Configuring ITD

This chapter describes how to configure the Intelligent Traffic Director (ITD) on the Cisco NX-OS device.

About ITD

Intelligent Traffic Director (ITD) is an intelligent, hardware-based, multi-terabit solution that allows you to build a scalable architecture for Layer 3 and Layer 4 traffic distribution, load balancing, and redirection.

Benefits of ITD:

- Multi-terabit solution at line rate
- Transparency to end device and stateless protocol benefits
- Reduced complexities and architecture scaling for alternative features like Web Cache Communication Protocol (WCCP) and policy-based routing
- Simplified provisioning and ease of deployment
- Legacy service appliances can co-exist with new ones
- Removes the requirement for an expensive external load balancer
- No certification, integration, or qualification needed between the devices and the Cisco NX-OS switch
- Order of magnitude OPEX savings : reduction in configuration, and ease of deployment
- CAPEX savings : No service module or external L3/L4 load-balancer needed. Every Nexus port can be used as load-balancer

ITD features:

- Hardware based multi-terabit/s L3/L4 load-balancing at wire-speed
- Zero latency load-balancing
- Redirect line-rate traffic to any devices, for example web cache engines, Web Accelerator Engines (WAE), video-caches, etc
- Capability to create clusters of devices, for example, Firewalls, Intrusion Prevention System (IPS), or Web Application Firewall (WAF), Hadoop cluster
- IP-stickiness

- Hardware based multi-terabit/s L3/L4 load-balancing at wire-speed
- Zero latency load-balancing
- Redirect line-rate traffic to any devices, for example web cache engines, Web Accelerator Engines (WAE), video-caches, etc
- Capability to create clusters of devices, for example, Firewalls, Intrusion Prevention System (IPS), or Web Application Firewall (WAF), Hadoop cluster
- IP-stickiness

- Resilient (like resilient ECMP), Consistent hash
- Virtual IP based L4 load-balancing
- Weighted load-balancing and Failaction are supported among nodes
- Load-balances to large number of devices/servers
- ACL along with redirection and load balancing simultaneously
- Bi-directional flow-coherency. Traffic from A–>B and B–>A goes to same node
- The servers/appliances don’t have to be directly connected to Nexus switch
- Monitoring the health of servers/appliances with IP SLA-based probes
- N + M redundancy (N number of nodes and M number of hot-standbys)
- Automatic failure handling of servers/appliances
- VRF support, vPC support
- Supports both IPv4 and IPv6 (all platforms do not support IPv6)
- The feature does not add any load to the supervisor CPU
- Handles unlimited number of flows
- Nondisruptive node addition or deletion
- Simultaneous redirection and load balancing
- Rate sharing across multiple ITD services in the same switch

Use case examples:

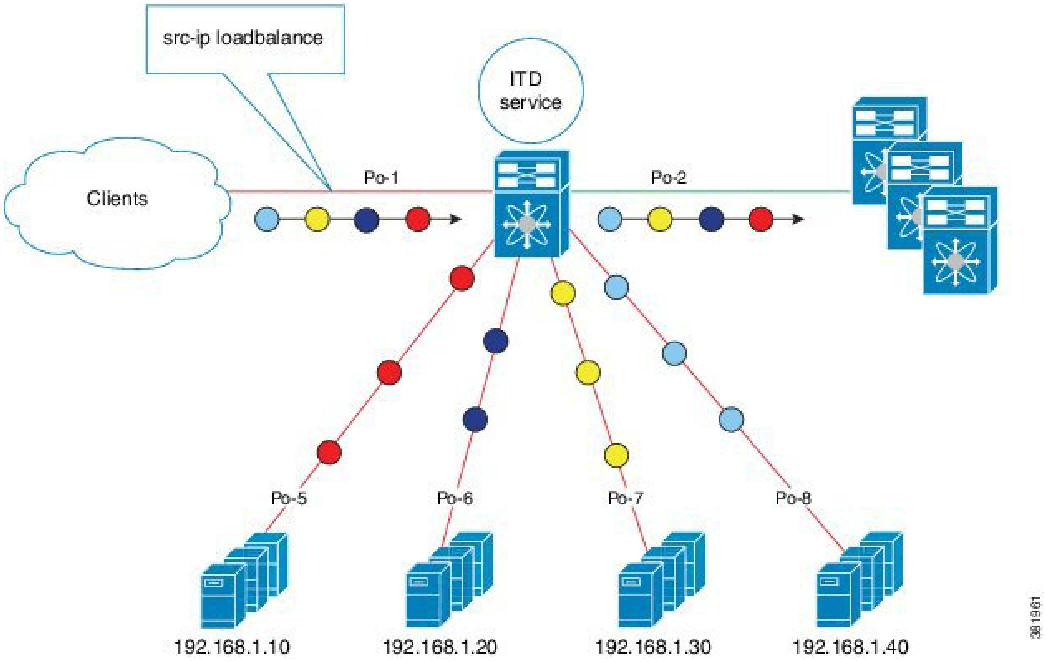
- Load-balance to cluster of Firewalls.
- Scale IPS, IDS and WAF by load-balancing to standalone devices
- Scale the NFV solution by load-balancing to low cost VM/container based NFV
- Scale the WAAS / WAE solution. Traffic redirection mechanism for the Wide Area Application Services (WAAS) or Web Accelerator Engine (WAE) solution
- Scale the VDS-TC (video-caching) solution
- Scale Layer-7 load-balancers, by distributing traffic to L7 LBs
- Replaces ECMP or the port channel to avoid rehashing . ITD is resilient, and doesn’t cause re-hashing on node add/delete/failure
- Server load balancing in DSR (Direct Server Return) mode
- Scales up NG intrusion prevention systems (IPSs) and web application firewalls (WAFs) by load balancing to standalone devices
- Load balances to Layer 5 through Layer 7 load balancers

Deployment Modes

One-Arm Deployment Mode

You can connect servers to the switch in one-arm deployment mode. In this topology, the server is not in the direct path of client or server traffic, which enables you to plug a server into the network with no changes to the existing topology or network.

Figure 1: One-Arm Deployment Mode

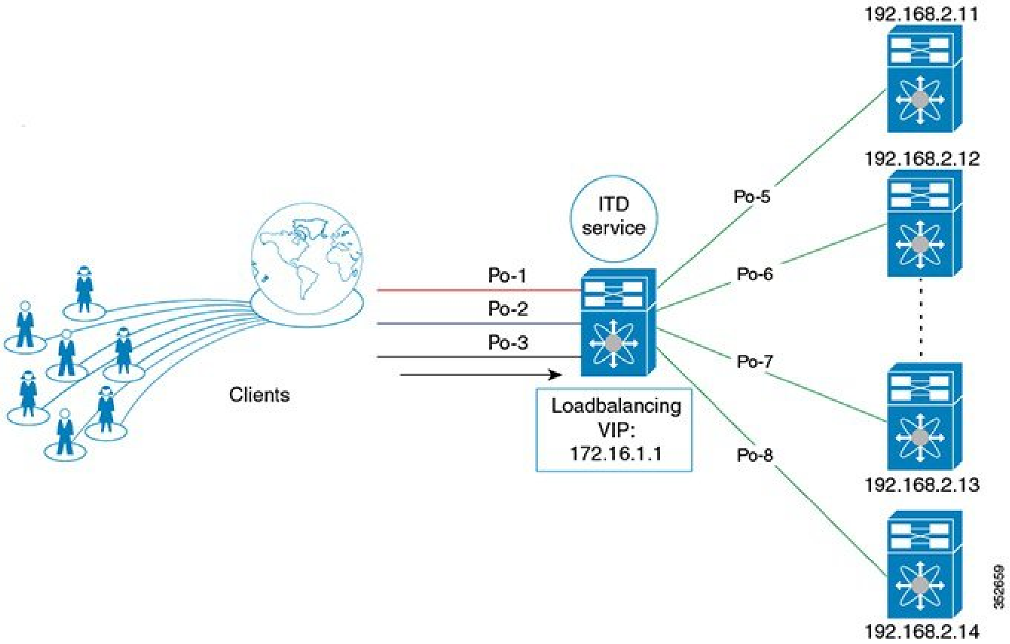


Server Load-Balancing Deployment Mode

The ITD service can be configured to host a virtual IP (VIP) on the switch. Internet traffic destined for the VIP will be load balanced to the active nodes. The ITD service is not a stateful load balancer.

Note You need to configure the ITD service manually and in a similar manner on each switch.

Figure 2: ITD Load Distribution with VIP



Device Groups

Nodes can be a physical server, virtual server, or a service appliance where traffic can be load balanced. These nodes are grouped together under a device group, and this device group can be mapped to a service.

ITD supports device groups. When you configure a device group, you can specify the following:

- The device group's nodes
- The device group's probe

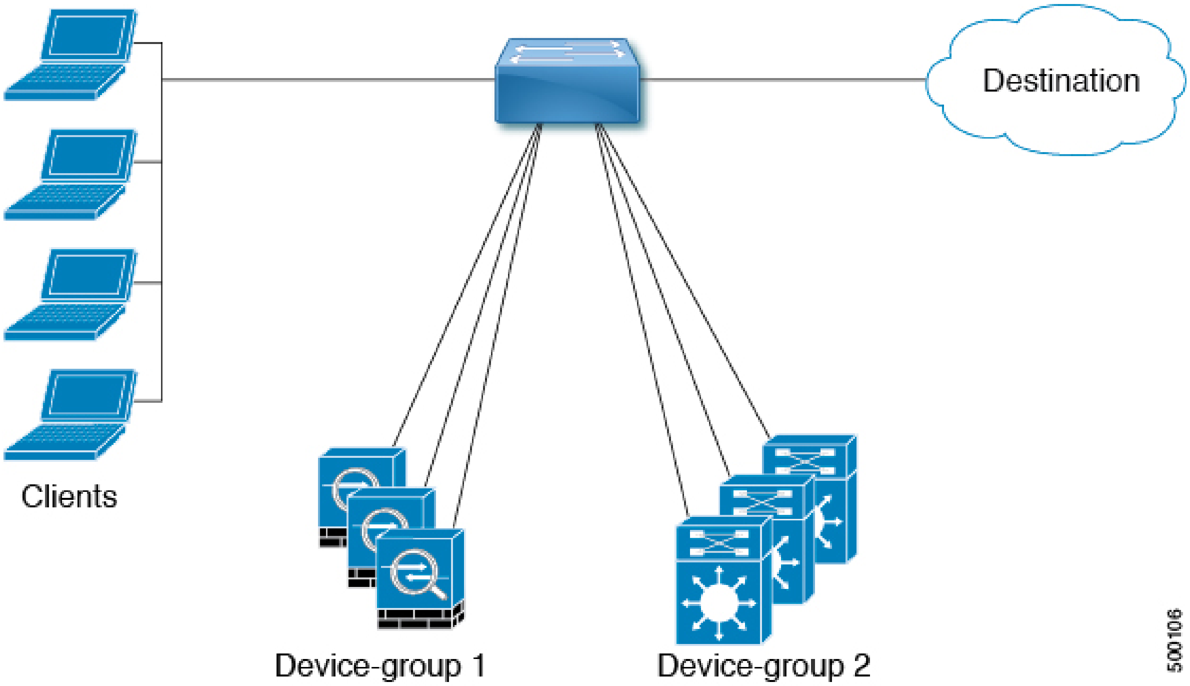
You can configure probes at the device-group level or at the node level. With node-level probing, each node can be configured with its own probe, allowing for further customization per node. Node-level probes are useful in scenarios where each node needs to be monitored differently for failure conditions.

Multiple Device Groups in an ITD Service

device groups are supported in an ITD service (as shown in the figure below). An ITD service generates a single route map with different sequences that point to different device groups.

Each device group represents different types of traffic requiring different services but arriving on the same ingress interface. Traffic on the interface is redirected to the appropriate device group based on the virtual IP address. Supporting multiple device groups per ITD service on the same interface allows ITD to scale.

Figure 3: Multiple Device Groups in an ITD Service



For a configuration example showing how to configure multiple device groups in an ITD service, see .

VRF Support

The ITD service can be configured in the default VRF as well as in non-default VRFs.

Ingress interfaces and device-group nodes must all belong to the same VRF for the ITD service to redirect traffic. You must ensure that all ingress interfaces and node members of the associated device group are reachable in the configured VRF.

Include and Exclude ACLs

Include ACL

The include ACL feature allows you to assign an access control list (ACL) to an ITD service. Only traffic matching the ACE is load-balanced toward the nodes and other traffic follows default routing rules.

You can configure up to 8 access-lists under one ITD service. You can associate each access list with its own device-group (Multi-ACL). When specific device-group is associated with one user ACL, that device-group takes priority and overwrites the default device-group. With this feature, ITD can load-balance traffic matching different ACLs to different device-groups.

Exclude ACL

You can configure an exclude ACL to specify the traffic that you want ITD to exclude from the ITD load balancer. The traffic, which the exclude ACL selects, is RIB-routed and bypasses ITD. An exclude ACL can filter based on both source and destination fields. The exclude ACL precedes the virtual IP address.

Virtual IP Address Filtering

A virtual IP address can be used to filter traffic for ITD. A virtual IP address and subnet mask combination for traffic filtering is supported for the destination field only.

