TOMORROW starts here.

Next Generation Branch Networks: Services, Design and Implementation

BRKCRS-2000

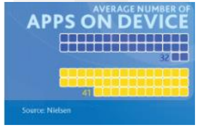
Matt Bolick

Technical Marketing Architect

Mobile Device Network Traffic

Average Number of Apps per Device*:

41



Average App Size**:

23 MB iOS

6 MB Android

25 MB Windows

OS Update File Size***:

750 MB iOS 7 for iPhone 5

168 MB Jelly Beans 4.1

400 MB Windows 7

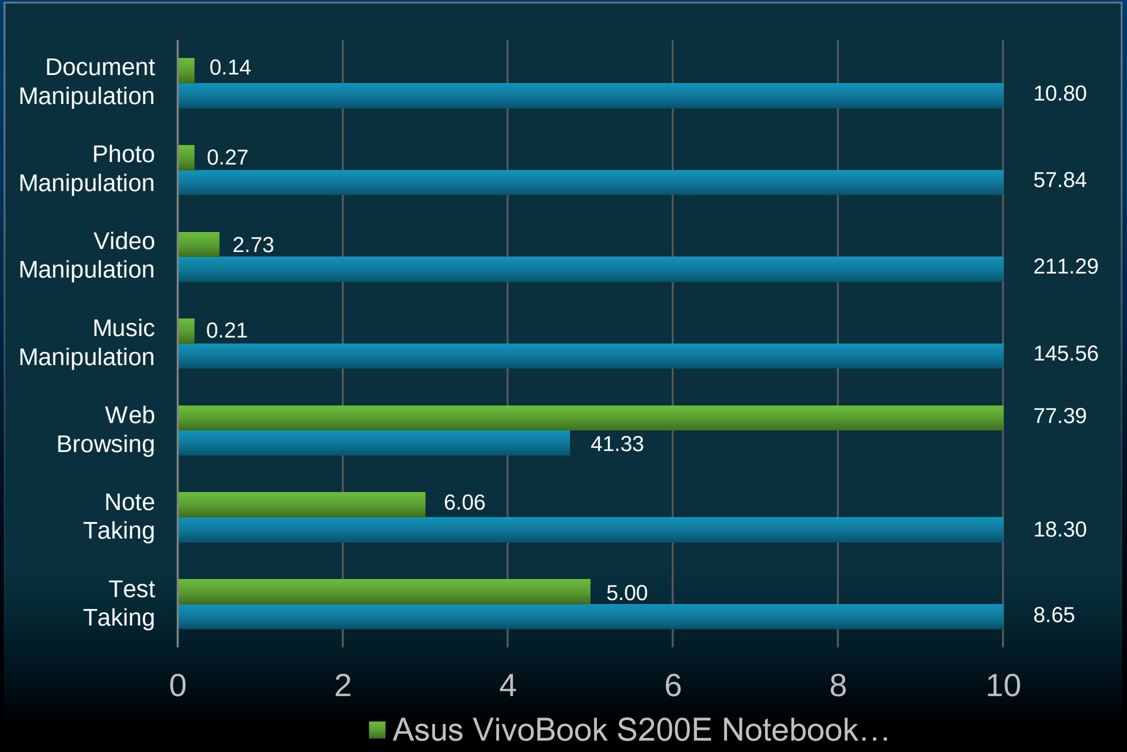
Sources:
* http://www.nielsen.com/us/en/newswire/2012/state-of-the-appnation-%C3%A2%C2%80%C2%93-a-year-of-change-and-growth-in-u-s-smartphones.html
** https://www.abiresearch.com/press/average-size-of-mobile-games-for-ios-increased-by-
*** http://www.wirelessandmobilenews.com/2013/05/samsung-galaxy-s3-iii-update-android-4.2.1-jelly-bean.html
http://theiphonewiki.com/wiki/Firmware#iPad_4
http://answers.microsoft.com/en-us/windows/forum/windows_other-windows_update/what-is-average-monthly-size-of-update-downloads/dfe9bb34-c2dd-478e-a6cb-0a26228cf552

© 2014 Cisco and/or its affiliates. All rights reserved.

Chromebook Creates an Average of 152 Times More Traffic

Third-Party Lab Test:
Chromebook vs.
Windows 8 Laptop

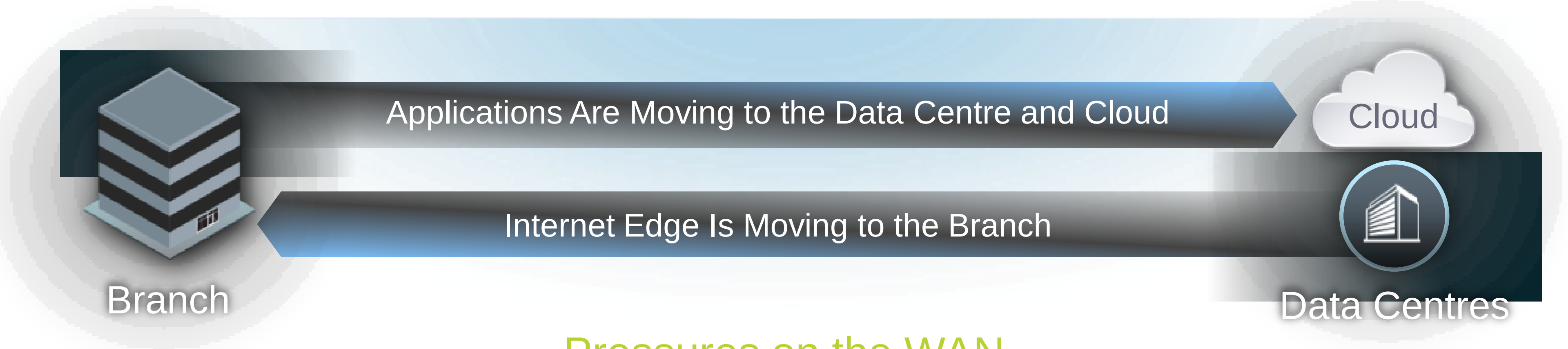
- Chromebook creates as high as 692.2 times more network traffic
- On average, Chromebook creates152 times more network traffic



http://principledtechnologies.com/Microsoft/Chromebook_PC_network_traffic_0613.pdf

Emerging Branch Demands

The Application Landscape Is Changing


Applications Are Moving to the Data Centre and Cloud
Internet Edge Is Moving to the Branch
Branch
Cloud
Data Centres

Pressures on the WAN

Cloud

50% of CIOs Expect to Operate via the Cloud by 2015

Mobility

6X More Mobile Data Traffic by 2015

Fat Apps

2/3 of Mobile Traffic Will Be Video

© 2014 Cisco and/or its affiliates. All rights reserved.

The Branch is More Relevant Than Ever

- Where You Engage Customers
- Source of Business Intelligence
- Up to 80% of Your Employees

To Grow Your Business and Innovate, Your Remotes Sites Must Keep Pace With HQ

© 2014 Cisco and/or its affiliates. All rights reserved.

Advantages of Added Intelligence in the WAN

- Common Design Across a Variety of Transport Options
- Dramatic Bandwidth, Price Performance Benefits
- Higher Network Availability
- Performance Matched to Application Needs

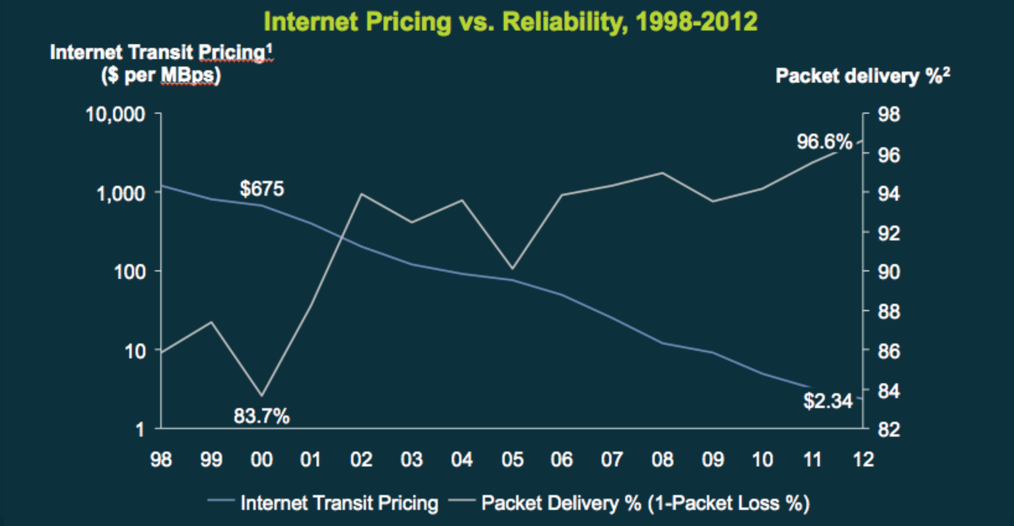
© 2014 Cisco and/or its affiliates. All rights reserved.

Evolution of WAN Transport Options

Low Cost Alternative

46%

of Organisations Are Planning to Transition to Internet Connections

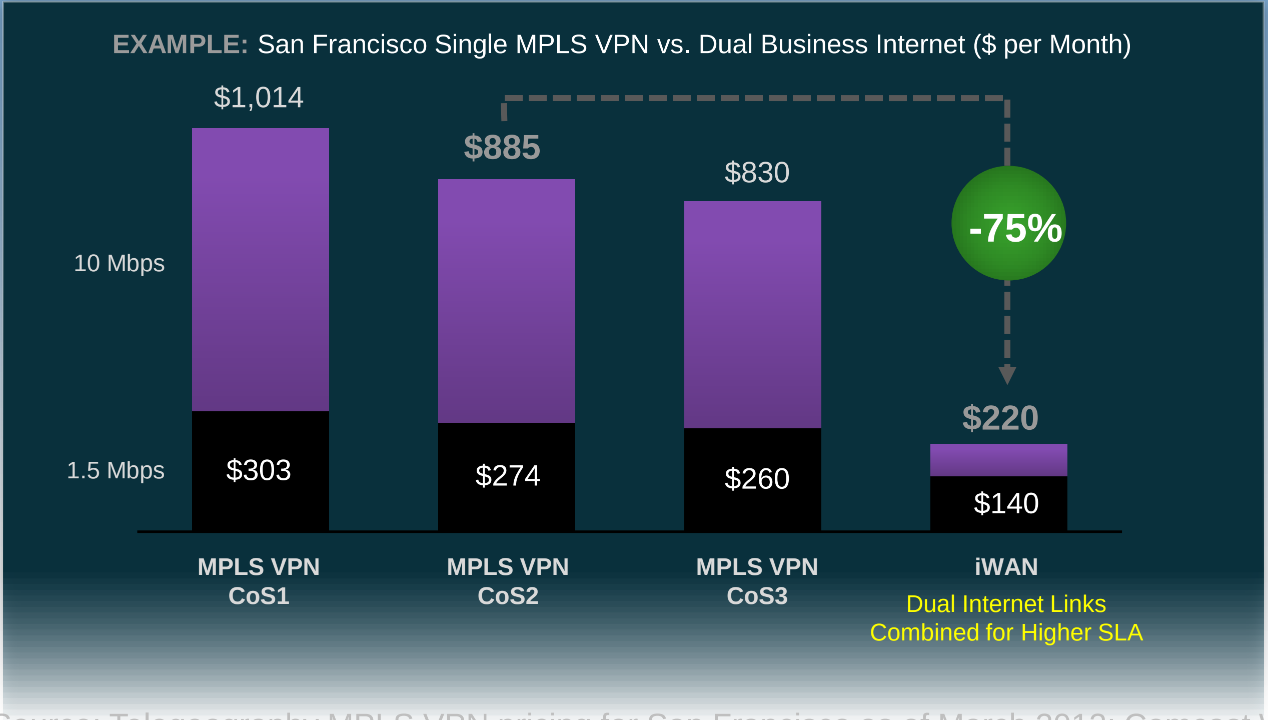


1. Internet Transit Pricing based on surveys and informal data collection primarily from Internet Operations Forums—'street pricing' estimates
2. Packet delivery based on 15 years of ping data from PingER for WORLD (global server sample) from EDU.STANFORD.SLAC in California

Source: William Norton (DrPeering.net); Stanford ping end-to-end reporting (PingER)

Flexibility from a Transport Agnostic Design

EXAMPLE: San Francisco Single MPLS VPN vs. Dual Business Internet ($ per Month)



$665 Savings/Month x
12 Months X 1,000 Sites

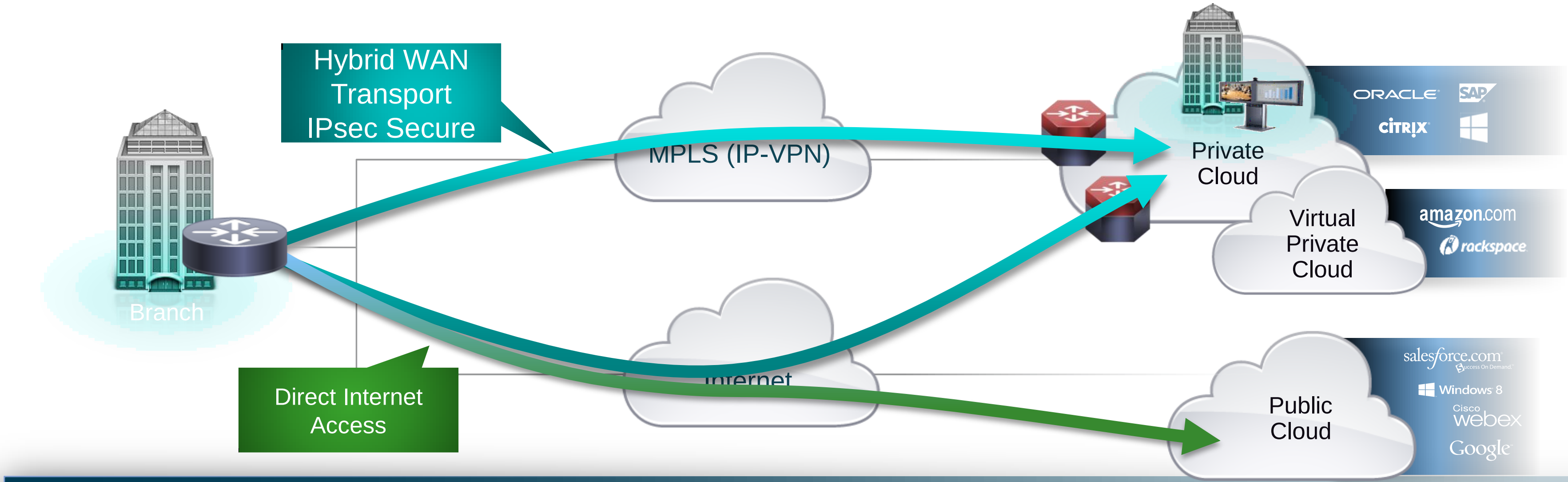
= $8M Savings
per Year

Source: Telegeography MPLS VPN pricing for San Francisco as of March 2013; Comcast Web site; Verizon website

© 2014 Cisco and/or its affiliates. All rights reserved.

Hybrid Transport Options in the Enterprise

Secure WAN Transport and Internet Access



- Secure WAN transport for private and virtual private cloud access
- Leverage local Internet path for public cloud and Internet access
- Increased WAN transport capacity; and cost effectively!
- Improve application performance (right flows to right places)

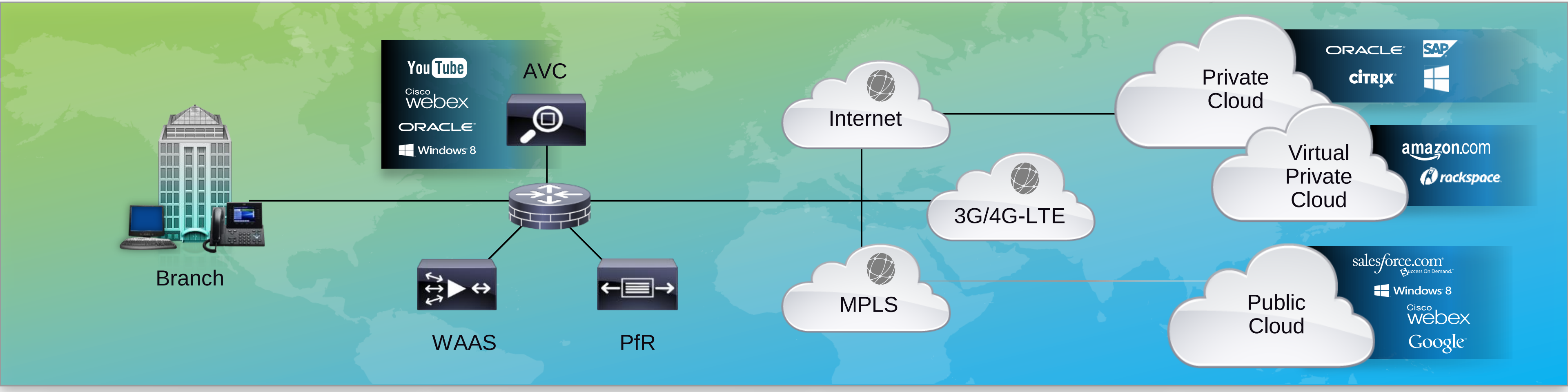
Intelligent WAN: Leveraging the Internet

So What is New Here?

- Transport Agnostic Design with High Reliability
- SLAs for Business-Critical Applications
- Centralised Security Policy for Internet Access
- Dramatically Lower WAN Costs Without Compromise

Added Intelligence within the Network

Full Menu of Capabilities to Squeeze Value from the WAN



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 utilisation of all bandwidth
- Improved network availability
- **Performance Routing (PfR)**

Application Optimisation

- Application monitoring with Application Visibility and Control (AVC)
- Application Acceleration and bandwidth savings with WAAS

Secure Connectivity

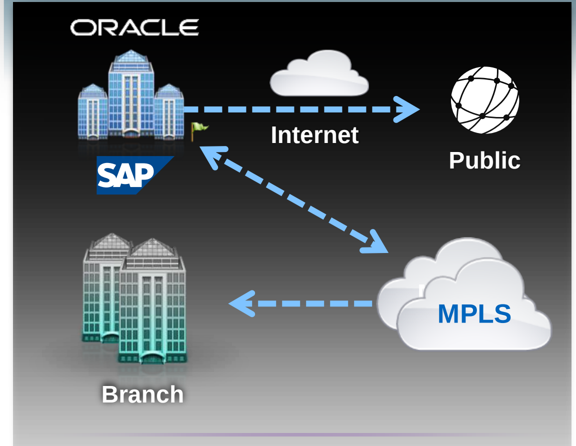
- Certified strong encryption
- Comprehensive threat defence with ASA and IOS Firewall/IPS
- Cloud Web Security (CWS) for scalable secure direct Internet access

© 2014 Cisco and/or its affiliates. All rights reserved.

