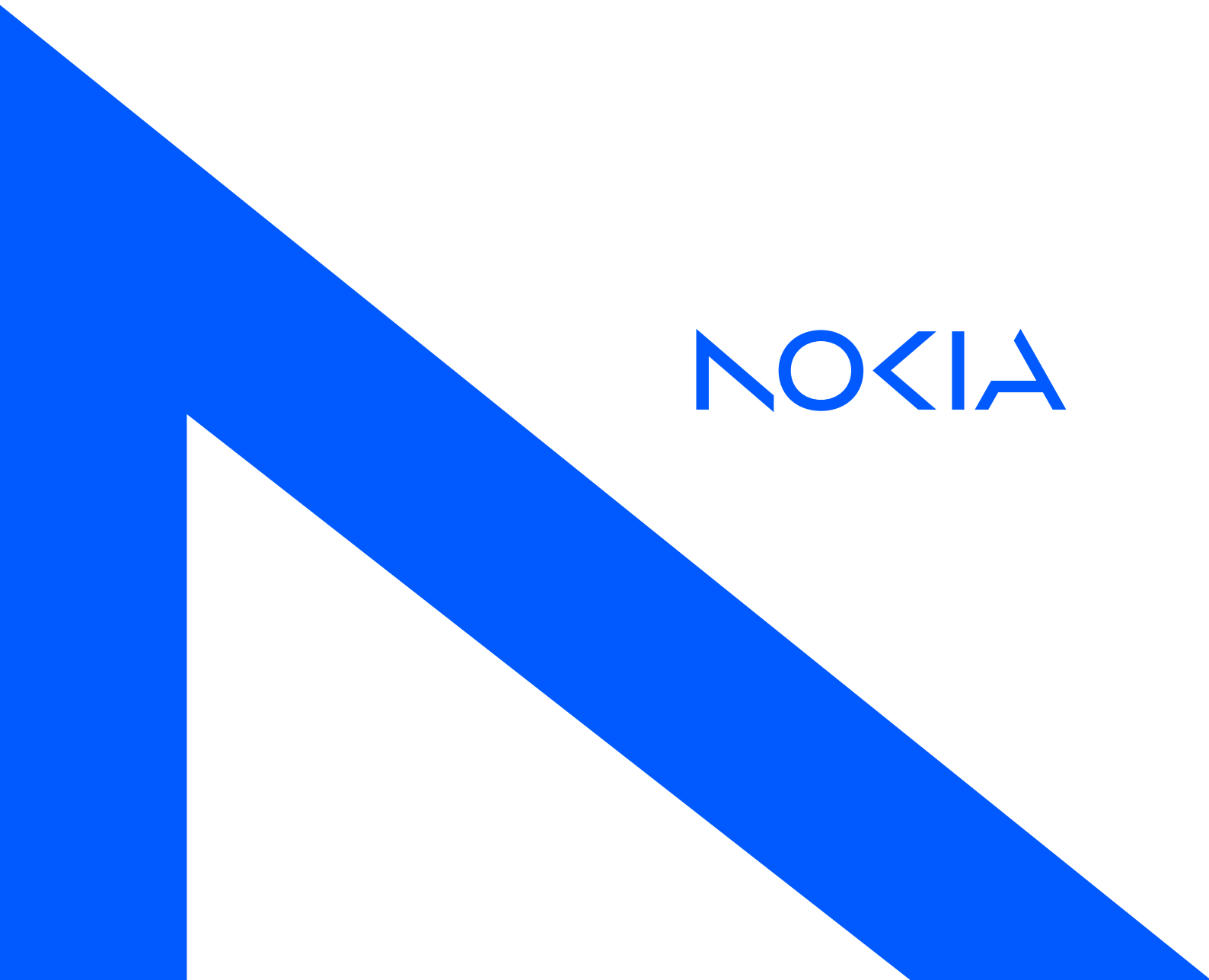
Ethernet Virtual Private Networks on Nokia routing platforms

Delivering a solid virtual private network infrastructure

Application note



Contents

EVPN: the need and the opportunity

The virtualization of network infrastructure must respond to increasingly stringent criteria from many sectors. Virtual Private Networks (VPNs) must scale massively in both capacity and reach. They must be secure, efficient and resilient, and able to be rapidly instantiated, assured and torn down to support dynamic workloads and microservice chains across multiple domains. Operational management must be intuitive, consistent and highly automated across the lifecycle.

Ethernet VPN (EVPN) has evolved to be the right technology to meet these criteria and support a growing set of use cases in virtual networking, effectively and efficiently.

While services such as virtual private LAN service (VPLS) and Provider Backbone Bridges (PBB) may be viewed as somewhat mature technologies for Ethernet services, they do have shortcomings:

- Reliance on flooding and learning to build the Layer 2 forwarding database
- Burdensome static configuration in the absence of a dynamic control plane
- Scalability challenges
- Limited multi-homing capabilities
- Lack of fundamental operational automation

Ethernet Virtual Private Network (EVPN) has evolved to address these criteria and more, and can support an expanding set of use cases in virtual networking, effectively and efficiently.

