ASR 1000 Update

Shabaz Yousaf

SRTG

Many of the products and features described herein remain in varying stages of development and will be offered on a when-and-if-available basis. This roadmap is subject to change at the sole discretion of Cisco, and Cisco will have no liability for delay in the delivery or failure to deliver any of the products or features set forth in this document.

Aims of this Session

An introductory deck to show some ASR and Secure WAN details, and not in-depth CLI!

Primary Aims:

ASR 1000 Familiarity

A quick look at the ASR 1000 series
What's new
Example packet flow

Secure WAN Familiarity

A brief look at different WAN methods including GET VPN and FlexVPN
A more in-depth look at DMVPN

ASR 1000 Overview

Platforms Quick Overview

Service-rich

The platforms complement each other – customers can launch features and be confident they will work end-to-end. Proof point is the BN deployment guides

One IOS

- IOS features are directly taken and put on IOS-XE middleware that interfaces with the ASR 1000 hardware. Where higher performance is required, the feature is ported to the QFP

Fits Modern Enterprise use-cases

Typical uses include:

- Branch routers (primarily ISRs); ASR as high-end CPE
- WAN aggregation with security (primarily ASR)
- Enterprise Edge with DoS/DDoS protection in HW (ASR), IPv6 capability
- Cloud and DC Enablement with OTV (ASR), Cloud APIs, QoS
- Manages Services CE

Price-Performance

Breadth of 100Mbit/sec – 100Gbit/sec is supported;
On all platforms, performance figures typically include services; there is headroom in the CPUs

Up to 100Gbit/sec with services enabled; achieved by moving all major features onto the QFP and dedicated hardware

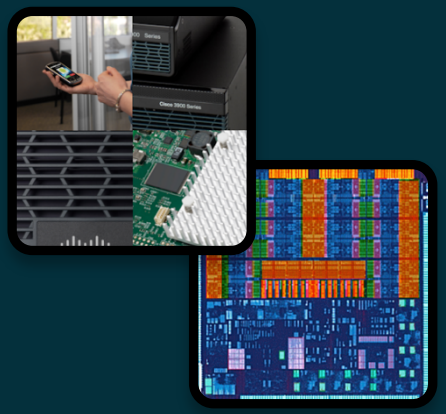
Hardware crypto available on all platforms (embedded in ASR), DPI on all platforms (scale depends on platform and usage)

Feature-rich

Interface rich

Hardware Encryption

Multi-core CPUs



Redundancy and Reliability

Feature Innovation

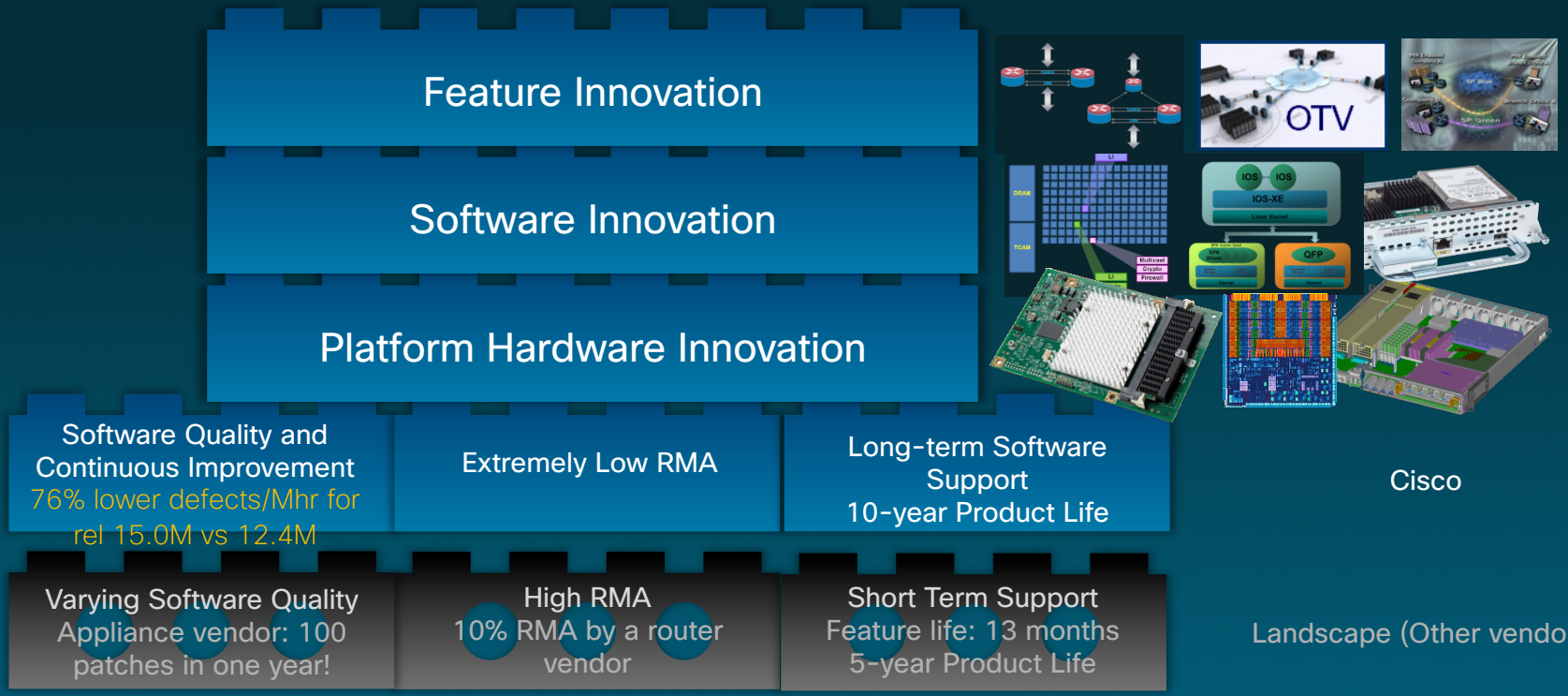
L2- and L3-based High Availability mechanisms, OTV for DCs, Performance Routing

Software Innovation

Fully separated data plane, Software Redundancy, SRE local services

Hardware Innovation

Low RMA, Second generation QFP, Full backplane redundancy, multiple WAN interfaces for redundancy



Cisco ASR 1000 Series Routers: Overview

2.5 Gbps to 100Gbps Range—Designed Today for Up to 360 Gbps in the Future

Compact, Powerful Router

- Line-rate performance 2.5G to 100G+ with services enabled
- Investment protection with modular engines, IOS CLI and SPAs for I/O
- Hardware based QoS engine with 128K queues

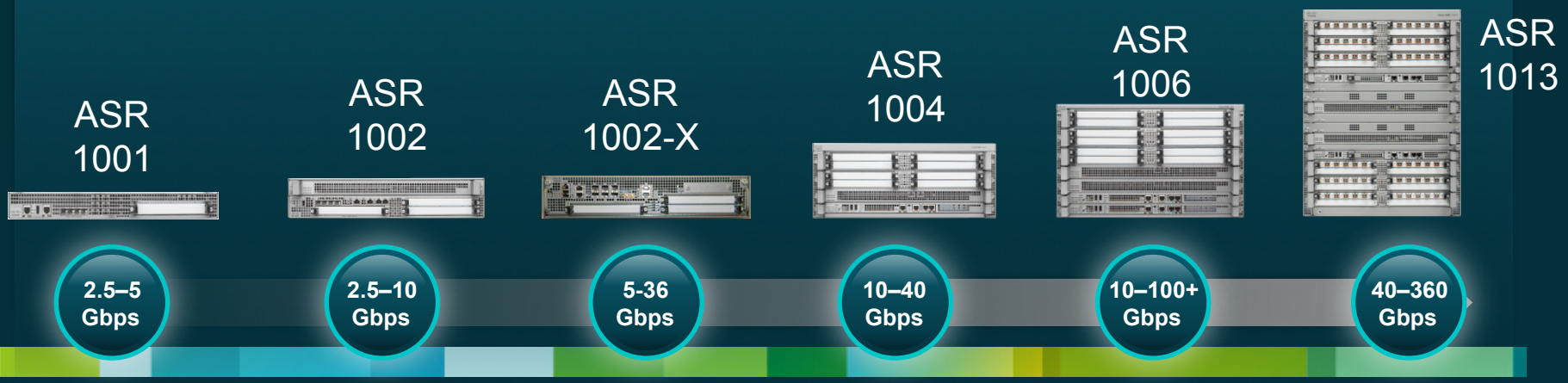
Business-Critical Resiliency

- Fully separated control and forwarding planes
- Hardware and software redundancy
- In-service software upgrades

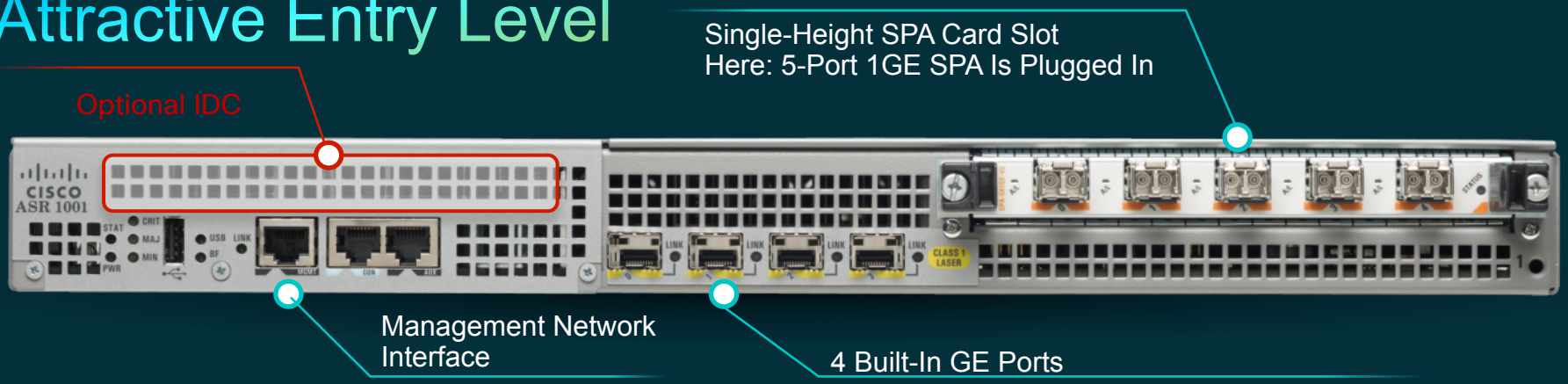
Instant On Service Delivery

- Integrated firewall, VPN, encryption, NBAR, CUBE-ENT,CUBE-SP
- Scalable on-chip service provisioning through software licensing

Embedded High-Performance Resilient Services



Cisco ASR 1001
Attractive Entry Level



- Small Footprint (1-rack unit height)
- Performance range of 2.5 to 5-Gbps
- 4G (Default) & 8G & 16G Memory options
- Up to 1.8 Gbps crypto throughput built-in
- 1 single height SPA slot for I/O connectivity and 4 built-in GE ports + optional daughter card
- High Availability with SW redundancy support

Six versions shipping

- ASR1001
- ASR1001-2XOC3POS
- ASR1001-4XT3
- ASR1001-8XCHT1E1
- ASR1001-4X1GE
- ASR1001-HDD (160 GB Hard Disk Drive)

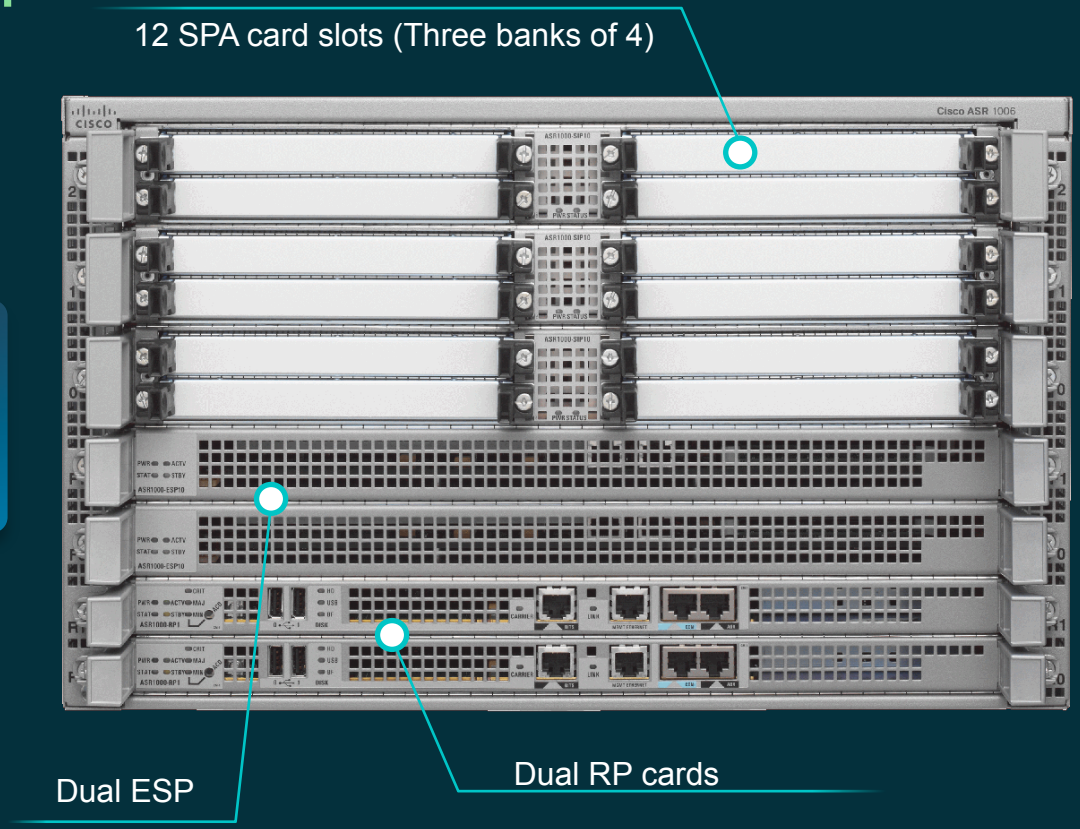
For all models and bundle SKU information, please refer to "Cisco ASR 1000 Series Aggregation Services Routers Ordering Guide" at: http://www.cisco.com/en/US/products/ps9343/prod_bulletins_list.html

ASR 1006
Redundant ESP, RP

Fully hardware redundant, 6RU size

10–100+Gbit/sec throughput

Dense interface capability (12 SPA slots)



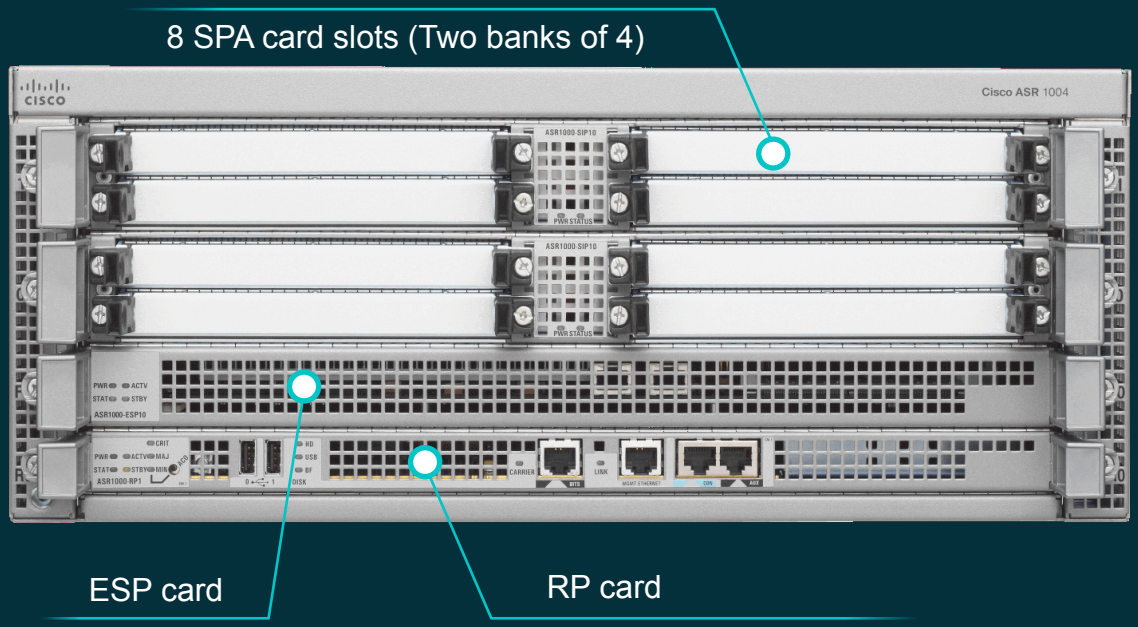
For all models and bundle SKU information, please refer to “Cisco ASR 1000 Series Aggregation Services Routers Ordering Guide” at: http://www.cisco.com/en/US/products/ps9343/prod_bulletins_list.html

ASR 1004
4RU, Swappable RP and ESP

Swappable RP, ESP cards

10-40 Gbit/sec throughput

8 SPA card slots



For all models and bundle SKU information, please refer to “Cisco ASR 1000 Series Aggregation Services Routers Ordering Guide” at: http://www.cisco.com/en/US/products/ps9343/prod_bulletins_list.html

