CLOUD NETWORKING FOR ENTERPRISE CAMPUS

APPLICATION NOTE

Alcatel·Lucent Enterprise

EXECUTIVE SUMMARY

This application note proposes Virtual Extensible LAN (VXLAN) as a solution technology to deliver departmental segmentation, business unit isolation and transparent subnet extensions over existing enterprise campus networks.

Today's legacy campus networks are difficult to expand because they suffer from VLAN sprawl and are based on complex combinations of Multiprotocol Label Switching (MPLS) and single or double VLAN tagging.

Using carrier-class technology like MPLS in the enterprise LAN creates challenges. MPLS is neither dynamic nor flexible, its complexity and reliability are costly in CAPEX and OPEX, and it is difficult to find MPLS experts who understand the enterprise needs. Alcatel-Lucent Enterprise provides a VXLAN Layer 2/Layer 3 VPN solution that fits the enterprise needs and delivers agile value-added services, while simplifying the transformation of the campus networks to meet user needs. This solution requires no MPLS expertise, keeps the deployment simple and requires minimal or no administrative intervention or changes to the network backbone.

This approach streamlines the delivery of campus network services by operating as a virtualized cloud to ensure rapid provisioning and provide excellent backbone stability for 100 percent uptime. These capabilities are available at minimal or no cost to the enterprise and take advantage of current staff expertise. The result is a resilient and transparent physical infrastructure that can deliver dynamic turnkey services to the enterprise users with the agility of a cloud infrastructure provider.

CHALLENGE

Enterprises, such as hospitals, universities, airports, as well as city networks benefit from hosting a variety of network services for different groups over a single physical infrastructure that delivers multi-tenant services through network virtualization abstractions. Services available with this infrastructure include Layer 2 and Layer 3 multi-tenancy, security zones, bridge extensions, routing domains, and data center interconnections.

The following are some of the most common use cases in the enterprise.

- Departmental segregation: In some enterprises, different business units manage their own IP addressing space, VLANs, routing, security, and so on. This may be the result of a merger, or caused by the organizational structure; for example, different schools in a university or multiple hospitals in a health system. The IT organization acts as a service provider for the individual business units by configuring Layer 2 and Layer 3 VPNs. These VPNs provide isolation, so that these individual networks don't conflict with each other, and abstraction, so that IT and the business units need not be concerned with changes outside of their administrative domain.

  Virtualized networks offer protection for the infrastructure. A design principle for any network is to secure the physical infrastructure, which can be easily done with VPNs by encapsulating all traffic for the departments or business units and transporting the encapsulated traffic transparently through the core. This limits the exposure of the core network to traffic on the subnets of the business units. Each business unit can communicate within its tenancy without firewalls, and can communicate when needed with other business unit networks through firewalls.

- Subnet extension: Sometimes, it becomes necessary for subnets to extend across the campus to support devices or applications that rely on Layer 2 connectivity. In a case like this a Layer 2 VLAN extension is required to ensure privacy and isolation. This may be the case, for example, in a hospital with biomedical devices such as patient monitors and infusion pumps. Commonly there are hundreds of VLANs, including private VLANs and research VLANs, that have to extend from the data center to multiple buildings or from external locations to multiple buildings.

  Take, for example, radiology: the MRI, CAT scan and x-ray machines are all on one network with the server. The only way out of that network is through a firewall. There are machines in every hospital, on most floors, and some are mobile. The server is in one data center and the firewalls could be in another one. As a result, that one subnet has to extend to every building and data center through the core over the same routed links used by other subnets.

  Simple VLAN tagging can deliver this outcome, however, at the expense of creating large Layer 2 domains that become part of the backbone, which can lead to stability, scalability and performance problems (for example, large spanning trees, broadcasts, MAC learning). By contrast, Layer 2 VPNs can be used to extend subnets where required, while isolating the network from these issues.