Port Number-Based Filtering

Port numbering can be used to filter traffic for ITD. The following methods are supported to filter traffic based on Layer 4 ports (for example, port 80):

- Matching destination ports

  Any source or destination IP address with destination port 80 is matched. (For example: The virtual IP address is configured as **0.0.0.0 0.0.0.0 tcp 80**.)

- Matching source ports

  Any port other than 80 bypasses ITD, and port 80 is redirected. (For example: The exclude ACL is configured as **permit tcp any neq 80 any**.)

- Matching multiple port numbers

  Multiple virtual IP address lines in ITD can be configured, one for each port.

Hot-Standby

The hot-standby feature reconfigures the switch to look for an operational hot-standby node and select the first available hot-standby node to replace the failed node. ITD reconfigures the switch to redirect the traffic segment that was originally headed toward the failed node to the hot-standby node. The service does not impose any fixed mapping of hot-standby nodes to active nodes.

When the failed node becomes operational again, it is reinstated as an active node. The traffic from the acting hot-standby node is redirected back to the original node, and the hot-standby node reverts to the pool of standby nodes.

When multiple nodes fail, traffic destined to all failed nodes gets redirected to the first available hot-standby node.

The hot-standby node can be configured only at the node level . At the node level, the hot-standby node receives traffic only if its associated active node fails.

ITD supports N + M redundancy where M nodes can act as hot-standby nodes for N active nodes.

Multiple Ingress Interfaces

You can configure the ITD service to apply traffic redirection policies on multiple ingress interfaces. This feature allows you to use a single ITD service to redirect traffic arriving on different interfaces to a group of nodes.

System Health Monitoring

ITD monitors health of the nodes and applications running on those nodes periodically to detect any failures and to handle the failure scenarios.

ICMP, TCP, UDP probes are supported.

Health of an Interface Connected to a Node

leverages the IP service level agreement (IP SLA) feature to periodically probe each node. ITD uses the Internet Control Message Protocol (ICMP) to periodically probe each node. The probes are sent at a 10-second frequency by default and can be configured down to 1 second. They are sent simultaneously to all nodes. You can configure the probe as part of the pool group configuration.

A probe is declared to have failed after retrying three times by default. At this point, the node state becomes "Failed," and its status becomes "PROBE_FAILED."

Node Failure Handling

Upon marking a node as down, the ITD performs the following tasks automatically to minimize traffic disruption and to redistribute the traffic to remaining operational nodes:

- Determines if a standby node is configured to take over from the failed node.
- If the standby node is operational, it is identified the node as a candidate node for traffic handling.
- Redefines the standby node as active for traffic handling, if an operational standby node is available
- Programs automatically to reassign traffic from the failed node to the newly active standby node.

Failaction Reassignment

Failaction for ITD enables traffic to the failed nodes to be reassigned to one or more active nodes. When the failed node becomes active again, it resumes serving connections. If all the nodes are down, the packets are routed automatically. All Failaction mechanisms are supported for both IPv4 and IPv6 services.

Note You must configure a probe under an ITD device group before enabling the failaction feature.

Failaction Node Reassign

When a node goes down, the traffic buckets associated with the node are reassigned to the first active node found in the configured set of nodes. If the newly reassigned node also fails, traffic is reassigned to the next available active node.

Failaction Node Least-Bucket

When a node goes down, the traffic buckets associated with the node are reassigned to an active node that is currently receiving traffic from the least number of traffic buckets. For each subsequent node failure, the active node with least traffic buckets is recomputed and all the buckets directed to a failed node are redirected to this node, thereby allowing the re-assigned buckets to be distributed over multiple active nodes.

Failaction Bucket Distribute

When the service is enabled, ITD uses an internal algorithm to preselect varied sequences of primary nodes as alternate backup paths for with different priorities for each primary node. When a node goes down, the traffic to the node will be re-directed to the first active backup node with the highest priority, and so on, for subsequent failures, thereby minimizing the convergence delays.

the primary nodes of a device-group or up to 32 primary nodes of a device-group (whichever is lesser) shall be preselected with different priorities for each node.

Note This algorithm is intended for relatively even traffic distribution but doesn't guarantee even distribution with node failures.

Failaction Node-Per-Bucket

When a particular node fails, the node with least number of buckets are identified and the buckets are distributed across the other active nodes, starting from the node with least buckets.

ITD repeatedly identifies the least buckets node currently and assign one bucket to the node until all buckets are reassigned. Hence all buckets are distributed evenly among all remaining active nodes.

Note identifies the nodes to fail-over, based on the weights of the nodes. If a node doesn't have a weight configured a default weight of 1 is used.

No Failaction Reassignment

When failaction node reassignment is not configured, there are two possible scenarios:

No Failaction Reassignment with a Probe Configured

The ITD probe can detect the node failure or the lack of service reachability. If the node fails, the traffic is routed and does not get reassigned, as failaction is not configured. Once the node recovers, the recovered node starts to handle the traffic.

No Failaction Reassignment without a Probe Configured

Without a probe configuration, ITD cannot detect the node failure. When the node is down, ITD does not reassign or redirect the traffic to an active node.

Licensing Requirements

For a complete explanation of Cisco NX-OS licensing recommendations and how to obtain and apply licenses, see the *Cisco NX-OS Licensing Guide*.

Supported Platforms

Starting with Cisco NX-OS release 7.0(3)I7(1), use the Nexus Switch Platform Support Matrix to know from which Cisco NX-OS releases various Cisco Nexus 9000 and 3000 switches support a selected feature.

Guidelines and Limitations for ITD

ITD has the following configuration guidelines and limitations:

ITD Support Summary

See the following table for a list of the ITD support levels.

Table 1: ITD support levels

Feature	ITDv4	ITDv6	Comments
Device group level	• TCP • ICMP • UDP	• TCP • ICMPv3	Introduced in Cisco NX-OS Release 10.1(1)
Per Node-Probe Level	Yes	Yes	Introduced in Cisco NX-OS Release 10.1(1)
Hot-Standby	Yes	Yes	Introduced in Cisco NX-OS Release 10.1(1)
Weight	Yes	Yes	Introduced in Cisco NX-OS Release 10.1(1)
Non-Disruptive Operation			
ACL Refresh	Yes	Yes	Introduced in Cisco NX-OS Release 10.1(1)
Primary Nodes	Yes	Yes	Introduced in Cisco NX-OS Release 10.1(1)
Hot Standby Nodes	No	No	Introduced in Cisco NX-OS Release 10.1(1)
Service-Level			
Include ACL	Yes	Yes	Introduced in Cisco NX-OS Release 10.1(1)

Feature	ITDv4	ITDv6	Comments
Failaction methods	- **reassign** - **least-bucket** - **node-per-bucket** - **bucket distribute**	- **reassign** - **least-bucket** - **node-per-bucket** - **bucket distribute**	Introduced in Cisco NX-OS Release 10.1(1)
Exclude-ACL	Yes	Yes	Introduced in Cisco NX-OS Release 10.1(1) The deny ACEs are not supported.
Supported Platforms	Cisco Nexus C36180YC-R and C3636C-R switches	Cisco Nexus C36180YC-R and C3636C-R switches	Introduced in Cisco NX-OS Release 10.1(1)

Default Settings for ITD

This table lists the default settings for ITD parameters.

Table 2: Default ITD Parameters

Parameters	Default
Probe frequency	10 seconds
Probe retry down count	3
Probe retry up count	3
Probe timeout	5 seconds

Configuring ITD

Enabling ITD

Before you can access the ITD commands, you must enable the ITD feature.

Before you begin

Ensure that you have installed the Network Services license.

Ensure that policy-based routing (PBR) is enabled.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **feature itd**
3. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **feature itd** **Example:** `switch(config)# feature itd`	Enables the ITD feature. By default, ITD is disabled.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring a Device Group

You can create an ITD device group and then specify the group's nodes and probe. can configure multiple device groups.

Before you begin

Ensure that the ITD feature is enabled.

that the following commands are configured: **feature sla sender** and **feature sla responder**.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **itd device-group** *name*
3. [**no**] **node {ip | ipv6} {***ipv4-address* | *ipv6-address***}**
4. [**no**] **weight** *weight*
5. [**no**] **mode hot-standby**
6. **exit**
7. Repeat Steps 3 through 5 for each node.
8. [**no**] **probe** {**icmp** | **http** | **tcp port** *port-number* | **udp port** *port-number* | **dns** [**frequency** *seconds*] [[**retry-down-count** | **retry-up-count**] *number*] [**timeout** *seconds*]
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **itd device-group** *name*
	Example:
	`switch(config)# itd device-group dg1`
	`switch(config-device-group)#`
		Creates an ITD device group and enters device group configuration mode. You can enter up to 32 alphanumeric characters.

Step 3	[**no**] **node {ip | ipv6} {***ipv4-address* | *ipv6-address***}**
	Example:
	`switch(config-device-group)# node ip 20.20.20.3`
	`switch(config-dg-node)#`
	Example:
	`switch(config-device-group)# node ipv6`
	`2001::198:1:1:11`
	`switch(config-dg-node)#`
		Specifies the nodes for ITD.

Step 4	[**no**] **weight** *weight* **Example:** `switch(config-dg-node)# weight 6`	Specifies the weight of the node for ITD. The range is from 1 to 256.

Step 5	[**no**] **mode hot-standby**
	Example:
	`switch (config-device-group)# node ipv6 50::1`
	`switch(config-device-group-node)# mode hot-standby`
		Configures the node as a hot-standby node for the device group.

Step 6	**exit**
	Example:
	`switch(config-dg-node)# exit`
	`switch(config-device-group)#`
		Exits device group node configuration mode.

Step 7	Repeat Steps 3 through 5 for each node.	

Step 8	[**no**] **probe** {**icmp** | **http** | **tcp port** *port-number* | **udp port** *port-number* | **dns** [**frequency** *seconds*] [[**retry-down-count** | **retry-up-count**] *number*] [**timeout** *seconds*]
	Example:
	`switch(config-device-group)# probe icmp frequency`
	` 100`
		Configures the cluster group service probe.
		can specify the following protocols as the probe for the ITD service:
		• ICMP
		• TCP
		• UDP
		The options are as follows:

	Command or Action	Purpose
		• **frequency**—Specifies the frequency of the probe in seconds. The range is from 1 to 604800. • **retry-down-count**—Specifies the number of recounts undertaken by the probe when the node goes down. The range is from 1 to 5. • **retry-up-count**—Specifies the number of recounts undertaken by the probe when the node comes back up. The range is from 1 to 5. • **timeout**—Specifies the length of the timeout period in seconds. The range is from 1 to 604800.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config-device-group)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring an ITD Service

Before you begin

Ensure that the ITD feature is enabled.

Ensure that the device group to be added to the ITD service has been configured.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **itd** *service-name*
3. [**no**] **device-group** *device-group-name*
4. [**no**] **ingress interface** *interface*
5. [**no**] **load-balance** {**method** {**src** {**ip** | **ip-l4port** [**tcp** | **udp**] **range** *x y*} | **dst** {**ip** | **ip-l4port** [**tcp** | **udp**] **range** *x y*}} | **buckets** *bucket-number* | **mask-position** *mask-position* | }
6. **[no] virtual [ip | ipv6] {** *ipv4-address ipv4-network-mask* | *ipv6-address ipv6-network-mask* **}**[{ **proto** {*port_num* | *port_any*}}] [{**advertise**} {**enable** | **disable**}] [device-group *dgrp_name*]
7. Enter one of the following commands to determine how traffic is reassigned after a node failure:
    - [**no**] **failaction node reassign**
    - [**no**] **failaction node least-bucket**
    - [**no**] **failaction bucket distribute**
    - [**no**] **failaction node per-bucket**
8. [**no**] **vrf** *vrf-name*
9. [**no**] **exclude access-list** *acl-name*
10. **no shutdown**
11. (Optional) **show itd** [*itd-name*]

12. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **itd** *service-name*
	Example:
	`switch(config)# itd service1`
	`switch(config-itd)#`
		Configures an ITD service and enters ITD configuration mode. You can enter up to 32 alphanumeric characters.

Step 3	[**no**] **device-group** *device-group-name* **Example:** `switch(config-itd)# device-group dg1`	Adds an existing device group to the ITD service. The *device-group-name* specifies the name of the device group. You can enter up to 32 alphanumeric characters. **Note** You can add multiple device groups to the ITD service.
Step 4	[**no**] **ingress interface** *interface* **Example:** `switch(config-itd)# ingress interface ethernet 4/1-10`	Adds an ingress interface or multiple interfaces to an ITD service. Use a comma (",") to separate multiple interfaces. Use a hyphen ("-") to separate a range of interfaces. Configure the required VRF and interface modes prior to associating the interface to the service.

Step 5	[**no**] **load-balance** {**method** {**src** {**ip** | **ip-l4port** [**tcp** | **udp**] **range** *x y*} | **dst** {**ip** | **ip-l4port** [**tcp** | **udp**] **range** *x y*}} | **buckets** *bucket-number* | **mask-position** *mask-position* | }
	Example:
	`switch(config-itd)# load-balance method src ip buckets 16`
		Configures the load-balancing options for the ITD service.
		The options are as follows:
		• **method** —Specifies the source or destination IP-address-based load or traffic distribution.
		• **buckets** —Specifies the number of buckets to create. One or more buckets are mapped to a node. Buckets must be configured in powers of two. The range is from 2 to 256.
		Note If you configure more buckets than the number of nodes, the buckets are applied in a round-robin fashion across all the nodes.
		• **mask-position** —Specifies the load-balance mask position number.
		• For services with include-acl, use least-bit (with or without mask position) to distribute fewer consecutive IP hosts to the same bucket.

