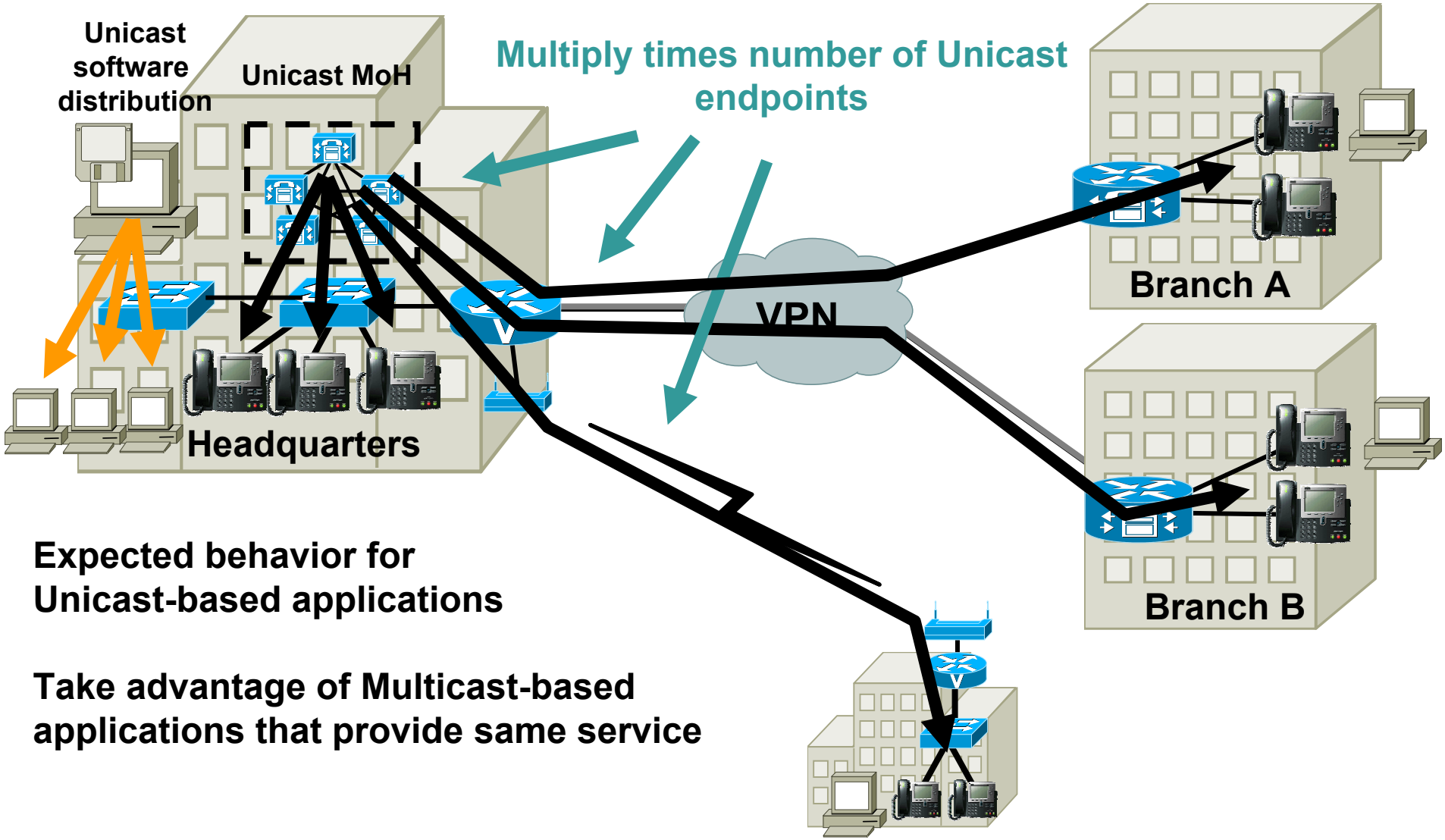
Secure Multicast

Agenda

- Why IP Multicast?
- IP Multicast Security Challenges
- Secure IP Multicast Solution and Benefits
- Technical Details
- Platform Support and Useful Links

Why IP Multicast?

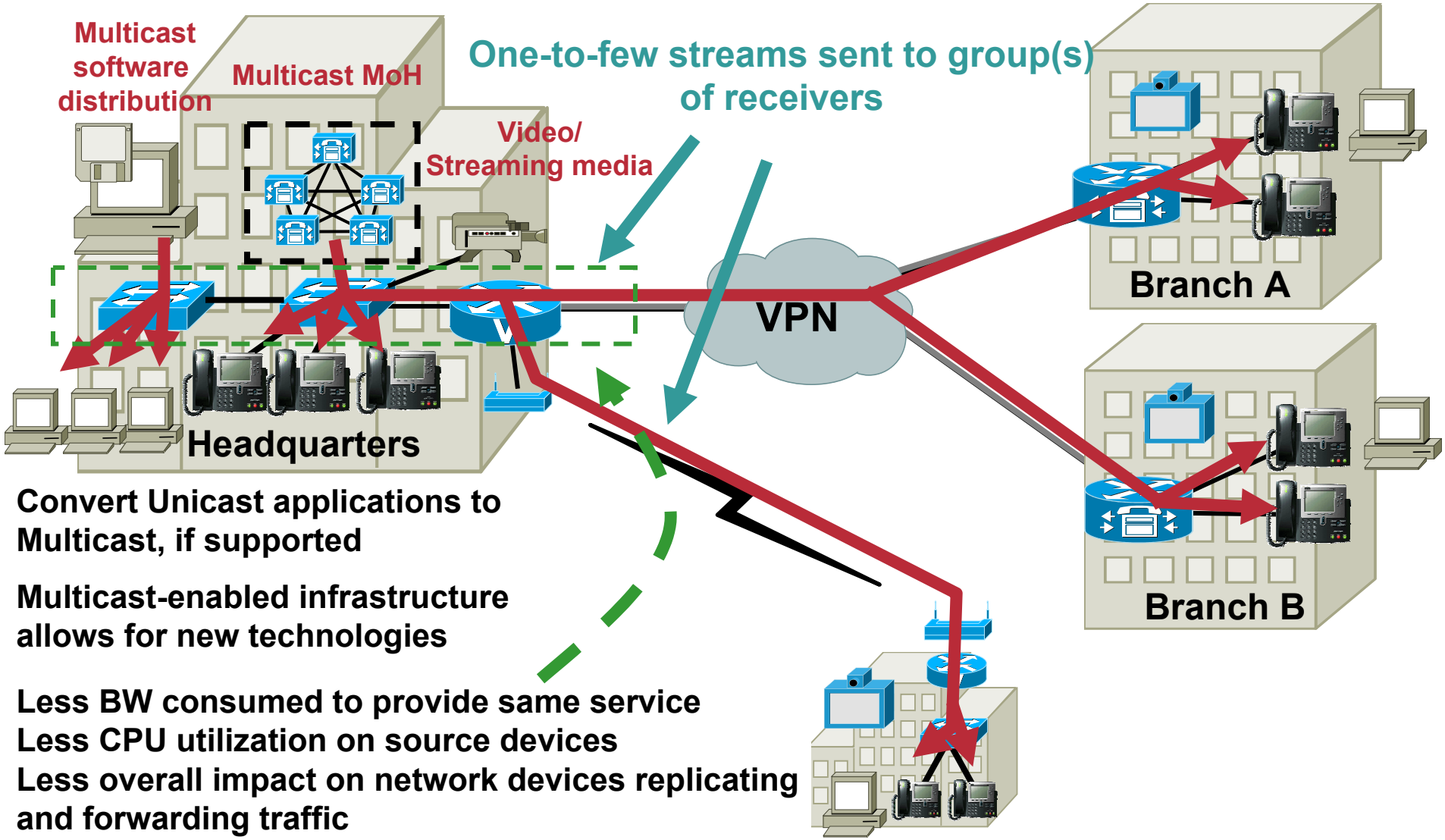
Unicast vs. Multicast



Expected behavior for Unicast-based applications

Take advantage of Multicast-based applications that provide same service

Unicast vs. Multicast



Convert Unicast applications to Multicast, if supported

Multicast-enabled infrastructure allows for new technologies

Less BW consumed to provide same service
Less CPU utilization on source devices
Less overall impact on network devices replicating and forwarding traffic

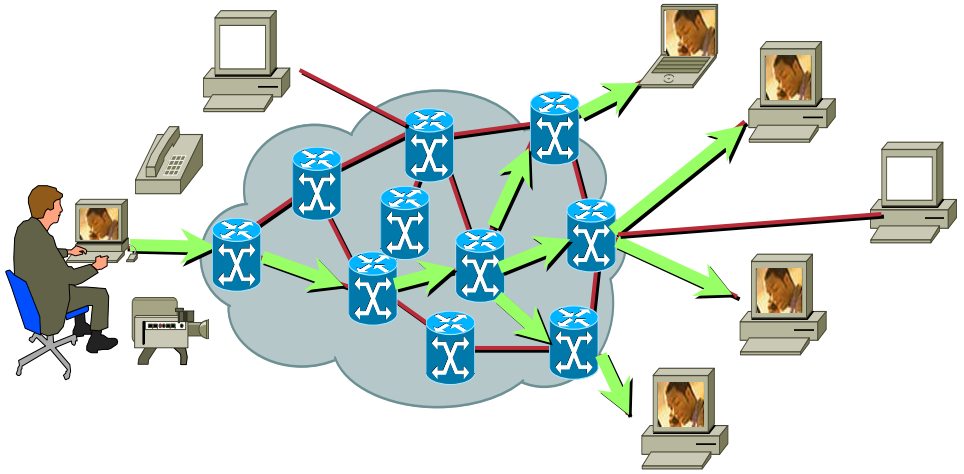
Why IP Multicast over VPN?

- Efficiently deploy and scale distributed group applications across a VPN
- Reduce network load associated with sending the same data to multiple receivers
- Alleviates high host/router processing requirements for serving individual connections across VPN tunnels
- To IP Multicast, VPN is just another WAN type

IP Multicast Security Challenges

Secure Multicast : Business Problem

Securely and efficiently protect Multicast network data traffic from multimedia, video, voice, on an IP network



Benefits:

- Help in complying with mandates for encryption
- Increase productivity & save cost

Applications		
Service Provider	**Enterprise**	**Small/Medium Business**
• Native IPv4 / IPv6 Internet secured Multicast • Secured Multicast VPN • Triple-play & video broadcast	• Stock trading, corporate communications, e-learning, hoot-and-holler over IP, videoconferencing, content delivery, conferencing	• e-learning • IP surveillance • Content delivery • Videoconferencing

Cisco IOS Secure Multicast

Overcoming Existing IP Multicast Security Challenges

Cisco.com

Tunnel Based		Secure Multicast
Bolted on	→	Built in
Complex architecture	→	Seamless integration
Wasted capital	→	Investment protection
Rigid design	→	Flexible design
Simple transport	→	Intelligent transport

Fueled by demand for agility within a security framework

Secure IP Multicast Solution and Benefits

What is Secure Multicast

Features necessary to secure IP Multicast group traffic originating on or flowing through a Cisco IOS® device

- **A new security framework**

  Architecture and components necessary in order for Cisco IOS Software to provide scalable security to IP Multicast group traffic

- **A new key management paradigm**

  An ISAMKP domain of interpretation (DOI) for group key management called the “group domain of interpretation" (GDOI)

- **A way to provide scalable security to native IP Multicast packets**

  Scalable security (e.g. encryption and authentication) to native IP Multicast packets

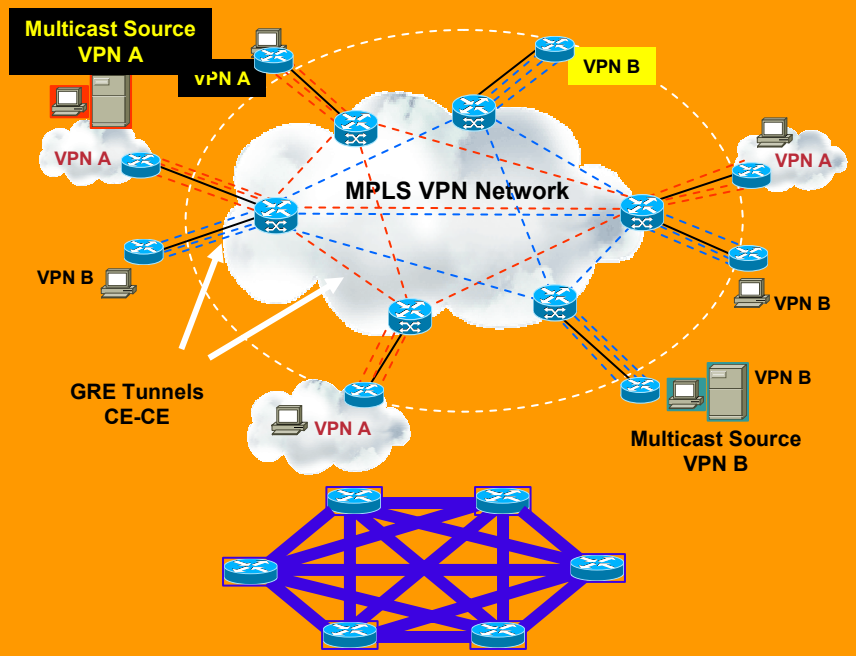
  Native Multicast encryption avoids the needless packet replication that occurs when encapsulating IP Multicast packets using Unicast tunnels

