# “멀티 클라우드 네트워크 (MCN)”

## Day 1. MCN 개요와 라우팅

| 구분 | 주제 | 세부 내용 |
|---|---|---|
| 이론 | Day 1<br>MCN 개요와 라우팅 | • 멀티클라우드 개요<br>• 멀티클라우드를 위한 라우팅 (CSP, 오픈소스)<br>• 라우팅 동작<br>• 라우팅 테이블 |
| | Day 2<br>가상 네트워크 간의 연동 | • CSP의 가상네트워크 구성<br>• Peering (가상 네트워크 연동)<br>• Transit Gateway/Virtual WAN/VCN<br>• 멀티 클라우드상의 가상 네트워크 연동 |
| | Day 3<br>하이브리드와 멀티 클라우드 | • CSP/제조사 하이브리드 클라우드 솔루션<br>• VPN(Virtual Private Network)<br>• 전용선(Direct Connect / Express Route)<br>• Cloud Hub |
| 이론/실습 | Day 4<br>프라이빗 링크 | • CSP의 프라이빗 링크 구성<br>• 서비스 엔드포인트(Endpoint)<br>• 프라이빗 링크(Private Link)<br>• 멀티클라우드 라우팅 구성 (실습) |
| | Day 5<br>멀티 클라우드 네트워킹 | • 멀티클라우드 아키텍쳐 (CSP, 제조사)<br>• 멀티클라우드 인프라 연동<br>• 멀티클라우드 인프라 관리<br>• 멀티클라우드 관리 플랫폼 (실습) |



4

# DAY 1. MCN 개요와 라우팅



❖ **Multicloud; Multi-cloud; Multi Cloud**

- 2곳 이상의 클라우드 벤더가 제공하는 2개 이상의 퍼블릭 또는 프라이빗 클라우드로 구성된 클라우드 접근 방식
- 복수의 클라우드 들의 서로 다른 네트워크 상에서 인프라 및 응용 서비스들이 단일 네트워크로 운영 관리하는 기술이 필요 (예: 오버레이 네트워크로 통합 관리 가능한 네트워크를 제공)

Source: https://itwiki.kr/w/%EB%A9%80%ED%8B%B0%ED%81%B4%EB%9D%BC%EC%9A%B0%EB%93%9C

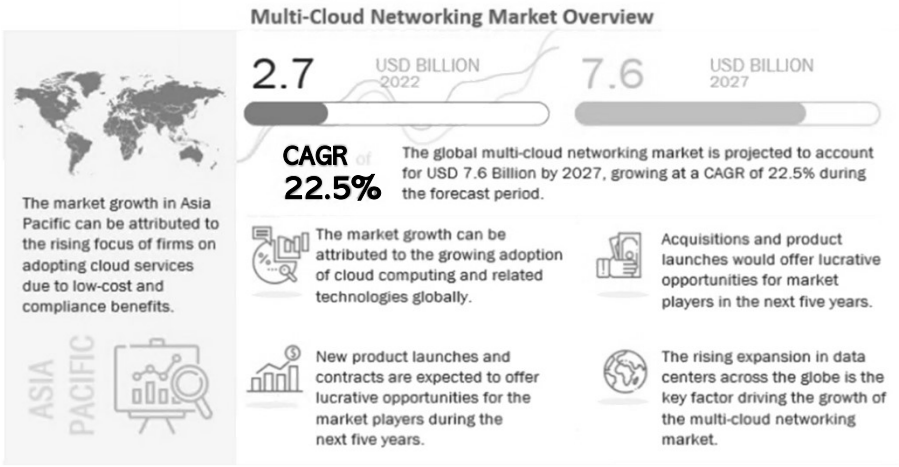


5

# DAY 1. MCN 개요와 라우팅



❖ **Multi-Cloud Networking 시장 전망: 연평균 22.5%** (Markets and Markets)




MARKETSANDMARKETS™

Source: 'https://www.marketsandmarkets.com/Market-Reports/multi-cloud-networking-market-80685691.html



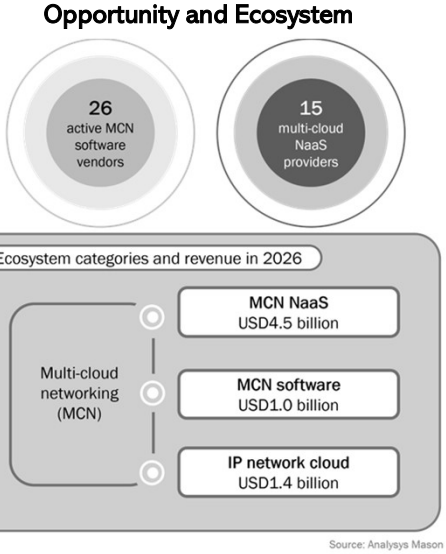
6

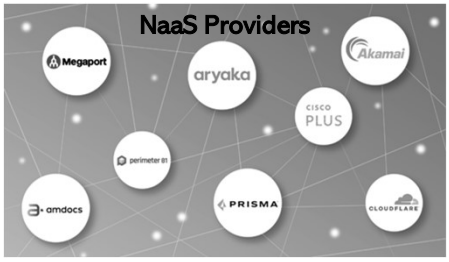
# DAY 1. MCN 개요와 라우팅



❖ **Multi-Cloud Networking: 생태계와 기회**

- MCN NaaS (15 multi-cloud NaaS providers)
- MCN Software (26 active MCN software vendors)
- IP network cloud




analysys mason

Source: https://www.analysysmason.com/research/content/reports/multi-cloud-networking-rma21/

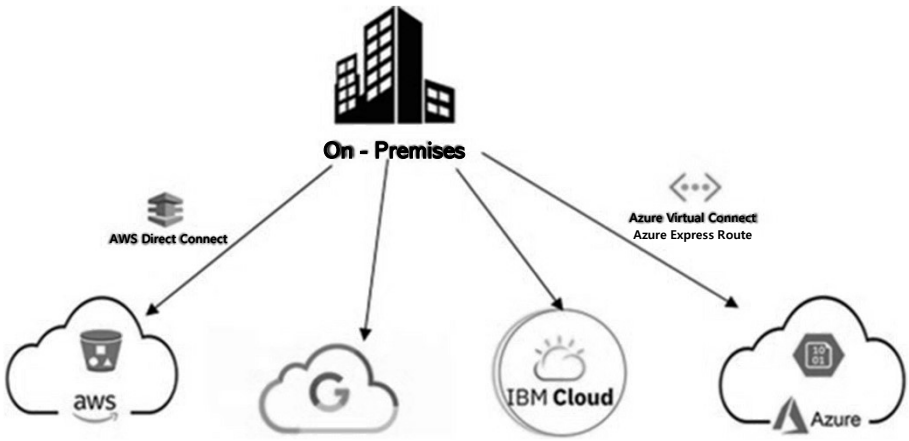


7

# DAY 1. MCN 개요와 라우팅



❖ 멀티클라우드 연결 - Multi-cloud interactions




Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)



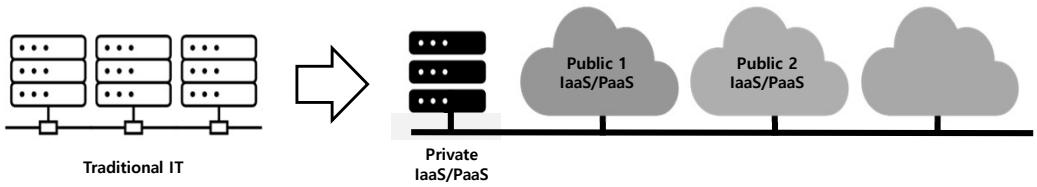
8

# DAY 1. MCN 개요와 라우팅



❖ **클라우드 운영 모델의 변화**

- **Run:** 전용 인프라 → 클라우드 상의 스케듈링
- **Connect:** 고정 IP 주소 → 서비스 기반 유동 IP
- **Secure:** IP 주소 기반 보안 정책 → Identity 기반
- **Provisioning:** 전용 서버 → 요청 기반 용량






9

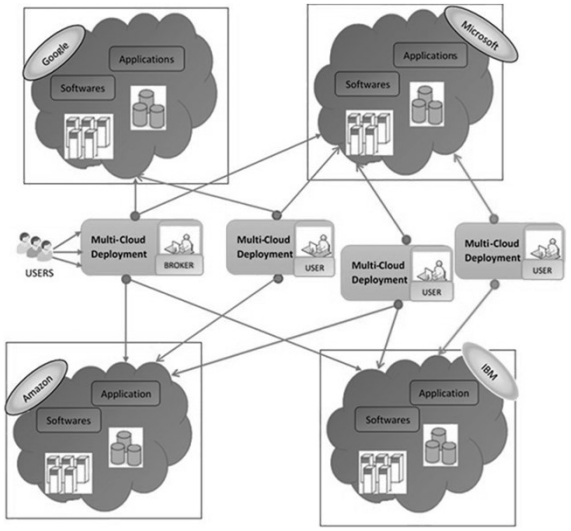
# DAY 1. MCN 개요와 라우팅



❖ 멀티클라우드 환경 - Multi-cloud environment

- Cloud Aggregators
- Cloud Integrators
- Cloud Customizers

**Cloud aggregators** are high-level consultants or architects who bring together multiple **cloud** services and offer them as a combined package to customers.




Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)





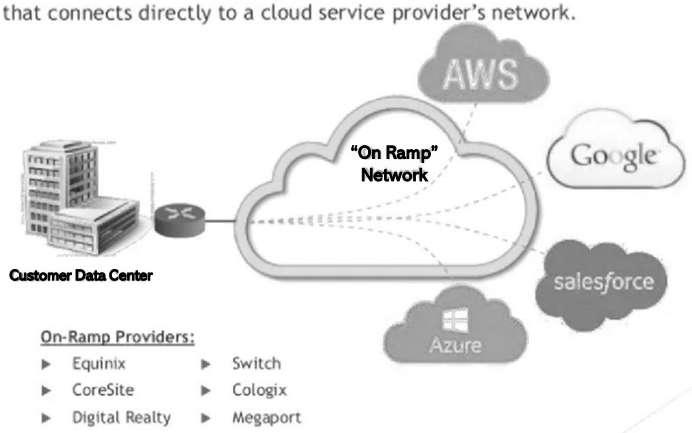
# DAY 1. MCN 개요와 라우팅



❖ 온램프 서비스 - Cloud "On-Ramp" Service Providers

- Equinix
- CoreSite
- Digital Realty
- Switch
- Cologix
- Megaport

▶ Cloud On Ramp Services provide a connection service within a data center that connects directly to a cloud service provider's network.




Source: Joseph Primicerio

# DAY 1. MCN 개요와 라우팅



❖ 제조사의 멀티클라우드 (예): Multi-Cloud Network (Cisco Cloud Network Controller)

- **Intra-cloud connectivity:** Extend segments across regions, Automate route propagation across virtual networks, Automate L4-L7 service insertion
- **Inter-cloud connectivity:** Automate route propagation across clouds, Extend routing domains and segments across Clouds, Automate L4-L7 service insertion
- **Hybrid cloud connectivity:** Automate Overlay connectivity for different types of Underlays, Extend routing domains and segments between On Premises and Cloud sites, Enable consistent networking and visibility between On Premises and Cloud
- **External network connectivity:** Standards-based IP connectivity to any network, Secure connectivity to external network spanning datacenters and branches.
- **L4-L7 service insertion:** Automate firewall and load balancer insertion, Automatically update routing and security policy to insert L4-L7 services, Integrate with third-party L4-L7 services and cloud native L4-L7 services
- **Brownfield VPC onboarding:** Safe and fast migration and rollback, Ability to use Cloud Network Controller with brownfield environments

Source: https://blogs.cisco.com/datacenter/modernize-your-multi-cloud-network-with-cisco-cloud-network-controller



12

# DAY 1. MCN 개요와 라우팅



❖ 제조사의 멀티클라우드 (예): F5의 Distributed Cloud Mesh vs. Other Multi-Cloud Solutions

| Features | Other solutions | Distributed Cloud Mesh |
|---|---|---|
| **Consolidated L3-L7 networking + security service** | x | v |
| **Multi-tenancy + self-service for NetOps and DevOps** | x | v |
| **Multi-layer security** | x | v |
| **App-to-app connections without exposing the underlying network** | x | v |
| **Global physical network** | x | v |
| **Automation assistance for NetOps** | v | v |
| **Security service insertion** | v | v |
| **Observability and analytics** | External | v |
| **Lifecycle management** | Controller | **SaaS** |

Source: https://www.f5.com/cloud/use-cases/multi-cloud-networking



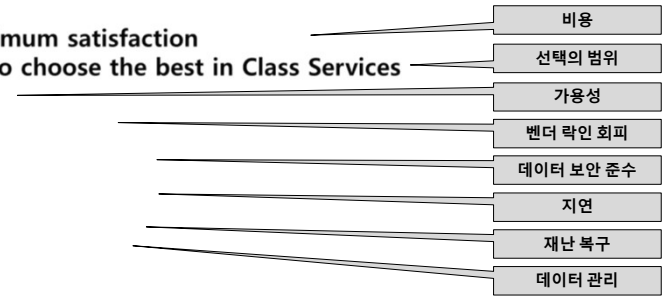
13

# DAY 1. MCN 개요와 라우팅



❖ 멀티클라우드 장점 - Benefts of Multi-Cloud

- Cost-effective service with optimum satisfaction
- One out of many alternatives to choose the best in Class Services
- Availability
- Avoiding Vendor Lock-in
- Data Privacy and Compliance
- Proximity/Low Latency
- Disaster Recovery
- Data Management




Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)



14

# DAY 1. MCN 개요와 라우팅



❖ Multi-Cloud 환경 이동 이유

**벤더 락인 우려 최고 솔루션 선택**

"Most organizations adopt a multicloud strategy out of a desire to avoid vendor lock-in or to take advantage of best-of-breed solutions" - Gartner analyst

**유연한 커스터마이징**

**Flexible Customization**
Each Cloud Service Provider has special Features

**위험 완화**

**Risk Mitigation**
Deploying critical systems across multiple Cloud services provides additional fault tolerance

**데이터 유실과 다운타임 최소화**

Minimize the threat of extensive data loss or downtime due to component failure in cloud.



15

# DAY 1. MCN 개요와 라우팅



❖ 멀티클라우드 환경의 도전

• Challenges in multi-cloud environment


Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)



16

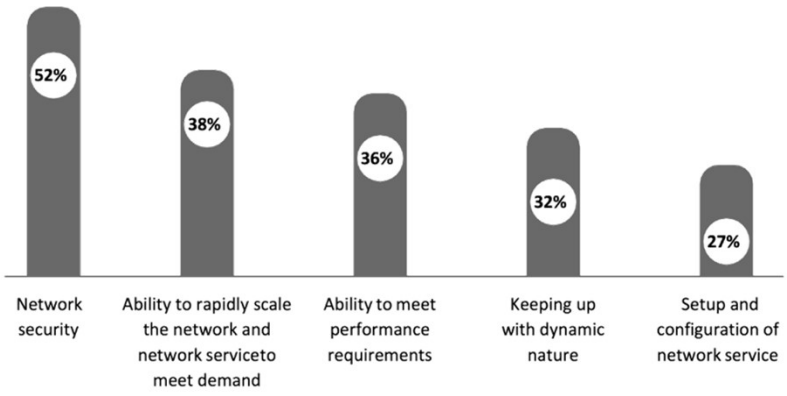
# DAY 1. MCN 개요와 라우팅



❖ 멀티클라우드 네트워킹의 도전 - Challenges of Multi-cloud networking

• Top five network challenges in modern multi-cloud environments

✓네트워크 보안
✓네트워크의 신속한 스케일 요구
✓성능 요구
✓클라우드 특징 다이나믹 지원
✓네트워크 서비스 구성




Source: https://www.wipro.com/infrastructure/the-strategy-to-build-secure-multi-cloud-networking/



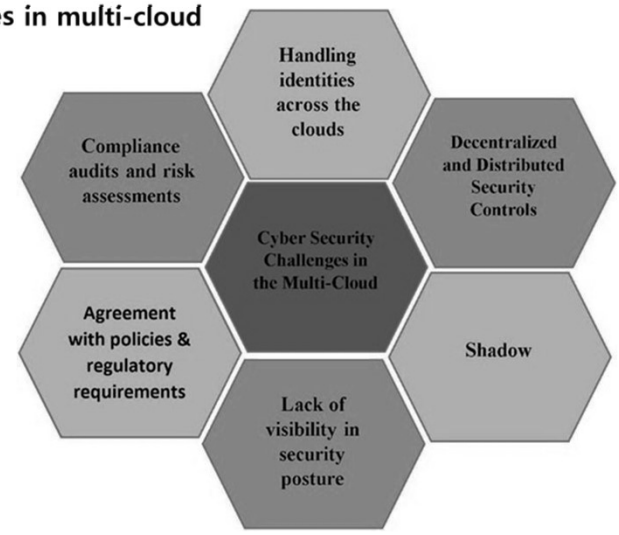
17

# DAY 1. MCN 개요와 라우팅



❖ 사이버보안 도전 - Cyber security challenges in multi-cloud

- 준수.. (Compliance..)
- 정책.. (Policy..)
- 가시화.. (Visibility..)
- 음영 (Shadow)
- 탈중앙 제어.. (Decentralized..)
- 클라우드간 ID.. (Identity..)




Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)



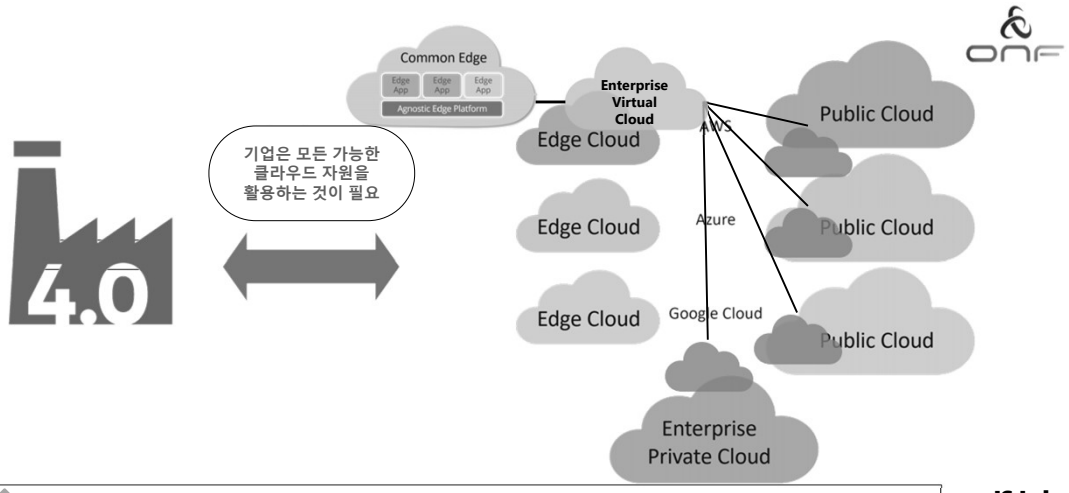


# DAY 1. MCN 개요와 라우팅



❖ 멀티클라우드는 기업의 뉴노멀 (ONF: Enterprise Multi-Cloud is the New Normal)

- Can't afford to be tied to just a single hyperscaler – 하나의 'Virtual Cloud' 필요

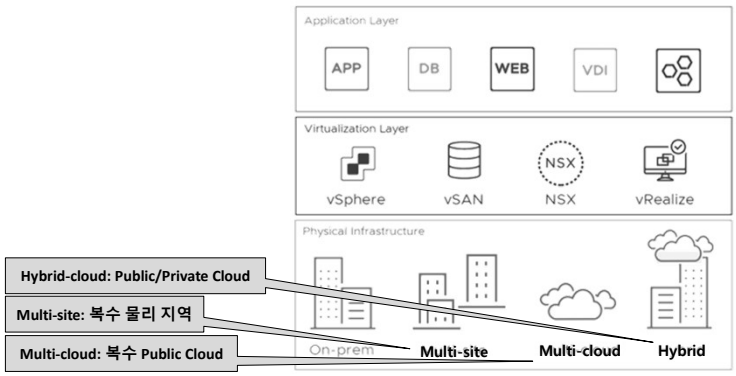


# DAY 1. MCN 개요와 라우팅



❖ 제조사의 멀티클라우드 (예): VMware

- VMware의 Multi-cloud
- NSX over Any Fabric Underlay, Site, Cloud




NSX Features and Values

- Hybrid Cloud Automation
- Service-defined Firewall
- Purpose built software
- Inherent extensible services: LB, DDI, NAT, VPN
- 3rd party service chaining
- Physical switching fabric choice
- Improves simplicity, resilience, stability
- Cloud ready, hardware independent SDN
- Easier to troubleshoot, problem scope minimized

Source: DEPLOYING VMWARE NSX WITH CISCO ACI UNDERLAY DESIGN GUIDE (VERSION: 2021)



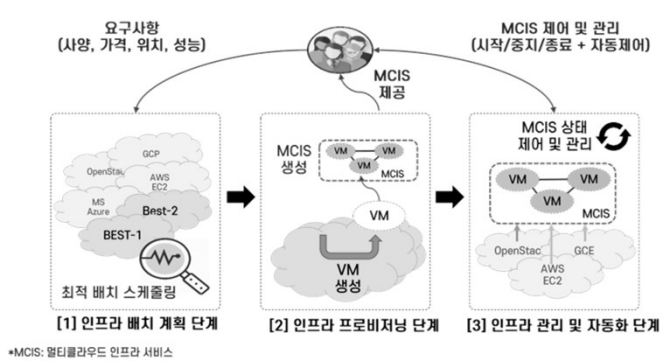
20

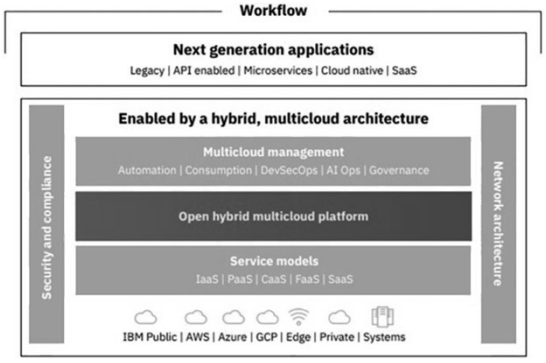
# DAY 1. MCN 개요와 라우팅



❖ MCIS: 멀티클라우드 인프라 서비스

❖ Dynamic workflow orchestration in hybrid multi-cloud




Source: @ ETRI Conference 2022 '멀티클라우드 인프라 통합 관리 기술' (손석호) 참조
Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)



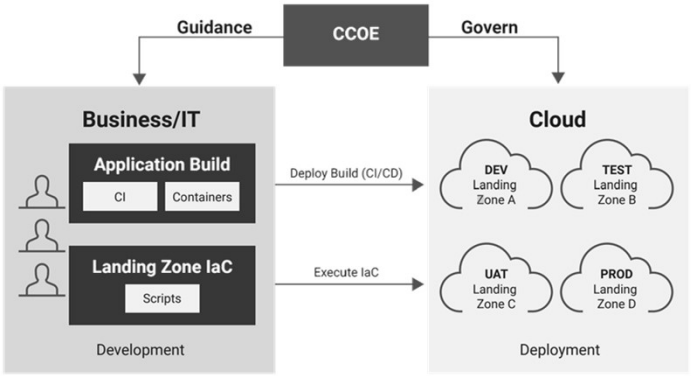
21

# DAY 1. MCN 개요와 라우팅



❖ 클라우드 적용을 위한 애자일 접근 - Agile approach for cloud deployments

- **A CCOE** (Centralized cloud center of excellence) **is a centralized governance function for the organization and acts in a consultative role for central IT, business-unit IT and cloud service consumers in the business. A CCOE is key to driving cloud-enabled IT transformation.**




Source: Infrastructure Architecture Essentials for Data Center and Cloud, Shankar Kambhampaty

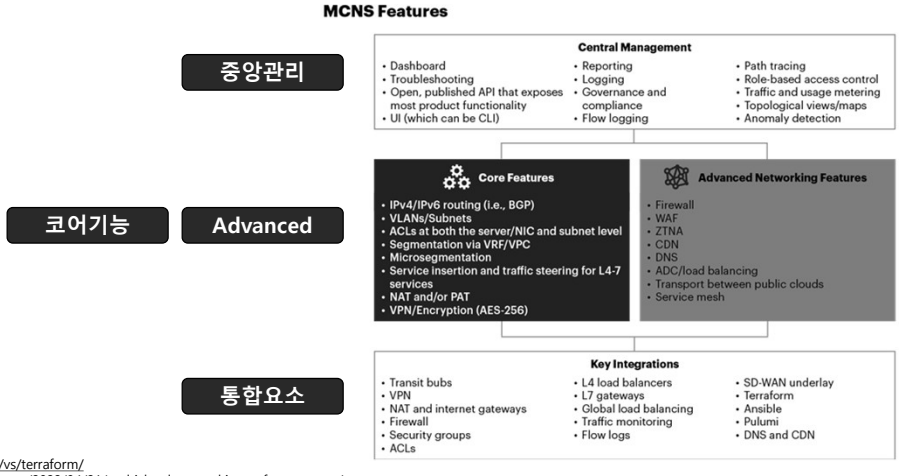


22

# DAY 1. MCN 개요와 라우팅



❖ 가트너(예): Multicloud Networking Software (MCNS)




Source: https://www.pulumi.com/docs/intro/vs/terraform/
Source: https://blogs.gartner.com/andrew-lerner/2022/04/21/multicloud-networking-software-mcns/



23

# DAY 1. MCN 개요와 라우팅



❖ MCNS (Multicloud Networking Software) 제조사

| 제조사 | 제품/서비스 또는 플랫폼 |
|---|---|
| Alkira | Cloud Networking |
| Arrcus | Arrcus Multi-Cloud Networking (MCN) |
| Arista Networks | Any Cloud Platform |
| Aviatrix | Aviatrix Cloud Network Platform |
| Cohesive Networks | VNS3 |
| Cisco | Cisco Cloud Services Router 1000V (CSR1kv), Cisco Catalyst 8000V Edge Software, Cisco Cloud APIC |
| F5 | F5 Distributed Cloud Platform |
| Prosimo | AXI Platform |
| VMware | NSX Cloud |

Source: https://www.gartner.com/doc/reprints?id=1-29S4R0C1&ct=220419&st=sb



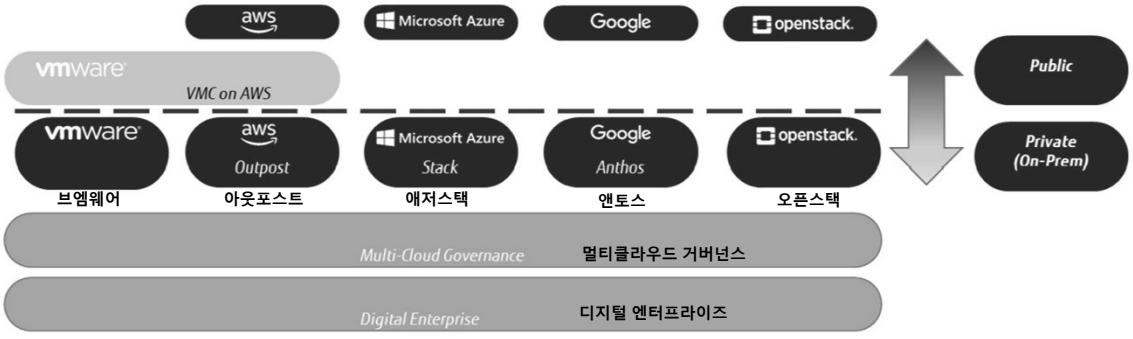


# DAY 1. MCN 개요와 라우팅



❖ 주요 멀티클라우드 플레이어 (Main players in the field)

- Public: AWS, Azure, Google, OpenStack, (VMware)
- Private(On-Prem): VMware, Outpost(AWS), Azure Stack, Anthos(Google), OpenStack

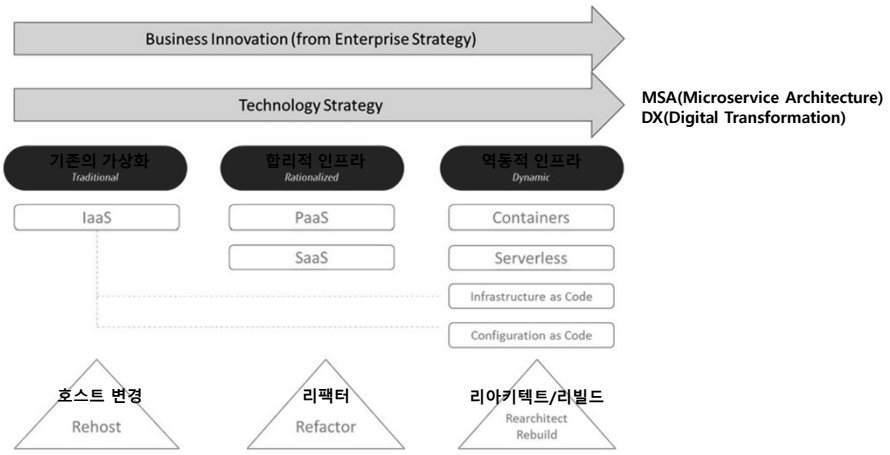



Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 48). Packt Publishing. Kindle Edition.

# DAY 1. MCN 개요와 라우팅



❖ Technology strategy following business innovation




Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 83). Packt Publishing. Kindle Edition.

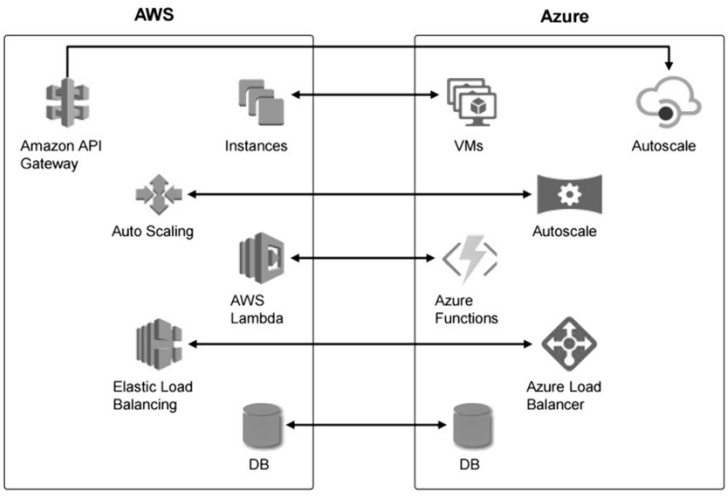




# DAY 1. MCN 개요와 라우팅



❖ 동일 서비스 고려하는 Multi-Cloud Architecture



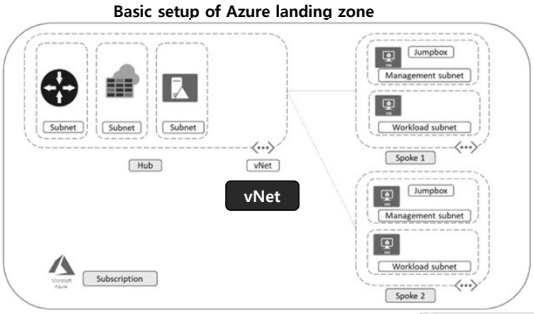
# DAY 1. MCN 개요와 라우팅



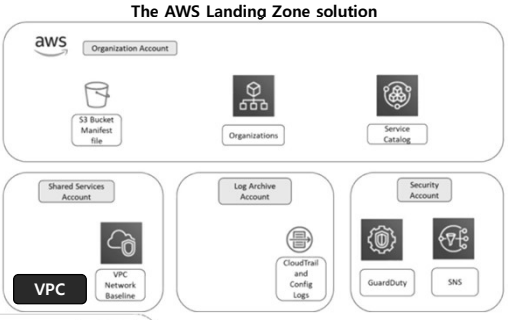
❖ Creating a multi-cloud landing zone and blueprint

• landing zone: 구현을 위한 클라우드 서비스 세트

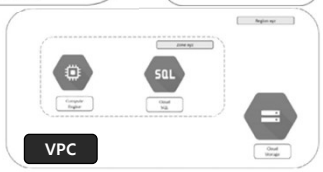
Basic setup of Azure landing zone




The AWS Landing Zone solution




Basic setup of a project in GCP, using Compute Engine and Cloud SQL






28

# DAY 1. MCN 개요와 라우팅



❖ Cloud Computing AWS, GCP, Azure

| PRODUCT | aws | Microsoft Azure | Google Cloud Platform |
|---|---|---|---|
| Virtual Servers | Instances | VMs | VM Instances |
| Platform-as-a-Service | Elastic Beanstalk | Cloud Services | App Engine |
| Serverless Computing | Lambda | Azure Functions | Cloud Functions |
| Docker Management | ECS | Container Service | Container Engine |
| Kubernetes Management | EKS | Kubernetes Service | Kubernetes Engine |
| Object Storage | S3 | Block Blob | Cloud Storage |
| Archive Storage | Glacier | Archive Storage | Coldline |
| File Storage | EFS | Azure Files | ZFS / Avere |
| Global Content Delivery | CloudFront | Delivery Network | Cloud CDN |
| Managed Data Warehouse | Redshift | SQL Warehouse | Big Query |

Source: https://medium.com/@muhammad.saad_16819/cloud-computing-aws-gcp-azure-and-digitalocean-408b7c450cea

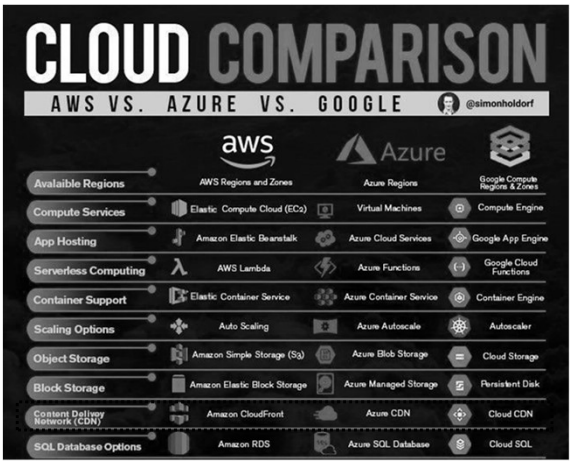


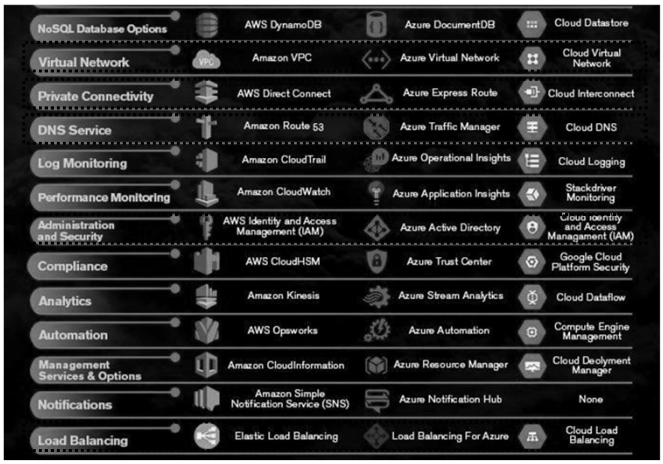
29

# DAY 1. MCN 개요와 라우팅



❖ 주요 클라우드 서비스 비교 (예): AWS vs. Azure vs. Google




Source: https://www.mltut.com/best-data-engineering-courses-online/?fbclid=IwAR3aKZl-e4YzUitFBny3HsZX5GoWdi31u8qxDfKl14bTBoX508VZcF8kgBM



30

# DAY 1. MCN 개요와 라우팅



❖ CSP의 주요 네트워크 서비스 (예): Key network services for AWS, Azure, and GCP

| Cloud Platform | Amazon Web Services (AWS) | Microsoft Azure | Google Cloud Platform (GCP) |
|---|---|---|---|
| **Virtual Network** | Amazon Virtual Private Cloud (VPC) | Virtual Networks (VNets) | Virtual Private Cloud |
| **Data Center integration** | Direct Connect | ExpressRoute | Google Cloud Interconnect |
| **Load Balancer** | Elastic Load Balancer | Load Balancer | Google Cloud Load Balancing |
| **DNS** | Amazon Route 53 | Azure DNS | Google Cloud DNS |
| **Firewall** | AWS Firewall / Web Application Firewall | Azure Firewall | Google Cloud firewalls |

Source: Infrastructure Architecture Essentials for Data Center and Cloud, Shankar Kambhampaty

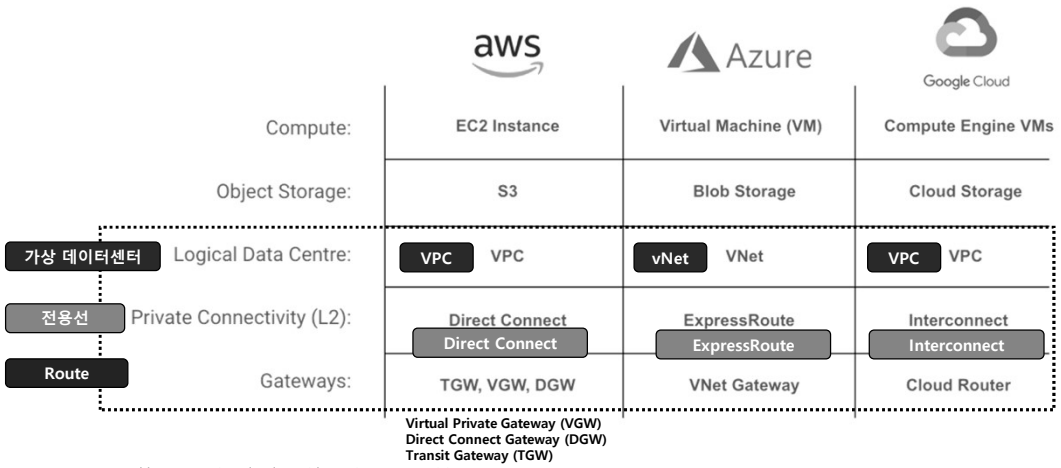


31

# DAY 1. MCN 개요와 라우팅



❖ CSP 네트워크 용어 (terminology alignment)




Source: https://www.megaport.com/blog/comparing-cloud-providers-private-connectivity/

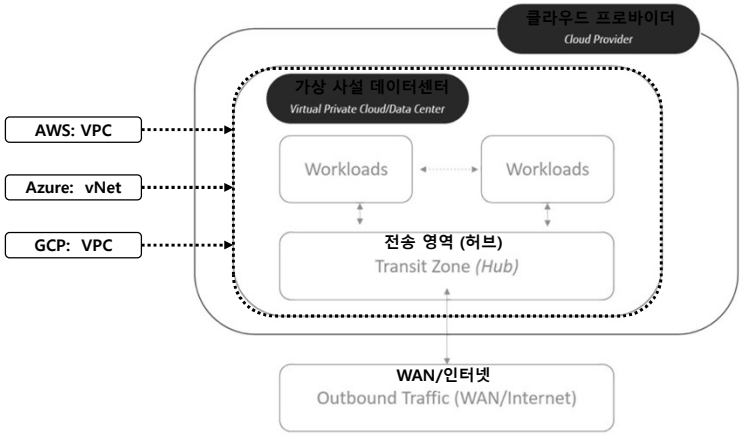


32

# DAY 1. MCN 개요와 라우팅



❖ High-level diagram of a virtual private cloud/data center




Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 74). Packt Publishing. Kindle Edition.