	Command or Action	Purpose

Step 6	**[no] virtual [ip | ipv6] {** *ipv4-address ipv4-network-mask* | *ipv6-address ipv6-network-mask* **}**[{ **proto** {*port_num* | *port_any*}}] [{**advertise**} {**enable** | **disable**}] [device-group *dgrp_name*]
	Example:
	`switch(config-itd)# virtual ip 100.100.100.100 255.255.255.255 udp 443 advertise enable active`
	Example:
	`switch(config-itd)# virtual ipv6 100::100 128 udp 443`
		Configures the virtual IPv4 or IPv6 address of the ITD service.
		The **proto** options (TCP or UDP) specify that the virtual IP address will accept flows from the specified protocol. The port range is from 0 to 65535.
		The [**advertise** {**enable** | **disable**}] option specifies whether the virtual IP route is advertised to neighboring devices. When the VIP advertise option is enabled, ITD will advertise the route to the Virtual IP address as long as one or more primary or hot-standby nodes are active in the device-group associated with the virtual IP or the default device-group under the service, as applicable. In order to enable the VIP advertise option, every primary and hot-standby node should be trackable via probes at the device-group or node level.
		Note The **advertise** {**enable** | **disable**} [**active**] option will issue a warning to use [**advertise** {**enable** | **disable**}] option.
		Note The **advertise enable** and the **advertise enable active** options are supported.
		Multiple instances of Virtual IP can be configured under a service with the same IP address , but different netmasks(or prefix length), protocols or ports. The user will need to ensure that the matches on the virtual IP, mask protocol and port are unique, so that traffic flows can load balance as intended.

Step 7	Enter one of the following commands to determine how traffic is reassigned after a node failure:
	• [**no**] **failaction node reassign**
	• [**no**] **failaction node least-bucket**
	• [**no**] **failaction bucket distribute**
	• [**no**] **failaction node per-bucket**
	Example:
	`switch(config-itd)# failaction node reassign`
	Example:
	`switch(config-itd)# failaction node least-bucket`
	Example:
	`switch(config-itd)# failaction bucket distribute`
	Example:
		Configures the fail-action mechanism to be used by the service.
		Note This algorithm is intended for relatively even traffic distribution but doesn't guarantee even distribution.

	Command or Action	Purpose
	`switch (config-itd)# failaction node per-bucket`	
Step 8	[**no**] **vrf** *vrf-name* **Example:** `switch(config-itd)# vrf RED`	Specifies the VRF for the ITD service.
Step 9	[**no**] **exclude access-list** *acl-name* **Example:** `switch(config-itd)# exclude access-list acl1`	Specifies the traffic that you want ITD to exclude from the ITD load balancer.
Step 10	**no shutdown** **Example:** `switch(config-itd)# no shutdown`	Enables the ITD service.
Step 11	(Optional) **show itd** [*itd-name*] **Example:** `switch(config-itd)# show itd`	Displays the status and configuration for specified ITD instances.
Step 12	(Optional) **copy running-config startup-config** **Example:** `switch(config-itd)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Assigning an ACL to an ITD Service

You can use the include access control list (ACL) feature to assign an ACL to an ITD service. For each access control entry (ACE) with the **permit** method in the ACL, this feature filters the unwanted traffic and generates IP access lists and a route map to load-balance the permitted traffic. Load balancing is supported using either the source or destination IP address.

Before you begin

Ensure that the ITD feature is enabled.

Ensure that the device group to be added to the ITD service has been configured.

Ensure that the ACL to be assigned to the ITD service has been configured.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **itd** *itd-name*
3. [**no**] **device-group** *device-group-name*
4. [**no**] **ingress interface** *interface*
5. [**no**] **load-balance** {**method** {**src** {**ip** | **ip-l4port** [**tcp** | **udp**] **range** *x y*} | **dst** {**ip** | **ip-l4port** [**tcp** | **udp**] **range** *x y*}} | **buckets** *bucket-number*}
6. [**no**] **failaction node-per-bucket**

7. **access-list** *acl-name*
8. [**no**] **shutdown**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **itd** *itd-name*
	Example:
	`switch(config)# itd service1`
	`switch(config-itd)#`
		Configures an ITD service and enters ITD configuration mode. You can enter up to 32 alphanumeric characters.

Step 3	[**no**] **device-group** *device-group-name* **Example:** `switch(config-itd)# device-group dg1`	Adds an existing device group to the ITD service. The *device-group-name* specifies the name of the device group. You can enter up to 32 alphanumeric characters.
Step 4	[**no**] **ingress interface** *interface* **Example:** `switch(config-itd)# ingress interface ethernet 4/1-10`	Adds an ingress interface or multiple interfaces to an ITD service. Use a comma (",") to separate multiple interfaces. Use a hyphen ("-") to separate a range of interfaces.

Step 5	[**no**] **load-balance** {**method** {**src** {**ip** | **ip-l4port** [**tcp** | **udp**] **range** *x y*} | **dst** {**ip** | **ip-l4port** [**tcp** | **udp**] **range** *x y*}} | **buckets** *bucket-number*}
	Example:
	`switch(config-itd)# load-balance method src ip buckets 16`
		Configures the load-balancing options for the ITD service.
		The options are as follows:
		• **method** —Specifies the source or destination IP-address-based load or traffic distribution.
		• **buckets** —Specifies the number of buckets to create. One or more buckets are mapped to a node. Buckets must be configured in powers of two. The range is from 2 to 256.
		Note If you configure more buckets than the number of nodes, the buckets are applied in a round-robin fashion across all the nodes.

Step 6	[**no**] **failaction node-per-bucket** **Example:** `switch(config-itd)# failaction node-per-bucket`	When a node failure happens the buckets assigned to this node will be distributed across the remaining active nodes. If weights are assigned to nodes, the distribution will be based on weights of the nodes.
Step 7	**access-list** *acl-name* **Example:**	Assigns an ACL to the ITD service.

	Command or Action	Purpose
	`switch(config-itd)# access-list itd_d`	
Step 8	[**no**] **shutdown** **Example:** `switch(config-itd)# no shutdown`	Enables the ITD service.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config-itd)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Nondisruptively Adding or Deleting Nodes

You can configure an ITD session that enables you to add or delete nodes in a device group without shutting down the ITD service. Doing so minimizes traffic disruption, which can occur when you shut down the ITD service.

Before you begin

Ensure that the ITD feature is enabled.

Ensure that the device group and the ITD service have been configured.

SUMMARY STEPS

1. **configure terminal**
2. **itd session device-group** *device-group-name*
3. [**no**] **node ip** {*ipv4-address* | *ipv6-address*}
4. {**commit** | **abort**}
5. (Optional) **show itd session device-group** [*name*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**itd session device-group** *device-group-name*
	Example:
	`switch(config)# itd session device-group dg1`
	`switch(config-session-device-group)#`
		Creates an ITD session for the specified device group.

	Command or Action	Purpose

Step 3	[**no**] **node ip** {*ipv4-address* | *ipv6-address*}
	Example:
	`switch(config-session-device-group)# node ip 2.2.2.1`
		Adds the specified node to the ITD device group. The **no** form of this command deletes the specified node from the ITD device group.
		Repeat this step for each node that you want to add or delete.

Step 4	{**commit** | **abort**}
	Example:
	`switch(config-session-device-group)# commit`
	`switch(config)#`
		The **commit** command updates the ITD device group with the new or modified set of nodes, reassigns buckets, and cleans up the ITD session configuration.
		The **abort** command ignores the ITD session configuration and does not update the ITD device group.

Step 5	(Optional) **show itd session device-group** [*name*] **Example:** `switch(config)# show itd session device-group dg1`	Displays all of the configured ITD sessions or the ITD session for the specified device group.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Nondisruptively Adding or Deleting ACEs in Include ACLs

You can add or delete the access control entries (ACEs) in the include ACL without shutting down the ITD service. Doing so minimizes traffic disruption, which can occur when you shut down the ITD service.

Before you begin

Ensure that the ITD feature is enabled.

Ensure that the device group and the ITD service have been configured.

Ensure that an ACL has been assigned to the ITD service.

SUMMARY STEPS

1. **configure terminal**
2. **itd session access-list** *acl-name* **refresh**
3. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
Step 2	**itd session access-list** *acl-name* **refresh** **Example:** `switch(config)# itd session access-list test1 refresh`	Internally reads the include ACL and programs the TCAM. ITD checks the old and new ACL ACEs and updates the ITD-generated ACLs. **Note** This command is required only for include ACLs.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying the ITD Layer-3 Configuration

To display the ITD layer-3 configuration, perform one of the following tasks:

Command	Purpose
show itd [*itd-name*] [**brief** | **vrf** [*vrf-name*]]	Displays the status and configuration for specified ITD instances. • Use the *itd-name* argument to display the status and configuration for a specific ITD instance. • Use the **brief** keyword to display summary status and configuration information. • Use the **vrf** keyword to display the VRFs for the specified ITD instance.
show itd session device-group [*name*]	Displays all of the configured ITD sessions or the ITD session for the specified device group.
show running-config services	Displays the configured ITD device group and services.

These examples show how to verify the ITD configuration:

```
switch# show itd

Name           Probe LB Scheme  Status   Buckets
-------------- ----- ---------- -------- -------
WEB            ICMP  src-ip     ACTIVE   2

Device Group                                         VRF-Name
-------------------------------------------------- -------------
WEB-SERVERS


Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
WEB_itd_pool                   Po-1         UP       -
```

```
Virtual IP     Netmask/Prefix            Protocol   Port
---------------------------------------- ---------- -----
10.10.10.100 / 255.255.255.255           IP           0

  Node  IP                  Config-State Weight Status     Track_id
  ------------------------- ------------ ------ ---------- ---------
  1     10.10.10.11         Active       1      OK           -

        Bucket List
        -----------------------------------------------------------------------
        WEB_itd_vip_1_bucket_1


  Node  IP                  Config-State Weight Status     Track_id
  ------------------------- ------------ ------ ---------- ---------
  2     10.10.10.12         Active       1      OK           -

        Bucket List
        -----------------------------------------------------------------------
        WEB_itd_vip_1_bucket_2
```

Configuration Examples for ITD

This example shows how to configure ITD and other pre-requisite features, and configure ITD device groups.

```
switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch-1(config)# feature itd
switch-1(config)# feature sla sender
switch-1(config)# feature pbr
switch-1(config)#
switch-1(config)#  itd device-group DG1
switch-1(config-device-group)#    probe icmp frequency 2 retry-down-count 2 retry-up-count
 1 timeout 1
switch-1(config-device-group)#    node ip 10.200.1.2
switch-1(config-dg-node)#   node ip 10.200.2.2
switch-1(config-dg-node)#
switch-1(config-dg-node)#
switch-1(config-dg-node)# itd device-group DG2
switch-1(config-device-group)#    probe icmp
switch-1(config-device-group)#    node ipv6 2007::2
switch-1(config-dg-node)#   node ipv6 2008::2
switch-1(config-dg-node)#
switch-1(config-dg-node)# end
switch-1#
```