Benefits of Cisco IOS Secure Multicast in VPN Deployments

Previous Limitation	Feature and Associated Benefits
Multicast traffic encryption was supported through IPsec tunnels: Not scalable Difficult to troubleshoot Limited QoS support	• Group mode encryption with group SA: No need for 2 IPSec + 1 IKE SA *per spoke* Allows much higher scalability, simplifies troubleshooting • Group controller/key server: Key and policies distributed using centralized mechanism • Extensible standards-based framework: Supports Multicast today and extends to support Unicast in future
No optimal security for native multicast in mVPN type architectures	Native Multicast encryption • Supports Multicast encryption in mVPN architectures • Day-one transparent interoperability between various core Cisco IOS® technologies; e.g. native multicast encryption
Overlay VPN network Overlay routing resulting in suboptimal convergence	Leverage core for Multicast replication • Investment protection: New architecture leverages the core and investment costs spent on building core

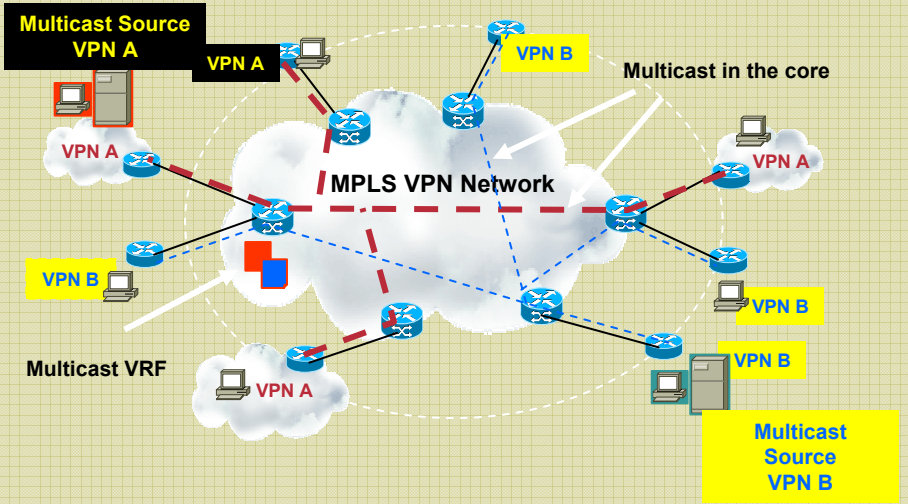
Secure Multicast Application: mVPN

Before



- Scalability – an issue (N^2 problem)
- Highly inefficient

After: Secure Multicast



- Multicast data traffic protected by IPSec
- Multicast key distribution solved by GDOI
- Allows MPLS VPN customers to access Multicast content
- Standards based

Large-Scale IPSec WAN Aggregation
Deployment Models

Comparison of Deployment Models

	Dynamic Routing	Meshing	HA	QoS	Multicast
IPSec only	No	No	Stateful failover	Yes*	No
IPSec and GRE	Yes	No	RP	Yes*	Yes (hub replicated)
DMVPN (Hub-Spoke)	Yes	No	RP	Yes*	Yes (hub replicated)
DMVPN (Spoke-Spoke)	Yes	Dynamic full mesh	RP	Yes*	Yes (hub-spoke)
IPSec VTI/Easy VPN	No	No	Stateful failover	Yes*	No
Secure Multicast	Yes	Yes	RP	Yes*	Scalable

*Note: See specific topologies for limitations

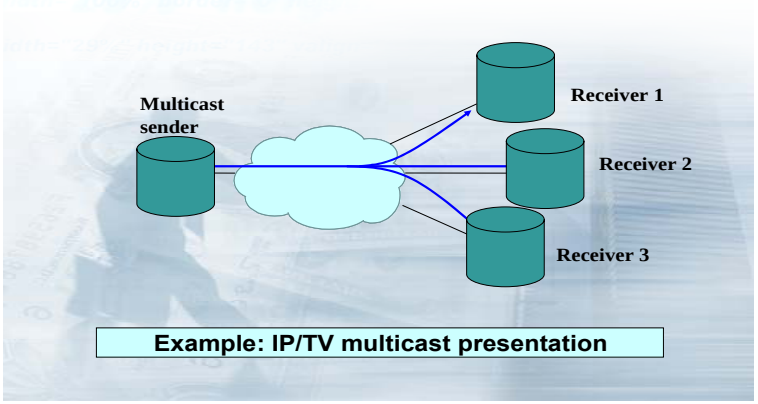
Secure IP Multicast Detailed Presentation Continued: Technical Details

What's a Group?

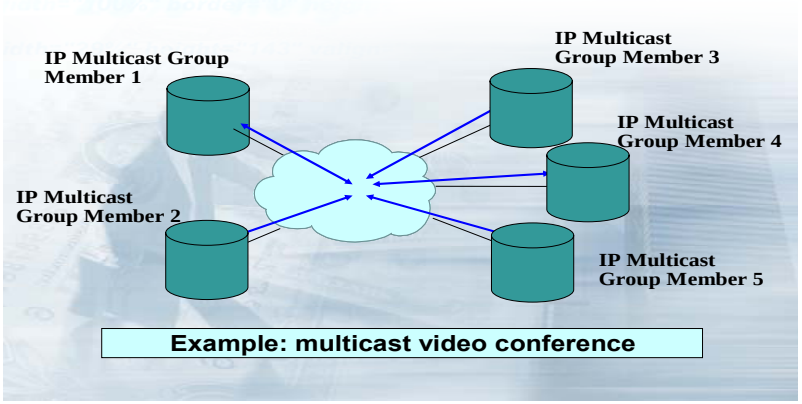
- Three or more parties who send and receive the same data transmitted over a network
- Transmission can be Multicast, or Unicast (identical data sent to multiple parties)
- Parties can be routers, PCs, telephones, any IP device
- There are many different examples of group topologies

Multicast Group Models: Example

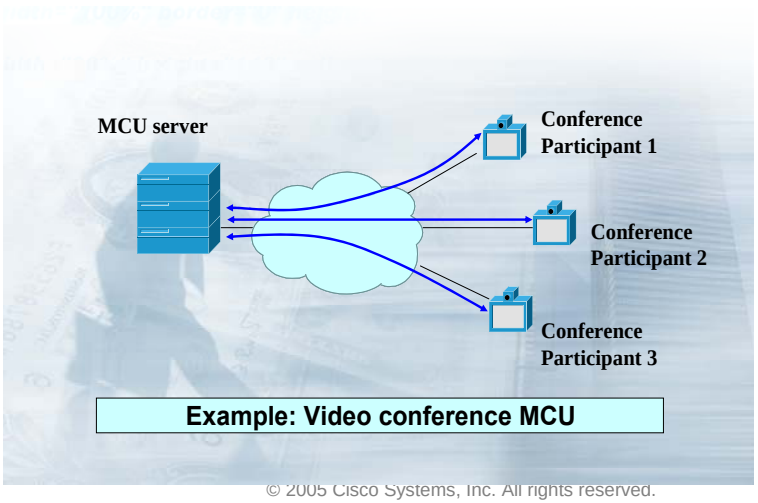
Multicast Models: Single-source Multicast



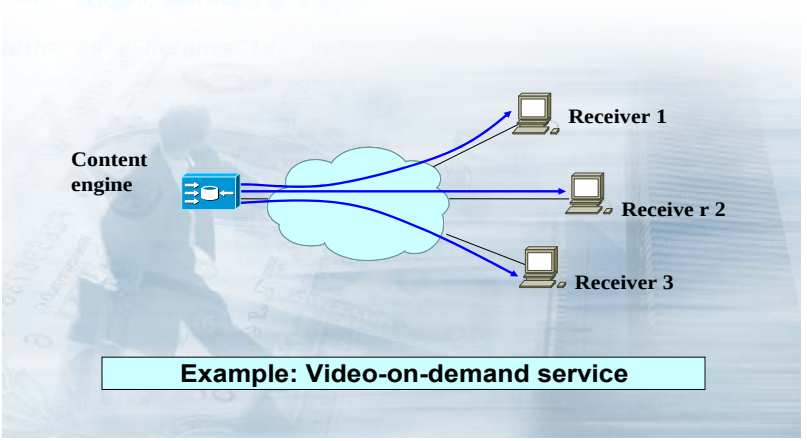
Multicast Models: Multiple-source Multicast



Multicast Models: Multipoint control unit



Multicast Models: Publish-Subscribe unicast



Secure Groups

To secure a group you need:

- Data Encryption Protocol
  - IPSec
  - SRTP
- Key Management Protocol
  - Provides keys for data encryption

IPSec Key Management

- **Pair-wise key management**
  - **IKE**
  - **KINK**
  - **Manual IPSec keys**
- **Group key management**
  - **Manual IPSec keys**
  - **GDOI (Group domain of interpretation for ISAKMP)**

GDOI enables native Multicast encryption

Relationship of GDOI to IKE: GDOI Coexists with IKE

- **IKE Phase 1 is used to provide confidentiality, integrity, and replay protection**

  IKE Phase 1 is UNCHANGED

- **A newly defined Phase 2 exchange (called GDOI registration) is run rather than IKE Phase 2.**

  IKE Phase 2 is UNUSED **and** UNCHANGED**.**

- **A new DOI number is used to differentiate GDOI exchanges from IKE Phase 2**

  At the end of IKE Phase 1 a state machine looks at the DOI number to determine next exchange

- **A GDOI service must listen on a port other than port 500 (IKE)**

Quick Comparison of IKEv1, IKEv2 vs. GDOI

	IKEv1	IKEv2	GDOI
RFC documents	2407/2408/ 2409	**RFC 4306**	**RFC 3547**
UDP port	500, 4500	500, **4500**	848
Phases	2, Ph. 1 (6/3 messages), Ph. 2 (3 messages)	2, Ph. 1 (4 messages), Ph. 2 (2 messages)	2, Ph. 1 (6/3 messages), Ph. 2 (4 messages)
Authentication Type	Signature, PSK, PKI	**Signature, PSK, PKI**	**Signature, PSK, PKI**
SA negotiation	Responder selects initiator's proposal	**Same as IKEV1, proposal structure simplified**	**Not negotiated, GDOI is used to push keys and policies**
Identity hiding	Yes in MM, No in AM	**Yes**	**Yes in MM, No in AM**
Keep-alives	No	**Yes**	**No**
Anti-DoS	No	**Yes**	**Yes**
UDP/NAT	No	**Yes**	**No**
Reliability	No	Yes	Yes
PFS	Yes	**Yes**	**Yes**
EAP/CP	No	**Yes**	**No**

RFC 3547—GDOI (Group Domain of Interpretation)

Spec located at: http://www.rfc-archive.org/getrfc.php?rfc=3547

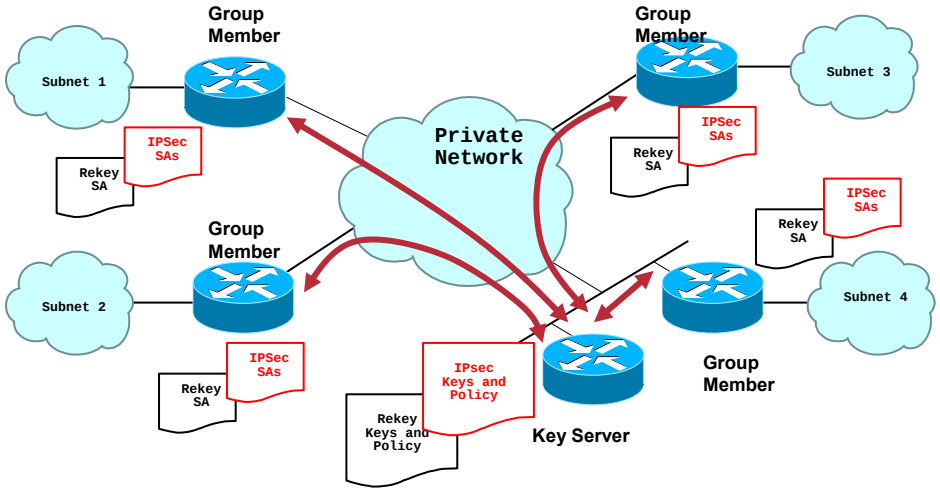
- An ISAKMP DOI for group key management
- RFC 3547—Cisco® championed the effort
- GDOI specification presents an ISAMKP DOI for group key management to support secure group communications
- GDOI describes a protocol for a group of systems (“group members”) to download keys and security policy from a key server
- GDOI manages group security associations, which are used by IPSec and potentially other data security protocols running at the IP or application layers

Secure Multicast: Implementation of Group Domain of Interpretation (GDOI)

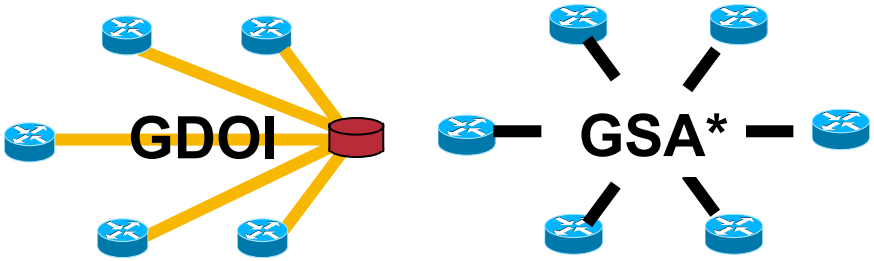
Key Distribution
Group domain of interpretation

- Key distribution mechanism (RFC3547)
  - IETF Multicast Security (msec) WG
- Group member security protections
  - IKE Phase 1 provides member authentication, confidentiality, and integrity
  - GDOI registration provides authorization and replay protection
- Distribute keys and policy for groups
  - –Security associations
  - –Secret keys, public keys
- Efficiently adjust group membership
- Intended for use with small or large groups.
  - –The desire to support large groups drives the design.

