Conquering OSPF: Optimize Your Network with OSPF

As networks grow, become more complex, and rate of change increases, a move to dynamic routing is often a good choice. Dynamic routing leverages routing protocols to transmit network updates between routers automatically as changes occur, allowing routers to update their routing tables with the best options to reach destinations without requiring manual intervention by network engineers.

OSPF, or Open Shortest Path First, is a widely deployed standard routing protocol that scales from small "single area" networks to large global wide area networks. CCNA candidates need to be comfortable configuring and verifying single area OSPFv2 deployments. In this lab we will explore:

- Configuring IOS routers to run OSPF and share network information with neighbors
- Configure and verify neighbor adjacency details such as Router IDs and Timers
- Designated Router/Backup Designated Router election
- Sharing a default route with OSPF

Setup and Scenario

In this set of lab-based demonstrations, you are the network engineer for a growing organization tasked with updating the network to support new network needs. The network was originally deployed using static routes as it was small, but now the network has grown from a single building to a "campus", and it is time to deploy dynamic routing.

You've been asked to:

- Enable OSPF between the core routers and the building 1 Layer 3 switch
- Ensure reliable internet access in case of a link failure to the primary router `cr-rtr1`
- Ensure the core routers provide routing updates to all building switches

*Be sure to **START** the lab before continuing to the demo labs.*

Part 1: Reviewing the Current State of the Network

Before we jump into configuring OSPF across the network, let's check the current status of the network and how it is operating.

1. Open a VNC connection to the desktop `user1`. Open the Internet browser and navigate to https://u.cisco.com.
   - You should see the Cisco U homepage.
2. Open the terminal application and `ping www.cisco.com`.
   - You should see pings return successfully.

     > If these steps fail, verify that your CML server is configured and deployed to allow Internet access for hosts through a NAT configured external connector node.
     >
     > If your server is ***not*** configured to allow this access, you can `ping 192.168.200.1` as an alternative test. This is a loopback address on `cr-rtr1`.
3. Open a VNC connection to the desktop `guest1` and repeat the tests.
   - **These tests should** *not ***work.***

Uh oh... something doesn't seem to be right with the network. See if you can figure out what is wrong and why the `guest1` desktop can't reach the internet.

▶ Answer to what is wrong

What did we learn?

While dynamic routing doesn't prevent misconfigurations, by reducing the manual management of a large number of static routes and instead allowing the routers to send routing updates directly, this does improve reliability and remove what can be difficult troubleshooting scenarios.

Part 2: Basics of Getting OSPF Up and Running

Minimal configuration needed to build neighbor relationships

We'll start with the minimal configuration necessary for OSPF relationships to be created between the core routers and building switch.

- Enable OSPF process
- Add the interfaces/networks between routers to OSPF area 0
- Start by configuring `bld1-sw`:

  ```
  router ospf 11
       network 172.20.1.0 0.0.0.255 area 0
  ```

- And now `cr-rtr1`:

```
router ospf 1
     network 172.20.1.0 0.0.0.255 area 0
```

- Some things to take note of:
  - Each router has a "process id". This value is locally significant on each router and does ***not*** need to match.
  - `network` statements with "wildcard masks" are used to match interfaces on the router to enable for OSPF
- Watch the console output on `cr-rtr1`. After some time you should see a message like the one below. This is an indication that OSPF has completed establishing the neighbor relationship between `bld1-sw` and `cr-rtr1` and is now exchanging routing information.

```
*Oct 18 06:04:22.574: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.199.1 on Ethernet0/2 from LOADING to FULL, Loadin
```

- There are many `show` commands available for OSPF, but we'll start with `show ip ospf neighbor` to view the current neighbors on `cr-rtr1`.

```
cr-rtr1# show ip ospf neighbor
    Neighbor ID     Pri   State           Dead Time   Address         Interface
    192.168.199.1     1   FULL/BDR        00:00:37    172.20.1.11     Ethernet0/2
```

  - The `Neighbor ID` is also called the "router ID", and represents the routers identity included in OSPF updates
  - `Pri` or "Priority" is used in "Designated Router" elections. Higher priority is better and values range from 0 -> 255
  - `FULL/BDR` indicates that our router has completed sharing routing information (or link state database information) with this neighbor (full), and that this neighbor is the "Backup Designated Router" on this link.
  - The `Dead Time` is a countdown clock for when this neighbor will be considered no longer valid. If it reaches `0`, the neighbor will be removed.
  - `Address` indicates the next hop address to the neighbor out of the `Interface`

    We'll be talking more about the Designated Router / Backup Designated Router (DR/BDR) election in the next step.

