Dynamic Application Policy Routing Configuration Guide, Cisco IOS XE Gibraltar 16.x

First Published: 2019-03-11

Last Modified: 2019-03-11

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E for Catalyst Switching and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

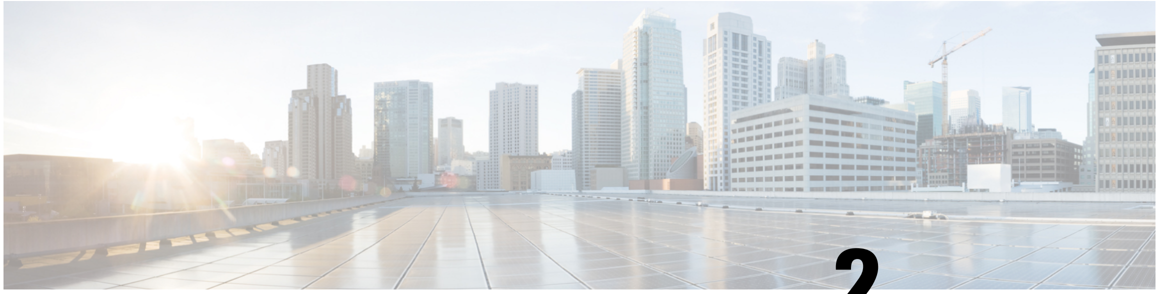
Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

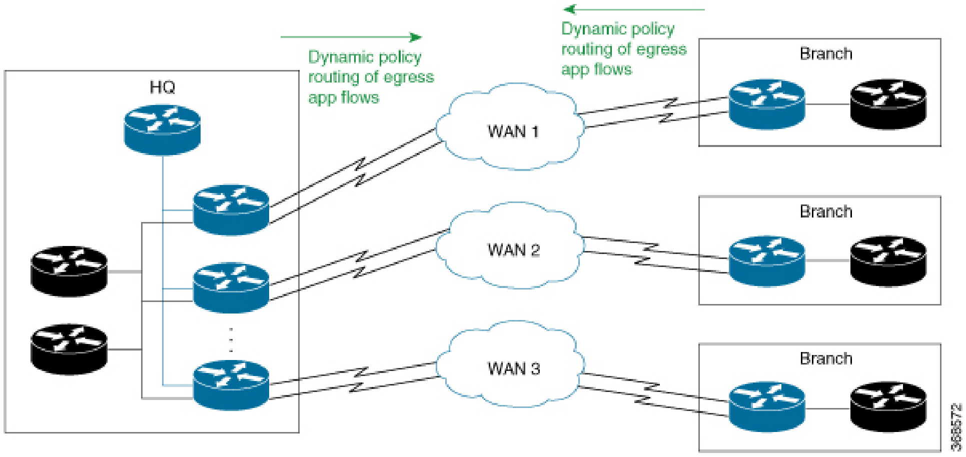


CHAPTER 2

DAPR Overview

Dynamic Application Policy Routing (DAPR) is a WAN-edge egress traffic engineering solution for multi-homed sites. DAPR monitors a WAN link bandwidth and utilization. Also, monitors egress application flow rates in real time and dynamically steers application flows to meet the policy criteria of link preference and link load balancing. DAPR does not have an overlay dependency and therefore cannot manage an overlay or underlay traffic. Typical use cases for DAPR are the WAN edge and the Internet edge.

Figure 1: Dynamic Application Policy Routing



Information about DAPR

This section includes the following topics:

DAPR Fundamentals

1. DAPR is site-local, single-sided, and egress-only:
   - Site-local: DAPR runs independently at each site (Branch, Campus, or Datacenter) with significance only at the local site. DAPR instances running at different sites of an enterprise are completely independent of one another.
   - Single-sided: DAPR has all its functionality and components that are localized at a site. DAPR does not require any components at or any co-ordination with remote sites.
   - Egress-only: DAPR manages only the traffic egressing a site (LAN to WAN). DAPR does not manage ingress traffic (WAN to LAN). More specifically, DAPR only manages the egress flows traversing DAPR-enabled LAN and WAN links.
2. DAPR is for multi-homed sites:
   - DAPR is for sites with multiple WAN links terminating on one or more WAN edge routers that are referred to as DAPR Border-Routers (BR).
   - DAPR provides policy routing of application flows across all the DAPR-enabled WAN links at a site.
3. Role of routing protocols in DAPR:
   - DAPR relies on the routing table (RIB) to determine an application flow destination reachability and hence is independent of routing protocols.
   - The routing protocols' role in DAPR is to make available all possible paths to a destination and not the best path selection. Tune the routing protocol metrics to ensure all possible paths to a destination (not just the best path) are available in the routing table either as equal cost or unequal cost routes.
   - DAPR performs the best path selection for application flows and enforcement.
4. DAPR application flow routing:
   - DAPR dynamic best path selection for application flow-groups is based on:
     - Policy criteria of the link preference and link load balancing:
     - Varying WAN link bandwidth or utilization
     - Varying application flow rates
   - DAPR currently does not monitor the link delay, jitter, and throughput as DAPR does not use any probes.
5. DAPR policy criteria:
   - Link load balancing - Ensures uniform utilization of DAPR. Enables WAN links at a site by dynamically steering application flows across WAN links based on changing link bandwidth or utilization and flow rates.
   - Link preference: Ensure application performance by dynamically steering application flows to specified preferred links.

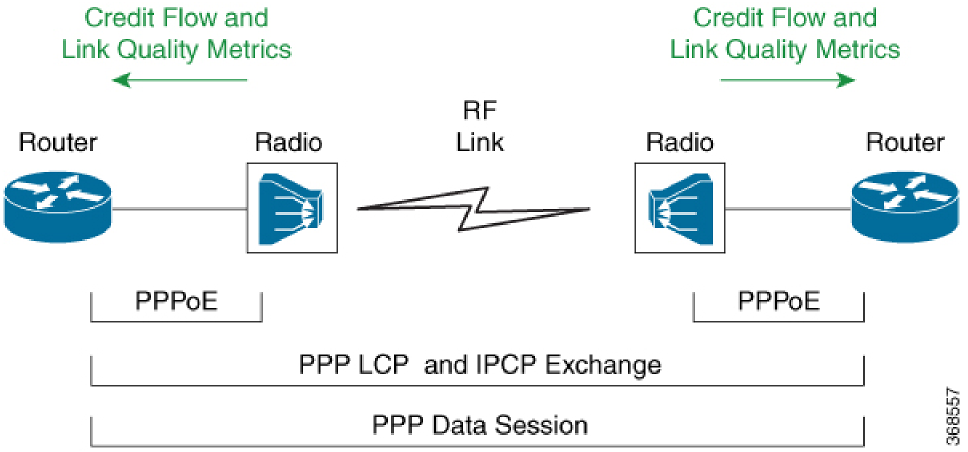
6. DAPR flow-groups:

   - DAPR identifies application flow-groups based on a 3-tuple of source IP-address, destination IP-address, and DSCP only.
   - DAPR currently does not support the identification of an application flow-groups using NBAR or 5-tuple of source-prefix, destination-prefix, protocol, source-ports, and destination-ports.

7. DAPR supports Radio aware routing (RAR) WAN links:

   - RAR is a solution for the variable bandwidth radio links used in mobile ad hoc networks (MANET). RAR helps in quick detection of neighbors and peers. It also tracks the bandwidth changes of radio links and makes it available to applications such as routing protocols and QoS shapers that rely on a link bandwidth. RAR implementation in Cisco IOS XE Gibraltar 16.11.1 is based on RFC-5578 (PPP over Ethernet (PPPoE) Extensions for Credit Flow and Link Metrics). RAR uses a point-to-point virtual-access interface per peer and updates the virtual-access interface bandwidth value when the corresponding radio link's bandwidth changes.

     Figure 2: Radio Aware Routing

     
     Credit Flow and Link Quality Metrics
Credit Flow and Link Quality Metrics
Router
Radio
RF Link
Radio
Router
PPPoE
PPPoE
PPP LCP and IPCP Exchange
PPP Data Session
368557

   - DAPR supports RAR and PPPoE virtual access interfaces as DAPR egress interfaces (DAPR-enabled WAN links). DAPR supports RAR bypass mode only.

