



Advanced EIGRP





Implementing advanced EIGRP features



Objectives

- Upon completing this lesson, you will be able to implement route summarization and load balancing in an EIGRP network. This ability includes being able to meet these objectives:

- Configuring Manual Route Summarization

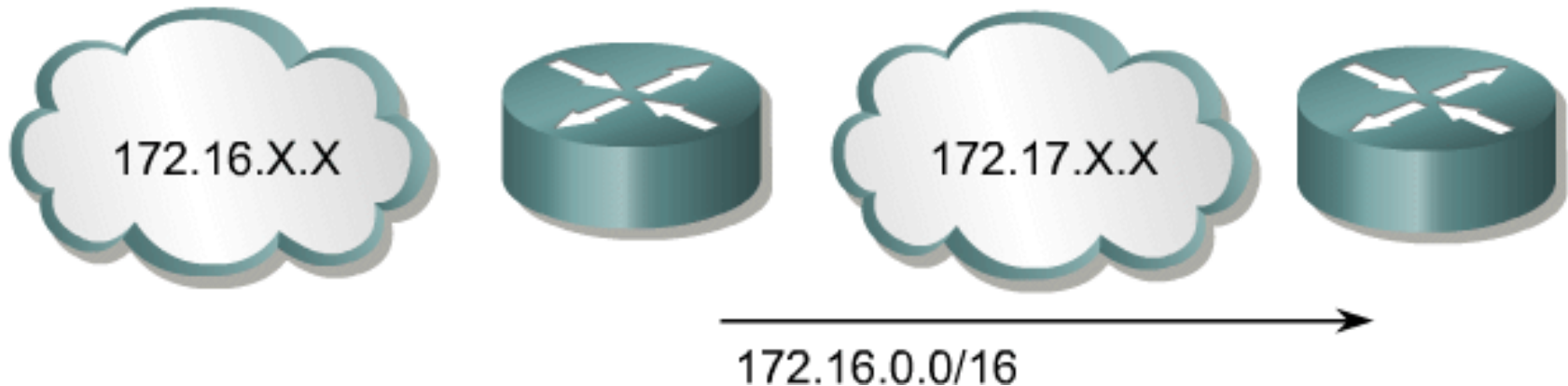
- Load Balancing Across Unequal Cost Paths

- Configuring EIGRP in a Frame Relay Hub-and-Spoke Topology

- Configuring EIGRP in a Hybrid Multipoint Topology

Route summarization

- Purpose: Smaller routing tables, smaller updates
- Automatic summarization:
 - On major network boundaries, subnetworks are summarized to a single classful (major) network.
 - **Automatic summarization occurs by default.**



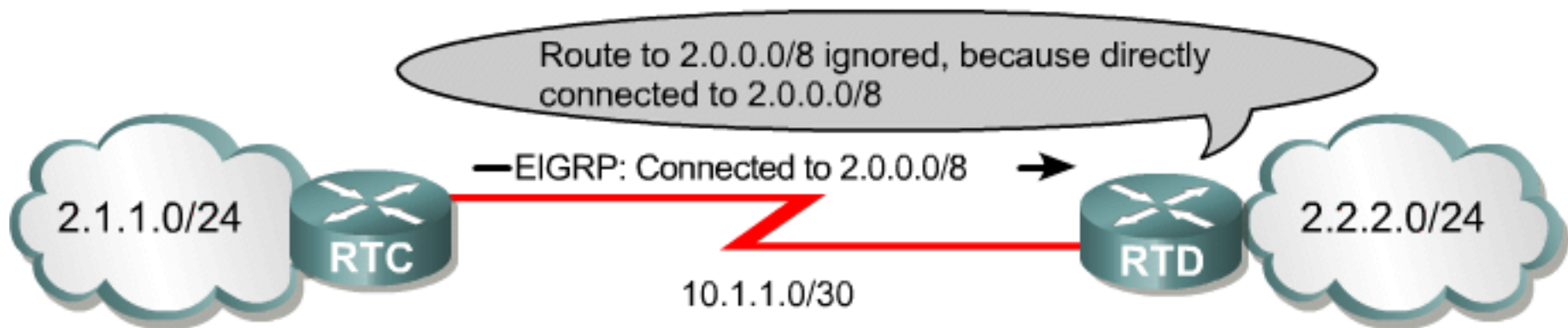
Manual route summarization characteristics

- Summarization is configurable on a per-interface basis in any router within a network.
- When summarization is configured on an interface, the router immediately creates a route pointing to null0.
 - Loop-prevention mechanism (explain)
- When the last specific route of the summary goes away, the summary is deleted.
- The minimum metric of the specific routes is used as the metric of the summary route.

Automatic route summarization issues

- By default route summarization is active. This can lead to problems with discontinuous networks

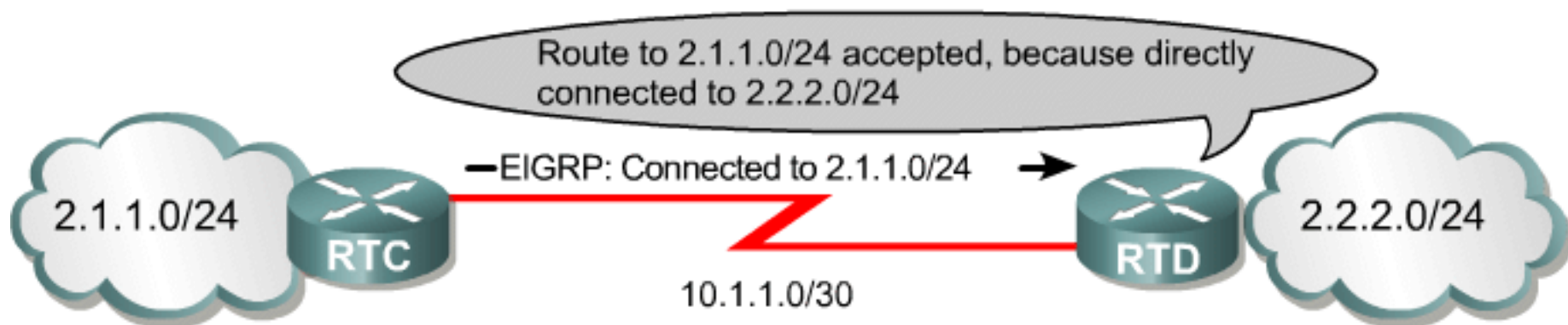
Discontinuous Networks with Autosummarization



Autosummarization prevents routers from learning about discontinuous subnets.

Disabled auto-summary

Discontiguous networks with the `no auto-summary` command configured on router RTC.



With summarization disabled, EIGRP routers will advertise subnets.

