

TOMORROW starts here.



Cisco *live!*

Intelligent WAN - Internet as the Enterprise WAN Carriage

BRKRST-2642

Brad Ford
Systems Engineer

Agenda

- IWAN Introduction and Business Drivers
- Transport-Independent Design
- Intelligent Path Control
- Security Connectivity
- Application Optimisation
- Management and Simplification

Explosion of Data Outside of Your Headquarters



Internet of Things



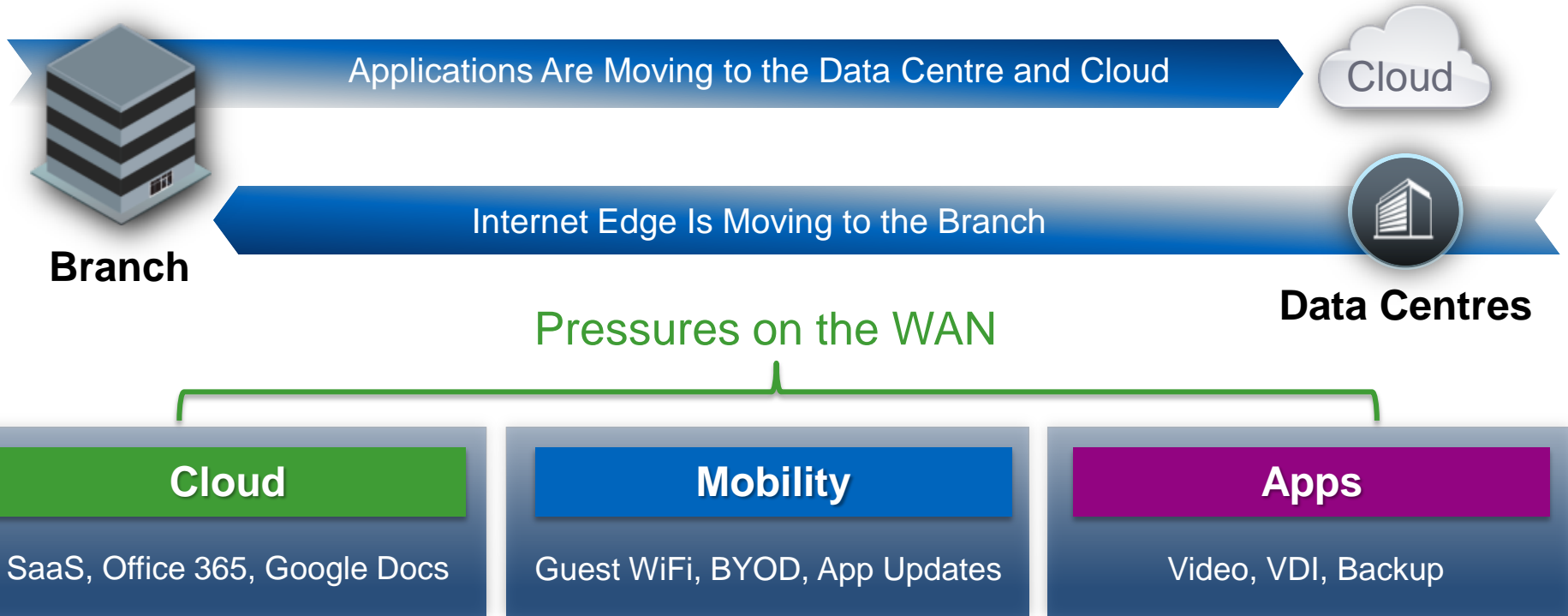
Mobility



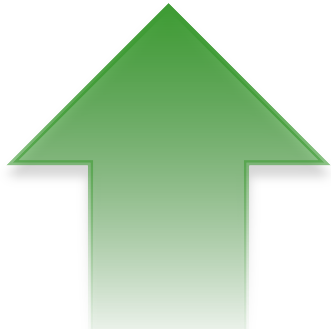
Video

Emerging Branch Demands

The Application Landscape Is Changing



The Branch Conundrum



**Bandwidth
Demands**



Budget



User Suffering

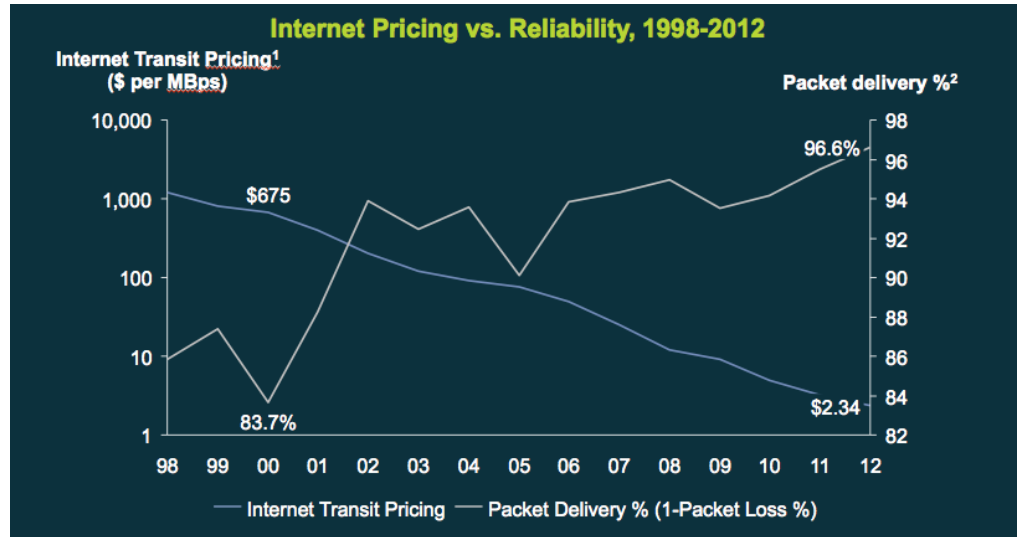
Time to Rethink your Branch-WAN Strategy

Internet Price vs Risk Improves Every Year

Low Cost Alternative

46%

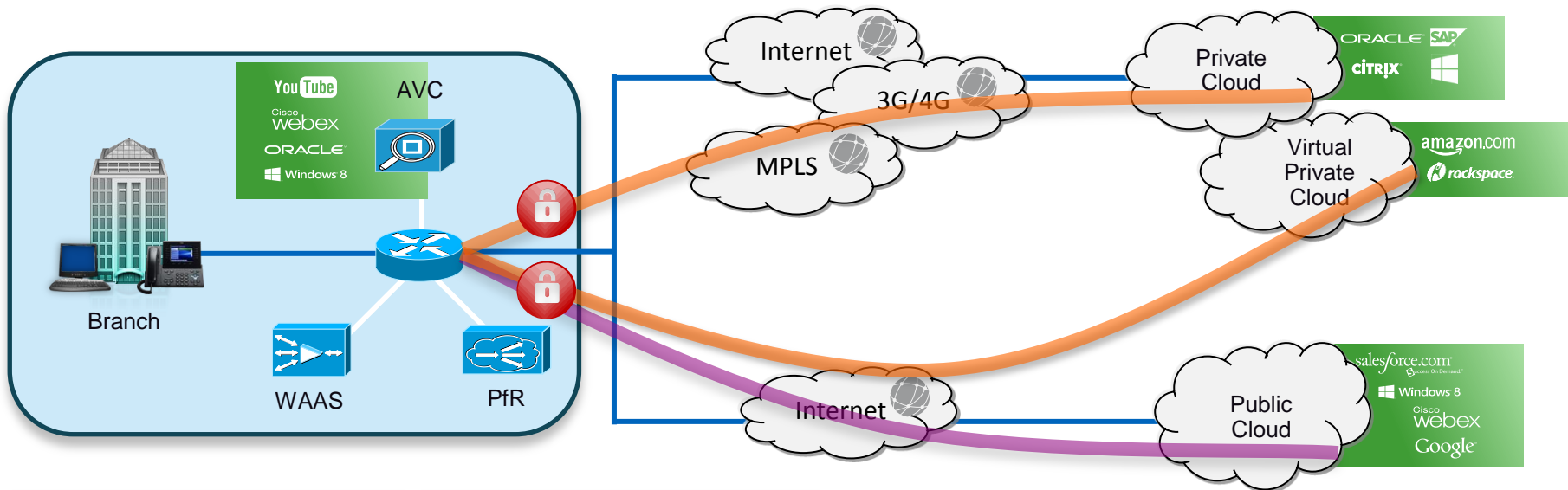
of Organisations Are
Planning to
Transition to Internet
Connections



1. Internet Transit Pricing based on surveys and informal data collection primarily from Internet Operations Forums—'street pricing' estimates
 2. Packet delivery based on 15 years of ping data from PingER for WORLD (global server sample) from EDU.STANFORD.SLAC in California
- Source: William Norton (DrPeering.net); Stanford ping end-to-end reporting (PingER)

Cisco Intelligent WAN


Solution Components



 **Transport Independent**

 **Intelligent Path Control**

 **Secure Connectivity**

 **Application Optimisation**

Simplified Provisioning and Deployment



Transport-Independent Design

Secure WAN Design Over Any Transport

Dynamic Multipoint VPN (DMVPN)

Transport-Independent

Simplifies WAN Design

- Easy multi-homing over any carrier service offering
- Single routing control plane with minimal peering to the provider

Flexible

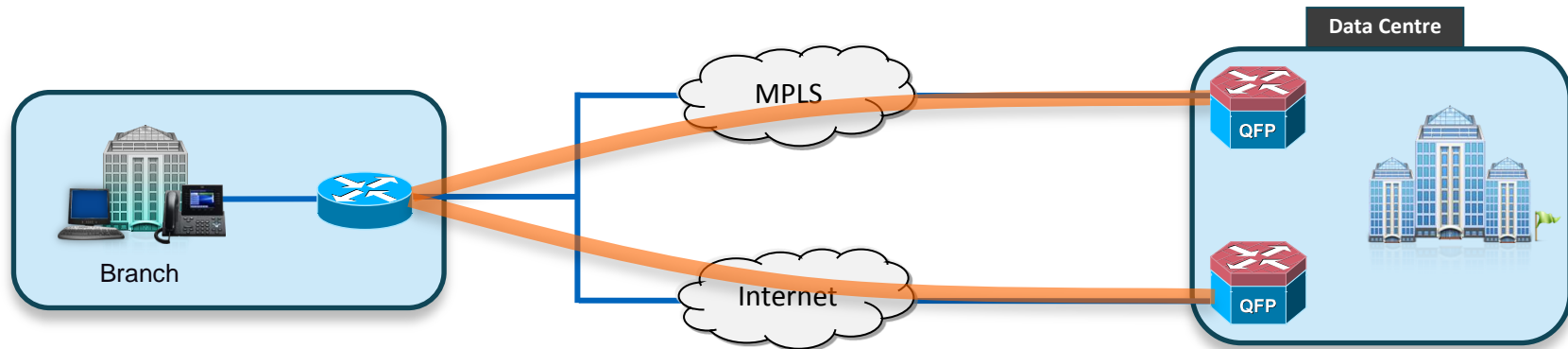
Dynamic Full-Meshed Connectivity

- Consistent design over all transports
- Automatic site-to-site tunnels
- Zero-touch hub configuration for new spokes

Secure

Proven Robust Security

- Certified crypto and firewall for compliance
- Scalable design with high-performance crypto in hardware



