ACI Update
ACI 1.1 “Brahmaputra” Release
Brahmaputra release overview

Key Software Features

• Azure Integration - Cisco ACI for the Microsoft private cloud: ACI integration with Microsoft System Center/AzurePack allows new cloud services for tenants and enterprise applications

• IPv6 (data-plane): Support for tenant addressing, contracts, shared services, routing

• ACI fabric as a transit domain: Enables border routers to perform bi-directional route distribution with other routing domains, including route peering with service appliances

• Scale: Profile-based multi-dimensional scale enhancements

• Security: Micro-segmentation and Distributed Firewall with AVS

• Troubleshooting/GUI: New wizard for troubleshooting, capacity dashboard, heat map, etc.

• External connectivity: Support for eBGP (v4/v6), OSPFv3, iBGPv6, EIGR
Brahmaputra release overview

Key Hardware Features

• ACI Spine: N9K-C9516: Cisco Nexus 9516 (Support slots 1-8 only)

• FEX: N2K-C2348UPQ: 48 100Mi/1/10 Gigabit Ethernet and Unified Port host interfaces (SFP+) and up to 6 QSFP+ 10/40 Gigabit Ethernet fabric interfaces.
Brahmaputra MR1 release overview

MR1 Key Software Features

Virtualization
- SCVMM clustering support
- vSphere 6.0 support

Routing
- Sharing L3out among Tenants for Verizon
- EIGRP to Static transit support

Operation
- ACI Capacity Planner (ACI Optimizer)
- Troubleshooting Wizard for Tenant Common

- Microsoft (partner.com) certification for ACI WAP plugin on partner website
- L3Ext connectivity for WAP tenants
- Support for 600 BGP sessions per Border Leaf (Scalability)
- AES Encryption for Config Export/Import
Brahmaputra release overview

Key Hardware Features

- N9K-M6PQ-E (6 ports x 40G Ethernet Expansion Module)
- N9K-C9372PX-E (48 ports x 10G SFP+, 6 ports x 40G QSFP+ TOR)
ACI 1.1 “Brahmaputra” Release

AVS Enhancements
Micro-segmentation & Distributed Firewall

ACI 1.1 “Brahmaputra” Release
Micro-Segmentation
(Attribute based EPG)
AVS Micro-Segmentation (Attribute based EPG)

• Before this feature, EPG is derived based on the encapsulation id (VLAN, VXLAN VNID) in the packet.

• This feature allows granular EPG derivation based on various attributes. (VM Name, Guest OS, MAC, IP etc.)

• This feature is available for virtual endpoints attached with Cisco AVS Distributed Virtual Switch only, not available with VMware DVS in ACI.

• Note: This doesn’t provide an Intra EPG security policy.
• APIC keeps fetching VM attributes from vCenter
• User creates a new EPG with Criterion and Attributes
• APIC pushes the Criterion to iLeaf.
• iLeaf does the attribute matching.
• iLeaf pushes the new EPG with the new encapsulation id to AVS via Opflex

Reclassified new EPG based on VM Attributes
Packet Flow

vLeaf sets the encap based on the new EPG

- Hardware in iLeaf derives the class-id and policies based on the new encapsulation id from the packets.
AVS Micro-Segmentation Implementation

• User Creates “Base EPG” in order to create port-group in vCenter

• User Creates “Attribute based EPG” and associate it to one or more VMM Domains.
  • A new encapsulation id (VLAN/VXLAN) is allocated for this EPG within each associated VMM domain.
  • Attribute based EPG is NOT pushed a new port-group to the VMware vCenter.
  • Dynamically put VMs from “Base EPG” to new “Attribute based EPG” if VMs match criterion (attribute).

• If no matching policy/rule is found in APIC, VMs will default back to “Base EPG” level policy/contracts.

• If VM matches multiple attributes, VM is classified based on preference of each attribute.
APIC GUI

- Tenant > Application Profiles > Application EPGs > EPG > VM Attribute
<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Precedence</th>
<th>Resolution Point</th>
<th>Resolution Trigger</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC</td>
<td>1</td>
<td>vLeaf</td>
<td>Packet Received</td>
<td>5c:01:23:ab:cd:ef</td>
</tr>
<tr>
<td>IP</td>
<td>2</td>
<td>vLeaf</td>
<td>Packet Received</td>
<td>192.168.1.0/24 192.168.33.77</td>
</tr>
<tr>
<td>VNIC DN</td>
<td>3</td>
<td>iLeaf</td>
<td>VNIC Attach</td>
<td>A1:23:45:67:89:0b</td>
</tr>
<tr>
<td>VM Identifier</td>
<td>4</td>
<td>iLeaf</td>
<td>VNIC Attach</td>
<td>vm-598</td>
</tr>
<tr>
<td>VM Name</td>
<td>5</td>
<td>iLeaf</td>
<td>VNIC Attach</td>
<td>HR_VDI_VM1</td>
</tr>
<tr>
<td>Hypervisor Identifier</td>
<td>6</td>
<td>iLeaf</td>
<td>VNIC Attach</td>
<td>host-25</td>
</tr>
<tr>
<td>VMM Domain (DVS)</td>
<td>7</td>
<td>iLeaf</td>
<td>VNIC Attach</td>
<td>AVS-SJC-DC1</td>
</tr>
<tr>
<td>Datacenter</td>
<td>8</td>
<td>iLeaf</td>
<td>VNIC Attach</td>
<td>SJC-DC1</td>
</tr>
<tr>
<td>Guest OS Type</td>
<td>9</td>
<td>iLeaf</td>
<td>VNIC Attach</td>
<td>Windows 2008</td>
</tr>
<tr>
<td>VM Custom Attribute</td>
<td>10</td>
<td>iLeaf</td>
<td>VNIC Attach</td>
<td>SG_DMZ</td>
</tr>
</tbody>
</table>
Use case 1
Isolate a Malicious VM