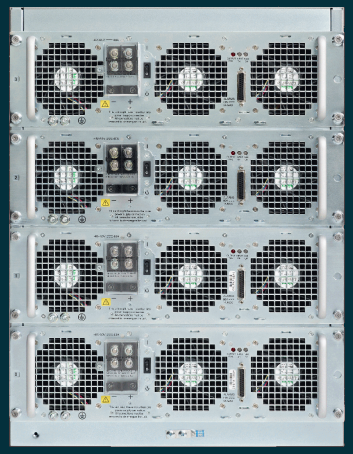
ASR 1013
Redundant ESP, RP

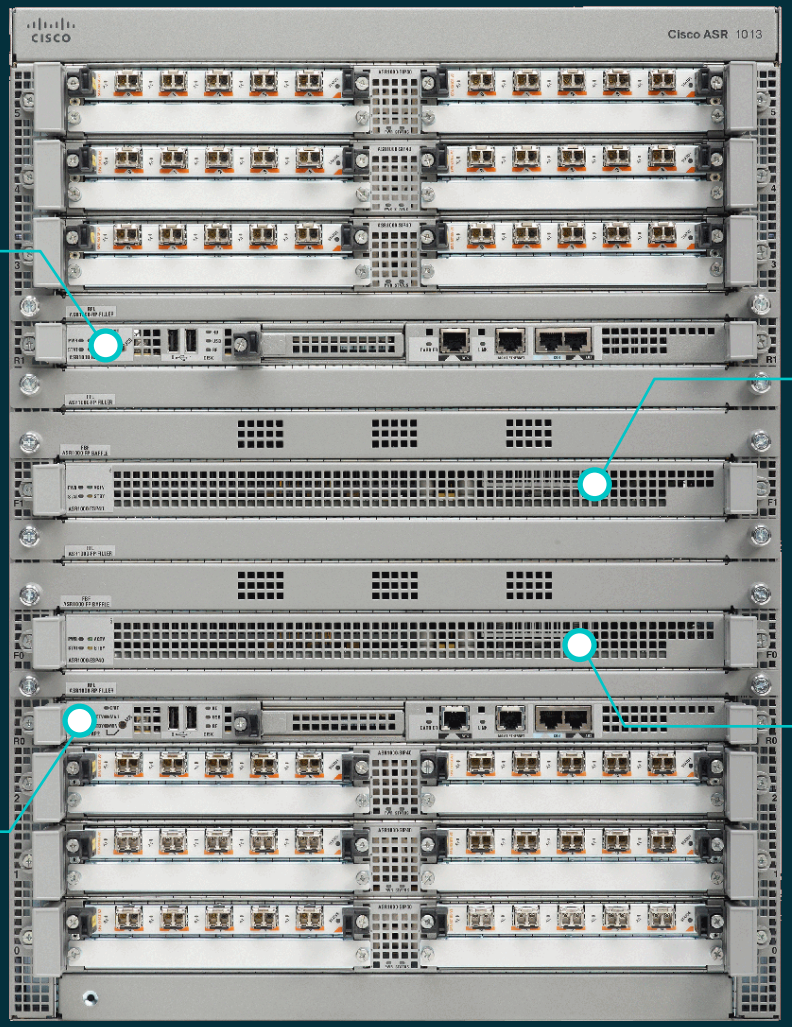
Fully hardware redundant, 13RU size

40-360 Gbit/sec throughput

Extremely Dense interface capability

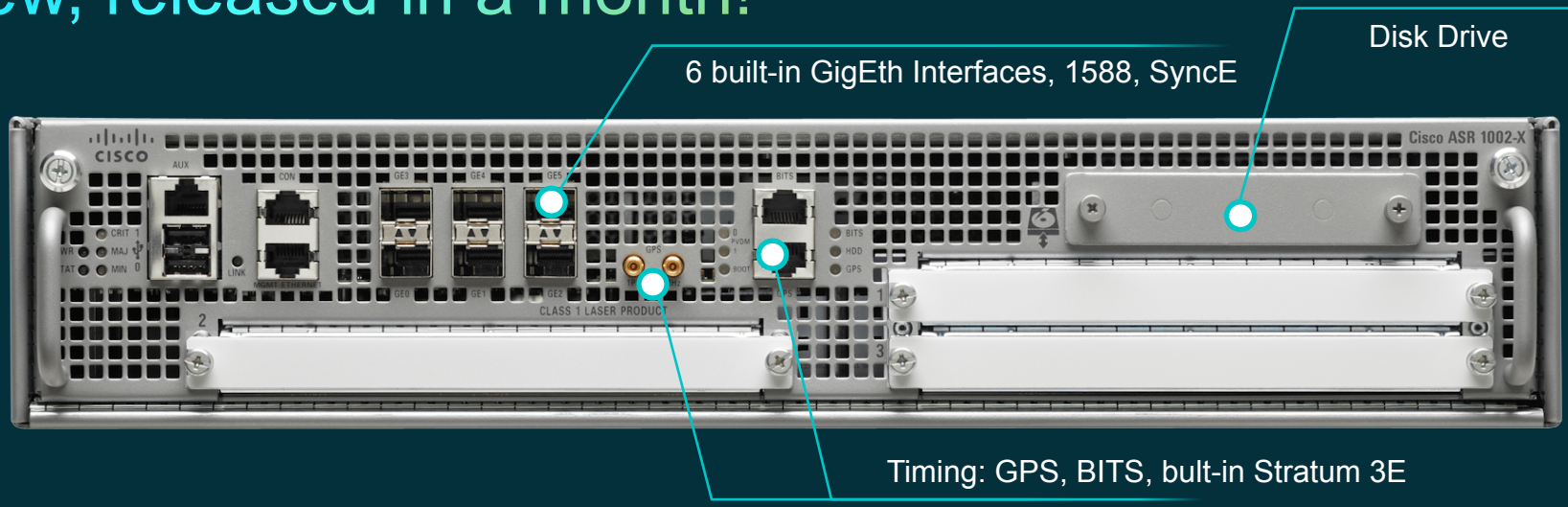
24 SPA slots



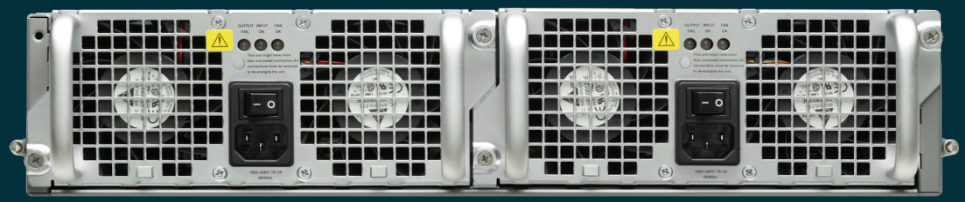


For all models and bundle SKU information, please refer to “Cisco ASR 1000 Series Aggregation Services Routers Ordering Guide” at: http://www.cisco.com/en/US/products/ps9343/prod_bulletins_list.html

ASR 1002-X
New, released in a month!

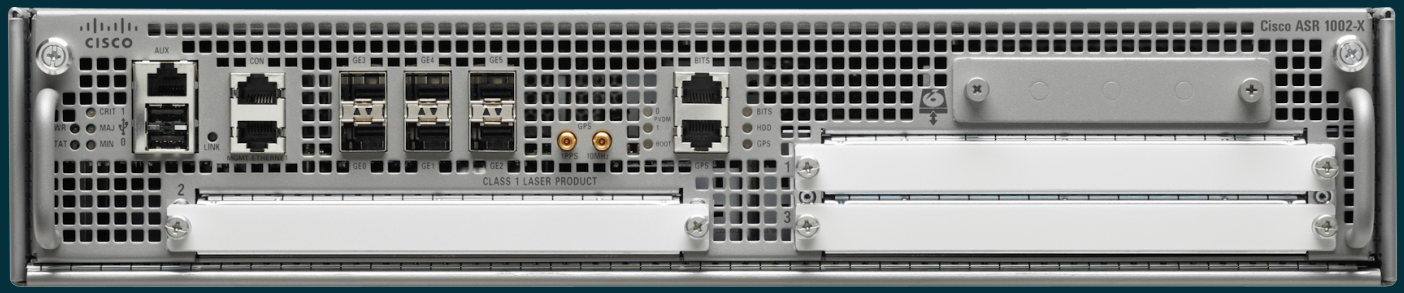


- Built-in 5-36Gbit/sec
- Significant boost in RP capability
- Second Generation QFP (aka Yoda)
- 30Mpps Performance
- 4Gbit/sec Crypto (8Gbit/sec PID released later)



For all models and bundle SKU information, please refer to “Cisco ASR 1000 Series Aggregation Services Routers Ordering Guide” at: http://www.cisco.com/en/US/products/ps9343/prod_bulletins_list.html

ASR1002-X Summary



Chassis & HW	• 2RU form factor • Integrated RP, ESP & SIP • Redundant AC/DC PSU, same as ASR1002
System BW	• 5G, 10G, 20G, 36G, via software upgrade
Performance	• Up to 23 Mpps (TBC)
Crypto BW	• 4G & 8G, via software upgrade
Control Plane	• 2.5GHz processor (4 core)
Data Plane	• Integrated ESP with SW selectable BW from 5G to 36G
I/O	• 3 SPA bays • 6 built-inGE ports (Copper/Fiber SFP, SyncE capable) • Console/Aux: RJ45 and USB Console • Management Ethernet • External USB storage • Optional HDD

Key Applications	• Enterprise: WAN Aggregation, Internet GW, Highend branch and DCI • SP Managed CPE and MetroE CPE • Entry Level PE router • Distributed BRAS/LNS
Broadband	• Up to 64 K sessions
IPSec	• 8Gbps (1400Bytes), 4K tunnels
FW/NAT	• 36G FW/NAT, 2 M sessions
Network Timing	• Stratum 3/G.813 Clocking, BITS timing, GPS, SyncE, 1588
Image Security	• Secure boot • Code Signing (FIPS-140-3)

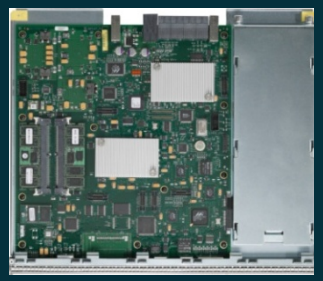
Embedded Services Processors - ESP

Based on Quantum Flow Processor (QFP)

http://www.cisco.com/en/US/partner/prod/collateral/routers/ps9343/data_sheet_c78-450070.html

	ESP-2.5G	ESP-5G	ESP-10G	ESP20G	ESP-40G	ASR1002-X ESP
System Bandwidth	2.5Gbps	5Gbps	10Gbps	20Gbps	40Gbps	5/10/20/36Gbps
Performance	4Mpps	7.5 Mpps	17Mpps	23Mpps	23Mpps	30Mpps
# of Processors	10	20	40	40	40	8/16/32/62
Clock Rate	900 Mhz	900 Mhz	900 Mhz	1.2 GHz	1.2 GHz	1.2 GHz
Crypto Engine BW (1400 Byte)	1.8Gbps	1.8Gbps	4Gbps	7Gbps	11Gbps	4Gbps
QFP Resource Memory	256MB	256MB	512MB	1GB	1GB	1GB
Packet Buffer	64MB	64MB	128MB	256MB	256MB	512MB
Control CPU	800 MHz	800 MHz	800 MHz	1.2 GHz	1.8 GHz	2.13 GHz
Control Memory	1GB	1GB	2GB	4GB	8GB	4/8/16GB
TCAM	10Mb	10Mb	10Mb	40Mb	40Mb	40Mb
Chassis Support	ASR1001 (integrated) Upgrade to 5-Gbps via license	ASR1001 (integrated) ASR 1002	ASR 1002, 1004, 1006	ASR 1004, 1006	ASR 1004, 1006, 1013	ASR1002-X

Route Processor - RP

	ASR1001	ASR1002-X	RP1	RP2
				
CPU	Dual-Core 2.2GHz Processor	Quad-Core Processor	General Purpose CPU based on 1.5GHz	Dual-Core 2.66GHz Processor
Memory	4GB default 8GB 16GB	4GB default 8GB 16GB	2GB default 4GB RP1 with 4GB built in toASR1002	8GB default 16GB
Built-in eUSB bootflash	8GB	8GB	1GB (8GB on integrated RP1 on ASR-1002)	2GB
Storage	External USB	160GB HDD (optional) & External USB	40GB HDD & external USB	80GB HDD & external USB
Cisco IOS XE Operating System	64 bit	64 bit	32 bit	64 bit
Chassis Support	ASR1001 RP integrated into the ASR1001 chassis	ASR1002-X RP integrated into the ASR1002-X chassis	RP1 module supported on ASR1004 and ASR1006. RP1 is integrated on the ASR1002 chassis	RP2 module supported on ASR1004, ASR1006, and ASR1013

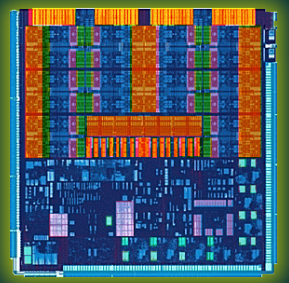
Data Sheet: http://www.cisco.com/en/US/partner/prod/collateral/routers/ps9343/data_sheet_c78-441072.html

ESP-80
New, released in a month!

Total Bandwidth	• 80 Gbps
Performance	• Up to 32 Mpps
QuantumFlow Processors	• 2
- Resource Memory	• 2 x 2 GB
- TCAM	• 1 x 80 Mb
- Packet Buffer	• 2 x 512 MB
Control CPU	• Dual-core CPU
- Frequency	• 1.73 GHz
- Memory	• 16 GB
Broadband	• Up to 58k sessions with queues
QoS	• Up to 232 K queues
IPSec Bandwidth (1400 B)	• 25 Gbps
FW/NAT	• 6M sessions
Chassis	• ASR 1006 (with ASR1006/13 P/S), ASR 1013
Route Processor	• RP2 + Future

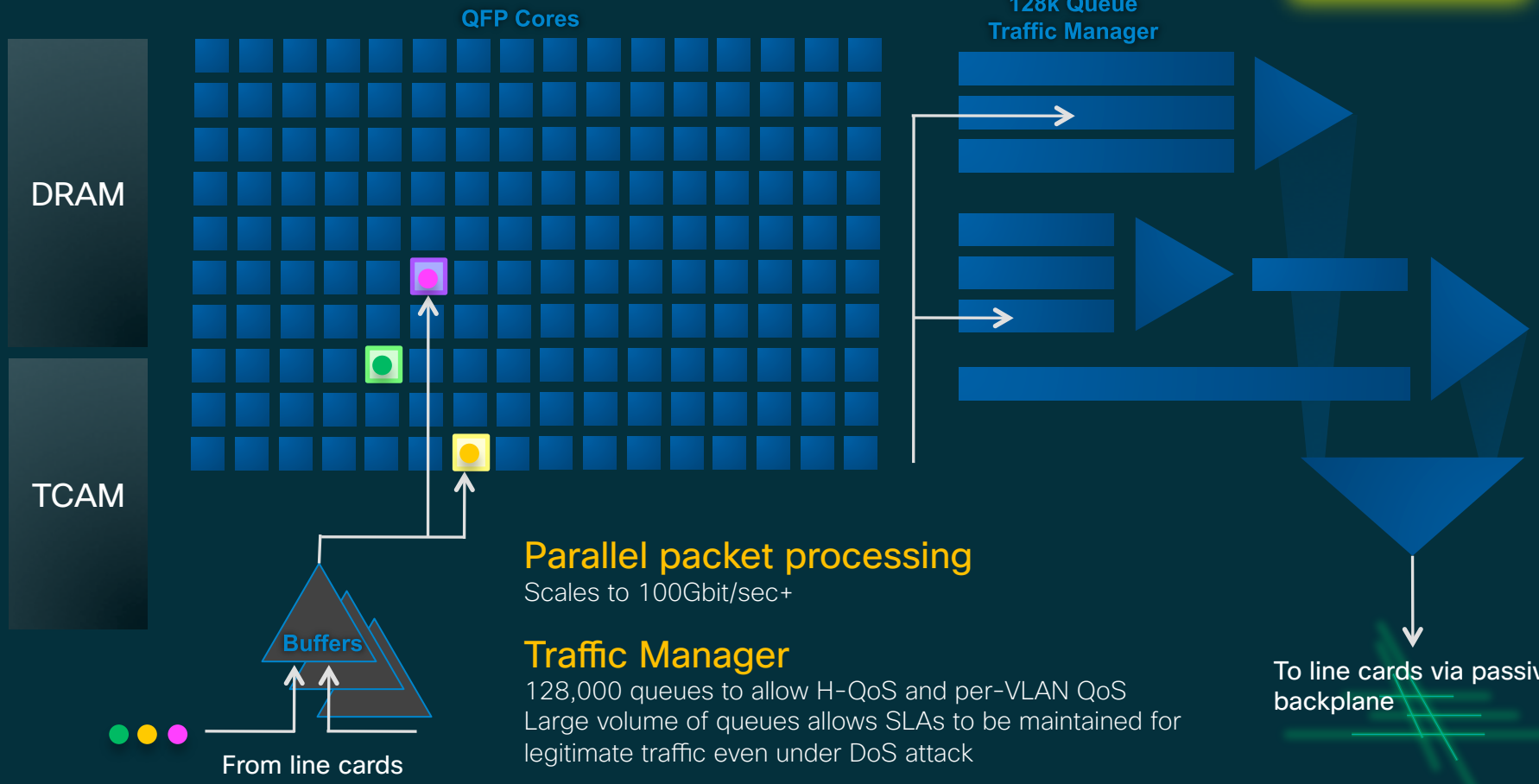
Cisco QFP

Ultra-low latency Packet Processing and QoS Implementation



Dynamic Ingress Buffers

Only turned on when needed, for minimal latency
Multiple priority buffers – QoS is maintained even during overload



Parallel packet processing

Scales to 100Gbit/sec+

Traffic Manager

128,000 queues to allow H-QoS and per-VLAN QoS
Large volume of queues allows SLAs to be maintained for legitimate traffic even under DoS attack

Integrated Programmability and Management APIs

Vast array of options – these are just a few

In-built computing languages
Choose the best API for the task at hand
APIs can be combined; multiple ones can be used simultaneously

