Cisco Live!
June 25–29, 2017 • Las Vegas, NV
Migrating Your Existing WAN to Cisco’s IWAN

BRKCRS-2007

Brad Edgeworth, CCIE#31574
Systems Engineer
@BradEdgeworth

Mani Ganesan, CCIE#27200
Product Manager, IWAN
@Mani_network
Cisco Spark

Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

Cisco Spark spaces will be available until July 3, 2017.

cs.co/clus17/#BRKCRS-2007
Introduction

Housekeeping

- “Advanced” Class
  - This is not an ‘Introduction to IWAN’ session
  - This is not an ‘IWAN Design’ session. Some design aspects will be discussed
  - This session is about how to migrate your existing WAN to Cisco’s Intelligent WAN
  - IWAN is prescriptive design. This session covers concepts that match this as much as possible to prevent complex problems during migration.....
  - This session is focused primarily on transport independence and performance routing. Specifically how to deploy it.

We tried to keep things in a logical order as much as possible, but there are some topics that are inter-dependent; so STAY AWAKE!
Recommended Reading

• Explains all key IWAN technologies and components

• VRL labs are available so that you can practice these concepts as you read them in the book

• Copies are available at the CLUS Cisco Press bookstore

Come Meet The Authors

• Anthony, Brad, David, and Jean-Marc are signing books at Cisco Press bookstore on Weds. 1:30 – 2 PM
Agenda

- Sequence of Migration
- Migration Planning and Tools
- End State IWAN Concepts:
  - QoS
  - DMVPN and Routing
- DMVPN Hub Router Placement Strategies
- Migrating Branch Routers
- Other Migration Scenarios (Dual MPLS → Hybrid Model Migration, IPsec Migration)
- Performance Routing (PfR)
Introduction
Intelligent WAN Solution Components

**Transport Independent**
- Consistent operational model
- Simple provider migrations
- Scalable and modular design
- DMVPN IPsec overlay design

**Intelligent Path Control**
- Application best path based on delay, loss, jitter, path preference
- Load balancing for full utilization of all bandwidth
- Improved network availability
- Performance Routing (PfR)

**Application Optimization**
- **AVC**: Application monitoring with Application Visibility and Control
- **WAAS**: Intelligent Edge Caching with Akamai Connect
- **WAAS**: Application Acceleration and bandwidth savings

**Secure Connectivity**
- Certified strong encryption
- Comprehensive threat defense with ASA and IOS firewall/IPS
- Scalable secure Direct Internet Access
Where to start?

IWAN is not all or nothing – so deploy in phases if that’s easier

DIA and App Optimization (WAAS and Akamai) can be deployed anytime during the process.

Start with transport independence before adding path control
- DMVPN is needed to run Performance Routing (PfRV3)
- Provides us consistent overlay routing across all transports

This session is focused on Transport Independence, PfR and Connectivity. This matters the most during migration
IWAN Topology

• Lan Prefixes:
  • 10.0.0.0/8 (Site Location is 2nd Octet)
  • HQ is 10.1.0.0/16 & 10.2.0.0/16
  • Remote Sites:
    • 10.3.0.0/16
    • 10.4.0.0/16
    • 10.5.0.0/16

• DMVPN Hub Routers
  • R11 & R21 MPLS Transport
  • R12 & R22 Internet Transport

• Transport:
  • 172.16.0.0/16 MPLS
  • 100.64.0.0/16 Internet
Planning the Migration
Why Migration Planning is critical?

- Moving all branch traffic from underlay to Overlay tunnels → Can be complicated
- WAN Migration may last for weeks for months
- Need to Maintain Universal connectivity between legacy and IWAN sites that are migrated
- Choose the right sites to act as migration sites (during migration phase) – based on circuit speeds and device capacity
- What is being migrated? All Branches or leaving some sites on the legacy WAN?
Where Do We Start Our IWAN Migration?

Gather Information and document them

- Inventory
- Licenses
- Software Version
- Top applications with AVC
- Existing Routing Design
- QoS Design
- Sites with Backdoor Links
Branch Optimization Analysis

Mon 21 Oct 2013 01:16 PM - ATL-xxx

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Input 5min (bps)</th>
<th>Output 5min (bps)</th>
<th>Input 5min Max (bps)</th>
<th>Output 5min Max (bps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>exchange</td>
<td>0</td>
<td>120000</td>
<td>2811000</td>
<td>1958000</td>
</tr>
<tr>
<td>skype</td>
<td>0</td>
<td>0</td>
<td>2678000</td>
<td>1879000</td>
</tr>
<tr>
<td>ftp</td>
<td>0</td>
<td>0</td>
<td>1595000</td>
<td>964000</td>
</tr>
<tr>
<td>rtp</td>
<td>0</td>
<td>0</td>
<td>2147000</td>
<td>61000</td>
</tr>
<tr>
<td>h323</td>
<td>0</td>
<td>0</td>
<td>1152000</td>
<td>569000</td>
</tr>
<tr>
<td>edonkey</td>
<td>0</td>
<td>0</td>
<td>810000</td>
<td>750000</td>
</tr>
<tr>
<td>Total</td>
<td>1409000</td>
<td>469000</td>
<td>30711000</td>
<td>16394000</td>
</tr>
</tbody>
</table>

Branch Optimization Analysis

c881#show flow monitor FLOWMON cache app name
Processed 32 flows
Aggregated to 9 flows