Group Domain of Interpretation



Addressing State Complexity



* GSA = Group Security Association

GDOI Group Key management

- In a group key management model, GDOI is the protocol run between a group member and a "group controller/key server" (GCKS).
- The GDOI protocol establishes security associations among authorized group members.
- A group member *registers* with the key server to obtain keys.
- The GDOI registration defines two phases of negotiation.
- Phase I is protected via IKE Phase I.
- The key server *rekeys* the group (pushes new keys) when needed. Rekey messages can be IP multicast packets for efficiency.
- Public signature keys and preshared keys, the only methods of IKE authentication.

GDOI Exchanges

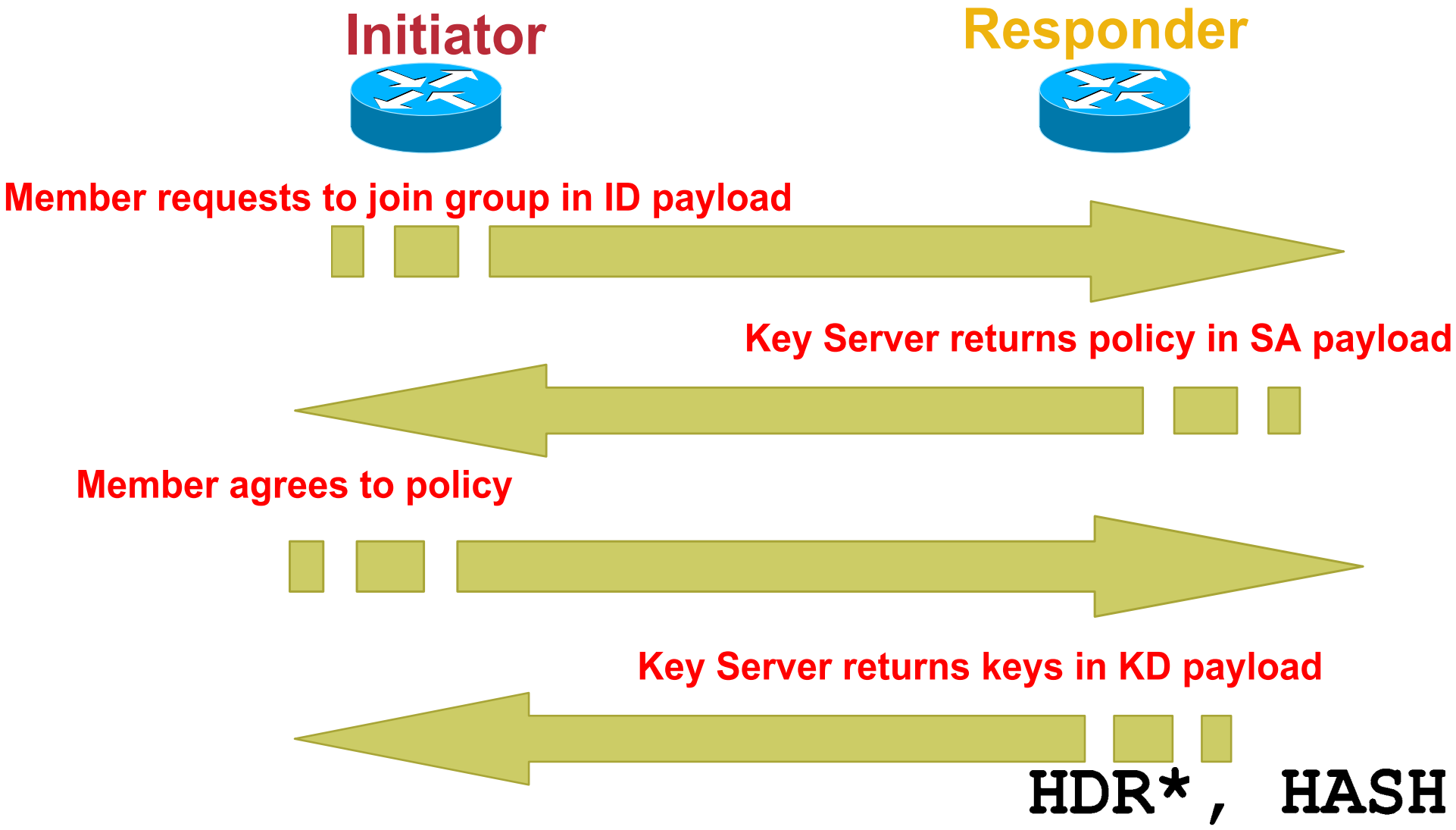
- **GDOI defines a registration exchange for initial group key mgmt**

  Follows the IKE Phase 1

- **GDOI defines a rekey exchange for subsequent key updates**

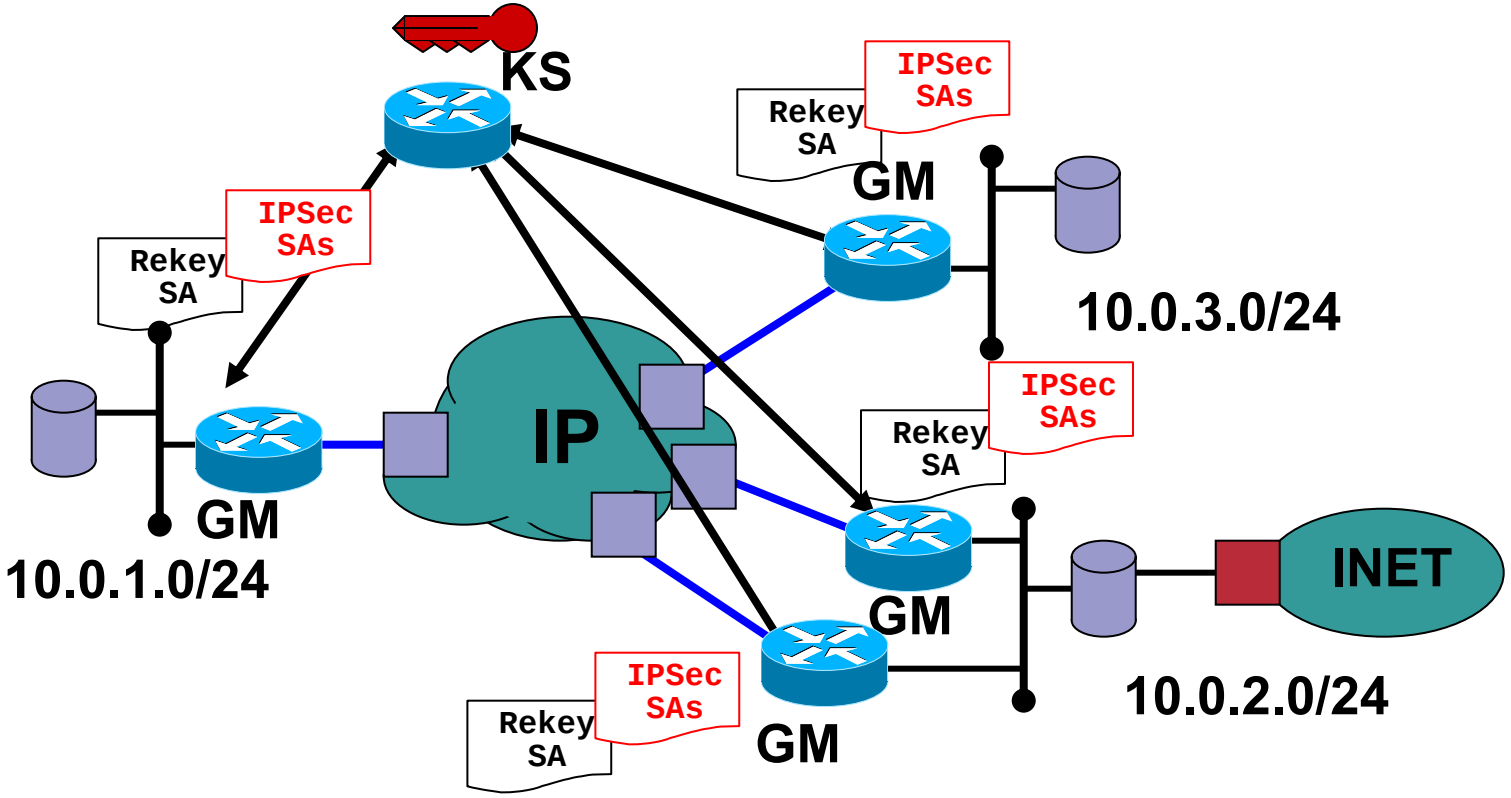
  Can be multicast for efficiency

Registration Protocol



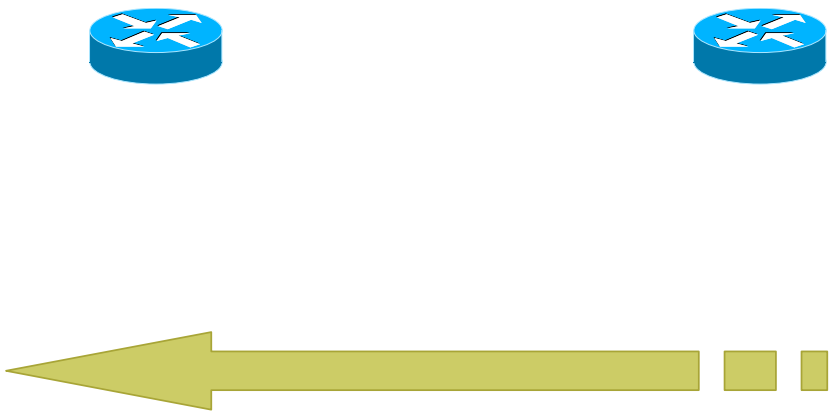
GDOI Registration

Key Distribution
Group domain
of interpretation



- Each router registers with the key server. The key server authenticates the router, performs an authorization check, and downloads the encryption policy and keys to the router