- Problem: Vulnerability is detected in a particular type of operating system (e.g. Windows). Network security administrator would like to isolate all Windows VM.

- Solution: Define Security EPG with criterion as “Operating System = Windows”. No contracts are provided or consumed by this EPG. It will stop all inter-EPG communication for the matching VMs.

- No VM attach/detach or placement of VM to a different port-group is needed.
Use case 2
Security across zones

• Problem: VMs belonging to different departments (e.g. HR, Sales) or different roles (Production, Test) are placed in the port-group. But isolation across departments are required. (e.g. HR-Web-VM should not be able to talk to Sales-Web-VM)

• Solution: Define EPGs, which match if the VM Name contains a matching string (e.g. HR, Sales etc).

• Each Attribute based EPG can have their own security policies.
Issues with stateless firewall

<table>
<thead>
<tr>
<th>Source class</th>
<th>Source Port</th>
<th>Destination class</th>
<th>Destination Port</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer</td>
<td>*</td>
<td>Provider</td>
<td>80</td>
<td>Permit</td>
</tr>
<tr>
<td>Provider</td>
<td>80</td>
<td>Consumer</td>
<td>*</td>
<td>permit</td>
</tr>
</tbody>
</table>

Consumer

IP_C, 1234, IP_P, 80, SYN
Connection Established

Not blocked by fabric

Not blocked by fabric

Provider

IP_P, 80, IP_C, 1234, SYN+ACK
IP_P, 80, IP_C, 2000, SYN+ACK
IP_P, 80, IP_C, 4000, SYN
IP_P, 80, IP_C, 4000, SYN+ACK

Problem: Server(provider) can connect to any clients (consumer)
Distributed Firewall Implementation

• iLeaf
  • Reflective ACL in the hardware is programmed to allow TCP packets only if ACK flag set.
  • This is done if the ‘stateful’ flag is set in the filter.

• vLeaf
  • Maintain connection table to track the flow.
  • In receiving the first TCP SYN packet, vLeaf create flow table entry.
  • If vLeaf doesn’t have flow entry, packet is dropped by vLeaf.

• In typical Firewall solution, the first packet is always sent to a policy engine. In ACI fabric, hardware acts as a policy store, so it doesn’t incur performance penalty to policy lookup.
Hardware Assisted Stateful firewall

Leaf evaluates stateless policy

Policy Enforcement done at iLeaf

Connection Tracking at vLeaf

- Create flow table entry
- Forward packet to iLeaf

On flow table hit forward packet to iLeaf

Create flow state only for TCP SYN packet received from PNIC

Response from VM Perform flow table lookup

Consumer A

Provider B

Deliver packet to destination VM

Table:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Proto</th>
<th>Src ip</th>
<th>Src port</th>
<th>Dst IP</th>
<th>Dst port</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>tcp</td>
<td>IP_A</td>
<td>1234</td>
<td>IP_B</td>
<td>80</td>
</tr>
<tr>
<td>A</td>
<td>tcp</td>
<td>IP_B</td>
<td>80</td>
<td>IP_A</td>
<td>1234</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Proto</th>
<th>Src ip</th>
<th>Src port</th>
<th>Dst IP</th>
<th>Dst port</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>tcp</td>
<td>IP_A</td>
<td>1234</td>
<td>IP_B</td>
<td>80</td>
</tr>
<tr>
<td>B</td>
<td>tcp</td>
<td>IP_B</td>
<td>80</td>
<td>IP_A</td>
<td>1234</td>
</tr>
</tbody>
</table>
Hardware Assisted Stateful firewall

Case 1: SYN + ACK attack from Provider

<table>
<thead>
<tr>
<th>Src class</th>
<th>Src port</th>
<th>Dest Class</th>
<th>Dest port</th>
<th>Flag</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>*</td>
<td>B</td>
<td>80</td>
<td>*</td>
<td>Allow</td>
</tr>
<tr>
<td>B</td>
<td>80</td>
<td>A</td>
<td>*</td>
<td>ACK</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Packet dropped by vLeaf because of missing flow entry