33

# DAY 1. MCN 개요와 라우팅



❖ Networking services compared: AWS vs Azure vs Google Cloud

• 가상 사설 데이터센터, BGP, VPN, 전용선, 방화벽

| SERVICE NAME | aws | Azure | |
|---|---|---|---|
| | Virtual Private Cloud (VPC) | VNet | Virtual Private Cloud (VPC) |
| | Border Gateway Protocol BGP (BGP) | Border Gateway Protocol BGP (BGP) | Border Gateway Protocol BGP (BGP) |
| | AWS Transit Gateway<br>AWS Direct Connect<br>AWS Site-to-Site VPN | VPN Gateway<br>ExpressRoute Gateway<br>Azure Firewall | Shared VPC<br>Cloud VPN<br>Cloud Interconnect |

Source: https://acloudguru.com/blog/engineering/networking-services-compared-aws-vs-azure-vs-google-cloud



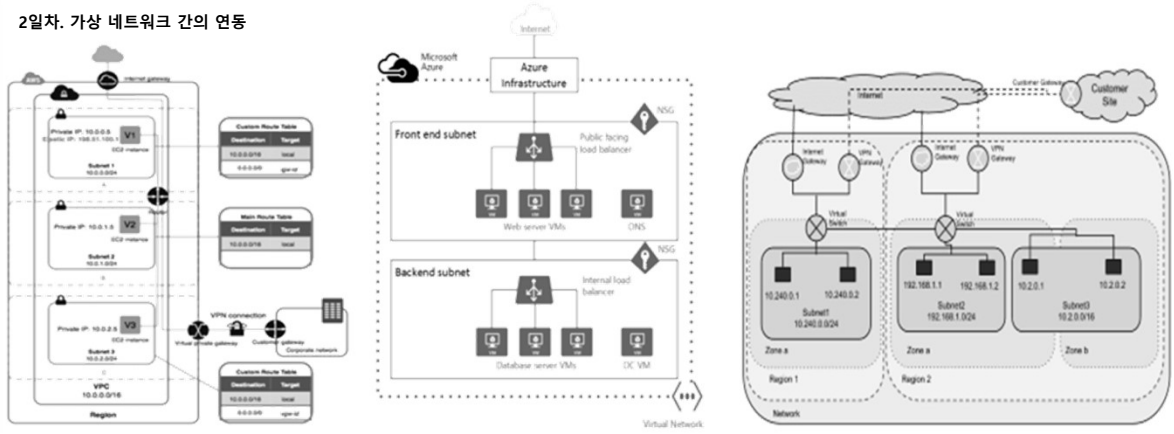


# DAY 1. MCN 개요와 라우팅



❖ 가상네트워크: AWS VPC, Azure VNET, GCP VPC

2일차. 가상 네트워크 간의 연동




Source: https://aviatrix.com/learn-center/answered-multi-cloud/how-to-do-multicloud-networking-abstraction-and-orchestration-across-aws-azure-and-google/

# DAY 1. MCN 개요와 라우팅



❖ IaaS Networking Services across AWS, Azure, GCP

| Network Services/Function | AWS | Azure | Google |
|---|---|---|---|
| **Network Administration** | Account | Subscription | Project |
| **Virtual Network** | VPC & Subnets | VNET & Subnet | VPC and Sub-Network |
| **DNS** | Route 53 | Traffic Manager | Cloud DNS |
| **VPN** | VGW | VPN Gateway | VPN Gateway |
| **Peering** | AWS Peering or DirectConnect | Azure Peering or ExpressRoute | Google Cloud Interconnect |
| **Load Balancer** | ELB | NLB | Cloud Load Balancer |
| **Security** | Sec Groups | Network Security Groups | Network ACLs |
| **Storage** | S3 | Blob Storage | Cloud Storage |
| **Notifications** | SNS | Notification hubs | Cloud Messaging |
| **Messaging** | SQS | Batch | Pub/Stub |
| **Logging** | CloudTrail | Operational Insights | Cloud Logging |
| **Monitoring** | CloudWatch | Application Insights | Cloud Monitoring |

5일차. 멀티클라우드 네트워킹
2일차. 가상 네트워크 간의 연동
3일차. 하이브리드와 멀티 클라우드
2일차. 가상 네트워크 간의 연동
4일차. 프라이빗 링크

Source: https://aviatrix.com/learn-center/answered-multi-cloud/how-to-do-multicloud-networking-abstraction-and-orchestration-across-aws-azure-and-google/



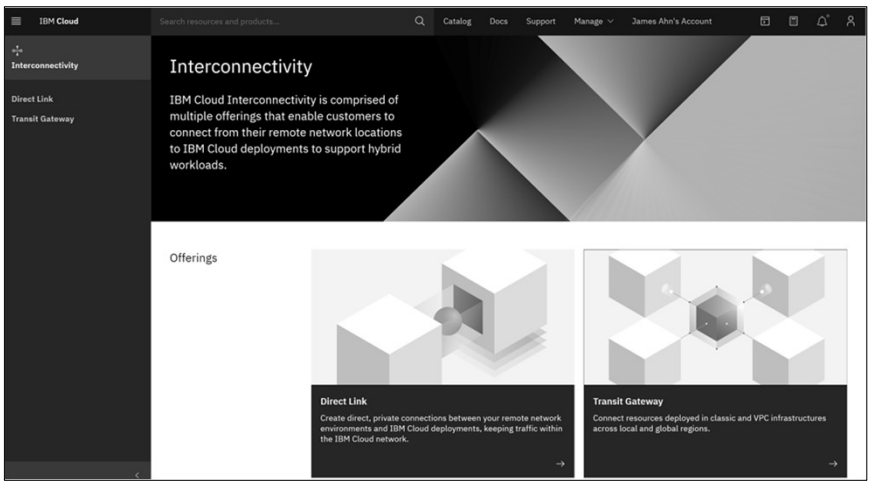


# DAY 1. MCN 개요와 라우팅



❖ CSP 포털 (예): IBM Cloud – Interconnectivity

- Direct Link
- Transit Gateway



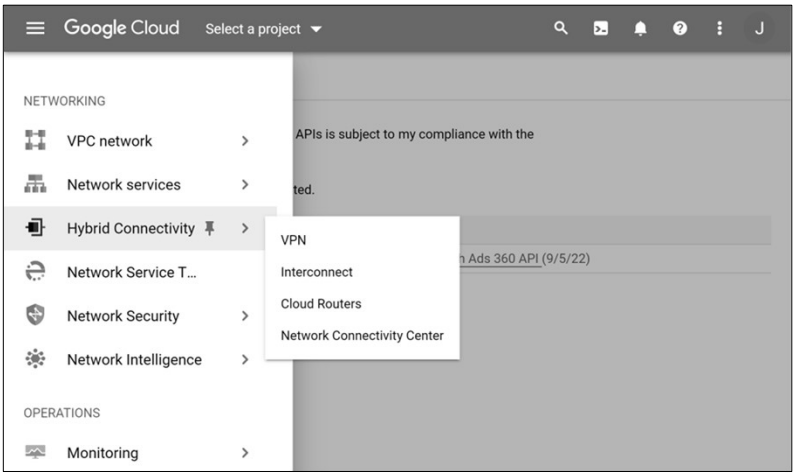

Source: https://cloud.ibm.com/catalog?category=network

# DAY 1. MCN 개요와 라우팅



❖ CSP 포털 (예): Google Cloud Networking – Hybrid Connectivity

- VPN
- Interconnect
- Cloud Routers
- Network Connectivity Center




Source: https://console.cloud.google.com/terms;updated=true?project=robust-fin-204013

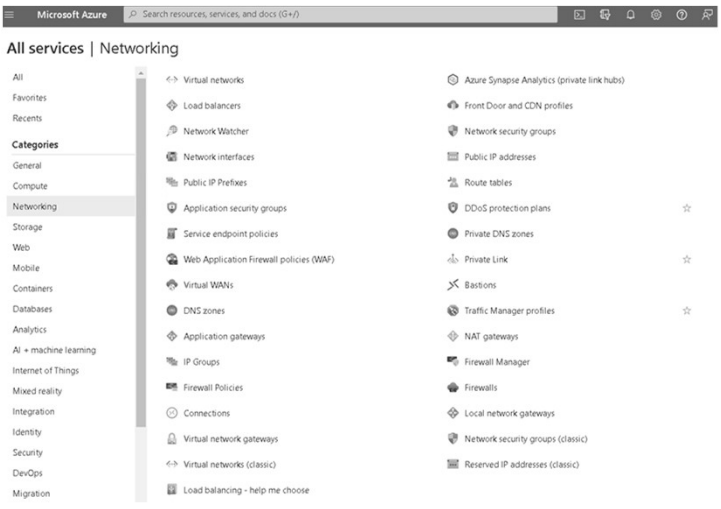




# DAY 1. MCN 개요와 라우팅



❖ CSP 포털 (예): Azure Networking



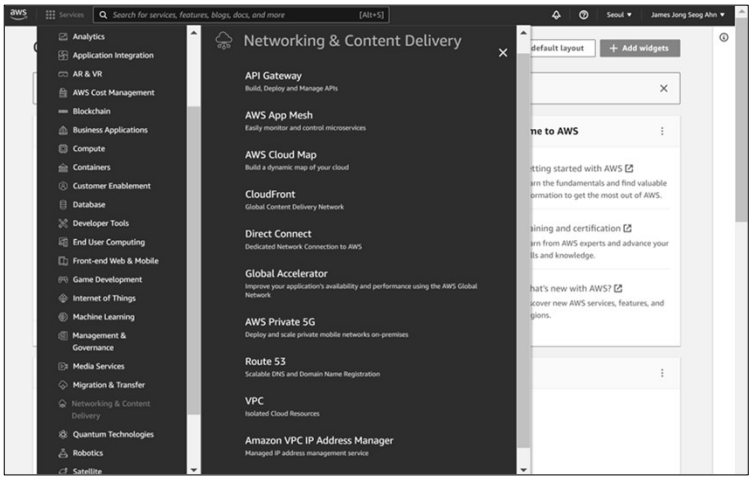

Source: https://portal.azure.com/#allservices/category/Networking

# DAY 1. MCN 개요와 라우팅



❖ CSP 포털 (예): Amazon AWS – Networking & Contents Delivery

- API Gateway
- AWS App Mesh
- AWS Cloud Map
- CloudFront
- Direct Connect
- Global Accelerator
- AWS Private 5G
- Route 53
- VPC
- Amazon VPC IP Address Manager




Source: https://ap-northeast-2.console.aws.amazon.com/console/home?region=ap-northeast-2#



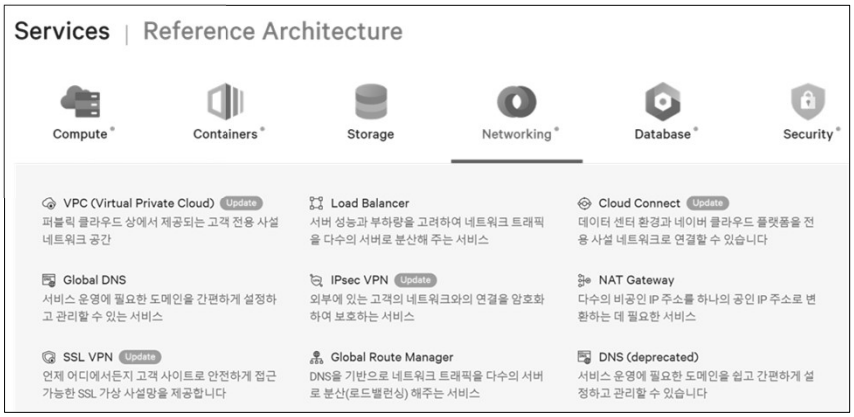


# DAY 1. MCN 개요와 라우팅



❖ CSP 포털 (예): Naver Cloud – Networking

- VPC
- Global DNS
- SSL VPN
- Load Balancer
- IPsec VPN
- Global Route Manager
- Cloud Connect
- NAT Gateway
- DNS

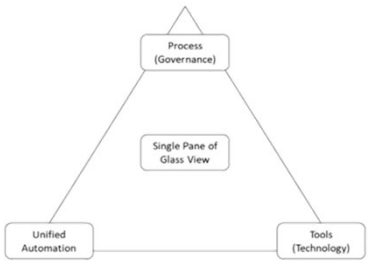


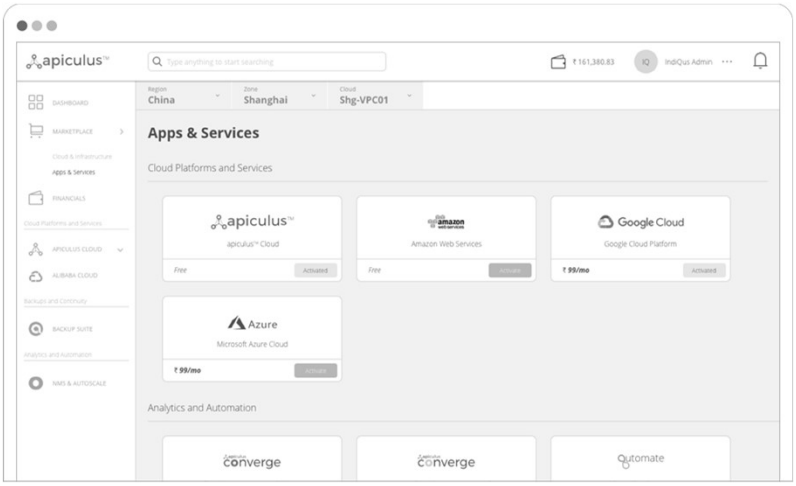

Source: https://www.ncloud.com/

# DAY 1. MCN 개요와 라우팅



❖ 멀티클라우드를 위한 Single pane of glass (제조사 예)




Source: https://www.apiculus.io/multicloud/



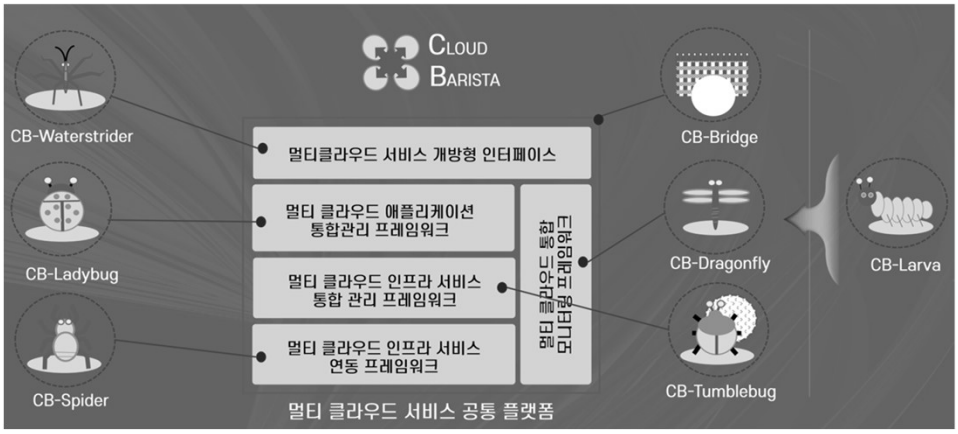


# DAY 1. MCN 개요와 라우팅



❖ 멀티클라우드 기술 (오픈소스 예): 클라우드바리스타 (ETRI)

- CB-Waterstrider
- CB-Ladybug
- CB-Spider
- CB-Bridge
- CB-Dragonfly
- CB-Tubblebug
- CB-Larva

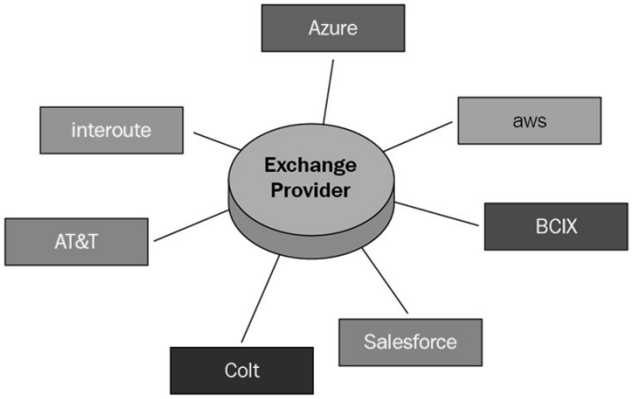



Source: @ ETRI Conference 2022 '멀티클라우드가 만들어가는 세상' (정영우) 참조

# DAY 1. MCN 개요와 라우팅



❖ Exchange providers




Source: Multi-Cloud for Architects (Published by Packt Publishing Ltd) Florian Klaffenbach, Markus Klein, Suresh Sundaresan





