Connectivity – FastConnect
Level 201
Jamal Arif
November 2018
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, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Objectives

After completing this lesson, you should be able to:

• Describe FastConnect Public and Private Peering
• Discuss FastConnect Redundancy
• Hybrid Architectures
• InterCloud Connectivity
• Pre-requisites: Connectivity – Level 100
• Pre-requisites: Connectivity – Level 200
FastConnect Use Case Scenarios

• Private Peering
  • Extension of the on premise network to the OCI VCN
  • Communication across connection with private IP addresses

• Public Peering
  • To access public OCI services over dedicated FastConnect connection
  • Access Object storage, OCI Console or APIs
  • Communication across connection with public IP addresses
FastConnect Use Scenarios

• Private Peering
  • Extension of the on premise network to the OCI VCN
  • Communication across connection with private IP addresses

• Public Peering
  • To access public OCI services over dedicated FastConnect connection
  • Access Object storage, OCI Console or APIs
  • Communication across connection with public IP addresses
FastConnect (Private Connection)
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 is enabled 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
Private Peering network design contd.. (2)

- BGP session will go down once customer reach to this limit
- Customer can request more than 2000 prefix per BGP session but it's based on the request not by default as there is billing involved with it.

**Prefix-advertisements**
- OCI will advertise all the Subnet routes that customer have created in their VCN over the BGP session
BGP advertisement and Traffic-flow

CPE/L3 Provider

Customer network

192.168.1.0/24
192.168.2.0/24
172.16.0.0/16

10.1.1.0/24
10.1.2.0/24
10.1.3.0/24

DRG routing-table
192.168.1.0/24
192.168.2.0/24
172.16.0.0/16
10.1.1.0/24
10.1.2.0/24
10.1.3.0/24

Dynamic Routing Gateway

VPN-GW

eBGP

VCN

CIDR 10.1.0.0/16

10.1.1.0/24

AVAILABILITY DOMAIN - 1

10.1.2.0/24

AVAILABILITY DOMAIN - 2

10.1.3.0/24

AVAILABILITY DOMAIN – 3

VCN

192.168.1.0/24
192.168.2.0/24
172.16.0.0/16

192.168.1.0/24
192.168.2.0/24
172.16.0.0/16
FastConnect Use Scenarios

- Private Peering
  - Extension of the on premise network to the OCI VCN
  - Communication across connection with private IP addresses
- Public Peering
  - To access public OCI services over dedicated FastConnect connection
  - Access Object storage, OCI Console or APIs
  - Communication across connection with public IP addresses
FastConnect (Public Peering Connection)
FastConnect (Public Peering Connection)

- You choose which of your organization's public IP prefixes you want to use with the virtual circuit. Each prefix must be /31 or less specific.

- Oracle verifies your organization's ownership of each prefix before sending any traffic for it across the connection.

- When configuring your edge for public peering, make sure to give higher preference to FastConnect over your ISP.

- Oracle prefers the most specific route when routing traffic from Oracle Cloud Infrastructure to other destinations that means even if you have a IGW, replies to your verified public prefixes will go over the FastConnect connection.

- You can add or remove public IP prefixes at any time by editing the virtual circuit.
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
Public Peering network design contd. (2)

- **BGP Prefix-limitation**
  - The only limit is number of prefixes (200) that customer can advertise over the VC/BGP session. BGP session will go down once customer reach to this limit.
  - Customer can request more than 200 prefix per BGP session but it's based on the request not by default as there is billing involved with it.
BGP advertisement and Traffic-flow

- Customer network: 129.254.0.0/17, 129.254.128.0/17, 1.1.1.0/24
- CPE: 1.1.1.0/24
- eBGP: 129.254.0.0/17, 129.254.128.0/17
- Internet: 129.146.128.0/17, 129.146.0.0/17, 1.1.1.0/24
- OCI Public services IPs: 129.146.128.0/17 (Block storage, Casper, etc.)
- Customer’s Public VCN IPs: 129.146.0.0/17
- OCI Region