Manual route summarization

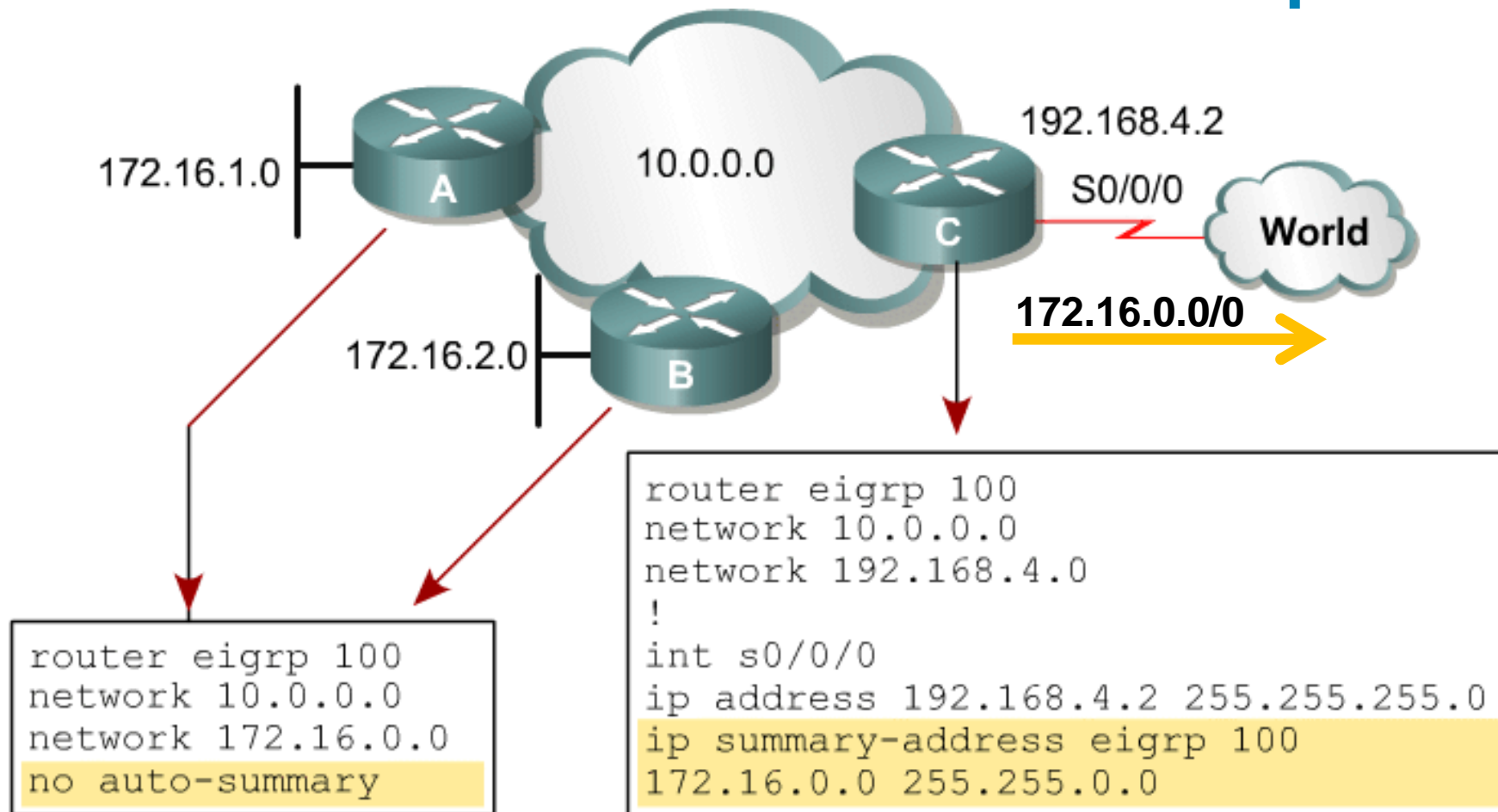
- Manual route summarization is configured in an interface basis.

(config-if) #

```
ip summary-address eigrp [as-number] [address] [mask]
```

Parameters	Description
<i>as-number</i>	EIGRP autonomous system (AS) number.
<i>address</i>	The IP address advertised as the summary address. This address does not need to be aligned on Class A, B, or C boundaries.
<i>mask</i>	The IP mask used to create the summary address.
<i>admin-distance</i>	(Optional) Administrative distance. A value from 0 to 255.

Manual route summarization example



Router C sees 172.16.1.0 and 172.16.2.0, but sends only 172.16.0.0/16 out S0/0/0.

Summary routing table

```
RouterC#show ip route
<output omitted>
Gateway of last resort is not set
  172.16.0.0/16 is variably subnetted, 3 subnets,
  2 masks
D    172.16.0.0/16 is a summary, 00:00:04, Null0
D    172.16.1.0/24 [90/156160] via 10.1.1.2, 00:00:04,
  FastEthernet0/0
D    172.16.2.0/24 [90/20640000] via 10.2.2.2,
  00:00:04, Serial0/0/1
C    192.168.4.0/24 is directly connected, Serial0/0/0
  10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.2.2.0/24 is directly connected, Serial0/0/1
C    10.1.1.0/24 is directly connected, FastEthernet0/0
D    10.0.0.0/8 is a summary, 00:00:05, Null0
RouterC#
```

Load balancing

- Routes with a metric equal to the minimum metric are installed in the routing table (equal cost load balancing).
- There can be up to six entries in the routing table for the same destination:
 - The number of entries is configurable.
Router (config-router) #maximum-paths *number*
 - The default is 4.
 - Set to 1 to disable load balancing.

Variance command

Router (config-router) #

```
variance multiplier
```

- Allows the router to include routes with a metric smaller than the *multiplier* times the minimum metric route to that destination.

variance Command Parameter

Parameter	Description
<i>multiplier</i>	A value from 1 to 128, used for load balancing. The default is 1, which indicates equal-cost load balancing. The <i>multiplier</i> defines the range of metric values that are accepted for load balancing by the EIGRP process.

Variance example

Network	Neighbor	FD	AD
Z	B	30	10
	C	20	10
	D	45	25

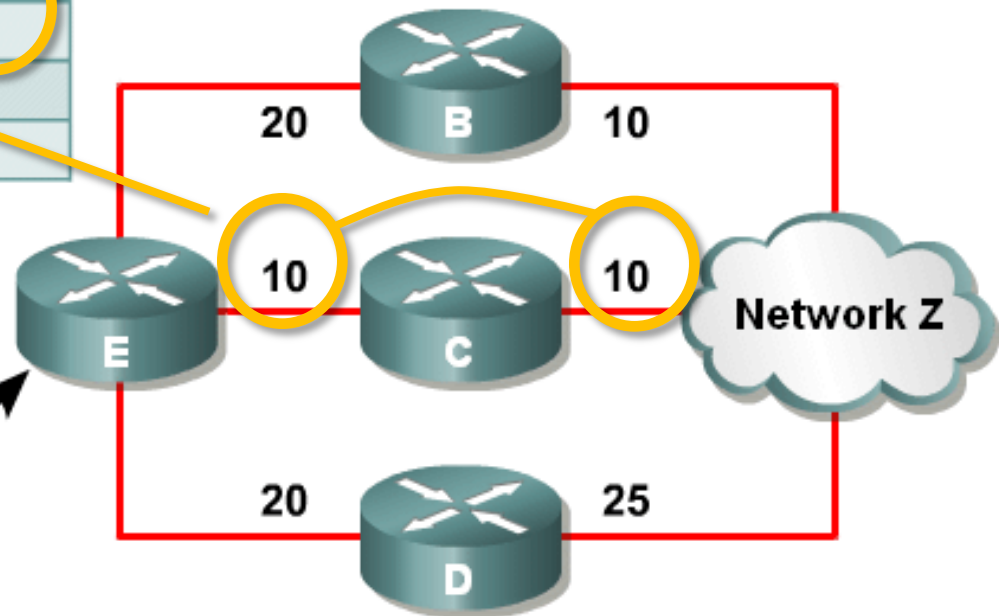
The two feasibility conditions are:

FD > alternate AD

FD * Variance > alternate FD

```
(config-router) #
```

```
variance 2
```



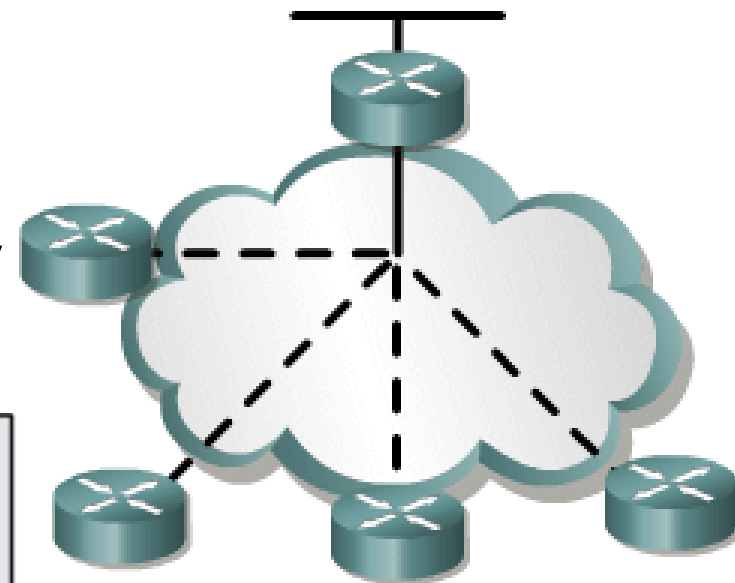
- Router E chooses router C to get to network Z because it has lowest FD of 20.
- With a variance of 2, router E chooses router B to get to network Z ($20 + 10 = 30 < [2 * (FD) = 40]$).
- Router D is never considered to get to network Z (because $25 > 20$).

