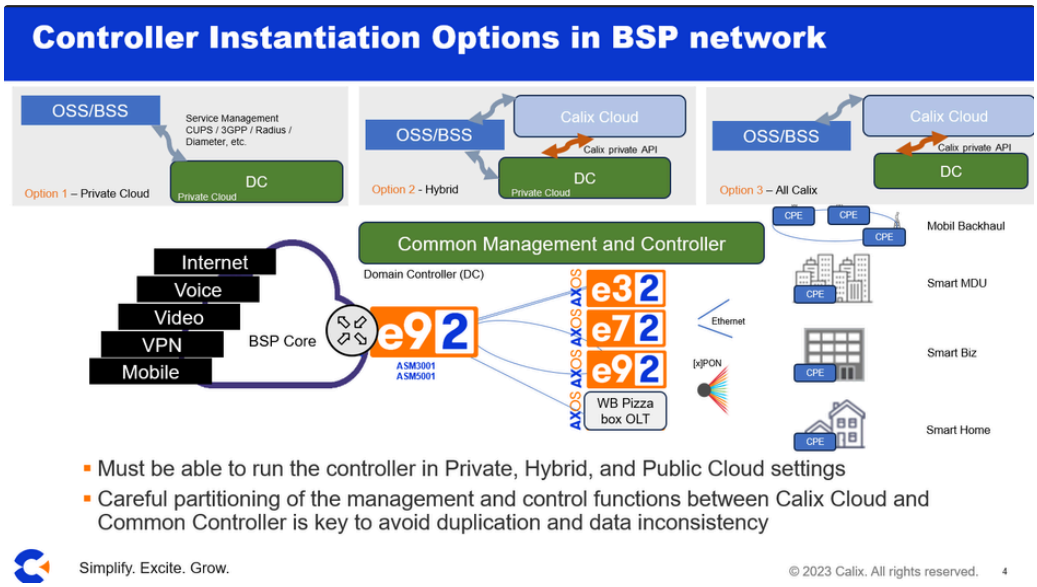
Calix 3.0



Summary of High level BSP Domain Controllers requirements:

- Tier 1: Calix Cloud runs in network infrastructure managed by the BSP
- Tier 2: The components responsible for managing AXOS systems execute in Access Controller (network infrastructure managed by the BSP). The remaining components execute in Calix Cloud. Larger Tier 2 may not be interested in deploying Calix Cloud and use Access Controller only
- Tier 3: The Calix Cloud runs in Calix-Managed Calix Cloud infrastructure.

Scaling requirements are as follows across the Access Controller cluster:

Type	Subscriber Size	Comment
Tier2	<5M subscribers	Ability to support Clustering per Geography /Regions Ability to run as appliances or on private Cloud
Tier 1	~50M subscribers or more (Note that VZ currently has 9M, therefore, this is a ~2030 target)	Ability to support Clustering per Geography /Regions Ability to run as appliances or on private Cloud
Tier 3	~100k subscribers	All infrastructure exists in Calix Cloud. The BSP does not want to be responsible for running server hardware or have control over their cloud infrastructure.

Tier 1:

Tier 1 customers are interested in Management, Provisioning OLT/ONT/RG, Health, Alarm functions. FCR (Netflow, Analytics) and Datalake AI/ML functions will not be used.

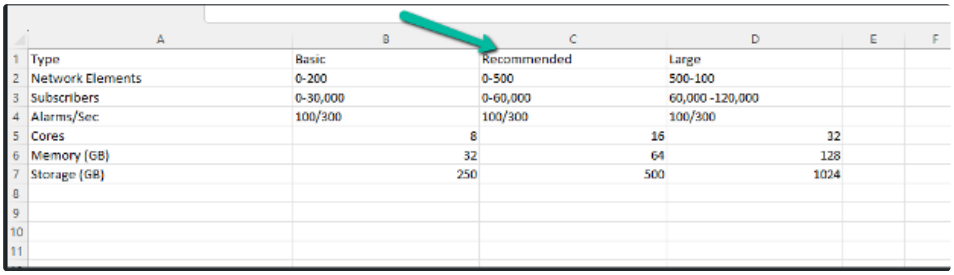
- Need to make Calix Cloud services as Cloud agnostic. Following changes needed:
  - Packaging and deployment (CloudOps team needs to investigate - Senthil, please followup)
    - servers/cluster recommendation
    - footprint required to pack MAP and CNAP micro-services along with its infra
  - CNAP, Service Manager, Health, Alarm micro-services:
    - Amazon SNS replacement for Alarm notifications
    - Amazon RDS replacement - Postgres DB
    - Amazon S3 replacement - if any?
  - MAP micro-services
    - details ?
- Scale ~50M subscribers
  - Single API/UI interface
- HA and geo-redundancy support - need more discussions