<table>
<thead>
<tr>
<th>APP NAME</th>
<th>flows</th>
<th>bytes</th>
<th>pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>prot icmp</td>
<td>4</td>
<td>7991530</td>
<td>5842</td>
</tr>
<tr>
<td>port http</td>
<td>4</td>
<td>407184</td>
<td>506</td>
</tr>
<tr>
<td>port netbios-ns</td>
<td>14</td>
<td>636420</td>
<td>1320</td>
</tr>
<tr>
<td>port ntp</td>
<td>4</td>
<td>407184</td>
<td>506</td>
</tr>
<tr>
<td>port ssh</td>
<td>1</td>
<td>14352</td>
<td>198</td>
</tr>
<tr>
<td>port dropbox</td>
<td>4</td>
<td>1216</td>
<td>6</td>
</tr>
<tr>
<td>port isakmp</td>
<td>2</td>
<td>58</td>
<td>2</td>
</tr>
</tbody>
</table>
### Capacity Management – Branch NBAR View

#### BU3 (top 10 apps) – 3Mbps sites

<table>
<thead>
<tr>
<th>App</th>
<th>Max bps (input) *</th>
<th>Max bps (output) *</th>
<th>Observations</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>2.9Mbps</td>
<td>2Mbps</td>
<td>Bandwidth Hog</td>
</tr>
<tr>
<td>Skype</td>
<td>2.4Mbps</td>
<td>2.2Mbps</td>
<td>Unauthorized App/Bandwidth Hog</td>
</tr>
<tr>
<td>Exchange</td>
<td>2.7Mbps</td>
<td>1.6Mbps</td>
<td>Bandwidth Hog</td>
</tr>
<tr>
<td>FTP</td>
<td>1.9Mbps</td>
<td>negligible</td>
<td>High Bandwidth Usage</td>
</tr>
<tr>
<td>eDonkey</td>
<td>1Mbps</td>
<td>1Mbps</td>
<td>Unauthorized/High Bandwidth Usage</td>
</tr>
<tr>
<td>RTP</td>
<td>1.3Mbps</td>
<td>750Kbps</td>
<td>High Volume/High Bandwidth Usage</td>
</tr>
<tr>
<td>Novadigm</td>
<td>1.1Mbps</td>
<td>400Kbps</td>
<td>Investigate</td>
</tr>
<tr>
<td>Skinny</td>
<td>1.6Mbps</td>
<td>negligible</td>
<td>High Volume/High Bandwidth Usage</td>
</tr>
<tr>
<td>Fasttrack</td>
<td>700Kbps</td>
<td>270Kbps</td>
<td>Unauthorized/High Bandwidth Usage</td>
</tr>
<tr>
<td>Citrix</td>
<td>1.2Mbps</td>
<td>negligible</td>
<td>High Bandwidth Usage/Monitor Latency</td>
</tr>
</tbody>
</table>

#### BU1 (top 10 apps) – 3-6Mbps sites

<table>
<thead>
<tr>
<th>App</th>
<th>Max bps (input) *</th>
<th>Max bps (output) *</th>
<th>Observations</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSLOG</td>
<td>negligible</td>
<td>Max Capacity</td>
<td>Bandwidth Hog</td>
</tr>
<tr>
<td>HTTP</td>
<td>Max Capacity</td>
<td>1Mbps</td>
<td>Bandwidth Hog</td>
</tr>
<tr>
<td>Secure HTTP</td>
<td>Max Capacity</td>
<td>600Kbps</td>
<td>Bandwidth Hog</td>
</tr>
<tr>
<td>IMAP</td>
<td>950Kbps</td>
<td>700Kbps</td>
<td>High Bandwidth Usage</td>
</tr>
<tr>
<td>SMTP</td>
<td>30Kbps</td>
<td>800Kbps</td>
<td>High Bandwidth Usage</td>
</tr>
<tr>
<td>Exchange</td>
<td>1.7Mbps</td>
<td>400Kbps</td>
<td>High Bandwidth Usage</td>
</tr>
<tr>
<td>Skype</td>
<td>600Kbps</td>
<td>1.2Mbps</td>
<td>Unauthorized/High Bandwidth Usage</td>
</tr>
<tr>
<td>eDonkey</td>
<td>250Kbps</td>
<td>600Kbps</td>
<td>Unauthorized/High Bandwidth Usage</td>
</tr>
<tr>
<td>Citrix</td>
<td>450Kbps</td>
<td>200Kbps</td>
<td>Monitor Latency</td>
</tr>
<tr>
<td>Xwindows</td>
<td>500Kbps</td>
<td>500Kbps</td>
<td>Check Security Impact</td>
</tr>
</tbody>
</table>

Depending on the type of network traffic, DIA deployment could be accelerated.
Migration steps

• Finalize the Design
• Deploy IWAN via a POC or Production Pilot
  • Learn the technology
  • Learn the applications
  • Test the migration strategy
  • Collect results from any POC/Production Pilot
• Identify sites for migration
• Make changes to infrastructure (if H/W upgrades are needed)
• Hub deployment
• Cut-Over Branches
• Clean-Up
Tools to simplify Deployment and Migration

- Application Policy Infrastructure Controller (APIC-EM)
- Prime Infrastructure IWAN Workflow
- CLI
Cisco Intelligent WAN App for APIC-EM

- Business Policy: App SLA
- Application Network Profile
- DMVPN SLA QoS Security Path Selection
- Simple Workflow Templates
- Zero Touch Provisioning
- Network, Applications Monitoring
- Business Level Policies
- Open Architecture

Business Policy Dictates Network Action
How can I easily connect new sites to the data center and enable the IWAN technologies?
End State IWAN Concepts: Quality of Service
Need for QoS from IWAN Perspective

- Replacing expensive MPLS service with business class internet
- PfR to load balance / provide resiliency / best path
- DMVPN overlay on MPLS and Internet
- Up to 2,000 remote sites per hub router in a single domain
- MPLS transport will have SP QoS, but with Internet transport we assume none
DMVPN Per Tunnel QoS

