

Silent Host Detection in Cisco SD-Access

September 2026

Document purpose and usage

This document explains how silent host detection identifies silent and previously undiscovered endpoints in enterprise and manufacturing Cisco SD-Access fabric networks. It describes the on-demand approach that the feature uses for host discovery, without interval-based probing and without fabric-wide flooding.

Use this document to assess how silent host detection improves endpoint reachability, endpoint visibility, and operational efficiency in networks that contain Internet of Things (IoT) devices and other endpoints that communicate at intervals.

After you read this document, you can

- evaluate silent host detection against your fabric design,
- enable silent host detection for a fabric subnet in Cisco Catalyst Center, and
- verify that each fabric edge node registers the subnet with the map server.

Target audience

This document explains how silent host detection identifies silent or previously undiscovered endpoints in enterprise and manufacturing Cisco SD-Access fabric networks. It describes the on-demand, scalable approach that the feature uses for host discovery, without interval-based probing and without fabric-wide flooding. It helps you understand the capabilities, the benefits, and the use cases for the feature.

Use this document to assess how silent host detection improves endpoint reachability, visibility, and operational efficiency in networks that contain IoT devices and devices that communicate at intervals.

Introduction

Enterprise and manufacturing networks support many endpoints that enter a silent or low-power state. These endpoints include IoT devices and operational technology devices.

When an endpoint becomes inactive, on-demand network discovery cannot identify or locate it. As a result, applications lose reachability to the endpoint, and the fabric loses visibility into it.

Silent host detection addresses this challenge. When a device sends traffic to an unknown endpoint, the Locator/ID Separation Protocol (LISP) control plane starts controlled, on-demand discovery.

This approach

- reduces flooding,
- improves scalability, and
- supports efficient endpoint discovery in enterprise and manufacturing environments.

Silent host challenge

The LISP architecture learns network information on demand and scales the network to actual traffic requirements. This on-demand approach works when endpoints register with the LISP mapping system.

When an endpoint becomes silent, it stops communicating with the network. The endpoint remains physically connected, but the mapping system no longer holds its location and reachability information.

Silent endpoints are common in environments that contain IoT devices and other devices that reduce activity to conserve energy. In enterprise and manufacturing networks, some devices communicate only at fixed intervals or after an event. When a device sends traffic to such an endpoint, the fabric must check whether the destination is a silent host or a nonexistent host.

Traditional methods for discovering silent hosts add network overhead.

- Probing that is based on Embedded Event Manager (EEM) scripts checks address ranges at fixed intervals. The probe generates traffic on many edge ports, and it requires you to estimate how often endpoints become silent.
- Approaches that are based on Wake-on-LAN convert traffic for an unknown destination into a directed broadcast. The broadcast floods the fabric every time a device sends traffic to a silent host.

These approaches limit your control over silent host discovery, restrict scale, and generate traffic even when the destination does not exist. Use the existing LISP on-demand resolution process instead and start discovery only when the fabric must locate an unknown destination.

