This chapter describes how to configure OSPF on ProCurve Routing Switches using the CLI and Web management interface.

To display OSPF configuration information and statistics, see “Displaying OSPF Information” on page 12-47.

For complete syntax information for the CLI commands shown in this chapter, see the Command Line Interface Reference for ProCurve 9300/9400 Series Routing Switches.

**NOTE:** ProCurve 9404M and ProCurve 9308M Routing Switches using basic management modules (M1) can contain 10000 routes by default. If you need to increase the capacity of the IP route table for OSPF, see the “Displaying and Modifying System Parameter Default Settings” section in the “Configuring Basic Features” chapter of the Installation and Getting Started Guide. ProCurve 9315M and 9408sl Routing Switches do not use basic management modules (M1).

### Overview of OSPF

OSPF is a link-state routing protocol. The protocol uses link-state advertisements (LSA) to update neighboring routers regarding its interfaces and information on those interfaces. The router floods these LSAs to all neighboring routers to update them regarding the interfaces. Each router maintains an identical database that describes its area topology to help a router determine the shortest path between it and any neighboring router.

ProCurve Routing Switches support the following types of LSAs, which are described in RFC 1583:

- Router link
- Network link
- Summary link
- Autonomous system (AS) summary link
- AS external link
- Not-So-Stubby Area (NSSA) external link

OSPF is built upon a hierarchy of network components. The highest level of the hierarchy is the **Autonomous System (AS)**. An autonomous system is defined as a number of networks, all of which share the same routing and administration characteristics.

An AS can be divided into multiple **areas** as shown in Figure 12.1 on page 12-2. Each area represents a collection of contiguous networks and hosts. Areas limit the area to which link-state advertisements are
broadcast, thereby limiting the amount of flooding that occurs within the network. An area is represented in OSPF by either an IP address or a number.

You can further limit the broadcast area of flooding by defining an area range. The area range allows you to assign an aggregate value to a range of IP addresses. This aggregate value becomes the address that is advertised instead all of the individual addresses it represents being advertised. You can assign up to 32 ranges in an OSPF area.

An OSPF router can be a member of multiple areas. Routers with membership in multiple areas are known as **Area Border Routers (ABRs)**. Each ABR maintains a separate topological database for each area the router is in. Each topological database contains all of the LSA databases for each router within a given area. The routers within the same area have identical topological databases. The ABR is responsible for forwarding routing information or changes between its border areas.

An **Autonomous System Boundary Router (ASBR)** is a router that is running multiple protocols and serves as a gateway to routers outside an area and those operating with different protocols. The ASBR is able to import and translate different protocol routes into OSPF through a process known as **redistribution**. For more details on redistribution and configuration examples, see "Enable Route Redistribution" on page 12-34.

**Figure 12.1  OSPF operating in a network**

**OSPF Point-to-Point Links**

OSPF point-to-point links are supported in software releases 07.8.00 and later on 10/100 and Gigabit Ethernet interfaces.
In an OSPF point-to-point network, where a direct Layer 3 connection exists between a single pair of OSPF routers, there is no need for Designated and Backup Designated Routers, as is the case in OSPF multi-access networks. Without the need for Designated and Backup Designated routers, a point-to-point network establishes adjacency and converges faster. The neighboring routers become adjacent whenever they can communicate directly. In contrast, in broadcast and non-broadcast multi-access (NBMA) networks, the Designated Router and Backup Designated Router become adjacent to all other routers attached to the network.

To configure an OSPF point-to-point link, see “Configuring an OSPF Point-to-Point Link” on page 12-46.

**Designated Routers in Multi-Access Networks**

In a network that has multiple routers attached, OSPF elects one router to serve as the designated router (DR) and another router on the segment to act as the backup designated router (BDR). This arrangement minimizes the amount of repetitive information that is forwarded on the network by forwarding all messages to the designated router and backup designated routers responsible for forwarding the updates throughout the network.

**Designated Router Election in Multi-Access Networks**

In a network with no designated router and no backup designated router, the neighboring router with the highest priority is elected as the DR, and the router with the next largest priority is elected as the BDR, as shown in Figure 12.2

**Figure 12.2 Designated and backup router election**

If the DR goes off-line, the BDR automatically becomes the DR. The router with the next highest priority becomes the new BDR. This process is shown in Figure 12.3.

**NOTE:** Priority is a configurable option at the interface level. You can use this parameter to help bias one router as the DR.
Figure 12.3  Backup designated router becomes designated router

If two neighbors share the same priority, the router with the highest router ID is designated as the DR. The router with the next highest router ID is designated as the BDR.

**NOTE:** By default, the HP router ID is the IP address configured on the lowest numbered loopback interface. If the Routing Switch does not have a loopback interface, the default router ID is the lowest numbered IP address configured on the device. For more information or to change the router ID, see "Changing the Router ID" on page 9-26.

When multiple routers on the same network are declaring themselves as DRs, then both priority and router ID are used to select the designated router and backup designated routers.

When only one router on the network claims the DR role despite neighboring routers with higher priorities or router IDs, this router remains the DR. This is also true for BDRs.

The DR and BDR election process is performed when one of the following events occurs:

- an interface is in a waiting state and the wait time expires
- an interface is in a waiting state and a hello packet is received that addresses the BDR
- a change in the neighbor state occurs, such as:
  - a neighbor state transitions from 2 or higher
  - communication to a neighbor is lost
  - a neighbor declares itself to be the DR or BDR for the first time

**OSPF RFC 1583 and 2178 Compliance**

HP routers are configured, by default, to be compliant with the RFC 1583 OSPF V2 specification. HP routers can also be configured to operate with the latest OSPF standard, RFC 2178.

**NOTE:** For details on how to configure the system to operate with the RFC 2178, see "Modify OSPF Standard Compliance Setting" on page 12-43.

**Reduction of Equivalent AS External LSAs**

An OSPF ASBR uses AS External link advertisements (AS External LSAs) to originate advertisements of a route to another routing domain, such as a BGP4 or RIP domain. The ASBR advertises the route to the external domain by flooding AS External LSAs to all the other OSPF routers (except those inside stub networks) within the local OSPF Autonomous System (AS).

In some cases, multiple ASBRs in an AS can originate equivalent LSAs. The LSAs are equivalent when they have the same cost, the same next hop, and the same destination. Software release 07.1.00 optimizes OSPF by
eliminating duplicate AS External LSAs in this case. The Routing Switch with the lower router ID flushes the duplicate External LSAs from its database and thus does not flood the duplicate External LSAs into the OSPF AS. AS External LSA reduction therefore reduces the size of the Routing Switch’s link state database.

This enhancement implements the portion of RFC 2328 that describes AS External LSA reduction. This enhancement is enabled by default, requires no configuration, and cannot be disabled.

Figure 12.4 shows an example of the AS External LSA reduction feature. In this example, ProCurve Routing Switches D and E are OSPF ASBRs, and thus communicate route information between the OSPF AS, which contains Routers A, B, and C, and another routing domain, which contains Router F. The other routing domain is running another routing protocol, such as BGP4 or RIP. Routers D, E, and F, therefore, are each running both OSPF and either BGP4 or RIP.

**Figure 12.4  AS External LSA reduction**

Notice that both Router D and Router E have a route to the other routing domain through Router F. In software releases earlier than 07.1.00, if Routers D and E have equal-cost routes to Router F, then both Router D and Router E flood AS External LSAs to Routers A, B, and C advertising the route to Router F. Since both routers are flooding equivalent routes, Routers A, B, and C receive multiple routes with the same cost to the same destination (Router F). For Routers A, B, and C, either route to Router F (through Router D or through Router E) is equally good.
OSPF eliminates the duplicate AS External LSAs. When two or more ProCurve Routing Switches configured as ASBRs have equal-cost routes to the same next-hop router in an external routing domain, the ASBR with the highest router ID floods the AS External LSAs for the external domain into the OSPF AS, while the other ASBRs flush the equivalent AS External LSAs from their databases. As a result, the overall volume of route advertisement traffic within the AS is reduced and the Routing Switches that flush the duplicate AS External LSAs have more memory for other OSPF data. In Figure 12.4, since Router D has a higher router ID than Router E, Router D floods the AS External LSAs for Router F to Routers A, B, and C. Router E flushes the equivalent AS External LSAs from its database.

**Algorithm for AS External LSA Reduction**

Figure 12.4 shows an example in which the normal AS External LSA reduction feature is in effect. The behavior changes under the following conditions:

- There is one ASBR advertising (originating) a route to the external destination, but one of the following happens:
  - A second ASBR comes on-line
  - A second ASBR that is already on-line begins advertising an equivalent route to the same destination.

In either case above, the router with the higher router ID floods the AS External LSAs and the other router flushes its equivalent AS External LSAs. For example, if Router D is offline, Router E is the only source for a route to the external routing domain. When Router D comes on-line, it takes over flooding of the AS External LSAs to Router F; while Router E flushes its equivalent AS External LSAs to Router F.

- One of the ASBRs starts advertising a route that is no longer equivalent to the route the other ASBR is advertising. In this case, the ASBRs each flood AS External LSAs. Since the LSAs either no longer have the same cost or no longer have the same next-hop router, the LSAs are no longer equivalent, and the LSA reduction feature no longer applies.

- The ASBR with the higher router ID becomes unavailable or is reconfigured so that it is no longer an ASBR. In this case, the other ASBR floods the AS External LSAs. For example, if Router D goes off-line, then Router E starts flooding the AS with AS External LSAs for the route to Router F.

**Support for OSPF RFC 2328 Appendix E**

Software release 07.5.04 and later provides support for Appendix E in OSPF RFC 2328. Appendix E describes a method to ensure that an OSPF router (such as a ProCurve Routing Switch) generates unique link state IDs for type-5 (External) link state advertisements (LSAs) in cases where two networks have the same network address but different network masks.

**NOTE:** Support for Appendix E of RFC 2328 is enabled automatically and cannot be disabled. No user configuration is required.

Normally, an OSPF router uses the network address alone for the link state ID of the link state advertisement (LSA) for the network. For example, if the router needs to generate an LSA for network 10.1.2.3 255.0.0.0, the router generates ID 10.1.2.3 for the LSA.

However, suppose that an OSPF router needs to generate LSAs for all the following networks:

- 10.0.0.0 255.0.0.0
- 10.0.0.0 255.255.0.0
- 10.0.0.0 255.255.255.0

All three networks have the same network address, 10.0.0.0. Without support for RFC 2328 Appendix E, an OSPF router uses the same link state ID, 10.0.0.0, for the LSAs for all three networks. For example, if the router generates an LSA with ID 10.0.0.0 for network 10.0.0.0 255.0.0.0, this LSA conflicts with the LSA generated for network 10.0.0.0 255.255.0.0 or 10.0.0.0 255.255.255.0. The result is multiple LSAs that have the same ID but that contain different route information.

When appendix E is supported, the router generates the link state ID for a network as follows:
1. Does an LSA with the network address as its ID already exist?
   - No – Use the network address as the ID.
   - Yes – Go to Step 2.

2. Compare the networks that have the same network address, to determine which network is more specific.
   The more specific network is the one that has more contiguous one bits in its network mask. For example, network 10.0.0.0 255.255.0.0 is more specific than network 10.0.0.0 255.0.0.0, because the first network has 16 ones bits (255.255.0.0) whereas the second network has only 8 ones bits (255.0.0.0).
   - For the less specific network, use the networks address as the ID.
   - For the more specific network, use the network’s broadcast address as the ID. The broadcast address is the network address, with all ones bits in the host portion of the address. For example, the broadcast address for network 10.0.0.0 255.255.0.0 is 10.0.0.255.

If this comparison results in a change to the ID of an LSA that has already been generated, the router generates a new LSA to replace the previous one. For example, if the router has already generated an LSA for network with ID 10.0.0.0 for network 10.0.0.0 255.255.255.0, the router must generate a new LSA for the network, if the router needs to generate an LSA for network 10.0.0.0 255.255.0.0 or 10.0.0.0 255.0.0.0.

Dynamic OSPF Activation and Configuration

OSPF is automatically activated when you enable it. The protocol does not require a software reload.

You can configure and save the following OSPF changes without resetting the system:
- all OSPF interface-related parameters (for example: area, hello timer, router dead time cost, priority, retransmission time, transit delay)
- all area parameters
- all area range parameters
- all virtual-link parameters
- all global parameters
- creation and deletion of an area, interface or virtual link

In addition, you can make the following changes without a system reset by first disabling and then re-enabling OSPF operation:
- changes to address ranges
- changes to global values for redistribution
- addition of new virtual links

You also can change the amount of memory allocated to various types of LSA entries. However, these changes require a system reset or reboot.

Dynamic OSPF Memory

Software release 07.1.00 and higher dynamically allocate memory for Link State Advertisements (LSAs) and other OSPF data structures.

In previous software releases, OSPF memory is statically allocated. If the Routing Switch runs out of memory for a given LSA type in releases earlier than 07.1.00, an overflow condition occurs and the software sends a message to the Syslog. To change memory allocation requires entering CLI commands and reloading the software.

Software release 07.1.00 and later eliminate the overflow conditions and do not require a reload to change OSPF memory allocation. So long as the Routing Switch has free (unallocated) dynamic memory, OSPF can use the memory.

Since dynamic memory allocation is automatic and requires no configuration, the following CLI commands and equivalent Web management options are not supported in software release 07.1.00:
Configuring OSPF

To begin using OSPF on the router, perform the steps outlined below:

1. Enable OSPF on the router.
2. Assign the areas to which the router will be attached.
3. Assign individual interfaces to the OSPF areas.
4. Define redistribution filters, if desired.
5. Enable redistribution, if you defined redistribution filters.
6. Modify default global and port parameters as required.
7. Modify OSPF standard compliance, if desired.

NOTE: OSPF is automatically enabled without a system reset.

Configuration Rules

- If a router is to operate as an ASBR, you must enable the ASBR capability at the system level.
- Redistribution must be enabled on routers configured to operate as ASBRs.
- All router ports must be assigned to one of the defined areas on an OSPF router. When a port is assigned to an area, all corresponding sub-nets on that port are automatically included in the assignment.

OSPF Parameters

You can modify or set the following global and interface OSPF parameters.

Global Parameters

- Modify OSPF standard compliance setting.
- Assign an area.
- Define an area range.
- Define the area virtual link.
- Set global default metric for OSPF.
- Change the reference bandwidth for the default cost of OSPF interfaces.
- Disable or re-enable load sharing.
• Enable or disable default-information-originate.
• Modify Shortest Path First (SPF) timers
• Define external route summarization
• Define redistribution metric type.
• Define deny redistribution.
• Define permit redistribution.
• Enable redistribution.
• Change the LSA pacing interval.
• Modify OSPF Traps generated.
• Modify database overflow interval.

**Interface Parameters**

• Assign interfaces to an area.
• Define the authentication key for the interface.
• Change the authentication-change interval
• Modify the cost for a link.
• Modify the dead interval.
• Modify MD5 authentication key parameters.
• Modify the priority of the interface.
• Modify the retransmit interval for the interface.
• Modify the transit delay of the interface.

**NOTE:** When using the CLI, you set global level parameters at the OSPF CONFIG Level of the CLI. To reach that level, enter `router ospf...` at the global CONFIG Level. Interface parameters for OSPF are set at the interface CONFIG Level using the CLI command, `ip ospf...`

When using the Web management interface, you set OSPF global parameters using the OSPF configuration panel. All other parameters are accessed through links accessed from the OSPF configuration sheet.

**Enable OSPF on the Router**

When you enable OSPF on the router, the protocol is automatically activated. To enable OSPF on the router, use one of the following methods:

**USING THE CLI**

```bash
ProCurveRS(config)# router ospf
```

This command launches you into the OSPF router level where you can assign areas and modify OSPF global parameters.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Select Enable next to OSPF.
3. Click the Apply button to save the change to the device's running-config file.
4. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.
**Note Regarding Disabling OSPF**

If you disable OSPF, the Routing Switch removes all the configuration information for the disabled protocol from the running-config. Moreover, when you save the configuration to the startup-config file after disabling one of these protocols, all the configuration information for the disabled protocol is removed from the startup-config file.