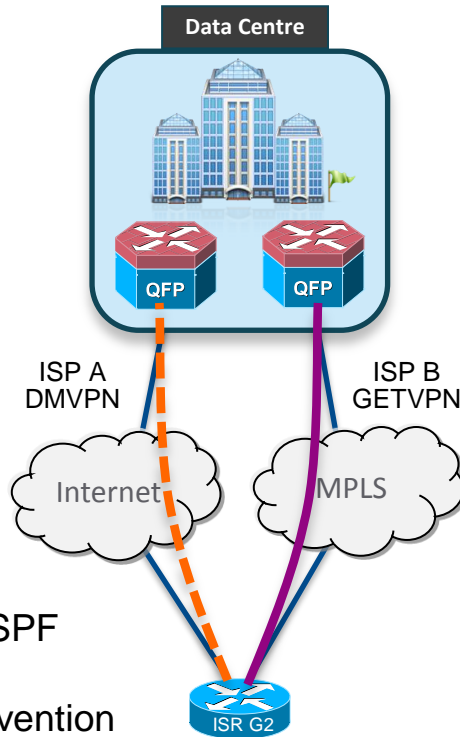
Hybrid WAN Designs

Active/Standby
WAN Paths
Primary With Backup

Two IPsec Technologies
GETVPN over MPLS
DMVPN over Internet

Two WAN Routing
Domains
MPLS: eBGP or Static
Internet: iBGP, EIGRP or OSPF
Route Redistribution
Route Filtering for Loop Prevention

TRADITIONAL HYBRID

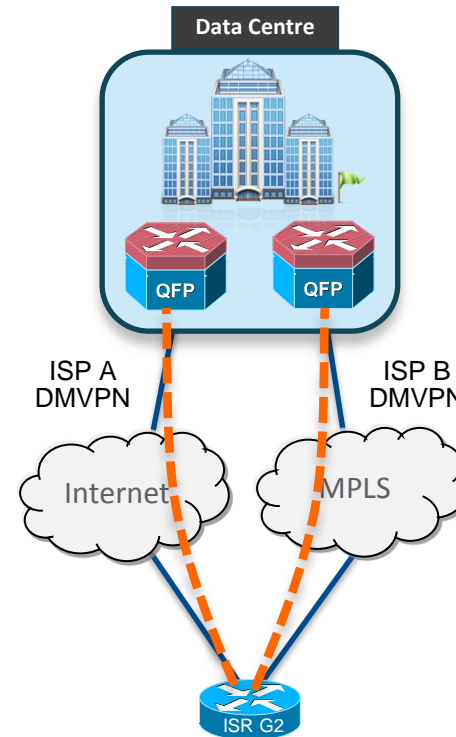


RECOMMENDED HYBRID

Active/Active
WAN Paths

One IPsec Overlay
DMVPN

One WAN Routing
Domain
iBGP, EIGRP
or OSPF



What is Dynamic Multipoint VPN?

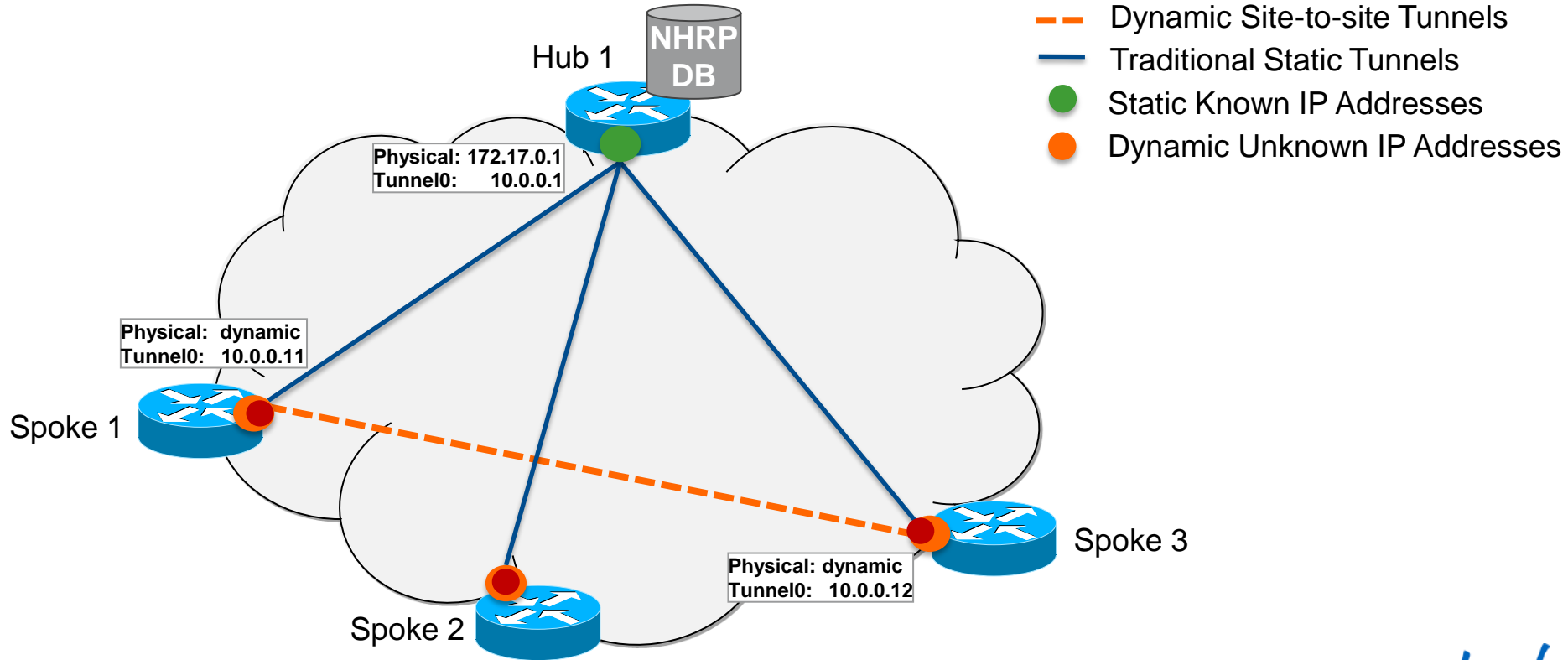
DMVPN is a Cisco IOS software solution for building IPsec+GRE VPNs in an easy, dynamic and scalable manner

- **Relies on two proven technologies**
 - **Next Hop Resolution Protocol (NHRP)**
 - Creates a distributed mapping database of VPN (tunnel interface) to real (public interface) addresses
 - **Multipoint GRE Tunnel Interface**
 - Single GRE interface to support multiple GRE/IPsec tunnels and endpoints
 - Simplifies size and complexity of configuration
 - Supports dynamic tunnel creation

DMVPN Phases

Phase 1 – 12.2(13)T	Phase 2 – 12.3(4)T	Phase 3 – 12.4.(6)T
<ul style="list-style-type: none">▪ Hub and spoke functionality▪ p-pGRE interface on spokes, mGRE on hubs▪ Simplified and smaller configuration on hubs▪ Support dynamically addressed CPEs (NAT)▪ Support for routing protocols and multicast▪ Spokes don't need full routing table – can summarise on hubs	<ul style="list-style-type: none">▪ Phase 1+▪ Spoke to spoke functionality▪ mGRE interface on spokes▪ Direct spoke to spoke data traffic reduces load on hubs▪ Hubs must interconnect in daisy-chain▪ Spoke must have full routing table – no summarisation▪ Spoke-spoke tunnel triggered by spoke itself▪ Routing protocol scale limitations	<ul style="list-style-type: none">▪ Phase 2+▪ More network designs and greater scaling▪ Same Spoke to Hub ratio▪ No hub daisy-chain▪ Spokes don't need full routing table – can summarise▪ Spoke-spoke tunnel triggered by hubs▪ Removes routing protocol limitations▪ NHRP routes/next-hops in RIB (15.2(1)T)

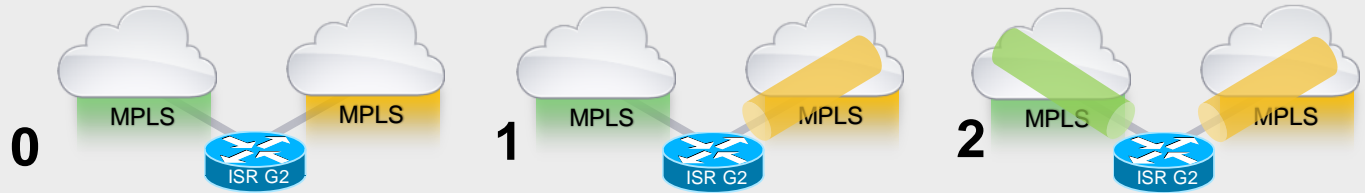
DMVPN How it Works



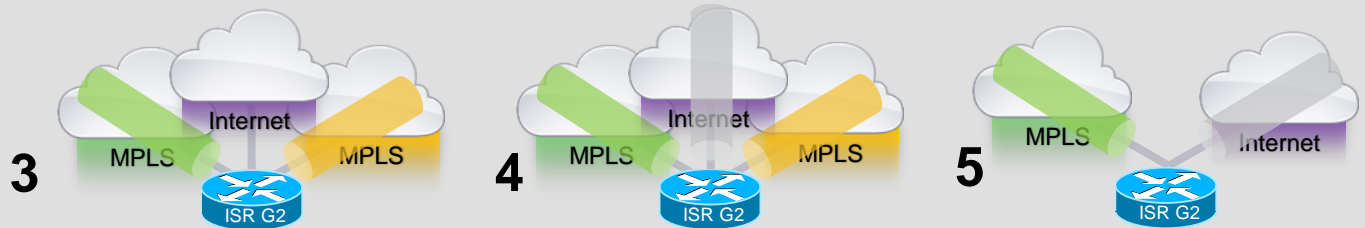
Traditional WAN to Internet Based WAN Transition

