Cisco IOS Software Release 15.0(1)M

Steven Koretsky

Product Manager

Network Software and Systems Technology Group

October, 2009

Agenda

- Cisco IOS Software Release 15 M and T
- Introducing Release 15.0(1)M
- Cisco IOS Packaging
- Release 15.0(1)M Numbering, Support Lifecycle, and Migration Considerations
- Summary

Cisco IOS Software Release 15 M and T

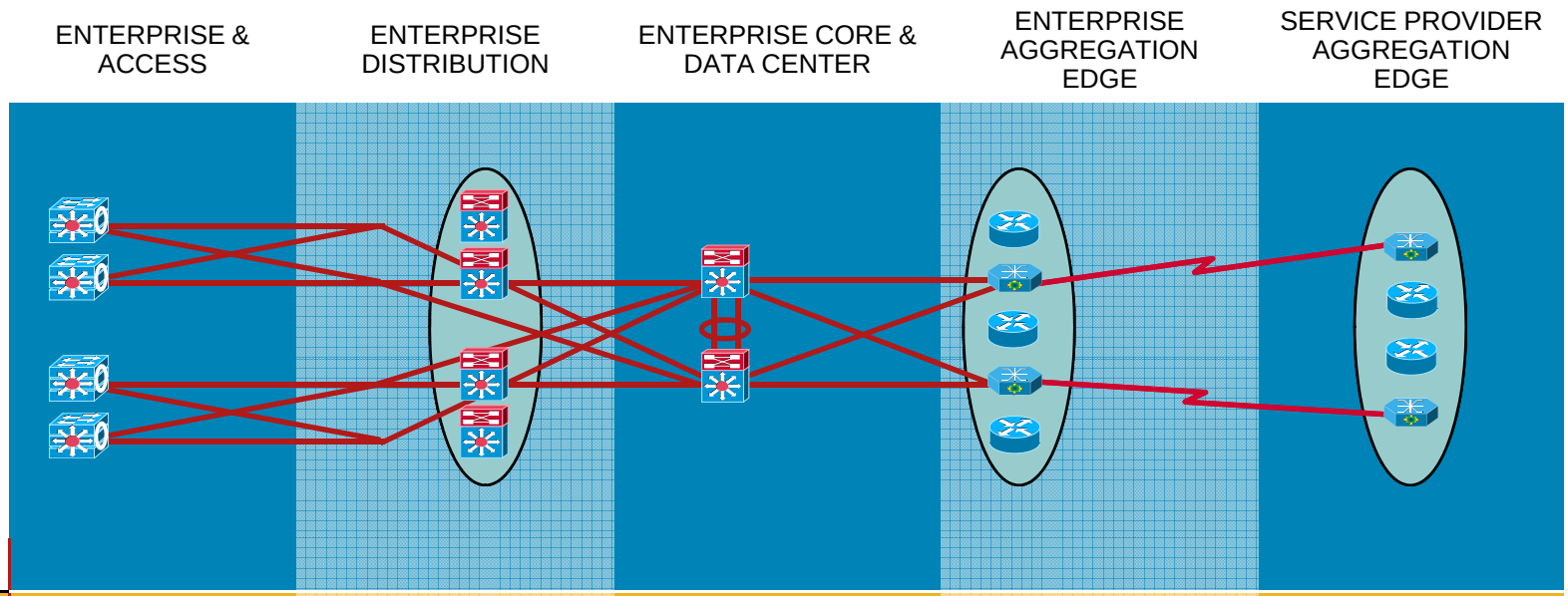
Extending Security, Voice, MPLS, and IP Services

Integrates a portfolio of new capabilities, including security, voice, and IP services, with powerful hardware support

Delivers advanced services for Enterprise and access customers

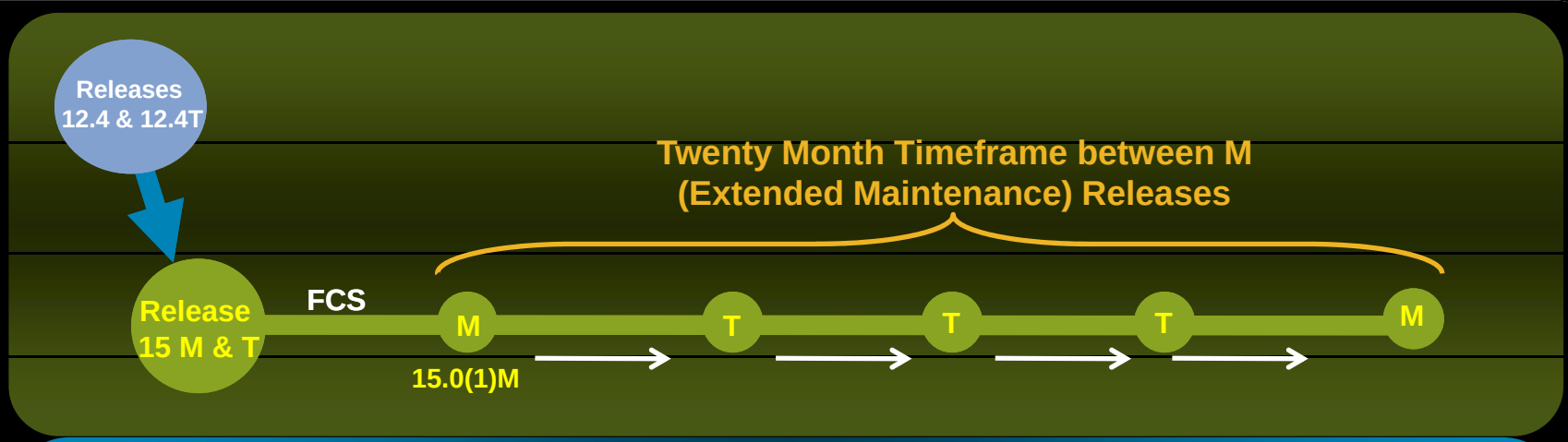
Series of regularly scheduled individual technology releases, each of which delivers aggregate functionality via its predecessor, and introduces new technology and features

Release 15 M and T Within the Cisco IOS Software Release Portfolio



	ENTERPRISE & ACCESS	ENTERPRISE DISTRIBUTION	ENTERPRISE CORE & DATA CENTER	ENTERPRISE AGGREGATION EDGE	SERVICE PROVIDER AGGREGATION EDGE
Release 15 M and T Enterprise & Access, Managed Services	✔				
Release 12.2SE & 12.2SG Mid-range and Low-end Ethernet LAN Switching	✔	✔			
Release 12.2SX High-end Ethernet LAN switching, Metro Ethernet	✔	✔	✔	✔	✔
Release 12.2SR Metro Ethernet, MPLS PE				✔	✔
IOS XE Software (ASR 1000) service provider edge and enterprise aggregation				✔	

Cisco IOS Release 15 M and T- Highlights



- Feature inheritance and platform support from 12.4(24)T and 12.4 Mainline
- M (Extended Maintenance) releases delivered on a more frequent basis, enabling customers to qualify, deploy, and remain on a release longer with active support
- T (Standard Maintenance) releases ideal for the very latest features & hardware support before the next M release becomes available
- Rebuilds of Release 15 M and T for ongoing bug fixes
- **Release 15.0(1)M is the first release**

FCS = First Customer Shipment

15 M and T Release Positioning

M Release

- **Ideal for long-term maintenance**
- **44 months support**
- **Comprehensive feature benefits**

(Previous, incremental & enhancements with new hardware support)

T Release

- **Short deployment cycle with latest features and hardware support**
- **18 months of support**
- **Incorporates features and hardware support delivered in previous M and T releases**

Cisco IOS Software Release 15 M & T

Key Features in Release 15.0(1)M

IP Routing

- BGP Graceful Restart (GR) Per Neighbor
- BGP RT Changes Without PE-CE Impact
- Graceful OSPF Restart (RFC 3623)
- Graceful Restart for OSPFv3 (Awareness)
- IS-IS VRF Support
- IS-IS MIB
- IS-IS Support for BFD
- LDP/IS-IS Sync and LDP Autoconfig
- OSPF Graceful Shutdown
- OSPF TTL Security Check (GTSM)
- PfR PIRO
- PfR EIGRP/mGRE
- SAF
- Static Routes Support for BFD
- MPLS VPN – InterAS option B
- MPLS VPN – BGP local convergence

Embedded Management

- Flexible NetFlow & NBAR Integration
- SNMP Proxy Event Detector
- SNMP Notification Event Detector Enhancement
- Logging Action Enhancements
- EEM policy description display
- EEM policy AAA bypass
- Multiple CLI execution in one TCL command

New Hardware

- Integrated Services Router 1900
- Integrated Services Router 2900
- Integrated Services Router 3900
- ISR 3800 NO VPN

Cisco IOS Software Release 15.0(1)M

Security

- GET VPN VRF-Aware GDOI on GM
- IOS IPS with Lightweight Signatures
- Ability to disable volume-based ipsec lifetime rekey
- DMVPN Enhancements

High Availability

- BFD for WAN interfaces
- VRF-aware BFD
- BFD Static Routes Support for IPv4

IP Multicast

- IGMP Static Group Range Support
- IP Multicast Load Splitting – ECMP using S, G and Next-Hop
- Multicast Address Group Range Support
- Multicast MIB VRF Support
- Multicast VPN Extranet Support
- Multicast VPN VRF Select
- PIM Triggered Join

Voice

- Cisco Unified Border Element (CUBE) Support for SRTP-RTP Internetworking
- CUBE support for Out-of-dialog SIP OPTIONS Ping messages to monitor SIP Servers
- UC Trusted Firewall Control Version 2
- UC Manager Express (UCME, Voice Gateways and Cisco Unified Border Element (CUBE) support for Service Advertisement Framework (SAF)

Call Admissions Control

- VRF lite aware RSVP
- RSVP Fast Local Repair
- RSVP Interface-based Receiver Proxy

Agenda

- Cisco IOS Software Release 15 M and T
- Introducing Release 15.0(1)M
- Cisco IOS Packaging
- Release 15.0(1)M Numbering, Support Lifecycle, and Migration Considerations
- Summary

Introducing Release 15.0(1)M

Cisco IOS Software Release 15.0(1)M

- **First in a series of individual Cisco IOS Release 15 M and T releases, each of which delivers aggregate functionality via its predecessor, and introduces new technology and hardware support:**
  - **Service Advertisement Framework (SAF), enabling network applications to dynamically discover the existence and configuration of other networked application and services.**
  - **Flexible NetFlow and NBAR integration, combining the strengths of both features to provide layers 2-7 per-flow application visibility and statistics.**
  - **Embedded Event Manager Version 3.1, which introduces significant enhancements for event detection, notification mechanisms, and command execution capabilities.**
  - **Support for the Cisco ISR G2 1900, 2900, and 3900 Series Routers, helping businesses and service providers transform the branch office experience and better enable rich media applications, such as hi-definition video and on-demand services.**

Cisco Integrated Services Router Generation 2 (ISR G2)

Hardware

erformance, Scalability, Availability

860, 880, 890

1941, 1941-W

2901, 2911, 2921, 2951

3925, 3945

Virtual Office

Secure Mobility

Customizable Applications

Secure Collaboration

Scalable Rich-Media Services

Enhancing the Customer Experience

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

ISR G2 Benefits

Hardware

Pay As You Grow

Services Ready Engine for Applications

Universal IOS Images

Service Performance Engine on 3900

Architectural Evolution

Multi-Core Processors

Multi-Gigabit Fabric

2x to 5x+ Performance Increase

Energwise

Services Integration

Medianet Ready Branch

Virtualized Branch Services(AxP)

GE Switch Modules

802.11n Wireless

Investment Protection

Broad support for existing ISR modules

Rich IOS feature support

Extensive NMS support

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

ISR G2 Positioning

Hardware

Cisco IOS Software Release 15.0(1)M

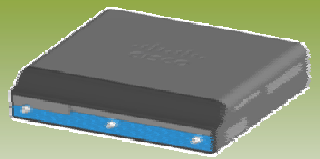
Performance and Services Density

802.11n 3G

860, 880, 890

802.11n

1941, 1941-W



2nd SM Slot on 2951

2901, 2911, 2921, 2951

Modular SPE Dual PS

3925, 3945

High Density and Performance for Concurrent Services

Embedded, Advanced Voice, Video, Data and Security Services

Embedded Wireless, Security and Data

The Integrated Services Router Portfolio

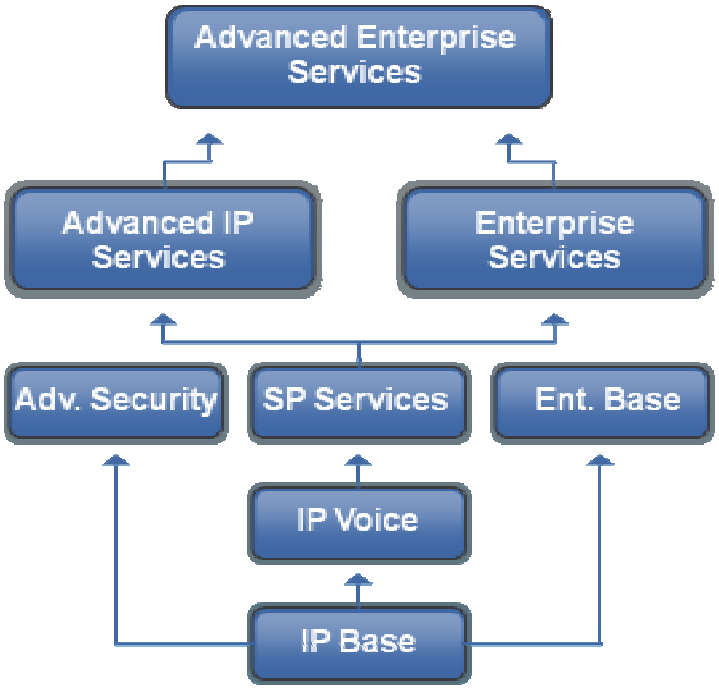
Small Office and Teleworker	Small Branch	Medium to Large Branch

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

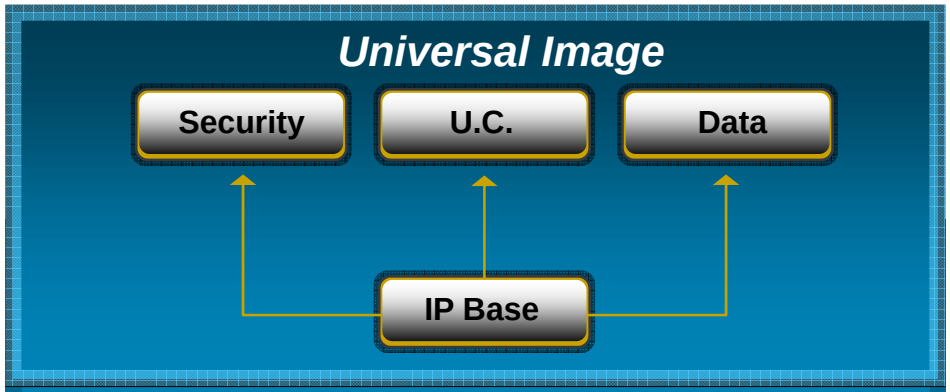
ISR G2 IOS Software Activation & Universal Image Support in Release 15.0(1)M