Easy to use

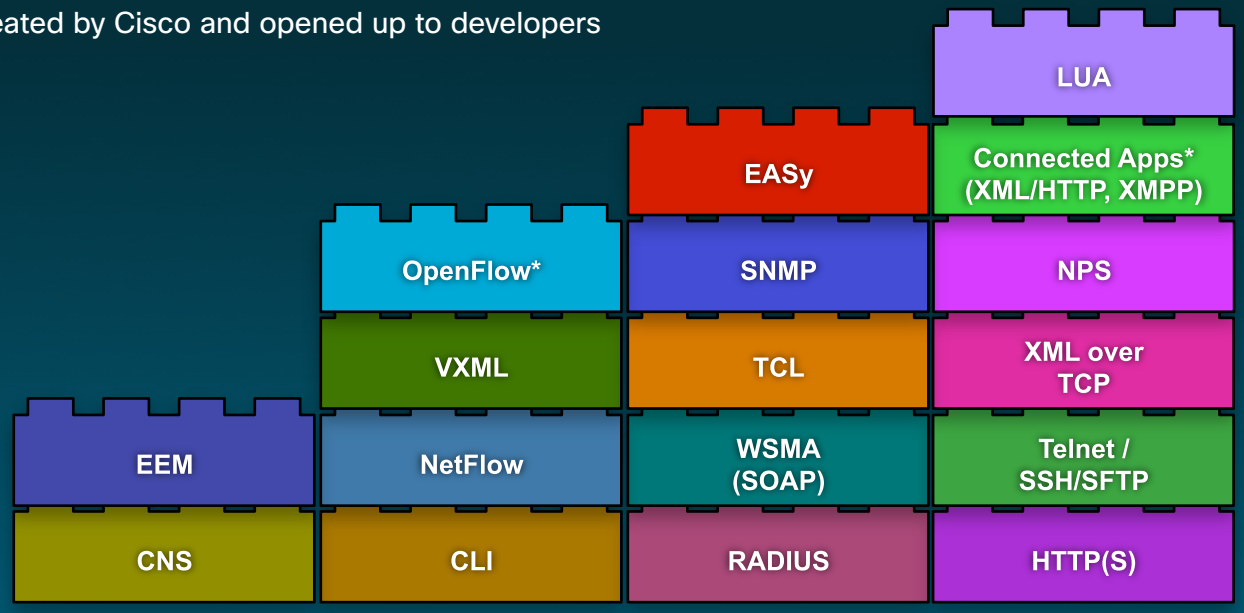
Standards based interfaces and programming languages, like HTTP and TCL
Free SDK available for WSMA – rapidly deploy web apps

Cisco Innovations

Features like NetFlow were created by Cisco and opened up to developers

Some Highlights

Full TCL implementation
WSMA
VXML
NPS



Secure WAN

Secure WAN

Hardened against Attacks

ISO/IEC IT security Common Criteria support

Latest FIPS-140-3 security requirements support

Suite B support – Mandated by Governments, healthcare, airports

Embedded IOS FW/IPS and ZBFW

Scalable

The same end-to-end solution scales from small businesses to large enterprises. Up to 4k sites per hub with DMVPN/FlexVPN and no limit with GET VPN

All forms of connectivity are supported – 3G, 4G, DSL, Ethernet

DMVPN

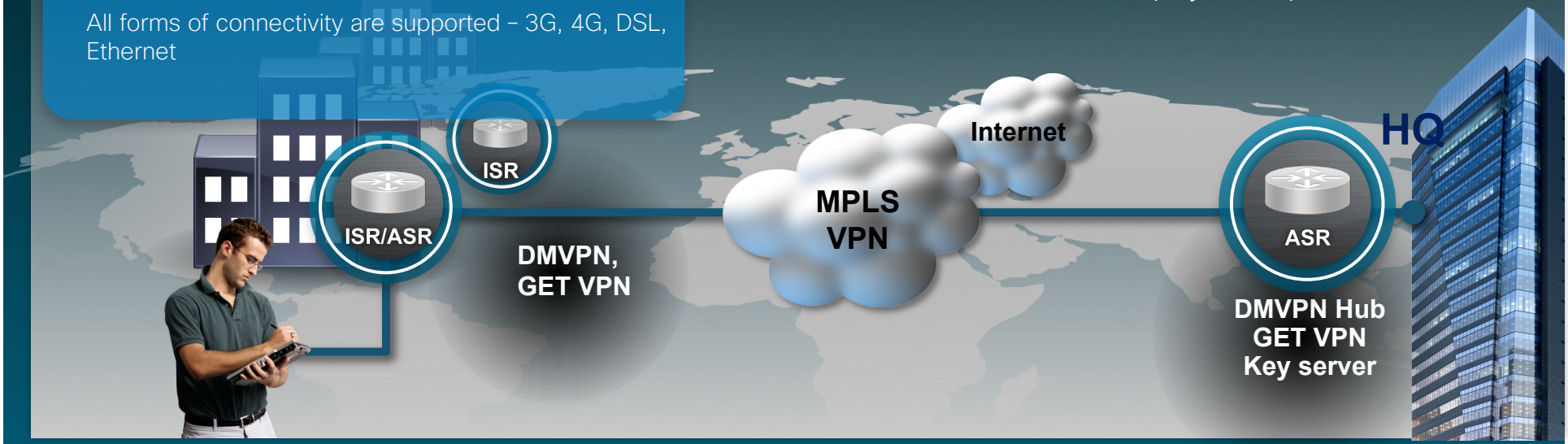
Proven, Dependable, Secure
Used by the multi-nationals and military customers
Hierarchical Super-Hub capability
QoS Preservation

GET VPN

Massively scalable, ultra-fast
Site-to-site and Multicast optimized
No overlay network required
QoS Preservation

FlexVPN

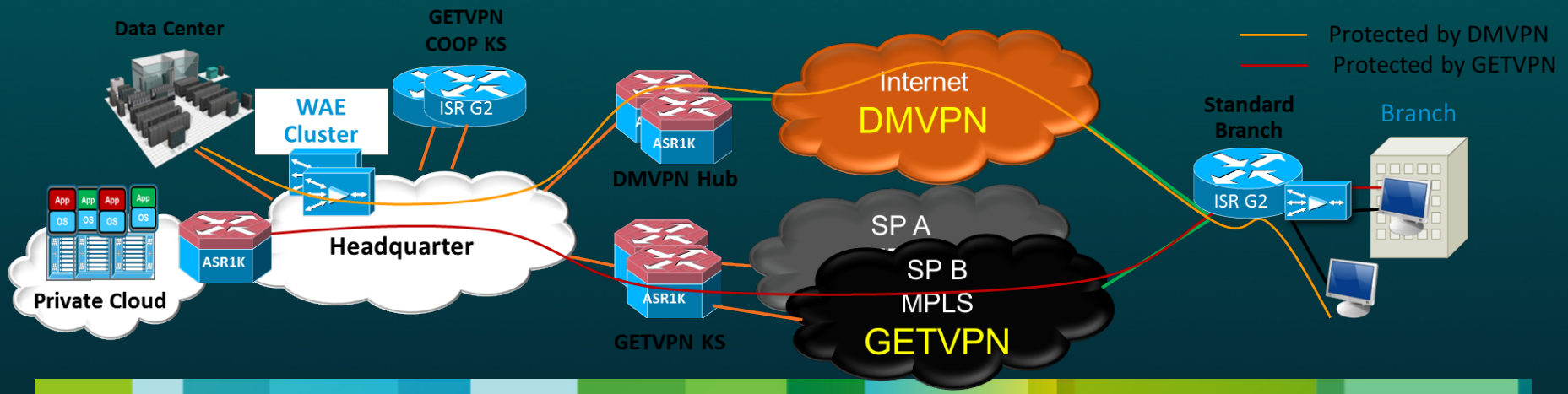
Faster tunnel set-up, simpler configuration
Supported by Windows natively
Supported by hard- and soft-clients
Mobile devices (Anyconnect)



Pervasive Security

Provide Secure, Reliable Access to Any Services

- Provide data privacy for accessing services across the WAN
  - GETVPN over MPLS provides any-to-any encryption
  - DMVPN over 3G/4G or Internet provides dynamic spoke-to-spoke tunnel
- Highly scalable WAN aggregation with encryption
  - 4000 DMVPN tunnels per ASR1K
  - Up to 8 Gbps of encryption throughput per ASR1K
- Full interoperation with QoS ensures service performance



Next Generation Enterprise WAN

Regional WAN Design

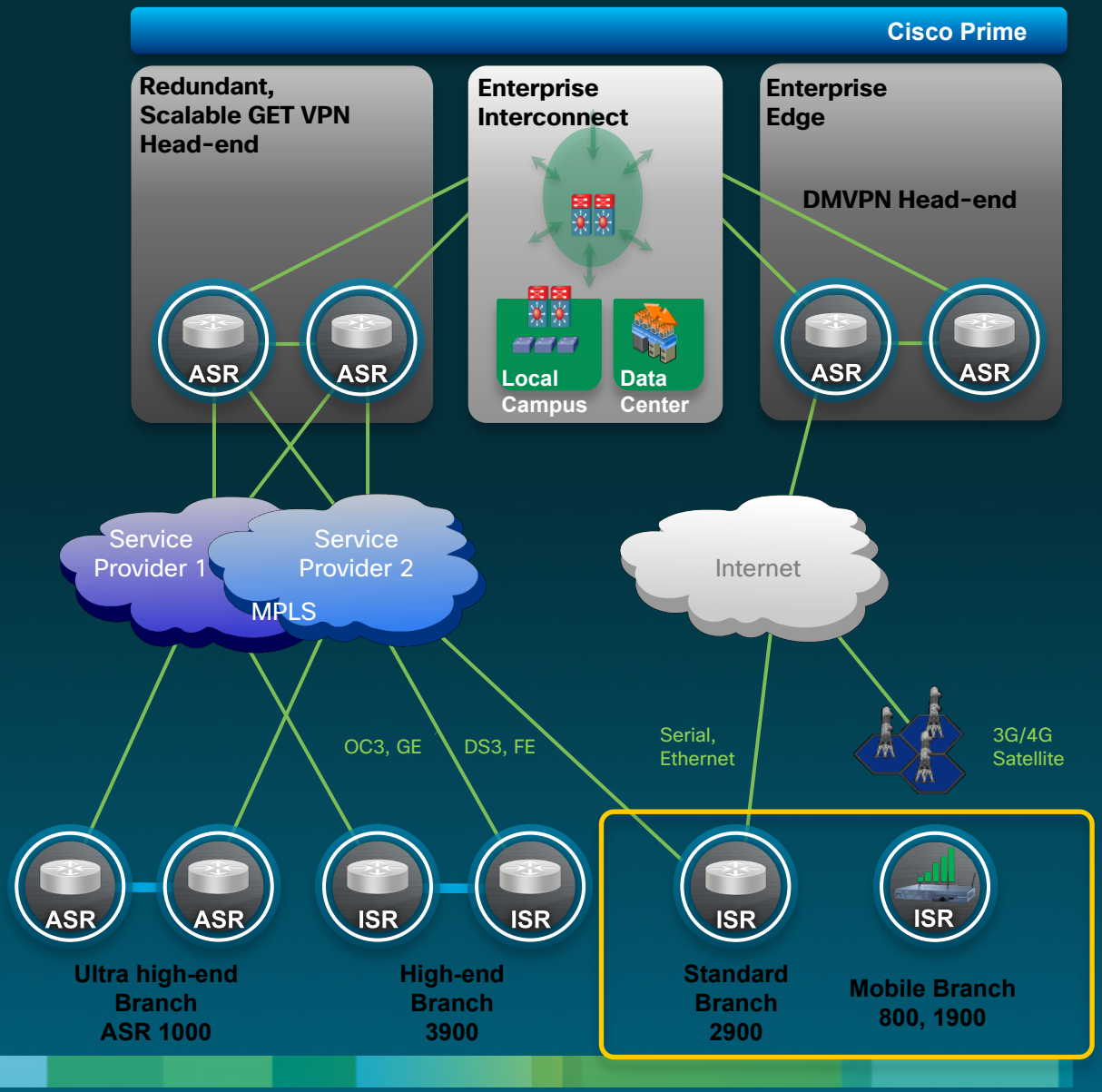
Secure WAN Highlights

GET VPN for fast encryption

DMVPN for connections via Internet

Scales to thousands of branches

Provides routing, security, encryption



Secure WAN

GET VPN Features

Extremely high throughput
Ultra low setup latency

Perfect for voice, video and better application response

Tunnel-less method; no concept of tunnel set-up rates, nor any set-up delay

Massively scalable – load balancing achievable

Optimal Routing

Uses the existing IP packet header

Ideal for secure WAN and DC interconnect

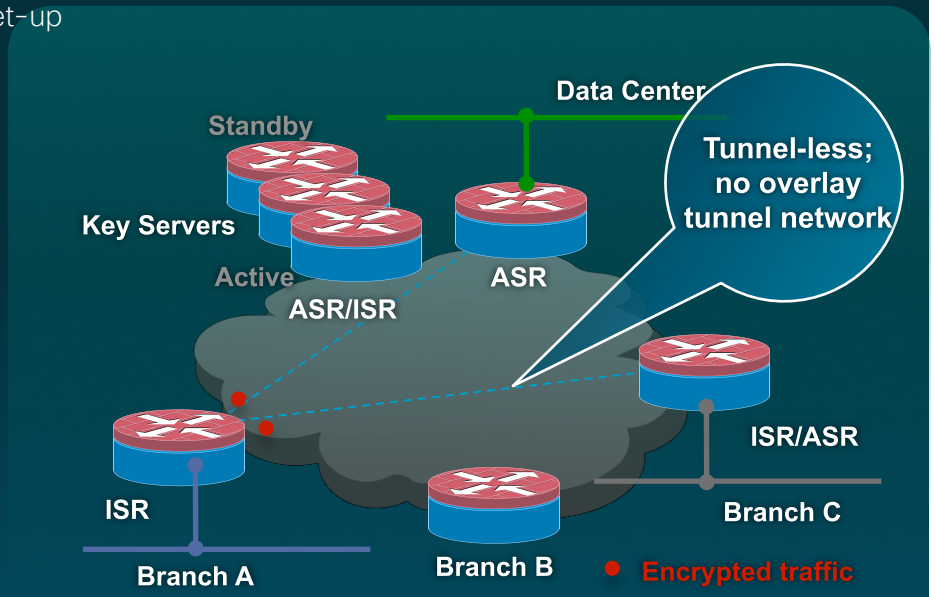
Useful for secure WAN to branches and site-to-site

Can be combined with OTV for secure, fast DC interconnections

Why ISR and ASR?

This technology is only available on ISR and ASR; competitor alternatives are not mature.

ISR in the branch can use GET VPN for ultra-fast secure connections, and can use DMVPN for backup connections over the Internet



22

FlexVPN

Motivation

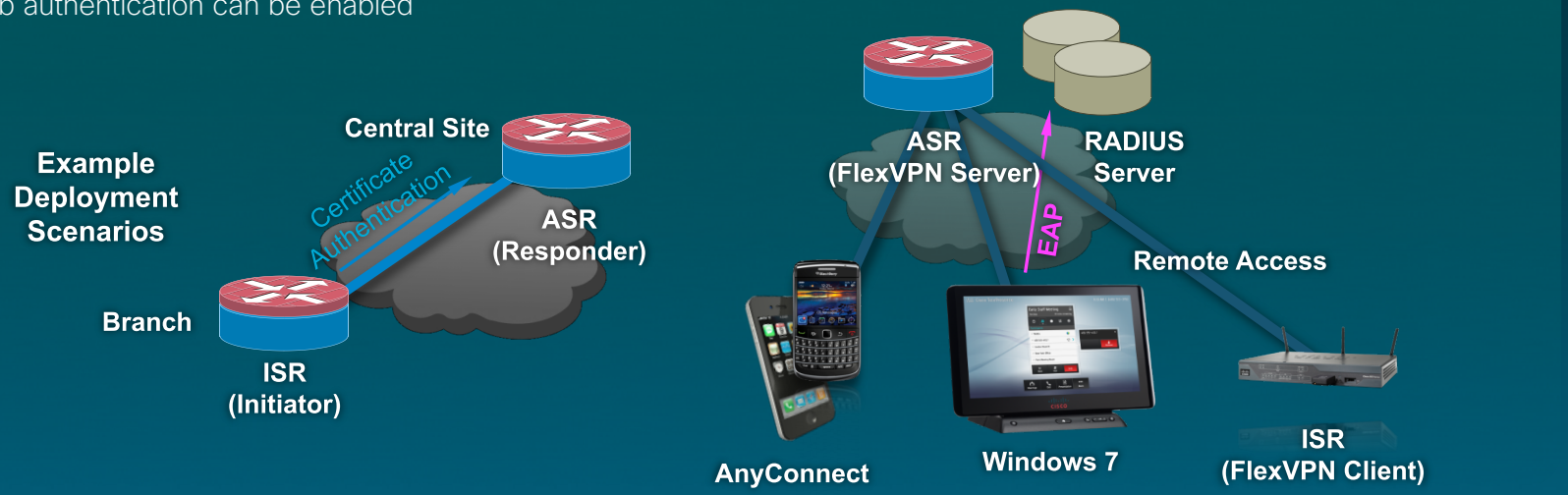
Many VPN methods are in use – DMVPN, EasyVPN, Crypto Maps
Simplification and compatibility
Latest, secure IPsec negotiation – IKEv2
Compatiblity with Windows 7 natively, and AnyConnect on mobile devices

Easy to migrate, Easy to use

Simplification of configuration
Similar 'look and feel' to the popular DMVPN

Architecture Benefits

IPv6/IPv4 agnostic
DoS attack resistant
Ideal for all enterprise connectivity, and for SP managed VPN offerings
All forms of connectivity can be enabled; Remote access, Client-Server, Site-Site, Hub-Spoke
Web authentication can be enabled



Secure WAN

DMVPN Features

Highly Regarded

Considered to provide extremely secure site-to-site connections
- As used by Government, Finance sector and Military/Paramilitary organizations

Scalable

Full mesh connectivity with simple configuration

No need to manually configure static IPsec tunnels
- As sites are added, just configure two tunnels