DAPR Terminology

The following are the terminologies that are used in the DAPR solution:

- Dynamic Application Policy Routing (DAPR): DAPR is the per-site dynamic policy routing solution for the application flows egressing WAN links.
- Route-Manager (RM): DAPR control plane entity at a site that dynamically computes policy conformant routes for the application flows egressing WAN links.
- Border-Router (BR): WAN edge routers at a site that export monitoring information to and enforce the application flow routes computed by the RM.

- Flow-groups: A group of application flows managed by DAPR as a unit. DAPR route computation and enforcement are on a per flow-group basis. Currently, flows are grouped only based on a 3 tuple of source-address, destination-address, and DSCP.
- Link-groups: An arbitrary group of links that specifies the preferred links in a link preference policy.
- DAPR egress interface: A DAPR enabled WAN interface.
- DAPR ingress interface: A DAPR enabled LAN interface. DAPR manages only the flows traversing DAPR ingress and egress interfaces.
- Ingress-BR: BR that receives a flow-group from LAN. Note that Ingress-BR is per flow-group. A flow-group can have one or more Ingress BRs wherein individual flows of a flow-group enter different BRs from the LAN side.
- Egress-BR: BR through which a flow-group leaves the site through WAN links. Note that Egress-BR is per flow-group. A flow-group can have a single Egress-BR even if the Ingress-BRs are many.
- Locally forwarded flow-groups: Flow-groups for which Ingress-BR and the computed Egress-BR is the same.
- Inter-BR forwarded flows: Flow-groups for which Ingress-BR and the computed Egress-BR are not the same. Such flows are forwarded from Ingress-BR to Egress-BR over the inter-BR IP or GRE tunnel that is referred to as auto-tunnel.
- Auto-tunnel: IP/GRE tunnel between each pair of BRs that are automatically created by DAP.
- Link out-of-policy (OOP) - A condition when DAPR egress exceeds the maximum percentage utilization threshold that is specified in the DAPR policy on RM.
    - Link soft-OOP: OOP link but not exceeding link capacity
    - Link hard-OOP: OOP link exceeding link capacity

DAPR Topologies

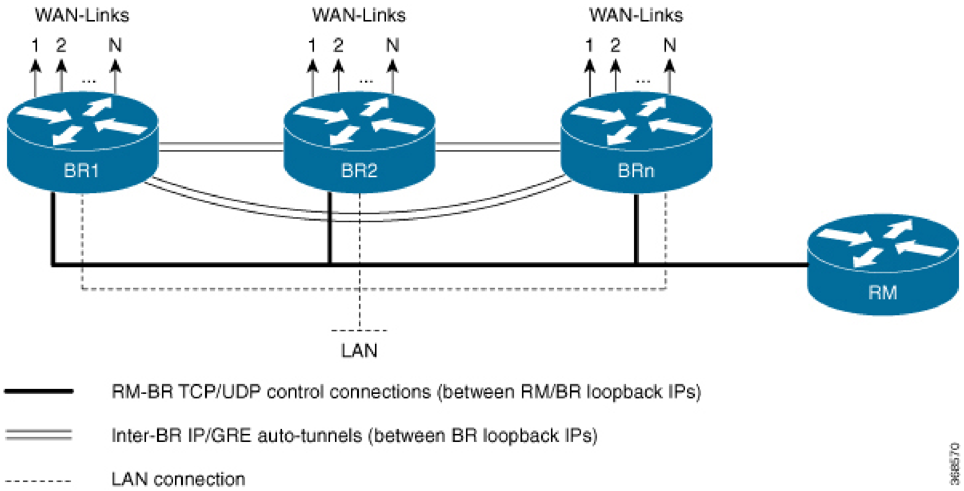
DAPR supports two topologies at a site:

- Standalone RM and BRs
- Co-located RM and BR

Standalone Route Manager and Border Routers

In this topology, Route-Manager (RM) and Border-Routers (BR) are deployed on separate routers. This is commonly used at large sites such as Campus or Headquarters, Datacenter, or large branch sites.