Hardware

Existing ISRs



ISR G2



- **Simplified Software Management**

  A single IOS Universal Image will ship with all ISR G2 platforms

  Four Cisco IOS enforceable licenses enable full suite of functionality that were previously offered in eight images

- **Less Costly Software Upgrades**

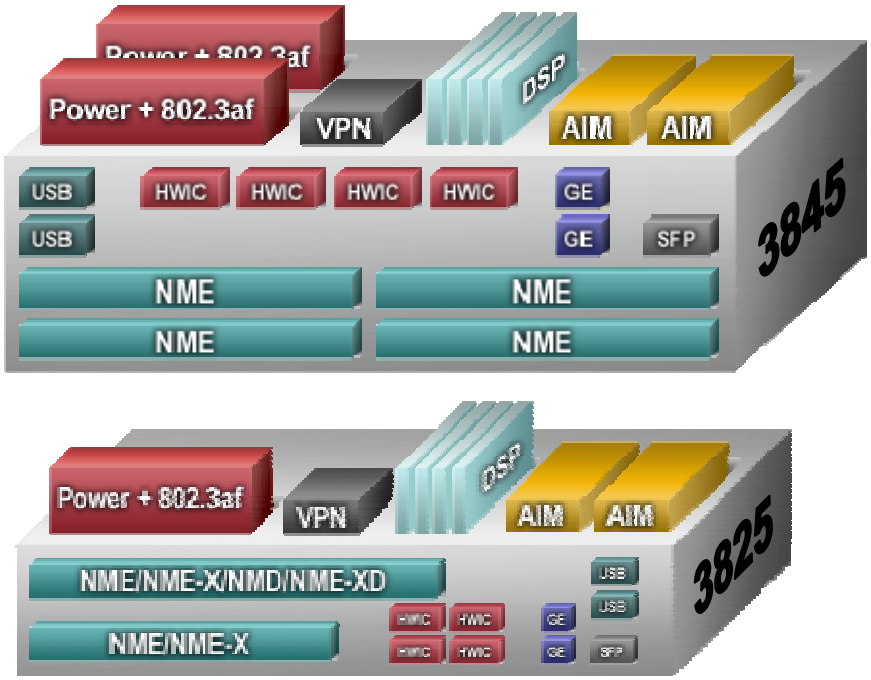
  Cisco IOS feature upgrades can be done by enabling a new license key, reducing the need for truck-roll to remote offices

- **Enable Development of New Software Based Business Models**

  Services on Demand—purchase upgrades as you need them via Cisco licensing

C3825-NOVPN and C3845-NOVPN Routers

Hardware



	C3825-NOVPN	C3845-NOVPN
Performance with Services	½ T3	1 T3
NME Slots	2	4
HWIC Slots	4	4
Dual Internal Power Supplies	N/A	Yes
Default/Max. Memory	256MB / 1G	256MB / 1G

- **New 38xx SKUs for NON-VPN Solutions**
- **Highest-Density, Maximum Performance Services Integration**

  Security: Threat Defense features , **No support for VPN Payload and Secure Voice to adhere to US Export compliance.**

  Voice: Highest densities for analog/digital voice support; CCME support for up to 250 IP phones

  Highest performance for maximum concurrent services at up to T3/E3 rates

  Integrated GE ports with copper/fiber support

  Integrated L2 switching with PoE

- **Maximum Modularity and Investment Protection**

  Up to 4 NME, DSP slots to run unprecedented number of services concurrently

  Supports existing NM, WIC/VIC/VWIC, AIMs (except AIM-VPN)

- **Superior Scalability and Availability**

  Architected for scalable services deployment; advanced availability features minimize network downtime

  Hot-Swap Modules, integrated redundant power

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

BGP Graceful Restart (GR) Per Neighbor

BGP Graceful Restart

Graceful restart is the mechanism by which BGP routing peers avoid a routing flap following a switchover

BGP Graceful Restart per Neighbor

This feature introduce the ability to enable or disable BGP graceful restart for every individual BGP neighbor was introduced.

Benefits

To limit BGP graceful restart to neighbors supporting it.

BGP Graceful Restart (GR) Per Neighbor Configuration Example


```
router bgp 45000
  template peer-session S1
    remote-as 40000
    ha-mode graceful-restart                        ← Graceful restart enable
    exit-peer-session
  template peer-session S2
    remote-as 50000
    ha-mode graceful-restart disable                ← Graceful restart enable
  exit-peer-session
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 150
  bgp graceful-restart stalepath-time 400
  address-family ipv4 unicast
    neighbor PG1 peer-group
    neighbor PG1 remote-as 45000
    neighbor PG1 ha-mode graceful-restart disable ← Per neighbor graceful restart disable
    neighbor 172.16.1.2 peer-group PG1
    neighbor 172.21.1.2 remote-as 45000
    neighbor 172.21.1.2 activate
    neighbor 172.21.1.2 ha-mode graceful-restart  ← Per neighbor graceful restart enable
```

BGP Route Target Changes Without PE-CE Impact

BGP Route Target

Creates or adds to a list of VPN extended communities used to determine which routes are imported / export by/to a VRF

BGP RT changes without PE-CE Impact

Allow to change BGP RT filters without impacting PE-CE routing protocol

Benefits

No route updates on CE and customer network during SP operation and BGP RT updates

OSPF Graceful Restart (RFC 3623) (Helper Mode Only)

OSPF Graceful Restart

OSPF Graceful Restart is the mechanism by which OSPF routing peers avoid a routing flap following a switchover

OSPF Graceful Restart (Helper Mode Only)

Enables OSPF peer router to give switching-over router a grace period to re-establish OSPF neighbor adjacencies while continuing to forward traffic

Benefits

Increases OSPF network availability

OSPFv3 Graceful Restart (RFC 5187) (Helper Mode Only)

OSPFv3 Graceful Restart

OSPFv3 Graceful Restart is the mechanism by which OSPFv3 routing peers avoid a routing flap following a switchover

OSPFv3 Graceful Restart (Helper Mode Only)

Enables OSPFv3 peer router to give switching-over router a grace period to re-establish OSPFv3 neighbor adjacencies while continuing to forward traffic

Benefits

Increases OSPFv3 network availability

OSPF Graceful Shutdown

Graceful Shutdown

Enables administrator to remove a router from the network gracefully without impacting data traffic

OSPF Graceful Shutdown

Enables OSPF router to inform its neighbors it is going offline, indicating its originating links as invalid and bringing down OSPF neighbor adjacencies

Benefits

Enables software upgrades and troubleshooting of OSPF router without impacting data traffic

OSPF TTL Security Check (GTSM)

TTL Security Check

Enables router to only accept packets having a specific IP TTL value

OSPF TTL Security Check (GTSM)

Simple security mechanism that ensures the OSPF neighbor is exactly the number of hops away as specified in the configuration

Benefits

Additional simple security mechanism to thwart OSPF-based attacks

ISIS VRF Support

VRF

Virtual Routing Forwarding context

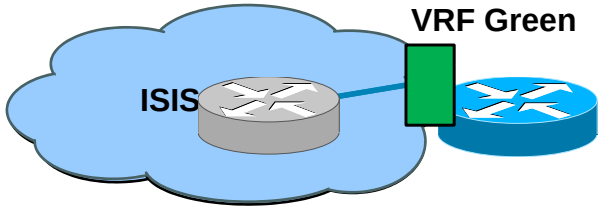
ISIS VRF support

This feature provides multiple VPN routing and forwarding (VRF)-aware Intermediate System-to-Intermediate System (IS-IS) instances.

Benefits

- Allow to support overlap of addresses
- Separate VPN
- Redistribution into L3VPN and MP-BGP

ISIS - VRF Support – Configuration Example




```
Router(config)# router isis
Router(config-router)# vrf first
Router(config-router)# net 49.000b.0000.0001.ffff.00
Router(config-router)# is-type level-1

Router(config)# interface POS 6/1
Router(config-if)# ip vrf forwarding green
Router(config-if)# ip address 172.16.2.1 255.255.255.0
Router(config-if)# ip router isis      ← IS-IS is enabled within VRF
Router(config-if)# no shutdown
```

ISIS MIB

MIB

Management Information Base

ISIS MIB

This feature introduces MIB support for the Intermediate System-to-Intermediate System (IS-IS) link-state routing protocol.

Benefits

The IS-IS MIB feature offers service providers an improved capability to continuously monitor the changing state of an IS-IS network by use of MIB objects.

IS-IS Support for BFD

BFD

BFD is a protocol intended to detect faults in the bidirectional path between two forwarding engines

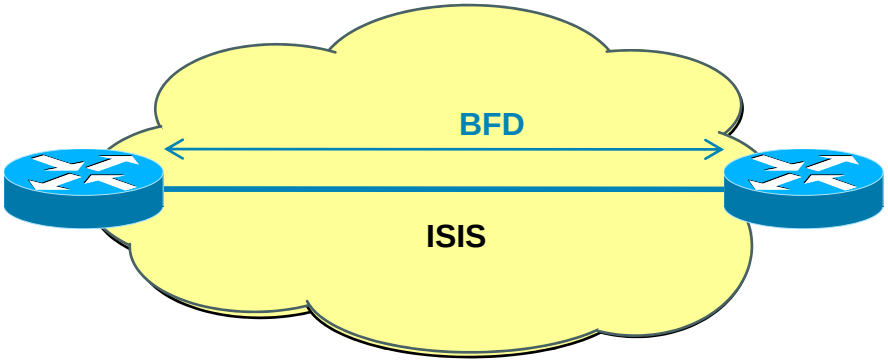
IS-IS Support for BFD

This feature allow IS-IS failure detection to be triggered by BFD

Benefits

-Reduce failure detection timers
-Detect failures over single or multi hop paths
-BFD could be shared between multiple protocols and therefore reduce CPU load.

ISIS - BFD support




```
interface FastEthernet 0/1
 ip address 172.16.10.1 255.255.255.0
ip router isis
 bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 3/0.1
ip address 172.17.0.1 255.255.255.0
ip router isis
!
router isis
net 49.0001.1720.1600.1001.00
bfd all-interfaces
```

MPLS VPN – InterAS option B

MPLS VPN InterAS

MPLS VPN – InterAS provide solution allow 2 or more network providers to interconnect enterprise or customers VPN's

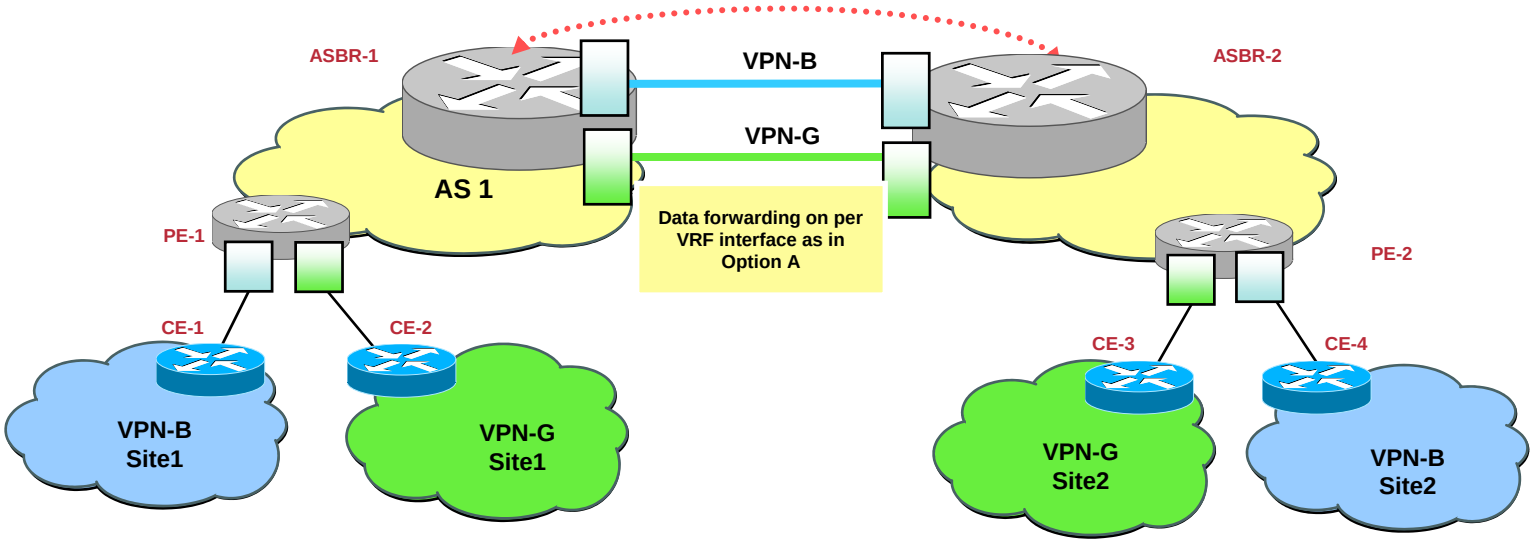
MPLS VPN Inter AS option AB

MPLS InterAS option AB combine the well known InterAS option A and option B define in MPLS-VPN standard by using option A data plane and option B control plane.

Benefits

Keep the IAS option A Data Plane Flexibility & Security and bring the IAS option B control plane scalability.

MPLS VPN Inter-AS Option AB



- **MPLS VPN Inter-AS option AB**
  - **Preserves per VRF-based IP forwarding in data plane with IP QOS benefit.**
  - **Improves scaling in control plane by reducing required number of BGP session to one.**

MPLS VPN – BGP Local Convergence

MPLS VPN Convergence

MPLS VPN – Converge provide Mechanism to switch from primary path to secondary path in case of node or link failure

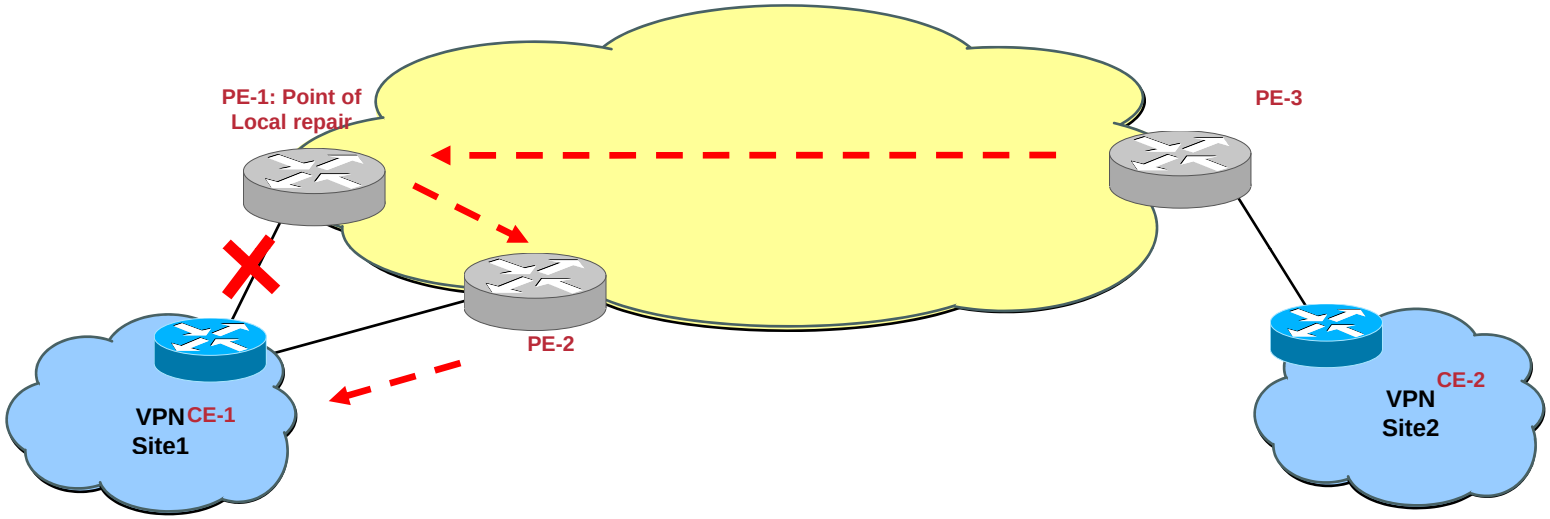
MPLS VPN – BGP Local Convergence

In case of PE-CE link failure, this new feature will locally install a backup path via alternate PE and this for a period of Maximum 5 minutes. Allow traffic to not be dropped during the end-end BGP convergence process

Benefits

Reduce classical BGP PE-CE link failure down time from few minutes to few second.

