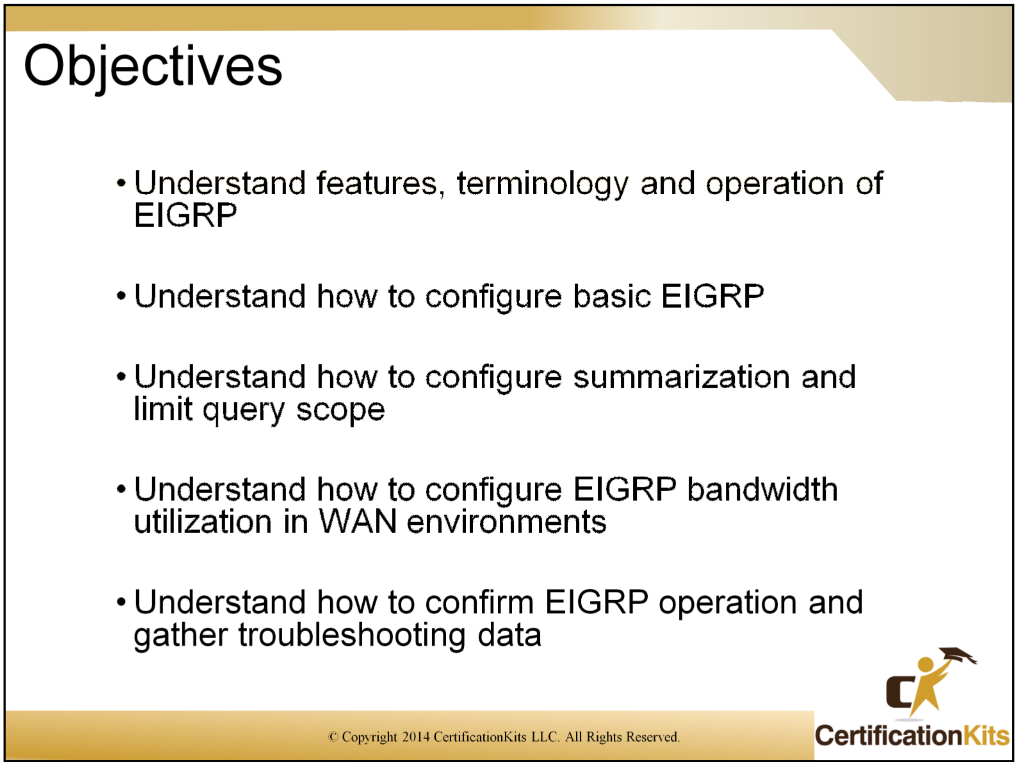
Implementing an EIGRP based Solution

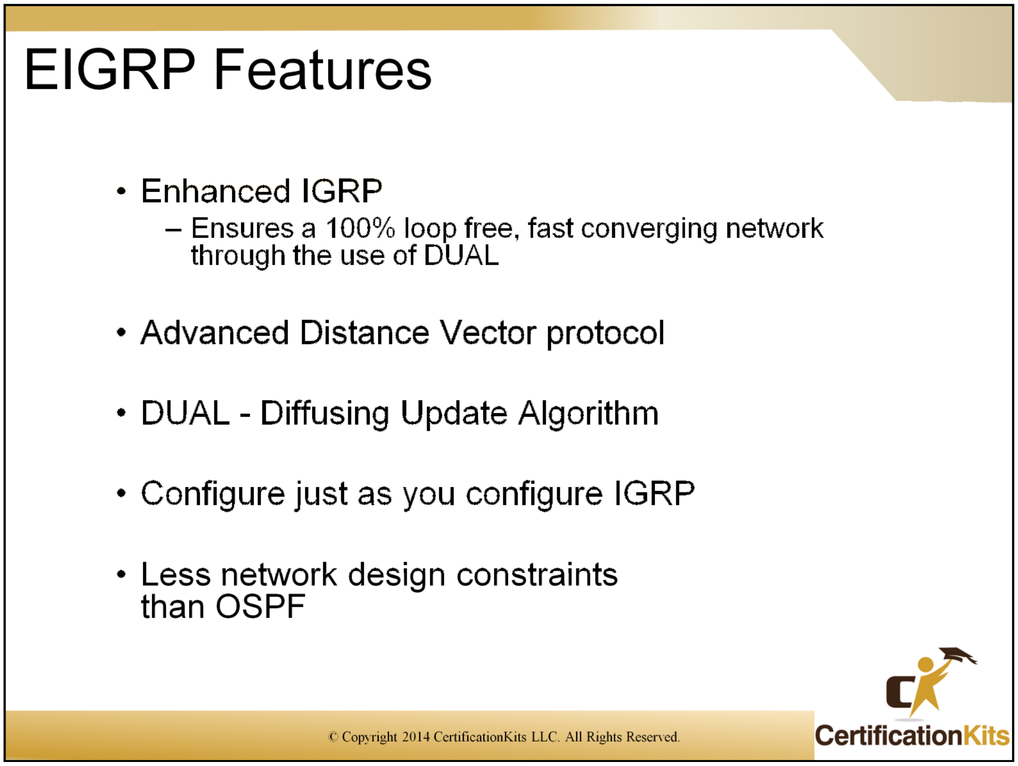
Chapter 2

CertificationKits

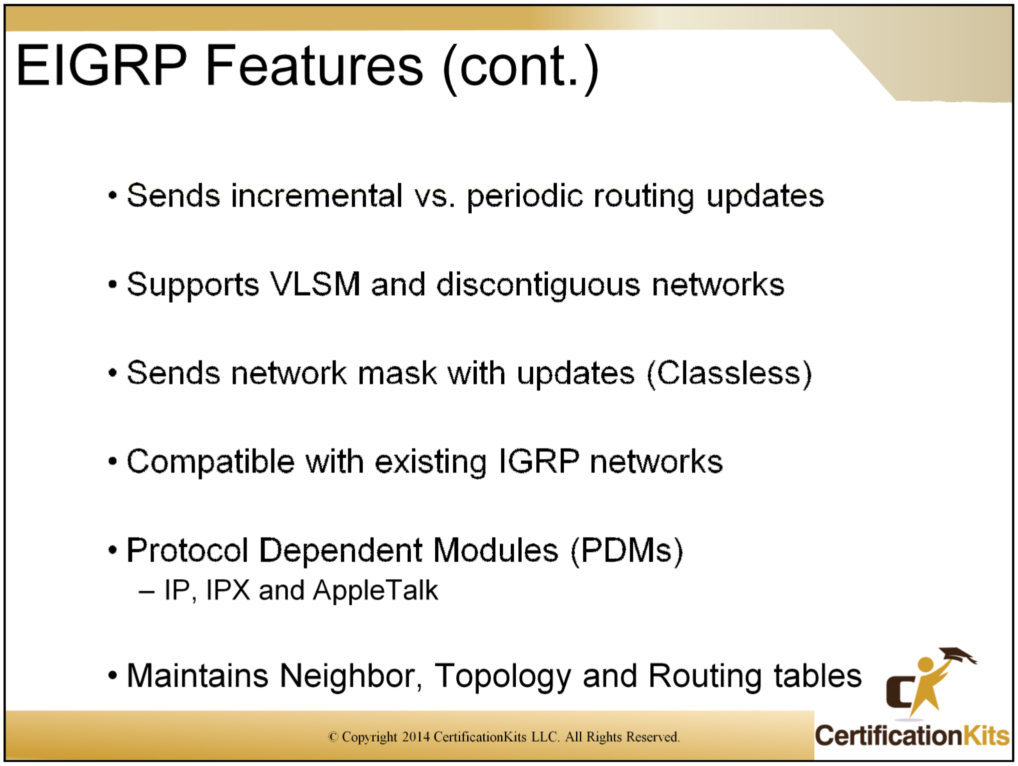


Ah, Enhanced IGRP. Cisco's proprietary routing protocol. The objectives of this chapter is to:

- Understand features, terminology and operation of EIGRP
- Understand how to configure basic EIGRP
- Understand how to configure summarization and limit query scope
- Understand how to configure EIGRP bandwidth utilization in WAN environments
- Understand how to confirm EIGRP operation and gather troubleshooting data



Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco Proprietary Routing Protocol. It has the same metrics as IGRP. It uses Diffusing Update Algorithm (DUAL) to guarantee a loop free topology. EIGRP uses less CPU resources than OSPF while also having fewer design constraints. It is considered an advanced distance vector routing protocol although it has some similarities to a link state routing protocol.



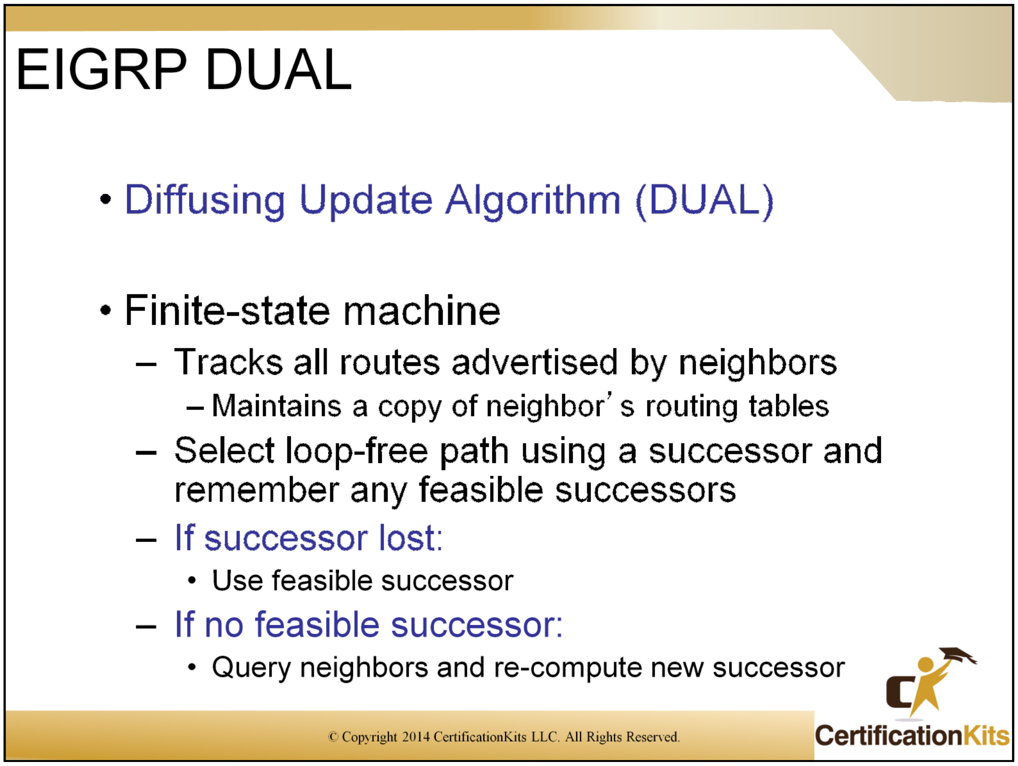
EIGRP, like OSPF communicates via multicast transmissions. The multicast address that EIGRP uses is 224.0.0.10.

EIGRP initially floods its routing information to all neighbors, but then scales back and does not send a routing update unless there is a change in the routing information.

EIGRP supports VLSM because it will send the prefix, or mask information along with all of its routing updates. EIGRP by default will automatically summarize to the classful boundary, however you can turn this feature off using the *no auto-summary* command under the EIGRP router configuration mode.

In the event you have IGRP configured in your network, EIGRP will do automatic redistribution in order to learn all of the available routes within IGRP.

EIGRP keeps separate neighbor tables, topology tables and routing tables for each of the protocols you have configured in your network environment.



