Chapter 8
Advanced Routing Protocols
Classful and Classless Routing Protocols

• **Classful routing protocols**
  – Summarize networks to their major network boundaries (Class A, B, or C)
  – Do not carry subnet mask information in their routing table updates
  – Cannot be used in networks with either discontiguous subnets or networks using variable length subnet masks (VLSM)
  – Examples: RIPv1 and IGRP
Classful and Classless Routing Protocols (continued)

<table>
<thead>
<tr>
<th>Command (1)</th>
<th>Version (1)</th>
<th>must be zero (2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Family Identifier (2)</td>
<td>must be zero (2)</td>
<td></td>
</tr>
<tr>
<td>IP Address (4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>must be zero (4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>must be zero (4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metric (4)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 8-1** RIPv1 message format
Figure 8-2  Network with discontiguous subnets
Figure 6-3  Configuring RIPv1 on RouterA
Classful and Classless Routing Protocols (continued)

After configuration of RouterC with RIPv1, RouterB erroneously believes it has two equal cost routes to the 192.168.12.0 network.

```
RouterB#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R  192.168.12.0/24 [120/1] via 172.16.0.2, 00:00:01, Serial0/0
   [120/1] via 10.0.0.2, 00:00:09, Serial0/1
C  172.16.0.0/16 is directly connected, Serial0/0
C  10.0.0.0/8 is directly connected, Serial0/1

RouterB#
```

Figure 8-5  Router B’s routing table—full network configuration
Classful and Classless Routing Protocols (continued)

A long repeat count was used to show the effects of the dual routes.

Only 50% of the pings reach RouterA's F0/0 interface. The other half are incorrectly routed to RouterC.

```
RouterB#ping
Protocol [ip]:
Target IP address: 192.168.12.33
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.12.33, timeout is 2 seconds:
!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..!U!..
Success rate is 50 percent (50/100), round-trip min/avg/max = 28/28/28 ms
```

Figure 8-6  Ping example
Classful and Classless Routing Protocols (continued)

- **Classless routing protocols**
  - Allow dynamic routing in discontiguous networks
  - Carry subnet mask information in the routing table updates
  - Examples: RIPv2, EIGRP, OSPF, and BGP
Classful and Classless Routing Protocols (continued)

<table>
<thead>
<tr>
<th>Address Family Identifier (2)</th>
<th>Route Tag (2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address (4)</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask (4)</td>
<td></td>
</tr>
<tr>
<td>Next Hop (4)</td>
<td></td>
</tr>
<tr>
<td>Metric (4)</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 8-7** RIPv2 update message format

Inclusion of the Subnet Mask field allows RIPv2 to carry subnet mask information.
Classful and Classless Routing Protocols (continued)

This command converts RIP to version 2.

Although RIPv2 can carry subnet mask information, by default it summarizes along major network boundaries. The no auto-summary command configures the router to use the subnet mask information in the update messages to configure its routing table.

```
RouterB(config)#router rip
RouterB(config-router)#version 2
RouterB(config-router)#no auto-summary
```

Figure 8-8  Configuring RIPv2
Classful and Classless Routing Protocols (continued)

RouterB#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, O - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.12.0/27 is subnetted, 2 subnets
R    192.168.12.64 [120/1] via 10.0.0.2, 00:00:09, Serial0/1
R    192.168.12.32 [120/1] via 172.16.0.2, 00:00:07, Serial0/0
C    172.16.0.0/16 is directly connected, Serial0/0
C    10.0.0.0/8 is directly connected, Serial0/1
RouterB#

Figure 8-9  RouterB’s routing table with RIPv2
Classful and Classless Routing Protocols (continued)

Once the routing table has the correct entries, all pings are successfully sent.

```
RouterB#ping
Protocol [ip]:
Target IP address: 192.168.12.33
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.12.33, timeout is 2 seconds:
0% packet loss
Success rate is 100 percent (100/100), round-trip min/avg/max = 28/28/40 ms
RouterB#
```

Figure 8-10  Extended Ping attempt with RIPv2
Routing Information Protocol version 2

- RIPv2 is a set of extensions to RIPv1
  - Still a distance-vector routing protocol that uses the normal measures of hold-down timers and split horizon to prevent routing loops
  - Suffers from RIPv1’s major drawback

- The major change from RIPv1 is RIPv2’s ability to carry subnet mask information
  - RIPv2 multicasts its updates using the multicast address of 224.0.0.9

