Configure LISP Layer 2 Extension

You can deploy Cisco Catalyst 8000V instances on public, private, and hybrid clouds. When enterprises move to a hybrid cloud, they need to migrate the servers to the cloud without making any changes to the servers. Enterprises may want to use the same server IP address, subnet mask, default gateway configurations, and their own IP addressing scheme in the cloud, and not be limited by the addressing scheme of the cloud provider infrastructure.

To fulfill this requirement, you can use LISP, which is an architecture that allows you to separate the location (enterprise data center or public cloud) and the identity (server IP address) so that you can create new servers on the cloud with the same IP address. In the LISP architecture, the endpoint ID-to-router locator (EID-to-RLOC) mapping of the server is updated to reflect the new location that is moved to the cloud. Further, no changes are required to the end systems, users, or servers because LISP handles the mapping between the identity and the location.

LISP operates as an overlay, encapsulating the original packet from the server into a User Datagram Protocol (UDP) packet along with an additional outer IPv4 or IPv6 header. This encapsulation holds the source and destination router locators and allows the server administrators to address the server in the cloud according to their own IP addressing scheme, independent of the cloud provider's addressing structure.

You can configure Layer 2 Extension on Cisco Catalyst 8000V instances running on Microsoft Azure, where the instance acts as the bridge between the enterprise data center and the public cloud. By configuring the Layer 2 Extension, you can extend your Layer 2 networks in the private data center to a public cloud to achieve host reachability between your site and the public cloud. You can also enable the migration of your application workload between the data center and the public cloud.

Benefits

- Move the Public IP addresses between different geographic locations or split them between different public clouds. In either case, the LISP IP-Mobility solution provides optimal routing between clients on the Internet and the public IP address that has moved, regardless of the location. To know more about achieving IP mobility for the Azure cloud, see Achieving IP Mobility.
- Carry out data migration with ease and optimize the workload IP address in your network. Usually, IP address changes cause complexity and additional delays in a solution. By using L2 extension for cloud, you can migrate workloads while retaining the original IP address without any network constraints. To learn more about this use case, see Data Migration Use Case.
- Virtually add a VM that is on the provider site to facilitate cloud bursting to virtually insert a VM in the Enterprise server while the VM runs on the provider site.
- Provide backup services for partial disaster recovery and disaster avoidance.

Prerequisites for configuring LISP Layer 2 Extension

- Ensure that the underlay for your solution is ready before you configure the L2 Extension.
- Since clouds do not support Address Resolution Protocol (ARP), and the cloud infrastructure is not aware of the hosts in the remote site, you must add a virtual IP to help the cloud route the packets appropriately to the edge router. To add a virtual or alias IP, see Add an IP address for an Azure interface.
- Each Cisco Catalyst 8000V instance must be configured with one external IP address. In this case, an IPsec tunnel is built either between the IP addresses of the two Cisco Catalyst 8000V instances, or between the Cisco Catalyst 8000V instance and the ASR1000 device. Ensure that the IPsec tunnel has a private address.
- Ensure that the IPsec tunnel is working between the IP address of the two Cisco Catalyst 8000V instances or between the Cisco Catalyst 8000V instance and the ASR1000 device.
- Depending on your solution, ensure that a ping is successful between: the two Cisco Catalyst 8000V instances, between a Cisco Catalyst 8000V and an ASR1000 device, and between the VMs and the hosts.

Restrictions for configuring LISP Layer 2 Extension

- If you move a host from the data center to the cloud or vice-versa, you must first add or remove the secondary address from the virtual IP table in the cloud.
- If you move a VM to the cloud, you must initiate packets to the Cisco Catalyst 8000V instance so that the Cisco Catalyst 8000V device realizes that the VM is now added from the data center to the cloud.
- High Availability does not work with the L2 Extension functionality.
- Azure supports a maximum of 256 IPs. The maximum number of hosts on the remote site or the data center is thus 256.

How to configure LISP Layer 2 Extension

To configure the L2 extension functionality, you must first deploy the Cisco Catalyst 8000V instance on Microsoft Azure and configure the instance as an xTR. You must then configure the mapping system to complete the deployment.

The LISP site uses the Cisco Catalyst 8000V instance configured as both an ITR and an ETR (also known as an xTR) with two connections to upstream providers. The LISP site then registers to the standalone device that you have configured as the map resolver/map server (MR/MS) in the network core. The mapping system performs LISP encapsulation and de-encapsulation of the packets that are going to the migrated public IPs within Azure. Optionally, for traffic that is leaving Azure, whenever a route to the destination is not found

on the C8000V routing table, the Cisco Catalyst 8000V instance routes that traffic through the PxTR at the enterprise data center.

