Advances in EIGRP

Feature Overview

Hierarchical Configuration (Named Mode)

EIGRP IPv6 Primer

EIGRP Overview

Compelling EIGRP Solutions

- EIGRP is easy to design and support
  - Faster system design and deployment time
  - Easier learning curve for support personnel
  - Lower Operational Costs (OpEx)
- Optimized for enterprise and commercial networks
  - Flexible design options
  - Sub-second convergence since inception
  - Simple for small networks, yet scalable for very large networks
- Excellent campus and hub-n-spoke WAN protocol
- Excellent scalability in DMVPN deployments
- Proven deployment
  - The most widely deployed enterprise routing protocol
  - Widely available across Cisco platforms suitable for enterprise and commercial

Configuration—Named Mode

EIGRP Named Mode Configuration Support

- EIGRP has been extended to support a hierarchical configuration
- Commands are scattered, unclear scope, and similar but different.
- Name-Mode
  - ✓ Clearly define the effect of the command, or the expected outcome.
  - ✓ Provides ONE place - ONE common way to define a feature
  - ✓ Allows you to enter information needed for a given mode (avoid missing AS configuration errors)
  - ✓ Enter it the same way! Reduce the time needed to learn a new protocol.
- Supports all current and future feature development in an extensible way
- Above all – allow users to keep the existing Config/Exec Mode in case users prefer the classic configuration mode

Configuration—Named Mode

```
router eigrp [virtual-instance-name | asystem]
 [no] shutdown
   .
   .
   .
```

- **Classic mode:**
  Configuring “router eigrp” command with a number
- **Named mode:**
  Configuring “router eigrp” command with the virtual-instance-name
  - ✓Named mode supports both IPv4 and IPv6, and VRF (Virtual Routing and Forwarding) instances
  - ✓Named mode allows you to create a single Instance of EIGRP which can be used for all family types
  - ✓Named mode supports multiple VRFs limited only by available system resources
  - ✓Named mode does not enable EIGRP for IPV4 routing unless configured

Configuration—Address-Family Mode

```
router eigrp [virtual-instance-name]
 address-family <protocol> [vrf <name>] autonomous-system <#>
   …
 exit-address-family
 service-family <protocol> [vrf <name>] autonomous-system <#>
   …
 exit-service-family
```

- Single place for all commands needed to completely define an instance
  “show run | section router eigrp”

- Defines what users are routing/distributing
  - ✓ “common look and feel”
  - ✓ Provide support for both routing (address-family) and services (service-family)
  - ✓ Can be configured for VRFs

- Assure subcommands are clear as to their scope
  - ✓ Static neighbors, peer-groups, stub, etc.
  - ✓ neighbor, neighbor remote, etc.

Configuration—Interface Mode

```
router eigrp [virtual-instance-name]
  address-family <protocol> autonomous-system <#>
    af-interface default
      …
    exit-af-interface
    af-interface <interface>
      …
    exit-af-interface
  exit-address-family
```

- EIGRP specific interface properties are configuration in the af-interface mode; For example: *authentication, timers, and bandwidth control*
- "**af-interface default**" applies to ALL interfaces

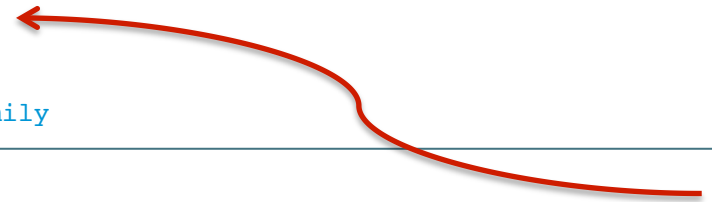
  Not all commands are supported
- "**af-interface <*interface*>**" applies to ONLY one interface

  Only "eigrp" specific commands are available

  Properties which are interface specific, such as delay and bandwidth, are still configured under the interface.

Configuration—Topology Mode

```
router eigrp [virtual-instance-name]
 address-family <protocol> autonomous-system <#>
   topology base
     …
  exit-topology
 exit-address-family
```



Applies to global, or default, routing table

- Topology specific configuration such as:
  - ✓ default-metric
  - ✓ event-log-size
  - ✓ external-client
  - ✓ metric config
  - ✓ timers config
  - ✓ redistribution

Configuration—Classic Mode Changes

The auto-summary command is a relic from the days of classful routing. It was *enabled* by default in pre-release 5 images.

- The auto-summarization feature is no longer widely used and 'no auto-summary' has since become the prevailing configuration
- CSCso20666 changed auto-summary behavior to *disabled* by default
- Because 'no auto-summary' is the factory default setting it will not nvgen -- auto-summary will now only nvgen if it is explicitly enabled

default	nvgen behavior	IOS Version (eigrp version)
auto-summary	'auto-summary' : does not nvgen 'no auto-summary' : nvgens	12.2SR(rel2), 12.2SX(rel3), 12.2SG(rel4)
auto-summary	'auto-summary' : nvgens 'no auto-summary' : nvgens	12.2S(rel1), 12.4T(rel1), 12.2SB(rel1)
no auto-summary	'auto-summary' : nvgens 'no auto-summary' : does not nvgen	15.0(rel5), 15.0T(rel5), 12SRE(rel5), 122XNE(rel5) 122XNF(rel5_1), 122(55)SG(rel5_2)

Routing Enhancements—IPv6 Support

Internet Protocol Version 6 (IPv6)

- EIGRP supports revision 6 of the Internet Protocol IPv6 (IPv6)
- Same EIGRP protocol, just IPv6 enabled
- A familiar look and feel means incumbent EIGRP operational expertise can be leveraged
- DUAL performs route computations for IPv6 without modifications
- Provides feature parity with most IPv4 Features:
  - ✓ EIGRP IPv6 MIBS
  - ✓ EIGRP IPv6 NSF/SSO
  - ✓ EIGRP IPv6 VRF-aware
  - ✓ EIGRP IPv6 BFD support
  - ✓ Etc.

```
interface Ethernet0/0
    ip address 1.1.1.1
    ipv6 enable
!
router eigrp ROCKS
  address-family ipv4 autonomous-system 1
      network 10.0.0.0 255.0.0.0
      af-interface Ethernet0/0
       hello 30
      exit-af-interface
  !
  address-family ipv4 vrf cisco autonomous 4453
      network 192.168.0.0
  !
  address-family ipv6 autonomous-system 1
     af-interface Ethernet0/0
       no shutdown
       bandwidth-percent 40
     exit-af-interface
  !
  address-family ipv6 vrf cisco autonomous 6473
     af-interface default
       no shutdown
     exit-af-interface
```

EIGRP-IPv6—IPv6 Addressing Primer

- An IPv6 address is an extended 128-bit / 16 bytes address that gives:
  2^{128} possible addresses (3.4×10^{38})

- IPv6 addresses:
  64 bits for the subnet ID, 64 bits for the interface ID
  Separated into 8 * 16-bit hexadecimal numbers
  Each block is separated by a colon (:)
  :: can replaced leading, trailing or consecutive zeros
  :: can only appear once

Examples:

2003:0000:130F:0000:0000:087C:876B:140B

2003:0:130F::87C:876B:140B

- EIGRP IPv6 Multicast transport:
  FF02:0:0:0:0:0:0:A or abbreviated to FF02::A

EIGRP-IPv6—Link-local Address

- A IPv6 Link-local address is used by EIGRP to source Hello packets and establish an adjacency
  - IPv6 Link-local address is never routed
  - IPv6 packet forwarding must be configured first under global configuration
  - They are auto assigned when users enable the interface

```
ipv6 unicast
interface Ethernet1/0
  ipv6 enable
```