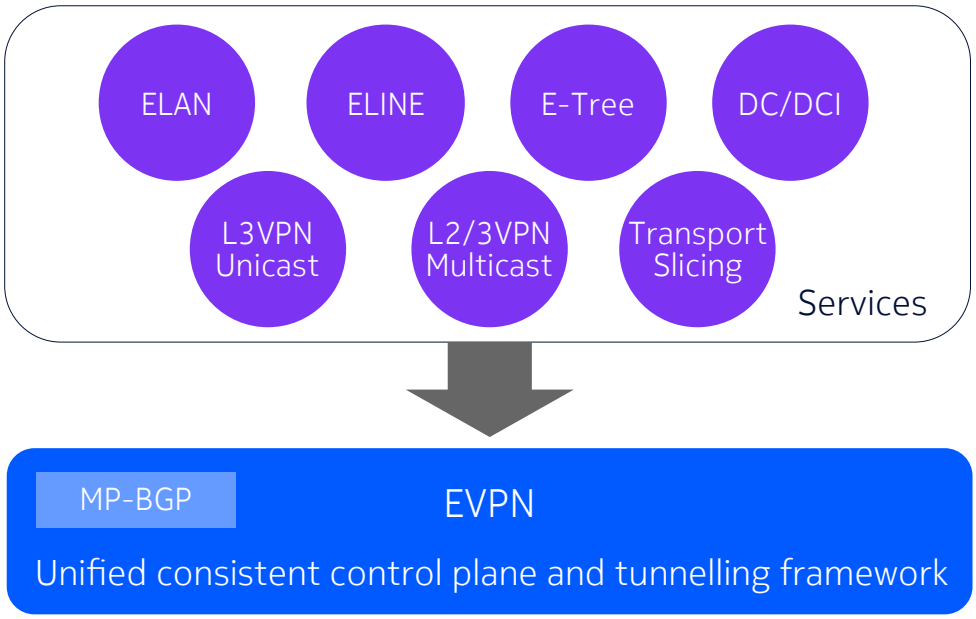
EVPN introduces a new Ethernet services delivery model that:

- Inherits a decade of VPLS operational experience in production networks
- Incorporates flexibility for service delivery over Layer 3 networks
- Abstracts and separates the control and data planes:
  - In the control plane, Multiprotocol Border Gateway Protocol (MP-BGP) carries Media access control/ Internet Protocol MAC/IP routing information.
  - Supports a choice of data plane encapsulation depending on application and preference.

EVPN enables network operators to address a broad set of current and emerging use cases in their networks, including:

- Layer 2 and 3 services
- Internet exchange point networks (IXPs)
- Data center networks
- Data centre interconnect
- Mobile transport networks
- SD-WAN networks
- Enterprise, industry and public sector networks
- Research and education networks

Figure 1. Unified service delivery: reducing operational complexity, increasing profitability



A high-level summary of EVPN benefits

This table provides an overview of some of the most important benefits of EVPN. Many of these benefits are in the areas of efficiency, scale, security and resiliency. These benefits translate into opportunities to improve profitability and address revenue opportunities across a comprehensive range of market segments, with a more flexible, operationally consistent and rapidly deployable solution set.

Need or issue with legacy VPNs	EVPN feature to address this need or issue	Benefit to network owner and/or user
Basic flooding and learning of MAC addresses leads to a high impact of broadcast traffic, as well as unknown unicast and multicast (BUM) traffic.	MP-BGP update control messages for autodiscovery (AD) and address advertisement greatly reduce flooding in the network.	Improved scaling beyond the limits of legacy VPNs and lowered resource consumption leading to improved energy efficiency and reduced capital expense for supporting a given service load.
Weak multi-homing capabilities.	Powerful and flexible single-active and all-active multihoming with automation, manual features and transient loop prevention.	Improved resiliency for users and applications brings improved uptime and increases user satisfaction. Better utilization of link groups into central sites brings benefits such as improving the return on capital investment.
Multiple protocols and control plane types are required to support a range of services across Layer 2, Layer 3 and multicast networks.	Consolidation and simplification on a unified MP-BGP control plane (with strong policy) for building Layer 2 and Layer 3 VPNs for a range of CSP and data center services with a variety of data plane encapsulations.	Reduced training requirements lower OPEX. Improved reliability and resiliency enabled by a focused, constrained knowledge base and tool suite for network operations, lead to increased availability for end-user services.
Time-consuming, often manual, operations are required to configure the network across the lifecycle of service.	Automation is built into EVPN from its inception. EVPN has auto-configuration capabilities that greatly reduce the need for manual configuration.	Day-to-day OPEX is reduced by the simplicity and automation capabilities of EVPN. Rapid, automated service lifecycle operations can unlock new use cases.
Service interruption in moving physical or virtual hosts.	Seamless host and virtual machine mobility.	Workloads can be moved dynamically as needed, bringing improved uptime for end-user applications.
Load balancing limitations.	Aliasing provides load balancing across multi-homed ethernet links.	Maximized bandwidth utilization in data center fabric reduces CAPEX.
Slow convergence on link/node failure as many routes are withdrawn.	Mass withdrawal capability for rapid convergence on link failure.	Improves service availability as the network adapts rapidly to its new state.
Prone to excessive Address Resolution Protocol and Neighbor Discovery (ND) traffic and malicious ARP/ND spoofing attacks.	Proxy ARP/ND reduces ARP/ND traffic and eliminates ARP/ND spoofing attacks. This addresses a scalability issue and a security issue.	Removal of a security exposure leads to better service availability. Alleviating the ARP/ND load on attached routers can improve overall performance,
WAN and data center separation.	WAN and data center integration for seamless services and consistent operations.	Consistent practices and skillsets across the end-to-end solution can reduce operational expenses and boost service uptime.