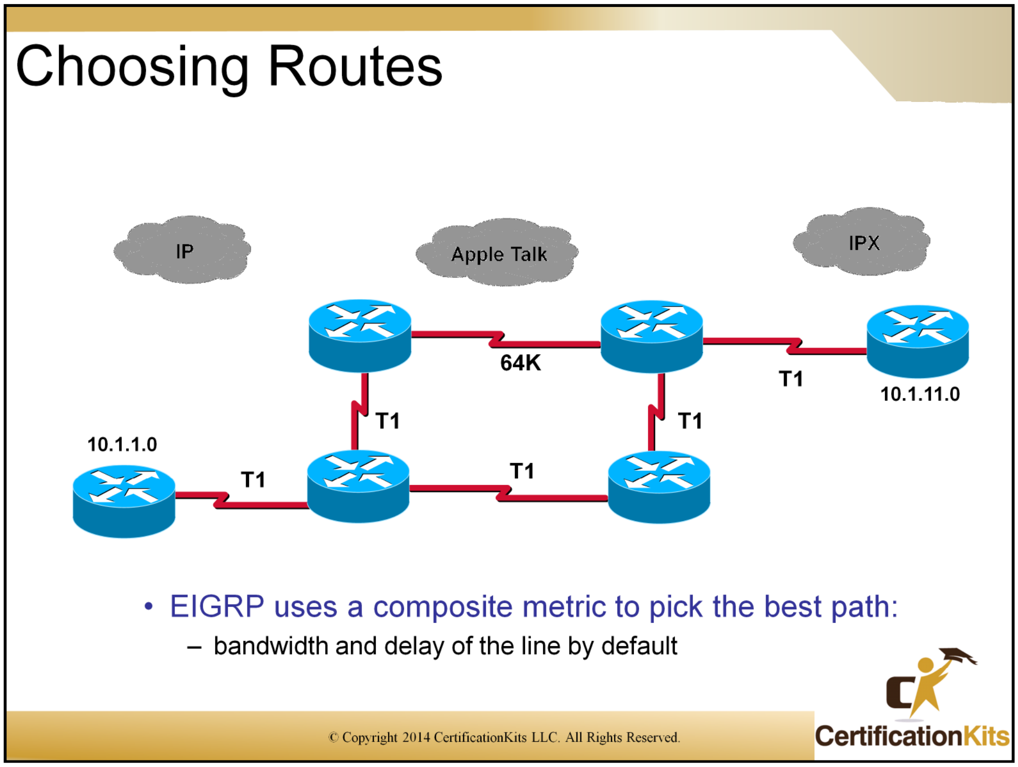
"Diffused" because routers still depend upon each other to provide "processed" information that is used as input to their own calculations

Depends upon complete reliability of communications between routers:

RTP – Reliable Transport Protocol

5 Types of Messages

Uses Multicasts to communicate 224.0.0.10



By default the EIGRP process only uses 2 'K' values, Bandwidth and Delay. If any other 'K' values are turned on for one EIGRP router, they must be turned on for all other EIGRP routers. If this is not done, then only those EIGRP routes using the same 'K' values will recognize themselves as neighbors.

Metric = [K1 x BW + (K2 x BW) / (256 - load) + K3 x delay] x [K5 / (reliability + K4)]

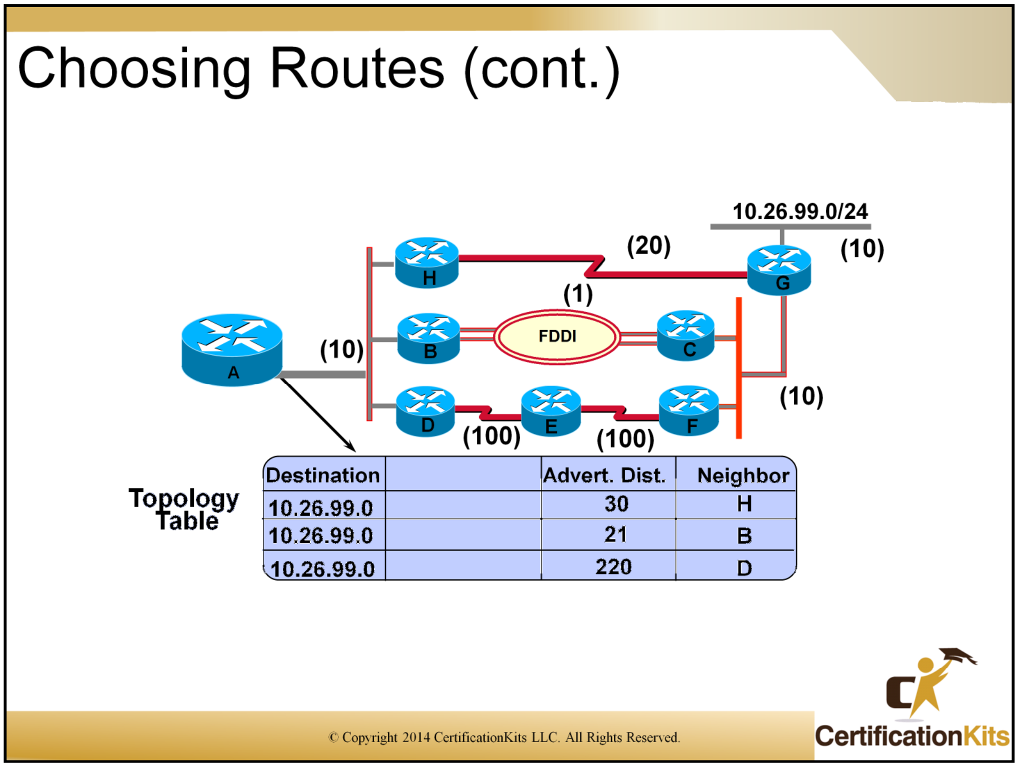
By default: K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0

Delay is sum of all the delays of the links along the paths Delay = [Delay in 10s of microseconds] x 256

BW is the lowest bandwidth of the links along the paths

BW = [10000000 / (bandwidth in Kbps)] x 256

By default, metric = lowest bandwidth in path + sum of all delays along path



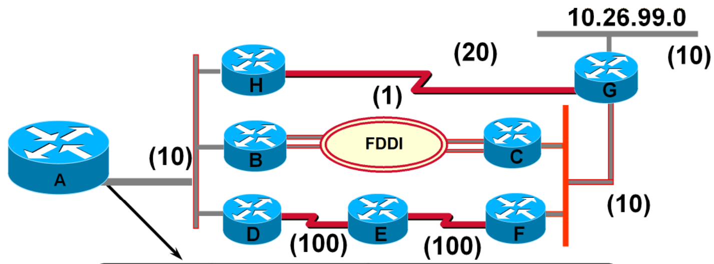
Here we are viewing a topology table. We are trying to identify the best route (successor) from RouterA to network 10.26.99.0 on Router G.

Neighbor H states that it can get to network 10.26.99.0 with an advertised distance of 30. Considering that Neighbor H can get to network 10.26.99.0 and it cost Router H 30, how much does it cost Router A to get to Router H?

It cost Router A 10 to get to Router H. So the Advertised Distances is now added to 10 which gives Router A a Feasible Distance of 40 to get to Network 10.26.99.0 via Router H.

Fill in the appropriate Feasible Distance now for the path though Router B and then for the path though Router D.

Choosing Routes (cont.)



Topology Table

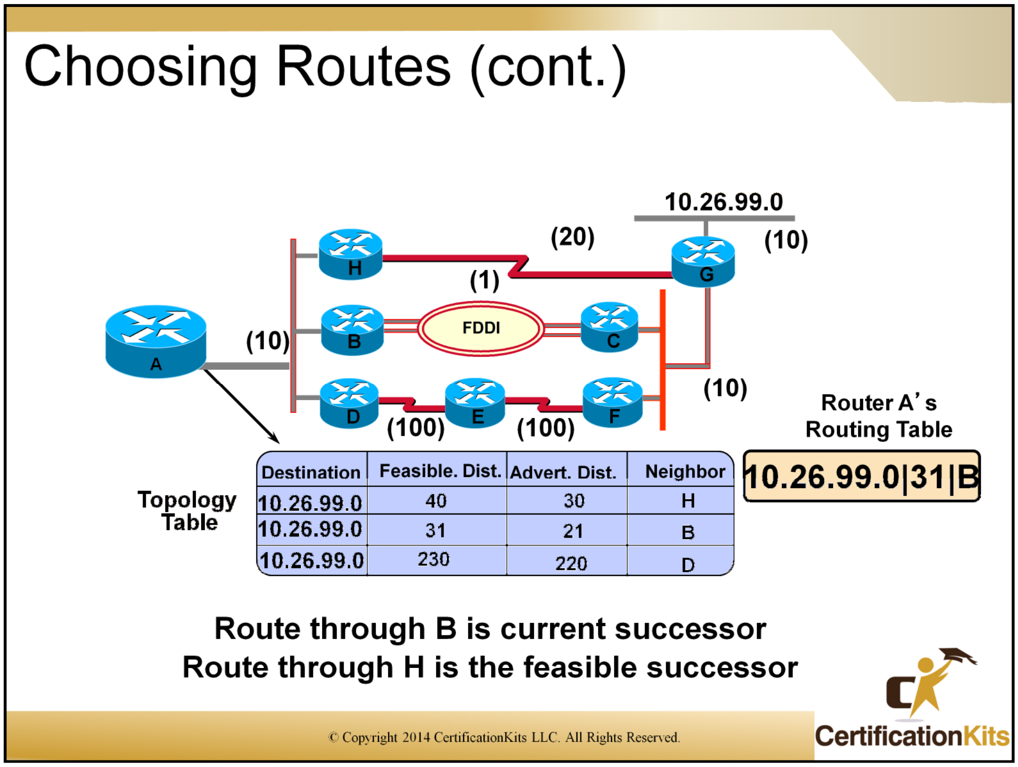
Destination	Feasible. Dist.	Advert. Dist.	Neighbor
10.26.99.0	40	30	H
10.26.99.0	31	21	B
10.26.99.0	230	220	D

Now that we have found the Feasible Distance for all of our neighbors, we can now define the Successor and see if we have a valid feasible successor available.

The Successor will be the least cost path to the remote network.

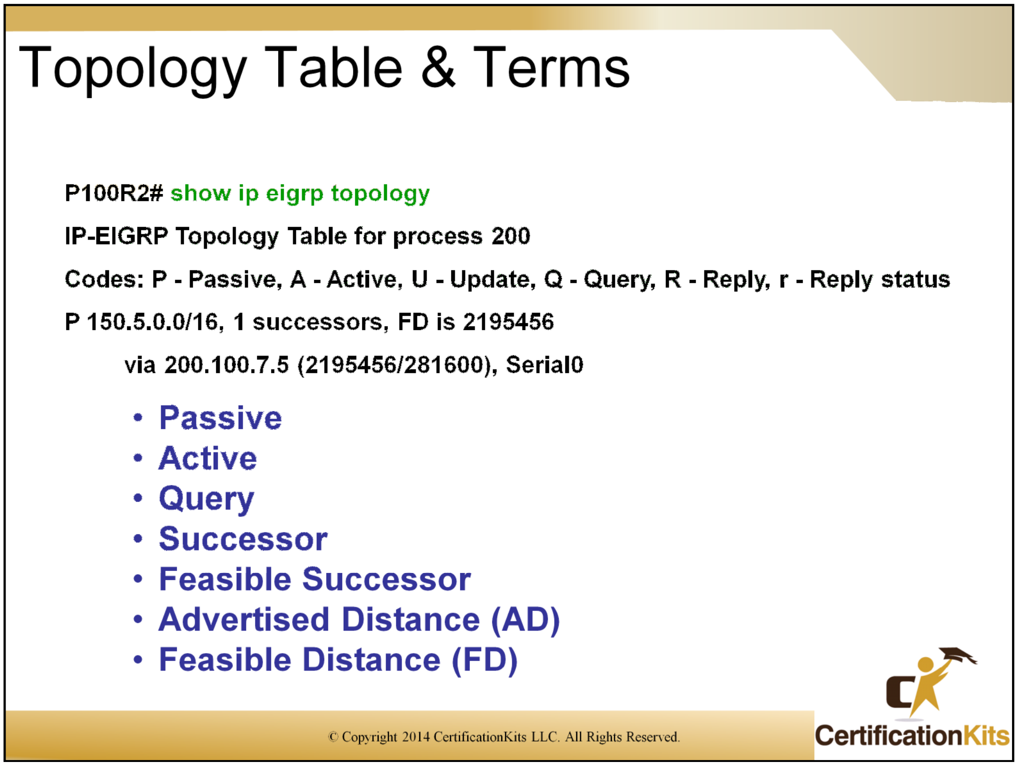
The next best route does not automatically become the feasible successor, the route has to match certain criteria.

The Feasible successor must have an advertised distance less than the current successors feasible distance.



Route through B is current successor because it has the least cost path to network 10.26.99.0.

Route through H is the feasible successor because it has an AD less than the currents Successors FD to network 10.26.99.0.