Migration Steps

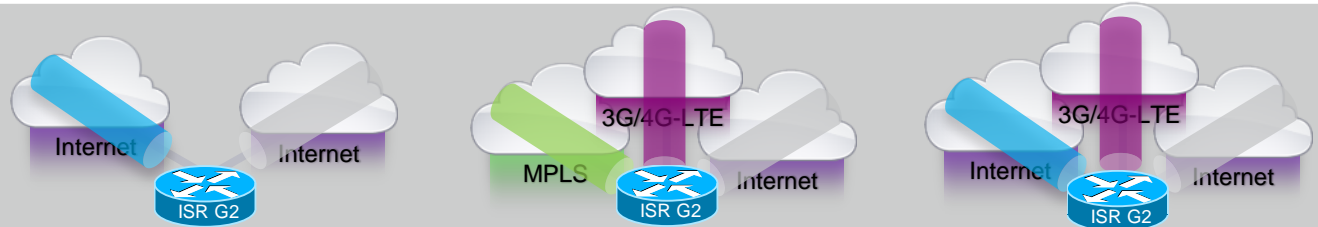
Adding DMVPN to MPLS WAN



Replacing a MPLS service with an Internet service



Other interesting IWAN Topologies



Transport Best Practices

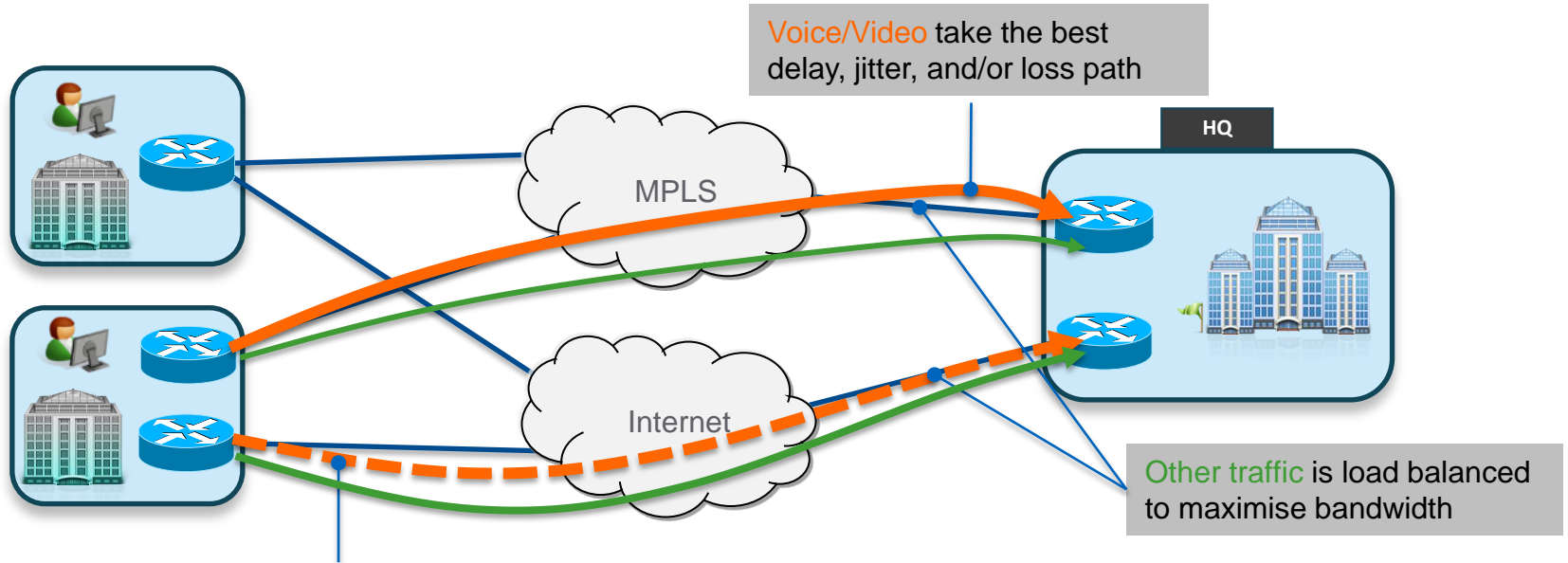
- Private peering with Internet providers
 - Use same Internet provider for hub and spoke sites
 - Avoids Internet Exchange bottlenecks between providers
 - Reduces round trip latency
- DMVPN
 - DMVPN Phase 2 for dynamic tunnels with PfR
 - Separate DMVPN network per provider for path diversity
 - Per Tunnel QoS
- Transport settings
 - Use the same MTU size on all WAN paths
 - Bandwidth settings should match offered rate
 - Use a front-side VRF to separate Internet and internal default routes
- Internet security
 - Use access-lists or firewalls to only permit DMVPN tunnel traffic
 - Hub Tunnel IP address should not be registered in DNS to hide it
- Routing Overlay
 - iBGP or EIGRP for high scale (1000+ sites)
 - Single routing process, simplified design





Intelligent Path Control

Intelligent Path Control with PfR



- PfR monitors network performance and routes applications based on application performance policies
- PfR load balances traffic based upon link utilisation levels to efficiently utilise all available WAN bandwidth

What Is Performance Routing (PfR)?

Tooling for Intelligent Path Control

“**Performance Routing (PfR)** provides additional intelligence to classic routing technologies to track the performance of, or verify the quality of, a path between two devices over a Wide Area Networking (WAN) infrastructure to determine the best egress or ingress path for application traffic....”

- *Cisco IOS technology*

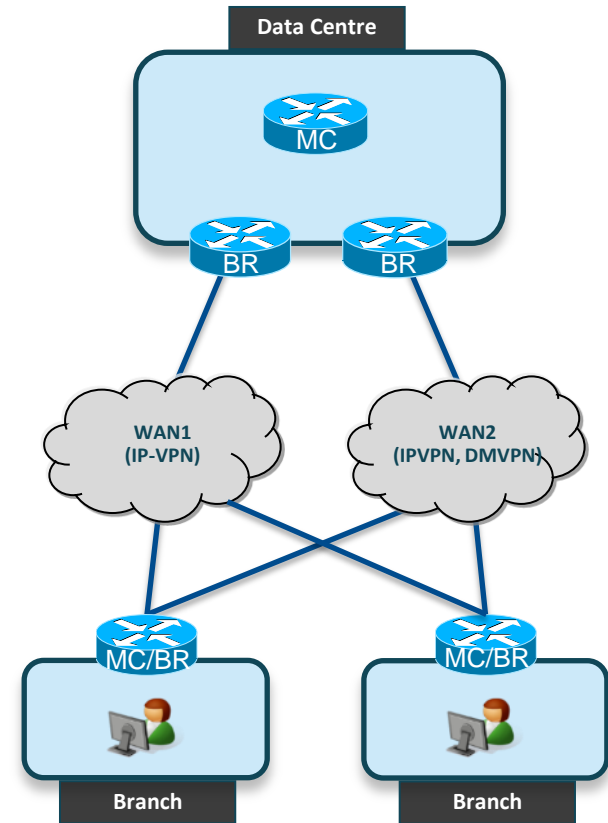
PfR vs Classical Routing

	CLASSICAL	PfR
Path Control	<ul style="list-style-type: none">• Topological state• Least cost path• Static user preference	<ul style="list-style-type: none">• Application-aware• Policy controlled• Measured performance
Metrics	<ul style="list-style-type: none">• Path cost• Interface state	<ul style="list-style-type: none">• Delay• Jitter• Bandwidth
Adaptive	Responds To: <ul style="list-style-type: none">• Link and node state changes (up/down)	Responds To: <ul style="list-style-type: none">• Measured performance changes (degradation)



Performance Routing Components

- The Decision Maker: Master Controller (MC)
 - Apply policy, verification, reporting
 - No packet forwarding/ inspection required
- The Forwarding Path: Border Router (BR)
 - Gain network visibility in forwarding path (learn, measure)
 - Enforce MC's decision (path enforcement)
- Optimise By:
 - Reachability, Delay, Loss, Jitter, MOS
 - Throughput, Load, and/or \$Cost

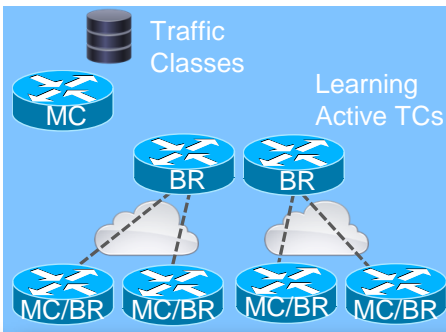


How PfR Works



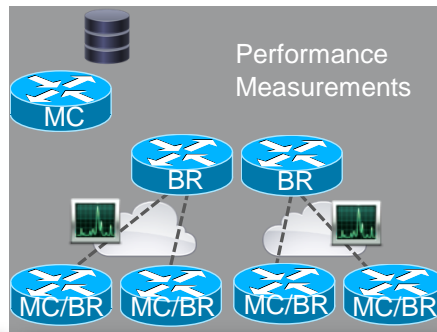
Define Your Traffic Policy

Identify Traffic Classes based on Applications or Transport Classifiers



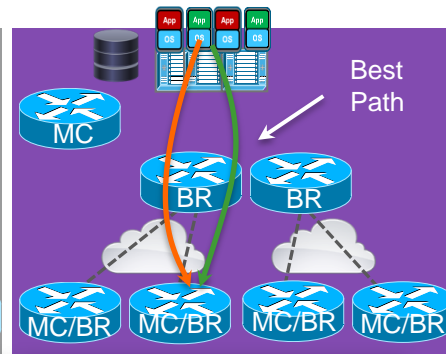
Learn the Traffic

ISR G2 and ASR Learn traffic classes flowing through BRs based on your policy definitions



Measurement

Measure the traffic flow and network performance actively or passively and report metrics to the MC



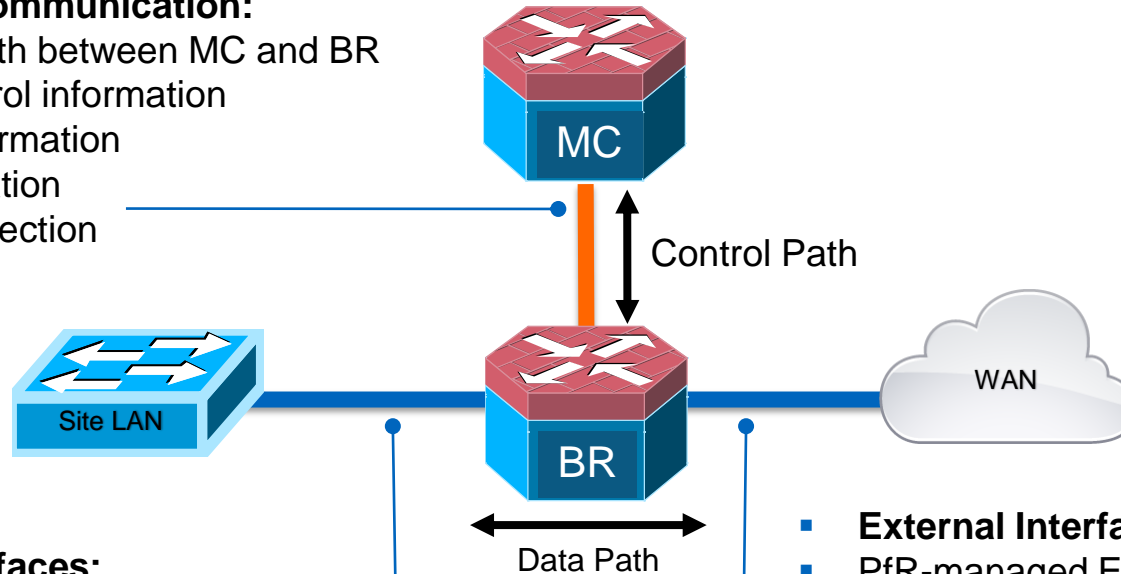
Path Enforcement

Master Controller commands path changes based on your traffic policy definitions

PfR Interface Definitions and Relationships

- **MC-BR Communication:**

- Control path between MC and BR
- Path Control information
- Traffic information
- Authentication
- TCP Connection



- **Internal Interfaces:**

- BR interface connecting to the site network
- Passive traffic monitoring with Netflow
- No explicit NF configuration needed
- At least 1 internal interface per BR

- **External Interfaces:**

- PfR-managed Exit Links to forward traffic
- Enabled on BR
- Configured on MC (for target discovery)
- Minimum of 2 interfaces per BR

Performance Routing

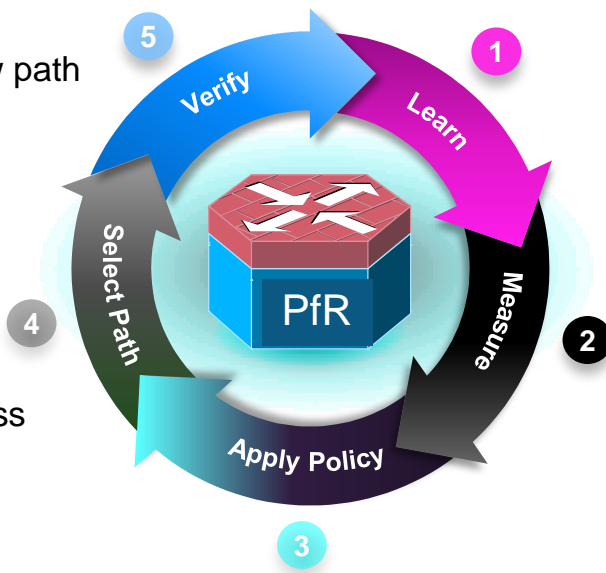
Control Loop

5. Verify New Path:

- Verify traffic is flowing on new path
- Revert to previous path if performance remains out-of-policy

4. Select Path:

- Direct BRs for each traffic class
- BRs inject best path into FIB
- Gather new path performance info



3. Apply Your Traffic Policy:

- Evaluate performance policies to Traffic Class measurement

1. Learn Your Traffic Classes:

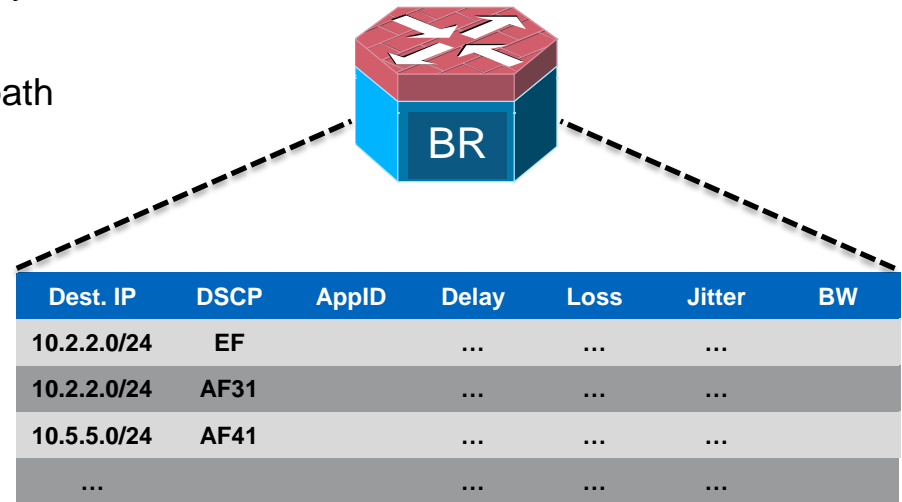
- Prefix-based flows
- ACL-based flows
- Application flows

