AWS Outposts Rack – Networking Reference Architecture
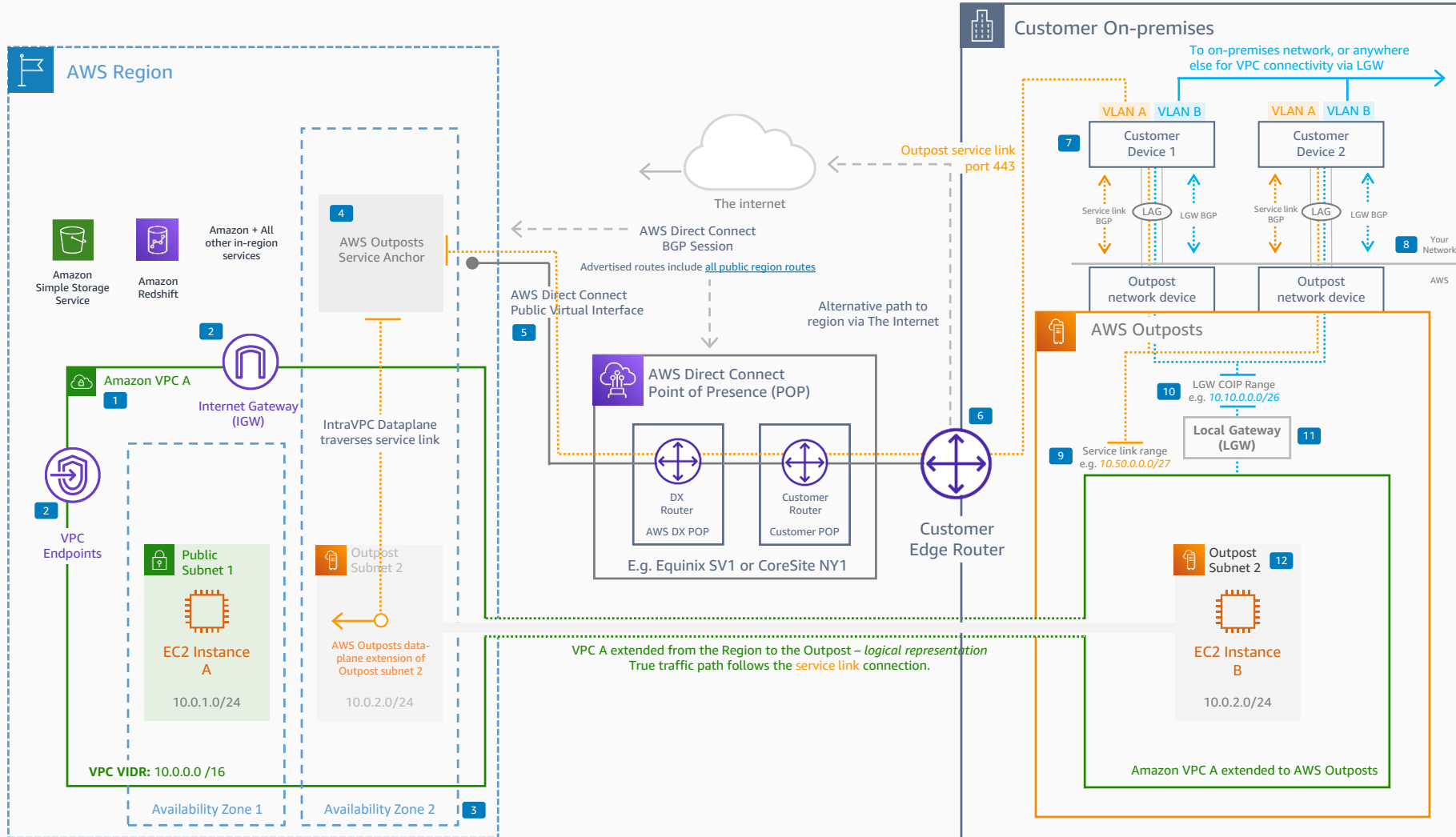
An architectural overview of AWS Outposts Rack connectivity for LAN, WAN, and Amazon VPC

1. Multiple AWS Virtual Private Cloud (VPC) can be associated with the same outpost.

2. Region level services can be connected to from the outpost via intra-VPC connectivity.

3. An outpost is homed to an availability zone.

4. **AWS Outposts** service link anchor is created within the availability zone of your choosing and fronted by public Amazon IPs. The Outpost will need connectivity back to these IPs to establish it's service-link connection for both control plane and data plane traffic.

5. An **AWS Direct Connect** public virtual interface (VIF) can be used to connect back to the AWS Outposts service anchor IPs. The direct connect public VIF will advertise all of the Amazon public ranges from Amazon to your router.

6. An edge router with either a **Direct Connect** connection back to the region or public internet can be used to reach the **Outposts** service anchor in the region. Network Address Translation (NAT) or Port Address Translation (PAT) can be used with this device for the service link. Service link establishment is initiated from the Outpost, never from the region.

7. Customer Devices need to support:
   Link aggregation - connections to the Outpost network devices will be added to a link aggregation group using LACP
   VLANs - Point to point virtual LANs (VLANs) are configured between each Outpost network device and your customer device. VLAN A is used for service link connectivity back to the AWS region, and VLAN B is used for Local Gateway (LGW) connectivity towards your on-premises network.
   Dynamic routing - Border Gateway Protocol (BGP) will be configured between each customer device and Outpost network device for each VLAN. 4 total BGP sessions are shown here between devices.

8. Demarcation between your network and the Outpost. The demarcation is the physical patch panel at the top of the rack. Fibers to the patch panel will be provided by you.

9. A Classless Inter-Domain Routing (CIDR) range is provided by you for the service link. This range is a /26 private or public IP range. The service link infrastructure range is used to address infrastructure in the outpost that needs connectivity back to the Outpost anchor in the AWS region.

10. A Classless Inter-Domain Routing (CIDR) range is provided by you for the LGW. This range, called the "Customer Owned IP" range (CoIP) range, is used by you to address instances inside the Outpost with Elastic IPs from this range that need connectivity to your on-premises workloads.

11. The Local Gateway, one per outpost, attached to one or multiple VPCs within the outpost. The LGW provides the NAT function between the Outpost VPC range and the appropriate Elastic IPs from the COIP range.

12. An Outpost subnet, created in an **Amazon VPC**, in an account that has an Outpost associated with it. Outpost subnets can also be shared with other accounts within the same organization.

AWS Reference Architecture