MPLS VPN BGP Local Convergence – Deployment Example



- **MPLS VPN BGP local convergence**
  - **Upon a PE-CE link failure, the egress PE (Point of Local Repair) switches VPN traffic to an alternative egress PE before the control plane has converged.**
  - **The feature improves VPN end-to-end convergence scenarios.**

Performance Routing (PfR) – Protocol Independent Route Optimization (PIRO)

IP Routing

PfR

Selects an optimal path for a destination prefix (or application) based on performance metrics, resulting in optimized application performance and availability

PIRO

Enables PfR to use the Routing Information Base (RIB) for parent route lookups

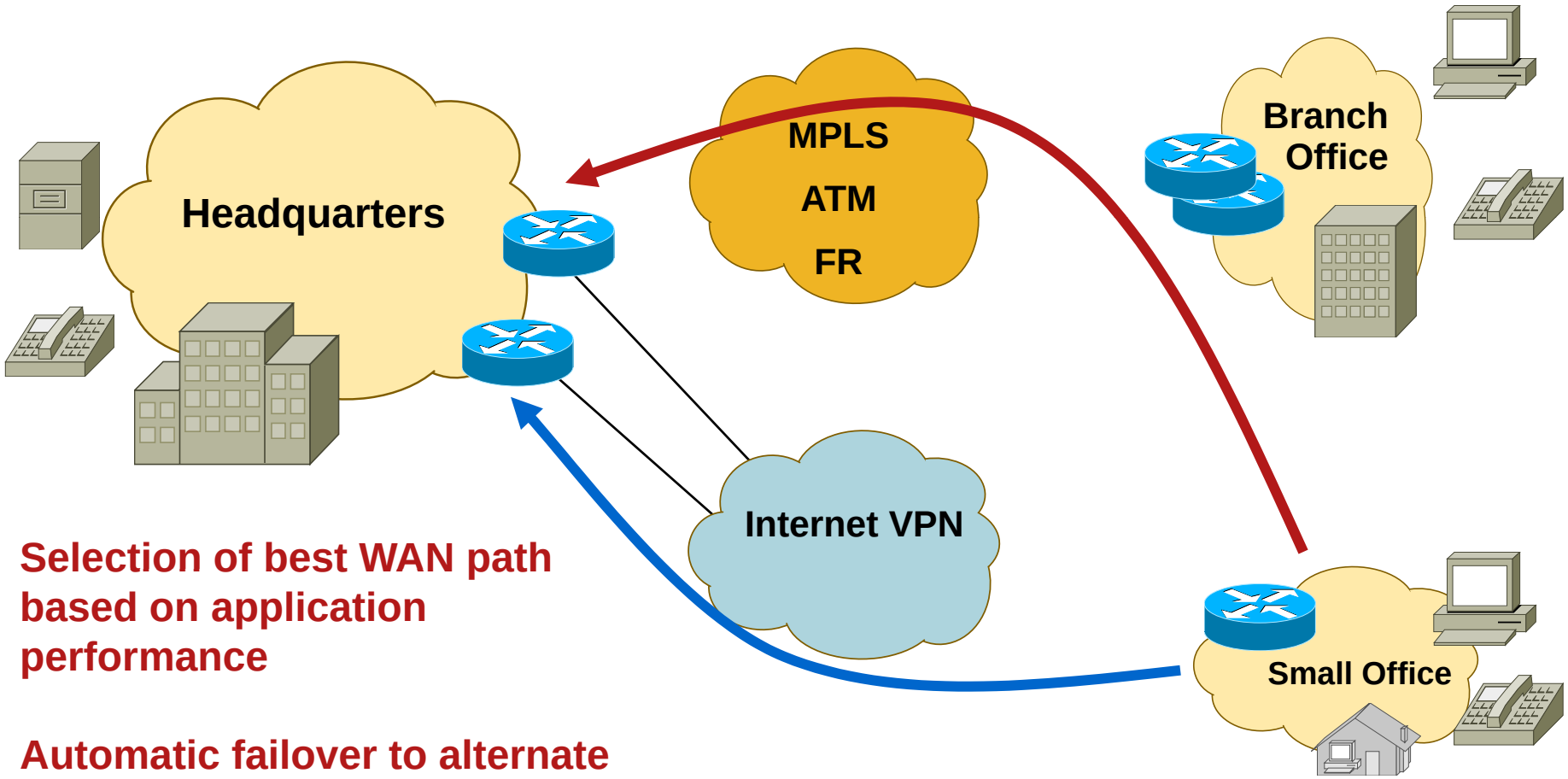
Benefits

Enables PfR support for EIGRP and OSPF networks

Cisco Performance Routing (PfR)

Two Paths
Two Providers

WAN Availability



Selection of best WAN path based on application performance

Automatic failover to alternate path when primary path cannot deliver performance policy

PfR EIGRP mGRE DMVPN Support

PfR

Selects an optimal path for a destination prefix (or application) based on performance metrics, resulting in optimized application performance and availability

EIGRP mGRE DMVPN Support

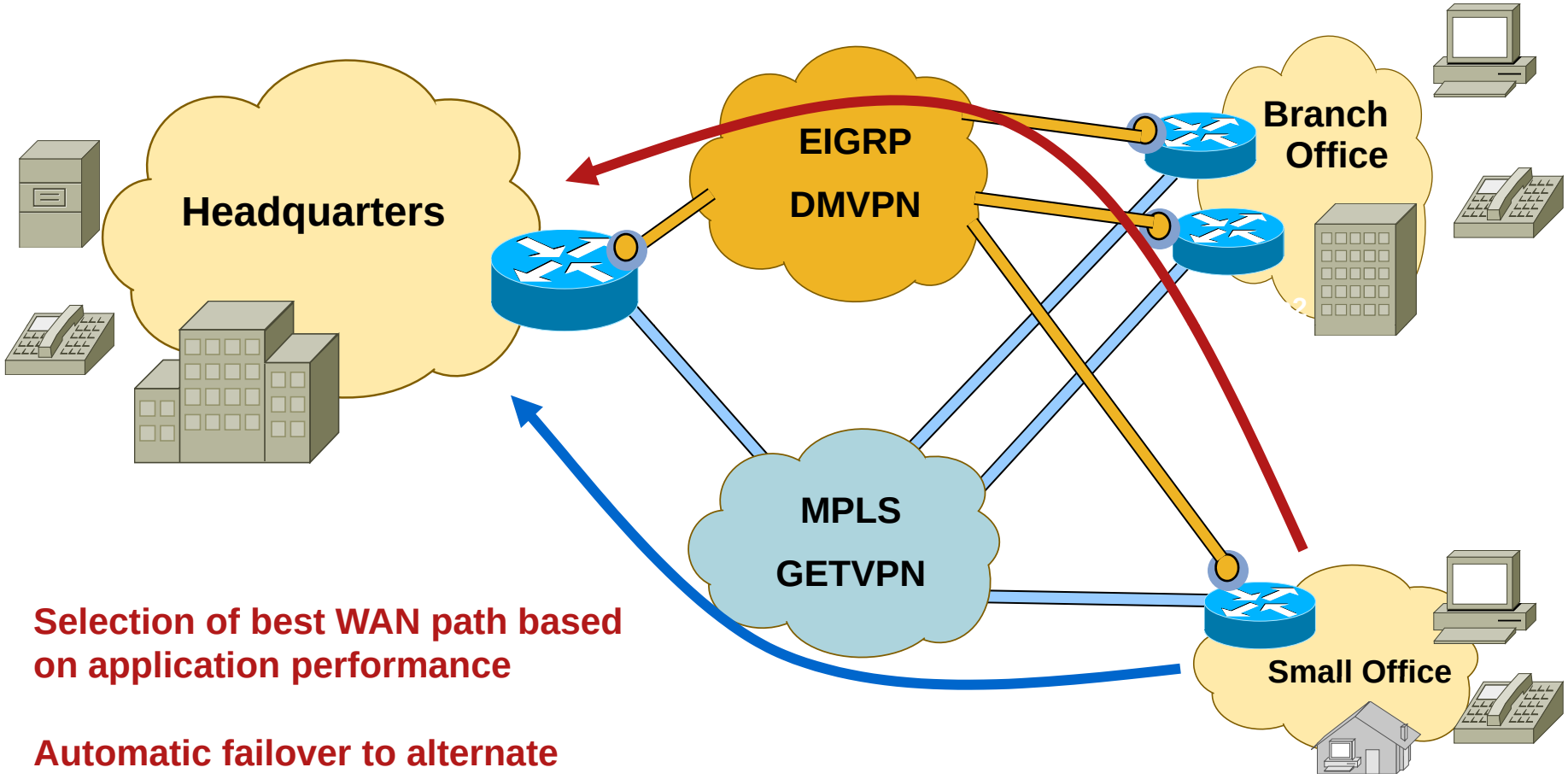
Enables PfR support for EIGRP route control with mGRE DMVPN

Benefits

Extends PfR applicability in the enterprise to EIGRP-based DMVPN networks

PfR EIGRP mGRE DMVPN Support

IP Routing



Selection of best WAN path based on application performance

Automatic failover to alternate path when primary path cannot deliver performance policy

EIGRP DVMPN mGRE Tunnel

MPLS GETVPN Link

Service Advertisement Framework (SAF)

Service Advertisement Framework (SAF)

Enables network applications to discover the existence and configuration of networked services

Initial SAF Applications

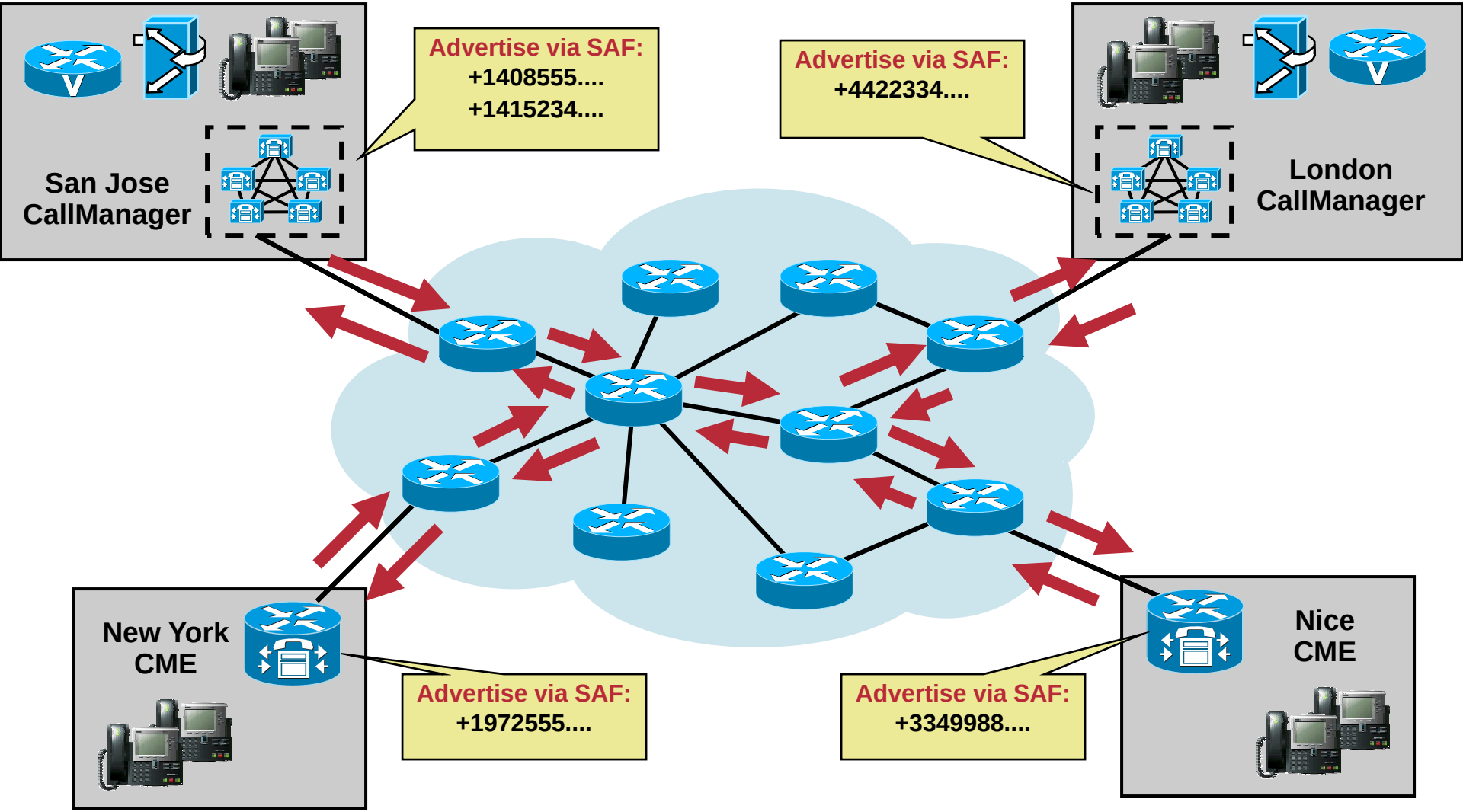
With UC 8.0, Cisco Unified Communications Manager (CUCM) and Call Manager Express (CME) use SAF for dynamic Call Agent discovery and automated dial plan configuration. UC 8.0 also includes SAF Client support for Cisco ISR-based Cisco Unified Border Element (CUBE), TDM Gateways and Cisco Survivable Remote Site Telephony (SRST) services.

