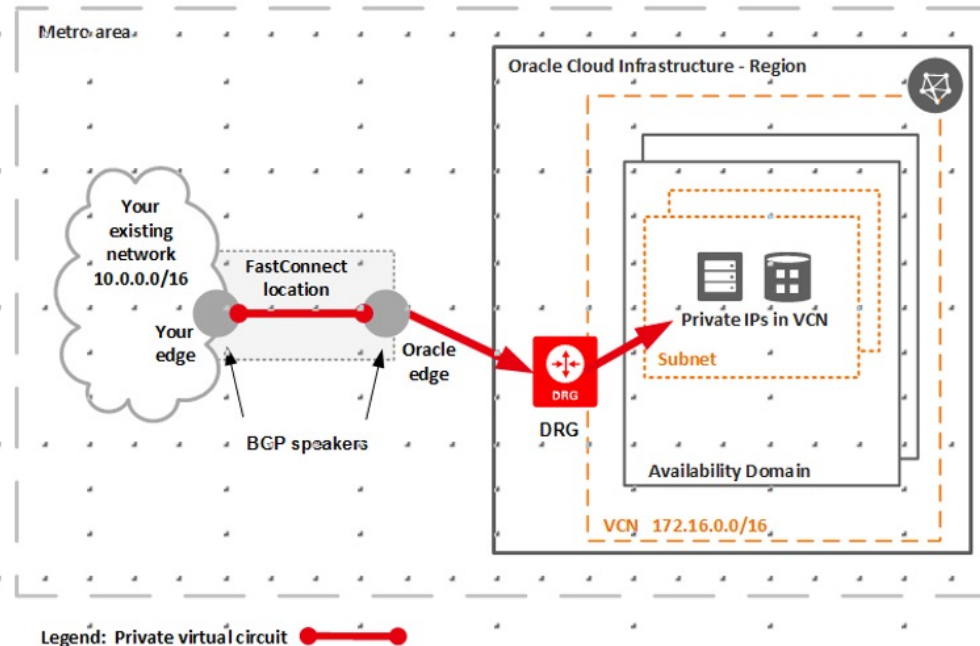
- Extend your existing infrastructure into Oracle Cloud Infrastructure resources using Private IPs in a virtual cloud network (VCN) accessed via **FastConnect**.

FastConnect Use Cases Summary

	FastConnect-Private Peering Infrastructure Extension	FastConnect-Public Peering Internet Alternative
Use case	To manage VCN resources privately – Infrastructure Extension	To access OCI's public service offering – INTERNET Alternative
Typical bandwidth	Higher bandwidth; increments of 1 Gbps, and 10 Gbps ports	Higher bandwidth; increments of 1 Gbps, and 10 Gbps ports
Protocols	BGP	BGP
Point-to-point BGP IPs	Customer assigns IPs (/30 or /31)	Oracle assign IPs (/30 or /31)
Prefix-advertisement	OCI advertises VCN subnet routes	OCI advertises public VCN routes and public services routes (Market Level Routes)
Prefix-validation	Not needed	OCI does validation that prefixes are owed by customer or not
Prefix-limit	2000	200
BGP ASN	Any ASN	Public ASN

FastConnect Redundancy

With FastConnect there are multiple types of redundancy

- Transit POP redundancy
- Router redundancy with-in a single Transit POP
- Partner redundancy
- Service redundancy

Oracle provides:

- **Per region:** 2 Oracle points of presence (POPs), for location redundancy. Each is connected to all of Oracle's Availability Domains in the region
- **Per Oracle POP:** 2 routers, for router redundancy

This means for every region, you could have up to 4 independent physical cables to Oracle.

Multicloud Architecture

ORACLE® + Microsoft Azure

- Oracle and Microsoft have announced a cloud interoperability partnership enabling customers to migrate and run mission critical enterprise workloads across Microsoft Azure and Oracle Cloud.

- Enterprises can now seamlessly use and connect Azure services to Oracle Cloud.

- This partnership delivers a highly-optimized, secure, and unified cloud experience for our customers.

- Only Oracle and Microsoft are providing a "connected cloud" which enables swift migration of on-premises applications and the ability to leverage a broader range of tools and ecosystems.

Partnership Benefits

| Licenses | Skillsets |
| Toolkits | Solutions |

Support

Virtual Networks, Functions, Containers, AKS, AI, IoT, etc.

Innovate across clouds

Choice of services

Leverage existing investme
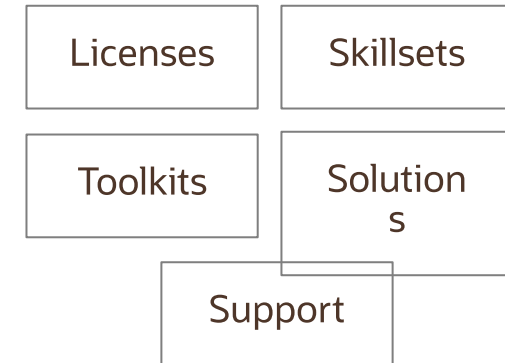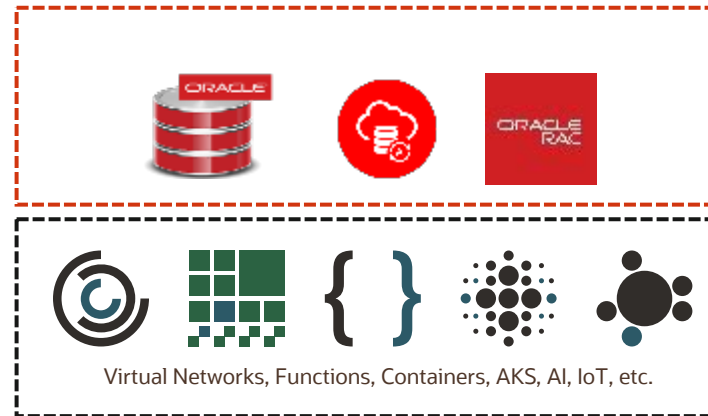
For the first time, you can now run enterprise grade multi-cloud applications between Oracle Cloud and Azure. Take advantage of direct and fast interconnect and unified identity.