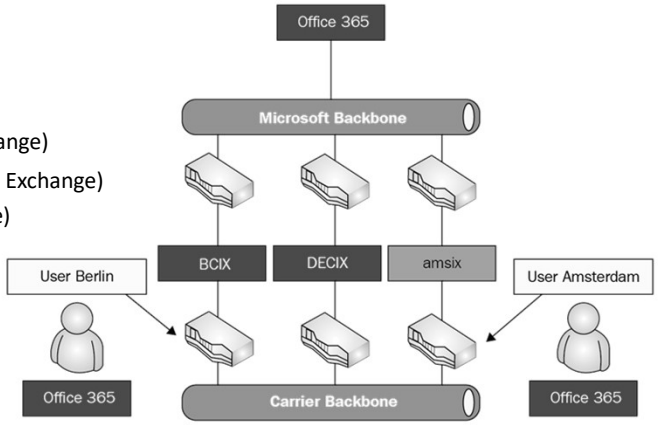
# DAY 1. MCN 개요와 라우팅



❖ Decentralized and centralized routing

• Decentralized routing

**BCIX** (Berlin Commercial Internet Exchange)
**DE-CIX** (Deutsche Commercial Internet Exchange)
**AMS-IX** (Amsterdam Internet Exchange)



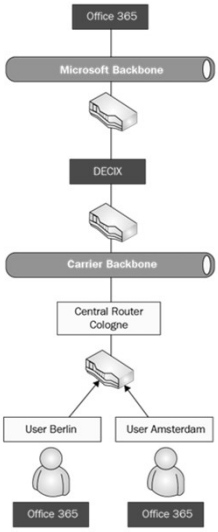

Source: Multi-Cloud for Architects (Published by Packt Publishing Ltd) Florian Klaffenbach, Markus Klein, Suresh Sundaresan

# DAY 1. MCN 개요와 라우팅



❖ Decentralized and centralized routing

• Centralized routing




Source: Multi-Cloud for Architects (Published by Packt Publishing Ltd) Florian Klaffenbach, Markus Klein, Suresh Sundaresan





# DAY 1. MCN 개요와 라우팅



❖ Networking services compared: AWS vs Azure vs Google Cloud

• Load Balancing

| aws | | Azure | | | |
|---|---|---|---|---|---|
| NETWORK LOAD BALANCER | LAYER 4 TCP/SSL | AZURE LOAD BALANCER | LAYER 4 TCP/UDP | INTERNAL | REGIONAL PASS-THROUGH TCP or UDP PROXY HTTP(S) |
| APPLICATION LOAD BALANCER | APPLICATION LAYER | AZURE APPLICATION GATEWAY | APPLICATION LAYER | | |
| ROUTE 53 | DNS | TRAFFIC MANAGER | DNS | EXTERNAL | REGIONAL OR GLOBAL PASS-THROUGH TCP or UDP PROXY TCP, SSL or HTTP(S) |
| | | FRONT DOOR | GLOBAL LOAD BALANCING | | |

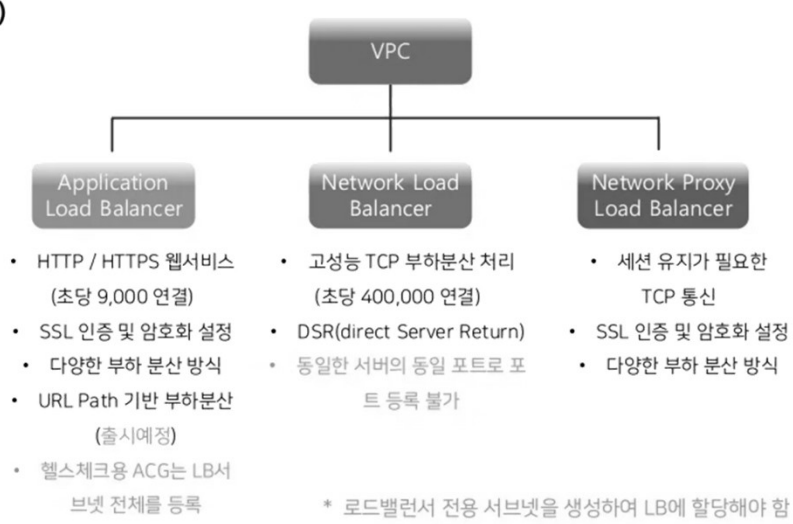
Source: https://acloudguru.com/blog/engineering/networking-services-compared-aws-vs-azure-vs-google-cloud

# DAY 1. MCN 개요와 라우팅



❖ 네이버클라우드플랫폼 (2020)

• 로드밸런서




Source: https://www.slideshare.net/n_cloudplatform/ss-239153998



48

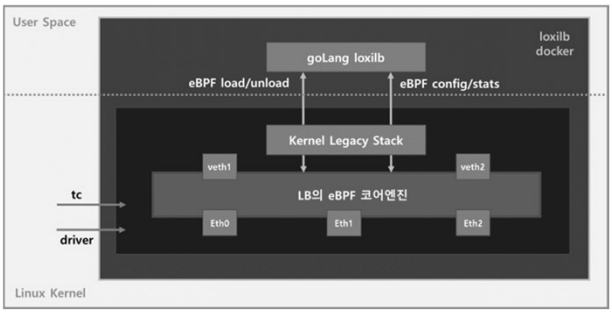
# DAY 1. MCN 개요와 라우팅

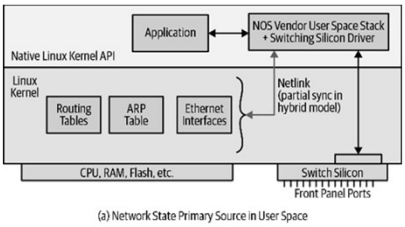


❖ How a user-space switching-silicon driver gets information

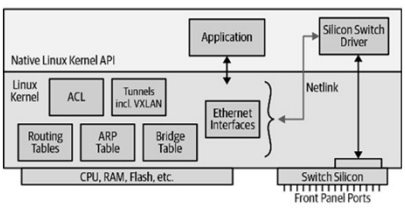
• **Kernel-space 생성 정보 수집 필요**
• **eBPF(Kernel-space sandbox app):** Cilium, LoxiLB, EKS Anywhere

**LoxiLB**




(a) Network State Primary Source in User Space




(b) Network State Primary Source in Kernel

Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY

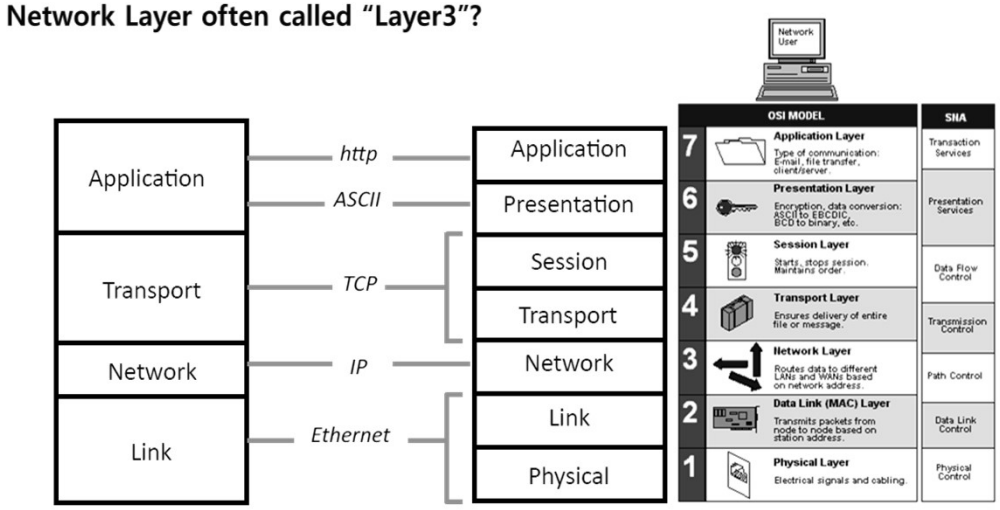


49

# DAY 1. MCN 개요와 라우팅



❖ **Why is the Network Layer often called "Layer3"?**




The 4-layer Internet model  The 7-layer OSI Model





# DAY 1. MCN 개요와 라우팅



❖ **IPv4 Classes**

- **Special addresses**
  IP Loopback Address 127.0.0.1
  Zero Addresses 0.0.0.0 through 0.255.255.255
  Private Addresses: 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16
- **Class A addresses begin with 0xxx, or 1 to 126 decimal.**
  Example 120.10.100.45 255.0.0.0
  120.10.100.45/8
- **Class B addresses begin with 10xx, or 128 to 191 decimal.**
  Example 172.102.16.241 255.255.0.0
  172.102.16.241/16
- **Class C addresses begin with 110x, or 192 to 223 decimal.**
  Example 198.178.102.2 255.255.255.0
  198.178.102.2/24
- **Class D addresses begin with 1110, or 224 to 239 decimal.**
- **Class E addresses begin with 1111, or 240 to 254 decimal**

✓ **Classes D and E are reserved and are not used for general IP address allocation**

# DAY 1. MCN 개요와 라우팅



❖ **Problems with the partitioning of IPv4 Address space**

- **Problems with the partitioning of IPv4 Address space**
- **Problem 1: Lack of support for mid-sized organizations**
  - ✓ Class B addresses support 64k host per network, too large
  - ✓ Class C addresses support 256 hosts per network, too small
- **Problem 2: Route table size getting too large**
  - ✓ Roughly 2 million plus networks for all class C address
- **Solution:**
  - ✓ Variable Length Subnet Masking (VLSM)
  - ✓ Classless Inter-Domain Routing (CIDR)



52

# DAY 1. MCN 개요와 라우팅



❖ **IPv6 Addressing Notation**

- **16 bytes (128 bits) long**
- **Full notation** depicts pairs of IPv6 bytes are separated by a colon and each byte in turn, is represented as a pair of hexadecimal numbers: E3D7:0000:0000:0000:51F4:9BC8:C0A8:6420
- **Shorthand notation** removes bytes with a zero value from the text representation (though the bytes are still present in the actual network address) as follows: E3D7::51F4:9BC8:C0A8:6420
- **Mixed notation** is used when IPv6 addresses are extensions of IPv4 addresses - the rightmost four bytes of an IPv6 address (the rightmost two byte pairs) may be rewritten in the IPv4 notation as follows: E3D7::51F4:9BC8:192.168.100.32
- This larger size means that IPv6 supports more than 300,000,000,000,000,000,000,000,000,000,000,000,000 possible addresses



53

# DAY 1. MCN 개요와 라우팅



❖ **Enterprise Routing – Basic Routing**

- **Routers use routing protocols to maintain their routing tables. Routing tables can be maintained either statically or dynamically.**
- **Static Routes**
  - ✓ Static routes are manually configured and entered into a switch's routing table. Static routes take default precedence over routes chosen by dynamic routing protocols.
- **Dynamic Routes**
  - ✓ Dynamic routes are learned when routers send routing table information to each other.
  - ✓ The three forms of dynamic routing that are most commonly used are Distance Vector, Link State and Path vector protocols.
  - ✓ Distance Vector Protocols
    - ✓ RIPv1 and RIPv2
    - ✓ DVMRP
  - ✓ Link State Protocols
    - ✓ OSPFv2
    - ✓ IS-IS
  - ✓ Path Vector Protocols
    - ✓ BGP4



54

# DAY 1. MCN 개요와 라우팅



❖ **Open Shortest Path First**

- **Open Shortest Path First (OSPF) is an IP-based routing protocol for networks using a Link State Routing (LSR) algorithm. OSPF falls into the category of Interior Gateway Protocols (IGPs).**
- **Simply put, OSPF establishes a routing path based on the shortest path between the source and destination. By using this method, OSPF establishes a route with as little network latency as possible.**

Source: Multi-Cloud for Architects (Published by Packt Publishing Ltd) Florian Klaffenbach, Markus Klein, Suresh Sundaresan



55

# DAY 1. MCN 개요와 라우팅



❖ Routers / Layer 3 Switching (Legacy):

- Switch packets between different physical networks, based upon Network-layer addressing
- Do not flood MAC-layer broadcasts from one attached network to another
- Are protocol dependent (IP routed to IP; IPX routed to IPX, etc.)
- Support packet fragmentation
- Support multiple Physical- and Mac-layer packet encapsulation types, and have the ability to translate from one type to another

클라우드의 SDN 제어기는 All-seeing Eye



56

# DAY 1. MCN 개요와 라우팅



❖ Routers / Layer 3 Switching for SDN:

- When communication is needed between VLANs
- When MAC-layer multicast/broadcast traffic is adversely effecting network performance
- When packet switching based upon upper-layer protocols is desired
- Where multiple active paths between systems is required
- Isolation of MAC-layer broadcast traffic. Routers allow VLANs to communicate but prevent the flow of broadcast traffic from one physical LAN to another
- Path Selection. Routers can use the best path which physically exists between source and destination systems. Some routers allow for load balancing over redundant paths
- Flexibility. Routers can support any desired network topology
- The total size of the network interconnected with routers is, for all practical purposes, unlimited

SDN 제어기에서 데이터플레인으로 플로우 전송

MAC 브로드캐스트 SDN 제어기로 전송

Service Mesh, 통신을 위한 SCTP등

MAC 브로드캐스트 SDN 제어기로 전송

SDN 제어기에서 데이터플레인으로 플로우 전송

클라우드의 SDN 제어기 All-seeing Eye or 고정



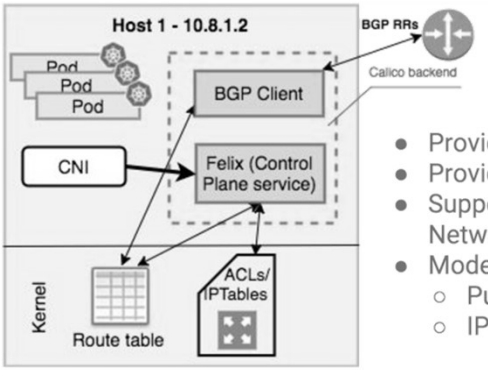
57

# DAY 1. MCN 개요와 라우팅



❖ Kubernetes CNI의 BGP 사용 (예): Calico Project

- Pure L3 based network solution
- Router per node
- Host-Host Networking
- IPAM/ pod Network
- Network Policy
- Modes
  - ✓ Pure BGP
  - ✓ IP-IP encap




- Pure L3 based network solution
- Router per node
- Provides host-host n/w'ing
- Provides IPAM & pod n/w
- Supports Kubernetes NetworkPolicy constructs
- Modes:
  - Pure BGP
  - IP-IP encap

Source: https://platform9.com/blog/kubernetes-networking-achieving-high-performance-with-calico/



58

# DAY 1. MCN 개요와 라우팅



❖ eBPF 사용 (예): Calico Project

- Calico's eBPF dataplane

| Factor | Standard Linux Dataplane | eBPF dataplane |
|---|---|---|
| **Throughput** | Designed for 10GBit+ | Designed for 40GBit+ |
| **First packet latency** | Low (kube-proxy service latency is bigger factor) | Lower |
| **Subsequent packet latency** | Low | Lower |
| **Preserves source IP within cluster** | Yes | Yes |
| **Preserves external source IP** | Only with externalTrafficPolicy: Local | Yes |
| **Direct Server Return** | Not supported | Supported (requires compatible underlying network) |
| **Connection tracking** | Linux kernel's conntrack table (size can be adjusted) | BPF map (fixed size) |
| **Policy rules** | Mapped to iptables rules | Mapped to BPF instructions |
| **Policy selectors** | Mapped to IP sets | Mapped to BPF maps |
| **Kubernetes services** | kube-proxy iptables or IPVS mode | BPF program and maps |
| **IPIP** | Supported | Supported (no performance advantage due to kernel limitations) |
| **VXLAN** | Supported | Supported |
| **Wireguard** | Supported (IPv4 and IPv6) | Supported (IPv4) |
| **Other routing** | Supported | Supported |
| **Supports third party CNI plugins** | Yes (compatible plugins only) | Yes (compatible plugins only) |
| **Compatible with other iptables rules** | Yes (can write rules above or below other rules) | Partial; iptables bypassed for workload traffic |
| **Host endpoint policy** | Supported | Supported |
| **Enterprise version** | Available | Available |
| **XDP DoS Protection** | Supported | Supported |
| **IPv6** | Supported | Not supported (yet) |

Source: https://projectcalico.docs.tigera.io/maintenance/ebpf/enabling-ebpf



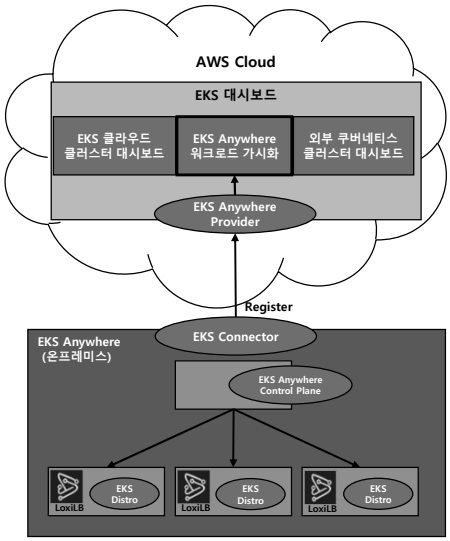
59

# DAY 1. MCN 개요와 라우팅



❖ eBPF 사용 (예): AWS EKS Anywhere

- Cilium (eBPF)
- MetalLB or LoxiLB (eBPF)


Source: https://cilium.io/

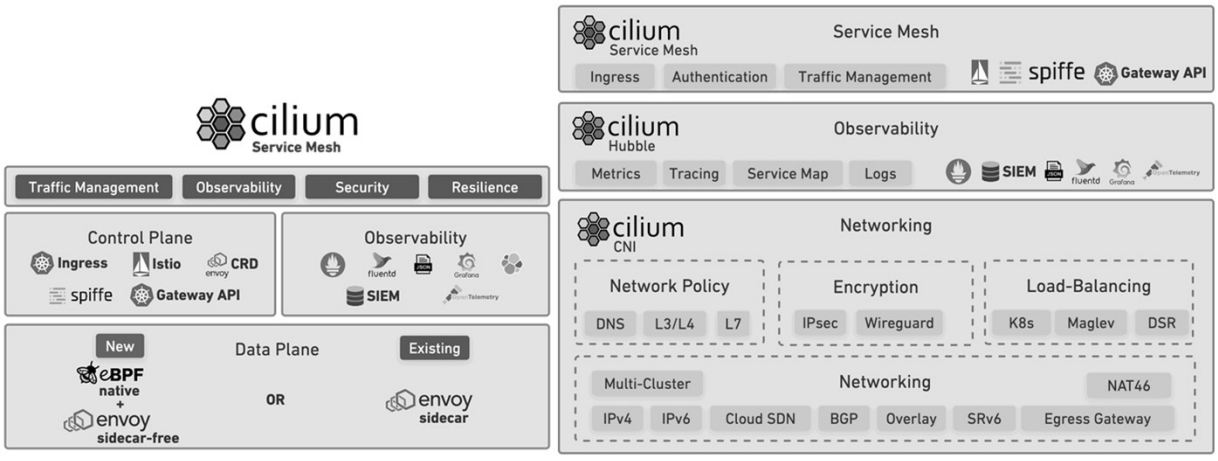


60

# DAY 1. MCN 개요와 라우팅



❖ eBPF 사용 (예): Cilium 1.12 Major Features




Source: https://www.cncf.io/blog/2022/07/20/cilium-1-12-ga-cilium-service-mesh-and-other-major-new-features-for-enterprise-kubernetes/



61

# DAY 1. MCN 개요와 라우팅



❖ UDP and TCP port numbers - 3 ranges

• "Well-Known Ports" (0–1023) are for the most important and widely-used protocols. On many Unix-like operating systems, normal user programs cannot use these ports, which prevented troublesome undergraduates on multi-user machines from running programs to masquerade as important system services. Today the same protections apply when hosting companies hand out command line Linux accounts.