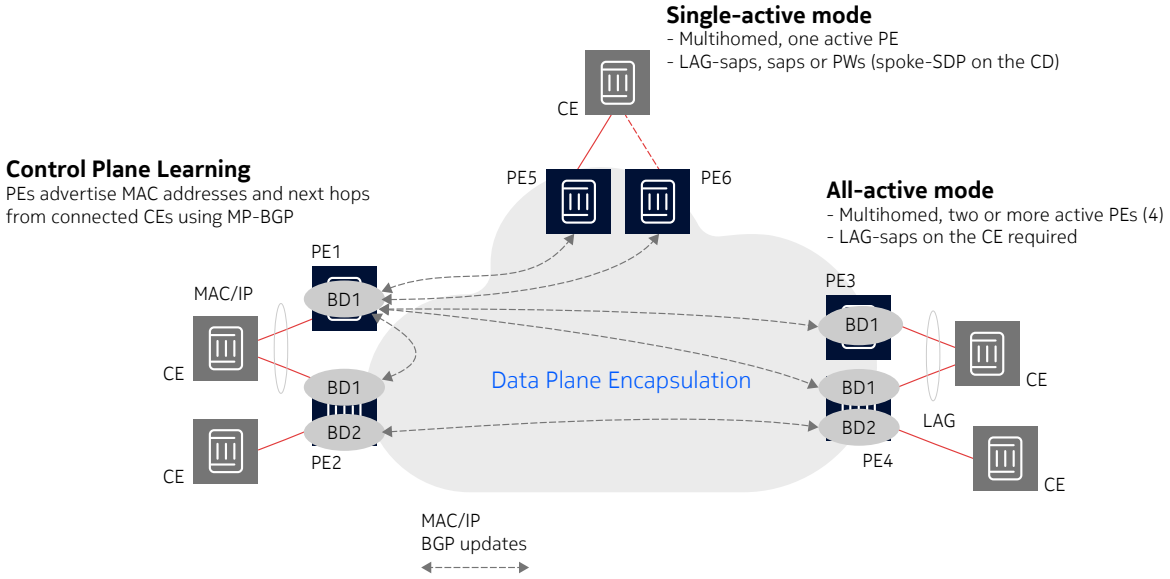
An introduction to EVPN technology

EVPN is a next-generation VPN solution that provides a unified architecture in both the control and data planes to support a broad range of business VPN services and network infrastructure use cases. This section provides a brief overview of some of the principal architectural features of EVPN.

The EVPN control plane is founded upon MP-BGP, which allows network reachability information such as Layer 2 MAC addresses and Layer 3 IP addresses to be efficiently signalled across the network.

EVPN provides resiliency via an all-active multihoming model, keeping traffic flowing even under failure conditions. In the data plane, a range of tunneling options are available, including MPLS or virtual extensible LAN (VXLAN). This unified, consistent architecture supports a wide range of networking use cases. Figure 2 shows some of the important concepts in EVPN.