This example shows how to create an ITD service with failaction as node per-bucket and the destination-based load balance method with static bucket count and associate the device groups to the service.

```
switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch-1(config)# itd SER1
switch-1(config-itd)#    device-group DG1
switch-1(config-itd)#    ingress interface Ethernet1/17
switch-1(config-itd)#    failaction node per-bucket
switch-1(config-itd)#    load-balance method dst ip buckets 4
switch-1(config-itd)# no sh
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.
```

```
switch-1(config-itd)#
switch-1(config-itd)# itd SER2
switch-1(config-itd)#    device-group DG2
switch-1(config-itd)#    ingress interface Ethernet1/18
switch-1(config-itd)#    failaction node per-bucket
switch-1(config-itd)#    load-balance method dst ip buckets 4
switch-1(config-itd)# no sh
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.

switch-1(config-itd)# end
switch-1#
switch-1# sh run services
!Command: show running-config services
!No configuration change since last restart
!Time: Tue Jan  5 21:05:40 2021

version 10.1(1) Bios:version 01.14
feature itd

itd device-group DG1
  probe icmp frequency 2 timeout 1 retry-down-count 2 retry-up-count 1
  node ip 10.200.1.2
  node ip 10.200.2.2


itd device-group DG2
  probe icmp
  node ipv6 2007::2
  node ipv6 2008::2

itd SER1
  device-group DG1
  ingress interface Eth1/17
  failaction node per-bucket
  load-balance method dst ip buckets 4
  no shut

itd SER2
  device-group DG2
  ingress interface Eth1/18
  failaction node per-bucket
  load-balance method dst ip buckets 4
  no shut
switch-1#
switch-1# show itd brief

Legend:
 C-S(Config-State): A-Active,S-Standby,F-Failed
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets    Interface
-------------- ---------- -------- ---------  --------------
SER1           dst-ip     ACTIVE   4          Eth1/17

Source Interface
----------------


Device Group                                       Probe  Port
-------------------------------------------------- ----- ------
DG1                                                 ICMP
```

```
Node  IP                  Cluster-id C-S WGT Probe Port     Probe-IP   STS
------------------------- ---------- -- --- ---- ----- --------------- --
1              10.200.1.2             A   1 ICMP                        OK
2              10.200.2.2             A   1 ICMP                        OK

Legend:
 C-S(Config-State): A-Active,S-Standby,F-Failed
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets    Interface
-------------- ---------- -------- ---------  ---------------
SER2           dst-ip     ACTIVE   4          Eth1/18

Source Interface
----------------


Device Group                                       Probe  Port
-------------------------------------------------- ----- ------
DG2                                                 ICMP


Node      IP                                Cluster-id C-S WGT Probe Port    Probe-IP
STS
------------------------------------------ ---------- --- --- ---- ----- ---------------
--
1                                   2007::2             A   1 ICMP
OK
2                                   2008::2             A   1 ICMP
OK


switch-1#
switch-1# sh itd

Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
SER1           dst-ip     ACTIVE   4

Source Interface
----------------


Device Group                                       Probe  Port
-------------------------------------------------- ----- ------
DG1                                                 ICMP

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
SER1_itd_pool                  Eth1/17      UP       1

  Node  IP                 Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id

  ------------------------ ---------- ------- --- ---- ----- --------------- -- --- -------

  1             10.200.1.2            Active   1 ICMP                      OK   2   10002


      Bucket List
      --------------------------------------------------------------------------
      SER1_itd_bucket_1, 3

  Node  IP                 Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id

  ------------------------ ---------- ------- --- ---- ----- --------------- -- --- -------

  2             10.200.2.2            Active   1 ICMP                      OK   3   10003


      Bucket List
      --------------------------------------------------------------------------
      SER1_itd_bucket_2, 4
Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
SER2           dst-ip     ACTIVE   4

Source Interface
----------------


Device Group                                       Probe  Port
-------------------------------------------------- ----- ------
DG2                                                 ICMP

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
SER2_itd_pool                  Eth1/18      UP       4


  Node  IP                                    Cluster-id Cfg-S  WGT
  ------------------------------------------- ---------- ------- ---
  1                                   2007::2            Active   1

      Probe Port    Probe-IP    STS Trk# Sla_id
      ---- ----- --------------- -- --- -------
      ICMP                       OK   5   10004

      Bucket List
      --------------------------------------------------------------------------
      SER2_itd_bucket_1, 3

  Node  IP                                    Cluster-id Cfg-S  WGT
  ------------------------------------------- ---------- ------- ---
  2                                   2008::2            Active   1

      Probe Port    Probe-IP    STS Trk# Sla_id
      ---- ----- --------------- -- --- -------
      ICMP                       OK   6   10005

      Bucket List
      --------------------------------------------------------------------------
      SER2_itd_bucket_2, 4

switch-1#

switch-1# sh run rpm

!Command: show running-config rpm
!No configuration change since last restart
!Time: Tue Jan  5 21:08:12 2021
```

```
version 10.1(1) Bios:version 01.14
feature pbr

route-map SER1_itd_pool permit 10
  match ip address SER1_itd_bucket_1
  set ip next-hop verify-availability 10.200.1.2 track 2 force-order
route-map SER1_itd_pool permit 11
  match ip address SER1_itd_bucket_2
  set ip next-hop verify-availability 10.200.2.2 track 3 force-order
route-map SER1_itd_pool permit 12
  match ip address SER1_itd_bucket_3
  set ip next-hop verify-availability 10.200.1.2 track 2 force-order
route-map SER1_itd_pool permit 13
  match ip address SER1_itd_bucket_4
  set ip next-hop verify-availability 10.200.2.2 track 3 force-order
route-map SER2_itd_pool permit 10
  match ipv6 address SER2_itd_bucket_1
  set ipv6 next-hop verify-availability 2007::2 track 5 force-order
route-map SER2_itd_pool permit 11
  match ipv6 address SER2_itd_bucket_2
  set ipv6 next-hop verify-availability 2008::2 track 6 force-order
route-map SER2_itd_pool permit 12
  match ipv6 address SER2_itd_bucket_3
  set ipv6 next-hop verify-availability 2007::2 track 5 force-order
route-map SER2_itd_pool permit 13
  match ipv6 address SER2_itd_bucket_4
  set ipv6 next-hop verify-availability 2008::2 track 6 force-order


interface Ethernet1/17
  ip policy route-map SER1_itd_pool

interface Ethernet1/18
  ipv6 policy route-map SER2_itd_pool

switch-1#
switch-1# show ip access-lists dynamic

IP access list SER1_itd_bucket_1
        10 permit ip any 1.1.1.0 255.255.255.63
IP access list SER1_itd_bucket_2
        10 permit ip any 1.1.1.64 255.255.255.63
IP access list SER1_itd_bucket_3
        10 permit ip any 1.1.1.128 255.255.255.63
IP access list SER1_itd_bucket_4
        10 permit ip any 1.1.1.192 255.255.255.63
switch-1#
switch-1# show run track

!Command: show running-config track
!No configuration change since last restart
!Time: Tue Jan  5 21:09:25 2021

version 10.1(1) Bios:version 01.14
track 1 interface Ethernet1/17 line-protocol
track 2 ip sla 10002 reachability
 delay up 2 down 4

track 3 ip sla 10003 reachability
 delay up 2 down 4

track 4 interface Ethernet1/18 line-protocol
track 5 ip sla 10004 reachability
```

```
 delay up 30 down 30

track 6 ip sla 10005 reachability
 delay up 30 down 30

switch-1#
switch-1# sh track
Track 1
  Interface Ethernet1/17 Line Protocol
  Line Protocol is UP
  1 changes, last change 00:05:54
  Tracked by:
    ISCM Configuration

Track 2
  IP SLA 10002 Reachability
  Reachability is UP
  2 changes, last change 00:05:50
  Latest operation return code: OK
  Latest RTT (millisecs): 1
  Tracked by:
    ISCM Configuration
    Route Map Configuration
  Delay up 2 secs, down 4 secs

Track 3
  IP SLA 10003 Reachability
  Reachability is UP
  2 changes, last change 00:05:50
  Latest operation return code: OK
  Latest RTT (millisecs): 1
  Tracked by:
    ISCM Configuration
    Route Map Configuration
  Delay up 2 secs, down 4 secs

Track 4
  Interface Ethernet1/18 Line Protocol
  Line Protocol is UP
  1 changes, last change 00:05:32
  Tracked by:
    ISCM Configuration

Track 5
  IP SLA 10004 Reachability
  Reachability is UP
  2 changes, last change 00:04:51
  Latest operation return code: OK
  Latest RTT (millisecs): 1
  Tracked by:
    ISCM Configuration
    Route Map Configuration
  Delay up 30 secs, down 30 secs
Track 6
  IP SLA 10005 Reachability
  Reachability is UP
  2 changes, last change 00:04:51
  Latest operation return code: OK
  Latest RTT (millisecs): 1
  Tracked by:
    ISCM Configuration
    Route Map Configuration
  Delay up 30 secs, down 30 secs
switch-1#
```

```
switch-1# show ip sla stat

IPSLAs Latest Operation Statistics

IPSLA operation id: 10002
        Latest RTT: 1 milliseconds
Latest operation start time: 21:11:12.861 UTC Tue Jan 05 2021
Latest operation return code: OK
Number of successes: 210
Number of failures: 1
Operation time to live: forever

IPSLA operation id: 10003
        Latest RTT: 1 milliseconds
Latest operation start time: 21:11:12.901 UTC Tue Jan 05 2021
Latest operation return code: OK
Number of successes: 210
Number of failures: 1
Operation time to live: forever

IPSLA operation id: 10004
        Latest RTT: 2 milliseconds
Latest operation start time: 21:11:04.995 UTC Tue Jan 05 2021
Latest operation return code: OK
Number of successes: 39
Number of failures: 1
Operation time to live: forever

IPSLA operation id: 10005
        Latest RTT: 1 milliseconds
Latest operation start time: 21:11:05.034 UTC Tue Jan 05 2021
Latest operation return code: OK
Number of successes: 39
Number of failures: 1
Operation time to live: forever
switch-1#
```

This example shows how to configure an ITD service with failaction as node reassign and fail action as node least-bucket with source-ip based load balance method.

```
switch-1(config)# feature itd
switch-1(config)#
switch-1(config)#
switch-1(config)# itd device-group DG1
switch-1(config-device-group)#   probe icmp frequency 2 timeout 1 retry-down-count 2
retry-up-count 1
switch-1(config-device-group)#   node ip 10.200.1.2
switch-1(config-dg-node)#   node ip 10.200.2.2
switch-1(config-dg-node)#
switch-1(config-dg-node)#
switch-1(config-dg-node)# itd device-group DG2
switch-1(config-device-group)#   probe icmp
switch-1(config-device-group)#   node ipv6 2007::2
switch-1(config-dg-node)#   node ipv6 2008::2
switch-1(config-dg-node)#
switch-1(config-dg-node)#
switch-1(config-dg-node)# itd SER1
switch-1(config-itd)#   device-group DG1
switch-1(config-itd)#   ingress interface Eth1/17
switch-1(config-itd)#   failaction node reassign
switch-1(config-itd)#   load-balance method src ip buckets 4
switch-1(config-itd)#   no shut
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.
```

```
switch-1(config-itd)#
switch-1(config-itd)# itd SER2
switch-1(config-itd)#   device-group DG2
switch-1(config-itd)#   ingress interface Eth1/18
switch-1(config-itd)#   failaction node least-bucket
switch-1(config-itd)#   load-balance method src ip
switch-1(config-itd)#   no shut
switch-1(config-itd)# end
switch-1#
switch-1# sh run services

!Command: show running-config services
!No configuration change since last restart
!Time: Tue Jan  5 21:21:41 2021

version 10.1(1) Bios:version 01.14
feature itd

itd device-group DG1
  probe icmp frequency 2 timeout 1 retry-down-count 2 retry-up-count 1
  node ip 10.200.1.2
  node ip 10.200.2.2

itd device-group DG2
  probe icmp
  node ipv6 2007::2
  node ipv6 2008::2

itd SER1
  device-group DG1
  ingress interface Eth1/17
  failaction node reassign
  load-balance method src ip buckets 4
  no shut

itd SER2
  device-group DG2
  ingress interface Eth1/18
  failaction node least-bucket
  load-balance method src ip
  no shut

switch-1#
```

This example shows how to add and delete ITD nodes using ITD sessions to be able to modify ITD configuration while the service is active.

```
switch-1(config)# itd session device-group DG1
switch-1(config-session-device-group)#                    no node ip 10.200.1.2
switch-1(config-session-device-group)#                    node ip 10.200.3.2
switch-1(config-session-dg-node)#                    node ip 10.200.4.2
switch-1(config-session-dg-node)#                    commit
switch-1(config)#                itd session device-group DG2
switch-1(config-session-device-group)#                    no node ipv6 2007::2
switch-1(config-session-device-group)#                    node ipv6 2009::2
switch-1(config-session-dg-node)#                    commit
switch-1(config)#  end
switch-1#
switch-1# sh run services

!Command: show running-config services
!No configuration change since last restart
!Time: Tue Jan  5 22:49:07 2021
```

```
version 10.1(1) Bios:version 01.14
feature itd

itd device-group DG1
  probe icmp frequency 2 timeout 1 retry-down-count 2 retry-up-count 1
  node ip 10.200.3.2
  node ip 10.200.2.2
  node ip 10.200.4.2

itd device-group DG2
  probe icmp
  node ipv6 2009::2
  node ipv6 2008::2

itd SER1
  device-group DG1
  ingress interface Eth1/17
  failaction node reassign
  load-balance method src ip buckets 4
  no shut

itd SER2
  device-group DG2
  ingress interface Eth1/18
  failaction node least-bucket
  load-balance method src ip
  no shut

switch-1#
switch-1# sh itd brief

Legend:
 C-S(Config-State): A-Active,S-Standby,F-Failed
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets    Interface
-------------- ---------- -------- ---------  --------------
SER1           src-ip     ACTIVE   4          Eth1/17

Source Interface
----------------


Device Group                                       Probe  Port
-------------------------------------------------- ----- ------
DG1                                                 ICMP


Node  IP                  Cluster-id C-S WGT Probe Port     Probe-IP   STS
------------------------- ---------- -- --- ---- ----- --------------- --
1              10.200.3.2             A   1 ICMP                       OK
2              10.200.2.2             A   1 ICMP                       OK
3              10.200.4.2             A   1 ICMP                       OK

Legend:
 C-S(Config-State): A-Active,S-Standby,F-Failed
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets    Interface
-------------- ---------- -------- ---------  --------------
SER2           src-ip     ACTIVE   2          Eth1/18

Source Interface
----------------
```

```
Device Group                                       Probe  Port
-------------------------------------------------- ----- ------
DG2                                                 ICMP


Node      IP                                Cluster-id C-S WGT Probe Port    Probe-IP
STS
------------------------------------------- ---------- --- --- ---- ----- ---------------
--
1                                   2009::2             A   1 ICMP
OK
2                                   2008::2             A   1 ICMP
OK


switch-1#
```

