Cisco Live!
July 10-14, 2016 • Las Vegas, NV
Your Time Is Now
Designing MPLS in Next Generation Data Center: Case Studies

BRKMP-2108
Khalil Jabr – Distinguished Engineer
Satish Kondalam – Technical Leader Engineering
Agenda

• Introduction
• Design Requirements
• Technology Involved
  • DC Network Fabrics – FabricPath, DFA, ACI, and VXLAN with EVPN
  • MPLS Features and Capabilities
  • The Service Layer
  • The WAN Connectivity
• Design Options
• Case Studies
• Lessons Learned
• Conclusion
Session Goals

At the end of the session, the participants should:

- Understand the design requirements
- Understand the technical building blocks
- Understand different designs and use cases and the reasoning behind them
- Understand the lessons learned
Customer Requirements – NG Data Center

- Multi-tenancy
- Highly Scalable DC Architecture
- L2 Connectivity Between Racks
- Optimized for East/West as well as North/South
- Minimize Oversubscription
- Scalable L4-7 Service Layer
- Highly available WAN
- Scalable WAN Architecture
- Some DCs connect via Internet
- Simplicity!
Strategy

- Multi-tenant
- Security and Separation
- Traffic Eng
- Scalable

Virtual FW/LB per tenant
- Flexible placement
- Incremental capacity

Flexible topology
- Minimize oversubscription
- Scale out and scale up
- No spanning tree
- Incremental scale

Network Topology (DC & WAN)

Virtualized L4-7 Services

Network Virtualization

NG DC
Background Info: The Building Blocks
Business Drivers & Solutions for Network Segmentation

- Multi-tenancy
- Mergers Acquisitions
- SOLUTIONS
  - VRF
  - L3VPN
  - Multicast VPN
  - 6VPE
- Compliance
- Shared services
Virtual Routing and Forwarding (VRF)

• Creates independent and separate IPv4 and IPv6 Address Spaces
• Full Unicast and Multicast routing protocols support
• Each non-default VRF is locally-significant on a given router
• Data traffic is not routed across VRFs with the default configuration
Segmentation with VRF lite

Not easy to manage with large number of VRFs
Connecting VRFs Through MPLS

RD: Makes Prefixes Unique
RT: Imports Prefixes into VRF

N7K supports GRE based Multicast VPN (rosen draft 10)
BGP Inter-AS Solution
MPLS Inter-AS Use Cases

- Connecting multi-tenant DCs
- Better Policy Control & Security
- WAN managed by other Vendors
- IGP Isolation
Extending MPLS with Inter-AS

- Back-to-Back VRFs (Option A)
- MP-eBGP for VPNv4 (Option B)
- Multihop MP-eBGP between RRs (Option C)
- MP-eBGP+Labels

ASBR1

AS #1 MPLS

PE11

CE1

VPN-R1

ASBR2

AS #2 MPLS

PE22

CE2

VPN-R2
Deployment & Implementation Scenarios

P-to-P tunneling (MPLS ⇔ MPLS)

- IP WAN Transport
- IPSEC Option for security
- P to P Tunnel
- Looks like an MPLS Link
- Drawbacks:
  - Cumbersome with multiple sites (MPLSoMGRE is an alternate solution)
  - MTU
DC Fabric to MPLS Handoff Designs
Modernized Data Center

Existing 2/3-Tier Designs

Modernized Operating System
Programmable Open APIs

Programmable SDN Overlay Model
L2 & L3 Wire-rate Overlay / Underlay
VXLAN / BGP Control Plane
Third Party Controllers

Application Centric Infrastructure
Any Hypervisor
Physical and Virtual
Open API’s and Controller

Broad and Deep Ecosystem
Fabric Handoff to MPLS

Let’s discuss MPLS handoff for following Fabric:

- vPC
- FabricPath
- Programmable Fabric (FabricPath)
- Programmable Fabric (VXLAN)
- ACI
MPLS Handoff (L3 DCI) for vPC Fabric