VLAN | Proto | Src ip | Src port | Dst IP | Dst port |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>tcp</td>
<td>IP_A</td>
<td>1234</td>
<td>IP_B</td>
<td>80</td>
</tr>
<tr>
<td>A</td>
<td>tcp</td>
<td>IP_B</td>
<td>80</td>
<td>IP_A</td>
<td>1234</td>
</tr>
</tbody>
</table>

VLAN | Proto | Src ip | Src port | Dst IP | Dst port |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>tcp</td>
<td>IP_A</td>
<td>1234</td>
<td>IP_B</td>
<td>80</td>
</tr>
<tr>
<td>B</td>
<td>tcp</td>
<td>IP_B</td>
<td>80</td>
<td>IP_A</td>
<td>1234</td>
</tr>
</tbody>
</table>

SYN + ACK packets Attack from Provider, for which connection is not initiated by Consumer (dest Port != 1234)
Hardware Assisted Stateful firewall

Case 2: SYN attack from Provider

Leaf evaluates stateful policy

SYN packets dropped by hardware on iLeaf because of missing ACK bit set.

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Proto</th>
<th>Src ip</th>
<th>Src port</th>
<th>Dst IP</th>
<th>Dst port</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>tcp</td>
<td>IP_A</td>
<td>1234</td>
<td>IP_B</td>
<td>80</td>
</tr>
<tr>
<td>A</td>
<td>tcp</td>
<td>IP_B</td>
<td>80</td>
<td>IP_A</td>
<td>1234</td>
</tr>
<tr>
<td>B</td>
<td>tcp</td>
<td>IP_A</td>
<td>1234</td>
<td>IP_B</td>
<td>80</td>
</tr>
<tr>
<td>B</td>
<td>tcp</td>
<td>IP_B</td>
<td>80</td>
<td>IP_A</td>
<td>1234</td>
</tr>
</tbody>
</table>
External L3 Out & L3 Transit Functionality

ACI 1.1 “Brahmaputra” Release
External L3 Connectivity

L3 Outside protocol support in FCS image

- OSPF nssa
- BGP (iBGP only)
- Static

New L3 outside protocol support in FCS+9

- OSPF normal areas, OSPFv3 (IPv6)
- BGP iBGP and eBGP, (supports IPv6), peering over OSPF
- EIGRP (IPv4 only)
# L3Outside Scale Limits

<table>
<thead>
<tr>
<th>Feature</th>
<th>Per Fabric</th>
<th>Per Leaf</th>
</tr>
</thead>
<tbody>
<tr>
<td># of Tenants</td>
<td>500</td>
<td>100</td>
</tr>
<tr>
<td># of L3 Contexts</td>
<td>500</td>
<td>100</td>
</tr>
<tr>
<td># of L3 Outsides</td>
<td>500</td>
<td>100</td>
</tr>
<tr>
<td># of L3 Outsides per VRF</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td># of L3 protocol peers</td>
<td>500</td>
<td>100</td>
</tr>
<tr>
<td># of External EPGs per L3out</td>
<td>n/a</td>
<td>24</td>
</tr>
<tr>
<td># of L3 interfaces Per L3out</td>
<td>n/a</td>
<td>16</td>
</tr>
<tr>
<td># of IPv4 prefixes</td>
<td>10,000 (IPv4 only)</td>
<td>10,000 (IPv4 only)</td>
</tr>
<tr>
<td># of IPv6 prefixes</td>
<td>5,000/2,500* (IPv6 only)</td>
<td>5,000/2,500* (IPv6 only)</td>
</tr>
<tr>
<td># of prefixes for policy enforcement</td>
<td>1,000</td>
<td>1,000</td>
</tr>
</tbody>
</table>

*5,000 /64 prefixes, 2,500 /1,000prefixes
L3out Connection Types

- L3Outs provided external L3 connectivity on Routed Interfaces, Routed Sub-Interfaces, and SVIs.
- When an SVI is used for an L3Out an External BD will be used for the L3out. Note: This is not a Tenant BD and cannot be used for tenant EPGs.
- If an L3Out is configured with multiple SVIs on different leaf switches with the same encap VLAN the External BD is extended across the fabric (they all use the same VNID).
- An External BD is not used for Routed Interfaces or Routed Sub-Interfaces.
- L3outs using Routed Interfaces and Routed Sub-Interfaces must still reference an External Routed Domain (Layer 3 Domain). A fault will be raised if the External Routed Domain is not configured on the L3out.
- The External Routed Domain is associated with an Attachable Access Entity Profile (AAEP).
- The External Routed Domain should be associated with a VLAN pool if using SVI interfaces. This is not required when using Routed Interfaces or Routed Sub-Interfaces.
- There is a limit of 3 x L3Outs per VRF but a single L3Out can include multiple interface profiles and peer with multiple external neighbors.
External OSPF Connectivity
External OSPF Connectivity Features

- Supports IPv4 and IPv6 (OSPFv2 and OSPFv3)
- Supports regular areas (including backbone area) and NSSA areas.
- OSPF point-to-point and broadcast network types (OSPF interface Policy)
- OSPF hello/dead interval configuration (OSPF Interface Policy)
- OSPF LSA throttle/pacing timers (OSPF Timer Policy)
- Graceful Restart (helper) (OSPF Timer Policy)
- Authentication (OSPFv2)
OSPF L3Out over Routed Interface and Routed Sub-Interfaces

OSPF Areas connected to border leaves are not joined via the fabric*. Routes learned from one OSPF area are redistributed into MP-BGP at the ingress leaf and then redistributed back out to OSPF at the egress leaf.