Cisco LISP silent host detection overview

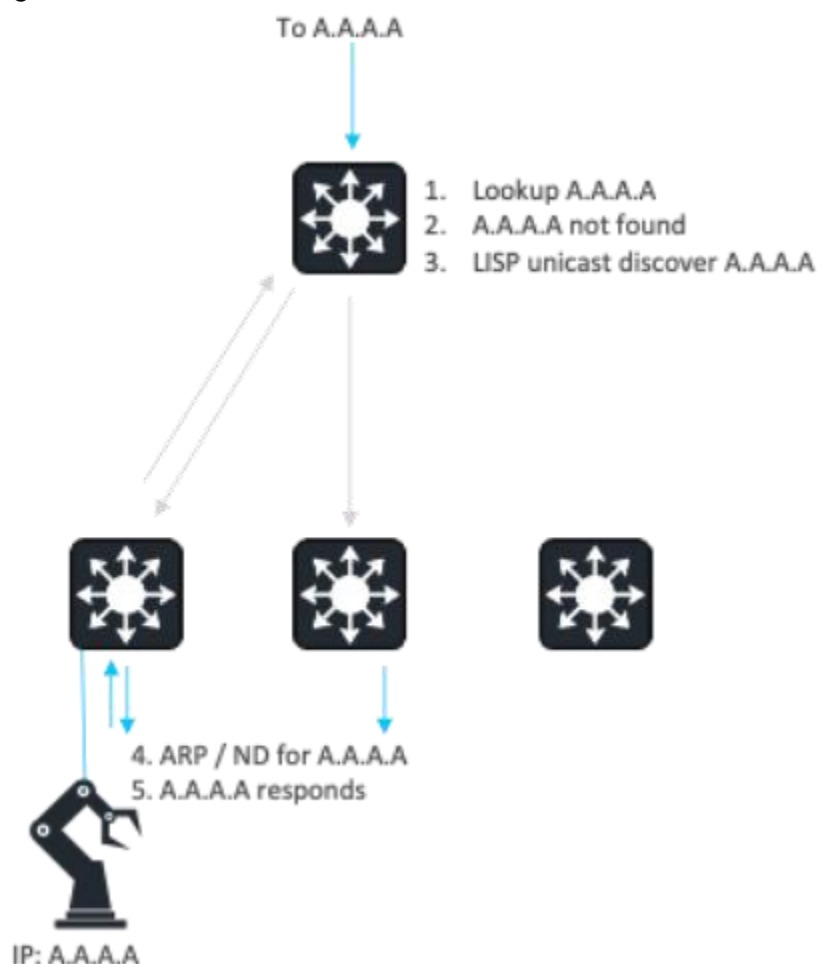
Silent host detection uses the LISP on-demand resolution process to identify endpoints that are silent or unregistered with the mapping system. When a device sends traffic to an unknown destination, the fabric starts the LISP map-resolution process. The mapping system evaluates the request and determines whether you enabled silent host discovery for the destination subnet or segment.

If a matching silent host discovery entry exists, the mapping system sends a discovery publication to the fabric edge nodes that host that subnet or segment. Each fabric edge node probes its local ports for the requested address range. If a silent endpoint is present, the endpoint responds to the probe, and the fabric edge node discovers the endpoint through the standard host-detection process. The fabric edge node then registers the endpoint with the mapping system, and the fabric forwards subsequent traffic to the endpoint.

The feature separates two actions. First, fabric edge nodes register the subnets or segments for which they can perform discovery. The mapping system then invokes the applicable fabric edge nodes only when a map-resolution request requires silent host discovery.

This design removes continuous network-wide probing and flooding. It also controls how often discovery starts, because the mapping system throttles repeated requests and probing activity. The design supports IPv4 and IPv6 subnet-based silent host detection.

Figure 1. LISP silent host detection overview



Solution architecture and workflow

Silent host detection uses these LISP components:

- **Fabric edge node (xTR):** Provides local host discovery capability.
- **Mapping system:** Maintains silent host discovery registrations and starts discovery.
- **Border node:** Starts resolution when traffic enters the fabric.
- **SISF:** Probes the local ports and reports discovered hosts to LISP.

Capability registration

A fabric edge node registers its ability to perform silent host discovery for a locally connected subnet or VLAN. The node associates the registration with the dynamic endpoint identifier (EID) group and sends the registration to the mapping system through the LISP control plane.

The mapping system stores these registrations in a separate Silent Host Discovery table. It associates each subnet or segment with the fabric edge nodes that can perform discovery. When several fabric edge nodes register support for the same subnet, the mapping system maintains the corresponding list of nodes.

Discovery trigger

The originating device sends a map request to the mapping system when the LISP mapping database does not contain the destination endpoint. A border node, an ITR, or another LISP device that handles the traffic generates the request.