WAN Flexibility with a Transport Agnostic Design

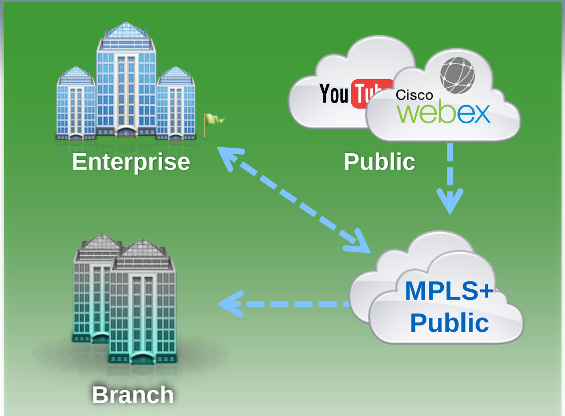
Pick the best transport in every geography with a common network design

Dual MPLS



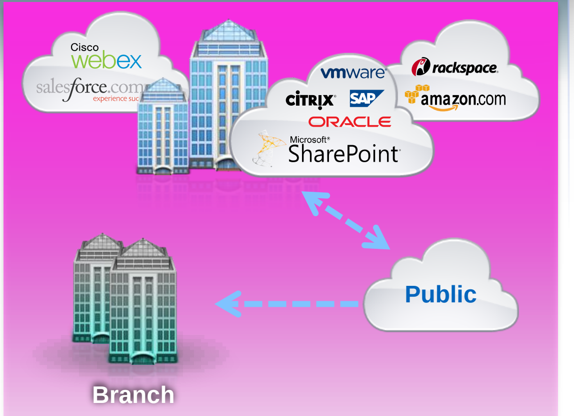
- ✓ Highest SLA guarantees
- – Tightly coupled to SP
- ẋ Expensive

✓ Hybrid



- ✓ More BW for key applications
- ✓ Balanced SLA guarantees
- – Moderately priced

✓ Dual Public



- ✓ Best price/performance
- ✓ Most SP flexibility
- – Enterprise responsible for SLAs

Consistent VPN Overlay Enables Security Across Transition

Transport-Independent Design

Flexibility in WAN Design

Flexible 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

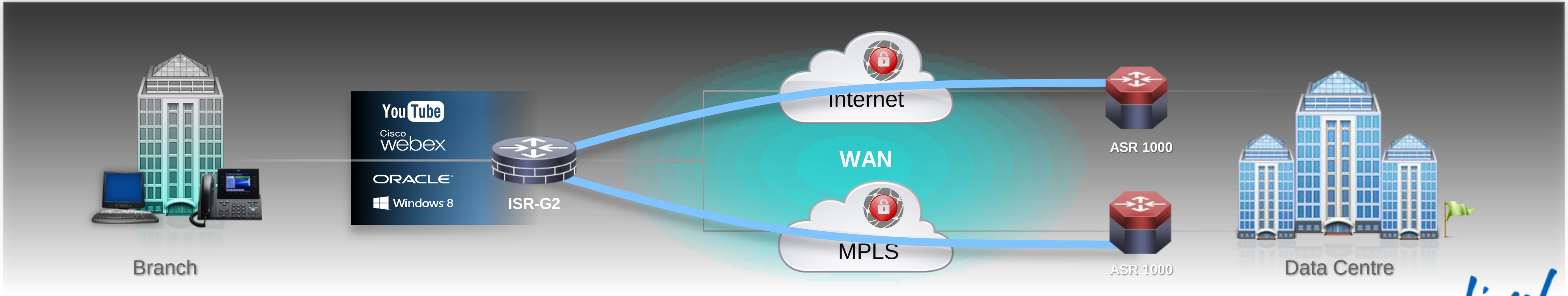
Dynamic Full-Meshed Connectivity

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

Secure

Proven Robust Security

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



© 2014 Cisco and/or its affiliates. All rights reserved.

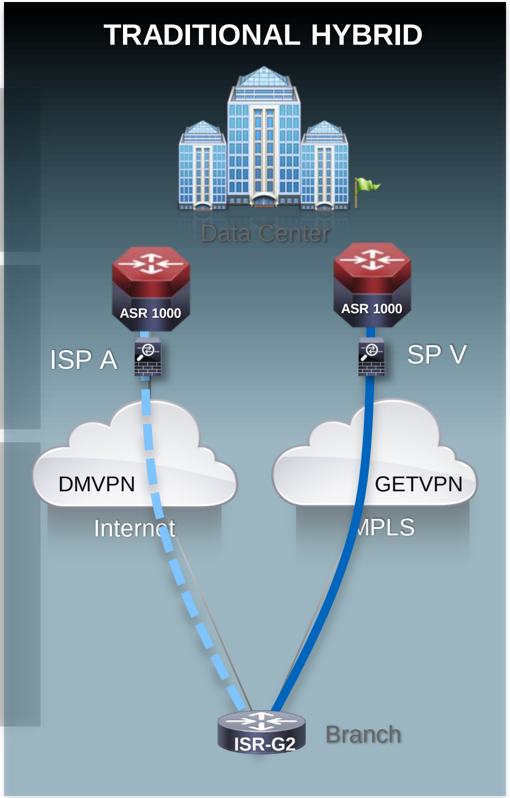
Hybrid WAN Designs

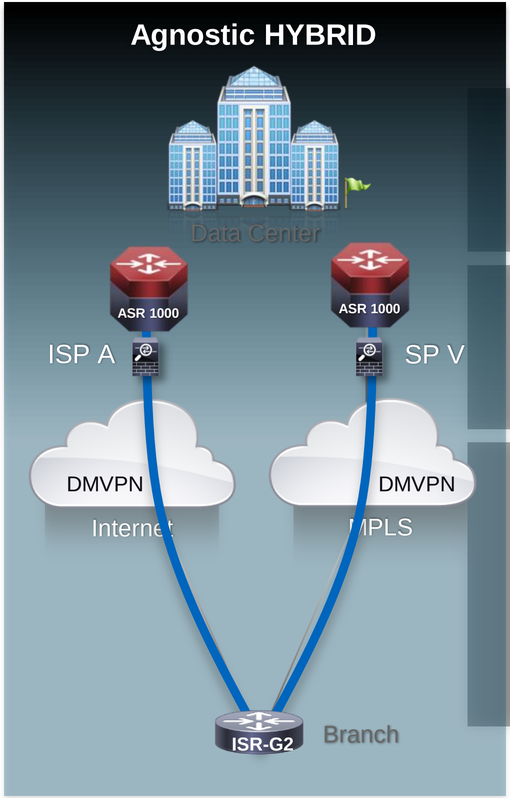
Traditional and Transport Agnostic

Active/Standby
WAN Paths
Primary With Backup

Two IPsec Technologies
GETVPN/MPLS
DMVPN/Internet

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





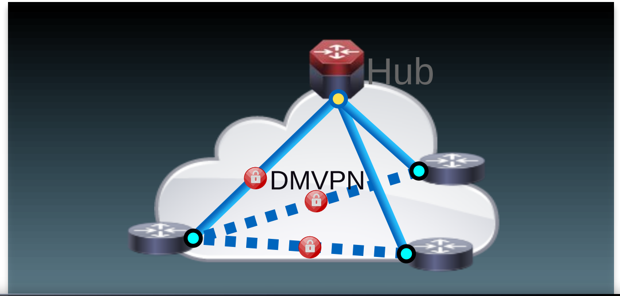
Active/Active
WAN Paths

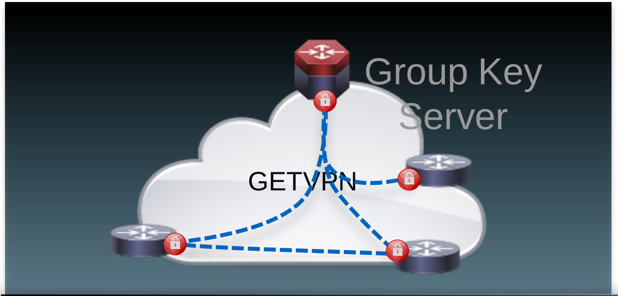
One IPsec Overlay
DMVPN

One WAN Routing
Domain
iBGP, EIGRP, or OSPF

© 2014 Cisco and/or its affiliates. All rights reserved.

DMVPN and GETVPN Comparison





Overlay Routing	Minimal-to-no Peering With Provider Easy Multi-Homing Designs Provider Blackhole Protection	BGP and Static Routing With Provider Provider Routes Traffic Between Sites Less Control Plane Overhead Traffic	**Native Routing**
Data Plane	**Any WAN Transport: Internet, MPLS** Site-to-Site Requires Tunnel Setup Hubsite Multicast Replication **Per-Tunnel QoS From Hub**	Private WANs Only: MPLS **No Tunnels for Site-to-Site Connectivity** **Multicast Replication in Provider Network**	**Data Plane**
IPsec	**Per Tunnel Keys** **Client IP Addressing Hidden From Provider**	Single Group Key for All Sites Client IP Addressing Exposed to Provider	**IPsec**

© 2014 Cisco and/or its affiliates. All rights reserved.

Transport Independent Designs

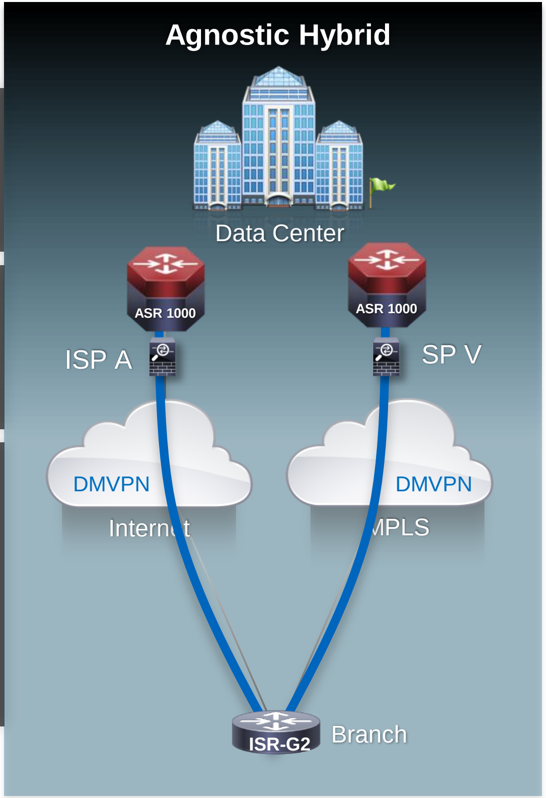
Same Design over MPLS, Internet, 3G/4G...

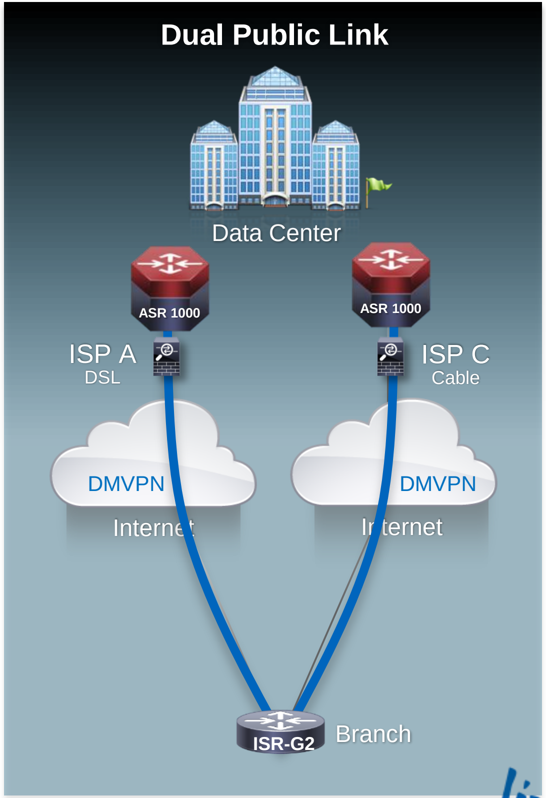
One Active/Active WAN Paths

One DMVPN IPsec Overlay

One WAN Routing Domains

iBGP, EIGRP, or OSPF





© 2014 Cisco and/or its affiliates. All rights reserved.

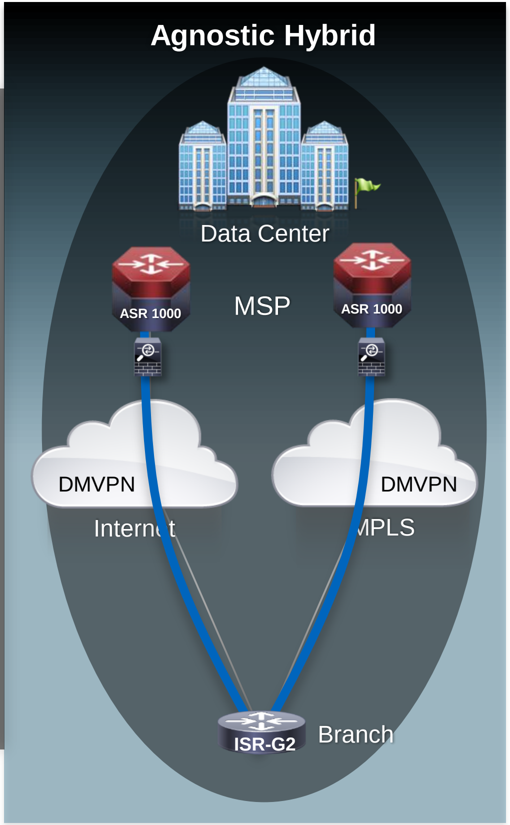
Self, Integrator, or Provider Managed

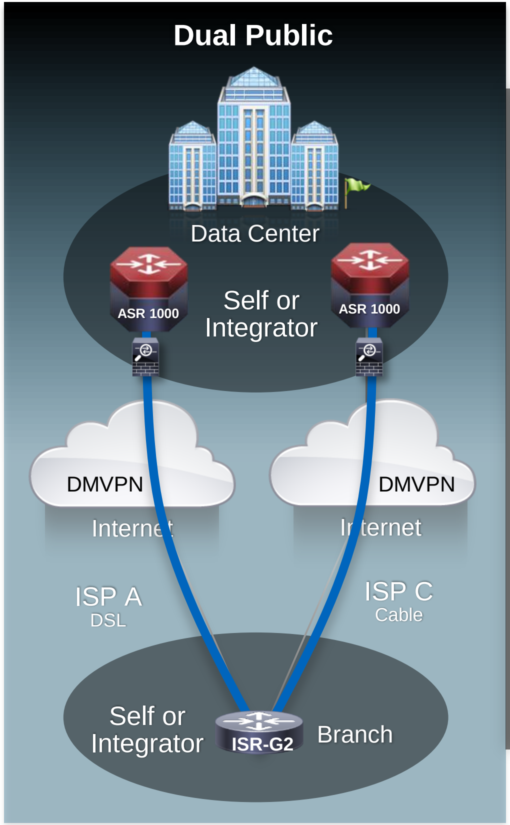
Managed Service Provider

Hybrid Model Typical

Increases HA Diversity

Competitive Service Offering





Self/Integrator Managed

Hybrid or Internet Models

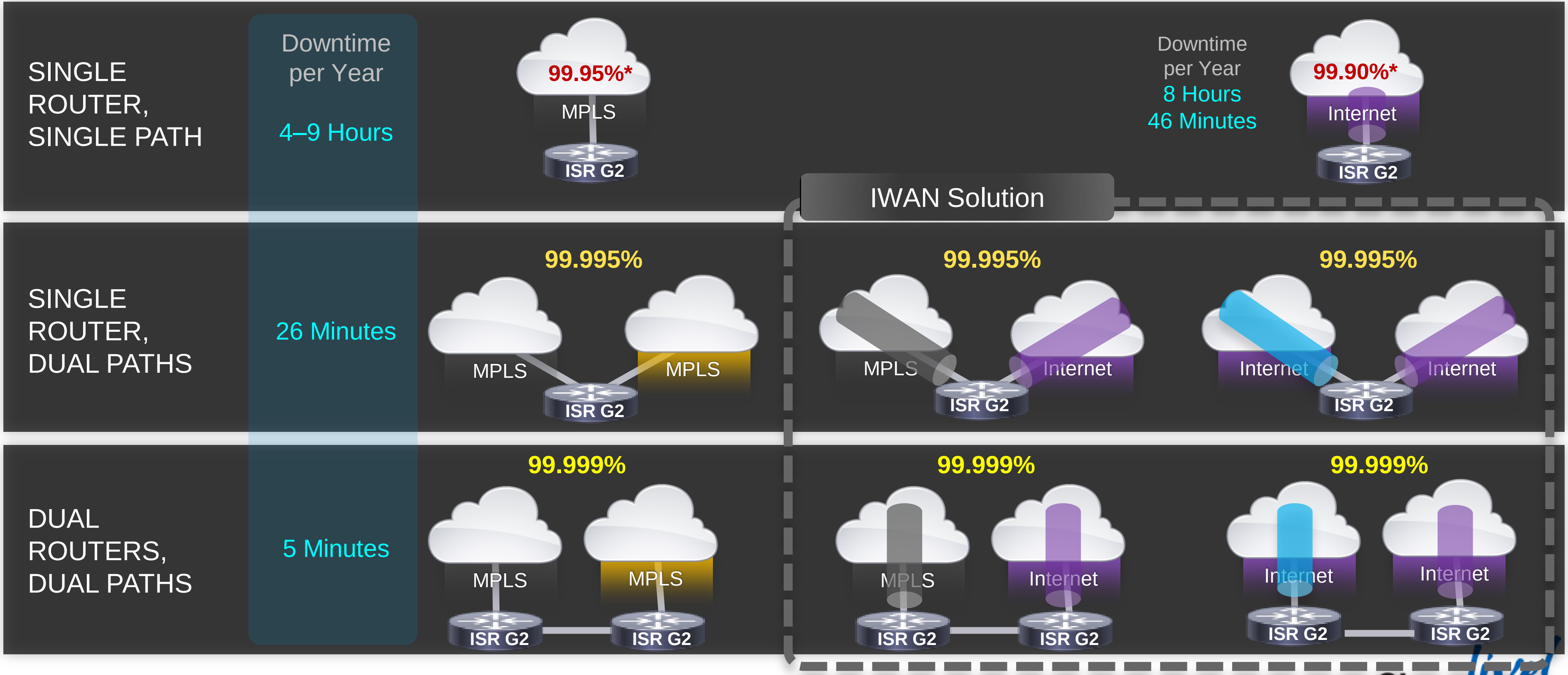
Ownership of Service Levels

Competitive Provider Selection

© 2014 Cisco and/or its affiliates. All rights reserved.