- Per-Site Shaping to Avoid Overruns
- Hub to spoke only

100 Mbps in to DMVPN cloud can easily overrun the lower speed committed rates at spoke sites.
IWAN QoS Requirements

Bandwidth Sharing Between Tunnels
Shape for Remote Site Last Mile

Shape for Service Rate

Per Site Bandwidth Sharing Within Tunnel

Hub BR

80 Mbps GE Service Rate

1.5 Mbps T1 Branch
1.5 Mbps T1 Branch
1.5 Mbps T1 Branch
45 Mbps T3 Branch
45 Mbps T3 Branch
10 Mbps T3 Branch
10 Mbps T3 Branch
45 Mbps T3 Branch
45 Mbps T3 Branch
10 Mbps T3 Branch
QOS settings for PFR

- QoS is based upon the following logic:
  - Ingress traffic is classified and marked accordingly (if not done elsewhere)
  - Egress traffic is shaped/queue based on QoS marking

- PFR maps traffic to classes based on the DSCP marking or application names. LAN Traffic should be marked on Ingress or before hitting the BRs

- As a best practice, use the same class names in PFR that were used for the QoS policies. Match DSCP for each PfR class with the DSCP used for the QoS policies.
  - Ensures DSCP is consistent between QOS and PFR policies
  - Makes it easier to identify the PFR policies
End State IWAN Concepts: DMVPN Tunnels and Routing
Various Acceptable DMVPN Layouts

Direct Connection

CE Router at Hub and Spoke

FW Protects Hub

Complex Scenario

R11 – DMVPN Hub

R41 – DMVPN Spoke
Internet Access Models

Centralized Access Model
Internet and Internal traffic routes across the WAN
A simple default route can be used for Internet traffic and Internal traffic

Distributed Access Model
Internet traffic routes direct to the ISP
A simple default route can be used for Internet traffic pointing to ISP
Internal traffic routes across the WAN
A simple default route can **NOT** be used for Internal traffic.
Route Summarization

• Advertise DC Specific Routes

• DC Specific Summaries:
  • 10.1.0.0/16
  • 10.2.0.0/16

• All DMVPN hubs advertise Enterprise prefix summary routes (10.0.0.0/8) for all the LAN and WAN networks

• DMVPN hubs advertise a default route that provides Internet connectivity.
IWAN EIGRP Routing Design

- Same EIGRP AS # for LAN and WAN
- DMVPN Hub advertise Default and Summary Route
- Delay added on to influence PfR uncontrolled traffic
- EIGRP Stub Site Feature on Branches
IWAN BGP Routing Flow

Branches with Directly Connected

Branches with Multiple Routers
DMVPN Migration: Hub Routers and Routing Logic
Network Traffic Flows During Migration

- Site-to-Site Traffic in Legacy WAN
- Site-to-Site Traffic in IWAN
- Traffic between Legacy and IWAN networks must flow through a migration site. This is located with the DMVPN hubs.
Three Methods of Hub Deployment or Migration

**Greenfield**
- New DMVPN Hub Routers
- New Circuits
- Simple Design

**Intermediate (IBlock)**
- New DMVPN Hub Routers
- Existing Circuits
- Medium Design

**Condensed**
- Existing CE Routers
- Existing Circuits
- Increased Complexity

Spoke Migration is not impacted by the Hub model.
Transport Drawing

Connectivity showed logical structure

Physical connectivity looks like

Sub-Interfaces can separate:
- **P2P traffic** (/30 IP on Sub-Interface)
- **Transit switching** (VLAN on MLS)

The same concept can apply to transport connectivity too.
Greenfield Deployment

Greenfield

- New DMVPN Hub Routers
- New Circuits
- Simple Design

- Not restricted to constraints of existing network
- The only routing interaction required with the existing network is connectivity to the LAN (Migration Site)
- Simple Post-Migration Cleanup Removal of CE1 and CE2
- Typically used when deploying new circuits or a parallel network
Greenfield Migration Routing Pattern

Benefits:
• Isolated environment. Changes on CE1 do not impact IWAN environment.
• Simple routing configuration
• Easy to troubleshoot and trace packet flows
• Bandwidth is sized appropriately for DMVPN traffic only.
• QoS policy on DMVPN hub is separated from Legacy QoS policy

Cons:
• Cost and timeline for new circuits
Intermediate Deployment

Intermediate (IBlock)
- New DMVPN Hub Routers
- Existing Circuits
- Medium Design

- Some constraints of existing network
- Existing circuits to SP are used. New links (logical/physical) between CEs and DMVPN hubs are required.
- CEs must advertise these new links to the SP so that spokes know how to reach the DMVPN hubs.
- Connectivity to the LAN is straightforward.
- Post-migration cleanup may be required
Intermediate Migration Routing Pattern

Benefits:
• Simple routing configuration
• Easy to troubleshoot and trace packet flows
• QoS policy on DMVPN hub is separated from Legacy QoS policy

Cons:
• Bandwidth for CE1 to the SP network must be sized accordingly.
• Changes on CE1 could impact IWAN environment.
• Some Clean-Up after Migration
IWAN Routing Protocol Diagram During Migration

EIGRP
IWAN Routing Protocol Diagram During Migration

BGP
Condensed Deployment

**Condensed**
- Existing CE Routers (verify capability)
- Existing Circuits
- Increased Complexity (QoS / Routing)

Do not Deviate from the I WAN CVD with this model, or be prepared to face problems or complications during migration.
Condensed Migration Routing Pattern

Benefits:
• Cost
• No real Clean-Up after Migration

Cons:
• Outage to all WAN networks is required during cutover.
• Advanced Routing (VRF Leaking)
• Hierarchical QoS is Not Supported on transport interface. If needed for legacy network, this prevents per-tunnel-QoS on DMVPN tunnel.
• Does your existing WAN have per-tunnel QoS? This could be enabled later
vrf definition MPLS01
  address-family ipv4
    import ipv4 unicast map VRF-LEAK-TO-MPLS01
    export ipv4 unicast map VRF-LEAK-FROM-MPLS01