The mapping system returns the expected negative map reply for the unknown destination. At the same time, the mapping system evaluates the requested address against the Silent Host Discovery table. If the longest prefix lookup identifies a matching silent host discovery entry, the mapping system starts the discovery process.

The request can identify a specific host address or a covering subnet. The prefix size controls the scope of the probe. A larger prefix lets the fabric edge node discover several silent hosts in one operation, but the node also probes more addresses.

Publication and local probing

After the mapping system identifies the applicable registration, it sends a publication (Map-Notify) to each registered fabric edge node. The publication contains the address or prefix that the node must discover, and it uses the silent host discovery encoding.

When the fabric edge node receives the publication, the node determines the associated dynamic EID group and calls the SISF probing function. SISF probes the local interfaces or ports that belong to the subnet or VLAN, and it probes both IPv4 and IPv6 hosts.

If a silent endpoint is present, the endpoint responds to the probe. SISF reports the result to LISP, and the fabric edge node registers the endpoint with the mapping system. The mapping system then advertises the discovered host to other LISP devices through the standard control-plane process.

Map-cache update and traffic convergence

After the endpoint registers, the mapping system publishes the host mapping to subscribed devices. Each device that installed a negative or unknown mapping clears that entry and installs the new host mapping.

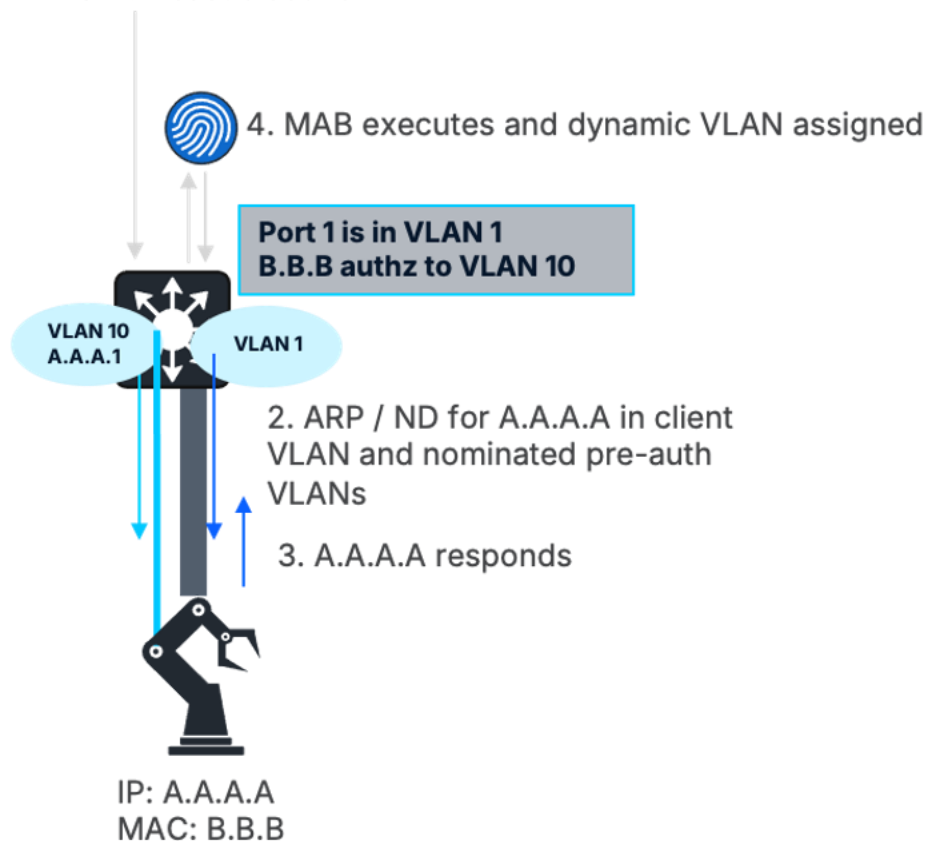
This update allows subsequent traffic to converge on the correct fabric edge node.