Rekey Protocol



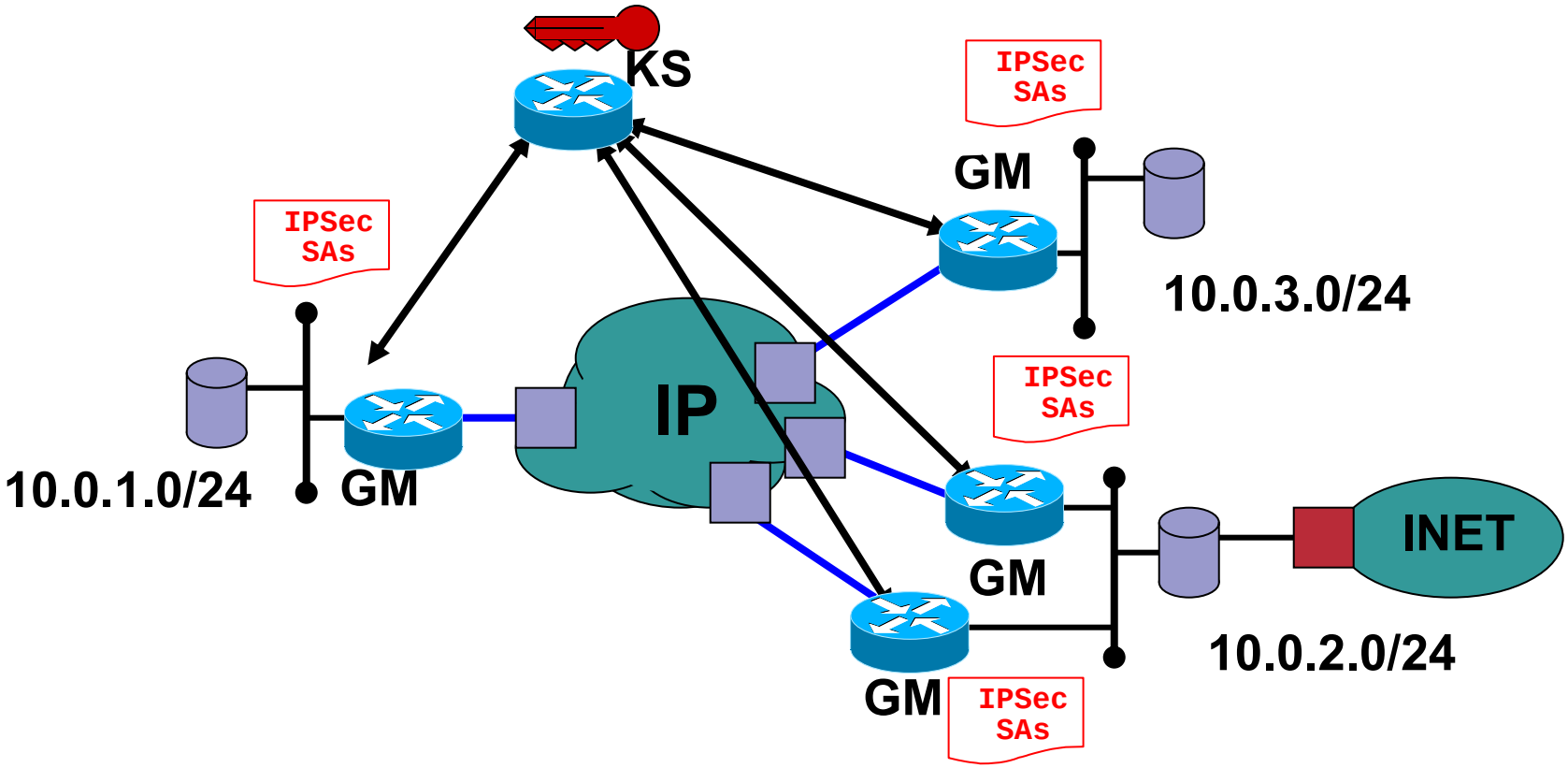
- The “cookie pair” in the ISAKMP HDR acts as a SPI which identifies the group
- SEQ contains a counter used for replay protection
- SA and KD are same format as during registration
- SIG contains a digital signature of the packet

Key Server returns keys in

GDOI Rekey

Key Distribution
Group domain
of interpretation

Cisco.com

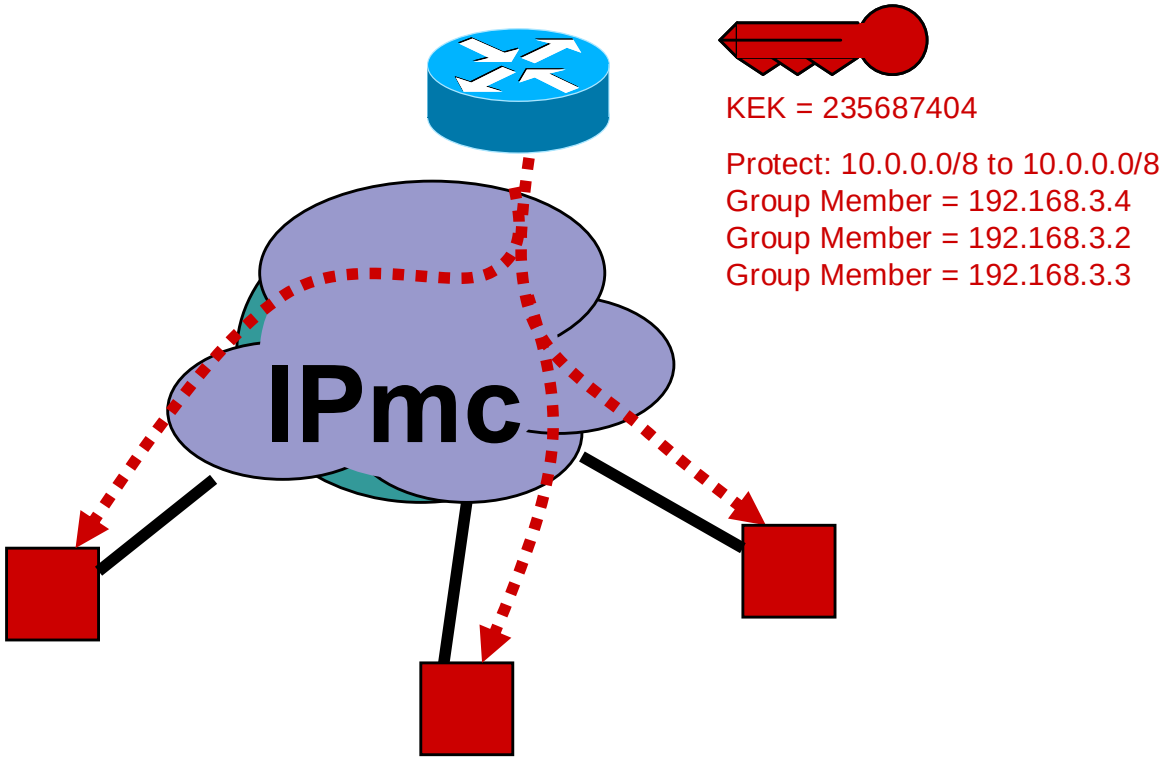


- The key server generates and pushes new IPSec keys and policy to the routers when necessary
- Rekey messages can also cause group members to be ejected from the group

Multicast / Unicast Key Distribution

Key Distribution
Group domain
of interpretation

- **Multicast key distribution over multicast-enabled network**
  - **Via multicast-formatted key message and network replication**
  - **Fallback to group member GDOI Unicast registration**

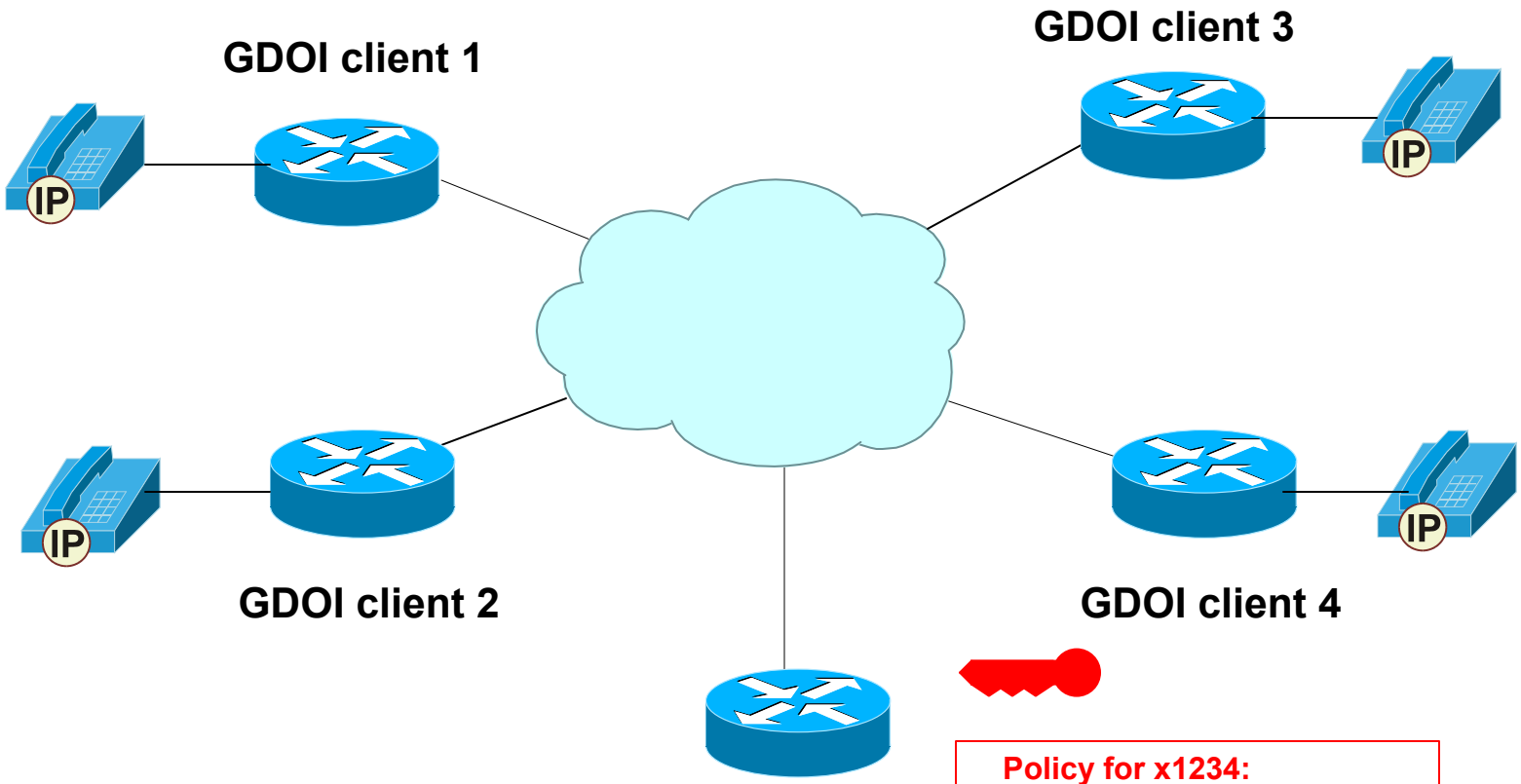


GDOI Example: VoIP Audio Conference

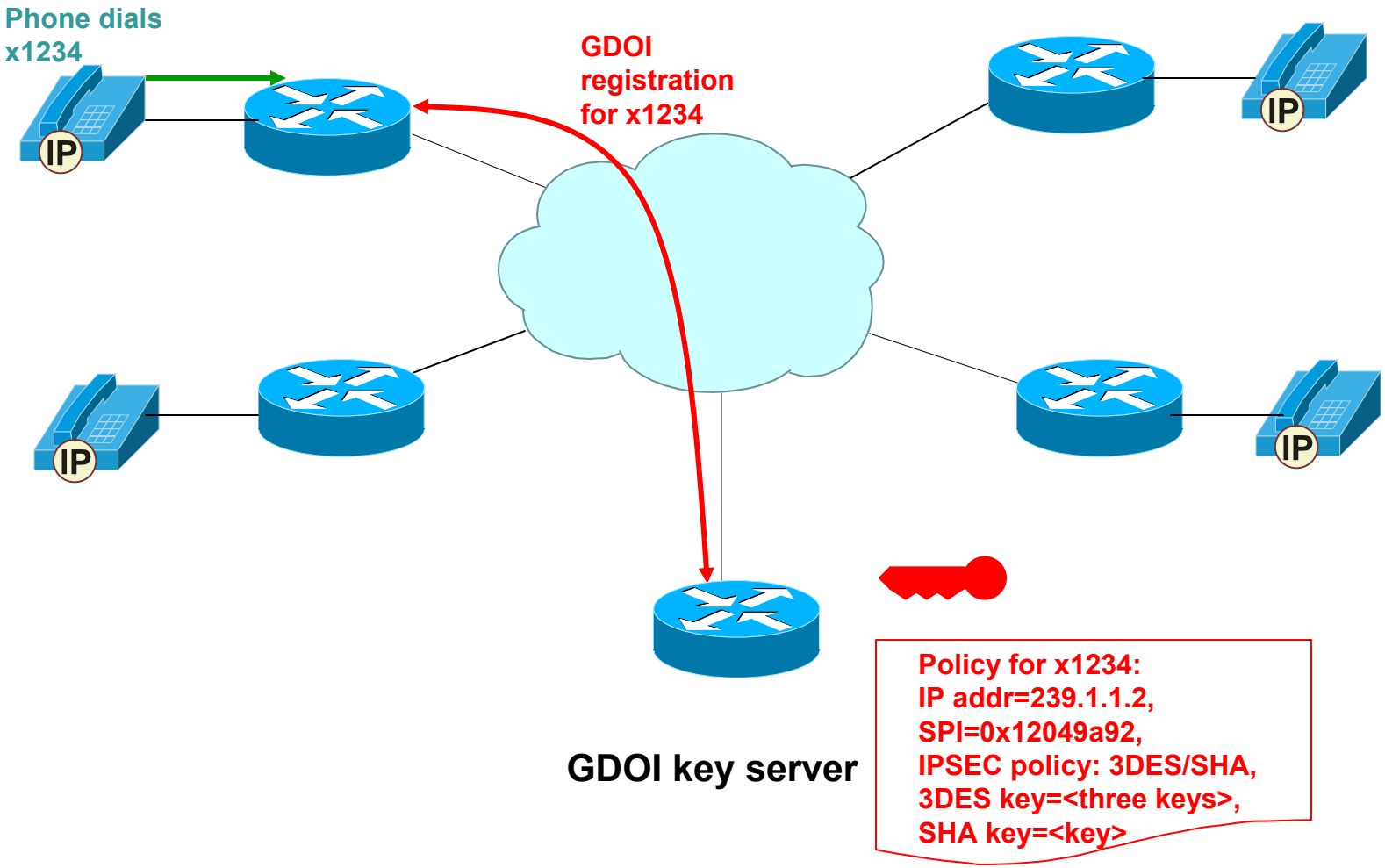
- VoIP phones behind IPSec- or SRTP-capable routers
- An audio conference is reached by dialing a special phone number
- Router recognizes that the phone number is associated with a conference

Note: A theoretical example is illustrated in following slides, but we don't actually have any such teleconference technology for IP phones.