*Exception when using SVI on multiple leaves with the same L3out and VLAN.
OSPF L3Out over VPC with SVI

When an SVI interface is used for an L3out connection an External BD will be created.

OSPF network will be broadcast. Service appliance will neighbor with both border leaf switches.

Note: Tenant EPGs cannot be placed in External BD.
SVI interfaces configured on the same L3Out

All SVIs configured under a single L3Out. L3out: ExtOSPFL3out
All SVIs use same encap (vlan-100)

BD VLAN: 14
VNIID: 15531929

Encap VLAN-100
OSPF Area 0

BD VLAN: 15
VNIID: 15531929

Encap VLAN-100
OSPF Area 0

OSPF Routes are still redistributed into MP-BGP but because the fabric encap (VNIID) is used on each leaf all routers can peer over fabric encap connecting the OSPF area.

External routers can also form OSPF adjacencies with each other via the fabric but those adjacencies are not shown. All routers will go through normal DR/BDR election process.
OSPF L3Out over VPC Failure Scenario

OSPF Adjacency will stay up over fabric encapsulation.

MP-BGP

VNID: 15531929

Border Leaf

BGP RR

BGP RR

Service Appliance running OSPF

OSPF Area 0

External BD

Link Failure

BD VLAN: 14
VNID: 15531929
EIGRP External Connectivity
EIGRP External Connectivity Features

- Supports EIGRP IPv4 only
- Supports One EIGRP L3out per VRF
- Hello/Hold timers (EIGRP Interface Policy)
- Passive Interface (EIGRP Interface Policy)
- 64 bit metric calculation (EIGRP Address Family Policy)
- Leaf cannot be EIGRP Stub but does recognize EIGRP stub neighbors
- Graceful Restart enabled by default (graceful restart aware) (not configurable)
Routed Interfaces and Routed Sub-Interfaces are also supported for EIGRP however only one EIGRP L3out per VRF is supported.

IPv6 is not supported for EIGRP.
EIGRP L3Out over VPC with SVI

VPC/SVI configuration for EIGRP is the same as OSPF.

When an SVI interface is used for an L3out connection, an External BD will be created.

Border leaf switches will peer with each other over the fabric (External BD VNID).

Note: Tenant EPGs cannot be placed in External BD.

Service appliance will neighbor with both border leaf switches.
EIGRP L3Out over VPC Failure Scenario

EIGRP Adjacency will stay up over fabric encap

Border Leaf

BGP RR

Service Appliance running EIGRP

EIGRP AS 1

MP-BGP

VNID: 15531929

Border Leaf

BGP RR

External BD

External BD

BD VLAN: 14 VNID: 15531929

BD VLAN: 14 VNID: 15531929

Link Failure

EIGRP Adjacency will stay up over fabric encap
BGP External Connectivity
BGP External Connectivity Features

- iBGP and eBGP Supported
- BGP over OSPF
- BGP over static route
- Local AS
- BGP Controls (next hop self, send community, send extended community, disable peer AS check, Allow self AS)
- Authentication
- Graceful Restart (helper)
Transit Fabric
Supported Transit Combinations

- Transit routing is supported only for specific L3 outside combinations. The table below shows the supported combinations for each L3 outside type.

<table>
<thead>
<tr>
<th>L3 Outside External Connection Type</th>
<th>Supported L3 out connection for transit</th>
<th>Protocol Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF</td>
<td>EIGRP, OSPF, All BGP connection types, Static</td>
<td>IPv4 and IPv6</td>
</tr>
<tr>
<td>iBGP over OSPF</td>
<td>OSPF, Static Route, eBGP over direct connection</td>
<td>IPv4 and IPv6</td>
</tr>
<tr>
<td>eBGP over OSPF</td>
<td>OSPF, eBGP over OSPF</td>
<td>IPv4 and IPv6</td>
</tr>
<tr>
<td>iBGP over Static route</td>
<td>OSPF, static route</td>
<td>IPv4 and IPv6</td>
</tr>
<tr>
<td>iBGP over direct connection</td>
<td>OSPF, static route</td>
<td>IPv4 and IPv6</td>
</tr>
<tr>
<td>eBGP over direct connection</td>
<td>OSPF, iBGP over OSPF, eBGP over direct connection, static route</td>
<td>IPv4 and IPv6</td>
</tr>
<tr>
<td>EIGRP</td>
<td>OSPF</td>
<td>IPv4 only</td>
</tr>
<tr>
<td>Static Route</td>
<td>OSPF, iBGP over OSPF, iBGP over static route, iBGP over direct connection, static route</td>
<td>IPv4 and IPv6</td>
</tr>
</tbody>
</table>
## Supported Transit Combination Matrix

- The matrix below shows can be used as a quick reference for the supported transit combinations.