! These route-maps are used to Permit/Block Routes between the VRF and Global BGP Tables
route-map VRF-LEAK-TO-MPLS01 permit 10
  match ip address prefix-list LEAK-TO-MPLS01
route-map VRF-LEAK-FROM-MPLS01 permit 10
  match ip address prefix-list LEAK-FROM-MPLS01
ip prefix-list VRF-LEAK-TO-MPLS01 permit 0.0.0.0/0 le 32
ip prefix-list VRF-LEAK-FROM-MPLS01 permit 0.0.0.0/0 le 32

router bgp 10
  address-family ipv4 vrf MPLS01
    neighbor 172.16.11.2 remote-as 65000
    neighbor 172.16.11.2 activate

! The local-as command is not required; but allows you to use a standard ASN for IWAN and still peer to MPLS SP using the ASN they want you to use
    neighbor 172.16.11.2 local-as 11 no-prepend replace-as dual-as
### Condensed - Leaking Routes Between BGP Global & VRF Tables

R11-DC1-Hub1# **show bgp ipv4 unicast**

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt;, 10.0.0.0</td>
<td>0.0.0.0</td>
<td>32768</td>
<td>i</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*&gt;, 10.1.0.0/16</td>
<td>0.0.0.0</td>
<td>32768</td>
<td>i</td>
<td></td>
<td></td>
</tr>
<tr>
<td>s&gt;, 10.1.0.11/32</td>
<td>0.0.0.0</td>
<td>0</td>
<td></td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>s&gt;, 10.1.12.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td></td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>s&gt;, 10.1.111.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td></td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>s&gt;i, 10.3.0.31/32</td>
<td>192.168.100.31</td>
<td>0</td>
<td>100</td>
<td>50000</td>
<td>?</td>
</tr>
<tr>
<td>s&gt;i, 10.3.3.0/24</td>
<td>192.168.100.31</td>
<td>0</td>
<td>100</td>
<td>50000</td>
<td>?</td>
</tr>
<tr>
<td>s&gt;, 10.4.0.41/32</td>
<td>172.16.11.2</td>
<td>0</td>
<td>65000</td>
<td>41</td>
<td>?</td>
</tr>
<tr>
<td>s&gt;, 10.4.4.0/24</td>
<td>172.16.11.2</td>
<td>0</td>
<td>65000</td>
<td>41</td>
<td>?</td>
</tr>
<tr>
<td>s&gt;, 10.5.0.51/32</td>
<td>172.16.11.2</td>
<td>0</td>
<td>65000</td>
<td>51</td>
<td>?</td>
</tr>
<tr>
<td>s&gt;, 10.5.0.52/32</td>
<td>172.16.11.2</td>
<td>0</td>
<td>65000</td>
<td>51</td>
<td>?</td>
</tr>
</tbody>
</table>
R11-DC1-Hub1# `show ip route bgp`

<table>
<thead>
<tr>
<th></th>
<th>Route Description</th>
<th>Age</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>10.0.0.0/8 [19/0], 04:34:53, Null0</td>
<td>Null0</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>10.1.0.0/16 [19/0], 04:34:53, Null0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>10.3.0.31/32 [19/0] via 192.168.100.31, 00:22:19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>10.3.3.0/24 [19/0] via 192.168.100.31, 00:22:19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>10.4.0.41/32 [201/0] via 172.16.11.2 (MPLS01), 00:28:19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>10.4.4.0/24 [201/0] via 172.16.11.2 (MPLS01), 00:28:19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>10.5.0.51/32 [201/0] via 172.16.11.2 (MPLS01), 00:28:19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>10.5.0.52/32 [201/0] via 172.16.11.2 (MPLS01), 00:28:19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>10.5.5.0/24 [201/0] via 172.16.11.2 (MPLS01), 00:28:19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>10.5.12.0/24 [201/0] via 172.16.11.2 (MPLS01), 00:28:19</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Other Condensed Techniques May Technically Work.....

Be aware of your traffic patterns:
- IWAN to Legacy
- IWAN to DC
- Legacy to DC

Additional load for transit traffic

Clean-up is still needed later on:
- Encapsulating tunnel IP changes

Going off the tried and true path may lead to problems later!
Hub Deployment Summary

Greenfield

• Keep It Simple Stupid (KISS). Remember your operations staff.
• Use Greenfield or IBlock when possible
  • Depending on bandwidth CSR1000Vs could be used
• Don’t go crazy if you go Condensed
IBlock Hub Deployment Demo
Migration Site - IBlock Deployment

Migration Site

DMVPN Hub
Routers

10.1.11.0/24

172.16.11.0/24

DMVPN Tunnel

Intelligent
WAN

Legacy CE
Routers

172.16.13.0/24

Legacy WAN

172.16.13.0/24

Site 3

SP

Site 4

DMVPN Hub

R11

CE1

R31

R41
Checking the Environment

• Verify the CE router is advertising the IBlock Transit Link
• Verify the IBlock Hub Router can reach Branch Legacy Networks
DMVPN Migration: Branch Routers
Branch Pre-Migration Tasks

• Make a list of what network applications work and what applications do *not work* before migrating the branch.

• Backup the existing router configurations to the local router & centralized repository.

• Allow local authentication / authorization to allow access to the router in a timely manner (assuming that TACACS or radius servers cannot be reached).

• Allow remote console sessions on routers from the workstation, and any peer routers.
Branch Migration Activities

During the migration the following tasks are done:

- DMVPN tunnel configuration
- Certificate enrollment if IPsec Tunnel Protection uses PKI
- Association of FVRF to the Encapsulating Interface
- Routing protocol changes
- PfR configuration deployed
Connectivity During Migration

- When the FVRF is associated to the transport interface, the IP address is removed from that interface.