Super-Hub hierarchy

Automatic Site-to-site IPsec Tunnels

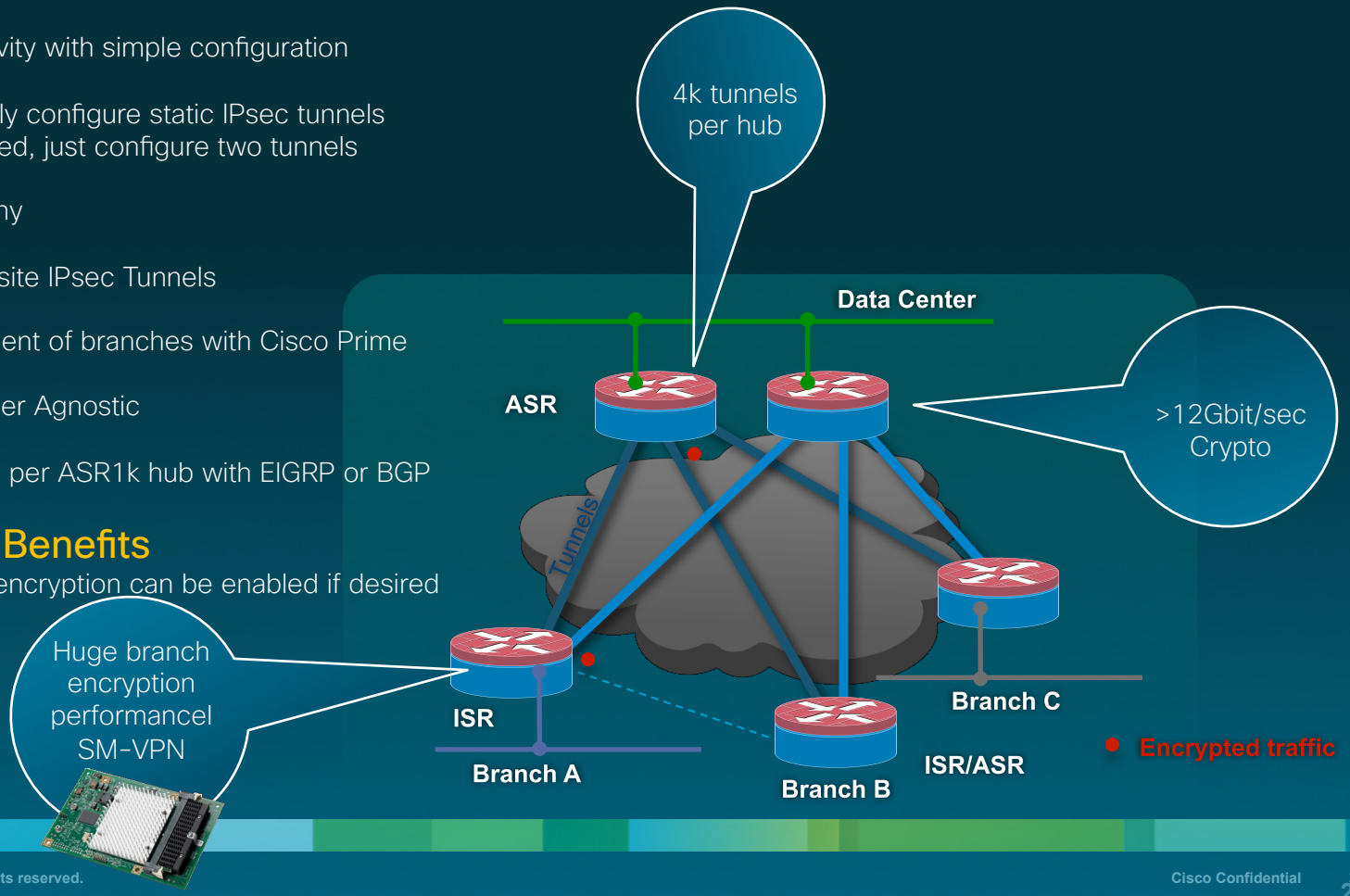
Automatic deployment of branches with Cisco Prime

Transport and Carrier Agnostic

Up to 4000 spokes per ASR1k hub with EIGRP or BGP

Architecture Benefits

Direct site-to-site encryption can be enabled if desired



Who uses DMVPN?

- Governments
- Enterprises and SPs
- Financial organizations
- Public references: AT&T, USPS, Telecom Italia, ePlus, Sprint

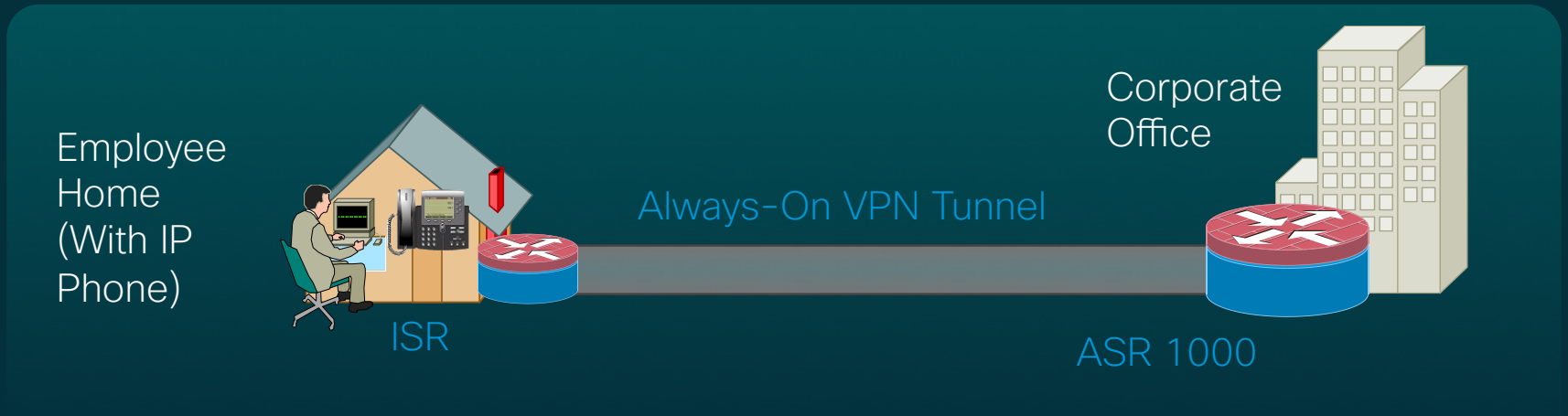
At some of our sites, we were spending almost $3000 a month for the circuits," ..." Now, we're saving as much as $2000 a month per site just on WAN connectivity costs alone, not including all the other advantages we get..."

Enterprise Network Designs
Point of Sale

- Typical examples include Bank ATM or retail credit and debit card networks
- Requirement is to terminate a very large number (up to 20,000+) of low-bandwidth spokes
- Server-load-balancing (SLB) designs for super hub

Enterprise Network Designs

Small Office or Home Office



- Used to provide work access from home or offsite locations
- Enterprise Class Teleworker (ECT) designs
- NAT support needed on most of the spokes
- Thousands of spokes
- Typical requirement is to support voice and data to and from the head-office (hub) location with occasional spoke-to-spoke voice

Service Provider Network Designs

Internet Service Provider

- VRF-aware DMVPN on the hubs to segregate customer traffic
- MPLS (2547oDMVPN); connecting provider edge devices over an IP network (current support only for hub and spoke)
- Hub-and-spoke and spoke-to-spoke networks
- Different size networks (number of spokes), but also supporting many DMVPN networks on the same set of hub routers

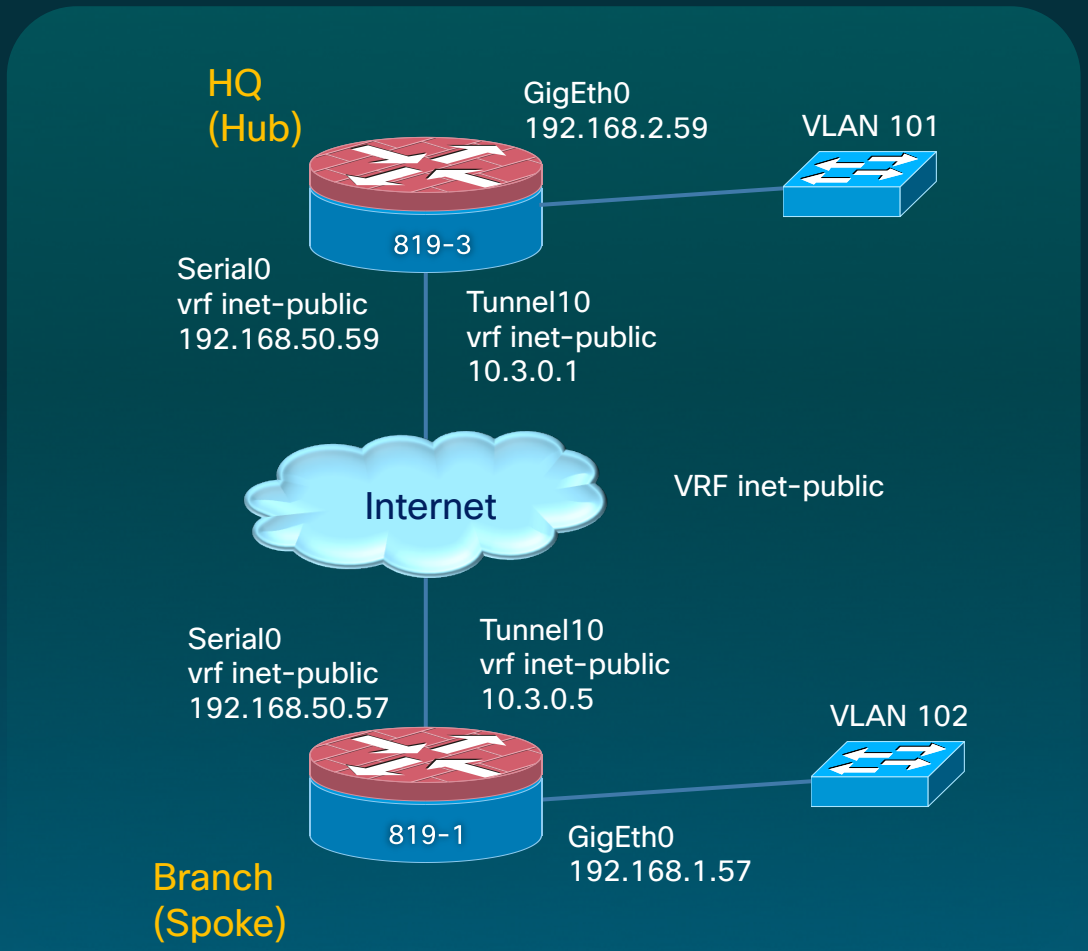
How does it work?

- DMVPN is a Cisco IOS® Software solution for building IPsec + GRE VPNs in an easy, dynamic, and scalable manner.
- DMVPN relies on two proven technologies:

  Next Hop Resolution Protocol (NHRP): Creates a distributed (NHRP) mapping database of all the spoke tunnels to real (public interface) addresses

  Multipoint GRE Tunnel Interface: Single GRE interface to support multiple GRE and IPsec tunnels; simplifies size and complexity of configuration

A (Small) Live DMVPN Topology



Headend QoS

- Important because Spoke may become congested
- A few different ways to implement are possible
- NG Ent-WAN proposes this method:

  Apply qos pre-classify on the tunnel interface

  Use a two-level hierarchy

  Child classes in policy-map are used for different traffic types (e.g. VOICE)

  Parent classs in policy-map are used for shaping for MOBILE and STANDARD branches (ACLs used to identify the branches)

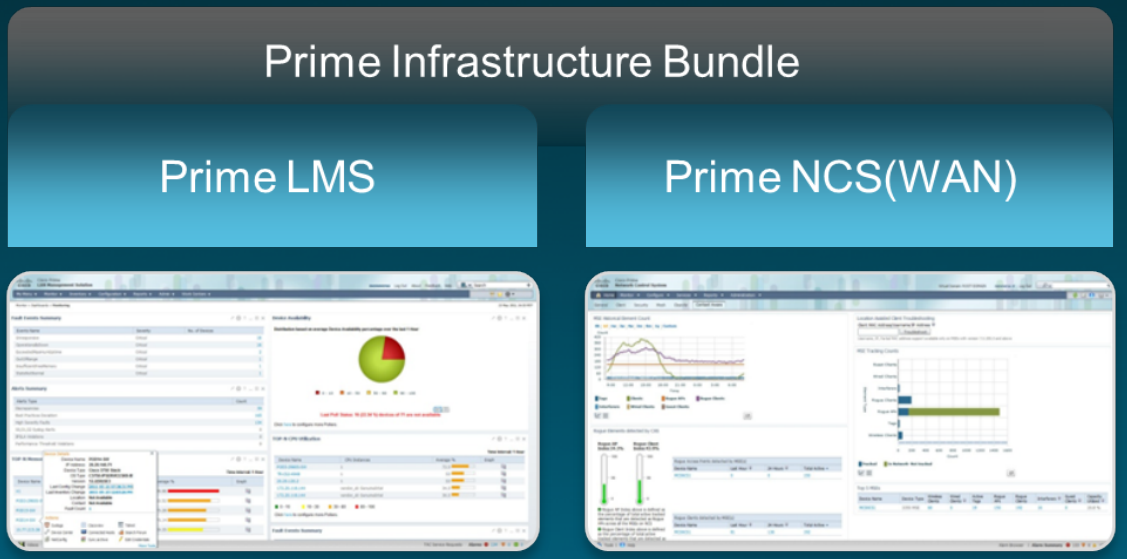
How to Deploy DMVPN Easily

Method # 1

Consult the NG Ent-WAN Regional WAN deployment guide
Step-by-step CLI for Hub and Spokes
http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns816/guide_c07-680894.html

Method # 2

Employ Prime NCS(WAN)
Available as a VM (can run on SRE for trials), as part of Cisco Prime Infrastructure Bundle



Deployment Guides

Best Practice Deployments

Borderless Networks Community

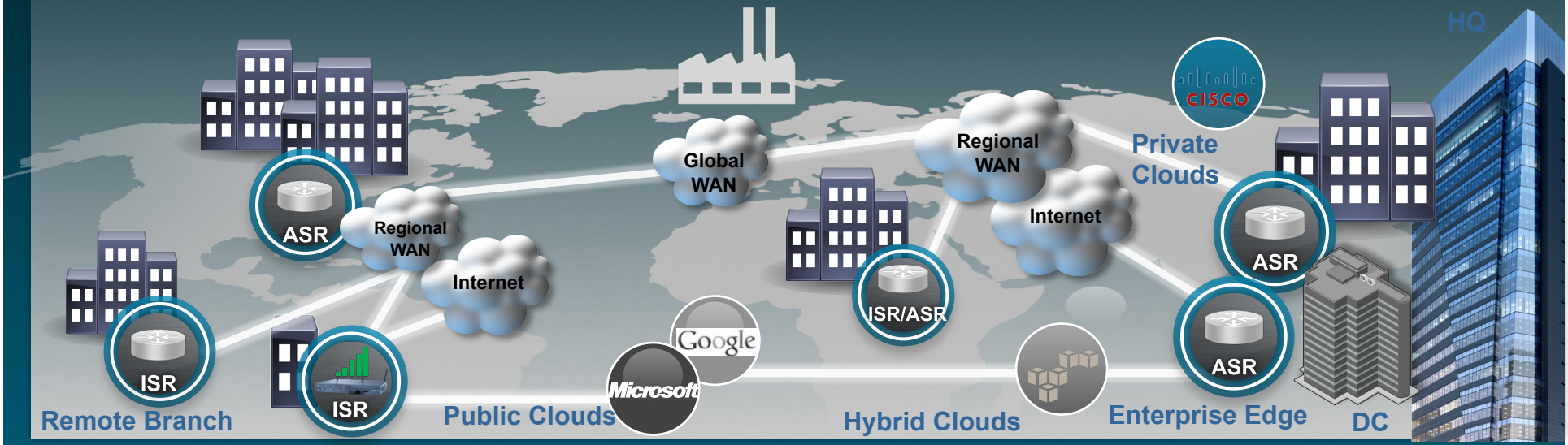
- Architectures to suit small businesses and large enterprises
- Downloadable design guides
- Upgrade portions of the network (e.g. Enterprise Edge) to a BN architecture, or enable functionality incrementally (e.g. IPv6 NAT64)

Easier Network Management

- Pre-built workflows and templates that can be customized where needed

Sector design zones
- **Education**
- **Financial**
- **Government**
- **Healthcare**
- **Manufacturing**
- **Retail**

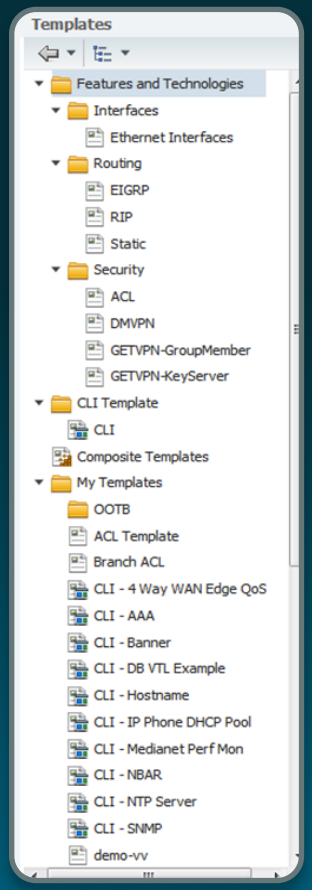
Branch/WAN design zone
Regional WAN Architecture Guide
Campus design zone
Data Center design zone
Security design zone
Mobility design zone
Collaboration design zone



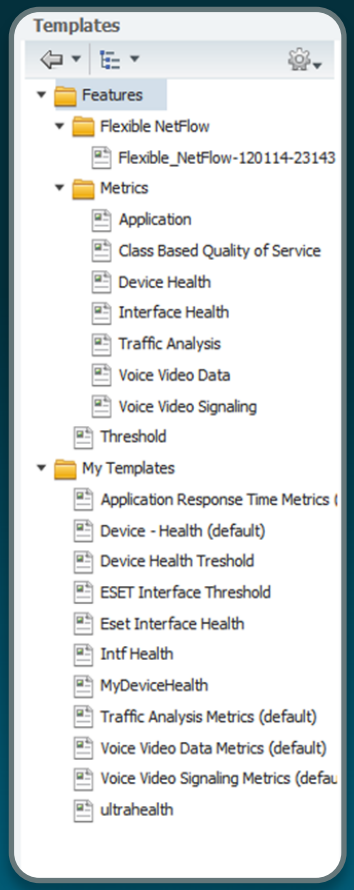
NCS (WAN)

