Implementing NSH Based Service Chaining

Service functions provide a range of features such as security, WAN acceleration, and server load balancing.

End-to-end delivery of packets require many service functions including firewall, NATs, monitoring functions, and other network and application specific functions. These service functions are tightly coupled to the physical network topology. Service functions are not easily created, destroyed, or moved, even when virtualized.

A Network Service Header (NSH) is inserted onto encapsulated packets or frames to realize service function paths. NSH also provides a mechanism for metadata exchange along the instantiated service path. NSH is the Service Function Chaining (SFC) encapsulation required to support the SFC Architecture (defined in RFC7665).

NSH is designed to be easy to implement across a range of devices, both physical and virtual, including hardware platforms. See https://tools.ietf.org/html/draft-ietf-sfc-nsh-05 for more details.

Components of NSH Based Service Chaining

NSH defines a new service plane protocol specifically for the creation of dynamic service chains and is composed of the following elements:

- Service Function Path (SFP) identification
- Transport independent service function chain
- Per-packet network and service metadata or optional variable type-length-value (TLV) metadata

Service Classifier

A service classifier (SC) performs packet classification for incoming or outgoing flows and directs the matched traffic to service function paths. It may direct one or more flows to a particular service function (SF) path and may direct several such streams to different service function paths. Subsequent classification may occur on different SFs.

A classifier may be applied for incoming traffic. The classfifier action parameters include service path identifier and service function index. It may also include context metadata.

Service Function Forwarder

A Service Function Forwarder (SFF) performs the following tasks:

1. Remove the outer encapsulation and trigger a lookup based on service path index (SPI) and service index (SI) to identify the outgoing encapsulation.
2. Add new encapsulation and forward the packet to the Service Function (SF) or to the next SFF.
3. Support proxy function, that is without adding NSH in case the SF is non-NSH aware.

Service Function

Service Function (SF) is responsible for specific treatment of received packets.

Flow of Packets in NSH Based Service Chaining

The following is the flow of packets in NSH based service chaining:

1. Packet arrives from the source through an input interface. Service policy is applied. Packet is classified to find the service chain (SPI, SI).
2. SFF looks up the service chain for the next hop (SF or SFF).
3. SFF encapsulates the packet with NSH and forwards the frame to SF. If there are multiple SNs per SF, load balancing occurs.
4. SF de-encapsulates the frame and restores the packet. SF processes the packet, decrements the service index, encapsulates the packet, and returns the frame back to SFF.
5. Steps 2 to 4 are repeated for each service index in the service function chain. After the last service function has serviced the packet, SFF decapsulates the NSH header and forwards the packet normally.

NSH Format

An NSH is composed of a 4-byte Base Header, a 4-byte Service Path Header and Context Headers. The Base Header provides information about the service header and the payload protocol. The Service Path Header provides path identification and location within a service path. The Context Headers carry metadata (context data) along a service path.

See https://tools.ietf.org/html/draft-ietf-sfc-nsh-05 for more details.

Configuring NSH Based Service Chaining

The following components must be configured as part of this procedure in the configuration mode:

1. Service Function Path (SFP)
2. Service Function (SF) and Service Function Forwarder (SFF)
3. Policy for Service Function Classifier (SFC)

Configuring the SF Path

An index defines the sequence of the SF or SFF in the SF path. The highest index value indicates that SF/SFF are placed first in the service chain. The SF path can contain more than one SFF. One SF path can have different configurations on different nodes.

The SF indices must be contiguous. Non-contiguous indices are allowed, however they are incorrect. Incorrect configurtion will cause packets to be dropped by the platform. The SF index can have a value between 1 and 255 (8 bits).

The following is a configuration example of SF path:

```
router(config)#service-function-chaining

/* SF Path Index */
    path id 10

/* SF and SFF indices */
        40 sf SF-NAME
        39 sff SFF-NAME
        38 terminate default-action
```

Configuring the SF and SFF

SF or SFF can be defined with a name. SF or SFF can use up to one **locator** keyword to define reachability information. Reachability information includes transport type and other parameters as displayed in the following examples.

```
/* SF configuration */
router(config)#service-function-chaining
    sf SFNAME
        locator SFLOCID /* locator ID */
            transport vxlan-gpe
                source-address ipv4 192.0.2.11
                destination-address ipv4 192.0.2.12

                vni 4030

/* SFF configuration */
router(config)#service-function-chaining
    sff SFFNAME
        locator SFFLOCID /* locator ID */
            transport vxlan-gpe
                source-address ipv4 192.0.2.15
                destination-address ipv4 192.0.2.16

                vni 4035
```

Configuring the Metadata

A classifier may be applied for incoming traffic. The classfifier action parameters include service path identifier and service function index. It may also include context metadata.