  R31-Site3(config-if)#vrf forwarding MPLS01
  % Interface GigabitEthernet0/1 IPv4 disabled and address(es) removed due to enabling VRF MPLS01
  R31-Site3(config-if)#ip address 172.16.31.1 255.255.255.252

- If there is a backdoor between sites, migrate those sites together
  - prevents possibility of route loops and transit routing
Assess the Connectivity Model at Branch

• Depending on the site’s connectivity model, the migration could be executed without loss of service to the users at the branch.

• Typically, remote sites have:
  - Single router with single transport
  - Single router with dual transport
  - Dual router with dual transport

Decide if migrations are remote or on-site
Migration Scripts

• Cisco tools use these or can be used for CLI

• Prevents for Typos/Fat-Fingering

• Allows for off-site migration

Example: EEM script allows for multiple commands to be entered even if console connectivity is lost.

```plaintext
event manager applet MIGRATE-PORTION
  event none
  action 010 cli command "enable"
  action 020 cli command "configure terminal"
  action 030 cli command "interface GigabitEthernet0/2"
  action 040 cli command "vrf forwarding INET01"
  action 050 cli command "ip address dhcp"
  ! Wait 20 seconds to allow DHCP to get a packet before no shutting tunnel
  action 060 wait 20
  action 070 99 syslog msg "FVRF Associated to Gi0/2"
```
Advanced EEM Script that Configures Routing Too!

! The wait command allows for the interface to obtain an IP address from DHCP
! Before the Internet DMVPN tunnel is brought online
   action 120 wait 15
   action 130 cli command "interface Tunnel 200"
   action 140 cli command "no shut"
   action 150 syslog msg "Interface Configurations Performed"
! The last section is to remove the previous routing protocol configuration.
! And then configure the routing protocols. Only a portion of this activity
! is shown, but this section should be completed based on your design.
   action 160 cli command "no router bgp 65000"
   action 170 cli command "no router ospf 1"
   action 180 cli command "router eigrp IWAN"
! Continue with rest of routing protocol configuration
   action 999 syslog msg "Migration Complete"
Migrating a Branch Router

Configure DMVPN

Configure EEM applet

** Copy run start

** Copy run start

** Reload in 15

Execute EEM

Connect back to router

Configure overlay routing

** reload cancel

** Recommended for CLI Migrations

Tunnel will remain down with no FVRF interface

• Either on Tunnel or FVRF

• Remove any existing routing

The entire process could be captured by a script

** Recommended for CLI Migrations

Tunnel will remain down with no FVRF interface

** Recommended for CLI Migrations

The entire process could be captured by a script
Branch Migration Demo
All Branches are Connected to Legacy Network
Things We Will Look At

- BGP Table
- The Routing Table
- Traffic Pattern from R41 to R31 (Traceroute from R41 to R31)
- DMVPN Status
R31 has been Migrated to IWAN

Migration Site

DMVPN Hub Routers
R11 10.1.11.0/24

Legacy CE Routers
CE1 10.1.13.0/24

Intelligent WAN
192.168.100.0/24

Site 3
R31

172.16.41.0/24

SP

172.16.13.0/24

Legacy WAN

172.16.13.0/24

Site 4
R41

192.168.100.0/24
Let’s Migrate R31 and Look At:

• BGP Table (Shouldn’t exist on R31)
• The Routing Table
• Traffic Pattern from R41 to R31 (Traceroute from R41 to R31)
• DMVPN Status
R31 and R41 are now both on IWAN

Migration Site

DMVPN Hub
Routers

Legacy CE
Routers

R11

Intelligent
WAN

192.168.100.0/24

Site 3

Site 4

CE1

Legacy
WAN

192.168.100.0/24

Site 4

Site 3

Legacy
WAN
Let’s Migrate R41 and Look At:

• BGP Table (Shouldn’t exist on R41)
• The Routing Table
• Traffic Pattern from R41 to R31 (Traceroute from R41 to R31)
• DMVPN Status
Post-Migration Cleanup
Post- Migration

If the final IWAN design does not migrate all devices to IWAN, then stop here!

Migration is considered complete once:

- All of the planned sites are communicating only via overlay tunnels
- The service provider network is used only for transport between DMVPN routers.
- The last task is to clean up the environment:
  - **Greenfield** – Remove previous WAN routers
  - **Intermediate (IBlock)** – Removal of link between LAN and CE Routers
    Potential removal of CE links
  - **Condensed** – Remove BGP Route Leaking Configuration
Post-Migration Clean-Up for Intermediate

Link Not Needed

DMVPN Hub

MPLS Network

DMVPN Spokes
Connect to This Interface

MPLS Network

DMVPN
Removal of the CE Device

CE1 could be removed depending on the following factors:

• Who owns the device? Your organization or the service provider?

• What additional value does CE1 add to the design or operational perspective?
Post Migration Clean up
CE Removal

- While removing CE1, if the cable connecting to the MPLS network & CE1 is pulled from CE1 and plugged into R11, DMVPN connectivity is going to break.

- R11’s IP address is on the 172.16.11.0/30 network and the service provider’s PE router is on the 172.16.13.0/30 network. One of the devices will have to change their IP address.

- DMVPN Spoke mappings is configured to the 172.16.11.1 NBMA Address.
Post Migration Clean up
How to fix IP Addressing Problem

Connectivity is restored by:

- Re-configure the NHRP on every branch site
  - Either add a second NBMA address (only 1 active at a time on each spoke)

- Terminate the DMVPN Tunnel on a Loopback
  - Little more complexity in VRF Routing & additional IP addresses consumed.

