SDN in practice

CISCO's Application Centric Infrastructure
1 Application centric infrastructure (ACI) overview

2 Endpoint Group (EPG)

3 EPG contracts

4 Application policy infrastructure controller (APIC)
ACI overview

Application Policy Infrastructure Controller (APIC)
Spine switches: no interconnection
Leaf switches: connected to each spine switch

The Application Policy Infrastructure Controller and the leaf and spine switches make up the ACI fabric

Source: [1]
ACI overview: Policy model

**Policy repository**: Collection of rules/policies applied to (virtual)endpoints

**Endpoint**: NIC, vNIC, IP address, or DNS name

**Endpoint registry**: Registry of endpoints currently known to ACI
  - **External endpoint**: any external network or element not a component of ACI
  - **Client endpoint**: Directly connected EP to leaf or indirectly through fabric extender (FEX).
Endpoint group (EPG)

Collection of endpoints with identical semantics.

EPG interaction is regulated with policies.

Policies: provide rules for connectivity, visibility and isolation.
Endpoints, EPG and relations

Endpoints are identifiers that represent application components: NIC, vNIC, subnet, etc.

Endpoint Group
An EPG is a collection of similar endpoints

A collection of EPGs and the policies that define the way they communicate is an application network profile

Source: [3]
EPG contracts

Control parameters between application tiers.

- Connectivity, visibility, QoS, etc

Specify rules/policies for groups of (virtual)endpoints regardless of location of the device

Contract contains:

- Filtering construct: list of classifiers
- Action construct: how to handle matching traffic.
Contract & EPG relation

Application Network Profile

- EPG Web
- EPG Application
- EPG Database
- EPG NFS

Source [3]
Contract elements

Endpoints in group WEB can access endpoints in group APP SERVER according to rules specified in the contract.

Specify rules and policies on groups of physical or virtual endpoints without understanding the specific identifiers and regardless of the physical location.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies <strong>subject</strong> to which actions will be applied</td>
<td>Identifies <strong>actions</strong> applied to the subject</td>
</tr>
<tr>
<td>QoS</td>
<td>Log</td>
</tr>
<tr>
<td>Layer 4 port ranges</td>
<td>Redirect (\rightarrow) SVC graph</td>
</tr>
<tr>
<td>TCP options</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Defined bidirectionally in a “provider”-centric way.

Source: [2]
APIC

Distributed system implemented as a cluster of controllers

Primary responsibility: distributing, tracking updating policies to ACI nodes.

Does not do forwarding!

Data distribution via sharding

Application centric construct definitions.

Northbound API: REST XML/JSON

Southbound API: Opflex
**Policy manager:** Defining and deployment of configurations.

**Topology manager:** Up-to-date topology and inventory information.

**Observer:** Monitoring state, health, performance metrics.

**Boot Manager:** Booting and firmware updates for Cisco elements.
Appliance director: Formation and control of the ACI cluster.

VMM manager: Interaction between policy manager and hypervisor.

Event Manager: Repository for events and faults.

Appliance element: Managing the state and inventory of the local APIC appliance.
Promise theory

- Complete overview of the state of the system.
- Implicit configuration

Source: [2]
Discussion

Application centric sounds great, but aren't there too many different applications?

- Would this cause an explosion of EPGs and would that matter?

APIC pushes all policies to the switches and is never in the data path, then how do you deal with faults/errors?

- Can they prevent this with monitoring?
- Or do you just need to define each application?

The papers provide nice concepts but where are the details? And do we need them in order to comment with anything substantial?
Resources

[1]: Application Centric Infrastructure Overview: Implement a Robust Transport Network for Dynamic Workloads

[2]: The Cisco Application Policy Infrastructure Controller

[3]: Cisco Application Policy Infrastructure Controller Data Center Policy Model