- RIPv2 provides a way to authenticate routing peers to provide enhanced security to a network
Figure 8-11  RIPv2 example network
Routing Information Protocol version 2 (continued)

```
RouterA(config)#router rip
RouterA(config-router)#version 2
RouterA(config-router)#no auto-summary
RouterA(config-router)#network 172.16.0.0
RouterA(config-router)#network 192.168.12.0
```

Figure 8-12  RIPv2 configuration commands

Specifies RIPv2 as the routing process.
RouterA#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 4 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface      Send Recv Triggered RIP Key-chain
    FastEthernet0/0  2   2
    Serial0/0        2   2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.12.0

Routing Information Sources:
  Gateway      Distance   Last Update
  172.16.0.1    120 00:00:06
  Distance: (default is 120)

Figure 8-13  Show IP protocols output with RIPv2
Routing Information Protocol version 2 (continued)

```plaintext
RouterB#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#router rip
RouterB(config-router)#version 2
RouterB(config-router)#no auto-summary
RouterB(config-router)#network 10.0.0.0
RouterB(config-router)#network 172.16.0.0
RouterB(config-router)#int s0/1
RouterB(config-if)#ip rip send version 1
RouterB(config-if)#ip rip receive version 1
RouterB(config-if)#^Z
RouterB#
```

By changing s0/1 the interface connected to the RIPv1 peer RouterC, to send and receive version 1 updates, all three routers can now share routing information.

**Figure 8-14** RouterB configuration for RIPv1 and RIPv2 support
If RouterB had not been configured to receive version 1 updates, this output would appear in the `debug ip rip` output. In this example, RouterB ignored a v1 update from Router C.

```
RouterB#debug ip rip
RIP protocol debugging is on
RouterB#
3d00h: RIP: received v2 update from 172.16.0.2 on Serial0/0
3d00h: 192.168.12.32/27 via 0.0.0.0 in 1 hop
3d00h: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (172.16.0.1)
3d00h: RIP: build update entries
3d00h: 10.0.0.0/8 via 0.0.0.0, metric 1, tag 0
3d00h: RIP: sending v2 update to 224.0.0.9 via Serial0/1 (10.0.0.1)
3d00h: RIP: build update entries
3d00h: 172.16.0.0/16 via 0.0.0.0, metric 1, tag 0
3d00h: 192.168.12.32/27 via 0.0.0.0, metric 2, tag 0
% Type "show ?" for a list of subcommands
RouterB#
3d00h: RIP: ignored v1 packet from 10.0.0.2 (illegal version)
RouterB#
RouterB#
RouterB#
```

**Figure 8-15** debug ip rip output
Routing Information Protocol version 2 (continued)

- Another enhancement of RIPv2: ability to authenticate routing peers
- Configuring RIPv2 authentication requires the following steps:
  - Define a key chain
  - Define keys in the key chain
  - Enable authentication on the interface by specifying the key chain to be used
  - Enable either clear text or MD5 authentication
  - Manage the keys (optional key lifetimes)
Routing Information Protocol version 2 (continued)

```
RouterB(config)#
RouterB(config)#key chain caudle
RouterB(config-keychain)#key 1
RouterB(config-keychain-key)#key-string ducks
RouterB(config-if)#interface s0/0
RouterB(config-if)#ip rip authentication key-chain caudle
RouterB(config-if)#ip rip authentication mode md5
RouterB(config-if)#

RouterA(config)#
RouterA(config)#key chain cannon
RouterA(config-keychain)#key 1
RouterA(config-keychain-key)#key-string ducks
RouterA(config-keychain-key)#interface s0/0
RouterA(config-if)#ip rip authentication key-chain cannon
RouterA(config-if)#ip rip authentication mode md5
RouterA(config-if)#
```

The two key-strings must match. In essence, this is the shared secret password between the two routers. Of course, because MD5 authentication has been specified, this key will not be sent between the two peers. Only a message digest of the two will be sent.