Benefits

SAF reduces operational costs by reducing the time to deploy and configure network based services

SAF for Unified Communications
Propagating Reachability for Call Agents

IP Routing

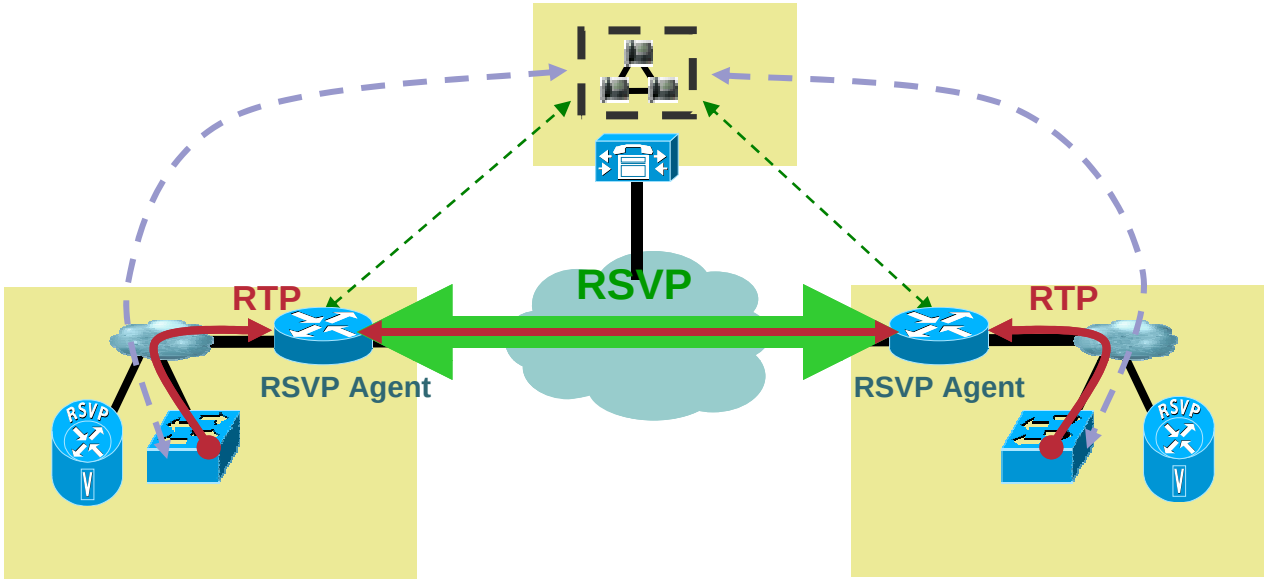


Cisco IOS Call Admission Control for Video and Voice applications

- Video and Voice applications required fixed and deterministic bandwidth and a Call Admission Control protocol to be operate efficiently.
- RSVP is the defacto AC protocol standard in IP world
- Release 15.0(1)M introduces a new set of RSVP extension to allows customers to deploy efficiently Video and Voice architecture and services. New extensions are:
  - RSVP-VRF Lite Admission Control
  - RSVP Fast Local Repair (also in 12(2)SRC)
  - RSVP Interface-based Receiver Proxy (also in 12(2)SRC)

RSVP and Unified Communication Admission Control

Call Admission Control



- Cisco RSVP Agent are starting and ending RSVP session in the WAN on behave of telephone handset to assure bandwidth is available and reservable.
- For example, an RSVP reservation pool can be created for voice traffic, and a separate RSVP reservation pool can be created for video traffic. This prevents video traffic from swamping voice traffic.

RSVP VRF Lite Aware Admission Control

Admission Control

RSVP provides Call Admission Control for Voice & Video application

RSVP –VRF Lite Aware Admission Contro

RSVP – VRF Lite Aware Admission Control allows you to set a RSVP ip bandwidth pool for an interface belonging to a MultiVRF (VRF lite) interface.

Benefits

Enables RSVP and VRF interoperability

RSVP Fast Local Repair

Admission Control

RSVP Call Admission Control for Voice & Video applications.

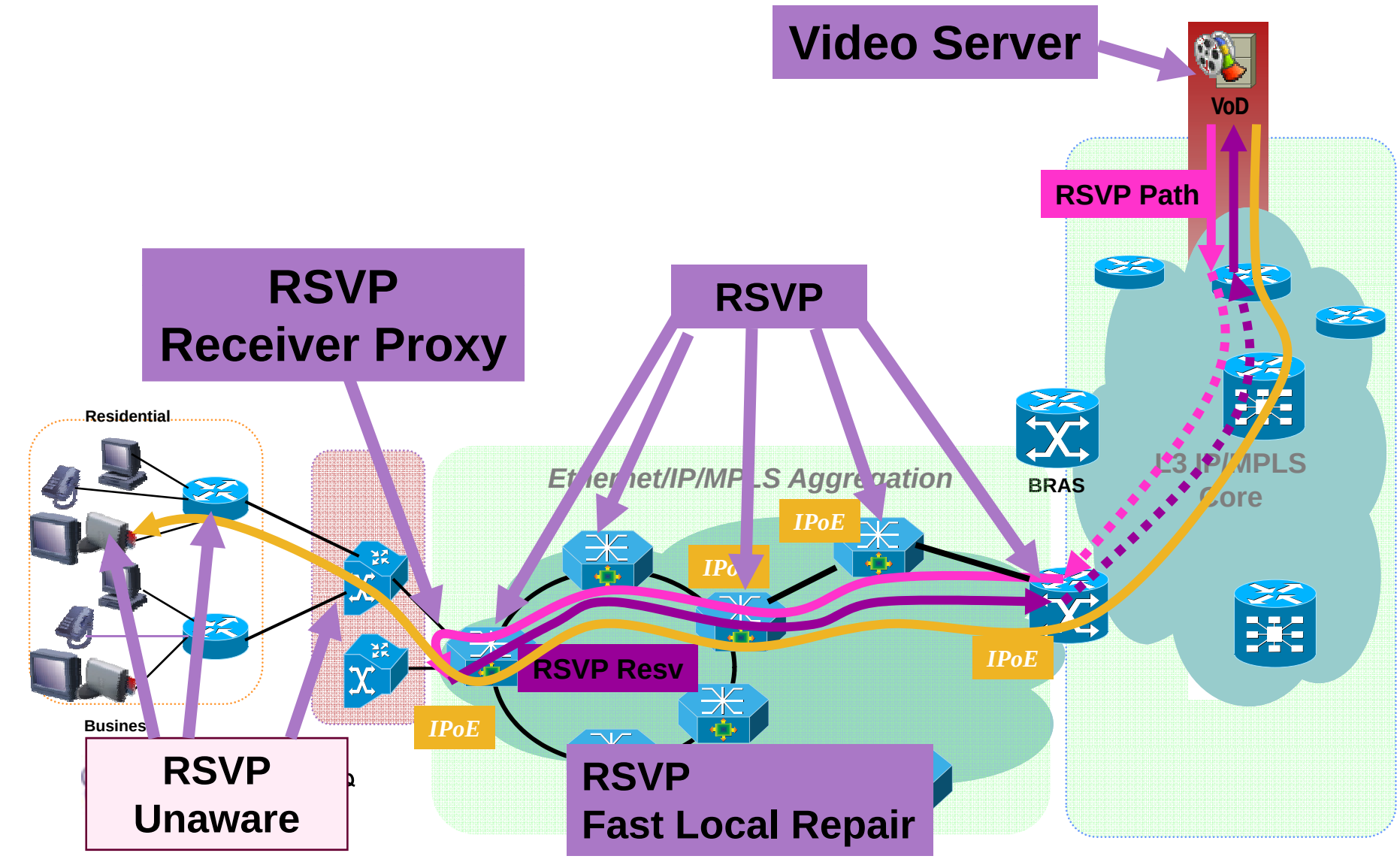
RSVP Fast Local Repair

RSVP Fast Local Repair enables sub-second response time to routing changes.

Benefits

Provides quick adaptation to routing changes without the overhead of the refresh period to guarantee the quality of service (QoS) for data flows. With fast local repair (FLR), Resource Reservation Protocol (RSVP) speeds up its response to routing changes from 30 seconds to a few seconds, assuring VoD end-to-end quality and security when link or node failures occur on oversubscribe links

RSVP Video CAC Components and Architecture



RSVP Interface Based Receiver Proxy

Receiver Proxy

RSVP receiver proxy signal reservations and guarantee bandwidth on behalf of a receiver that does not support RSVP. The configuration is done on per session based

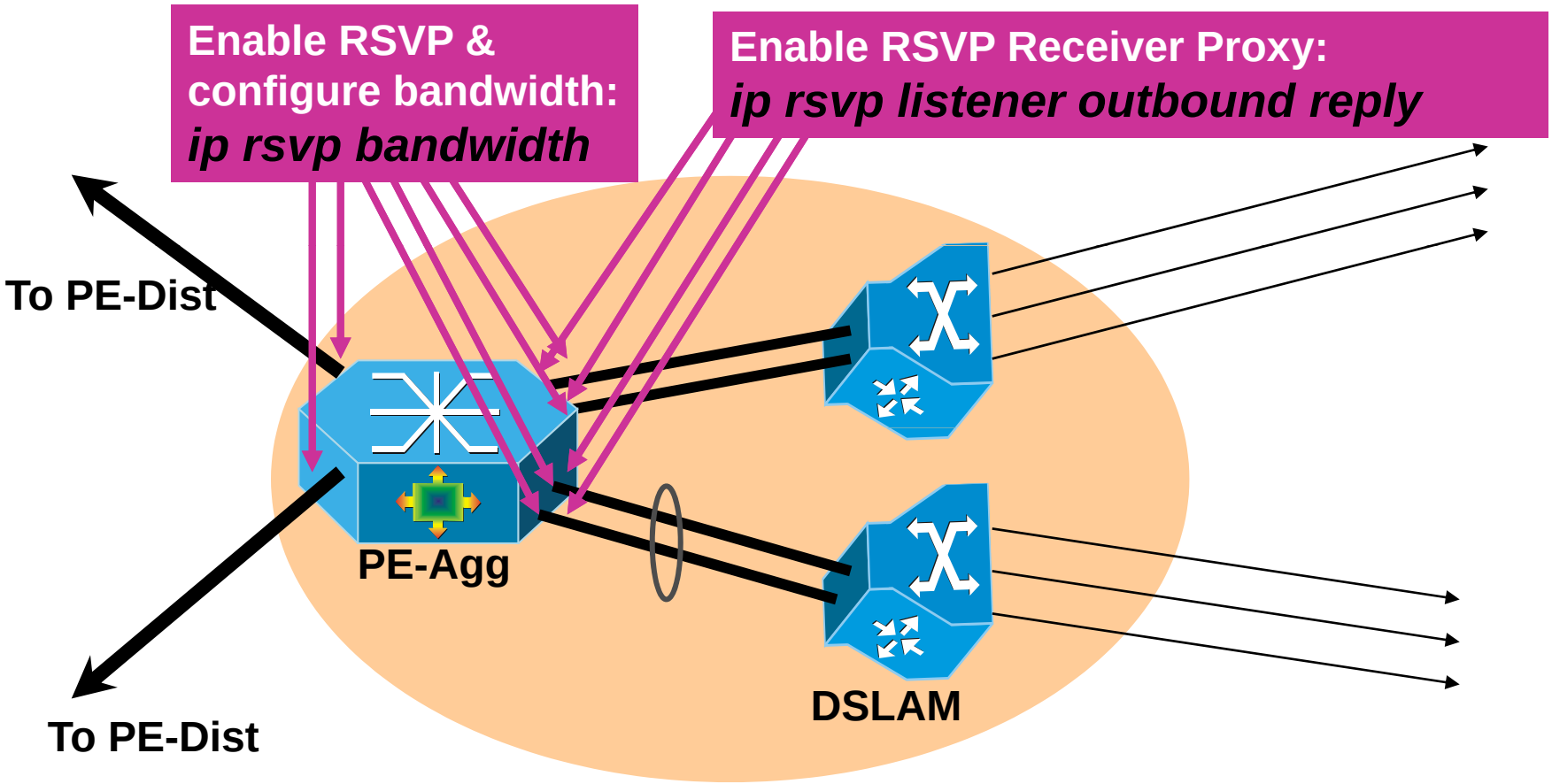
Interface Based Receiver Proxy

RSVP receiver proxy signal reservations and guarantee bandwidth on behalf of a receiver that does not support RSVP. The configuration is done on per interface based for aggregate of flows.

Benefits

The RSVP Interface-Based Receiver Proxy feature lets you configure a proxy router by outbound interface instead of configuring a destination address for each flow going through the same interface.

Using RSVP Receiver Proxy



Cisco IOS Multicast

Shipping since 1994

Cisco IOS Multicast is fundamentally changing the way we live, work, play, and learn by providing innovative solutions that are:

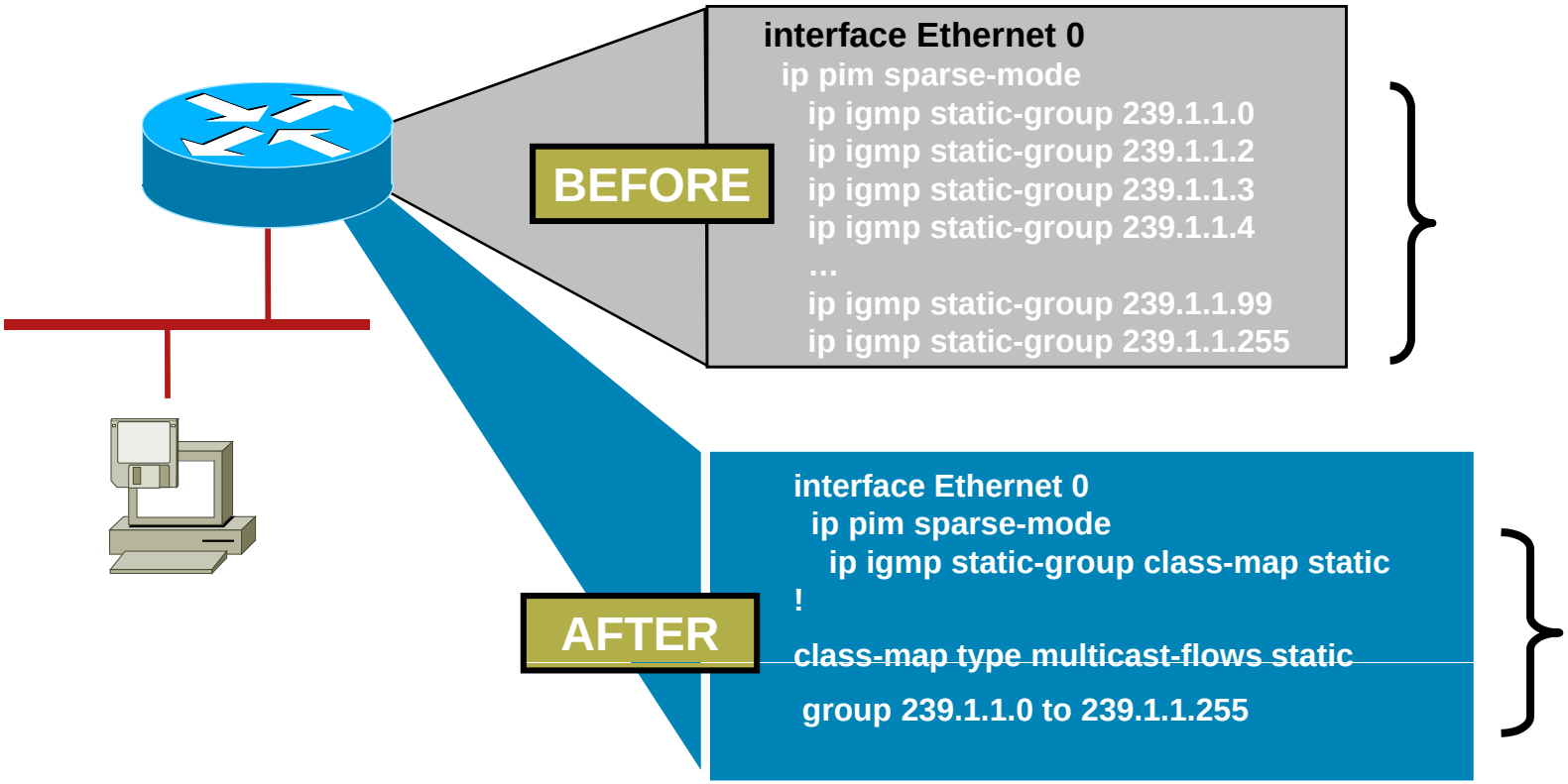
- Simple
- Highly available
- Virtualized
- Standards based
- Secure