Configuring wan links

- EIGRP supports different WAN links:
 - Point-to-point links**
 - NBMA** (Non Broadcast Multiple Access)
 - Multipoint links
 - Point-to-point links
- The default configuration parameters may not be the best option for all WAN links.
- EIGRP uses up to 50% of bandwidth by default; this bandwidth utilization can be changed



Point-to-Point



NBMA

```
interface serial10/0
bandwidth 32
ip bandwidth-percent eigrp 24 100
```

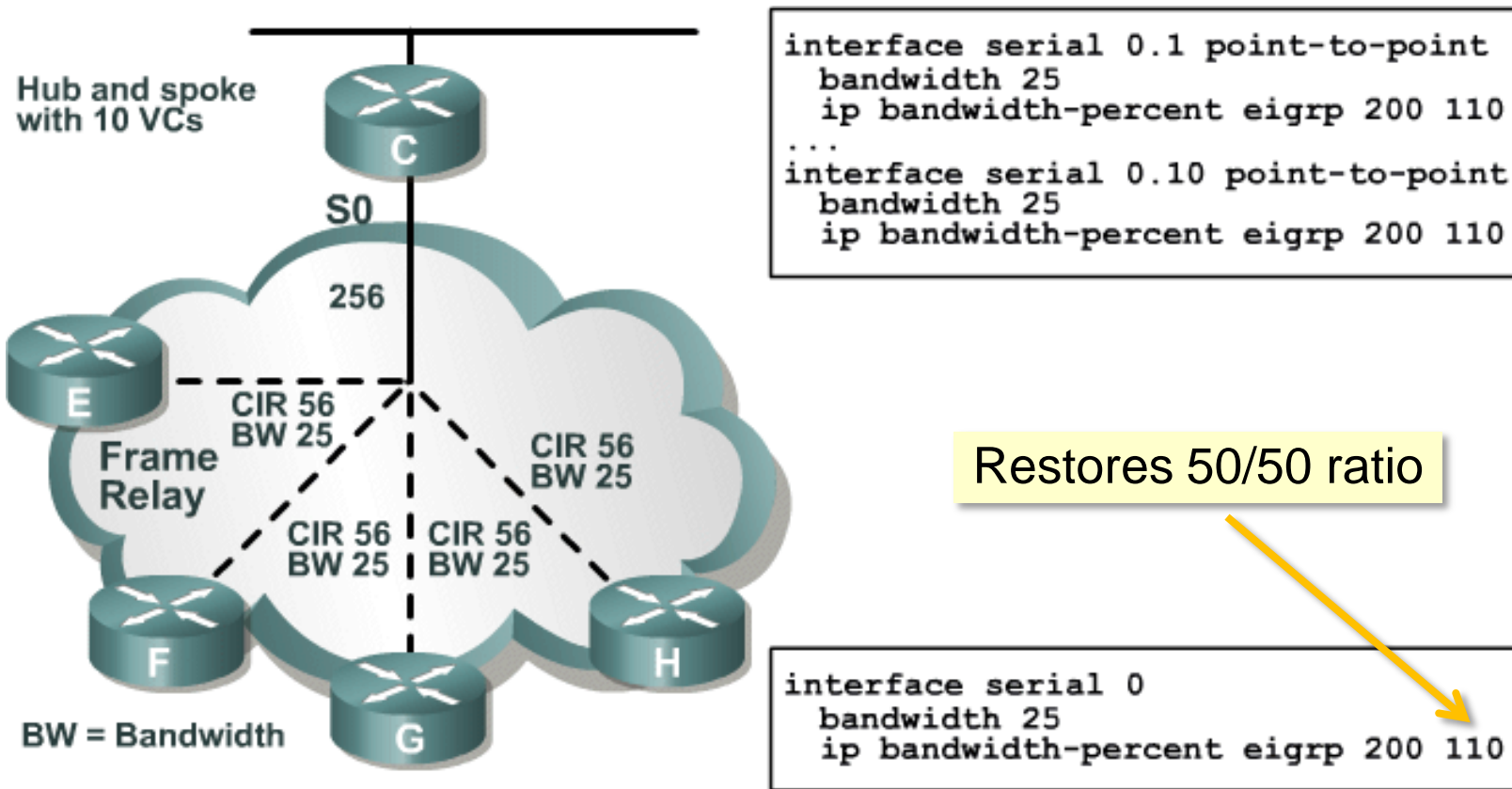
AS number

Percentage value = $100\% \times 32 = 32$ kbps

Bandwidth utilization over wan interfaces

- Bandwidth utilization over point-to-point sub-interfaces using Frame Relay:
 - Treats bandwidth as T1 by default.
 - Should manually configure bandwidth as the CIR of the PVC.
- Bandwidth utilization over multipoint Frame Relay, ATM, and ISDN PRI:
 - EIGRP uses the bandwidth on the physical interface divided by the number of neighbors on that interface to calculate the bandwidth attributed per neighbor.
- Each PVC can have a different CIR, creating an EIGRP packet-pacing problem.
- Multipoint interfaces:
 - Convert these to point-to-point configuration or manually configure bandwidth by multiplying the lowest CIR by the number of PVCs.

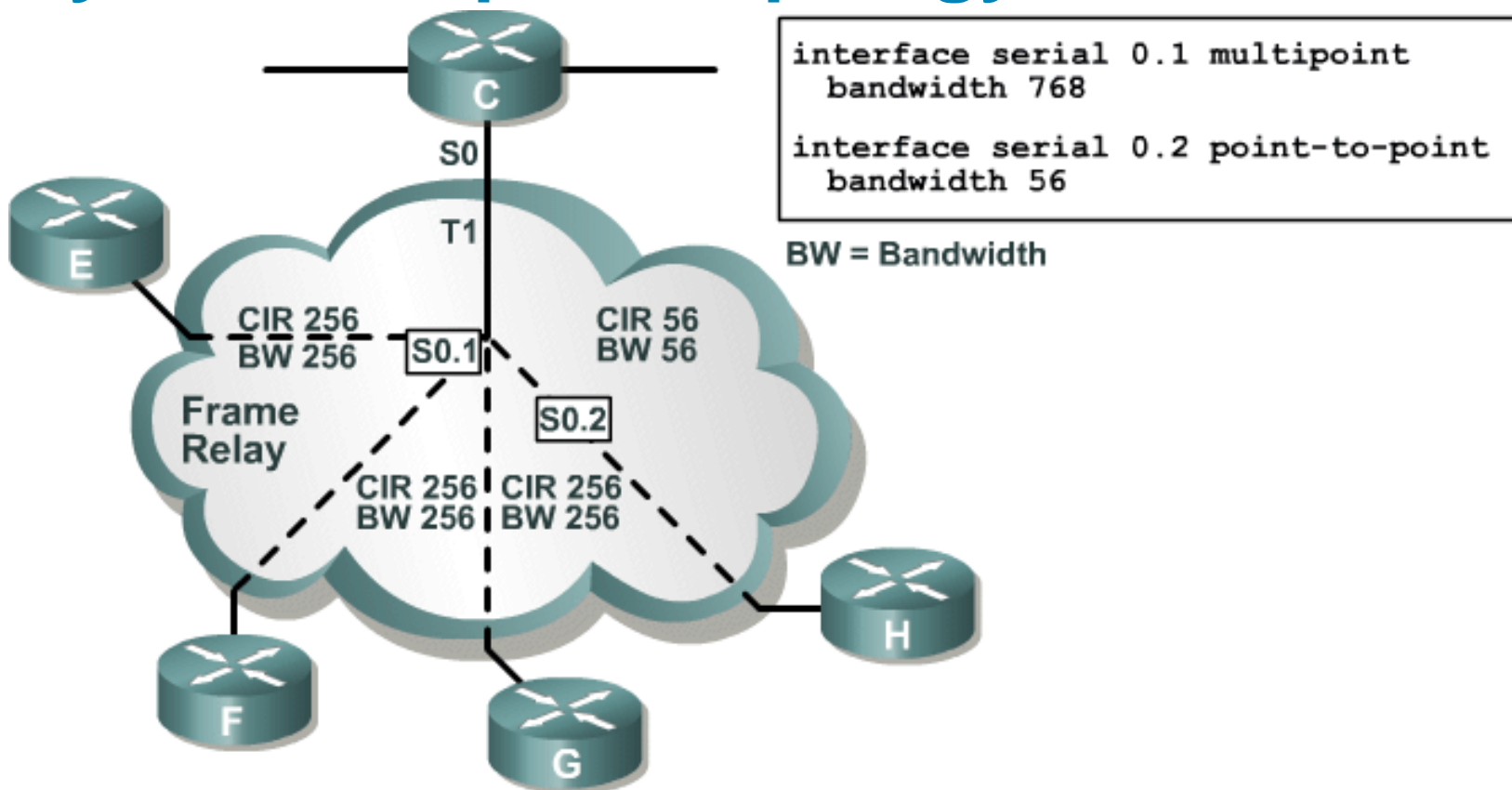
Frame Relay Hub and Spoke topology



Frame Relay Hub-and-Spoke

- Configure each VC as point-to-point, specify BW = 1/10 of link capacity
- Increase EIGRP utilization to 50% of actual VC capacity

Hybrid multipoint topology



Hybrid Multipoint

- Configure lowest CIR VC as point-to-point, specify BW = CIR.
- Configure higher CIR VCs as multipoint, combine CIRs.