The CLI displays a warning message such as the following:

```
ProCurveRS(config-ospf-router)# no router ospf
router ospf mode now disabled. All ospf config data will be lost when writing to flash!
```

The Web management interface does not display a warning message.

If you have disabled the protocol but have not yet saved the configuration to the startup-config file and reloaded the software, you can restore the configuration information by re-entering the command to enable the protocol (ex: `router ospf`), or by selecting the Web management option to enable the protocol. If you have already saved the configuration to the startup-config file and reloaded the software, the information is gone.

If you are testing an OSPF configuration and are likely to disable and re-enable the protocol, you might want to make a backup copy of the startup-config file containing the protocol's configuration information. This way, if you remove the configuration information by saving the configuration after disabling the protocol, you can restore the configuration by copying the backup copy of the startup-config file onto the flash memory.

**Assign OSPF Areas**

Once OSPF is enabled on the system, you can assign areas. Assign an IP address or number as the *area ID* for each area. The area ID is representative of all IP addresses (sub-nets) on a router port. Each port on a router can support one area.

An area can be **normal**, a **stub**, or a **Not-So-Stubby Area (NSSA)**.

- Normal – OSPF routers within a normal area can send and receive External Link State Advertisements (LSAs).
- Stub – OSPF routers within a stub area cannot send or receive External LSAs. In addition, OSPF routers in a stub area must use a default route to the area’s Area Border Router (ABR) or Autonomous System Boundary Router (ASBR) to send traffic out of the area.
- NSSA – The ASBR of an NSSA can import external route information into the area.
  - ASBRs redistribute (import) external routes into the NSSA as type 7 LSAs. Type-7 External LSAs are a special type of LSA generated only by ASBRs within an NSSA, and are flooded to all the routers within only that NSSA.
  - ABRs translate type 7 LSAs into type 5 External LSAs, which can then be flooded throughout the AS. You can configure address ranges on the ABR of an NSSA so that the ABR converts multiple type-7 External LSAs received from the NSSA into a single type-5 External LSA.

When an NSSA contains more than one ABR, OSPF elects one of the ABRs to perform the LSA translation for NSSA. OSPF elects the ABR with the highest router ID. If the elected ABR becomes unavailable, OSPF automatically elects the ABR with the next highest router ID to take over translation of LSAs for the NSSA. The election process for NSSA ABRs is automatic.

**EXAMPLE:**

To set up the OSPF areas shown in Figure 12.1 on page 12-2, use one of the following methods.

**USING THE CLI**

```
ProCurveRS(config-ospf-router)# area 192.5.1.0
ProCurveRS(config-ospf-router)# area 200.5.0.0
ProCurveRS(config-ospf-router)# area 195.5.0.0
ProCurveRS(config-ospf-router)# area 0.0.0.0
ProCurveRS(config-ospf-router) write memory
```

*Syntax: area <num> | <ip-addr>*
The `<num> | <ip-addr>` parameter specifies the area number, which can be a number or in IP address format. If you specify an number, the number can be from 0 – 2,147,483,647.

**NOTE:** You can assign one area on a router interface. For example, if the system or chassis module has 16 ports, 16 areas are supported on the chassis or module.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-write access.
2. If you have not already enabled OSPF, enable it by clicking on the Enable radio button next to OSPF on the System configuration panel, then clicking Apply to apply the change.
3. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
4. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
5. Click on the **Area** link to display the OSPF Area configuration panel, as shown in the following figure.

![OSPF Area](image)

**NOTE:** If the device already has OSPF areas, a table listing the areas is displayed. Click the Modify button to the right of the row describing an area to change its configuration, or click the **Add Area** link to display the OSPF Area configuration panel.

6. Enter the area ID in the Area ID field. The ID can be a number or an IP address.
7. Select the area type by clicking on the radio button next to its description in the Type field. For example, to select NSSA, click next to NSSA.
8. If you are configuring a stub area or NSSA, enter a cost in the Stub Cost field. The parameter is required for those area types but is not required for normal areas. You can specify from 1 – 16777215. There is no default.
9. Click the Add button to add the area to the running-config file.
10. Select the **Save** link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

**Assign a Totally Stubby Area**

By default, the Routing Switch sends summary LSAs (LSA type 3) into stub areas. You can further reduce the number of link state advertisements (LSA) sent into a stub area by configuring the Routing Switch to stop sending summary LSAs (type 3 LSAs) into the area. You can disable the summary LSAs when you are configuring the stub area or later after you have configured the area.

This feature disables origination of summary LSAs, but the Routing Switch still accepts summary LSAs from OSPF neighbors and floods them to other neighbors. The Routing Switch can form adjacencies with other routers regardless of whether summarization is enabled or disabled for areas on each router.
When you enter a command or apply a Web management option to disable the summary LSAs, the change takes effect immediately. If you apply the option to a previously configured area, the Routing Switch flushes all of the summary LSAs it has generated (as an ABR) from the area.

**NOTE:** This feature applies only when the Routing Switch is configured as an Area Border Router (ABR) for the area. To completely prevent summary LSAs from being sent to the area, disable the summary LSAs on each OSPF router that is an ABR for the area.

This feature does not apply to Not So Stubby Areas (NSSAs).

To disable summary LSAs for a stub area, use the following CLI method.

**USING THE CLI**

To disable summary LSAs for a stub area, enter commands such as the following:

```
ProCurveRS(config-ospf-router)# area 40 stub 99 no-summary
```

**Syntax:** area <num> | <ip-addr> stub <cost> [no-summary]

The `<num>` | `<ip-addr>` parameter specifies the area number, which can be a number or in IP address format. If you specify a number, the number can be from 0 – 2,147,483,647.

The `stub` `<cost>` parameter specifies an additional cost for using a route to or from this area and can be from 1 – 16777215. There is no default. Normal areas do not use the cost parameter.

The `no-summary` parameter applies only to stub areas and disables summary LSAs from being sent into the area.

**NOTE:** You can assign one area on a router interface. For example, if the system or chassis module has 16 ports, 16 areas are supported on the chassis or module.

**USING THE WEB MANAGEMENT INTERFACE**

You can configure a stubby area using the Web management interface, but you cannot disable summary LSAs for the area. You must use the CLI to disable the summary LSAs.

**Assign a Not-So-Stubby Area (NSSA)**

The OSPF Not So Stubby Area (NSSA) feature enables you to configure OSPF areas that provide the benefits of stub areas, but that also are capable of importing external route information. OSPF does not flood external routes from other areas into an NSSA, but does translate and flood route information from the NSSA into other areas such as the backbone.

NSSAs are especially useful when you want to summarize Type-5 External LSAs (external routes) before forwarding them into an OSPF area. The OSPF specification (RFC 2328) prohibits summarization of Type-5 LSAs and requires OSPF to flood Type-5 LSAs throughout a routing domain. When you configure an NSSA, you can specify an address range for aggregating the external routes that the NSSA’s ABR exports into other areas.

The HP implementation of NSSA is based on RFC 1587.
Figure 12.5 shows an example of an OSPF network containing an NSSA.

**Figure 12.5  OSPF network containing an NSSA**

This example shows two routing domains, a RIP domain and an OSPF domain. The ASBR inside the NSSA imports external routes from RIP into the NSSA as Type-7 LSAs, which the ASBR floods throughout the NSSA.

The ABR translates the Type-7 LSAs into Type-5 LSAs. If an area range is configured for the NSSA, the ABR also summarizes the LSAs into an aggregate LSA before flooding the Type-5 LSA(s) into the backbone.

Since the NSSA is partially “stubby” the ABR does not flood external LSAs from the backbone into the NSSA. To provide access to the rest of the Autonomous System (AS), the ABR generates a default Type-7 LSA into the NSSA.

### Configuring an NSSA

To configure an NSSA, use one of the following methods.

**USING THE CLI**

To configure OSPF area 1.1.1.1 as an NSSA, enter the following commands.

```
ProCurveRS(config)# router ospf
ProCurveRS(config-ospf-router)# area 1.1.1.1 nssa 1
ProCurveRS(config-ospf-router)# write memory
```

**Syntax:** area <num> | <ip-addr> nssa <cost> | default-information-originate

The `<num>` | `<ip-addr>` parameter specifies the area number, which can be a number or in IP address format. If you specify an number, the number can be from 0 – 2,147,483,647.
The **nssa <cost>** command specifies that this is a Not-So-Stubby-Area (NSSA). The `<cost>` specifies an additional cost for using a route to or from this NSSA and can be from 1 – 16777215. There is no default. Normal areas do not use the cost parameter. Alternatively, you can use the **default-information-originate** command to configure the NSSA to inject the default route into the NSSA.

**NOTE:** The Routing Switch does not inject the default route into an NSSA by default.

**NOTE:** You can assign one area on a router interface. For example, if the system or chassis module has 16 ports, 16 areas are supported on the chassis or module.

To configure additional parameters for OSPF interfaces in the NSSA, use the **ip ospf area** command at the interface level of the CLI.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-write access.
2. If you have not already enabled OSPF, enable it by clicking on the Enable radio button next to OSPF on the System configuration panel, then clicking Apply to apply the change.
3. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
4. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
5. Click on the **Area** link to display the OSPF Area configuration panel, as shown in the following figure.

![OSPF Area Configuration Panel](Image)

**NOTE:** If the device already has OSPF areas, a table listing the areas is displayed. Click the Modify button to the right of the row describing an area to change its configuration, or click the **Add Area** link to display the OSPF Area configuration panel.

6. Enter the area ID in the Area ID field. The ID can be a number or an IP address.
7. Select NSSA by clicking on the radio button next to NSSA in the Type field.
8. Enter a cost in the Stub Cost field. This parameter is required. You can specify from 1 – 16777215. There is no default.
9. Click the Add button to add the area.
10. Select the **Save** link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

**Configuring an Address Range for the NSSA**

If you want the ABR that connects the NSSA to other areas to summarize the routes in the NSSA before translating them into Type-5 LSAs and flooding them into the other areas, configure an address range. The ABR creates an aggregate value based on the address range. The aggregate value becomes the address that the ABR advertises instead of advertising the individual addresses represented by the aggregate. You can configure up to 32 ranges in an OSPF area.
**USING THE CLI**

To configure an address range in NSSA 1.1.1.1, enter the following commands. This example assumes that you have already configured NSSA 1.1.1.1.

```
ProCurveRS(config)# router ospf
ProCurveRS(config-ospf-router)# area 1.1.1.1 range 209.157.22.1 255.255.0.0
ProCurveRS(config-ospf-router)# write memory
```

**Syntax:** `[no] area <num> | <ip-addr> range <ip-addr> <ip-mask> [advertise | not-advertise]

The `<num>` | `<ip-addr>` parameter specifies the area number, which can be in IP address format. If you specify a number, the number can be from 0 – 2,147,483,647.

The `range` `<ip-addr>` parameter specifies the IP address portion of the range. The software compares the address with the significant bits in the mask. All network addresses that match this comparison are summarized in a single route advertised by the router.

The `<ip-mask>` parameter specifies the portions of the IP address that a route must contain to be summarized in the summary route. In the example above, all networks that begin with 209.157 are summarized into a single route.

The `advertise` | `not-advertise` parameter specifies whether you want the Routing Switch to send type 3 LSAs for the specified range in this area. The default is `advertise`.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-write access.
2. If you have not already enabled OSPF, enable it by clicking on the Enable radio button next to OSPF on the System configuration panel, then clicking Apply to apply the change.
3. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
4. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
5. Click on the Area Range link to display the OSPF Area Range configuration panel.
6. Click on the Add Area Range link to display the following panel.

```
Area Range

<table>
<thead>
<tr>
<th>Area ID:</th>
<th>1.1.1.1</th>
<th>Network Address:</th>
<th>209.157.22.1</th>
<th>Mask:</th>
<th>255.255.0.0</th>
</tr>
</thead>
</table>

Add Delete Reset
```

**NOTE:** If the device already has an OSPF area range, a table listing the ranges is displayed. Click the Modify button to the right of the row describing a range to change its configuration, or click the Add Area Range link to display the OSPF Area Range configuration panel.

7. Enter the area ID in the Area ID field.
8. Enter an IP address in the Network Address field.
Assigning an Area Range (optional)

You can assign a range for an area, but it is not required. Ranges allow a specific IP address and mask to represent a range of IP addresses within an area, so that only that reference range address is advertised to the network, instead of all the addresses within that range. Each area can have up to 32 range addresses.

**USING THE CLI**

**EXAMPLE:**

To define an area range for sub-nets on 193.45.5.1 and 193.45.6.2, enter the following command:

```
ProCurveRS(config)# router ospf
ProCurveRS(config-ospf-router)# area 192.45.1 range 193.45.0.0 255.255.0.0
ProCurveRS(config-ospf-router)# area 193.45.6.2 range 193.45.0.0 255.255.0.0
```

**Syntax:** area <num> | <ip-addr> range <ip-addr> <ip-mask>

The `<num>` | `<ip-addr>` parameter specifies the area number, which can be in IP address format.

The `range <ip-addr>` parameter specifies the IP address portion of the range. The software compares the address with the significant bits in the mask. All network addresses that match this comparison are summarized in a single route advertised by the router.

The `<ip-mask>` parameter specifies the portions of the IP address that a route must contain to be summarized in the summary route. In the example above, all networks that begin with 193.45 are summarized into a single route.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-write access.
2. If you have not already enabled OSPF, enable it by clicking on the Enable radio button next to OSPF on the System configuration panel, then clicking Apply to apply the change.
3. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
4. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
5. Click on the Area Range link to display the OSPF Area Range configuration panel.
6. Click on the Add Area Range link to display the Area Range panel.

**NOTE:** If the device already has an OSPF area range, a table listing the ranges is displayed. Click the Modify button to the right of the row describing a range to change its configuration, or click the Add Area Range link to display the OSPF Area Range configuration panel.

7. Enter the area ID in the Area ID field.
8. Enter an IP address in the Network Address field.
9. Enter a network mask in the Mask field. The software compares the address with the significant bits in the mask. All network addresses that match this comparison are summarized in a single route advertised by the router.
10. Click the Add button to add the area.
11. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.
Assigning Interfaces to an Area

Once you define OSPF areas, you can assign interfaces the areas. All router ports must be assigned to one of the defined areas on an OSPF router. When a port is assigned to an area, all corresponding sub-nets on that port are automatically included in the assignment.

To assign interface 8 of Router A to area 192.5.0.0 and then save the changes, use one the following methods:

**USING CLI**

To assign interface 1/8 of Router A to area 192.5.0.0 and then save the changes, enter the following commands:

```
RouterA(config-ospf-router)# interface e 1/8
RouterA(config-if-1/8)# ip ospf area 192.5.0.0
RouterA(config-if-1/8)# write memory
```

**USING WEB MANAGEMENT INTERFACE**

All router ports must be assigned to one of the defined areas on an OSPF router. When a port is assigned to an area, all corresponding sub-nets on that port are automatically included in the assignment.

To assign an interface to an area:

1. Log on to the device using a valid user name and password for read-write access.
2. If you have not already enabled OSPF, enable it by clicking on the Enable radio button next to OSPF on the System configuration panel, then clicking Apply to apply the change.
3. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
4. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
5. Click on the Interface link.
   - If the device does not have any OSPF interfaces, the OSPF Interface configuration panel is displayed, as shown in the following example.
   - If an OSPF interface is already configured and you are adding a new one, click on the Add OSPF Interface link to display the OSPF Interface configuration panel, as shown in the following example.
   - If you are modifying an existing OSPF interface, click on the Modify button to the right of the row describing the interface to display the OSPF Interface configuration panel, as shown in the following example.
1. Select the port (and slot if applicable) to be assigned to the area from the Port and Slot pulldown menus.
2. Select the IP address of the area to which the interface is to be assigned from the Area ID pull down menu.

**NOTE:** You must configure the area before you can assign interfaces to it.

3. Select the Enable option of the OSPF mode parameter to enable OSPF on the interface.
4. Click the Add button to save the change to the device’s running-config file.
5. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

**Modify Interface Defaults**

OSPF has interface parameters that you can configure. For simplicity, each of these parameters has a default value. No change to these default values is required except as needed for specific network configurations.