2. Measure:

- Network Performance
 - Passive: Netflow Data (Throughput)
 - Active: IPSLA Probes (Jitter, Delay)
- Network Availability
 - Reachability and Topology Info
 - Derived from Routing Processes

Learning Traffic Classes (TCs)

- PfR Operates on Traffic Classes flowing through BRs
- A traffic class is a subset of the traffic defined by policy that is to be optimised
- Traffic Class performance metrics are collected per path
- PfR can learn traffic classes in two ways
 - Automatic: dynamically learn flows that match TC definitions
 - Configuration: user defined traffic classes and prefixes to optimise
- Traffic classes can be identified using:
 - IP prefixes
 - ACL classes (e.g., well-known ports, CoS markings)
 - Application classes (e.g NBAR)

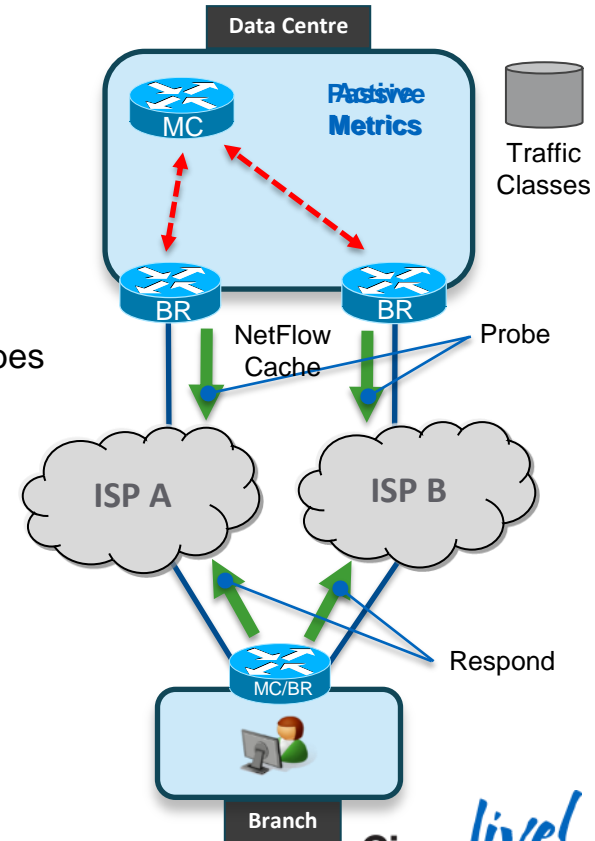


Example of a Traffic Class List

Measuring Network and Application Performance

- Passive Measurement
 - For Data or Best Effort Applications
 - Ingress/Egress Bandwidth and TCP Loss and Delay derived from Netflow
- Active Measurement
 - For Video, Voice and delay sensitive data applications
 - Path Jitter, Delay, Loss and MOS derived from IPSLA synthetic traffic probes
- PfR automatically enables Netflow and IPSLA
- MC Performance Database to determine Policy Enforcement actions

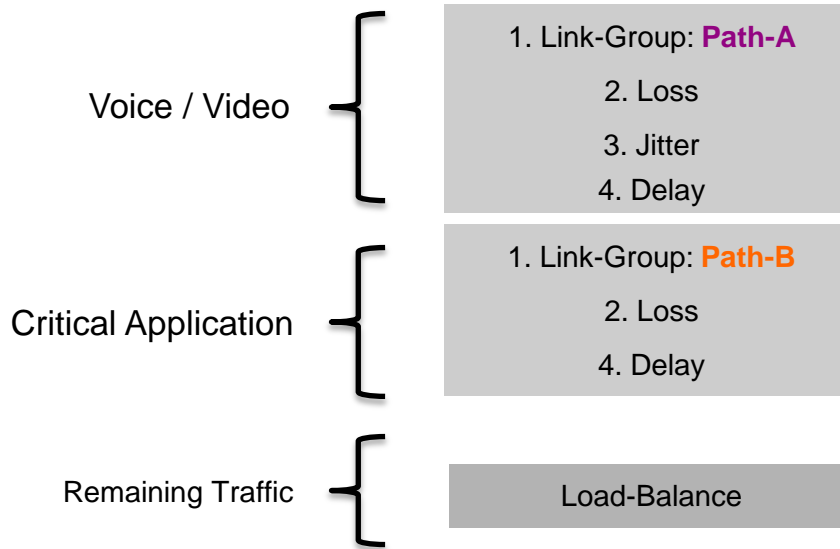
Destination Prefix	DSCP	App Id	Delay	Jitter	Loss	Ingress BW	Egress BW	BR	Exit
10.1.1.1/32	EF		60	10	0	20	40	BR1	Gi1/1
10.1.10.0/24	AF31		110	15	0	52	60	BR1	Gi1/2
...	0		89	26	1	34	10	BR2	Gi1/1



Defining Application Performance Policy

- Choose your policy actions for various traffic classes
- Alternate path selection based on flexible criteria

Example:



FLEXIBLE CRITERIA

Application Performance

Reachability

Delay

Loss

MOS

Jitter

Link

Load Balancing

Max Utilisation

Link-Group Path Preference

Bandwidth Costs (\$)

Load Balancing

- External link Load Balancing is enabled by default
- PfR Distributes traffic across a set of links to maintain efficient utilisation levels with a defined percentage range. Default utilisation range is +/- 20%
- External links can have different available bandwidth
e.g., Int 1/0 = 1.5Mbps, Int 1/1 = 15Mbps
- Load Balancing defaults can be modified by CLI
 - Utilisation Range
 - Max Utilisation 90%



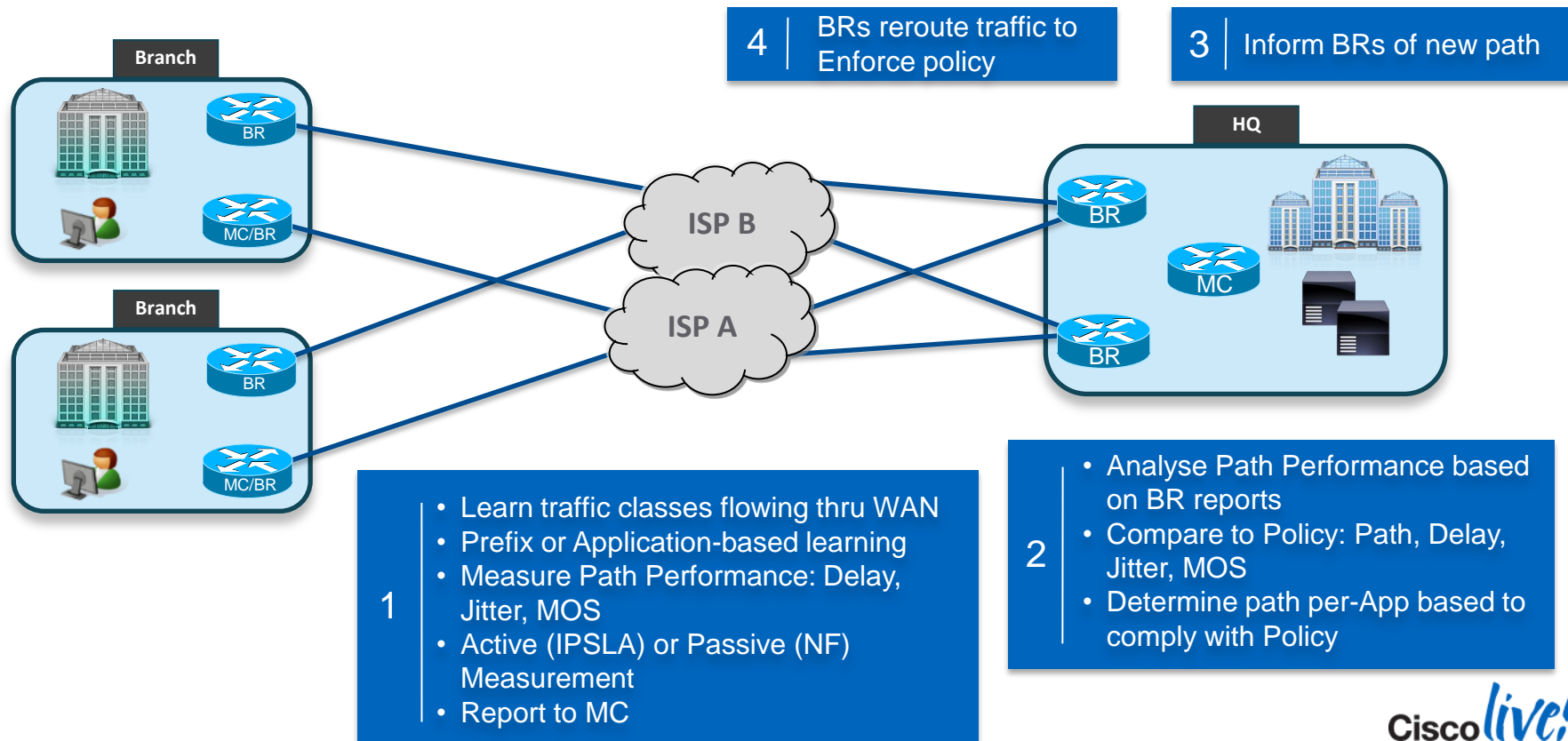
Path Enforcement

- Master controller monitors traffic classes and BR exit links for out-of-policy conditions
- Appropriate enforcement method is determined automatically by the MC
- MC commands the BRs to enforce path changes for policy compliance

Destination Prefix	Application
<ul style="list-style-type: none">• BGP<ul style="list-style-type: none">Egress: Route injection or BGP Local Preference attributeIngress: BGP AS-PATH Prepend or AS Community• EIGRP Route injection• Static Route injection• Protocol Independent Route Optimisation (PIRO) with PBR injection	<ul style="list-style-type: none">• Dynamic PBR• NBAR/CCE