  - Users can configure this manually on an interface
  - An IPv6 link-local is prefixed by FE80 and has a prefix length of /10

```
interface Ethernet1/0
  ipv6 address ?
  X:X:X:X::X          IPv6 link-local address
  X:X:X:X::X/<0-128>  IPv6 prefix
```

EIGRP-IPv6—Configuration Primer

classic router configuration

```
ipv6 unicast
interface Ethernet1/0
  ipv6 enable
int Ethernet 0/0
  ipv6 eigrp 6473
!
router eigrp 6473
  no shutdown
```

eigrp named mode configuration

```
ipv6 unicast-routing
!
interface Loopback0
 ipv6 enable
!
interface Ethernet0/0
 ipv6 address 2001:DB8::1/64
!
router eigrp CSCO
  address-family ipv6 autonomous-system 6473
    router-id 10.10.10.1
    af-interface default
      no shutdown
    topology base
```

- Router-ID is required and selected
  1. From highest loopback IPv4 address
  2. From first IPv4 address found on any physical interface.
- If no IPv4 address is available, a 32-bit router-id can be configured manually using the *router-id* command

EIGRP-IPv6—High-level Overview

Implementation	Provides feature parity with majority of IPv4 features (stubs, scaling, summarization, etc.) Uses the same reliable Multicast transport protocol used by IPv4 2 new TLVs used for both IPv4 and IPv6; INTERNAL_TYPE (0X0602), EXTERNAL_TYPE (0X0603) Same metrics used by IPv6 and IPv4
Important Differences	IPv6 Link-local address are used to establish an adjacency (FF02::A (all EIGRP routers); neighbors do not have to share the same global prefix (with exception of static neighbors where traffic is unicasted) Does not support the "default-information" command as there is no support in IPv6 for the configuration of default networks other than ::/0 Does not support the "auto-summary" command **No split-horizon in the case of EIGRP** for IPv6 (because IPv6 supports multiple prefixes per interface) **RouterID** which must be explicitly configured if there is no IPv4 address
Notes	Its just like EIGRP-IPv4 except where its different: "ipv6 unicast" must be configured under global mode to enable ipv6 routing "ipv6 enable" must be configured under all interfaces which will be enabled for ipv6

EtherChannel®/MLPPP/10G Support (Wide Metrics)

Summary, Summary Static Metrics, Route Leaking

Route-Map and Enhanced Route Tags

Hub & Spoke, Hub Co-Existence, Route Leaking

3rd **Party Next Hop, Dual Home DMVPN,** AddPath

Simple Network Management Protocol (SNMP)

Mobile Ad-hoc Network (MANET)

Performance Routing (PfR)

Routing Enhancements

Routing Enhancements

EIGRP Wide Metric Support

- EIGRP now offers support for links which exceed 2Gigabit

- Where does EIGRP get the component metrics?
  - → Bandwidth: default interface value or bandwidth command
  - → Delay: default interface value or delay command

```
Router1#show interface TenGigabitEthernet 2/0
TenGigabitEthernet2/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.0102 (bia aabb.cc00.0102)
  Internet address is 10.4.4.1/24
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255

Router1#sho interface GigabitEthernet e3/0
GigabitEthernet3/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.0103 (bia aabb.cc00.0103)
  Internet address is 10.5.5.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

- What does IOS Interfaces report?

  Bandwidth: 0-4294967295 kbps

  Delay: 10- 4294967295 micro-seconds; values are only good up to 1Gigabit

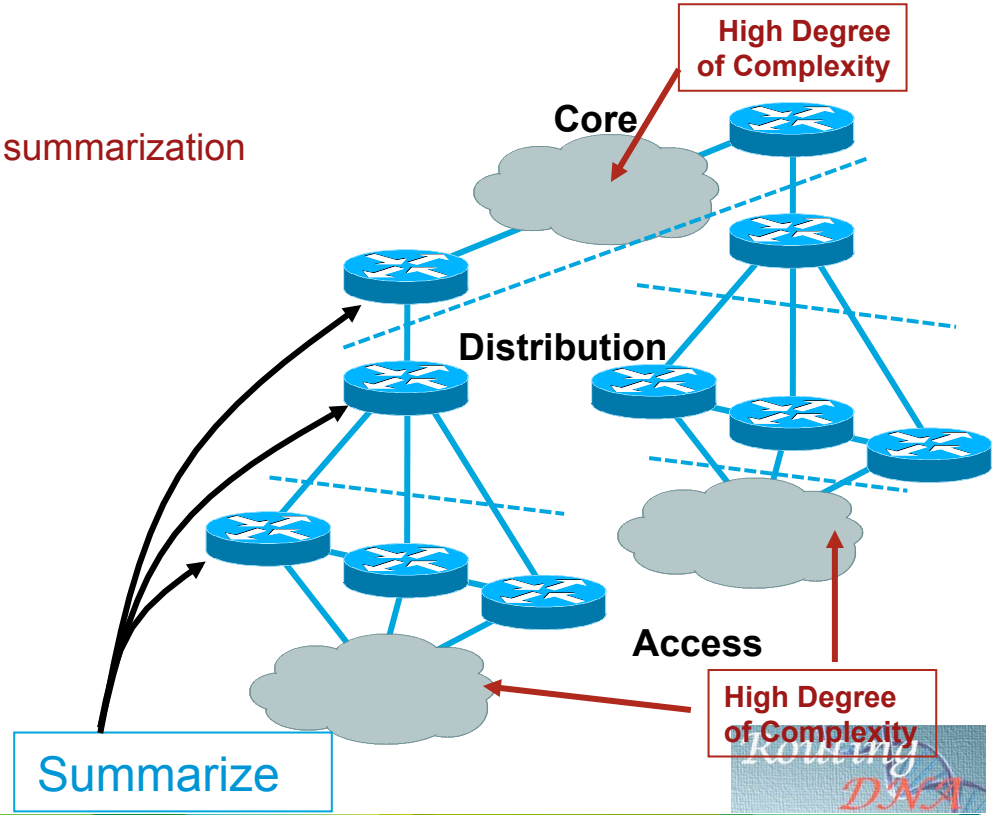
  Configuration is based on “10s of” microseconds

- EtherChannel® or MLPPP(Multilink PPP) can exceed this!

EIGRP Summary Enhancements

Very Large Network Hierarchy

- EIGRP supports very large hierarchy through summarization
- The depth of the hierarchy doesn't alter the way EIGRP is deployed; there are no "hard edges"
  - "Core", "Distribution", and "Access" are flexible terms that may not fit your topology
  - EIGRP does not force these boundaries
- Divide complexity with summarization points
- Summarize at every boundary where possible:
  - Aggregate reachability information
  - Aggregate topology information
  - Aggregate traffic flows
- A place to apply traffic policy



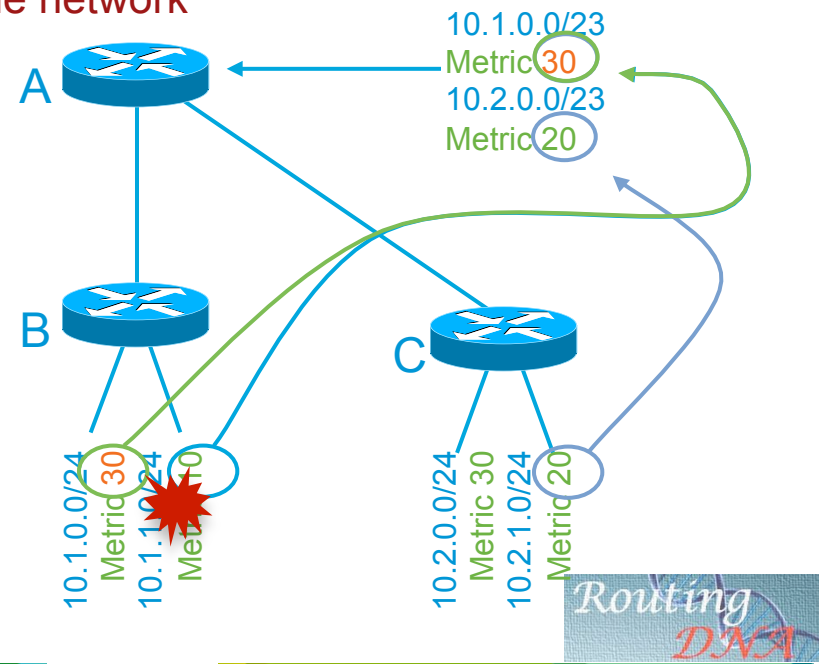
Routing Enhancements

Route Summarization

- EIGRP supports summarization at any point in the network
- EIGRP chooses the metric of the lowest cost component route as the summary metric

What happens if the summary metric changes?

- If the component the metric was taken from flaps, the summary flaps as well!
- Users are using the summary to hide reachability information, but it's passing metric information through
- Routers beyond the summary are still working to keep up with the changes

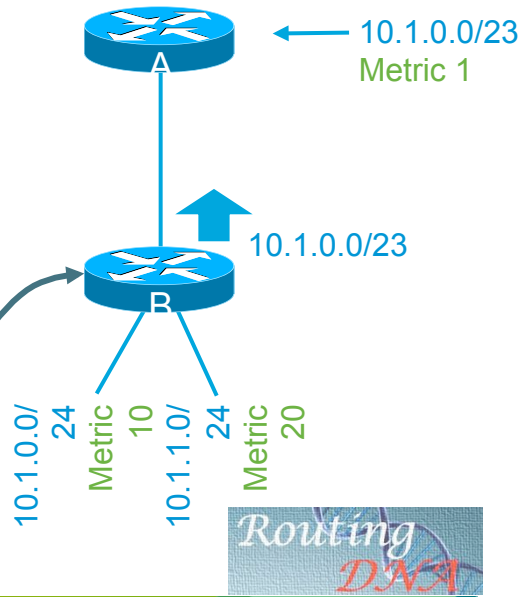


Routing Enhancements

Route Summary Static Metrics

- EIGRP summarization efficiency is greatly improved by predefining a summary's metric
- Could use a loopback interface or define a static route to null0
  - ✗ Metric will be constant, eliminating update
  - ✗ EIGRP still scans component routes for changes
  - ✗ EIGRP will never withdraw summary
- A better solution is to use the summary-metric command which established a constant metric value thereby:
  - ✓ Eliminates the updates
  - ✓ Eliminates re-computing the summary metric when components change
  - ✓ Allows the summary to be withdrawn when all comments are lost