Summary

- If the topology has discontinuous networks, turn the automatic summarization off.
- Manual route summarization is configured in an interface basis.
- Adjust the interface bandwidth for EIGRP to the best value depending of the topology used.
- Change the variance of EIGRP to allow for unequal cost load balancing.

Activity

- Make a simple EIGRP topology in Packet Tracer and study the characteristics of this protocol

Self Check

- Which issues has EIGRP with discontinuous subnetworks : _____
- Which commands are used to configure route summarization, _____ and _____
- How Does Load Balancing Work?

- How many types of wan networks support EIGRP?

Resources

- How Does Load Balancing Work?

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094820.shtml

- How Does Unequal Cost Path Load Balancing (Variance) Work in IGRP and EIGRP?

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a008009437d.shtml



Configuring EIGRP Authentication



Objectives

- Upon completing this lesson, you will be able to implement authentication in an EIGRP network. This ability includes being able to meet these objectives:

- Describe router authentication

- Describe the MD5 authentication used in EIGRP

- Configure MD5 authentication

- Troubleshoot MD5 authentication


Purpose of this Lesson

- Coverage of topics new to the “EIGRP” module of BSCI.
- What’s new in this module?
 - EIGRP Message Digest 5 (MD5) authentication and how to configure and troubleshoot it.

Router Authentication

- Many routing protocols support authentication such that a router authenticates the source of each routing update packet that it receives.
- Simple password authentication is supported by:
 - IS-IS
 - OSPF
 - RIPv2
- MD5 authentication is supported by:
 - OSPF
 - RIPv2
 - BGP
 - EIGRP

Simple Password vs. MD5 Authentication

- Simple password authentication:
 - Router sends packet and key.
 - Neighbor checks if received key matches its key.
 - Not secure.
- MD5 authentication 
 - Configure a “key” (password) and key-id; router generates a message digest, or hash, of the key, key-id and message.
 - Message digest is sent with packet; key is not sent.
 - Secure.

EIGRP MD5 Authentication

- EIGRP supports MD5 authentication.
- Router generates and checks every EIGRP packet. Router authenticates the source of each routing update packet that it receives.
- Configure a “key” (password) and key-id; each participating neighbor must have same key configured.

MD5 Authentication

- EIGRP MD5 authentication:

Router generates a message digest, or hash, of the key, key-id, and message.

EIGRP allows keys to be managed using key chains.

Specify key-id (number, key, and lifetime of key).

First valid activated key, in order of key numbers, is used.

Configuring EIGRP MD5 Authentication

Router (config-if) #

```
ip authentication mode eigrp autonomous-system md5
```

- Specifies MD5 authentication for EIGRP packets

Router (config-if) #

```
ip authentication key-chain eigrp autonomous-system  
name-of-chain
```

- Enables authentication of EIGRP packets using key in the *key-chain*

Configuring EIGRP MD5 Authentication (cont.)

Router (config) #

```
key chain name-of-chain
```

- Enters configuration mode for the **key-chain**

Router (config-keychain) #

```
key key-id
```

- Identifies key and enters configuration mode for the **key-id**

Configuring EIGRP MD5 Authentication (cont.)

Router (config-keychain-key) #

```
key-string text
```

- Identifies key string (password)

Router (config-keychain-key) #

```
accept-lifetime start-time {infinite | end-time | duration  
seconds}
```

- Optional: specifies when key will be accepted for received packets

Router (config-keychain-key) #

```
send-lifetime start-time {infinite | end-time | duration  
seconds}
```

- Optional: specifies when key can be used for sending packets

Example MD5 Authentication Configuration



R1 Configuration for MD5 Authentication

```
<output omitted>
key chain R1chain
  key 1
    key-string firstkey
    accept-lifetime 04:00:00 Jan 1 2006 infinite
    send-lifetime 04:00:00 Jan 1 2006 04:01:00 Jan 1 2006
  key 2
    key-string secondkey
    accept-lifetime 04:00:00 Jan 1 2006 infinite
    send-lifetime 04:00:00 Jan 1 2006 infinite
<output omitted>
interface FastEthernet0/0
  ip address 172.16.1.1 255.255.255.0
!
interface Serial0/0/1
  bandwidth 64
  ip address 192.168.1.101 255.255.255.224
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 R1chain
!
router eigrp 100
  network 172.16.1.0 0.0.0.255
  network 192.168.1.0
  auto-summary
```

R1 accepts 2 keys

But sends only key 2

R2 Configuration for MD5 Authentication

```
<output omitted>
key chain R2chain
  key 1
    key-string firstkey
    accept-lifetime 04:00:00 Jan 1 2006 infinite
    send-lifetime 04:00:00 Jan 1 2006 infinite
  key 2
    key-string secondkey
    accept-lifetime 04:00:00 Jan 1 2006 infinite
    send-lifetime 04:00:00 Jan 1 2006 infinite
<output omitted>
interface FastEthernet0/0
  ip address 172.17.2.2 255.255.255.0
!
interface Serial0/0/1
  bandwidth 64
  ip address 192.168.1.102 255.255.255.224
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 R2chain
!
router eigrp 100
  network 172.17.2.0 0.0.0.255
  network 192.168.1.0
  auto-summary
```

Verifying MD5 Authentication

```
R1#
*Jan 21 16:23:30.517: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor
192.168.1.102 (Serial0/0/1) is up: new adjacency

R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                Interface    Hold   Uptime    SRTT    RTO   Q   Seq
0   192.168.1.102           Se0/0/1     12    00:03:10  17      2280  0   14

R1#show ip route
<output omitted>
Gateway of last resort is not set
D    172.17.0.0/16 [90/40514560] via 192.168.1.102, 00:02:22, Serial0/0/1
    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D    172.16.0.0/16 is a summary, 00:31:31, Null0
C    172.16.1.0/24 is directly connected, FastEthernet0/0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.96/27 is directly connected, Serial0/0/1
D    192.168.1.0/24 is a summary, 00:31:31, Null0
R1#ping 172.17.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/15/16 ms
```

Troubleshooting MD5 Authentication

```
R1#debug eigrp packets
```

```
EIGRP Packets debugging is on
```

```
(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY,  
SIAREPLY)
```

```
*Jan 21 16:38:51.745: EIGRP: received packet with MD5 authentication, key id = 1
```

```
*Jan 21 16:38:51.745: EIGRP: Received HELLO on Serial0/0/1 nbr 192.168.1.102
```

```
*Jan 21 16:38:51.745: AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 pe  
erQ un/rely 0/0
```

```
R2#debug eigrp packets
```

```
EIGRP Packets debugging is on
```

```
(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY,  
SIAREPLY)
```

```
R2#
```

```
*Jan 21 16:38:38.321: EIGRP: received packet with MD5 authentication, key id = 2
```

```
*Jan 21 16:38:38.321: EIGRP: Received HELLO on Serial0/0/1 nbr 192.168.1.101
```

```
*Jan 21 16:38:38.321: AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 pe  
erQ un/rely 0/0
```