Intelligent Path Control

Putting It Together



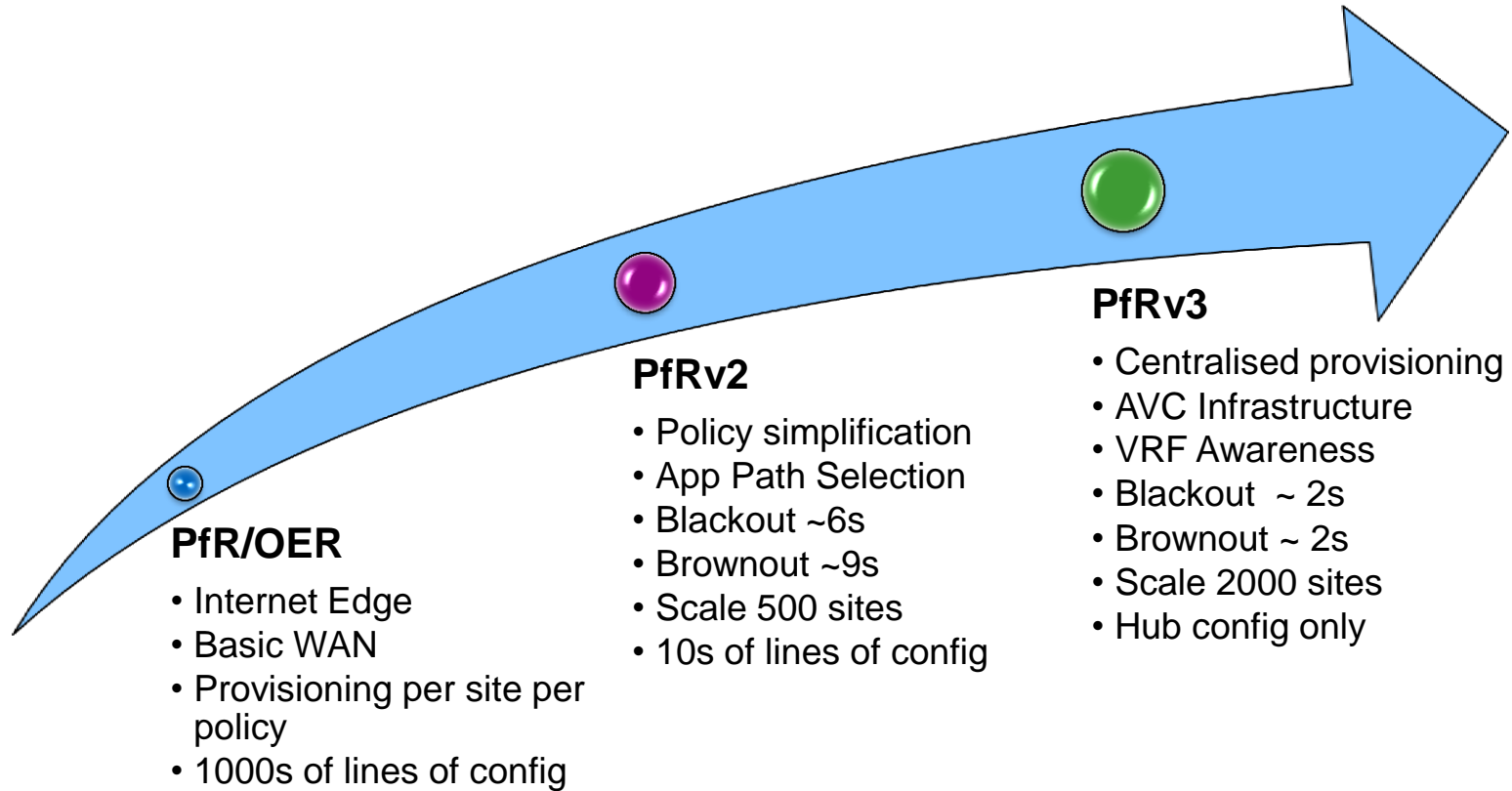
PfR Scale and Performance

	Scale	Notes
Typical Policies	2 TCs per site 650 Branches	Sufficient for protecting Voice/Video TC and load balancing all data traffic
Advanced Policies	4 TCs per site 300 Branches	Multiple application policies and load balancing
Max TCs	18K concurrent	ASR1002-X highest scale MC and BR

Recommended Hardware		
Hub or DC	ASR1002-X	Dedicated PfR MC, PfR BR+DMVPN Hub
Hub or DC	ISR 3945E	Dedicated IPSLA shadow router
Branch	ISR 892 FSP ISR1900 or better ASR1001 or better	Branch MC/BR+DMVPN spoke

PfR Evolution

Focusing on simplification and scale





Securing Connectivity

Securing the WAN

IPSec VPN and Firewall

Step 1: Secure Transport

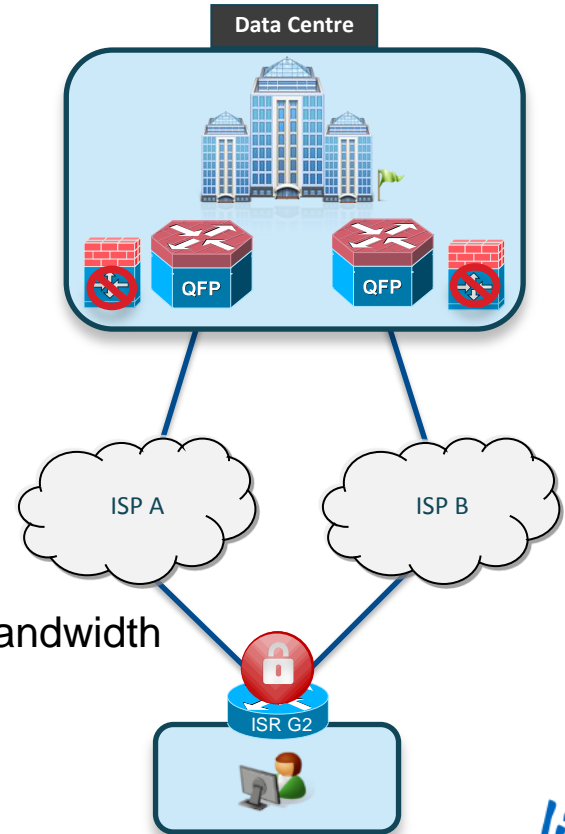
- IPSec with DMVPN overlay
 - Secure transport independent overlay
 - Add Strong Cryptography: IKEv2 + AES-GCM 256

Step 2: Threat Defence

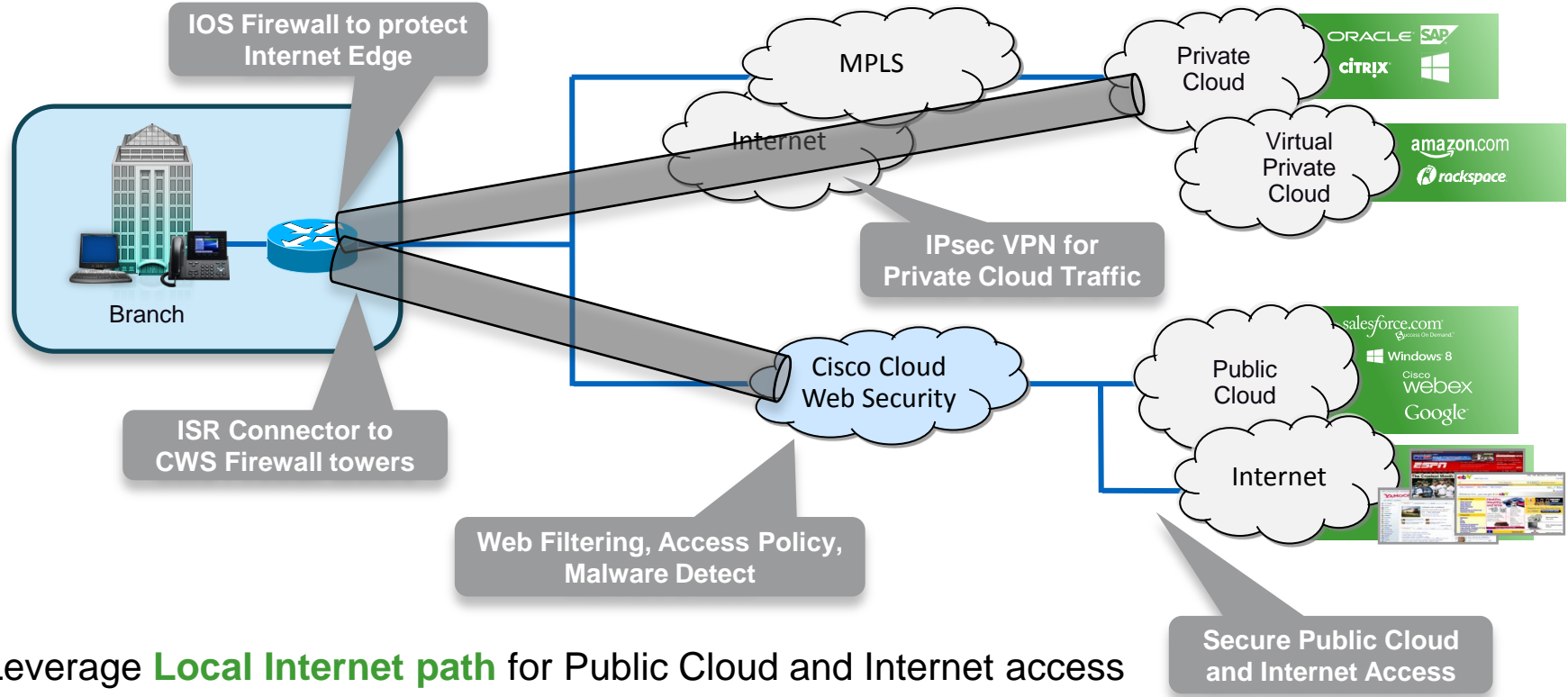
- IOS Zone-based Firewall
 - DHCP addressing for Internet and tunnel interfaces
 - Don't put tunnel addresses into DNS

Step 3: Choose your performance level

- Size router based on Encryption with Services and WAN bandwidth
 - Head-end: ASR1000 or ISR4451X
 - Branch: ISR-G2



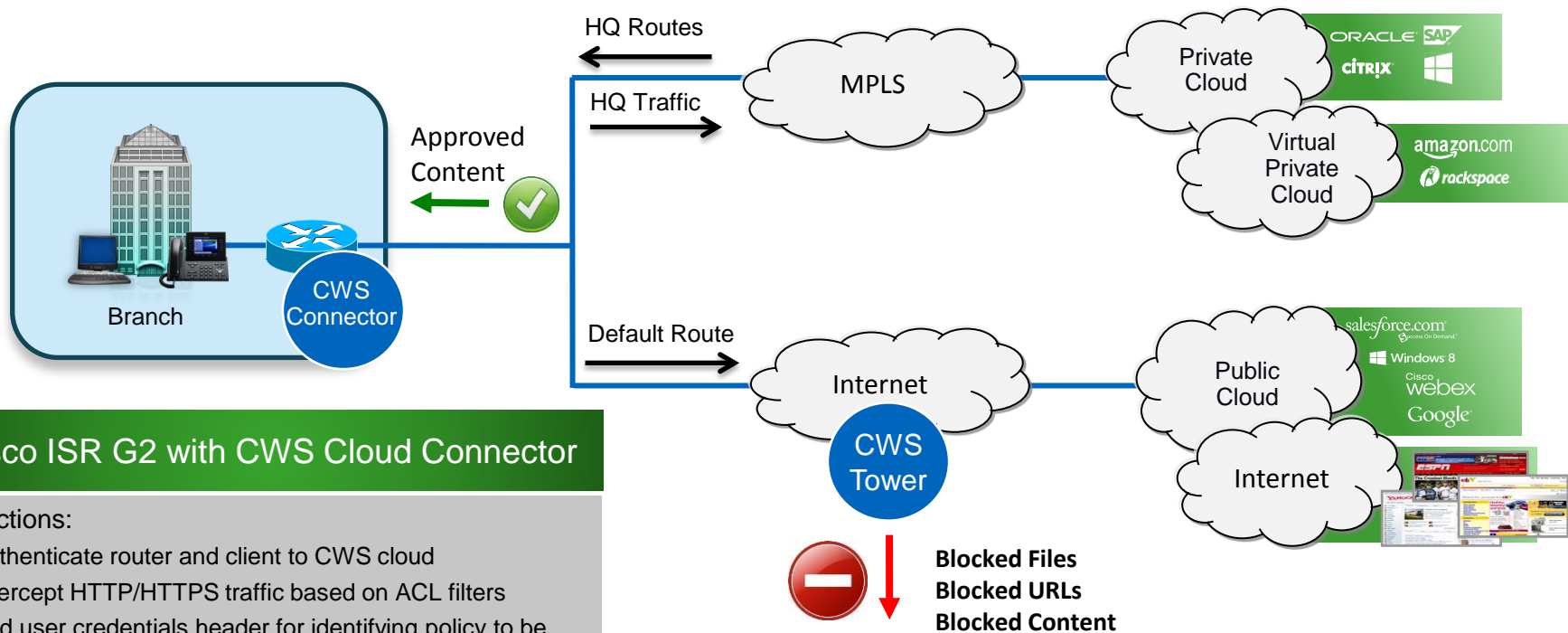
Secure Access for Public Cloud and Internet