Perform the following steps to enable and configure the LISP xTR functionality when using a LISP map server and map resolver for mapping services:

Deploy Cisco Catalyst 8000V with Multiple Interfaces

Perform the following steps to deploy Cisco Catalyst 8000V with multiple interfaces.

Procedure

Step 1 Select **Virtual machines** in the left hand side panel.

Step 2 Click **Add**.

Step 3 Enter "C8000V".

Finds the Cisco Catalyst 8000V VM deployments in the Azure Marketplace.

Step 4 Choose the deployment of your choice, with 2,4, or 8 NICs.

Step 5 Click **Create**.

Step 6 **Virtual Machine name** - Select the **Basics** sub-menu and enter a name for the virtual machine.

Name of the cloud-based network used by Microsoft Azure to represent a private network.

Step 7 **Username** - Select a user name.

The Username for the Cisco Catalyst 8000V virtual machine which you can use to log into the Cisco Catalyst 8000V instance.

Step 8 **Authentication type** - Enter a Password (default) or SSH public key.

Step 9 **Cisco IOS XE Image Version** - Select the Cisco IOS XE version.

Step 10 **Subscription** - (Optional) Change the subscription name.

A default subscription name is provided, based on the name of the virtual machine. You can change this default subscription name.

Step 11 **Resource Group** - Select either **Create new** or **Use existing**.

You can only create a Cisco Catalyst 8000V in a new Resource Group (or in a completely empty existing resource group). To remove a Resource Group, first delete the Cisco Catalyst 8000V VM and then delete the Resource Group.

Step 12 Click **OK**.

Step 13 Select the **Cisco C8000V Settings** sub-menu and then select **Number of Network Interfaces in C8000V**.

Step 14 Select the number of interfaces: 2, 4, or 8.

Step 15 **License Type** - Select either **BYOL** or **PAYG** as the license type.

Note
PAYG licensing type is not supported in SD Routing devices.

Step 16 **Managed Disk** - Select **Enabled**.

Step 17 **Storage Account** - Enter a name for the storage account.

For more information on storage accounts, see the Microsoft Azure Resources section in this guide.

Step 18 **Virtual machine size** - Select the appropriate virtual machine size.

Based on the number of interfaces that you are using, select the appropriate virtual machine size. Microsoft Azure supports different image types with different performance expectations. To view the supported instance types and the virtual machine sizes, see the following links:

- Dv2 and DSv2 series
- Fsv2 series

Step 19 **Custom Data** - Select **Yes** if you want to provide a bootstrap configuration file.

For further information about providing a bootstrap configuration file for the Cisco Catalyst 8000V instance, see *Deploying a Cisco Catalyst 8000V VM Using a Day 0 Bootstrap File* section and the *Customdata-examples* section.

Step 20 **Availability Set** - Select **Yes**.

Step 21 **Availability Set name** - Enter a name for the availability set.

Step 22 **Availability Set fault domain count** - Enter the availability set fault domain count.

Fault domains define the group of VMs that share a common power source and network switch. Availability sets arrange virtual machines across fault domains.

Step 23 **Availability Set update domain count** - Enter the availability set update domain count.

An update domain is a group of VMs and underlying physical hardware that can be rebooted at the same time.

Step 24 **Boot diagnostics** - Enter the boot diagnostics.

For more information on boot diagnostics, see the *Information About Deploying Cisco Catalyst 8000V in Microsoft Azure* section.

Step 25 **Diagnostics Storage account** - Enter the storage account name.

Step 26 **Public IP Address** - Enter the public IP address name.

For more information on the public IP address, see the *Microsoft Azure Resources* section.

Step 27 **DNS label** - (Optional) Change the name of the DNS label.

The DNS label is the name of the public IP address to be assigned to the Cisco Catalyst 8000V. A default value for the DNS label is shown in the text box, which is the VM name followed by "`-dns`".

Step 28 **Virtual network** - Choose one of the following: **Create New** or **Use existing**.

For a new virtual network, enter the name and the IP address.

Step 29 Click **Subnets** - Enter the subnet names and the IP addresses.

Step 30 Check that all the Cisco Catalyst 8000V Settings are acceptable, and then click **OK**.

The **3 Summary** sub-menu is highlighted.

Step 31 Click **OK**.

The **4 Buy** sub-menu is highlighted.

Step 32 Click **Create**

The VM is created and the purchase is confirmed.

Step 33 Click **Virtual machines** on the left hand panel.

After a few minutes, the status of the recently created VM changes from Creating to Running. Make a note of the Public IP address name.