AS300
MP-iBGP
VPNv4/VPNv6
WAN
Inter-as Option B

MP-eBGP
VPNv4/ VPNv6

MP-iBGP
VPNv4/ VPNv6

AS100

N7x00
N5000/N6000
N2000

L2/L3 Boundary

RED VLAN <-> Red VRF
Orange VLAN <-> Orange VRF

N5000/N6000
N2000

Inter-as Option B

N5000/N6000
N2000

L2/L3 Boundary

AS200

NX-OS 7.2
DC Fabric w/FabricPath

- Externally the Fabric looks like a single switch
- Internally, ISIS adds Fabric-wide intelligence and ties the elements together.
- Provides in a plug-and-play fashion:
  - Optimal, low latency connectivity any to any
  - High bandwidth, high resiliency
  - Open management and troubleshooting
- ISIS for multipathing and reachability
MPLS Handoff (L3 DCI) for FabricPath

RED VLAN <-> Red VRF
Orange VLAN <-> Orange VRF

AS300
MP-iBGP
VPNv4/VPNv6
WAN

Inter-as Option B

MP-eBGP
VPNv4/VPNv6

L2/L3 Boundary

FabricPath

N7x00

AS 100

N5000/N6000

L2/L3 Boundary

FabricPath

N7x00

AS 200

N5000/N6000
Programmable Fabric
FabricPath & VXLAN
Programmable Fabric (FabricPath & VXLAN)

Bundled 'functions' are 'Modular', 'Flexible' and 'follows' your 'Choice' of 'Integration' and 'Speed' of 'Adoption'!
Programmable Fabric (FabricPath)

Host and Subnet Route Distribution

- DC Fabric with a FabricPath based data plane and MP-iBGP control plane.
- Use MP-iBGP on the leaf nodes to distribute internal host/subnet routes and external reachability information.
- Introduced Segment ID to increase name space to 16M identifier in the fabric.
MPLS (L3) DCI for Programmable Fabric (FabricPath)

IP Forwarding between Fabrics across **Layer-3 based DCI**

**Fabric #1**
- BGP AS 65500

**Fabric #2**
- BGP AS 65505

Leaf switches: N5600/N6000
Spine switches: N5600/N6000 & N7x00(F2e,F3)
BL Switches: N5600/N6000, & N7x00 (F3)
DCI: N7x00 & ASR9000

**Layer-3 DCI (MPLS/L3VPN)**
- BGP AS 65555

**Two Box Solution**
MPLS (L3) DCI for Programmable Fabric (FabricPath)

IP Forwarding between Fabrics across **Layer-3 based DCI**

Fabric #1
BGP AS 65500

MP-iBGP Control plane

Fabric #2
BGP AS 65505

MP-iBGP Control plane

Layer-3 DCI (MPLS/L3VPN)
BGP AS 65555

N7x00 with F3 Single VDC

Single Box Solution
Programmable Fabric (VXLAN)

- Overlay technology with IP underlay
- Overlay tunnel encapsulation is done on VTEP device, it can be a virtual/physical switch.
- Host information like IP & MAC and overlay IP address (VTEP) IP is advertised by a new BGP address (EVPN) family.
- VXLAN header has 24bit VNI field that increases name space to 16M identifier
Control Protocol for VXLAN

VTEPs advertise host routes (IP+MAC) to local hosts

1. East
2. South
3. West

Overlay Forwarding Table
Host1 <MAC,IP>, VTEP IP A
Host2 <MAC,IP>, VTEP IP B

Overlay Forwarding Table
Host1 <MAC,IP>, VTEP IP A

BGP propagates routes for the host to all other VTEPs

Overlay Forwarding Table
Host1 <MAC,IP>, VTEP IP A
Host2 <MAC,IP>, VTEP IP B

BGP Route Reflector

BGP MPLS Based Ethernet VPN (draft-ietf-l2vpn-evpn-02)
Network Virtualization Overlay Solution using EVPN (draft-sd-l2vpn-evpn-overlay-02)
Seamless Host Mobility across DC