- Leverage **Local Internet path** for Public Cloud and Internet access
- Improve application performance (right flows to right places)

Direct Internet Access

Cisco ISR CWS Connector



Cisco ISR G2 with CWS Cloud Connector

Functions:

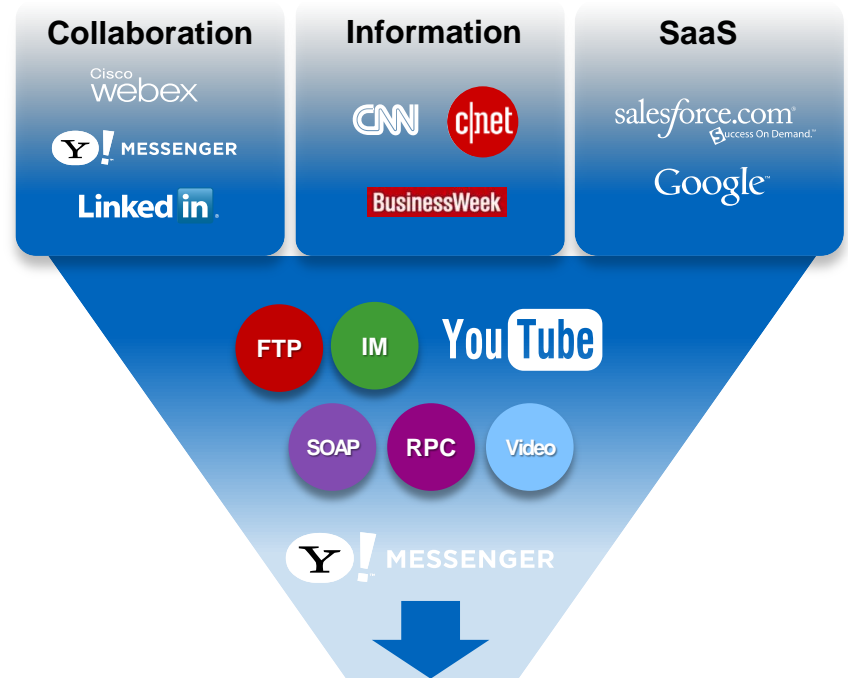
- Authenticate router and client to CWS cloud
- Intercept HTTP/HTTPS traffic based on ACL filters
- Add user credentials header for identifying policy to be applied (encrypted)
- Traffic Relay: replace client Source IP address with egress port IP or Loopback address
- Redirect to CWS for scanning



Application Optimisation

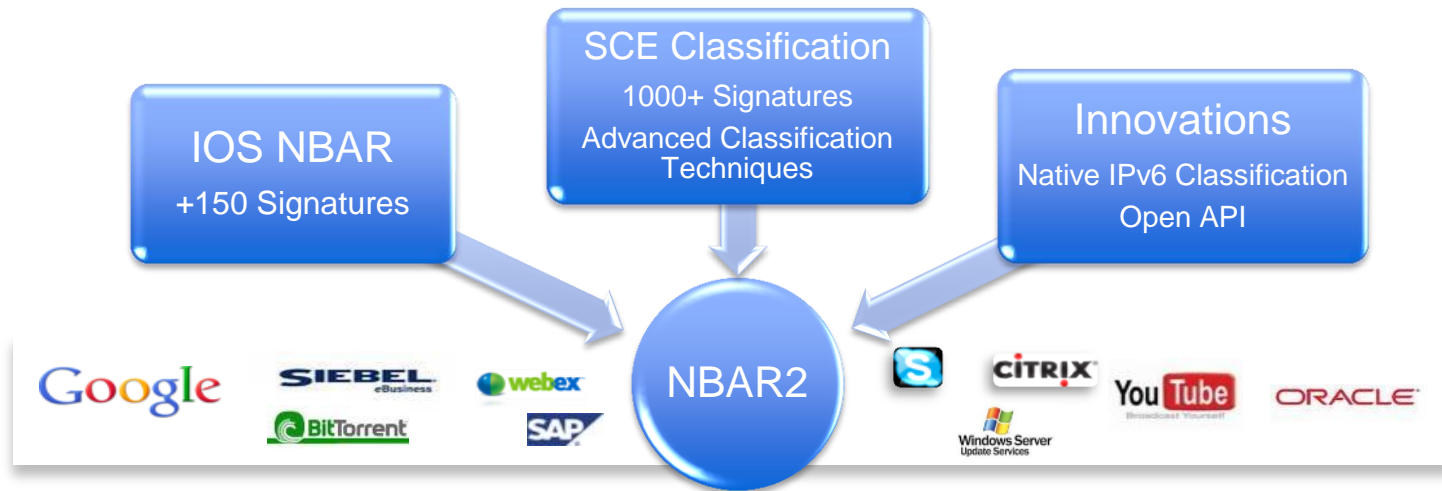
Today's Network Is an IT Blind Spot

- Static port classification is no longer enough
- More and more apps are opaque
- Increasing use of encryption and obfuscation
- Application consists of multiple sessions (video, voice, data)
- What if user experience is not meeting business needs?



HTTP is the new TCP

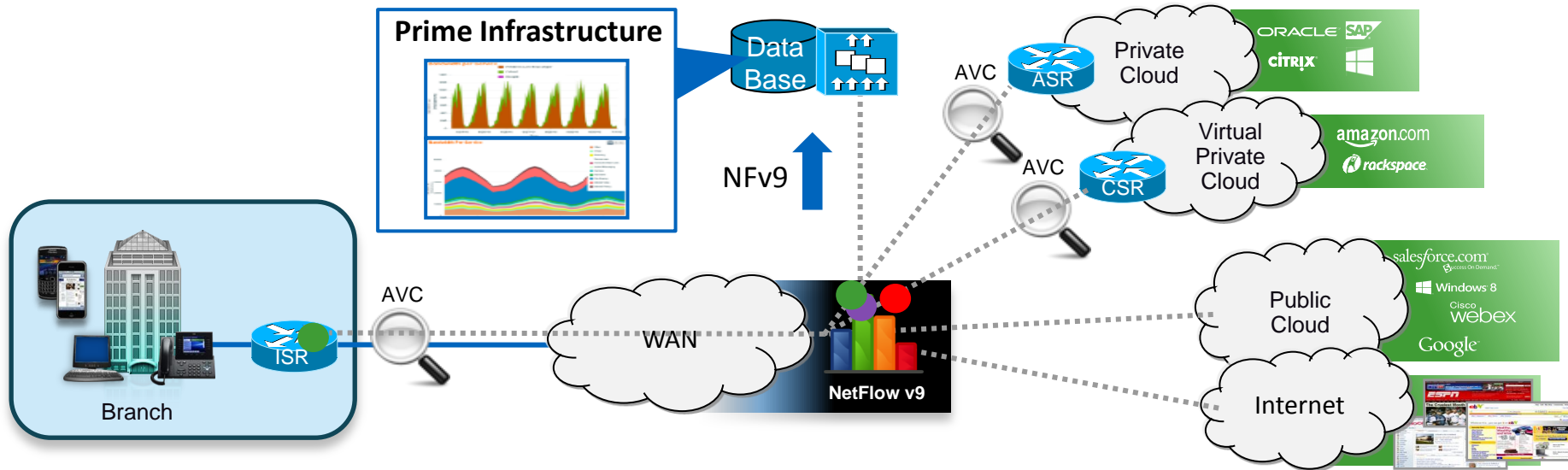
Next Generation NBAR (NBAR2)



- DPI engine provides Advanced Application Classification and Field Extraction Capabilities from SCE
- Protocol Pack allows adding more applications without upgrading or reloading IOS
- NBAR2 Protocol Library:
 - http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html
- NBAR2 Protocol List:
 - http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6558/ps6616/product_bulletin_c25-627831.html

Application Performance Monitoring

Track and Report Application Flows and Performance



1. Application Recognition

Router identifies applications using L3 to L7 Information

2. Data Collection and Exporting

Collect application performance metrics & export to mgmt tool

3. Management Tool

Advanced reporting tool aggregates and reports application performance

4. Control

Control app network usage to improve app performance

Per Site Traffic Shaping to Avoid Overruns

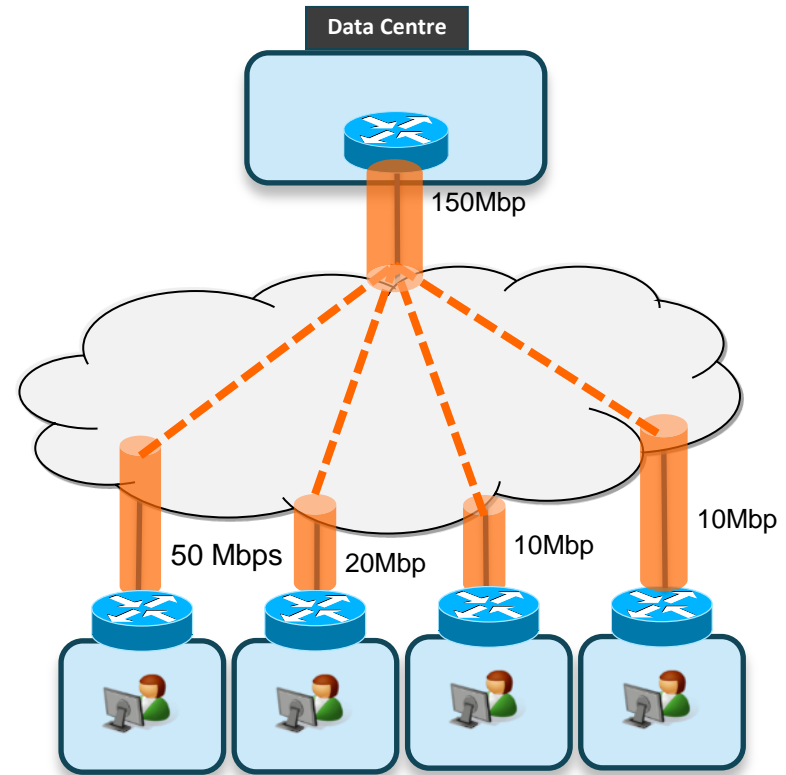
DMVPN Per-Tunnel QoS

- User NHRP group to dynamically provision HQoS policy on a DMVPN hub per-spoke basis

Spoke: Configure NHRP group name

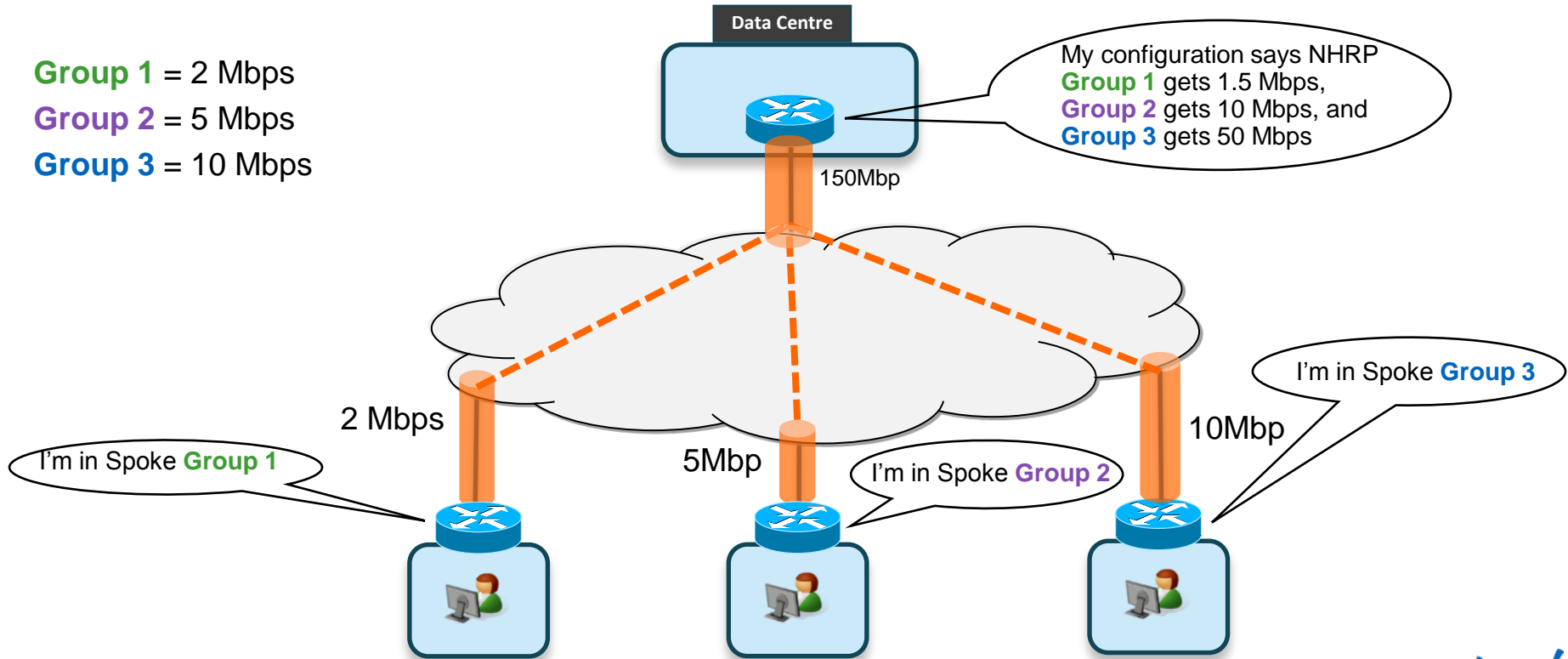
Hub: NHRP group name mapped to QoS template policy