Oracle, Inc.
### Private and Public Peering

<table>
<thead>
<tr>
<th></th>
<th>FastConnect-Private</th>
<th>FastConnect-Public</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use case</strong></td>
<td>To manage VCN resources privately</td>
<td>To access OCI’s public service offering</td>
</tr>
<tr>
<td><strong>Typical bandwidth</strong></td>
<td>Higher bandwidth; increments of 1 Gbps, and 10 Gbps ports</td>
<td>Higher bandwidth; increments of 1 Gbps, and 10 Gbps ports</td>
</tr>
<tr>
<td><strong>Protocols</strong></td>
<td>BGP</td>
<td>BGP</td>
</tr>
<tr>
<td><strong>Point-to-point IPs</strong></td>
<td>Customer assigns IPs (/30 or /31)</td>
<td>Oracle assign IPs (/30 or /31)</td>
</tr>
<tr>
<td><strong>Prefix-advertisement</strong></td>
<td>OCI advertises VCN subnet routes</td>
<td>OCI advertises public VCN routes and public Services routes</td>
</tr>
<tr>
<td><strong>Prefix-validation</strong></td>
<td>Not needed</td>
<td>OCI does validation that prefixes are owed by customer or not</td>
</tr>
<tr>
<td><strong>Prefix-limit</strong></td>
<td>2000</td>
<td>200</td>
</tr>
<tr>
<td><strong>BGP ASN</strong></td>
<td>Any ASN</td>
<td>Public ASN</td>
</tr>
</tbody>
</table>
FastConnect Redundancy – Best Practices
FastConnect Redundancy

• Have multiple redundant connections into OCI and avoid having *single points of failure* in your design.

• For IPSec VPN - OCI recommends using multiple connections from *redundant* physical devices at the customer premises. High availability connections require redundant hardware, even when connecting from the same physical location.

• OCI FastConnect provides multiple redundancy options, and it's recommended to use multiple vendors if financially feasible to ensure you have redundant network connections.

• Plan for sufficient network capacity with your FastConnect virtual circuits to ensure individual circuits are not overwhelmed in case of failures on redundant circuits.

• Have a service level redundancy by creating an IPsec VPN service alongside FC. Oracle always prioritizes FC over VPN connection.
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. Your ideal goal is to have 2 virtual circuits per customer, one per Oracle POP
Redundancy: Connectivity Model
Colocation or colocation via third party Network Provider

• Transit POP redundancy
Redundancy: Connectivity Model
Colocation or colocation via third party Network Provider

Router redundancy with-in a single Transit POP
Redundancy: Connectivity Model
Oracle Partner (Layer 2)

• For a **Layer 2** partner, a given virtual circuit can run on only a single port group (formerly known as Cross-Connect) (LAG), or single cross-connect (an individual cable, no LAG).

• Redundancy can be achieved by provisioning **2nd** virtual circuit.

• Partner will make sure that 2**nd** virtual circuit will land on redundant cross-connect LAG between them and Oracle.

• Redundant cross-connect LAG could land in same POP or different POP depending upon connectivity between partner and oracle.

• Active/Active or Active/Passive setup is possible with “LP” and “AS_PATH” BGP attributes influencing egress traffic from customer and OCI respectively.
Redundancy: Connectivity Model
Oracle Partner (Layer 2) – Transit pop redundancy
Redundancy: Connectivity Model
Oracle Partner (Layer 2) – Router redundancy

Partner Edge

FastConnect POP Location 1

Oracle Edge

Router 1

Virtual Circuit 1

Virtual Circuit 2

Router 2

Cross-connect Group (LAG)

Virtual Circuit

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

For Redundancy

<table>
<thead>
<tr>
<th>Customer</th>
<th>Partner</th>
<th>Oracle</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Order 2X VC with Oracle • Order 2X cross-connects to partner</td>
<td>• Min 2X Circuits to Oracle • Provisions 2nd VC on redundant cross-connect</td>
<td>• Min 2X Circuits to Partner • Agreement with partner to Provision 2nd VC on redundant cross-connect</td>
</tr>
</tbody>
</table>
Redundancy: Connectivity Model
Oracle Partner (Layer 3)

• For a **Layer 3** partner, a given virtual circuit can run on multiple cross-connect groups (LAGs) or multiple cross-connects (a cross-connect is an individual cable, no LAG), which provides router redundancy for the virtual circuit.