Applications that take advantage of Cisco multicast technologies and solutions include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, video, and news

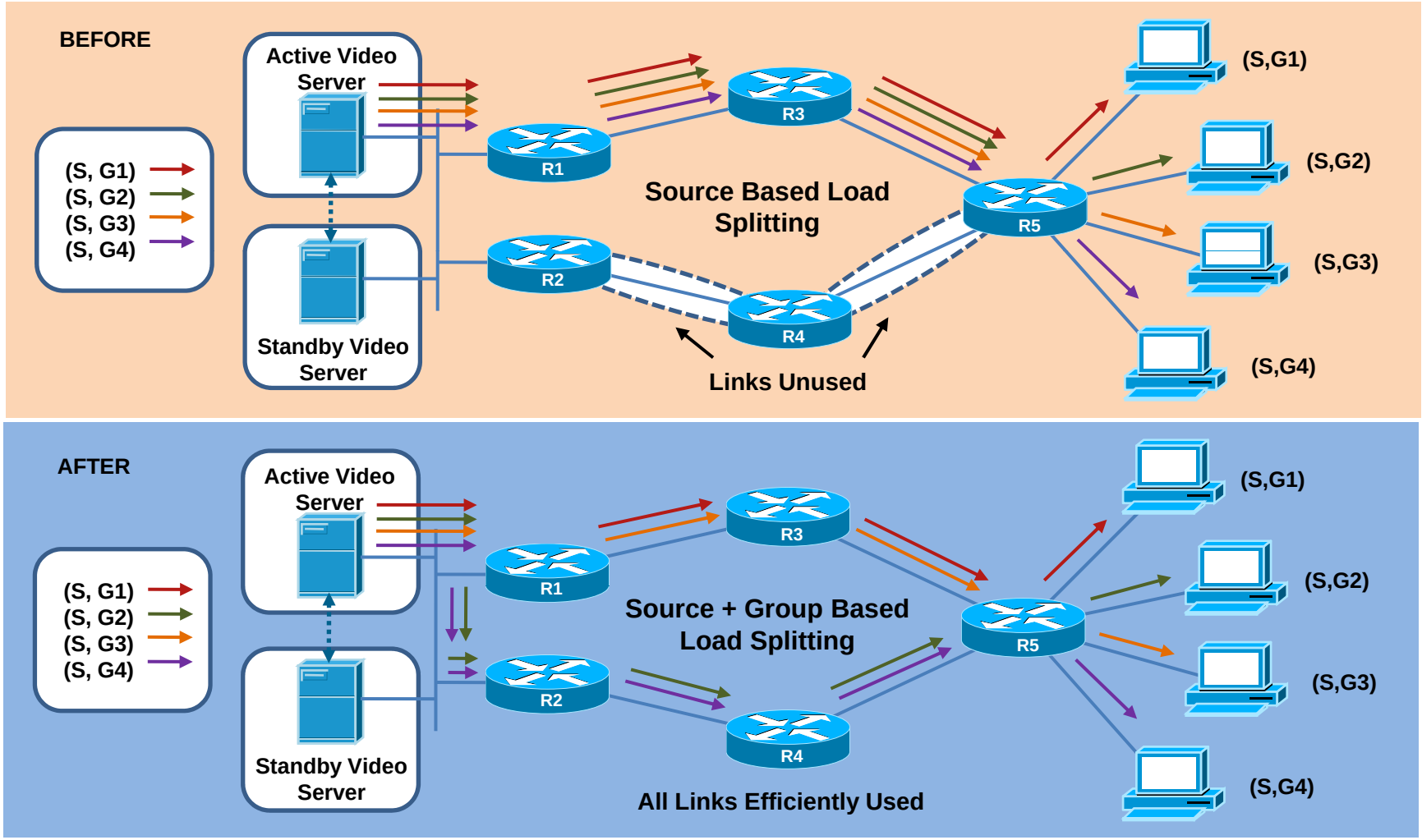
IGMP Static Group Range Support

Introduces capability to configure group ranges in class maps and attach class maps to the ip igmp static-group command

Helps significantly reduce configuration overhead and simplifies administration



IP Multicast Load Splitting – ECMP using S, G and Next-Hop



IP Multicast Load Splitting – ECMP using S, G and Next-Hop (Cont.)

Introduces flexible support for ECMP multicast load splitting by adding support for load splitting based on source and group address and on source, group, and next-hop address

Prior to the introduction of this feature, the Cisco IOS software only supported ECMP multicast load splitting based on source address

This feature enables multicast traffic from devices that send many streams to groups or that broadcast many channels, such as IPTV servers or MPEG video servers, to be effectively load split across equal-cost paths

Enables optimal usage of network resources

IPv4: Multicast Address Group Range Support

Disables IPv4 multicast protocol actions and traffic forwarding for unauthorized groups or channels on all the interfaces in a router for a range of groups

Benefits:

Provides ability to disable PIM, IGMP and MSDP control plane actions

No IGMP (cache), PIM, MRIB/MFIB state created for denied groups

Drops all data packets for denied groups

Without allow-override

Additional line of defense (against erroneous CLI configurations)

With allow-override

Default groups for users, can be overridden by per-interface commands – for use with AAA

IPv6: Multicast Address Group Range Support

Disables IPv6 multicast protocol actions and traffic forwarding for unauthorized groups or channels on all the interfaces in a router for a range of groups.

Benefits

- **Provides ability to disable PIMv6, MLD and MSDP control plane actions**
- **No MLD (cache), PIMv6, MRIB/MFIB state created for denied groups**
- **Drops all data packets for denied groups**

Without allow-override: Additional line of defense (against erroneous CLI configurations)

With allow-override: Default groups for users can be overridden by per-interface commands – for use with AAA

Multicast MIB VRF Support

The set of Multicast MIBs are made to be mVRF aware to help customers manage their Cisco devices in a multicast VPN environment using SNMP.

Benefits

SNMP gets and sets can be made to the individual VRFs

The MIB will have the ability to detect conditions for a trap inside of a VRF and lookup the additional information in the VRF context

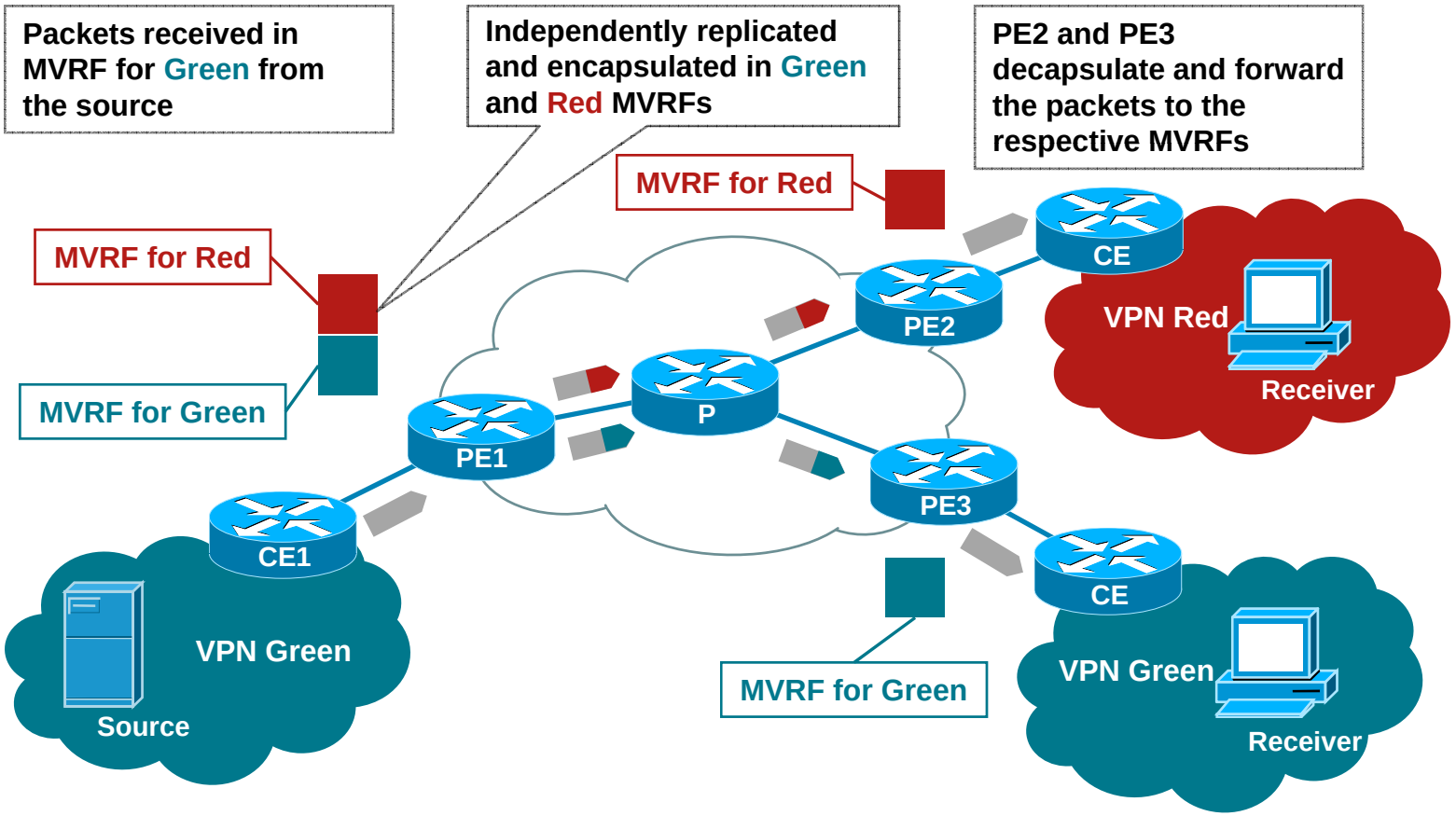
Traps will be sent to a manager located inside a VRF

The following set of Multicast MIBs is made to be mVRF aware.

- PIM-MIB
- CISCO-PIM-MIB
- MSDP-MIB
- IGMP-STD-MIB
- CISCO-IPMROUTE-MIB
- IPMROUTE-STD-MIB

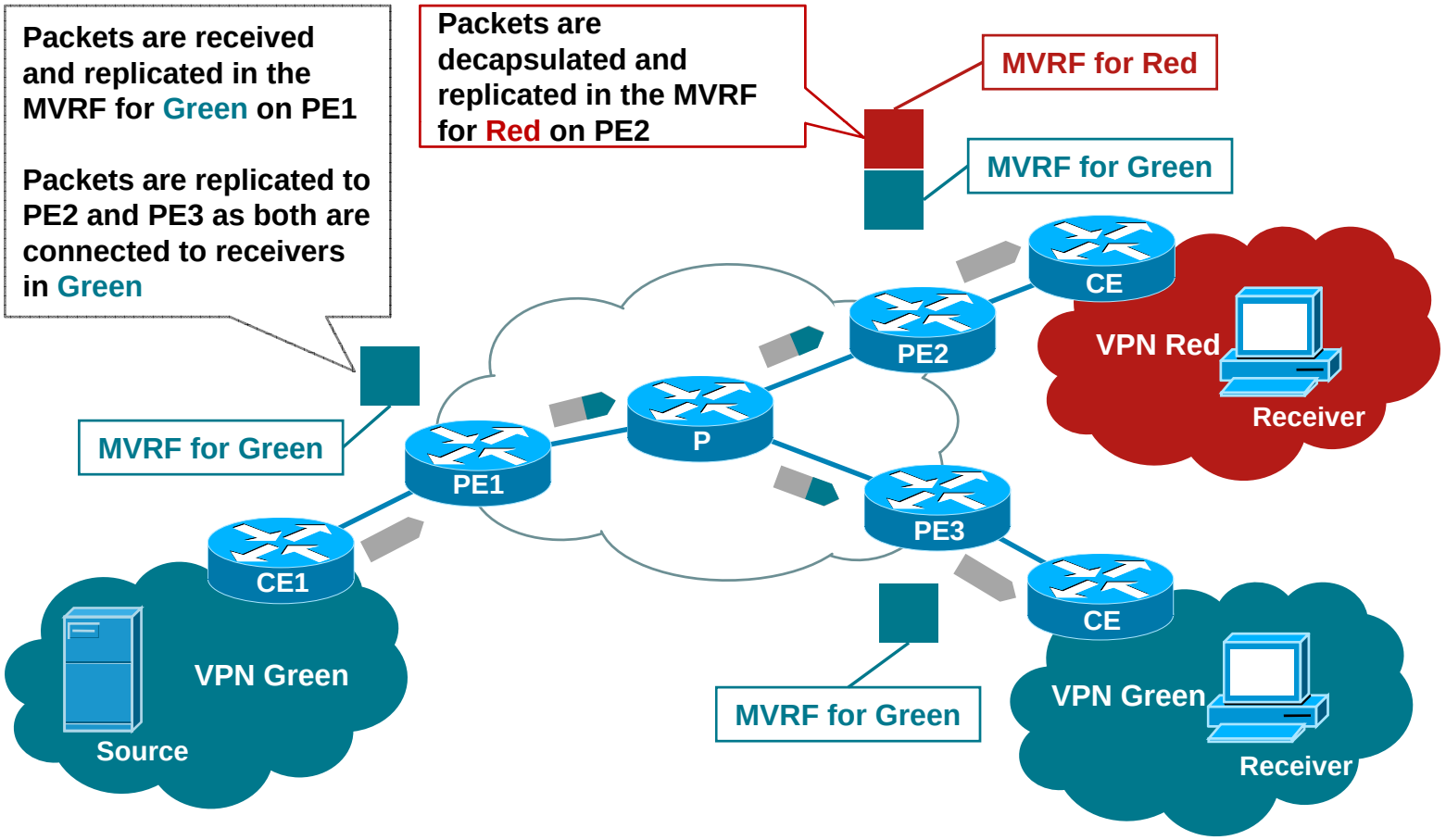
Multicast VPN Extranet Support

Introduces extranet capabilities in Multicast VPN that allow VPN closed user groups to share information and common multicast information to be distributed across multiple VPN customers



Multicast VPN Extranet Support (Cont.)