A one-stop-shop for all the database and cloud services customers need – the best of Oracle Cloud and Microsoft Azure combined.

Migrate entire sets of on-premises applications and databases to the cloud without having to re-architect technology or change customer support.

What does the partnership include: Three Pillars

1. Technology integration

- Private interconnect with FastConnect and ExpressRoute
- Unified identity and access management

2. Application interoperability

- Tested, validated, and supported application deployments
- Innovate across clouds
- Large choice of services
- Leverage existing investments

3. Collaborative support model

Joint, collaborative, standard support model

- Seamless issue resolution
- Customers can contact either Microsoft or Oracle when encountering an issue

Microsoft Azure + **ORACLE**

Microsoft Azure — Cross-cloud SSO and Interconnect — ORACLE Cloud Infrastructure

Interoperability

- Azure DevOps
- Azure Stream Analytics
- Azure Databricks
- Azure Cognitive Services
- Azure IoT Hub
- Azure Kubernetes Service
- And other services…

- Oracle Cloud Infrastructure
- Oracle Autonomous Database
- Oracle Exadata
- Oracle Applications
- Oracle RAC
- Oracle Analytics Cloud
- And other services…

Common Use-cases

SSO, cross-cloud
interconnect

App A	App B	App C	App D
Java	E-Business Suite	.NET	.NET
Oracle DB	Oracle DB	SQL Server	SQL Server

Oracle Cloud ⟷ Azure

Supported Deployments:

- Full stack Oracle or custom applications on Oracle Database on OCI and Full stack apps on Azure that interoperate and share data

- Oracle Apps (PSFT, JDE.,) on Azure using Oracle Database on OCI

- Custom .NET application on Azure using Oracle Database on OCI

- Custom Cloud Native applications on Azure using Oracle Autonomous DB

- Applications/Oracle Database in OCI, Azure Data Lake for analytics & Cognitive Services for AI

- SQL Azure, SQL Server, SQL DW on Azure and Oracle Analytics Cloud, Data Science service on OCI

Architecture - Azure OCI Interconnect
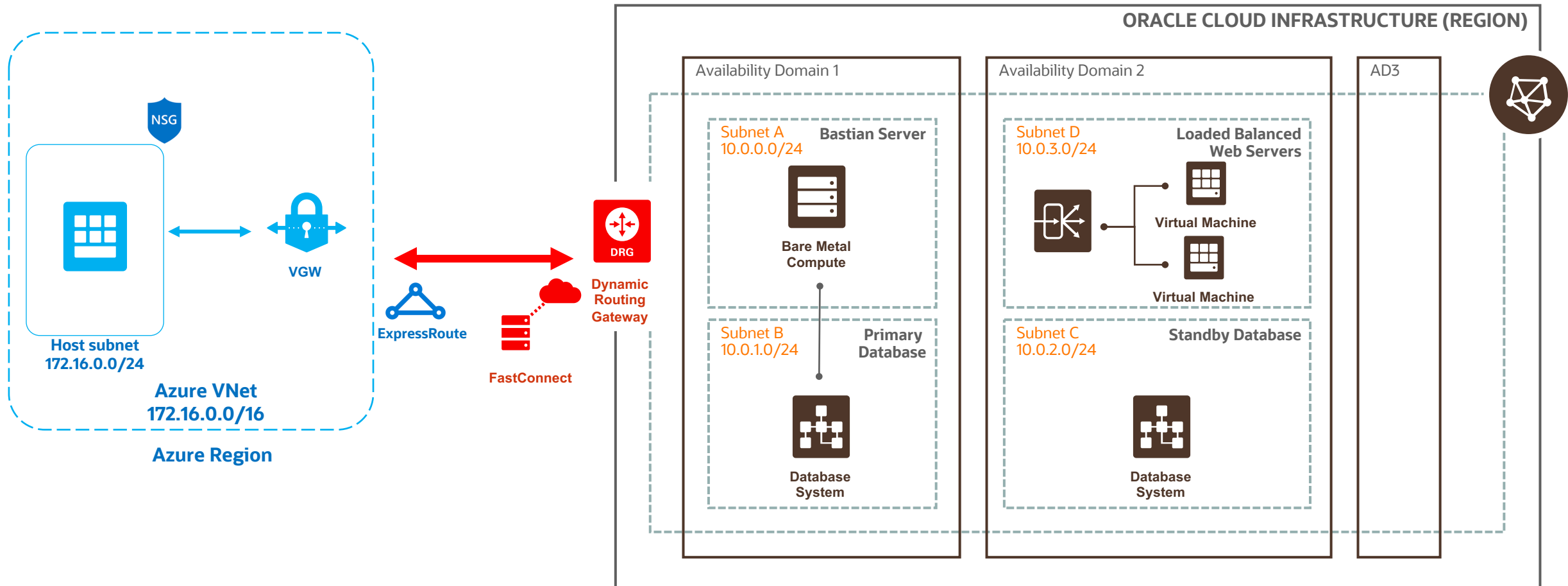
Oracle Cloud Infrastructure Global Locations
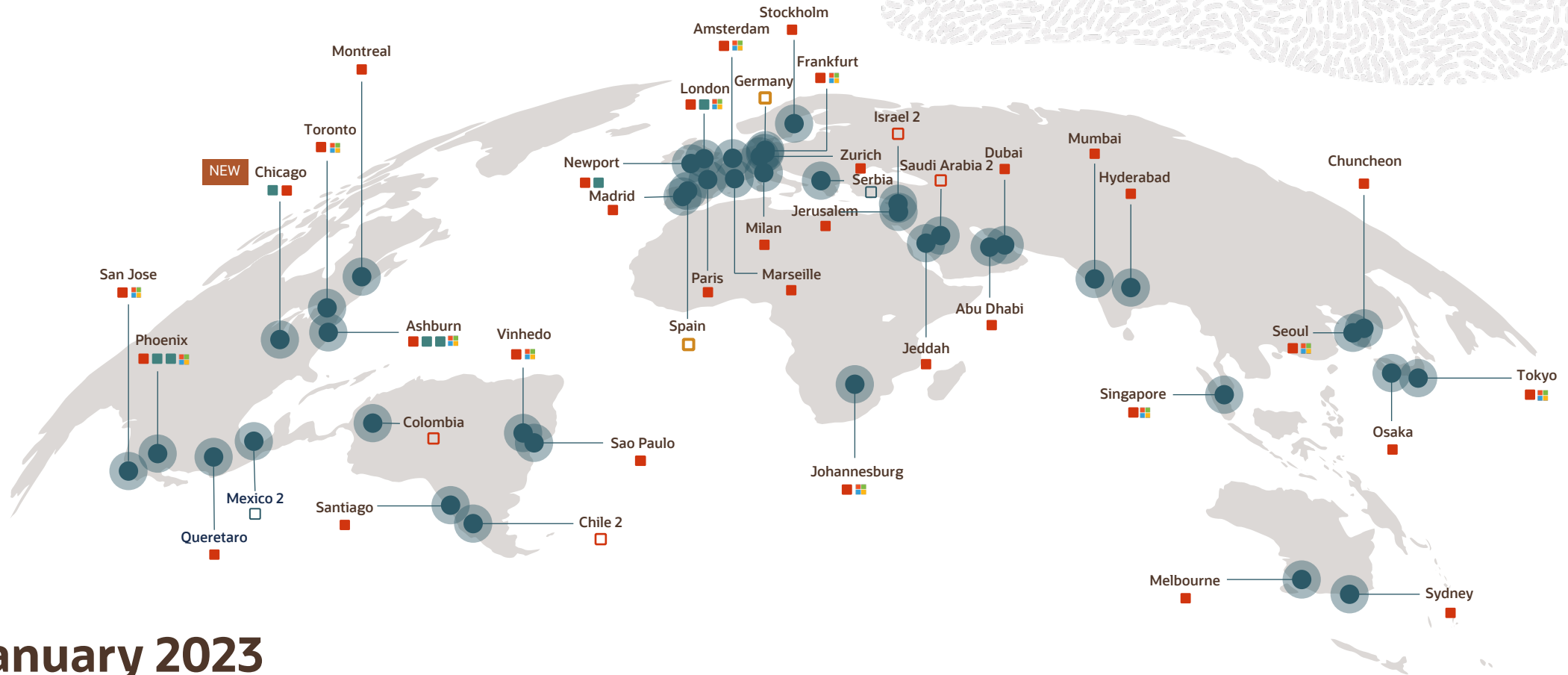
January 2023

