Cloudbursting Use Case for SDNP

draft-mcdysan-sdnp-cloudbursting-usecase-00

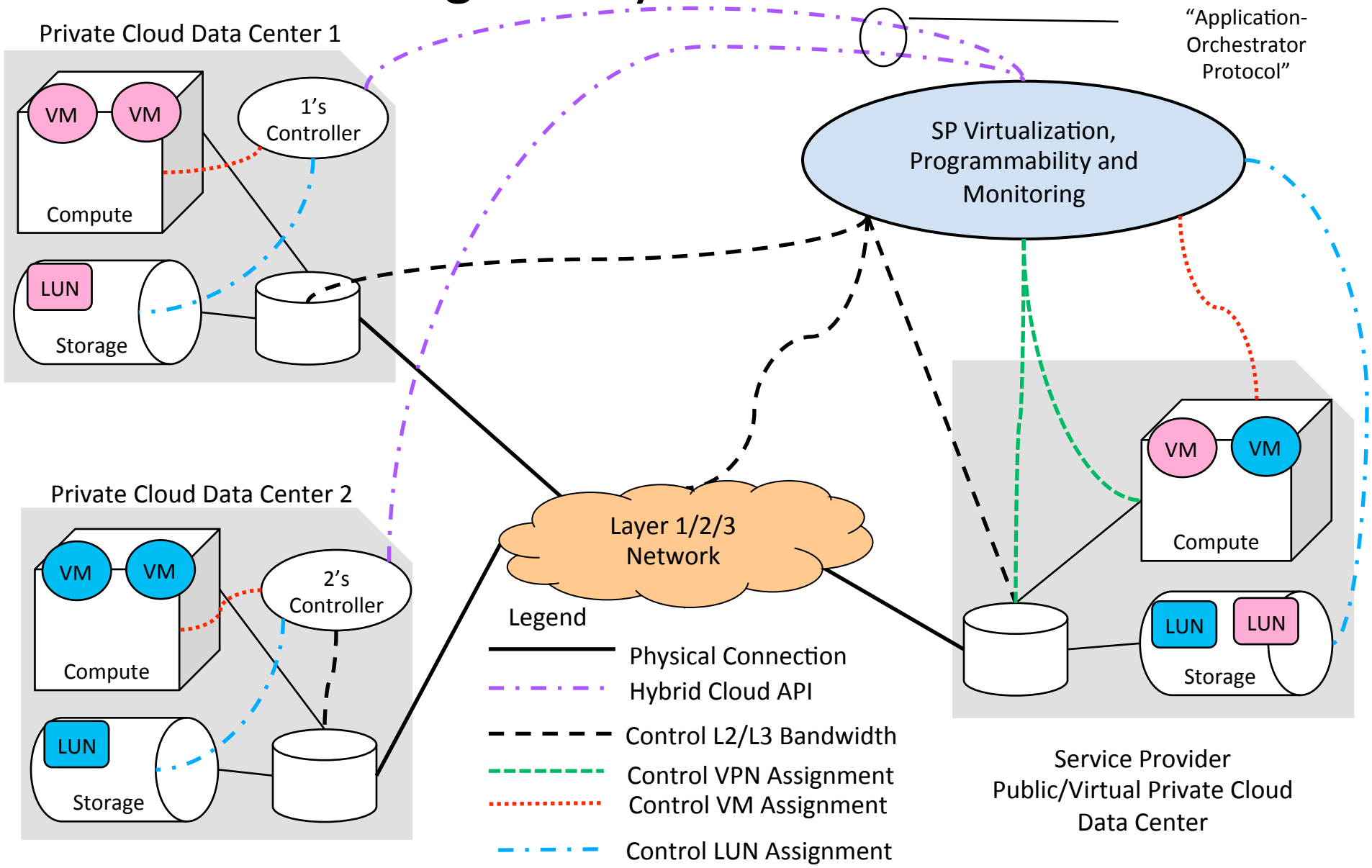
Dave McDysan

Verizon

Background, Motivation & Requirements

- NIST Cloud Computing Based Terminology
  - Private Cloud – operated by an enterprise
  - Public Cloud – multi-tenant data center operated by a service provider
  - Virtual Private Cloud – multi-tenant data center intended to be a dynamic extension of a private cloud
  - Hybrid Cloud – Dynamically instantiated instance of a public (or virtual private) cloud to (temporarily) augment capacity of a private cloud
- Cloud computing capacity requires control and management at least:
  - Layer 1/Layer 2/Layer 3 bandwidth configuration and monitoring (scheduler weight setting, policer setting, reserving/scheduling/requesting bandwidth (e.g., MS-PW, counter collection)
  - VPN membership (e.g., VLAN, L2VPN/L3VPN, etc.) configuration, discovery, policy
  - Compute resources: virtual machines, virtual memory, OS, software assignment and activation on a physical computer
  - Storage resources: Partition(s) (e.g., Logical Unit Name (LUN)) assigned to physical storage
  - Other data center resources (firewalls, load balancers, NAT, gateways, security functions, etc.)
  - Interconnection, reachability, bandwidth, quality, resiliency for all of the above
- More detail for sections 6.2, 6.3 of draft-pan-sdn-dc-problem-statement-and-use-cases-00
- Requirements for some of the above previously submitted to opsawg in Quebec City (see references in draft)
- May also have performance, resiliency, and diversity related requirements (see CSO references in draft)

Cloudbursting in a Hybrid Cloud Environment



Problems to be Solved (Somewhere, Somehow)

- Private Cloud customer desires a single interface (e.g., "Application-to-Orchestrator protocol") to invoke a dynamic cloudburst comprised of previously described aspects of a hybrid cloud service
  - Orchestration System may not be able to meet all requirements and may respond with alternative(s)
  - All aspects of the transaction must either succeed or fail
  - Must be able to perform negotiation
- Security considerations include consistent configuration of security elements in private and and public/virtual private data center elements
- Should use interfaces standardized by IETF or other SDOs
  - May be control plane (signaling, routing) and/or management style
  - May define extensions to existing protocols, or if absolutely necessary new protocols
- Not all interfaces need be standardized
  - For example, those used within a private data center
- Problem space can be partitioned between private and public/virtual private data center elements as summarized in the draft
- Overall framework outlining this class of use case (and similarities with others) and how existing protocols can be used, identification of specific gaps, and optimization/standardization opportunities would be a useful IETF output