Scalable and efficient method to transport and replicate customer multicast information across an MPLS network between different VPN's

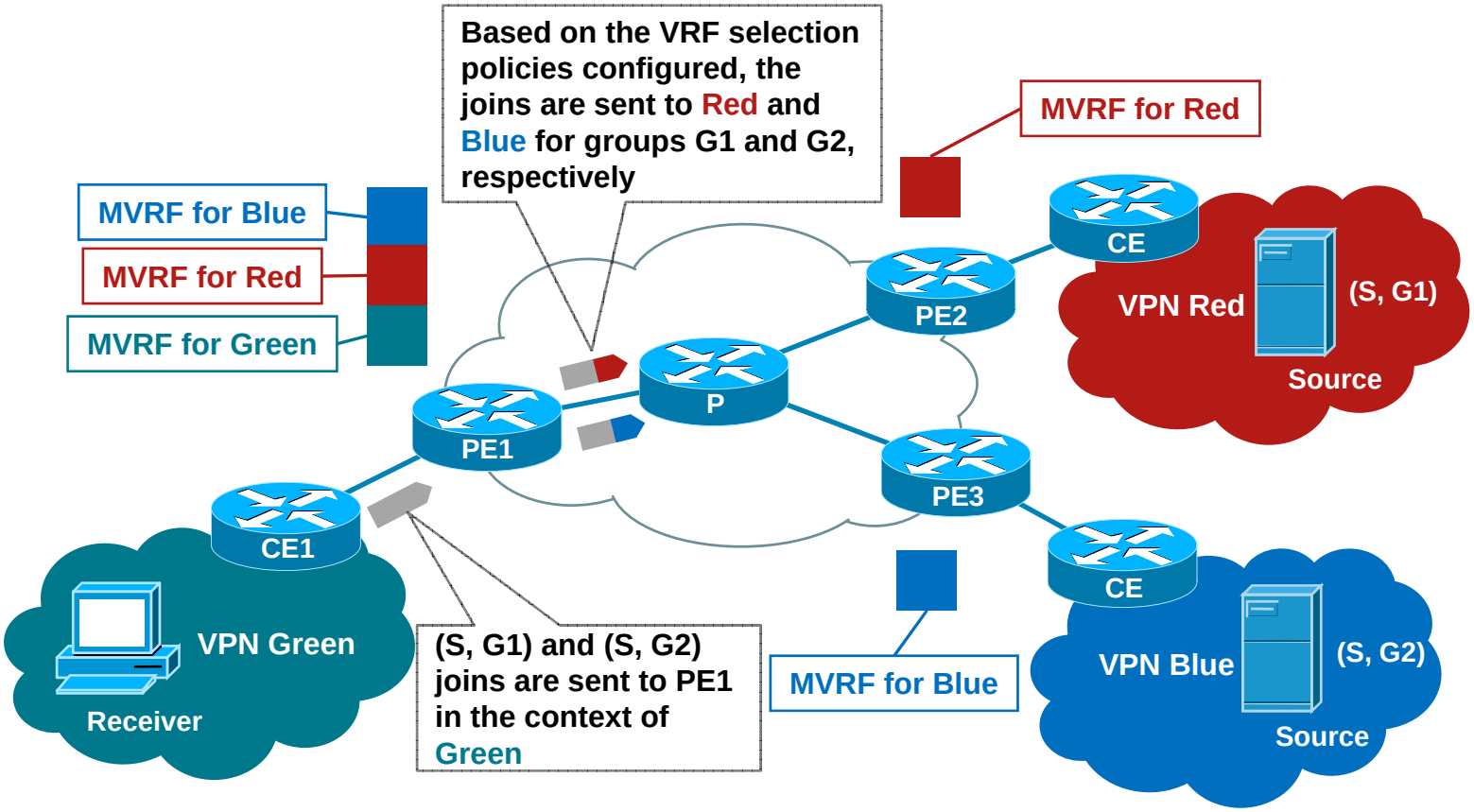


Multicast VPN Extranet Support (Cont.)

- Allows Service Providers to offer next generation of flexible extranet services that enable business partnerships between different enterprises
- Efficient content distribution between Enterprises
- Efficient sharing of multicast resources with external or business partners
- Efficient content distribution from Service Providers or content provider to its different VPN customers
- Integrated transparently with unicast MPLS VPN services

Multicast VPN VRF Select

Provides the capability for Reverse Path Forwarding (RPF) lookups to be performed to the same source address in different VPN routing and forwarding (VRF) instances using the group address as the VRF selector



PIM Triggered Joins

This feature utilizes the Generation ID (GenID) value as a mechanism to trigger adjacent Protocol Independent Multicast (PIM) neighbors on an interface to send PIM join messages for all (*, G) and (S, G) mroutes that use that interface as a reverse path forwarding (RPF) interface

This immediately reestablishes mroute states

Benefits

- Improves the reconvergence of multicast routes (mroutes)
- Helps prevent mroute state in the control plane from timing out
- Prevents temporary blackouts of multicast traffic

Bidirectional Forwarding Detection (BFD) Release 15.0(1)M Enhancements

High Availability

- **BFD - Client for IPv4 static route**

  New BFD Client feature which delivers a comprehensive solution to monitor and detect the status of static routes between two adjacent peers.

  - Even if no routing protocol is run between the two peers, it is now possible to monitor any static routes
  - Provides fast failure detection for scenarios where the next-hop in a static route is down but the interface remains up

- **BFD - VRF aware support**

  New BFD features which extends BFD failure detection capability within a VRF context.

  Provides a comprehensive solution to improve and enhance end-to-end reliability and availability of Layer 3 VPN networks.

BFD Release 15.0(1)M Enhancements (Cont.)

High Availability

- **BFD - WAN interfaces support**

  Extends BFD support to the most commonly used WAN interface type so that fast failure detection in the forwarding path can be achieved and therefore increase overall network availability and reliability.

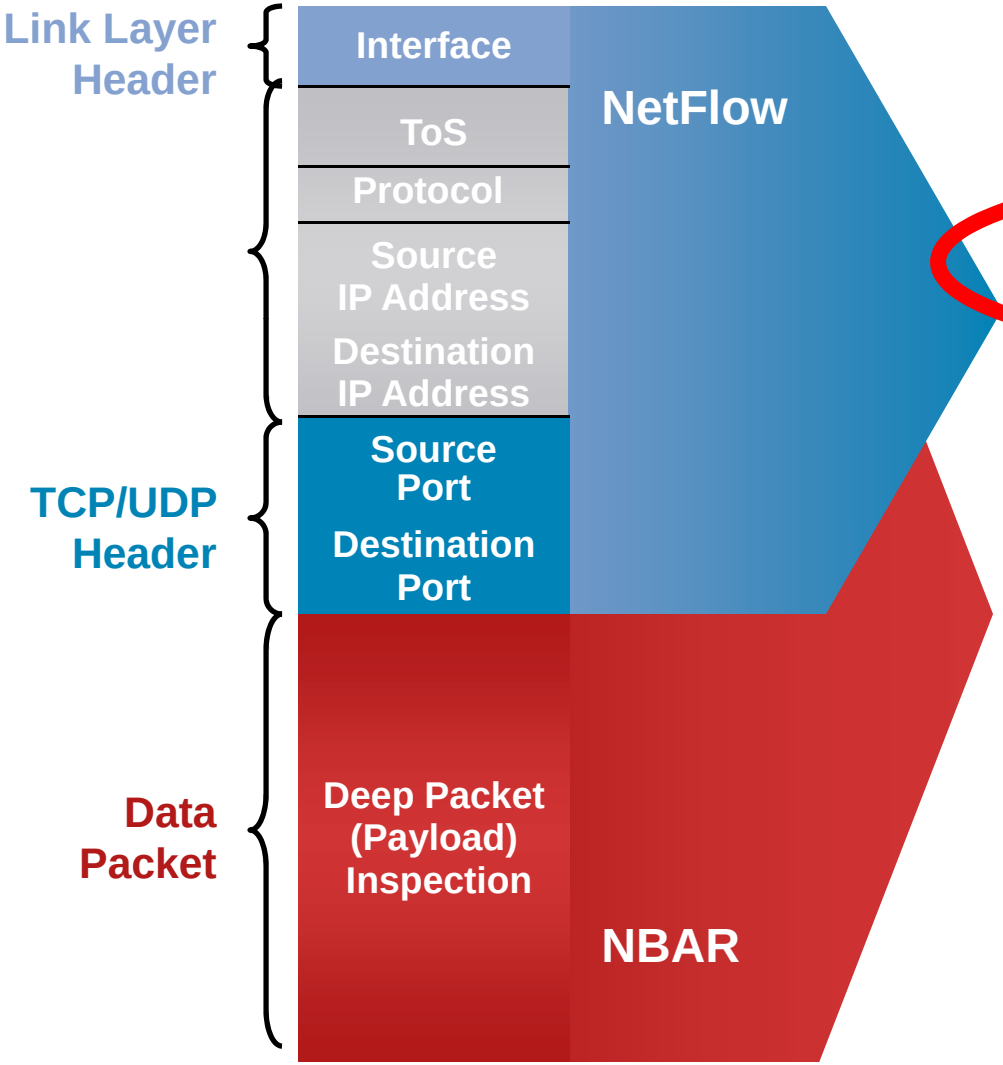
  Allows a single standard protocol to be used as failure detection for divers interface types

  Supported Interfaces:

Interface Type	Encapsulation
ATM	ATM interface with AAL5 MUX, AAL5 SNAP, AAL0 encapsulations ATM sub interface
POS	POS interface with HDLC and PPP Encapsulations POS sub interface
Serial	Serial interface, Serial interfaces with FR Encapsulation Serial sub interface with FR Encapsulation
VLAN	802.1q

NetFlow and NBAR Differentiation

Embedded Management



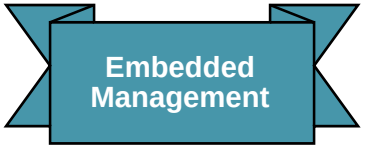
NetFlow

- ✓ Monitors data in Layers 2 thru 4
- ✓ Determines applications by combination of Port or Port/IP Addressed
- ✓ Flow information who, what, when, where

NBAR

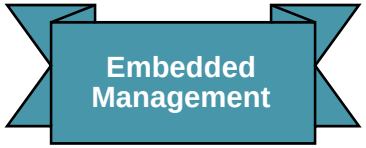
- ✓ Examines data from Layers 3 thru 7
- ✓ Utilizes Layers 3 and 4 plus packet inspection for classification
- ✓ Stateful inspection of dynamic-port traffic
- ✓ Packet and byte counts

Application / Protocol Dynamics



- Applications could no longer be identified by looking at L2/L3/L4 header pattern at packet level
  - Applications could allocate TCP/UDP ports dynamically (e.g. Voice, Oracle, SAP, Citrix,..) => **Required Flow Correlations**
  - Yesterday's application become today's **transport** (e.g. YouTube which use HTTP as transport) **=> Required Recursive Inspection**
  - Applications using reserved UDP/TCP port to traverse Firewall (Skype, Bittorent using TCP port 80)
  - Applications leveraging Encryption (Skype, Microsoft domain isolation,..)
- NetFlow and NBAR Integration is a MUST

NBAR Integration in Flexible NetFlow



- NetFlow has been used to provide visibility on Network utilization – who/what/where/when
- NBAR (Network Based Application Recognition)

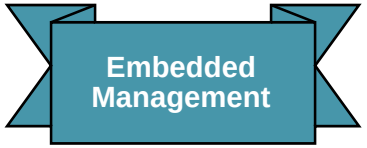
  offers a Deep Packet Inspection mechanism
- Combining L2/L3/L4 Flow visibility from Flexible NetFlow and Application awareness from NBAR to offer Application Visibility in Flow record

  Through this integration, a new field “Application name” will be available into Flow record definition

For more information visit:

- NBAR - www.cisco.com/go/nbar
- NetFlow – www.cisco.com/go/nf
- Flexible NetFlow – www.cisco.com/go/fnf

Cisco IOS Embedded Event Manager (EEM)

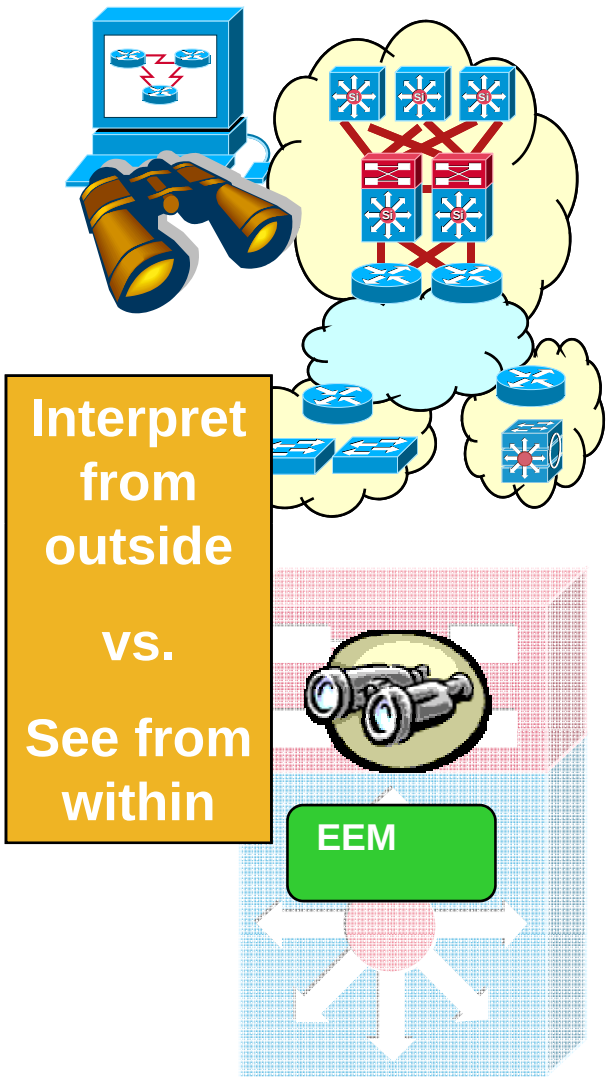


- An extremely flexible and powerful subsystem within Cisco IOS Software
- Adapt device behavior and insert business logic without IOS upgrade
- Real-time detection of wide range of embedded events
- Onboard automation and programmability interface