Data Center East: BGP AS #100

Data Center West: BGP AS #200

Two DCs are directly connected at the Agg. eVPN Routes exchanged via eBGP

VXLAN Packet

Layer 2 and Layer 3 Multi-Tenancy
Seamless Host Mobility – Intra and Inter DC
MPLS handoff for Programmable Fabric (VXLAN)

Leaf switches: N9300, N9500, N5600 (Roadmap)
Spine switches: N9500, N9300, N7x00
BL switches: N9300, N9500, N7x00(F3)
DCI: N7x00 & ASR9000

N7K NX-OS 7.2

Leafs
VTEP

Spines

RR

RR

BGP EVPN Control Plane
VXLAN Data Plane

VLAN/VRF to VNI

VNI to VLAN/VRF

Border Leafs

Two Box Solution

Inter-AS Option A

MPLS Cloud
MPLS handoff for Programmable Fabric (VXLAN)

Leaf switches: N9300, N9500, N5600 (Roadmap)
Spine switches: N9500, N9300, N7x00
BL Routers: N7x00 (Roadmap), ASR9000 (Summer 2015)
Application Centric Infrastructure (ACI)
Cisco ACI Logical Network Provisioning Stateless Hardware
Cisco ACI Network Profile
Policy-Based Fabric Management

• Extend the principle of Cisco UCS® Manager service profiles to the entire fabric
• Network profile: stateless definition of application requirements
  − Application tiers
  − Connectivity policies
  − Layer 4 – 7 services
  − XML/JSON schema
• Fully abstracted from the infrastructure implementation
  − Removes dependencies of the infrastructure
  − Portable across different data center fabrics

The Network Profile Fully Describes the Application Connectivity Requirements

```xml
<Network-Profile = Production_Web>
  <App-Tier = Web>
    <Connected-To = Application_Client>
      <Connection-Policy = Secure_Firewall_External>
        <Connected-To = Application_Tier>
          <Connection-Policy = Secure_Firewall_Internal & High_Priority>
            ...
            <App-Tier = DataBase>
              <Connected-To = Storage>
                <Connection-Policy = NFS_TCP & High_BW.Low_Latency>
                  ...
```
ACI Adoption – Network (Layer 2 and 3 Fabric)

- Common Commercial, Enterprise, SP Use Case
- Network Operations
- Network Automation
- Any Subnet, Any Where
- Network Capacity and Bandwidth
- With or Without VMM Integration
- L2 used for L4-L7 Integration
- Limited use of contracts

![Diagram showing ACI adoption and network configuration]

Bridge Domain Settings (host BDs):
- ARP Flooding: disabled
- Unicast Routing: enabled
- L2 Unknown Unicast: flood

Bridge Domain Settings (FW_out BD):
- ARP Flooding: enabled
- Unicast Routing: disabled
DC Fabric and WAN/DCI Integration Overview

No worry, I will take care

- Control Plane: MP-BGP (EVPN AF), one session for all tenants
- Data Plane: VXLAN to MPLS interworking
- Auto provisioning: DCI and WAN

Next-gen ACI, VXLAN

Integration Interworking

Scalable, Resilient, Optimized, End-to-End
ACI with Nexus 7k and ASR 9k - DCI

Classical Handoff

- L2 – 802.1Q trunked VLANs
- L3 – iBGP/LISP/OSPFv2/Static VRF-lite (802.1Q data plane)
- 4K VLAN ID space shared by L2 & L3 handoff
  Per VRF VLAN IDs allocated for L3 iBGP peering
ACI to DCI integration and handoff normalization

Handoff Normalization

- Scalable Border-Leaf to DCI peering
  Single Adjacency
  L2 + L3 tenant host information
- MP-BGP Control Plane
- VXLAN Data Plane
- Scalable Tenant Handoff
- Automated Tenant Handoff
Services Layer
Data Center Building Blocks