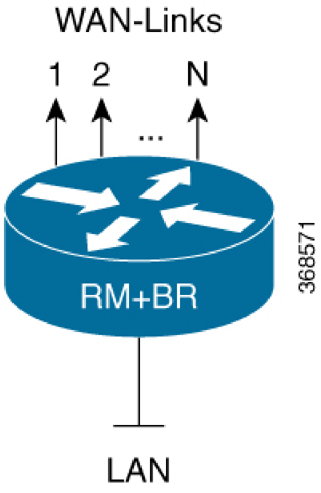
Figure 3: DAPR Standalone RM and BR


WAN-Links
1 2 ... N
WAN-Links
1 2 ... N
WAN-Links
1 2 ... N
BR1
BR2
BRn
RM
LAN
RM-BR TCP/UDP control connections (between RM/BR loopback IPs)
Inter-BR IP/GRE auto-tunnels (between BR loopback IPs)
LAN connection
368570

Co-located Route Manager and Border Routers

In this topology, RM and BR are deployed on a single router. This is commonly used at small sites with a single WAN edge router such as small branch sites.

Figure 4: DAPR Co-located RM and BR



DAPR Components

DAPR solution comprises the following control and data plane functions:

DAPR Control Plane

1. Collection of site-wide metrics for the flow-route computation.
   - Flows and flow-metrics (byte or packet count and input or output interfaces)
   - Flow destination reachability information

- WAN link metrics (such as bandwidth & utilization)

2. Computation of per flow-group policy routes based on the site-wide metrics.
3. Synchronized programming of the per flow-group policy-route decisions (forwarding state) on the WAN edge routers (BRs).

DAPR Data Plane

1. Enforcement of the per flow-group policy-routes bypassing normal routing.
2. Inter-BR traffic forwarding to enforce policy-route decisions where the Ingress and Egress BRs for a traffic flow group are not the same.

DAPR comprises of the following entities and inter-communication:

Route Manager

Route-manager is a control plane entity that performs following functions:

1. Registration of BRs:
    a. Authentication and authorization of BRs
    b. Push policy parameters (e.g. link thresholds) and neighbor-BR information
2. Periodic processing.
    a. Information pull from BRs:
        - Bandwidth and utilization of DAPR egress interfaces.
        - Routes for prefixes reachable through DAPR egress interfaces.
        - Egress flows on DAPR egress interfaces and flow parameters.

    b. Route computation:
        - Best route computation for new application flow groups.
        - Route re-computation for existing out-of-policy flow groups.
        - Route re-computation for existing flow groups that are impacted by events such as WAN link down, route delete and so on.

    c. Route push to BRs for enforcement:
        - Flow-group routes are pushed only to ingress-BRs (BRs receiving the flow-group from LAN).
        - Flow-group routes specify egress BR and interface through which the flows must egress. Flow-groups that must egress through other BRs are forwarded over inter-BR auto-tunnels.
3. Event processing:
    a. Processing of RM and BR events.
    b. Route re-computation for relocation of flow groups.

  c. Push re-computed routes to BRs for enforcement.

Border Router

Border router performs the following:

1. Registration with RM:
   a. Register DAPR egress and ingress interfaces (DAPR-enabled WAN and LAN interfaces).
   b. Create auto-tunnels to neighbor BRs learnt from RM, for inter-BR traffic forwarding.
2. Provide monitoring information to RM (periodically pulled by RM):
   a. Bandwidth and utilization of DAPR egress interfaces.
   b. Prefixes reachable through DAPR egress interfaces.
   c. Application flow groups egressing DAPR egress interfaces.
      - State of auto-tunnels to neighbor BRs.
3. Event notifications to RM:
   a. Reachability events such as DAPR egress down and prefix unreachable.
   b. Threshold violation events.
   c. Inter-BR reachability such as auto-tunnel down.
4. Enforcement of application flow-group routes received from RM.
   a. Enforce routes by bypassing routing and using pre-routing.
   b. For routes with non-local egresses, forward traffic to egress/neighbor BRs over auto-tunnels.

Route Manager and Border Router Communication

DAPR control connections are between the RM and BR loopback IP addresses. DAPR uses two protocols for RM and BR control communication.

- TCP based control protocol is used for registration, information pull and route push by RM and event notifications from BRs.
- UDP based FNF (Flexible Netflow v9) protocol is used by BRs to periodically export the egress flows on DAPR egress interfaces.