Figure 2. Principal architectural concepts of EVPN



Control plane learning

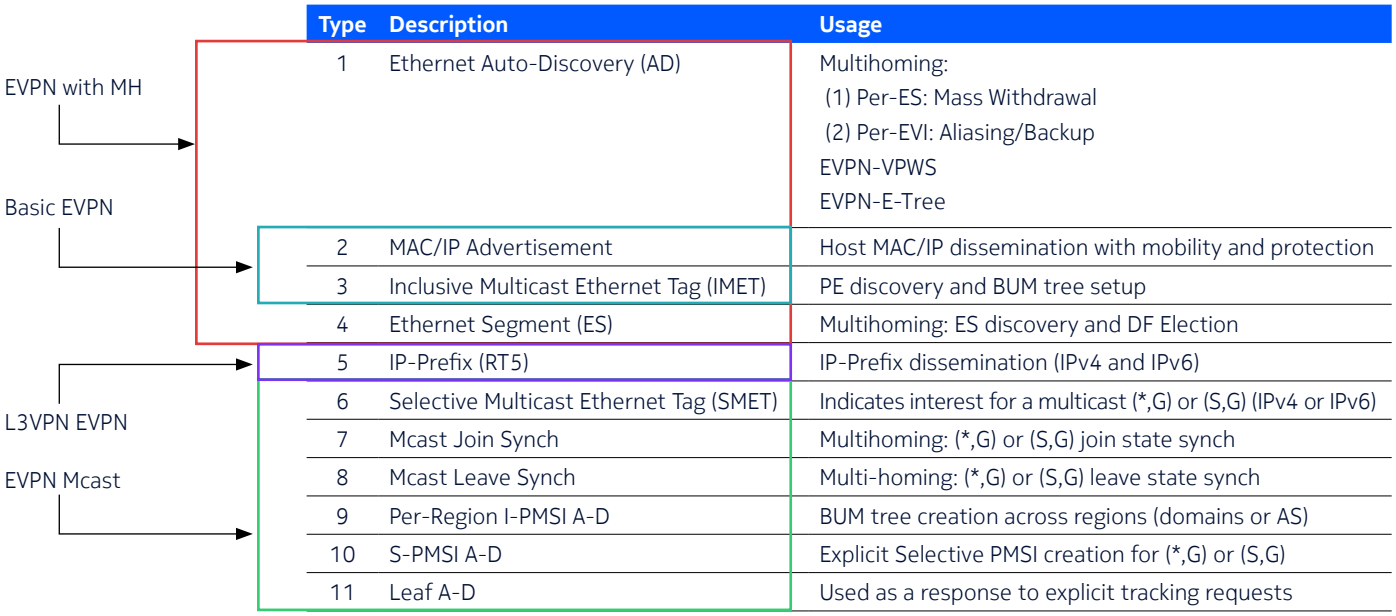
The efficient learning and distribution of address reachability is crucial in any data network. In the EVPN architecture, MAC address learning at the Provider Edge (PE) still happens in a conventional manner as Ethernet frames are seen on the locally connected media to the Customer Edge (CE). However, the multiprotocol extensions to BGP (MP-BGP) for EVPN enable the efficient, and massively scalable, distribution of addresses over the network using control messages. EVPN peers share locally learned MAC address information using MP-BGP messages to enable remote address learning. MP-BGP thus allows the efficient construction and operation of overlay VPNs on the routed infrastructure of the network.

As shown in figure 2, BGP update messages are used to advertise learned MAC addresses and next hops between PEs that support a common broadcast domain. The EVPN control plane uses local and remote learning to build a comprehensive, distributed view of the overlay virtual network in terms of Layer 2 MAC reachability. This control message-based approach is much more efficient and scalable than relying on the traditional flooding of unknown traffic. In addition, this approach can be extended to enable many high-value capabilities in the network. These include Layer 3 VPNs, multihoming and multicast services.

Route Types

Route Type is a key concept in the control plane. MP-BGP for EVPN supports a range of Route Types, as shown in Figure 3.

Figure 3. EVPN MP-BGP Route Types



Type	Description	Usage
1	Ethernet Auto-Discovery (AD)	Multihoming: (1) Per-ES: Mass Withdrawal (2) Per-EVI: Aliasing/Backup EVPN-VPWS EVPN-E-Tree
2	MAC/IP Advertisement	Host MAC/IP dissemination with mobility and protection
3	Inclusive Multicast Ethernet Tag (IMET)	PE discovery and BUM tree setup
4	Ethernet Segment (ES)	Multihoming: ES discovery and DF Election
5	IP-Prefix (RT5)	IP-Prefix dissemination (IPv4 and IPv6)
6	Selective Multicast Ethernet Tag (SMET)	Indicates interest for a multicast (*,G) or (S,G) (IPv4 or IPv6)
7	Mcast Join Synch	Multihoming: (*,G) or (S,G) join state synch
8	Mcast Leave Synch	Multi-homing: (*,G) or (S,G) leave state synch
9	Per-Region I-PMSI A-D	BUM tree creation across regions (domains or AS)
10	S-PMSI A-D	Explicit Selective PMSI creation for (*,G) or (S,G)
11	Leaf A-D	Used as a response to explicit tracking requests

BGP updates can perform different roles. The role being performed is indicated by the Route Type.

Basic Layer 2 EVPN (RT-2 and RT-3)

Route Types 2 and 3 are fundamental to the construction of a Layer 2 VPN on top of a Layer 3 (routed) infrastructure.

Route Type 3 (Inclusive Multicast Ethernet Tag, or IMET) is a good place to start in examining Route Types because it plays a fundamental role in establishing the structure of the VPN on the network infrastructure. This includes the discovery of the VPN components at the PE and the construction of trees for the distribution of BUM traffic.

RT-3 advertises information such as:

- VPN participation
- Tunnel type
- Encapsulation type

EVPN speakers at the PE use RT-3 to advertise, to their EVPN peers across the network, the VPNs in which they wish to participate. Referring to Figure 2, each of the EVPN speakers identified as BD1 will (as necessary) send MP-BGP updates to all peers to establish the VPN. Following this, BUM traffic will be forwarded to only those EVPN peers that are members of the appropriate VPN. Thus, RT-3 removes the need for a lot of unscalable static configuration. It also ensures that BUM traffic only goes to peers that should see it and it dynamically establishes the datapath tunnel infrastructure.