• "Registered Ports" (1024–49151) are not usually treated as special by operating systems—any user can write a program that grabs port 5432 and pretends to be a PostgreSQL database, for example—but they can be registered by the IANA for specific protocols, and the IANA recommends that you avoid using them for anything but their assigned protocol.

• The remaining port numbers (49152–65535) are free for any use. They, as we shall see, are the pool on which modern operating systems draw in order to generate

Internet Assigned Numbers Authority (IANA)

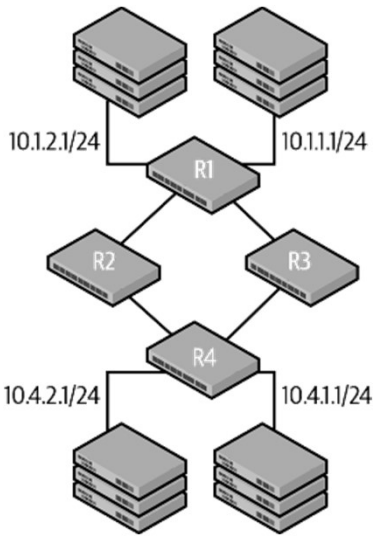


62

# DAY 1. MCN 개요와 라우팅



❖ 라우터 network (예)




Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY

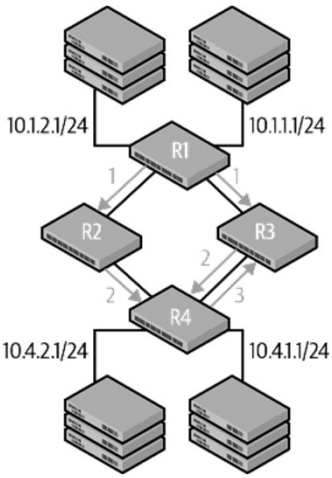


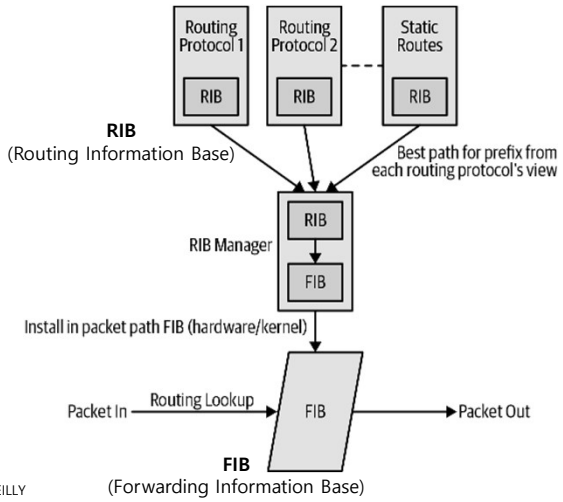
63

# DAY 1. MCN 개요와 라우팅



- Distance vector routing protocol packet exchange from R1 to R4
- RIB versus FIB




Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY

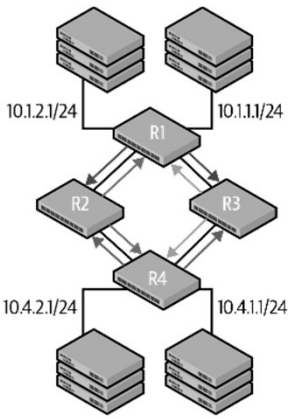


64

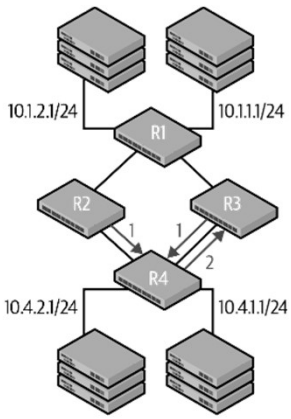
# DAY 1. MCN 개요와 라우팅



- link-state routing protocol packet exchange




(a) Initial LSA sent by all routers to their neighbors




(b) R1's LSA flooded by all the routers

Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY

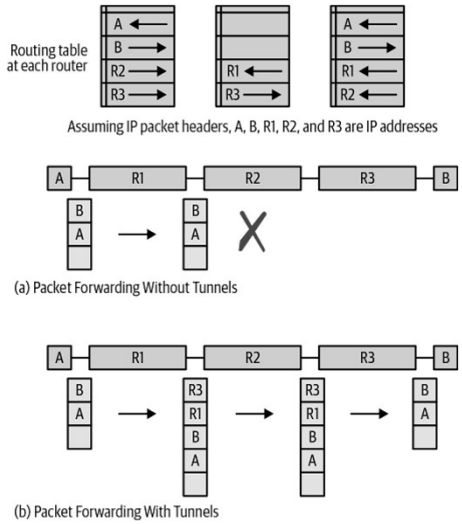


65

# DAY 1. MCN 개요와 라우팅



❖ Packet forwarding in network tunnels




Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY



66

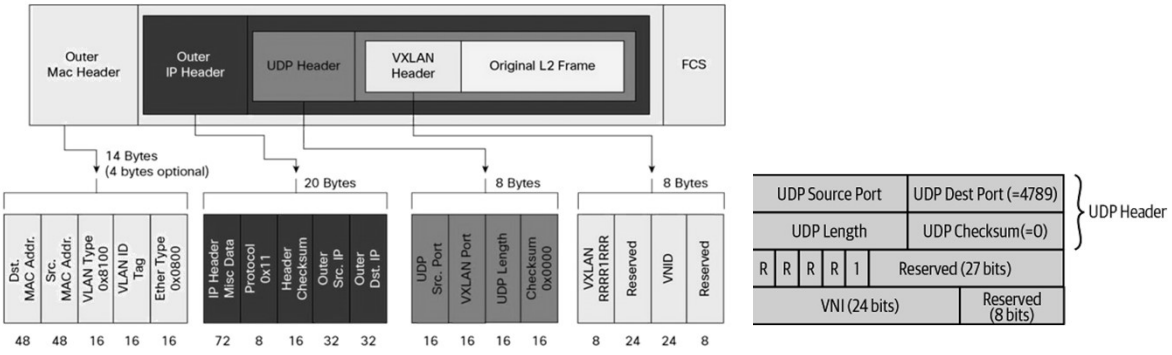
# DAY 1. MCN 개요와 라우팅



❖ VXLAN header format

• Frame 길이 확장: 50 바이트 (=14+20+8+8)

Figure 1. VXLAN Packet Format




Source: https://www.cisco.com/c/ko_kr/support/docs/ios-nx-os-software/nx-os-software/200262-Configure-VxLAN-Flood-And-Learn-Using-Mu.html
Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY



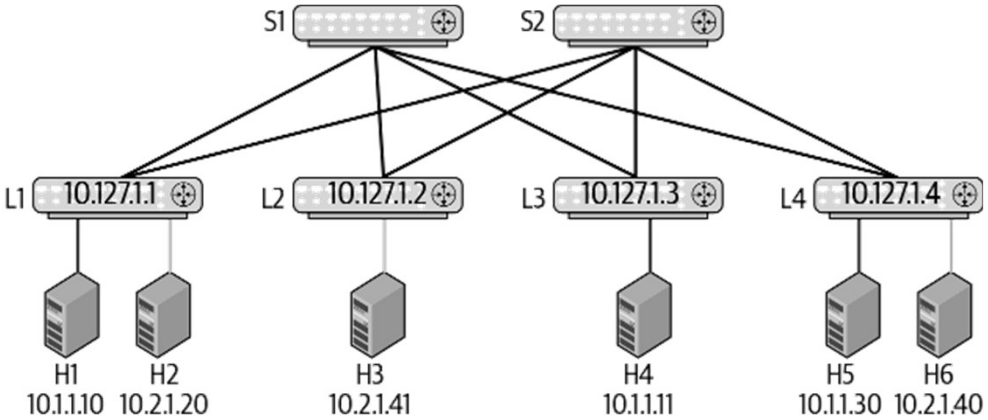
67

# DAY 1. MCN 개요와 라우팅



❖ VXLAN packet flow

Before VXLAN?




Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY

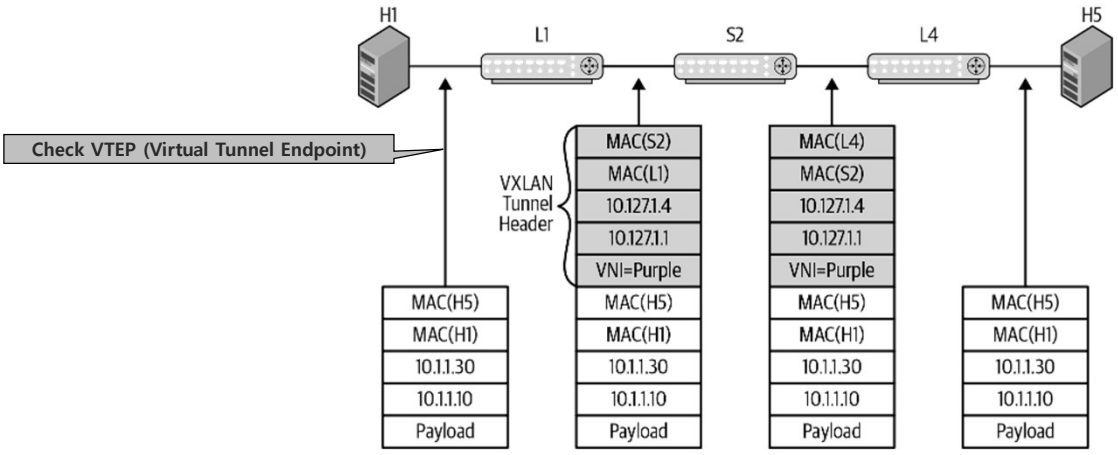


68

# DAY 1. MCN 개요와 라우팅



❖ Packet headers with VXLAN basic bridging




Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY

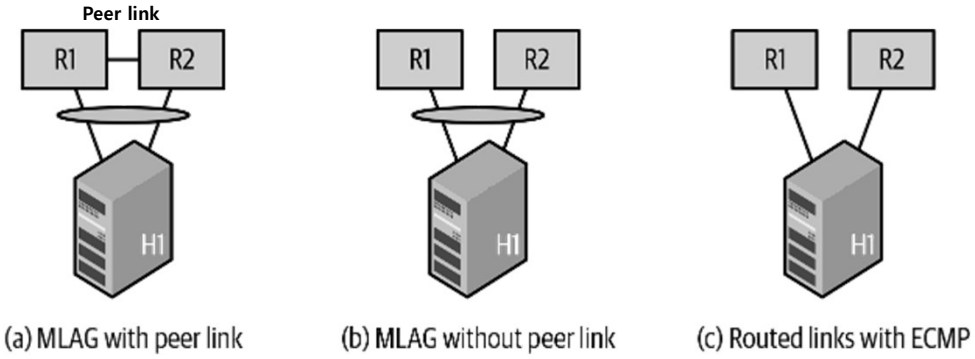


69

# DAY 1. MCN 개요와 라우팅



❖ Dual-attached host models




(a) MLAG with peer link (b) MLAG without peer link (c) Routed links with ECMP

Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY

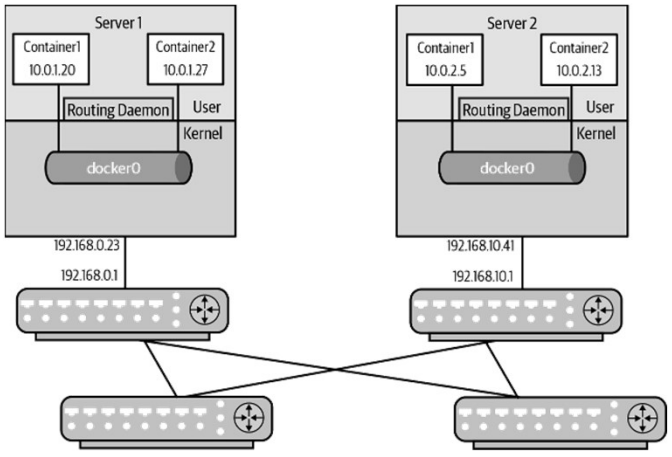


70

# DAY 1. MCN 개요와 라우팅



❖ Routing for multihost container networking




Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY

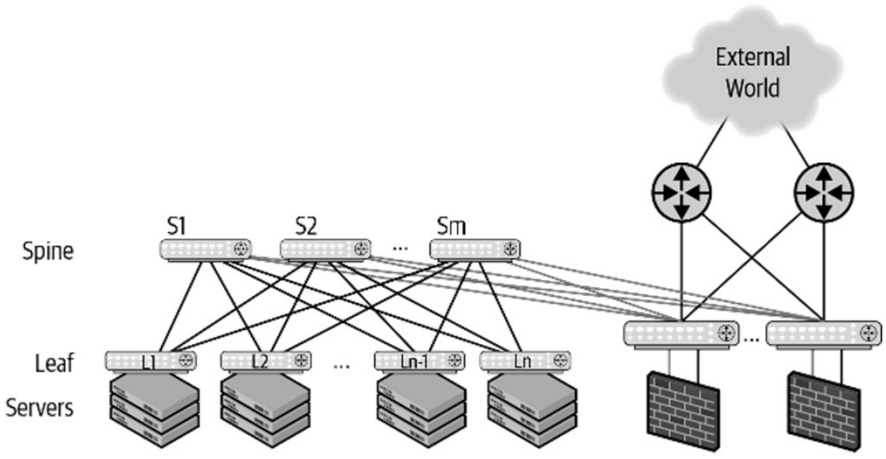


71

# DAY 1. MCN 개요와 라우팅



❖ Connecting Clos via firewall to the external world




Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY



72

# DAY 1. MCN 개요와 라우팅



❖ Inventory (Ansible)

ANSIBLE

```
vx ansible_host=192.168.121.154
eos ansible_host=192.168.121.109
server01 ansible_host=192.168.121.86
server02 ansible_host=192.168.121.82

[servers]
server01
server02

[cumulus]
vx

[arista]
eos

[linux:children]
cumulus
linux

[routers:children]
vx
```

Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY



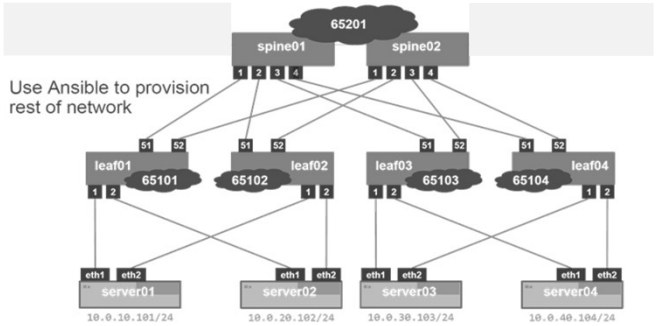
73

# DAY 1. MCN 개요와 라우팅



❖ **Ansible Template** (Playbook)

❖ **ansible-playbook.yml**




74

# DAY 1. MCN 개요와 라우팅



❖ **Operation for Ansible "ansible-playbook.yml"**


```
cumulus@oob-mgmt-server:~/NetworkAutomation$ ansible-playbook.yml
...
PLAY RECAP *********************************************************************************
leaf01                     : ok=10   changed=7    unreachable=0    failed=0
leaf02                     : ok=10   changed=6    unreachable=0    failed=0
leaf03                     : ok=10   changed=6    unreachable=0    failed=0
leaf04                     : ok=10   changed=6    unreachable=0    failed=0
server01                   : ok=3    changed=1    unreachable=0    failed=0
server02                   : ok=3    changed=1    unreachable=0    failed=0
server03                   : ok=3    changed=1    unreachable=0    failed=0
server04                   : ok=3    changed=1    unreachable=0    failed=0
spine01                    : ok=10   changed=6    unreachable=0    failed=0
spine02                    : ok=10   changed=6    unreachable=0    failed=0
Wednesday 11 October 2017  19:42:59 +0000 (0:00:05.074)       0:01:16.673 *****
===============================================================================
reset : Clear config ---------------------------------------------------------- 16.03s
Net 6 -- Deploy Configuration To All Leafs ------------------------------------ 13.61s
Net 6 -- Deploy Configuration to All Spines ----------------------------------- 9.70s
reset : Restore NTP ----------------------------------------------------------- 7.97s
Restart Networking ------------------------------------------------------------ 5.07s
Restart PTM Daemon to Apply new Topology.dot file ----------------------------- 3.87s
Gathering Facts --------------------------------------------------------------- 3.21s
Gathering Facts --------------------------------------------------------------- 3.01s
Restart the netq-agent -------------------------------------------------------- 2.93s
reset : Copy the Default Interface Configuration in Place --------------------- 2.83s
Download the topology.dot file from the OOB-MGMT-SERVER ----------------------- 2.11s
Gathering Facts --------------------------------------------------------------- 1.80s
reset : Apply Default Interface Configuration --------------------------------- 1.76s
Copy Interfaces Configuration File -------------------------------------------- 1.52s
Gathering Facts --------------------------------------------------------------- 1.20s
cumulus@oob-mgmt-server:~/NetworkAutomation$
```