- Another very useful command is `show ip ospf interface brief`.

```
cr-rtr1# show ip ospf interface brief
    Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
    Et0/2        1     0               172.20.1.1/24      10    DR    1/1
```

  - This command lists all interfaces on a router that are participating in OSPF. This can be helpful when troubleshooting to ensure that the interfaces you expect to have neighbors, are actually configured for OSPF.
  - The "non-brief" version of the command has even more information that can be helpful for troubleshooting.
- Run these commands on `bld1-sw` and compare the results.
- Go ahead and configure `cr-rtr2`:

```
router ospf 2
     network 172.20.1.0 0.0.0.255 area 0
```

- Very quickly you should see messages on the `cr-rtr2` console that neighbor relationships with the other two routers have been established.

```
*Oct 18 06:26:52.796: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.199.1 on Ethernet0/2 from LOADING to FULL, Loadin
    *Oct 18 06:26:52.796: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.200.1 on Ethernet0/2 from LOADING to FULL, Lo
```

  This was so much faster than the initial relationship between `cr-rtr1` and `bld1-sw` because the designated router election process was already complete on the "broadcast" network connecting the three routers.

- Run the `show ip ospf neighbor` and `show ip ospf interface brief` commands on all three devices.
  - Each device should now have 2 neighbors
  - `cr-rtr2` should be in a state of `FULL/DROTHER` for the other routers

Exploring Designated Router election and status

Every interface running OSPF has a "network type" that impacts some of the details with how OSPF runs and operates. Ethernet interfaces have a type of "broadcast". Broadcast networks can have many different OSPF speaking routers on a single network segment. If every router exchanged links state databases with every other router on a broadcast network, this would result in a large amount of duplicate traffic.

To be more efficient, OSPF elects a "Designated Router" (DR) to collect routing information from all other routers on the segment, and distribute ***ALL*** information to every other router. And because we like redundancy in networking, a "Backup Designated Router" (BDR) is also identified. The BDR also distributes routing information to other routers. If the DR fails, the BDR will take over immediately, and a new BDR will be elected.

Like with spanning-tree, explicitly identifying the DR/BDR in an network is advised. "Core" or "hub" routers are the best candidates for this role, with "stub" routers often configured to *never* become a DR/BDR.

The OSPF priority value configured on an interface determines the outcome of a DR/BDR election. The higher the priority, the more likely it will become the DR/BDR. A priority of `0` will prevent a router from participating in the election.

Now we will update the configuration in our network to use the core routers for DR/BDR, and prevent the building switches (layer 3 switches) from becoming a DR or BDR.

Note: DR/BDR status on a network does NOT preempt. This means that if a new router with a higher priority comes onto a network segment with a DR already elected, the new router will NOT become the DR. If the current DR or BDR fails, this new router will then take over the role of BDR.

1. Start by using the `show ip ospf neighbor` command on each router to verify the current priority and DR/BDR roles for each router.
2. On `cr-rtr1`, increase the ospf priority of interface `Ethernet0/2` to 10.

```
interface ethernet0/2
     ip ospf priority 10
```

- You can verify the change with the `show ip ospf interface eth0/2` command
- Access the console on `bld1-sw` and run the `show ip ospf neighbor` command. You should now see the increased priority for `cr-rtr1`.

```
Neighbor ID      Pri   State           Dead Time   Address         Interface
    192.168.200.1    10   FULL/DR         00:00:32    172.20.1.1      Ethernet0/0
    192.168.255.64    1   FULL/DROTHER    00:00:36    172.20.1.2      Ethernet0/0
```

- Now configure a priority of `0` on `bld1-sw` interface `ethernet0/0` to remove it from the `DR/BDR` election process.

```
interface ethernet0/0
     ip ospf priority 0
```

- Check the OSPF neighbor status on the switch again.

```
Neighbor ID      Pri   State           Dead Time   Address         Interface
    192.168.200.1    10   FULL/DR         00:00:38    172.20.1.1      Ethernet0/0
    192.168.255.64    1   FULL/BDR        00:00:35    172.20.1.2      Ethernet0/0
```

  - Now `cr-rtr2` is the BDR for the network segment.