Route Type 2 (MAC/IP advertisement) is used for the distribution of MAC addresses (and optionally associated IP addresses) to populate forwarding tables and suppress broadcast flooding. MAC addresses are learned locally at the PE via conventional data plane traffic learning mechanisms. These MAC addresses are then advertised in MP-BGP updates (with Route Type 2) to the EVPN peers. This control plane mechanism scales in a linear fashion along with network growth. MP-BGP advertises MAC addresses (and possibly associated IP addresses) for next-hop resolution across the network with EVPN Network Layer Reachability Information (NRLI).

This control plane approach using RT-2 MP-BGP updates enables several powerful features that add value to MAC learning:

- Filtering policies can be applied.
- Virtualization and isolation of EVPN instances are possible using the route target community to control the import and export of routes.
- Traffic load balancing becomes possible for multi-homed CEs with Equal Cost Multiple Path (ECMP) MAC routes.

Route Type 2 is supported by all EVPN switches and routers and is described in RFC 7432: BGP MPLS-Based Ethernet VPN.

Layer 3 VPN (RT-5)

While RT-2 allows Layer 2 VPN, to be constructed based on MAC addresses, RT-5 uses IP prefix advertisement to enable support for Layer 3 VPNs. RT-5 routes enable the decoupling of the advertisement of an IP address prefix from a MAC address binding. In RT-2, by contrast, any IP addresses are bound to corresponding MAC addresses. RT-5 is used for IP prefix advertisements with interface-ful and interface-less models.

As in traditional IP VPNs there is an IP Virtual routing and forwarding (VRF) function on PE routers for each Layer 3 overlay VPN. PEs exchange MP-BGP updates carrying IP prefixes. These prefixes are installed in VRFs to establish overlay Layer 3 VPNs. Associated route targets can trigger the application of appropriate policy information.

For more detail on this and other EVPN topics in a video format, see Nokia TechTalks- EVPN Route Types

Multihoming (RT-1 and RT-4)

One of the most important aspects of the development of EVPN is the creation of a robust and feature-rich multihoming capability while maintaining backwards compatibility with less-capable legacy VPN approaches. EVPN uses its MP-BGP control plane to implement this comprehensive multihoming capability.

Referring to Figure 2, the EVPN architecture supports two principal modes of multihoming, single-active (SA) and all-active (AA). SA multihoming has only one active PE at a time and supports link aggregation group (LAG) or pseudowire to the CE. In AA multihoming, there can be two or more active PEs, up to a maximum of four, operating over LAG to the CE. The set of links that connect the CE to the PE are collectively known as the Ethernet segment (ES). In keeping with the flexible nature of EVPN, an ES on a PE can be comprised of several transport types: LAG, port, MPLS tunnel, QinQ or VXLAN instance. Links within the ES can be physical or virtual. Load balancing of flows to PEs is accomplished using ECMP and is known as aliasing.

Multihoming operations can be fully automated or proceed under manual control as desired. An elected designated forwarding (DF) PE handles the flooding of BUM traffic to the ES , avoiding potential duplication. The use of split-horizon prevents loops by ensuring that BUM traffic sent from the CE to the non-DF PE is not replicated back to the ES.

Mass withdrawal of routes is another great scaling advantage of EVPN in multihoming. A BGP control message (RT-1) accomplishes this very efficiently compared to the torrent of MAC flush messages generated in legacy VPLS. This presents scaling issues in terms of message processing and convergence times.

For more detail on this and other EVPN topics in a video format, see Nokia TechTalks - EVPN multi-homing: an open alternative to MLAG

Data plane encapsulation

The data plane is concerned with the forwarding of packets. Traffic is identified and shared among VPN peers and encapsulated with a tunnel label or labels across a common core infrastructure. In communications service provider (CSP) deployment, the tunnel types are typically MPLS. In a data center or campus network, VXLAN is often used for the data plane. Segment routing (SR) is attracting increasing interest as a tunneling technology. SR is efficient and deterministic, and offers traffic engineering and policy advantages.