Troubleshooting MD5 Authentication Problem

MD5 authentication on both R1 and R2, but R1 key 2 (that it uses when sending) changed

```
R1(config-if)#key chain R1chain
R1(config-keychain)#key 2
R1(config-keychain-key)#key-string wrongkey

R2#debug eigrp packets
EIGRP Packets debugging is on
  (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY,
  SIAREPLY)
R2#
*Jan 21 16:50:18.749: EIGRP: pkt key id = 2, authentication mismatch
*Jan 21 16:50:18.749: EIGRP: Serial0/0/1: ignored packet from 192.168.1.101, opcode = 5 (invalid authentication)
*Jan 21 16:50:18.749: EIGRP: Dropping peer, invalid authentication
*Jan 21 16:50:18.749: EIGRP: Sending HELLO on Serial0/0/1
*Jan 21 16:50:18.749:   AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
*Jan 21 16:50:18.753: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.1.101
  (Serial0/0/1) is down: Auth failure

R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
R2#
```

Summary

- There are two types of router authentication: simple password and MD5.
- When EIGRP authentication is configured, the router generates and checks every EIGRP packet and authenticates the source of each routing update packet that it receives. EIGRP supports MD5 authentication.
- To configure MD5 authentication, use the **ip authentication mode eigrp** and **ip authentication key-chain** interface commands. The key chain must also be configured, starting with the key chain command.
- Use **debug eigrp packets** to verify and troubleshoot MD5 authentication.

Activity

- Using the network created in the last class using EIGRP as your routing protocol, follow the steps in this module to add security to EIGRP.
- Be sure to verify your connections by running the show commands discussed in the module both before and after you implement security.

```
show ip protocols, show ip eigrp interfaces, show  
ip eigrp neighbors, show ip eigrp topology, and  
show ip eigrp traffic
```

- NOTE: before adding any security, you should always verify your connection first to avoid additional troubleshooting later.

Self Check

- Name the two types of router authentication:
_____ and _____
- Which two commands are used to configure MD5 authentication, _____ and _____
- What debug command will verify and troubleshoot MD5 authentication?

Resources

- http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a008009405c.shtml
- http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a00800ca5a9.html
- http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f07.shtml

▪



Configuring EIGRP in an Enterprise Network



Objectives

Upon completing this lesson, you will be able to describe, recognize, and correct common EIGRP issues and problems. This ability includes being able to meet these objectives:

- Explain factors affecting scalability in large internetworks
- Explain how EIGRP uses queries to update its routing tables in the event a route is lost and there is no feasible successor
- Explain how to mark the spokes of large network as stubs to reduce EIGRP queries and thus improve network scaling
- Explain why SIA connections occur
- Explain how to minimize active routes
- Describe how graceful shut down prevents loss of packets when routers go down

Purpose of this Lesson

Coverage of topics new to the “EIGRP” module of BSCI.

- What’s new in this module?
 - Configuring EIGRP in large scale (enterprise) networks

Factors That Influence EIGRP Scalability

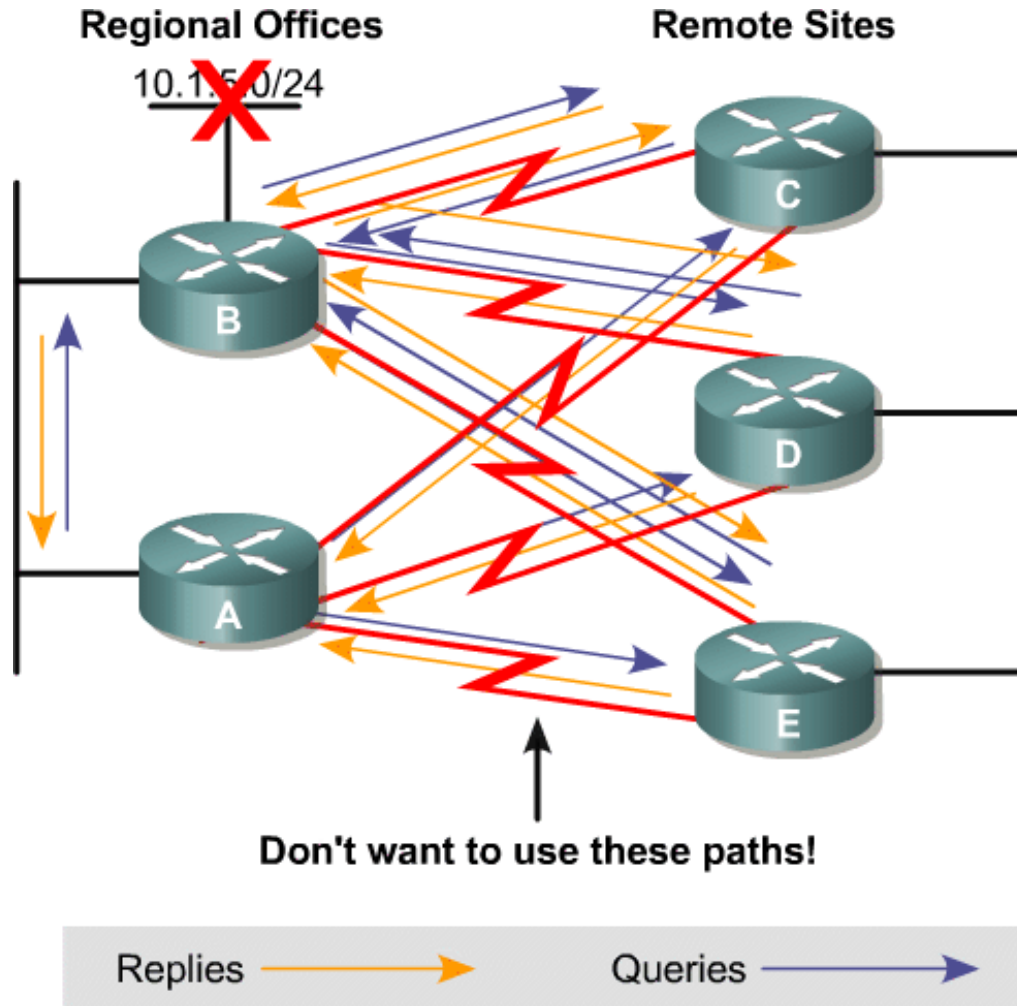
- Quantity of routing information exchanged between peers: without proper route summarization, this can be excessive.
- Number of routers that must be involved when a topology change occurs.
- Depth of topology: the number of hops that information must travel to reach all routers. (No more than 7 routers)
- Number of alternate paths through the network. (Too much isn't better)

EIGRP Query Process

- Queries are sent when a route is lost and no feasible successor is available.
- The lost route is now in “active” state.
- Queries are sent to all neighboring routers on all interfaces except the interface to the successor (split horizon).
- If the neighbors do not have their lost-route information, queries are sent to their neighbors.
- If a router has an alternate route, it answers the query; this stops the query from spreading in that branch of the network.
- If the router does not receive a reply to all the outstanding queries within 3 minutes (the default time), the route goes to the SIA (Stuck In Active) state.

Updates and Queries in Hub-and-Spoke Topology

The EIGRP stub routing feature can prevent this problem by restricting the remote router from advertising the hub router routes back to other hub routers.