Network Availability with Various Transports

Redundancy and Path Diversity Matter



	Downtime per Year
SINGLE ROUTER, SINGLE PATH	4–9 Hours
SINGLE ROUTER, DUAL PATHS	26 Minutes
DUAL ROUTERS, DUAL PATHS	5 Minutes

Downtime per Year
8 Hours
46 Minutes

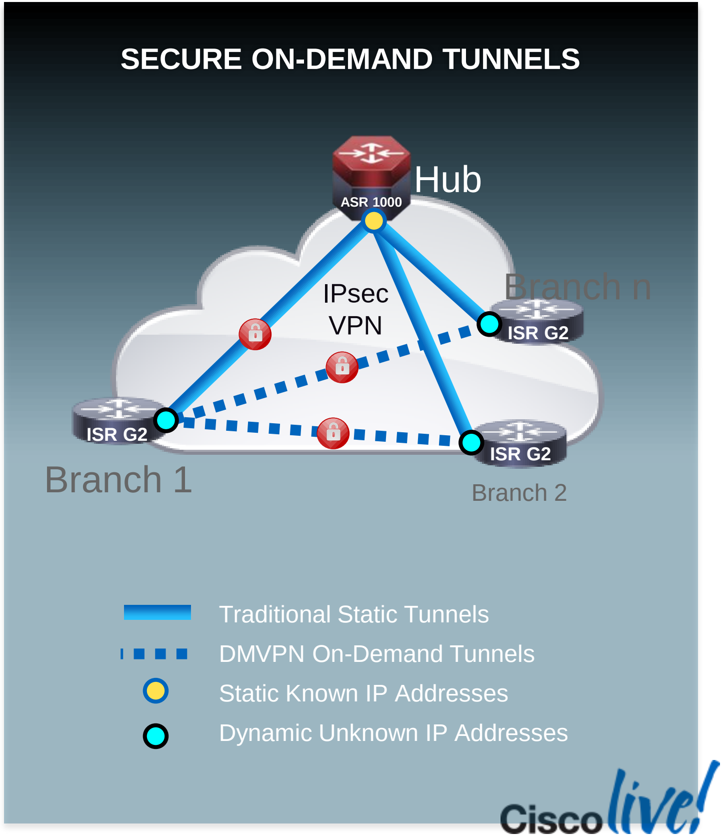
IWAN Solution

* Typical MPLS and Business Grade Broadband Availability SLAs and Downtime per Year, calculated with Cisco AS DAAP tool.

© 2014 Cisco and/or its affiliates. All rights reserved.

Over-the-Top WAN Design WithnDynamic Multipoint VPN (DMVPN)

- Branch spoke sites establish an IPsec tunnel to and register with the hub site
- IP routing exchanges prefix information for each site
  - BGP or EIGRP are typically used for scalability
- Only the WAN IP addresses need to be known by the WAN transport
  - WAN interface IP address can be used for the tunnel source address
- Data traffic flows over the DMVPN tunnels
- When traffic flows between spoke sites, the hub assists the spokes to establish a site-to-site tunnel
- Per-tunnel QOS is applied to prevent hub site oversubscription to spoke sites



© 2014 Cisco and/or its affiliates. All rights reserved.

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

Major Features

Configuration reduction and no-touch deployment

Supports:

Passenger protocols (IP(v4/v6) unicast, multicast and dynamic Routing Protocols)

Transport protocols (NBMA) (IPv4 and IPv6)

Remote peers with dynamically assigned transport addresses.

Spoke routers behind dynamic NAT; Hub routers behind static NAT.

Dynamic spoke-spoke tunnels for partial/full mesh scaling.

Works with MPLS; GRE tunnels and/or data packets in VRFs and MPLS switching over the tunnels

Wide variety of network designs and options.

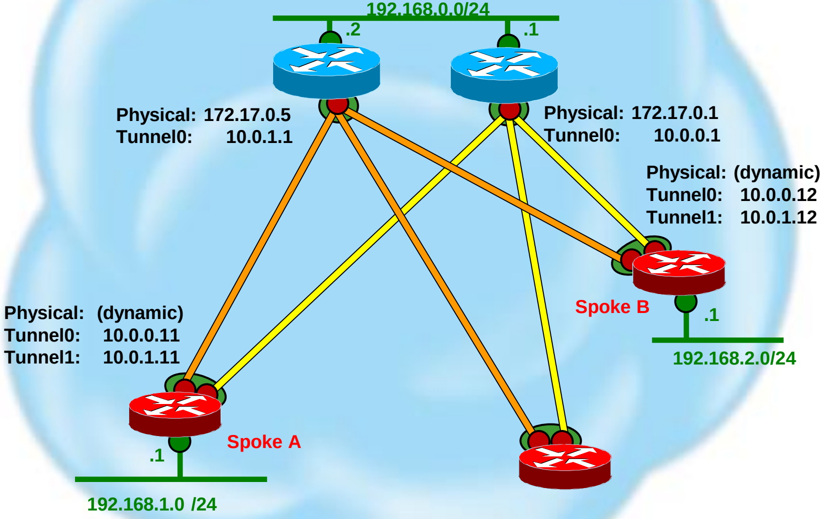
DMVPN Phases

Phase 1 – 12.2(13)T	Phase 2 – 12.3(4)T	Phase 3 – 12.4.(6)T
• **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**	• 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**	• 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

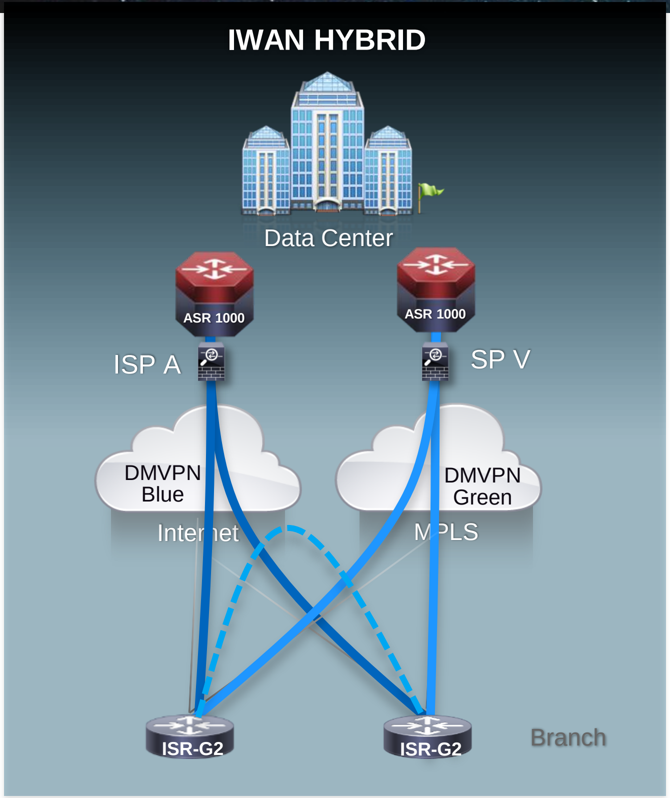
- Spokes build a dynamic permanent GRE/IPsec tunnel to the hub, but not to other spokes. They register as clients of the NHRP server (hub).
- Active-Active redundancy model – two or more hubs per spoke
  - All configured hubs are active and are routing neighbours with spokes
  - Routing protocol routes are used to determine traffic forwarding
- When a spoke needs to send a packet to a destination (private) subnet behind another spoke, it queries via NHRP for the real (outside) address of the destination spoke.
- Now the originating spoke can initiate a dynamic GRE/IPsec tunnel to the target spoke (because it knows the peer address).
- The dynamic spoke-to-spoke tunnel is built over the mGRE interface.
- When traffic ceases then the spoke-to-spoke tunnel is removed.

Dual DMVPN Design
Single mGRE tunnel on Hub, two mGRE tunnels on Spokes



© 2014 Cisco and/or its affiliates. All rights reserved.

Transport Agnostic DMVPN Design



DMVPN Phase 2

- Site-to-Site dynamic tunnels
- PfRv2 interoperability

Multiple DMVPNs for Path Diversity

- High Availability
- Brown out isolation – PfR
- Load Balancing – PfR and Routing Protocol

Performance Routing (PfR)

- Monitors performance on Tunnel Interfaces
- Reroutes traffic between Tunnel Interfaces

Consistent simplified routing overlay

- BGP, EIGRP and OSPF
- Single routing domain
- Simple ECMP or best path provisioning

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco Router Security Certifications

	FIPS 140-2, Level 2	**Common Criteria** EAL4	**NSA Suite B*** Software Support	**NSA Suite B*** Hardware Assist
Cisco ISR 890 Series	✓	✓	✓	✓
Cisco ISR 1900 Series	✓	✓	✓	✓
Cisco ISR 2900 Series	✓	✓	✓	✓
Cisco ISR 3900 Series	✓	✓	✓	✓
Cisco ISR 3900E Series	✓	✓	✓	✓
Cisco ASR 1000 Series	✓	✓	N/A	✓**

* NSA endorses Suite B (RFC-4869) cryptography for both unclassified and most-classified information

http://www.cisco.com/go/securitycert

** ASR 1002-X and ESP-100

© 2014 Cisco and/or its affiliates. All rights reserved.

Add Strong Encryption: Branch to HQ Suite-B Support

Threat Landscape Is Changing

- Communications and IT infrastructures must be defended against cyber attacks and exploitation
- Attackers are persistent and well funded
- Computing advances are driving a move to higher cryptographic strengths

ISR and ASR1K Platforms

- Future-ready: Meets security and scalability requirements for 20 years
- Efficiency and scale: Hardware crypto acceleration

	Old Encryption Hazards	Cisco Suite-B	Commodity Routers
AES, 3DES	1GB Encryption Limit	●	🔴
HMAC-MD5	Theoretical Weaknesses	●	🔴
DH, RSA	Significant Risk	●	🔴
RSA	Significant Risk	●	🔴
MD5, SHA1	Collision Attacks	●	🔴
Entropy	Significant Risk	●	🔴
TLS1.0, IKEv1	Known Flaws, Lack of Authenticated Encryption	IKEv2	🔴

© 2014 Cisco and/or its affiliates. All rights reserved.

ISR IPsec Performance

For Your Reference

	891	1921	1941	2901	2911	2921	2951	3925	3945	3925E	3945E	4451-X
Encryption Throughput* (Max/IMIX)	75 Mbps	51 Mbps	58 Mbps	58 Mbps	64 Mbps	80 Mbps	150 Mbps	212 Mbps	244 Mbps	633 Mbps	800 Mbps	1.3 Gbps
ISM-VPN Encryption Throughput* (Max/IMIX)	NA	NA	170 Mbps	170 Mbps	170 Mbps	215 Mbps	395 Mbps	715 Mbps	715 Mbps	NA	NA	NA
Tunnels (no ISM / with ISM)	50	150	150 / 500	150 / 700	225 / 1000	900 / 1500	1000 / 2000	1500 / 2500	2000 / 3000	1500	2000	4000

* Throughput is unidirectional performance with a single IPSec Tunnel and stateless traffic

© 2014 Cisco and/or its affiliates. All rights reserved.

ASR1000 IPsec DMVPN Performance

For Your Reference

	ASR1001	ASR1000-ESP5	ASR1000-ESP10	ASR1000-ESP20	ASR1000 ESP40	ASR1000-ESP100	ASR1002-X
Supported Chassis	ASR 1001 (RP2)	ASR 1002 (RP1)	ASR 1002, 1004, 1006	ASR 1004 and 1006	ASR1004/6 and 1013	ASR1006, ASR1013	ASR1002-X (RP2)
Encryption Throughput* (Max/IMIX)	1.8/1 Gbps	1.8 Gbps	4/2.5 Gbps	7/6 Gbps	11/7 Gbps	30/16 Gbps	4/4 Gbps
VRFs (RP2/RP1)**	4,000	1,000	4,000/1,000	4,000/1,000	4,000/1,000	4,000/1,000	4,000
Total Tunnels***	4,000	4,000	4,000	4,000	4,000	4,000	4,000
Tunnel Setup Rate With RP2/RP1 (IPsec, per sec) **	130	90	130/90	130/90	130/90	130/90	130
DMVPN/BGP Adjacencies (RP2/RP1)	3,500	1,000	4,000/1,000	4,000/1,000	4,000/1,000	4,000/1,000	4,000
DMVPN/EIGRP Adjacencies (RP2/RP1)	3,500	1,000	4,000/1,000	4,000/1,000	4,000/1,000	4,000/1,000	4,000
DMVPN/OSPF Adjacencies (RP2/RP1)	1,000	750	1,000/750	1,000/750	1,000/750	1,000/750	1,000

* Throughput is unidirectional performance

** RP2 is only supported in ASR1004 , ASR1006, and ASR1013

*** Total tunnels are for IPsec and GRE+IPSec only

Intelligent Path Control

Improving Application Delivery and WAN Efficiency

Getting the Most Out of Your WAN Investment

Benefits of Intelligent Path Control

Lower
WAN Costs

Enabling
Internet-Based WANs

Full Utilisation
of All WAN Bandwidth

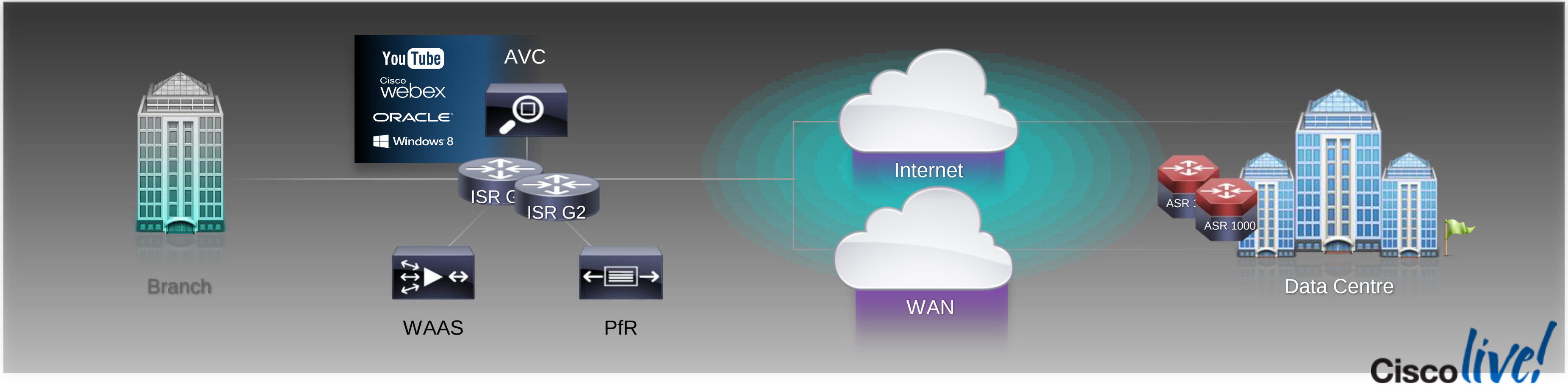
Efficient Distribution of Traffic Based Upon Load, Circuit Cost, and Path Preference

Improved
Application Performance

Per Application Best Path Based on Delay, Loss, Jitter Measurements

Increased
Application Availability

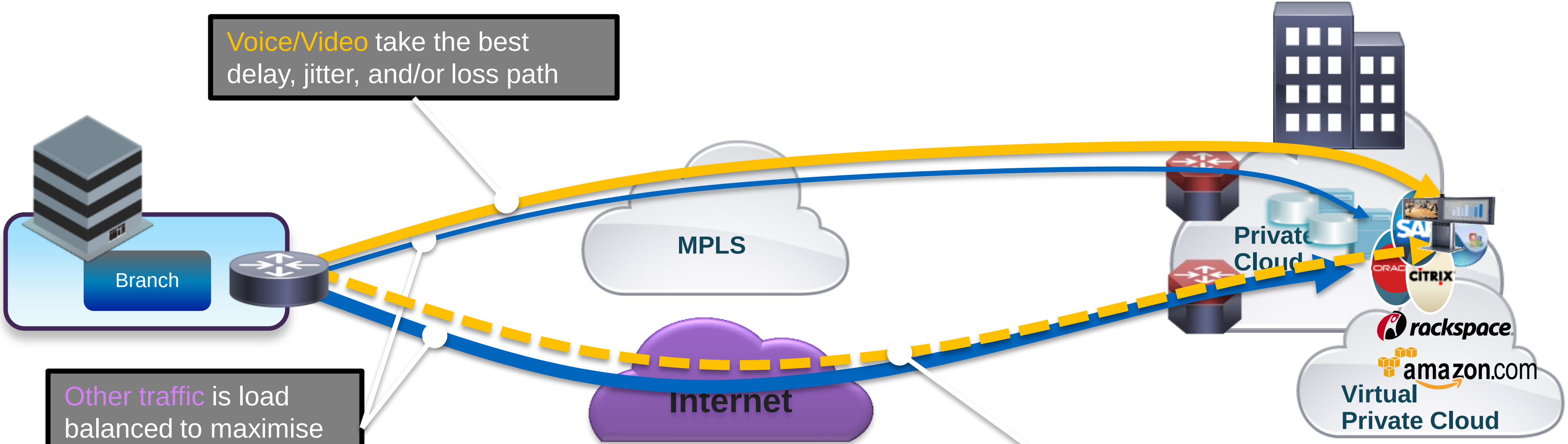
Protection From Carrier Black Holes and Brownouts



© 2014 Cisco and/or its affiliates. All rights reserved.

Intelligent Path Control with PfR

Voice and Video use-case



Voice/Video take the best delay, jitter, and/or loss path

Other traffic is load balanced to maximise bandwidth

Voice/Video will be rerouted if the current path degrades below policy thresholds

- 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

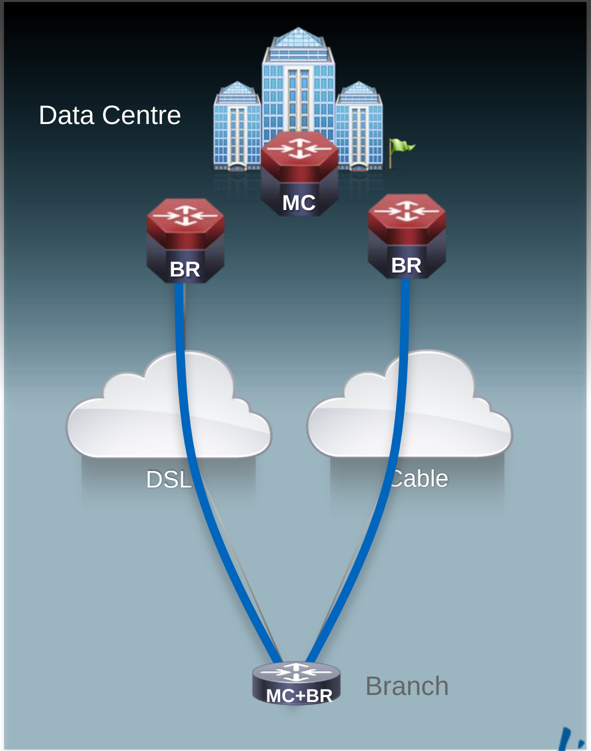
© 2014 Cisco and/or its affiliates. All rights reserved.

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
- Two components: Master controller and border router



© 2014 Cisco and/or its affiliates. All rights reserved.