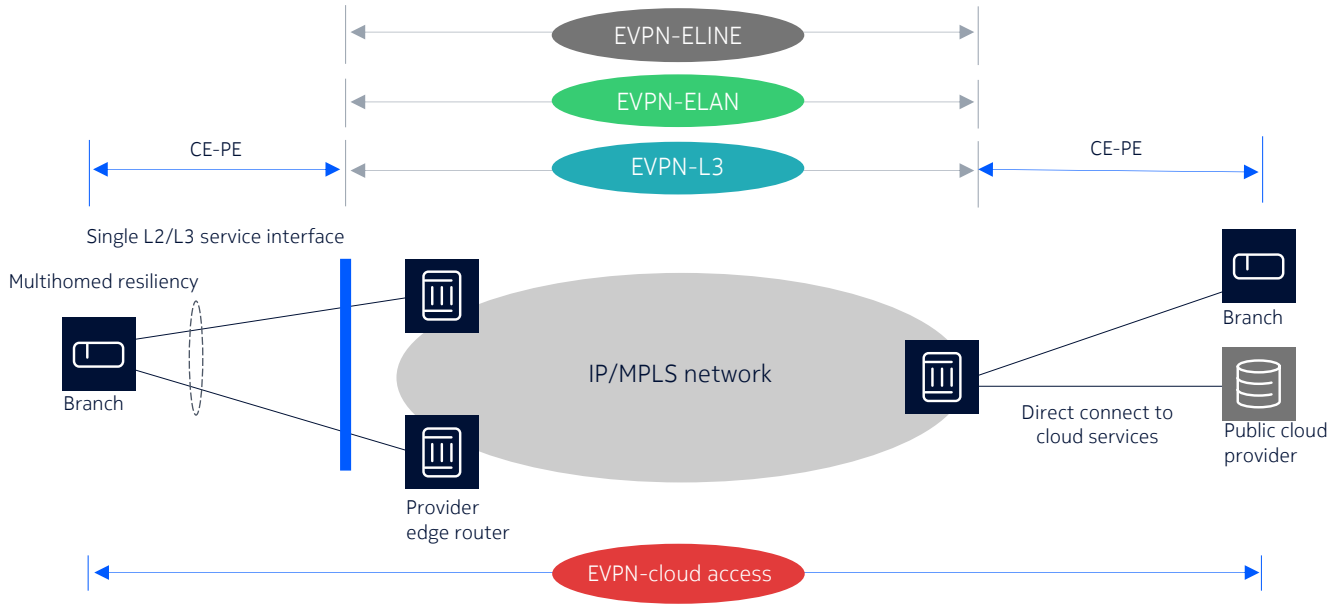
Key EVPN use cases

The advanced features of EVPN provide CSPs, and network operators generally, with the ability to offer improved solutions to their customers and address new and emerging market segments. The following sections describe some of the key use cases supported by EVPN.

Layer 2 and 3 services

Service providers can use the EVPN control and data plane architecture to offer a broad range of integrated Layer 2 and Layer 3 business services, as shown in Figure 4. Services such as ELAN, ELINE and E-Tree, along with Layer 3 IP VPN services such as unicast and multicast offerings, are all supported with a robust, consistent, simplified and feature-rich operational model.

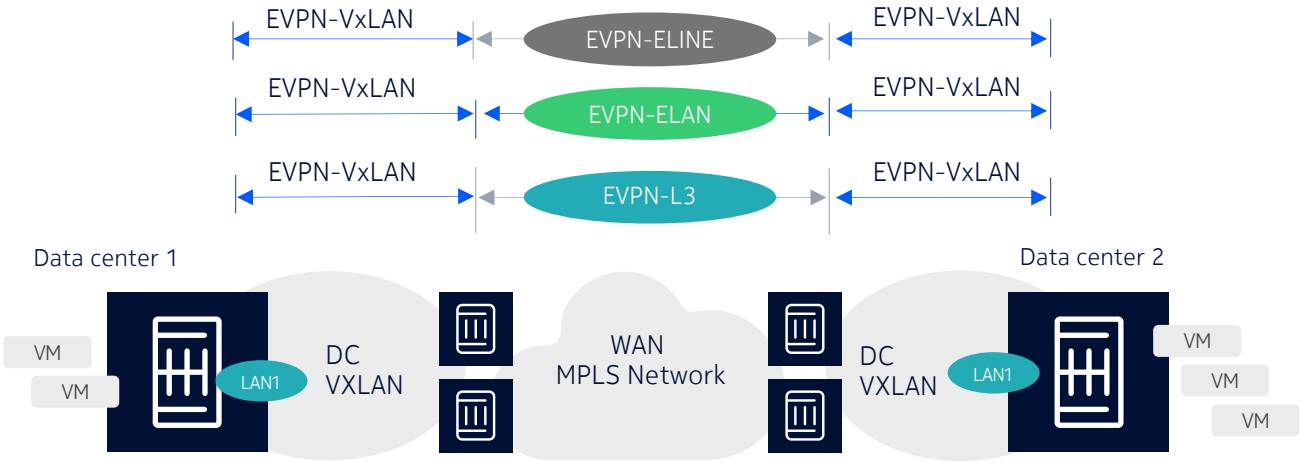
Figure 4. Layer 2 and Layer 3 services



Data center and data center interconnect networks

EVPN infrastructure is ideal for the construction of a powerful, reliable and flexible data center network fabric, and its load balancing capabilities maximize bandwidth utilization. EVPN is common to the data center and WAN, ensuring seamless, unified connectivity from end to end as shown in Figure 5. It enables scalable Layer 2 or Layer 3 connectivity with a common control and data plane and virtualized data centers. The ability to move hosts and virtual machine-based workloads using IP/MAC mobility dynamically and seamlessly delivers excellent availability and service quality and allows data center compute resources to be used efficiently. Consistent practices and skillsets across the end-to-end solution from the data center into the WAN bring reduced OPEX.

