A Question…

Case Study: How XYZ Co. Leveraged Existing Investment to Transform the WAN

Owen Parsons (BSc. Internet Computing, CCNA-RS, CCDA)

Network & Security Architect

January 17, 2019

Today’s Topic

- A case study of the WAN transformation or “FlexVPN Project” for XYZ Co.
- XYZ Co. is mining company with operations in the US and EMEA
- Project scope covered the global WAN
- A foundation level understanding of the material is assumed

Agenda

1 Challenges

2 Solutions

3 Results

Challenges

Business Challenges

Business Challenge		IT Department Challenge
• Inconsistent / unreliable application experience	→	• Lack of visibility & control toolset, inconsistent QoS
• Crew welfare – poor social Internet	→	• Fix without impacting business applications
• 24/7 operations & multiple time zones	→	• Keep the network up with no NOC, no on-call & 1.5 engineers
• Global cost reduction targets	→	• Very small discretionary budget

IT & Technical Challenges

- Remit to reduce reliance on MPLS services
- QoS policy limitations & complexity due to NNI service
- Remit to enhance security
- Most sites without qualified remote hands
- Requirement for 3rd party interoperability
- Site inconsistencies (e.g. ISR 4K, ISR G2, PPPoE, VSAT, bandwidth, MTU)

Solutions

Features, Products and Services

Network Infrastructure

- Cisco ISR 4300
- Cisco ISR G2 2900
- Cisco Catalyst 4500
- Cisco Catalyst 3650
- Cisco ASA 5500-X

Toolset

- Cisco Prime Infrastructure
- LiveAction LiveNX*
- Opengear Smart OOB*

Services

- Cisco Umbrella
- Microsoft CA Services

Features

- FlexVPN
- ZBFW
- EEM
- DIA
- NetFlow
- BGP
- IP SLA
- NBAR
- VRF
- HQF
- DMVPN
- Anycast
- NAT
- EIGRP