LISP pre-authorization VLAN

When a host becomes silent, port-based authentication for that host times out. The switch then removes the dynamic VLAN assignment for the host, and the port joins the default VLAN, VLAN 1, or the static VLAN that you configured for that port.

The preauthentication VLAN replicates the discovery probe into the VLAN that you define. The fabric edge node then discovers the silent host and delivers traffic to the host from the fabric VLAN.

1. LISP unicast discover A.A.A.A



Deployment scenarios and use cases

Use silent host detection in LISP-based enterprise networks that contain endpoints which become inactive while they stay connected to the network. The feature applies to environments that contain IoT devices, low-power endpoints, and devices that communicate at intervals.

Enterprise and manufacturing networks

In an enterprise or manufacturing deployment, a device sends traffic only at intervals. When another endpoint requires access to that device, the LISP mapping database might not yet contain the destination. Silent host detection responds to the request and locates the endpoint through a controlled probe.

Use this approach when you must preserve on-demand operation and still reach endpoints that become silent. It removes scheduled probing and prevents flooding when a device sends traffic to an unknown endpoint.

Single-site deployment

In a single-site deployment, several fabric edge nodes connect to local endpoint subnets. A border node or another LISP device starts a map-resolution request when a device sends traffic to an unknown host. A central map server, or an MSMR, evaluates the request and invokes the fabric edge nodes that registered the corresponding subnet.

Each applicable fabric edge node probes its local ports. The node that receives a response from the silent host discovers and registers the endpoint. The mapping system then distributes the host information to the devices that require it.

Multisite deployment

In a multisite deployment, each site can contain its own borders, fabric edges, and mapping systems. The site mapping system drives silent host discovery within the local site.

Border devices advertise aggregate fabric subnets to the transit control plane. When traffic reaches the border for the site containing the destination subnet, the border queries the site mapping system. The site mapping system then follows the same discovery process used in a single-site deployment and invokes the registered fabric edges.

This preserves the local nature of the discovery process while allowing traffic to reach endpoints across multiple sites.

Extranet scenarios

Silent host detection supports the common extranet case, in which a provider instance or an external network sends traffic to a silent host in a subscriber instance.

After the traffic reaches the border node, the border node applies the relevant VRF or policy handling and sends the map request to the mapping system in the subscriber instance. Silent host discovery then proceeds as it does for a nonextranet destination.

Enabling Silent Host Detection with Cisco Catalyst Center

Silent host detection is disabled by default. Enable silent host detection for the applicable dynamic EID group. When you add the configuration, the fabric edge node registers its silent host discovery capability with the mapping system.

This section describes the Cisco Catalyst Center workflow, and the device verification steps for a Cisco SD-Access deployment.

Prerequisites

Silent host detection requires Cisco Catalyst Center Release 3.2.3 and Cisco IOS XE Release 26.1.2 in a fabric deployment.

Refer to [Catalyst center 3.2.3 release notes](#).

Catalyst Center configuration workflow

Procedure 1. To enable silent host detection with Cisco Catalyst Center:

Step 1. If the ports that connect to silent hosts belong to a VLAN other than VLAN 1, mark the subnet as a candidate for the preauthentication VLAN.

Step 2. Enable silent host detection for the subnet so that the fabric edge nodes register the subnet for silent host discovery.

Figure 2. Silent host detection enabled for a subnet
Create Anycast Gateways

Configuration Attributes

Each Layer 3 Virtual Network can be assigned one or more Anycast Gateways. An Anycast Gateway has an associated VLAN and Layer 2 Virtual Network. Each of these has multiple configuration parameters and attributes.