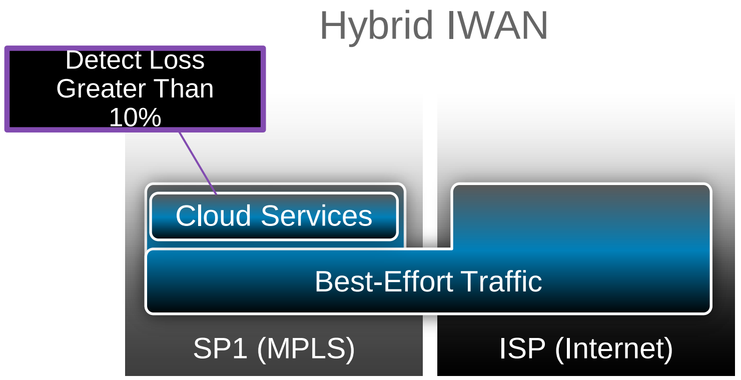
PfR Enhances Classical Routing

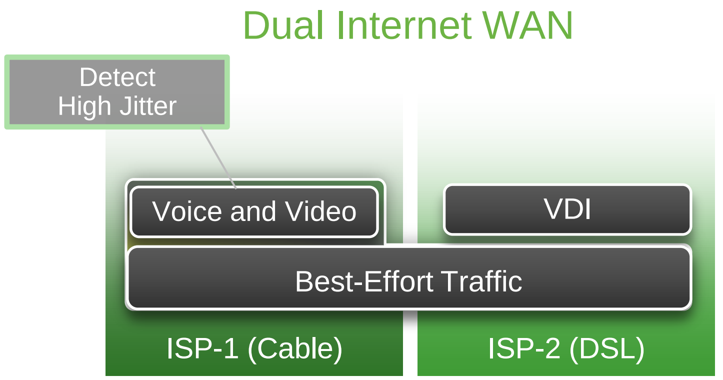
	CLASSICAL	PfR
Path Control	- Topological state - Least cost path - Static user preference	- Application-aware - Policy controlled - Measured performance
Metrics	- Path cost - Interface state	+ - Delay - Jitter - Bandwidth
Adaptive	Responds To: - Link and node state changes (up/down)	Responds To: - Measured performance changes (degradation)

© 2014 Cisco and/or its affiliates. All rights reserved.

What PfR Does

Protecting Critical Applications While Increasing Bandwidth Utilisation





Cloud Services and Load-Balancing Policy

- Protect business cloud applications from brownouts
  - Loss less than 5%
- Preferred path for critical applications: SP1 (MPLS)
- Increase WAN bandwidth efficiency by load-sharing traffic over all WAN paths, MPLS + Internet

Multimedia and Critical Data Policy

- Protect voice and video quality
  - Latency less than 150 ms; Jitter less than 20 ms
- Protect VDI applications from brownouts
  - Loss less than 5%
- Voice and video preferred path SP-A
- VDI preferred path SP-B
- Increase utilisation by load sharing

© 2014 Cisco and/or its affiliates. All rights reserved.

Performance Routing - Components

The Decision Maker: Master Controller (MC)

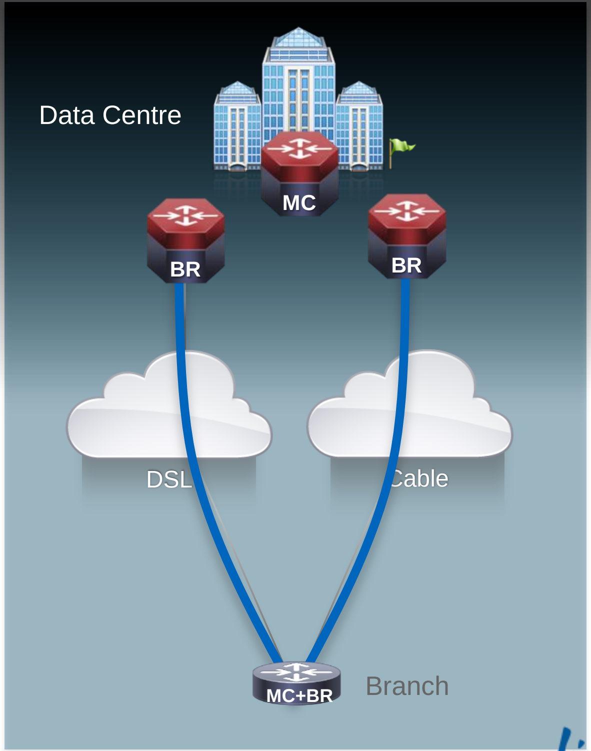
- Discover BRs, collect statistics
- Apply policy, verification, reporting
- No packet forwarding/ inspection required

The Forwarding Path: Border Router (BR)

- Gain network visibility in forwarding path (Learn, measure)
- Enforce MC's decision (path enforcement)
- Does all packet forwarding

Optimise By:

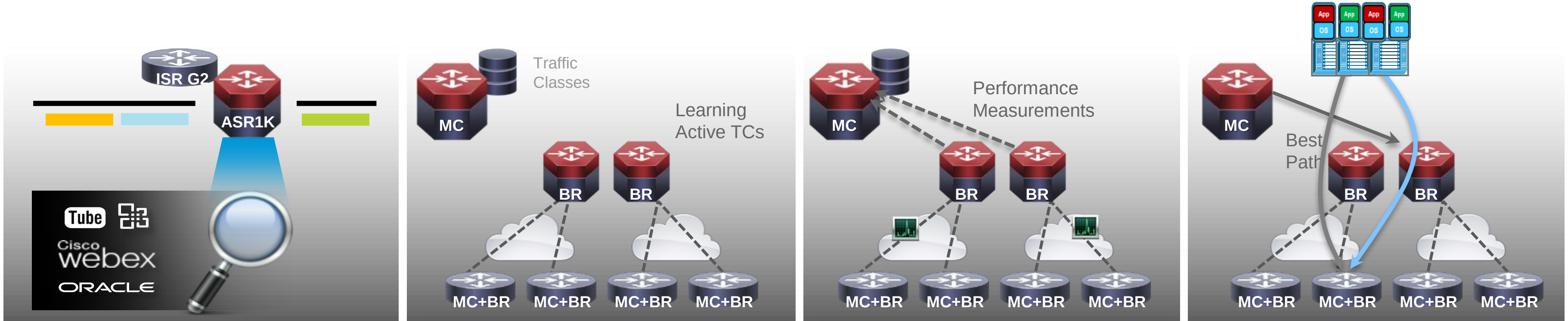
- Reachability, Delay, Loss, Jitter, MOS,
- Throughput, Load, and/or $Cost



© 2014 Cisco and/or its affiliates. All rights reserved.

How PfR Works

Key Operations



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 Border Routers (BRs) based on your policy definitions

Measurement

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

Path Enforcement

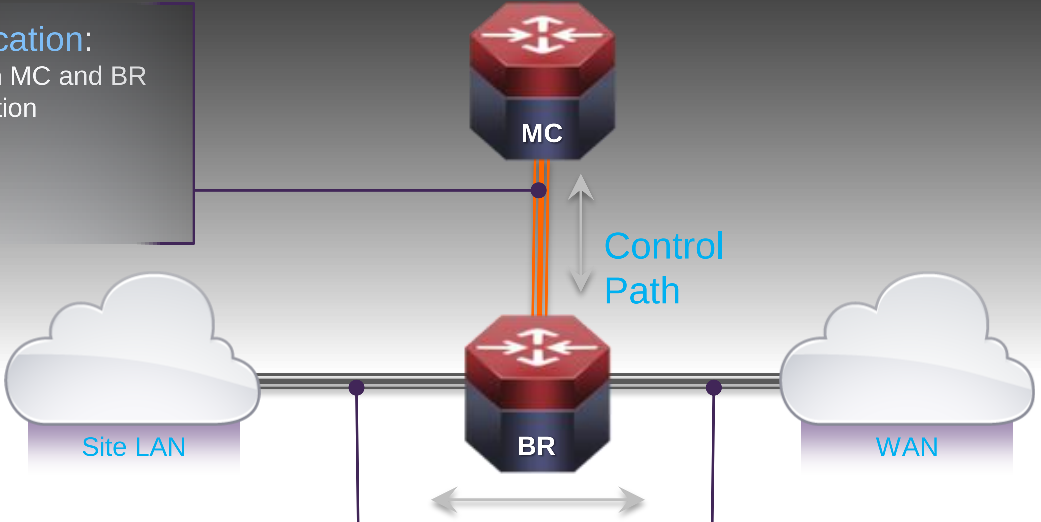
Master Controller commands path changes based on your traffic policy definitions

© 2014 Cisco and/or its affiliates. All rights reserved.

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:

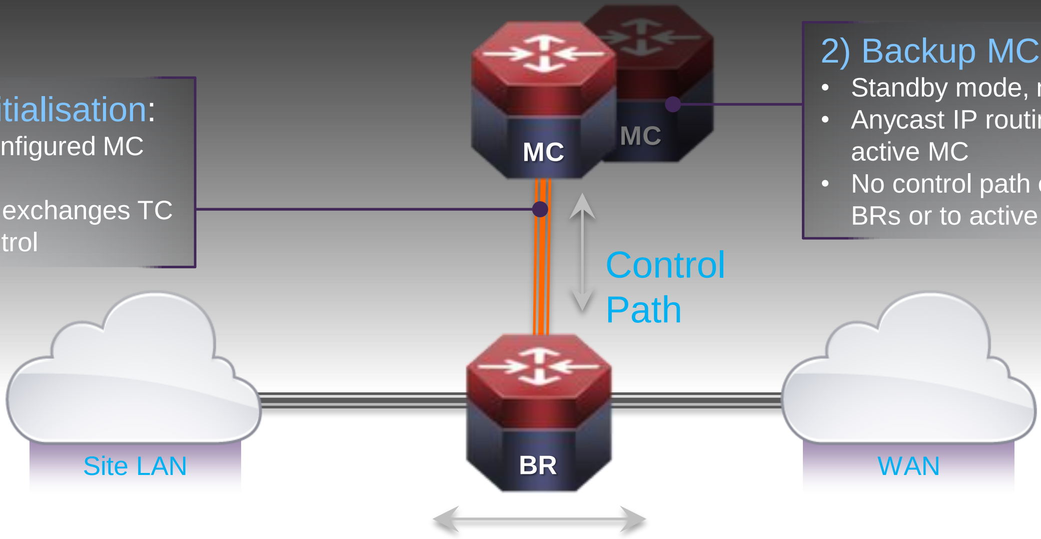
- PfR-managed Exit Links to forward traffic
- Enabled on BR
- Configured on MC (for target discovery)
- Minimum of 2 interfaces per BR

© 2014 Cisco and/or its affiliates. All rights reserved.

PfR Master Controller Redundancy

1) Control Path initialisation:

- BRs peer with the configured MC IP address
- MC-BR Control path exchanges TC metrics and path control



2) Backup MC

- Standby mode, no state sharing
- Anycast IP routing metric determines active MC
- No control path established between BRs or to active MC

3) Control Path Failure

- If the BRs lose connectivity to the MC then all PfR path control is removed
- BRs continue to forward all traffic based on normal IP routing

4) MC failover

- BRs will attempt to reestablish communications with the MC
- Anycast IP routing will direct BR connection requests to the Standby MC
- PfR control takes over again, goto 1)

© 2014 Cisco and/or its affiliates. All rights reserved.

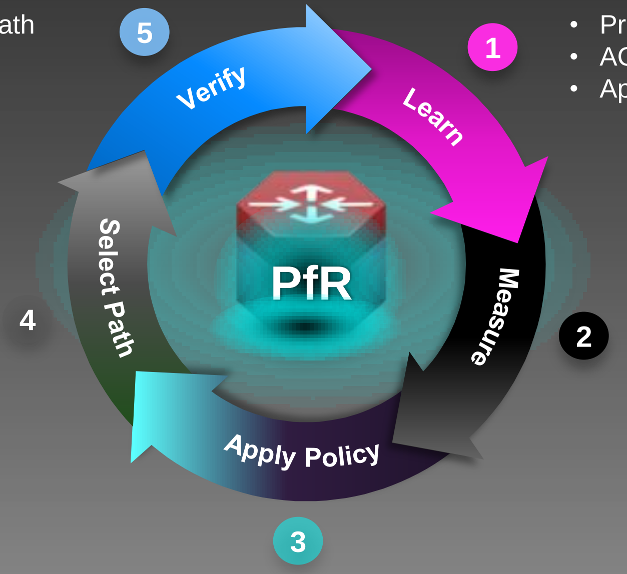
Performance Routing - Control Loop

Verify New Path:

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

Learn Your Traffic Classes:

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



Select Path:

- Send Good path to BRs for each traffic class
- BRs inject best path into FIB
- Gather new path performance info

Measure:

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

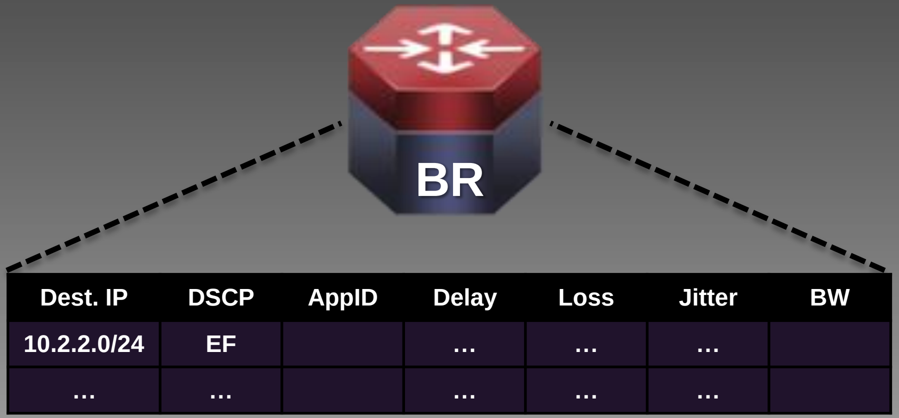
Apply Your Traffic Policy:

- Compute Path Performance
- Compare to defined policy per traffic class
  Passive Mode: BW, Delay (TCP), Loss (TCP)
  Active Mode: Delay, Loss, Jitter, MOS

© 2014 Cisco and/or its affiliates. All rights reserved.

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)

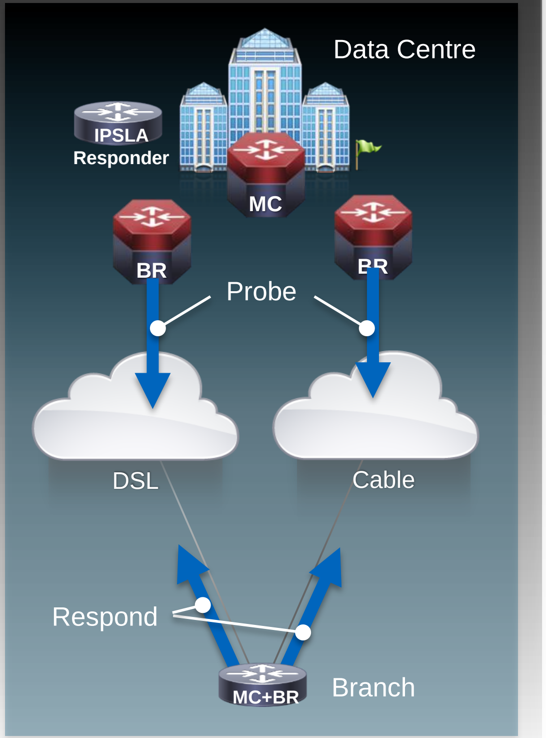


Dest. IP	DSCP	AppID	Delay	Loss	Jitter	BW
10.2.2.0/24	EF		…	…	…	
…	…		…	…	…	

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
  - No knowledge or config experience needed
- MC Performance Database to determine Policy Enforcement actions
- Dedicated IPSLA Responder to offload probing from branch in large deployments



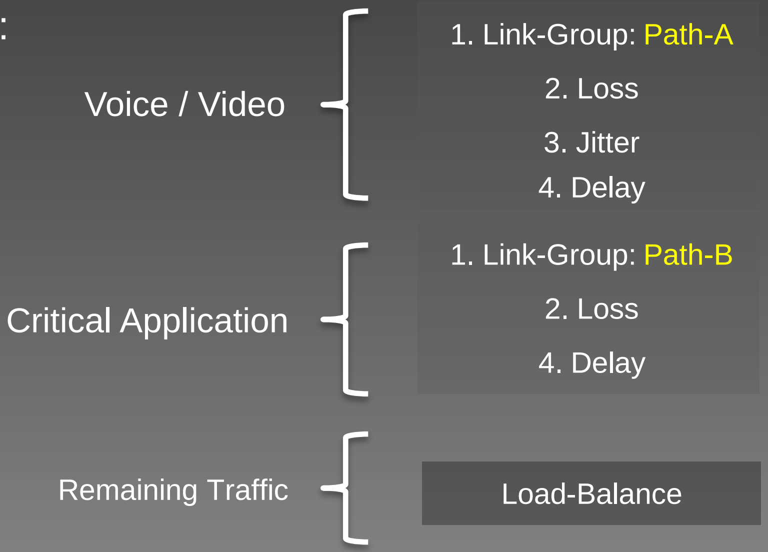
Destination Prefix	DSCP	App Id	Delay	Jitter	Loss	Ingress BW	Egress BW	BR	Exit
10.1.1.1/32	EF		60	10	0	20	40	BR1	Gi1/1
10.1.10.0/24	AF31		110	15	0	52	60	BR1	Gi1/2
…	0		89	26	1	34	10	BR2	Gi1/1

© 2014 Cisco and/or its affiliates. All rights reserved.

Defining Application Performance Policy

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

Example:



Voice / Video

1. Link-Group: Path-A
2. Loss
3. Jitter
4. Delay

Critical Application

1. Link-Group: Path-B
2. Loss
4. Delay

Remaining Traffic

Load-Balance

FLEXIBLE CRITERIA

Application Performance

Reachability
Delay
Loss
MOS
Jitter

Link

Load Balancing
Max Utilisation
Link-Group Path Preference
Bandwidth Costs ($)

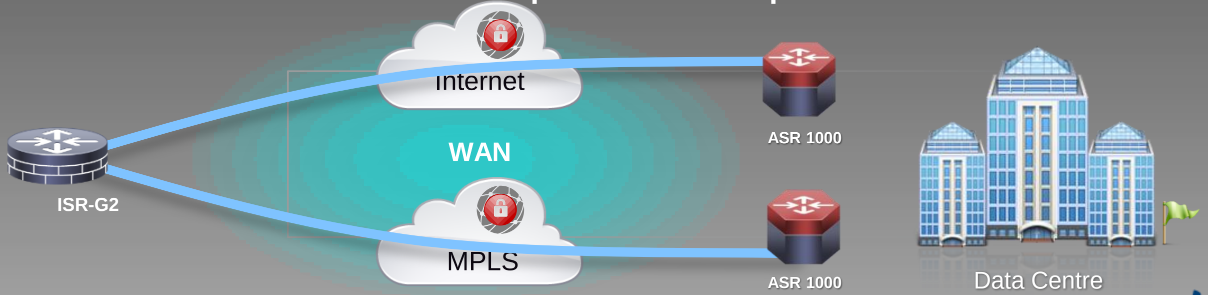
© 2014 Cisco and/or its affiliates. All rights reserved.