**USING THE CLI**

Port default values can be modified using the following CLI commands at the interface configuration level of the CLI:

- `ip ospf area <ip-addr>`
- `ip ospf auth-change-wait-time <secs>`
- `ip ospf authentication-key [0 | 1] <string>`
- `ip ospf cost <num>`
- `ip ospf dead-interval <value>`
- ip ospf hello-interval <value>
- ip ospf md5-authentication key-activation-wait-time <num> | key-id <num> [0 | 1] key <string>
- ip ospf passive
- ip ospf priority <value>
- ip ospf retransmit-interval <value>
- ip ospf transmit-delay <value>

For a complete description of these parameters, see the summary of OSPF port parameters in the next section.

**USING THE WEB MANAGEMENT INTERFACE**

To modify OSPF port parameters when using the Web:

1. Log on to the device using a valid user name and password for read-write access.
2. If you have not already enabled OSPF, enable it by clicking on the Enable radio button next to OSPF on the System configuration panel, then clicking Apply to apply the change.
3. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
4. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
5. Click on the Interface link.

**NOTE:** If the device already has OSPF interfaces, a table listing the interfaces is displayed. Click the Modify button to the right of the row describing the interface to change its configuration, or click the Add OSPF Interface link to display the OSPF Interface configuration panel.

6. Select the port (and slot if applicable) from the pulldown menu(s).
7. Select the area ID from the Area ID pulldown menu.
8. Select the OSPF mode to enable or disable OSPF on the interface.
9. Click on the checkbox next to Passive if you do not want the interface to send or receive OSPF route updates. By default, all OSPF interfaces are active and thus can send and receive OSPF route information. Since a passive interface does not send or receive route information, the interface is in effect a stub network. OSPF interfaces are active by default.
10. Select the authentication method for the interface from the pulldown menu. Options are None, Simple, or MD5.

**NOTE:** If you select MD5 as the authentication method, enter a value for the MD5 authentication ID, key and key activation time in the associated fields. If you select Simple, enter an authentication key. If you select No Authentication as the authentication method, you do not need to specify anything in the Simple and MD5 fields.

11. Modify the default values of the following interface parameters as needed: hello interval, retransmit interval, transmit delay, dead interval, priority, and cost.
12. Click the Add button (if you are adding a new neighbor) or the Modify button (if you are modifying a neighbor that is already configured) to apply the changes to the device’s running-config file.
13. Select the Save link at the bottom of the dialog, then select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

**OSPF Interface Parameters**

The following parameters apply to OSPF interfaces.

*Area:* Assigns an interface to a specific area. You can assign either an IP address or number to represent an OSPF Area ID. If you assign a number, it can be any value from 0 – 2,147,483,647.
**Auth-change-wait-time:** OSPF gracefully implements authentication changes to allow all routers to implement the change and thus prevent disruption to neighbor adjacencies. During the authentication-change interval, both the old and new authentication information is supported. The default authentication-change interval is 300 seconds (5 minutes). You change the interval to a value from 0 – 14400 seconds.

**Authentication-key:** OSPF supports three methods of authentication for each interface—none, simple password, and MD5. Only one method of authentication can be active on an interface at a time. The default authentication value is none, meaning no authentication is performed.

- The simple password method of authentication requires you to configure an alphanumeric password on an interface. The simple password setting takes effect immediately. All OSPF packets transmitted on the interface contain this password. Any OSPF packet received on the interface is checked for this password. If the password is not present, then the packet is dropped. The password can be up to eight characters long.
- The MD5 method of authentication requires you to configure a key ID and an MD5 Key. The key ID is a number from 1 – 255 and identifies the MD5 key that is being used. The MD5 key can be up to sixteen alphanumeric characters long.

**Cost:** Indicates the overhead required to send a packet across an interface. You can modify the cost to differentiate between 100 Mbps and 1000 Mbps (1 Gbps) links. The default cost is calculated by dividing 100 million by the bandwidth. For 10 Mbps links, the cost is 10. The cost for both 100 Mbps and 1000 Mbps links is 1, because the speed of 1000 Mbps was not in use at the time the OSPF cost formula was devised.

**Dead-interval:** Indicates the number of seconds that a neighbor router waits for a hello packet from the current router before declaring the router down. The value can be from 1 – 65535 seconds. The default is 40 seconds.

**Hello-interval:** Represents the length of time between the transmission of hello packets. The value can be from 1 – 65535 seconds. The default is 10 seconds.

**MD5-authentication activation wait time:** The number of seconds the Routing Switch waits until placing a new MD5 key into effect. The wait time provides a way to gracefully transition from one MD5 key to another without disturbing the network. The wait time can be from 0 – 14400 seconds. The default is 300 seconds (5 minutes).

**MD5-authentication key ID and key:** A method of authentication that requires you to configure a key ID and an MD5 key. The key ID is a number from 1 – 255 and identifies the MD5 key that is being used. The MD5 key consists of up to 16 alphanumeric characters. The MD5 is encrypted and included in each OSPF packet transmitted.

**Passive:** When you configure an OSPF interface to be passive, that interface does not send or receive OSPF route updates. By default, all OSPF interfaces are active and thus can send and receive OSPF route information. Since a passive interface does not send or receive route information, the interface is in effect a stub network. OSPF interfaces are active by default.

**NOTE:** This option affects all IP sub-nets configured on the interface. If you want to disable OSPF updates only on some of the IP sub-nets on the interface, use the `ospf-ignore` or `ospf-passive` parameter with the `ip address` command. See “Assigning an IP Address to an Ethernet Port” on page 9-16.

**Priority:** Allows you to modify the priority of an OSPF router. The priority is used when selecting the designated router (DR) and backup designated routers (BDRs). The value can be from 0 – 255. The default is 1. If you set the priority to 0, the Routing Switch does not participate in DR and BDR election.

**Retransmit-interval:** The time between retransmissions of link-state advertisements (LSAs) to adjacent routers for this interface. The value can be from 0 – 3600 seconds. The default is 5 seconds.

**Transit-delay:** The time it takes to transmit Link State Update packets on this interface. The value can be from 0 – 3600 seconds. The default is 1 second.

**Encrypted Display of the Authentication String or MD5 Authentication Key**
The optional `0 | 1` parameter with the `authentication-key` and `md5-authentication key-id` parameters affects encryption.

For added security, software release 07.1.10 and later encrypts display of the password or authentication string. Encryption is enabled by default. The software also provides an optional parameter to disable encryption of a password or authentication string, on an individual OSPF area or OSPF interface basis.
When encryption of the passwords or authentication strings is enabled, they are encrypted in the CLI regardless of the access level you are using. In the Web management interface, the passwords or authentication strings are encrypted at the read-only access level but are visible at the read-write access level.

The encryption option can be omitted (the default) or can be one of the following.

- **0** – Disables encryption for the password or authentication string you specify with the command. The password or string is shown as clear text in the running-config and the startup-config file. Use this option if you do not want display of the password or string to be encrypted.
- **1** – Assumes that the password or authentication string you enter is the encrypted form, and decrypts the value before using it.

**NOTE:** If you want the software to assume that the value you enter is the clear-text form, and to encrypt display of that form, do not enter 0 or 1. Instead, omit the encryption option and allow the software to use the default behavior.

If you specify encryption option 1, the software assumes that you are entering the encrypted form of the password or authentication string. In this case, the software decrypts the password or string you enter before using the value for authentication. If you accidentally enter option 1 followed by the clear-text version of the password or string, authentication will fail because the value used by the software will not match the value you intended to use.

---

**Change the Timer for OSPF Authentication Changes**

When you make an OSPF authentication change, the software uses the authentication-change timer to gracefully implement the change. The software implements the change in the following ways:

- **Outgoing OSPF packets** – After you make the change, the software continues to use the old authentication to send packets, during the remainder of the current authentication-change interval. After this, the software uses the new authentication for sending packets.
- **Inbound OSPF packets** – The software accepts packets containing the new authentication and continues to accept packets containing the older authentication for two authentication-change intervals. After the second interval ends, the software accepts packets only if they contain the new authentication key.

The default authentication-change interval is 300 seconds (5 minutes). You change the interval to a value from 0 – 14400 seconds.

OSPF provides graceful authentication change for all the following types of authentication changes in OSPF:

- Changing authentication methods from one of the following to another of the following:
  - Simple text password
  - MD5 authentication
  - No authentication
- Configuring a new simple text password or MD5 authentication key
- Changing an existing simple text password or MD5 authentication key

**USING THE CLI**

To change the authentication-change interval, enter a command such as the following at the interface configuration level of the CLI:

```
ProCurveRS(config-if-2/5)# ip ospf auth-change-wait-time 400
```

**Syntax:** `[no] ip ospf auth-change-wait-time <secs>`

The `<secs>` parameter specifies the interval and can be from 0 – 14400 seconds. The default is 300 seconds (5 minutes).
NOTE: For backward compatibility, the `ip ospf md5-authentication key-activation-wait-time <seconds>` command is still supported.

**Block Flooding of Outbound LSAs on Specific OSPF Interfaces**

By default, the Routing Switch floods all outbound LSAs on all the OSPF interfaces within an area. You can configure a filter to block outbound LSAs on an OSPF interface. This feature is particularly useful when you want to block LSAs from some, but not all, of the interfaces attached to the area.

After you apply filters to block the outbound LSAs, the filtering occurs during the database synchronization and flooding.

If you remove the filters, the blocked LSAs are automatically re-flooded. You do not need to reset OSPF to re-flood the LSAs.

NOTE: You cannot block LSAs on virtual links.

**USING THE CLI**

To apply a filter to an OSPF interface to block flooding of outbound LSAs on the interface, enter the following command at the Interface configuration level for that interface.

```
ProCurveRS(config-if-1/1)# ip ospf database-filter all out
```

The command in this example blocks all outbound LSAs on the OSPF interface configured on port 1/1.

**Syntax:** `[no] ip ospf database-filter all out`

To remove the filter, enter a command such as the following:

```
ProCurveRS(config-if-1/1)# no ip ospf database-filter all out
```

**USING THE WEB MANAGEMENT INTERFACE**

You cannot configure filters to block flooding on OSPF interfaces using the Web management interface.

**Assign Virtual Links**

All ABRs (area border routers) must have either a direct or indirect link to the OSPF backbone area (0.0.0.0 or 0). If an ABR does not have a physical link to the area backbone, the ABR can configure a virtual link to another router within the same area, which has a physical connection to the area backbone.

The path for a virtual link is through an area shared by the neighbor ABR (router with a physical backbone connection), and the ABR requiring a logical connection to the backbone.

Two parameters fields must be defined for all virtual links—transit area ID and neighbor router.

- The **transit area ID** represents the shared area of the two ABRs and serves as the connection point between the two routers. This number should match the area ID value.

- The **neighbor router** field is the router ID (IP address) of the router that is physically connected to the backbone, when assigned from the router interface requiring a logical connection. When assigning the parameters from the router with the physical connection, the router ID is the IP address of the router requiring a logical connection to the backbone.

NOTE: By default, the HP router ID is the IP address configured on the lowest numbered loopback interface. If the Routing Switch does not have a loopback interface, the default router ID is the lowest numbered IP address configured on the device. For more information or to change the router ID, see “Changing the Router ID” on page 9-26.
**NOTE:** When you establish an area virtual link, you must configure it on both of the routers (both ends of the virtual link).

---

**Figure 12.6** Defining OSPF virtual links within a network

![Diagram showing OSPF virtual links](image)

---

**USING THE CLI**

**EXAMPLE:**

Figure 12.6 shows an OSPF area border router, 9308A, that is cut off from the backbone area (area 0). To provide backbone access to 9308A, you can add a virtual link between 9308A and 9308C using area 1 as a transit area. To configure the virtual link, you define the link on the router that is at each end of the link. No configuration for the virtual link is required on the routers in the transit area.

To define the virtual link on 9308A, enter the following commands:

```
ProCurveRSA(config-ospf-router)# area 1 virtual-link 209.157.22.1
ProCurveRSA(config-ospf-router)# write memory
```

Enter the following commands to configure the virtual link on 9308C:

```
ProCurveRSC(config-ospf-router)# area 1 virtual-link 10.0.0.1
ProCurveRSC(config-ospf-router)# write memory
```

**Syntax:** area <ip-addr> | <num> virtual-link <router-id>
[authentication-key | dead-interval | hello-interval | retransmit-interval | transmit-delay <value>]

The `area <ip-addr> | <num>` parameter specifies the transit area.
The <router-id> parameter specifies the router ID of the OSPF router at the remote end of the virtual link. To display the router ID on a ProCurve Routing Switch, enter the show ip command.

See “Modify Virtual Link Parameters” on page 12-25 for descriptions of the optional parameters.

**USING THE WEB MANAGEMENT INTERFACE**

To configure a virtual link:

1. Log on to the device using a valid user name and password for read-write access.
2. If you have not already enabled OSPF, enable it by clicking on the Enable radio button next to OSPF on the System configuration panel, then clicking Apply to apply the change.
3. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
4. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
5. Click on the Virtual Link link.

   - If the device does not have any OSPF virtual links, the OSPF Virtual Link Interface configuration panel is displayed, as shown in the following example.
   - If an OSPF virtual link is already configured and you are adding a new one, click on the Add OSPF Virtual Link link to display the OSPF Virtual Link Interface configuration panel, as shown in the following example.
   - If you are modifying an existing OSPF virtual link, click on the Modify button to the right of the row describing the virtual link to display the OSPF Virtual Link Interface configuration panel, as shown in the following example.

![OSPF Virtual Link Interface](image)

6. Select the transit area ID from the pulldown menu. The transit area is the area ID of the area shared by both routers.
7. Select an authentication method from the pulldown menu. If you select Simple, enter the authentication key in the appropriate field. If you select MD5, enter the MD5 authentication ID, key, and wait time.
NOTE: For descriptions of the authentication parameters, see “Modify Virtual Link Parameters” on page 12-25.

8. Enter the router ID of the neighbor router.

9. Modify the default settings of the following parameters if needed: hello interval, transit delay, retransmit interval and, dead interval.

NOTE: For a description of all virtual link parameters and their possible values, see “Modify Virtual Link Parameters” on page 12-25.

10. Click Add to save the change to the device’s running-config file.

11. Select the Save link at the bottom of the dialog, then select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

12. Log onto the neighbor router and configure the other end of the virtual link.

Modify Virtual Link Parameters

OSPF has some parameters that you can modify for virtual links. Notice that these are the same parameters as the ones you can modify for physical interfaces.

USING THE CLI

You can modify default values for virtual links using the following CLI command at the OSPF router level of the CLI, as shown in the following syntax:

Syntax: area <num> | <ip-addr> virtual-link <ip-addr> [authentication-key [0 | 1] <string>] [dead-interval <num>] [hello-interval <num>] [md5-authentication key-activation wait-time <num>] [key-id <num> [0 | 1] key <string>] [retransmit-interval <num>] [transmit-delay <num>]

The parameters are described below. For syntax information, see the Command Line Interface Reference for ProCurve 9300/9400 Series Routing Switches.

USING THE WEB MANAGEMENT INTERFACE

To modify virtual link default values:

1. Log on to the device using a valid user name and password for read-write access.

2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.

3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.

4. Click on the Virtual Link link to display a table listing the virtual links.

5. Click on the Modify button to the right of the row describing the virtual link you want to modify. The OSPF Virtual Link Interface configuration panel is displayed.

6. Modify the parameters as needed. (See the following section for descriptions of the parameters.)

7. Click Add to save the change to the device’s running-config file.

8. Select the Save link at the bottom of the dialog, then select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

9. Log on to the neighbor router and configure parameter changes to match those configured for the local router.

Virtual Link Parameter Descriptions

You can modify the following virtual link interface parameters:

Authentication Key: This parameter allows you to assign different authentication methods on a port-by-port basis. OSPF supports three methods of authentication for each interface—none, simple password, and MD5. Only one method of authentication can be active on an interface at a time.
The simple password method of authentication requires you to configure an alphanumeric password on an interface. The password can be up to eight characters long. The simple password setting takes effect immediately. All OSPF packets transmitted on the interface contain this password. All OSPF packets received on the interface are checked for this password. If the password is not present, then the packet is dropped.