Configure a tunnel between Cisco Catalyst 8000V on Azure and Cisco Catalyst 8000V on the enterprise system

The communication between the Cisco Catalyst 8000V instance deployed within the enterprise data center and the Cisco Catalyst 8000V instance deployed within the public cloud is secured by an IP Security (IPsec) tunnel established between them. The LISP-encapsulated traffic is protected with the IPsec tunnel that provides data origin authentication, integrity protection, anti-reply protection, and confidentiality between the public cloud and the enterprise.

Procedure

Step 1 Configure a Cisco Catalyst 8000V instance on Microsoft Azure.

Run the **interface Loopback** command. Loopback is used as the LISP RLOC which identifies where the migrated customer IP space is located.

Run the **interface Tunnel** command to connect to the Cisco Catalyst 8000V instance on the cloud.

```
interface Loopback1
 ip address 33.33.33.33 255.255.255.255
!
interface Tunnel2
 ip address 30.0.0.2 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 173.39.145.79
 tunnel protection ipsec profile p2p_pf1
!
interface GigabitEthernet2
 ip address 10.10.10.140 255.255.255.0
 negotiation auto
 lisp mobility subnet1 nbr-proxy-reply requests 3
 no mop enabled
 no mop sysid
!
```

Step 2 Configure a second Cisco Catalyst 8000V instance on the enterprise site.

```
interface Loopback1
 ip address 11.11.11.11 255.255.255.255

interface Tunnel2
 ip address 30.0.0.1 255.255.255.0
 tunnel source GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel destination 52.14.116.161
 tunnel protection ipsec profile p2p_pf1
!
!
interface GigabitEthernet3
```

```
 ip address 10.10.10.2 255.255.255.0
 negotiation auto
 lisp mobility subnet1 nbr-proxy-reply requests 3
 no mop enabled
 no mop sysid
!
```

Configure LISP xTR on the Cisco Catalyst 8000V Instance Running on Azure

Procedure

To configure LISP xTR on the Cisco Catalyst 8000V instance running on the service provider, follow the configuration steps in the Configuring LISP (Location ID Separation Protocol) section.

The Cisco Catalyst 8000V instance on Azure uses the enterprise LISP router as the proxy ETR. Whenever the routing table points to the default route, it sends the traffic to the PETR.

Run the router **lisp command** to enable LISP. Execute the **itr map resolver** and the **itr map server** commands, to configure the Cisco Catalyst 8000V instance on the enterprise as the map server/map resolver.

Example:

```
router lisp
 locator-set azure
  33.33.33.33 priority 1 weight 100
  exit-locator-set
 !
 service ipv4
  itr map-resolver 11.11.11.11
  itr
  etr map-server 11.11.11.11 key cisco
  etr
  use-petr 11.11.11.11
  exit-service-ipv4
 !
 instance-id 0
  dynamic-eid subnet1
   database-mapping 10.10.10.0/24 locator-set azure
   map-notify-group 239.0.0.1
   exit-dynamic-eid
  !
  service ipv4
   eid-table default
   exit-service-ipv4
  !
  exit-instance-id
 !
 exit-router-lisp
!
router ospf 11
 network 30.0.0.2 0.0.0.0 area 11
 network 33.33.33.33 0.0.0.0 area 11
!

router lisp
 locator-set dmz
  11.11.11.11 priority 1 weight 100
```

```
 exit-locator-set
!
service ipv4
 itr map-resolver 11.11.11.11
 etr map-server 11.11.11.11 key cisco
 etr
 proxy-etr
 proxy-itr 11.11.11.11
 map-server
 map-resolver
 exit-service-ipv4
!
instance-id 0
 dynamic-eid subnet1
  database-mapping 10.10.10.0/24 locator-set dmz
  map-notify-group 239.0.0.1
  exit-dynamic-eid
 !
 service ipv4
  eid-table default
  exit-service-ipv4
 !
 exit-instance-id
!
site DATA_CENTER
 authentication-key cisco
 eid-record 10.10.10.0/24 accept-more-specifics
 exit-site
!
exit-router-lisp
!
router ospf 11
 network 11.11.11.11 0.0.0.0 area 11
 network 30.0.0.1 0.0.0.0 area 11
!

!
!
```

Verify the LISP Layer 2 Traffic Between Cisco Catalyst 8000V on Azure and Cisco Catalyst 8000V on the Enterprise System

Procedure

Run the following show lisp commands to verify the LISP Layer 2 traffic:

Example:

```
Router#show ip lisp database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1
Entries total 2, no-route 0, inactive 0

10.0.1.1/32, dynamic-eid subnet1, inherited from default locator-set dc
  Locator  Pri/Wgt  Source     State
33.33.33.33    1/100  cfg-addr   site-self, reachable
```

```
10.0.1.20/32, dynamic-eid subnet1, inherited from default locator-set dc
  Locator  Pri/Wgt  Source     State
33.33.33.33    1/100  cfg-addr   site-self, reachable
Router-azure#show ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 4 entries

0.0.0.0/0, uptime: 00:09:49, expires: never, via static-send-map-request
  Negative cache entry, action: send-map-request
10.0.1.0/24, uptime: 00:09:49, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
10.0.1.4/30, uptime: 00:00:55, expires: 00:00:57, via map-reply, forward-native
  Encapsulating to proxy ETR
10.0.1.100/32, uptime: 00:01:34, expires: 23:58:26, via map-reply, complete
  Locator  Uptime    State      Pri/Wgt     Encap-IID
11.11.11.11  00:01:34  up           1/100       -
Router-azure#show lisp dynamic-eid detail
% Command accepted but obsolete, unreleased or unsupported; see documentation.

LISP Dynamic EID Information for VRF "default"

Dynamic-EID name: subnet1
  Database-mapping EID-prefix: 10.0.1.0/24, locator-set dc
  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: 239.0.0.1
  Number of roaming dynamic-EIDs discovered: 2
  Last dynamic-EID discovered: 10.0.1.20, 00:01:37 ago
    10.0.1.1, GigabitEthernet2, uptime: 00:09:23
      last activity: 00:00:42, discovered by: Packet Reception
    10.0.1.20, GigabitEthernet2, uptime: 00:01:37
      last activity: 00:00:40, discovered by: Packet Reception

Router-DC#show ip lisp
Router-DC#show ip lisp data
Router-DC#show ip lisp database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1
Entries total 1, no-route 0, inactive 0

10.0.1.100/32, dynamic-eid subnet1, inherited from default locator-set dc
  Locator  Pri/Wgt  Source     State
11.11.11.11    1/100  cfg-addr   site-self, reachable
Router-DC#show ip lisp
Router-DC#show ip lisp map
Router-DC#show ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 2 entries

10.0.1.0/24, uptime: 1d08h, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
10.0.1.20/32, uptime: 00:00:35, expires: 23:59:24, via map-reply, complete
  Locator  Uptime    State      Pri/Wgt     Encap-IID
33.33.33.33  00:00:35  up           1/100

Router-DC#show lisp dynamic-eid detail
% Command accepted but obsolete, unreleased or unsupported; see documentation.

LISP Dynamic EID Information for VRF "default"

Dynamic-EID name: subnet1
  Database-mapping EID-prefix: 10.0.1.0/24, locator-set dc
  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: 239.0.0.1
  Number of roaming dynamic-EIDs discovered: 1
  Last dynamic-EID discovered: 10.0.1.100, 1d08h ago
    10.0.1.100, GigabitEthernet2, uptime: 1d08h
```

```
      last activity: 00:00:47, discovered by: Packet Reception

Router-DC#show lisp site
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           ID
dc             never     no     --                            10.0.1.0/24
               00:08:41  yes#   33.33.33.33                   10.0.1.1/32
               00:01:00  yes#   33.33.33.33                   10.0.1.20/32
               1d08h     yes#   11.11.11.11                   10.0.1.100/32
Router-DC#show ip cef 10.0.1.20
10.0.1.20/32
  nexthop 33.33.33.33 LISP0
Router-DC#

Router#show lisp instance-id 0 ipv4 database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1
Entries total 7, no-route 0, inactive 4

10.20.20.1/32, locator-set dc
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
10.230.1.5/32, dynamic-eid subnet1, inherited from default locator-set dc
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
10.230.1.6/32, Inactive, expires: 01:20:16
10.230.1.7/32, Inactive, expires: 01:20:16
10.230.1.8/32, dynamic-eid subnet1, inherited from default locator-set dc
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
10.230.1.31/32, Inactive, expires: 01:21:52
10.230.1.32/32, Inactive, expires: 01:20:16
Router-OnPrem#show lisp instance-id 0 ipv4 map
Router#show lisp instance-id 0 ipv4 map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 6 entries

10.20.0.0/16, uptime: 22:39:53, expires: never, via static-send-map-request
Negative cache entry, action: send-map-request
10.230.1.0/24, uptime: 22:39:53, expires: never, via dynamic-EID, send-map-request
Negative cache entry, action: send-map-request
10.230.1.6/32, uptime: 22:37:05, expires: never, via away, send-map-request
Negative cache entry, action: send-map-request
10.230.1.7/32, uptime: 22:37:05, expires: never, via away, send-map-request
Negative cache entry, action: send-map-request
10.230.1.31/32, uptime: 22:38:14, expires: 01:21:45, via map-reply, complete
Locator Uptime State Pri/Wgt Encap-IID
11.11.11.11 22:38:14 up 1/100 -
10.230.1.32/32, uptime: 22:37:05, expires: never, via away, send-map-request
Negative cache entry, action: send-map-request
```