Multi-tenant Fabric

Data Center 1

- Leaf
- Border Leaf
- Spine
- DC Edge Router

Data Center 2

- Leaf
- Border Leaf
- Spine
- DC Edge Router

Multi-tenant Fabric

AS100

AS200

MPLS Cloud WAN

End user connecting via internet

Campus

End user connecting via internet

AS100

AS200

End user connecting via internet

Campus
Firewall Options

• Three options to consider
  • Virtual Firewall (ASA 1000v) and VSG
    • Virtualized services
    • High scale
    • Leverages vPath technology
  • IOS Zone Based Firewall
    • Router based
    • Native routing
  • ASA
    • Purpose built hardware
    • Advanced firewall and security features

• Next slides explore the ASA and ZBFW options
ASA FW + Fusion Router

• Fusion router:
  • Inter-VPN connectivity
  • Shared resource connectivity
    • Internet, servers, etc.

• ASA contexts:
  • VPN isolation / protection
  • Per VPN policies: ACL, NAT …
  • 256 contexts per FW
  • Map to VLANs

Context functionality available on the ASA
Now With the DC Fabric

SLB local to server VLANs

SLB

Firewall

VRF A
Default Gateway

Common Services

Servers

VRF B
Default Gateway

DMZ/PCI

L2 VNI

Trunk Server VLANs to SLB

L2 VLAN

Firewall

SLB
Def. Gateway

Core
Zone Based Firewall w/ASR1000

- Hardware Based Performance
- IOS Based
- Zone-pair
- VRF-aware
- Fusion VRF (Gray VRF in later slides)
- **Native MPLS Connectivity**
- Per Zone Firewall Policy
Cisco ASR1000: VASI Feature

- A point to point virtual link
- Internal to the router
- Connects two VRFs together
- Allows for direct peering (IGP/BGP)
- Allows for ACLs, NAT, WCCP etc
- VRF aware firewall applied prior to traversing the virtual link
Programmability & Automation on Nexus Switches
Overlay & Underlay Management

- **Overlay** manager
  - Provision VXLAN on Virtual and Physical end-points
  - e.g. VTS

- **NMS/EMS for Underlay** management
  - PoAP, Topology Discovery and Inventory, Telemetry, Image Management, etc.
  - e.g. DCNM

- **Loosely coupled**
  - API for information exchange
  - Combine Underlay/Overlay management under single pane of glass
Virtual Topology System (VTS)

Network-Centric Overlay Provisioning and Management System

- Automated Overlay Provisioning
  - Network Centric group policy model
  - Network Centric Services
  - Service Chaining

- Seamless to Underlay
  - Standalone Nexus 9K, Nexus 2K-7K
  - Software and hardware VTEPs
  - Third-Party (Future)

- Open Standards Based
  - RestFUL Northbound APIs
  - Multi-protocol support
  - Multi-Hypervisor

- Scalable multi-tenantancy
  - MP-BGP control plane
  - Physical and Virtual device support
  - High performance virtual forwarding

- Overlay Management
  - Topology Discovery
  - Manage Overlay resources
  - Overlay troubleshooting

Virtual Topology System (VTS) provides seamless overlay to underlay connectivity, supporting network-centric group policy models, multi-protocol support, and open standards-based APIs. It also offers scalable multi-tenantancy and automated overlay provisioning, ensuring high performance and reliability in network-centric services.
DCNM 7 Fabric Management Views

POAP Device Mapping

VXLAN Overlay, Search

Pod Visualization / Cable Plan

VM Dashboard Integration
DCNM & Cisco Prime Configuration Templates

- Create configuration template using simple template language
- Define Variables for devices and build configuration
- Preview configuration before applying
- Reduce manual errors

Cisco Prime also supports template based configuration for N7K
NXAPI – Providing programmatic access to Nexus switches over HTTP/S (returns output in easy to read JSON format)