Search

Layer 3 Virtual Networks

.../San Jose/SJC23

VN1

IP Address Pool

IOT [25.1.2.0/24]

+ Add additional IP address pools

☐ IP-Directed Broadcast ⓘ ☐ Intra-Subnet Routing ⓘ ☐ TCP MSS Adjustment ⓘ

☐ Silent Host Discovery ⓘ

VLAN

VLAN Name: 25_1_2_0-VN1

VLAN ID: 1001 ⓘ

Traffic Type: ☒ Data ☐ Voice

Security Group: Security Group

☒ Auto generate VLAN name ☒ Candidate Pre-Auth VLAN ⓘ

Layer 2 Virtual Network

Create Anycast Gateways

Each Layer 3 Virtual Network can be assigned one or more Anycast Gateways. An Anycast Gateway has an associated VLAN and Layer 2 Virtual Network. Each of these has multiple configuration parameters and attributes.

✓

2

3

4

Q Search

Layer 3 Virtual Networks

.../San Jose/SJC23

VN1

Anycast Gateway

IP Address Pool

Client [25.1.1.0/24]

+ Add additional IP address pools

☐ IP-Directed Broadcast ⓘ
 ☐ Intra-Subnet Routing ⓘ
 ☐ TCP MSS Adjustment ⓘ

☒ Silent Host Discovery ⓘ
[Edit Pre-Auth VLANs](#)

VLAN

VLAN Name **VLAN ID** **Traffic Type**

25_1_1_0-VN1
☒ Data ☐ Voice
 Security Group
☐ Critical VLAN

☒ Auto generate VLAN name
 ☐ Candidate Pre-Auth VLAN ⓘ

Step 3. If the port falls back to VLAN 1 or to another static VLAN, edit the pre-authentication VLAN setting and select each VLAN that must receive the probe.

Figure 3. Preauthentication VLAN selection

Create Anycast Gateways

✓

2

3

4

Q Search

2 available

☐ default (1)
 ☐ 25_1_2_0-VN1 (1001)