In order to view the EIGRP topology table enter the following command:

Router# show ip eigrp topology

IP-EIGRP Topology Table for process 200
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status
P 150.5.0.0/16, 1 successors, FD is 2195456
via 200.100.7.5 (2195456/281600), Serial0

Passive: A route is passive if it is up and no changes are occurring

Active: A route is active if it is down and the EIGRP process is actively trying to find a replacement

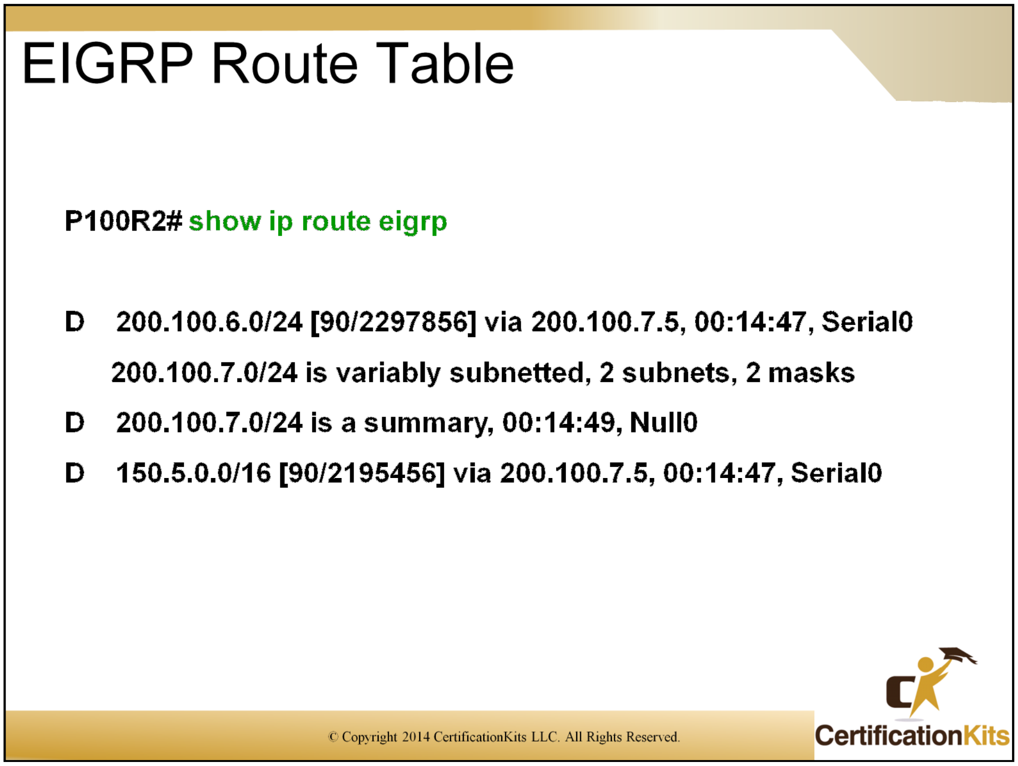
Query: A query happens with the Successor Route goes down and there is no known Feasible successor.

Successor: Primary Route (up to 6, default 4)

Feasible Successor: Backup Route (up to 6, default 4)

Advertised Distance: Distance to a remote network from the perspective of the advertising router

Feasible Distance: Distance to a remote network from my perspective which includes the cost of getting to the neighbor that provided the advertised distance

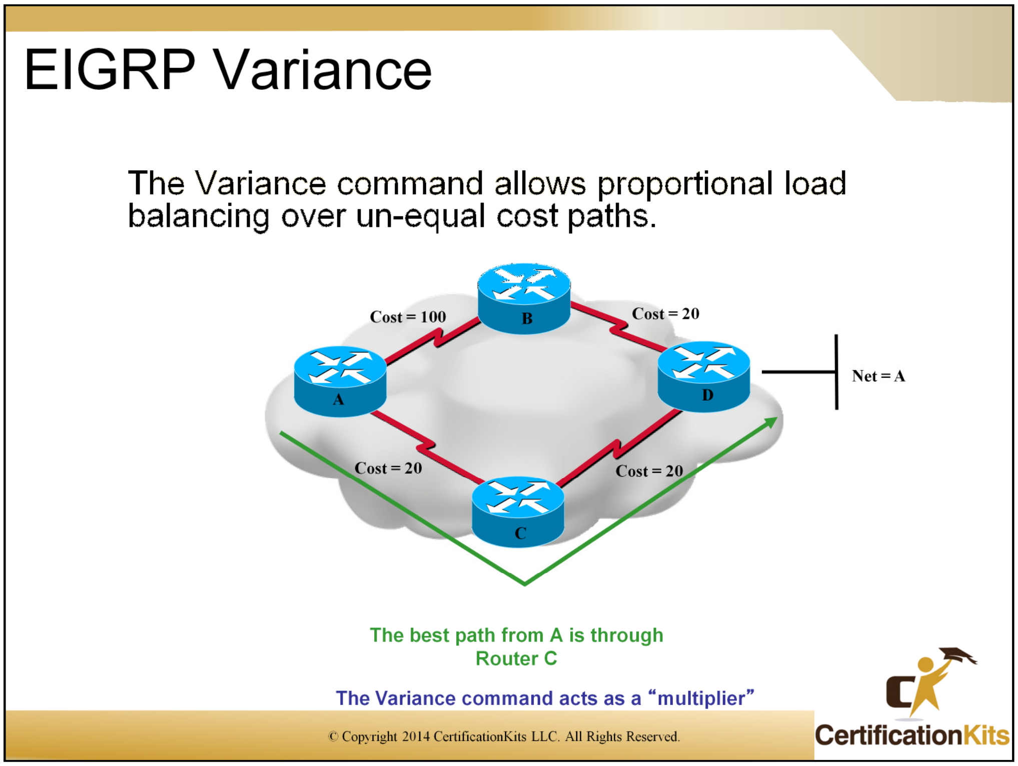


The EIGRP routing table represents the best routes found by EIGRP. These routes will be presented to the Route processor for it to decide if they should be placed in the forwarding table (the routers routing table).

Uses “D” for internal

Uses “EX” for external

Default administrative distance of 90



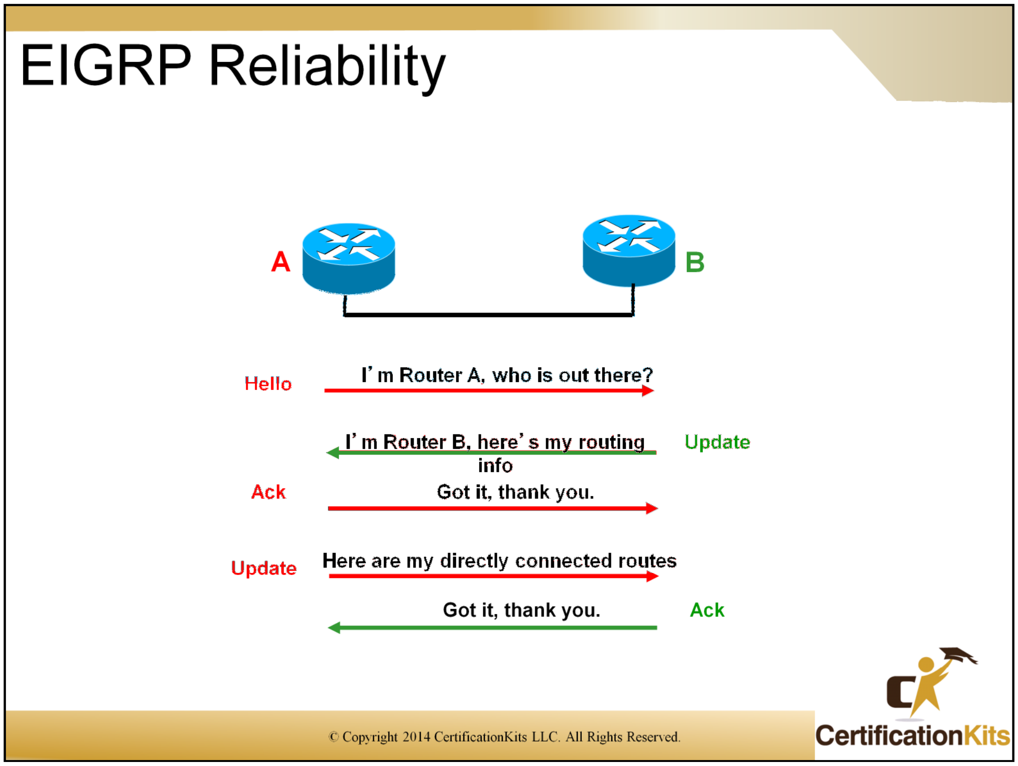
By default EIGRP can load balance over 4 equal paths to same network and can be configured to support up to 6 (maximum paths command)

The Variance command allows proportional load balancing over un-equal cost paths. The Variance command acts as a "multiplier"

The following example illustrates the syntax:

```
Router Eigrp 100
    Variance 2
```

This allows paths whose metric is 2 times greater than the best

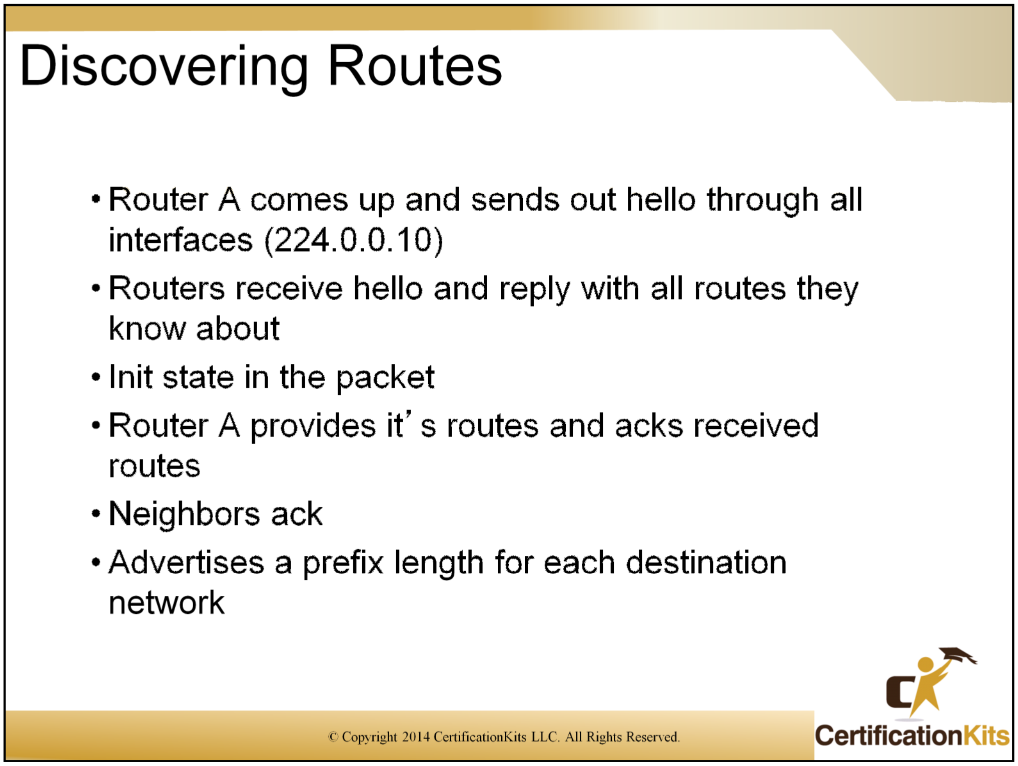


EIGRP reliable packets are packets that require explicit acknowledgement:

> **Update** - used to convey reachability of destinations. When a new neighbor is discovered, update packets are sent so the neighbor can build up its topology table. In this case, update packets are unicast. In other cases, such as a link cost change, updates are multicast. Updates are always transmitted reliably.
>
> **Query** - always multicast unless they are sent in response to a received query. In this case, it is unicast back to the successor that originated the query. Queries are transmitted reliably.
>
> **Reply** - always sent in response to queries to indicate to the originator that it does not need to go into Active state because it has feasible successors. Replies are unicast to the originator of the query. Replies are transmitted reliably.

EIGRP unreliable packets are packets that do not require explicit acknowledgement:

> **Hello** - multicast for neighbor discovery/recovery (sent every 5 [**LAN**] or 60 [**WAN**] seconds)
>
> **ACK** - always sent using a unicast address and contain a non-zero acknowledgment number.