<table>
<thead>
<tr>
<th>L3 Outside Connection Type</th>
<th>OSPF</th>
<th>iBGP over OSPF</th>
<th>eBGP over OSPF</th>
<th>iBGP over Static route</th>
<th>iBGP over direct connection</th>
<th>eBGP over direct connection</th>
<th>EIGRP</th>
<th>Static Route</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>iBGP over OSPF</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>eBGP over OSPF</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>iBGP over Static route</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>iBGP over direct connection</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>eBGP over direct connection</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>EIGRP</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Static Route</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

✗ = Unsupported/Untested combinations.
ACI fabric is a transit network

- Fabric runs MP-BGP between spines and leaves
- L3outs on different leaves are in separate L3 domains.
- Routes learned from L3outs are redistributed into BGP on border leaves
- OSPF domains are not joined via the fabric. Leaf switches are ASBRs
- Routes are redistributed from MP-BGP to OSPF as External Type-5 LSAs
- BGP route reflectors configured on Spines (up to two)
Redistribution of Routes from L3Outs

- ACI Fabric runs MP-BGP
- Routes learned from L3Outs on border leaf switches are redistributed into MP-BGP at the ingress leaf.
- Routes are redistributed to leaf switches where same VRF is present.
Route Control/Security Control Enforcement

- L3Outs have both route control and security control.
- **Route Control Subnets** controls the exchange of routing information (prefixes) into and out of the fabric (control-plane).
- **Security Import Subnets** controls the forwarding of packets into and out of L3Out connections (data-plane)
- Security control is applied to both transit forwarding and tenant to outside forwarding.
- Security control is a whitelist model (same as Tenant EPG to EPG policy)
- Security control for transit traffic supports prefix filtering only (no L4 ports)
- Route control and security control prefixes are configured at the L3Out external EPG (**InstP**) but are applied at the VRF level.
APIC GUI Enhancements
ACI 1.1 “Brahmaputra” Release

Carly Stoughton
Technical Marketing Engineer, INSBU

@_vCarly
APIC 1.1 GUI Enhancements - Summary

- Capacity Dashboard
- Simplified Interface Configuration (“form-based”)
- Interface Selector Override
- Interface, Domain, & AEP Superwizard for simple Access Policy configuration
- Physical Port Operational tab
- Simplified OOB Management Access Control
- Application Profile Cloning
- Quick Create Application Profiles wizard
- Detailed EPG Info and Statistics
- Multiple Static Paths with the same VLAN for EPGs in one step
- Global, Granular Object Search
- Firmware & Maintenance Group Filters
Capacity Dashboard
Capacity Dashboard (NEW!)

• **What**  Provides a dashboard of object usage and switch resource utilization on the ACI fabric.

• **Why**  Allows admins to monitor if they are reaching the maximum capacity of fabric objects, and which switches’ TCAMs are filling up. Admins can identify hot spots, and determine if the fabric needs to grow or design needs to be reconsidered.

• **Where**  Fabric > Inventory > Pod 1 > Operational > Capacity Dashboard
Per-switch hardware memory utilization broken out into various network forwarding objects