#Your python code
#!/usr/env python
import json
import requests
url = "http://172.25.91.139/ins"
payload = [{"jsonrpc": '2.0', 'method': 'cli', 'params': ['show version',1], 'id': '1'}]

#Your python code

Switch# conf t
Switch(config)# feature nxapi
Switch(config)# exit
Show bgp VPNv4 Unicast Summary
Show mpls ldp neighbor
Show ip route vrf vrf1
Ping 10.1.0.1 vrf vrf1

```python
import json
url='http://YOURIP/ins'
switchuser='USERID'
switchpassword='PASSWORD'
myheaders={'content-type':'application/json-rpc'}
payload=[
    {
        "jsonrpc": "2.0",
        "method": "cli",
        "params": {
            "cmd": "show bgp vpnv4 unicast summary",
            "version": 1.2
        }
    },
    {
        "jsonrpc": "2.0",
        "result": {
            "body": {
                "TABLE_vrf": {
                    "ROW_vrf": {
                        "vrf-name-out": "default",
                        "vrf-router-id": "192.168.0.1",
                        "vrf-local-as": "100",
                        "TABLE_af": {
                            "ROW_af": {
                                "af-id": "1",
                                "TABLE_saf": {
                                    "ROW_saf": {
                                        "safi": 128
                                    }
                                }
                            }
                        }
                    }
                }
            }
        }
    }
]
```

Useful for both Configuration and verification scripting
Customer Requirements – Review

- Multi-tenancy
- Highly Scalable DC Architecture
- L2 Connectivity Between Racks
- Optimized for East/West as well as North/South
- Minimize Oversubscription
- Scalable L4-7 Service Layer
- Highly available WAN
- Scalable WAN Architecture
- Some DCs connect via Internet
- Keep it Simple!
Pulling the Building Blocks Together

MPLS  Fabric  WAN  Firewalls
Design Case Studies
MPLS Layer 3 VPN – Multi-POD

• Requirement:
  ➢ Secure Segmentation for Hosted / Enterprise Data Centers or Campus networks via MPLS VPNs

• Solution:
  ➢ One MPLS network infrastructure for all services
  ➢ MPLS PE boundary in POD EoR/ToR access/ aggregation layer
  ➢ Below MPLS boundary: L2 or L3 (VRF-lite with PE-CE)
  ➢ Direct PE-PE or PE-P-PE networks
  ➢ Scaling POD architecture without operational overhead using Fabric Extenders
MPLS Handoff for vPC Fabric

DC Design of a Large Enterprise in India

MPLS WAN

N7700 core switch Aggregating 3 floors

Intra-DC MPLS Cloud

Floor Aggregation Switch

N7700

HSRP MPLS PE

Spine N9500

Server Hall Double sided vPC

Double sided vPC

Leaf N9300

20 Hosts

4 Server Hall per floor

MPLS WAN

Intra-DC MPLS Cloud

Floor Aggregation Switch

N7700

HSRP MPLS PE

Spine N9500

Server Hall Double sided vPC

Leaf N9300

20 Hosts

4 Server Hall per floor
MPLS Handoff for FabricPath Fabric

- Design of a large European university
- Requirement of separating departments and maintain it across campus & Datacenter
- Datacenter built with FabricPath
- Enabled MPLS VPN on DC edge switch and Campus core switch for end to end segmentation from campus to Datacenter.

![Diagram of MPLS Handoff for FabricPath Fabric Case Study]
MPLS Handoff for Standalone Fabric (FabricPath)

• DC Design of a leading natural gas and oil producer from North America

• L3 DCI for Standalone Fabric (FabricPath) with N7700 (F3) Linecard
MPLS to VXLAN Customer Deployment

Leaf switches: N9300, N5600
Spine switches: N7x00,
MPLS Routers: ASR9K
Design Option Leveraging FabricPath
Zone Based Design

- Segmentation by separating default gateway
- Each segment considered a Zone
- Each Zone has unique FWs and LBs
- Can leverage VDCs
- Simple