41 regions; 8 more planned

12 Azure Interconnect Regions

Copyright © 2022, Oracle and/or its affiliates.

Your network requirements

Advanced Network Topics

DRG Routing Engine

Design

1. Each VCN, FastConnect, IPSEC, or RPC connection is "connected" to the DRG via an Attachment.

2. Each "Attachment" has a route table assigned, which directs ingress traffic to a specific egress attachment.

Operation

1. A Packet arrives from VCN or on-premise into the DRG

2. The DRG routing engine determines which Attachment to egress the packet out of based on the associated route table.

IP Packet

On-Premise

Route Table #2, #3, etc.
Route Target : Dest Att
Route Target : Dest Att

(3)

| IPSEC Attachment | IPSEC Attachment | FC Attachment |

DRG 1

DRG Routing Engine

RPC Attachment ↔ RPC Attachment **DRG 2**

| VCN 1 Attachment | VCN 2 Attachment | VCN 3 Attachment |

(1)

VCNs

(2) Route Table #1
Route Target : Dest Att

IP Packet

(1) Packet arrives into DRG from VCN (VCN attachment) or on-premise (FC/IPSEC attachment) or remote region (RPC attachment).
(2) A route lookup is performed on the route table associated with the ingress attachment.
(3) The packet is forwarded by the DRG routing engine out an Egress attachment.

DRG Enhancements: Remote On Ramp

- FastConnect or IPSEC VPN in Region (A)

- Able to access resources in Region (B)

- Uses the OCI Private backbone.

- Can also provide redundancy.