• Customer would get 2 BGP sessions tied to single virtual circuit by default running over redundant cross-connect group or cross-connects.

• Partner and Oracle will make sure that 2\textsuperscript{nd} BGP session will land on redundant cross-connect LAG between partner and Oracle.

• Customer can still provision 2\textsuperscript{nd} virtual circuit with additional cost should they need redundancy with virtual circuits.
Redundancy: Connectivity Model
Oracle Partner (Layer 3) – Transit pop redundancy

FastConnect POP 1
Partner
Router 1
Router 2

Virtual Circuit 1

Oracle POP 1
Router 1
Router 2

FastConnect POP Location 2
Partner
Router 1
Router 2

Virtual Circuit 2

Oracle POP 2
Router 1
Router 2

Cross-connect Group (LAG)
Virtual Circuit
Cross-Connect (Physical Connection)
Redundancy: Connectivity Model
Oracle Partner (Layer 3) – Router redundancy

Partner Edge

FastConnect POP Location 1

Oracle Edge

Router 1

Virtual Circuit 1

Router 2

Cross-connect Group (LAG)

Virtual Circuit

Cross-Connect (Physical Connection)
Layer 3 Partners : Verizon, BT

Customer DC

Partner X Network

Virtual Circuit -1

Virtual Circuit -2

For Redundancy

Customer
• Order 2X VC with Oracle
• Order 2X cross-connects to partner

Partner
• Min 2X Circuits to Oracle
• Runs 2 BGP sessions with Oracle

Oracle
• Min 2X Circuits to Partner
• Runs 2 BGP sessions with Partner.

Oracle require redundancy with Partners

Customer responsible for redundancy

Oracle POP 1

Oracle POP 2

OCI Region

Router 1

Router 2

Router 1

Router 2

BGP Session 1

BGP Session 2

BGP Session 1

BGP Session 2

BGP Session 1

BGP Session 2

BGP Session 1

BGP Session 2

BGP Session 1

BGP Session 2

BGP Session 1

BGP Session 2
Partner or Provider Redundancy

- For partner or provider level redundancy, customer should have redundant links to partner.
- Most Partners already have redundant links to OCI.
- Connections on different routers on partner’s network.
- Provision virtual circuits across multiple provider links
Service Redundancy

- Customer can provision IPsec along with FastConnect.
- IPsec can be treated as back up in case FastConnect fails.
- Egress traffic from OCI will prefer FastConnect.*
- Bandwidth, latency concerns over IPsec.
- Highly recommended if customer has single FastConnect to OCI.
## IPsec VPN and FastConnect

<table>
<thead>
<tr>
<th></th>
<th>Site-to-Site VPN</th>
<th>FastConnect</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use case</strong></td>
<td>Dev/test and small scale production workloads</td>
<td>Enterprise-class and mission critical workloads, Oracle Apps, Backup, DR</td>
</tr>
<tr>
<td><strong>Supported Services</strong></td>
<td>All OCI Services within VCN – compute – VMs and BMs, Database</td>
<td>All OCI Services within VCN – compute – VMs and BMs, Database</td>
</tr>
<tr>
<td><strong>Typical bandwidth</strong></td>
<td>Typically &lt; 250 Mbps aggregate</td>
<td>Higher bandwidth; increments of 1 Gbps, and 10 Gbps ports</td>
</tr>
<tr>
<td><strong>Protocols</strong></td>
<td>IPsec</td>
<td>BGP</td>
</tr>
<tr>
<td><strong>Routing</strong></td>
<td>Static Routing</td>
<td>Dynamic Routing</td>
</tr>
<tr>
<td><strong>Connection Resiliency</strong></td>
<td>active-active</td>
<td>active-active</td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td>Yes, by default</td>
<td>No * (can be achieved using virtual firewall)</td>
</tr>
<tr>
<td><strong>Pricing</strong></td>
<td>• Billable port hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No data transfer charge between ADs</td>
<td></td>
</tr>
<tr>
<td><strong>SLA</strong></td>
<td>No SLA</td>
<td>99.9% Availability SLA</td>
</tr>
</tbody>
</table>
Hybrid Architectures using FastConnect
Hybrid Architectures