0/2 selected

Q Search

No data selected

Cancel

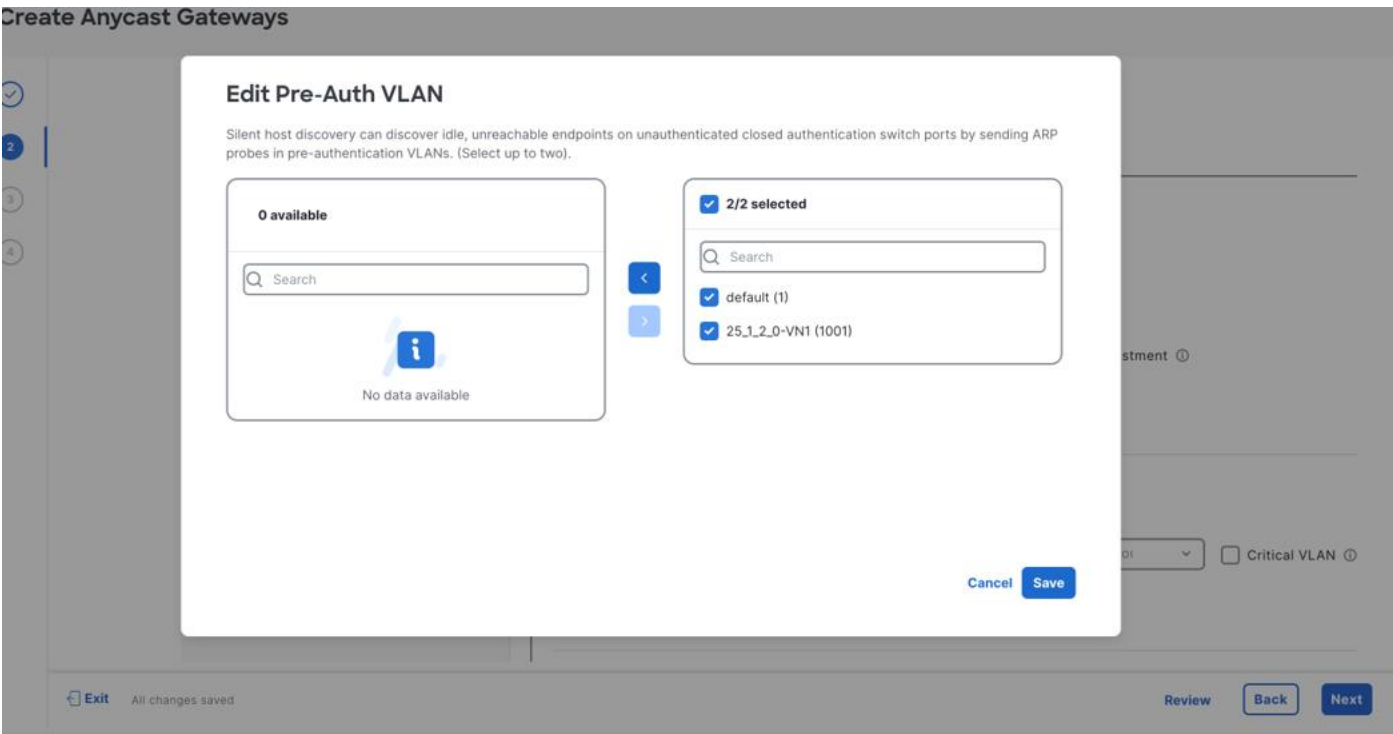
Save

Exit

All changes saved

Review

Back



Note: Cisco Catalyst Center does not enable flooding or directed broadcast for a subnet that uses silent host discovery.

SJC23View Site HierarchySite Actions ⓘ

Fabric InfrastructureLayer 3 Virtual NetworksLayer 2 Virtual NetworksAnycast GatewaysWireless SSIDsAuthentication TemplatePort Assignment

Q Search

RefreshExport+ Create Anycast Gatewaysⓘ

tier	Associated VLAN Name	Associated VLAN ID	Associated Layer 3 Virtual Network	Fabric Enabled Wireless	Wireless Flooding	Layer 2 Flooding	Resource Guard	Critical VLAN	IP-Directed Broadcast
	25_1_1_0-VN1	1022	VN1	--	--	--	--	--	--
	25_1_2_0-VN1	1001	VN1	--	--	--	--	--	--
	TEST_DHCP	600	VN1	--	--	✓	--	--	--

Verification and monitoring

Procedure 2. To verify silent host detection:

Step 1. Check the router LISP configuration on the fabric edge node.

Step result: Silent host detection is enabled for the EID.