```
router eigrp ROCKS
  address-family ipv4 auto 4453
    network 10.0.0.0
    af-interface Ethernet0/0
      summary-address 10.1.0.0/23
    exit-af-interface
    topology base
      summary-metric 10.1.0.0/23 10000 1 255 1 1500
```

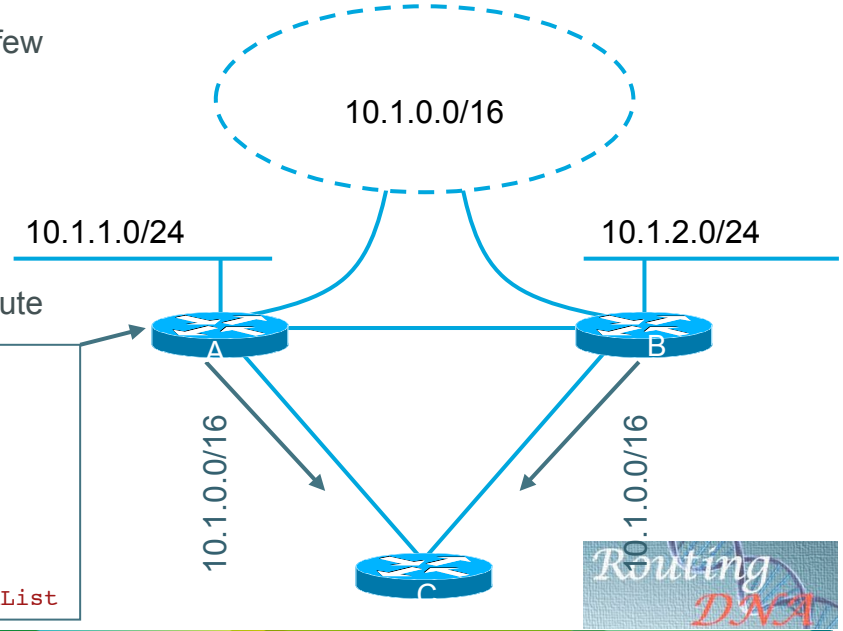


Routing Enhancements

Route Summary Leaking

- EIGRP allows user definable summary components to leak past the summary boundary
- For optimal routing, users would like C to be able to receive as few routes as possible, but still optimally route to 10.1.1.0/24 and 10.1.2.0/24 dynamically
- Combination of static routes and could be used but its difficult to maintain
- The simplest way is to configure a leak-map on the summary route

```
route-map LeakList permit 10
  match ip address 1
!
access-list 1 permit 10.1.1.0
!
router eigrp ROCKS
  address-family ipv4 autonomous-system 4453
    af-interface Serial0/0
      summary-address 10.1.0.0 255.255.0.0 leak-map LeakList
```



Routing Enhancements

EIGRP Route-Map Support

- EIGRP supports revision 6 of the Internet Protocol IPv6 (IPv6)
- EIGRP has supported route-maps for years, but in a limited capacity
- They could only be used during redistribution out of the routing table from another protocol
- Enhanced support of route maps allows EIGRP to use a route map to prefer one path over another
- As shown below, route-maps can now be applied on the distribute-list in statement, so the filters can be applied even before the prefix hits the topology table

```
route-map setmetric permit 10
 match interface serial 0/0
 set metric 1000 1 255 1 1500
route-map setmetric permit 20
  match interface serial 0/1
 set metric 2000 1 255 1 1500
....
router eigrp ROCKS
  address-family ipv4 auto 4453
    topology base
    distribute-list route-map setmetric in
```

Routing Enhancements

EIGRP Enhanced Route Tags

- EIGRP has been extended to support a more flexible route tag method
  - ✓ Dotted-Decimal notation easier to read
  - ✓ Support mask for multiple tag matching
  - ✓ Supports IPv4 and IPv6

Classic Route Tag

```
route-map current-route-tag-usage permit 10
 match tag 451580 451597 451614 451631
 set metric 1100
!
Router# show ip route tag
```

Enhanced Route Tag