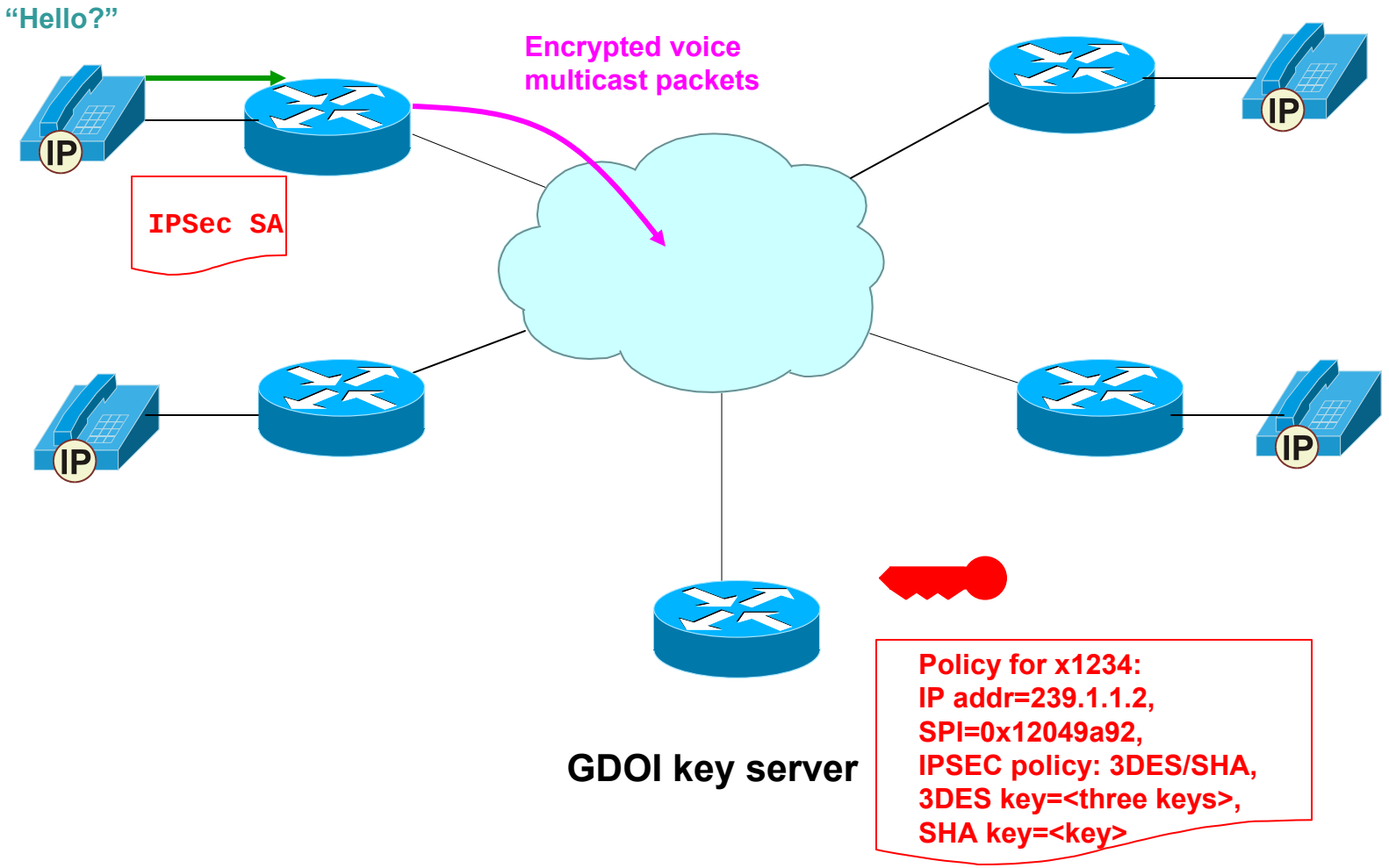
Configuration Setup



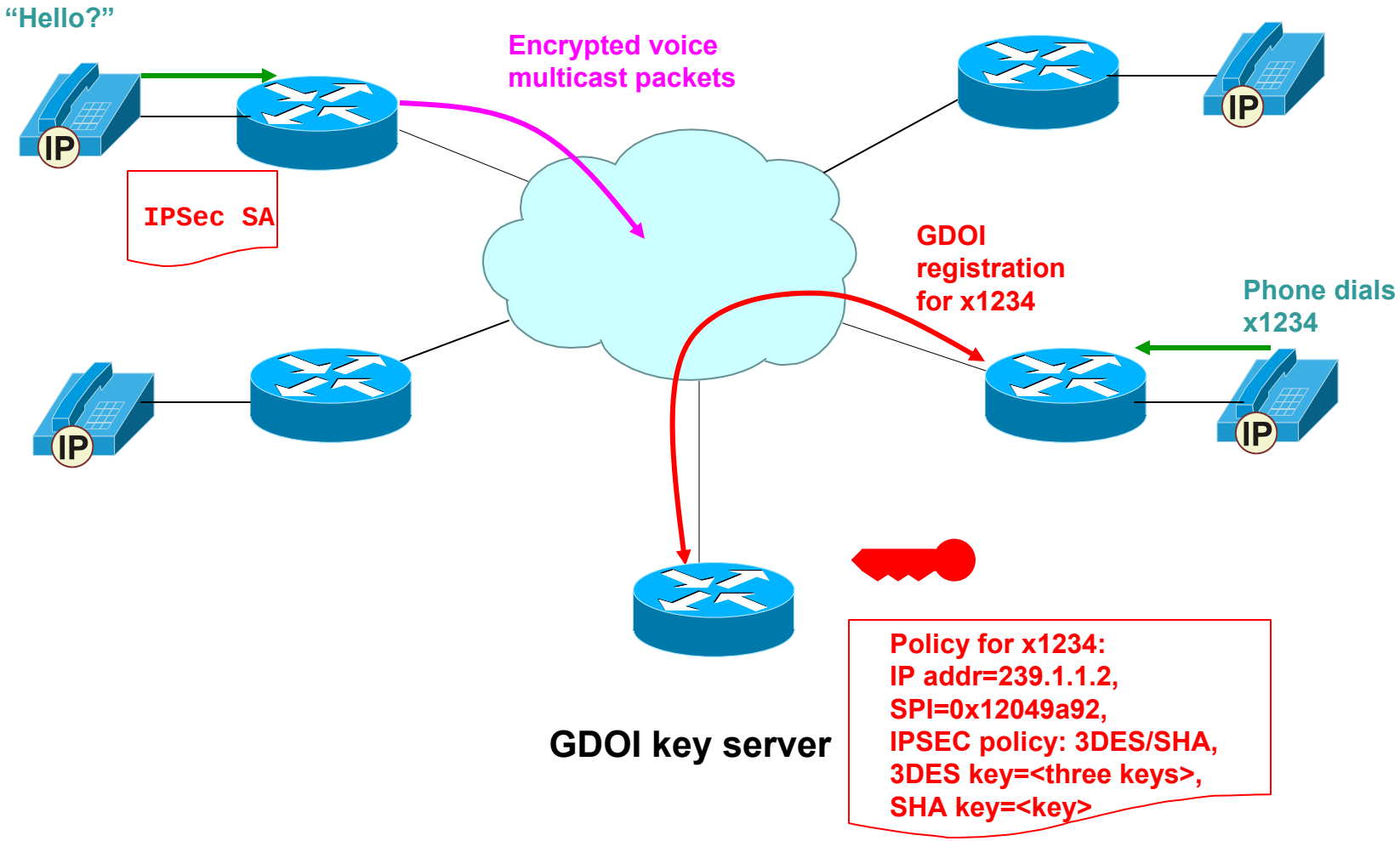
First Client Call



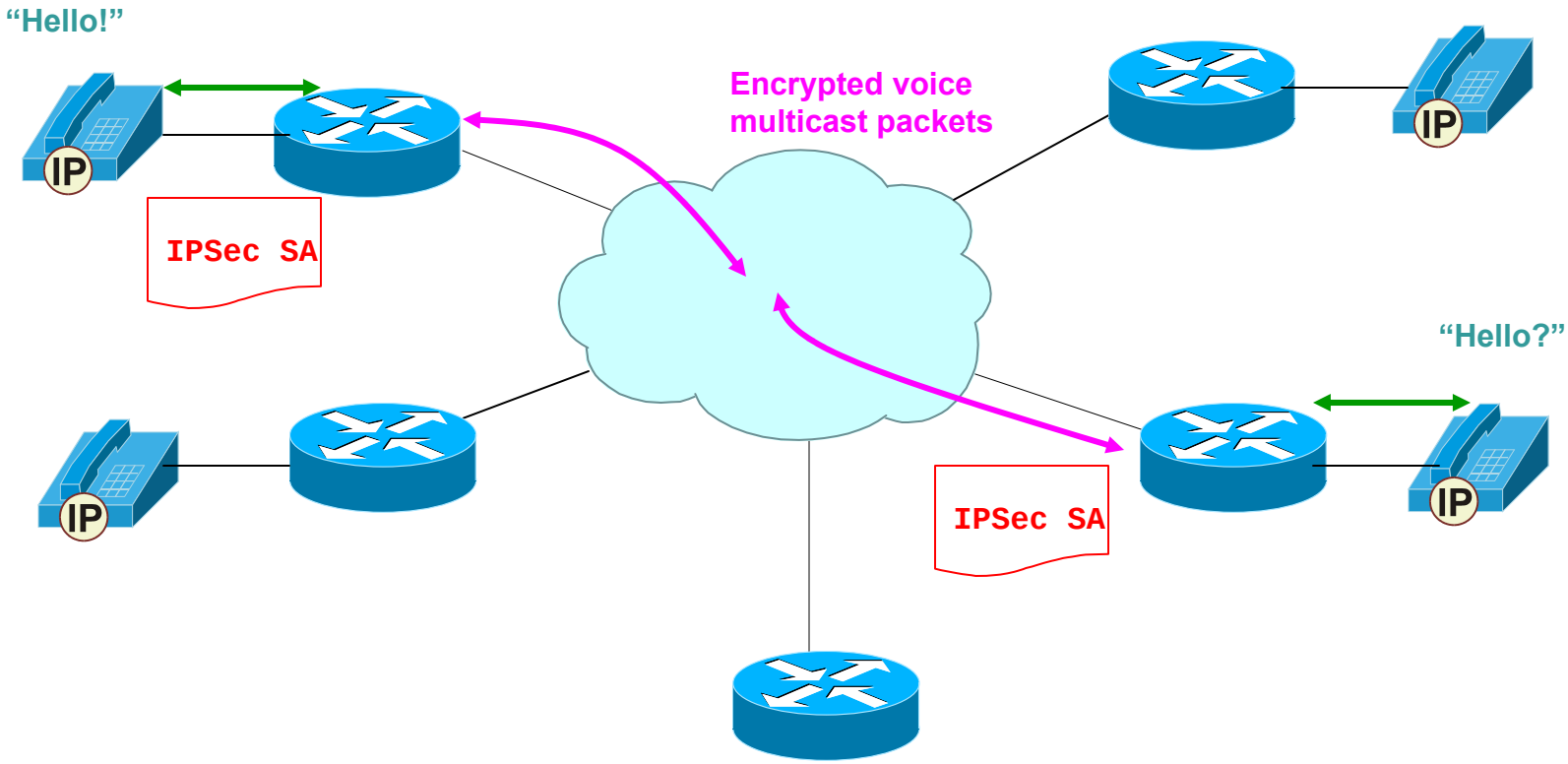
First Client Call Completed



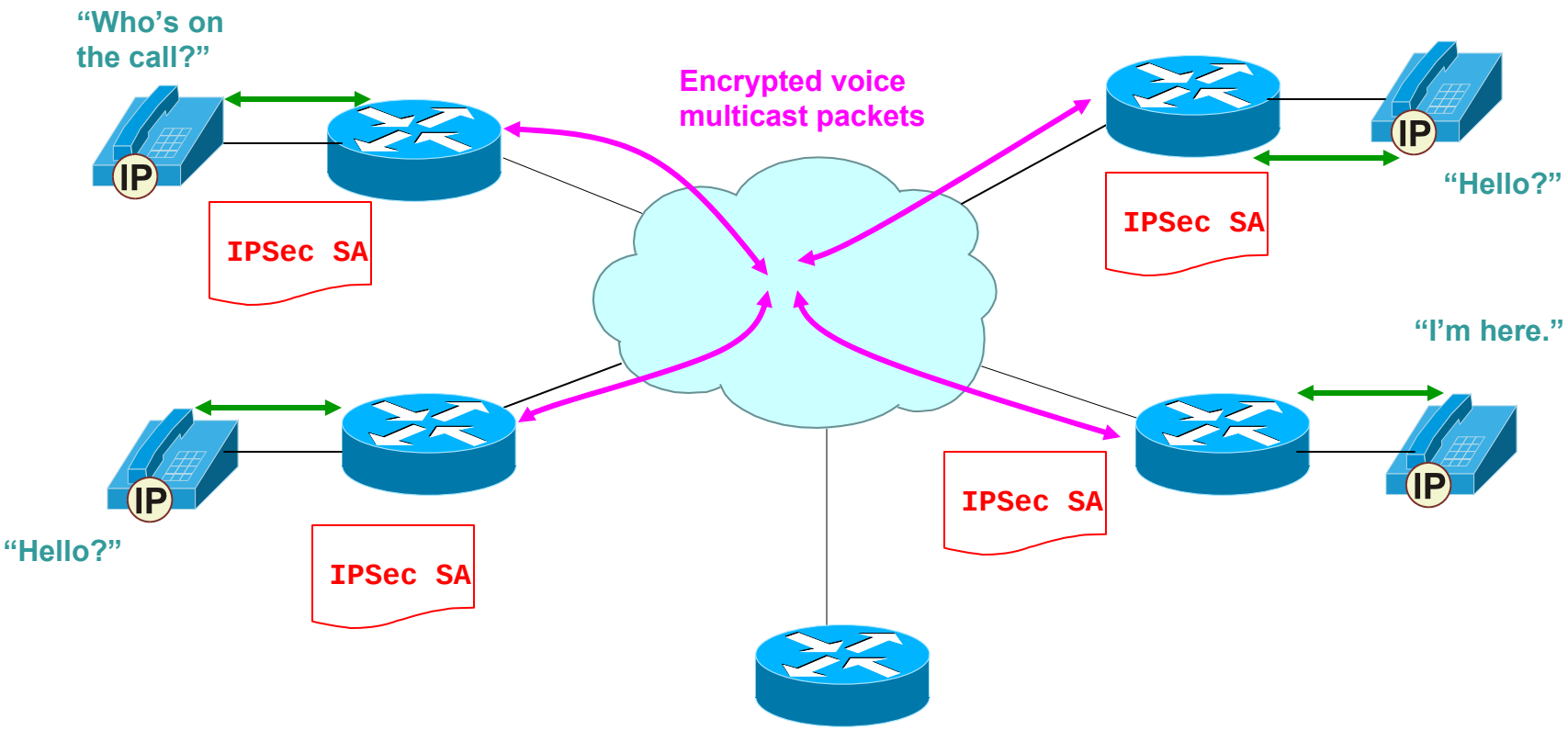
Second Client Call



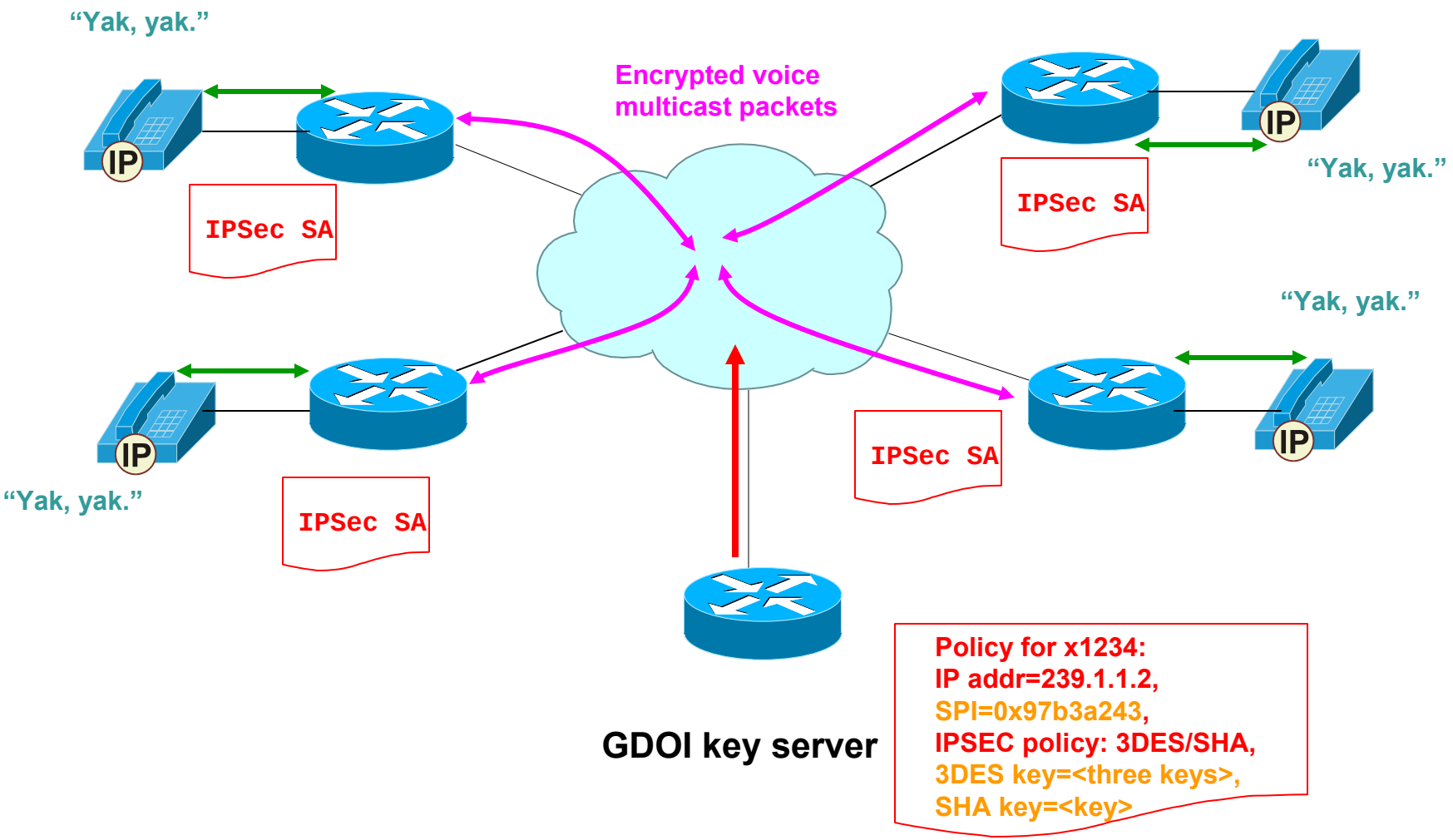
Second Client Call Completed



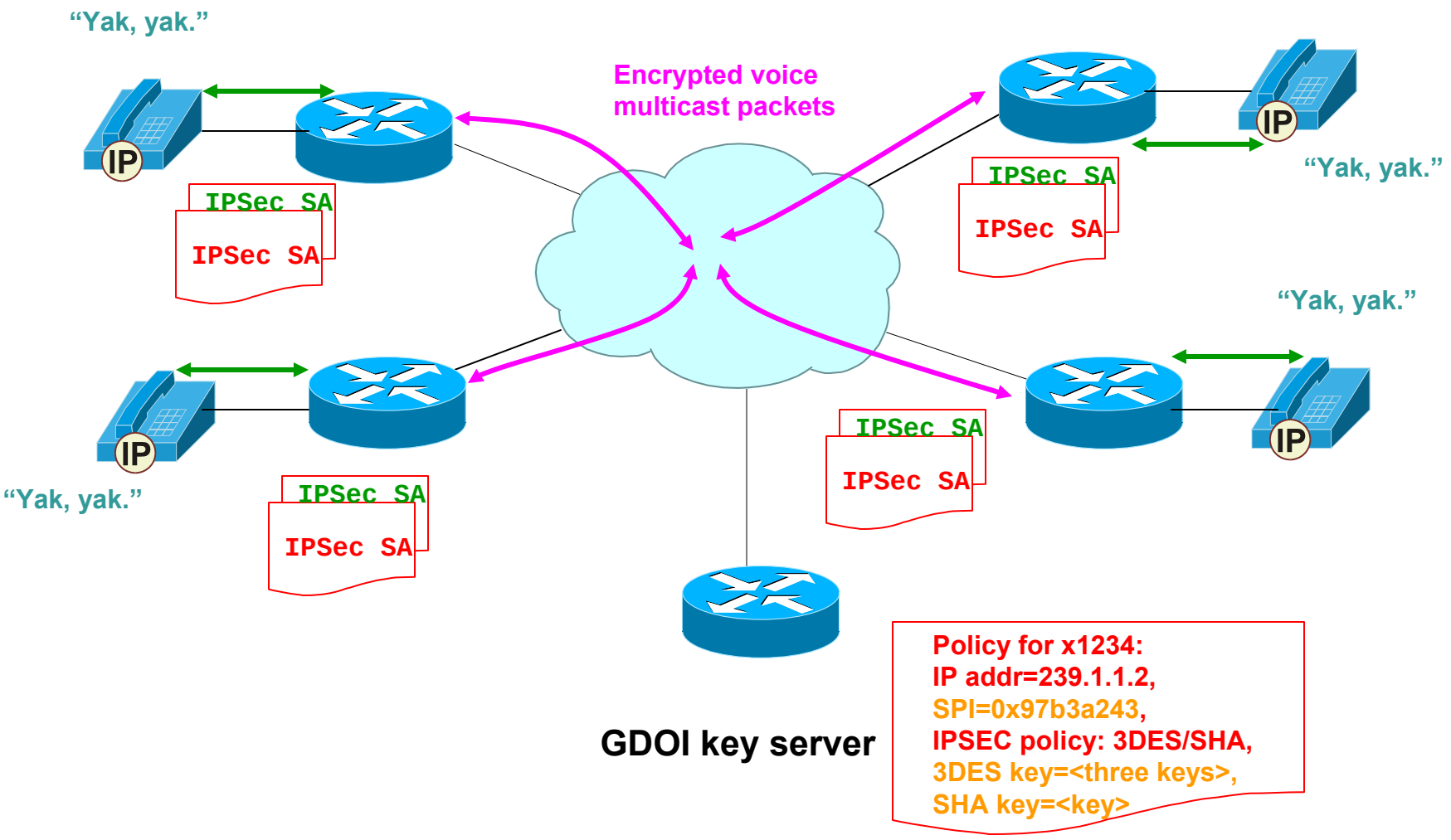
Conference Call Complete



Rekey Message Sent



New SA Installed



Cisco IOS CLI-Configuration

Steps in configuration

- Key server configuration
- Group members
- Clearing a GM registration with a key server
- Verifying secure multicast

ISAKMP Policies

```
crypto isakmp policy 1
authentication pre-share
crypto isakmp key p address 10.0.3.1
crypto isakmp key p address 10.0.3.2
crypto isakmp key p address 10.0.4.2
```

Key Server Config

```
crypto ipsec transform-set e esp-des
crypto ipsec transform-set gdoi-p esp-3des esp-sha-hmac

crypto ipsec profile gdoi-p
set security-association lifetime seconds 3600
set transform-set gdoi-p
crypto gdoi group gdoigroupname
identity number 3333
server local
rekey address ipv4 1020
rekey lifetime seconds 36000
  rekey authentication mypubkey rsa mykeys
  sa ipsec 1
     profile gdoi-p

    match address ipv4 101
```

```
! The following line is the access control list downloaded from the key server to the group member
! This line tells the group members which encrypted traffic is acceptable in this SSM configuration:
access-list 101 permit ip host 10.0.1.1 host 192.168.5.1

! The following line is the rekey access control list to which multicast addresses the rekeys are to be sent:
access-list 102 permit udp host 10.0.5.2 eq 848 host 192.168.1.2 eq 848
```

Cisco IOS CLI-Configuration

Steps in configuration

- Key server configuration
- Group members
- Clearing a GM registration with a key server
- Verifying secure multicast

ISAKMP Policies

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key key1 address 10.0.5.2
```

Group Member Config

```
crypto gdoi group diffint
 identity number 3333
 server address ipv4 10.0.5.2

crypto map diffint 10 gdoi
 set group diffint

interface Loopback0
 ip address 10.65.9.2 255.255.255.255
 ip pim sparse-dense-mode

ip pim bidir-enable
ip pim send-rp-announce Loopback0 scope 16 group-list 1
ip pim send-rp-discovery scope 16
```