- Coordinate IP address change with SP and migrate 1 DMVPN hub at a time.
  - SP would change the IP addressing on the peer link.
Case Study: Migrating at Scale
Migration Site Traffic Flows

New York is the Migration Site

35 MS – Los Angeles to New York
25 MS – Miami to New York
70 MS total Los Angeles to Miami using Migration Site

Within VoIP Guidelines
Migrating Multiple Regions

New York is the Migration Site

130 MS – Madrid to New York
150 MS – Milan to New York
280 MS total Madrid to Milan using Migration Site

Exceeds VOIP Guidelines

Direct is 50-70 MS which is in VOIP Guidelines
Migrating Multiple Regions

Install a Migration Site in London
Install a Migration Site in New York.

London and New York are connected by existing WAN transport

IWAN Branches have Tunnels to both Hub Sites
Migrating Multiple Regions

IWAN Branches have Tunnels to both Hub Sites.

Europe Branches prefer to connect to all networks via the London Hub (regardless of Branch location)

U.S Branches prefer to connect to all networks via the U.S Hub (regardless of Branch location)
Think about how the transport connects across the continents.

Limited connection points and probably riding the same transport as if they were direct.

Examine traffic flows and try to migrate by regions, to prevent Branch site-to-site traffic patterns that exceed recommended performance guidelines.
Reasons for not having regional migration…

Hardware cannot support Hub functionality

Bandwidth concerns at proposed hub sites cannot handle additional load for migration traffic.
Alternate to using Regional Migration Site:
Routing Flows that Need to be Examined:

Uses FVRF Route Leaking with Conditional Approval/Reject
(as shown in Condensed Configuration)

Receiving Routes at IWAN Branch
- (Transport Side)
- (From IWAN Hub)

Advertising Routes at IWAN Branch
- Towards the IWAN Hub
  *(What happens to those routes after the IWAN Hub)*
- Towards the Transport

Advertising DC Routes to Transport
Receiving Routes at IWAN Branch (From IWAN Hub)

Hub receives the route, but advertises a summary that contains it.

Branch receives the hub summary and tags it. That route is not leaked from Global to FVRF.

Branch tags on receipt and blocked from insertion to FVRF

VRF Export Map Blocks Tag
Receiving Routes at IWAN Branch (From Transport)

Branch receives the branch route in a FVRF routing protocol and tags it.

Branch checks and blocks any routes advertised from another IWAN Site.

Route is leaked from FVRF into Global.

Route is blocked from being advertised to the hubs.

Branch tags on receipt and blocked from advertisement to Hub.
Route Selection at IWAN Branch

Longest match wins.

IWAN Branch will go direct through SP transport.
Advertising Routes at IWAN Branch (Towards IWAN Hub)

Branch advertises the route to Hub

Hub advertises to CE router
CE router prepends AS or blocks
SP advertises to R61
Advertising Routes at IWAN Branch (Towards Transport)

Branch advertises route to SP with BGP community.

SP advertises route to Migration CE, and is blocked by community.

Route via IWAN Path is preferred.

SP advertises route to remote branch

Branch route is filtered on CE inbound from transport
Route Selection at Legacy Branch

Shortest AS-Path Wins

Traffic from R31’s transport (leaked) interface is preferred
Preventing Transport Routing Between IWAN Sites

IWAN Branch receives the other IWAN Branch route in a FVRF routing protocol, but it is blocked because the community matches what IWAN Branches advertise to the transport.

Branch blocks routes with community used by other IWAN routers.

If R61 is IWAN, Block the 100:100 Community Inbound.
Advertising DC Routes to Transport

CE advertises routes to SP with BGP Community 100:200

SP advertises route to Remote Branch which accepts the route.

SP advertises route to IWAN Branch which discards based on community.

IWAN Branch uses Summary Route (via R11)

IWAN Branch discards route based on 100:200 BGP Community
Keep in Mind About Not Using a Migration Site

- There is a lot of route tagging and leaking between VRFs.
- This can cause confusion for operation staff and Junior Network Engineers
- How much traffic do you have that really falls in to the use case scenario? Could these sites be grouped together, to keep things simple?
Case Study: Migration from Dual MPLS to Hybrid Model
Migration from Dual MPLS to Hybrid Model

- Traditional Dual MPLS with Mutual Redistribution between IGP and BGP
- Install new MPLS1 DMVPN Hub (Just like shown earlier)
- Install new Internet DMVPN Hub
- Turn up DMVPN interfaces on MPLS and Internet Hubs
- Migrate Branch Sites.
  - MPLS1 → MPLS1 DMVPN Tunnel
  - Install new Internet Circuit
  - Internet DMVPN Tunnel turned up
  - MPLS2 → Shutdown and Circuit termination
Clean-Up from Dual MPLS to Hybrid Model

Now that all sites have migrated on to IWAN, there is not a need for connectivity to MPLS SP2.

- Remove CE2 (Connected to MPLS SP2)
- Remove the link between MLS5 and CE1
Now comes the decision to remove CE1 or keep it. If it is removed, then this is what your topology will look like.
Case Study: Migration of VPLS or Metro Ethernet Topologies
• Router cannot forward L3 and L2 on the same interface
• Requires Insertion of a Switch from VPLS Hand-off
• QoS Shaping can be done outbound on newly inserted switch

Same Subnet on CE1 and DMVPN FVRF Interface
Case Study: Migration of Existing Point-to-Point IPsec Topologies
Migrating P2P IPSEC WAN to IWAN

- Add the DMVPN hub router into the network

- The placement of hub depends on where the IPSEC tunnels are currently terminated – Firewall or a router

If IPSEC is terminated on FW, then place the hub router behind it (pass-through)

- Migrate sites based on traffic patterns - Non-transit sites first
Important PfR Concepts for IWAN
Performance Routing v3
Running in an Enterprise Domain

- One Master Controller defined as the Hub MC
- Centralized location for policy definition

BRKRSST-3362 Implementing Performance Routing
Deploying Intelligent Path Control

Prepare to run PFR

- DMVPN is a Requirement for PfR

- Policy
  - Start with a Single Class and Load Balancing disabled
    - All other classes will follow routing
  - Enable an additional class
    - Monitor Traffic Classes and Load on the Network (CPU, Interface Utilization etc.)
  - Enable additional classes and load balancing
  - Three Performance Classes, Voice, Video, and Critical Application, plus Load Balancing is a good start to baseline.
Enterprise Prefix

**Legacy Site Prefixes**

**Branch Site Prefixes**

**Hub Site Prefixes**

Site prefixes for particular sites with PFRv3 enabled

Branches learn Site Prefixes Dynamically (or statically configured)

Hubs act as transit sites – site-prefix statically defined

Without Enterprise-Prefix: all the traffic between PfR sites will be learned as PfR Internet traffic class and delay, jitter, etc. cannot be monitored.