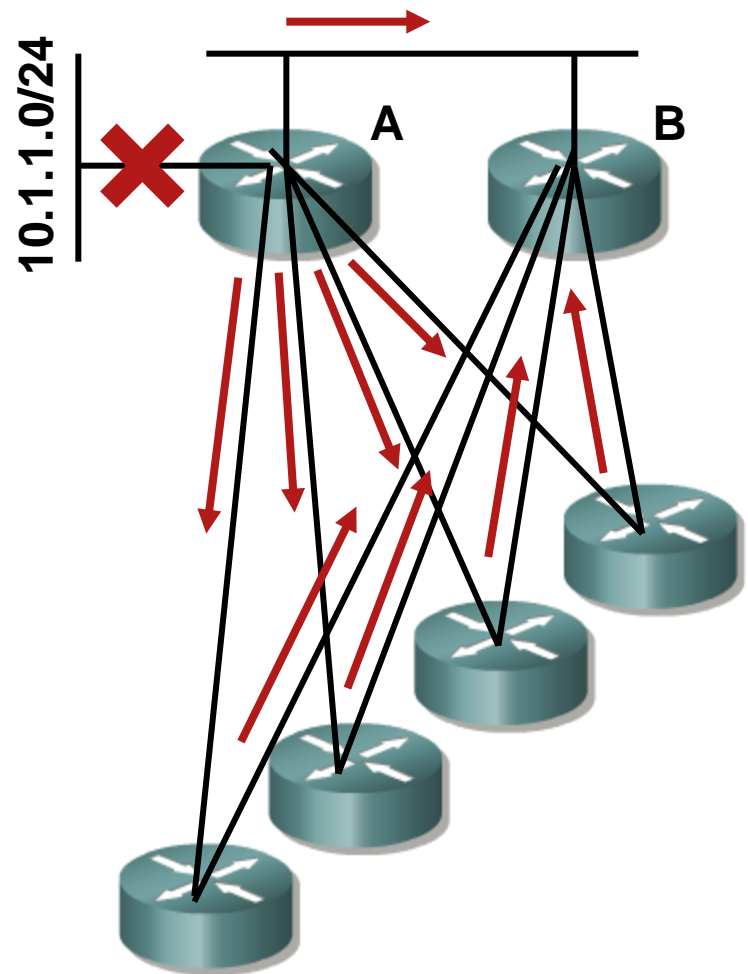


EIGRP Stub

- The EIGRP Stub Routing feature
 - Improves network stability
 - Reduces resource utilization and
 - Simplifies remote router (spoke) configuration
- Stub routing is commonly used in hub-and-spoke topology
- Stub router sends a special peer information packet to all neighboring routers to report its status as a stub router
- Any neighbor that receives a packet informing it of the stub status does not query the stub router for any routes

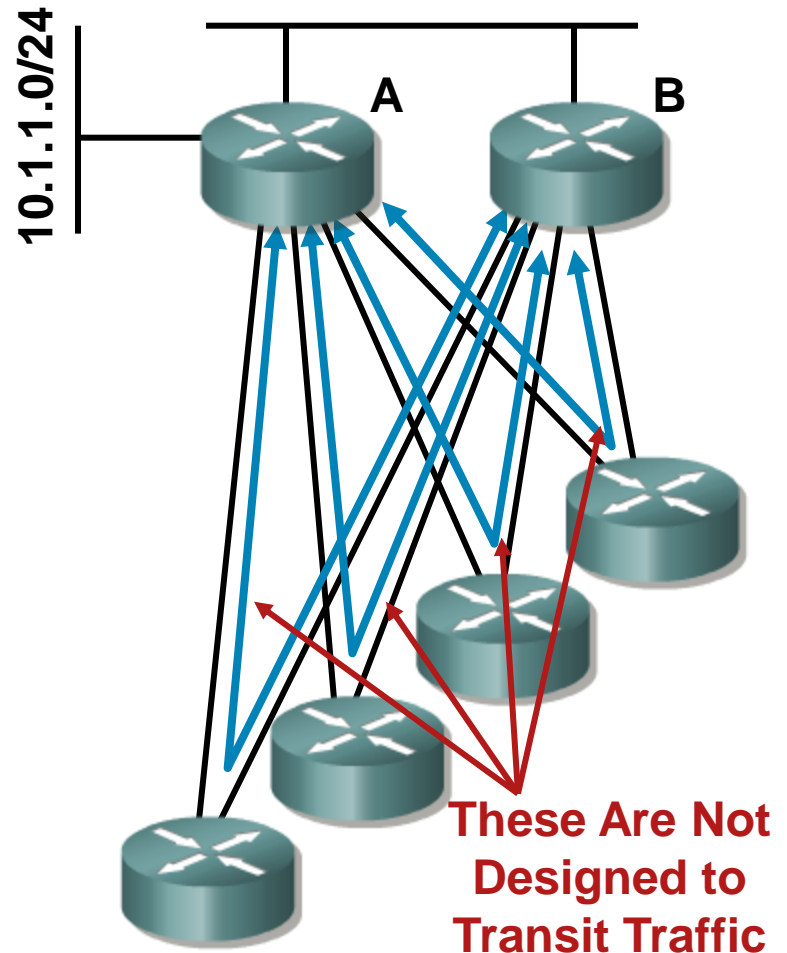
Stub Review

- If A loses its connection to 10.1.1.0/24, it must build and transmit five queries: one query to each remote, and one query to B
- Each of the remote sites will also build a query towards B
- B receives five queries which it must process and answer



Stub Review

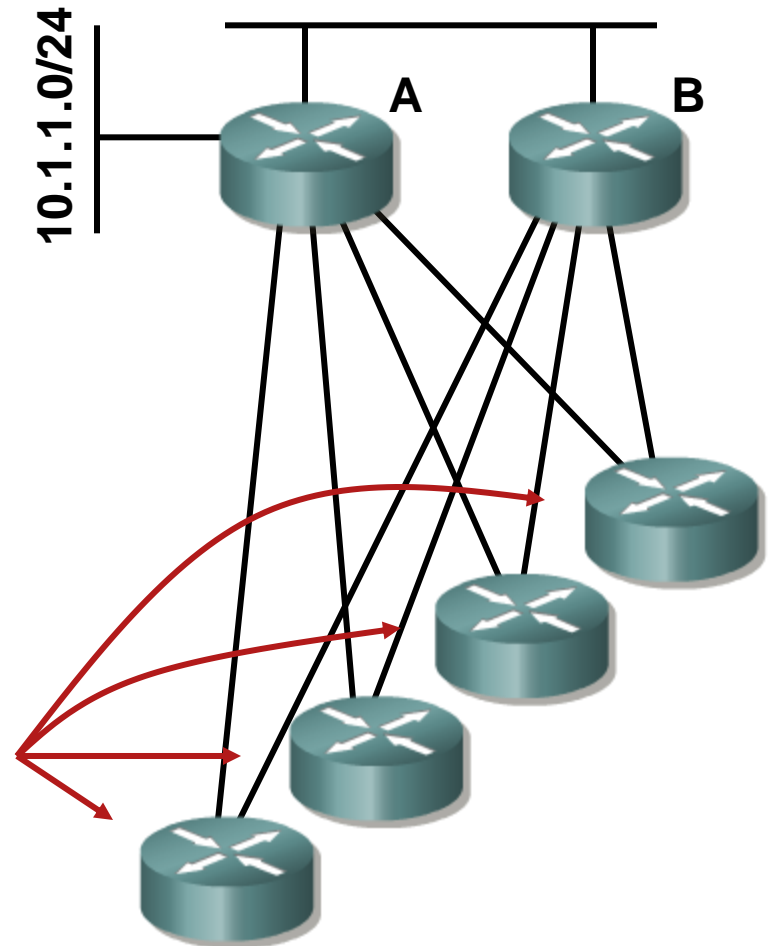
- If these spokes are remotes sites, they typically have two connections for redundancy, not so they can transit traffic between A and B
- A should never use the spokes as a path to anything reachable through B, so there's no reason to learn about, or query for, routes through these spokes



Stub Review

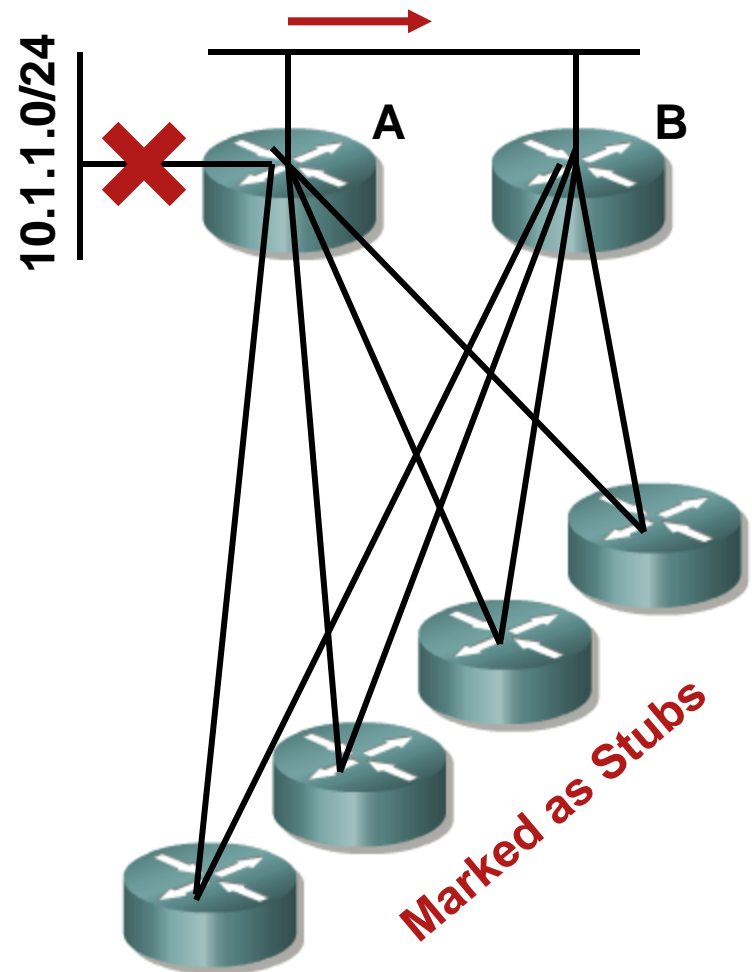
To signal A and B that the paths through the spokes should not be used for transit traffic, the spoke routers can be configured as stubs

```
router#config t#  
router(config)#router eigrp 100  
router(config-router)#eigrp stub  
router(config-router)#
```



