



ISIS Local Microloop Protection

The ISIS Local Microloop Protection feature enables link-state routing protocols, such as the Intermediate System-to-Intermediate System (ISIS) protocol, to prevent or avoid local microloops during network convergence after a link-down event.

- [Information About ISIS Local Microloop Protection, on page 1](#)
- [How to Configure ISIS Local Microloop Protection, on page 2](#)
- [Configuration Examples for ISIS Local Microloop Protection, on page 4](#)
- [Additional References for IS-IS Local Microloop Protection, on page 5](#)
- [Feature Information for ISIS Local Microloop Protection, on page 5](#)

Information About ISIS Local Microloop Protection

.

Microloops

When changes occur in a network topology because of the failure or restoration of a link or a network device, IP Fast Reroute enables rapid network convergence by moving traffic to precomputed backup paths until regular convergence mechanisms move traffic to a newly computed best path, also known as a post-convergence path. This network convergence may cause short microloops between two directly or indirectly connected devices in the topology. Microloops are caused when different nodes in the network calculate alternate paths at different times and independently of each other. For instance, if a node converges and sends traffic to a neighbor node, which has not converged yet, traffic may loop between the two nodes.

Microloops may or may not result in traffic loss. If the duration of a microloop is short, that is the network converges quickly, packets may loop for a short duration before their TTL expires. Eventually, the packets will get forwarded to the destination. If the duration of the microloop is long, that is one of the routers in the network is slow to converge, packets may expire their TTL or the packet rate may exceed the bandwidth, and packets may get dropped.

Microloops that are formed between a failed device and its neighbors are called local uloops, whereas microloops that are formed between devices that are multiple hops away are called remote uloops. The ISIS Local Microloop Protection feature helps networks avoid local uloops. Local uloops are usually seen when there is no local loop-free alternate (LFA) path available, especially in ring or square topologies. In such topologies, remote LFAs provide backup paths for the network. However, the fast-convergence benefit of the remote LFA is at risk because of the high probability of uloop creation. The ISIS Local Microloop Protection feature can be used to avoid microloops or local uloops in such topologies.

When to Use Microloop Avoidance

The ISIS Local Microloop Protection feature supports the following local link down events

- Interface-down events
- Adjacency-down events due to BFD sessions going down.
- Adjacency-down events due to neighbor holdtime expiration

The ISIS Local Microloop Protection feature can be used whether or not a topology is supported by loop-free alternates (LFAs). When you use this feature for prefixes that have repair paths installed in the forwarding plane, this feature will support interface-down events and adjacency-down events if bidirectional forwarding detection (BFD) sessions are down. If this feature is used whether or not a repair path has been installed in the forwarding plane, this feature will also support adjacency-down events caused by neighbor holdtime expiration.

The value of using this feature also depends on whether the remote event that caused loss of adjacency on the neighbor is detectable by the local forwarding plane; that is whether the forwarding plane will react and switch to using preprogrammed repair paths. For instance, when a link fails, the reaction time of the local forwarding plane depends on the media. If the media is optical, the failure is likely to be detected within milliseconds, in which case microloop avoidance is useful. If the media is copper, the local detection will be much slower or nonexistent, in which case using microloop avoidance is disadvantageous. However, if the timeout of the neighbor adjacency is due to reasons other than link failure, such as local congestion, lack of CPU time, and long input queues, these reasons are undetectable by the local forwarding plane and therefore, are not good candidates for microloop avoidance.



Note When remote loop-free alternates (RLFAs) are enabled in a network, microloop avoidance is enabled by default for all protected prefixes (prefixes that have repair paths).

How to Configure ISIS Local Microloop Protection

Configuring Microloop Protection

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis***[area-tag]*
4. **microloop avoidance** [**disable** | **protected**]
5. **end**
6. **show running-config**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | router isis[area-tag] Example: Device(config)# router isis | Enables Intermediate System-to-Intermediate System (IS-IS) as the IP routing protocol and enters router configuration mode. |
| Step 4 | microloop avoidance [disable protected] Example: Device(config-router)# microloop avoidance protected | Enables local microloop avoidance for protected prefixes. Note If you use the microloop avoidance command without any of the keywords, microloop avoidance is configured for all prefixes in the network, whether or not they are protected. The protected keyword ensures that microloop avoidance is enabled only for protected prefixes. |
| Step 5 | end Example: Device(config-router)# end | Returns to privileged EXEC mode. |
| Step 6 | show running-config Example: Device# show running-config | Displays the current running configuration. |

Modifying the RIB-update value

SUMMARY STEPS

1. enable
2. configure terminal
3. router isis [area-tag]
4. microloop avoidance[rib-update-delay delay-time]
5. end
6. show running-config

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | router isis [area-tag] Example: Device(config)# router isis | Enables Intermediate System-to-Intermediate System (IS-IS) as the IP routing protocol and enters router configuration mode. |
| Step 4 | microloop avoidance[rib-update-delay delay-time] Example: Device(config-router)# microloop avoidance rib-update-delay 6000 | Configures Routing Information Base (RIB) update delay value to avoid microloops in a network. |
| Step 5 | end Example: Device(config-router)# end | Returns to privileged EXEC mode. |
| Step 6 | show running-config Example: Device# show running-config | Displays the current running configuration. |

Configuration Examples for ISIS Local Microloop Protection

Example: Configuring Microloop Protection

The following example shows how to configure microloop protection for protected prefixes:

```
Device> enable
Device# configure terminal
Device(config)# router isis
Device(config-router)# microloop avoidance protected
Device(config-router)# end
```

The following example shows how to configure microloop avoidance for protected and unprotected prefixes:

```
Device> enable
Device# configure terminal
Device(config)# router isis
```

```
Device(config-router)# microloop avoidance
Device(config-router)# end
```

The following example shows how to modify the rib-update delay:

```
Device> enable
Device# configure terminal
Device(config)# router isis
Device(config-router)# microloop avoidance rib-update-delay 6000
Device(config-router)# end
```

Additional References for IS-IS Local Microloop Protection

Related Documents

| Related Topic | Document Title |
|--|---|
| IS-IS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples | <i>Cisco IOS IP Routing: ISIS Command Reference</i> |
| Overview of IS-IS concepts | “Integrated IS-IS Routing Protocol Overview” module |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for ISIS Local Microloop Protection

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