* Only Routing is used between Non-PfR and PfR enabled site in Enterprise Prefix

**Placing Legacy Site Prefixes at Hub Sites, provides PfR for half of the path**
Hubs: Site-Prefix lists before anything is migrated

Enterprise Prefix: 10.0.0.0/8
Site1 Prefix-List: 10.1.0.0/16

Migration Site

DMVPN Hub Routers
R11  R12

Legacy CE Routers
CE1  CE2

Intelligent WAN

Routing

Legacy WAN

Site 3

Site 4
Hub MC (R10)
domain IWAN
vrf default
  master hub
    enterprise-prefix prefix-list ENTERPRISE_PREFIX
    site-prefixes prefix-list SITE_PREFIX

!
ip prefix-list ENTERPRISE_PREFIX seq 10 permit 10.0.0.0/8
ip prefix-list SITE_PREFIX seq 10 permit 10.1.0.0/16
# Hub1 Site- Prefix Table Before Anything is Migrated

```
R10-DC1-MC#show domain IWAN master site-prefix
  Change will be published between 5-60 seconds
  Next Publish 01:46:29 later
  Prefix DB Origin: 10.1.0.10
  Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured; M-
  shared

<table>
<thead>
<tr>
<th>Site-id</th>
<th>Site-prefix</th>
<th>Last Updated</th>
<th>DC Bitmap</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.0.10</td>
<td>10.1.0.10/32</td>
<td>00:13:41 ago</td>
<td>0x1</td>
<td>L</td>
</tr>
<tr>
<td>10.1.0.10</td>
<td>10.1.0.0/16</td>
<td>00:13:41 ago</td>
<td>0x1</td>
<td>C,M</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>*10.0.0.0/8</td>
<td>00:13:41 ago</td>
<td>0x1</td>
<td>T</td>
</tr>
</tbody>
</table>
```

BRKCRS-2007 © 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public 103
R31 on Site 3 migrated to IWAN

Migration Site

DMVPN Hub Routers

R11
R12

Legacy CE Routers

CE1
CE2

Intelligent WAN

Site 3

Legacy WAN

Site 4
## Hub1 Site Prefix Table After R31 is Migrated

R10-DC1-MC#show domain IWAN master site-prefix

Change will be published between 5-60 seconds
Next Publish 01:46:29 later
Prefix DB Origin: 10.1.0.10
Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured; M-
shared

<table>
<thead>
<tr>
<th>Site-id</th>
<th>Site-prefix</th>
<th>Last Updated</th>
<th>DC Bitmap</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.0.10</td>
<td>10.1.0.10/32</td>
<td>00:23:41 ago</td>
<td>0x1L</td>
<td></td>
</tr>
<tr>
<td>10.1.0.10</td>
<td>10.1.0.0/16</td>
<td>00:23:41 ago</td>
<td>0x1C,M</td>
<td></td>
</tr>
<tr>
<td>10.3.0.31</td>
<td>10.3.0.31/32</td>
<td>00:01:11 ago</td>
<td>0x0S</td>
<td></td>
</tr>
<tr>
<td>10.3.0.31</td>
<td>10.3.3.0/24</td>
<td>00:01:11 ago</td>
<td>0x0S</td>
<td></td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>*10.0.0.0/8</td>
<td>00:23:41 ago</td>
<td>0x1T</td>
<td></td>
</tr>
</tbody>
</table>
No PFR control for Site 3 to Site 4 traffic (IWAN to Non-IWAN site)

Enterprise Prefix: 10.0.0.0/8
Site1 Prefix-List: 10.1.0.0/16
Add 10.0.0.0/8 to Hub1 Site-Prefix

Hub MC (R10)
domain IWAN
  vrf default
  master hub
    enterprise-prefix prefix-list ENTERPRISE_PREFIX
    site-prefixes prefix-list SITE_PREFIX
!
ip prefix-list ENTERPRISE_PREFIX seq 10 permit 10.0.0.0/8
ip prefix-list SITE_PREFIX seq 10 permit 10.1.0.0/16
ip prefix-list SITE_PREFIX seq 20 permit 10.0.0.0/8
After 10.0.0.0/8 is added to Hub1 Site-Prefix

R10-DC1-MC#show domain IWAN master site-prefix
Change will be published between 5-60 seconds
Next Publish 01:46:29 later
Prefix DB Origin: 10.1.0.10
Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured; M-
shared

<table>
<thead>
<tr>
<th>Site-id</th>
<th>Site-prefix</th>
<th>Last Updated</th>
<th>DC Bitmap</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.0.10</td>
<td>10.1.0.10/32</td>
<td>00:28:42 ago</td>
<td>0x1</td>
<td>L</td>
</tr>
<tr>
<td>10.1.0.10</td>
<td>10.1.0.0/16</td>
<td>00:28:42 ago</td>
<td>0x1</td>
<td></td>
</tr>
<tr>
<td>10.3.0.31</td>
<td>10.3.0.31/32</td>
<td>00:06:19 ago</td>
<td>0x0</td>
<td></td>
</tr>
<tr>
<td>10.3.0.31</td>
<td>10.3.3.0/24</td>
<td>00:06:19 ago</td>
<td>0x0</td>
<td></td>
</tr>
<tr>
<td>10.1.0.10</td>
<td>*10.0.0.0/8</td>
<td>00:00:30 ago</td>
<td>0x1</td>
<td>T</td>
</tr>
</tbody>
</table>