Case Study: BRKMPL-2108
Design: Firewall Placement w/Virtualization

Case Study
Option 1: Traffic Flow

Case Study
Option 1: Solution w/ASA Cluster

- Use ASA cluster for firewalling
- One ASA context per virtual segment
- **Scale up** by growing ASA cluster and add additional clusters
- VRF or VDC sandwich design
- Core layer is simple. No VRFs.
- Traffic symmetry is automatically handled by ASA cluster
Virtual Firewall per VRF

- VDC or VRF Sandwich Design
- Virtual firewalls assigned to VRF by VLAN association
- One pair of physical or virtual firewall per VRF
- Each firewall requires two VLANs; inside and outside
- Firewall in transparent or routed mode
- Can be made simpler by delegating default gateway functionality to the firewall
Sample VRF w/ASA

Agg001

H3RP .65

Agg002

.67

VLAN100

active .71

FW

VLAN101

.72

204.16.208.64/27

SubAgg001

VLAN102

.68

.69

SubAgg002

VLANs 110-119
IP: 10.1.x.0/24

ACE

.70

Default Gateway
Option 2: Traffic Flow

Case Study
Comparing Options

- **Option1: ASA Firewall**
  - Scales up by way of distributing customers to firewalls and leveraging clusters
  - Stateful HA
  - Purpose built hardware
  - Management tools
  - Inter-VRF traffic flow leverages spine layer

- **Option2: ASR1k ZBFW:**
  - MPLS attached
  - Additional services like NAT and WCCP
  - Hardware forwarding
  - No concerns about trunking VLANs

- There is absolutely nothing wrong with going with either option. The choice is dependent on many factors such as requirements, comfort level with product, management and operations etc.
Option2: Zone Based Firewall (ZBFW)

- ASR1k Hardware Performance
- Native MPLS Attachment
- VRF-Aware
- Attach Anywhere with MPLS Reachability
**Option 2: ZBFW w/VASI Details**

- Native MPLS termination
- **Gray VRF** interconnects tenant VRFs
- Leverage **VASI**
- Each ‘tenant’ gets a security policy zone-pair
- NAT possible and WCCP Possible on VASI
Option 2: Firewall Design w/ Zone Based Firewall

- Redundancy by way of routing
- Active/Standby
  - Leverage metrics
- Limiting factors:
  - Throughput
  - Number of connections
  - Number of conn/sec

Services VRF

MPLS

Gray VRF

VASI

MPLS

VASI

Gray VRF

VRFs 100-199

VRFs 100-199
Option 2: Firewall Design w/ Zone Based Firewall

- Per-VRF loadbalancing
- N+1 redundancy
- Very scalable design
- Grow as you go
- Scalability is additive
Option2: Firewall Design w/Zone Based Firewall

- Second Gray VRF for further segmentation
- Same logic as before
  - Per-vrf loadbalancing
  - Grow as you go
Inter-DC Flow Connectivity

- Symmetric traffic flow is critical
Case Study

- Spine/leaf architecture
- FabricPath for L2 multi-pathing
- No spanning tree
- Default gateway at spine layer
- ASR1ks w/ZBFW for firewall layer
- Nexus 5k/2k at the access
How do I Scale Up?
WAN Design
WAN Requirements

• Highly available
• IGP reconvergence or instability should not affect other DCs
• Minimize state in the WAN
• Add/remove data centers without network outage
• Connect DCs with fiber, leased lines and encrypted tunnels
• Traffic engineering
A WAN Core Layer – Dual Plane

- **IGP Isolation** between each plane
- Isolate topology changes
- Flexible topology
- Highly redundant
- Similar to two provider environments
- Traffic Engineering
Back to Design

- WAN Core routers are co-located in major DCs
- DC Core routers connect directly to WAN core routers
- No connection between WAN core routers
A WAN Core Layer – With Inter-AS