The following is a configuration example of metadata disposition:

```
router(config)#service-function-chaining
    metadata-disposition d-mdata
    type 1 format dc-allocation
    match-entry dc-match
    tenant-id 100
    redirect ipv4 nexthop vrf default 100.20.10.2

service-function-chaining
```

```
    path 254
    15 terminate metadata-disposition d-mdata default-action redirect ipv4 nexthop vrf
default 192.10.1.2
```

Configuring a Policy for Service Function Classifier

For SFCs, Policy Based Routing (PBR) policy is used and the class maps are used as class templates. The SFC configuration is supported only in the ingress direction. A SF path can be associated with the class under the policy configuration. The service function path identifier must be configured prior to this association. The path identifier can have a value between 1 and 16777215 (24 bits).

Use the **service-function-path** *path-id* command to configure the SF path identifier. The following is an example to configure a PBR policy for GRE packets:

```
router#configure

/* Configuring a VRF: */
router(config)#vrf gre-vrf address-family ipv4 unicast
router(config-vrf-af)#exit
router(config-vrf)#exit

/* Associating an interface with VRF: */
router(config)#interface gigabitEthernet 0/2/0/1
router(config-if)#vrf gre-vrf
router(config-if)#exit
router(config)#interface gigabitEthernet 0/2/0/1
router(config-if)#ipv4 address 198.51.100.0/24
router(config-if)#exit

/* Creating an ACL: */
router(config)#ipv4 access-list gre-access-list
router(config-ipv4-acl)#1 permit gre host 192.0.2.1 host 192.168.18.1
router(config-ipv4-acl)#2 permit gre host 192.0.2.2 host 192.168.18.2
router(config-ipv4-acl)#3 permit gre host 192.0.2.3 host 192.168.18.3
router(config-ipv4-acl)#4 permit gre host 192.0.2.4 host 192.168.18.4
router(config-ipv4-acl)#commit
router(config-ipv4-acl)#exit

/* Configuring a class map with the ACL: */
router(config)#class-map type traffic match-any gre-class
router(config-cmap)#match access-group ipv4 gre-access-list
router(config-cmap)#end-class-map

/* Configuring metadata disposition: */
router(config)#service-function-chaining
router(config-service-function-chaining)#metadata-disposition d-mdata
router(config-service-function-chaining)#type 1 format dc-allocation
router(config-service-function-chaining)#match-entry dc-match
router(config-service-function-chaining)#tenant-id 100
router(config-service-function-chaining)#redirect ipv4 nexthop vrf default 192.168.10.2

router(config)#service-function-chaining
router(config-service-function-chaining)#path 254
router(config-service-function-chaining)#15 terminate metadata-disposition d-mdata
default-action redirect ipv4 nexthop vrf default 192.10.1.2

/* Configuring a PBR policy and SF path identifier: */
router(config)#policy-map type pbr gre-policy
router(config-pmap)#class type traffic gre-class
router(config-pmap-c)#service-function-path 10 index 40 metadata mname
router(config-pmap-c)#exit
router(config-pmap)#class type traffic class-default
router(config-pmap)#end-policy-map

/* Applying NSH policy per interface basis: */
router(config)#interface TenGigE 0/2/0/1
router(config)#service-policy type pbr input gre-policy

/* This command is supported with submode. */
router(config-vrf)#commit
router(config-vrf)#exit
```

Verifying NSH Based Service Chaining

Use the following commands to view and verify statistics for NSH based service function chaining:

- Service function forwarder statistics

  ```
  show service-function-chaining sff-local statistics [location <LOCATION-ID>]
  ```

- Service function path statistics

  ```
  show service-function-chaining path <PATH-ID> [si <index>] statistics [location
  <LOCATION-ID>]
  ```

- Service function locator statistics

  ```
  show service-function-chaining sf <NAME> statistics [location <LOCATION-ID>]
  ```

- Service function forwarder locator statistics

  ```
  show service-function-chaining sff <NAME> statistics [location <LOCATION-ID>]
  ```

Additional References

The following sections provide references related to HSRP

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Quality of Service Commands on Modular Quality of Service Command Reference for Cisco ASR 9000 Series Routers*
Class-based traffic shaping, traffic policing, low-latency queuing, and Modified Deficit Round Robin (MDRR)	*Configuring Modular Quality of Service Congestion Management on Modular QoS Configuration Guide for Cisco ASR 9000 Series Routers*
WRED, RED, and tail drop	*Configuring Modular QoS Congestion Avoidance on Modular QoS Configuration Guide for Cisco ASR 9000 Series Routers*
HSRP commands	*HSRP Commands on IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*

Related Topic	Document Title
master command reference	*Cisco ASR 9000 Series Aggregation Services Router Commands Master List*
getting started material	*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*
Information about user groups and task IDs	*Configuring AAA Services on System Security Configuration Guide for Cisco ASR 9000 Series Routers*

Standards and RFCs

Standard/RFC	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support