Getting An Insider's View with EEM

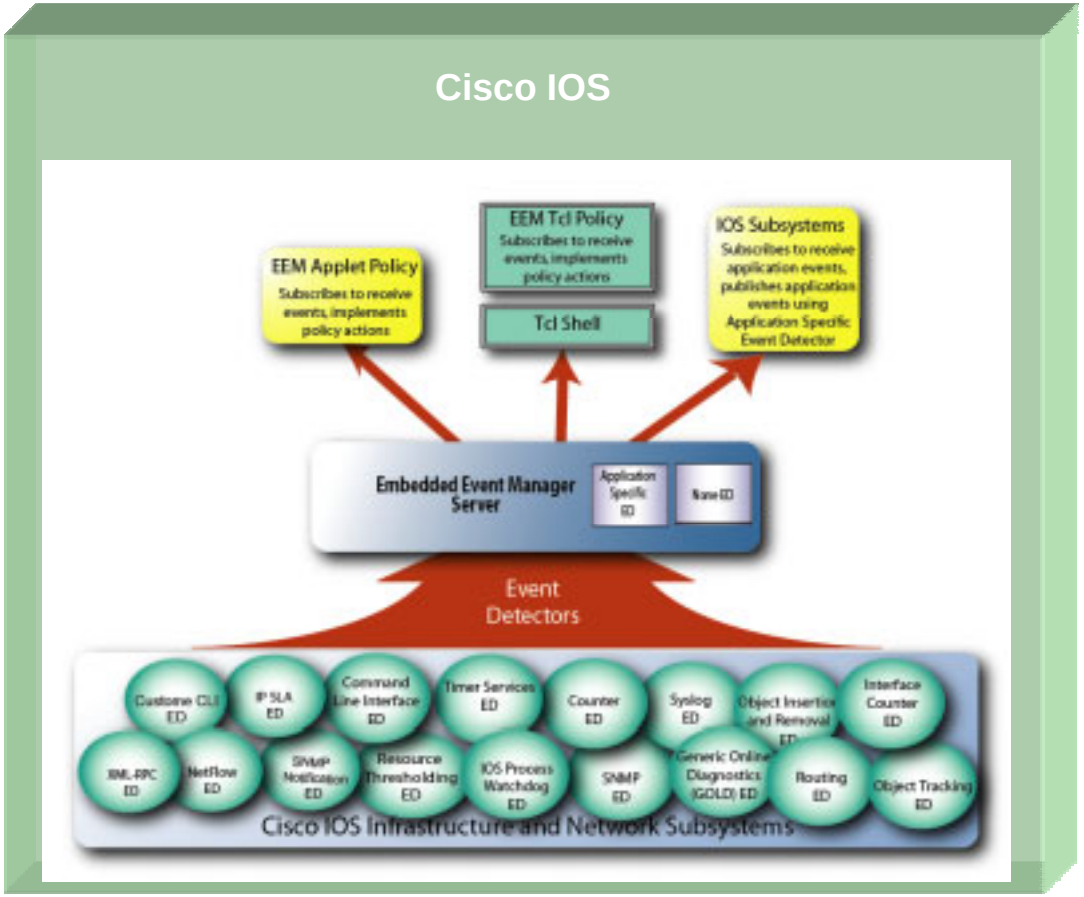
Embedded Management

- **RELIABLE** – Captures reliable information within the box when connectivity to external systems are not available or reliable
- **QUICK** – Onboard logic provides instant reaction when certain condition is detected and wins precious time to capture critical information
- **DETAILED** -- An insider's view allow you get more granularity information than you could have afford through external communication
- **EVENT-DRIVEN** – EEM supports many event detectors integrated with IOS modules to generate event and allow you to avoid constant polling
- **DISTRIBUTED** – Scripts are distributed to each network devices and runs locally when triggered supported distributed and collaborative processing for complex network management tasks

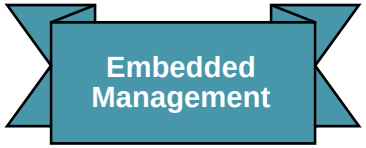


EEM Basic Architecture

- Event detectors
  - Integrated with IOS modules
  - System event detection
- EEM server
  - The **brain** of the system
- Policies (scripts)
  - CLI-based (Applet)
  - TCL-based

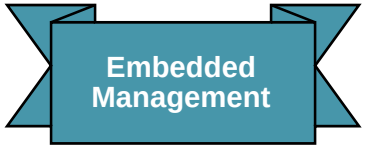


Existing EEM Event Detectors



- EEM 1.0
  - SNMP ED
  - Syslog ED
- EEM 2.0
  - Application ED
  - Interface ED
  - Counter ED
  - Timer ED
  - Watchdog ED
- EEM 2.1
  - CLI ED
  - None ED
  - Object Insertion Removal (OIR) ED
  - GOLD ED
- EEM 2.2
  - Embedded Object Tracking (EOT) ED
  - Resource ED
  - Redundancy framework ED
- EEM 2.4
  - SNMP notification ED
  - XML-RPC ED
- EEM 3.0
  - Custom CLI ED
  - Routing ED
  - NetFlow ED
  - IP SLA ED

EEM Version 3.1 Enhancements: Release 15.0(1)M



- SNMP Object Event Detector

  Intercept incoming SNMP get/set requests and generate customized response

  Provide convenient way to customize SNMP MIB interface for Cisco devices without IOS image upgrade

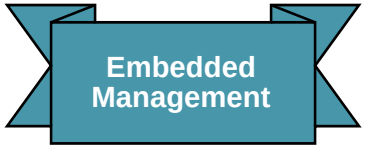
- SNMP Notification Event Detector Enhancement

  Enhanced SNMP notification ED to intercept and process outgoing SNMP traps in addition to the incoming ones

- EEM Policy Description Enhancement

  Show command enhancement to display one line description for EEM policies

EEM 3.1 Enhancements: Release 15.0(1)M (Cont.)



- CLI Authorization Bypass

  Allow user to disable authorization control for CLI execution from EEM policies

- Logging Action Enhancement

  Allow EEM policies to generate Syslog messages with user defined Syslog facility names

- EEM TCL Library Enhancements

  Allow the execution of multiple CLI commands in one function call with a combined result

IOS Intrusion Prevention System (IPS) Enhancements in Release 15.0(1)M

Security

Feature/Enhancement	Benefits
Lightweight IPS Engines for existing and new signatures optimized for HTTP, SMTP and FTP protocols	Memory efficient traffic scanning for attack signatures consuming up to 40 % less memory on the router.
New Default IOS IPS Category signatures updated frequently by Cisco Signature Team	More comprehensive and effective attack coverage by default. Much quicker inclusion of most relevant new threat signatures within the default set (category).
Chaining of Traffic Scanning (Regular Expression) Tables	Capability to load more signatures simultaneously and provide protection for larger number of threats and vulnerabilities, especially with more default memory on the new ISR G2 routers.
Configurable Threshold (Upper Limit) to be dedicated to IPS feature	Avoid unintended allocation of large amount of router memory by IPS signature Tables Prevent IPS feature to consume all the free processing memory available and cause performance and other operational problems

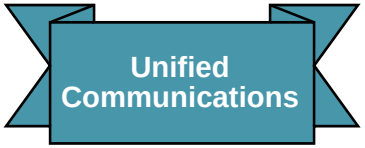
http://www.cisco.com/go/ips

Other Security Enhancements: Release 15.0(1)M

Feature	Why Important
GET VPN VRF-Aware GDOI on GM	Adding to the existing “GET VPN VRF-Lite” support that provides data plane traffic separation, this **provides control plane traffic separation** (group registration and rekeys) for a dedicated management VRF **so different SP customers or Enterprise depts can share the same key servers** or alternatively have separate key servers.
Ability to disable volume-based ipsec lifetime rekey	Provides **options to disable IPsec volume-based lifetimes, that may waste system resources in high throughput environments**, or increase the upper limit value for ipsec volume lifetime.
DMVPN Enhancements	Provides **improvements for managing and reporting** on DMVPN tunnels such as tunnel health and recovery, interface status, syslog and MIB

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

Unified Communications and Voice Enhancements: Release 15.0(1)M



Feature	Why Important
Cisco Unified Border Element (CUBE) Support for SRTP-RTP Internetworking	Critical to securing unified communications deployments, secure-RTP allows customers to deploy security and interwork with CUCM.
CUBE support for Out-of-dialog SIP OPTIONS Ping messages to monitor SIP Servers	Allows for the monitoring and management of SIP trunk capacity and status.
UC Trusted Firewall Control Version 2	Offers expanded support through Unified Communications Manager Express, Cisco Unified Border Element and Unified Communications Manager to an external Firewall to indicate on which UDP ports to expect the media.
UC Manager Express(UCME, Voice Gateways and Cisco Unified Border Element (CUBE) support for Service Advertisement Framework (SAF)	Adds support for SAF which is designed to allow networking applications to discover the existence, location, and configuration of networked services within networks.

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

Agenda

- Cisco IOS Software Release 15 M and T
- Introducing Release 15.0(1)M
- Cisco IOS Packaging
- Release 15.0(1)M Numbering, Support Lifecycle, and Migration Considerations
- Summary

Cisco IOS Packaging Introduction and Benefits

- **Simplification**

  Minimize user disruption during the software selection process

- **Consolidation**

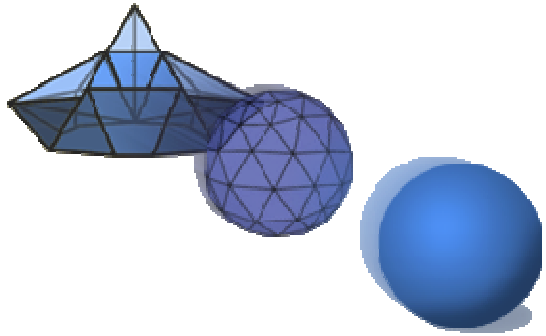
  Streamline packaging across hardware that runs Cisco IOS Software

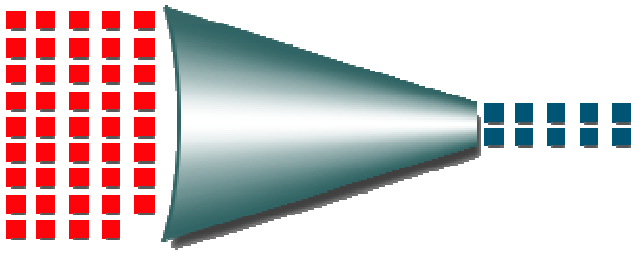
- **Consistency**

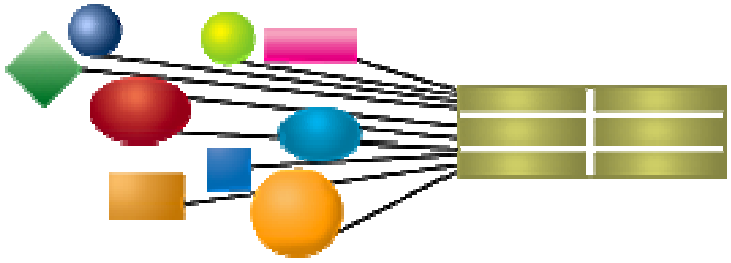
  Consistent image names

  Consistent functionality across hardware that runs Cisco IOS Software

  Consistent Cisco IOS Software pricing

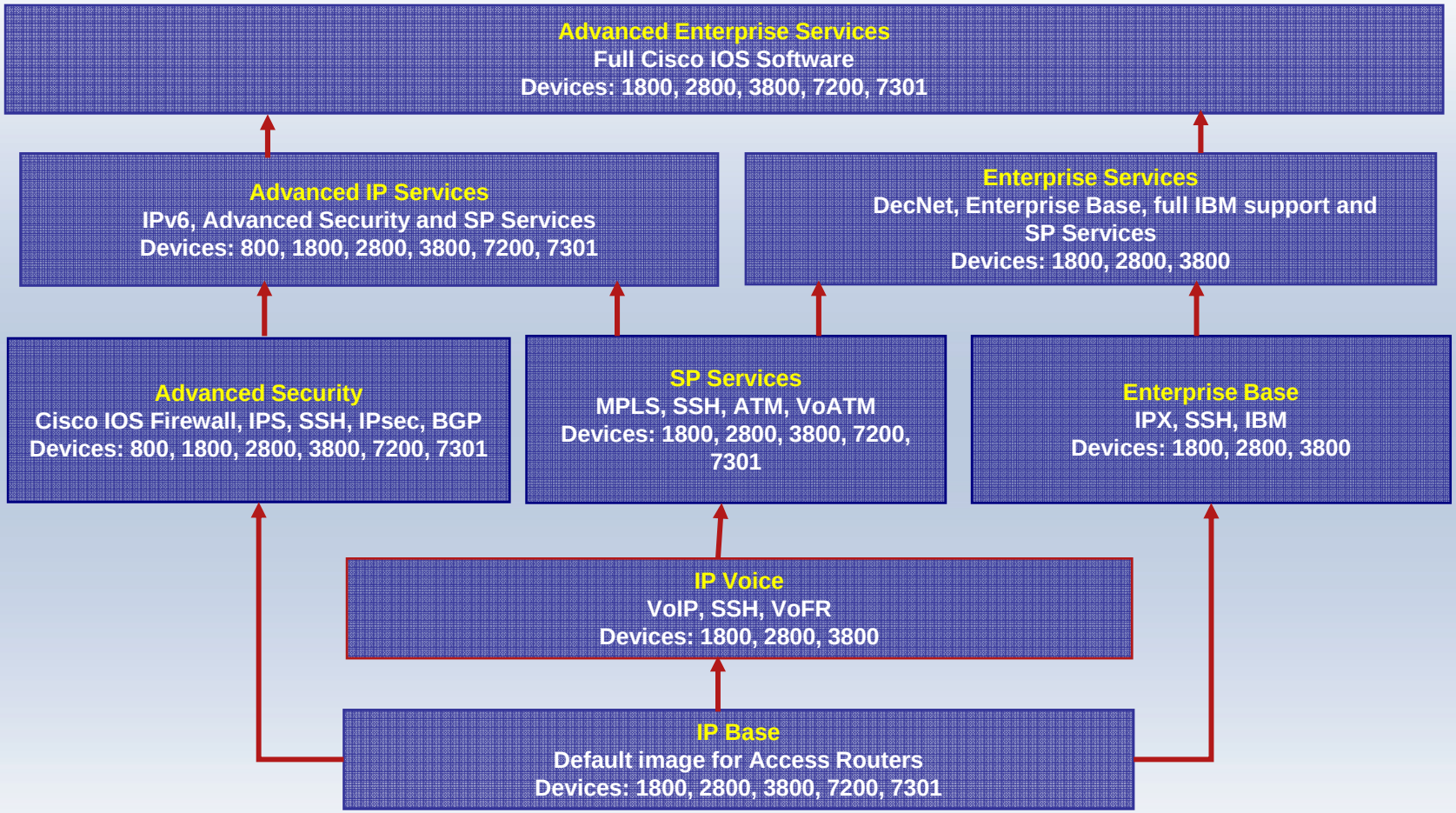






Release 15.0(1)M Feature Sets:

Existing ISR 800, 1800, 2800, 3800, 7200, and 7301 Routers Supported in Release 12.4T



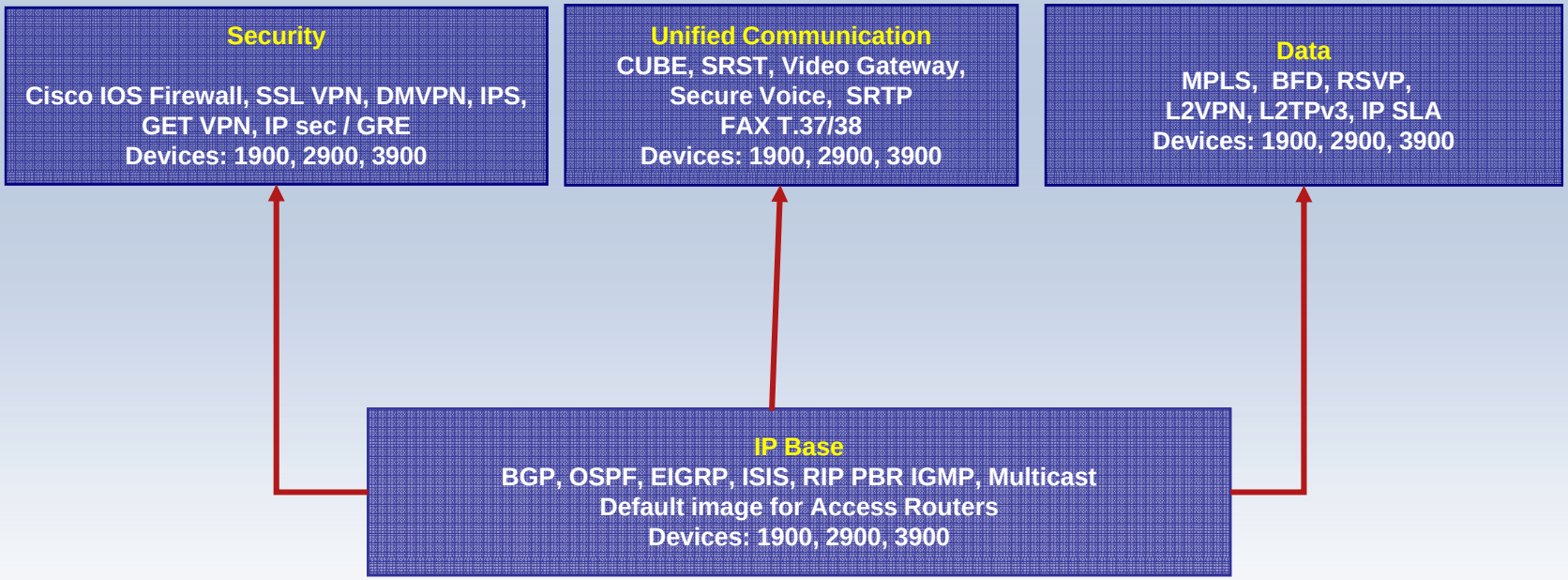
Hardware-specific feature sets may affect respective Cisco IOS Software Package availability by platform. Refer to the Cisco Product & Services support page on Cisco.com to obtain additional information specific to your hardware platform:
http://www.cisco.com/en/US/products/index.html
For more information on Cisco IOS Software packaging visit:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5460/prod_bulletins_list.html

Release 15.0(1)M ISR G2 Feature Sets:

ISR 1900, 2900, and 3900 platforms only

Simplified Software Packaging Model

1. **A single IOS Universal Image will ship with all next Generation ISR Platforms**
2. **IOS technology package upgrades can be done by enabling a new license key, reducing the need for truck-rolls to remote offices**
3. **Pay as you grow ~ Purchase upgrades as you need them via Cisco licensing.**



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

Features Not Supported in Cisco IOS Software Release 15.0(1)M

- **AppleTalk features are not supported from Cisco IOS Software Release 15.0(1)M onward. Refer to the following product bulletin for more details:**

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps5460/product_bulletin_c25-520459.html

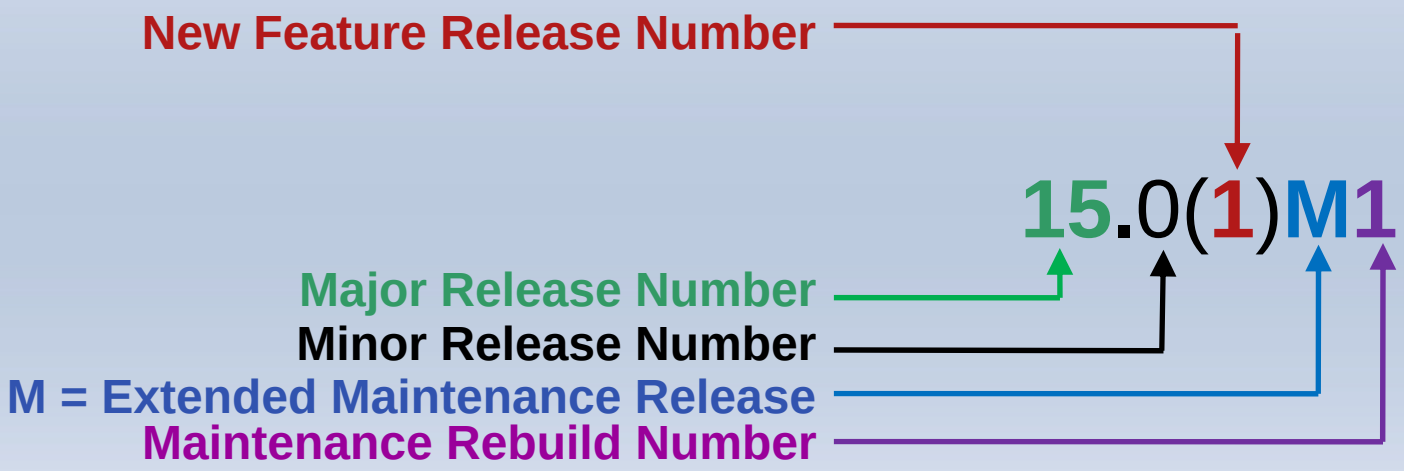
- **Cisco Service Selection Gateway (SSG) feature is not supported from Cisco IOS Software Release 15.0(1)M onward. Refer to the following product bulletin for more information:**

  http://www.cisco.com/en/US/prod/collateral/routers/ps341/end_of_life_notice_c51-501483.html

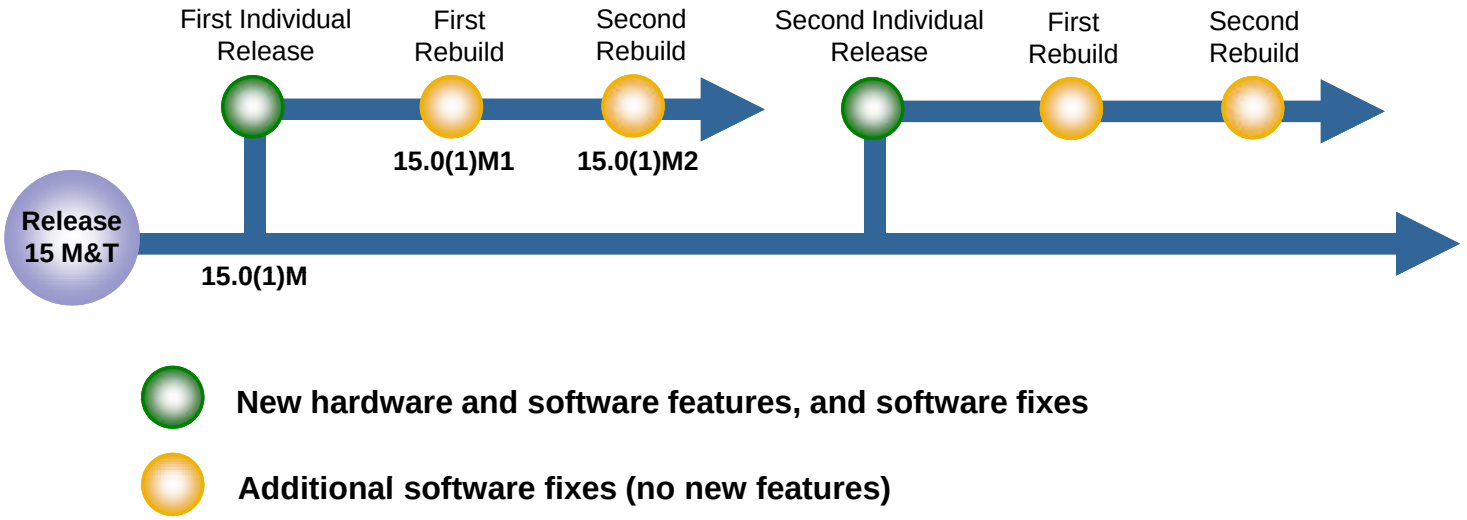
Agenda

- Cisco IOS Software Release 15 M and T
- Introducing Release 15.0(1)M
- Cisco IOS Packaging
- Release 15.0(1)M Numbering, Support Lifecycle, and Migration Considerations
- Summary

Release 15.0(1)M Release Numbering

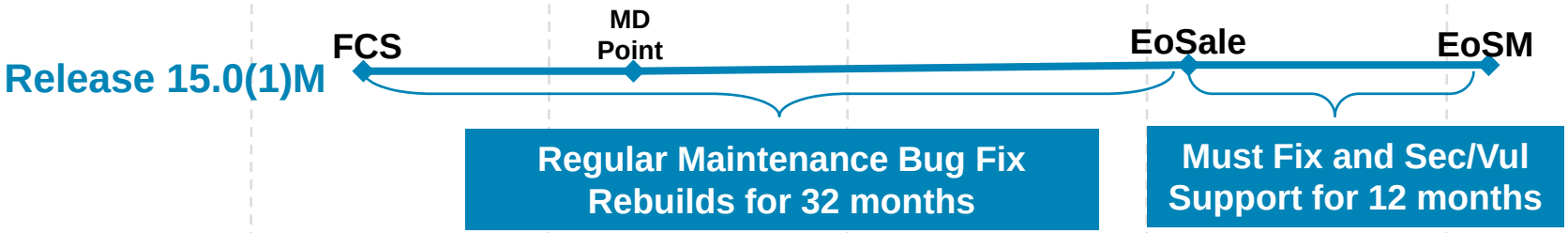


Cisco IOS Software Release 15.0(1)M New Feature Release and Maintenance Rebuild Relationship



- **Release 15.0(1)M includes incremental new software features and hardware support, features previously delivered in Release 12.4T, and software fixes**
- **After its initial introduction, Release 15.0(1)M will receive ongoing maintenance (bug fixes) through release rebuilds**
- **Rebuilds are identified by a release number suffix increment:**
  - **The 1st maintenance rebuild of Release 15.0(1)M will be numbered 15.0(1)M1**
  - **The 2nd maintenance rebuild of Release 15.0(1)M will be numbered 15.0(1)M2**

Release 15.0(1)M * Support Lifecycle and Milestones



Milestone	Definition	Date
First Customer Shipment (FCS)	The date the software release is first available to customers on Cisco Software Download Center http://www.cisco.com/public/sw-center/	Day 0
Maintenance Deployment Point (MD Point)	Maintenance Deployment (MD) designation is based on extensive Cisco internal and customer-focused testing efforts, assessment of the release stability in customer networks, and ongoing Cisco IOS Software improvements.	Typically 9-12 months (3rd or 4th maintenance rebuild) after the initial posting (FCS date) of the release on Cisco.com Software Download Center
End of Sale Date (EoSale)	The day the release is no longer orderable or included in manufacturing shipments of Cisco hardware.	32 months after FCS date
End of Software Maintenance (EoSM)	This is the last date that Cisco Engineering may release any final software maintenance releases or software fixes for the release.	44 months after FCS date

*** Release 15.0(1)M is an Extended Maintenance Release**

Transition from Release 12.4 and 12.4T

- **Release 12.4(15)T - extended support until January, 2012**
- **Release 12.4(24)T - last 12.4T new feature release**
- **Release 12.4(25) - last 12.4 Mainline release**
- **Next Extended Maintenance release after 12.4(25) is Release 15.0(1)M**
- **Release 15.0(1)M inherits features from 12.4(24)T, adds incremental new features, hardware support**

Migration Scenarios from 12.4 and 12.4T *

Release	End of Sale Announcement	End of Sale Date	End of Software Maintenance Date	Software Migration Path
All 12.4T releases before Release 12.4(15)T	July 1, 2009	July 1, 2009	July 1, 2009	Release 15.0(1)M , or Release 12.4(15)T (See Note *)
Release 12.4(15)T	January, 2010	January, 2011	January, 2012	Release 15.0(1)M (See Note *)
Release 12.4(20)T and Release 12.4(22)T	July 1, 2009	December 30, 2009	June 30, 2010. Bug fix support after 12/30/09 is provided via Release 15.0(1)M and later releases.	Release 15.0(1)M
Release 12.4(24)T	January, 2010	June, 2010	January, 2011	Release 15.0(1)M
Release 12.4 Mainline	January, 2010	January, 2011	January, 2012	Release 15.0(1)M (See note *) Release 12.4(25) for bug fix support on 12.4 Mainline (until end of software maintenance for 12.4 Mainline).

* NOTE: Several Cisco hardware platforms ended support on Release 12.4(15)T, and also end support on 12.4 Mainline. These platforms will not be supported in Release 15.0(1)M and later releases. Refer to the following bulletin for more information:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6968/ps6441/product_bulletin_c25_466578.html

Agenda

- Cisco IOS Software Release 15 M and T
- Introducing Release 15.0(1)M
- Cisco IOS Packaging
- Release 15.0(1)M Numbering, Support Lifecycle, and Migration Considerations
- Summary

Summary

Cisco IOS Software Release 15.0(1)M

- **First in a series of individual Cisco IOS Release 15 M & T releases, each of which delivers aggregate functionality via its predecessor, and introduces new technology and hardware support:**
  - **Service Advertisement Framework (SAF), enabling network applications to dynamically discover the existence and configuration of other networked application and services.**
  - **Flexible NetFlow and NBAR integration, combining the strengths of both features to provide layers 2-7 per-flow application visibility and statistics.**
  - **Embedded Event Manager Version 3.1, which introduces significant enhancements for event detection, notification mechanisms, and command execution capabilities.**
  - **Support for the Cisco ISR G2 1900, 2900, and 3900 Series Routers, helping businesses and service providers transform the branch office experience and better enable rich media applications such as high definition video and on-demand services.**

References

- Release 15.0(1)M, New Features and Hardware Support, Product Bulletin No. 561938

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps10587/ps10591/ps10621/product_bulletin_c25-561938.html

- Cisco IOS and NX-OS Software Page

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

- Download Cisco IOS Software Releases (Cisco.com login access required)

  http://www.cisco.com/kobayashi/sw-center/index.shtml

- Cisco Feature Navigator – A web-based application that quickly matches Cisco IOS Software release features to supported hardware

  http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

- Cisco Products and Services End of Life Policy

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