```
ip access-list standard route-tag-mask
 permit 100.160.60.60 0.0.3.3
!
route-map enhanced-route-tag permit 10
 match ip address tag route-tag-mask
 set metric 1100
!
Router# show ip route tag 100.160.61.60 0.0.3.3
```

Assigning internal routes a default tag

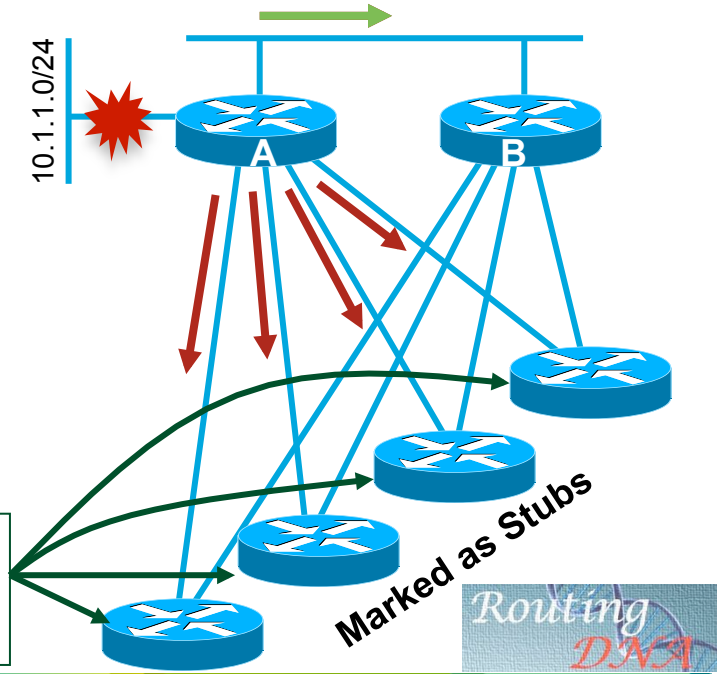
```
router eigrp ROCKS
 address-family ipv4 vrf tagit 4452
   topology base
    route-tag 100.160.61.61
```

Routing Enhancements

EIGRP Hub and Spoke (STUBS)

- EIGRP offers the best scaling performance of all IGPs
  - When a route or link is lost
    - → EIGRP query's ALL neighbors
    - → Each neighbors using it to reach the destination will also query their neighbors
  - Marking the spokes as stubs, allows EIGRP
    - ✓ To signal the Hubs (A and B) that they are not valid transit paths
    - ✓ When the route to 10.1.1.0/24 is lost, A will not query the remotes, only B, and in turn will not query B the remote stubs
    - ✓ Reduces the total number of queries in this example to 1

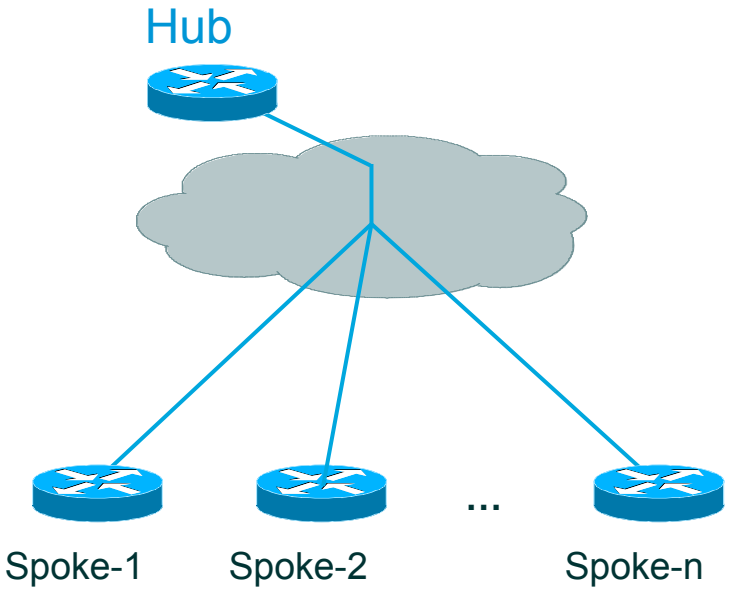
```
router eigrp ROCKS
  address-family ipv6 autonomous-system 6473
    stub connected
```



Routing Enhancements

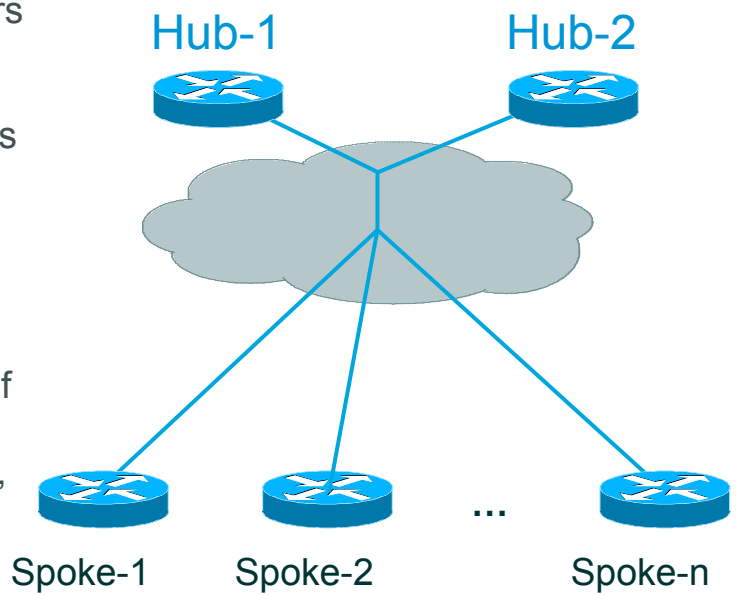
EIGRP STUBS—Hub Co-Existence

- EIGRP offers flexibility to allow multiple HUB on the same LAN segment
- Stub routing is disabled if the hub has a mix of stub and non-stub neighbors on an interface
  - ✗ Prevents the deployment of multiple hubs on the shared media such as Ethernet or multipoint interface
  - ✗ A configuration mistake on a spoke as non-stub can also disable the stub routing feature causing instability in a large network due to queries
- What if you want to have dual hubs for redundancy?



Routing Enhancements

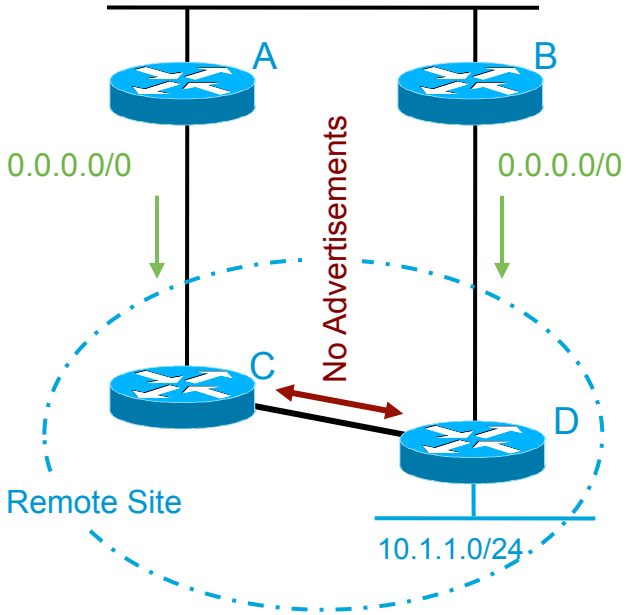
- The ability to send a query to a neighbor subset was added to allow for the coexistence of both stub and non-stub neighbors on the same interface
- A hub router can now send queries to the non-stub neighbors and suppress queries to the stub neighbors
- A query can either be sent unicast, or multicast by using the existing conditional-received method
- For packet transmission efficiency, queries are sent unicast if the number of non-stub peers are less than five, or less than 10% of the total number of peers on the interface; otherwise, multicast is used



Routing Enhancements

EIGRP Hub and Spoke Stub Route Leaking

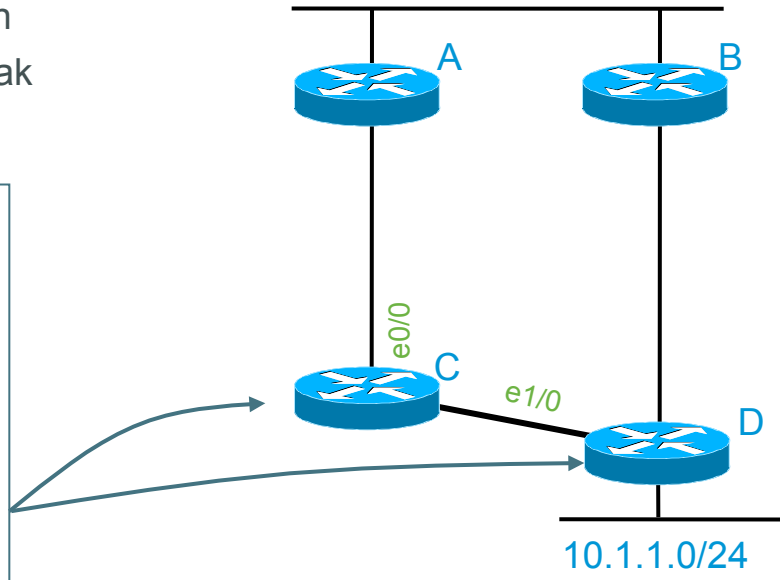
- EIGRP offers additional control over routes advertised by Stubs
- Assume a user has a single remote site with two routers, and that user wants to mark the entire site as a “stub site”:
  - We could mark both C and D as stub
  - A and B advertise only a default to C and D
- However, configured as stubs, C and D don’t advertise learned routes to each other
- This means:
  - C is not advertising the default route to D
  - D cannot reach A though C
  - A can not reach D tough C



Routing Enhancements

- The solution is for C and D to advertise a subset of their learned routes, even though they are both stubs
- This can be accomplished by:
  - Adding the “leak-map” to the stub configuration
  - Creating a route map to specify the route to leak between C and D