- GRE, IPsec & L2 header are included in calculations for shaping and bandwidth.
- Queuing and shaping is performed at the outbound physical interface



Per Site Traffic Shaping to Avoid Overruns

- Group 1** = 2 Mbps
- Group 2** = 5 Mbps
- Group 3** = 10 Mbps

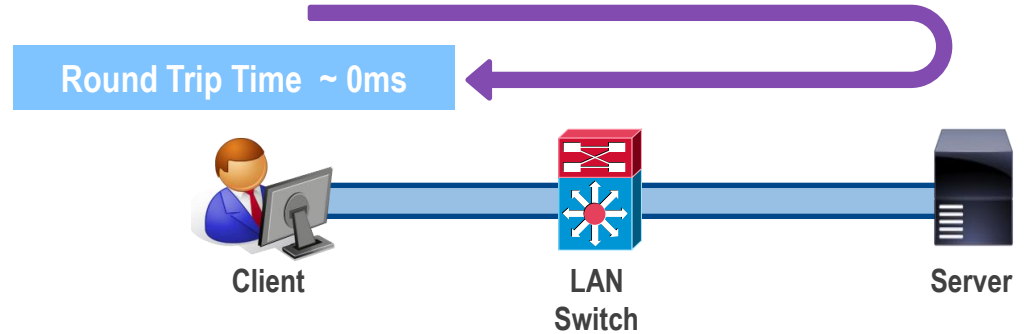


WAAS Overview

Application Delivery Challenges

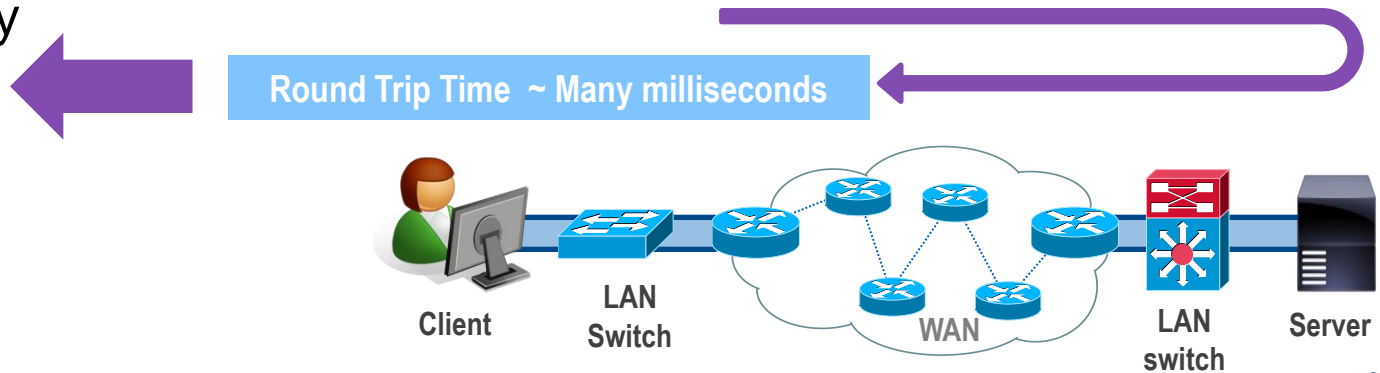
- LAN Connectivity

- High bandwidth
- No latency
- Reliable



- WAN Connectivity

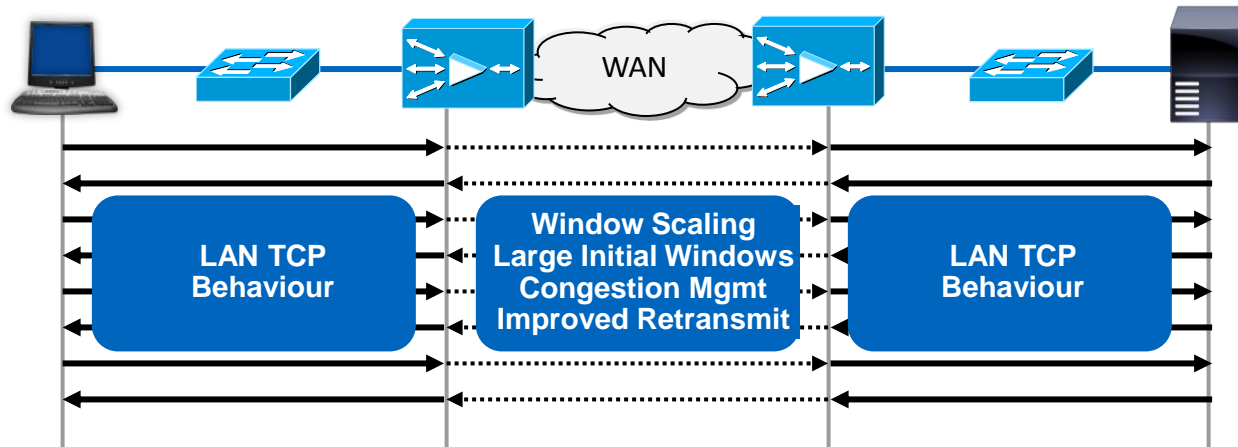
- Latency
- Low bandwidth
- Congestion
- Packet Loss



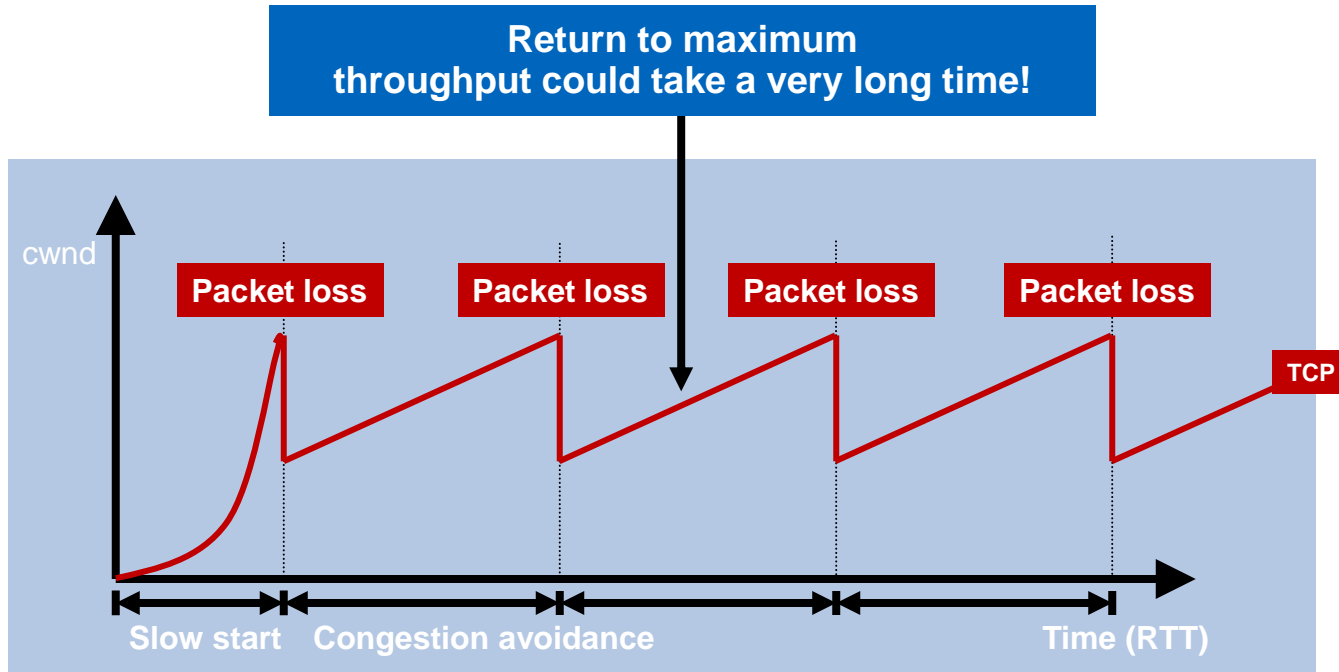
WAAS

TCP Performance Improvement

- Transport Flow Optimisation (TFO) overcomes TCP and WAN bottlenecks
- Shields nodes connections from WAN conditions