<table>
<thead>
<tr>
<th>Switch</th>
<th>Mac (learned)</th>
<th>IPv4 (learned)</th>
<th>IPv6 (learned)</th>
<th>Multicast</th>
<th>Policy CAM</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>node-139</td>
<td>16% 2001 of 12288</td>
<td>19% 2411 of 12288</td>
<td>0% 0 of 8192</td>
<td>8000 of 8192</td>
<td>&lt;1% 39 of 4096</td>
<td>6% 218 of 3500</td>
</tr>
<tr>
<td>node-140</td>
<td>16% 2002 of 12288</td>
<td>19% 2411 of 12288</td>
<td>0% 0% 0 of 8192</td>
<td>8000 of 8192</td>
<td>1% 41 of 4096</td>
<td>30% 1059 of 3500</td>
</tr>
<tr>
<td>node-141</td>
<td>16% 2002 of 12288</td>
<td>19% 2411 of 12288</td>
<td>0% 0% 0 of 8192</td>
<td>8000 of 8192</td>
<td>1% 41 of 4096</td>
<td>30% 1059 of 3500</td>
</tr>
<tr>
<td>node-142</td>
<td>16% 2001 of 12288</td>
<td>19% 2411 of 12288</td>
<td>0% 0% 0 of 8192</td>
<td>8000 of 8192</td>
<td>1% 41 of 4096</td>
<td>30% 1059 of 3500</td>
</tr>
<tr>
<td>node-143</td>
<td>14% 1823 of 12288</td>
<td>18% 2232 of 12288</td>
<td>0% 0% 0 of 8192</td>
<td>8000 of 8192</td>
<td>1% 41 of 4096</td>
<td>30% 1059 of 3500</td>
</tr>
<tr>
<td>node-144</td>
<td>16% 1994 of 12288</td>
<td>19% 2409 of 12288</td>
<td>0% 0% 0 of 8192</td>
<td>8000 of 8192</td>
<td>1% 43 of 4096</td>
<td>55% 1942 of 3500</td>
</tr>
<tr>
<td>node-145</td>
<td>16% 2002 of 12288</td>
<td>19% 2412 of 12288</td>
<td>0% 0% 0 of 8192</td>
<td>8000 of 8192</td>
<td>1% 42 of 4096</td>
<td>35% 1250 of 3500</td>
</tr>
<tr>
<td>node-146</td>
<td>16% 2002 of 12288</td>
<td>19% 2411 of 12288</td>
<td>0% 0% 0 of 8192</td>
<td>8000 of 8192</td>
<td>1% 43 of 4096</td>
<td>58% 2034 of 3500</td>
</tr>
<tr>
<td>node-147</td>
<td>16% 1994 of 12288</td>
<td>19% 2409 of 12288</td>
<td>0% 0% 0 of 8192</td>
<td>8000 of 8192</td>
<td>1% 43 of 4096</td>
<td>58% 2034 of 3500</td>
</tr>
<tr>
<td>node-148</td>
<td>16% 2002 of 12288</td>
<td>19% 2412 of 12288</td>
<td>0% 0% 0 of 8192</td>
<td>8000 of 8192</td>
<td>1% 43 of 4096</td>
<td>58% 2034 of 3500</td>
</tr>
<tr>
<td>node-149</td>
<td>16% 1994 of 12288</td>
<td>19% 2409 of 12288</td>
<td>0% 0% 0 of 8192</td>
<td>8000 of 8192</td>
<td>1% 43 of 4096</td>
<td>58% 2034 of 3500</td>
</tr>
</tbody>
</table>

Tenant object utilization
Values in the left-hand pane may exceed 100% since the maximums listed are the Cisco-validated limits, not hardware limits.

These are based on hardware limits.
### Usage Overview

<table>
<thead>
<tr>
<th>Switch</th>
<th>Mac (learned)</th>
<th>IPv4 (learned)</th>
<th>IPv6 (learned)</th>
<th>Multicast</th>
<th>Policy CAM</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>node-139</td>
<td>16% 2001 of 12288</td>
<td>16%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
<td>6%</td>
</tr>
<tr>
<td>node-140</td>
<td>16% 2001 of 12288</td>
<td>16%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
<td>6%</td>
</tr>
<tr>
<td>node-141</td>
<td>16% 2002 of 12288</td>
<td>16%</td>
<td>0%</td>
<td>0%</td>
<td>97%</td>
<td>30%</td>
</tr>
<tr>
<td>node-142</td>
<td>16% 2001 of 12288</td>
<td>16%</td>
<td>0%</td>
<td>0%</td>
<td>97%</td>
<td>30%</td>
</tr>
<tr>
<td>node-143</td>
<td>16% 2001 of 12288</td>
<td>16%</td>
<td>0%</td>
<td>0%</td>
<td>97%</td>
<td>30%</td>
</tr>
<tr>
<td>node-144</td>
<td>16% 2001 of 12288</td>
<td>16%</td>
<td>0%</td>
<td>0%</td>
<td>97%</td>
<td>30%</td>
</tr>
<tr>
<td>node-145</td>
<td>16% 2001 of 12288</td>
<td>16%</td>
<td>0%</td>
<td>0%</td>
<td>97%</td>
<td>30%</td>
</tr>
<tr>
<td>node-146</td>
<td>16% 2001 of 12288</td>
<td>16%</td>
<td>0%</td>
<td>0%</td>
<td>97%</td>
<td>30%</td>
</tr>
<tr>
<td>node-147</td>
<td>16% 2001 of 12288</td>
<td>16%</td>
<td>0%</td>
<td>0%</td>
<td>97%</td>
<td>30%</td>
</tr>
<tr>
<td>node-148</td>
<td>16% 2001 of 12288</td>
<td>16%</td>
<td>0%</td>
<td>0%</td>
<td>97%</td>
<td>30%</td>
</tr>
</tbody>
</table>

**To refresh stats**
Simplified Interface & Policy Configuration
Simplified Interface & Policy Configuration (NEW!)

- **What**  Easily configure interfaces, Port Channels, and vPCs directly from the topology view.
- **Why**  Creating, managing, and associating access policies and profiles can be confusing and time consuming.
- **Where**  Fabric > Inventory > Pod 1 > Switch > Topology
Create and configure interfaces, Port Channels, and vPCs by right-clicking a port.
Configure interface without using access policies (interface policies, policy groups, profiles, selectors etc.), overrides policy
Simplified Port Channel Creation

Simply create a Port Channel without using access policies (interface policies, policy groups, profiles, selectors etc.)
Simplified Virtual Port Channel Creation