```
route-map LeakList permit 10
  match ip address 1
  match interface e0/0
route-map LeakList permit 20
  match ip address 2
  match interface e1/0
!
access-list 1 permit 10.1.1.0
access-list 2 permit 0.0.0.0
!
router eigrp ROCKS
  address-family ipv4 autonomous-system 100
    eigrp stub leak-map LeakList
```



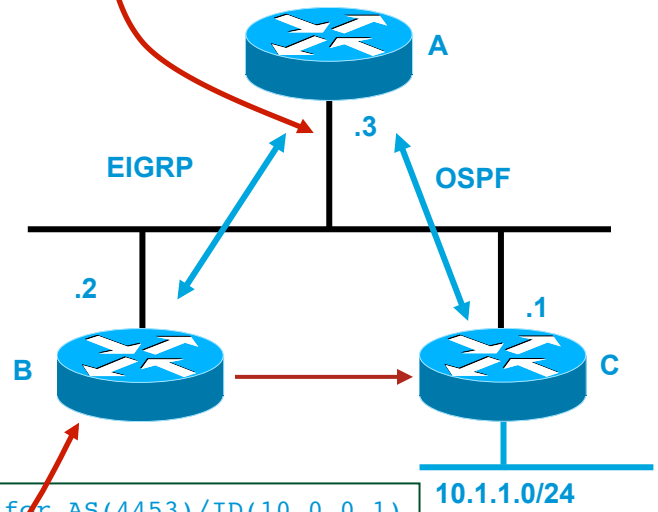
3rd Party Next Hop

Available in:
12.3(07)XI
12.2(23.01)S
12.3(02.03)B
12.3(01.02)T
012.003(001.003)

EIGRP Support for 3rd Party Next Hops

- EIGRP offers 3rd party next hop support at LAN redistribution points
- Example: A, B and C share the same broadcast segment
  - A redistributes OSPF into EIGRP
  - B isn't running OSPF
  - C isn't running EIGRP
- For redistributed OSPF routes B normally shows A as next hop despite a direct connection to C
- A now sends updates to B with C as the next-hop
- EIGRP preserves the next hop in redistribution from broadcast networks

```
router eigrp ROCKS
  address-family ipv4 auto 4453
    af-interface Ethernet0/0
      no next-hop-self
```

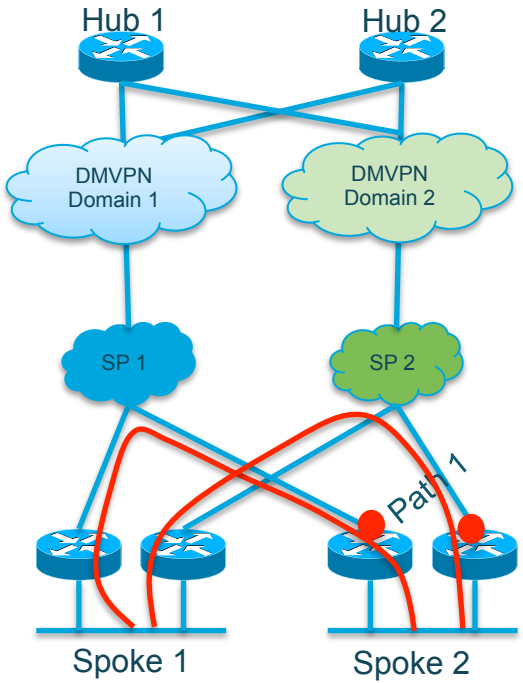