The MD5 method of authentication encrypts the authentication key you define. The authentication is included in each OSPF packet transmitted.

**MD5 Authentication Key**: When simple authentication is enabled, the key is an alphanumeric password of up to eight characters. When MD5 is enabled, the key is an alphanumeric password of up to 16 characters that is later encrypted and included in each OSPF packet transmitted. You must enter a password in this field when the system is configured to operate with either simple or MD5 authentication.

**MD5 Authentication Key ID**: The Key ID is a number from 1 – 255 and identifies the MD5 key that is being used. This parameter is required to differentiate among multiple keys defined on a router.

**MD5 Authentication Wait Time**: This parameter determines when a newly configured MD5 authentication key is valid. This parameter provides a graceful transition from one MD5 key to another without disturbing the network. All new packets transmitted after the key activation wait time interval use the newly configured MD5 Key. OSPF packets that contain the old MD5 key are accepted for up to five minutes after the new MD5 key is in operation.

The range for the key activation wait time is from 0 – 14400 seconds. The default value is 300 seconds.

**Hello Interval**: The length of time between the transmission of hello packets. The range is 1 – 65535 seconds. The default is 10 seconds.

**Retransmit Interval**: The interval between the re-transmission of link state advertisements to router adjacencies for this interface. The range is 0 – 3600 seconds. The default is 5 seconds.

**Transmit Delay**: The period of time it takes to transmit Link State Update packets on the interface. The range is 0 – 3600 seconds. The default is 1 second.

**Dead Interval**: The number of seconds that a neighbor router waits for a hello packet from the current router before declaring the router down. The range is 1 – 65535 seconds. The default is 40 seconds.

**Encrypted Display of the Authentication String or MD5 Authentication Key**

The optional 0 | 1 parameter with the authentication-key and md5-authentication key-id parameters affects encryption.

For added security, software release 07.1.10 and later encrypts display of the password or authentication string. Encryption is enabled by default. The software also provides an optional parameter to disable encryption of a password or authentication string, on an individual OSPF area or OSPF interface basis.

When encryption of the passwords or authentication strings is enabled, they are encrypted in the CLI regardless of the access level you are using. In the Web management interface, the passwords or authentication strings are encrypted at the read-only access level but are visible at the read-write access level.

The encryption option can be omitted (the default) or can be one of the following.

- **0** – Disables encryption for the password or authentication string you specify with the command. The password or string is shown as clear text in the running-config and the startup-config file. Use this option of you do not want display of the password or string to be encrypted.

- **1** – Assumes that the password or authentication string you enter is the encrypted form, and decrypts the value before using it.

**NOTE**: If you want the software to assume that the value you enter is the clear-text form, and to encrypt display of that form, do not enter 0 or 1. Instead, omit the encryption option and allow the software to use the default behavior.

If you specify encryption option 1, the software assumes that you are entering the encrypted form of the password or authentication string. In this case, the software decrypts the password or string you enter before using the value for authentication. If you accidentally enter option 1 followed by the clear-text version of the password or string, authentication will fail because the value used by the software will not match the value you intended to use.
Changing the Reference Bandwidth for the Cost on OSPF Interfaces

Each interface on which OSPF is enabled has a cost associated with it. The Routing Switch advertises its interfaces and their costs to OSPF neighbors. For example, if an interface has an OSPF cost of ten, the Routing Switch advertises the interface with a cost of ten to other OSPF routers.

By default, an interface’s OSPF cost is based on the port speed of the interface. The cost is calculated by dividing the reference bandwidth by the port speed. The default reference bandwidth is 100 Mbps, which results in the following default costs:

- 10 Mbps port – 10
- All other port speeds – 1

You can change the reference bandwidth, to change the costs calculated by the software.

The software uses the following formula to calculate the cost:

\[
\text{Cost} = \frac{\text{reference-bandwidth}}{\text{interface-speed}}
\]

If the resulting cost is less than 1, the software rounds the cost up to 1. The default reference bandwidth results in the following costs:

- 10 Mbps port's cost = 100/10 = 10
- 100 Mbps port's cost = 100/100 = 1
- 1000 Mbps port's cost = 100/1000 = 0.10, which is rounded up to 1
- 155 Mbps port's cost = 100/155 = 0.65, which is rounded up to 1
- 622 Mbps port's cost = 100/622 = 0.16, which is rounded up to 1
- 2488 Mbps port's cost = 100/2488 = 0.04, which is rounded up to 1

The bandwidth for interfaces that consist of more than one physical port is calculated as follows:

- Trunk group – The combined bandwidth of all the ports.
- Virtual interface – The combined bandwidth of all the ports in the port-based VLAN that contains the virtual interface.

The default reference bandwidth is 100 Mbps. You can change the reference bandwidth to a value from 1 – 4294967.

If a change to the reference bandwidth results in a cost change to an interface, the Routing Switch sends a link-state update to update the costs of interfaces advertised by the Routing Switch.

**NOTE:** If you specify the cost for an individual interface, the cost you specify overrides the cost calculated by the software.

Interface Types To Which the Reference Bandwidth Does Not Apply

Some interface types are not affected by the reference bandwidth and always have the same cost regardless of the reference bandwidth in use:

- The cost of a loopback interface is always 0.
- The cost of a virtual link is calculated using the Shortest Path First (SPF) algorithm and is not affected by the auto-cost feature.
- The bandwidth for tunnel interfaces is 9 Kbps and is not affected by the auto-cost feature.

Changing the Reference Bandwidth

To change reference bandwidth, use the following CLI method.

**USING THE CLI**

To change the reference bandwidth, enter a command such as the following at the OSPF configuration level of the CLI:

---

June 2005
ProCurveRS(config-ospf-router)# auto-cost reference-bandwidth 500

The reference bandwidth specified in this example results in the following costs:

- 10 Mbps port's cost = 500/10 = 50
- 100 Mbps port's cost = 500/100 = 5
- 1000 Mbps port's cost = 500/1000 = 0.5, which is rounded up to 1
- 155 Mbps port's cost = 500/155 = 3.23, which is rounded up to 4
- 622 Mbps port's cost = 500/622 = 0.80, which is rounded up to 1
- 2488 Mbps port's cost = 500/2488 = 0.20, which is rounded up to 1

The costs for 10 Mbps, 100 Mbps, and 155 Mbps ports change as a result of the changed reference bandwidth. Costs for higher-speed interfaces remain the same.

**Syntax:** [no] auto-cost reference-bandwidth <num>

The <num> parameter specifies the reference bandwidth and can be a value from 1 – 4294967. The default is 100, which results in the same costs as previous software releases.

To restore the reference bandwidth to its default value and thus restore the default costs of interfaces to their default values, enter the following command:

ProCurveRS(config-ospf-router)# no auto-cost reference-bandwidth

**Define Redistribution Filters**

Route redistribution imports and translates different protocol routes into a specified protocol type. On HP routers, redistribution is supported for static routes, OSPF, RIP, and BGP4. When you configure redistribution for RIP, you can specify that static, OSPF, or BGP4 routes are imported into RIP routes. Likewise, OSPF redistribution supports the import of static, RIP, and BGP4 routes into OSPF routes. BGP4 supports redistribution of static, RIP, and OSPF routes into BGP4.

**NOTE:** The Routing Switch advertises the default route into OSPF even if redistribution is not enabled, and even if the default route is learned through an IBGP neighbor. IBGP routes (including the default route) are not redistributed into OSPF by OSPF redistribution (for example, by the OSPF redistribute command).

In Figure 12.7 on page 12-29, an administrator wants to configure the 9308M Routing Switch acting as the ASBR (Autonomous System Boundary Router) between the RIP domain and the OSPF domain to redistribute routes between the two domains.

**NOTE:** The ASBR must be running both RIP and OSPF protocols to support this activity.

To configure for redistribution, define the redistribution tables with deny and permit redistribution filters.

- If you are using the CLI, use the **deny** and **permit** redistribute commands for OSPF at the OSPF router level.
- If you are using the Web management interface, click on the plus sign next to Configure in the tree view, click on the plus sign next to OSPF, then select the **Redistribution Filter** link from the OSPF configuration sheet.

**NOTE:** Do not enable redistribution until you have configured the redistribution filters. If you enable redistribution before you configure the redistribution filters, the filters will not take effect and all routes will be distributed.
**Figure 12.7** Redistributing OSPF and static routes to RIP routes

**USING THE CLI**

**EXAMPLE:**
To configure the 9308M Routing Switch acting as an ASBR in Figure 12.7 to redistribute OSPF, BGP4, and static routes into RIP, enter the following commands:

```
ProCurveRSASBR(config)# router rip
ProCurveRSASBR(config-rip-router)# permit redistribute 1 all
ProCurveRSASBR(config-rip-router)# write memory
```

**NOTE:** Redistributioin is permitted for all routes by default, so the `permit redistribute 1 all` command in the example above is shown for clarity but is not required.

You also have the option of specifying import of just OSPF, BGP4, or static routes, as well as specifying that only routes for a specific network or with a specific cost (metric) be imported, as shown in the command syntax below:

**Syntax:**
```
deny | permit redistribute <filter-num> all | bgp | connected | rip | static
    [address <ip-addr> <ip-mask> [match-metric <value> [set-metric <value>]]]
```
EXAMPLE:
To redistribute RIP, static, and BGP4 routes into OSPF, enter the following commands on the Routing Switch acting as an ASBR:

ProCurveRSASBR(config)# router ospf
ProCurveRSASBR(config-ospf-router)# permit redistribute 1 all
ProCurveRSASBR(config-ospf-router)# write memory

Syntax: deny | permit redistribute <filter-num> all | bgp | connected | rip | static
         address <ip-address> <ip-mask>
         [match-metric <value>] | set-metric <value>

NOTE: Redistribution is permitted for all routes by default, so the permit redistribute 1 all command in the example above is shown for clarity but is not required.

You also have the option of specifying import of just OSPF, BGP4, or static routes, as well as specifying that only routes for a specific network or with a specific cost (metric) be imported, as shown in the command syntax below:

Syntax: [no] redistribution bgp | connected | rip | static [route-map <map-name>]

For example, to enable redistribution of RIP and static IP routes into OSPF, enter the following commands.

ProCurveRS(config)# router ospf
ProCurveRS(config-ospf-router)# redistribution rip
ProCurveRS(config-ospf-router)# redistribution static
ProCurveRS(config-ospf-router)# write memory

NOTE: The redistribution command does not perform the same function as the permit redistribute and deny redistribute commands. The redistribute commands allow you to control redistribution of routes by filtering on the IP address and network mask of a route. The redistribution commands enable redistribution for routes of specific types (static, directly connected, and so on). Configure all your redistribution filters before enabling redistribution.

NOTE: Do not enable redistribution until you have configured the redistribution filters. If you enable redistribution before you configure the redistribution filters, the filters will not take affect and all routes will be distributed.

USING THE WEB MANAGEMENT INTERFACE

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
4. Click on the Redistribution Filter link.
   - If the device does not have any OSPF redistribution filters, the OSPF Redistribution Filter configuration panel is displayed, as shown in the following example.
   - If an OSPF redistribution filter is already configured and you are adding a new one, click on the Add Redistribution Filter link to display the OSPF Redistribution Filter configuration panel, as shown in the following example.
5. If you are modifying an existing OSPF redistribution filter, click on the Modify button to the right of the row describing the filter to display the OSPF Redistribution Filter configuration panel, as shown in the following example.

![OSPF Redistribution Filter](image)

6. Optionally, enter the IP address and mask if you want to filter the redistributed routes for a specific network range.

7. Optionally, enter the filter ID or accept the ID value in the Filter ID field.

8. Optionally, select the filter action, Deny or Permit. The default is Permit.

9. Optionally, select the types of routes the filter applies to in the Protocol section. You can select one of the following:
   - All (the default)
   - Static
   - RIP
   - BGP
   - Connected

10. Optionally, enable matching on RIP metric and enter the metric.

11. Optionally, enable setting the OSPF metric for the imported routes and specify the metric.

12. Click the Add button to apply the filter to the device’s running-config file.

13. Select the Save link at the bottom of the dialog, then select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

**Prevent Specific OSPF Routes from Being Installed in the IP Route Table**

By default, all OSPF routes in the OSPF route table are eligible for installation in the IP route table. You can configure a distribution list to explicitly deny specific routes from being eligible for installation in the IP route table.

**NOTE:** This feature does not block receipt of LSAs for the denied routes. The Routing Switch still receives the routes and installs them in the OSPF database. The feature only prevents the software from installing the denied OSPF routes into the IP route table.
To configure an OSPF distribution list:

- Configure a standard or extended ACL that identifies the routes you want to deny. Using a standard ACL lets you deny routes based on the destination network, but does not filter based on the network mask. To also filter based on the destination network’s network mask, use an extended ACL.

- Configure an OSPF distribution list that uses the ACL as input.

**NOTE:** If you change the ACL after you configure the OSPF distribution list, you must clear the IP route table to place the changed ACL into effect. To clear the IP route table, enter the `clear ip route` command at the Privileged EXEC level of the CLI.

### USING THE CLI

The following sections show how to use the CLI to configure an OSPF distribution list. Separate examples are provided for standard and extended ACLs.

**NOTE:** The examples show named ACLs. However, you also can use a numbered ACL as input to the OSPF distribution list.

#### Using a Standard ACL as Input to the Distribution List

To use a standard ACL to configure an OSPF distribution list for denying specific routes, enter commands such as the following:

```
ProCurveRS(config)# ip access-list standard no_ip
ProCurveRS(config-standard-nacl)# deny 4.0.0.0 0.255.255.255
ProCurveRS(config-standard-nacl)# permit any any
ProCurveRS(config-standard-nacl)# exit
ProCurveRS(config)# router ospf
ProCurveRS(config-ospf-router)# distribute-list no_ip in
```

The first three commands configure a standard ACL that denies routes to any 4.x.x.x destination network and allows all other routes for eligibility to be installed in the IP route table. The last three commands change the CLI to the OSPF configuration level and configure an OSPF distribution list that uses the ACL as input. The distribution list prevents routes to any 4.x.x.x destination network from entering the IP route table. The distribution list does not prevent the routes from entering the OSPF database.

**Syntax:** [no] distribute-list <acl-name> | <acl-id> in [<interface type>] [<interface number>]

**Syntax:** [no] ip access-list standard <acl-name> | <acl-id>

**Syntax:** deny | permit <source-ip> <wildcard>

The `<acl-name> | <acl-id>` parameter specifies the ACL name or ID.

The `in` command applies the ACL to incoming route updates.

The `<interface type>` parameter is available in release 07.6.04 and later releases of these branch releases. It identifies the interface type (i.e., `e` (ethernet) or `ve` (virtual)) on which to apply the ACL.

The `<interface number>` parameter is available in release 07.6.04 and later releases of these branch releases. It specifies the interface number on which to apply the ACL. Enter only one valid interface number. If necessary, use the `show interface brief` command to display a list of valid interfaces. If you do not specify an interface, the HP device applies the ACL to all incoming route updates.

If you do not specify an interface type and interface number, the device applies the OSPF distribution list to all incoming route updates.

The `deny | permit` parameter indicates whether packets that match the policy are dropped or forwarded.

The `<source-ip>` parameter specifies the source address for the policy. Since this ACL is input to an OSPF distribution list, the `<source-ip>` parameter actually is specifying the destination network of the route.

The `<wildcard>` parameter specifies the portion of the source address to match against. The `<wildcard>` is a four-part value in dotted-decimal notation (IP address format) consisting of ones and zeros. Zeros in the mask mean
the packet’s source address must match the <source-ip>. Ones mean any value matches. For example, the <source-ip> and <wildcard> values 4.0.0.0 0.255.255.255 mean that all 4.x.x.x networks match the ACL.

If you want the policy to match on all destination networks, enter any any.