- Verify that `bld1-sw` does NOT become a DR/BDR no matter what by saving the running configuration (`write mem`) on `cr-rtr2` and then **STOPPING** the router.

  Only **STOP** the **router**. Do not wipe it, or stop the entire lab.

- Wait 40 seconds for the dead timer to expire, and check the neighbor status on `cr-rtr1`.

```
*Oct 18 07:00:55.340: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.255.64 on Ethernet0/2 from FULL to DOWN, Neighbor

    cr-rtr1#show ip ospf neighbor

    Neighbor ID      Pri   State           Dead Time   Address         Interface
    192.168.199.1     0    FULL/DROTHER    00:00:31    172.20.1.11     Ethernet0/2
```

  Even though there isn't another router to be the BDR on the network segment, `bld1-sw` stays in `DROTHER` state.

- **START** `cr-rtr2`. Shortly after coming online, it should regain the `BDR` state.

Configuring Router (Neighbor) IDs

Every OSPF router needs to have a unique router ID assigned. If one is not explicitly configured, the router will chose the IP address of one of its interfaces to act as the router ID. The highest IP address assigned to a loopback address will be chosen. If no loopbacks are configured, the highest IP address on a non-loopback active interface will be selected.

```
   Neighbor ID     Pri   State           Dead Time   Address         Interface
   172.20.1.2        1   FULL/BDR        00:00:32    172.20.1.2      Ethernet0/2
   192.168.199.1     0   FULL/DROTHER    00:00:33    172.20.1.11     Ethernet0/2
   192.168.200.1    10   FULL/DR         00:00:30    172.20.1.1      Ethernet0/2
```

Above in red we see the automatically assigned router IDs. Can you tell which router is which?

Relying on automatic router ID assignment is not recommended, because as interface configurations on routers change, the router ID will also change. While this won't prevent OSPF from working, it can make operating and troubleshooting the network more difficult as router id values adjust.

Router IDs "look like" IP addresses, but they needn't be an IP address on a router. Any IP address can be used. We will configure some easy to see and identify router IDs for our network.

Router	Router Id
`cr-rtr1`	`1.1.1.1`
`cr-rtr2`	`2.2.2.2`
`bld1-sw`	`11.11.11.11`

1. Open the console for `cr-rtr1` and configure the router ID under the `router ospf` process.

```
router ospf 1
     router-id 1.1.1.1
```

```

```

2. You should see a message like the one shown below. To improve stability, routers identify their router ID when the OSPF process starts up and maintain that same ID, no matter configuration changes, until the OSPF process restarts. This can occur when the router reloads, or a `clear ip ospf process` command is ran.

```
% OSPF: Reload or use "clear ip ospf process" command, for this to take effect
```

3. Another very useful verification command is `show ip protocols`. This command provides information on all routing protocols running on a router. Use it to verify the router-id on `cr-rtr1`. Notice that it still shows the automatically identified router ID value.

```
    show ip protocols | begin ospf

    ! Output
    Routing Protocol is "ospf 1"
    .
    Router ID 192.168.200.1
```

Number of areas in this router is 1. 1 normal 0 stub 0 nssa Maximum path: 4 Routing for Networks: 172.20.1.0 0.0.0.255 area 0 .

4. Now restart OSPF on the router to apply the change. You will be asked to confirm because this will be a disruptive change on the network.

```
clear ip ospf process
```

5. Verify that the router ID has changed.

```
show ip protocols | inc ID

    # Output
    Router ID 1.1.1.1
```

6. Repeat the process on `cr-rtr2` and `bld1-sw` to set their router IDs and reset the OSPF process to apply the change.

    Note 💡: The OSPF process ID configured on each router is unique. `cr-rtr2` is `router ospf 2` and `bld1-sw` is `router ospf 11`

7. On `bld1-sw` look at the OSPF neighbors and see the new, more easily recognozied Router IDs.

```
bld1-sw# show ip ospf neighbor

    Neighbor ID     Pri   State           Dead Time   Address         Interface
    1.1.1.1          10   FULL/DR         00:00:38    172.20.1.1      Ethernet0/0
    2.2.2.2           1   FULL/BDR        00:00:36    172.20.1.2      Ethernet0/0
```

Advertising Dynamic Routes

Now that we have the OSPF neighbor relationships created between our three routers, the time has come to replace the static routes with dynamic routes managed by OSPF.