```
EIGRP-IPv4 VR(ROCKS) Topology Table for AS(4453)/ID(10.0.0.1)
....
P 10.1.1.0/24, 1 successors
         via 10.1.2.1
```

3rd Party Next Hop: Dual DMVPN

EIGRP Dual Hub DMVPN, Dual Domain DMVPN

- EIGRP has been enhanced to handle Dual Hub and Dual DMVPN domains
- Dual Hubs - Co-Existence
  - Support for dual hubs for redundancy
  - load-balancing
- Dual DMVPN Domains
  - Enables load-balancing for dual DMVPN domain
  - Spoke to spoke load balancing and redundancy
  - EIGRP honors the 'no next-hop self' command on the hub sites



3rd Party Next Hop: Add-Path

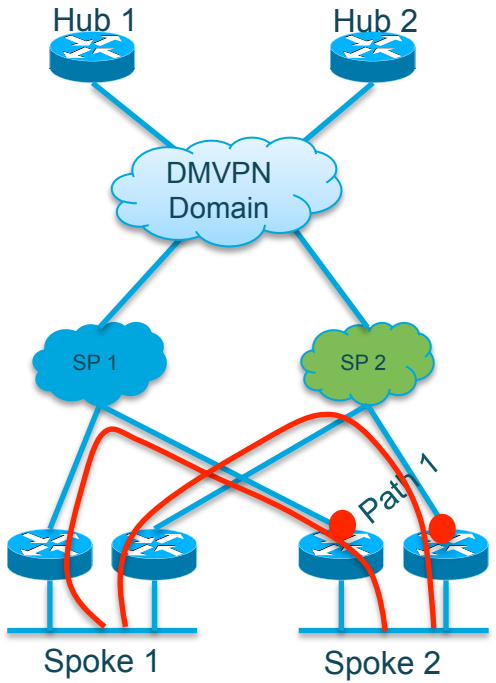
EIGRP DMVPN, MultiPath, AddPath

- EIGRP has been enhanced to carry multiple next-hops
- Equal Cost MultiPath (Releases 15.2(3)T, 15.2(1)S)

  Destination network is reachable via more than one DMVPN (mGRE tunnel) and the ip next-hop needs to be preserved over both paths

- Add-path (`Release 15.3(1)S`)

  Spoke site has multiple DMVPN spoke routers and want to be able to load-balance spoke-spoke tunnels going into this spoke site



Routing Enhancements—SNMP

Simple Network Management Protocol (SNMP)

- EIGRP supports 68 MIB objects in 4 major tables

EIGRP Traffic Statistics
- AS Number
- Number of Hellos, Updates,
- Queries, and Replies Sent/Received

EIGRP Topology Data
- Destination Net/Mask
- Active State, Feasible Successors
- Origin Type, Distance
- Reported Distance

EIGRP Interface Data
- Peer Count
- Reliable/Unreliable Queues
- Pending Routes
- Hello Interval

EIGRP Peer Data
- Peer Address, Interface
- Hold Time, Up Time
- SRTT/RTO
- Version

eigrpRouteSIA and eigrpAuthFailure can trigger SNMP traps

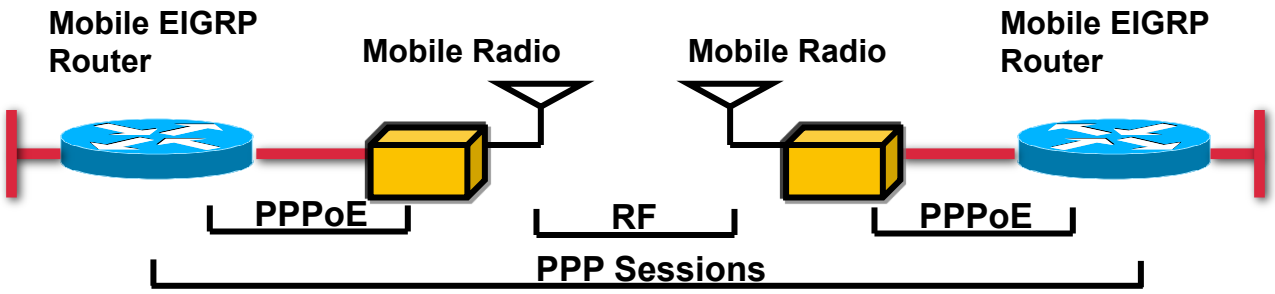
Additional information

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
http://www.cisco.com/go/mibs
ftp://ftp.cisco.com/pub/mibs/oid/

MANET—Dynamic Cost Routing

Mobile Ad-hoc Network (MANET)

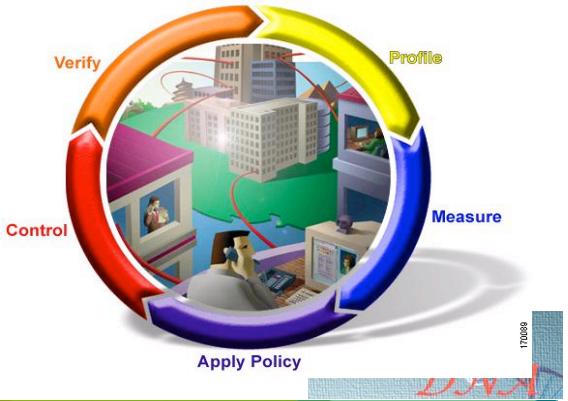
- Cisco supports RFC4938bis and Dynamic Cost Routing via/using EIGRP
- The fundamental requirement for MANET applications is effective integration of routing and radio technologies
- Effective routing requires immediate recognition of topology changes, the ability to respond to radio link quality fluctuations, and a means by which routers can receive and act upon feedback from a radio network
- New Virtual Multipoint Interface (VMI) and L2L3 API connects Layer 2 RF network with layer 3



Routing Enhancements

Performance Routing (PfR)

- Cisco IOS Performance Routing (PfR) supports route control using EIGRP
- Monitors traffic performance for prefixes passively with NetFlow and/or actively using IP SLA probes
- Chooses best performing path to a given destination
  - ✓ Delay, MOS
  - ✓ Load Balancing
  - ✓ For prefix, traffic-class and application



Additional information:

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

Hash-based Message Authentication Code (HMAC)

Adaptive Security Appliances (ASA) Firewall

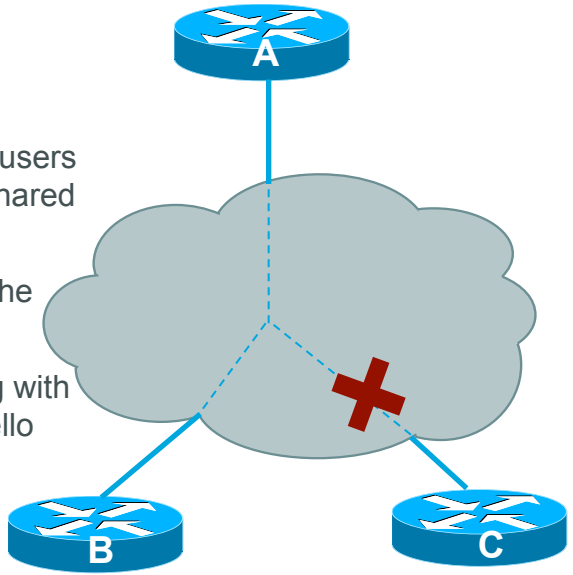
Security Enhancements

* Named mode only

EIGRP Security Enhancements

Hash-based Message Authentication Code (HMAC)

- EIGRP offers Secure Hash Algorithms SHA2-256 bit Algorithms
- The addition of SHA2-256 HMAC authentication to EIGRP packets ensures that users routers only accept routing updates from other routers that know the same pre-shared key
- This prevents someone from purposely or accidentally adding another router to the network and causing a problem
- The SHA2 key is a concatenation of the user-configured shared secret key along with the IPv4/IPv6 address from which this particular packet is sent. This prevents Hello Packet DoS replay attacks with a spoofed source address
- Simpler configuration mode using a common ‘password’
- Keychain support when additional security is needed



EIGRP Security Enhancements

- Simple configuration using only one password

```
router eigrp ROCKS
  address-family ipv4 auto 4453
    af-interface default
      authentication mode hmac-sha-256 my-password
    exit-af-interface
```

- Additional security can be added with key-chains

```
key chain DC012-CHAIN
  key 1
  key-string securetraffic
!
router eigrp ROCKS
  address-family ipv4 auto 4453
    af-interface default
      authentication mode hmac-sha-256 my-password
      authentication key-chain DC012-CHAIN
    exit-af-interface
```

- Interface inheritance can simplify configuration