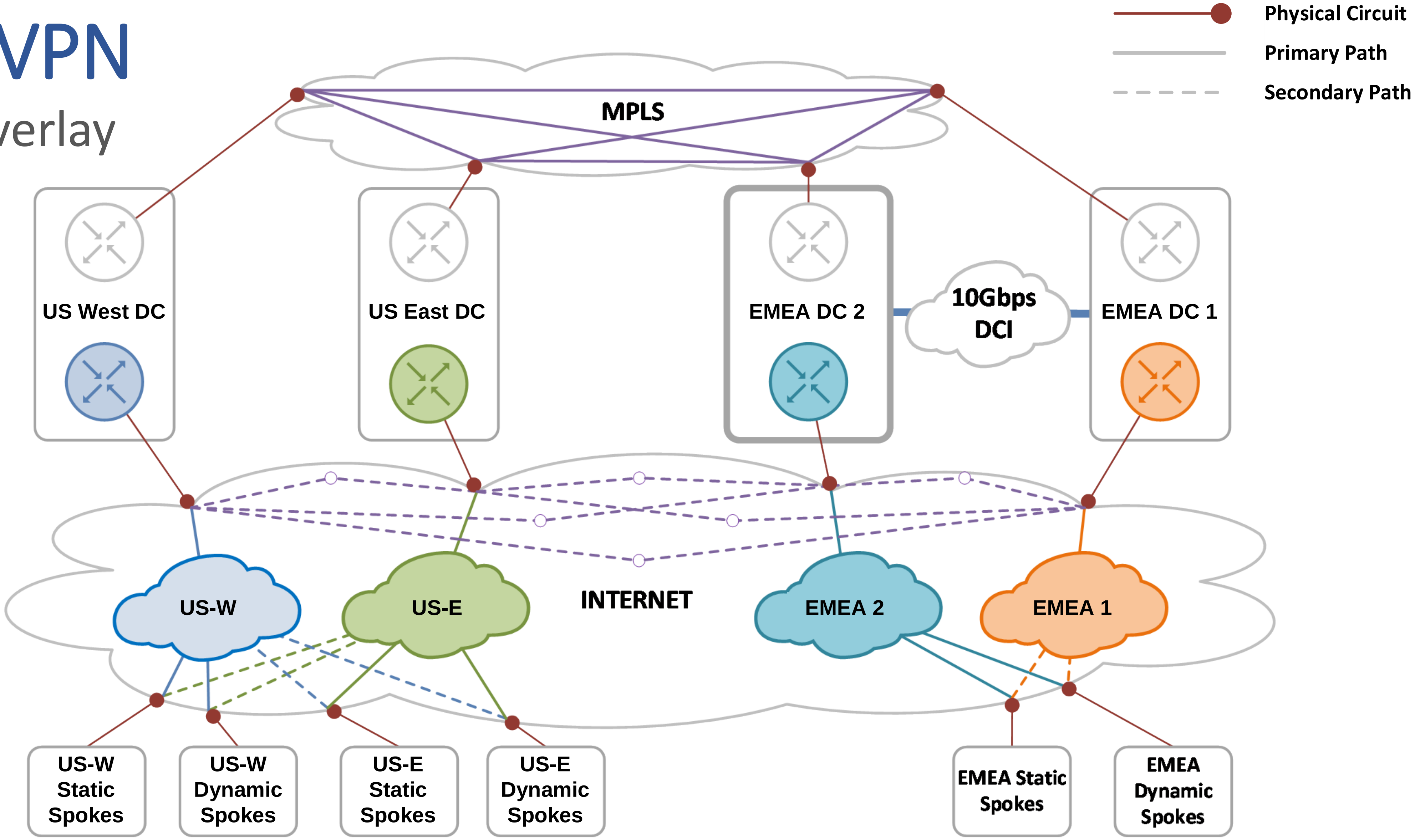
**New items*

FlexVPN

- A single global WAN overlay fabric
  - Transport & connection independence
  - Dynamic, policy based path selection
  - Service chaining support
  - A simple control and management toolset
  - Strong security through PKI & encryption

FlexVPN

Full Overlay



Complimentary & Integrated Solutions

FlexVPN works with everything

- QoS – FlexVPN per-tunnel, egress shaping, ingress policing
- DMVPN over FlexVPN for backhauled spoke social Internet access
- DIA for spoke Internet access on larger bandwidth sites
- Umbrella & ZBFW for web security
- Automation of operations – EEM, zero-touch, self-documenting
- Toolset – Prime Infrastructure, LiveAction & Opengear

Results

FlexVPN Project

Challenges met

✓Application experience

- Modular, hierarchical, automated QoS polices and decoupling internal markings from provider

✓Crew welfare

- Great feedback for both DMVPN and DIA deployments

✓3rd party interoperability

- IKEv2 and BGP – typically supported on modern, enterprise class edge devices
- Riverbed SteelHead WAN optimization

FlexVPN Project

Challenges met

✓Security enhancements

- PKI based AAA, Smart Defaults, MPLS encryption, VRF segmentation, ZBFW

✓Reduced reliance on MPLS services

- Demonstrated reliable, quality, secure communications over Internet

✓Network uptime & service availability

- Up to 4 failover paths to corporate services per spoke

✓Site inconsistencies

- **Flex**VPN is accurate – non-prescriptive deployment, modular & reusable CLI

FlexVPN Project

Challenges met

✓Resource challenges

- Reusable modular CLI & scripting/automation = faster deployment
- Globally consistent & self-documenting configuration = faster troubleshooting
- Happy users = fewer support calls

✓Budget challenges

- Using features already available within existing hardware and licensing resulted in insignificant spend

The answer to the original question

Other Solutions

And why I didn’t use them

- IWAN
  - Too prescriptive, unofficially heading towards legacy
- SD-WAN (née Viptela)
  - Wasn’t integrated yet, several sites are ISR G2
- DMVPN
  - FlexVPN is the evolution of DMVPN, with less configuration
- A different vendor
  - Wouldn’t meet the goal of leveraging existing investment

Questions

?

Thank You

Overtime Slides

Spoke Internet Access

Via Hub when < 10Mbps

- All Internet traffic backhauled to regional hubs
- Failover between hubs (upstream failure only)
- Umbrella on spoke, ZBFW on hub
- QoS via tunnel-in-tunnel, egress shaping & scavenger class

DIA when >= 10Mbps

- Local breakout of all social and corporate Internet traffic
- No failover (single local circuit)
- Umbrella & ZBFW on spoke
- QoS via ingress policing & egress shaping

Quality of Service

QoS Challenges

- How do I prevent a large bandwidth site from flooding a smaller bandwidth site?
- How do I provide good social Internet without affecting business critical applications?
- How do I control Internet traffic?