Load Balancing

Maximising Link Utilisation to Increase Available Bandwidth

- 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%

50% 15Mbps = 7.5Mbps



50% T1 = 750kbps

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

- BGP
  - Egress: Route injection or BGP Local Preference attribute
  - Ingress: BGP AS-PATH Prepend or AS Community
- EIGRP Route injection
- Static Route injection
- Protocol Independent Route Optimisation (PIRO) with PBR injection

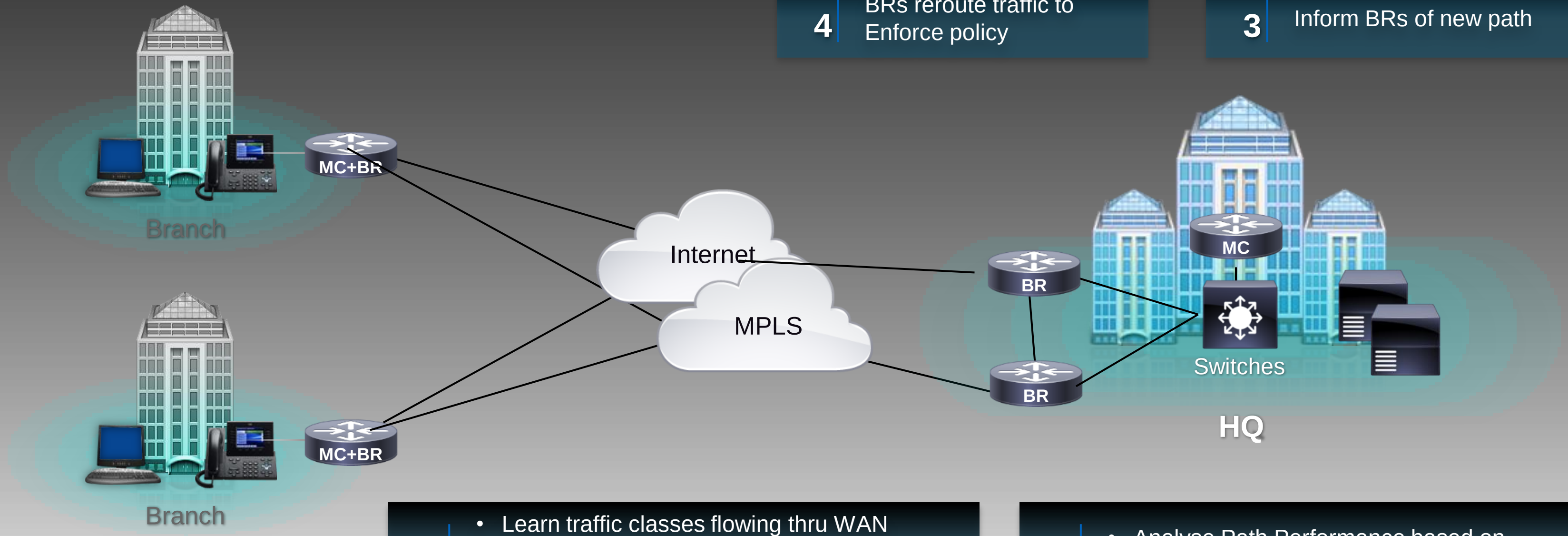
Application

- Dynamic PBR
- NBAR/CCE

© 2014 Cisco and/or its affiliates. All rights reserved.

Intelligent Path Control - Illustration

Putting It Together



1
- Learn traffic classes flowing thru WAN
- Prefix or Application-based learning
- Measure Path Performance: Delay, Jitter, MOS
- Active (IPSLA) or Passive (NF) Measurement
- Report to MC

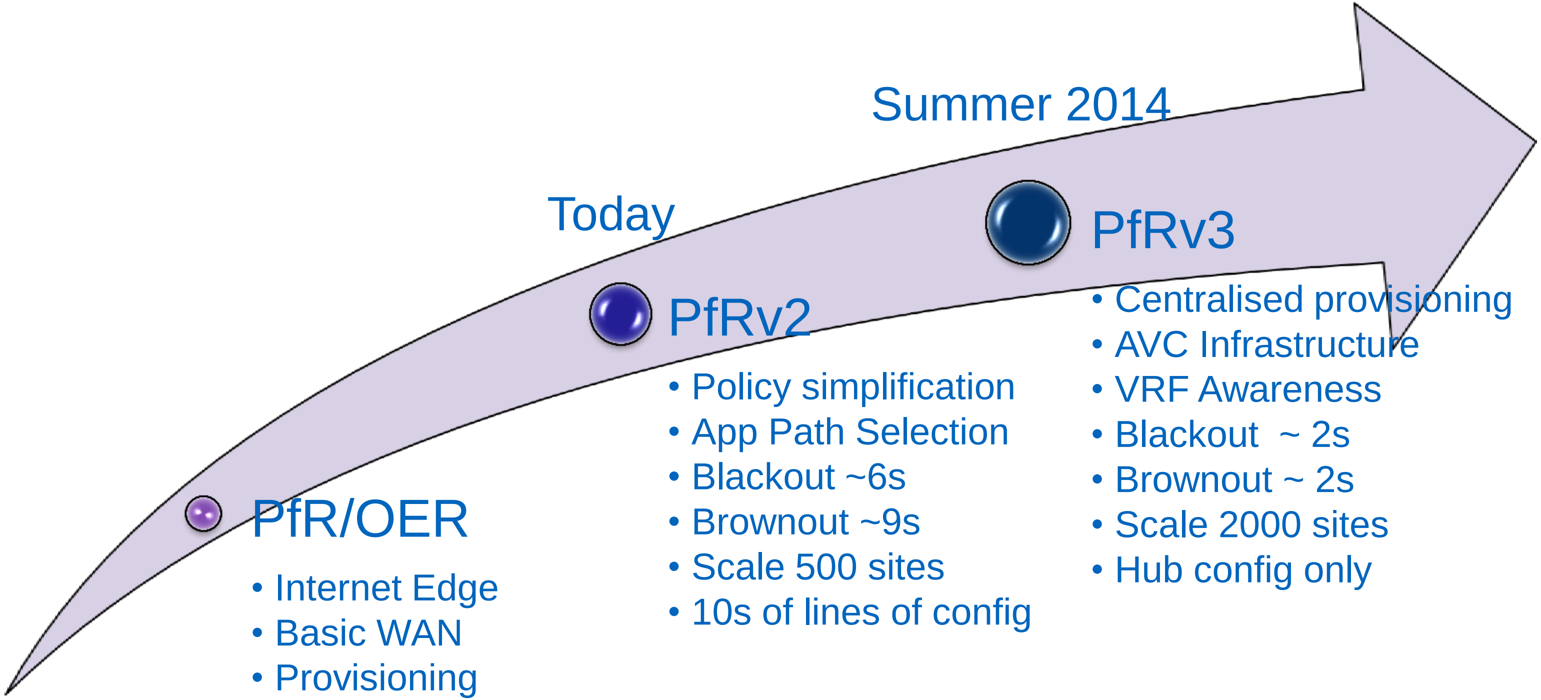
2
- Analyse Path Performance based on BR reports
- Compare to Policy: Path, Delay, Jitter, MOS
- Determine path per-App based to comply with Policy

3 Inform BRs of new path

4 BRs reroute traffic to Enforce policy

© 2014 Cisco and/or its affiliates. All rights reserved.

PfR Evolution – Focusing on Simplification and Scale



PfR/OER

- Internet Edge
- Basic WAN
- Provisioning per site per policy
- 1000s of lines of config

Today

PfRv2

- Policy simplification
- App Path Selection
- Blackout ~6s
- Brownout ~9s
- Scale 500 sites
- 10s of lines of config

Summer 2014

PfRv3

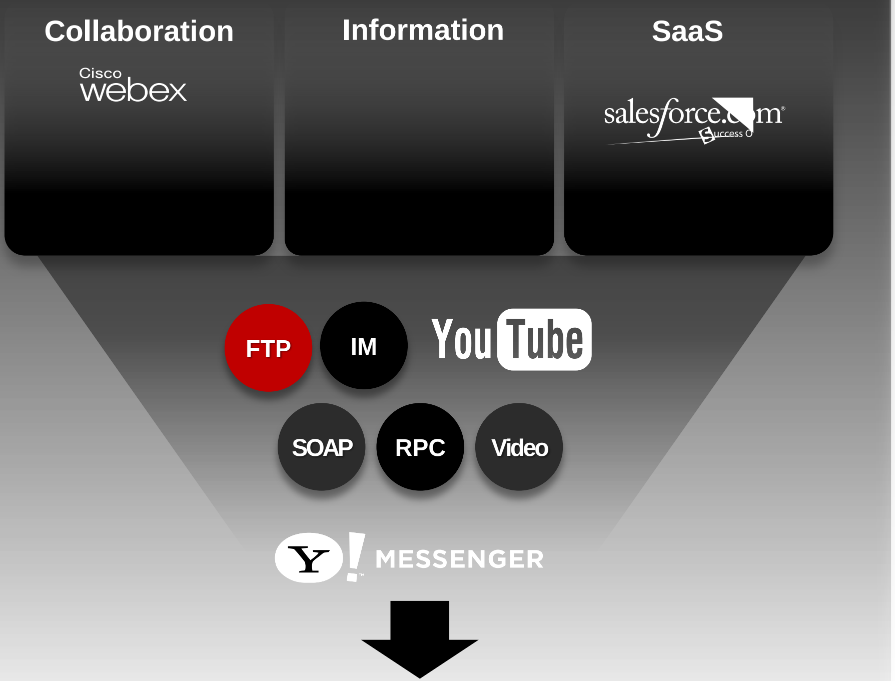
- Centralised provisioning
- AVC Infrastructure
- VRF Awareness
- Blackout ~ 2s
- Brownout ~ 2s
- Scale 2000 sites
- Hub config only

© 2014 Cisco and/or its affiliates. All rights reserved.

Optimise Application Performance

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?

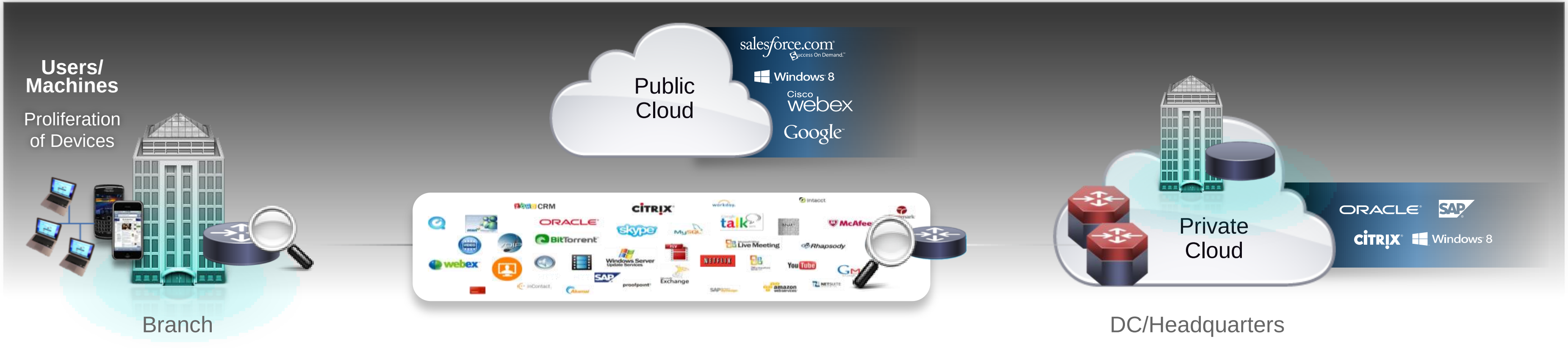


HTTP is the new TCP

© 2014 Cisco and/or its affiliates. All rights reserved.

Make Your Network Application Aware

Cisco Application Visibility and Control



Users/ Machines

Proliferation of Devices

Branch

Public Cloud

Private Cloud

DC/Headquarters

Cisco AVC

No Probes

- Rich data collection using NetFlow v9/IPFIX
- No additional hardware (and included in AX license)
- Easy to integrate into many reporting tools

Smart Capacity Planning

- Better use of costly bandwidth
- Per-branch and per-application level reporting

Business Aligned Privacy Enforcement

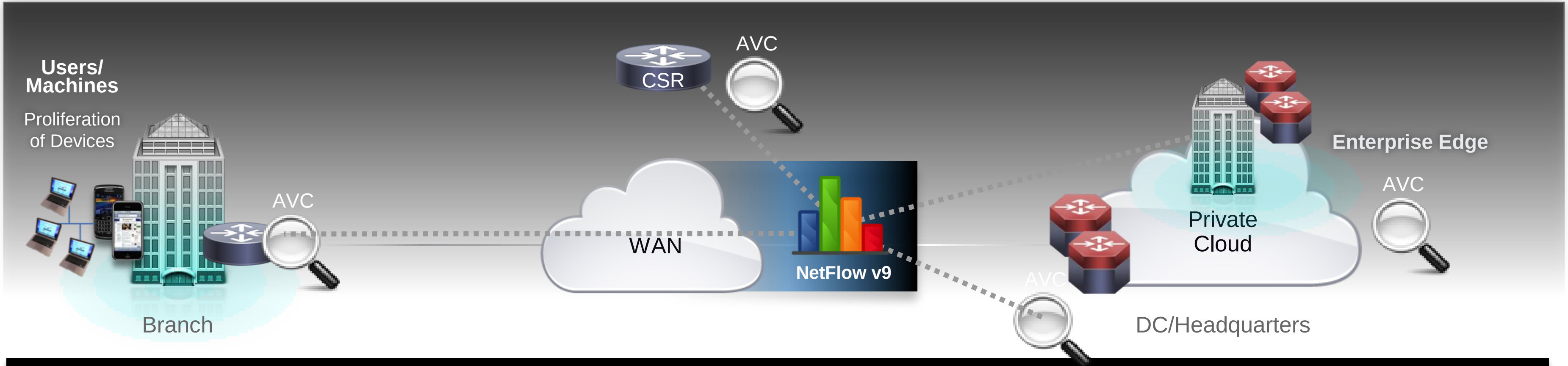
- No need for complex IP and port ACLs
- See inside HTTP flows to identify specific Cloud applications

60% of IT Professionals Cite Performance as Key Challenge for Cloud

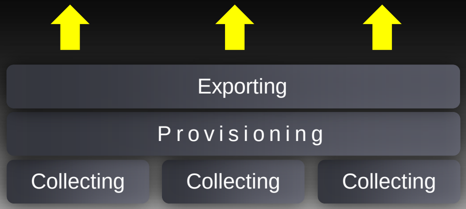
© 2014 Cisco and/or its affiliates. All rights reserved.

Application Performance Monitoring

Track and Report Application Flows and Performance



NetFlow v9 Export/IPFIX Export



NetFlow/IPFIX Records

(Same provisioning, same format)

- Traffic statistics records
- Application Response Time records
- Media monitoring records (Application, Jitter, Loss, etc)

Partner Tools Ecosystem

InfoVista
Plixer
ActionPacked
CompuWare
CA Technologies
Living Objects
Glue

© 2014 Cisco and/or its affiliates. All rights reserved.

Add Application Classification

Group Your Traffic by Application Using NBAR

Advanced Traffic Classification

PROTOCOL

- Protocol
- Category
- Sub-Category
- Application-Group
- HTTP
- RTP
- …

Citrix
Exchange
Oracle
Lync
YouTube
Skype
Kazaa
…

Enterprise App
Browsing
Email
Gaming
IM
Voice and Video
File Sharing
…

URL
Host
MIME
Client Header
Server Header
From
Location
Referer
Server
User-Agent

Mark DSCP for WAN SLA

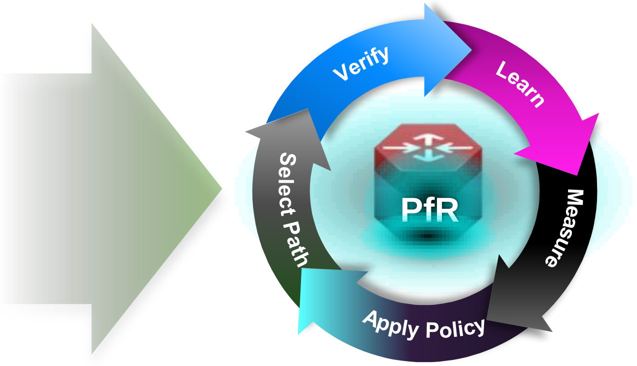
- Police and Shape
- Set DSCP based on Application
- Monitor flows
- …

PfR Path Selection

- Business Critical
- Real Time
- Video
- Best Effort
- …

Apply QoS

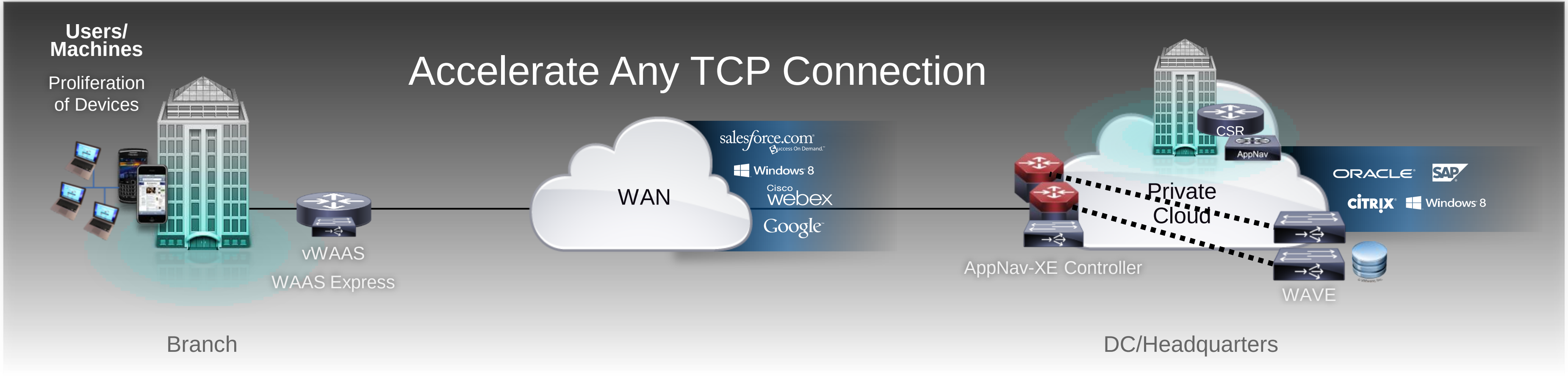
- Bandwidth guarantees
- Packet drop
- Queuing Policy
- Traffic Logging



© 2014 Cisco and/or its affiliates. All rights reserved.