```
router eigrp DC012-md5
  address-family ipv4 auto 4453
    af-interface default
      authentication key-chain DC012-CHAIN
    exit-af-interface
    af-interface Ethernet0
      authentication mode hmac-sha-256 ADMIN
    exit-af-interface
    af-interface Ethernet1
      authentication mode hmac-sha-256 CAMPAS
    exit-af-interface
    af-interface Ethernet2
      authentication mode hmac-sha-256 LAB
      authentication key-chain DC012-LAB
    exit-af-interface
```

EIGRP Security Enhancements

Adaptive Security Appliances (ASA) Firewall

- The Cisco ASA 5500 series offers EIGRP support
- Common portable EIGRP core code with a platform dependent OS-shim
- Supports EIGRP stub and other key features
- Newer platforms supported

Additional information:

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

Aggressive Timers

Bidirectional Forwarding Detection (BFD)

Loop Free Alternate Fast Reroute (LFA FRR)

Graceful Restart (GR) / Nonstop Forwarding (NSR)

Non-Stop Routing (NSR)

Multipoint Enhancements

DMVPN Scaling Improvements

Improving Convergence

Improving Convergence

1. Failure detection

   How quickly a device on the network can detect and react to a failure

2. Information propagation

   How quickly the failure in the previous stage is communicated to other devices

3. Repair

   How quickly devices are notified of a failure and can calculate an alternate path

✧ *Improvements in any of these stages provides an improvement in overall convergence*

Improving Convergence—Detection

EIGRP Aggressive Timers (Fast Hellos)

- EIGRP supports aggressive timers to increase link failure detection

  Aggressive Timers does not provide sub-second failure detection

  Timers can be tuned to a minimum of 1 second

```
router eigrp ROCKS
  address-family ipv6 auto 6473
    af-interface default
      hello-interval ?
      <1-65535>  Seconds between hello transmissions
```

Additional information

There are reasons for not recommending using aggressive timers. For example, depending on the number of interfaces, 1 sec rates can become CPU intensive and lead to spikes in processing/ memory requirements.

Improving Convergence—Detection

Bidirectional Forwarding Detection (BFD)

- Cisco IOS Bidirectional Forwarding Detection (BFD) is a fast Hello at Layer 2.5
  - BFD exhibits lower overhead than aggressive hellos
  - BFD is a heartbeat at Layer 2.5, provides sub-second failure detection
  - BFD can provide reaction time close to 50 milliseconds
- EIGRP uses BFD facilities which send extremely fast keep-alives between routers
  - BFD and EIGRP work together, with EIGRP as the upper layer protocol
  - BFD relies on EIGRP to tell it about Neighbors
  - Notifies EIGRP quickly about changes in Layer 2 state

Additional information:

http://tools.ietf.org/html/draft-ietf-bfd-generic-02

https://tools.ietf.org/html/draft-ietf-bfd-base-05

Improving Convergence—Propagation

Fast Network Convergence

- Cisco IOS Bidirectional Forwarding Detection (BFD) is a fast Hello at Layer 2.5
- FAST Convergence already part of the EIGRP standard
- Customers have been using EIGRP to achieve sub-second convergence for years
- Proper network design is a must:
  - ✓ Design to use address summarization to limit query scope
  - ✓ Design to provide at least one feasible successor
- Users can sort typical convergence times:
  - ✓ EIGRP with a feasible successor
  - ✧ Link state protocols
  - ✗ EIGRP without a feasible successor

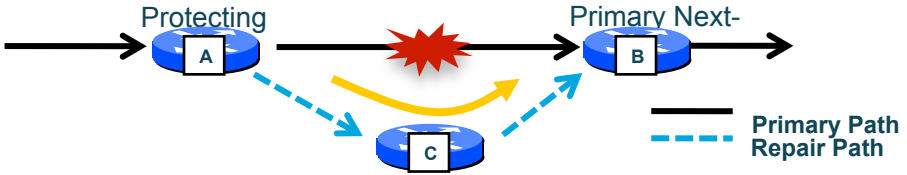
Improving Convergence—Propagation

- For paths with feasible successors convergence time is in the milliseconds
  - The existence of feasible successors is dependent on the network design
- For paths without feasible successors, convergence time is dependent on the number of routers that have to handle and reply to the query
  - Queries are blocked one hop beyond aggregation and route filters
  - Query range is dependent on network design
- Good design is the key to fast convergence in an EIGRP network

Improving Convergence—Repair

Loop Free Alternate Fast Reroute (LFA FRR)

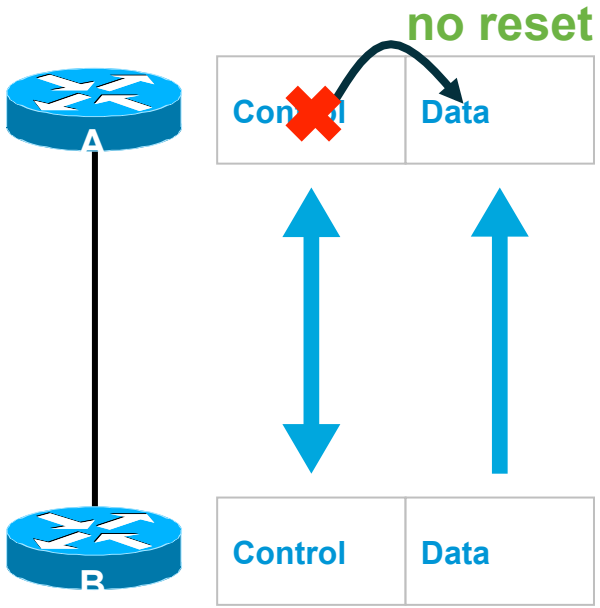
- Cisco IOS EIGRP supports Loop Free Alternate Fast Reroute (LFA FRR)
- IP-FRR is a mechanism that reduces traffic disruption to 10s of milliseconds in the event of link or node failure
  - ✓ Uses existing Feasible Successors, so there is no additional computational load
  - ✓ Automatically enabled on all EIGRP interfaces covered by network statement
  - ✓ Per-prefix LFA FRR enabled via route-maps
  - ✓ Repair paths can be of equal or unequal cost (thought variance command)
  - ✓ Repair paths are computed for all prefixes though not all prefixes may have a FS (repair path)
- Please note:
  - ✗ It runs at the process level
  - ✗ Does not guarantee time limit
  - ✗ Performance depends on tuning and platform implementation



Improving Convergence—Repair

Graceful Restart (GR) / Nonstop Forwarding (NSR)

- EIGRP offers supports for GR/NSF
- Fast Hellos is a way of detecting failures fast and routing around them (BFD is preferred)
- Fast Hellos or BFD are at cross purposes with HA/NSF!
- Graceful Restart (GR) is a way to rebuild forwarding information in routing protocols when the control plane has recovered from a failure
- Nonstop Forwarding (NSF) is a way to continue forwarding packets while the control plane is recovering from a failure

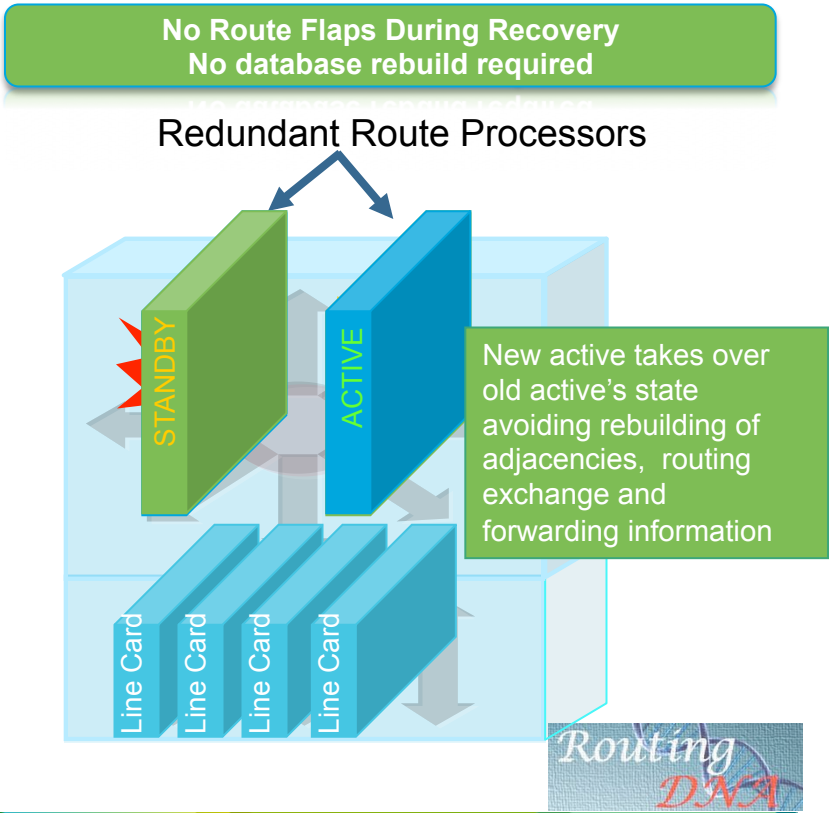


The fundamental premise of GR/NSF is to route through temporary failures, rather than around them!

Improving Convergence—Repair

Non-Stop Routing (NSR)

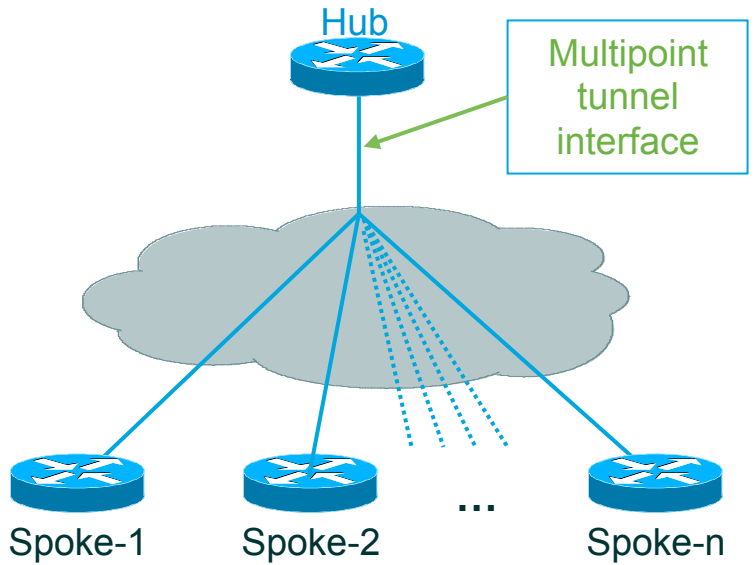
- Nonstop Routing (NSR) is a stateful redundancy mechanism for intra-chassis Route Processor (RP) failover
- NSR, unlike NSF with SSO:
  - Allows routing process on active RP to synchronize all necessary data and states with routing protocol process on standby RP
  - When switchover occurs, routing process on a newly active RP has all the necessary data and states to continue running without requiring any help from its neighbor(s)
  - Standards are not necessary as NSR does NOT require additional communication with protocol peers



Routing Enhancements

Multipoint Interface Enhancements

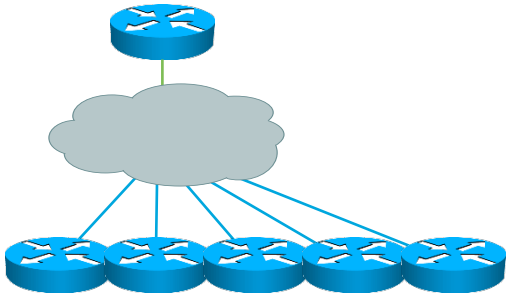
- EIGRP enhances multi-point interface stability
- When bringing up an interface with hundreds of neighbors, EIGRP may converge slowly, symptoms include:
  - → Continuous neighbor resets
  - → Packet retransmission timeout
  - → Stuck-in-Actives
  - → Hold time expirations
- EIGRP uses the bandwidth on the main interface divided by the number of neighbors on that interface to get the bandwidth available per neighbor



Routing Enhancements

- Interface type may appear to EIGRP to be a shared interface but the underlying network may not match up with the bandwidth defined on the interface.
- The minimum packet pacing interval can be lowered to a minimum value of 1 ms by using the bandwidth or bandwidth percentage commands