If you prefer to specify the wildcard (mask value) in Classless Interdomain Routing (CIDR) format, you can enter a forward slash after the IP address, then enter the number of significant bits in the mask. For example, you can enter the CIDR equivalent of “4.0.0.0 0.255.255.255” as “4.0.0/8”. The CLI automatically converts the CIDR number into the appropriate ACL mask (where zeros instead of ones are the significant bits) and changes the non-significant portion of the IP address into zeros.

NOTE: If you enable the software to display IP sub-net masks in CIDR format, the mask is saved in the file in “<mask-bits>” format. To enable the software to display the CIDR masks, enter the ip show-subnet-length command at the global CONFIG level of the CLI. You can use the CIDR format to configure the ACL entry regardless of whether the software is configured to display the masks in CIDR format.

If you use the CIDR format, the ACL entries appear in this format in the running-config and startup-config files, but are shown with sub-net mask in the display produced by the show ip access-list command.

Using an Extended ACL as Input to the Distribution List
To use an extended ACL to configure an OSPF distribution list for denying specific routes, enter commands such as the following:

ProCurveRS(config)# ip access-list extended no_ip
ProCurveRS(config-ext-nacl)# deny ip 4.0.0.0 0.255.255.255 255.255.0.0 0.0.0.255
ProCurveRS(config-ext-nacl)# permit ip any any
ProCurveRS(config-ext-nacl)# exit
ProCurveRS(config)# router ospf
ProCurveRS(config-ospf-router)# distribute-list no_ip in

The first three commands configure an extended ACL that denies routes to any 4.x.x.x destination network with a 255.255.0.0 network mask and allows all other routes for eligibility to be installed in the IP route table. The last three commands change the CLI to the OSPF configuration level and configure an OSPF distribution list that uses the ACL as input. The distribution list prevents routes to any 4.x.x.x destination network with network mask 255.255.0.0 from entering the IP route table. The distribution list does not prevent the routes from entering the OSPF database.

Syntax: [no] ip access-list extended <acl-name> | <acl-id>

Syntax: deny | permit <ip-protocol> <source-ip> <wildcard> <destination-ip> <wildcard>

The <acl-name> | <acl-id> parameter specifies the ACL name or ID.

The deny | permit parameter indicates whether packets that match the policy are dropped or forwarded.

The <ip-protocol> parameter indicates the type of IP packet you are filtering. When using an extended ACL as input for an OSPF distribution list, specify ip.

The <source-ip> <wildcard> parameter specifies the source address for the policy. Since this ACL is input to an OSPF distribution list, the <source-ip> parameter actually is specifying the destination network of the route.

The <wildcard> parameter specifies the portion of the source address to match against. The <wildcard> is a four-part value in dotted-decimal notation (IP address format) consisting of ones and zeros. Zeros in the mask mean the packet’s source address must match the <source-ip>. Ones mean any value matches. For example, the <source-ip> and <wildcard> values 4.0.0.0 0.255.255.255 mean that all 4.x.x.x networks match the ACL.

If you want the policy to match on all network addresses, enter any any.

If you prefer to specify the wildcard (mask value) in Classless Interdomain Routing (CIDR) format, you can enter a forward slash after the IP address, then enter the number of significant bits in the mask. For example, you can enter the CIDR equivalent of “4.0.0.0 0.255.255.255” as “4.0.0/8”. The CLI automatically converts the CIDR
number into the appropriate ACL mask (where zeros instead of ones are the significant bits) and changes the non-
significant portion of the IP address into zeros.

**NOTE:** If you enable the software to display IP sub-net masks in CIDR format, the mask is saved in the file in
"/<mask-bits>" format. To enable the software to display the CIDR masks, enter the `ip show-subnet-length`
command at the global CONFIG level of the CLI. You can use the CIDR format to configure the ACL entry
regardless of whether the software is configured to display the masks in CIDR format.

If you use the CIDR format, the ACL entries appear in this format in the running-config and startup-config files, but
are shown with sub-net mask in the display produced by the `show ip access-list` commands.

The `<destination-ip> <Wildcard>` parameter specifies the destination address for the policy. Since this ACL is input
to an OSPF distribution list, the `<destination-ip>` parameter actually is specifying the network mask of the
destination. The `<wildcard>` parameter specifies the portion of the destination address to match against. If you
want the policy to match on all network masks, enter **any any**.

**Modify Default Metric for Redistribution**
The default metric is a global parameter that specifies the cost applied to all OSPF routes by default. The default
value is 10. You can assign a cost from 1 – 15.

**NOTE:** You also can define the cost on individual interfaces. The interface cost overrides the default cost.

**USING THE CLI**
To assign a default metric of 4 to all routes imported into OSPF, enter the following commands:

```
ProCurveRS(config)# router ospf
ProCurveRS(config-ospf-router)# default-metric 4
```

**Syntax:** default-metric <value>
The `<value>` can be from 1 – 16,777,215. The default is 10.

**USING THE WEB MANAGEMENT INTERFACE**
To modify the cost that is assigned to redistributed routes:

1. Log on to the device using a valid user name and password for read-write access.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
4. Click on the **Redistribution Filter** link to display a table listing the redistribution filters.
5. Click on the Modify button to the right of the row describing the virtual link you want to modify. The **OSPF**
   Virtual Link Interface configuration panel is displayed.
6. Enter a value from 1 – 15 in the Default Metric field.
7. Click Add to save the change to the device's running-config file.
8. Select the Save link at the bottom of the dialog, then select Yes when prompted to save the configuration
   change to the startup-config file on the device's flash memory.

**Enable Route Redistribution**
To enable route redistribution, use one of the following methods.

**NOTE:** Do not enable redistribution until you have configured the redistribution filters. Otherwise, you might
accidentally overload the network with routes you did not intend to redistribute.
**USING THE CLI**

To enable redistribution of RIP and static IP routes into OSPF, enter the following commands.

```
ProCurveRS(config)# router ospf
ProCurveRS(config-ospf-router)# redistribution rip
ProCurveRS(config-ospf-router)# redistribution static
ProCurveRS(config-ospf-router)# write memory
```

**Example Using a Route Map**

To configure a route map and use it for redistribution of routes into OSPF, enter commands such as the following:

```
ProCurveRS(config)# ip route 1.1.0.0 255.255.0.0 207.95.7.30
ProCurveRS(config)# ip route 1.2.0.0 255.255.0.0 207.95.7.30
ProCurveRS(config)# ip route 1.3.0.0 255.255.0.0 207.95.7.30
ProCurveRS(config)# ip route 4.1.0.0 255.255.0.0 207.95.6.30
ProCurveRS(config)# ip route 4.2.0.0 255.255.0.0 207.95.6.30
ProCurveRS(config)# ip route 4.3.0.0 255.255.0.0 207.95.6.30
ProCurveRS(config)# ip route 4.4.0.0 255.255.0.0 207.95.6.30
ProCurveRS(config)# route-map abc permit 1
ProCurveRS(config-route-map abc)# match metric 5
ProCurveRS(config-route-map abc)# set metric 8
ProCurveRS(config-route-map abc)# router ospf
ProCurveRS(config-ospf-router)# redistribute static route-map abc
```

The commands in this example configure some static IP routes, then configure a route map and use the route map for redistributing static IP routes into OSPF.

The `ip route` commands configure the static IP routes. The `route-map` command begins configuration of a route map called “abc”. The number indicates the route map entry (called the “instance”) you are configuring. A route map can contain multiple entries. The software compares packets to the route map entries in ascending numerical order and stops the comparison once a match is found.

The `match` command in the route map matches on routes that have 5 for their metric value (cost). The `set` command changes the metric in routes that match the route map to 8.

The `redistribute static` command enables redistribution of static IP routes into OSPF, and uses route map “abc” to control the routes that are redistributed. In this example, the route map allows a static IP route to be redistributed into OSPF only if the route has a metric of 5, and changes the metric to 8 before placing the route into the OSPF route table.

The following command shows the result of the redistribution filter. Since only one of the static IP routes configured above matches the route map, only one route is redistributed. Notice that the route’s metric is 5 before redistribution but is 8 after redistribution.

```
ProCurveRS(config-ospf-router)# show ip ospf database extensive
```

<table>
<thead>
<tr>
<th>Index</th>
<th>Aging</th>
<th>LS ID</th>
<th>Router</th>
<th>Netmask</th>
<th>Metric</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>4.4.0.0</td>
<td>10.10.10.60</td>
<td>ffff0000</td>
<td>80000008</td>
<td>0000</td>
</tr>
</tbody>
</table>

**Syntax:** [no] redistribution bgp | connected | rip | static [route-map <map-name>]

The bgp | connected | rip | static parameter specifies the route source.

The route-map <map-name> parameter specifies the route map name. The following match parameters are valid for OSPF redistribution:

- match ip address | next-hop <acl-num>
• `match metric <num>`
• `match tag <tag-value>`

The following set parameters are valid for OSPF redistribution:

• `set ip next hop <ip-addr>`
• `set metric [+ | -]<num> | none`
• `set metric-type type-1 | type-2`
• `set tag <tag-value>`

**NOTE:** You must configure the route map before you configure a redistribution filter that uses the route map.

**NOTE:** When you use a route map for route redistribution, the software disregards the permit or deny action of the route map.

**NOTE:** For an external route that is redistributed into OSPF through a route map, the metric value of the route remains the same unless the metric is set by a `set metric` command inside the route map. The `default-metric <num>` command has no effect on the route. This behavior is different from a route that is redistributed without using a route map. For a route redistributed without using a route map, the metric is set by the default-metric `<num>` command.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to OSPF in the tree view to expand the list of BGP option links.
4. Click on the **General** link to display the OSPF configuration panel, as shown in the following figure.

![OSPF Configuration Panel](image)

5. Select the Enable radio button next to Redistribution.
6. Click the **Apply** button to apply the change to the device's running-config file.
7. Select the **Save** link at the bottom of the dialog, then select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

**Disable or Re-enable Load Sharing**

HP routers can load share among up to eight equal-cost IP routes to a destination. By default, IP load sharing is enabled. The default is 4 equal-cost paths but you can specify from 2 – 8 paths.

The router software can use the route information it learns through OSPF to determine the paths and costs. Figure 12.8 shows an example of an OSPF network containing multiple paths to a destination (in this case, R1).

**Figure 12.8  Example OSPF network with four equal-cost paths**

In the example in Figure 12.8, the HP router has four paths to R1:

- HP->R3
- HP->R4
- HP->R5
- HP->R6

Normally, the HP router will choose the path to the R1 with the lower metric. For example, if R3’s metric is 1400 and R4’s metric is 600, the HP router will always choose R4.

However, suppose the metric is the same for all four routers in this example. If the costs are the same, the router now has four equal-cost paths to R1. To allow the router to load share among the equal cost routes, enable IP load sharing. The software supports four equal-cost OSPF paths by default when you enable load sharing. You can specify from 2 – 8 paths.

**NOTE:** The HP router is not source routing in these examples. The router is concerned only with the paths to the next-hop routers, not the entire paths to the destination hosts.

OSPF load sharing is enabled by default when IP load sharing is enabled. To configure IP load sharing parameters, see “Configuring IP Load Sharing” on page 9-51.
Configure External Route Summarization

When the Routing Switch is an OSPF Autonomous System Boundary Router (ASBR), you can configure it to advertise one external route as an aggregate for all redistributed routes that are covered by a specified address range.

When you configure an address range, the range takes effect immediately. All the imported routes are summarized according to the configured address range. Imported routes that have already been advertised and that fall within the range are flushed out of the AS and a single route corresponding to the range is advertised.

If a route that falls within a configured address range is imported by the Routing Switch, no action is taken if the Routing Switch has already advertised the aggregate route; otherwise the Routing Switch advertises the aggregate route. If an imported route that falls within a configured address range is removed by the Routing Switch, no action is taken if there are other imported route(s) that fall within the same address range; otherwise the aggregate route is flushed.

You can configure up to 32 address ranges. The Routing Switch sets the forwarding address of the aggregate route to zero and sets the tag to zero.

If you delete an address range, the advertised aggregate route is flushed and all imported routes that fall within the range are advertised individually.

If an external LSDB overflow condition occurs, all aggregate routes are flushed out of the AS, along with other external routes. When the Routing Switch exits the external LSDB overflow condition, all the imported routes are summarized according to the configured address ranges.

NOTE: If you use redistribution filters in addition to address ranges, the Routing Switch applies the redistribution filters to routes first, then applies them to the address ranges.

NOTE: If you disable redistribution, all the aggregate routes are flushed, along with other imported routes.

NOTE: This option affects only imported, type 5 external routes. A single type 5 LSA is generated and flooded throughout the AS for multiple external routes. Type 7-route redistribution is not affected by this feature. All type 7 routes will be imported (if redistribution is enabled). To summarize type 7 LSAs or exported routes, use NSSA address range summarization.

To configure route summarization, use the following CLI method.

USING THE CLI

To configure a summary address for OSPF routes, enter commands such as the following:

```
ProCurveRS(config-ospf-router)# summary-address 10.1.0.0 255.255.0.0
```

The command in this example configures summary address 10.1.0.0, which includes addresses 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. For all of these networks, only the address 10.1.0.0 is advertised in external LSAs.

**Syntax:** summary-address <ip-addr> <ip-mask>

The `<ip-addr>` parameter specifies the network address.

The `<ip-mask>` parameter specifies the network mask.

To display the configured summary addresses, enter the following command at any level of the CLI:

```
ProCurveRS(config-ospf-router)# show ip ospf config
```

* OSPF Redistribution Address Ranges currently defined:

```
Range-Address   Subnetmask
1.0.0.0          255.0.0.0
1.0.1.0          255.255.255.0
1.0.2.0          255.255.255.0
```

**Syntax:** show ip ospf config
**USING THE WEB MANAGEMENT INTERFACE**

You cannot configure OSPF route summarization using the Web management interface.

**Configure Default Route Origination**

When the Routing Switch is an OSPF Autonomous System Boundary Router (ASBR), you can configure it to automatically generate a default external route into an OSPF routing domain. This feature is called “default route origination” or “default information origination”.

By default, ProCurve Routing Switches do not advertise the default route into the OSPF domain. If you want the Routing Switch to advertise the OSPF default route, you must explicitly enable default route origination.

When you enable OSPF default route origination, the Routing Switch advertises a type 5 default route that is flooded throughout the AS (except stub areas and NSSAs). In addition, internal NSSA ASBRs advertise their default routes as translatable type 7 default routes.

The Routing Switch advertises the default route into OSPF even if OSPF route redistribution is not enabled, and even if the default route is learned through an IBGP neighbor.

**NOTE:** ProCurve Routing Switches never advertise the OSPF default route, regardless of other configuration parameters, unless you explicitly enable default route origination using the following method.

If the Routing Switch is an ASBR, you can use the “always” option when you enable the default route origination. The always option causes the ASBR to create and advertise a default route if it does not already have one configured.

If default route origination is enabled and you disable it, the default route originated by the Routing Switch is flushed. Default routes generated by other OSPF routers are not affected. If you re-enable the feature, the feature takes effect immediately and thus does not require you to reload the software.

**NOTE:** The ABR (Routing Switch) will not inject the default route into an NSSA by default and the command described in this section will not cause the Routing Switch to inject the default route into the NSSA. To inject the default route into an NSSA, use the `area <num> | <ip-addr> nssa default-information-originate` command. See “Assign a Not-So-Stubby Area (NSSA)” on page 12-12.

To enable default route origination, use the following CLI method.

**USING THE CLI**

To enable default route origination, enter the following command:

```
ProCurveRS(config-ospf-router)# default-information-originate
```

To disable the feature, enter the following command:

```
ProCurveRS(config-ospf-router)# no default-information-originate
```

**Syntax:** `[no] default-information-originate [always] [metric <value>] [metric-type <type>]`

The `always` parameter advertises the default route regardless of whether the router has a default route. This option is disabled by default.

The `metric <value>` parameter specifies a metric for the default route. If this option is not used, the default metric is used for the route.

The `metric-type <type>` parameter specifies the external link type associated with the default route advertised into the OSPF routing domain. The `<type>` can be one of the following:

- 1 – Type 1 external route
- 2 – Type 2 external route

If you do not use this option, the default redistribution metric type is used for the route type.
NOTE: If you specify a metric and metric type, the values you specify are used even if you do not use the always option.