Domain creation centralized

Simply create a vPC and a domain on one screen without using access policies (interface policies, policy groups, profiles, selectors etc.)
Simplified Access Policy Configuration Wizard

-OR-

Configure Interface, PC, and VPC

Configure in-band management access
Configure out-of-band management access
Create a CDP (or other) interface policy
Configure an interface, PC, and VPC
All policies configurable in one screen
Select a switch to configure an interface.
**Configure Interface, PC, And VPC**

### Configured Switch Interfaces

<table>
<thead>
<tr>
<th>NODE ID</th>
<th>INTERFACES</th>
<th>IF TYPE</th>
<th>ENCAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>330</td>
<td>1/21</td>
<td>VPC</td>
<td>Bare Metal VLANs: (1001-4000)</td>
</tr>
<tr>
<td>399</td>
<td>1/10-11</td>
<td>Individual</td>
<td>Bare Metal VLANs: (3700-3709)</td>
</tr>
<tr>
<td>370</td>
<td>1/12-18</td>
<td>PC</td>
<td>Bare Metal VLANs: (2-601,1102-1109)</td>
</tr>
<tr>
<td>322</td>
<td>1/23</td>
<td>VPC</td>
<td>Bare Metal VLANs: (1001-4000)</td>
</tr>
</tbody>
</table>

### VPC Switch Pairs

<table>
<thead>
<tr>
<th>VPC DOMAIN ID</th>
<th>SWITCH 1</th>
<th>SWITCH 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>777</td>
<td>111</td>
<td>112</td>
</tr>
<tr>
<td>666</td>
<td>113</td>
<td>115</td>
</tr>
<tr>
<td>10</td>
<td>150</td>
<td>149</td>
</tr>
<tr>
<td>31</td>
<td>160</td>
<td>159</td>
</tr>
<tr>
<td>201</td>
<td>201</td>
<td>202</td>
</tr>
<tr>
<td>301</td>
<td>321</td>
<td>322</td>
</tr>
<tr>
<td>302</td>
<td>324</td>
<td>323</td>
</tr>
<tr>
<td>303</td>
<td>326</td>
<td>325</td>
</tr>
<tr>
<td>304</td>
<td>328</td>
<td>327</td>
</tr>
</tbody>
</table>

---

**All interface policies configurable here**

---
New Attached Device Type field. Config options change based on selection to provide all required input and objects on one screen.
e.g. Bare Metal requires a domain and VLAN pool.
ESX Hosts requires vCenter VMM domain, etc.
Tenant Enhancements
### Application EPG - EPG dmz

#### Detailed contract information displayed per-EPG

<table>
<thead>
<tr>
<th>TO EPG</th>
<th>TYPE</th>
<th>CONTRACT SUBJECT</th>
<th>FILTER ETHRT-PROTOCOL-SRC/DPORT TO DEST/DPORT</th>
<th>EGRESS 1MIN CUMULATIVE PACKETS</th>
<th>INGRESS 1MIN CUMULATIVE PACKETS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CiscoFed1183/sap/zone1</td>
<td>Consumer</td>
<td>CiscoFed1183/CiscoFed1183/Sacc4/n...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CiscoFed1183/sap/zone1</td>
<td>Provider</td>
<td>CiscoFed1183/webQ/W1/1183/Http</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall1183b/CiscoFed1183b/1-n-CiscoFed1183</td>
<td>Consumer</td>
<td>un/loc-CiscoFed1183/GraphOnI_C [un...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall1183b/CiscoFed1183b/1-n-CiscoFed1183</td>
<td>Provider</td>
<td>un/loc-CiscoFed1183/GraphOnI_C [un...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>BD</td>
<td>Domain</td>
<td>Static Path</td>
<td>Static Path VLAN</td>
<td>Provided Contract</td>
</tr>
<tr>
<td>--------</td>
<td>---------------</td>
<td>-----------------</td>
<td>-------------</td>
<td>------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Fed</td>
<td>CiscoFed1183Dmz</td>
<td>L3dom_1 (L3ext)</td>
<td></td>
<td></td>
<td>CiscoFed1183Cext2</td>
</tr>
</tbody>
</table>

Creates EPGs in one line, including BD, domain, path, and contracts
Labels are added to the cloned contracts to differentiate from the source AP

Only have to specify a name for the clone
Detailed per-EPG statistics
Enhancements to EPG based on a static path
Simplified access control for OOB management ports
Additional Enhancements
Granular, global object search – e.g. can search for an endpoint using MAC or IP address
New interface Operational tab displays detailed port information.
ACI Brahmaputra MR 1
FCS 1.1(2) release

August 2015
ACI Brahmaputra MR 1 - 1.1(2) release

- New Hardware
- New Software
- Higher Scale Tested
New Software

• ACI Fundamentals
  • ACI Capacity Planner
  • AES Encryption of APIC configuration files
  • Improvements to Troubleshooting Wizard

• Virtualization
  • vSphere 6.0
  • SCVMM clustering
  • L3Ext connectivity for WAP tenants
  • Microsoft certification for ACI WAP WAP plugin on partner website

• ACI Routing
  • Shared VRF and L3out among Tenants
  • EIGRP to static transport

• Software now supports N2K-C2348UPQ FEX
Scale Improvements

- Support for 12 FEX per leaf
- Support for 600 BGP sessions per Border Leaf
New Hardware

- N9K-C9372PX-E – 48x10G SFP+, 6x40G
- N9K-M6PQ-E – 6x40G expansion module
- The new ASIC will support IP based EPG
  - Note: Software will be supported in the future
What's New?

