Managing advanced network zone infrastructure

Advanced networking introduces a lot of complexity to the underlying infrastructure. Careful thought needs to be put into designing your physical networks, traffic flow, and the host networking bridges that form the foundation. In advanced networking we are opened up to the concepts of public traffic, isolation methods such as VLAN, GRE, and STT, as well as physical networks. Lets take a look at the following example to understand how all these components work together.The hosts have only three physical interfaces. We have four traffic types, and require two physically isolated guest networks. Lets break this down. We know physical networks are managed at the zone level, this is also true for traffic management. This means we must determine traffic binding and physical networks during zone creation. If we weigh the purpose of each traffic type, we might come to the following conclusion for mapping our physical networks and traffic tokens:

- PHYSICAL NETWORK 1: Storage(Red), Management(Blue).
- PHYSICAL NETWORK 2: Guest(Green).
- PHYSICAL NETWORK 3: Guest(Green).
- PHYSICAL NETWORK 4: Public(Yellow).

Please note, this alone will not actually isolate physically isolate traffic. You may have noticed we defined four physical networks and we only have three physical interfaces. This will administratively isolate traffic based on the traffic type to physical network relationship. This will also let us choose the isolation method used for each physical network. We can select from VLAN, GRE, and STT. In order to actually separate the physical traffic we need to configure the traffic binding. To do this, we edit each traffic token, and assign labels as follows:

- PHYSICAL NETWORK 1: VLAN
    - Storage(Red) = cloudBrManagement
    - Management(Blue) = cloudBrManagement
- PHYSICAL NETWORK 2: GRE
    - Guest(Green) = cloudBrGuest1
- PHYSICAL NETWORK 3: VLAN
    - Guest(Green)) = cloudBrGuest2
- PHYSICAL NETWORK 4: STT
    - Public(Yellow) = cloudBrGuest1

Now this is where it gets interesting. You will notice we bound the traffic as follows, and assigned several types of isolation:

- **cloudBrManagement**: Storage(Red), Management(Blue). (VLAN)
- **cloudBrGuest1:** Public(Yellow), Guest(Green). (GRE, STT)
- **cloudBrGuest2:** Guest(Green). (VLAN)

The traffic labels are the exact names of bridges that reside on the host (*Yes it is possible to assign a dynamic bridge created by ACS guest networks as the traffic label on a physical network in a new zone. This form of nested networking leads to communication issues and routing errors if not performed correctly, and yields no foreseeable benefit*). It is also possible as shown to assign more then one type of isolation to a host bridge. If you choose to do such a thing, make sure you have equipment that can handle multiple forms of isolation on a single port channel.
This both reflects the flexibility and the complexity of Apache CloudStack's Advanced Networking Zones. And at first this model can be quite confusing, so let's dissect it. The physical networks allow ACS to interpret our networking scheme as two guest only networks, one public network, and one multiple traffic network. Because the physical hosts only have three physical interfaces we need to map our five traffic types creatively over them. We chose to map the storage and management traffic types to a single interface attached to the bridge; cloudBrManagement. Also considering the public traffic is more similar to guest traffic rather than infrastructure traffic, we bound it to the same interface as the first guest traffic type, attached to the bridge; cloudBrGuest1. This leaves one traffic type remaining, the second guest type, and we bound this to the final interface attached to the bridge; cloudBrGuest2.

This leaves us with ACS reporting four distinct networks, five types of traffic, and three forms of isolation, all bound between three actual bridges on the hosts containing physical interfaces. We can assign guest networks to either physical network by creating network offerings with tags, and they will be physically isolated from each other. This can be important if a guest system requires more isolation than VLANs provide, such as certain PCI compliant designs. This may not seem to be a practical solution, it does however highlight the flexibility of network infrastructure design in advanced networking zones.