OCI Ashburn

VCN A
10.0.0/24

DRG

**RPC Peering
OCI Backbone**

OCI London

VCN B
10.0.1.0/24

DRG

**Fastconnect /
IPSEC**

CPE

**On-prem Subnet
192.168.0.0/24**

**Customer On-premise
Location A**
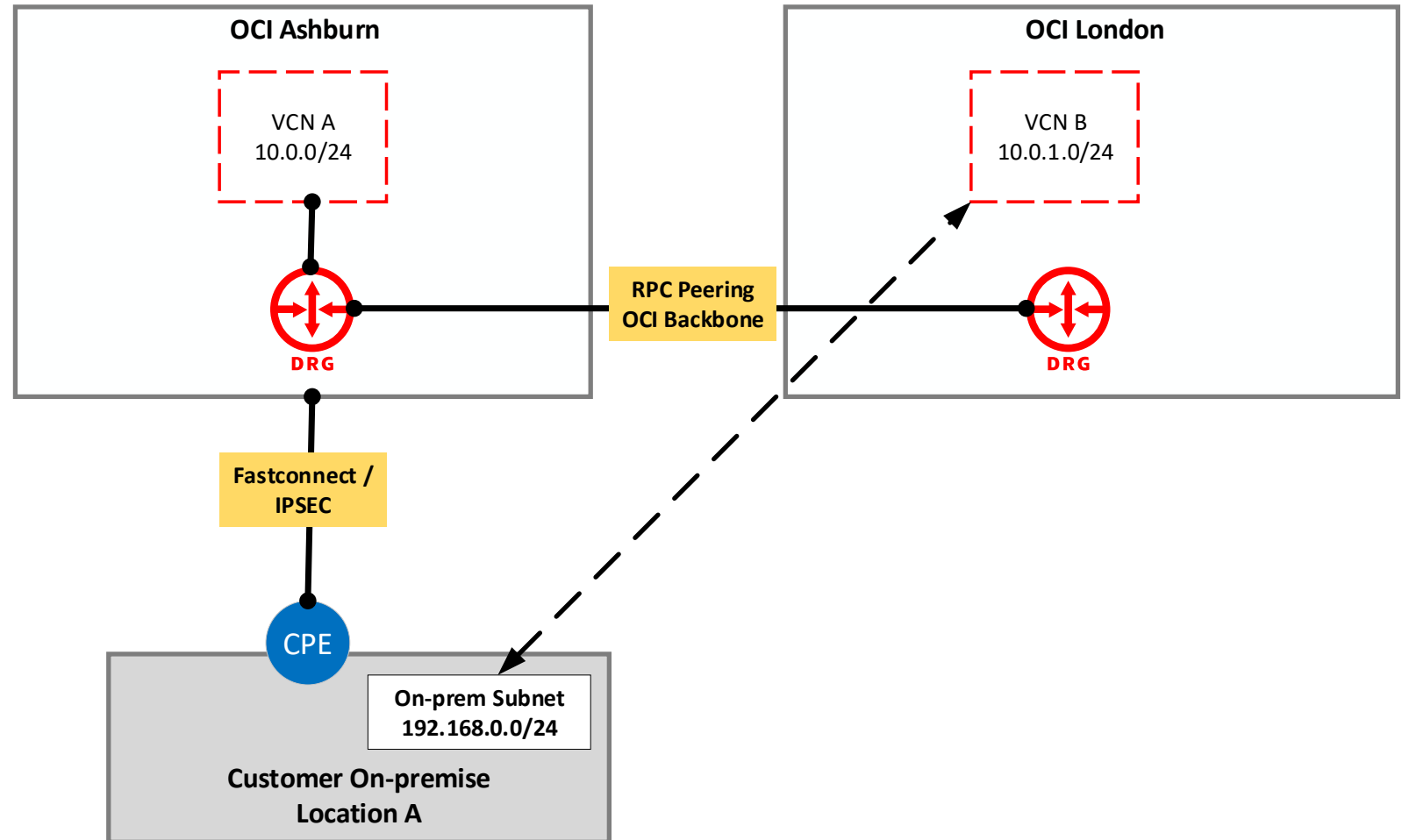
DRG : ECMP (Active/Active) support

- OCI now support "ECMP" for Active/Active load sharing.
- Bundle up to (8) IPSEC or FastConnect connections.
- Enabled on a per-route table basis.

OCI Ashburn

VCN A
10.0.0/24

DRG   DRG *

**Fastconnect
w/ ECMP**

10GB + 10GB =
20GB usable
capacity

CPE   CPE

**On-prem Subnet
192.168.0.0/24**

**Customer On-premise
Location A**
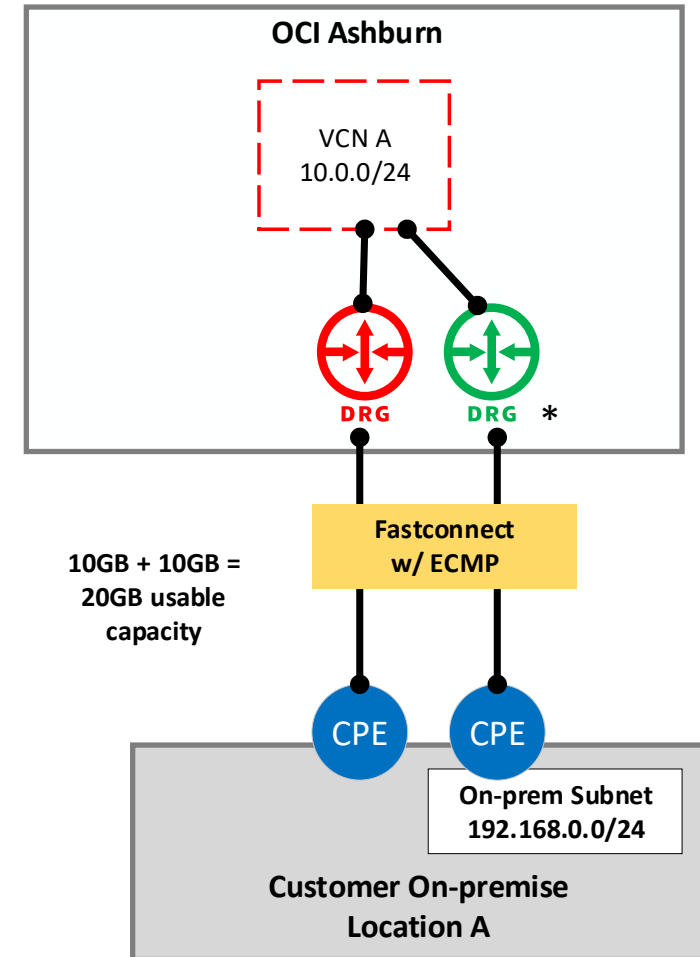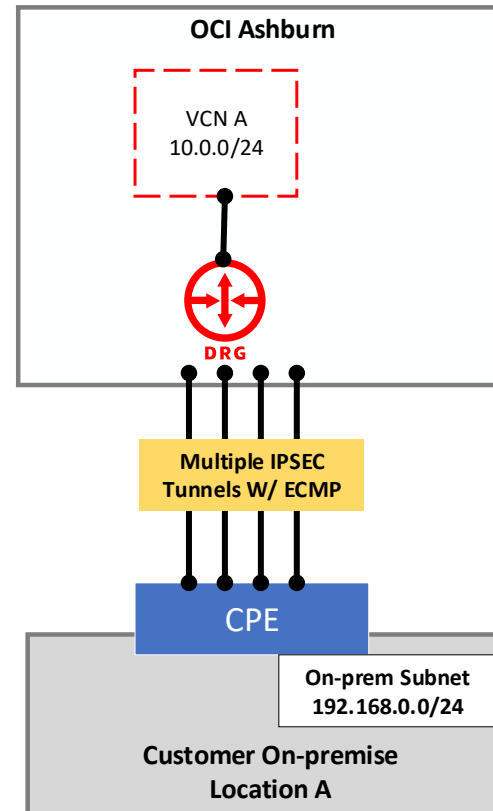
* OCI only has a single DRG , but it can contain multiple physical routers.
For clarity, the second DRG refers to a different physical Oracle (PE) router.