```
interface Ethernet0/0
 ip address 10.0.3.2 255.255.255.0
1 ip mtu 1000
 ip pim sparse-dense-mode
 no ip route-cache
 crypto map diffint
```

Cisco IOS CLI-Configuration

Cisco.com

Steps in configuration

- Key server configuration
- Group members
- Clearing a GM registration with a key server
- Verifying secure multicast

clear crypto gdoi

Clears current group-member registration with the key server and starts a new registration.

All current group-member policy is deleted. A new registration is started.

show crypto gdoi

Displays information about a GDOI configuration.

Multicast Group Security Configuration

Cisco.com

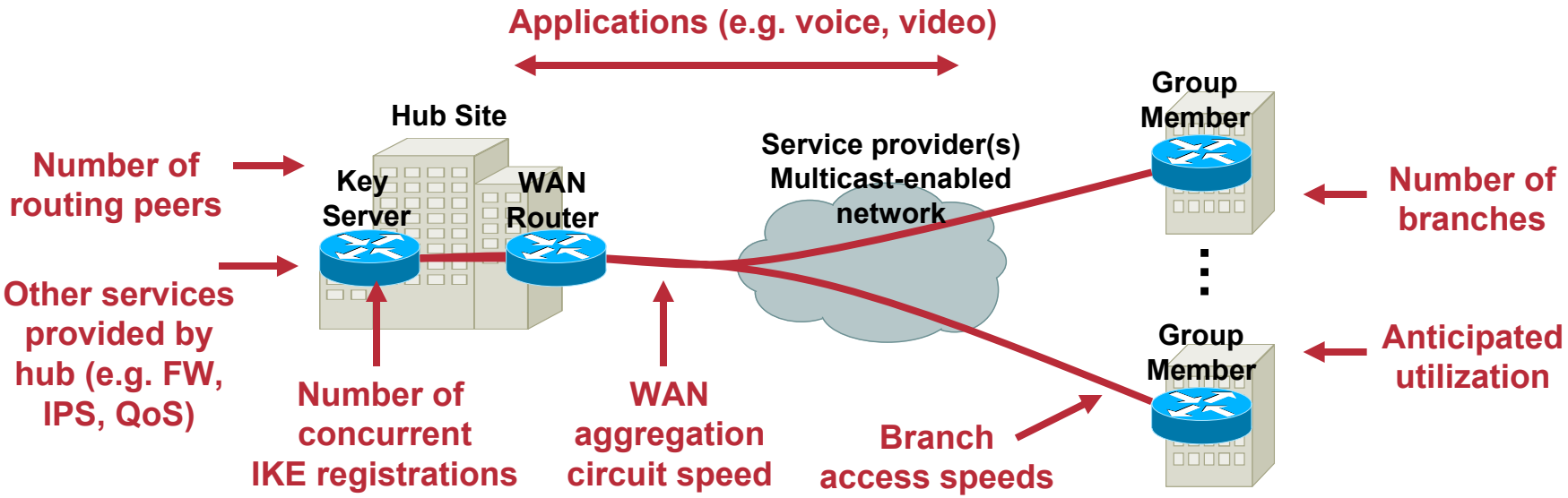
Group Controller / Key Server Configuration

```
crypto ipsec transform-set gdoi-trans esp-3des esp-sha-hmac
crypto ipsec profile gdoi-p
   set security-association lifetime seconds 120
   set transform-set gdoi-trans
crypto gdoi group diffint
   identity number 3333
   rekey address ipv4 101
   rekey lifetime seconds 300
   rekey authentication mypubkey rsa <mykeys>
   server local
     sa ipsec 1
       profile gdoi-p
       match address ipv4 120
   address ipv4 <gdoi_source>
access-list 120 permit ip <s_prefix/mask> <d_prefix/mask>
access-list 101 permit udp host <gdoi_source> eq 848 host <mroute> eq 848
ip pim ssm default
```

Group Member Configuration