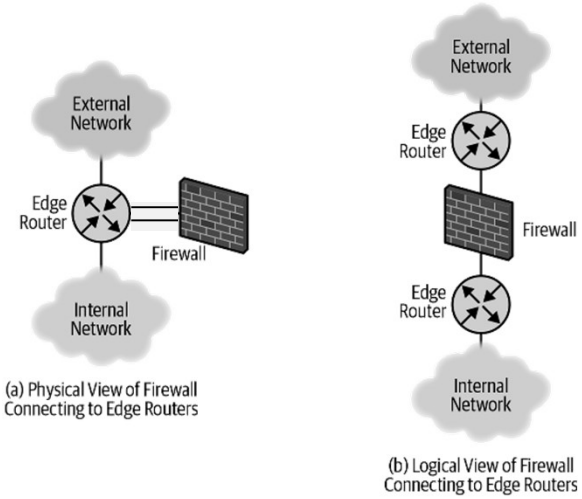


75

# DAY 1. MCN 개요와 라우팅



❖ Forcing traffic through a firewall




Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY



76

# DAY 1. MCN 개요와 라우팅



❖ Virtual Routers:

| Vendor | Name | Commercial or Open Source |
|---|---|---|
| **Cisco** | CSR (Cloud Service Router) | Commercial |
| **Cisco** | ISRv (Integrated Services Virtual Router) | Commercial |
| **Juniper** | vMX | Commercial |
| **Brocade (acquired)** | Vyatta | Commercial |
| **Alcatel Lucent** | VSR | Commercial |
| **VMware** | NSX | Commercial |
| **Cloud Router** | Cloud Router | Open Source |
| **VyOS** | VyOS | Open Source |
| **Quagga** | Linux Router (Quagga) | Open Source |
| **OCP** | Software for Open Networking in the Cloud (SONiC) | Open Source |



77

# DAY 1. MCN 개요와 라우팅



❖ Open Source Router OS Software for Small or Large Networks

1. VyOS
2. RouterOS from MicroTik
3. OpenWRT
4. pfsense
5. ClearOS
6. IPFire
7. DD-WRT
8. Advanced Tomato
9. Fresh Tomato
10. Zeroshell
11. OPNSense
12. Fli4l
13. Sophos XG Home Firewall/Router

- **VyOS는 Debian GNU/Linux 기반의 오픈 소스 네트워크 운영 체제, 표준 amd64, i586 및 ARM 시스템에서 실행, 클라우드 배포를 위한 라우터 및 방화벽 플랫폼으로 사용**

Source: https://www.networkstraining.com/best-open-source-router-os/

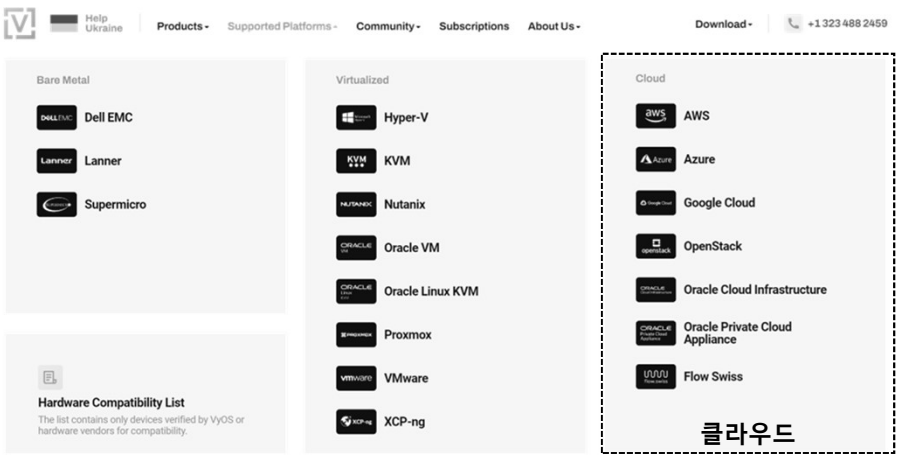


78

# DAY 1. MCN 개요와 라우팅



❖ VyOS의 클라우드 지원




Source: https://vyos.io/



79

# DAY 1. MCN 개요와 라우팅



❖ Easily and securely connect to multiple cloud solutions from one place (VyOS)


Source: https://vyos.io/use-cases/cloud-gateway

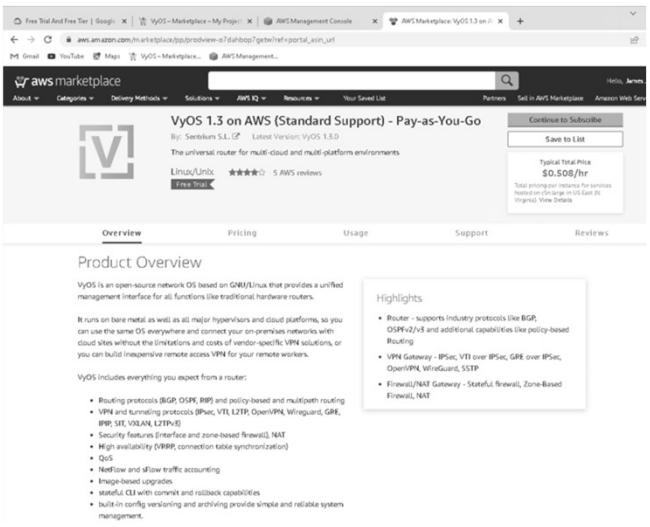




# DAY 1. MCN 개요와 라우팅



❖ VyOS @ Amazon AWS

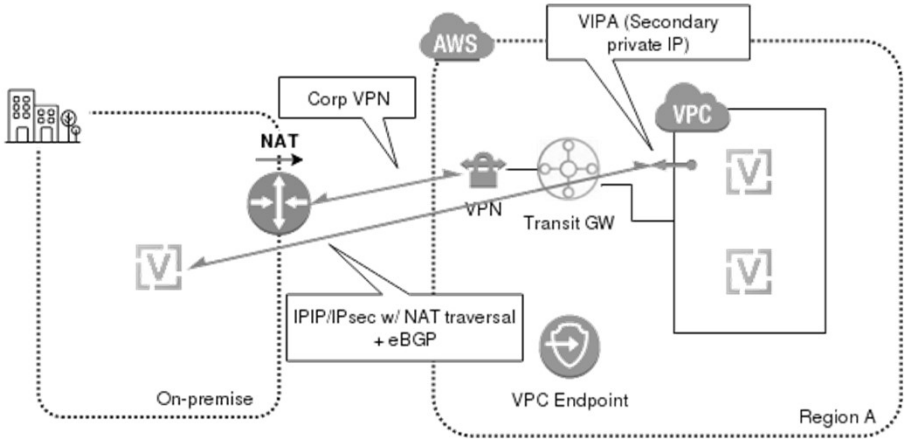



Source: https://aws.amazon.com/marketplace/pp/prodview-o7dahbop7getw?ref=portal_asin_url

# DAY 1. MCN 개요와 라우팅



❖ VyOS HA in AWS




Source: https://blog.stratio.com/vyos-ha-in-aws/

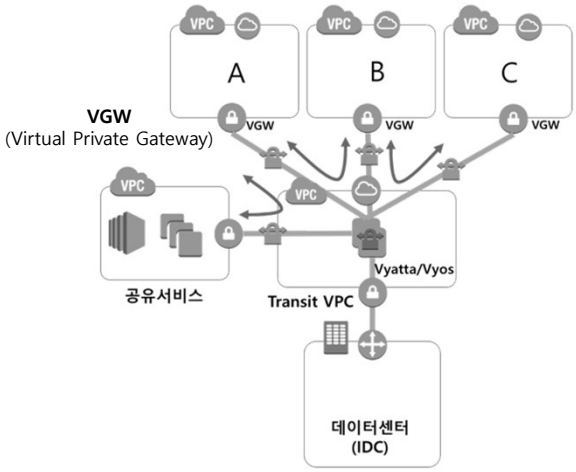


82

# DAY 1. MCN 개요와 라우팅



❖ Vyatta 및 VyOS를 통한 Cloud HUB 디자인




Source: https://aws.amazon.com/ko/blogs/korea/transit-vpc-cloud-hub-design-using-aws-marketplace-tools/

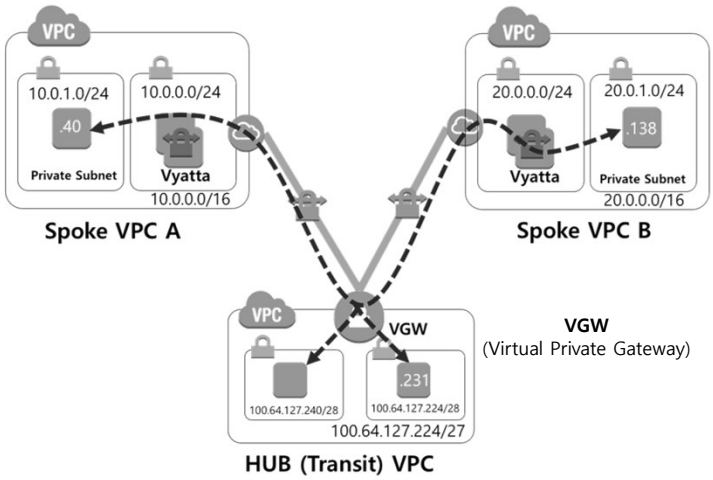


83

# DAY 1. MCN 개요와 라우팅



❖ Cloud HUB 구성 테스트 하기




Source: https://aws.amazon.com/ko/blogs/korea/transit-vpc-cloud-hub-design-using-aws-marketplace-tools/

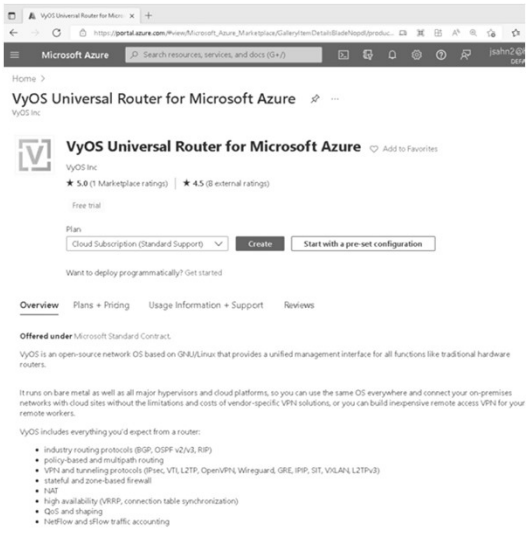


84

# DAY 1. MCN 개요와 라우팅



❖ VyOS @ Microsoft Azure




Source: Microsoft Azure

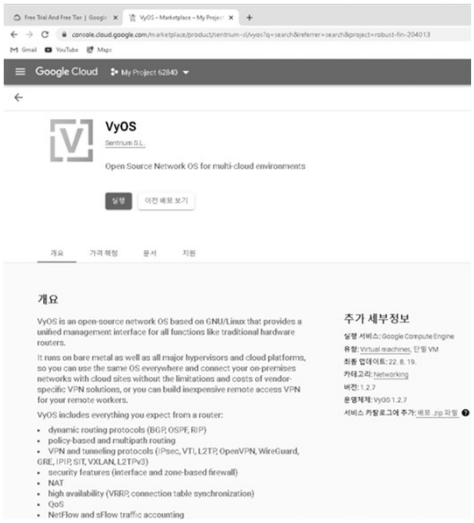


85

# DAY 1. MCN 개요와 라우팅



❖ VyOS @ Google Cloud Platform (GCP)




Source: https://vyos.io/

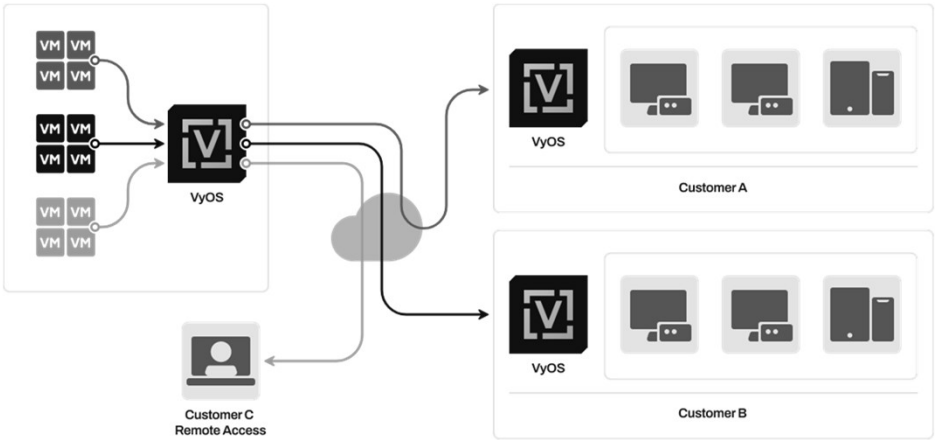


86

# DAY 1. MCN 개요와 라우팅



❖ VyOS on VMware




Source: https://vyos.io/solutions/vyos-on-vmware

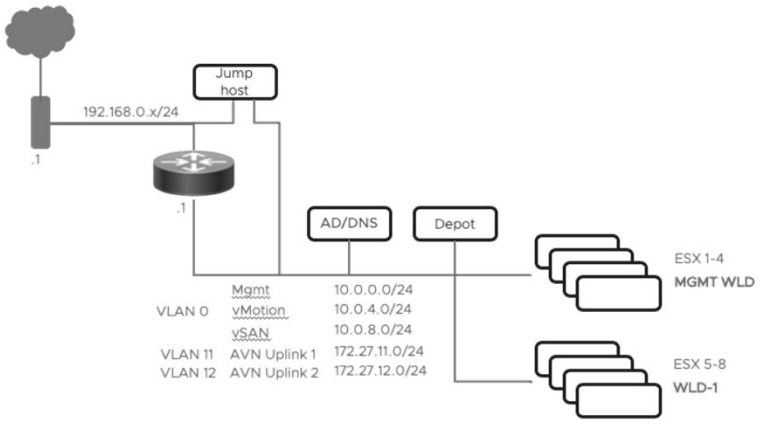


87

# DAY 1. MCN 개요와 라우팅



❖ VMware Cloud Foundation (VCF) with VyOS




Source: https://datareload.com/vmware-cloud-foundation-vcf-with-vyos/

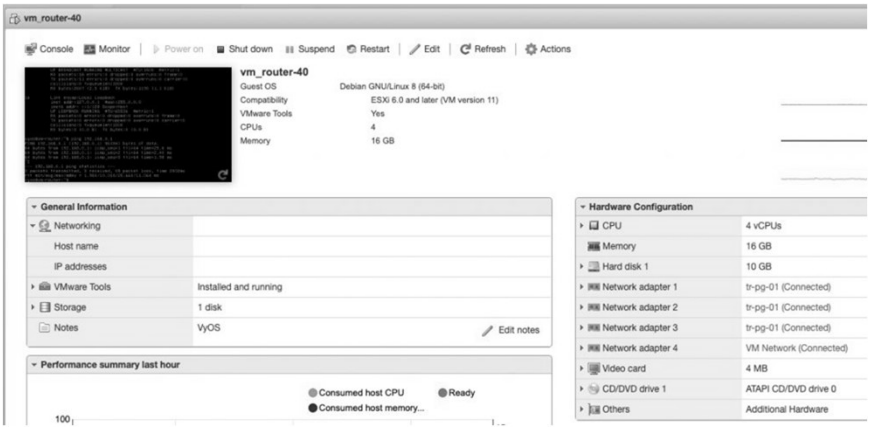


88

# DAY 1. MCN 개요와 라우팅



❖ VMware Cloud Foundation (VCF) with VyOS




Source: https://datareload.com/vmware-cloud-foundation-vcf-with-vyos/

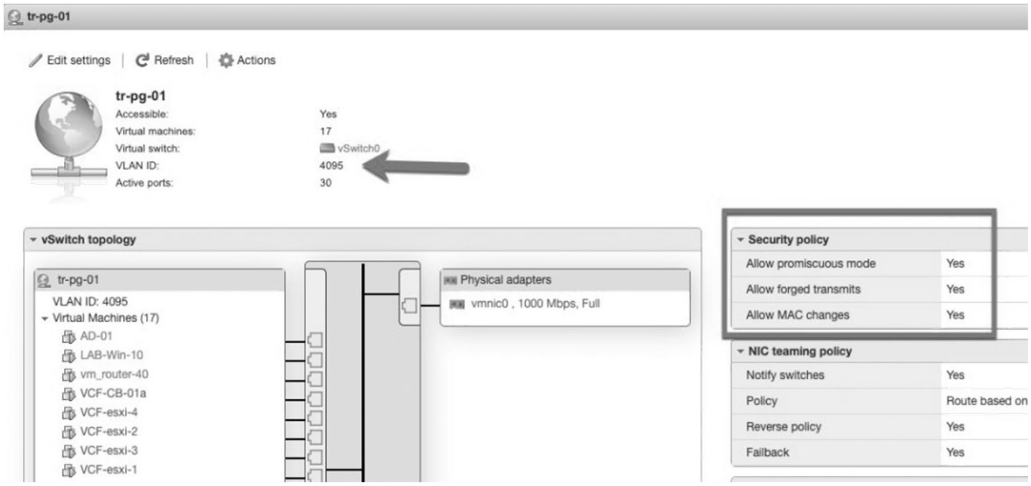


89

# DAY 1. MCN 개요와 라우팅



❖ VMware Cloud Foundation (VCF) with VyOS




Source: https://datareload.com/vmware-cloud-foundation-vcf-with-vyos/





# DAY 1. MCN 개요와 라우팅



❖ Border Gateway Protocol routing

- The Border Gateway Protocol (BGP) is the successor to the Exterior Gateway Protocol. BGP is designed for routing between AS. BGP supports a metric and is able to make intelligent routing decisions. BGP can work with the internal routing protocol OSPF. Route aggregation is mostly used and supported in Classless Inter-Domain Routing (CIDR).