OCI Ashburn

VCN A
10.0.0/24

DRG

**Multiple IPSEC
Tunnels W/ ECMP**

CPE

**On-prem Subnet
192.168.0.0/24**

**Customer On-premise
Location A**

DRG: L3 Firewall

- All traffic between VCNs is routed via L3 NVA (Network Virtual Appliance – or Firewall)

- Routing tables are used to direct traffic via a specific VCN, and the DRG-attachment routing table forces all traffic to the NVA.
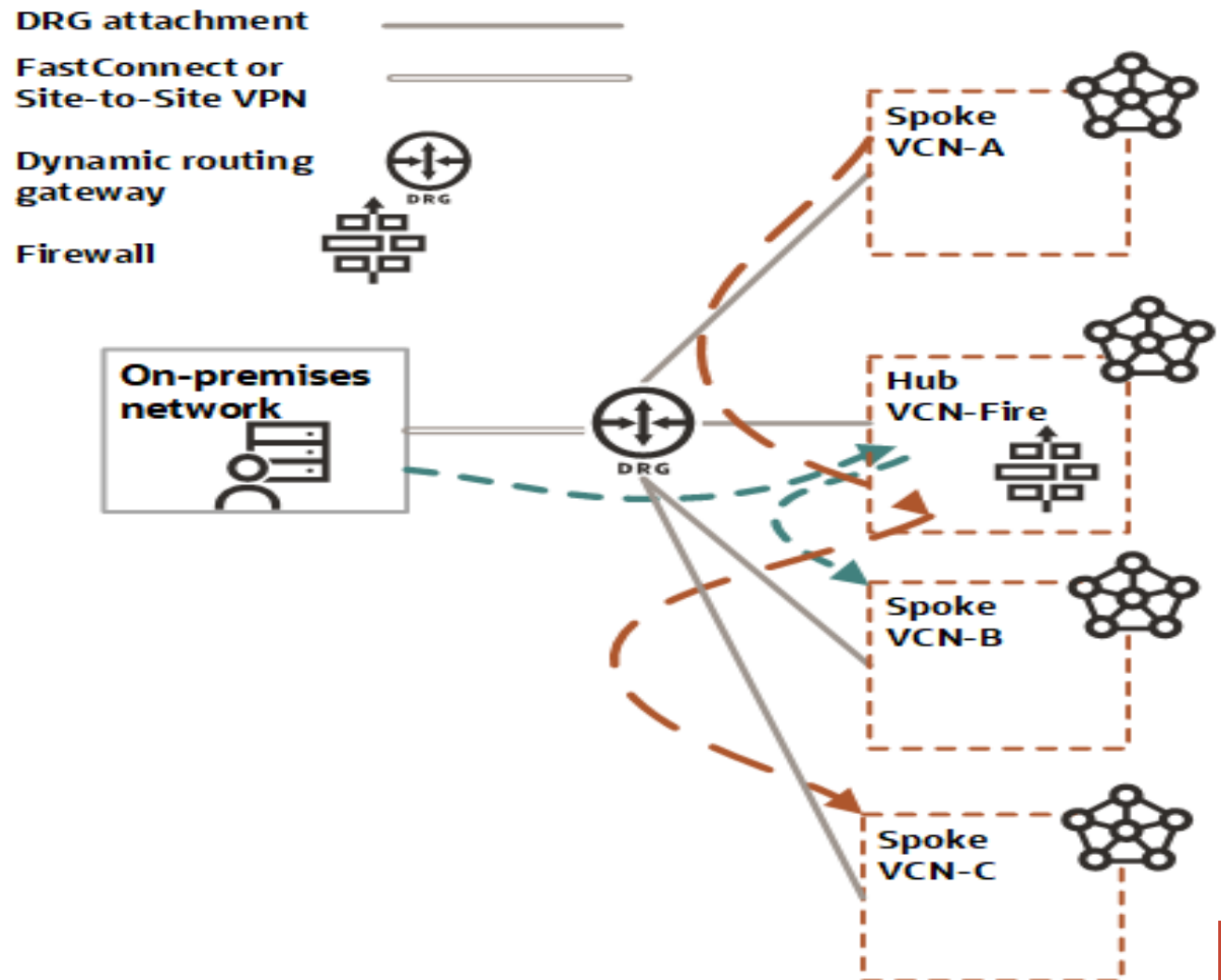
Redundancy: Connectivity Model

- Transit POP redundancy

FastConnect POP Location 1

Customer Edge 1

FastConnect Redundancy

Oracle Edge 1

Virtual Circuit 1

Router 1

Router 1

FastConnect POP Location 2

Customer Edge 2

Oracle Edge 2

Virtual Circuit 2

Router 1

Router 1

Cross-connect Group (LAG)