Stub Review

- Marking the spokes as stubs allows them to signal A and B that they are not transit paths
- A will not query stubs, reducing the total number of queries in this example to one
- Marking the remotes as stubs also reduces the complexity of this topology; B now believes it only has one path to 10.1.1.0/24, rather than five



Configuring EIGRP Stub

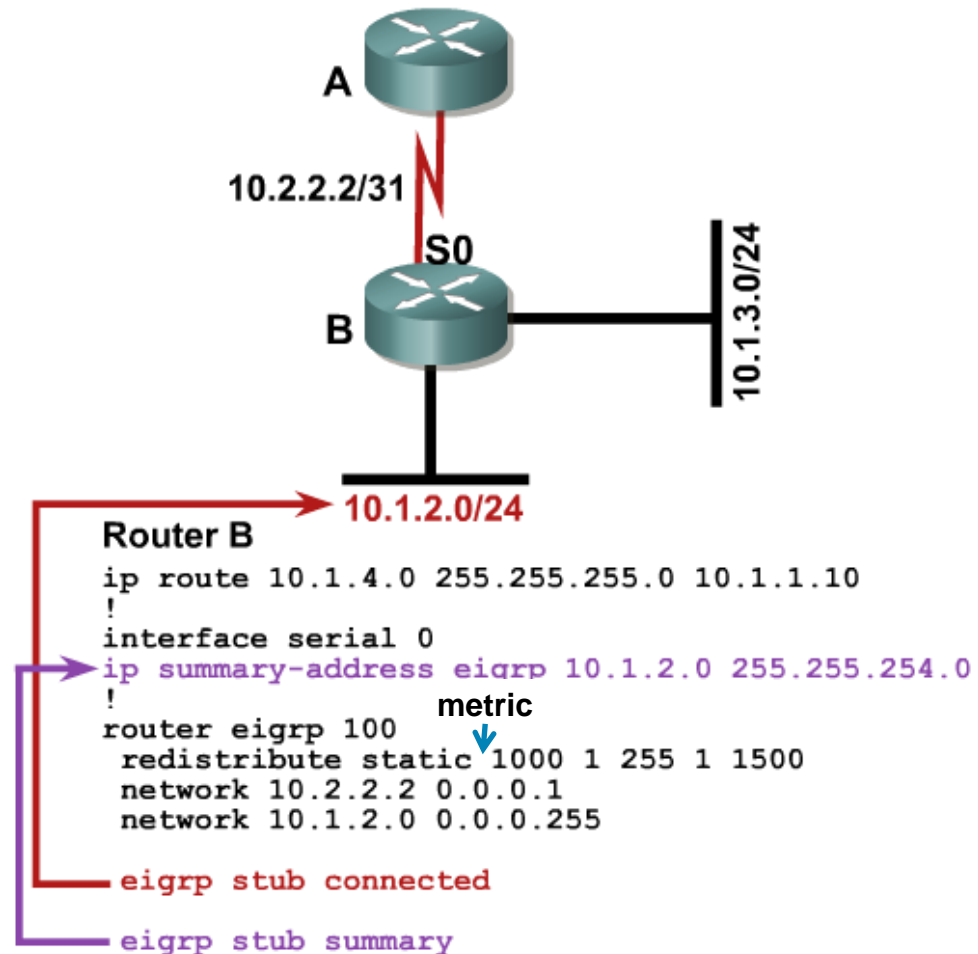
Router (config-router) #

```
eigrp stub [receive-only|connected|static|summary]
```

- **receive-only:** Prevents the stub from sending any type of route.
- **connected:** Permits stub to send connected routes (may still need to redistribute).
- **static:** Permits stub to send static routes (must still redistribute).
- **summary:** Permits stub to send summary routes.
- Default is **connected** and **summary**.

Example: EIGRP stub Parameters

- If **stub connected** is configured:
 - B will advertise 10.1.2.0/24 to A.
 - B will not advertise 10.1.2.0/23, 10.1.3.0/24, or 10.1.4.0/24.
- If **stub summary** is configured:
 - B will advertise 10.1.2.0/23 to A.
 - B will not advertise 10.1.2.0/24, 10.1.3.0/24, or 10.1.4.0/24.



Example: EIGRP stub Parameters (Cont.)

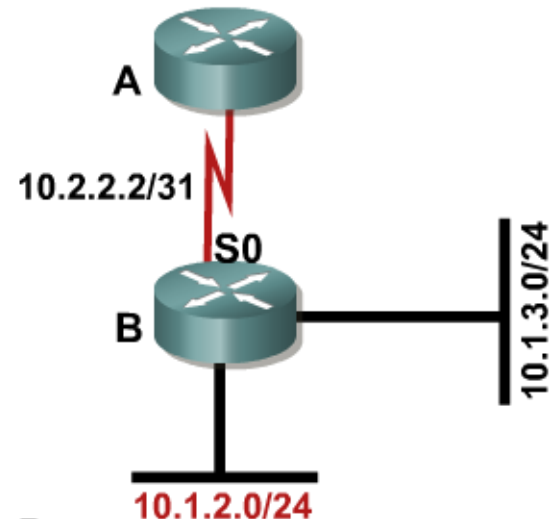
- If **stub static** is configured:

B will advertise 10.1.4.0/24 to A.

B will not advertise 10.1.2.0/24, 10.1.2.0/23, or 10.1.3.0/24.

- If **stub receive-only** is configured:

B won't advertise anything to A, so A needs to have a static route to the networks behind B to reach them.



Router B

```
ip route 10.1.4.0 255.255.255.0 10.1.1.10
!
interface serial 0
ip summary-address eigrp 10.1.2.0 255.255.254.0
!
router eigrp 100
  redistribute static metric 1000 1 255 1 1500
  network 10.2.2.2 0.0.0.1
  network 10.1.2.0 0.0.0.255
!
eigrp stub static
!
eigrp stub summary
```

EIGRP Query Process Stuck-in-Active

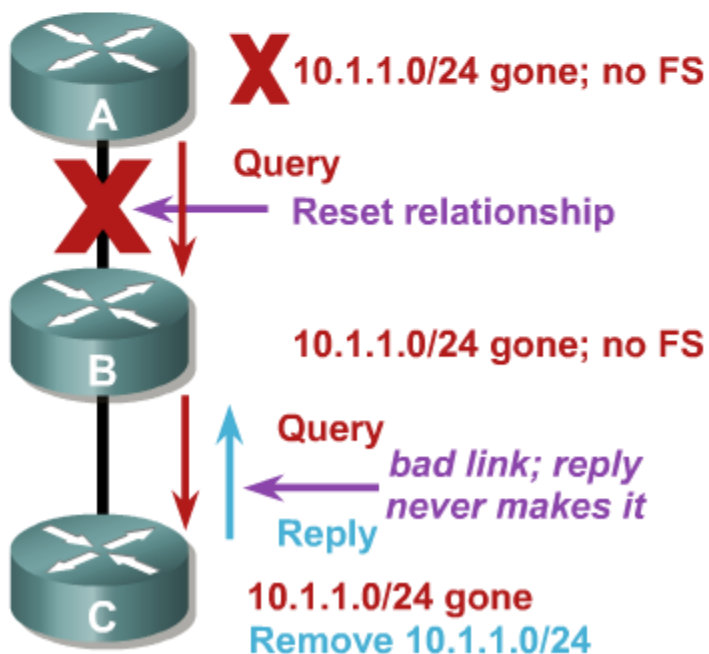
- The router has to get all the replies from the neighbors with an outstanding query before the router calculates the successor information.