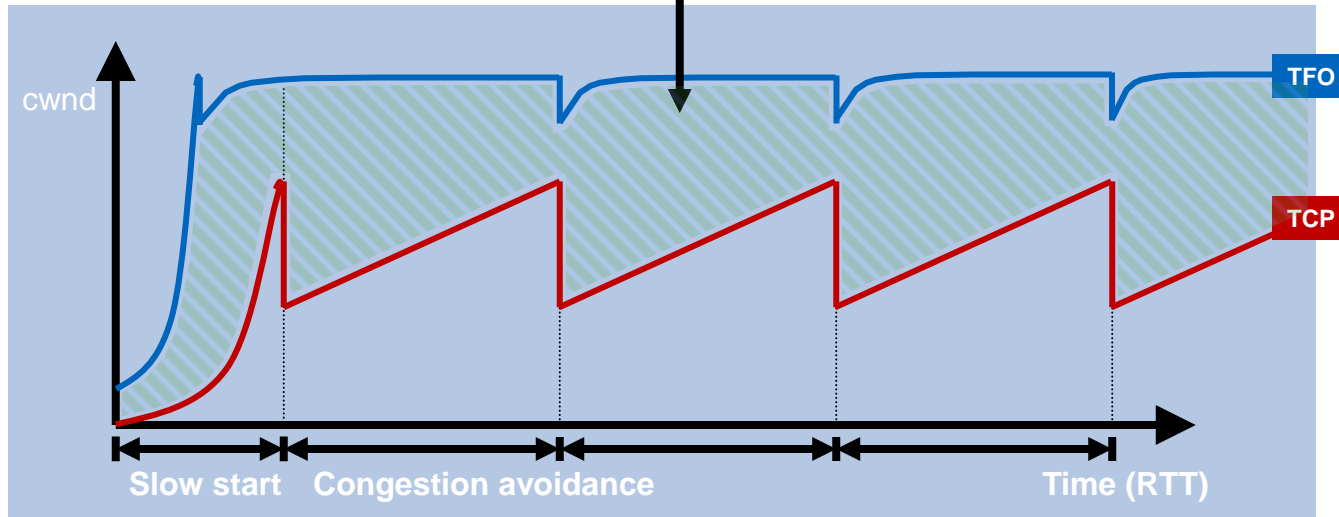


Comparing TCP and Transport Flow Optimisation



Comparing TCP and Transport Flow Optimisation

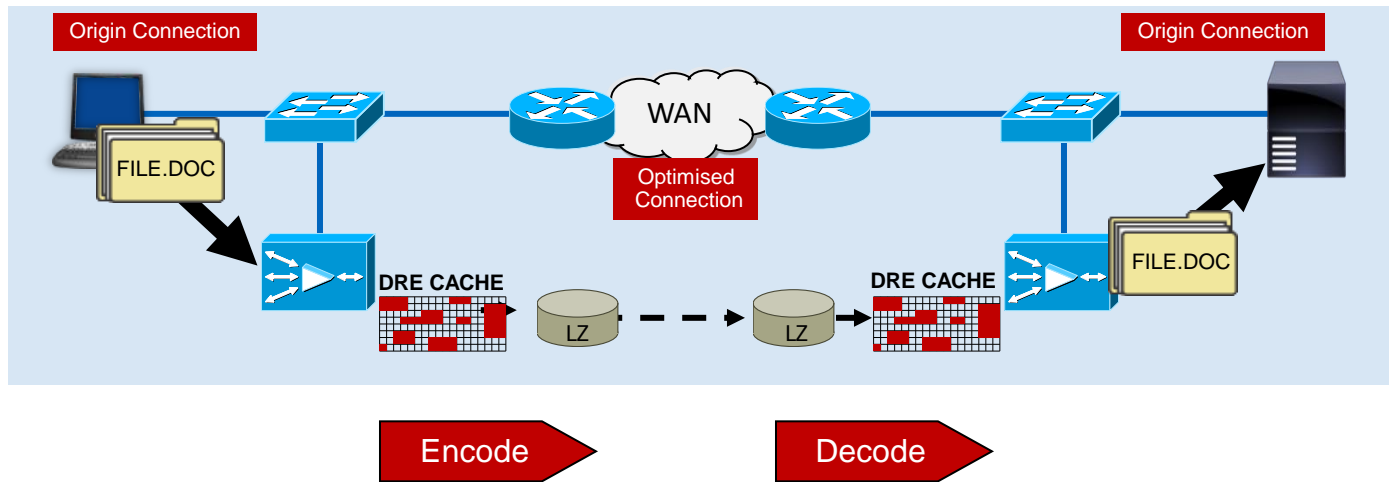
Cisco TFO provides significant throughput improvements over standard TCP implementations



WAAS Overview

DRE and LZ Manage Bandwidth Utilisation

- Data Redundancy Elimination (DRE) provides advanced compression to eliminate redundancy from network flows regardless of application
- LZ compression provides generic compression for all traffic



Important Notes

- NBAR2 today does not support asymmetric routing which is more likely with PfR (work in progress)
- AVC with WAAS requires NBAR2 applied on LAN, before optimisation
- PfRv2 does not support NBAR2, apply NBAR2 to LAN interface to classify applications with appropriate DSCP.
- PfRv2 requires WCCP GRE interfaces to be configured as PfR internal interfaces
- PfRv2 does not support WAAS Express—use WAAS
- NBAR2 + Performance Monitoring can be CPU/Memory resource intensive
- Size routers based on throughput with desired services enabled



Management and Simplification

Cisco Prime Lifecycle Services

Improve Network Control and Operational Productivity

Network Configuration



Plug-n-Play deployment automation

Discovery, Inventory, SWIM, Templates, Archive, etc

Converged wired and wireless workflows

CWS, VPN, Firewall, ACL, routing, VLAN

Network Health



Sites, Users and Role based access control

Static and Dynamic Grouping, Virtual Domains

RF Design, Device Health Dashboards, Fault and Reports

Device 360, Interface 360

Network Compliance and Support



Industry and Regulatory Compliance

Smart Interactions

Northbound REST APIs

Prime Infrastructure Toolbar and Mobile Application

Prime Infrastructure Plug-n-Play Options

No CLI Skills Required

PnP 1

Cisco Integrated Customisation Services (CICS)

- ISR router is delivered with CICS factory installed bootstrap config
- Installer connects LAN/WAN cables at the site

PnP 2

USB stick to bootstrap the ISR

- Installer connects LAN/WAN cables
- ISR loads bootstrap config from USB memory stick

PnP 3

Prime Plug-n-Play Application

- Installer connects LAN/WAN cables + a USB console cable to a Laptop/iPhone/iPad
- PnP Application bootstraps the router

PnP 4

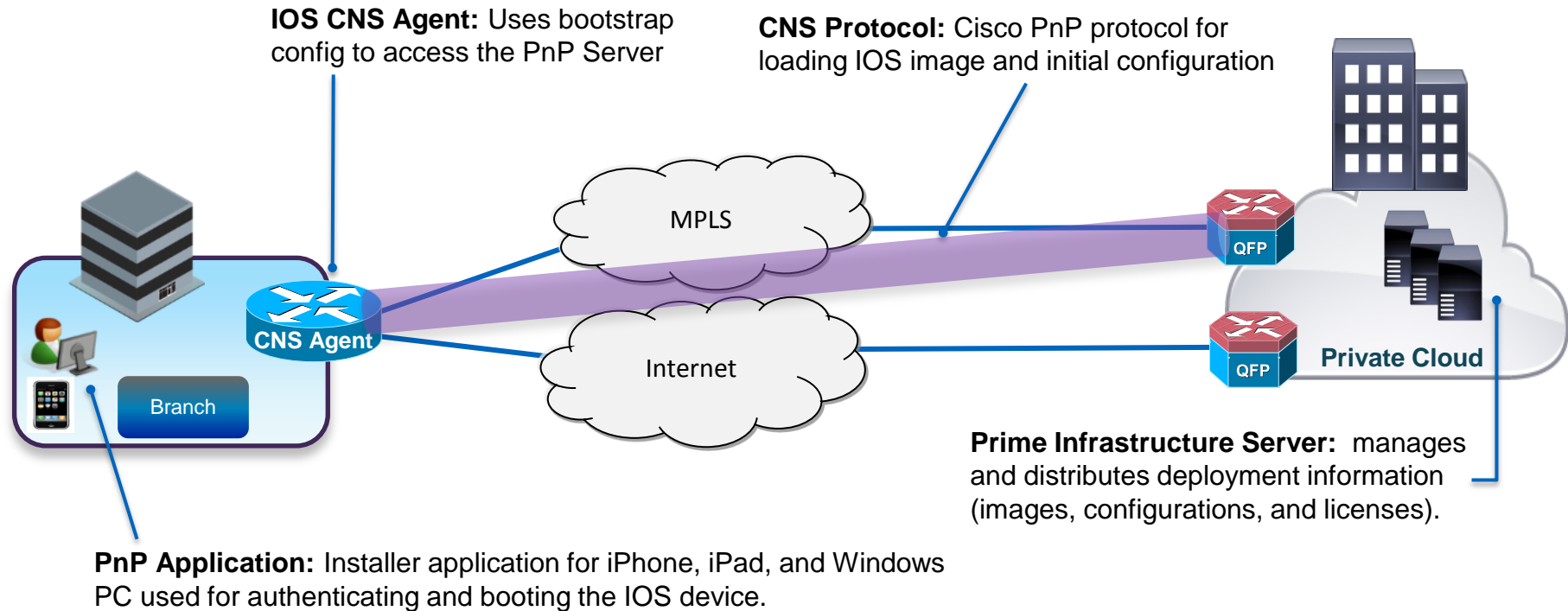
Cisco Configuration Professional Express (ISR Device GUI)

- Installer connects LAN/WAN cables + a PC to a LAN port
- CCP Express Application to bootstrap the router

Plug-n-Play Application

Solution Components

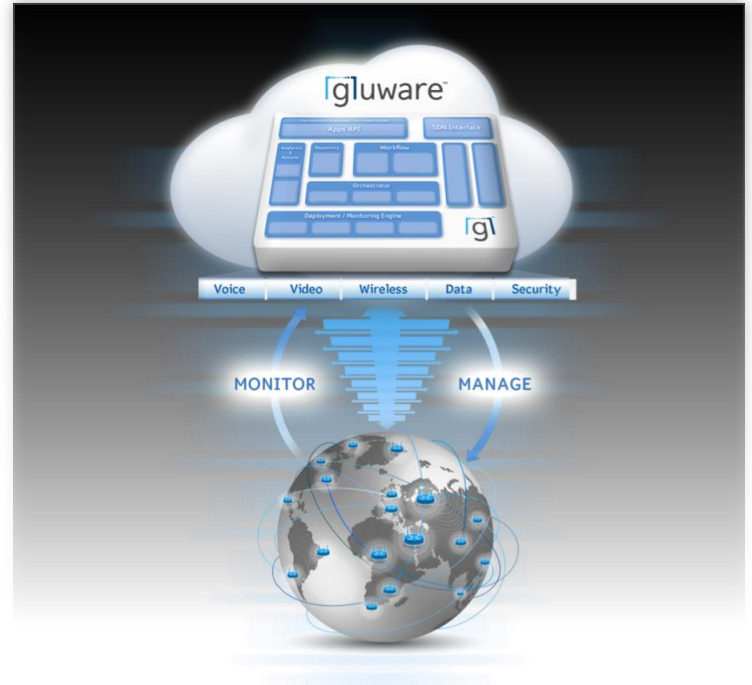
PnP 3



Glue Networks NGWAN/IWAN Orchestration



- Cloud-based SaaS subscription model
- Eliminates manual building of WANs
- Automated WAN orchestration and management
- Quick configuration updates and IOS upgrades
- Rapidly delivers nextgen and IWAN features
- Forward compatible with SDN and OnePK for app aware WANs
- Broadband and MPLS support for centralised hybrid WAN management for IWAN

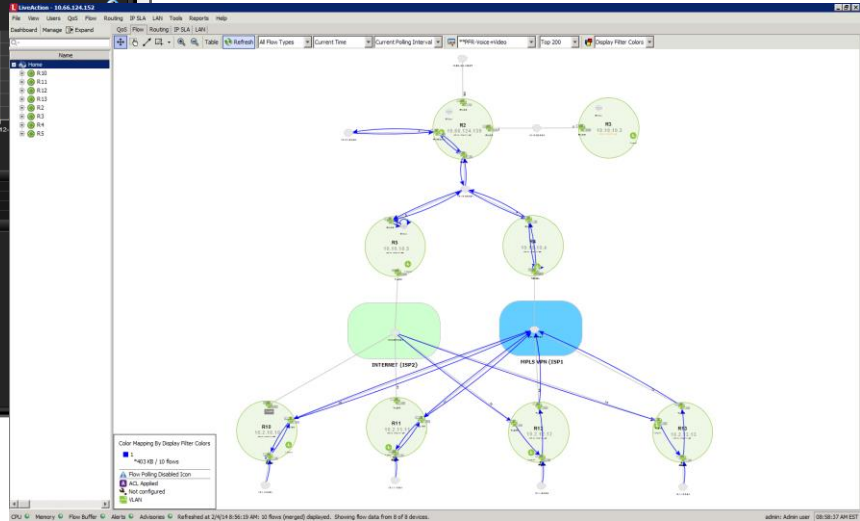


NMS Reporting Partners

Plixer










ActionPacked



LiveAction

- NetFlow Partners – Plixer, ActionPacked
- Cisco Prime Infrastructure 2.x – Future

Management Tool Matrix

Simplify Deployment	Prime Infrastructure 		
Transport Independent Design	Prime Infrastructure 		
Intelligent Path Control			
Application Optimisation	WAAS Central Manager 	 (AVC)	
Secure Connectivity	Prime Infrastructure 		
Network Health and Status	Prime Infrastructure 		

Summary

- Price Performance and Availability of Internet transport has significantly improved
- Public Cloud & SAAS applications make internet transport of critical applications a real consideration
- SLAs for Business Critical Applications
- Centralised Security Policy for Internet Access
- Under Your Control
- Simplify Deployment Through Plug-and-Play Tools



Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm



Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.

www.CiscoLiveAPAC.com



CISCO TM