**Figure 8-16** RIPv2 authentication commands
Routing Information Protocol version 2 (continued)

Because RouterB has been configured with MD5 authentication and RouterA has not, RouterB will not accept routing updates from RouterA.

```
RouterB#debug ip rip
RIP protocol debugging is on
RouterB#
3d01h: RIP: ignored v2 packet from 172.16.0.2 (invalid authentication)
3d01h: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (172.16.0.1)
3d01h: RIP: build update entries
3d01h: 10.0.0.0/8 via 0.0.0.0, metric 1, tag 0
3d01h: 192.168.13.0/24 via 0.0.0.0, metric 2, tag 0
3d01h: RIP: sending v1 update to 255.255.255.255 via Serial0/1 (10.0.0.1)
3d01h: RIP: build update entries
3d01h: network 172.16.0.0 metric 1
```

Figure 8-17  RIPv2 authentication failure
Figure 8-18  RIPv2 authentication success

RouterB, for backward compatibility with RouterC, is broadcasting RIPv1 updates out S0/1.

RouterB is multicasting RIPv2 updates out its S0/0 interface.

MD5 authentication is taking place between RouterA and RouterB.

```
RouterB#debug ip rip
3d01h: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (172.16.0.1)
3d01h: RIP: build update entries
3d01h: 10.0.0.0/8 via 0.0.0.0, metric 1, tag 0
3d01h: 192.168.13.0/24 via 0.0.0.0, metric 2, tag 0
3d01h: RIP: sending v1 update to 255.255.255.255 via Serial0/1 (10.0.0.1)
3d01h: RIP: build update entries
3d01h: network 172.16.0.0 metric 1
3d01h: network 192.168.12.0 metric 1
3d01h: RIP: received packet with MD5 authentication
3d01h: RIP: received v2 update from 172.16.0.2 on Serial0/0
3d01h: 192.168.12.32/27 via 0.0.0.0 in 1 hops
3d01h: RIP: received v1 update from 10.0.0.2 on Serial0/1
3d01h: 192.168.13.0 in 1 hops
3d01h: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (172.16.0.1)
3d01h: RIP: build update entries
3d01h: 10.0.0.0/8 via 0.0.0.0, metric 1, tag 0
3d01h: 192.168.13.0/24 via 0.0.0.0, metric 2, tag 0
3d01h: RIP: sending v1 update to 255.255.255.255 via Serial0/1 (10.0.0.1)
3d01h: RIP: build update entries
3d01h: network 172.16.0.0 metric 1
3d01h: network 192.168.12.0 metric 2
```
Enhanced Interior Gateway Routing Protocol

• Enhanced Interior Gateway Routing Protocol (EIGRP)
  – A Cisco proprietary classless protocol designed to overcome the limitations found in IGRP
  – Still a distance-vector routing protocol at its core

• Protocol Dependent Modules (PDMs)
  – Allow EIGRP to carry multiple routed protocols within their own native packet formats

• EIGRP uses nonperiodic, partial, and bounded routing table updates
Enhanced Interior Gateway Routing Protocol (continued)

• EIGRP makes use of a composite metric comprised of six different factors:
  – Hops, Load, Bandwidth, Reliability, Delay, MTU

• By default, the formula used for metric calculation in EIGRP is:
  \[
  \text{Metric} = \left[ (K1 \times \text{Bandwidth} + \frac{K2 \times \text{Bandwidth}}{256 - \text{load}}
  + K3 \times \text{Delay}) \times \frac{K5}{\text{reliability} + K4} \right] \times 256
  \]
Figure 8-19  EIGRP example network
A "D" in the routing table signifies a route learned via an EIGRP neighbor.

EIGRP can see when a route has been redistributed from another routing protocol. Therefore, it marks the route as an external route learned from an EIGRP neighbor.

```plaintext
RouterA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

192.168.12.0/27 is subnets
  C 192.168.12.32 is directly connected, FastEthernet0/0
D  EX 192.168.13.0/24 [170/21026560] via 172.16.0.1, 00:01:00, Serial0/0
C 172.16.0.0/16 is directly connected, Serial0/0
D 172.20.0.0/16 [90/20514560] via 172.16.0.1, 00:01:00, Serial0/0
D  EX 10.0.0.0/8 [170/21024000] via 172.16.0.1, 00:01:00, Serial0/0
RouterA#
```

**Figure 8-20** EIGRP/IGRP route redistribution
EIGRP Components

• Protocol Dependent Modules (PDM)
  – Allow EIGRP to support multiple Network layer routed protocols

• Neighbor discovery and maintenance
  – Allow EIGRP to discover neighbors and keep track of their status
  – EIGRP must be able to keep updates bounded, sent only to those peers that need the information
  – EIGRP must build a neighbor table of directly connected peers
EIGRP Components (continued)