**USING THE WEB MANAGEMENT INTERFACE**

You cannot configure OSPF default route origination using the Web management interface.

**Modify SPF Timers**

The Routing Switch uses the following timers when calculating the shortest path for OSPF routes:

- **SPF delay** – When the Routing Switch receives a topology change, the software waits before it starts a Shortest Path First (SPF) calculation. By default, the software waits five seconds. You can configure the SPF delay to a value from 0 – 65535 seconds. If you set the SPF delay to 0 seconds, the software immediately begins the SPF calculation after receiving a topology change.

- **SPF hold time** – The Routing Switch waits for a specific amount of time between consecutive SPF calculations. By default, the Routing Switch waits ten seconds. You can configure the SPF hold time to a value from 0 – 65535 seconds. If you set the SPF hold time to 0 seconds, the software does not wait between consecutive SPF calculations.

You can set the delay and hold time to lower values to cause the Routing Switch to change to alternate paths more quickly in the event of a route failure. Note that lower values require more CPU processing time.

You can change one or both of the timers. To do so, use the following CLI method.

**USING THE CLI**

To change the SPF delay and hold time, enter commands such as the following:

```
ProCurveRS(config-ospf-router)# timers spf 10 20
```

The command in this example changes the SPF delay to 10 seconds and changes the SPF hold time to 20 seconds.

**Syntax:** timers spf <delay> <hold-time>

The `<delay>` parameter specifies the SPF delay.

The `<hold-time>` parameter specifies the SPF hold time.

To set the timers back to their default values, enter a command such as the following:

```
ProCurveRS(config-ospf-router)# no timers spf 10 20
```

**USING THE WEB MANAGEMENT INTERFACE**

You cannot configure the SPF timers using the Web management interface.

**Modify Redistribution Metric Type**

The redistribution metric type is used by default for all routes imported into OSPF unless you specify different metrics for individual routes using redistribution filters. Type 2 specifies a big metric (three bytes). Type 1 specifies a small metric (two bytes). The default value is type 2.

**USING THE CLI**

To modify the default value to type 1, enter the following command:

```
ProCurveRS(config-ospf-router)# metric-type type1
```

**Syntax:** metric-type type1 | type2

The default is type2.

**USING THE WEB MANAGEMENT INTERFACE**

To modify the default metric type:
1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.

2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.

3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.

4. Click on the General link to display the OSPF configuration panel.

5. Select either Type 1 or Type 2 for the redistribution metric type.

6. Click the Apply button to save the change to the device’s running-config file.

7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

**Modify Administrative Distance**

ProCurve Routing Switches can learn about networks from various protocols, including Border Gateway Protocol version 4 (BGP4), RIP, and OSPF. Consequently, the routes to a network may differ depending on the protocol from which the routes were learned. The default administrative distance for OSPF routes is 110. See “Changing Administrative Distances” on page 13-36 for a list of the default distances for all route sources.

The router selects one route over another based on the source of the route information. To do so, the router can use the administrative distances assigned to the sources. You can bias the Routing Switch’s decision by changing the default administrative distance for RIP routes.

**Configuring Administrative Distance Based on Route Type**

You can configure a unique administrative distance for each type of OSPF route. For example, you can use this feature to prefer a static route over an OSPF inter-area route but you also want to prefer OSPF intra-area routes to static routes.

The distance you specify influences the choice of routes when the Routing Switch has multiple routes for the same network from different protocols. The Routing Switch prefers the route with the lower administrative distance.

You can specify unique default administrative distances for the following route types:

- Intra-area routes
- Inter-area routes
- External routes

The default for all these OSPF route types is 110.

**NOTE:** This feature does not influence the choice of routes within OSPF. For example, an OSPF intra-area route is always preferred over an OSPF inter-area route, even if the intra-area route’s distance is greater than the inter-area route’s distance.

To configure administrative distances for OSPF route types, use the following CLI method.

**USING THE CLI**

To change the default administrative distances for inter-area routes, intra-area routes, and external routes, enter the following command:

```
ProCurveRS(config-ospf-router)# distance external 100
ProCurveRS(config-ospf-router)# distance inter-area 90
ProCurveRS(config-ospf-router)# distance intra-area 80
```

**Syntax:** distance external | inter-area | intra-area <distance>

The external | inter-area | intra-area parameter specifies the route type for which you are changing the default administrative distance.
The <distance> parameter specifies the new distance for the specified route type. Unless you change the distance for one of the route types using commands such as those shown above, the default is 110.

To reset the administrative distance to its system default (110), enter a command such as the following:

```
ProCurveRS(config-ospf-router)# no distance external 100
```

**Configure OSPF Group Link State Advertisement (LSA) Pacing**

The Routing Switch paces LSA refreshes by delaying the refreshes for a specified time interval instead of performing a refresh each time an individual LSA's refresh timer expires. The accumulated LSAs constitute a group, which the Routing Switch refreshes and sends out together in one or more packets.

The pacing interval, which is the interval at which the Routing Switch refreshes an accumulated group of LSAs, is configurable to a range from 10 – 1800 seconds (30 minutes). The default is 240 seconds (four minutes). Thus, every four minutes, the Routing Switch refreshes the group of accumulated LSAs and sends the group together in the same packet(s).

**Usage Guidelines**

The pacing interval is inversely proportional to the number of LSAs the Routing Switch is refreshing and aging. For example, if you have approximately 10,000 LSAs, decreasing the pacing interval enhances performance. If you have a very small database (40 – 100 LSAs), increasing the pacing interval to 10 – 20 minutes might enhance performance slightly.

**Changing the LSA Pacing Interval**

To change the LSA pacing interval, use the following CLI method.

**USING THE CLI**

To change the LSA pacing interval to two minutes (120 seconds), enter the following command:

```
ProCurveRS(config-ospf-router)# timers lsa-group-pacing 120
```

**Syntax:** `[no] timers lsa-group-pacing <secs>`

The `<secs>` parameter specifies the number of seconds and can be from 10 – 1800 (30 minutes). The default is 240 seconds (four minutes).

To restore the pacing interval to its default value, enter the following command:

```
ProCurveRS(config-ospf-router)# no timers lsa-group-pacing
```

**USING THE WEB MANAGEMENT INTERFACE**

You cannot configure this option using the Web management interface.

**Modify OSPF Traps Generated**

OSPF traps as defined by RFC 1850 are supported on HP routers. OSPF trap generation is enabled on the router, by default.

**USING THE CLI**

When using the CLI, you can disable all or specific OSPF trap generation by entering the following CLI command:

```
ProCurveRS(config-ospf-router)# no snmp-server trap ospf
```

To later re-enable the trap feature, enter `snmp-server trap ospf`.

To disable a specific OSPF trap, enter the command as `no snmp-server trap ospf <ospf-trap>`.

These commands are at the OSPF router Level of the CLI.

Here is a summary of OSPF traps supported on HP routers, their corresponding CLI commands, and their associated MIB objects from RFC 1850:

- **interface-state-change-trap** – [MIB object: OspfIfstateChange]
- **virtual-interface-state-change-trap** – [MIB object: OspfVirtIfStateChange]
Configuring OSPF

- neighbor-state-change-trap – [MIB object: ospfNbrStateChange]
- virtual-neighbor-state-change-trap – [MIB object: ospfVirtNbrStateChange]
- interface-config-error-trap – [MIB object: ospfIfConfigError]
- virtual-interface-config-error-trap – [MIB object: ospfVirtIfConfigError]
- interface-authentication-failure-trap – [MIB object: ospfIfAuthFailure]
- virtual-interface-authentication-failure-trap – [MIB object: ospfVirtIfAuthFailure]
- interface-receive-bad-packet-trap – [MIB object: ospfIfRxBadPacket]
- virtual-interface-receive-bad-packet-trap – [MIB object: ospfVirtIfRxBadPacket]
- interface-retransmit-packet-trap – [MIB object: ospfTxRetransmit]
- virtual-interface-retransmit-packet-trap – [MIB object: ospfVirtIfTxRetransmit]
- originate-lsa-trap – [MIB object: ospfOriginLsa]
- originate-maxage-lsa-trap – [MIB object: ospfMaxAgeLsa]
- link-state-database-overflow-trap – [MIB object: ospfLsdbOverflow]
- link-state-database-approaching-overflow-trap – [MIB object: ospfLsdbApproachingOverflow]

**EXAMPLE:**
To stop an OSPF trap from being collected, use the CLI command: **no trap <ospf-trap>**, at the Router OSPF level of the CLI. To disable reporting of the neighbor-state-change-trap, enter the following command:

```bash
ProCurveRS(config-ospf-router)# no trap neighbor-state-change-trap
```

**EXAMPLE:**
To reinstate the trap, enter the following command:

```bash
ProCurveRS(config-ospf-router)# trap neighbor-state-change-trap
```

**Syntax:** **[no]** snmp-server trap ospf <ospf-trap>

**USING THE WEB MANAGEMENT INTERFACE**
To disable a specific OSPF trap or traps:

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
4. Click on the Trap link to display the OSPF Trap panel.
5. Select the Disable radio button beside each OSPF trap you want to disable.
6. Click the Apply button to save the change to the device's running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

**Modify OSPF Standard Compliance Setting**
HP routers are configured, by default, to be compliant with the RFC 1583 OSPF V2 specification.

**USING THE CLI**
To configure a router to operate with the latest OSPF standard, RFC 2178, enter the following commands:

```bash
ProCurveRS(config)# router ospf
ProCurveRS(config-ospf-router)# no rfc1583-compatibility
```

**Syntax:** **[no]** rfc1583-compatibility
**USING THE WEB MANAGEMENT INTERFACE**

To configure a router to operate with the latest OSPF standard, RFC 2178:

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
4. Click on the General link to display the OSPF configuration panel.
5. Select Disable next to RFC 1583.
6. Click the Apply button to save the change to the device’s running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

**Modify Exit Overflow Interval**

If a database overflow condition occurs on a router, the router eliminates the condition by removing entries that originated on the router. The exit overflow interval allows you to set how often a Routing Switch checks to see if the overflow condition has been eliminated. The default value is 0. The range is 0 – 86400 seconds (24 hours). If the configured value of the database overflow interval is zero, then the router never leaves the database overflow condition.

**NOTE:** Software release 07.1.00 and later dynamically allocate OSPF memory as needed. See “Dynamic OSPF Memory” on page 12-7.

**USING THE CLI**

To modify the exit overflow interval to 60 seconds, enter the following command:

```
ProCurveRS(config-ospf-router)# data-base-overflow-interval 60
```

**Syntax:** database-overflow-interval <value>

The <value> can be from 0 – 86400 seconds. The default is 0 seconds.

**USING THE WEB MANAGEMENT INTERFACE**

To modify the exit overflow interval:

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
4. Click on the General link to display the OSPF configuration panel.
5. Enter a value from 0 – 86400 in the Exit Overflow Interval field.
6. Click the Apply button to save the change to the device’s running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

**Modify the Maximum Number of Routes**

**NOTE:** This section applies only to devices that are running software earlier than release 07.1.00. See “Dynamic OSPF Memory” on page 12-7.
The OSPF route table holds 16000 routes by default. You can change the maximum number of routes the Routing Switch’s OSPF table can hold to a value from 4000 – 32000.

**USING THE CLI**

To change the maximum number of OSPF routes to 32000, enter the following command:

```bash
ProCurveRS(config-ospf-router)# max-routes 32000
ProCurveRS(config-ospf-router)# end
ProCurveRS# reload
```

*Syntax:* `max-routes <num>`

The `<num>` indicates the number of OSPF routes allowed and can be from 4000 – 32000. The change takes effect after the router is rebooted.

**USING THE WEB MANAGEMENT INTERFACE**

You cannot modify the maximum number of OSPF routes using the Web management interface.

**Modify LSDB Limits**

**NOTE:** This section applies only to devices that are running software earlier than release 07.1.00. See “Dynamic OSPF Memory” on page 12-7.

On Routing Switches with 32MB or greater memory, you can modify the number of link-state advertisements (LSAs) that the router allows before a database overflow condition is declared on the system. These parameters are part of the router's compliance with RFC 1765.

The following table lists the types of LSAs for which you can configure the table sizes, the default number of entries the tables can hold, and the range of maximum values you can specify. You cannot configure the LSA tables globally; you must configure them for individual LSA types. Make sure you save the running-config file and reload after changing a table size. The change does not take effect until you reload or reboot.

**Table 12.1: Configurable LSA Table Sizes**

<table>
<thead>
<tr>
<th>LSA Type</th>
<th>Default Maximum Number of Entries</th>
<th>Range of Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>External (type 5)</td>
<td>2000</td>
<td>500 – 8000</td>
</tr>
<tr>
<td>Network (type 2)</td>
<td>2000</td>
<td>200 – 2000</td>
</tr>
<tr>
<td>Router (type 1)</td>
<td>2200</td>
<td>200 – 2200</td>
</tr>
<tr>
<td>Summary (type 3 and type 4)</td>
<td>2000</td>
<td>500 – 18000</td>
</tr>
</tbody>
</table>

**USING THE CLI**

To change the maximum number of summary LSA entries from 2000 to 18000, enter the following commands:

```bash
ProCurveRS(config-ospf-router)# maximum-number-of-lsa summary 18000
ProCurveRS(config-ospf-router)# write memory
```

*Syntax:* `maximum-number-of-lsa external | network | router | summary <value>`

**USING THE WEB MANAGEMENT INTERFACE**

To modify the number of IP OSPF external link state advertisements:

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
4. Click on the General link to display the OSPF configuration panel.
5. Enter a value from 500 – 8000 in the External LSDB Limit field.
6. Click the Apply button to save the change to the device’s running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

### Configuring an OSPF Point-to-Point Link

OSPF point-to-point links are supported in software releases 07.8.00 and later.

In an OSPF point-to-point link, a direct Layer 3 connection exists between a single pair of OSPF routers, without the need for Designated and Backup Designated routers. In a point-to-point link, neighboring routers become adjacent whenever they can communicate directly. In contrast, in broadcast and non-broadcast multi-access (NBMA) networks, the Designated Router and the Backup Designated Router become adjacent to all other routers attached to the network.

### Configuration Notes and Limitations

- This feature is supported in software releases 07.8.00 and later.
- This feature is supported on 10/100, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces.
- This feature is supported on physical interfaces. It is not supported on virtual interfaces.
- HP supports numbered point-to-point networks, meaning the OSPF router must have an IP interface address which uniquely identifies the router over the network. HP does not support unnumbered point-to-point networks.

### Configuring an OSPF Point-to-Point Link

To configure an OSPF point-to-point link, enter commands such as the following:

```
ProCurveRS(config)# interface eth 1/5
ProCurveRS(config-if-1/5)# ip ospf network point-to-point
```

This command configures an OSPF point-to-point link on Interface 5 in slot 1.

**Syntax:** `[no] ip ospf network point-to-point`

### Viewing Configured OSPF Point-to-Point Links

See “Displaying OSPF Neighbor Information” on page 12-51 and “Displaying OSPF Interface Information” on page 12-53.

### Specify Types of OSPF Syslog Messages to Log

**NOTE:** This section applies only to devices that are running software release 07.6.04 or later.

Starting with release 07.6.04, you can specify which kinds of OSPF-related Syslog messages are logged. In releases prior to 07.6.04, by default all OSPF Syslog messages are logged. In configurations with a large amount of OSPF activity, this can result in the HP device’s Syslog buffer and the Syslog server filling up with OSPF messages.

By default, the only OSPF messages that are logged are those indicating possible system errors. If you want other kinds of OSPF messages to be logged, you can configure the HP device to log them.

For example, to specify that all OSPF-related Syslog messages be logged, enter the following commands.

```
ProCurveRS(config)# router ospf
ProCurveRS(config-ospf-router)# log all
```

**Syntax:** `[no] log all | adjacency | bad_packet [checksum] | database | memory | retransmit`
The log command has the following options:

The all option causes all OSPF-related Syslog messages to be logged. If you later disable this option with the no log all command, the OSPF logging options return to their default settings.