Enhancing Cisco Nexus 9300 portfolio with 1RU ACI leaf capable switches and 6p 40G expansion module.

- Nexus 9372PX-E – 48p 10G SFP+, 6p 40G QSFP
- Nexus 9372TX-E – 48p 10G BASE-T, 6p 40G QSFP
- Nexus M6PQ-E – 6p 40G QSFP expansion module used in Nexus 9396PX/TX, 93128TX

The new switches and expansion module are a minor hardware revision of existing switches to enable **IP based EPG classification** in ACI mode. The switches are transparent and are at feature parity in NX-OS mode.
ACI Fundamentals
ACI Capacity Planner

• Provides two operations:
  • Future planning:
    • Enter future network requirements in config template, ACI Capacity planner tells you how many leafs you will need for your network, how to deploy each application and external EPG on each leaf without violating any constraints
  • Current planning
    • Enter existing topology, ACI Capacity planner will help determine if you have what you need, if you are exceeding any limits, suggest how to deploy each application and external EPG on each leaf
    • Supported in future releases
ACI Capacity Planner

Create a new profile to get started

ACI Capacity Planner located under Operations
ACI Capacity Planner

Enter network requirements

Drag and drop number of required Tenants, EPGs, Contracts, L2 and L3 Out
ACI Capacity Planner

- View the number of leafs needed for your network
- View suggested deployment for each leaf
- Determine resource utilization
Introducing new way of encrypting properties which are marked secure.

Instead of using symmetric key we are using passphrase based AES scheme to encrypt these fields.

User will have to configure passphrase if they want secure properties to be exported. If they don’t configure this passphrase secure properties are removed from exported configuration.

While doing import we will check if configured passphrase matches to config which user is trying to import. If it doesn’t match import will fail by default.

Note:
- For backward compatibility any older config import will work fine without any issues.
- Any export done in BMR1 and onward this is mandatory for exporting secure fields.
Troubleshooting Wizard

• Now supported for Tenant “Common”
  • In B release you could not search in Tenant common, only search in user Tenant
Virtualization
SCVMM Clustering

• Support for standalone SCVMM (available in B release)
• Now ACI supports highly available SCVMM as a cluster
  • IP address of VMM domain = Cluster IP or FQDN
  • “Set-Apic-ConnInfo’ PowerShell which sets the certificate information and APIC IP address on host
L3Ext connectivity for WAP tenants

- Microsoft Windows Azure Pack, it allows a tenant network to initiate outgoing traffic destined outside the fabric and to attract traffic from outside.
- BD, EPG, Contract, application profile under tenant “common”
- Default contract required in Tenant “common”
The BD, External EPG naming scheme must be identical to what’s listed in the config guide.
Default provider contract is required
WAP Tenant can now create a Firewall between the “External” and user-defined Network
Cisco ACI Plugin is now officially certified as a Microsoft Partner
ACI Routing
Sharing VRF and L3out Among Tenants
Current Implementation

- BD and subnet, L3outside defined under tenant “common”.
- EPG, Contract, application profile under individual tenants.
- Dynamic routing protocol with external routers.

<table>
<thead>
<tr>
<th>Tenant-Pepsi</th>
<th>Tenant-Coke</th>
<th>Tenant-Common</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td>Web</td>
<td>BD-Coke</td>
</tr>
<tr>
<td>C</td>
<td>App</td>
<td>192.168.102.1/24</td>
</tr>
<tr>
<td>C</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>DB</td>
<td>DB</td>
<td>BD-Pepsi</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.168.101.1/24</td>
</tr>
</tbody>
</table>
• L3outside defined under tenant “common”
• BD, EPG, Contract, application profile under individual tenants
• Static routes with L3outside only for now.

Static route now
dynamic protocol(future)
Access Shared Services Located Out of ACI Fabric

Current Design

- Each tenant has its own VRF (due to overlapping IP). Tenants need to access services/resources reachable via L3out.

- VRF-lite between border leaf and external router.

- Each tenant has its own L3outside connection

- VRF route leak on external router.

- Each tenant needs to define external EPG and contract in order to access the shared services
Sharing L3out Cross VRF
Planned for 11.1 maintenance release

- Each tenant needs to have its own VRF
- L3outside is under tenant “common”. All tenants the same L3outside
- Each tenant can access the shared services provided by workloads in external EPG
- Address L3out and external EPG scale.
TOMORROW starts here.