# Hybrid cloud networking use cases

Hybrid clouds are a special case of cloud internetworking. When providers have full control over their VM subnets, normally TOSCA models can be expected to permit cloud providers to control the network fabric in such a way as to optimize their resources, while providing the scalability and other –ilities expected by their customers.

Internetworking with the on-premise services (or even services hosted at other public clouds) need some conventions to permit interoperability and scalability, and there may also be QOS constraints that benefit from scalable WAN connections, and not merely scalable in metrics such as bandwidth.

It is likely that many of the IETF and IEEE standards that have emerged to deal with piecing together LANS via WAN links will be applicable to internetworking public clouds with on premise clouds or hosts.

To provide some background I have enclosed a diagram to illustrate a (fairly challenging) internetworking integration requirement. It is hoped that by considering some of the issues that arise, some useful required features that are needed by separated tiers can be identified and named.

# Bridging LANS over PseudoWire WAN links.

Suppose that a webtier’s guest VMs use a private IP range CIDR block (e.g. 10.9.8.0/24) as their virtual subnet and are to support a webapp that requires a service located behind the DMZ (on the internal private subnet) of a company.

Furthermore, suppose that the company requires a VPN capable of “bridging” the virtual subnet of the webtier with their own internal subnet.

Finally, suppose that the service is known by its (private) IP address and it is expected that however bridging occurs, IP resolution to MAC address will be by means of ARP resolution protocol. (Briefly, ARP resolution protocol allows the service-consumer, knowing the server’s IP address, to emit a “who has IP address x.y.z.w” and receive the MAC address to then enable making service requests and receiving service responses.) This is an IP connection on the local subnet, even though behind the scenes a WAN link is involved and is generically known as a L2VPN.

The diagram attached to this message identifies the usual suspects in a L2VPN, and relates them to cloud and on-premise “sides” Locate the box surrounding the WebAppTier$Subnet. Ignore the arrows to the Public Routable IP. A virtual lan has a connection to a router that has a local interface to that virtual subnet and sets up an “access circuit” (AC) to provider edge/equipment that is configurable to create a pseudo wire (PW) to another PE unit with an AC into a virtual or metal LAN that needs to appear “local” to the WebAppTier subnet.

In fact, the PW can make use of the public ip network by using an encrypted tunnel or can use other layer2 packet or circuit communications. As long as the bandwidth and latencies match with the local lan expectations, a bridged local subnet is created.

However, certain kinds of coordination can be useful. Consider IP assignment. All IP assignments could be manually pre-arranged by static assignments, but also DHCP could be used. If DHCP is used, is there a single DHCP server for the entire bridged subnet, or local ones? If separate DHCP servers are used, can the ranges they can allocate be specified so that conflicting IP assignments are prohibited? Or can the DHCP be configured not to allocate a statically allocated IP on the server/customer side?

All of these issues are obviously resolvable in various ways, but it might be useful to begin to investigate some specific requirement and capability types (and possible properties or API calls) that can enhance a TOSCA model to indicate what are the expectations when setting up the virtual networks. (We will assume that MAC collisions can be avoided in the usual uuid like ways.)

Here are some possible hybrid internetworking requirements (for the particular case of configurations with one backend server that is to appear in the local ARP domain.)

1. Server has static IP using subnet X.Y.Z.0/24 and requires all clients to be on X.Y.Z.0/24 subnet.
2. Webtier has capability of using any private cidr block reserving server IP address from allocation.

There are others but perhaps this proposal is specific enough for us to begin discussion.

I will enclose some RFC references in a message to be sent later.