Virtual Circuit

Cross-Connect (Physical Connection)
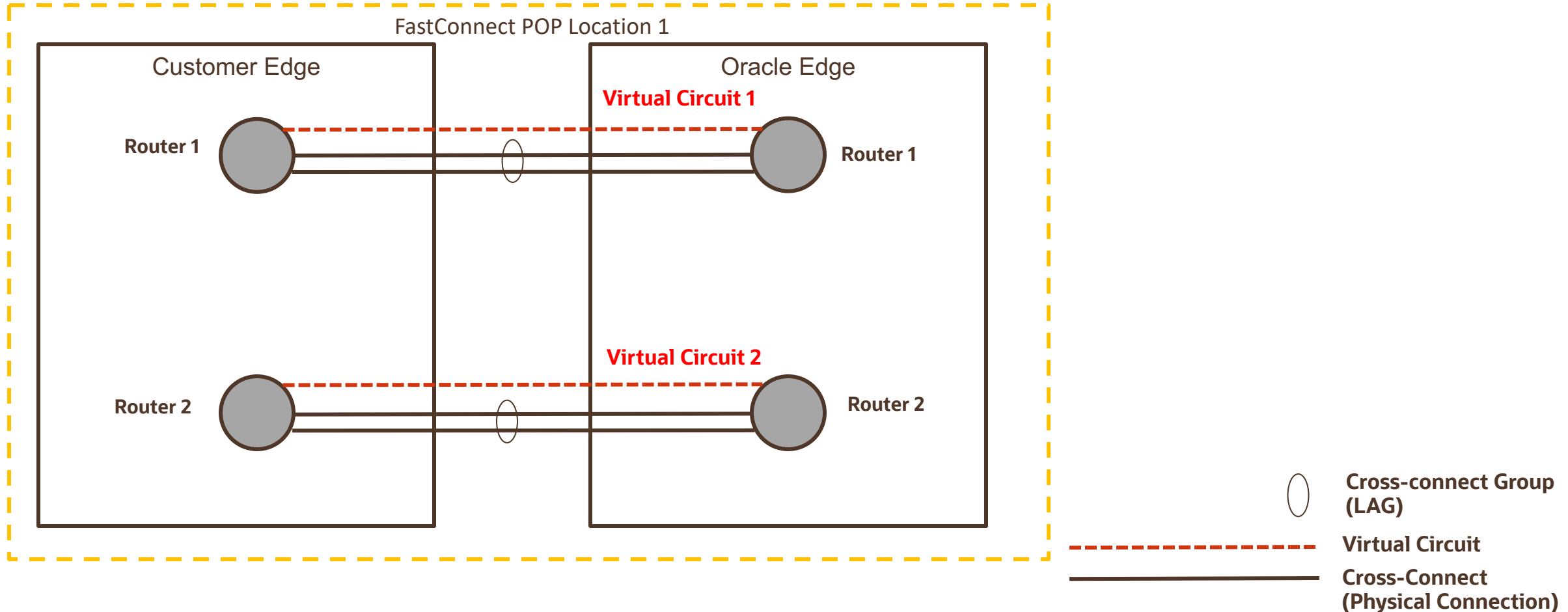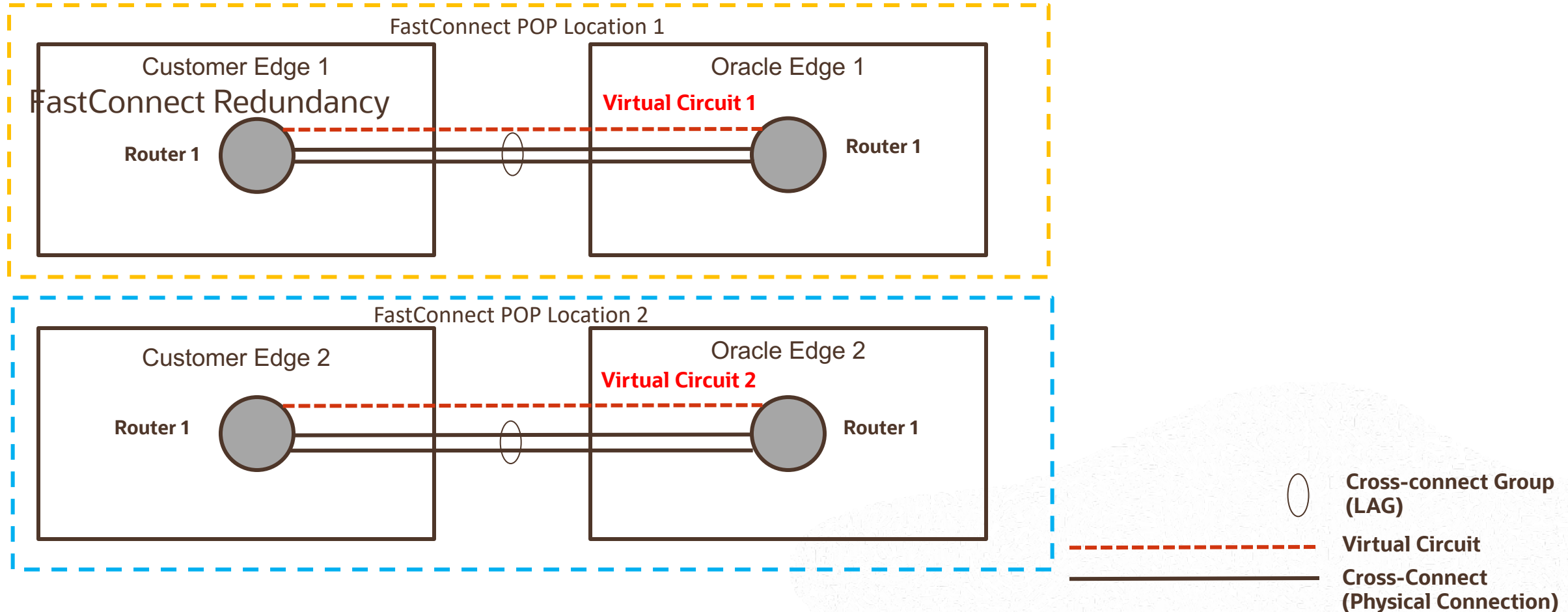
Layer 2 Partners : Megaport, Equinix, CenturyLink