• **Reliable Transport Protocol (RTP)**
  – Because EIGRP is protocol-independent, it cannot use existing Transport layer protocols to carry its various packet types
  – Instead, Cisco developed an entirely new layer 4 protocol
  – RTP can actually provide both reliable and unreliable delivery
  – Routing table updates are an example of an EIGRP packet type that uses reliable multicast via RTP
## EIGRP Components (continued)

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>Purpose</th>
<th>Transport Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hellos</td>
<td>Maintain neighbor status</td>
<td>Multicast, unreliable</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>Reply to reliable multicast request</td>
<td>Unicast, unreliable</td>
</tr>
<tr>
<td>Updates</td>
<td>Carry route information</td>
<td>Unicast for update to single router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multicast for update to group of routers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reliable delivery</td>
</tr>
<tr>
<td>Queries</td>
<td>Used by DUAL to compute best paths</td>
<td>Multicast or unicast, reliable delivery</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replies</td>
<td>Used by DUAL to compute best paths</td>
<td>Unicast, reliable delivery</td>
</tr>
</tbody>
</table>

**Table 8-1**  EIGRP packet types
EIGRP Components (continued)

• **Diffusing Update Algorithm (DUAL)**
  – The heart and soul of EIGRP
  – Allows EIGRP to quickly recover from a link outage and route around network problems
  – Key terms associated with DUAL
    • **Successor**
    • **Feasible distance (FD)**
    • **Reported distance (RD)**
    • **Feasible successor**
    • **Feasibility condition**
    • **Adjacency**
EIGRP Components (continued)

- DUAL uses the EIGRP topology table to track the status of all links in a network
  - The EIGRP topology table contains information about all the networks a router can reach

- The `show ip eigrp topology` command
  - Displays information garnered from the DUAL process
Figure 8-21  DUAL example network
EIGRP Components (continued)

Neighbors are listed in the order they are learned.

Neighbors’ IP addresses are listed.

Interface column specifies the interface from which RouterA is receiving its neighbor’s Hello packets.

```
RouterA#show ip eigrp neighbors
IP-EIGRP neighbors for process 52

+-------+-------+-----------------+-------+-------+-------+-------+
| #     | Address| Interface   | Hold (sec) | Uptime | SRTT (ms) | RTO Cnt | Seq Num |
|-------|--------+------------+------------+---------+-----------+---------+---------|
| 1     | 192.168.20.2 | Sel  | 11 01:03:49 |         | 647       | 3882    | 0       | 5       |
| 0     | 172.16.0.1   | Se0   | 13 22:44:45 |         | 395       | 2370    | 0       | 16      |
```

**Figure 8-22** Output of the `show ip eigrp neighbors` command output

**Figure 8-21** DUAL example network
EIGRP Components (continued)

RouterA#show ip eigrp topology
IP-EIGRP Topology Table for AS(52)/ID(192.168.12.33)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - reply Status, s - sia Status
P 10.0.0.0/8, 2 successors, FD is 21024000
   via 192.168.20.2 (21024000/20512000), Serial0/1
   via 172.16.0.1 (21024000/20512000), Serial0/0
P 192.168.12.32/27, 1 successors, FD is 28160
   via Connected, FastEthernet0/0
P 192.168.13.0/24, 1 successors, FD is 20514560
   via 192.168.20.2 (20514560/28160), Serial0/1
P 192.168.20.0/24, 1 successors, FD is 20512000
   via Connected, Serial0/1
P 172.20.0.0/16, 1 successors, FD is 20514560
   via 172.16.0.1 (20514560/28160), Serial0/0
P 172.16.0.0/16, 1 successors, FD is 20512000
   via Connected, Serial0/0
RouterA#

Figure 8-23  Output of the show ip eigrp topology command  

Figure 8-21  DUAL example network
EIGRP Components (continued)

RouterB's feasible distance is the distance it will advertise to RouterA as its reported distance (RD). In short, the RD is the best path a neighboring router has to the destination network.