Figure 5: DAPR Registration

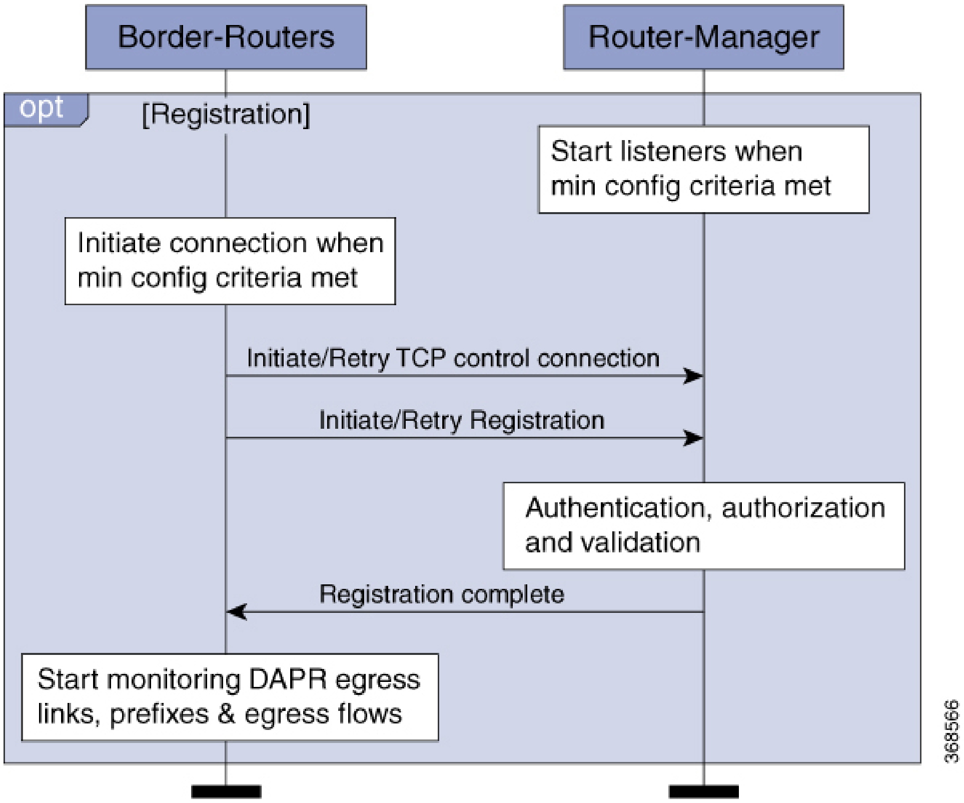

Border-Routers
Router-Manager
opt
[Registration]
Start listeners when min config criteria met
Initiate connection when min config criteria met
Initiate/Retry TCP control connection
Initiate/Retry Registration
Authentication, authorization and validation
Registration complete
Start monitoring DAPR egress links, prefixes & egress flows
368566