Add WAN Optimisation

Speed and Bandwidth Benefits on top of the WAN



Faster Applications, More Users, Less Bandwidth

- 90% HD Video optimisation and better user experience
- Twice as many Citrix users over same WAN, 70% faster
- Toyota: ROI in less than one year, 65% BW cost savings

Easy to Deploy

- Works with existing branch routers (and existing AX license

Scalable

- AppNav Controller and WAVE pool is scalable
- Native HA capability

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco WAAS

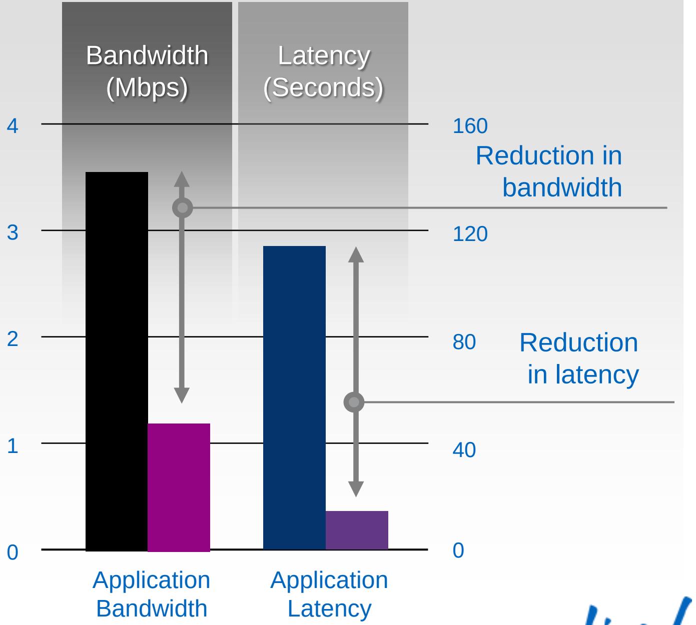
Enhancing User Experience and WAN Efficiency

PROBLEM

- Application latency
- WAN bandwidth inefficiencies

SOLUTION

- Reduce load
  - Data redundancy elimination (DRE), compression, and TCP optimisation
- Application optimisation
  - Fewer protocol messages and metadata caching



© 2014 Cisco and/or its affiliates. All rights reserved.

AKAMAI

© 2014 Cisco and/or its affiliates. All rights reserved.

Securing Your WAN

Securing the WAN

IPSec VPN and Firewall

Step 1: Secure Transport

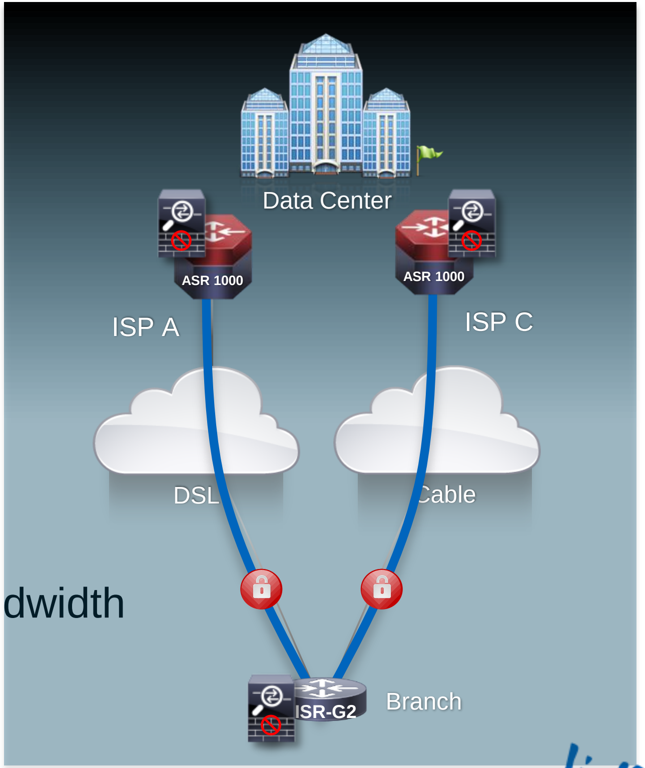
- IPSec with DMVPN overlay
  - Secure transport independent overlay
  - Add Strong Cryptography: IKEv2 + AES-GCM 256

Step 2: Threat Defence

- IOS Zone-based Firewall
- Minimise exposure
  - 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



© 2014 Cisco and/or its affiliates. All rights reserved.

Add Network Integrated Threat Defence

IOS Zone-Based Firewall

Control the Perimeter:

- External and internal protection: internal network is no longer trusted
- Protocol anomaly detection and stateful inspection

Communicate Securely:

- Call flow awareness (SIP, SCCP, H323)
- Prevent DoS attacks

Flexible:

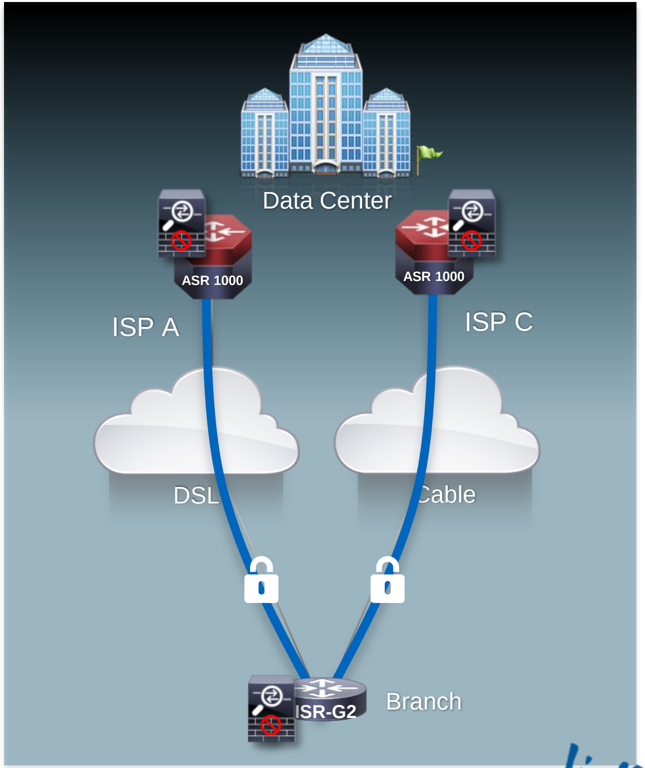
- Split Tunnel-Branch/Remote Office/Store/Clinic
- Internal FW—International or un-trusted locations/segments, addresses regulatory compliances

Integrated:

- No need for additional devices, expenses and power
- Works with other Cisco Services: SRE, Scansafe, WaaS Express

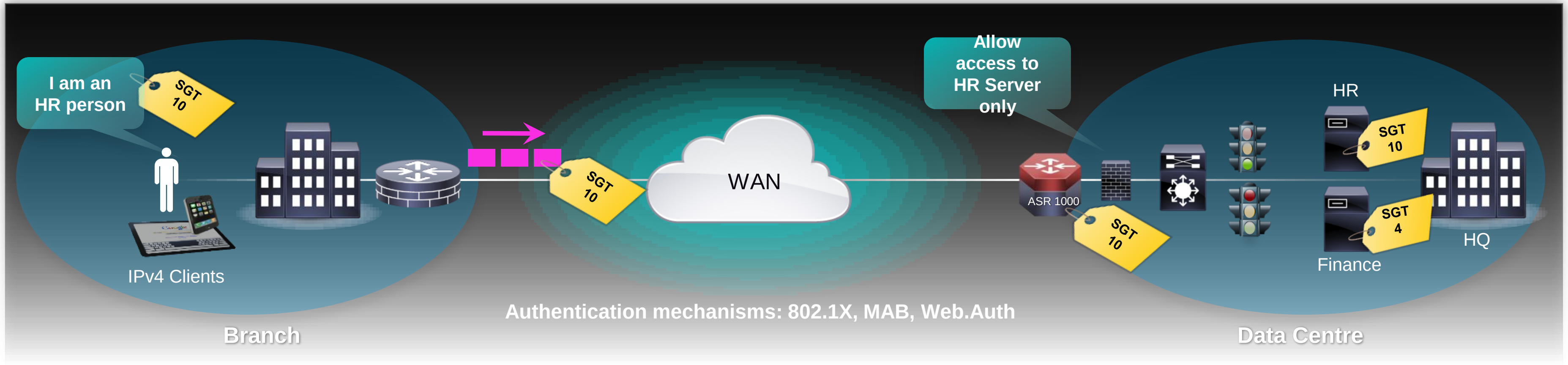
Manageable:

- Supports CLI, SNMP, CCP, and CSM
- Supports Cisco Configuration Engine



© 2014 Cisco and/or its affiliates. All rights reserved.

TrustSec SGT over DMVPN



Authentication mechanisms: 802.1X, MAB, Web.Auth

Problem Statement

- BYOD support for non-IT standard devices
- Enforcing consistent security policy

Solution Overview

- Secure Group Tagging (SGT) for Context-aware Firewall enforcement
- Secure Group Tag transport over DMVPN, FlexVPN, GETVPN

Solution Characteristics

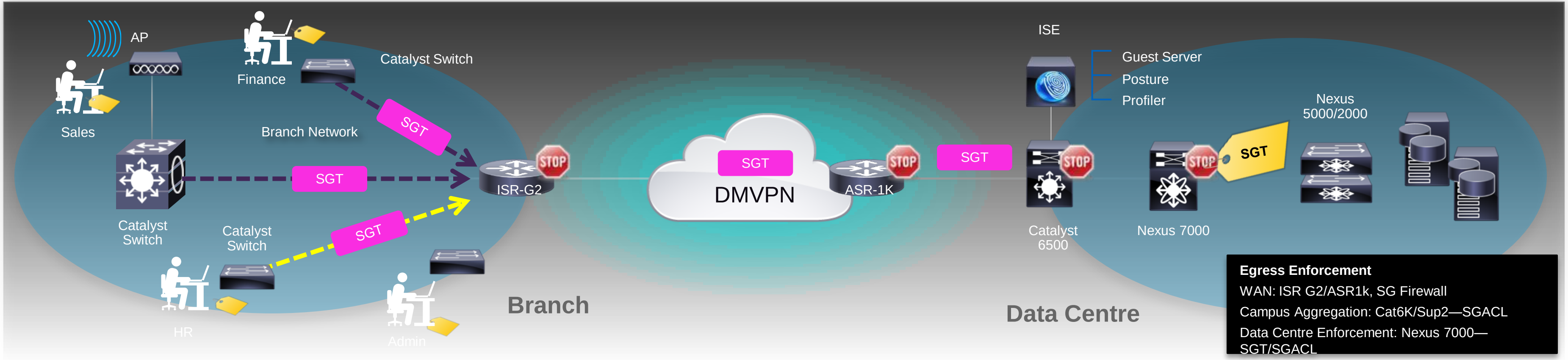
- Secure Identity-based access; keep outsiders out
- Control Access and service levels based on Identity
- Authorised access for users and devices

Scalability

- 100 Gbps FW (ASR1K with ESP100)
- Support up to 6M Sessions at 350K CPS (ASR1K with ESP100)

© 2014 Cisco and/or its affiliates. All rights reserved.

Add Secure Identity and BYOD



Egress Enforcement
WAN: ISR G2/ASR1k, SG Firewall
Campus Aggregation: Cat6K/Sup2—SGACL
Data Centre Enforcement: Nexus 7000—SGT/SGACL

- DMVPN Inline Tagging—ISR G2 (IOS 15.2(2)T), ASR1k (XE 3.11*)
- SG Firewall for Egress Enforcement
- SGT Capability exchange during DMVPN IKEv2 negotiations
- Learn SGT from SXP or Auth-methods
- Simple one command configuration – DMVPN “crypto ikev2 cts sgt”

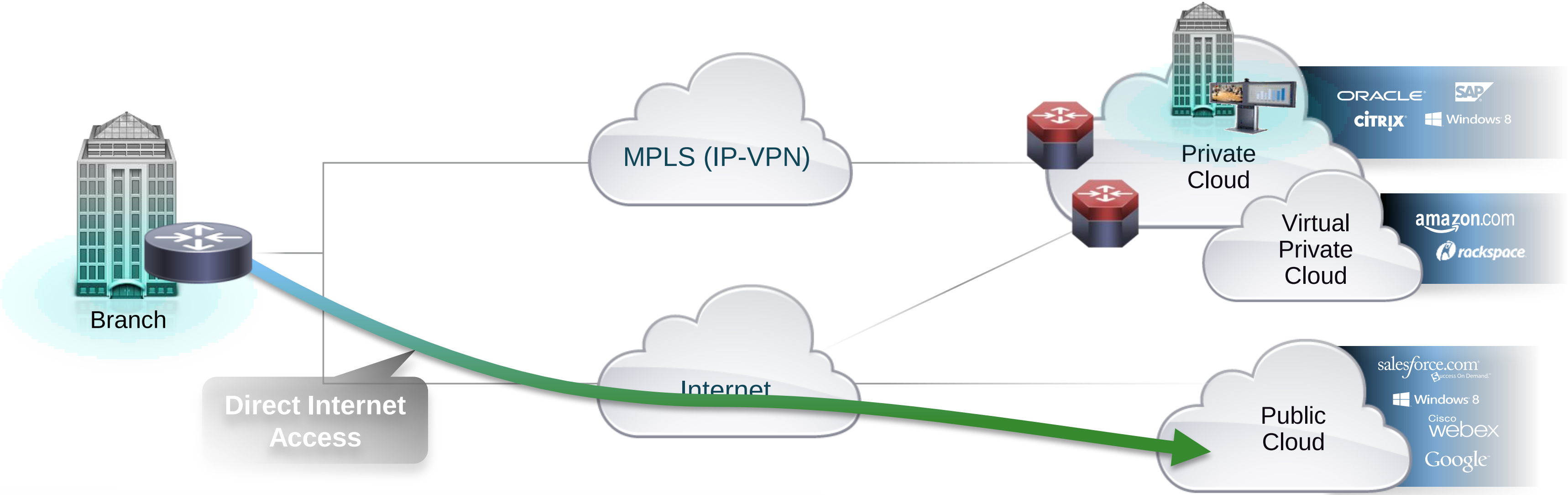
*ASR1k IOS (XE3.11) will be available in Fall 2013.

© 2014 Cisco and/or its affiliates. All rights reserved.

Branch Internet Access

Direct Internet Access

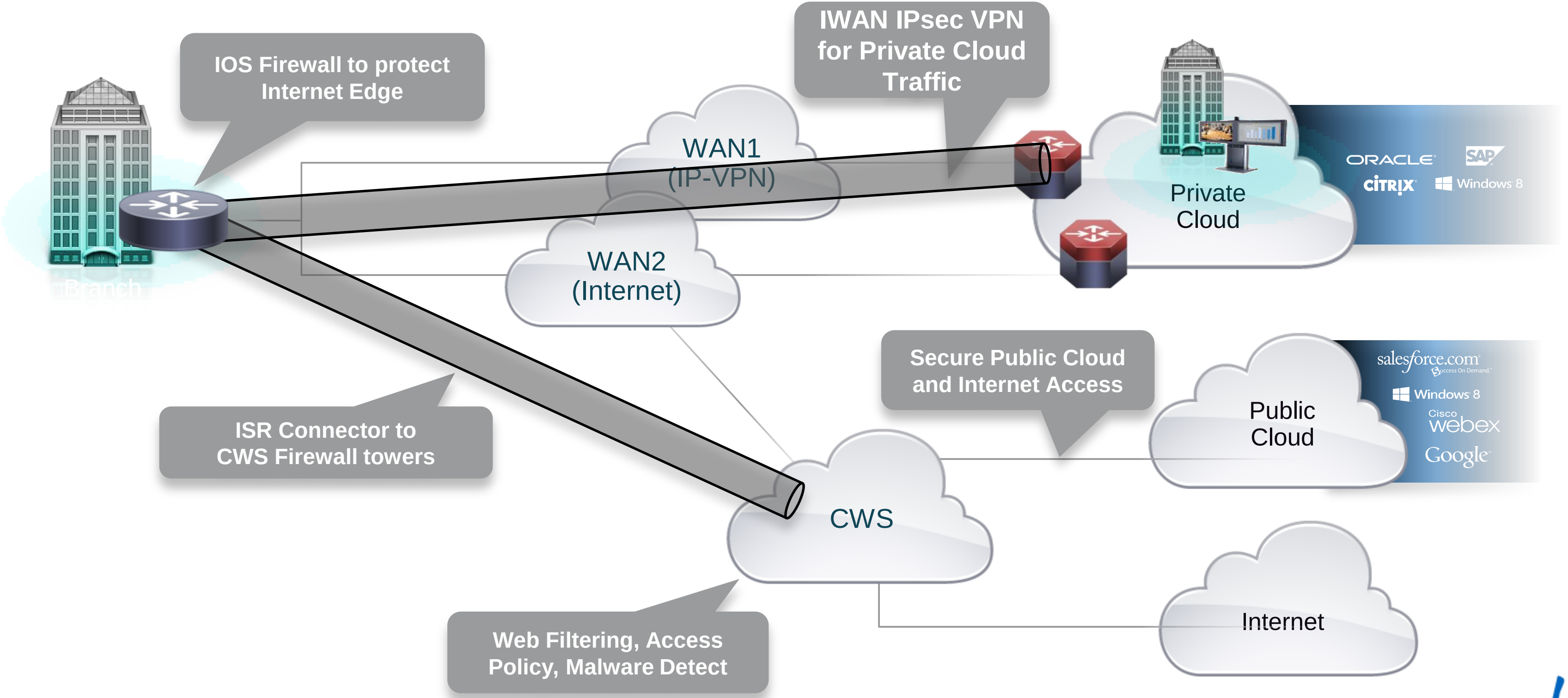
Passing off Internet Traffic at the Branch



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

© 2014 Cisco and/or its affiliates. All rights reserved.