Quality of Service

QoS Solutions – Flood Prevention

- FlexVPN hub-to-spoke per-tunnel QoS
- Utilised certificate attributes to dynamically apply QoS policies*

CN=wcrgw01.xyzco.local,OU=**flex-ap#FlexClient#1.75m#**,O=xyzcoUS-W,L=FlexClient,C=US

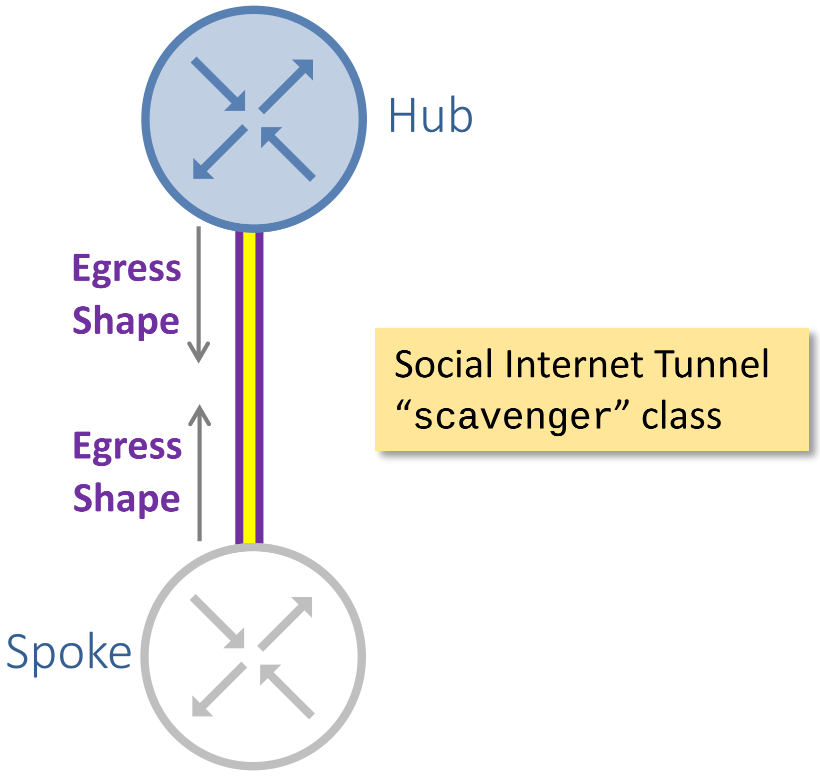
Matches a QoS policy on the hub ***exactly***

- FlexVPN Mesh per-tunnel QoS
  - Tested, but ingress policing proved more suitable

Quality of Service

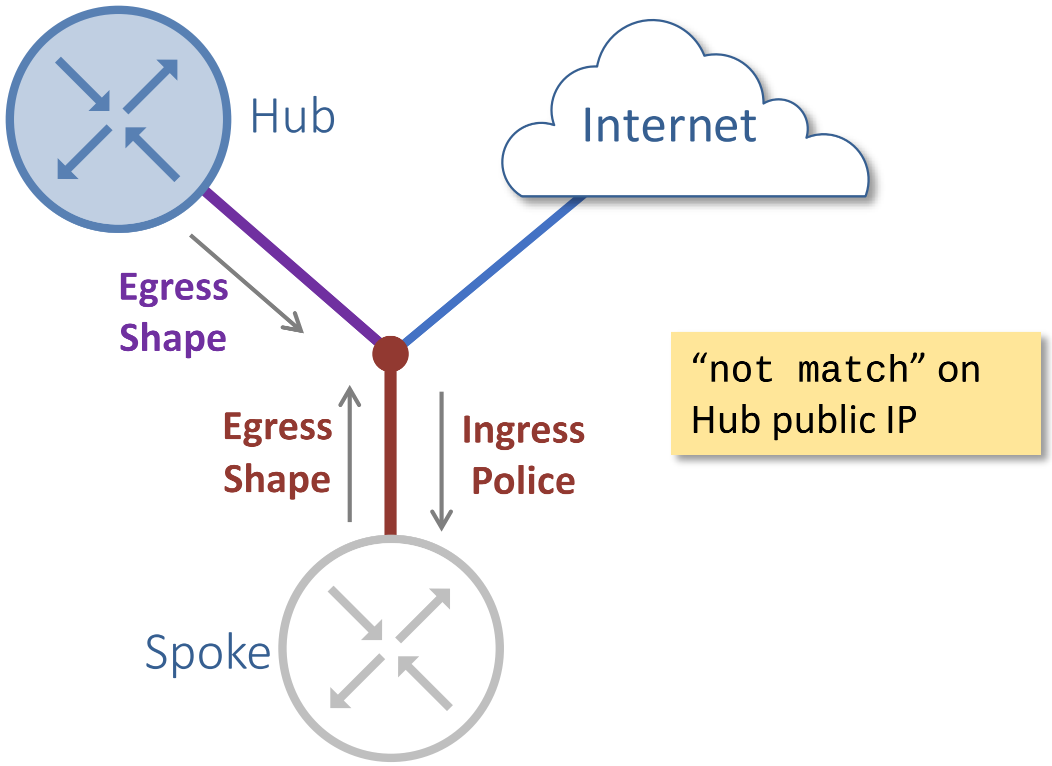
QoS Solutions – Social Internet & Internet Control