Example Screenshots

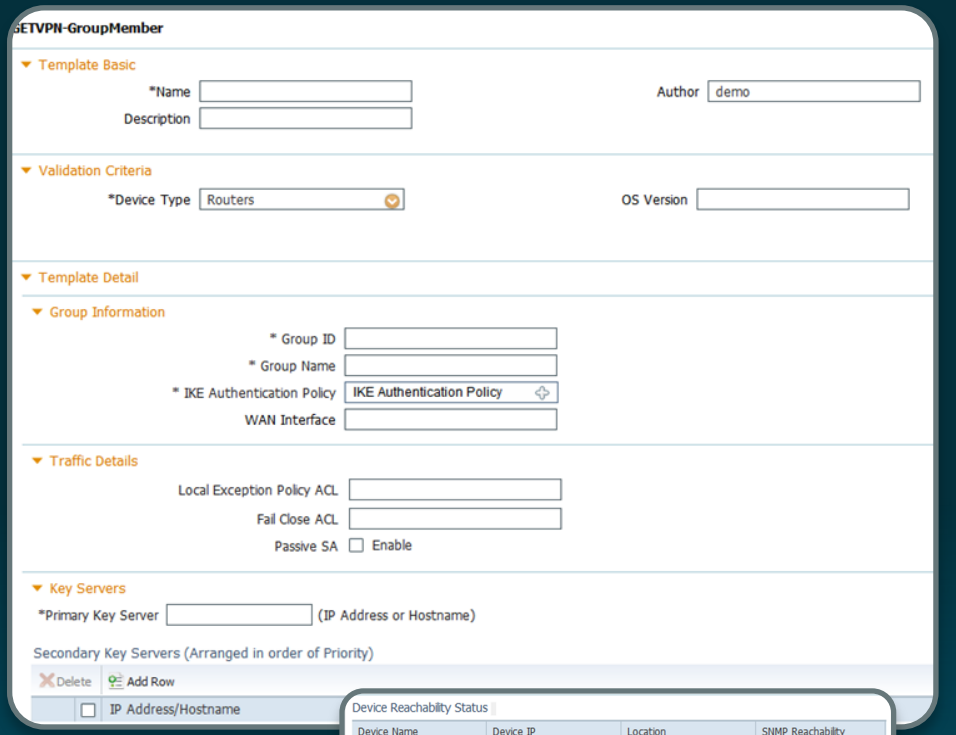
Configuration Templates

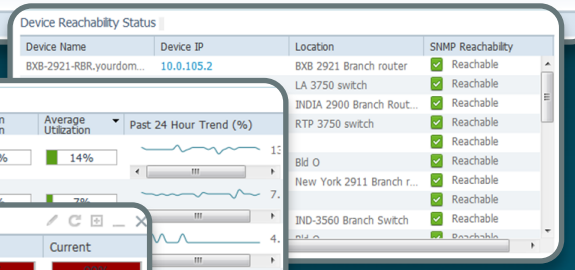


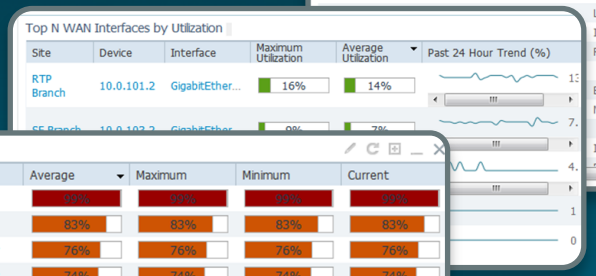
Monitoring Templates

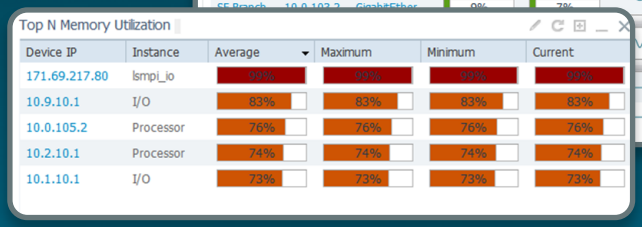


Example – GET VPN Group Member Configuration









Summary

Extremely Reliable, High Throughput Routers

Best offerings to help businesses implement their goals

The underlying core reliability, performance, routing, security and encryption features are highly regarded

All solutions are highly scalable and can be deployed with a single router in each branch

Feature-rich Secure WAN solutions

GET VPN – Fast, tunnel-less, ideal for MPLS
DMVPN – Easy to use, ideal for Internet
Supports Multicast and QoS
Many different deployment scenarios – Enterprise and SP

Easy-to-deploy

Simple-to-deploy; Zero-touch configuration for new branches

Next-Gen Enterprise WAN features are easy for customers to deploy with deployment guides and Cisco Prime

36

AVC and Performance Routing

Shabaz Yousaf

SRTG

Aims of this Session

Primary Aims:

Explain why AVC is important

A quick look at how AVC works, and why it is so useful
Application Performance (and Network Agility)

Performance Routing Introduction

A look at how PfR works, it's benefits and example scenarios
An introduction to the CLI!

Application Performance and AVC

ISR-ASR Engaged Solutions

3900

2951
2921

2911
2901

1941
1921

860
860VAE
880
890

Integrated Services Router

Cisco Prime

Reduce risk ■ Adopt new services ■ Easy to integrate

BYOD

WAAS
ScanSafe
FlexVPN
TrustSec

Cloud

Cloud Connectors
WAAS
ScanSafe
Application Visibility

Video

Medianet
Performance Routing
Application Velocity
CUBE

VDI

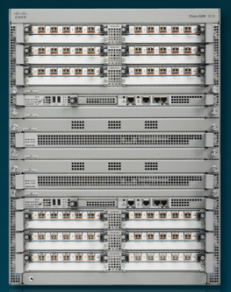
WAAS
GET VPN
Performance Routing

Internet of things

IPv6
Performance Routing

Network Systems

End-to-End Connectivity
Routing
Security
Encryption
Cisco Virtual Office



ASR1013

ASR1006

ASR1004

ASR1002-X

ASR1002

ASR1001

Aggregation Services Router

Why AVC

Many reasons; here are a sample!

Networks are more complicated

Business solutions and offerings must address the same fundamental concerns as ever – reliability and security and performance!!

Deeper insight is needed into what the network is being used for by users, and what performance are they getting?

Higher media consumption and cloud opportunities

Ensuring better application performance and better user experience

Deploy new applications and see the adoption and network performance dynamically

Respond to performance issues

Workforce evolution/ mobile workers, Mobile access

New productivity opportunities

Making the best use of throughput and connectivity

Maintain the user experience and app performance regardless of location

Better Application Performance

Application Visibility and Performance

Use WAN more effectively

Deep Packet Inspection - Better QoS through accurate traffic classification – prioritise corporate apps
DPI runs in the branch for excellent QoS
DPI runs at the WAN and Enterprise Edge for full visibility and QoS

Identify how the network is being used

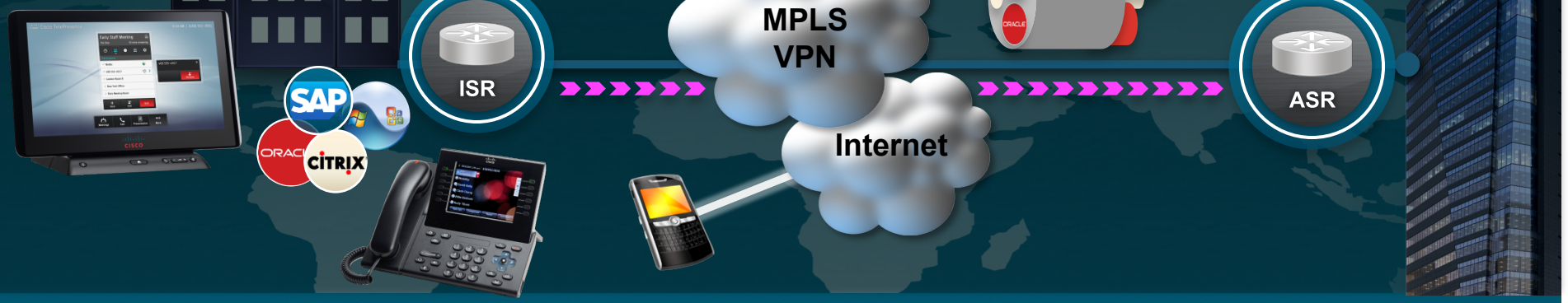
Branch , Head-end and Enterprise Edge capable of DPI
See where network growth needs to occur

Identify WAN, Internet and Application bottlenecks

Get detailed metrics showing network and server latencies
Branch and HQ data together provides accurate reports easily visible with Cisco Prime

Works with Application Acceleration/WAN Optimization and PfR

Compatible with WAAS Express and all WAAS options this year
Application-aware performance routing

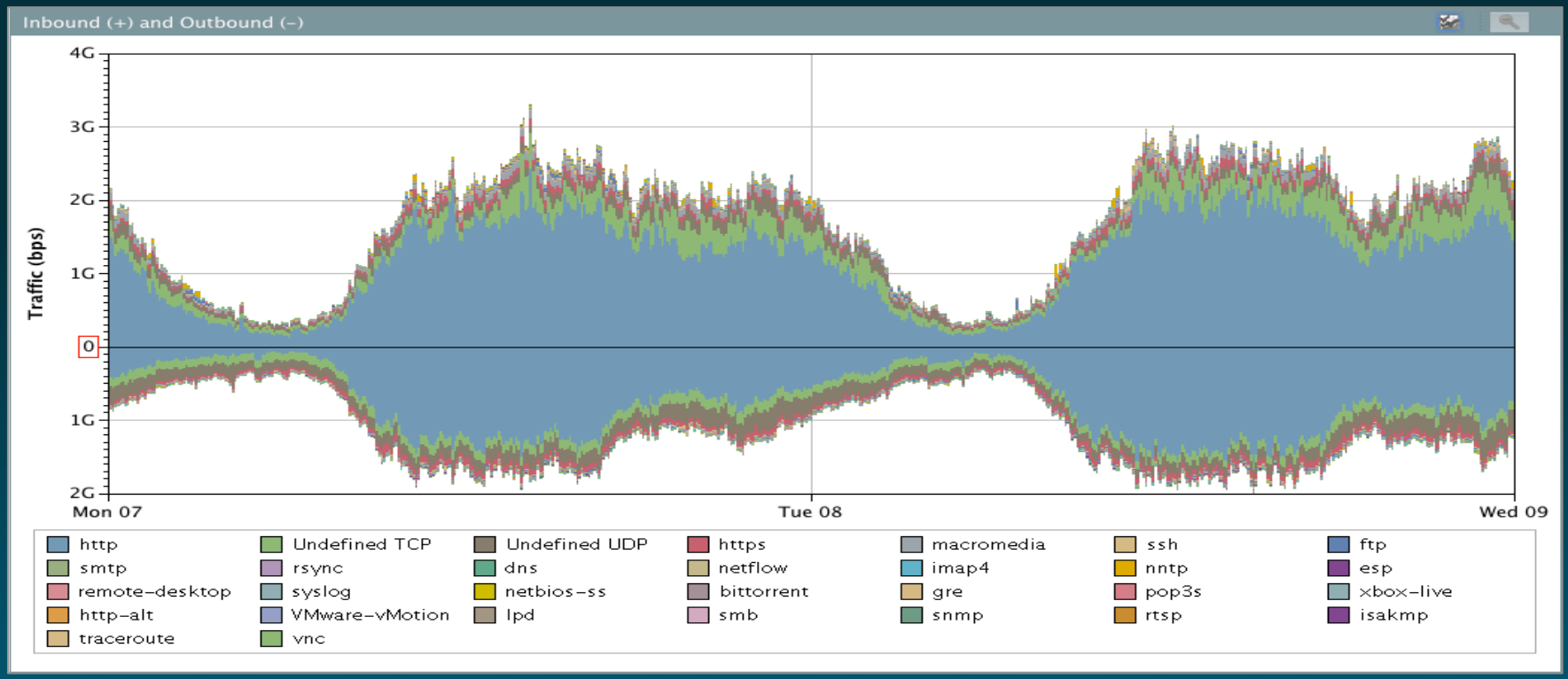


Use case - University

Application Visibility and Performance

Layer 4 (non-app-aware)

Overall Internet usage from a large university in the US



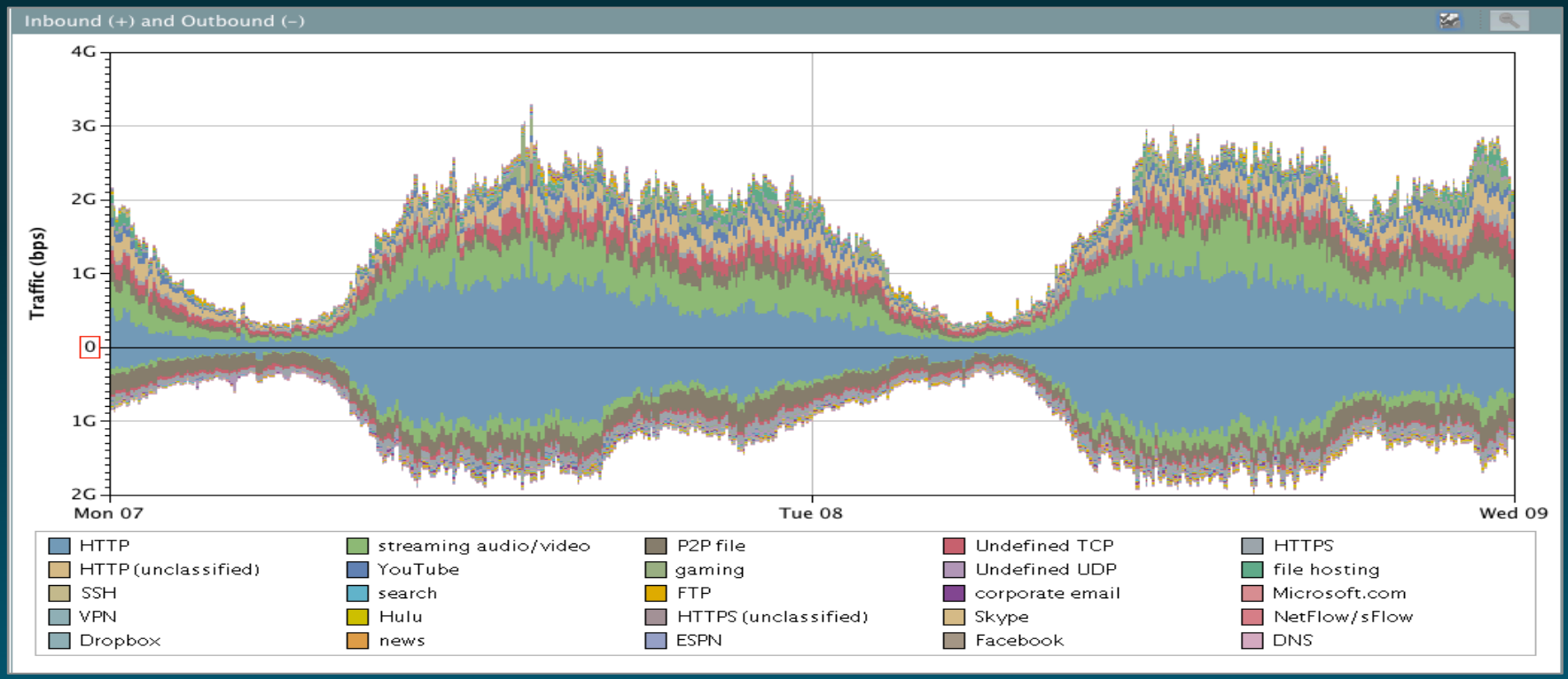
43

Use case - University

Application Visibility and Performance

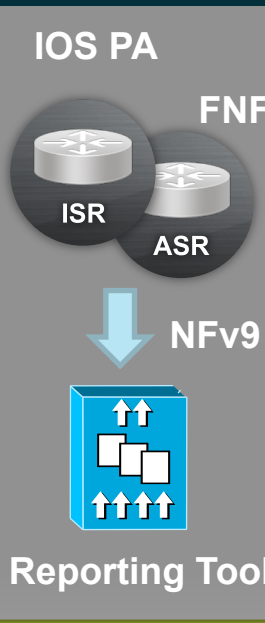
Layer 7 Inspection

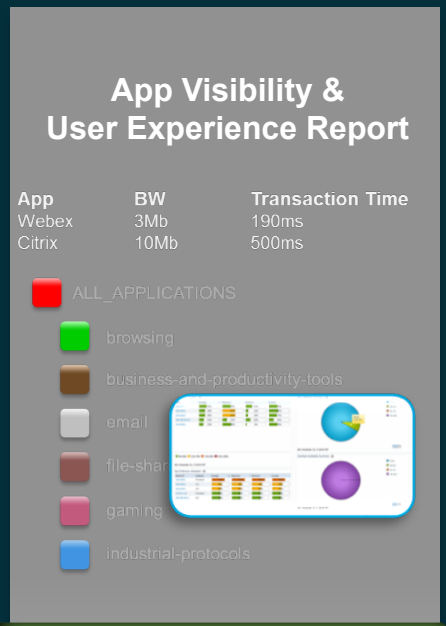
Overall Internet usage from a large university in the US

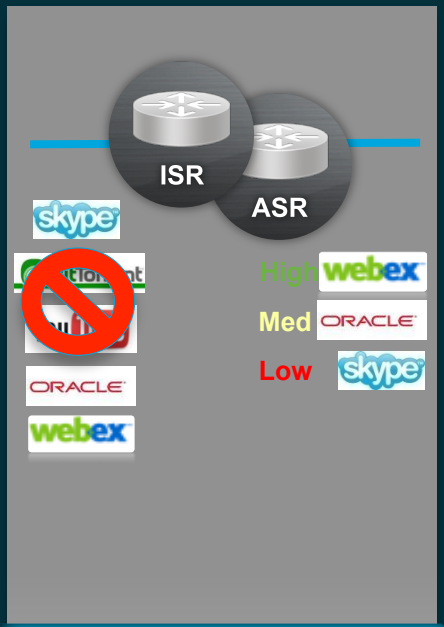


44

How AVC works







Deep Packet Inspection

DPI engine (NBAR2) identifies applications using L7 signatures

Perf. Collection & Exporting

ISR G2 & ASR collect application bandwidth and response time metrics, and export to management tool

Reporting Tool

Advanced reporting tool aggregates and reports application performance

Control

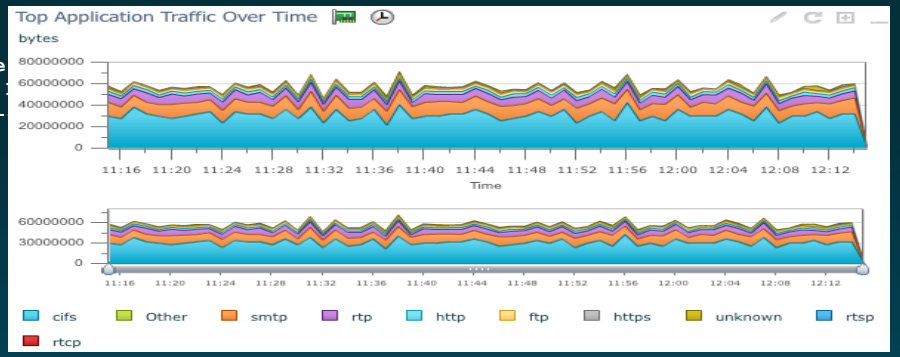
Use QoS or PfR to control application network usage to improve application performance