This example shows how to filter traffic for an ITD service using user-defined access-lists.

```
switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch-1(config)# ip access-list acl4
switch-1(config-acl)#                  10 permit ip 7.7.1.0/24 6.6.1.0/24
switch-1(config-acl)#                  20 permit ip 7.7.2.0/26 6.6.2.0/26
switch-1(config-acl)#                ipv6 access-list acl6
switch-1(config-ipv6-acl)#                  10 permit ipv6 2004::5/120 2005::5/120
switch-1(config-ipv6-acl)#                  20 permit ipv6 2004::100/122 2005::100/122
switch-1(config-ipv6-acl)#
switch-1(config-ipv6-acl)#
switch-1(config-ipv6-acl)#  itd SER1
switch-1(config-itd)#                   shut
switch-1(config-itd)#                   access-list acl4
switch-1(config-itd)#                   no shut
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.

switch-1(config-itd)#                 itd SER2
switch-1(config-itd)#                   shut
switch-1(config-itd)#                   access-list ipv6 acl6
switch-1(config-itd)#                   no shut
switch-1(config-itd)# end
switch-1#
switch-1# sh run services

!Command: show running-config services
!No configuration change since last restart
!Time: Tue Jan  5 22:57:25 2021

version 10.1(1) Bios:version 01.14
feature itd

itd device-group DG1
  probe icmp frequency 2 timeout 1 retry-down-count 2 retry-up-count 1
  node ip 10.200.3.2
  node ip 10.200.2.2
  node ip 10.200.4.2

itd device-group DG2
  probe icmp
  node ipv6 2009::2
  node ipv6 2008::2
```

```
itd SER1
  device-group DG1
  ingress interface Eth1/17
  failaction node reassign
  load-balance method src ip buckets 4
  access-list acl4
  no shut

itd SER2
  device-group DG2
  ingress interface Eth1/18
  failaction node least-bucket
  load-balance method src ip
  access-list ipv6 acl6
  no shut

switch-1#
```

This example demonstrates how to exclude traffic from an ITD service using user-defined access-lists.

```
switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch-1(config)# itd SER1
switch-1(config-itd)# shut
switch-1(config-itd)# no access-list acl4
switch-1(config-itd)# exclude access-list acl4
switch-1(config-itd)# no sh
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.

switch-1(config-itd)# itd SER2
switch-1(config-itd)# sh
switch-1(config-itd)# no access-list ipv6 acl6
switch-1(config-itd)# exclude access-list acl6
switch-1(config-itd)# no sh
switch-1(config-itd)# end
switch-1#
switch-1# sh run services

!Command: show running-config services
!No configuration change since last restart
!Time: Tue Jan  5 23:01:38 2021

version 10.1(1) Bios:version 01.14
feature itd

itd device-group DG1
  probe icmp frequency 2 timeout 1 retry-down-count 2 retry-up-count 1
  node ip 10.200.3.2
  node ip 10.200.2.2
  node ip 10.200.4.2

itd device-group DG2
  probe icmp
  node ipv6 2009::2
  node ipv6 2008::2

itd SER1
  device-group DG1
  ingress interface Eth1/17
  failaction node reassign
  load-balance method src ip buckets 4
  exclude access-list acl4
  no shut
```

```
itd SER2
  device-group DG2
  ingress interface Eth1/18
  failaction node least-bucket
  load-balance method src ip
  exclude access-list acl6
  no shut

switch-1#
```

This example shows how to update the rules for a user-defined access-list and enable the changes for ITD services using such user ACLS.

```
switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch-1(config)# ip access-list acl5
switch-1(config-acl)#                    10 permit ip 7.7.1.0/24 6.6.1.0/24
switch-1(config-acl)#                itd SER1
switch-1(config-itd)#                    shut
switch-1(config-itd)#                    access-list acl5
switch-1(config-itd)#                    no shut
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.

switch-1(config-itd)#  ip access-list acl5
switch-1(config-acl)#                   20 permit ip 7.7.2.0/26 6.6.2.0/26
switch-1(config-acl)#                itd session access-list acl5 refresh
switch-1(config)#  end
switch-1#
switch-1# sh run services

!Command: show running-config services
!No configuration change since last restart
!Time: Tue Jan  5 23:07:42 2021

version 10.1(1) Bios:version 01.14
feature itd

itd device-group DG1
  probe icmp frequency 2 timeout 1 retry-down-count 2 retry-up-count 1
  node ip 10.200.3.2
  node ip 10.200.2.2
  node ip 10.200.4.2

itd device-group DG2
  probe icmp
  node ipv6 2009::2
  node ipv6 2008::2

itd SER1
  device-group DG1
  ingress interface Eth1/17
  failaction node reassign
  load-balance method src ip buckets 4
  access-list acl5
  exclude access-list acl4
  no shut

itd SER2
  device-group DG2
  ingress interface Eth1/18
  failaction node least-bucket
  load-balance method src ip
  exclude access-list acl6
  no shut

switch-1#
```

This example shows how to use an ITD service specifically for traffic destined to defined ITD virtual IP addresses.

```
switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch-1(config)# itd SER1
switch-1(config-itd)#                            shut
switch-1(config-itd)#                            no access-list acl5
switch-1(config-itd)#                            load-balance method src ip buckets 64
switch-1(config-itd)#                            virtual ip 6.6.1.1 255.255.255.192
switch-1(config-itd)#                            virtual ip 6.6.1.64 255.255.255.192
switch-1(config-itd)#                            failaction node per-bucket
switch-1(config-itd)#                            no shut
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.

switch-1(config-itd)#                          itd SER2
switch-1(config-itd)#                            shut
switch-1(config-itd)#                            load-balance method src ip buckets 64
switch-1(config-itd)#                            virtual ipv6 2005::100 121
switch-1(config-itd)#                            virtual ipv6 2005:: 121
switch-1(config-itd)#                            failaction bucket distribute
switch-1(config-itd)#                            no shut
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.

switch-1(config-itd)#  end
switch-1#
switch-1# sh run services

!Command: show running-config services
!No configuration change since last restart
!Time: Tue Jan  5 23:17:20 2021

version 10.1(1) Bios:version 01.14
feature itd

itd device-group DG1
  probe icmp frequency 2 timeout 1 retry-down-count 2 retry-up-count 1
  node ip 10.200.3.2
  node ip 10.200.2.2
  node ip 10.200.4.2

itd device-group DG2
  probe icmp
  node ipv6 2009::2
  node ipv6 2008::2

itd SER1
  device-group DG1
  virtual ip 6.6.1.1 255.255.255.192
  virtual ip 6.6.1.64 255.255.255.192
  ingress interface Eth1/17
  failaction node per-bucket
  load-balance method src ip buckets 64
  exclude access-list acl4
  no shut
```

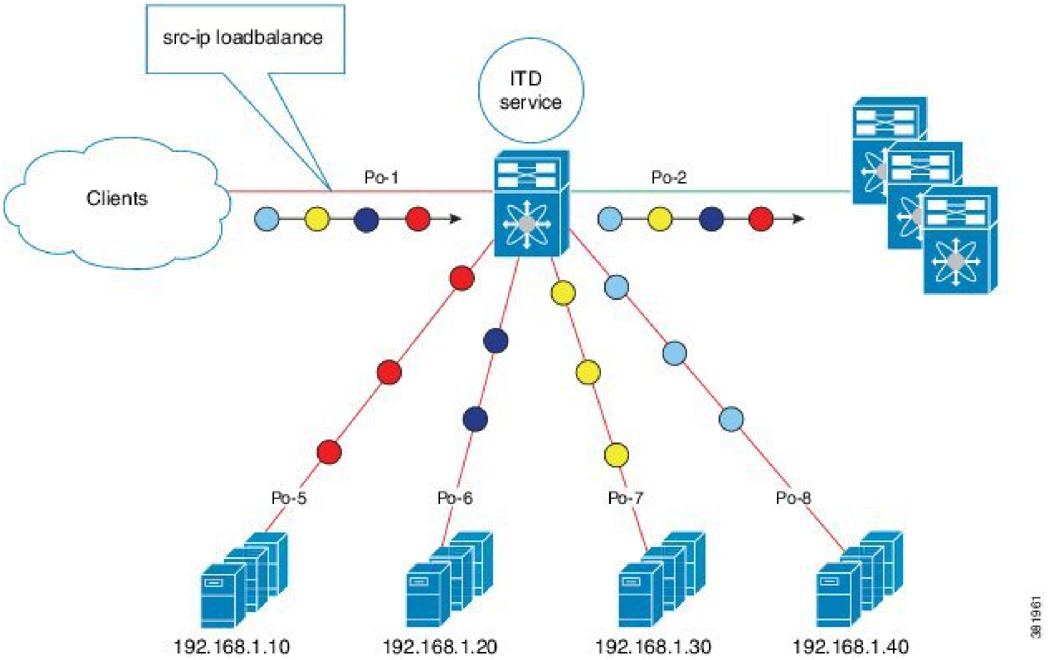
```
itd SER2
  device-group DG2
  virtual ipv6 2005::100 121
  virtual ipv6 2005:: 121
  ingress interface Eth1/18
  failaction bucket distribute
  load-balance method src ip buckets 64
  exclude access-list acl6
  no shut

switch-1#
switch-1# sh itd brief

Legend:
 C-S(Config-State): A-Active,S-Standby,F-Failed
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets    Interface
-------------- ---------- -------- ---------  --------------
SER1           src-ip     ACTIVE   64         Eth1/17

Source Interface
----------------


Exclude ACL
-------------------------------
 acl4

Device Group                                       Probe  Port
-------------------------------------------------- ----- ------
DG1                                                 ICMP

Virtual IP                              Netmask/Prefix Protocol     Port
------------------------------------------------------ ------------ ----------
6.6.1.1 / 255.255.255.192                              IP           0


Node  IP                  Cluster-id C-S WGT Probe Port     Probe-IP   STS
------------------------- ---------- -- --- ---- ----- --------------- --
1              10.200.3.2            A   1 ICMP                       OK
2              10.200.2.2            A   1 ICMP                       OK
3              10.200.4.2            A   1 ICMP                       OK

Virtual IP                              Netmask/Prefix Protocol     Port
------------------------------------------------------ ------------ ----------
6.6.1.64 / 255.255.255.192                             IP           0


Node  IP                  Cluster-id C-S WGT Probe Port     Probe-IP   STS
------------------------- ---------- -- --- ---- ----- --------------- --
1              10.200.3.2            A   1 ICMP                       OK
2              10.200.2.2            A   1 ICMP                       OK
3              10.200.4.2            A   1 ICMP                       OK

Legend:
 C-S(Config-State): A-Active,S-Standby,F-Failed
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets    Interface
-------------- ---------- -------- ---------  --------------
SER2           src-ip     ACTIVE   64         Eth1/18

Source Interface
```

```
----------------


Exclude ACL
-------------------------------
 acl6

Device Group                                       Probe  Port
-------------------------------------------------- ----- ------
DG2                                                 ICMP

Virtual IP                              Netmask/Prefix Protocol     Port
------------------------------------------------------ ------------ ----------
2005::100 / 121                                        IP           0


Node      IP                                Cluster-id C-S WGT Probe Port    Probe-IP
STS
------------------------------------------- ---------- --- --- ---- ----- ---------------
--
1                                   2009::2             A   1 ICMP
OK
2                                   2008::2             A   1 ICMP
OK

Virtual IP                              Netmask/Prefix Protocol     Port
------------------------------------------------------ ------------ ----------
2005:: / 121                                           IP           0


Node      IP                                Cluster-id C-S WGT Probe Port    Probe-IP
STS
------------------------------------------- ---------- --- --- ---- ----- ---------------
--
1                                   2009::2             A   1 ICMP
OK
2                                   2008::2             A   1 ICMP
OK

switch-1#
```

Configuration Example: One-Arm Deployment Mode

The configuration below uses the topology in the following figure:

Figure 4: One-Arm Deployment Mode



Step 1: Define the device group.

```
switch(config)# itd device-group DG
switch(config-device-group)# node ip 210.10.10.11
switch(config-device-group)# node ip 210.10.10.12
switch(config-device-group)# node ip 210.10.10.13
switch(config-device-group)# node ip 210.10.10.14
switch(config-device-group)# probe icmp
```

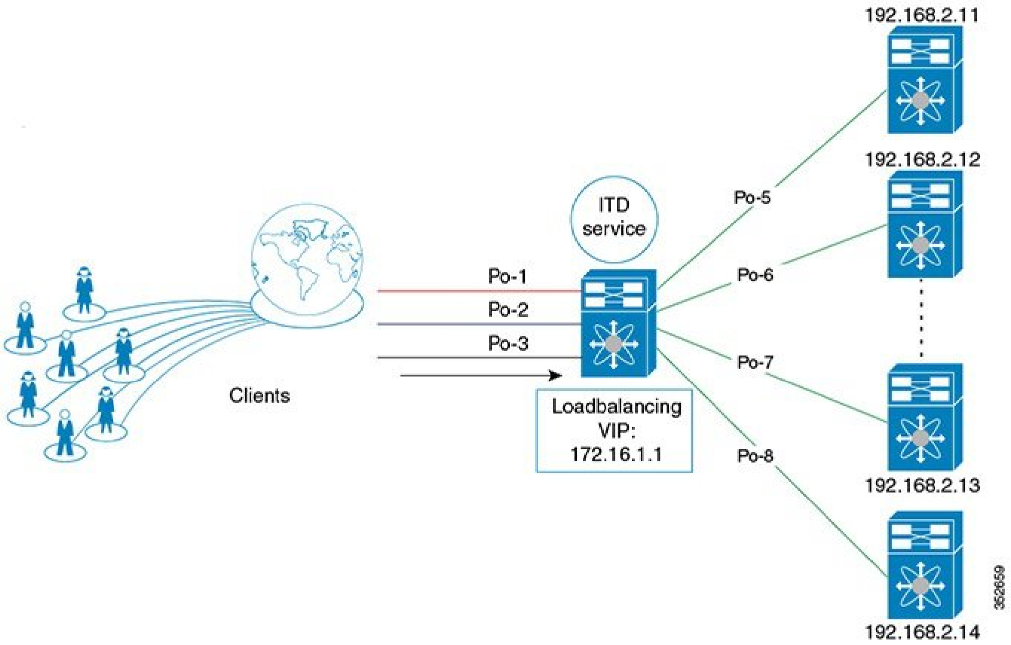
Step 2: Define the ITD service.