Previously this was 255.255.255.255
After 10.0.0.0/8 is added to Hub1 Site-Prefix

Enterprise Prefix:
10.0.0.0/8

Site1 Prefix-List:
10.0.0.0/8
10.1.0.0/16
Hub1 Site-Prefix Table After Site4 is Migrated

R10-DC1-MC#show domain IWAN master site-prefix
   Change will be published between 5-60 seconds
   Next Publish 01:46:29 later
   Prefix DB Origin: 10.1.0.10
   Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured; M-shared

<table>
<thead>
<tr>
<th>Site-id</th>
<th>Site-prefix</th>
<th>Last Updated</th>
<th>DC Bitmap</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.0.10</td>
<td>10.1.0.10/32</td>
<td>00:33:41 ago</td>
<td>0x1</td>
<td>L</td>
</tr>
<tr>
<td>10.1.0.10</td>
<td>10.1.0.0/16</td>
<td>00:33:41 ago</td>
<td>0x1</td>
<td></td>
</tr>
<tr>
<td>10.3.0.31</td>
<td>10.3.0.31/32</td>
<td>00:11:24 ago</td>
<td>0x0</td>
<td>S</td>
</tr>
<tr>
<td>10.3.0.31</td>
<td>10.3.3.0/24</td>
<td>00:11:24 ago</td>
<td>0x0</td>
<td>S</td>
</tr>
<tr>
<td>10.4.0.41</td>
<td>10.4.0.41/32</td>
<td>00:01:09 ago</td>
<td>0x0</td>
<td>S</td>
</tr>
<tr>
<td>10.4.0.41</td>
<td>10.4.4.0/24</td>
<td>00:01:09 ago</td>
<td>0x0</td>
<td>S</td>
</tr>
<tr>
<td>10.1.0.10</td>
<td>*10.0.0.0/8</td>
<td>00:05:19 ago</td>
<td>0x1</td>
<td>T</td>
</tr>
</tbody>
</table>
R41 on site 4 is migrated to IWAN

Enterprise Prefix:
10.0.0.0/8

Site1 Prefix-List:
10.0.0.0/8
10.1.0.0/16

Migration Site

DMVPN Hub
Routers

Legacy CE
Routers

Site 3
Legacy 
WAN
R31

R11
R12

PfR Managed
PfR Managed

Intelligent 
WAN

Site 4
PfR Managed

Legacy
WAN

Site 4

R41
IWAN Brownfield migration using APIC-EM IWAN App
Using IWAN App for Brownfield Deployment

Converting existing WAN deployment to IWAN deployments

Brownfield WAN (No IWAN)
- OSPF / EIGRP
- Static / eBGP
- MPLS
- MC/BR
- HR2
- HR1

IWAN Brownfield (IWAN APP)
- OSPF / EIGRP
- DMVPN1
- BR1
- BR2
- MC
- R3

Brownfield can support all platforms supported by IWANAPP (ISR, ASR, ISR4k)
Brownfield workflow

1. Discover non-IWAN Branch from APIC-EM
2. Validation Checks – Image, License, Pre-existing IWAN
3. Layer on IWAN config
Brownfield readiness validation by IWAN-APP

**Need to remove**
- Pfr configuration
- Crypto certificate
- DMVPN
- Front VRF on WAN Interface
- License

**Warnings**
- Qos policy check
- Qos marking
- App recognition: NBAR
- EZPM
APIC-EM Demo - Add Brownfield Device

Add Brownfield Device
IWAN app Day N – Application Troubleshooting

**Monitoring**

- WAN Link Utilization
- Application Bandwidth Utilization
- Jitter / Pkt-loss / Delay Violations
- Policy Compliance

**Troubleshooting**

- QoS Troubleshooting
- DMVPN Tunnel not coming up
- Not supported deployments
- Routing loops: Detect site prefix overlap
Organizational and Business Constraints
Avoid implementation that doesn’t map back to logical design determined necessary to address key requirements.

Must have strong understanding of current state environment to ensure implementation success.
Business Constraints and Migration Planning

• Identify sites for migration
  • Single Migration Site or Regional Migration site (Transit)
• Make changes to infrastructure (if H/W upgrades are needed)
  • Circuit Capacity, Encryption throughput
  • New Circuits if adding a new broadband link
• Finalize and install Deployment and Monitoring tools → APIC-EM / Live Action
  • Verify connectivity from tools to remote devices with SSH, SNMP
• Identifying Applications, failover models so that a test plan can be created
• Branch Migrations - Zero Touch PnP or Brownfield, On-site or Remote
  • Open necessary FW ports for Zero touch remote devices to make contact
  • Grouping of Branches, phases of migration
  • Remote or on site
  • Change window needed – single or dual router branch
Summary
Session Summary

• Documenting the existing network.

• Create a high-level migration plan.

• Deploy a proof-of-concept or production pilot of the network. The first remote site should always be in a lab. This allows for the operational teams to be comfortable with the technology while they start to learn about the actual applications in use in the network. As well, any issues to the IWAN routing architecture should not impact production during this phase.

• Testing the execution plans in a lab environment and modify accordingly.

• Deploying DMVPN hub routers.

• Migrate Branch routers.

• Post-migration cleanup tasks.

• Migrating other WAN transports/technologies

• PfR

Ask your boss for a raise!
You improved business application responsiveness while saving the company $$$$
Complete Your Online Session Evaluation

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

• Complete your session surveys through the Cisco Live mobile app or on www.CiscoLive.com/us.

Don’t forget: Cisco Live sessions will be available for viewing on demand after the event at www.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
Thank you