```
ip pim ssm default
```

Secure Multicast:
General Design Considerations



- HW encryption modules required and recommended
- Running routing protocols doesn't require a tunneling protocol
- Set MTU on all network devices to 1400 to avoid fragmentation
- Summarize routes

Secure Multicast: General Design Considerations Which Mode—Sparse or Dense

"Sparse mode Good! Dense mode Bad!"

Source: *"The Caveman's Guide to IP Multicast", ©2000, R. Davis*

PIM-SM (RFC 2362)

- Assumes no hosts wants multicast traffic unless they specifically ask for it
- Uses a rendezvous point (RP)
  - Senders and receivers "rendezvous" at this point to learn of each others existence.
    - Senders are "registered" with RP by their first-hop router
    - Receivers are "joined" to the shared tree (rooted at the RP) by their local designated router (DR)
- Appropriate for…
  - Wide scale deployment for *both* densely and sparsely populated groups in the enterprise
  - Optimal choice for all production networks regardless of size and membership density

RP Resource Demands

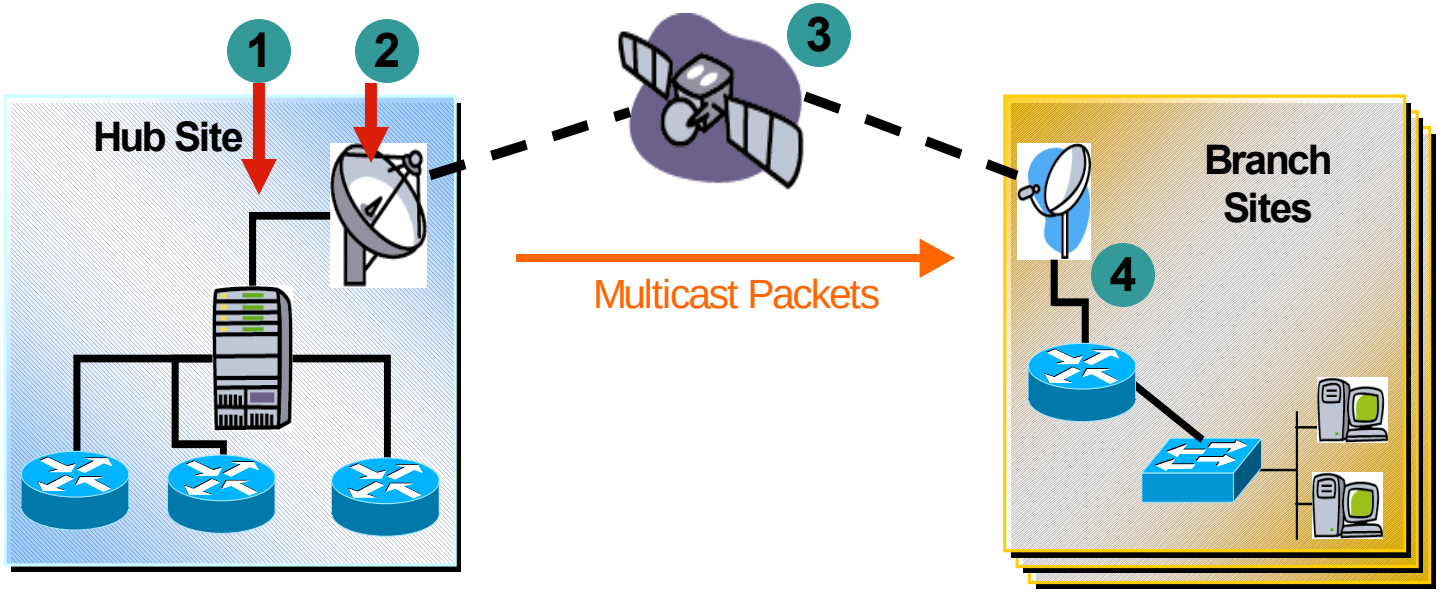
- (*,G) entry – 260 bytes + outgoing interface list overhead
- (S,G) entry – 212 bytes + outgoing interface list overhead
- Outgoing interface list overhead—80 bytes per OIL entry

Example of 10 groups with 6 sources per group:
of (*,G)s > (260 + (<# of OIL entries> x 80) = 10 (260 + (3 x 80)) = 5000 bytes for (*,G)
of (S,G)s > (212 + (<# of OIL entries> x 80) = 60 (212 + (3 x 80)) = 27,120 bytes for (S,G)
Total of 32,120 bytes for mroute table memory requirements

GDOI Usage

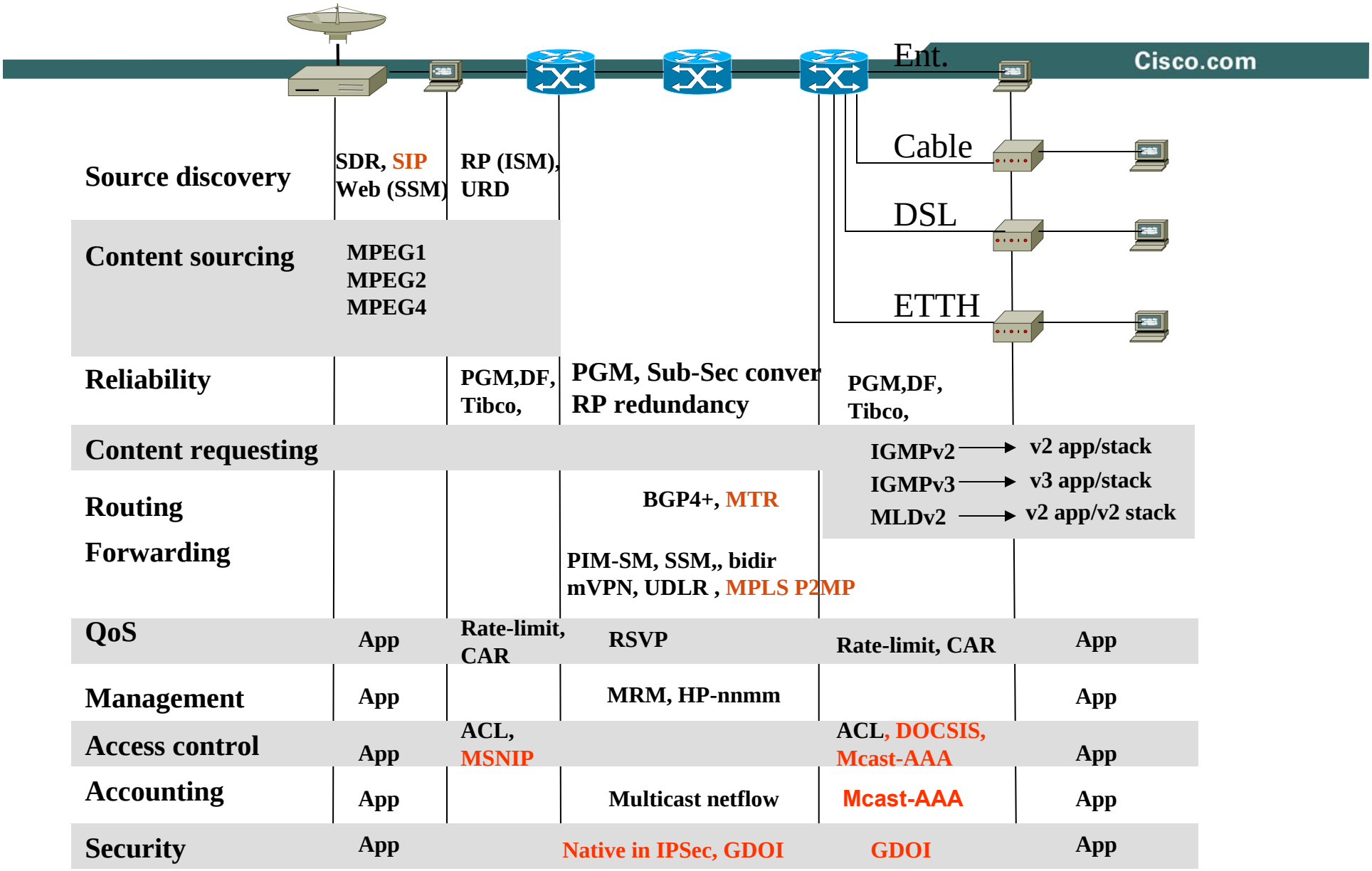
- **Application scenarios:**
  - **Encryption of IP packets sent over satellite links**
  - **Hoot-and-holler audio conferencing**
  - **Multicast router control traffic**
  - **Real-time content replication**
  - **IP/TV**
  - **mVPN**

Application Scenario: Encryption of IP Packets Sent over Satellite Links



1. The hub site encrypts IP multicast packets and forwards them to the satellite-sending unit
2. The satellite-sending unit transmits the IP packets to the satellite
3. The satellite retransmits the IP packet toward the dish antennas located at branch sites
4. The router in the branch site decrypts multicast packets and forwards the packet to branch

Elements of End-to-End Architecture



Application Scenario: Encryption of IP Packets Sent over Satellite Links

Key features:

- **Hardware accelerated**
- **Support for dynamic routing (EIGRP, OSPF, etc.)**

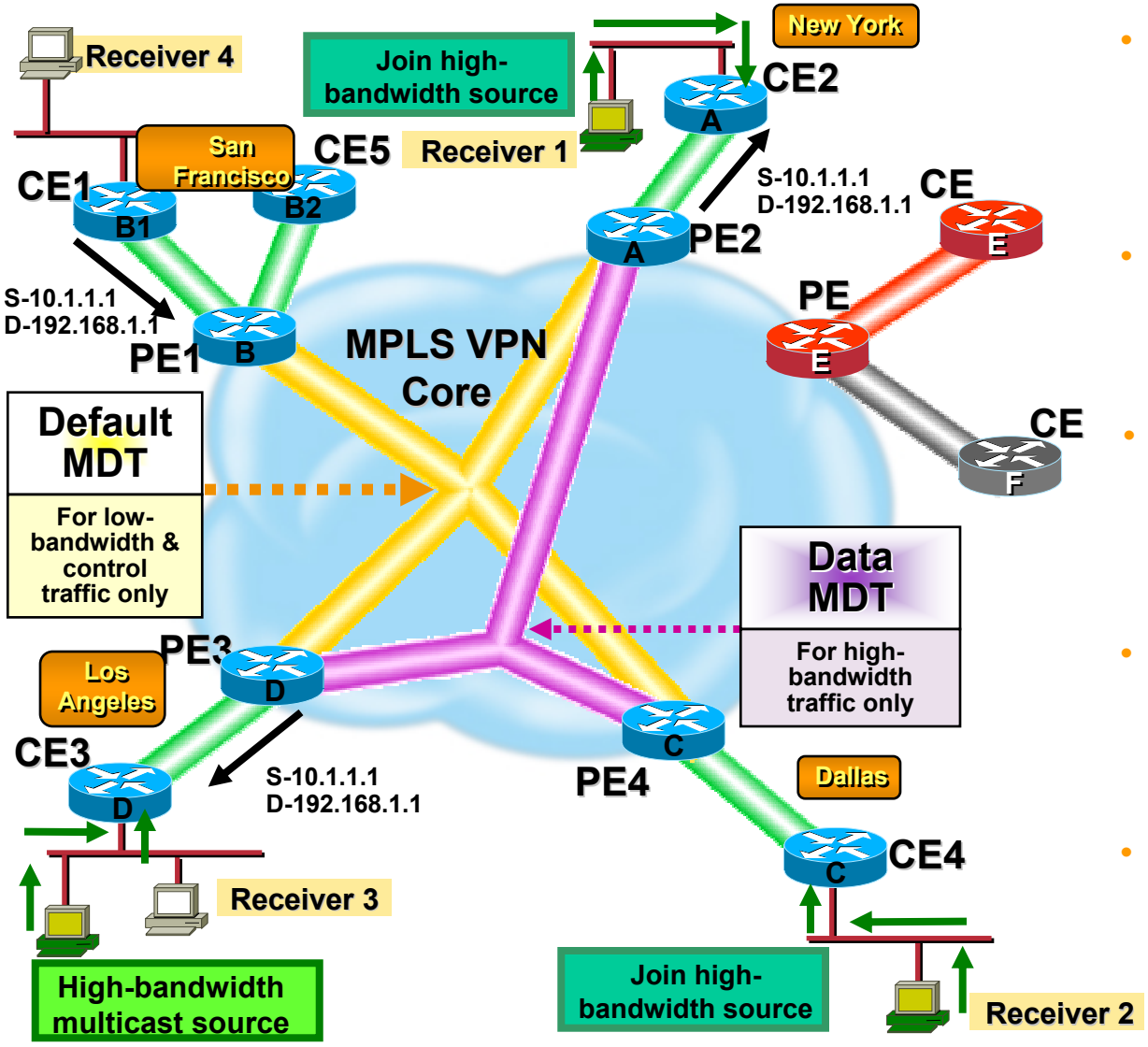
Good for:

- **The solution is good for enterprise, commercial, and governmental organizations who wish to enable secure video communications through the use of broadband satellite connectivity**
- **Branch offices with more than 1-2 subnets**
- **Multicast requirements**

Application Scenario: Encryption of IP Packets Sent over Satellite Links—*Best Practices*

- For multicast control traffic enable PIM sparse mode
- Digital certificates/PKI for group member authentication

Application Scenario: Security for Multicast VPN



- Customer CE devices joins the MPLS core through provider's PE devices
- The MPLS core forms a default MDT for a given customer
- A high-bandwidth source for that customer starts sending traffic
- Interested receivers 1 & 2 join that high-bandwidth source
- Data-MDT is formed for this high-bandwidth source
- GDOI is used to protect the multicast data

Application Scenario: Security for Multicast VPN

Key features:

- Security for mVPN packets which are flowing through the provider in a native multicast deployment
- DoS protection for the mVPN edge systems
- Comprehensive protection: Protection in the customer premise between CPE devices, protection in the provider domain between PE devices
- Dynamic routing (EIGRP, OSPF, etc.)

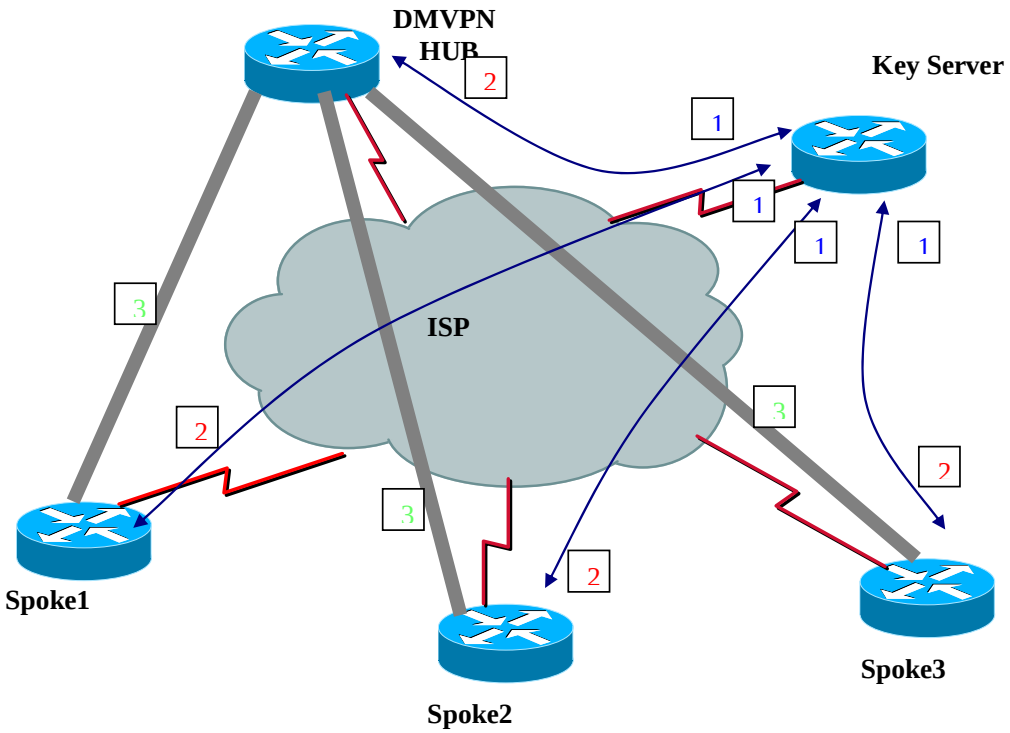
Good for:

- Customers already using mVPN but need security
- Up to 240 branch offices with more than 1-2 subnets
- Multicast requirements

Application Scenario: Security for Multicast VPN–*Best Practices*

- Digital certificates/PKI for tunnel authentication
- For multicast control traffic enable PIM sparse mode
- Protected GDOI key server behind a edge router

Application Scenario: Integration of GDOI with Dynamic Multipoint VPN



- DMVPN hub and all spokes are configured as group members. All group members register with the key server.
- Key server distributes group and IPSec policy information to all group members.
- A spoke-to-hub tunnel Is established using NHRP. All packets traveling via the DMVPN tunnel are now encrypted using group key.
- The spoke sends a NHRP resolution request to the hub for any spoke-spoke communication
- Upon receiving NHRP resolution reply from the hub, the spoke sends traffic directly to other spokes with group key encryption.

Benefit: By using secure multicast functionality in DMVPN network , the delay caused by IPSec negotiation is eliminated

Note : Multicast traffic will still be forwarded to hub for any spoke to spoke even with this deployment.

Application Scenario: Integration of GDOI with Dynamic Multipoint VPN

Key features:

- **GDOI with DMVPN**
- **Dynamic routing (EIGRP, OSPF, etc.)**
- **Dead Peer Detection (DPD)**

Good for:

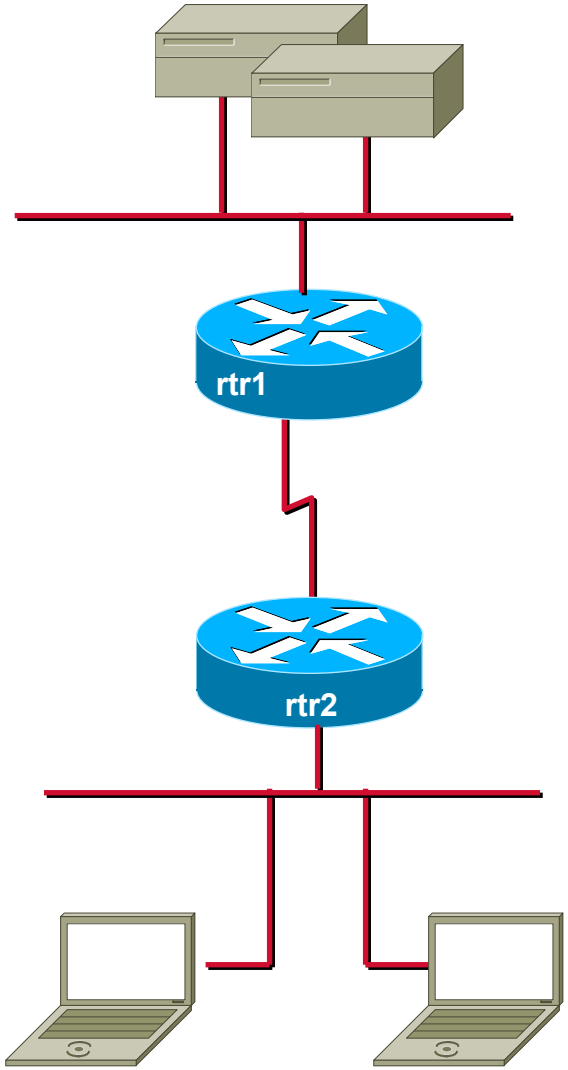
- **DMVPN customers wishing to deploy voice with VPN**
- **Branch offices with more than 1-2 subnets**
- **Multicast requirements**

Application Scenario: Integration of GDOI with Dynamic Multipoint VPN–*Best Practices*

Cisco.com

- EIGRP (or OSPF, etc.) dynamic routing, <1000 peers per head end
- Primary and secondary (or more) IPSec/GRE tunnels to alternate head ends, using routing cost for preference
- Typically static crypto maps, unless branches have dynamic IP addresses, then dynamic crypto map required on head end
- Configure DPD to detect loss of communication
- Digital certificates/PKI for tunnel authentication

Application Scenario: : Secure PIM Control Traffic with IPSec



PIM control packets can be encrypted

- **Session peer is set to 224.0.0.13 (PIM control messages)**
- **Supports multiple IPSec options**
  - Hash functions: MD5, SHA1
  - Security protocols: Authentication Header(AH), Encapsulating Security Payload (ESP)
  - Encryption algorithms: DES, 3DES, AES
  - Recommended IPSec mode: Transport
  - Recommended key method: Manual
- **IPSec AH is the recommended security protocol in the PIM-SM and PIM-Bidir IETF drafts**
- **Initial Cisco IOS® Software Release – 12.4(6)T**

Platform Support and Useful Links

Cisco IOS Platform Support

Cisco.com

Platform	Group Member	Key Server
Software	Yes	Not recommended
Cisco® 850/870 Series Access routers	Yes	Not recommended
Cisco 1800/1841	Yes	Not recommended
Cisco 2800	Yes	Yes
Cisco 3800 (AIM-II/AIM-III)	Yes	Yes
Cisco 7200 NPEG1, VAM2+	Yes	Yes
Cisco 7300 NPEG1, VAM2+	Yes	Yes
Cisco 7200 NPEG2, VAM2+	No	Yes
Cisco 7300 NPEG2, VAM2+	No	No
Cisco 7200 NPEG2, VSA	No	No
Cisco 7300 NPEG2, VSA	No	No
Cisco 7600 VPN-SPA	No	No

Useful Links

Cisco.com

- **http://www.cisco.com/go/multicast**