**Figure 8-24**  RouterB show ip eigrp topology command output

**Figure 8-21**  DUAL example network
EIGRP Components (continued)

Only one successor exists for the 192.168.13.0 network, but EIGRP still keeps the second route in the topology table in case the primary route fails. This is one reason convergence is so fast with EIGRP.

```
RouterA#show ip eigrp topology all-links
IP-EIGRP Topology Table for AS(52)/ID(192.168.12.33)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status
P 10.0.0.0/8, 2 successors, FD is 21024000, serno 15
  via 192.168.20.2 (21024000/20512000), Serial0/1
  via 172.16.0.1 (21024000/20512000), Serial0/0
P 192.168.12.22/27, 1 successors, FD is 28160, serno 1
  via Connected, FastEthernet0/0
P 192.168.13.0/24, 1 successors, FD is 20514560, serno 16
  via 192.168.20.2 (20514560/28160), Serial0/1
  via 172.16.0.1 (21024560/20514560), Serial0/0
P 192.168.20.0/24, 1 successors, FD is 20512000, serno 14
  via Connected, Serial0/1
P 172.20.0.0/16, 1 successors, FD is 20514560, serno 8
  via 172.16.0.1 (20514560/28160), Serial0/0
  via 192.168.20.2 (21026560/20514560), Serial0/1
P 172.16.0.0/16, 1 successors, FD is 20512000, serno 2
  via Connected, Serial0/0
```

**Figure 8-25** Output of `show ip eigrp topology all-links` command

**Figure 8-21** DUAL example network
EIGRP Configuration

• EIGRP configuration is nearly identical to IGRP configuration

• EIGRP is classless
  – However, it summarizes to classful network boundaries by default
  – The `no auto-summary` command turns off this default behavior

• Highly recommended to use the `bandwidth` command to set the actual bandwidth on serial links
EIGRP Configuration (continued)

RouterA>enable
RouterA#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#router eigrp 52
RouterA(config-router)#no auto-summary
RouterA(config-router)#network 192.168.20.0
RouterA(config-router)#network 172.16.0.0
RouterA(config-router)#network 192.168.12.0
RouterA(config-router)#^Z
RouterA#

Figure 8-26  EIGRP configuration

Figure 8-21  DUAL example network
The first number is the administrative distance and the second is the metric to the network. In this case, the two successors from the EIGRP topology table have been installed as equal cost paths in the routing table.

RouterA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
    D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
    i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
    * - candidate default, U - per-user static route, o - ODR
    P - periodic downloaded static route

Gateway of last resort is not set

  192.168.12.0/27 is subnetted, 1 subnets
C    192.168.12.32 is directly connected, FastEthernet0/0
D    192.168.13.0/24 [90/20514560] via 192.168.20.2, 00:00:03, Serial0/1
C    172.16.0.0/16 is directly connected, Serial0/0
D    172.20.0.0/16 [90/20514560] via 172.16.0.1, 00:00:03, Serial0/0
C    192.168.20.0/24 is directly connected, Serial0/1
D    10.0.0.0/8 [90/21024000] via 192.168.20.2, 00:00:03, Serial0/1
    [90/21024000] via 172.16.0.1, 00:00:03, Serial0/0

Figure 8-27  EIGRP routing table

Figure 8-21  DUAL example network
EIGRP Configuration (continued)

- EIGRP supports optional authentication of routing peers
- Configuring EIGRP authentication requires the following steps:
  - Define a key chain
  - Define keys in the key chain
  - Enable authentication on the interface by specifying the key chain to be used
  - Manage the keys (optional key lifetimes)
Note that the IOS is case-sensitive, so the key chain name must match exactly when linked to EIGRP.

Note also that at least one key-string or shared secret must match for the two peers to authenticate.

```
RouterA(config)#key chain EIGRPKEYS
RouterA(config-keychain)#key 1
RouterA(config-keychain-key)#key-string caudle
RouterA(config-keychain-key)#exit
RouterA(config-keychain)#exit
RouterA(config)#interface s0/0
RouterA(config-if)#ip authentication key-chain eigrp 52 EIGRPKEYS
RouterA(config-if)#ip authentication mode eigrp 52 md5
RouterA(config-if)#

RouterB(config)#key chain EIGRPKEYS
RouterB(config-keychain)#key 1
RouterB(config-keychain-key)#key-string caudle
RouterB(config-keychain-key)#exit
RouterB(config-keychain)#exit
RouterB(config)#int s0/0
RouterB(config-if)#ip authentication key-chain eigrp 52 EIGRPKEYS
RouterB(config-if)#ip authentication mode eigrp 52 md5
RouterB(config-if)#
```

Figure 8-28  EIGRP authentication
Open Shortest Path First

- **Open Shortest Path First (OSPF)**
  - An open standards, link-state routing protocol that supports classless routing, variable-length subnet masks, and authentication

- Link-state routing protocols allow routers to share a common view of the entire network
  - Each router sends out link-state advertisements (LSAs) describing its attached links to all routers in an area