Secure Internet Access with Cisco Cloud Web Security (CWS)



IOS Firewall to protect Internet Edge

IWAN IPsec VPN for Private Cloud Traffic

ISR Connector to CWS Firewall towers

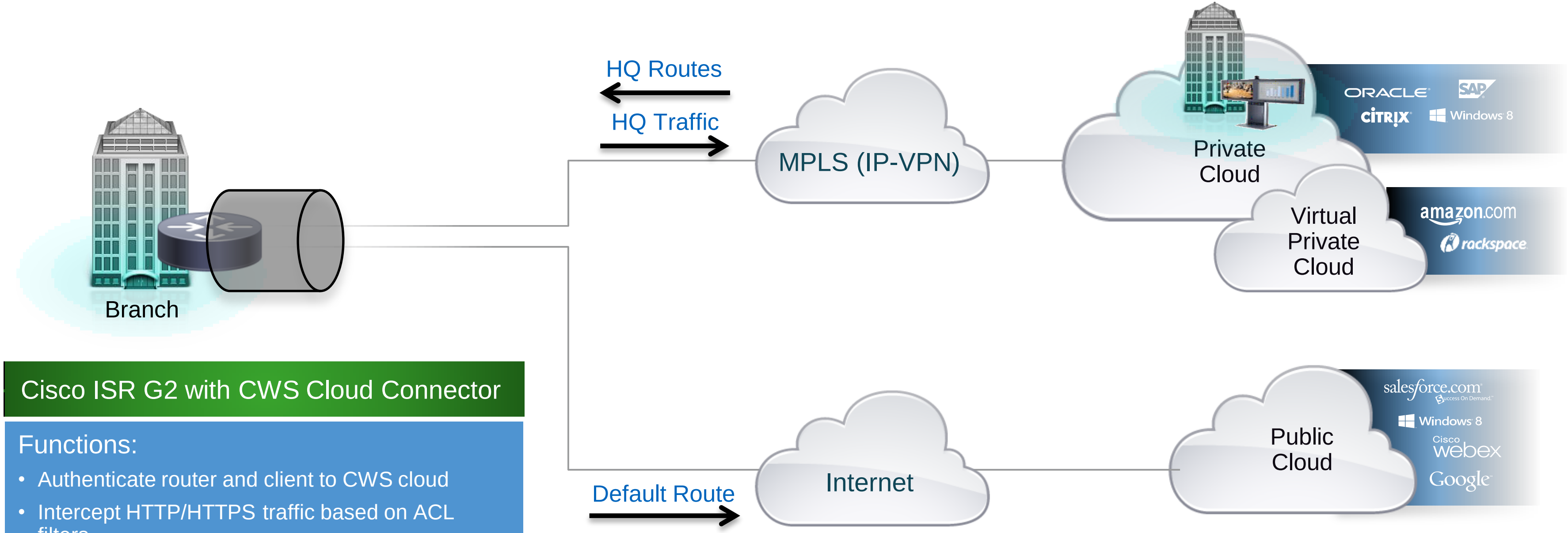
Secure Public Cloud and Internet Access

Web Filtering, Access Policy, Malware Detect

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco ISR CWS Connector

How it Works



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

Functions:

- Act as HTTP proxy to complete requests
- Allow/Block or Warn based on user or group policy
- Scan for Malware

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco Cloud Web Security (CWS) Overview

Administrator

Centralised Policy and Granular Reporting

- Flexible reporting with over 75 attributes
- Deep, drill down visibility
- Overview, trending and forensic data

Office Based User

Roaming User

Mobile Devices

CWS

User Granularity

- Integration with existing network infrastructure (e.g., routers, firewalls)
- Integration with Directory Services
- Numerous deployment options

Policy Control

- Web 2.0 content control
- BI-directional content control
- Dynamic Web Classification
- HTTP/HTTPS scanning
- Searth*Ahead*

Security

- Outbreak intelligence
- Billions of Web requests every day
- Real-time content analysis of all Web content
- Effective zero-day threat protection

Internet

CWS Offers Consistent, Enforceable, High-Performance Web Security and Policy, Regardless of Where or How Users Access the Internet

Simplified Branch Deployments

Remote Site Deployment Challenges

- Limited remote site IT staffing
- Travel costs
- Travel time lost productivity
- Upgrade and change control downtime risks
- Lengthy project schedules

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco Simplified Deployment Solutions

1. Cisco Prime Infrastructure

    Provides Enterprise and Integrator life-cycle network management applications

2. Glue Networks

    Delivers Cloud based simplified deployment portal

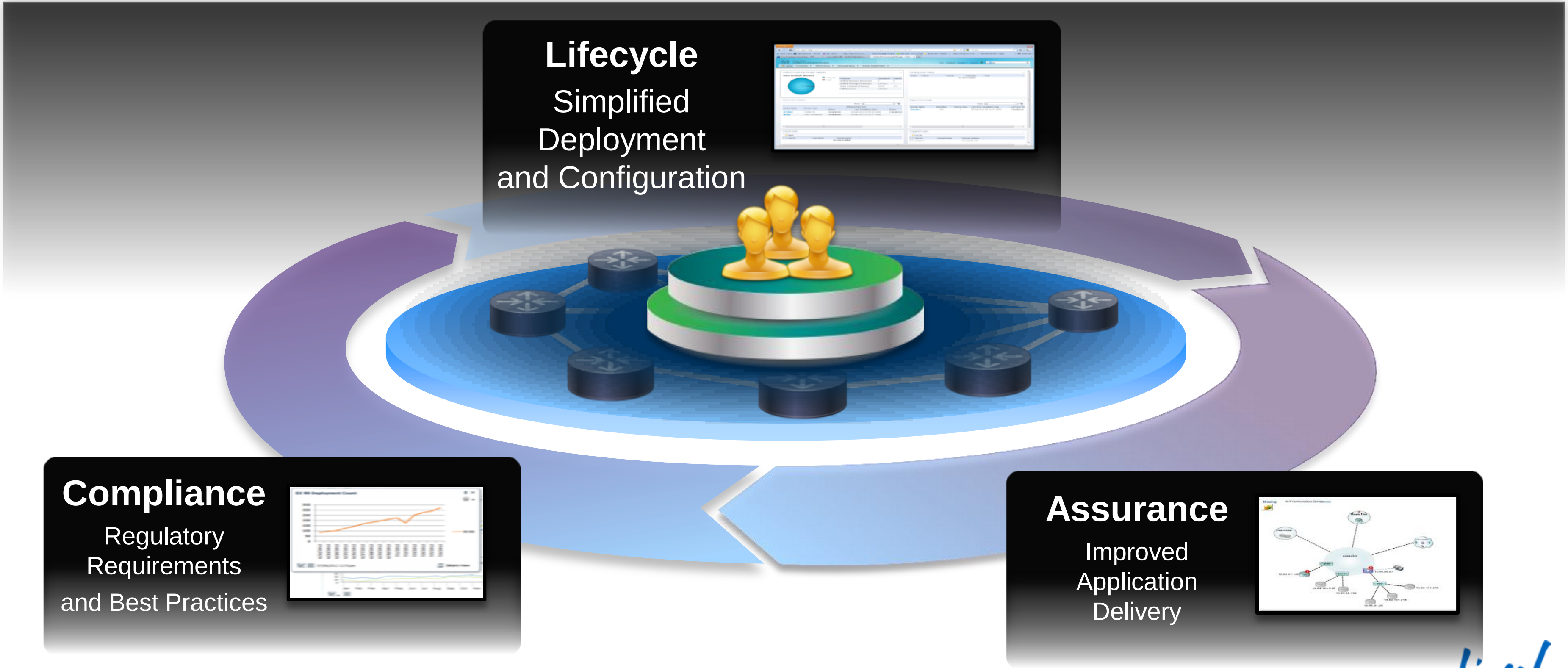
3. SDN ready with OnePK

    Comprehensive programmability kit to enable SDN provisioning applications

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco Prime Infrastructure

Realising the Vision of One Management



Lifecycle

Simplified Deployment and Configuration

Compliance

Regulatory Requirements and Best Practices

Assurance

Improved Application Delivery

© 2014 Cisco and/or its affiliates. All rights reserved.

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

© 2014 Cisco and/or its affiliates. All rights reserved.

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

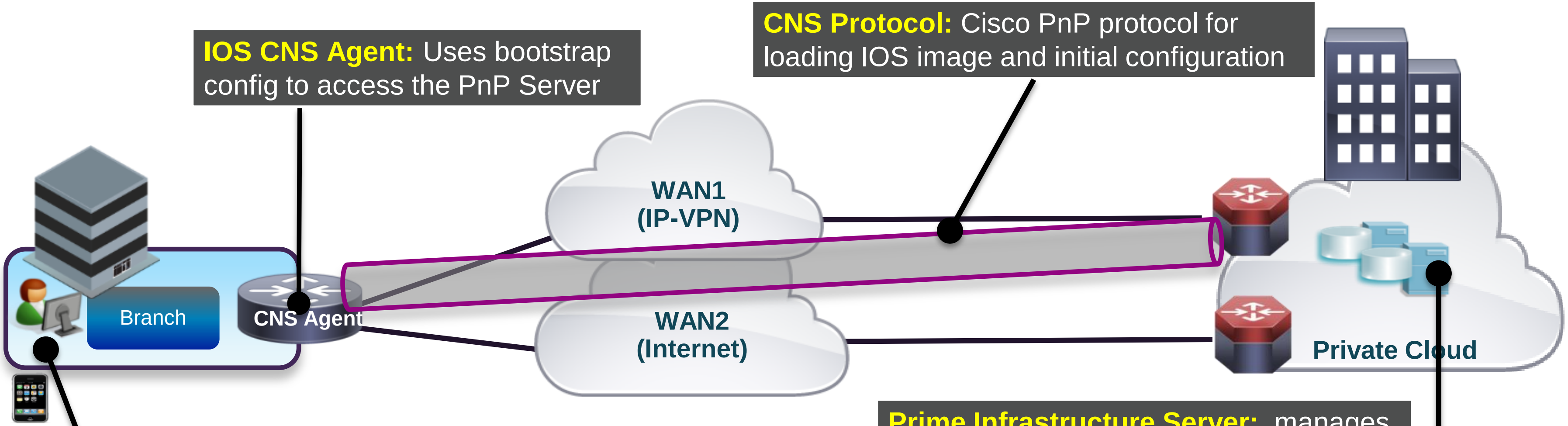
PnP 4

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

© 2014 Cisco and/or its affiliates. All rights reserved.

Plug-n-Play Solution Components



IOS CNS Agent: Uses bootstrap config to access the PnP Server

CNS Protocol: Cisco PnP protocol for loading IOS image and initial configuration

Prime Infrastructure Server: manages and distributes deployment information (images, configurations, and licenses).

PnP Application: **Installer application for iPhone, iPad, and Windows PC used for authenticating and booting the IOS device.**

© 2014 Cisco and/or its affiliates. All rights reserved.

PnP 3

Plug-n-Play Application Workflow Overview

1 Pre-Provisioning In Prime Infrastructure

- Administrator creates a Plug and Play device profile in Prime Infrastructure
- Administrator specifies device names, desired configuration, SW image, and optionally the device serial numbers.
- A deployment PIN number is generated for each device and can be emailed to the installer

2 Installation at the End Location

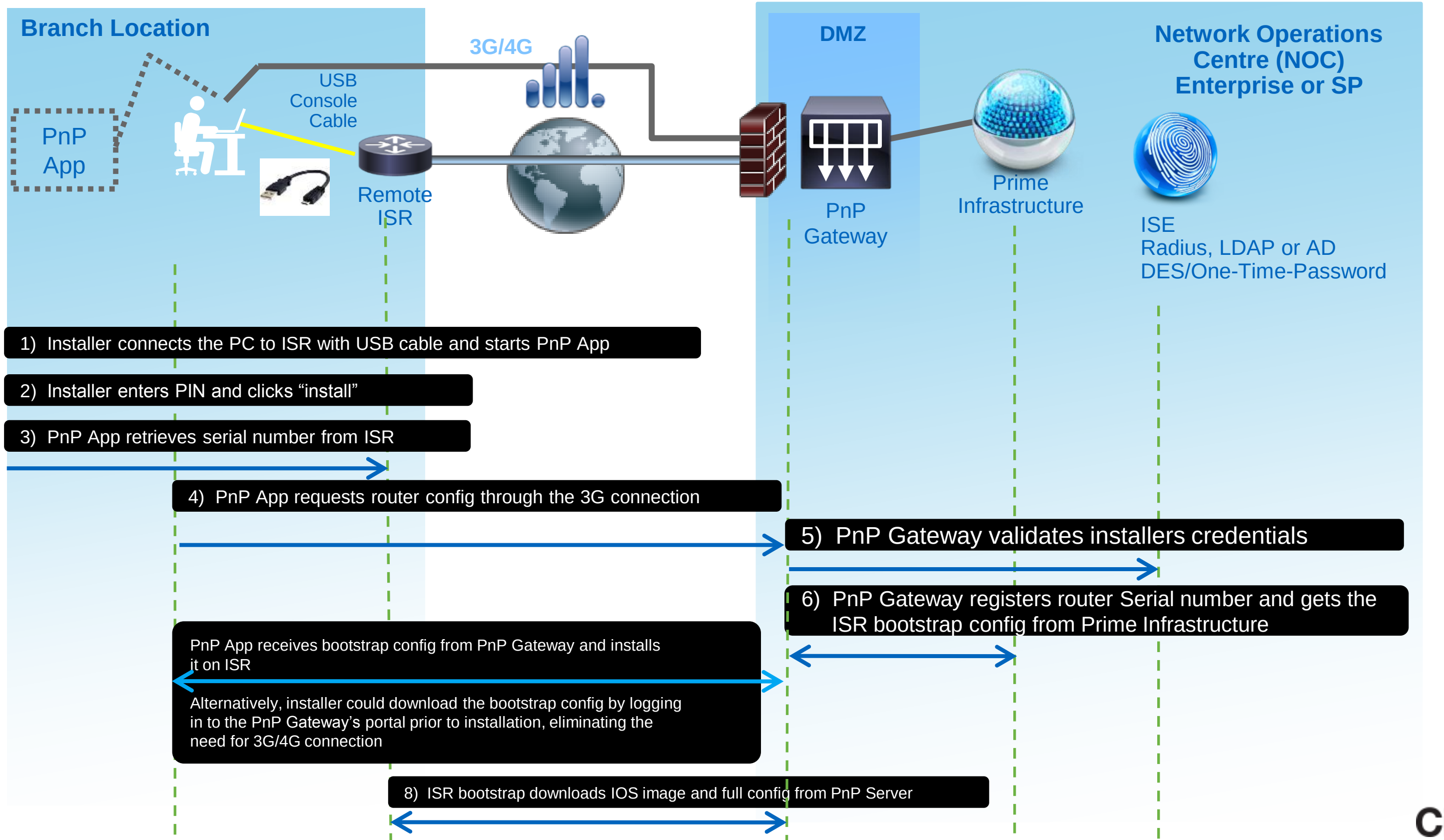
- Installer receives the device, mounts the device and connects the cables.
- Installer launches Plug-and-Play application and enters the PIN
- Plug-and-Play application registers the device serial number with Prime and then downloads bootstrap configuration to the device
- Device downloads the SW image and full configuration from Prime, Plug-and-Play application displays status

© 2014 Cisco and/or its affiliates. All rights reserved.

Prime Plug-n-Play Application

Simplified Branch Router Deployment

PnP 3



1) Installer connects the PC to ISR with USB cable and starts PnP App

2) Installer enters PIN and clicks “install”

3) PnP App retrieves serial number from ISR

4) PnP App requests router config through the 3G connection

5) PnP Gateway validates installers credentials

6) PnP Gateway registers router Serial number and gets the ISR bootstrap config from Prime Infrastructure

PnP App receives bootstrap config from PnP Gateway and installs it on ISR

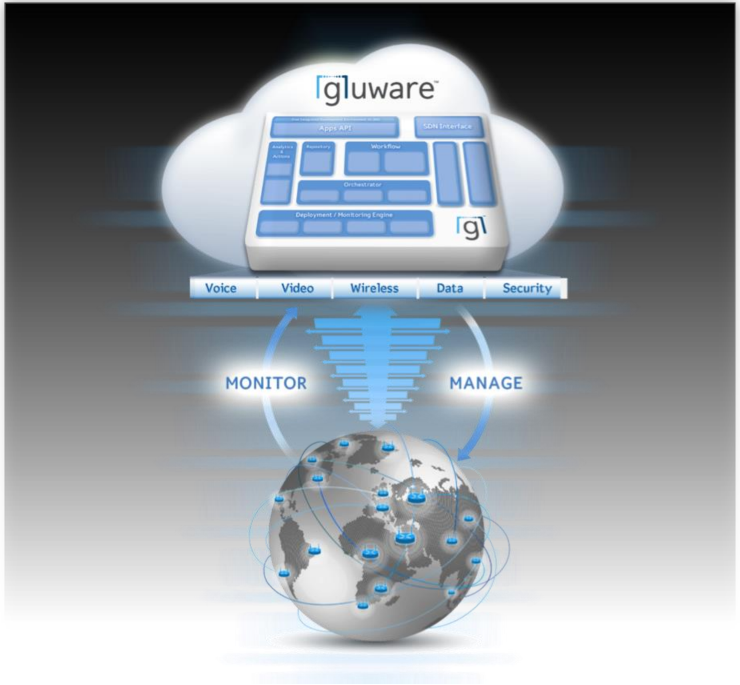
Alternatively, installer could download the bootstrap config by logging in to the PnP Gateway’s portal prior to installation, eliminating the need for 3G/4G connection

8) ISR bootstrap downloads IOS image and full config from PnP Server

© 2014 Cisco and/or its affiliates. All rights reserved.

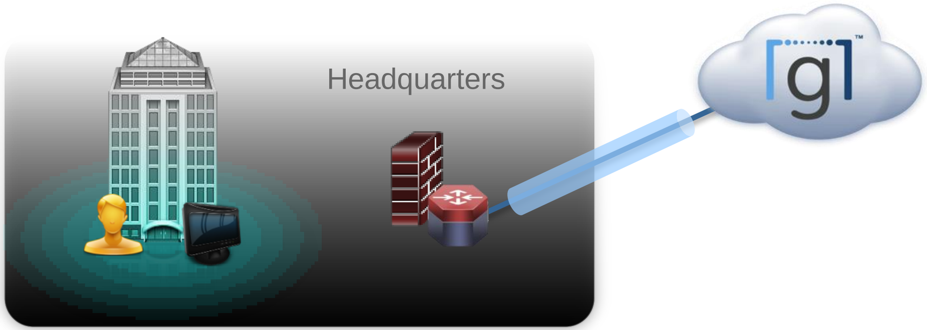
Glue Networks Orchestration

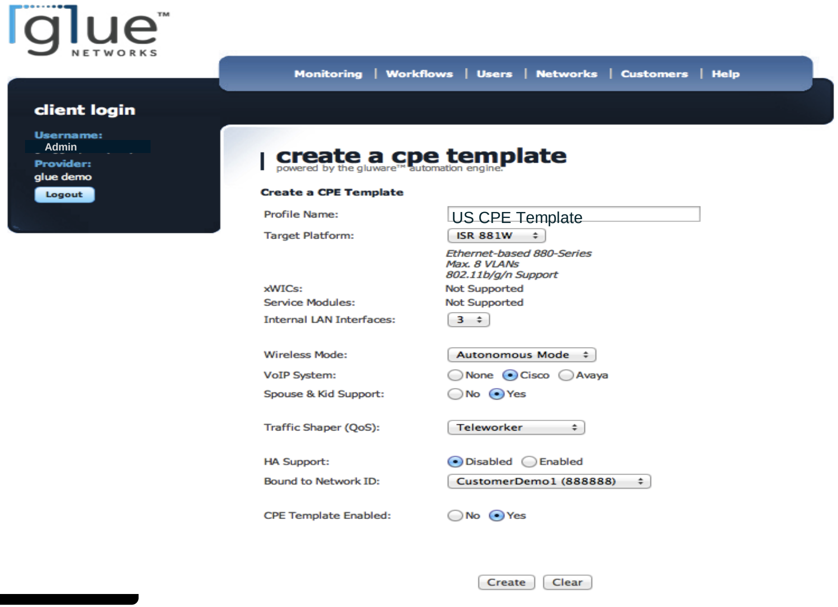
- Cloud-based SaaS subscription model
- Eliminates manual building of WANs
- Automated WAN orchestration and management
- Quick configuration updates and IOS upgrades
- Rapidly delivers nextgen and IWAN features
- Forward compatible with SDN and OnePK for app aware WANs
- Broadband and MPLS support for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



Launched in Q4CY13

Glue Networks Headend Provisioning




glue™
NETWORKS
Monitoring | Workflows | Users | Networks | Customers | Help
Logout
Create
Clear

client login

Username: Admin

Provider: glue demo

create a cpe template
powered by the gluware™ automation engine

Create a CPE Template

Profile Name: US CPE Template

Target Platform: ISR 881W
Ethernet-based 880-Series
Max. 8 VLANs
802.11b/g/n Support

xWICs: Not Supported

Service Modules: Not Supported

Internal LAN Interfaces: 3

Wireless Mode: Autonomous Mode

VoIP System: ○ None ● Cisco ○ Avaya

Spouse & Kid Support: ○ No ● Yes

Traffic Shaper (QoS): Teleworker

HA Support: ● Disabled ○ Enabled

Bound to Network ID: CustomerDemo1 (888888)

CPE Template Enabled: ○ No ● Yes

1) IT Admin connects to Gluware web management portal

2) Via Gluware portal, Admin configures template definitions for IWAN features; Network, HA, Security, QoS, PfR, etc.