Figure 4. Silent host detection enabled for the EID

```
EX1-FE-9300-1#sh run | s router lisp
router lisp
domain-id 1392658141
locator-table default
locator-set rloc_ab4440e9-fac3-42c2-9d91-10166ff07bd0
IPv4-interface Loopback0 priority 10 weight 10
exit-locator-set
!
locator default-set rloc_ab4440e9-fac3-42c2-9d91-10166ff07bd0
service ipv4
encapsulation vxlan
itr map-resolver 204.1.2.3
itr map-resolver 204.1.2.11
etr map-server 204.1.2.3 key 6 ePdQd^DKQgFQgA^PhB[[gdGLCdUBLVBCZCfKV^CgcEBC^
etr map-server 204.1.2.3 proxy-reply
etr map-server 204.1.2.11 key 6 \YHKFWMOXUECCeAbPbLXN\EGg_HFXFZ]PWM]BP'AAO_AC
etr map-server 204.1.2.11 proxy-reply
etr
sgt
no map-cache away-eids send-map-request
proxy-itr 204.1.2.1
exit-service-ipv4
!
service ethernet
itr map-resolver 204.1.2.3
itr map-resolver 204.1.2.11
itr
etr map-server 204.1.2.3 key 6 QQYZWI[AA^feIMPHAhfbAN^cZNi]Z_dJOUKggeTQRO_GM
etr map-server 204.1.2.3 proxy-reply
etr map-server 204.1.2.11 key 6 KXMJ`\TBX\^dIa]MHRGLISIWgNX`IbKTbCU[RSdCDHGci
etr map-server 204.1.2.11 proxy-reply
etr
exit-service-ethernet
!
instance-id 4099
remote-rloc-probe on-route-change
dynamic-eid 25_1_1_0-VN1-IPV4
database-mapping 25.1.1.0/24 locator-set rloc_ab4440e9-fac3-42c2-9d91-10166ff07bd0 silent-host-detection
exit-dynamic-eid
!
dynamic-eid 25_1_2_0-VN1-IPV4
database-mapping 25.1.2.0/24 locator-set rloc_ab4440e9-fac3-42c2-9d91-10166ff07bd0
exit-dynamic-eid
!
service ipv4
eid-table vrf VN1
map-cache 0.0.0.0/0 map-request
exit-service-ipv4
!
exit-instance-id
```

```

instance-id 8188
remote-rloc-probe on-route-change
service ethernet
  eid-table vlan 600
  broadcast-underlay 239.0.17.1
  flood arp-nd
  flood unknown-unicast
  database-mapping mac locator-set rloc_ab4440e9-fac3-42c2-9d91-10166ff07bd0
  dynamic-eid detection multiple-addr bridged-vm
exit-service-ethernet
!
exit-instance-id
!
instance-id 8189
remote-rloc-probe on-route-change
service ethernet
  eid-table vlan 1001
  database-mapping mac locator-set rloc_ab4440e9-fac3-42c2-9d91-10166ff07bd0
exit-service-ethernet
!
exit-instance-id
!
instance-id 8190
remote-rloc-probe on-route-change
service ethernet
  eid-table vlan 1021
  database-mapping mac locator-set rloc_ab4440e9-fac3-42c2-9d91-10166ff07bd0
exit-service-ethernet
!
exit-instance-id
!
ipv4 locator reachability minimum-mask-length 32
ipv4 source-locator Loopback0
exit-router-lisp
FX1-FE-9300-1#

```

Step 2. Check the VLAN interface configuration.

Step result: The VLAN interface includes the LISP pre-authentication VLANs configuration for the default VLAN and for the pre-authentication VLAN that you selected for silent host detection.

Figure 5. Pre-authentication VLAN configuration on the VLAN interface

```
EX1-FE-9300-1#sh run int vlan 1021
Building configuration...

Current configuration : 348 bytes
!
interface Vlan1021
  description Configured from Catalyst Center
  mac-address 0000.0c9f.f068
  vrf forwarding VN1
  ip address 25.1.1.1 255.255.255.0
  ip helper-address 58.1.1.2
  no ip redirects
  ip proxy-arp
  ip route-cache same-interface
  no lisp mobility liveness test
  lisp mobility 25_1_1_0-VN1-IPV4
  lisp silent-host pre-auth vlan 1 1001
end

EX1-FE-9300-1#sh run int vlan 1001
Building configuration...

Current configuration : 309 bytes
!
interface Vlan1001
  description Configured from Catalyst Center
  mac-address 0000.0c9f.fb7a
  vrf forwarding VN1
  ip address 25.1.2.1 255.255.255.0
  ip helper-address 58.1.1.2
  no ip redirects
  ip proxy-arp
  ip route-cache same-interface
  no lisp mobility liveness test
  lisp mobility 25_1_2_0-VN1-IPV4
end

EX1-FE-9300-1#sh run int vlan 1
Building configuration...

Current configuration : 62 bytes
!
interface Vlan1
  no ip address
  ip proxy-arp
  shutdown
end

EX1-FE-9300-1#
```

Step 3. Verify that LISP on the fabric edge node enabled silent host detection for the subnet and registered the subnet with the map server.