- Each router needs to hold a topological database of the entire area
Open Shortest Path First (continued)

<table>
<thead>
<tr>
<th>Distance-vector</th>
<th>Link-state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Periodically broadcasts entire routing table to neighbor routers</td>
<td>Multicasts links to all neighbor routers in the AS on startup; all other routing table updates contain only updated routes; typically, updates only occur when a network topology change occurs</td>
</tr>
<tr>
<td>Slow to converge</td>
<td>Fast to converge due to link-state advertisements</td>
</tr>
<tr>
<td>Prone to routing loops because of routing by rumor nature</td>
<td>Less prone to routing loops because all other routers share a common view of the network</td>
</tr>
<tr>
<td>Easy to configure and administer</td>
<td>Harder to configure; requires greater memory and processing power on each router</td>
</tr>
<tr>
<td>Consumes relatively more bandwidth</td>
<td>Consumes relatively less bandwidth</td>
</tr>
</tbody>
</table>

**Table 8-2** Major characteristics of distance-vector and link-state routing protocols
Open Shortest Path First (continued)

• OSPF is ideally suited for large networks
  – Uses a concept known as areas to bound link-state advertisements

• An area is the portion of a network within which LSAs are contained
  – All OSPF routers configured with the same area identification will accept LSAs from one another
Figure 8-29  OSPF areas
OSPF Concepts

• **Link**
  – A router’s interface

• **Link-state**
  • The status of a link on a router

• **Area**
  – Defines the confines within which LSAs are contained

• **Cost**
  – The default metric for OSPF
OSPF Concepts (continued)

<table>
<thead>
<tr>
<th>Link Type</th>
<th>Cisco Default Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>FDDI, Fast Ethernet and faster</td>
<td>1</td>
</tr>
<tr>
<td>Ethernet</td>
<td>10</td>
</tr>
<tr>
<td>E1 (2.048 Mbps)</td>
<td>48</td>
</tr>
<tr>
<td>T1 (1.544 Mbps)</td>
<td>64</td>
</tr>
<tr>
<td>56 Kbps</td>
<td>1785</td>
</tr>
</tbody>
</table>

**Table 8-3**  Cisco’s default OSPF costs for certain link types
OSPF Concepts (continued)

```
RouterA#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.12.33
  Number of areas in this router is 0.0 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway    Distance    Last Update
    Distance: (default is 110)
```

**Figure 8-30** Determining OSPF reference bandwidth

OSPFCost
calculation
based on
FastEthernet
as the reference
bandwidth.
OSPF Concepts (continued)

- **Adjacencies database**
  - Contains information about all OSPF peers with which a router has successfully exchanged Hello packets

- **Topological database**
  - Holds the common view of the network formed from the link-state advertisements that are received

- **Designated routers (DRs)**

- **Backup designated routers (BDRs)**
OSPF Concepts (continued)

RouterB#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#interface serial 0/0
RouterB(config-if)#ip ospf hello-interval 5
RouterB(config-if)#ip ospf dead-interval 20
RouterB(config-if)#

Figure 8-31 Configuring OSPF timers
OSPF Concepts (continued)

Figure 8-32  OSPF on a broadcast, multi-access network
OSPF Concepts (continued)

```
RouterC(config-if)#interface loopback 0/1  
RouterC(config-if)#ip address 1.1.1.1 255.255.255.255
```

Figure 8-33  Loopback address configuration
OSPF Operation

• Steps
  – An OSPF router forms adjacencies with neighbors
  – A DR and BDR are elected in OSPF
  – Routers will flood their link-state advertisements and go through the process of selecting the best route to each network

• OSPF uses **Dijkstra’s Shortest Path First** algorithm to find the best path
  – Each router sees itself as the central point from which a loop-free, best-cost path to each network is determined
OSPF Operation (continued)

Figure 8-34  OSPF example network
OSPF Operation (continued)

The router ID is the highest IP address on an active interface on the neighbor router.

Once neighbors are in a FULL state, they have correctly formed adjacency with one another.