The following documents the steps that are taken in order build EIGRP Routes:

1. Router A comes up and sends out hello through all interfaces (224.0.0.10)

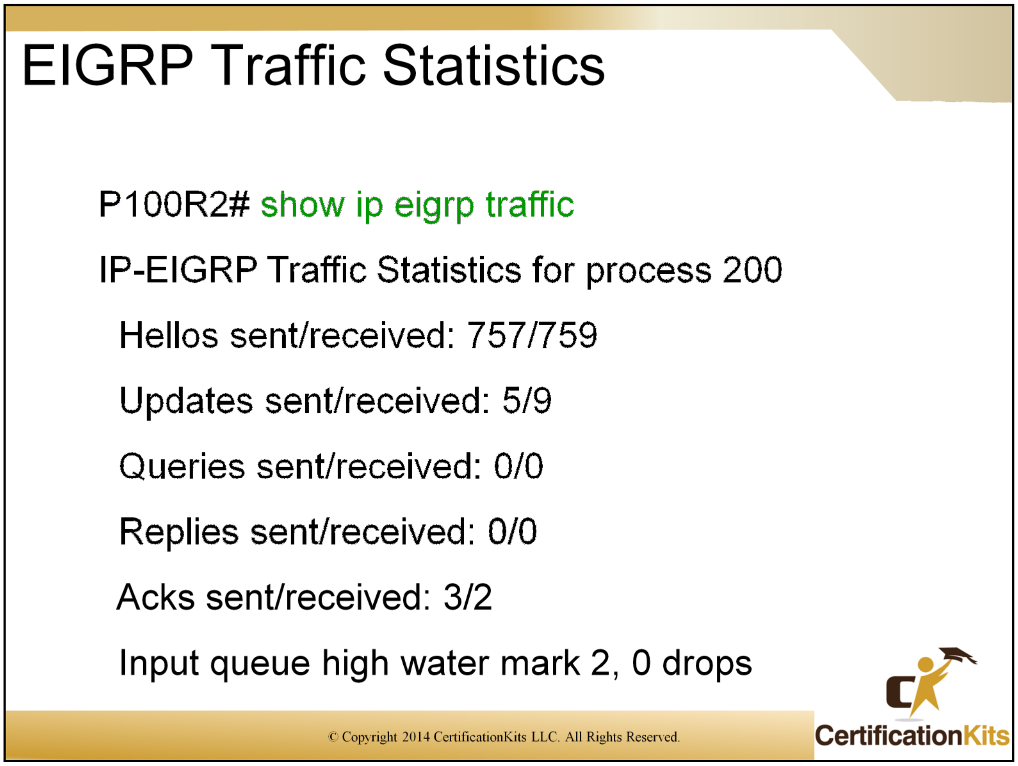
2. Routers receive hello and reply with all routes they know about

3. Init state in the packet

4. Router A provides it’s routes and acks received routes

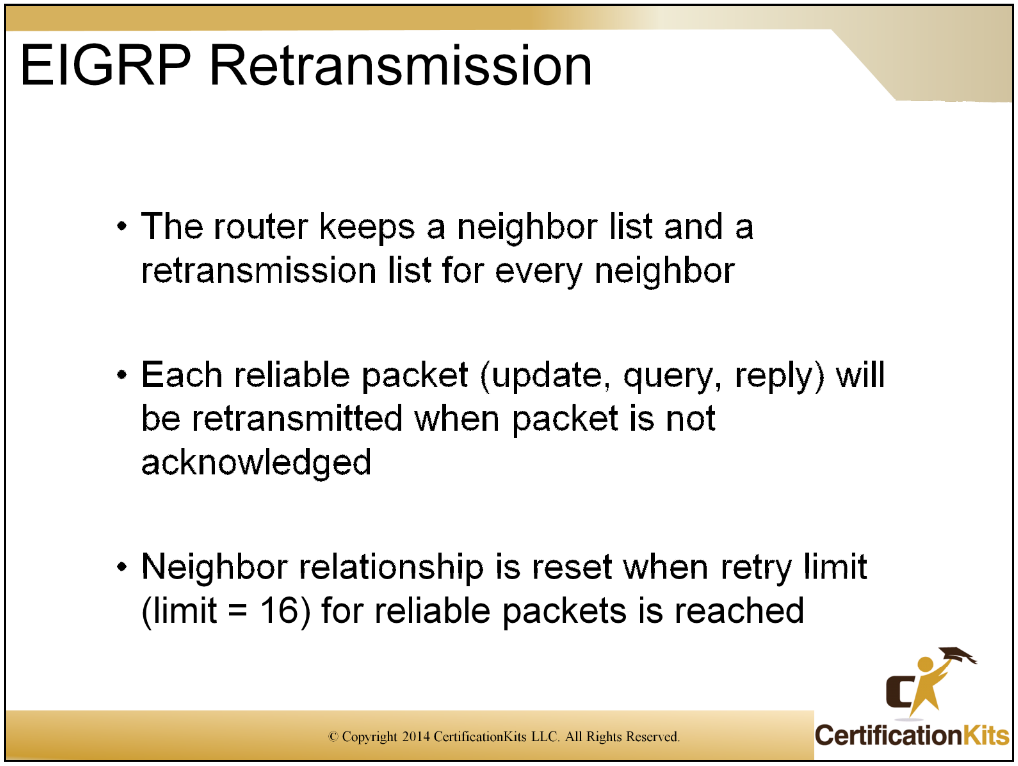
5. Neighbors ack

6. Advertises a prefix length for each destination network



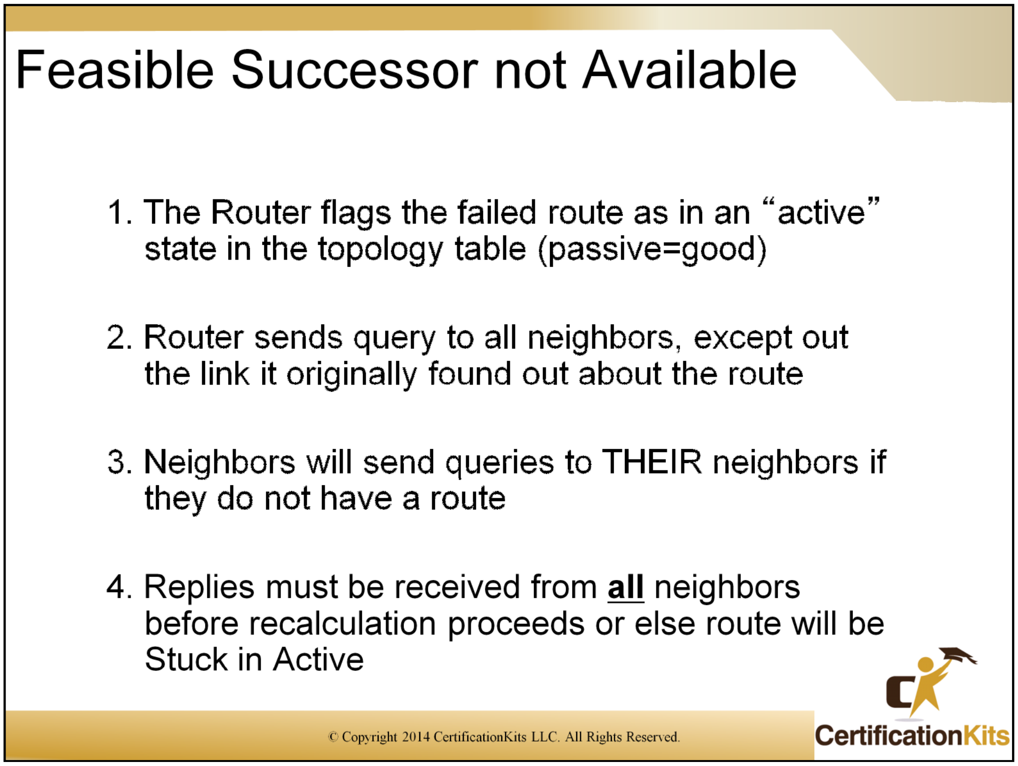
To find out EIGRP traffic statistics, such as how may hellos/updates/queries/replies and acknowledgements have been sent and received, you should issue the following IOS command:

Router# show ip eigrp traffic



EIGRP transport has window size of one (stop and wait mechanism). Every single reliable packet needs to be acknowledged before the next sequenced packet can be sent. If one or more peers are slow in acknowledging, all other peers suffer from this.

Solution: The non-acknowledged multicast packet will be retransmitted as a unicast to the slow neighbor



If your successor is lost, and your DUAL was unable to find a feasible successor a query is sent out to all of the EIGRP neighbors. Each neighbor should respond to the query, if there is no response to the query, the route will become stuck in active. If all neighbors do respond, EIGRP evaluates their responses and calculates the most appropriate route to become the Successor.

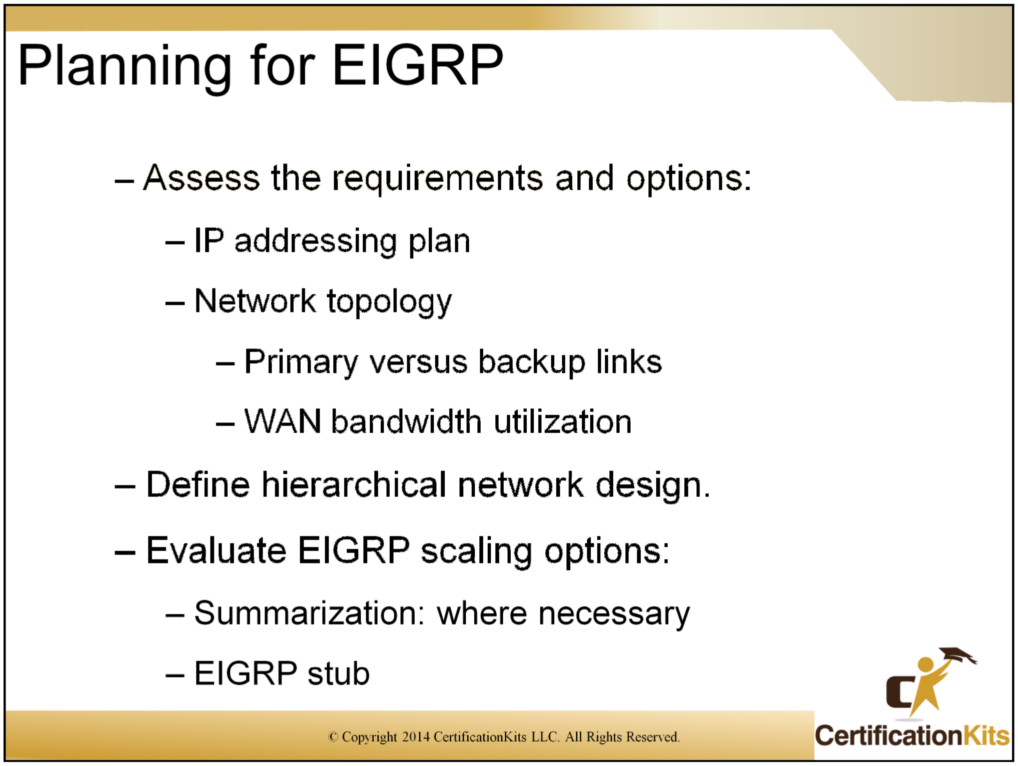
In some circumstances, it takes a very long time for a query to be answered. So long, in fact, that the router that issued the query gives up and clears its connection to the router that isn't answering, effectively restarting the neighbor session.

The most basic SIA routes occur when it simply takes too long for a query to reach the other end of the network and for a reply to travel back. One of the most effective techniques for containing EIGRP queries is to use route summarization or stub networks.