Via Hub – Egress Only



Social Internet Tunnel
“scavenger” class

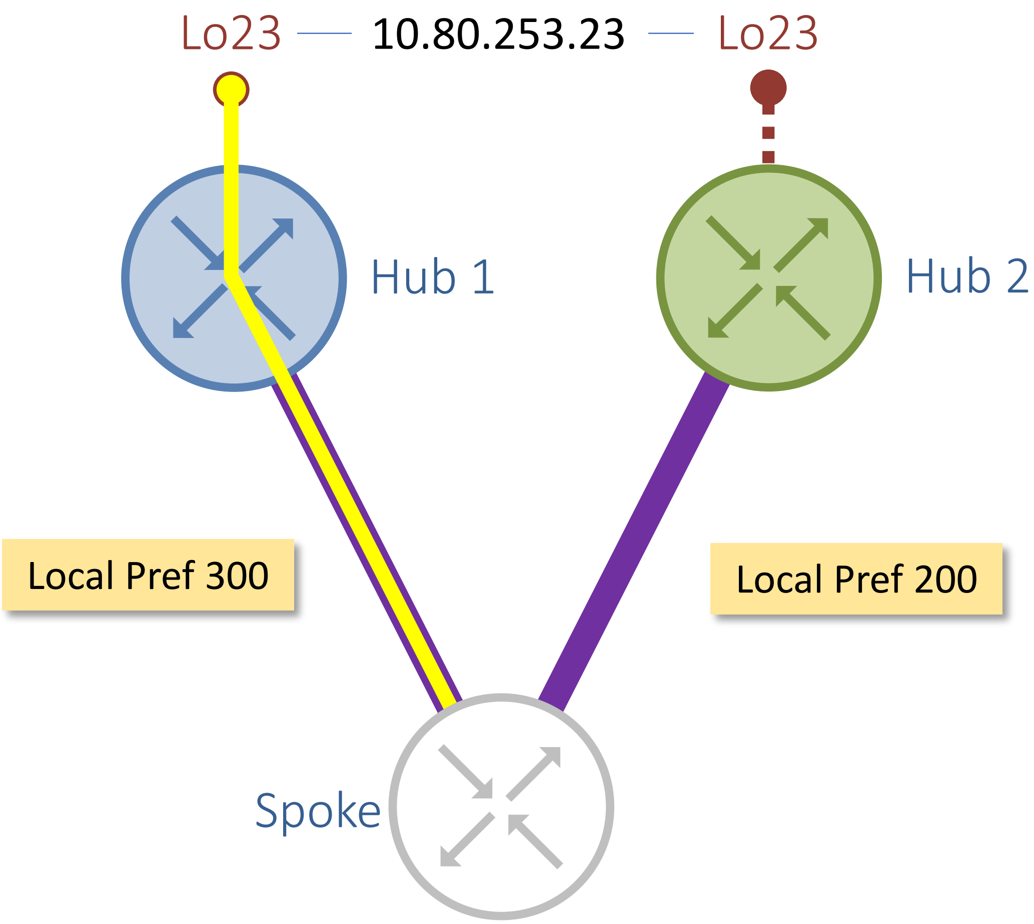
DIA – Ingress/Egress



“not match” on
Hub public IP

Social Internet DMVPN

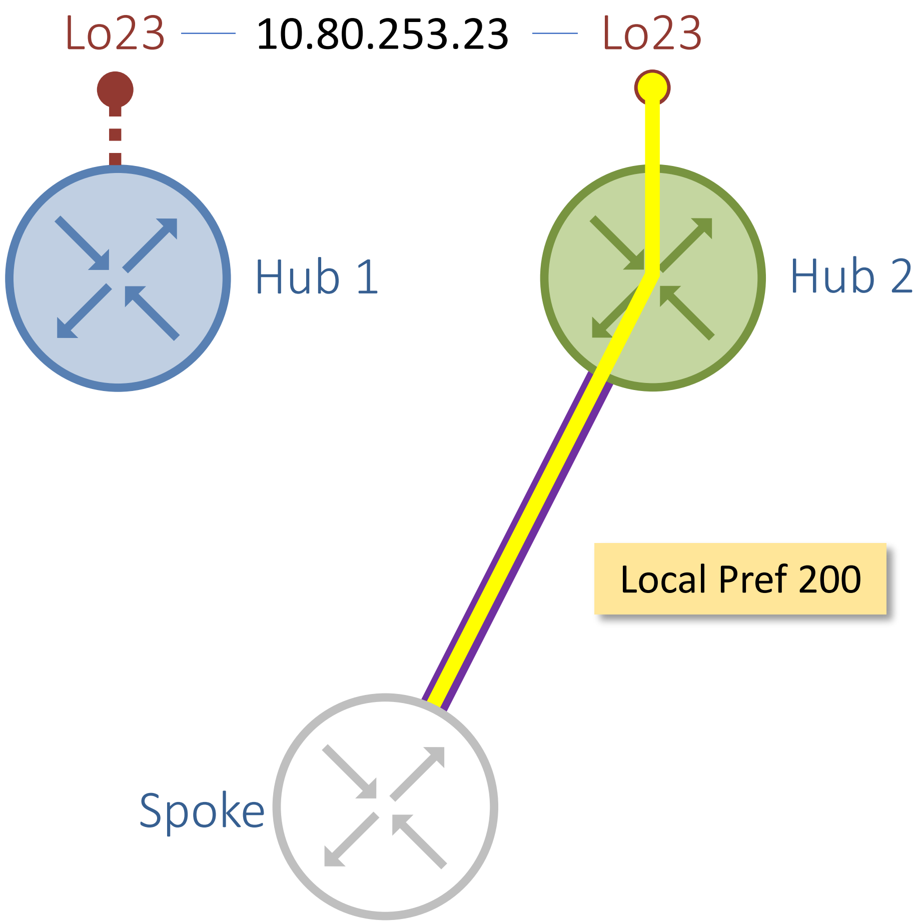
Anycast Redundancy



- iBGP (global routing table)
  - Hubs send 0.0.0.0/0
  - Spoke sends 10.x.0.0/16
  - Metric = Local Preference
- Hubs have Lo23 Anycast IP
- Spoke connects to mGRE Tu25323 via preferred Lo23 IP
- EIGRP (social VRF)
  - Hub sends 0.0.0.0/0
  - Spoke sends 10.x.23.0/24

Social Internet DMVPN

Anycast Redundancy - Failover



- FlexVPN tunnel to Hub 1 is lost
- DMVPN tunnel to Hub 1 drops
- Spoke has a route to Lo23 IP via FlexVPN tunnel to Hub 2
- Spoke establishes DMVPN tunnel to Hub 2
- EIGRP (social VRF) establishes and service is restored

Solutions for Reducing Overhead

Minimal Touch Configuration

- Modular & reusable CLI constructs
  - Easy templating in Prime Infrastructure
- Automation of operations
  - Routing protocols, dynamic BGP peers, Virtual Templates, mGRE, IP pools, EEM, FlexVPN AAA based configuration etc.
- Near zero-touch on hubs for FlexVPN
  - dVTI = zero touch
  - sVTI = one push from PI and one from LiveNX

Solutions for Reducing Overhead

Interface & Path Information

- GRE supports CDP
  - sVTI – CDP triggers EEM script event to update interface description
  - dVTI – Can’t update description of VA interface, check CDP table directly
- Tunnel interface IPs in DNS
  - Standard provider practice, significantly enhances traceroute