<table>
<thead>
<tr>
<th>Neighbor ID</th>
<th>Pri</th>
<th>State</th>
<th>Dead Time</th>
<th>Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.20.2</td>
<td>1</td>
<td>FULL/</td>
<td>00:00:30</td>
<td>10.0.0.2</td>
<td>Serial0/1</td>
</tr>
<tr>
<td>192.168.20.1</td>
<td>1</td>
<td>FULL/</td>
<td>00:00:32</td>
<td>172.16.0.2</td>
<td>Serial0/0</td>
</tr>
</tbody>
</table>

**Figure 8-35**  Output of `show ip ospf neighbor` command
## OSPF Operation (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Hello</td>
<td>Neighbor discovery and adjacency maintenance</td>
</tr>
<tr>
<td>2</td>
<td>Database Description</td>
<td>Summarizes topological database between routers during initialization of neighbor relationship</td>
</tr>
<tr>
<td>3</td>
<td>Link State Request</td>
<td>Request Link State information from a neighbor’s database</td>
</tr>
<tr>
<td>4</td>
<td>Link State Update</td>
<td>Advertises available links via network flooding</td>
</tr>
<tr>
<td>5</td>
<td>Link State Acknowledgement</td>
<td>Response to flooded links sent via Link State Updates</td>
</tr>
</tbody>
</table>

*Table 8-4  OSPF Packet Types*
Single-Area OSPF Configuration

- OSPF offers a huge number of configuration options
  - Including multiple areas of different types

```
RouterB(config)#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#router ospf 1
RouterB(config-router)#network 172.20.0.0 0.0.255.255 area 0
RouterB(config-router)#network 172.16.0.0 0.0.255.255 area 0
RouterB(config-router)#network 10.0.0.0 0.255.255.255 area 0
RouterB(config-router)#exit
RouterB(config)#
```

Once OSPF is turned on, you must then specify which networks will be advertised. Note that OSPF does not use subnet masks. Instead, it uses wildcard masks. Also, each network must be associated with an area (in this case, area 0).

Figure 8-36 Single-area OSPF configuration
Single-Area OSPF Configuration (continued)

This ip route command sets a default route that sends all traffic without an entry in the routing table out serial0/1.

The default-information originate command causes RouterB to advertise its default route to the network.

Figure 8-37  Default route configuration in OSPF

RouterB(config-if)#ip route 0.0.0.0 0.0.0.0 serial0/1
RouterB(config-if)#router ospf 1
RouterB(config-router)#default-information originate
RouterB(config-router)#
OSPF Authentication

• Routing update authentication is a basic security requirement for all modern routing protocols
• OSPF provides authentication of routing table updates via several methods
  – No authentication (the default)
  – Authentication with passwords sent in clear text
  – Authentication using MD5 hashing of a shared secret key
OSPF Authentication (continued)

- To perform MD5 authentication of routing updates in OSPF, two steps must be completed:
  - Configuration of authentication keys on each OSPF interface
  - Configuration of area authentication

![OSPF Authentication Example Network](image.png)

*Figure 8-38* OSPF authentication example network
OSPF Authentication (continued)

```
RouterA(config)#int s0/3/0
RouterA(config-if)#ip ospf message-digest-key 1 md5 TiAspw34

RouterB(config)#interface s0/3/0
RouterB(config-if)#ip ospf message-digest-key 1 md5 TiAspw34
RouterB(config-if)#
```

**Figure 8-39** OSPF interface authentication commands

```
RouterA(config)#router ospf 1
RouterA(config-router)#area 0 authentication message-digest

RouterB(config)#router ospf 1
RouterB(config-router)#area 0 authentication message-digest
```

**Figure 8-40** OSPF routing protocol authentication commands

Turns on MD5 authentication and sets the password to “secureme.”

Turns on MD5 authentication for area 0.
RouterA#sh ip ospf
Routing Process "ospf 1" with ID 192.168.12.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPF's 10000 msecs
Maximum wait time between two consecutive SPF's 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
  Area BACKBONE(0)
Number of interfaces in this area is 2
Area has message digest authentication
SPF algorithm last executed 00:00:57.676 ago
SPF algorithm executed 9 times
Area ranges are
Number of LSA 2. Checksum Sum 0x0113D3
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

Figure 8-41  Verifying OSPF authentication

MD5 authentication is turned on.
Controlling Route Traffic

- **passive-interface command**
  - An important entry-level command for controlling route traffic
  - Disrupts the function of EIGRP and OSPF

- The command causes a router to listen only on the passive interface
  - Therefore, if used with EIGRP or OSPF, the router will not send Hellos out the interface

- The result is a link that is seen as having no neighbors on it
  - Therefore, it will not be used to form adjacencies
Controlling Route Traffic (continued)

Figure 8-42  Passive-interface example