- DCs connect using dark fiber, GRE, or leased lines
- The IGP used in the WAN core is separate
- DCs peer to the WAN core using eBGP
- **Inter-AS option C**
  - Only feed infra routes to WAN Core
  - VPN exchanged between RRs at each DC
- Advantages:
  - Scale & Flexibility
  - IGP Isolation
  - Adding/removing DCs is seamless
  - High level of HA
Imagine

VPN Traffic (blue plane)

Internet Traffic (red plane)
Summary

• CLOS Architecture for Scale and Flexibility
• FabricPath for any VLAN Anywhere in the DC
• Spine layer with Integrated MPLS PE
• Firewalls Native Attached to MPLS
• Scalable Architecture
• Grow as you Go
• Highly Flexible WAN that Scales and Highly Redundant
• Flexible Growth with Multiple DCs
A 6 Geo Example

Global WAN
Big Picture

Sin

SJ

APAC2

EMEA2

Ash

London
A 6 Geo Example
Key to Layout

Circuits Follow Submarine Cables

http://www.submarinecablemap.com
Big Picture

Big Picture w/Regional IWAN
Lessons Learned - 1

• Fabric Scale
  • MAC, SVI and VLAN limits
  • Topology size (number of switch-IDs) and links

• Active/Active HSRP
  • Requires either vPC or GLBP today
  • Anycast HSRP in the 6.2 release. Requires a new release on the N5k (roadmap)

• Hardware Choices
  • FabricPath vs VXLAN vs ACI
  • MPLS Handoff
  • Inter-AS option C on ASR9k today

• Firewall design
  • Asymmetric routing challenges with ASR1k. Requires BGP metric
  • DC to DC flows with symmetry. Requires supernet routes
Lessons Learned - 2

- Inter-AS
  - Option C not supported on N7k yet (roadmap)

- GRE: MTU requirement

- Routing over VASI:
  - OSPF and iBGP were possible options over VASI initially
  - eBGP support with local-AS/Remote-AS support in 3.7.2 release on the ASR1k
  - Deciding on which routes to advertise from Gray VRF requires BGP filters

- MPLS PE placement
  - VRF-lite harder to manage and operate
  - Direct handoff to the Nexus 7k or the ASR9k makes the design simpler

- Virtual firewalls, like the vASA, would make an interesting solution
MPLS Sessions at Cisco Live

- BRKMPL-1100  Introduction to MPLS
- BRKMPL-1102  MPLS Enterprise Switching Product Update and Designs
- BRKMPL-2100  Deploying MPLS Traffic Engineering
- BRKMPL-2102  Designing MPLS-based IP VPNs
- BRKMPL-2108  Designing MPLS in Next Generation Data Center: A Case Study
- BRKMPL-2110  Enterprise MPLS - Customer Case Studies
- BRKMPL-2115  MPLS Architectural approaches for Data Center and Cloud
- BRKMPL-2333  E-VPN & PBB-EVPN: the Next Generation of MPLS-based L2VPN
- BRKMPL-3124  Troubleshooting End-to-End MPLS
- LTRMPL-2104  Cisco WAN Automation Engine (WAE) Network Programmability with Segment Routing
- LTRMPL-3102  Enterprise Network Virtualization using IP and MPLS Technologies: Advanced
- TECMPL-3200  SDN WAN Orchestration in MPLS and Segment Routing Networks
Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.

- Complete your session surveys through the Cisco Live mobile app or from the Session Catalog on CiscoLive.com/us.

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Lunch & Learn
• Meet the Engineer 1:1 meetings
• Related sessions
Please join us for the Service Provider Innovation Talk featuring:

Yvette Kanouff | Senior Vice President and General Manager, SP Business
Joe Cozzolino | Senior Vice President, Cisco Services

Thursday, July 14th, 2016
11:30 am - 12:30 pm, In the Oceanside A room

What to expect from this innovation talk
• Insights on market trends and forecasts
• Preview of key technologies and capabilities
• Innovative demonstrations of the latest and greatest products
• Better understanding of how Cisco can help you succeed

Register to attend the session live now or watch the broadcast on cisco.com
Thank you