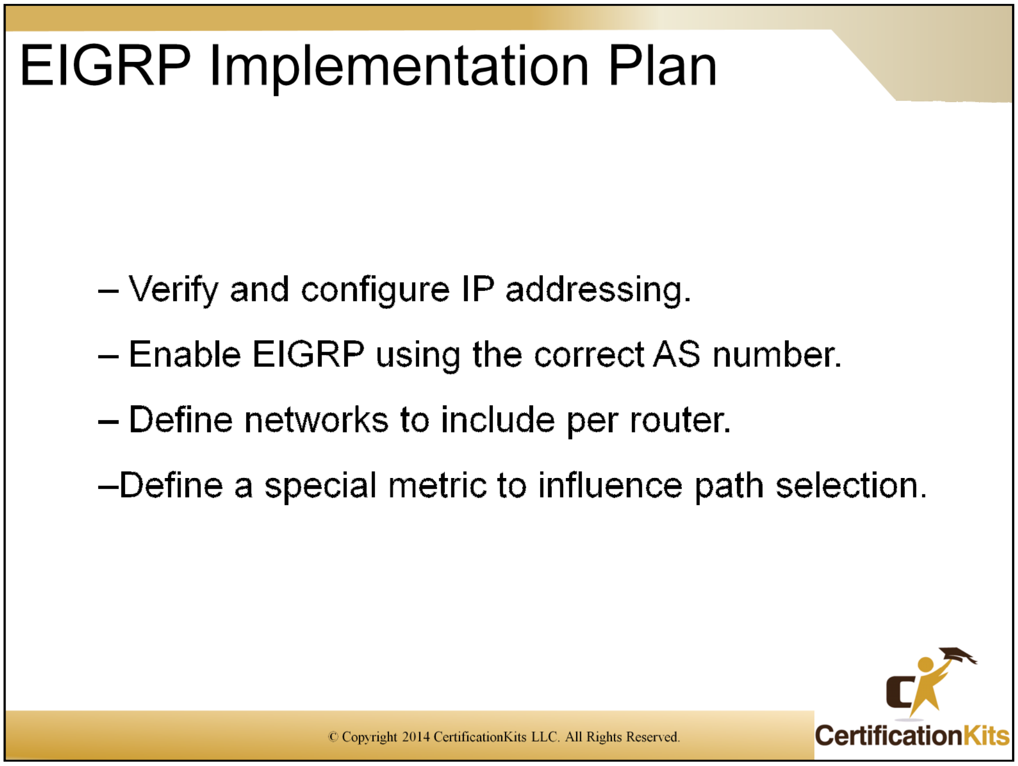
Stub networks are configured in a hub and spoke network and is configured only on the stub router. The command is

```
router eigrp 100
   eigrp stub
```

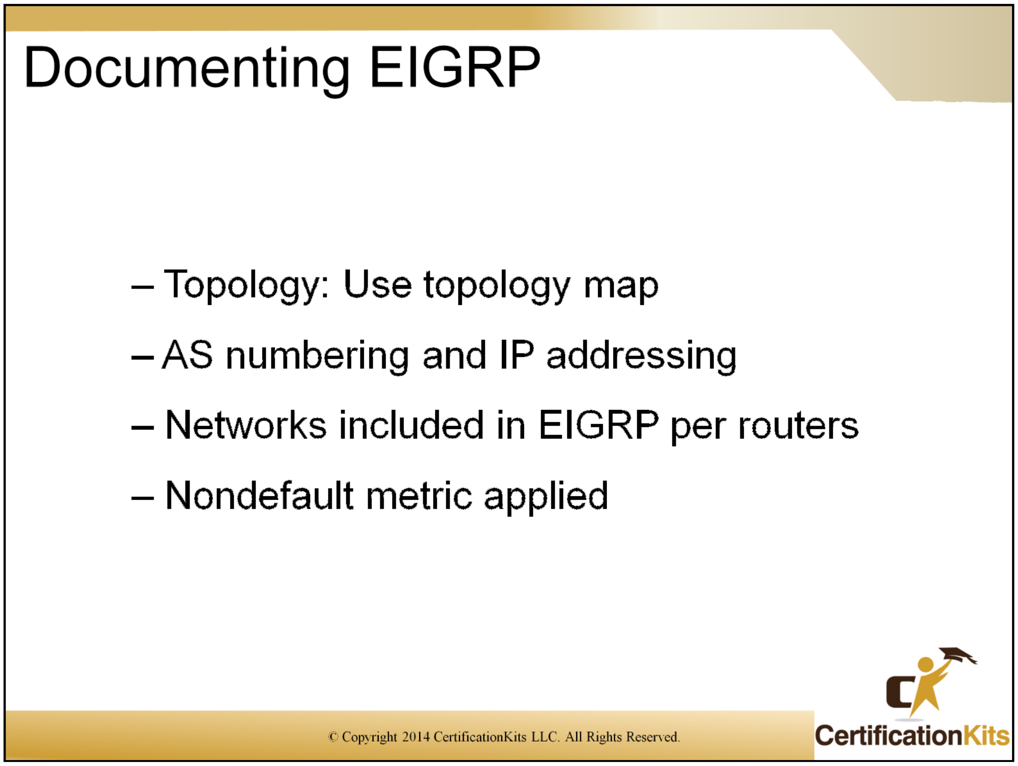
The result of this configuration is that the stub routers will send updates about routes they have to the hub router but the hub router will never query the stub router for updates in the event of a route being lost.



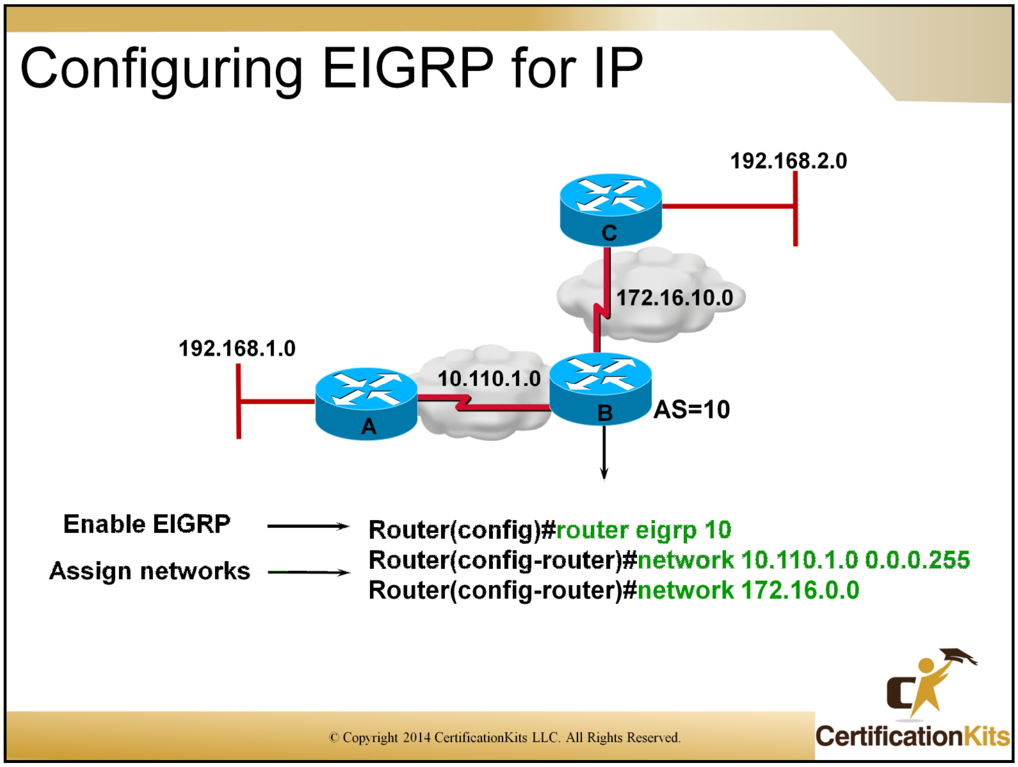
When implementing EIGRP (as well as other routing protocols) coming up with an IP Address plan that maps to a network topology is key. The IP Address plan should be implemented with IP Address summarization in mind which if implemented properly can decrease routing table sizes on routers while increasing efficiency.



When implementing remember that unlike OSPF which uses a Process ID for the routing instance which can be different on each router, EIGRP uses an Autonomous System number which MUST be the same on all routers that will be exchanging routes via EIGRP. Networks must be defined under the respective EIGRP instance. Special configuration can be utilized to influence path selection.



The implementation of EIGRP should be documented which will be key in troubleshooting. Make sure to keep the documentation current by updating it when changes are made to the network.



The only funky thing that you have to do is configure the Autonomous Systems that EIGRP will operate in. An autonomous system is simply a group of networks within the same administrative domain.

In order to configure EIGRP in the above diagram you would follow these steps for the appropriate routers:

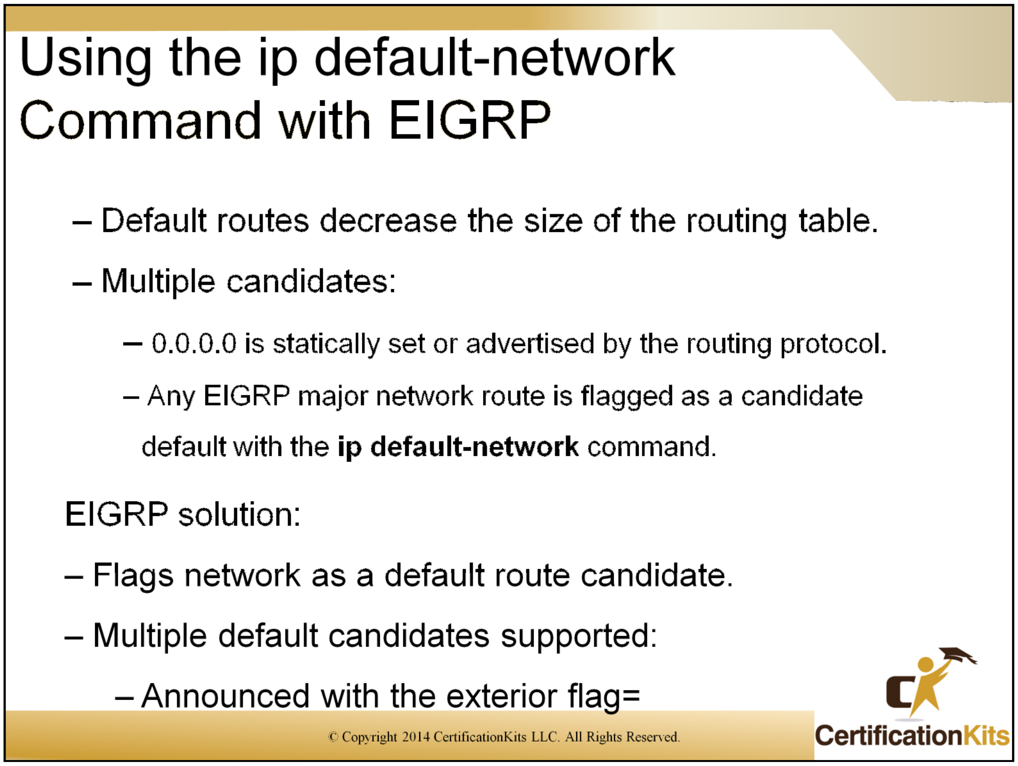
RouterA(config)#router eigrp 10
RouterA(config-router)#network 10.0.0.0
RouterA(config-router)#network 192.168.1.0

RouterB(config)#router eigrp 10
RouterB(config-router)#network 10.0.0.0
RouterB(config-router)#network 172.16.0.0

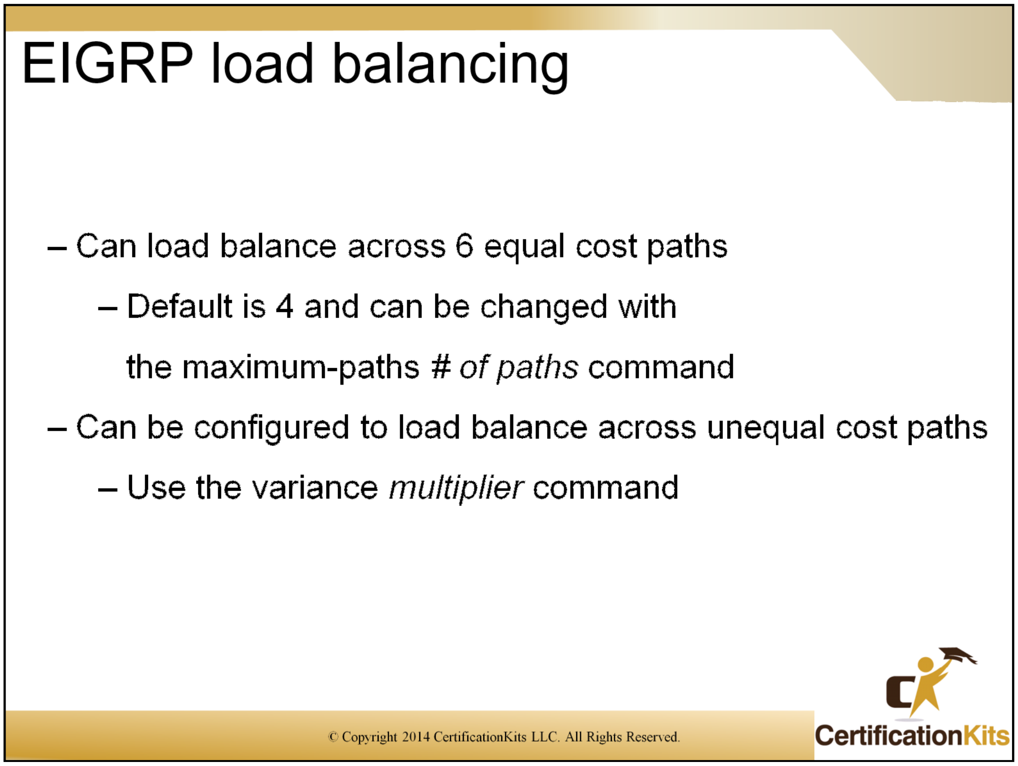
RouterC(config)#router eigrp 10
RouterC(config-router)#network 192.168.2.0
RouterC(config-router)#network 172.16.0.0

Just as we discussed earlier that each router must have the same 'K' values enabled in order to become neighbors, they must also belong to the same Autonomous System in order for them to recognize each other as neighbors.