Tier2:

A new Access Controller(AC) to Manage, Provision/automation function for IAE and AXOS based White Box (No support for EXA is required). There will be two mode of operations, **Access Controller with Calix Cloud** and **Access Controller without Calix Cloud.**

- Access Controller Functions:
  - Single tarball package as restrictive Internet access to Calix Cloud (if deployed with CC)
  - GUI - need something similar to SMx + what additional pages?
  - IAE System Turn-Up - ZTP with golden config
    - L2 OLT (E9-2 PON/E7-2 PON/Whitebox)
    - L2 Switch (E7-2 Agg)
    - L3/L2 Switch/Router(E3-2/E9 series)
    - L3/L2 BNG/Switch/Router(E9 series)
  - IAE Upgrades : workflow tool
  - Inventory management
  - Network topology
    - The AC must discover, track and maintain a topology database of network elements, providing a view of their status, configuration and topology.
    - This database will be used by controller applications to function. For example, an end-to-end service application would need to understand the topology.
    - The AC will not directly manage the topology - it does not perform control plane/protocol processing of the topology - those are handled by the network elements
    - Discovery options
      - Call Home
      - LLDP
    - Supported topologies?
      - Single
      - Tree (Agg/OLT)
      - Ring (Agg/OLT)

        - Full Mesh
        - L2/L3?
    - IAE config workflows & Ongoing Config Updates (OLT or ONT config profile updates).
    - IAE Service Provisioning - support Subscriber Services APIs
    - IAE end-to-end orchestration ASM5k<>ONT (new Req)
    - White Box Management (new Req)
        - Secure boot of a certified Calix image. An uncertified image must be rejected.
        - Config Req
            - Similar to a E9-2 PON line card.
        - Nodal management
            - The white box OLT will be nodally managed by the ASM50001 like how all other E9-2 PON line cards are managed. Like all other E9-2 PON line cards, managing the white-box OLT directly will not be possible.
    - Security API Token auth. In addition TACACS, LDAP & RADIUS auth is also needed with RBAC
    - In case mode of operation with Calix Cloud - Inventory discovery, topology, NETCONF events need to be reported to CC. Alarm, health management, Performance Monitoring, Historical data is supported in CC only.
    - HA and clustering support with External LB - similar to SMx
    - Scale and hardware guidelines are similar to SMx (standalone instance) as below:



	A	B	C	D	E	F
1	Type	Basic	Recommended	Large		
2	Network Elements	0-200	0-500	500-100		
3	Subscribers	0-30,000	0-60,000	60,000 -120,000		
4	Alarms/Sec	100/300	100/300	100/300		
5	Cores	8	16	32		
6	Memory (GB)	32	64	128		
7	Storage (GB)	250	500	1024		
8						
9						
10						
11						

    -

Summary of High level MSP requirements

MSP Controller needs to manage, provision Calix network elements (WAN Router, POE switches, AP(WiFi), third party Camera). Functions required are Common management and control:

- device on-boarding
- provisioning
- WiFi management
- alarm correlation
- telemetry and insights
- DPI/Security ?
- network and service automation ?

These functions need to be supported in two packaging/Controller form or could be in single Controller package:

MSP Site Controller: management and provision WAN Router, POE switches, AP(WiFi), Camera, and Security functions.

MSP HQ Controller: include all Calix network elements at the HQ, in addition to connectivity and management of the local site as well as multi-sites.

Note*: Although functions are totally different compared to Access Controller, but we can leverage some of the provisioning tool-chain (netconf/yang, SNMP), security, packaging of AC.*

Reference Documents

- PLL requirements
  - Detailed Controller Use Case Document: UC: CCL-82420 CDAS Network Automation
  - High-Level Controller Use Case Document: Controller High Level Requirements.docx