FastConnect Redundancy

OCI Region

Oracle requires redundancy with Partners

Customer responsible for redundancy

Customer DC

CPE

PE

Partner X Network

Virtual Circuit -1

Virtual Circuit -2

PE

PE

Oracle POP 1

Router 1

Oracle POP 2

Router 1

BGP Session
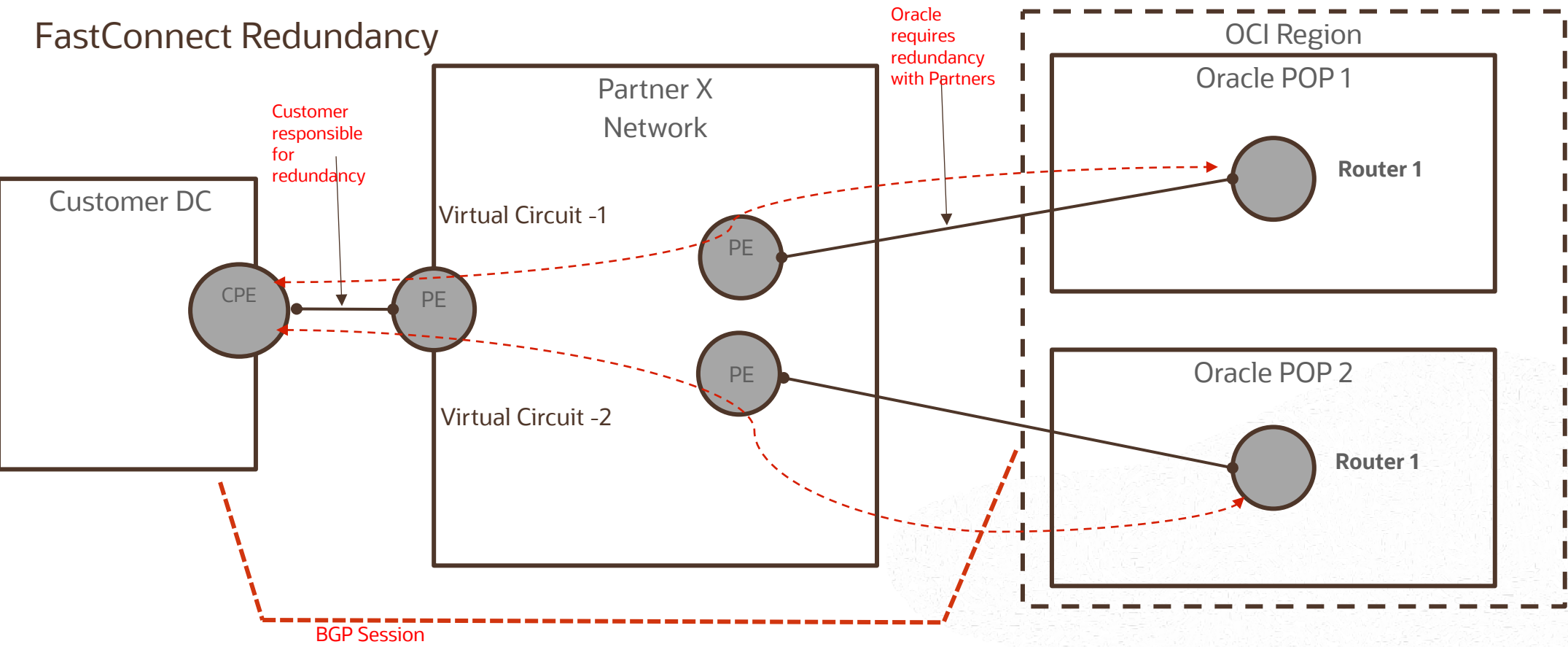
Layer 3 Partners :Verizon, BT
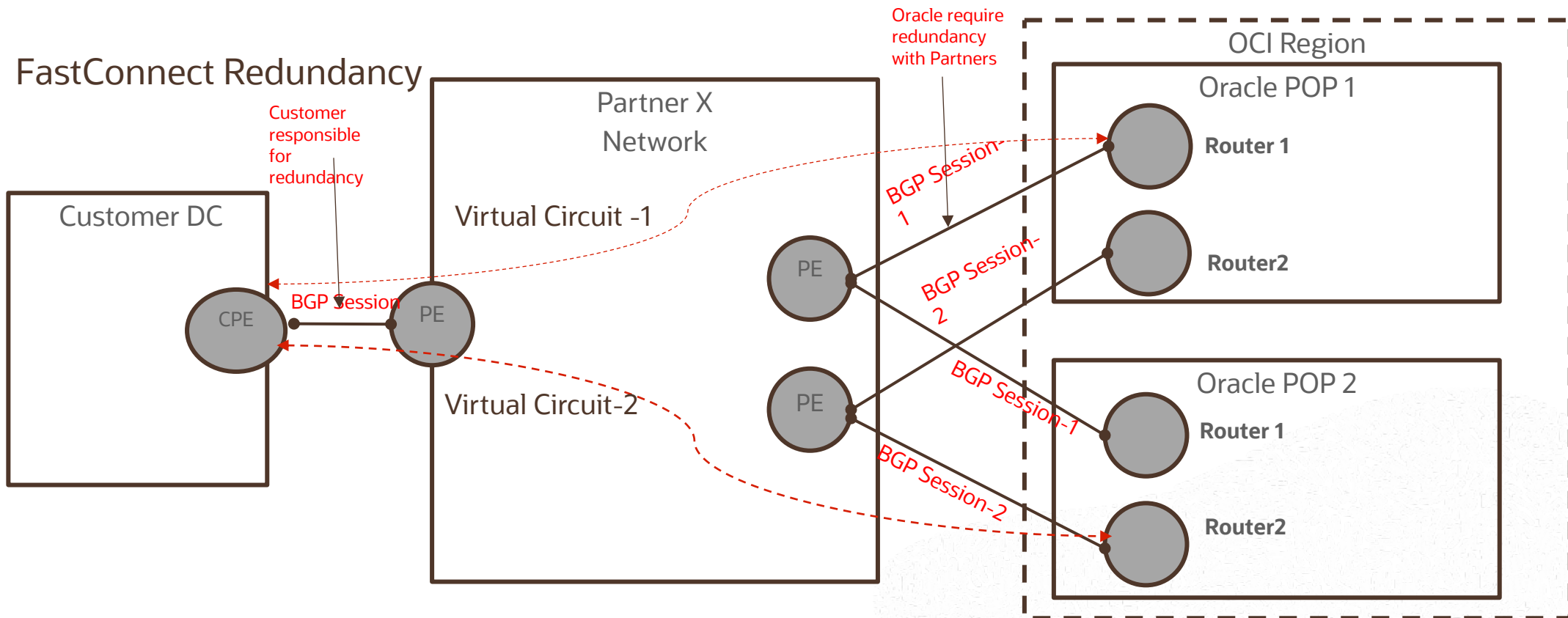
Private Peering network design