If any neighbor fails to reply to the query within three minutes, by default, the route is SIA, and the router resets the neighbor relationship with the neighbor that fails to reply.

Active Process Enhancement

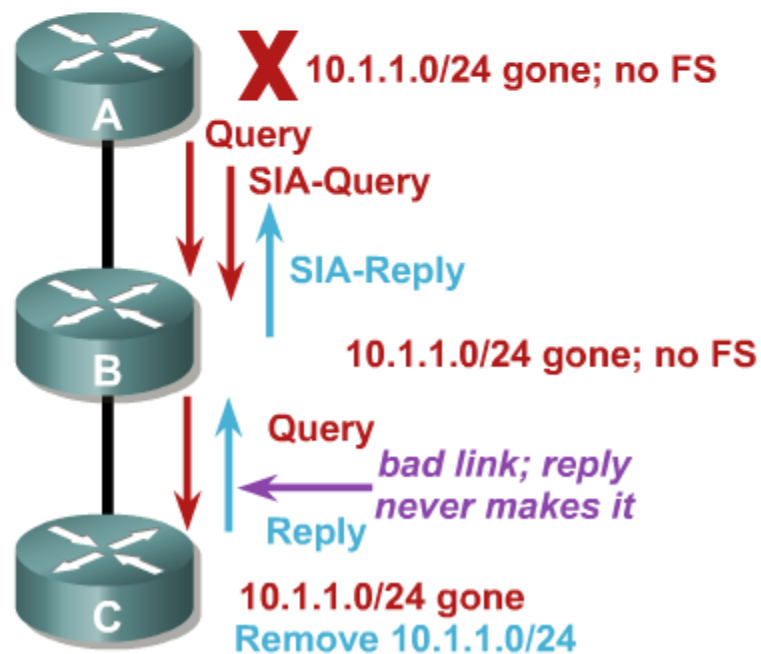
Before

- Router A resets relationship to router B when the normal active timer expires. However, the problem is the link between router B and C.

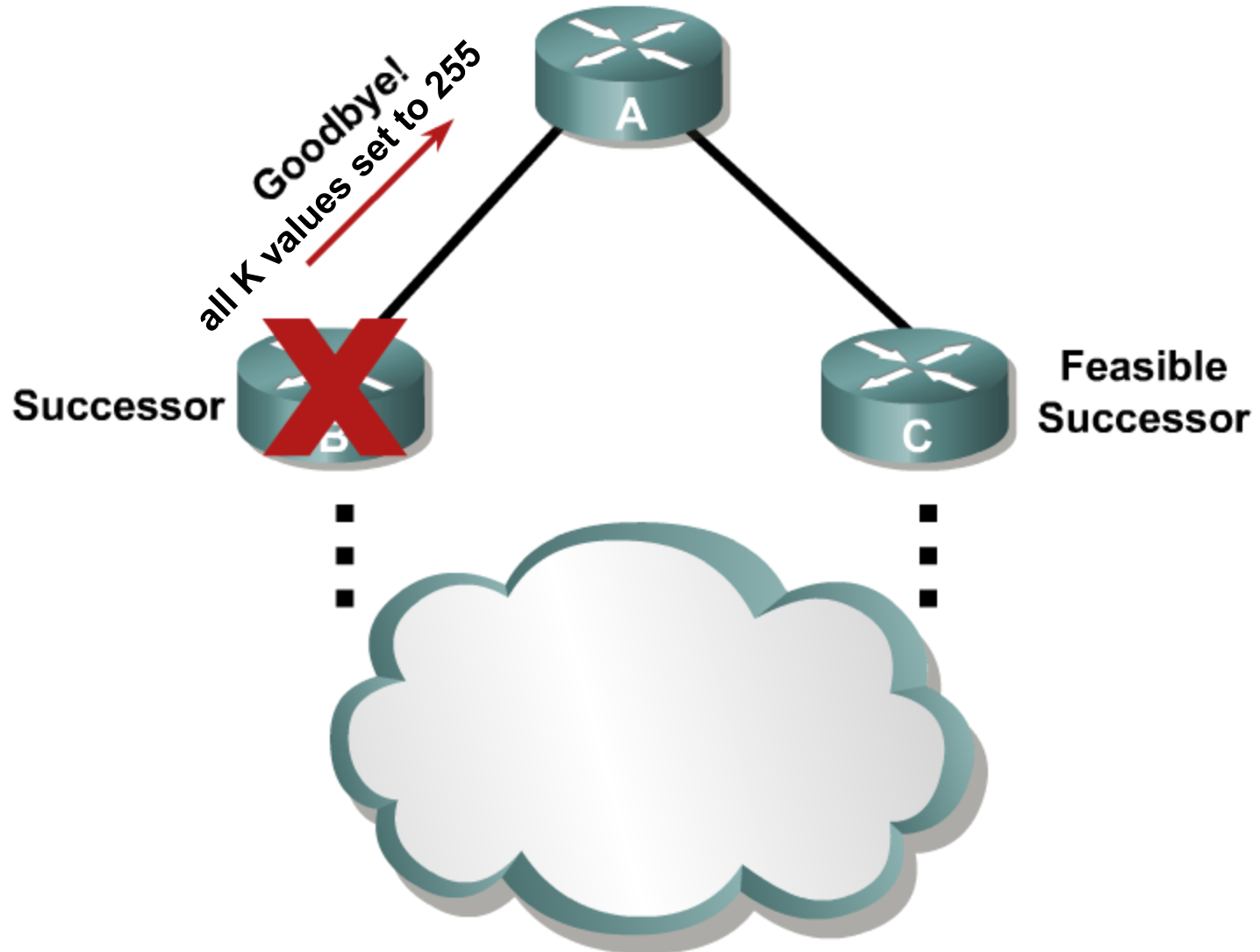


After

- Router A sends an SIA-Query at half of the normal active timer. Router B acknowledges the query there by keeping the relationship up.



Graceful Shutdown



Summary

- Factors that affect network scalability include:
 - Amount of information exchanged between neighbors
 - Number of routers
 - Depth of the topology
 - Number of alternate paths through the network
- When a route is lost and no feasible successor is available, queries are sent to all neighboring routers on all interfaces.
- The `igrp stub` command is used to enable the stub routing feature, which improves network stability, reduces resource utilization, and simplifies stub router configuration.

Summary (Cont.)

- Once a route goes active and the query sequence is initiated, it can only come out of the active state and transition to passive state when it receives a reply for every generated query. If the router does not receive a reply to all the outstanding queries within 3 minutes (the default time), the route goes to the SIA state.
- The active process enhancement feature enables an EIGRP router to monitor the progression of the search for a successor route so that neighbor relationships are not reset unnecessarily.
- With graceful shutdown, a goodbye message is broadcast when an EIGRP routing process is shut down, to inform adjacent peers about the impending topology change.

Activity

- Using the network created before using EIGRP as your routing protocol, follow the steps in this module to add a stub to EIGRP. Be sure you are running `debug eigrp` to watch communication of your links.
- You can also verify your connections by running the show commands discussed in the previous module once you have added your stub route.
 - `show ip protocols`, `show ip eigrp interfaces`, `show ip eigrp neighbors`, `show ip eigrp topology`, and `show ip eigrp traffic`
- With debugging still running, shut down your stub connection and observe the communication on your debug output.

Self Check

- What factors affect the scalability of a network:
- What command is used to enable the stub routing feature?
- What is the purpose of enabling EIGRP stub routing?
- When routes are lost and no feasible successor can be found, how does EIGRP reestablish its connection?

Resources

- http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a008009405c.shtml
- http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a00800ca5a9.html
- http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f07.shtml
- http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_chapter09186a008017d003.html

▪

Q and A