The adjacency option logs essential OSPF neighbor state changes, especially on error cases. This option is disabled by default.

The bad_packet checksum option logs all OSPF packets that have checksum errors. This option is enabled by default.

The bad_packet option logs all other bad OSPF packets. This option is disabled by default.

The database option logs OSPF LSA-related information. This option is disabled by default.

The memory option logs abnormal OSPF memory usage. This option is enabled by default.

The retransmit option logs OSPF retransmission activities. This option is disabled by default.

Displaying OSPF Information

You can use CLI commands and Web management options to display the following OSPF information:

- Trap, area, and interface information – see “Displaying General OSPF Configuration Information” on page 12-48.
- Area information – see “Displaying OSPF Area Information” on page 12-50.
- Neighbor information – see “Displaying OSPF Neighbor Information” on page 12-51.
- Interface information – see “Displaying OSPF Interface Information” on page 12-53.
- Route information – see “Displaying OSPF Route Information” on page 12-55.
- External link state information – see “Displaying OSPF External Link State Information” on page 12-57.
- Link state information – see “Displaying OSPF Link State Information” on page 12-58.
- Virtual Neighbor information – see “Displaying OSPF Virtual Neighbor Information” on page 12-60.
- Virtual Link information – see “Displaying OSPF Virtual Link Information” on page 12-60.
- ABR and ASBR information – see “Displaying OSPF ABR and ASBR Information” on page 12-60.
- Trap state information – see “Displaying OSPF Trap Status” on page 12-61.
Displaying General OSPF Configuration Information

To display general OSPF configuration information, enter the following command at any CLI level:

```
ProCurveRS> show ip ospf config
```

```
Router OSPF: Enabled
Redistribution: Disabled
Default OSPF Metric: 10
OSPF Redistribution Metric: Type2
OSPF External LSA Limit: 25000
OSPF Database Overflow Interval: 0
RFC 1583 Compatibility: Enabled
Router id: 207.95.11.128

Interface State Change Trap:          Enabled
Virtual Interface State Change Trap:  Enabled
Neighbor State Change Trap:          Enabled
Virtual Neighbor State Change Trap:  Enabled
Interface Configuration Error Trap:     Enabled
Virtual Interface Configuration Error Trap:  Enabled
Interface Authentication Failure Trap:     Enabled
Virtual Interface Authentication Failure Trap:  Enabled
Interface Receive Bad Packet Trap:    Enabled
Virtual Interface Receive Bad Packet Trap:  Enabled
Interface Retransmit Packet Trap:      Enabled
Virtual Interface Retransmit Packet Trap:  Enabled
Originate LSA Trap:                      Enabled
Originate MaxAge LSA Trap:            Enabled
Link State Database Overflow Trap:     Enabled
Link State Database Approaching Overflow Trap:  Enabled

OSPF Area currently defined:  
Area-ID  Area-Type Cost
0        normal  0

OSPF Interfaces currently defined:  
Ethernet Interface: 3/1-3/2
ip ospf md5-authentication-key-activation-wait-time 300
ip ospf cost 0
ip ospf area 0

Ethernet Interface: v1
ip ospf md5-authentication-key-activation-wait-time 300
ip ospf cost 0
ip ospf area 0
```

**Syntax:** show ip ospf config

**Using the Web Management Interface**

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
4. Click on the General link to display the OSPF configuration panel.

**Displaying CPU Utilization Statistics**
You can display CPU utilization statistics for OSPF and other IP protocols.

**USING THE CLI**
To display CPU utilization statistics for OSPF for the previous one-second, one-minute, five-minute, and fifteen-minute intervals, enter the following command at any level of the CLI:

```
proCurveRS# show process cpu
```

<table>
<thead>
<tr>
<th>Process Name</th>
<th>5Sec(%)</th>
<th>1Min(%)</th>
<th>5Min(%)</th>
<th>15Min(%)</th>
<th>Runtime(ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>0.01</td>
<td>0.03</td>
<td>0.09</td>
<td>0.22</td>
<td>9</td>
</tr>
<tr>
<td>BGP</td>
<td>0.04</td>
<td>0.06</td>
<td>0.08</td>
<td>0.14</td>
<td>13</td>
</tr>
<tr>
<td>GVRP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>ICMP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>IP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>OSPF</td>
<td>0.03</td>
<td>0.06</td>
<td>0.09</td>
<td>0.12</td>
<td>11</td>
</tr>
<tr>
<td>RIP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>STP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>VRRP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
</tbody>
</table>

If the software has been running less than 15 minutes (the maximum interval for utilization statistics), the command indicates how long the software has been running. Here is an example:

```
proCurveRS# show process cpu
The system has only been up for 6 seconds.
```

<table>
<thead>
<tr>
<th>Process Name</th>
<th>5Sec(%)</th>
<th>1Min(%)</th>
<th>5Min(%)</th>
<th>15Min(%)</th>
<th>Runtime(ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>0.01</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>BGP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>GVRP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>ICMP</td>
<td>0.01</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>1</td>
</tr>
<tr>
<td>IP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>OSPF</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>RIP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>STP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>VRRP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
</tbody>
</table>

To display utilization statistics for a specific number of seconds, enter a command such as the following:

```
proCurveRS# show process cpu 2
Statistics for last 1 sec and 80 ms
```

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Sec(%)</th>
<th>Time(ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>BGP</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>GVRP</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>ICMP</td>
<td>0.01</td>
<td>1</td>
</tr>
<tr>
<td>IP</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>OSPF</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>RIP</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>STP</td>
<td>0.01</td>
<td>0</td>
</tr>
<tr>
<td>VRRP</td>
<td>0.00</td>
<td>0</td>
</tr>
</tbody>
</table>

When you specify how many seconds’ worth of statistics you want to display, the software selects the sample that most closely matches the number of seconds you specified. In this example, statistics are requested for the previous two seconds. The closest sample available is actually for the previous 1 second plus 80 milliseconds.
**Syntax:** show process cpu [<num>]

The `<num>` parameter specifies the number of seconds and can be from 1 – 900. If you use this parameter, the command lists the usage statistics only for the specified number of seconds. If you do not use this parameter, the command lists the usage statistics for the previous one-second, one-minute, five-minute, and fifteen-minute intervals.

**USING THE WEB MANAGEMENT INTERFACE**

You cannot display this information using the Web management interface.

**Displaying OSPF Area Information**

To display global OSPF area information for the router, use one of the following methods.

**USING THE CLI**

To display OSPF area information, enter the following command at any CLI level:

```
ProCurveRS> show ip ospf area
```

<table>
<thead>
<tr>
<th>Indx</th>
<th>Area</th>
<th>Type</th>
<th>Cost</th>
<th>SPFR</th>
<th>ABR</th>
<th>ASBR</th>
<th>LSA</th>
<th>Chksum(Hex)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.0.0.0</td>
<td>normal</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0000781f</td>
</tr>
<tr>
<td>2</td>
<td>192.147.60.0</td>
<td>normal</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0000fee6</td>
</tr>
<tr>
<td>3</td>
<td>192.147.80.0</td>
<td>stub</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>000181cd</td>
</tr>
</tbody>
</table>

**Syntax:** show ip ospf area [<area-id>] | [<num>]]

The `<area-id>` parameter shows information for the specified area.

The `<num>` parameter displays the entry that corresponds to the entry number you enter. The entry number identifies the entry's position in the area table.

This display shows the following information.

**Table 12.2: CLI Display of OSPF Area Information**

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indx</td>
<td>The row number of the entry in the router's OSPF area table.</td>
</tr>
<tr>
<td>Area</td>
<td>The area number.</td>
</tr>
<tr>
<td>Type</td>
<td>The area type, which can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• nssa</td>
</tr>
<tr>
<td></td>
<td>• normal</td>
</tr>
<tr>
<td></td>
<td>• stub</td>
</tr>
<tr>
<td>Cost</td>
<td>The area's cost.</td>
</tr>
<tr>
<td>SPFR</td>
<td>The SPFR value.</td>
</tr>
<tr>
<td>ABR</td>
<td>The ABR number.</td>
</tr>
<tr>
<td>ASBR</td>
<td>The ABSR number.</td>
</tr>
<tr>
<td>LSA</td>
<td>The LSA number.</td>
</tr>
</tbody>
</table>
Configuring OSPF

USING THE WEB MANAGEMENT INTERFACE
1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Monitor in the tree view to expand the list of monitoring options.
3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
4. Click on the Area link.

Displaying OSPF Neighbor Information
To display OSPF neighbor information for the router, use one of the following methods.

NOTE: Releases prior to 07.6.04 support the command show ip ospf neighbor only. However, this command includes the details displayed in show ip ospf neighbor detail, as shown in the second example below.
Software releases 07.6.04 and later include a new command, show ip ospf neighbor detail, in addition to the show ip ospf neighbor command. Both of these commands are described below.

USING THE CLI
To display OSPF neighbor information for the router, use one of the following methods.

Syntax:
show ip ospf neighbor [router-id <ip-addr>] | [<num>] | [detail]
The router-id <ip-addr> parameter displays only the neighbor entries for the specified router.
The <num> parameter displays only the entry in the specified index position in the neighbor table. For example, if you enter "1", only the first entry in the table is displayed.
The detail parameter applies to releases 07.6.04 and later. This parameter displays detailed information about the neighbor routers.

Table 12.2: CLI Display of OSPF Area Information (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chksum(Hex)</td>
<td>The checksum for the LSA packet. The checksum is based on all the fields in the packet except the age field. The Routing Switch uses the checksum to verify that the packet is not corrupted.</td>
</tr>
</tbody>
</table>

Using the CLI

ProCurveRS> show ip ospf neighbor
Port Address Pri State Neigh Address Neigh ID
8 212.76.7.251 1 full 212.76.7.200 173.35.1.220

To display detailed OSPF neighbor information, enter the following command at any CLI level:

ProCurveRS# show ip ospf neighbor detail

Syntax: show ip ospf neighbor [router-id <ip-addr>] | [<num>] | [detail]

The router-id <ip-addr> parameter displays only the neighbor entries for the specified router.
The <num> parameter displays only the entry in the specified index position in the neighbor table. For example, if you enter "1", only the first entry in the table is displayed.
The detail parameter applies to releases 07.6.04 and later. This parameter displays detailed information about the neighbor routers.
These displays show the following information.

### Table 12.3: CLI Display of OSPF Neighbor Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port through which the Routing Switch is connected to the neighbor.</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address of this Routing Switch’s interface with the neighbor.</td>
</tr>
</tbody>
</table>
| Pri | The OSPF priority of the neighbor.  
  * For multi-access networks, the priority is used during election of the Designated Router (DR) and Backup designated Router (BDR).  
  * For point-to-point links, this field shows one of the following values:  
    * 1 = point-to-point link  
    * 3 = point-to-point link with assigned subnet |
| State | The state of the conversation between the Routing Switch and the neighbor. This field can have one of the following values:  
  * Down – The initial state of a neighbor conversation. This value indicates that there has been no recent information received from the neighbor.  
  * Attempt – This state is only valid for neighbors attached to non-broadcast networks. It indicates that no recent information has been received from the neighbor.  
  * Init – A Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor. (The router itself did not appear in the neighbor’s Hello packet.) All neighbors in this state (or higher) are listed in the Hello packets sent from the associated interface.  
  * 2-Way – Communication between the two routers is bidirectional. This is the most advanced state before beginning adjacency establishment. The Designated Router and Backup Designated Router are selected from the set of neighbors in the 2-Way state or greater.  
  * ExStart – The first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial Database Description (DD) sequence number. Neighbor conversations in this state or greater are called adjacencies.  
  * Exchange – The router is describing its entire link state database by sending Database Description packets to the neighbor. Each Database Description packet has a DD sequence number, and is explicitly acknowledged. Only one Database Description packet can be outstanding at any time. In this state, Link State Request packets can also be sent asking for the neighbor's more recent advertisements. All adjacencies in Exchange state or greater are used by the flooding procedure. In fact, these adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets.  
  * Loading – Link State Request packets are sent to the neighbor asking for the more recent advertisements that have been discovered (but not yet received) in the Exchange state.  
  * Full – The neighboring routers are fully adjacent. These adjacencies will now appear in router links and network link advertisements. |
Configuring OSPF

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.

2. Click on the plus sign next to Monitor in the tree view to expand the list of monitoring options.

3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.

4. Click on the Neighbor link.

Displaying OSPF Interface Information

To display OSPF interface information for the router, use one of the following methods.

**USING THE CLI**

To display OSPF interface information, enter the following command at any CLI level:

```
ProCurveRS# show ip ospf interface 192.168.1.1
```

**Ethernet 2/1, OSPF enabled**

```
IP Address 192.168.1.1, Area 0
OSPF state ptr2ptr, Pri 1, Cost 1, Options 2, Type pt-2-pt Events 1
Timers (sec): Transit 1, Retrans 5, Hello 10, Dead 40
DR: Router ID 0.0.0.0 Interface Address 0.0.0.0
BDR: Router ID 0.0.0.0 Interface Address 0.0.0.0
Neighbor Count = 0, Adjacent Neighbor Count = 1
Neighbor: 2.2.2.2
Authentication-Key: None
MD5 Authentication: Key None, Key-Id None, Auth-change-wait-time 300
```

**Syntax:** `show ip ospf interface [<ip-addr>]`

The `<ip-addr>` parameter displays the OSPF interface information for the specified IP address.

---

**Table 12.3: CLI Display of OSPF Neighbor Information (Continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neigh Address</td>
<td>The IP address of the neighbor. For point-to-point links, the value is as follows:</td>
</tr>
<tr>
<td></td>
<td>- If the Pri field is &quot;1&quot;, this value is the IP address of the neighbor router's interface.</td>
</tr>
<tr>
<td></td>
<td>- If the Pri field is &quot;3&quot;, this is the subnet IP address of the neighbor router's interface.</td>
</tr>
<tr>
<td>Neigh ID</td>
<td>The neighbor router's ID.</td>
</tr>
<tr>
<td>Ev</td>
<td>The number of times the neighbor's state changed.</td>
</tr>
<tr>
<td>Opt</td>
<td>The sum of the option bits in the Options field of the Hello packet. This information is used by HP technical support. See Section A.2 in RFC 2178 for information about the Options field in Hello packets.</td>
</tr>
<tr>
<td>Cnt</td>
<td>The number of LSAs that were retransmitted.</td>
</tr>
</tbody>
</table>
The following table defines the highlighted fields shown in the above example output of the `show ip ospf interface` command.

<table>
<thead>
<tr>
<th>This field</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the interface.</td>
</tr>
<tr>
<td>OSPF state</td>
<td>ptr2ptr (point to point)</td>
</tr>
</tbody>
</table>
| Pri | The link ID as defined in the router-LSA. This value can be one of the following:  
1 = point-to-point link  
3 = point-to-point link with an assigned subnet |
| Cost | The configured output cost for the interface. |
| Options | OSPF Options (Bit7 - Bit0):  
• unused:1  
• opaque:1  
• summary:1  
• dont_propagate:1  
• nssa:1  
• multicast:1  
• externals:1  
• tos:1 |
| Type | The area type, which can be one of the following:  
• Broadcast = 0x01  
• NBMA = 0x02  
• Point to Point = 0x03  
• Virtual Link = 0x04  
• Point to Multipoint = 0x05 |
| Events | OSPF Interface Event:  
• Interface_Up = 0x00  
• Wait_Timer = 0x01  
• Backup_Seen = 0x02  
• Neighbor_Change = 0x03  
• Loop_Indication = 0x04  
• Unloop_Indication = 0x05  
• Interface_Down = 0x06  
• Interface_Passive = 0x07 |
| Adjacent Neighbor Count | The number of adjacent neighbor routers. |
| Neighbor: | The neighbor router's ID. |
USING THE WEB MANAGEMENT INTERFACE

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.

2. Click on the plus sign next to Monitor in the tree view to expand the list of monitoring options.

3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.

4. Click on the Interface link.

Displaying OSPF Route Information

To display OSPF route information for the router, use one of the following methods.