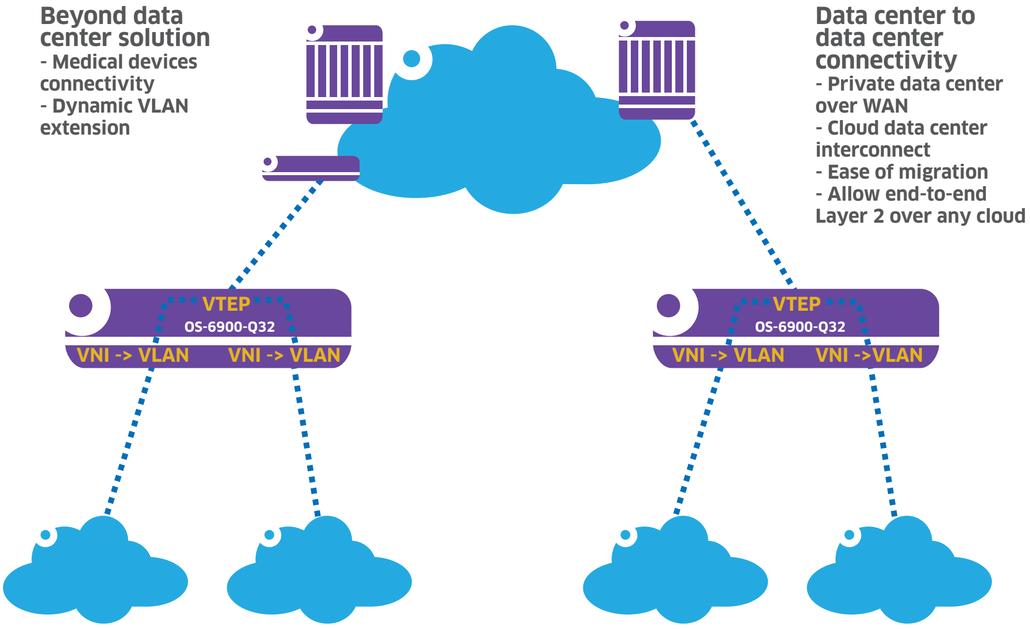
SOLUTION

The Alcatel-Lucent Enterprise Operating System (AOS) supports automated service delivery for secured authenticated Layer 2 and Layer 3 VPNs using network virtualization technologies, such as VXLAN and device virtualization through a high-availability virtual chassis.

VXLAN is an encapsulation technology defined by IETF for tunneling Layer 2 VPNs over a Layer 3 backbone. VXLAN has been enhanced by Alcatel-Lucent Enterprise to support inter-VPN routing, service visibility and policy control in the hardware.

The solution focuses on using VXLAN to create network segments overlaid on top of Layer 2 or Layer 3 campus networks. Each VXLAN network segment is independent of the underlying campus network, which may be based on a routed corporate network with arbitrary VLAN boundaries.

Figure 1: VXLAN simplifies the enterprise network


Beyond data center solution
- Medical devices connectivity
- Dynamic VLAN extension
Data center to data center connectivity
- Private data center over WAN
- Cloud data center interconnect
- Ease of migration
- Allow end-to-end Layer 2 over any cloud
VTEP
OS-6900-Q32
VNI -> VLAN
VNI -> VLAN
VTEP
OS-6900-Q32
VNI -> VLAN
VNI ->VLAN

VXLAN was originally developed for data centers' server-to-server connectivity. It encapsulates the original Ethernet frame by adding a VXLAN header and uses User Datagram Protocol / Internet Protocol (UDP/IP) for transport. The VXLAN Tunneling Endpoints (VTEPs) can be implemented on the switch hardware or vSwitch software bridge. An Alcatel-Lucent OmniSwitch® acting as a VTEP gateway can bridge (or route) between different VXLAN segments and standard VLANs to extend Layer 2/Layer 3 environments transparently over the routed network.

Each VXLAN segment is identified by a 24-bit field, known as VXLAN Network Identifier (VNI), allowing up to 16 million VXLANs compared to 4000 VLANs in 802.1Q. Like in VLANs, the OmniSwitch VTEP performs data plane source learning and orchestrated learning.

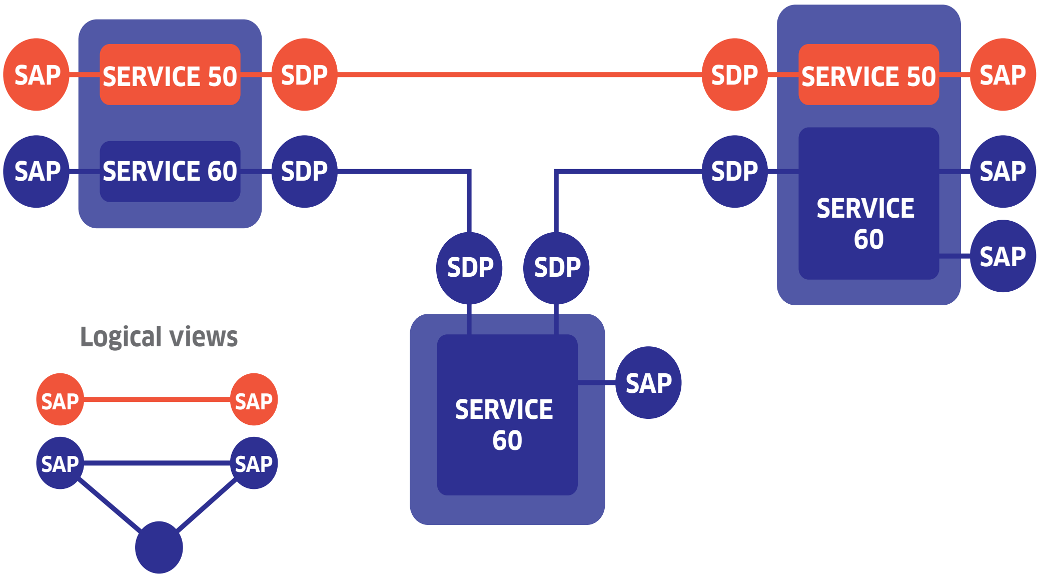
VXLAN support in the Omniswitch is provided under the AOS service manager as either a head-end or tandem service that is designed for carrying unicast, unknown destination, broadcast, and multicast frames by mapping the destination MAC address to the remote VTEP.