If EIGRP routers do not share the same Autonomous System, then in order for them to share routing information, they must redistribute their routes to each other.



Default routes are defined with the **ip default-network** command when using EIGRP.

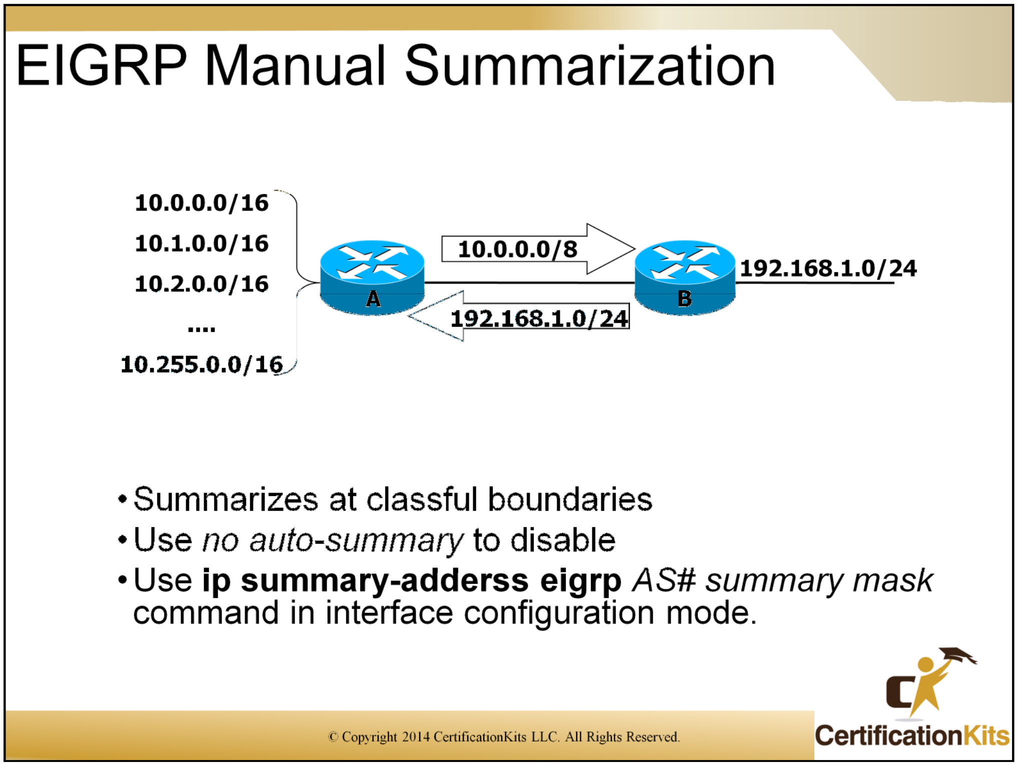


Equal-metric load balancing is the capability of a router to distribute traffic over all its network ports that have the same metric to the destination address. Load balancing increases the use of network segments and increases the effective network bandwidth.

For IP, Cisco IOS Software applies load balancing between a maximum of four equal-metric paths by default. You can configure the maximum number of parallel routes that an IP routing protocol can support using the **maximum-paths** router configuration command. Up to six equally good routes can be kept in the routing table.

Note: Setting the **maximum-paths** value to 1 disables load balancing.

When a packet is process-switched, load balancing over equal-metric paths occurs on a per-packet basis. When packets are fast-switched, load balancing over equal-metric paths occurs on a per-destination basis. (Therefore, if you are testing load balancing, do not ping to or from routers with fast-switching interfaces, because the packets that are generated locally by this router are process-switched rather than fast-switched, and the ping might produce confusing results.)



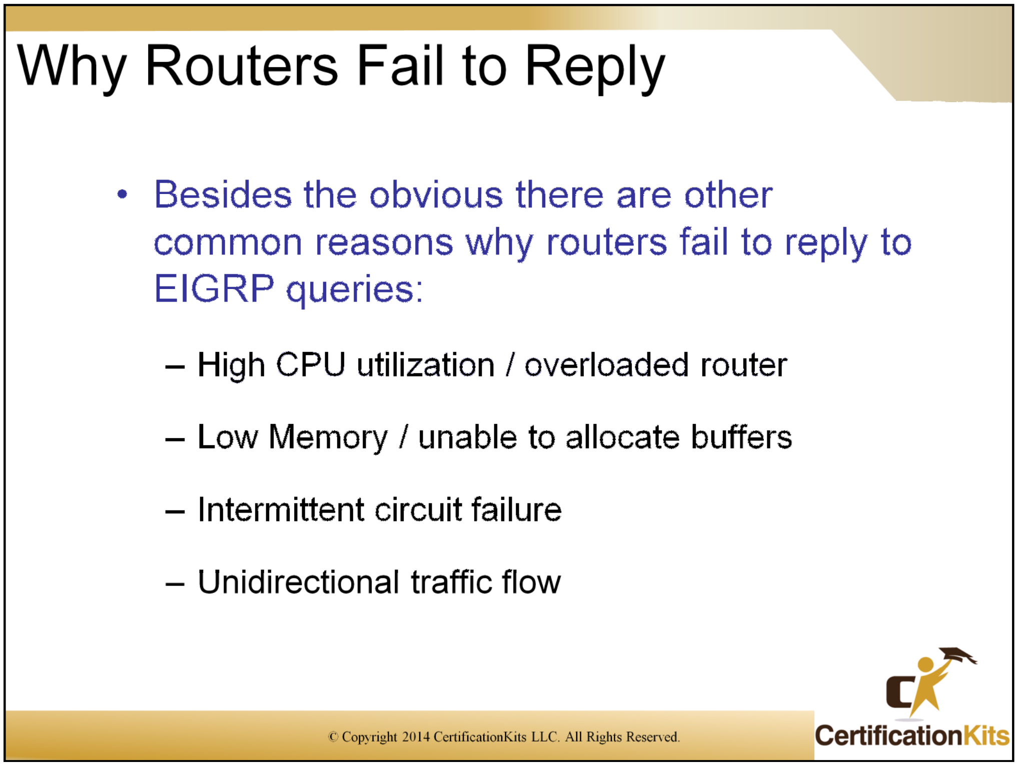
- Summarizes at classful boundaries

- To summarize at any subnet or supernet:

  (config-if)# **ip summary-address eigrp *as net mask***

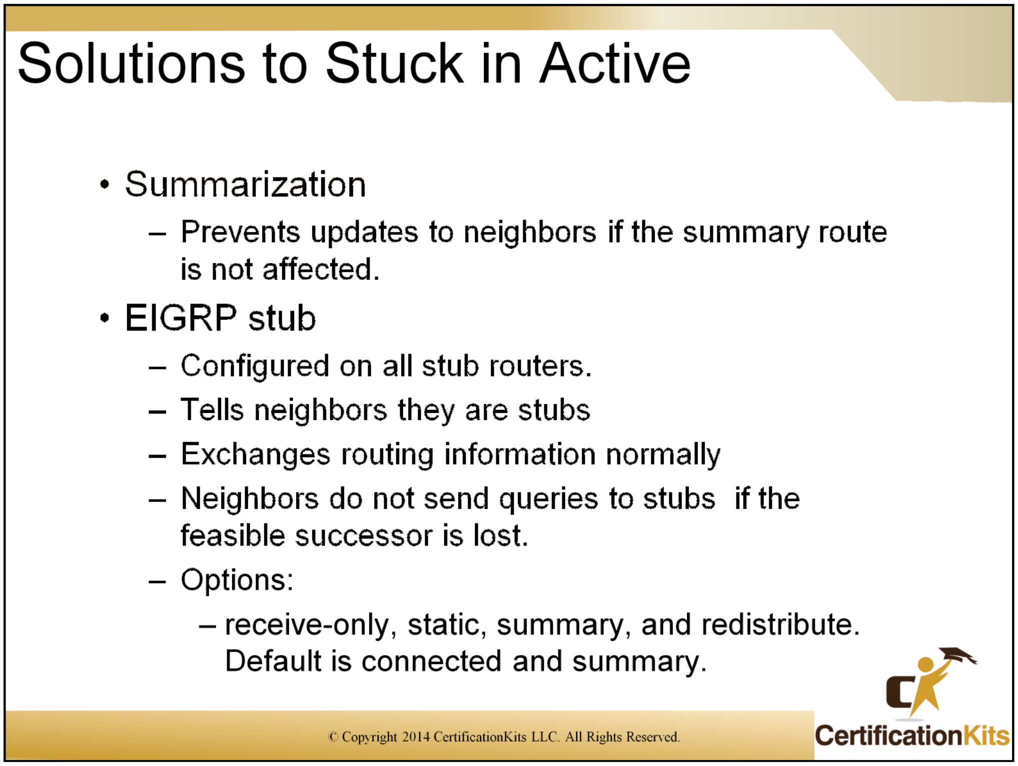
- Inserts a null0 interface entry

- Typically no auto-summary is also configured – if not then the detailed routes may still appear along with your summary route.



Summarization can also be used to limit the scope of a query for a route that is in the "active" state. If a neighbor fails to reply to query within 3 minutes the route if flagged Stuck in Active and the router resets the neighbor relationship. In some cases, routers that have no way of helping answer a query can cause the route to become SIA – we want to reduce this occurrence.

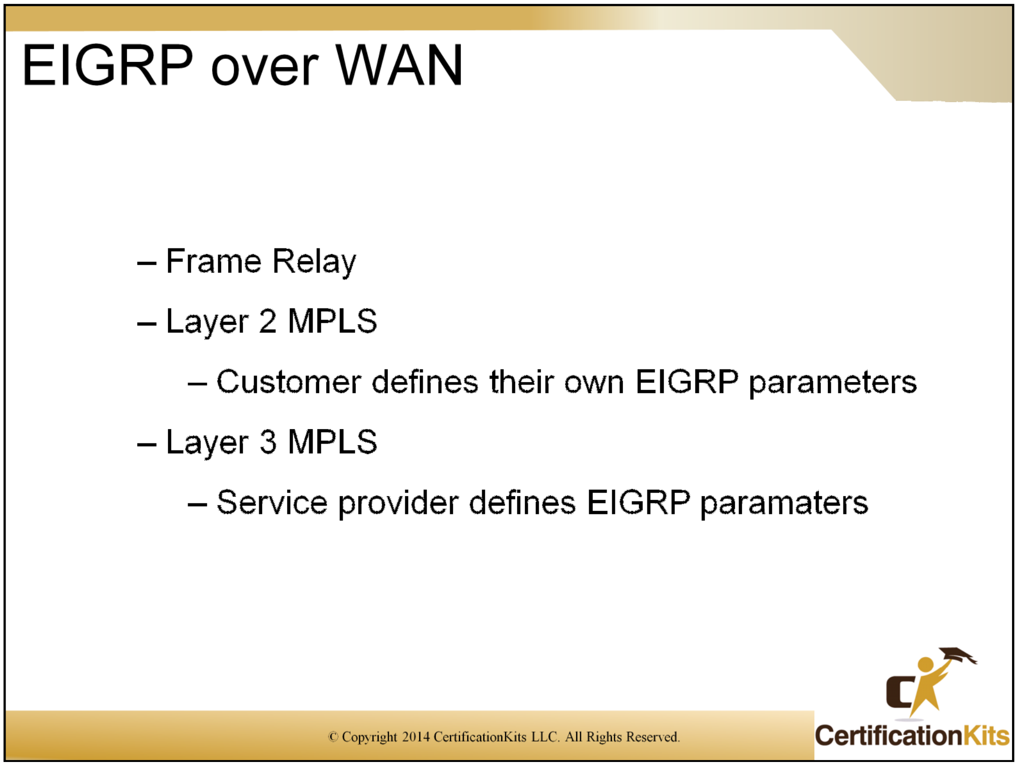
- High CPU utilization / overloaded router
- Low Memory / unable to allocate buffers
- Intermittent circuit failure
- Unidirectional traffic flow