```
router(config-if)#ip bandwidth-percent eigrp 4453...
```



- Improvements to EIGRP transport to speedup convergence and increase neighbor scaling
- On a fast interface or a tunnel interface which has unreliable pacing value, EIGRP packet transmissions can also be driven using the neighbor acknowledgements (ACK-driven).
- Startup Update Packets exchanged at neighbor startup may now be sent using multicast

Routing Enhancements

Dynamic Multipoint VPN (DMVPN)

- EIGRP Distance Vector style matches with DMVPN NBMA network style
- Feasible successor for quick spoke-to-hub convergence
- Good scaling with reasonably fast convergence (hello 5, hold 15)
- Good metric control
  - Change metrics, route tagging, filtering or summarization at hub and/or spoke
  - Can be used to control load-balancing of spoke ←→ hub(s) traffic
  - Automatic metric increase per DMVPN hop
- Some issues with Equal Cost Multi-Path (ECMP) route selection
  - Between DMVPNs and preserving correct next-hop
  - Spoke-spoke tunnel load-balancing for spoke sites with multiple spoke routers
  - Recent features fixed these issues

Routing Enhancements—DMVPN

- Initial convergence testing was done with 400 peers with 10,000 prefixes to each peer
- Measure initial bring up convergence until all neighbors are established and queues empty

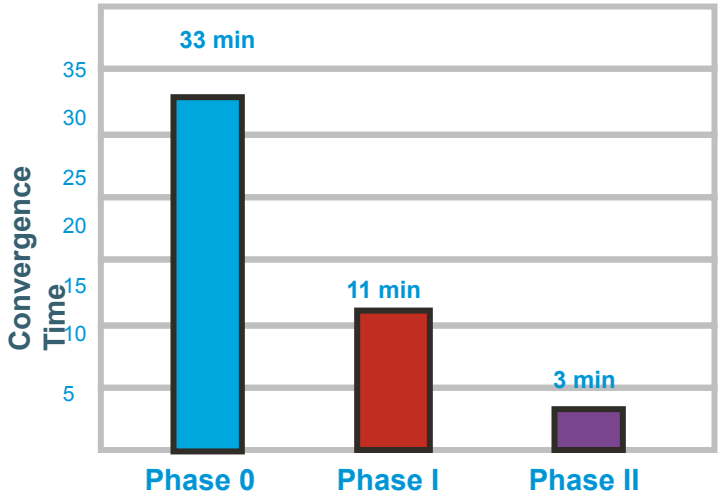
  EIGRP DMVPN Phase 0 (prior to 12.4(7))

  EIGRP DMVPN Phase I (12.4(7) and later)

  EIGRP DMVPN Phase II (CSCei03733)

  EIGRP DMVPN Phase III (Future)

- Currently, the practical maximum is:
  - ✓ 600 while advertising no more than 5k prefixes per spoke
  - ✓ 3500 while advertising no more than 1 prefix per spoke



Thank you.