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 1
switch(config-itd)# device-group DG
switch(config-itd)# no shutdown
```

Configuration Example: Server Load-Balancing Deployment Mode

The configuration below uses the topology in the following figure:

Figure 5: ITD Load Distribution with VIP



Step 1: Define the device group.

```
switch(config)# itd device-group DG
switch(config-device-group)# node ip 192.168.2.11
switch(config-device-group)# node ip 192.168.2.12
switch(config-device-group)# node ip 192.168.2.13
switch(config-device-group)# node ip 192.168.2.14
switch(config-device-group)# probe icmp
```

Step 2: Define the ITD service.

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 1
switch(config-itd)# ingress interface port-channel 2
switch(config-itd)# ingress interface port-channel 3
switch(config-itd)# device-group DG
Switch(config-itd)# virtual ip 172.16.1.1 255.255.255.255
switch(config-itd)# no shutdown
```

Configuration Example: ITD as WCCP Replacement (Web-Proxy Deployment Mode)

A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A web-proxy server specifically operates as an intermediary between a local network and the Internet. Typically, a web-proxy server needs the network device to redirect Internet-bound web traffic toward it (forward flow); however, subsequent packet forwarding only requires the network device to forward the packet regularly.

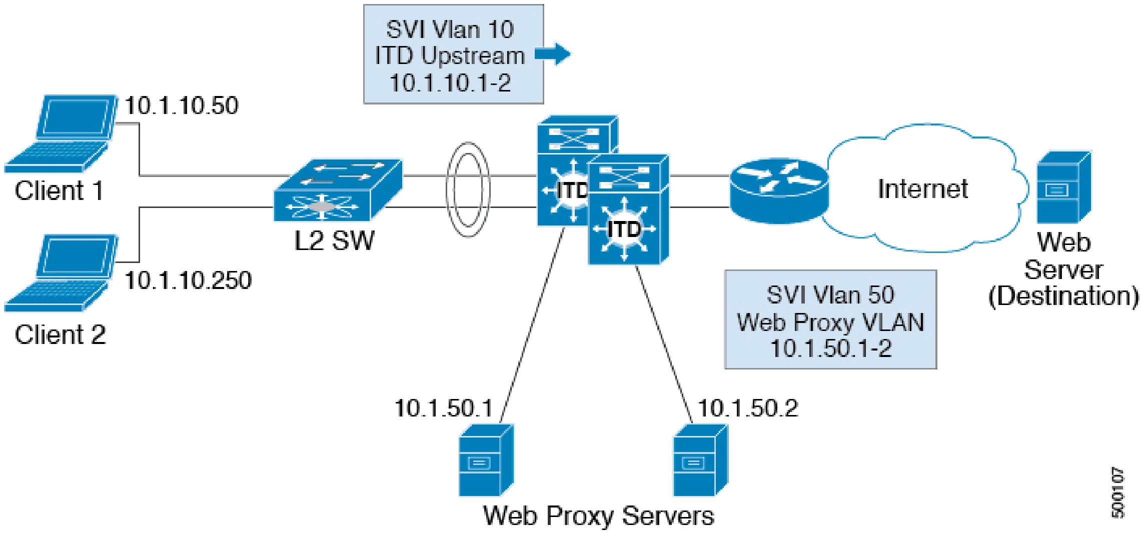
In a web-proxy deployment with ITD, the switch matches the Internet-bound web traffic and load balances it toward the proxy servers. The proxy servers work in an autonomous mode (independent of WCCP and as Active-Active) and handle the traffic that gets redirected to them. The node health probing done through ITD serves the purpose of tracking the state of the nodes and removing or adding them back appropriately based on their availability. Standby servers can also be configured at the group level or node level for redundancy.

ITD redirection is normally only required in the forward direction in the client-facing VLAN. Subsequently, the packets are routed or forwarded without any ITD redirection or distribution. ITD with such web-proxy deployments only need one ITD service, which is configured for the forward direction. However, reverse traffic redirection is required, with traffic selection based on the source Layer 4 ports. Flow symmetry also needs to be maintained by reversing the LB parameter.

With ITD for web-proxy deployments, ITD probes are used to check the availability of the web-proxy server, which is critical because traffic sent toward a failed proxy server is lost.

The configuration below uses the topology in the following figure:

Figure 6: Web-Proxy Deployment Mode



In this example, destination port 80/443 (ingress VLAN 10) to the Internet will be distributed to web-proxy servers 10.1.50.1 and 10.1.50.2. Traffic on VLAN 10 destined to private networks (10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12) will not be sent to the proxy.

Step 0: Configure an access-list

```
ip access-list ACL1
  10 permit ip any any tcp 80
  20 permit ip any any tcp 443
```

Step 1: Configure the ITD device group web-proxy servers and point to the server IP addresses.

```
itd device-group Web_Proxy_Servers
  probe icmp
  node ip 10.1.50.1
  node ip 10.1.50.2
```

Step 2: Configure an exclude ACL to exclude all traffic destined to private IP addresses.

```
ip access-list itd_exclude_ACL
  10 permit ip any 10.0.0.0/8
  20 permit ip any 192.168.0.0/16
  30 permit ip any 172.16.0.0/12
```

Step 3: Apply the exclude ACL.

```
Itd Web_proxy_SERVICE
  device-group Web_Proxy_Servers
  exclude access-list itd_exclude_ACL
  access-list ACL1
  ingress interface Vlan 10
  failaction node reassign
  load-balance method src ip
  no shutdown
```

If return traffic redirection is also required for any reason, the following additional configuration steps are needed.

Note Only port filtering is possible using the Layer 4 range operator. Also, the exclude ACL supports only permit entries.

Step 4: Configure the return exclude ACL to exclude all but ports 80 and 443.

```
ip access-list itd_exclude_return
  10 permit tcp any range 0 79 any
  20 permit tcp any range 81 442 any
  30 permit tcp any range 444 65535 any
```

Step 5: Configure the return ITD service for the return traffic and apply the exclude ACL.

```
Itd Web_proxy_SERVICE
  device-group Web_Proxy_Servers
  exclude access-list itd_exclude_return
  ingress interface Vlan 20   <- Internet-facing ingress interface on the Nexus switch
  failaction node reassign
  load-balance method dst ip  <- Flow symmetry between forward/return flow achieved by
flipping the LB parameter
  no shutdown
```

Configuration Example: Firewall on a Stick

ITD Services

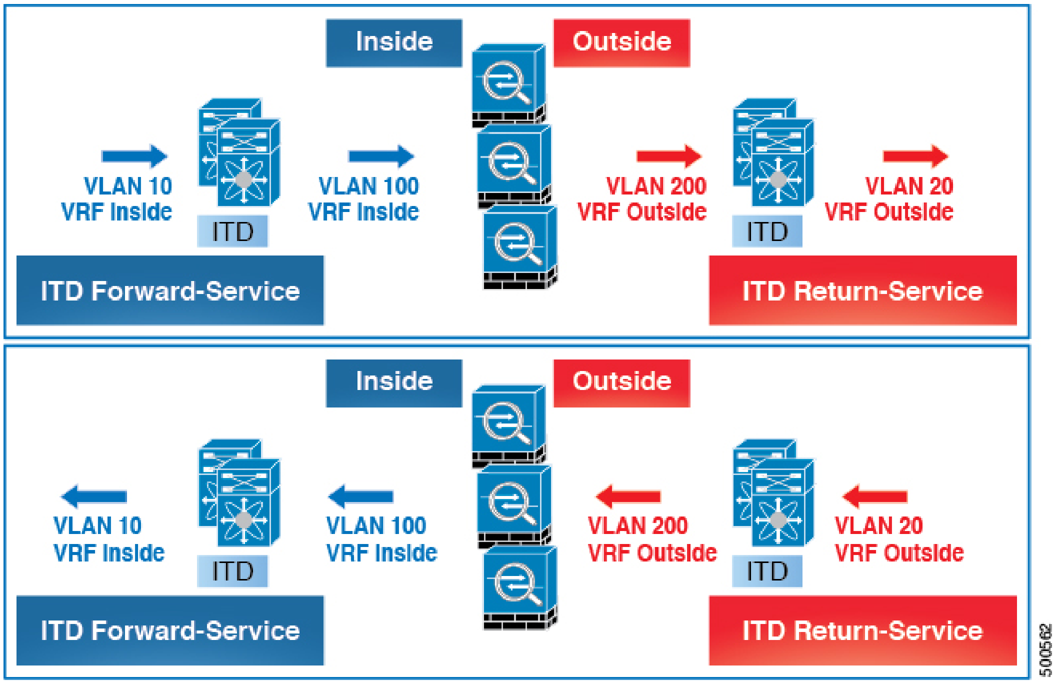
An ITD service configuration defines the ITD traffic distribution for a particular direction of the traffic flow. If both directions of a flow need to be redirected, two ITD services need to be configured, one for the forward traffic flow and one for the return traffic flow. Because an ASA has different inside and outside interface IP addresses, two different device groups also need to be configured to point to the corresponding inside and outside IP addresses.

ASA VLANs

The ITD forward and return services are attached to the inside and outside VLAN SVIs on the Nexus switch. Because a security application such as a firewall needs to examine all traffic, no traffic filtering is configured on the services. As a result, any traffic that hits the SVI is redirected to the corresponding ASA interfaces.

If the ASA interfaces are configured on the same VLANs as that of the switch, the traffic going to the switch from the firewall is redirected to the ASA due to the presence of an ITD service on another VLAN on the switch. Therefore, a pair of separate VLANs is required to prevent traffic looping between the firewalls and the Nexus switch.

Figure 7: ITD ASA Deployment



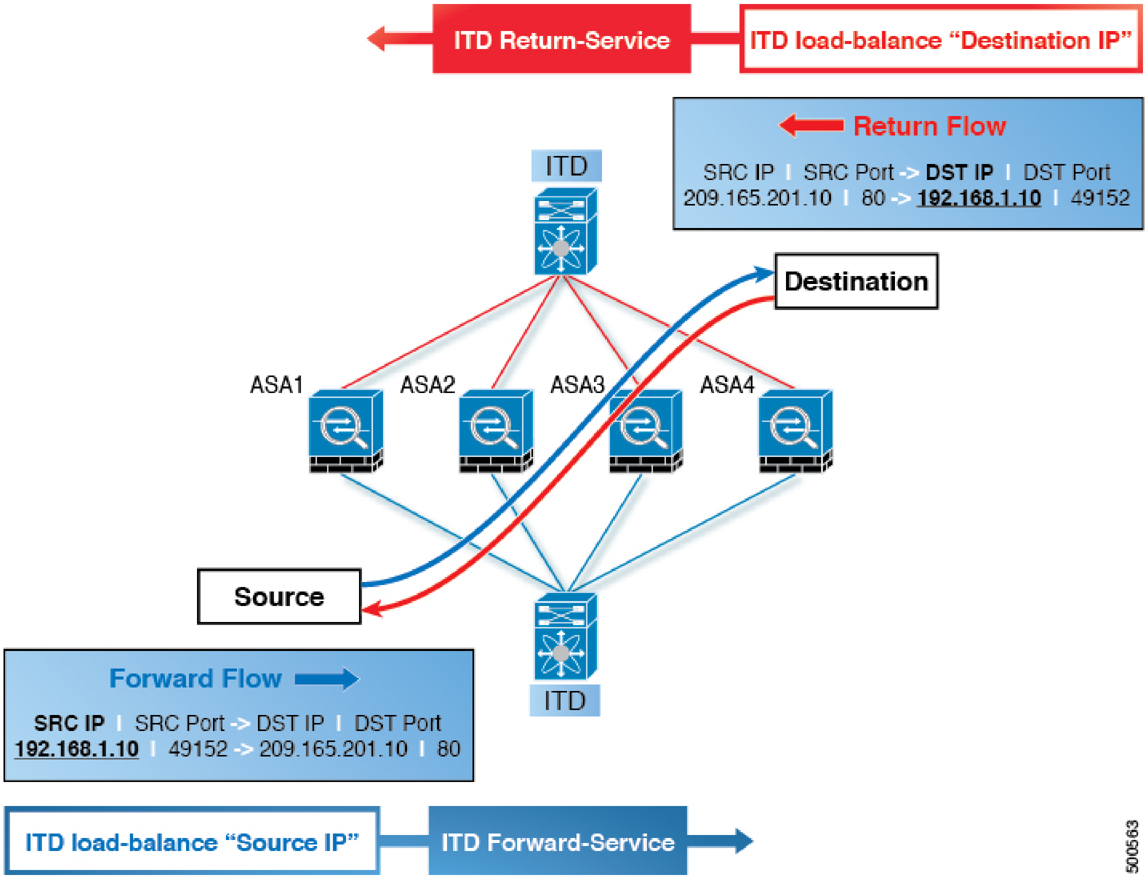
This diagram shows VLANs 10 and 20 as the inside and outside interfaces toward the source and destination on the network. VLANs 100 and 200 are used toward the ASAs to ensure loop-free traffic.