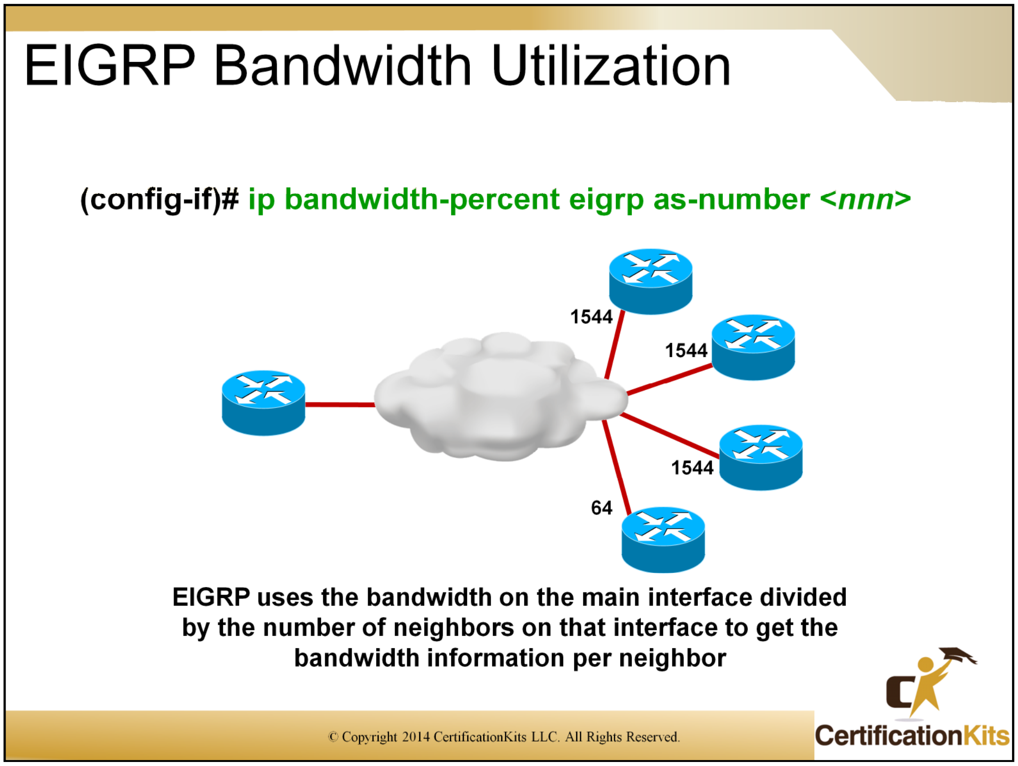
The only additional command that is needed is the eigrp stub command in the stub router configuration.

Router(config)# **router eigrp 200**

Router(router-config)# **eigrp stub**



While BGP is typically used in the WAN, EIGRP works well in small environments.



Specifies what percentage of bandwidth EIGRP packets will be able to utilize on this interface

By default, EIGRP uses up to 50% of the link bandwidth. This parameter uses the value specified by the interface's bandwidth command – usually equal to the CIR. If bandwidth is set artificially low you may need to set this parameter greater than 100. This is used for greater EIGRP load control.

Each PVC might have a different CIR, this might create an EIGRP packet pacing problem. EIGRP uses the bandwidth on the main interface divided by the number of neighbors on that interface to get the bandwidth information per neighbor.

Solution for Multipoint interfaces:

Convert to point-to-point configuration

or

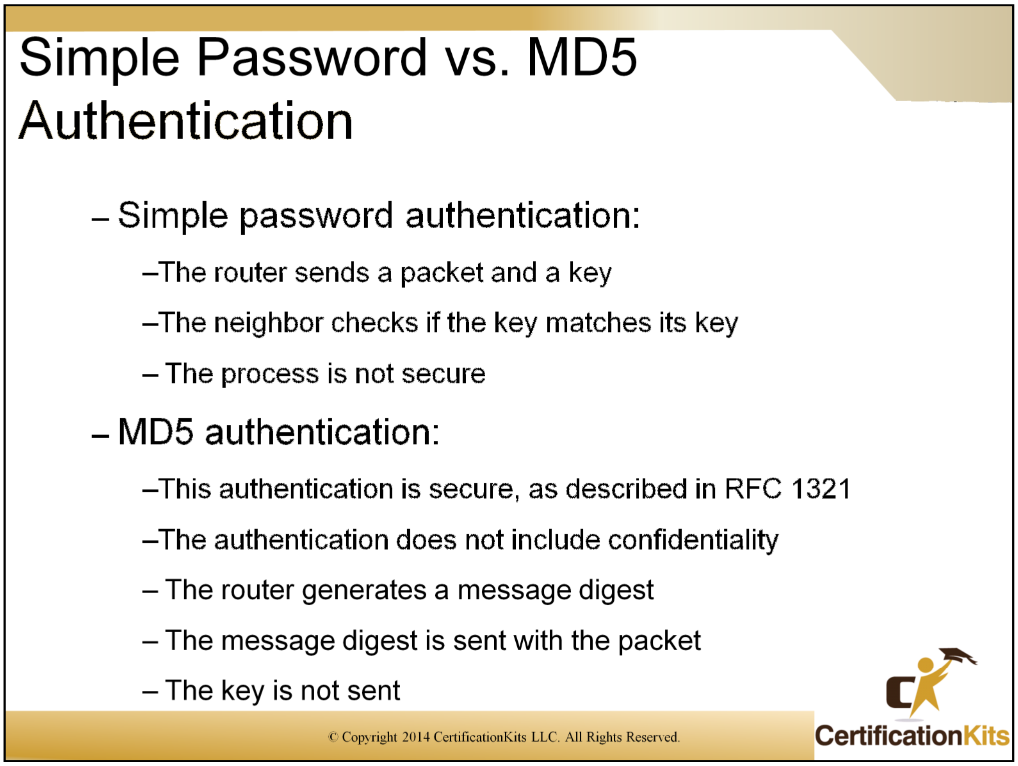
Manually configure bandwidth = (lowest CIR x number of PVCs) [bw=320 for above example]

Router Authentication

- Implement security to the routing protocol by supporting authentication.
- A router authenticates the source of each routing update packet that it receives.
- Prevent false routing updates from updating the routing table:
  - Prevent deliberate false routing updates sourced by unapproved sources.
  - Ignore malicious updates, preventing them from disrupting the routing or taking down the adjacency
- Two types of authentication are available:
  - Simple Password
    - OSPF and RIPv2
  - MD5
    - EIGRP, OSPF, RIPv2, and BGP

CertificationKits

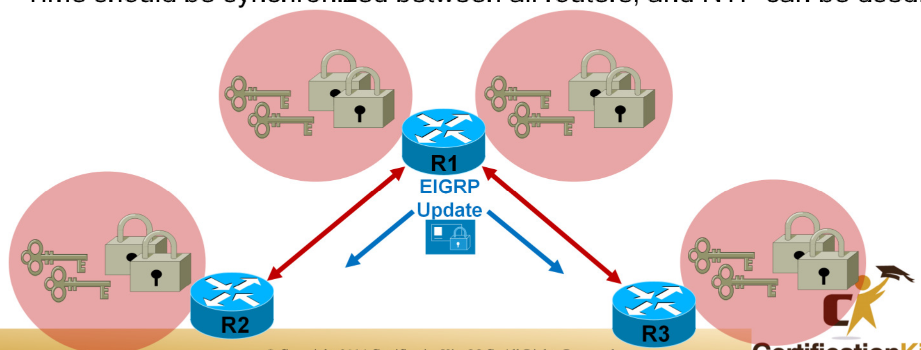
Router authentication can be used to validate the source of the routing update prior to adding the information to the routing table. This can prevent attacks that attempt to inject false, potentially malicious routing updates.



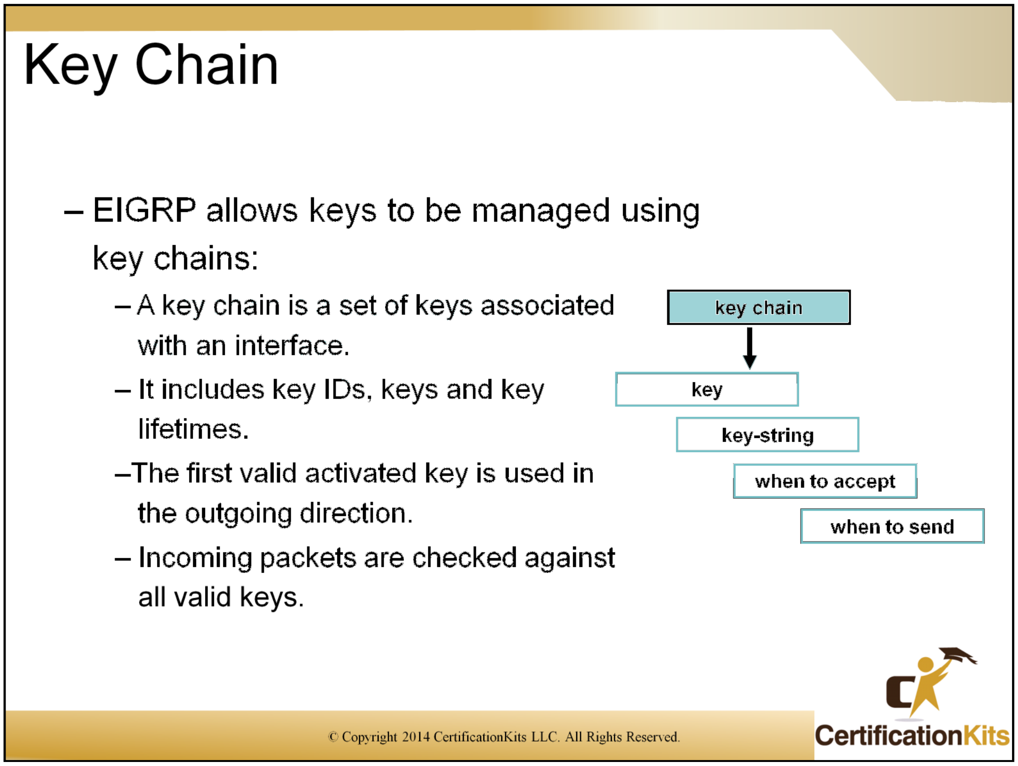
There are two types of authentication that Cisco routers support: Simple password and MD5 authentication. The type support is dependant on the routing protocol. MD5 is more secure than simple password.

MD5 Authentication for EIGRP

- EIGRP supports MD5 authentication.
- The router generates MD5:
  - Multiple keys can be configured in all EIGRP routers.
- The receiving router computes the MD5 hash from the received EIGRP information.
- Time should be synchronized between all routers, and NTP can be used.

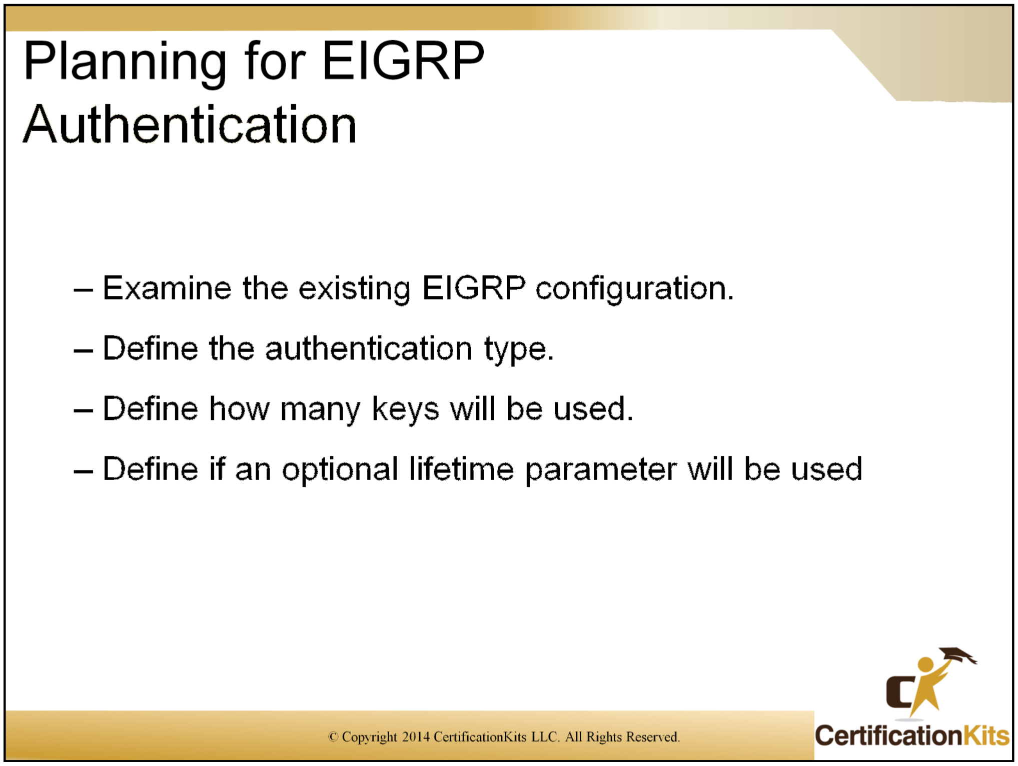


MD5 authentication is supported within EIGRP. As mentioned earlier, it is a good practice to enable MD5 authentication when utilizing EIGRP as a security precaution to thwart off potentially malicious routes from being injected.