3) From the profiles/policies an IWAN Network profile is created.

4) Gluware engine creates configurations for targeted Headends (ISRs/ASRs

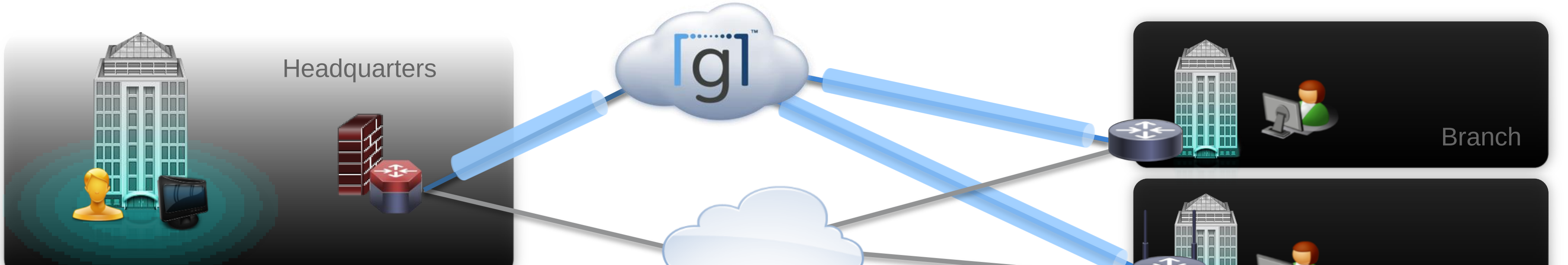
5) Admin securely connects Head End router to Gluware, initiating provisioning process

6) Head End provisioning is completed and validated automatically with Gluware

7) IT Admin creates CPE templates for Branch and Teleworker routers via Gluware portal

© 2014 Cisco and/or its affiliates. All rights reserved.

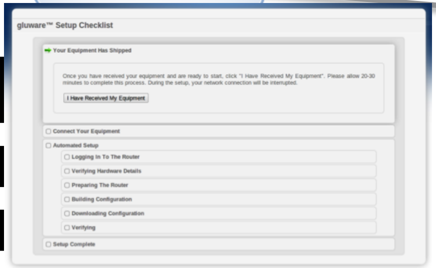
Glue Networks Branch Provisioning and Orchestration



1) End user receives gear and either (a) connects PC/laptop behind router OR (b) inserts USB key into router

1a) User clicks on link in eMail to provision via FirstConnect

1b) User inserts USB key to provision via USBConnect



gluware™ Setup Checklist

➡ Your Equipment Has Shipped

Once you have received your equipment and are ready to start, click "I Have Received My Equipment". Please allow 20-30 minutes to complete this process. During the setup, your network connection will be interrupted.

- □ Connect Your Equipment
- □ Automated Setup
  - □ Logging In To The Router
  - □ Verifying Hardware Details
  - □ Preparing The Router
  - □ Building Configuration
  - □ Downloading Configuration
  - □ Verifying
- □ Setup Complete

2) Either connect mode allows router to “call home to Glue” to begin provisioning

3) Gluware validates SN, creates secure SSH tunnel, and downloads bootstrap configuration

4) Router reboots and bootstrap performs validation of IOS, licenses, etc.

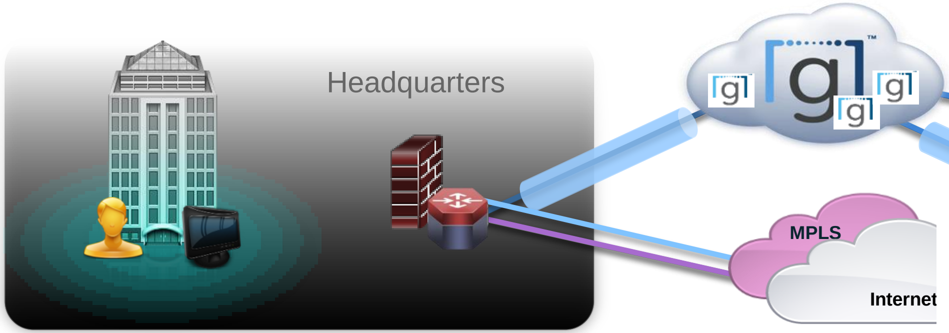
5) Gluware provisions router line-by-line with full validation, error checking, and self healing

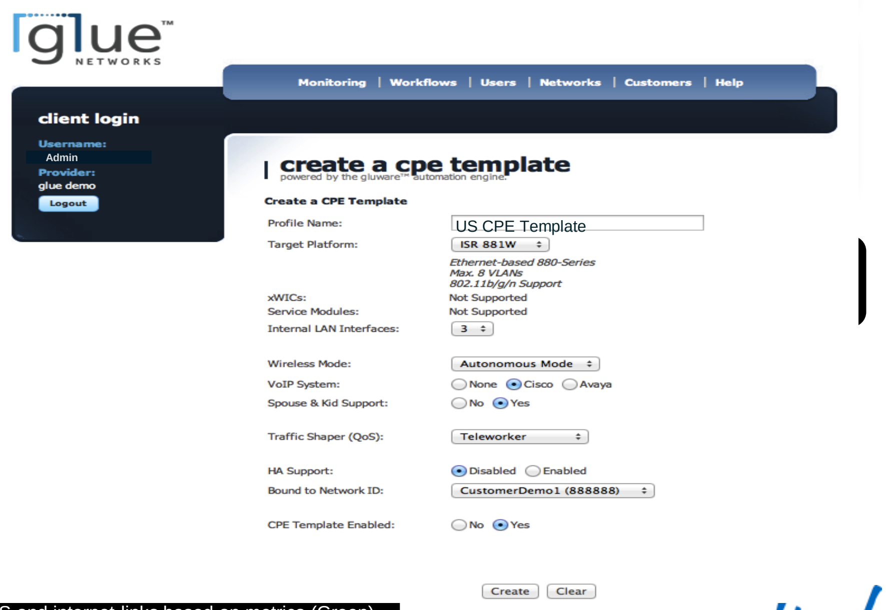
6) Gluware completes provisioning and routers begin participating in customer network immediately.

7) Once routers are provisioned, they move into Lifecycle Management with on-going monitoring (5 minute intervals). Configuration changes and IOS upgrades are handling with the Gluware engine.

© 2014 Cisco and/or its affiliates. All rights reserved.

Glue Networks Orchestration




glue NETWORKS
Monitoring | Workflows | Users | Networks | Customers | Help
Logout
Create
Clear

client login

Username: Admin

Provider: glue demo

create a cpe template

powered by the gluware™ automation engine.

Create a CPE Template

Profile Name:	US CPE Template
Target Platform:	ISR 881W *Ethernet-based 880-Series* *Max. 8 VLANs* *802.11b/g/n Support*
xWICs:	Not Supported
Service Modules:	Not Supported
Internal LAN Interfaces:	3
Wireless Mode:	Autonomous Mode
VoIP System:	○ None ● Cisco ○ Avaya
Spouse & Kid Support:	○ No ● Yes
Traffic Shaper (QoS):	Teleworker
HA Support:	● Disabled ○ Enabled
Bound to Network ID:	CustomerDemo1 (888888)
CPE Template Enabled:	○ No ● Yes

1) IT Admin logs into Gluware web admin portal

2) IT Admin updates network profile via template changes

3) IT Admin schedules date/time for changes to be delivered to routers from Gluware

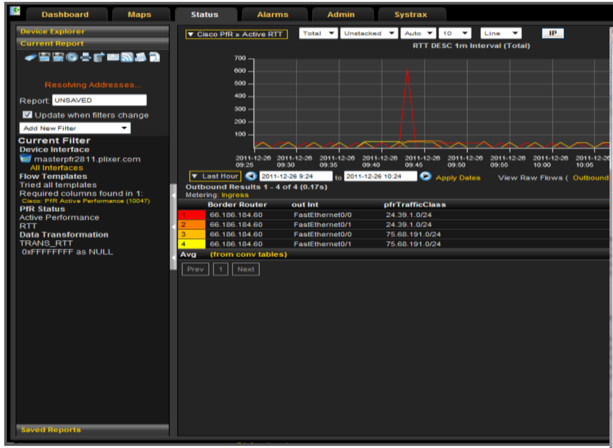
4) At targeted time, Gluware initiates delivery of configuration changes to ro

5) Once configuration update is complete, the changes to the r

6) Gluware applies prioritisation of traffic across MPLS and internet links based on metrics (Green)

© 2014 Cisco and/or its affiliates. All rights reserved.

NMS Reporting Partners



▼ Cisco PfR » Active RTT

Report: UNSAVED

☑ Update when filters change

Add New Filter

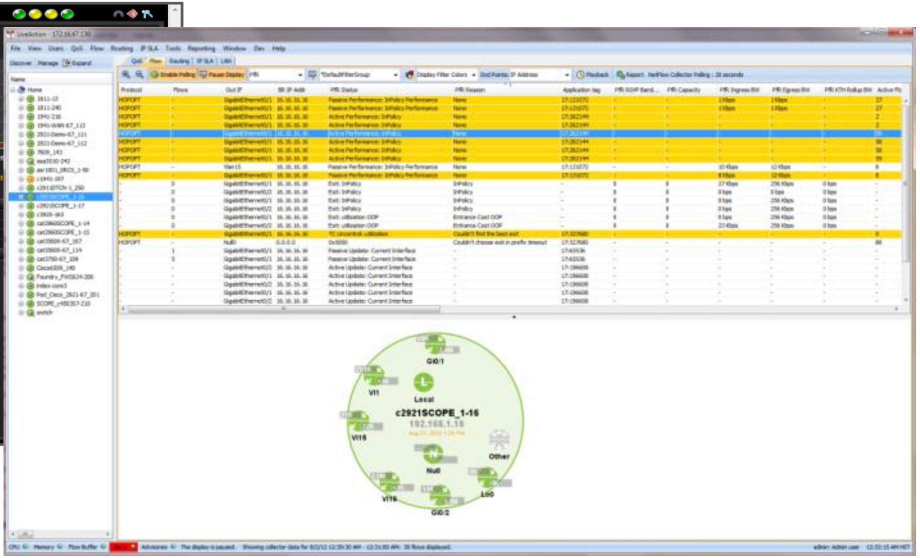
Current Filter
Device Interface
masterpfr2811.plixer.com
All Interfaces
Flow Templates
Tried all templates
Required columns found in 1:
Cisco: PfR Active Performance (10047)
PfR Status
Active Performance
RTT
Data Transformation
TRANS_RTT
0xFFFFFFFF as NULL

▼ Last Hour 2011-12-26 9:24 to 2011-12-26 10:24 Apply Dates View Raw Flows (Outbound

Outbound Results 1 - 4 of 4 (0.17s)
Metering: Ingress

	Border Router	out Int	pfrTrafficClass
1	66.186.184.60	FastEthernet0/0	24.39.1.0/24
2	66.186.184.60	FastEthernet0/1	24.39.1.0/24
3	66.186.184.60	FastEthernet0/0	75.68.191.0/24
4	66.186.184.60	FastEthernet0/1	75.68.191.0/24
Avg	(from conv tables)		

Scrutinizer™
NetFlow & sFlow Analyzer



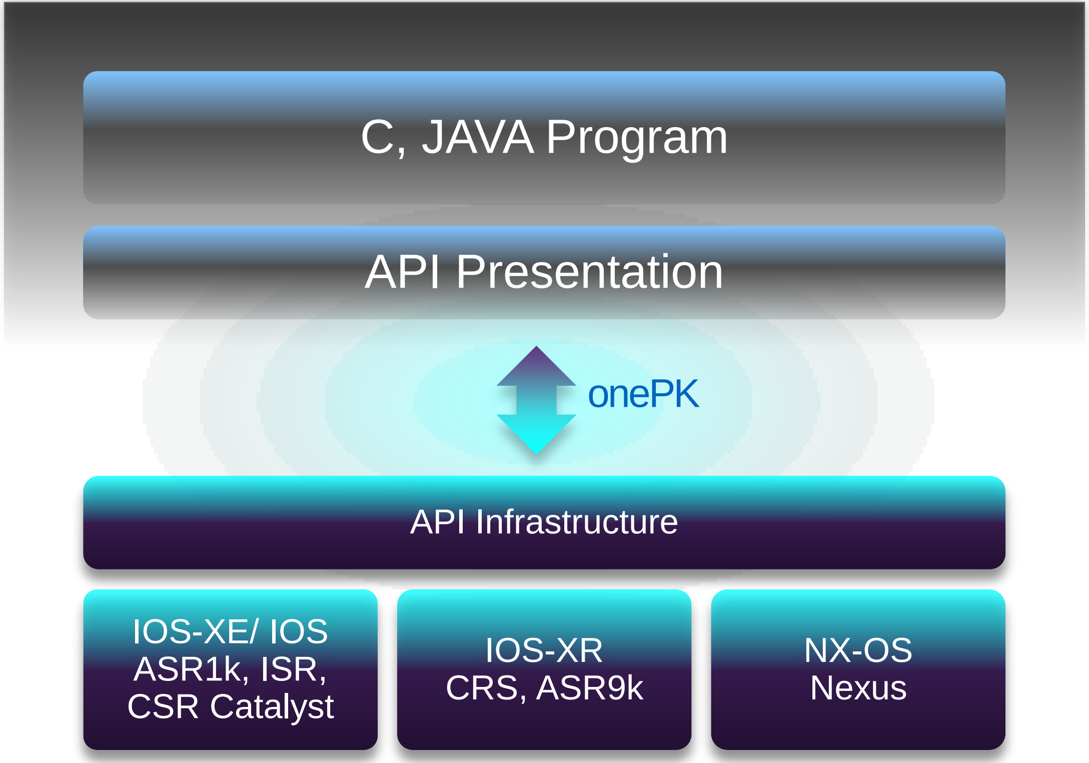
LiveAction

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

© 2014 Cisco and/or its affiliates. All rights reserved.

SDN Provisioning Ready

One Platform Kit (onePK)



BENEFITS

- Provides a consistent, programmable interface across Cisco platforms
- Industry's most comprehensive programmability kit: ***Branch, Campus, Data Centre, Service Provider, Cloud***
- Supports a wide array of APIs

© 2014 Cisco and/or its affiliates. All rights reserved.

Why Choose a Cisco WAN?

Why Choose a Cisco WAN?

Integrated Platform
for IT Simplicity

Up to 72%
in Savings

The Alternative:
Overlay Appliances

Router
WAN Path Selection
App Visibility & Control
WAN Opt.
Firewall
IP Sec VPN

Granular Control Everywhere

- Branch → ISR G2 & 4451-X
- DC → ASR1K
- Cloud → CSR1000V

Proven Security at Scale

- Any to Any Security
- Protect All Branch Resources
- Secure Direct Internet Access

Unmatched Context-based Routing

- App-Aware
- Endpoint-Aware
- Network-Aware

Quick ROI
Faster than Alternatives

$$$

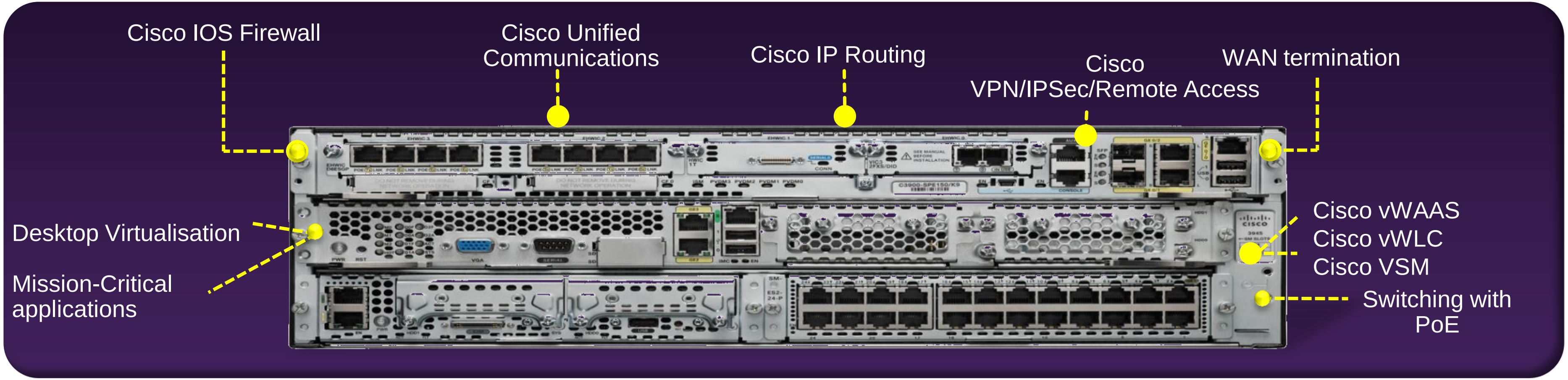
Many pay off in
6-12 months

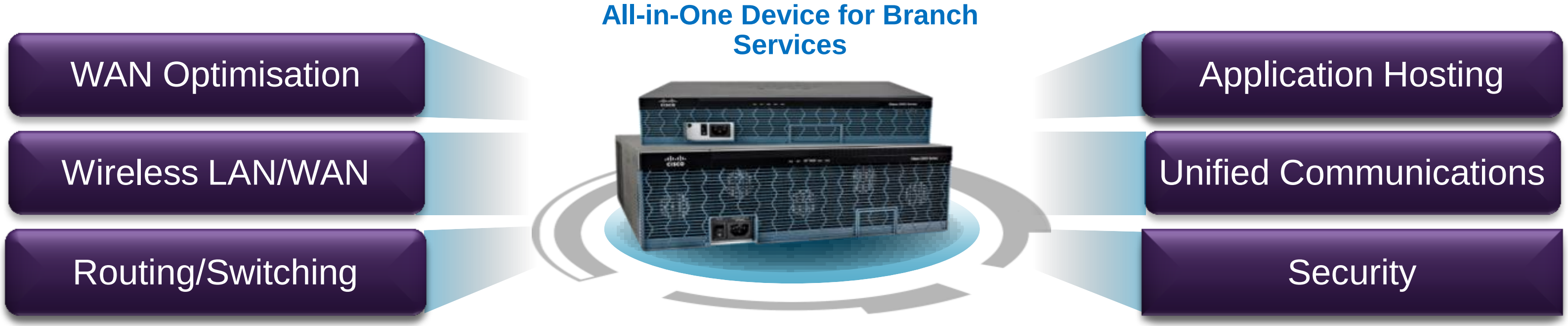
- Savings enables Business Innovation

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco ISR Branch in a Box

Use the Slots on the Most Widely Deployed Branch Device





© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco Wide Area Solution

Uncompromised Experience Over Any Connection

- Lower Costs without Tradeoffs
- Maximise Your WAN Investment
- Unleash Your Business Potential

© 2014 Cisco and/or its affiliates. All rights reserved.

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