Flow Symmetry

Firewalls typically inspect traffic flows in both the forward and return directions. Due to the stateful nature of the inspection, it is generally required that flow symmetry be maintained during normal operation of firewalls that are not clustered. Even for clustered firewalls, the asymmetry of traffic flows results in the increased redirection of flows over cluster control links. The increase of asymmetric flows adds unnecessary overhead to the firewalls and adversely impedes performance.

Flow symmetry can be achieved using the inherent IP persistence and deterministic nature of the ITD algorithms. A typical ITD configuration for firewalls uses one ITD service for the forward flow and one ITD service for the return flow. Configuring these two ITD services in such a way that the value of the load-balance parameter remains the same for both services ensures that flow symmetry is maintained.

Figure 8: Flow Symmetry in ITD ASA Deployment

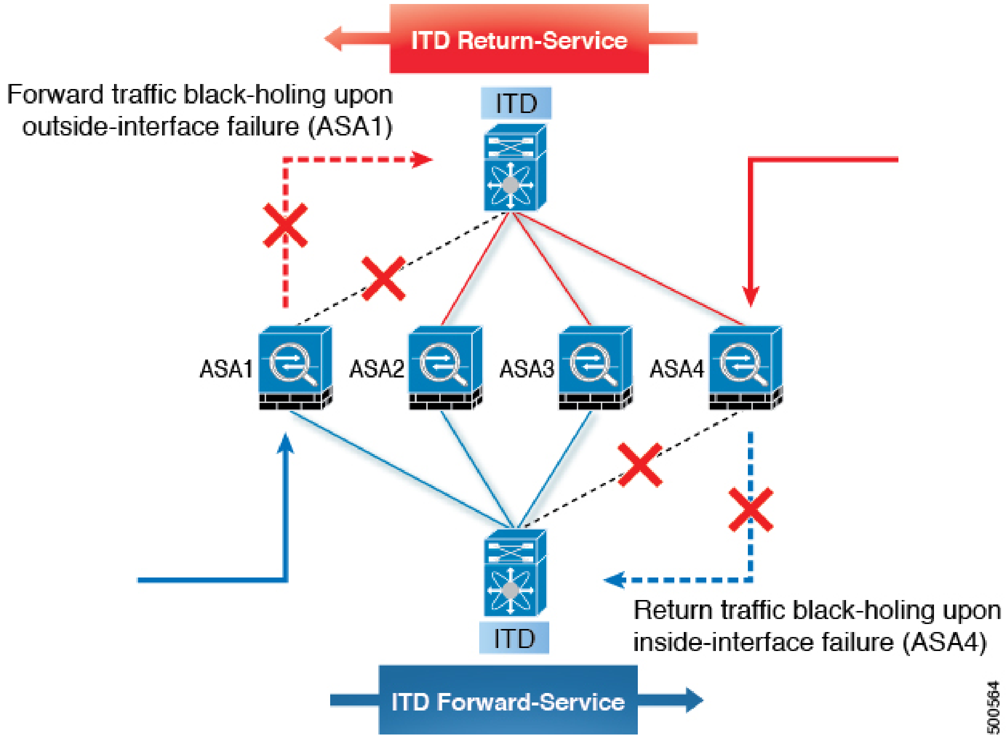


This diagram shows how the source IP address of the forward flow and the destination IP address of the reverse flow remain constant. Choosing the appropriate parameter for the each ITD service ensures flow symmetry due to ITD IP persistence.

Link Failures

When the ASA inside or outside interface fails, the traffic coming into the other side of that ASA can be lost because the egress interface for traffic is down. The ITD peer switch node state synchronization feature can resolve this issue by removing the remote side of the ASA from ITD and synchronizing the node states across the switches.

Figure 9: ASA Failure Scenario

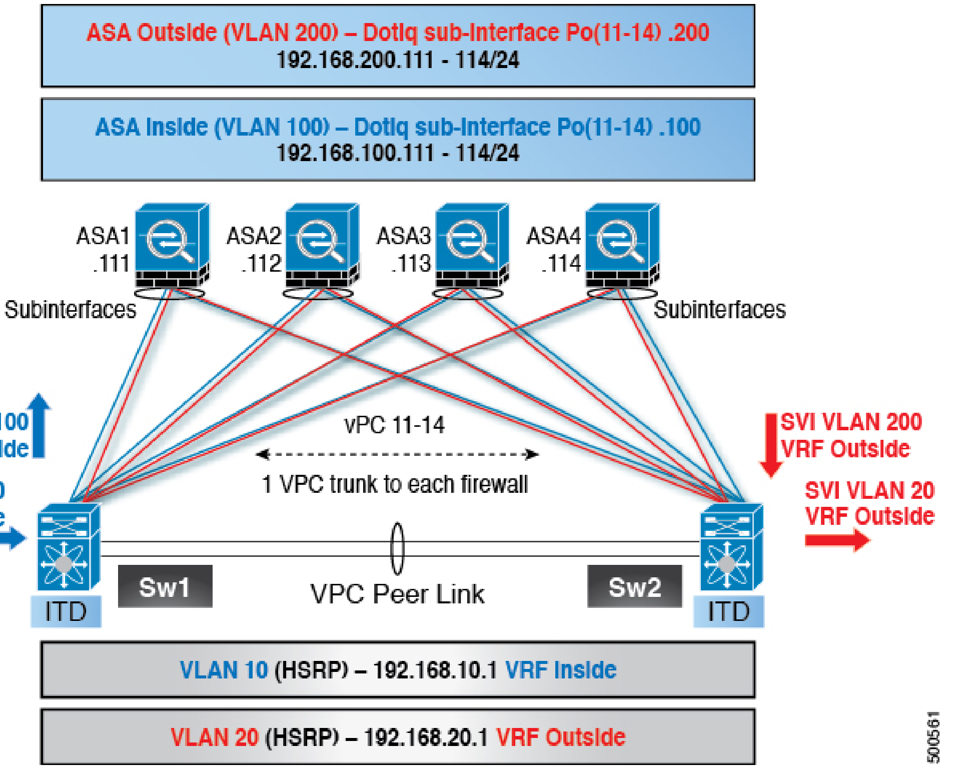

ITD Return-Service
Forward traffic black-holing upon outside-interface failure (ASA1)
ITD
ASA1
ASA2
ASA3
ASA4
ITD
Return traffic black-holing upon inside-interface failure (ASA4)
ITD Forward-Service
500564

The ITD peer switch node state synchronization feature is supported only in a dual-switch non-vPC (or single switch) topology. ASA clustering also solves this problem because clustering ensures that the ASA is fully brought down in the case of such failures. The firewall-on-a-stick implementation (single link or vPC) does not address this issue because the ASA inside and outside interfaces belong to the same physical (or virtual) interface.

Configuration Example

In a firewall on a stick deployment, vPC port-channel (or single port) trunks are typically used to connect the ASAs to the switches. In this configuration, the inside and outside interfaces are dot1q subinterfaces (VLAN 100 and 200), and the switches have two VLANs or SVIs each in the inside and outside contexts without physical port separation between them.

Figure 10: Firewall on a Stick (with vPC) Deployment



Step 1: Configure the switch.

Note This example shows a partial configuration of switch Sw1. The configuration needs to be extended appropriately toward all the ASAs similarly. Other features are assumed to be configured already.

```
interface vlan 10
  description Inside_Vlan_to_Network
  vrf member INSIDE
  ip address 192.168.10.10/24
  hsrp 10
    ip address 192.168.10.1

interface vlan 20
  description Outside_Vlan_to_Network
  vrf member OUTSIDE
  ip address 192.168.20.10/24
  hsrp 20
    ip address 192.168.20.1

interface vlan 100
  description Inside_Vlan_to_ASA
  vrf member INSIDE
  ip address 192.168.100.10/24
  hsrp 100
    ip address 192.168.100.1

interface vlan 200
  description Outside_Vlan_to_ASA
  vrf member OUTSIDE
  ip address 192.168.200.10/24
  hsrp 200
    ip address 192.168.200.1

interface port-channel 11
  description VPC_TO_ASA1
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  vpc 11
  no shutdown

interface ethernet 4/25
  description Link_To_ITD-ASA-1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  channel-group 11 mode active
  no shutdown

interface port-channel 41
  description Downstream_vPC_to_network
  switchport mode trunk
  switchport trunk allowed vlan 10,20
  vpc 41
  no shutdown

interface ethernet 5/1-4
  description Downstream_vPC_member
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20
  channel-group 41
  no shutdown


itd device-group FW_INSIDE
    #Config Firewall Inside interfaces as nodes
  node ip 192.168.100.111
  node ip 192.168.100.112
  node ip 192.168.100.113
  node ip 192.168.100.114
probe icmp frequency 5 timeout 5 retry-count 1

itd device-group FW_OUTSIDE
    #Config Firewall Outside interfaces as nodes
  node ip 192.168.200.111
  node ip 192.168.200.112
  node ip 192.168.200.113
  node ip 192.168.200.114
probe icmp frequency 5 timeout 5 retry-count 1

itd INSIDE
  vrf INSIDE
    #applies ITD service to VRF 'INSIDE'
  device-group FW_INSIDE
    #FW inside interfaces attached to service.
  ingress interface vlan 10
    #applies ITD route map to vlan 1101 interface
  failaction node reassign
    #To use the next available Active FW if an FW goes offline
  load-balance method src ip buckets 16
    #distributes traffic into 16 buckets
    #load balances traffic based on Source IP.
    #OUTSIDE service uses Dest IP.
  no shut

itd OUTSIDE
  vrf OUTSIDE
    #applies ITD service to VRF 'OUTSIDE'
  device-group FW_OUTSIDE
  ingress interface vlan 20
  failaction node reassign
  load-balance method dst ip buckets 16
    #load balances traffic based on Dest IP.
    #INSIDE service uses Src IP.
  no shut
```

Step 2: Configure ASA.

```
interface port-channel 11
  nameif aggregate
  security-level 100
  no ip address

interface port-channel 11.100
  description INSIDE
  vlan 100
  nameif inside
  security-level 100
  ip address 192.168.100.111 255.255.255.0

interface port-channel 11.200
  description OUTSIDE
  vlan 200
  nameif outside
  security-level 100
  ip address 192.168.200.111 255.255.255.0

same-security-traffic permit inter-interface

interface TenGigabitEthernet 0/6
  description CONNECTED_TO_SWITCH-A-VPC
  channel-group 11 mode active
  no nameif
  no security-level

interface TenGigabitEthernet 0/7
  description CONNECTED_TO_SWITCH-B-VPC
  channel-group 11 mode active
  no nameif
  no security-level
```

The following points apply to this example topology:

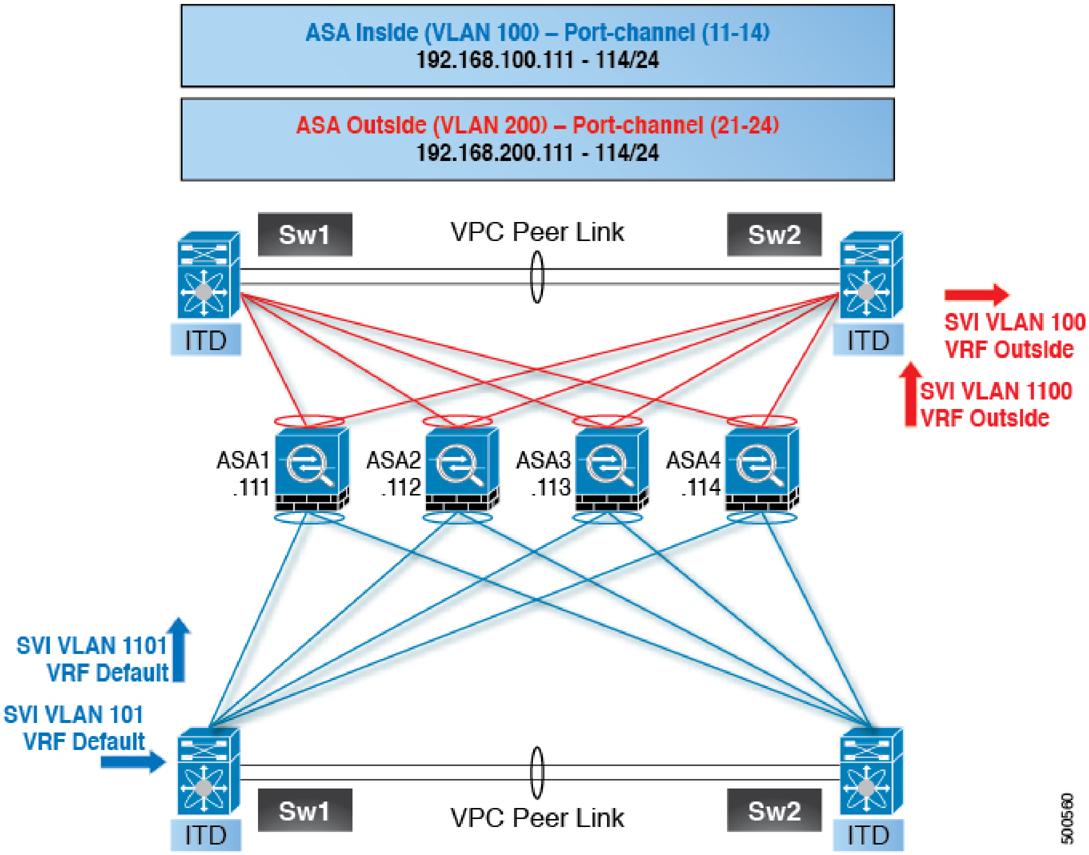
- VLANs 10, 20, 100, and 200 and their SVIs are mapped to appropriate VRFs.
- This example uses an ITD load-balancing configuration to achieve flow symmetry.
- In a vPC scenario, as long as one member of the vPC is up, there is no change to ITD. The ITD redirection on the switch with a failed vPC leg will traverse the peer switch through the peer link as in a typical vPC deployment.
- In this topology, traffic is not lost upon physical link failure because the inside and outside interfaces are tied to the same physical or virtual interface on the ASA (dot1q subinterfaces).