• In Hybrid deployments, customers have on-premises workloads that require connectivity with OCI services (compute instances with in a VCN or OCI public services like Object Storage)

• Three ways to establish this connectivity
  • Accessing OCI resources using Public IPs over Public Internet
  • Accessing OCI resources using Private IPs leveraging site-to-site IPsec VPN over public Internet
  • Accessing OCI resources using over a private dedicated circuit leveraging OCI FastConnect

• Typical application architectures that require hybrid connectivity
  • Three-Tier Web Application
Three-Tier Web Applications

- During phased application migration, hybrid connectivity is required for instance your web and app servers are in OCI and DB on-premises.
Three-Tier Web Applications (2)

- Another way to load balancer traffic between multiple environments is to use DNS based Load Balancing
- DNS record mapping to your domain name that has IP of OCI Public Load Balancer and your on-premises load balancer
Network Consistent Apps with dedicated Virtual Circuit

a. Same VCN

- Create multiple Virtual Circuits over FC physical connection (different router same POP or different routers different POP) and use
  - AS PATH prepends to make 1Gbps virtual circuit primary for dev traffic and 10Gbps Virtual Circuit Primary for Prod Traffic
Network Consistent Apps with dedicated Virtual Circuit
a. Separate VCN

- Create multiple Virtual Circuits with different DRG over FC physical connection (different router same POP or different routers different POP) and use
  - AS PATH prepends to make 1Gbps virtual circuit primary for dev traffic and 10Gbps Virtual Circuit Primary for Prod Traffic
Accessing OCI Public Services (Object Storage) over FC Public Peering

- Accessing Object Storage services on OCI is one of the common hybrid connectivity use cases
- 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
Intercloud Connectivity
Multi-Cloud Connectivity using FastConnect

Customer directly connected to both clouds.
- Private circuit to both clouds
- Customer responsible for routing.
- Reduced latency depending on where customer is located.
- Minimum incremental cost, minimum implementation time

Customer connected to partner who has connectivity to multiple cloud providers.
- Partners are coming up with virtual router(or equivalent) products (E.g MCR)
- Virtual router would keep latency to minimum
- Customer may have existing relationships which would lead to minimal implementation time.
- Enables seamless, direct access to multiple clouds.
Demo: Via Partner

- Partners who has multi-cloud connectivity.
- Minimal implementation time due to existing relationship.
- Minimized cost due existing relationship.
- Reduced troubleshooting time for operational issue.
- Enables seamless, direct access to multiple clouds.
AWS – OCI Connectivity via Megaport
Logical Connectivity – L3
AWS – OCI Connectivity via Megaport

- Setup VCN and associate a DRG with VCN
- Create a FC Virtual Circuit with Megaport Partner
- Setup a Megaport Cloud Router
- Create a VXC from MCR to OCI (use OCID and BGP info from OCI)
  - FastConnect VC provisioned with OCI
- Setup a VPC and associate a Virtual Private Gateway on AWS
- Create a VXC from MCR to AWS
  - Accept VIF on AWS
  - Propagate routes to VPC Route table
- AWS – OCI Connectivity Provisioned

Demo available on Confluence (Demo Section)
Summary

After completing this lesson, you should have learned:

• FastConnect Public and Private Peering
• FastConnect Redundancy Options
• Intercloud connectivity options
• Hybrid Architectures using FastConnect
ORACLE
Cloud Infrastructure

cloud.oracle.com/iaas
cloud.oracle.com/tryit