1. Start with the Building 1 networks. On the console for `bld1-sw`, look at the IP interfaces configured.

```
show ip int bri | exc unassigned
```

2. Compare the networks with the static routes on `cr-rtr1`.

```
show ip route static
```

3. Other than the network on `bld1-sw` interface `Ethernet0/0` which is the transit network to the routers, each of the networks on the switch should have associated static routes.

    The routers also each have a static default route. `cr-rtr1`'s static route was learned through DHCP and targets the `internet-gateway`. `cr-rtr2`'s static route was manually configured to route through `cr-rtr1` over the direct transit link.

4. OSPF is a "link state" routing protocol, which means decisions are made by exchanging details about the "links" each router has. Look at the links advertised by `bld1-sw` into OSPF.

    This command can be ran on any router.

```
show ip ospf database router adv-router 11.11.11.11
```

    - There are several different types of "LSAs" used by OSPF to describe different types of networks. The `router` LSAs are used to describe all directly connected networks
    - This command is limiting the output only to LSA data advertised by `bld1-sw` - as identified by its router ID.

5. How many links are advertised by the switch? Which links?

6. Add a `network` statement under the OSPF router process configuration on `bld1-sw` to begin advertising the Vlan 10 interface for users into area 0. Remember that OSPF uses wildcard masks for matching interfaces identified in network statements.

```
router ospf 11
     network 192.168.11.0 0.0.0.255 area 0
```

7. Look at the Link State Database again, do you see the new network listed? How is this "link" different than the other "link"?
8. Now that the "user" network is included in OSPF, check the OSPF routes in the routing table on `cr-rtr1`.

```
show ip route ospf
```

   - Is the route listed? Why not?

   ▶ Answer:

9. Remove the static route on both `cr-rtr1` and `cr-rtr2` for the "user" network.

```
no ip route 192.168.11.0 255.255.255.0 172.20.1.11
```

10. Check the OSPF routes again. Is it there?
11. `network` statements aren't the only way to add interfaces and networks into OSPF, there is also an interface configuration command that can be used. Use it to advertise the `iot` network on `bld1-sw`.

```
interface vlan 20
     ip ospf 11 area 0
```

   It is important to use the correct OSPF process number in this command.

12. Complete the configuration to ensure that the network `192.168.199.0/24` is listed as an "OSPF" route on both core routers.
13. Use either `network` statements or the interface configuration method to advertise the "security" and "guest" networks with OSPF. Be sure that they are listed as "OSPF" routes in the routing tables for the core routers.
14. Verify the routing table on `cr-rtr1` and `cr-rtr2` to confirm that you now have four OSPF entries, one for each of the VLANs in Building 1.
15. Verify that both desktops can still access the Internet. Either by browsing to https://u.cisco.com using a VNC connection, or by pinging `8.8.8.8`.

Part 3: Further OSPF Exploration with Enhancements, Troubleshooting, and Tuning

You've now completed the basic setup of OSPF on this network, moving from static routing to dynamic routing. But that isn't the end of the OSPF journey. In this part, you will explore a few more aspects of OSPF.

Troubleshooting OSPF Neighbor Relationships

Look at the network topology. Notice the direct link between the two core routers? This transit network provides an alternative path between the routers should either router lose its link to the "Core Routing" network segment shared with `bld1-sw`. In this step, we will extend OSPF area 0 to include this link.

1. From the console connection of `cr-rtr1`, use the interface configuration command to add `Ethernet0/1` to ospf area 0.

```
interface eth0/1
     ip ospf 1 area 0
```

2. Repeat on `cr-rtr2`, using OSPF process 2.
3. The DR/BDR election takes 40 seconds (the equivalent of the "dead timer") to complete. Wait that time and check the status of the neighbor relationship on both routers using the following commands:

```
show ip ospf neighbor
    show ip ospf interface brief
```

   - Which routers is the designated router for the link?
   - Did the routers form a neighbor relationship?
   - What is wrong?