- To support routing protocol neighbors over a vPC, the **layer3 peer-router** command needs to be configured within the vPC domain.
- VRFs are needed because Layer 3 interfaces are used to connect to both inside and outside firewall interfaces. VRFs are put in place to prevent traffic from being (inter-VLAN) routed around the firewall in certain cases.
- Traffic is directed toward ASAs using policy-based routing, so routes are not needed.

Configuration Example: Firewall in Dual-Switch Sandwich Mode with vPCs

For sandwich mode with vPCs, the inside and outside ASA interfaces are each assigned to separate port-channel bundles. As a result of the vPCs, a single link failure does not impede the traffic flow, and ITD will continue to forward through the peer switch's link toward the ASA.

Figure 11: Dual-Switch Sandwich Mode with vPCs



Step 1: Configure the two switches.

```
switch #1:
interface vlan 10
  description INSIDE_VLAN
  ip address 192.168.10.10/24

interface vlan 100
  description FW_INSIDE_VLAN
  ip address 192.168.100.10/24

interface port-channel 11
  description To_ASA-1_INSIDE
  switchport mode access
  switchport access vlan 100
  vpc 11

interface ethernet 4/1
  description To_ASA-1_INSIDE
  switchport mode access
  switchport access vlan 100
  channel-group 11 mode active


switch #2:
interface vlan 20
  description OUTSIDE_VLAN
  ip address 192.168.20.10/24

interface vlan 200
  description FW_OUTSIDE_VLAN
  ip address 192.168.200.10/24

interface port-channel 21
  description To_ASA-1_OUTSIDE
  switchport mode access
  switchport access vlan 200
  vpc 11

interface ethernet 4/25
  description To_ASA-1_OUTSIDE
  switchport mode access
  switchport access vlan 200
  channel-group 21 mode active
```

Step 2: Configure ASA.

```
interface port-channel 11
  description INSIDE
  vlan 100
  nameif inside
  security-level 100
  ip address 192.168.100.111 255.255.255.0

interface port-channel 21
  description OUTSIDE
  vlan 100
  nameif outside
  security-level 100
  ip address 192.168.200.111 255.255.255.0

same-security-traffic permit inter-interface

interface TenGigabitEthernet 0/6
  description CONNECTED_TO_SWITCH-A-VPC
  channel-group 11 mode active
  no nameif
  no security-level

interface TenGigabitEthernet 0/7
  description CONNECTED_TO_SWITCH-B-VPC
  channel-group 11 mode active
  no nameif
  no security-level

interface TenGigabitEthernet 0/8
  description CONNECTED_TO_SWITCH-A-VPC
  channel-group 21 mode active
  no nameif
  no security-level

interface TenGigabitEthernet 0/9
  description CONNECTED_TO_SWITCH-B-VPC
  channel-group 21 mode active
  no nameif
  no security-level
```

The following points apply to this example topology:

- This example uses an ITD load-balancing configuration to achieve flow symmetry.
- In a vPC scenario, as long as one member of the vPC is up, there is no change to ITD. The ITD redirection on the switch with a failed vPC leg will traverse the peer switch through the peer link as in a typical vPC deployment.
- In this topology, traffic loss can occur if one of the port channels on the ASA (or a single physical link in a non-vPC topology) fails.
- To support routing protocol neighbors over a vPC, the **layer3 peer-router** command needs to be configured within the vPC domain.
- Traffic is directed toward ASAs using policy-based routing, so routes are not needed.

Configuration Example: Firewall in Layer 3 Clustering

An ASA cluster consists of multiple ASAs acting as a single unit. Grouping multiple ASAs together as a single logical device provides the convenience of a single device (management and integration into a network) while achieving increased throughput and redundancy of multiple devices.

ITD can load balance to individual mode Layer 3 ASA clusters. ITD is complementary to clustering in that ITD provides the predictability of knowing which flows are handled by each firewall. Instead of relying on OSPF ECMP and port-channel hashing algorithms, you can use ITD buckets to determine these flows.

With Layer 3 clusters, the flow owner can be predetermined based on the bucket allocation. Without ITD and Layer 3 clustering, the initial choice of owner is typically unpredictable. With ITD, the owner can be predetermined.

ASA clustering also uses a backup flow owner. For every flow traversing any particular firewall in the cluster, another firewall stores the state of that flow and the ASA that owns the flow. If the real active flow owner fails, ITD failaction reassign will cause all flows (the bucket) from the failed owner ASA to shift to the next active node listed in the device group. If the new firewall to receive this traffic is not the backup owner for the flows it receives, it should receive the flow state information from the backup owner and process the traffic seamlessly.

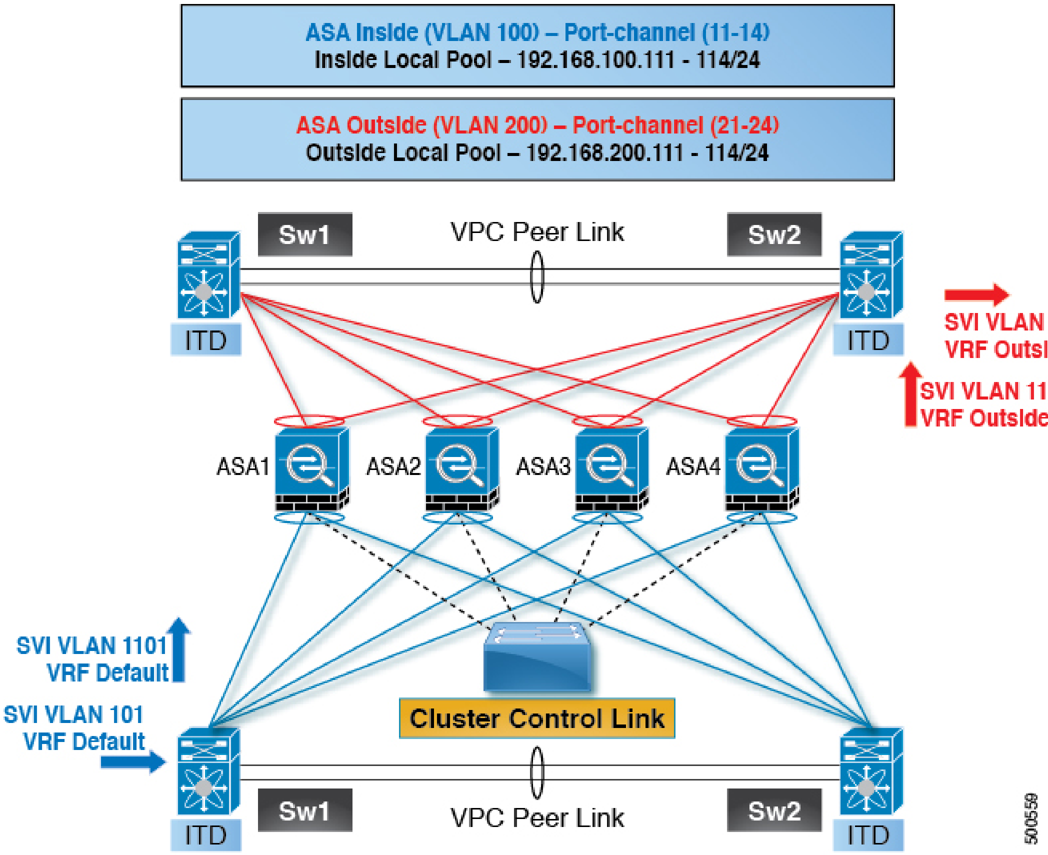
A potential drawback to using ASA clustering with ITD is that backup flows and other cluster table operations consume memory and CPU resources that non-clustered firewalls do not. Therefore, firewall performance might improve when using non-clustered firewalls.

The following table shows a summary comparison of the impact to the cluster control link (CCL) that occurs with ECMP versus ITD when the ASA device status changes.

Table 3: ECMP versus ITD - CCL Impact Summary Comparison

ASA Status	ITD	ECMP
Steady State	Minimal traffic on the CCL and expected traffic types. Exact same load distribution irrespective of the type of line card and switch.	Minimal traffic on the CCL if the same line card type and switch model is used everywhere. If differing hardware is used, a higher level of asymmetry might occur, causing traffic on the CCL network. Each hardware has a different hash function. Two switches (for example, in a vPC) might send the same flow to different ASA devices, causing CCL traffic.
Single ASA Failure	No additional traffic on the CCL. ITD offers IP stickiness and resilient hashing.	All flows are rehashed, and additional traffic redirection occurs on the CCL. Traffic to all ASA devices in the cluster might be affected.
Single ASA Recovery	Traffic redirection can occur on the CCL between two ASA devices in the cluster: the recovered ASA that receives a bucket and the ASA that previously serviced that bucket.	Additional traffic redirection can occur on the CCL. Traffic to all ASA devices in the cluster might be affected.
ASA Addition	Minimal additional traffic on the CCL.	All flows are rehashed, and additional traffic redirection occurs on the CCL. Traffic to all ASA devices in the cluster might be affected.

Figure 12: ASA Cluster with Dual-Switch Sandwich with vPC



Step 1: Configure the two switches.

Note The introduction of clustering does not change the ITD configuration. The ITD configuration depends on the type of topology. In this example, the configuration is the same as in the dual-switch sandwich with vPC topology.

```
switch #1:
interface vlan 10
  description INSIDE_VLAN
  ip address 192.168.10.10/24

interface vlan 100
  description FW_INSIDE_VLAN
  ip address 192.168.100.10/24

interface port-channel 11
  description To_ASA-1_INSIDE
  switchport mode access
  switchport access vlan 100
  vpc 11

interface ethernet 4/1
  description To_ASA-1_INSIDE
  switchport mode access
  switchport access vlan 100
  channel-group 11 mode active


switch #2:
interface vlan 20
  description OUTSIDE_VLAN
  ip address 192.168.20.10/24

interface vlan 200
  description FW_OUTSIDE_VLAN
  ip address 192.168.200.10/24

interface port-channel 21
  description To_ASA-1_OUTSIDE
  switchport mode access
  switchport access vlan 200
  vpc 11

interface ethernet 4/25
  description To_ASA-1_OUTSIDE
  switchport mode access
  switchport access vlan 200
  channel-group 21 mode active
```

Step 2: Configure ASA.

```
cluster group ASA-CLUSTER-L3
  local-unit ASA1
  cluster-interface port-channel 31
  ip address 192.168.250.100 255.255.255.0
  piority 1
  health-check holdtime 1.5
  clacp system-mac auto system-priority 1
  enable

mac-address pool MAC-INSIDE aaaa.0101.0001 - aaaa.0101.0008
mac-address pool MAC-OUTSIDE aaaa.0100.0001 - aaaa.0100.0008
ip local pool IP-OUTSIDE 192.168.200.111-192.168.200.114
ip local pool IP-INSIDE 192.168.100.111-192.168.100.114

interface port-channel 11
  description INSIDE
  lacp max-bundle 8
  mac-address cluster-pool MAC-INSIDE
  nameif inside
  security-level 100
  ip address 192.168.100.11 255.255.255.0 cluster-pool IP-INSIDE

interface port-channel 21
  description OUTSIDE
  lacp max-bundle 8
  mac-address cluster-pool MAC-OUTSIDE
  nameif outside
  security-level 100
  ip address 192.168.200.11 255.255.255.0 cluster-pool IP-OUTSIDE

interface port-channel 31
  description Clustering Interface
  lacp max-bundle 8

interface TenGigabitEthernet 0/6
  channel-group 11 mode active
  no nameif
  no security-level
  no ip address

interface TenGigabitEthernet 0/7
  channel-group 11 mode active
  no nameif
  no security-level
  no ip address

interface TenGigabitEthernet 0/8
  channel-group 21 mode active
  no nameif
  no security-level
  no ip address

interface TenGigabitEthernet 0/9
  channel-group 21 mode active
  no nameif
  no security-level
  no ip address

interface TenGigabitEthernet 1/0
  channel-group 31 mode on
  no nameif
  no security-level
  no ip address

interface TenGigabitEthernet 1/1
  channel-group 31 mode on
  no nameif
  no security-level
  no ip address
```

In this example, port channels 11 and 21 are used for the inside and outside interfaces. Port channel 31 is the clustering interface. Individual interfaces are normal routed interfaces, each with its own IP address taken from a pool of IP addresses. The main cluster IP address is a fixed address for the cluster that always belongs to the current primary unit. Similarly, a MAC address POOL is also configured and used under the corresponding inside or outside port channel.

Related Documents