  - Simplified with PowerShell

Social Internet DMVPN

How did it help?

✓Application experience

- Full circuit bandwidth available to business applications on demand

✓Crew welfare

- Full circuit bandwidth available to social Internet when not required by business applications

✓Resource challenges

- Zero-touch deployment hub-side and *almost* identical spoke configuration
    - ‘ip address dhcp’ option missing/removed on spoke ISR4k tunnel configuration

Direct Internet Access

How did it help?

✓Application experience

- Increasing bandwidth available for corporate applications resulted in great feedback

✓Resource challenges

- Happy users = fewer support calls
- Zero-touch deployment on hubs

✓Budget challenges

- Maximised ROI on all spoke Internet services and reduced load on the hub Internet

LiveAction LiveNX

How did it help?

✓QoS toolset & consistency

- Central QoS management = global consistency
- Second-to-none visibility of the entire WAN+

✓Resource challenges

- Able to rapidly pin-point issues (proactively)
- Effort of MACs dramatically reduced
- Very easy setup, very intuitive interface

Opengear Out-Of-Band

How did it help?

✓Remote hands

- After easy deployment significantly reduces reliance on remote hands
- Remote hands only need basic knowledge

✓Resource challenges

- Reduced cross-time zone resource scheduling
- True OOB - takes the fear out of remote changes

NOTE: Where this wasn't an option EEM saved the day