   ▶ Answer

4. The link between the two routers is a direct connection between two routers. There will only ever be 2 hosts on this link, so a `/30` subnet is correct. Change the configuration on `cr-rtr2` for `interface eth0/1` to use the same IP address but the correct subnet mask.
   - You should quickly see the below message indicating that the neighbor relationship was established. Use the OSPF `show` commands to verify the current status is as expected.

```
*Oct 28 06:27:50.762: %OSPF-5-ADJCHG: Process 2, Nbr 1.1.1.1 on Ethernet0/1 from LOADING to FULL, Loading D
```

Advertising a Default Route Dynamically

Currently a static route is used on `bld1-sw` to send Internet traffic through `cr-rtr1` as the primary path, with a floating static route configured to use `cr-rtr2` as an alternative.

```
bld1-sw# show run | section ip route
    ip route 0.0.0.0 0.0.0.0 172.20.1.1
    ip route 0.0.0.0 0.0.0.0 172.20.1.2 10
```

Testing the floating static default route

1. Test that this is working by starting a ping from the `user1` desktop to the Internet with the command `ping 8.8.8.8`.
2. Once it is running, `shutdown` interface `Ethernet0/2` on `cr-rtr1`. This will break the path to the internet from `bld1-sw`.

   `Ethernet0/2` is the interface that connects to the transit network between the devices.

3. What happens to the ping from the desktop?
4. Did the floating static route work? Why not?

   ▶ Answer

5. Re-enable the interface on `cr-rtr1` and verify that the ping resumes working.

Advertise a default route from `cr-rtr1` into OSPF

A default network is added to OSPF with the special command `default-information originate`.

1. Add this command to the `router ospf` process configuration on `cr-rtr1`.

```
router ospf 1
     default-information originate
```

2. Default routes are considered "external networks" within OSPF. Check for an "external LSA" on any router.

```
show ip ospf database external
```

3. We already have seen that static routes will be preferred over OSPF routes, remove both static default routes from `bld1-sw`.

```
no ip route 0.0.0.0 0.0.0.0 172.20.1.2 10
    no ip route 0.0.0.0 0.0.0.0 172.20.1.1
```

4. Check the default route on `bld1-sw` now.

```
show ip route
    show ip route 0.0.0.0
```

   The second command provides some additional route details, including the "type" of OSPF route it is. The "External type 2" matches the LSA database output we saw.

Testing Dynamic Default Routing

With the changes made, test that `bld1-sw` can maintain a valid path to the Internet even if the link to `cr-rtr1` fails.

1. Test that the primary path is working by tracing the first four hops in the path to `8.8.8.8` on `user1`.

```
traceroute -m 4 -n 8.8.8.8

    # Output
    1  192.168.11.1  0.940 ms  0.816 ms  0.738 ms
    2  172.20.1.1  1.556 ms  1.173 ms  1.294 ms
    3  192.168.255.1  1.593 ms  1.754 ms  1.583 ms
    4  10.1.1.1  1.916 ms  1.722 ms  2.042 ms
```

   Hop 2, `172.20.1.1` is `cr-rtr1` as expected.

2. Start a ping from the `user1` desktop to the Internet with the command `ping 8.8.8.8`. Let it run to look for impact of an outage.
3. Once it is running, `shutdown` interface `Ethernet0/2` on `cr-rtr1`. This will break the path to the internet from `bld1-sw`.

   `Ethernet0/2` is the interface that connects to the transit network between the devices.

4. What happens to the ping from the desktop?
   - No pings should be lost, or possibly 1 or 2 ping packets, because OSPF updates the interface state before IOS actually takes the interface down.
5. Stop the ping on `user1`, and repeat the `traceroute`.

```
traceroute -m 4 -n 8.8.8.8
    traceroute to 8.8.8.8 (8.8.8.8), 4 hops max, 46 byte packets
    1  192.168.11.1  1.085 ms  0.618 ms  0.701 ms
    2  172.20.1.2  1.956 ms  1.494 ms  1.183 ms
    3  172.20.0.1  2.472 ms  2.116 ms  1.793 ms
    4  192.168.255.1  2.517 ms  2.358 ms  2.448 ms
```

Hop 2 is now `172.20.1.2`, or `cr-rtr2`. At hop 3, `172.20.0.1`, traffic goes across the transit link to `cr-rtr1` to reach the Internet.