**자치시스템 (AS) 상호 간에 적용되는 라우팅 프로토콜 (Inter-Domain Routing Protocol)**
**즉, 독립 운용되는 대규모 네트워크 (AS) 간에, 네트워크 정보를 교환하기 위해 주로 사용됨**

**BGP version 1 (1989), BGP version 4 (1995 : CIDR 및 Supernetting 도입적용)**
**일반적으로 BGP라고 하면 현재의 BGP-4를 의미**

autonomous systems (AS)

Source: Multi-Cloud for Architects (Published by Packt Publishing Ltd) Florian Klaffenbach, Markus Klein, Suresh Sundaresan

# DAY 1. MCN 개요와 라우팅



❖ BGP 주요 개념 용어

- BGP의 AS(자치시스템) 간의 연결유형 구분 ☞ (BGP AS)
- BGP 경로 결정을 위한 라우팅 메트릭 ☞ (BGP Path Attribute)
  - BGP에서 Route의 특성을 기술하는 매개변수들의 집합으로 Path Attribute이라 함
- BGP 라우팅 프로토콜을 수행하는 라우터의 구분 ☞ (BGP 라우터)
- BGP 라우터 간 Session 설정 ☞ (BGP 이웃 협상)
  - EBGP (External BGP) Session : 다른 AS 상호 간에 변방 라우터들끼리 접속
  - IBGP (Internal BGP) Session : 동일 AS 내부의 변방 라우터들 간 내부접속

autonomous systems (AS)

Source: http://www.ktword.co.kr/test/view/view.php?m_temp1=1326



92

# DAY 1. MCN 개요와 라우팅



❖ Routing – Border Gateway Protocol (BGP) Topics

- The Protocol and Its Use
- Autonomous Systems (AS)
- BGP Messaging (Neighbor Establishment and Termination)
- Internal Border Gateway Protocol/External Border Gateway Protocol
- BGP Basic Configuration
- Route Injection
- BGP Attributes & Route Selection
- Route Aggregation
- BGP Monitoring & Clearing
- Advanced Topics

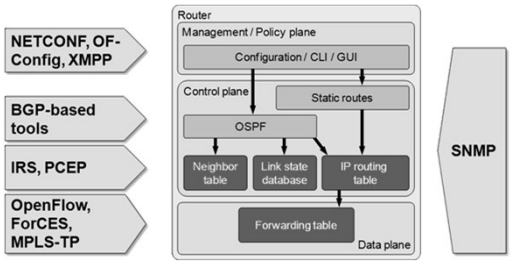


93

# DAY 1. MCN 개요와 라우팅



- The Border Gateway Protocol (BGP) is an exterior gateway protocol (EGP) that is used to exchange routing information among routers in different autonomous systems (ASs)
- EGP and IGP differ in how best possible path is determined for a given route:
  - IGP determines best route by established metric for complete path
  - RIP utilizes hop count as a metric to determine best route
  - OSPF can use metrics such as various interface costs to determine best route
  - EGP directs traffic from source AS to destination AS based on path knowledge and path attributes. Path attributes are route parameters that can influence the direction traffic will flow in






94

# DAY 1. MCN 개요와 라우팅



- The protocol is used to define an administrative boundary between autonomous systems
- The process of routing with BGP is often referred to as external routing
- BGP is a Path Vector Protocol
- BGP routing information includes the complete route to each destination along with detailed information on how the route should be handled
- Utilizes Classless Inter-Domain Routing (CIDR) which Eliminates shortcomings of original classful IP addressing by allowing aggregation of blocks of IP addresses to reduce size of routing tables



95

# DAY 1. MCN 개요와 라우팅



❖ Autonomous Systems

- A Autonomous System (AS) is collection of networks with the same routing policy
- Usually running a single routing protocol (IGP) within the interior
- Typically under a single ownership and administration
- Originally identified by a unique AS numbers (1-65535)
- As of January 2009 expanded to 4,294,967,296. (See RFC 4893, BGP Support for Four-octet AS Number Space)
- AS numbers 64512 through 65534 are designated for private use



96

# DAY 1. MCN 개요와 라우팅



❖ Autonomous Systems: collections of connected IP routing prefixes under the control of one or more network providers or operators.

❖ Autonomous Systems defined under RFC 1930: https://www.rfc-editor.org/rfc/rfc1930

| Provider | Primary ASN | Additional ASN |
|---|---|---|
| Microsoft | 8075 | 12076 |
| Amazon Web Services | 16509 | 38895 |
| Netflix | 2906 | 40027 |
| Salesforce | 14340 | 45422 |
| Level 3 | 3549 | 3356 |

Source: Multi-Cloud for Architects (Published by Packt Publishing Ltd) Florian Klaffenbach, Markus Klein, Suresh Sundaresan

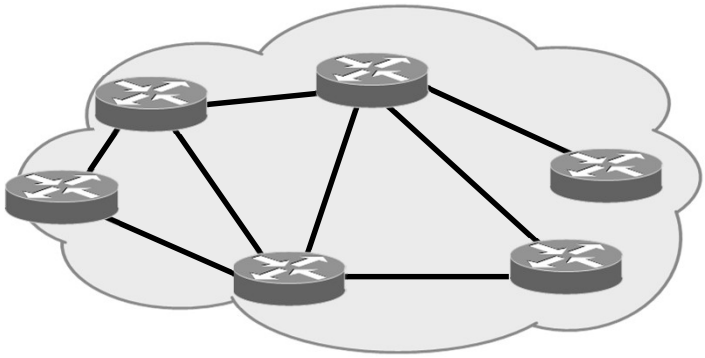


97

# DAY 1. MCN 개요와 라우팅



- Routing – BGP
- Autonomous Systems
- Routers in the below diagram are under one authority for management



AS-100

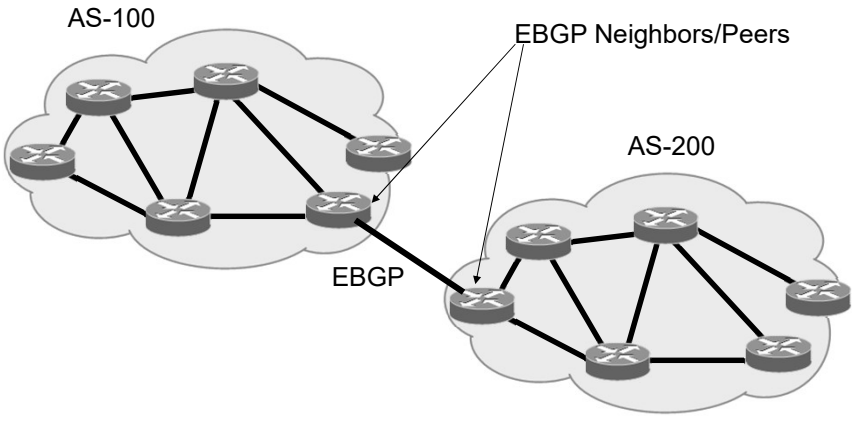


98

# DAY 1. MCN 개요와 라우팅



- Interfacing Two ASs
  - Routing – BGP
  - Autonomous Systems





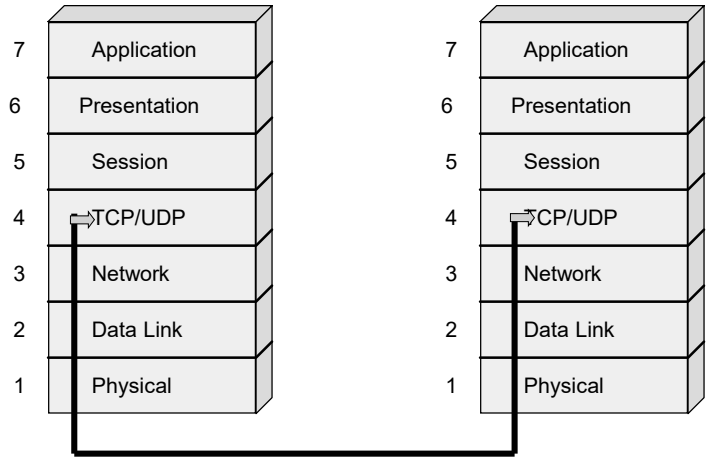

99

# DAY 1. MCN 개요와 라우팅

100

❖ Routing – BGP

- Peer Establishment / Packet Exchange
- Establish TCP session




JS Lab

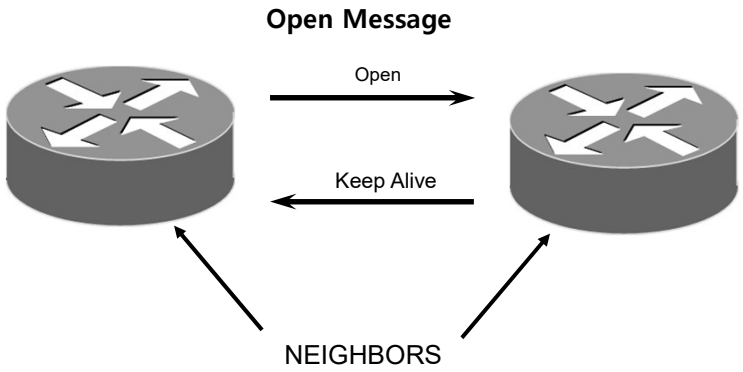
100

# DAY 1. MCN 개요와 라우팅

101

❖ Routing – BGP

- Neighbor Establishment & Termination
- Open Message



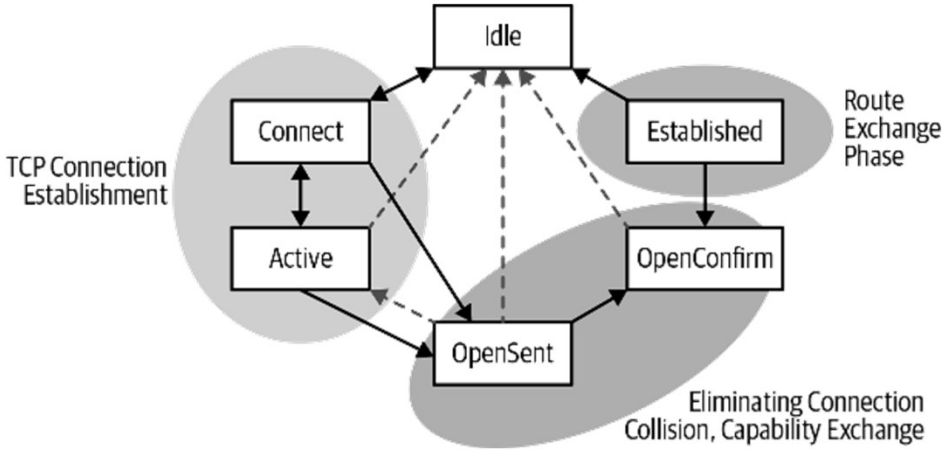

JS Lab

101

# DAY 1. MCN 개요와 라우팅



❖ BGP state machine




Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY



102

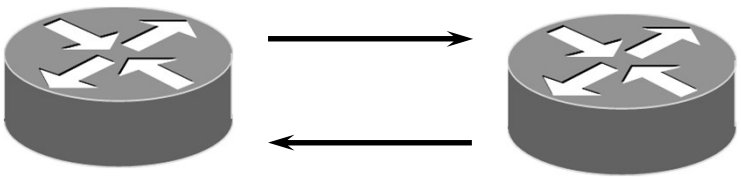
# DAY 1. MCN 개요와 라우팅



❖ Routing – BGP

- Neighbor Establishment & Termination
- Keepalive Messages

**Keepalive Messages**



Keepalives simply to let BGP neighbors know about the current state of the connection. They are used to maintain the link when routers have no routing updates to exchange.



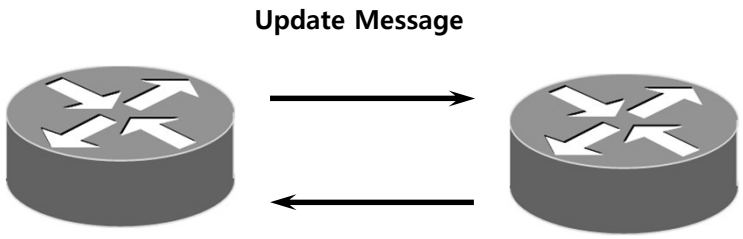
103

# DAY 1. MCN 개요와 라우팅



❖ Routing – BGP

- Neighbor Establishment & Termination
- Update Message




BGP uses Update Messages to exchanged or withdraw routes. Detailed information about the route is passed using attributes which are present in the update packet.



104

# DAY 1. MCN 개요와 라우팅



❖ BGP update message and format for multiprotocol network addresses

| BGP Header |
|---|
| Withdrawn Routes Length |
| Withdrawn Routes List |
| Total Path Attributes List |
| Path Attributes List |
| NLRI (Advertised Routes List) |

(a) BGP Update Message Format

| AFI |
|---|
| SAFI |
| Length of Next Hop Network Addr |
| Next Hop Network Addr |
| Reserved (1 byte) |
| Advertised Routes List (NLRI) |

(b) Format for Advertising MultiProtocol Routes

Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY



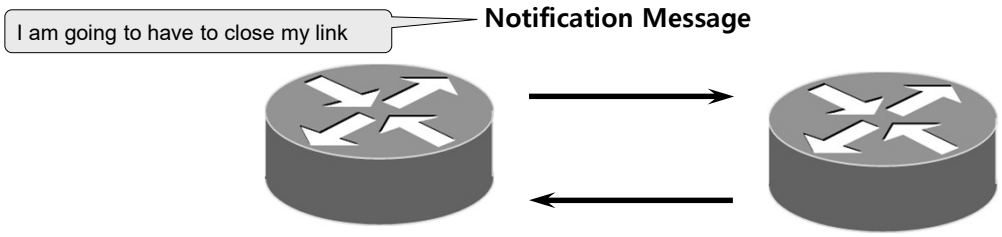
105

# DAY 1. MCN 개요와 라우팅

106

❖ Routing – BGP

- Neighbor Establishment & Termination
- Notification Message






106

# DAY 1. MCN 개요와 라우팅

107

❖ Routing – BGP: IBGP/EBGP

- The BGP protocol specifies two types of BGP Neighbor Relationships IBGP and EGBP:
- External Neighbors (EBGP) reside in different ASs
- Internal Neighbors (IBGP) reside in the same AS
- IBGP is used to carry BGP route information across an ISP backbone
- EBGP is used to exchange BGP route information with different ASs



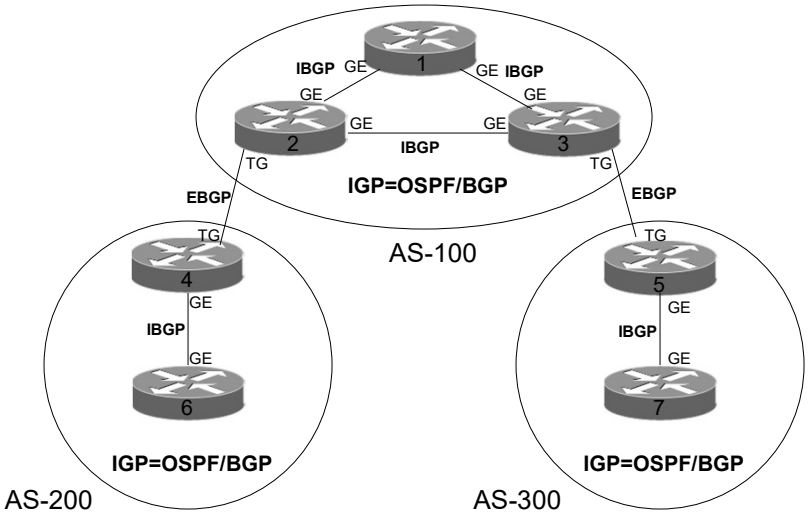
107

# DAY 1. MCN 개요와 라우팅



❖ Routing – BGP: IBGP/EBGP

• Basic IBGP/EBGP Model





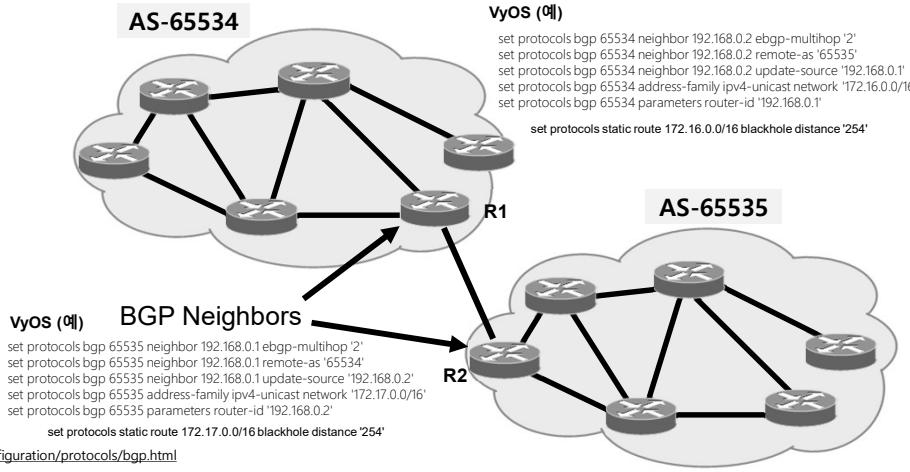

108

# DAY 1. MCN 개요와 라우팅



❖ Routing – BGP: IBGP/EBGP

• Basic Configuration: Enabling BGP & Identify Your Neighbors




Source: https://docs.vyos.io/en/equuleus/configuration/protocols/bgp.html



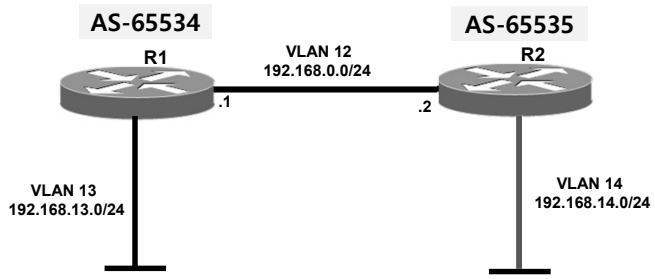
109

# DAY 1. MCN 개요와 라우팅



❖ Routing – BGP: Basic Configuration

• Enabling BGP & Identify Your Neighbors (EBGP)




**VyOS (예)**

```
set protocols bgp 65534 neighbor 192.168.0.2 ebgp-multihop '2'
set protocols bgp 65534 neighbor 192.168.0.2 remote-as '65535'
set protocols bgp 65534 neighbor 192.168.0.2 update-source '192.168.0.1'
set protocols bgp 65534 address-family ipv4-unicast network '172.16.0.0/16'
set protocols bgp 65534 parameters router-id '192.168.0.1'
    set protocols static route 172.16.0.0/16 blackhole distance '254'
```

**VyOS (예)**

```
set protocols bgp 65535 neighbor 192.168.0.1 ebgp-multihop '2'
set protocols bgp 65535 neighbor 192.168.0.1 remote-as '65534'
set protocols bgp 65535 neighbor 192.168.0.1 update-source '192.168.0.2'
set protocols bgp 65535 address-family ipv4-unicast network '172.17.0.0/16'
set protocols bgp 65535 parameters router-id '192.168.0.2'
    set protocols static route 172.17.0.0/16 blackhole distance '254'
```

**Configure:**

- The AS the router belongs to
- The BGP router ID
- Neighbor IP address and remote AS
- Route injection of a directly connected interface via **network** command



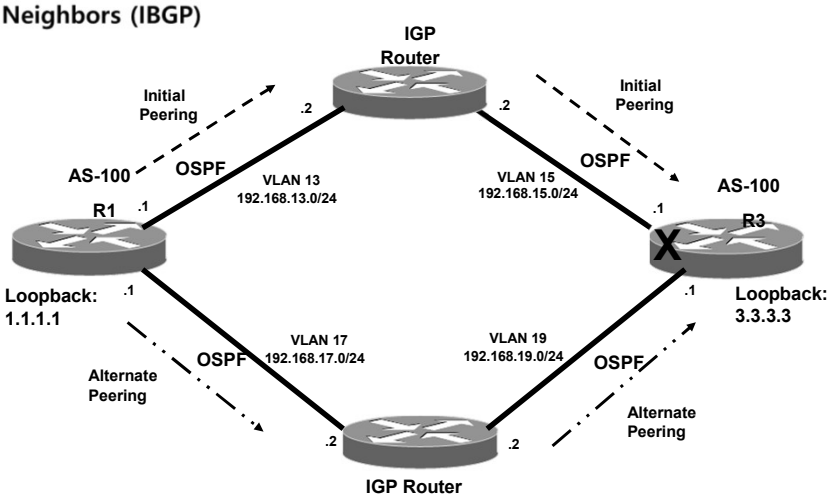
110

# DAY 1. MCN 개요와 라우팅



❖ Routing – BGP: Basic Configuration

• Enabling BGP & Identify Your Neighbors (IBGP)






111

## ❖ Routing – BGP: Basic Configuration

- Route Injection

**BGP Route Injection:**

Condition 1 for announcing IP into BGP

The BGP process must be aware of the route.
It can become aware of the route by:

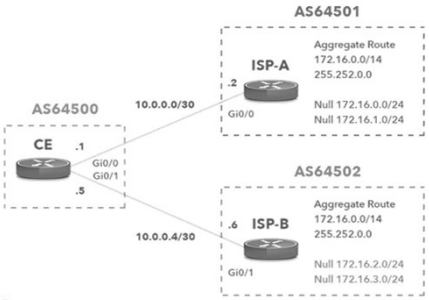
A BGP Neighbor
Redistributed from another routing protocol
A local network statement

Condition 2

The Route must already be present in the IP Routing Table

Could be a Static Route
Could be a directly connected route
It could have been installed by the IGP (OSPF, RIP, etc…)

**BGP Conditional Route Injection**




Source: https://www.noction.com/blog/bgp-conditional-route-injection





## ❖ Routing – BGP: Basic Configuration

- Attributes

**BGP Attributes:**

▪Routing information exchanged by BGP routers includes the complete route to each destination, as well as additional information about the route. This additional information is referred to as attributes

▪BGP attributes are a set of parameters that describe the characteristics of a route.