- **Routing Protocol**

    OCI currently supporting BGP(Border Gateway protocol) as a routing protocols for FastConnect connectivity to connect to partners as well as customers

    BGP is standardized exterior gateway protocols designed to exchange routing and reachability information between ASNs

    BGP is open standard protocol supported by all hardware vendor

- **BGP IP address assignment**

    Customer/L3 Provider can use any /30 or /31 ip address that they want to use.

    This IP address is used for point to point addressing as well as BGP peer addresses

Private Peering network design contd..

- BGP ASN

    Similar to public and private addresses there are private (64512- 65535) & public ASN(1 - 64511) allocation

    OCI only supports 2 byte ASN

    The BGP ASN for OCI will be 31898 regardless of region

    Customer can use any ASN that they comfortable using

LAG Support (Cross-Connect Groups)

    You can aggregate multiple physical links in to a single logical channel based on IEEE 802.3ad also known as LACP (Link Aggregation Control Protocol)

    LAG provides Link level redundancy and OCI always recommend partners and customer to build LAG even with Single physical member so when we have to scale up there is no downtime

Private Peering network design contd.. (2)

BGP Authentication

    OCI supports BGP authentication mechanisms like Message Digest5 (MD5) algorithms. When authentication in enable any TCP segment belonging to BGP exchanged between peers is verified and accepted only if Authentication is successful.

    Most types of authentication require administration and can disproportionately consume router resources as a result. OCI doesn't recommend using it unless customer have hardcore requirement.

    OCI will not use MD5 with partners

Prefix-Acceptance

    OCI will accept any-prefix advertise by customer over the FastConnect BGP session

    No restriction on prefix-length

    The only limit is number of prefixes(2000) that customer can advertise over the VC/BGP session

Public Peering network design

- **BGP IP address assignment**

  - In contrast to FastConnect-private, Customer's Layer 3 point-to-point interface will be part of shared Internet routing-instance instead of unique DRG routing-instance.

  - Because of customers is going to share same routing-instance we need to make sure that the IP addresses are unique.

  - OCI will assign the point to point IPs from range(169.254.0.0/16)

BGP Prefix-advertisement

  - OCI will advertise all the public prefixes for specific region customer is peering with

  - Public prefixes will include IP ranges that covers all public service offering by OCI

  - Public prefixes will also covers all the customer's public VCN host prefixes

Public Peering network design contd.

- **BGP Prefix-acceptance**

  - Customer provides list of prefixes that they want to advertise via console

  - OCI accepts the public-prefixes only if prefixes are owned by customer.

  - OCI Check multiple Internet Route Registry database(Using Dyn tool) to verify who owns the prefixes before accepting the prefix from the customer.

- **BGP ASN**

  - OCI will use 31898 ASN

  - Customer needs public ASN to peer with OCI

ORACLE

Oracle Cloud always free tier:
oracle.com/cloud/free/

OCI training and certification:
oracle.com/cloud/iaas/training
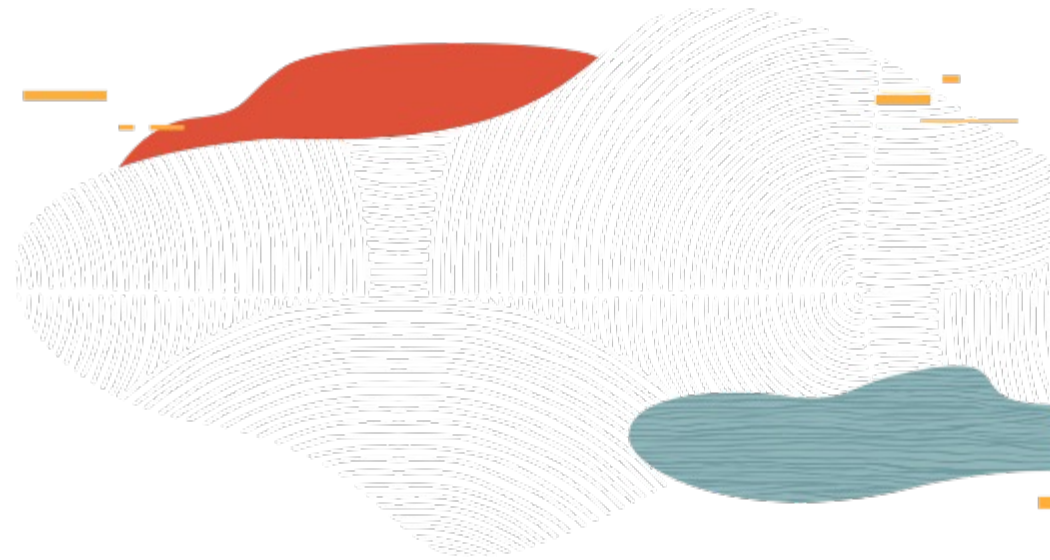oracle.com/cloud/iaas/training/register-for-training.html
oracle.com/cloud/iaas/training/certification.html

OCI hands-on labs:
ocitraining.qloudable.com/provider/oracle

Oracle learning library videos on YouTube:
youtube.com/user/OracleLearning

Thank you