Enabling OSPF

Before configuring OSPF, first enable OSPF data-gathering from each Lumeta component's system interface card. This feature enables Lumeta Command Centers and Scouts behave like non-forwarding routers—listening to and recording route information as if it were a router, but not forwarding network traffic like a true >router does.

Provide each Lumeta system in a zone with the identifiers so that other routers will provide it with routing information.

1. Browse **Settings** > **Lumeta Systems**.
2. Select the first available system.
3. Browse to the **eth0** (or eth1) tab for the system's interface and then click **Edit OSPF**.
4. Complete the form.
    a. Set the Area to 0.
    b. Assign a unique Router ID such as 1.1.1.1 that does not match any other IP addresses on your system. Consider naming subsequent systems using a similar pattern such as 2.2.2.2, 3.3.3.3, and 4.4.4.4
    c. Select an Authentication Type such as None.
    By default, passwords are not included in OSPF packets.
    d. Optionally add an Authentication Phrase (i.e., test)
    Every packet carries an 8-byte password. Received packets lacking this password are ignored. This option is not available in OSPFv3.authentication cryptographic. An authentication code is appended to every packet. The specific cryptographic algorithm is selected by option algorithm for each key. The default cryptographic algorithm for OSPFv2 keys is Keyed-MD5 and for OSPFv3 keys is HMAC-SHA-256. Passwords are not sent open via network, so this mechanism is quite secure.
    e. Select **Enable OSPF Data Gathering**.
5. Click **Update**.

Next, you may want to configure OSPF on a particular collector.