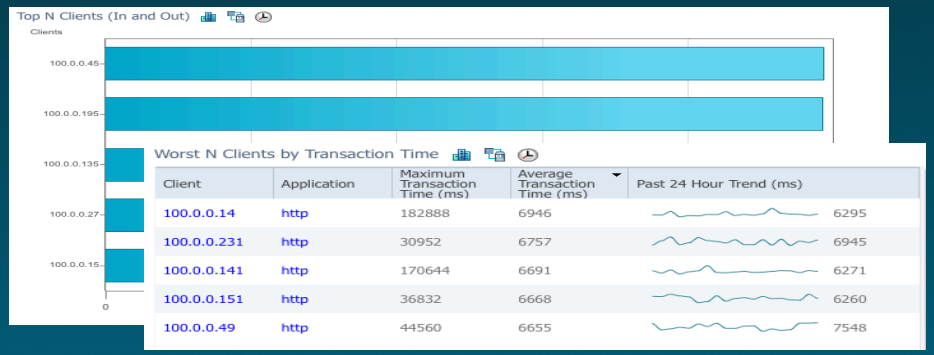
Application Visibility with NBAR2

- Example CLI

```
Router#show ip nbar protocol-discover top-n 10
 GigabitEthernet0/0/3
                         Input                  Output
                         -----                  ------
   Protocol              Packet Count           Packet Count
                         Byte Count             Byte Count
                         30sec Bit Rate (bps)   30sec Bit Rate
                         30sec Max Bit Rate (bps) 30sec Max Bit
   ----------------------- ------------------------ --------------
   sunrpc                135                    2799106
                         21850                  4237830347
                         0                      0
                         4000                   47720000
   ftp                   92340159               186761181
                         4989796991             263959173216
                         211000                 11160000
                         284000                 15170000
   netflix               67438860               84034631
                         51098349136            100709287113
                         2171000                4223000
                         3278000                6476000
   webex-meeting         45807530               163458047
                         2497543722             129842885217
                         115000                 5998000
                         152000                 7799000
   bittorrent            59667396               156155174
                         12768822744            103187176646
                         555000                 4715000
                         697000                 5077000
```

- Application Information is exported in FNF records. Reporting tool displays top client and server for particular applications





Application Visibility and Performance

Solution Detail

Branch and WAN aggregation

Cisco Performance Agent is part of the branch AVP solution
High levels of DPI can occur at the WAN aggregation point using the ASR 1000

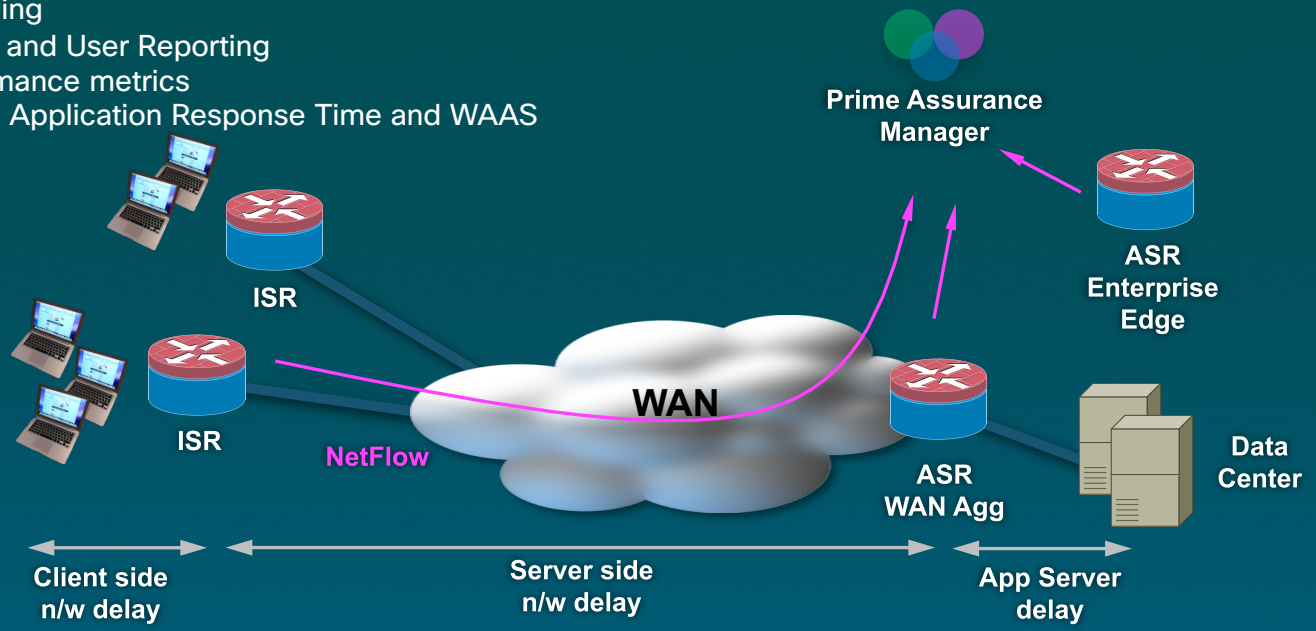
Cisco Prime Assurance Manager provides detailed reporting

Enterprise Edge

High levels of AVP can be achieved by using the ASR 1000

Capabilities

DPI across multiple packets to precisely determine the application
Traffic classification based on application
Traffic policing
Application and User Reporting
30+ performance metrics
- including Application Response Time and WAAS



WAN Optimization

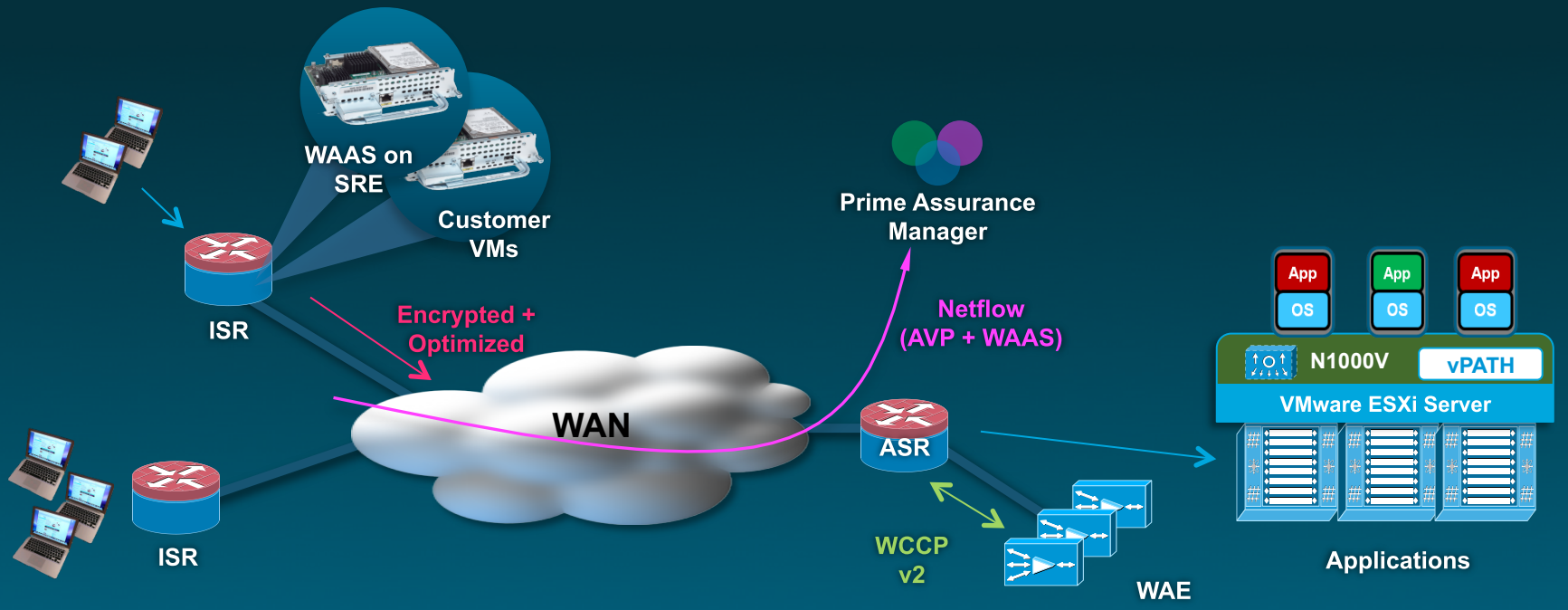
Example Deployment Scenario

DC options

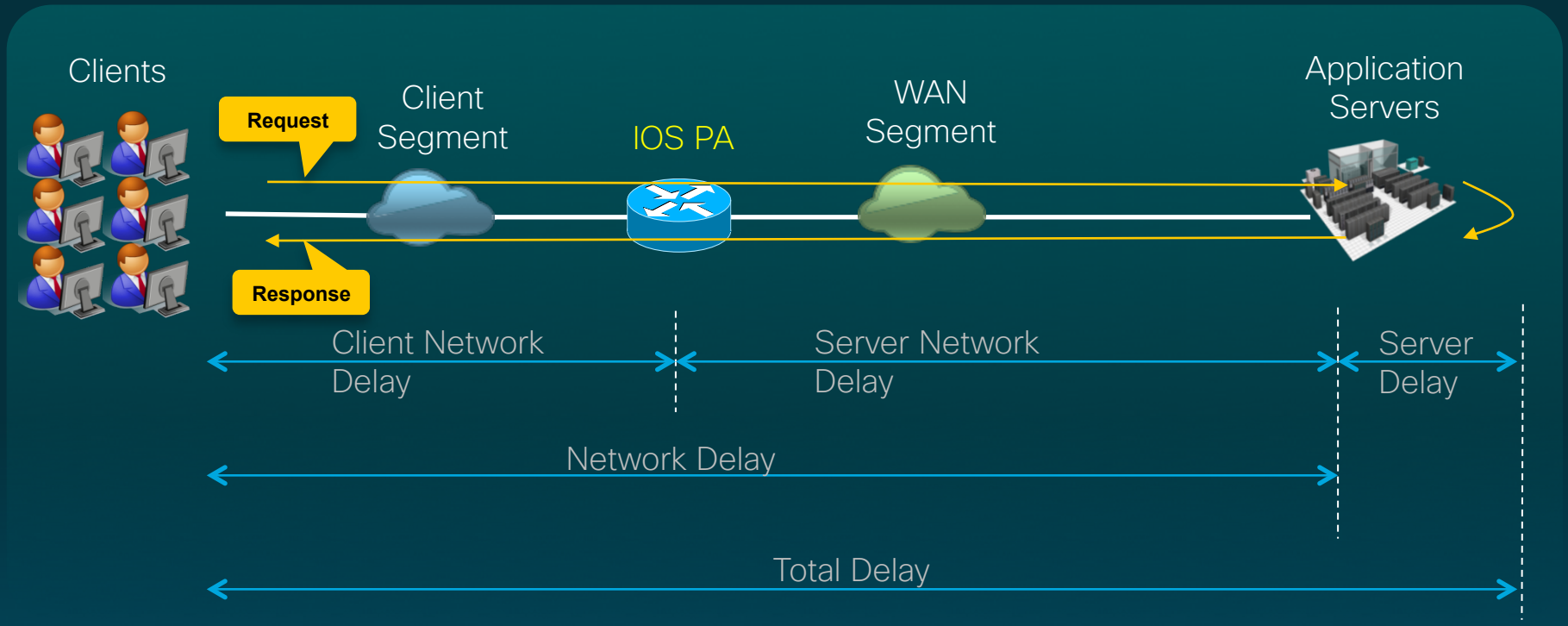
WAAS appliance connects to ASR 1000 using WCCPv2 with no changes to the network
Virtual WAAS (vWAAS) also possible on VM

Branch options

WAAS on SRE is the ideal option for branches
Alternative: WAAS Express runs in IOS and is good for branches with less traffic and have already been deployed
For large branches, an external WAE appliance can be used

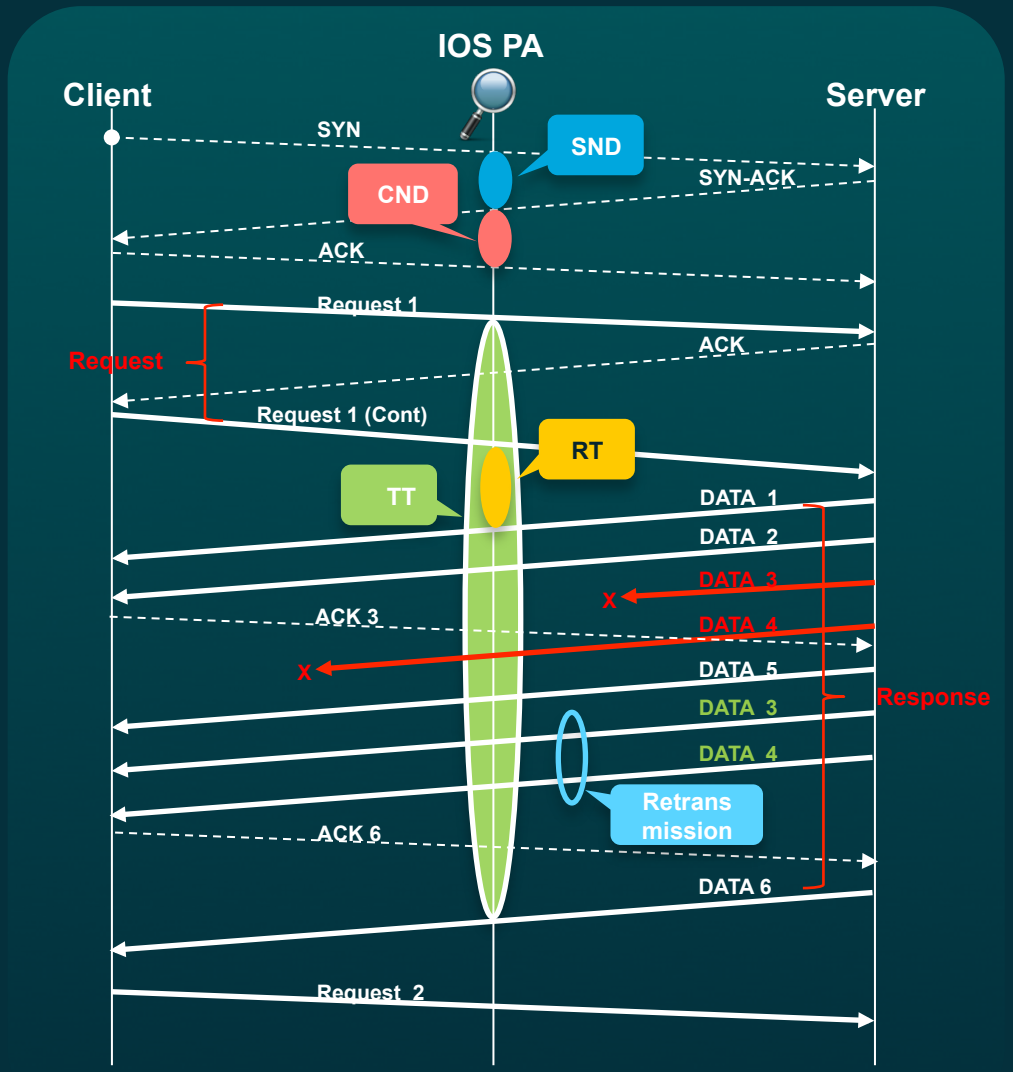


Per-application Latency Breakdown



- Separate application delivery path to client and server segments
- Server network delay is typically WAN delay
- Understands WAAS Express and provides proper latency breakdown

Understand ART Metrics Calculation



- Response Time (RT)
  - t(First response pkt) – t(Last request pkt)
- Transaction Time (TT)
  - t(Last response pkt) – t(First request pkt)
- Network Delay (ND)
  - ND = CND + SND
- Application Delay (AD)
  - AD = RT – SND

Quantify User Experience

Identify Server Performance Issue

List of Metrics reported by PA

Traditional FNF Metrics

- Application ID (from NBAR2)
- Client/Server Bytes
- Client/Server Packets
- Source MAC Address
- Input/Output Interface
- IP DSCP

WAAS Express Metrics

Input/Output Bytes

WAAS Connection Mode
TFO, TFO/LZ, TFO/DRE, TFO/LZ/DRE

Input/Output DRE Bytes

Input/Output LZ Bytes

ART Metrics

CND – Client Network Delay (min/max/sum)

SND – Server Network Delay (min/max/sum)

ND – Network Delay (min/max/sum)

AD – Application Delay (min/max/sum)

Total Response Time (min/max/sum)

Total Transaction Time (min/max/sum)

Number of New Connections

Number of Late Responses

Number of Responses by Response Time
(7-bucket histogram)