The user or device access into the VTEPs can be controlled by AOS Universal Network Profiles (UNP) and Learned Port Security (LPS) features. UNPs are network policy containers where the administrator defines authentication (MAC-auth or 802.1X) policies, device classification (MAC, tag/double-tag ID, IP host/subnet or combinations) policies, access list policies, quality of service policies, quality assurance policies and application fingerprinting policies.

The AOS VXLAN service consists of the following components:

- Access Port: a port where the user traffic ingresses or egresses.
- Service: a bridging domain for user traffic represented as VXLAN ID when routed over the network.
- Service Access Point (SAP): a virtual port where the user traffic ingresses the service as untagged, tagged, or double-tagged.
- Service Distribution Point (SDP): service binding to the far-end node (Unicast SDP) or a group of far-end nodes (Multicast SDP) to which the encapsulated tunnel traffic is directed.

Figure 2: VXLAN service configured with AOS SAP and SDP constructions



The access port can be configured on a fixed port or a link aggregation group. The administrator can specify how to handle (drop, peer and tunnel) the Layer 2 control packets (for example, STP, LLDP, AMAP, GVRP, MVRP) accessing the access port and egress VLAN translation policies.

The administrator can specify the multicast mode used for broadcast, unknown unicast and multicast (BUM) traffic:

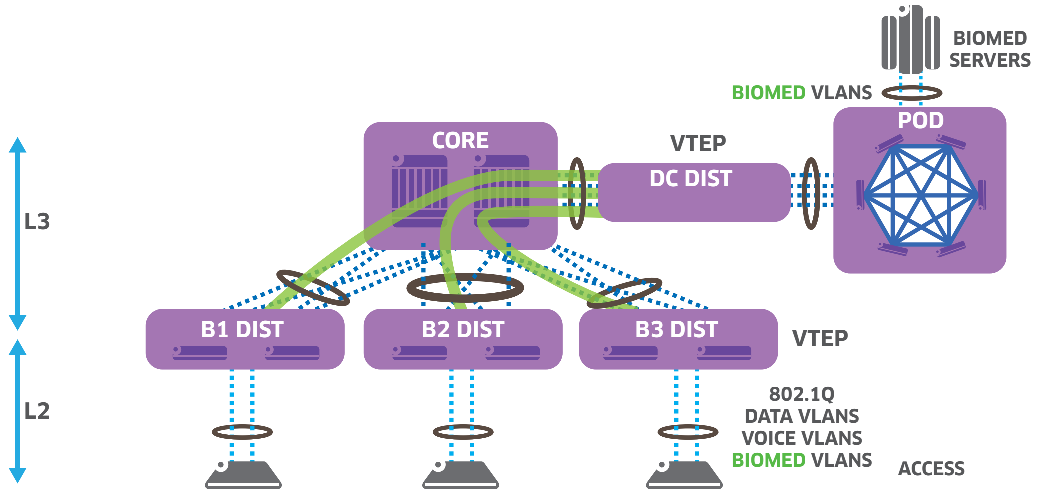
- Tandem: In this mode, PIM multicast routing is used to discover the neighbor VTEP nodes in the same multicast group. Each VTEP dynamically creates unicast SDPs to the remote VTEPs that share the same VXLANs and a mesh-SDP for BUM traffic replication.
- Head-end: In this mode, the administrator specifies the unicast address to reach the far-end VTEP nodes though unicast SDPs. The SDPs can be orchestrated and dynamically created by UNP. BUM traffic is replicated to each the unicast SDP, and one copy is sent to all remote VTEPs sharing the same VXLANs.

With VXLAN, the failure domain is limited to a single location where the VTEP gateway is located.

BENEFITS OF VXLAN

- VXLAN is easy to configure, and extends Layer 2 user VLANs across the existing enterprise routed Layer 3 network. Users anywhere in the enterprise can be added to their department VLAN.
- VXLAN operates as an overlay network and requires no changes to the underlying core network. This promotes a stable no-touch network backbone without frequent configuration changes caused by end-user needs.
- VXLAN works with UNP, LPS and other OmniSwitch features to provide auto-provisioning to minimize effort and save network staff time.
- VXLAN is a simple solution that works with the existing enterprise network. It does not require MPLS skills or special staff training to configure and install.

Figure 3: Enterprise networks can use VXLAN to extend VLANs to remote locations and to connect virtualized and non-virtualized servers



CONCLUSION

The application of VXLAN in the campus brings additional services to extend LANs into data centers, private clouds or public clouds. It allows IT to offer solutions that simplify the transformation process in mergers and acquisitions by extending the transparent connectivity for new business units, temporary contractors and out-sourcing.

Alcatel-Lucent Enterprise believes that the virtualization technologies are not limited to data center solutions, and that network virtualization overlay (NVO) is a viable solution for providing departmental segregation and extending VLANs in a campus network. NVO applied to the campus brings the agility, dynamism and flexibility of the cloud into the enterprise LAN offering rapid IT delivery to improve and simplify the outcome of the business needs.

Alcatel·Lucent
Enterprise