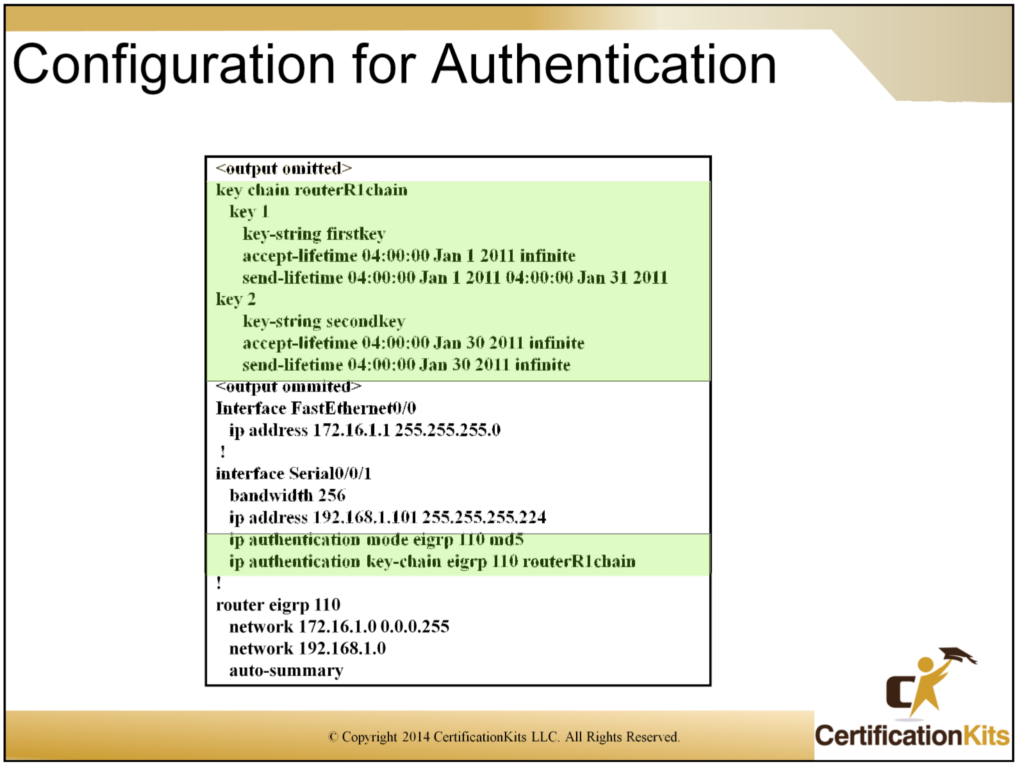
Key chains are used when configuring authentication. Each key within a key chain can specify a "lifetime" which is the time duration the key will be active. IOS examines keys in order from lowest to highest and utilizes the first valid key it finds.

Since keys cannot be utilized when they are not within a valid time, it is critical that for a given key chain, activation times within keys should overlap. Another critical point when implementing is to ensure the router has the correct time synchronize to an external source.

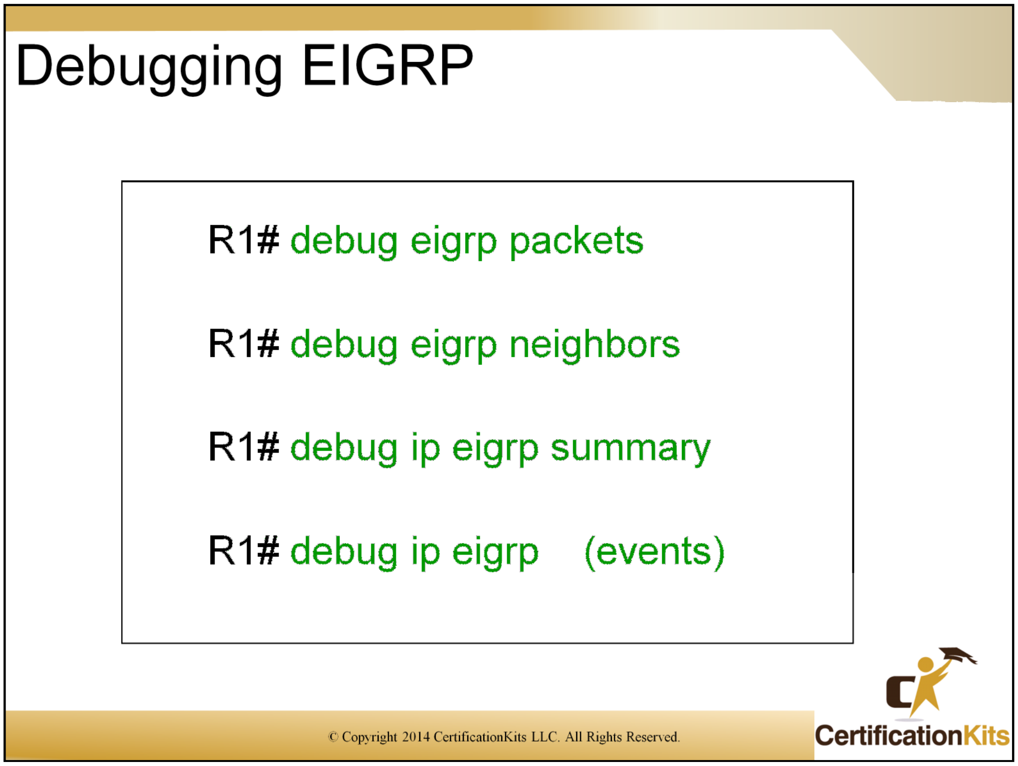


Network requirements must be determined prior to configuring EIGRP authentication. This includes things such as EIGRP autonomous system (AS), EIGRP participating interfaces and participating routers.

Gather all the information and start configuring EIGRP for authentication then verify everything is working properly.



Above is an example of configuring EIGRP to used MD5 authentication. Notice that key chain is configured in global configuration mode while the applying of the authentication is performed under the specific interface, not under **router eigrp**.

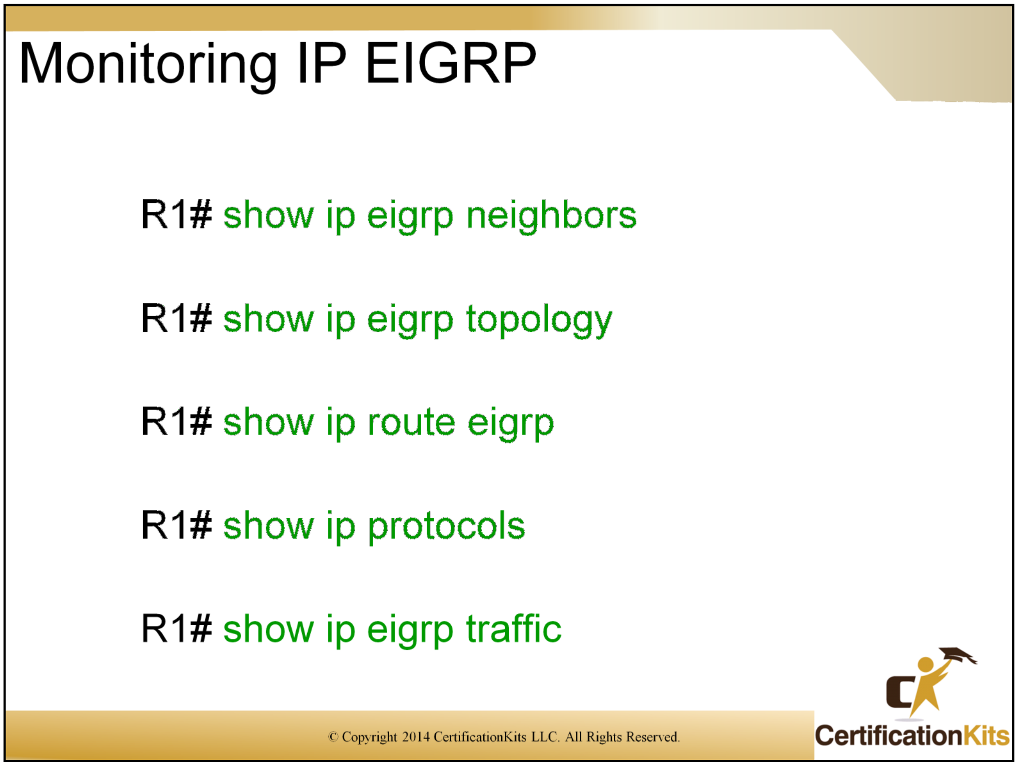


debug eigrp packets - View eigrp packet transmissions

debug eigrp neighbors - View eigrp building and maintaining Neighbor tables

debug ip eigrp summary - View summarized eigrp traffic

debug ip eigrp (events) - View all eigrp events



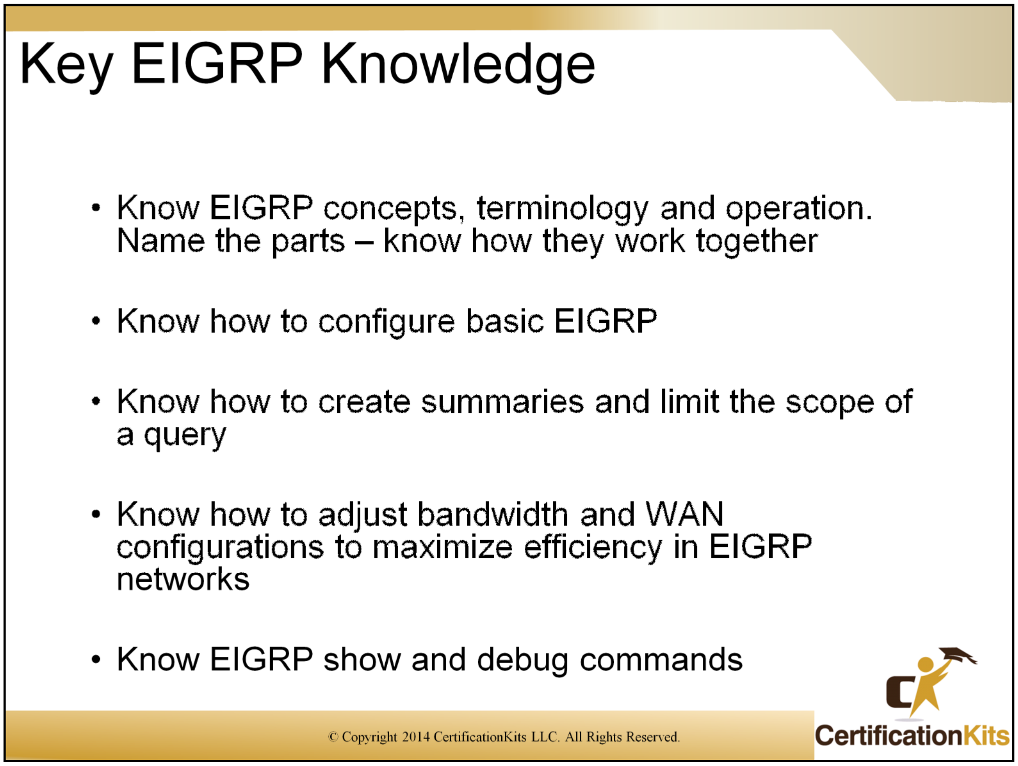
show ip eigrp neighbors – Shows the neighbor table

show ip eigrp topology – Shows the topology table

show ip route eigrp – Shows routes from EIGRP

show ip protocols – Show ip routing protocols configured, the interaction between them as well info about redistribution

show ip eigrp traffic – Shows statistics in reference to hello, updates, queries, replies, and acknowledgements



The above slide list key concepts that should be known when learning about EIGRP.