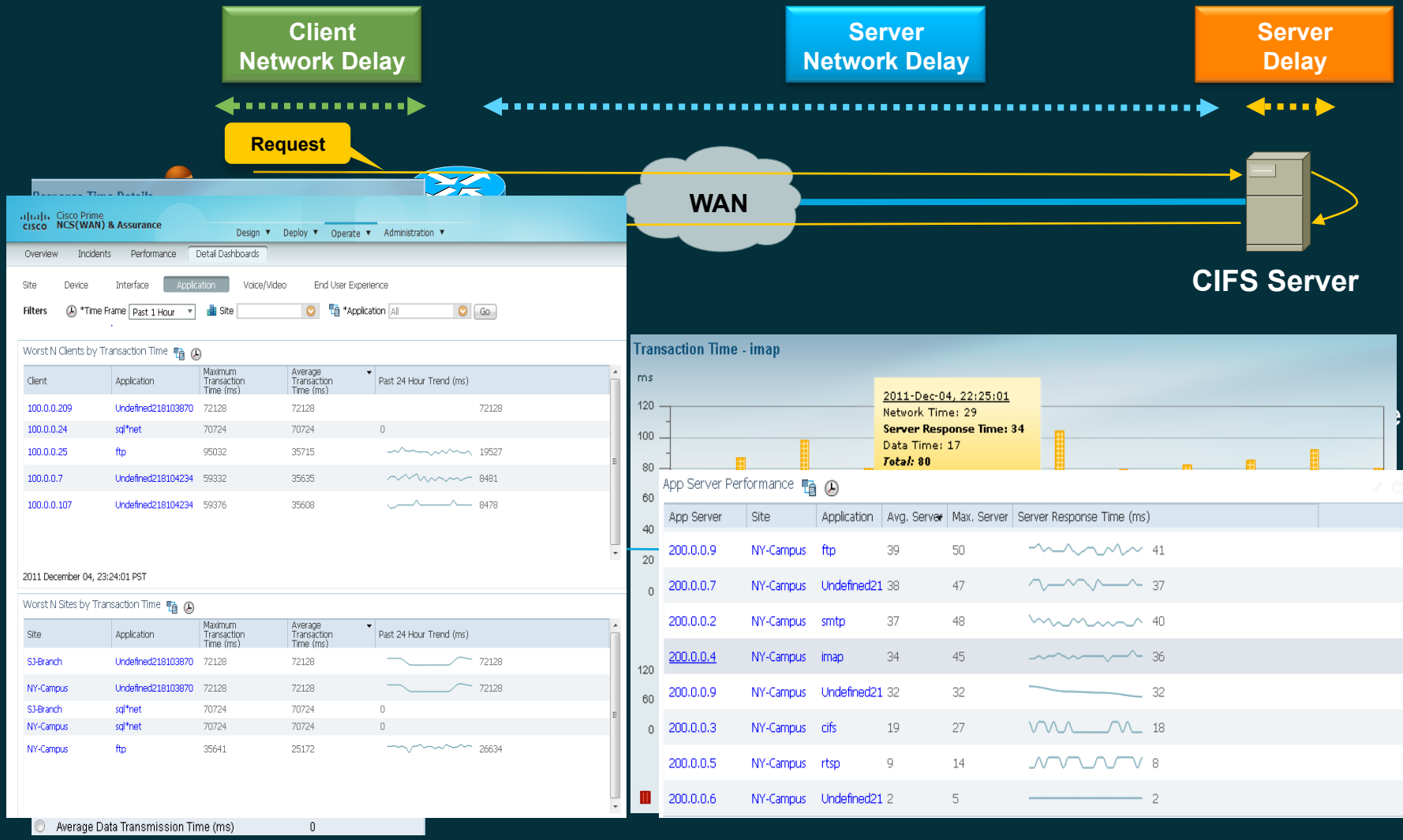
Number of Retransmissions

Number of Transactions

Client/Server Bytes

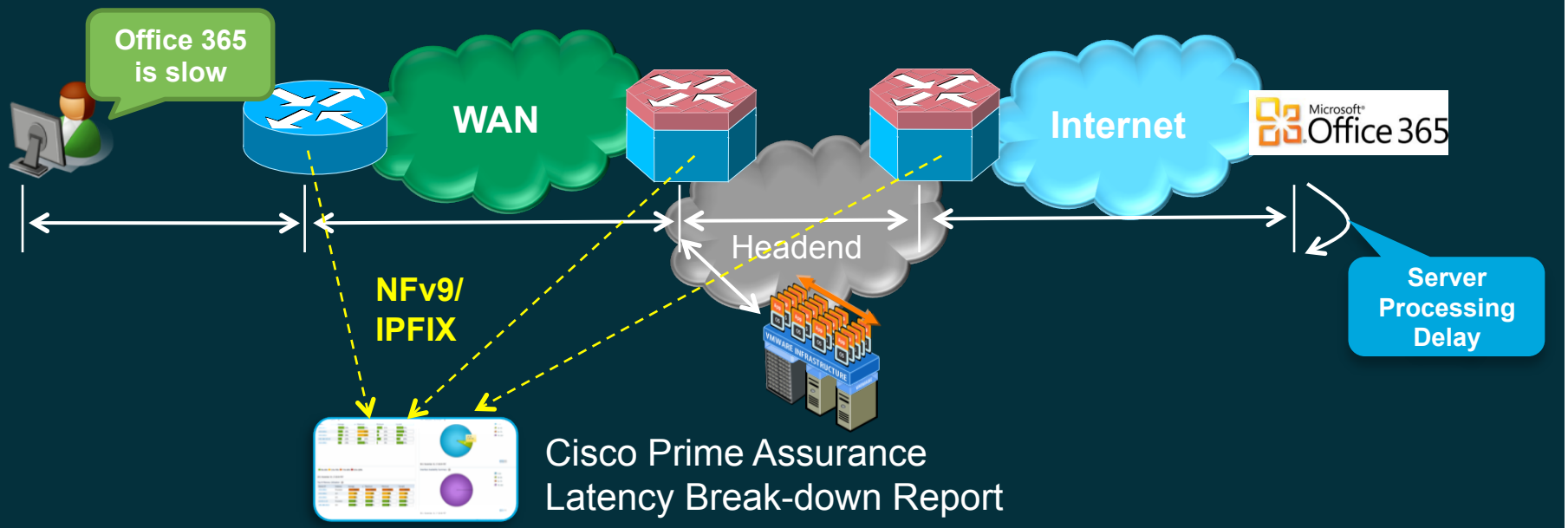
Client/Server Packets

Monitor User Experience with PA



Monitor Cloud Delivery End-to-end

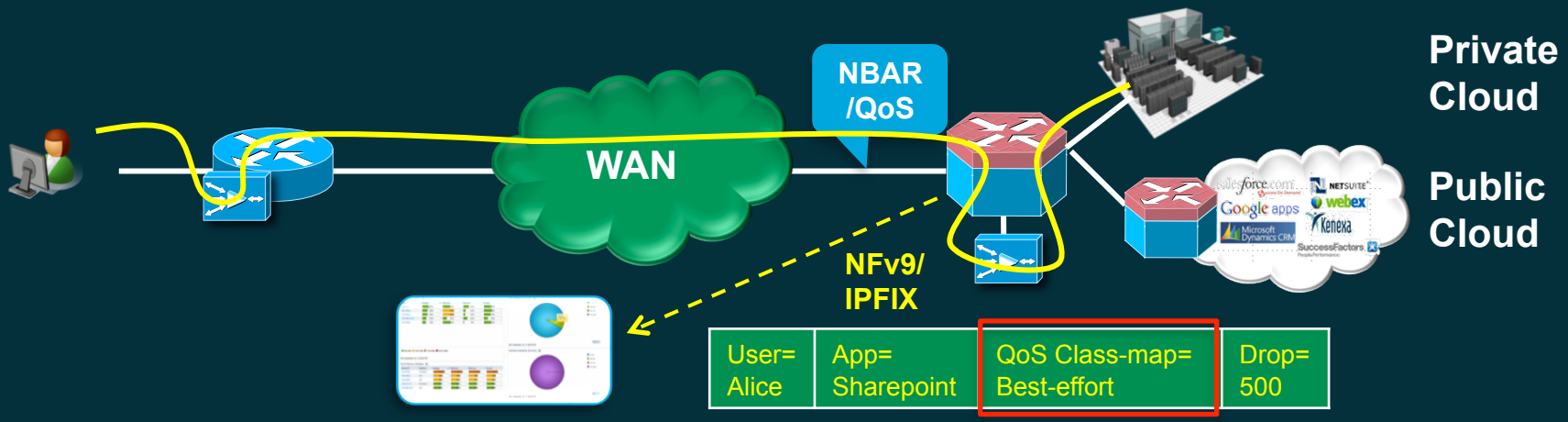
XE 3.8S
15.2(4)M



Application = Office 365	Branch = 5 ms	WAN = 50 ms	Headend = 10 ms	Internet = 100 ms	Server = 200 ms

- Faster problem resolution by providing break down network latency
- All devices report response time and latency metrics to PAM
- PAM correlates all metrics and provide end-to-end latency view of the application delivery (network too slow vs application too slow)

Enhance Network Visibility



QoS Class ID Export

XE 3.8S
15.2(4)M

- Provide association of network to application performance
- Is application delivered through the right QoS class?

Visibility into WAAS Optimized Flows

XE 3.8S

- Application Visibility on WAN with or without WAAS
- WAAS-awareness (pre and post optimization legs) performance metrics
- Application level QoS or PfR with or without WAAS

Performance Routing (PfR)

Better Application Performance

Dynamic Routing – AVP with Performance Routing (PfR)

Greatly reduced WAN costs

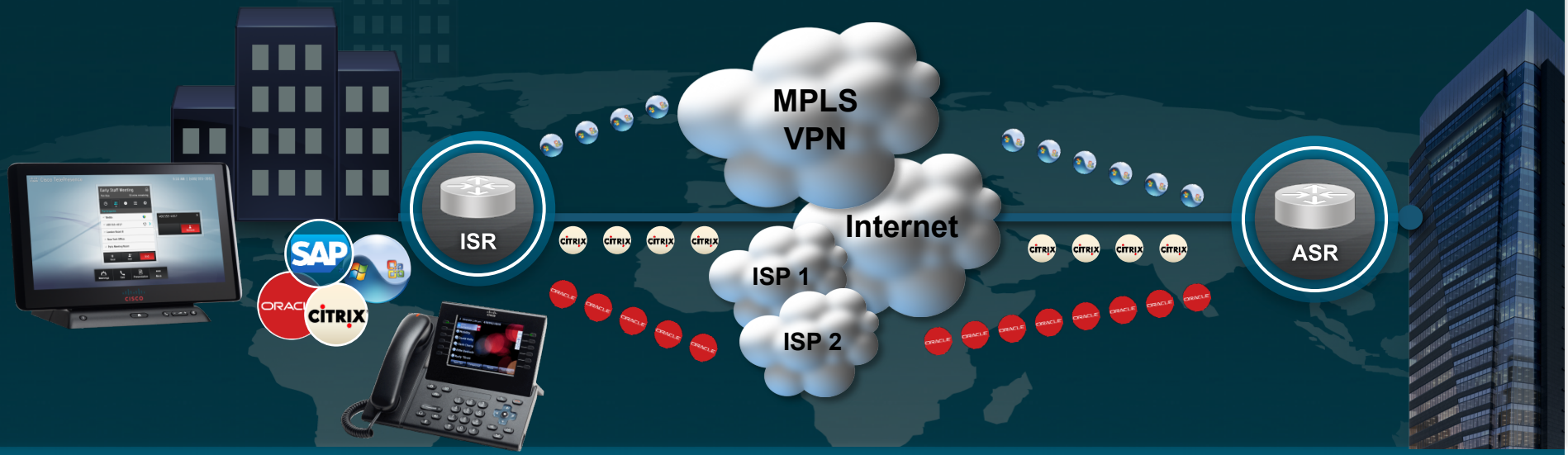
Use the most cost effective routes automatically while maintaining an SLA

Improved performance - Media and Application aware routing

Automatically routes voice and video quality over the best performing path - routes can be determined before the call is even made!

Phased deployment is possible

- Enable learning mode on just one router (e.g. one branch)
- When satisfied, instruct the router to enforce policies
- Happy with the settings? Deploy on all routers



PfR Benefits

- Automatically handle failures in the network
  - Route around failures in WAN or Internet connectivity
- Save costs
  - Route traffic according to least cost paths – ideal for Enterprise Edge or Branch connectivity
- Improved application performance
  - Maintain SLA, route traffic to maintain certain packet loss, jitter, MOS

Who is using it?

- Over 200 large customers using it today – Hotels, Banks, SPs, Enterprises

Performance Routing

Solution Detail

Example Scenarios

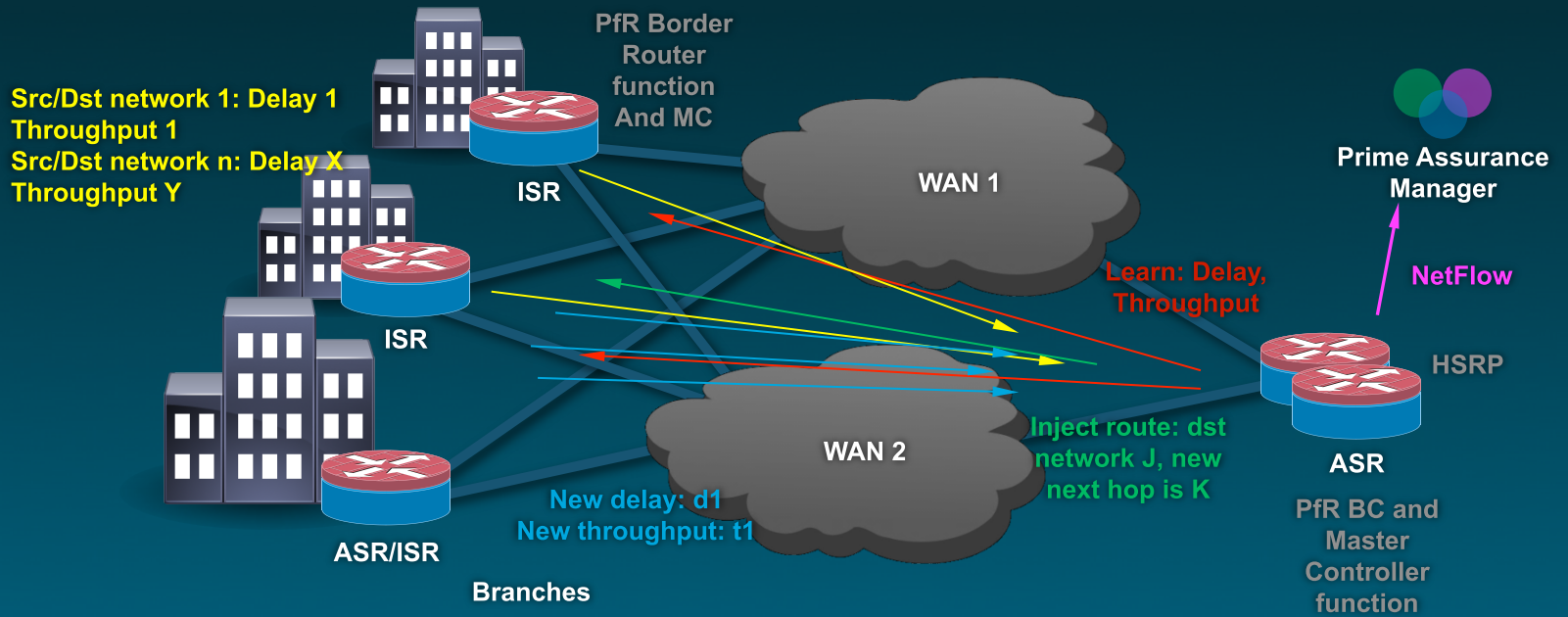
Branches connected to more than one link, e.g. MPLS VPN and Internet via DSL, or two DSL, etc
Head end connected to multiple links or Enterprise Edge connecting to multiple providers/links

How it works

■ ■ Master Controller (which can be the same device as the Border Router) sends a message to the BRs to collect statistics and send them to the MC

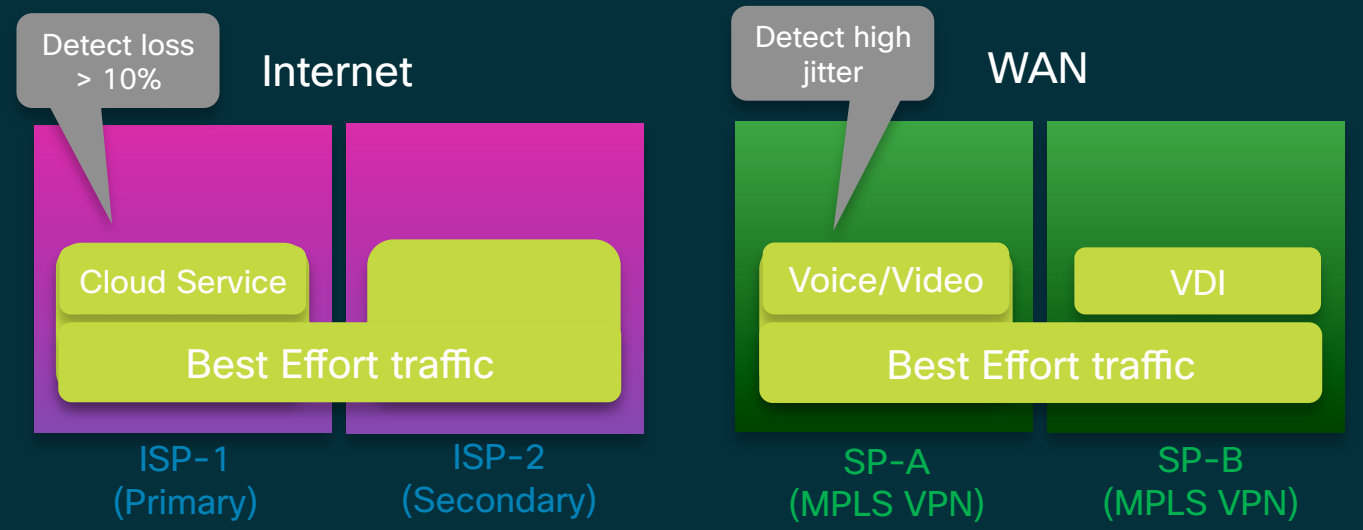
MC sorts information from all the BRs based on the policy (e.g. policy to reduce latency), and picks the worst performers

■ ■ Once MC has decided that a route may need to be enforced to improve the worst performer, it will tell that BR to repeatedly send stats, and then will insert the route to the BR whilst monitoring the stats – this cycle is a loop for optimizing the performance!