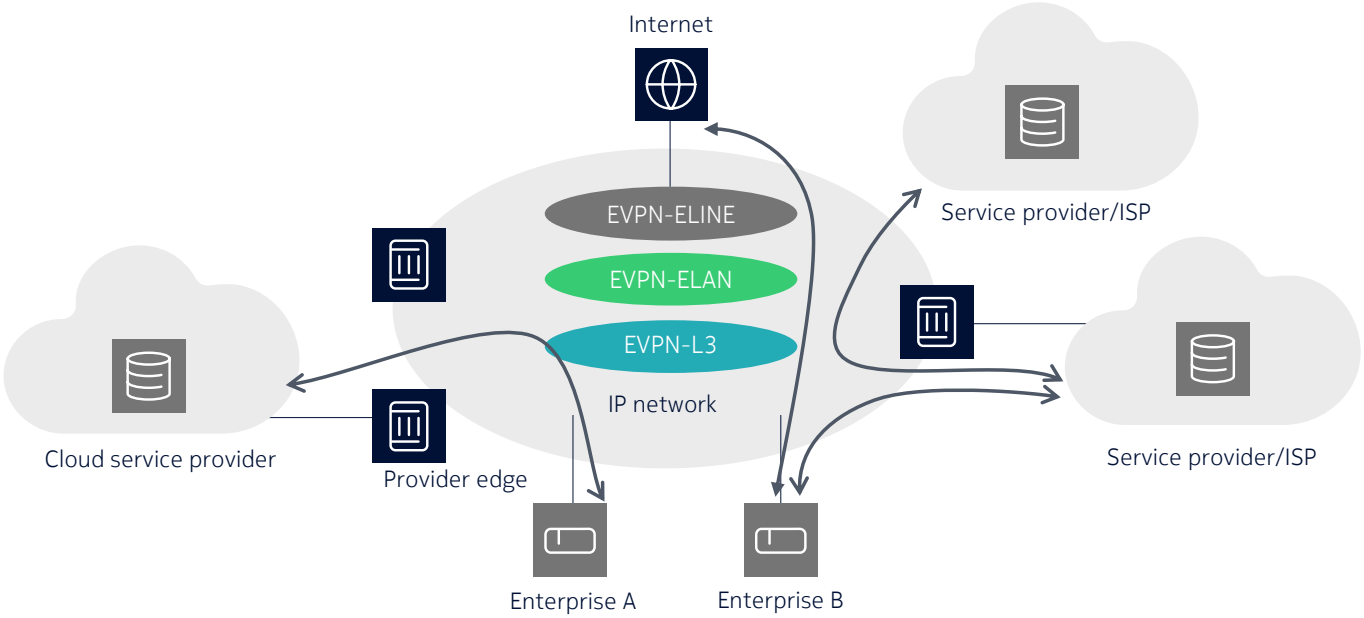
Figure 5. Data center and data center interconnect networks



Internet exchange point networks

IXPs can deliver high capacity, reliable and secure interconnection capability to bring together the infrastructure of the internet over an EVPN peering fabric. Single or all-active multihoming can be supported to the peering fabric VLAN. Specific features to suppress unwanted and possibly malicious ARP and ND traffic are built into EVPN, further contributing to the smooth and secure operation of internet services over a clean and secure peering fabric.

Figure 6. Internet exchange point networks (IXPs)



Mobile transport networks

The evolving mobile transport network must be efficient and secure. As mobile transport slicing is deployed, it will be increasingly important to be able to rapidly instantiate, modify, monitor and tear down transport slices. EVPN is the perfect solution for transport slicing. Its built-in automation characteristics enable efficient operations.

SD-WAN networks

SD-WAN controllers, which guide and inform the overlay data plane, can use BGP EVPN peering to efficiently advertise network addresses at Layer 2 and Layer 3.

Enterprise, industry and public sector networks & research and education networks

Many of the features that make EVPN attractive for CSPs are also highly beneficial in crucial enterprise, industry, research and public sector networks. These include operational consolidation and simplification, efficient resource consumption, and strong resiliency and reliability via powerful multihoming.

Nokia support for EVPN

EVPN is a common network routing application supported across the Nokia IP networks portfolio. Nokia began investing in EVPN in 2014 and offers a robust, comprehensive suite of service capabilities that have been deployed and validated by many network operators for a variety of applications. The company has been extremely active in the standardization of EVPN functionality within the Internet Engineering Task Force (IETF) and has led or contributed to many of the initiatives that have brought EVPN to the level of sophistication and breadth of utility seen today.

The progression of Nokia EVPN

Nokia has done extensive development work on EVPN capabilities. While by no means exhaustive, the following sections show the cumulative growth in capability of EVPN within the Nokia IP networks portfolio across all targeted applications.

EVPN for Cloud and Data Center Gateways : Universal Data Center Gateway functionality

EVPN-VXLAN (including VXLANv6) with VXLAN-to-VPLS gateway capability and EVPN to virtual private wire service (VPWS). The IP networks portfolio supports Layer 2 and integrated routing and bridging (IRB) with asymmetric and interface-ful IRB, assisted replication and host routing.