Figure 6. Silent host detection registration on the fabric edge node

```
EX1-FE-9300-1#sh lisp instance-id 4099 ipv4 database silent-host-detection
LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf VN1 (IID 4099), LSBs: 0x1
Entries total 1, no-route 0, inactive 0, do-not-register 0

25.1.1.0/24, inherited from default locator-set rloc_ab4440e9-fac3-42c2-9d91-10166ff07bd0
  Uptime: 2d20h, Last-change: 2d20h, Last-Silent-Host-Probe: never
  Domain-ID: local
  Service-Insertion: N/A
  Locator    Pri/Wgt  Source      State
  204.1.2.1   10/10   cfg-intf    site-self, reachable
EX1-FE-9300-1#
```

Step 4. Verify on the map server that every fabric edge node registered the EID subnet for silent host detection.

Figure 7. Fabric edge node registrations on the map server

```
EX1-FB-9300#sh lisp instance-id 4099 ipv4 server silent-host-detection
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport

Site Name      Last      Up      Who Last      Inst      EID Prefix
Register      Registered
site_uci       never    no      --            4099      0.0.0.0/0
               00:05:33 yes#    204.1.2.1:13698 4099      25.1.1.0/24
               never    no      --            4099      25.1.2.0/24
```

EX1-FB-9300#\$stance-id 4099 ipv4 server silent-host-detection 25.1.1.0/24

LISP Site Registration Information

Site name: site_uci

Description: map-server configured from Catalyst Center

Allowed configured locators: any

Requested EID-prefix:

EID-prefix: 25.1.1.0/24 instance-id 4099

First registered: 00:05:44

Last registered: 00:05:44

Routing table tag: 0

Origin: Configuration, accepting more specifics

Merge active: Yes

Proxy reply: Yes

Skip Publication: No

Force Withdraw: No

TTL: 1d00h

State: complete

Extranet IID: Unspecified

Registration errors:

Authentication failures: 0

Allowed locators mismatch: 0

ETR 204.1.2.1:13698

last registered 00:05:44, proxy-reply, map-notify

TTL 1d00h, merge, hash-function sha1

state complete, no security-capability

nonce 0x27210374-0x6AFE4AB3

xTR-ID 0x3D495888-0x3ACC7192-0x58192C63-0xF43EA779

site-ID unspecified

Domain-ID 1392658141

Multihoming-ID unspecified

sourced by reliable transport

Locator	Local	State	Pri/Wgt	Scope	RDP
204.1.2.1	yes	up	10/10	IPv4 none	[-]

ETR 204.1.2.2:53066

last registered 00:05:44, proxy-reply, map-notify

TTL 1d00h, merge, hash-function sha1

state complete, no security-capability

nonce 0xEC4E0977-0x7F55BE59

xTR-ID 0xAC2CEE30-0x620D9607-0x80120368-0xAE7C3A51

site-ID unspecified

Domain-ID 1392658141

Multihoming-ID unspecified

sourced by reliable transport

Locator	Local	State	Pri/Wgt	Scope	RDP
204.1.2.2	yes	up	10/10	IPv4 none	[-]

Merged locators

Locator	Local	State	Pri/Wgt	Scope	Registering ETR	RDP
204.1.2.1	yes	up	10/10	IPv4 none	204.1.2.1:13698	[-]
204.1.2.2	yes	up	10/10	IPv4 none	204.1.2.2:53066	[-]

EX1-FB-9300#

Benefits and conclusion

Silent host detection provides a controlled method for discovering endpoints that are silent, intermittently active, or unregistered in the LISP mapping database. It uses the existing LISP map-resolution process and starts discovery only when a device requests the destination.

The approach removes continuous probing and network-wide flooding. Fabric edge nodes advertise their discovery capability for specific subnets or segments. The mapping system then determines when and where discovery occurs. Throttling controls repeated requests and limits probing for nonexistent destinations.

The design supports IPv4 and IPv6 subnet-based discovery, and it applies to single-site, multisite, and supported extranet scenarios. The mapping system, the fabric edge node, SISF, and the LISP control plane work together to improve endpoint reachability and visibility. This design preserves the scalable, on-demand behavior of the LISP architecture.

In enterprise and manufacturing networks that contain devices which communicate at intervals, silent host detection locates silent endpoints when a device requests them, and it probes only the ports that host the requested subnet.