AVC and PfR Examples

Protecting Critical Applications



Cloud Service and Load Balancing Policy

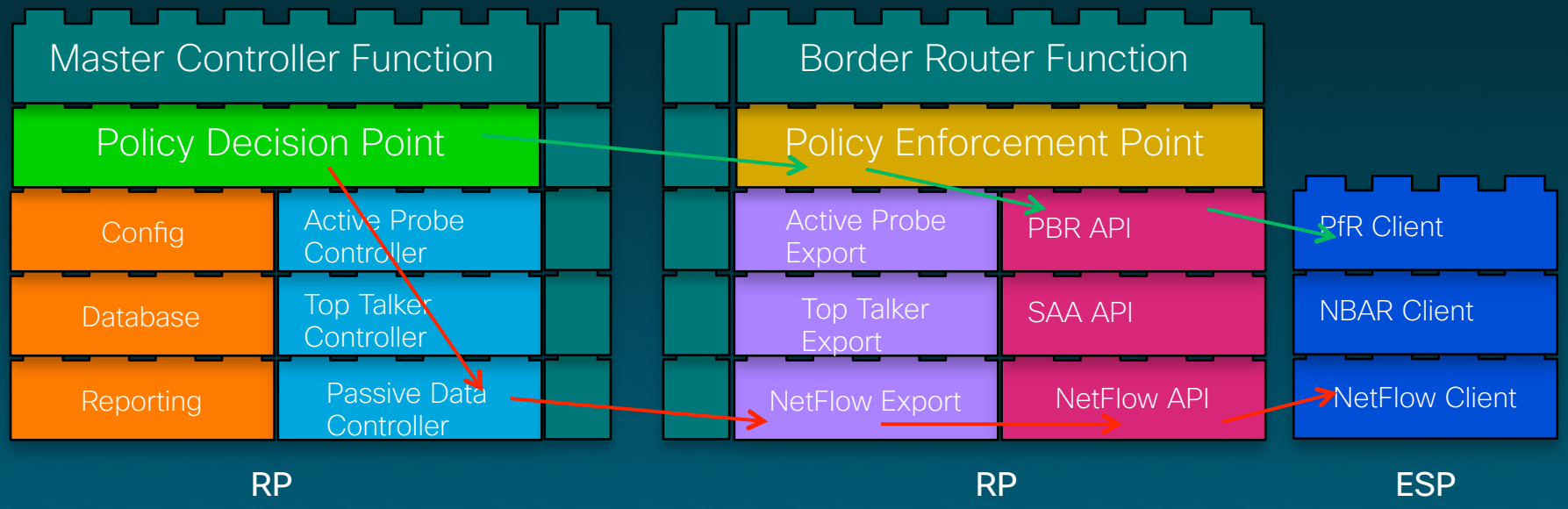
- Protect business Cloud applications from Internet brownout, Loss <10%
- Cloud Service preferred path – ISP1
- Maximize all ISP bandwidth by load sharing all other Internet traffic

Multimedia and Critical Data Policy

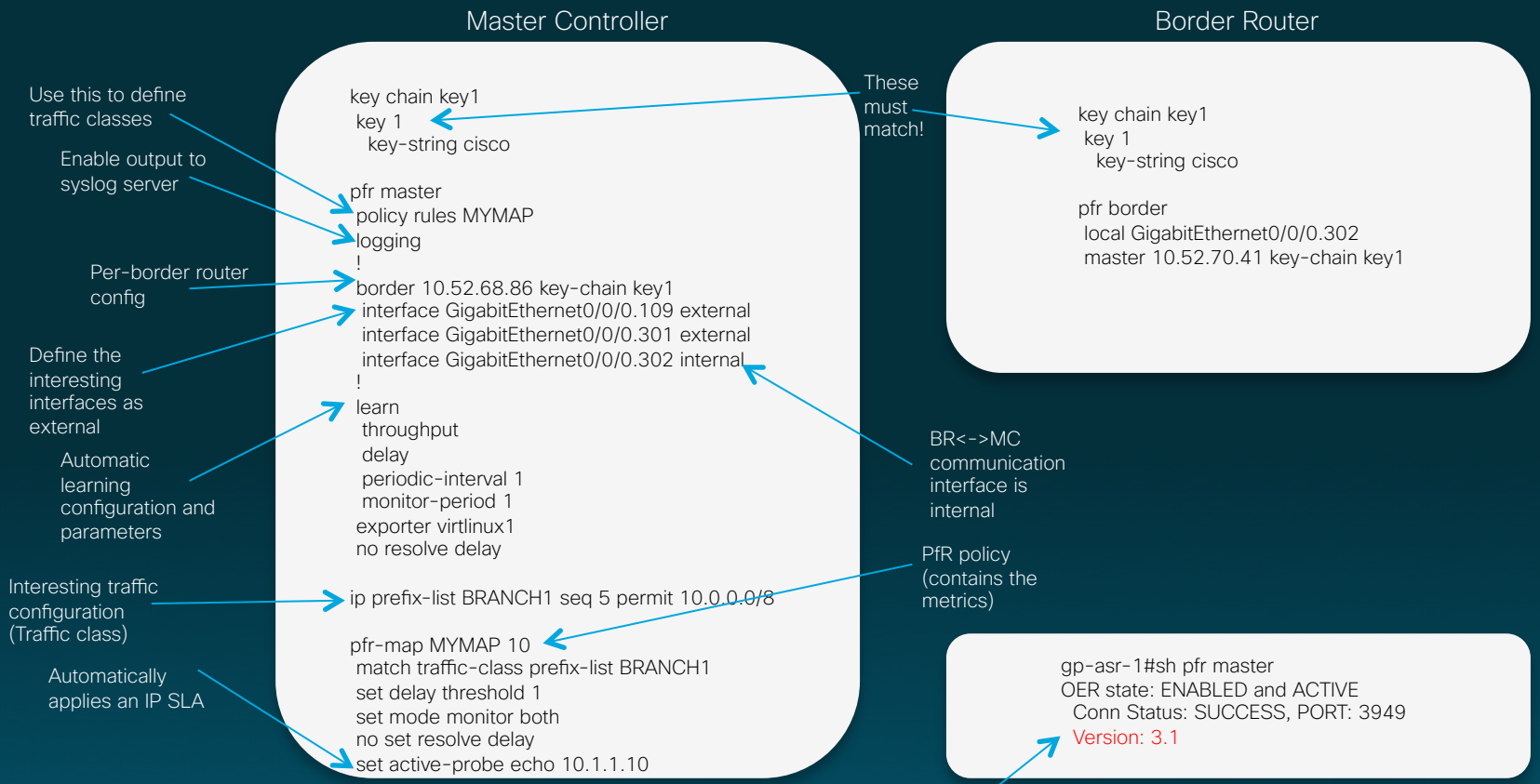
- Protect voice and video quality, Latency < 200ms; Jitter < 30ms
- Protect VDI applications from brownouts, i.e. Loss < 5%
- Voice & Video preferred path SP-A
- VDI preferred path SP-B
- Maximize utilization by load sharing

PfR Building Blocks

- TCP/IP comms between MC and BR
- High performance – QFP-accelerated NBAR2, NetFlow. TCAM for reroute policies
- Example message flows:
  - Red: Setting/querying statistics via NetFlow
  - Green: Programming in a new route



Example configuration



- Note: Double-check the IOS and IOS-XE images!

  When configured for Master or Border, the 'show pfr master/border' command will indicate a version number; the version integer numbers must match, and the MC version fractional number must match or have a higher value.

Performance

- Testing is currently underway!
- Active probe intervals of 10-15 seconds are typical, to rapidly detect any issues
- Aggregation site MC: Number of peerings (a branch may have two peerings)
  - RP1: 500 (each with 5 probes)
  - RP2: 2000 (each with 5 probes)
- PfR Policy (pfr-map) entries MC:
  - RP1: 2000
  - RP2: TBD
- Branch site BR (or BR+MC): Number of external interfaces
  - Tested: 5
  - Future: 120
- Probes scaling BR (or BR+MC)
  - Fast (4sec interval):
    - RP1: 100
    - RP2: 400
  - Normal:
    - RP1: 5000
    - RP2: TBD

What is supported?

- MC and BR – supported on both ASR and ISR G2
- Prime support (Prime Infrastructure and Prime Assurance)
  - Available in Prime Infra release 2.1 (End of CY12 / Q1CY13)
  - Note: Configuration can still be deployed with Prime NCS(WAN) templates today
- Performance improvements
  - Available in IOS-XE release 3.8 (Nov 2012)
  - Ability to support 1000 branches per MC

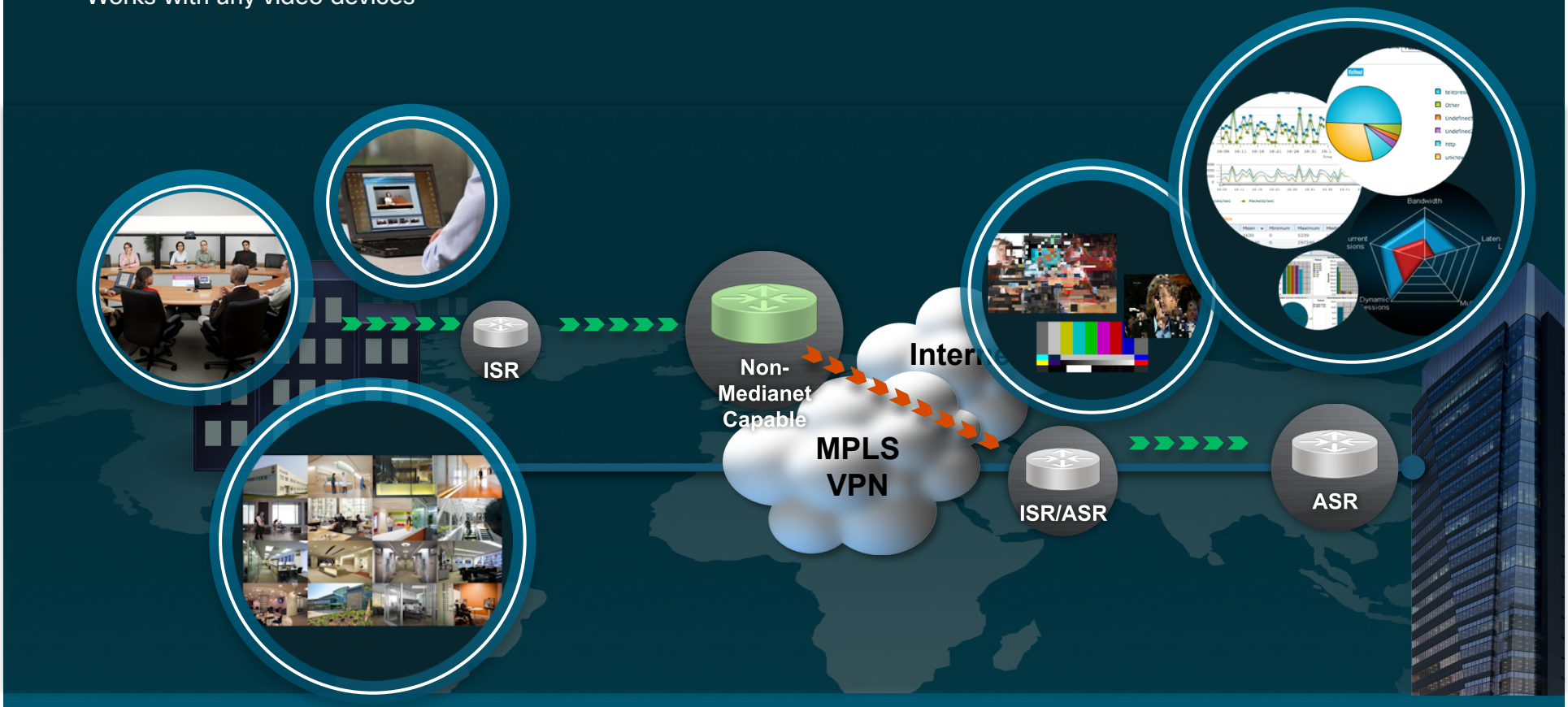
MediaNet

Voice and Video Enablement - Medianet

End-to-end worry-free video enablement
Plan for, detect in advance and solve video issues before they are even reported

Future-proof
Works with any video devices

Easy and Cost-effective
Built-in router based service
Eliminate the need for probes, hardware and on-site visits



Medianet

Solution Highlights and Features Overview

Highlights

Rapidly becoming an essential solution for any customer looking to grow their use of video apps

Extensive reporting capabilities; many thresholds and combinations can be set

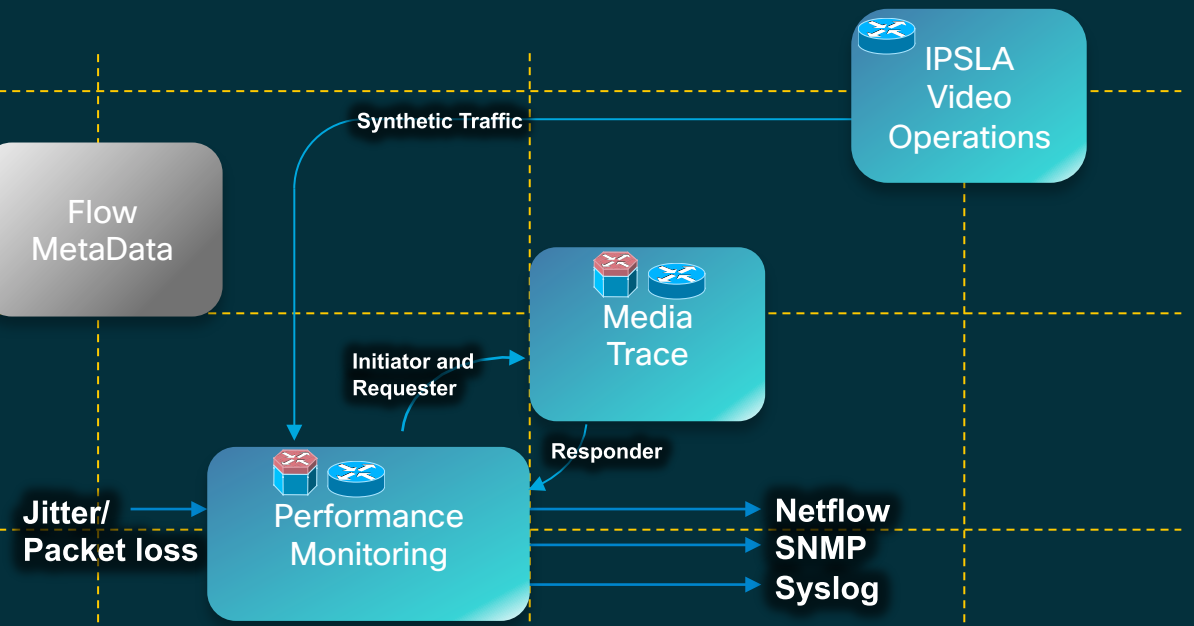
Cisco Prime Assurance Manager can collect and display the results

Ability to automate tasks (e.g. use a server to send an e-mail alert whenever a syslog message is generated if a security camera video stream is lost)

Media Awareness
Detection and Optimization of different media and applications

Endpoint aware
Automatic detection and configuration

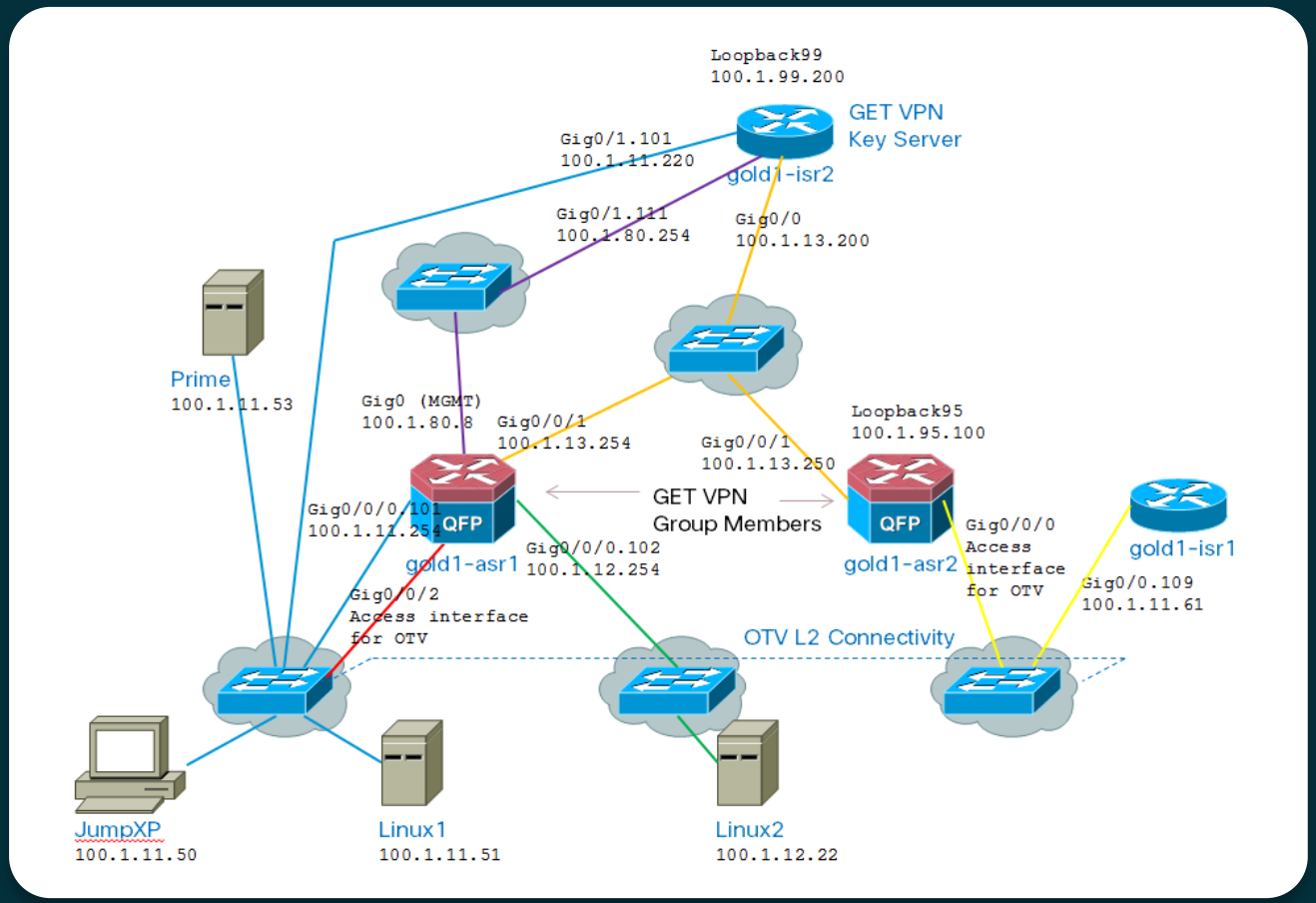
Network Aware
Automatically respond to changes in devices and service availability



Visibility | Diagnostics | Network Assessment

Labs

- Accessible via the Partner Portal



Summary

- Highly efficient DPI engine – a level of performance and accuracy that was previously only available to large Service Providers
- Identifies 1000+ apps, and is customizable
- Excellent application performance – QoS preserved and best routing
- Detailed reporting
- PfR – Dynamically maintaining a good application experience. Forward-compatible with Private Cloud deployments

Thank You!