EVPN for WAN networks: Metro Ethernet Forum Services

EVPN-MPLS, including multihoming, EVPN-to-VPLS interworking and EVPN-to-VPWS interworking. The IP networks portfolio also supports PBB on EVPN, plus PBB E-tree and EVPN-E-tree. Proxy Address resolution protocol (ARP)/Neighbour discovery (ND) and Interior Gateway Protocol (IGMP) snooping are also supported.

EVPN Cloud-WAN integration: Hyper scale and tight integration with SR and SR-Policy

EVPN-VXLAN/MPLS, including virtual ESs with loop protection and enhanced security.

EVPN: The grand unified VPN service: Moving all VPN services to EVPN

- Complete Layer 2 service
- Layer 3 services (IP VPN)
- Layer 2 and Layer 3 comprehensive multicast including Optimized Inter-Subnet Multicast (OISM) and Protocol Independent Multicast (PIM)
- SR v6 services:
  - EVPN VPWS SRv6, EVPN IP prefix routes in interface-less mode for SRv6, EVPN ELAN (and multihoming), EVPN compressed segment identifiers (SIDs).
  - Service Gateway (MPLS-SRv6)
  - MPLS or SRv6 PW-Headend
  - EVPN ELAN MPLS-SRv6 GW
  - EVPN IFL MPLS-SRv6 GW and D-PATH

EVPN Layer 3 smart forwarding:

- EVPN Unequal ECMP
- EVPN IP Aliasing

Hardware platforms

EVPN functionality is available across a range of Nokia platforms, from compact, 1RU devices such as the Nokia 7250 IXR-e series to the high-scale Nokia 7750 SR-14s. These platforms provide capacities and form factors to suit any point of presence or installation. The Nokia Data Center Fabric solution includes the Nokia 7250 IXR-6e/10e, the 7250 IXR-6/10, the Nokia 7220 IXR-H series and the Nokia 7220 IXR-D series of interconnect routers. These platforms are designed for the leaf and spine layers of data center fabrics, delivering high-scale interconnectivity for data center and cloud environments.

Automation

EVPN requires a programmable, network automation framework environment targeted for IP networks today and into the future as the network extends from the wide area into centralized and distributed clouds. EVPN is ideally suited to deployment in a NetOps-based, model-driven environment. It can accelerate network operations through ready-to-use Nokia applications for automating the management of the entire network and services lifecycle.

Automation must contribute to the secure, efficient and resilient operation of the network. It must allow services to be rapidly instantiated, assured and deleted as needed to support dynamic workloads and microservice chains across multiple domains.

Summary

EVPN has become the VPN technology of choice outside and inside the data center.

Interest in EVPN originally arose because network architects and operators were looking for an efficient way to provide intra- and inter-subnet forwarding, along with all-active multihoming in data centers. Later, it was found that EVPN could resolve the same and many other issues in the WAN for CSPs deploying Metro Ethernet Forum services (E-LAN, E-LINE, E-Tree, etc.). EVPN also supports comprehensive solutions for Layer 3 VPNs and highly efficient Layer 2 and Layer 3 multicast networking.

Nokia has shown leadership in EVPN standardization and pragmatic application of EVPN technology in some of the most demanding networking environments globally. The success of these deployments best demonstrates the technological and commercial superiority of EVPN.

Abbreviations

AD	Autodiscovery
ARP	Address Resolution Protocol
BD	broadcast domain
BGP	Border Gateway Protocol
BUM	broadcast, unknown-unicast and multicast
CE	Customer Edge
DCI	data center interconnect
ECMP	equal cost multiple paths
ES	Ethernet segment
EVPN	Ethernet VPN
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IMET	Inclusive Multicast Ethernet Tag
IRB	integrated routing and bridging
LAG	link aggregation group
MAC	media access control
MEF	Metro Ethernet Forum
MP-BGP	Multiprotocol Border Gateway Protocol
MPLS	Multiprotocol Label Switching
ND	Neighbour Discovery
NLRI	network layer reachability information
NSP	Network Services Platform
OISM	Optimized Inter-Subnet Multicast
OSPF	Open Shortest Path First
PBB	Provider Backbone Bridge
PE	Provider Edge
PIM	Protocol Independent Multicast
RR	route reflection
SR	Service Router
SR OS	Service Router Operating System
SRL	Service Router Linux
SRLG	Shared Risk Link Group
SR-MPLS	segment routing for MPLS
SR-TE	segment routing – traffic engineering
SRv6	segment routing for IPv6
VPLS	virtual private LAN service
VPWS	virtual private wire service
VRF	virtual routing and forwarding
VXLAN	virtual extensible LAN
WAN	wide area network

Principal standards

RFC 7432	BGP MPLS-based Ethernet VPN
RFC 7623	PBB-EVPN
RFC 8214	EVPN-VPWS
RFC 8317	EVPN E-Tree
RFC 8560	Seamless Integration of EVPN with VPLS and PBB-VPLS, needed for migration
RFC 8584	Framework for DF Election extensibility, defines AC-influence DF Election
RFC 9161	Proxy-ARP/ND full specification
draft-ietf-bess-evpn-pref-df	Preference and non-revertive DF Election

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID213310 (May)