

WHY WE NEED NETWORK ABSTRACTION

Highly virtualized data centers are exposing cracks in traditional network constructs such as VLANs. New approaches that abstract the physical network, including network overlays, are key to providing flexibility and scale.

The move to highly virtualized data centers and cloud models is straining the network. While traditional data center networks were not designed to support the dynamic nature of today's workloads, the fact is, the emergence of highly virtualized environments is merely exposing issues that have always existed within network constructs. VLANs, VRFs, subnets, routing, security, and so on have been stretched well beyond their original intent. The way these constructs are currently used limits scale, application expansion, contraction and mobility.

VLANs are a simple example. 802.1Q tagging supports a theoretical limit of 4,096 VLANs, with actual implementation typically being lower. This means that in a multitenant environment, your scale is

limited to about 4,000 tenants--in theory. In reality, the number is much lower because we tie IP subnets to VLANs, and tenants will typically require more than one subnet.

VRFs become another issue as tenants expand. Each tenant network is different and may require separate routing decisions, overlapping subnets, and so on. This leads to hardware limitations, as VRFs are typically run as separate instances of the routing protocol, requiring CPU resources.

Security is another example of unintended interdependency. Today's networks deploy security based on constructs such as addressing, location and VLAN. This has been necessary but is not ideal. The application or service dictates security requirements, so those requirements should be coupled there instead.

Layer 2 adjacency is another complex issue for modern networks. Many applications must exist in the same Layer 2 domain to support capabilities such as virtual machine motion, which causes a need for larger and larger L2 domains. This requires that the VLANs be

configured on, and trunked to, any physical switches that a VM may end up on.

While each of these constructs has individual complexities, the real problem arises with the unintended dependencies. IP addressing is broken down into subnets traditionally tied to VLANs on a 1-to-1 basis. This means that an application's L3 communication is dictated by its broadcast domain needs and vice versa. Routing is then tied to the IP scheme, and security, load balancing and quality-of-service policy is often applied based on the VLAN or subnet. These are further tied to physical location based on device configuration (including VLAN, VRF and QoS settings).

There is a need for abstraction of these constructs to provide the originally intended independence that will allow networks to scale as required. This need is shown in current standards pushes:

LISP, SDN and VXLAN, for example, are all aimed in some way at removing the tie of location and allowing the application to dictate requirements rather than the infrastructure dictating it.

Within the data center, overlays such as **VXLAN** are one possible solution.

Overlay technologies allow for independent logical networks to be built on top of existing IP infrastructure. They provide some of the abstraction tools required, such as allowing L2 adjacency across L3 networks. Additionally, overlays greatly increase the scale of constructs such as VLANs, moving from 4,000-plus logical networks well into the millions.

These overlays provide one piece of the puzzle of network abstraction. The next step is policy configuration. Rather than traditional methods of applying policy such as security, load balancing and QoS to underlying constructs, these policies should be applied to the applications themselves. Systems like OpenFlow are moving toward this through flow-level programmability, but still have a way to go.

The end goal of the modern network will be service-driven policies and controls. By removing the interdependencies that have been built into today's networks, we will gain the flexibility required by modern compute needs. The purpose of the data center is service delivery, and all aspects must be designed to accomplish that goal.

Source: <http://www.networkcomputing.com/networking/why-we-need-network-abstraction/d/d-id/1233988?>