▪The BGP process uses attributes to select the best route to a destination

▪Attributes are categorized as being (Optional or Mandatory) and (Transitive or Non-Transitive)

- Well-known mandatory:Recognized by all BGP peers, passed to all peers, and present in all Update messages. Well-known mandatory attributes include:- Next-hop- Origin- AS PATH
- Well-known discretionary:Recognized by all routers, passed to all peers, and optionally included in the Update message. Well-known discretionary attributes include:- Local Preference- Atomic Aggregate
- Optional transitive:Possibly recognized by BGP routers and passed to BGP peers. Optional transitive attributes are marked as partial when not recognized. Optional transitive attributes include:- Aggregator- Community
- Optional non-transitive:Possibly recognized by BGP routers but not passed to peers. Optional non-transitive attributes include:- Multi-exit discriminator (MED)- Originator ID- Cluster-ID

Source: https://www.catchpoint.com/network-admin-guide/bgp-attributes

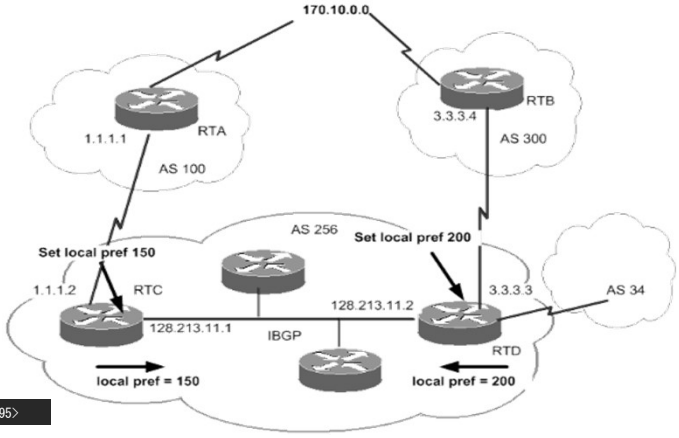
# DAY 1. MCN 개요와 라우팅



❖ Routing – BGP: Basic Configuration

- Attributes
- Local preference

**Local preference:** This attribute is used to influence a preferred exit point from the local autonomous system (AS). The higher value will determine the exit point for the AS.




VyOS Set BGP local preference attribute. (예)

```
set policy route-map <text> rule <1-65535> set local-preference <0-4294967295>
```



114

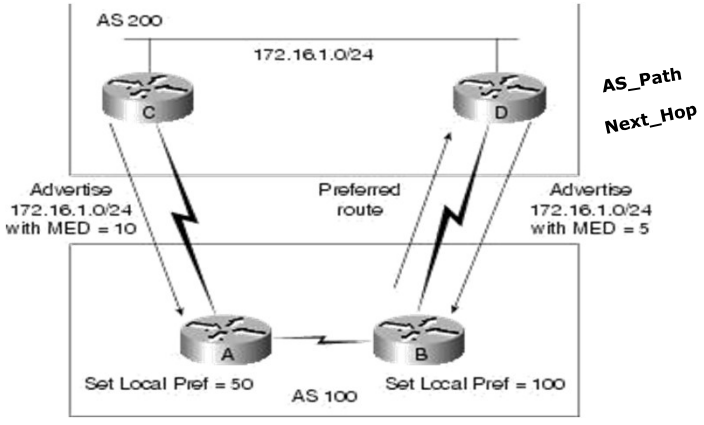
# DAY 1. MCN 개요와 라우팅



❖ Routing – BGP: Basic Configuration

- Attributes
- Multi-Exit Discriminator (MED)

**Multi-Exit Discriminator (MED):** It is a suggestion to external neighbors about the preferred path into an AS that has multiple entry points. The lower value MED will determine the entry point





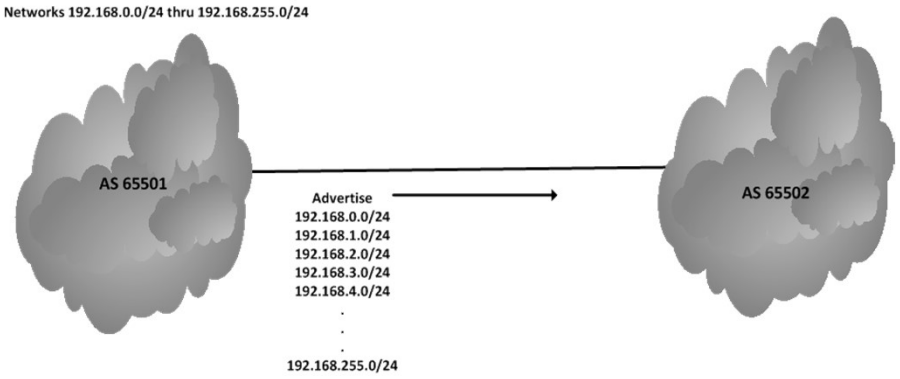

115

# DAY 1. MCN 개요와 라우팅



❖ Routing – BGP: Route Aggregation

- No Aggregation
- Route Aggregation




VyOS BGP aggregator attribute: AS number or IP address of an aggregation. (예)

```
set policy route-map <text> rule <1-65535> set aggregator <as|ip> <1-4294967295|x.x.x.x>
```



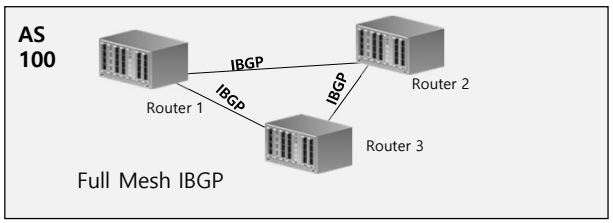
116

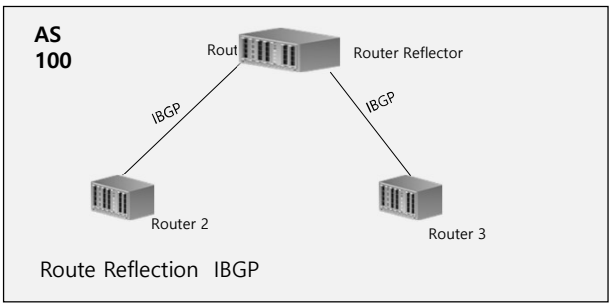
# DAY 1. MCN 개요와 라우팅



❖ Routing – BGP: Advanced Topics

- Route Reflection




VyOS Route Reflection Configuration. (예)

```
set protocols bgp <asn> parameters no-client-to-client-reflection
```



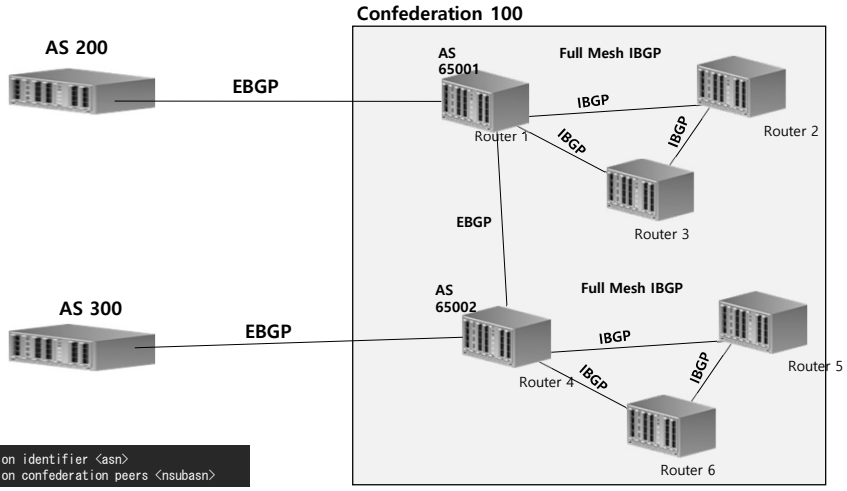
117

# DAY 1. MCN 개요와 라우팅



❖ Routing – BGP: Advanced Topics

• Confederations




**VyOS Confederation Configuration. (예)**

```
set protocols bgp <subasn> parameters confederation identifier <asn>
set protocols bgp <subasn> parameters confederation confederation peers <nsubasn>
```



118

# DAY 1. MCN 개요와 라우팅



❖ Routing – BGP: Advanced Topics

• Implementing a BGP Route-Map: AS-Path Regular Expressions

**VyOS (예)**

```
set policy as-path-list FavoriteAS rule 10 action permit
set policy as-path-list FavoriteAS rule 10 regex "^64555_"
```

```
# show policy as-path-list sky-sti-in
rule 10 {
action permit
description SKY-STI.IN
regex ^133803$
}
rule 11 {
action deny
regex .+
}
```

Source: https://m.clien.net/service/board/lecture/17610900

| Character | Description | Example |
|---|---|---|
| ^ | Start of string. | ^200 matches any string starting with "200". |
| $ | End of string. | 200$ matches any string ending with "200". |
| . | Matches any character. | 2.0 match "200", "210", "220" |
| * | Matches the preceding element zero or more times. | 22* matches "2"," 22", "222" |
| .* | Matches any character any number of times. | This is a match all. |
| [] | Matches a single chacter inside the brackets. | [d] matches the character "d". |
| [-] | Matches a range. | [0-9] matches any number from 0 to 9. |
| () | Specifies a subexpression. | (200:500) is treated as a single entity. |
| [^] | Matches any single charater not specified in the brackets. | [^er] matches all characters except for "e" and "r". |
| ? | Matches the preceding exactly. | 200? matches "200" only. |
| + | Matches the preceding element one or more times. | 200? matches "200", "200200", "200200200". |
| \| | Matches either the expression before or the expression after the operator (the choice operator). | 100 \| 250 matches either "100" or "250" |



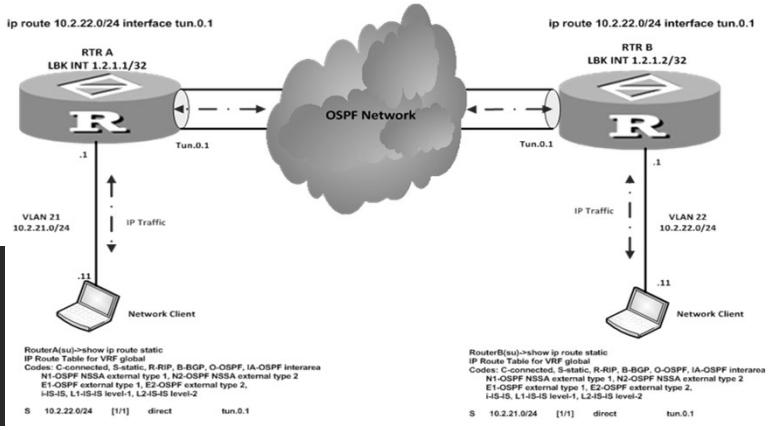
119

# DAY 1. MCN 개요와 라우팅



❖ Routing - Layer 3 Tunneling

• Traffic Flow




**BGP L2VPN/EVPN support via VXLAN transport**

```
# Underlay information specifically here for BGP multipath
set protocols bgp 65010 address-family ipv4-unicast maximum-paths ibgp '4'

# Underlay information specifically here to announce dummy interfaces through BGP
set protocols bgp 65010 address-family ipv4-unicast redistribute connected

# Overlay information used by EVPN routers to announce all VNIs that are configured
set protocols bgp 65010 address-family l2vpn-evpn advertise-all-vni

set protocols bgp 65010 neighbor 172.29.1.0 peer-group 'evpn'
set protocols bgp 65010 neighbor 172.29.2.0 peer-group 'evpn'
set protocols bgp 65010 parameters log-neighbor-changes
set protocols bgp 65010 peer-group evpn address-family ipv4-unicast nexthop-self
set protocols bgp 65010 peer-group evpn address-family l2vpn-evpn nexthop-self
set protocols bgp 65010 peer-group evpn remote-as '65010'
```

Source: https://blog.vyos.io/evpn-vxlan-vyos

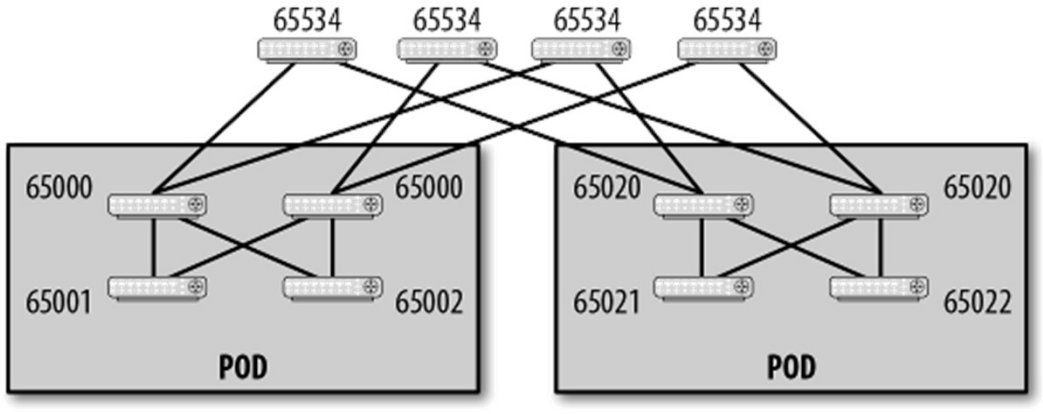


120

# DAY 1. MCN 개요와 라우팅



❖ BGP ASN numbering in a three-tier Clos topology




Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY

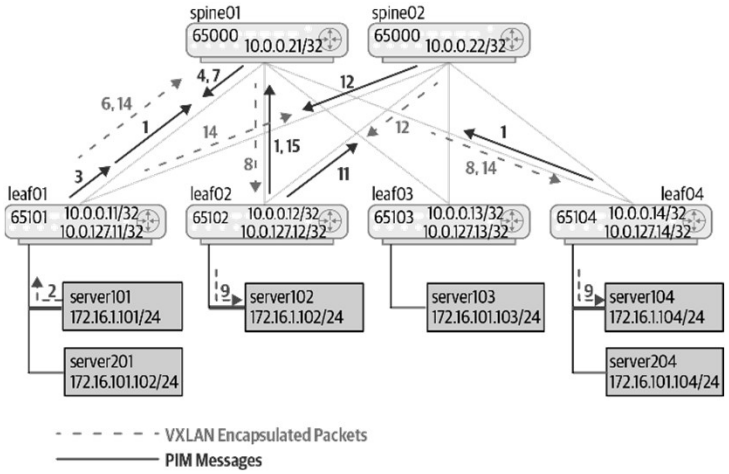


121

# DAY 1. MCN 개요와 라우팅



❖ EVPN bridging packet sequence with routed multicast underlay




Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY



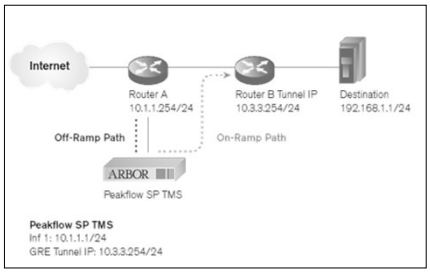
122

# DAY 1. MCN 개요와 라우팅



❖ BGP for Middle Box

- Some vendor recommends that you configure each traffic device as an iBGP route reflector client with each BGP router.




The following example specifies that the neighbors 200.10.1.2 and 200.10.2.2 are a clients of route reflector 1.1.1.1:

```
Router 1(rw-config)->router bgp 100
Router 1(su-config-bgp)->bgp router-id 1.1.1.1
Router 1(su-config-
Router 1(su-config-
Router 1(su-config-
Router 1(su-config-
Router 1(su-config-
```

```
Router 2(rw-config)->router bgp 100
Router 2(su-config-bgp)->bgp router-id 2.2.2.2
Router 2(su-config-bgp)->neighbor 1.1.1.1 remote-as 100
```

At this point, customers just have to add static routes for their attacked prefixes to black-hole traffic at AS300 edges:

```
Cust10(config)#ip route 192.168.10.20 255.255.255.255 fa1/0 tag 100
```

```
RouterA(rw-config)-> interface tunnel 1
RouterA(su-config-tun.0.1)->tunnel mode gre
RouterA(su-config-tun.0.1)->tunnel source 1.1.1.1
RouterA(su-config-tun.0.1)->tunnel destination 1.1.1.2
RouterA(su-config-tun.0.1)->ip address 10.1.1.1/30
```

```
RouterB(su-config-tun.0.1)->tunnel source 1.1.1.2
RouterB(su-config-tun.0.1)->tunnel destination 1.1.1.1
RouterB(su-config-tun.0.1)->ip address 10.1.1.2/30
RouterB(su-config-tun.0.1)->no shutdown
RouterB(su-config-tun.0.1)->exit
```



123


409