6. Re-enable the interface on `cr-rtr1` and verify the path returns to directly through `cr-rtr1`.

Configuring the Backup Default Gateway

`cr-rtr2` is configured to prefer the a path to the internet through `cr-rtr2` over the direct link it has to the `internet-gateway`. But if `cr-rtr1` goes down completely, it needs to provide an alternative path to the Internet. If multiple `default-information originate` routers are configured on a network, the `metric` can be used to perfer one path over another.

> Note 💡 : `cr-rtr2` is configured with IP SLA tracking as part of the static route through `cr-rtr1`. IP SLA tracking is out of scope for the CCNA, but feel free to look at the configuration and research the topic on your own.

1. Configure `cr-rtr2` to originate a default route with a metric of `10000`.

```
router ospf 2
     default-information originate metric 10000
```

2. Use `show ip ospf database external` to see the new LSA from `cr-rtr2`. How does it differ from the external LSA from `cr-rtr1`? Why does the `Forward Address` point to `cr-rtr1`?
3. Start a ping to `8.8.8.8` from `user1` to test for outage impact.
4. Save the running configuraiton on `cr-rtr1` so none of your changes are lost.

```
copy running-config startup-config
```

5. **Stop** but do ***NOT*** *Wipe* `cr-rtr1`.
6. Monitor the ping and syslog messages on the routers.
7. Once the pings being working again, check the routing table on `bld1-sw`.
   - What is the default gateway now?
   - What is the metric of the default route now?
8. **Start** `cr-rtr1`.
   - Once it restarts, verify the default route on `bld1-sw` has returned to the path through `cr-rtr1`.

Speeding up failure detection

Routers do not always have a chance to send out updates when a failure happens. In these cases, the OSPF timers configured on the network are used to remove invalid routes.

Testing Recovery Time When a Cable Breaks

1. Start a ping from the `user1` desktop to the Internet with the command `ping 8.8.8.8`. Let it run to look for impact of an outage.
2. Open the console for `bld1-sw` and run the command `show clock` to display the current time on the switch.
3. Find and click the link from `cr-rtr1` to the switch that connects to `cr-rtr2` and `bld1-sw` and choose "Delete".
4. Wait and monitor the console output on the `bld1-sw` and the results of the ping. Once the pings begin responding again, press `Cntrl-C` to stop the ping and answer these questions.
   - How many pings were lost?
   - Use the timestamp from the `show clock` command, and the syslog message about `%OSPF-5-ADJCHG: ... FULL to DOWN, Neighbor Down: Dead timer expired` to calculate how long it took for the network to respond to the outage
   - Why?
     - ▶ Answer:
5. Replace the deleted link from `cr-rtr1` to the switch. Use interface `Ethernet 0/2` on the router and any port on the switch.

Configuring a Faster Neighbor Outage Detection

The two timers in OSPF for neighbor relationships are the "hello interval" timer and the "dead interval" timer. The hello interval is how often a hello packet is sent between routers to build and maintain neighbor relationships. The dead interval is how long a router will wait for a hello packet on a link before marking a neighbor as "dead". The defaults on Cisco IOS are 10 second hello interval and 40 second dead interval (the default dead interval is 4 times the hello interval).

These defaults are pretty good and work for many networks, but sometimes you want to detect and recover from failures faster. You can do this by reducing the intervals on specific interfaces. IP networks by design are not 100% reliable, so using a 4x hello interval for the dead interval is a good practice. And always remember you are balancing faster response time with extra overhead on the network.

Also important to remember, the OSPF timers are one of the factors that must match in order for neighbor relationships to be built and maintained. So changing timers are disruptive to the network.

1. On `bld1-sw` interface `Ethernet 0/0` change the timers to 1 second hello, and 4 second dead.

   ```
   interface eth0/0
        ip ospf hello-interval 1
        ip ospf dead-interval 4
   ```

2. If you wait 40 seconds, you'll see messages about the neighbor relationships with the other routers going down. Why is this?

3. Change the timers on `cr-rtr1` and `cr-rtr2` interfaces `Ethernet 0/2` to match.

Testing the new recovery time

Repeat the test cable break. Use the same process and answer these questions:

- How many pings were lost?
- Use the timestamp from the `show clock` command, and the syslog message about `%OSPF-5-ADJCHG: ... FULL to DOWN, Neighbor Down: Dead timer expired` to calculate how long it took for the network to respond to the outage
- Why?

▶ Answer:

Much faster!