USING THE CLI

To display OSPF route information, enter the following command at any CLI level:

```
ProCurveRS> show ip ospf routes
```

<table>
<thead>
<tr>
<th>Index</th>
<th>Destination</th>
<th>Mask</th>
<th>Path_Cost</th>
<th>Type2_Cost</th>
<th>Path_Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>212.95.7.0</td>
<td>255.255.255.0</td>
<td>1</td>
<td>0</td>
<td>Intra</td>
</tr>
<tr>
<td></td>
<td>Adv_Router</td>
<td>Link_State</td>
<td>Dest_Type</td>
<td>Tag</td>
<td>Flags</td>
</tr>
<tr>
<td>173.35.1.220</td>
<td>212.95.7.251</td>
<td>Network</td>
<td>Valid</td>
<td>00000000</td>
<td>0000</td>
</tr>
<tr>
<td>Paths Out_Port</td>
<td>Next_Hop</td>
<td>Type</td>
<td>Arp_Index</td>
<td>State</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>5/6</td>
<td>209.95.7.250</td>
<td>OSPF</td>
<td>8</td>
<td>84</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Index</th>
<th>Destination</th>
<th>Mask</th>
<th>Path_Cost</th>
<th>Type2_Cost</th>
<th>Path_Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>11.3.63.0</td>
<td>255.255.255.0</td>
<td>11</td>
<td>0</td>
<td>Inter</td>
</tr>
<tr>
<td></td>
<td>Adv_Router</td>
<td>Link_State</td>
<td>Dest_Type</td>
<td>Tag</td>
<td>Flags</td>
</tr>
<tr>
<td>209.95.7.250</td>
<td>11.3.63.0</td>
<td>Network</td>
<td>Valid</td>
<td>00000000</td>
<td>0000</td>
</tr>
<tr>
<td>Paths Out_Port</td>
<td>Next_Hop</td>
<td>Type</td>
<td>Arp_Index</td>
<td>State</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>5/6</td>
<td>209.95.7.250</td>
<td>OSPF</td>
<td>8</td>
<td>84</td>
</tr>
</tbody>
</table>

Syntax: `show ip ospf routes [ip-addr]`

The `ip-addr` parameter specifies a destination IP address. If you use this parameter, only the route entries for that destination are shown.

This display shows the following information.

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>The row number of the entry in the router's OSPF route table.</td>
</tr>
<tr>
<td>Destination</td>
<td>The IP address of the route's destination.</td>
</tr>
<tr>
<td>Mask</td>
<td>The network mask for the route.</td>
</tr>
<tr>
<td>Path_Cost</td>
<td>The cost of this route path. (A route can have multiple paths. Each path represents a different exit port for the Routing Switch.)</td>
</tr>
<tr>
<td>Type2_Cost</td>
<td>The type 2 cost of this path.</td>
</tr>
</tbody>
</table>
### Table 12.5: CLI Display of OSPF Route Information (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path_Type</td>
<td>The type of path, which can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- Inter – The path to the destination passes into another area.</td>
</tr>
<tr>
<td></td>
<td>- Intra – The path to the destination is entirely within the local area.</td>
</tr>
<tr>
<td></td>
<td>- External1 – The path to the destination is a type 1 external route.</td>
</tr>
<tr>
<td></td>
<td>- External2 – The path to the destination is a type 2 external route.</td>
</tr>
<tr>
<td>Adv_Router</td>
<td>The OSPF router that advertised the route to this ProCurve Routing Switch.</td>
</tr>
<tr>
<td>Link_State</td>
<td>The link state from which the route was calculated.</td>
</tr>
<tr>
<td>Dest_Type</td>
<td>The destination type, which can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- ABR – Area Border Router</td>
</tr>
<tr>
<td></td>
<td>- ASBR – Autonomous System Boundary Router</td>
</tr>
<tr>
<td></td>
<td>- Network – the network</td>
</tr>
<tr>
<td>State</td>
<td>The route state, which can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- Changed</td>
</tr>
<tr>
<td></td>
<td>- Invalid</td>
</tr>
<tr>
<td></td>
<td>- Valid</td>
</tr>
<tr>
<td></td>
<td>This information is used by HP technical support.</td>
</tr>
<tr>
<td>Tag</td>
<td>The external route tag.</td>
</tr>
<tr>
<td>Flags</td>
<td>State information for the route entry. This information is used by HP technical support.</td>
</tr>
<tr>
<td>Paths</td>
<td>The number of paths to the destination.</td>
</tr>
<tr>
<td>Out_Port</td>
<td>The router port through which the Routing Switch reaches the next hop for this route path.</td>
</tr>
<tr>
<td>Next_Hop</td>
<td>The IP address of the next-hop router for this path.</td>
</tr>
<tr>
<td>Type</td>
<td>The route type, which can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- OSPF</td>
</tr>
<tr>
<td></td>
<td>- Static Replaced by OSPF</td>
</tr>
<tr>
<td>Arp_Index</td>
<td>The index position in the ARP table of the ARP entry for this path's IP address.</td>
</tr>
<tr>
<td>State</td>
<td>State information for the path. This information is used by HP technical support.</td>
</tr>
</tbody>
</table>

**USING THE WEB MANAGEMENT INTERFACE**

You cannot display the OSPF route table using the Web management interface.
Displaying the Routes that Have Been Redistributed into OSPF

You can display the routes that have been redistributed into OSPF. To display the redistributed routes, enter the following command at any level of the CLI:

```
ProCurveRS# show ip ospf redistribute route
  4.3.0.0 255.255.0.0 static
  3.1.0.0 255.255.0.0 static
  10.11.61.0 255.255.255.0 connected
  4.1.0.0 255.255.0.0 static
```

In this example, four routes have been redistributed. Three of the routes were redistributed from static IP routes and one route was redistributed from a directly connected IP route.

**Syntax:** `show ip ospf redistribute route [<ip-addr> <ip-mask>]`

The `<ip-addr> <ip-mask>` parameter specifies a network prefix and network mask. Here is an example:

```
ProCurveRS# show ip ospf redistribute route 3.1.0.0 255.255.0.0
  3.1.0.0 255.255.0.0 static
```

Displaying OSPF External Link State Information

To display external link state information for the router, use one of the following methods.

**USING THE CLI**

To display external link state information, enter the following command at any CLI level:

```
ProCurveRS> show ip ospf database external-link-state
```

Ospf ext link-state by router ID 130.130.130.241 are in the following:

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Aging</th>
<th>LS ID</th>
<th>Router</th>
<th>Seq(hex)</th>
<th>Chksum</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>279</td>
<td>130.132.75.48</td>
<td>130.130.130.241</td>
<td>80000004</td>
<td>00000ace</td>
<td>EXTR</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>278</td>
<td>130.132.80.112</td>
<td>130.130.130.241</td>
<td>80000004</td>
<td>0000f793</td>
<td>EXTR</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>279</td>
<td>130.132.81.208</td>
<td>130.130.130.241</td>
<td>80000004</td>
<td>000081b0</td>
<td>EXTR</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>284</td>
<td>130.132.46.224</td>
<td>130.130.130.241</td>
<td>80000004</td>
<td>000063e1</td>
<td>EXTR</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>285</td>
<td>130.132.40.64</td>
<td>140.140.140.243</td>
<td>80000004</td>
<td>0000e6ff</td>
<td>EXTR</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>286</td>
<td>130.132.33.160</td>
<td>150.150.150.245</td>
<td>80000004</td>
<td>0000751d</td>
<td>EXTR</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>296</td>
<td>130.131.241.16</td>
<td>150.150.150.245</td>
<td>80000004</td>
<td>0000e25</td>
<td>EXTR</td>
</tr>
</tbody>
</table>

**Syntax:** `show ip ospf database external-link-state [advertise <num>] [extensive] [link-state-id <ip-addr>] [router-id <ip-addr>] [sequence-number <num(Hex)>] [status <num>]`

The `advertise <num>` parameter displays the hexadecimal data in the specified LSA packet. The `<num>` parameter identifies the LSA packet by its position in the router's External LSA table. To determine an LSA packet's position in the table, enter the `show ip ospf external-link-state` command to display the table. See “Displaying the Data in an LSA” on page 12-59 for an example.

The `extensive` option displays the LSAs in decrypted format.

**NOTE:** You cannot use the `extensive` option in combination with other display options. The entire database is displayed.

The `link-state-id <ip-addr>` parameter displays the External LSAs for the LSA source specified by `<ip-addr>`.

The `router-id <ip-addr>` parameter shows the External LSAs for the specified OSPF router.

The `sequence-number <num(Hex)>` parameter displays the External LSA entries for the specified hexadecimal LSA sequence number.
The `status <num>` option shows status information.

This display shows the following information.

### Displaying OSPF Link State Information

#### USING THE WEB MANAGEMENT INTERFACE

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Monitor in the tree view to expand the list of monitoring options.
3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
4. Click on the `External Link State DB` link.

#### Displaying OSPF Link State Information

To display link state information for the router, use one of the following methods.

#### USING THE CLI

To display link state information, enter the following command at any CLI level:

```
ProCurveRS> show ip ospf database link-state
```

**Syntax:** `show ip ospf database link-state [advertise <num>] | [asbr] | [extensive] | [link-state-id <ip-addr>] | [network] | [nssa] | [opaque-area] | [router] | [router-id <ip-addr>] | [sequence-number <num(Hex)>] | [status <num>] | [summary]`

The `advertise <num>` parameter displays the hexadecimal data in the specified LSA packet. The `<num>` parameter identifies the LSA packet by its position in the router’s External LSA table. To determine an LSA packet’s position in the table, enter the `show ip ospf external-link-state` command to display the table. See “Displaying the Data in an LSA” on page 12-59 for an example.

The `asbr` option shows ASBR information.

The `extensive` option displays the LSAs in decrypted format.

**NOTE:** You cannot use the `extensive` option in combination with other display options. The entire database is displayed.

---

**Table 12.6: CLI Display of OSPF External Link State Information**

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
<td>The OSPF area the router is in.</td>
</tr>
<tr>
<td>Aging</td>
<td>The age of the LSA, in seconds.</td>
</tr>
<tr>
<td>LS ID</td>
<td>The ID of the link-state advertisement from which the Routing Switch learned this route.</td>
</tr>
<tr>
<td>Router</td>
<td>The router IP address.</td>
</tr>
<tr>
<td>Seq(hex)</td>
<td>The sequence number of the LSA. The OSPF neighbor that sent the LSA stamps it with a sequence number to enable the Routing Switch and other OSPF routers to determine which LSA for a given route is the most recent.</td>
</tr>
<tr>
<td>Chksum</td>
<td>A checksum for the LSA packet. The checksum is based on all the fields in the packet except the age field. The Routing Switch uses the checksum to verify that the packet is not corrupted.</td>
</tr>
<tr>
<td>Type</td>
<td>The route type, which is always EXTR (external).</td>
</tr>
</tbody>
</table>
The **link-state-id** `<ip-addr>` parameter displays the External LSAs for the LSA source specified by `<IP-addr>`.

The **network** option shows network information.

The **nssa** option shows network information.

The **opaque-area** option shows information for opaque areas.

The **router-id** `<ip-addr>` parameter shows the External LSAs for the specified OSPF router.

The **sequence-number** `<num(Hex)>` parameter displays the External LSA entries for the specified hexadecimal LSA sequence number.

The **status** `<num>` option shows status information.

The **summary** option shows summary information.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.

2. Click on the plus sign next to Monitor in the tree view to expand the list of monitoring options.

3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.

4. Click on the Link State DB link.

**Displaying the Data in an LSA**

You can use the CLI to display the data the Routing Switch received in a specific External LSA packet or other type of LSA packet. For example, to display the LSA data in entry 3 in the External LSA table, enter the following command:

```
ProCurveRS> show ip ospf database external-link-state advertise 3
05 84 02 05 82 83 0d 60 82 82 f1 80 00 00 02 e4 05
00 24 ff ff ff f0 80 00 00 00 00 00 00 00 00 00 00
```

**Syntax:** show ip ospf database external-link-state [advertise `<num>`] | [link-state-id `<ip-addr>`] | [router-id `<ip-addr>`] | [sequence-number `<num(Hex)>`] | [status `<num>`]

To determine an external LSA's or other type of LSA's index number, enter one of the following commands to display the appropriate LSA table:

- **show ip ospf database link-state advertise `<num>`** – This command displays the data in the packet for the specified LSA.

- **show ip ospf database external-link-state advertise `<num>`** – This command displays the data in the packet for the specified external LSA.

For example, to determine an external LSA's index number, enter the following command:

```
ProCurveRS> show ip ospf external-link-state
Index Aging LS ID Router Seq(hex) Chksum
1 1332 130.132.81.208 130.130.130.241 80000002 000085ae
2 1325 130.132.116.192 130.130.130.241 80000002 0000a37d
3 1330 130.132.88.112 130.130.130.241 80000002 0000fb91
4 1333 130.132.75.48 130.130.130.241 80000002 00000ecc
5 1338 130.132.46.224 130.130.130.241 80000002 000067df
```

*additional entries omitted for brevity...*
**USING THE WEB MANAGEMENT INTERFACE**

You cannot display the contents of an LSA using the Web management interface.

**Displaying OSPF Virtual Neighbor Information**

To display OSPF virtual neighbor information for the router, use one of the following methods.

**USING THE CLI**

To display OSPF virtual neighbor information, enter the following command at any CLI level:

```
ProCurveRS> show ip ospf virtual-neighbor
```

*Syntax:* show ip ospf virtual-neighbor [<num>]

The `<num>` parameter displays the table beginning at the specified entry number.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Monitor in the tree view to expand the list of monitoring options.
3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
4. Click on the Virtual Neighbor link.

**Displaying OSPF Virtual Link Information**

To display OSPF virtual link information for the router, use one of the following methods.

**USING THE CLI**

To display OSPF virtual link information, enter the following command at any CLI level:

```
ProCurveRS> show ip ospf virtual-link
```

*Syntax:* show ip ospf virtual-link [<num>]

The `<num>` parameter displays the table beginning at the specified entry number.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Monitor in the tree view to expand the list of monitoring options.
3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
4. Click on the Virtual Interface link.

**Displaying OSPF ABR and ASBR Information**

To display OSPF ABR and ASBR information for the router, use one of the following methods.

**USING THE CLI**

To display OSPF ABR and ASBR information, enter the following command at any CLI level:

```
ProCurveRS> show ip ospf border-routers
```

*Syntax:* show ip ospf border-routers [<ip-addr>]

The `<ip-addr>` parameter displays the ABR and ASBR entries for the specified IP address.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Monitor in the tree view to expand the list of monitoring options.
3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
4. Click on the ABR ASBR Routers link.

Displaying OSPF Trap Status
To display the state (enabled or disabled) of the OSPF traps, use one of the following methods.

All traps are enabled by default when you enable OSPF. To disable or re-enable an OSPF trap, see “Modify OSPF Traps Generated” on page 12-42.

USING THE CLI
To display the state of each OSPF trap, enter the following command at any CLI level:

    ProCurveRS> show ip ospf trap

    Interface State Change Trap:                      Enabled
    Virtual Interface State Change Trap:              Enabled
    Neighbor State Change Trap:                       Enabled
    Virtual Neighbor State Change Trap:               Enabled
    Interface Configuration Error Trap:               Enabled
    Virtual Interface Configuration Error Trap:       Enabled
    Interface Authentication Failure Trap:            Enabled
    Virtual Interface Authentication Failure Trap:    Enabled
    Interface Receive Bad Packet Trap:                Enabled
    Virtual Interface Receive Bad Packet Trap:        Enabled
    Interface Retransmit Packet Trap:                 Enabled
    Virtual Interface Retransmit Packet Trap:         Enabled
    Originate LSA Trap:                               Enabled
    Originate MaxAge LSA Trap:                        Enabled
    Link State Database Overflow Trap:                Enabled
    Link State Database Approaching Overflow Trap:   Enabled

Syntax: show ip ospf trap

USING THE WEB MANAGEMENT INTERFACE
1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to OSPF in the tree view to expand the list of OSPF option links.
4. Click on the Trap link to display the OSPF Trap panel.