Figure 6: DAPR Periodic Processing

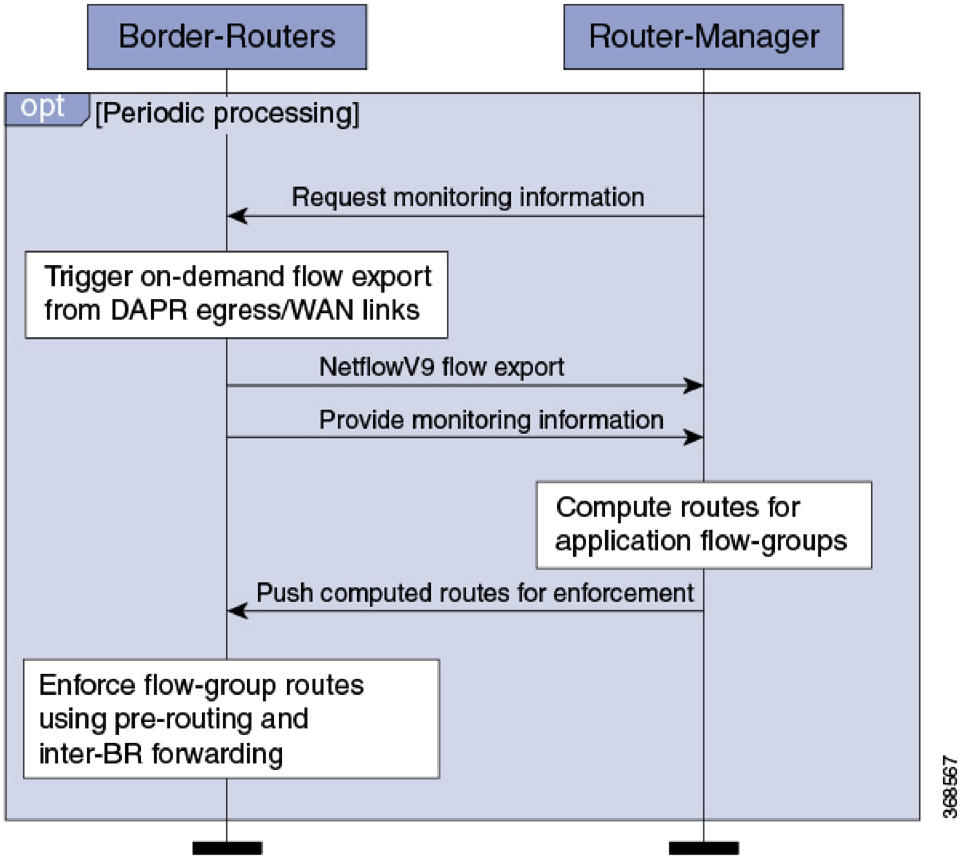
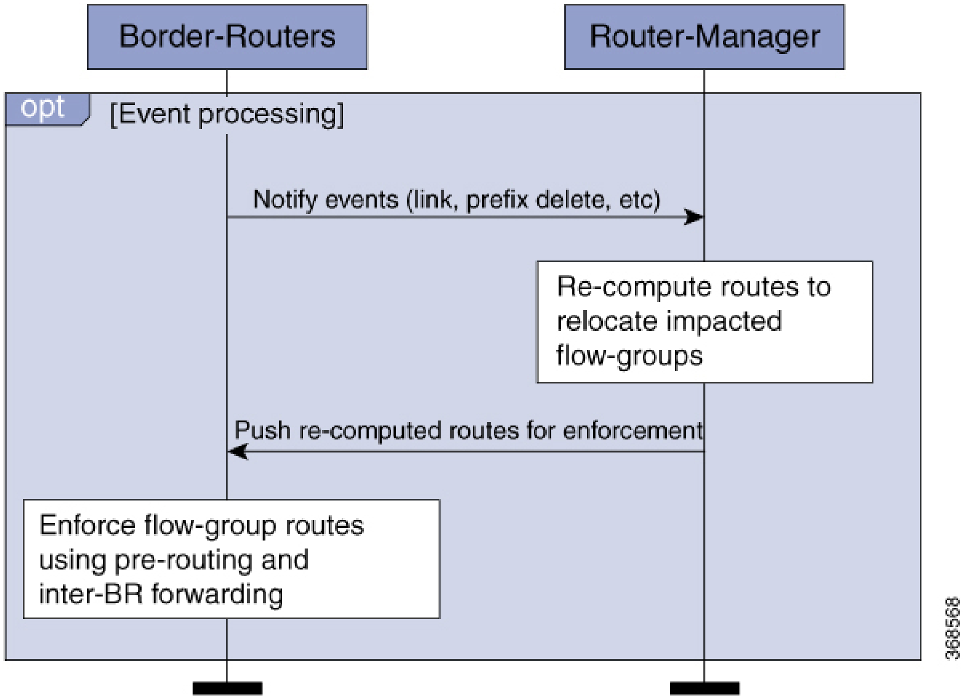

Border-Routers
Router-Manager
opt
[Periodic processing]
Request monitoring information
Trigger on-demand flow export from DAPR egress/WAN links
NetflowV9 flow export
Provide monitoring information
Compute routes for application flow-groups
Push computed routes for enforcement
Enforce flow-group routes using pre-routing and inter-BR forwarding
368567

Figure 7: DAPR Event Processing

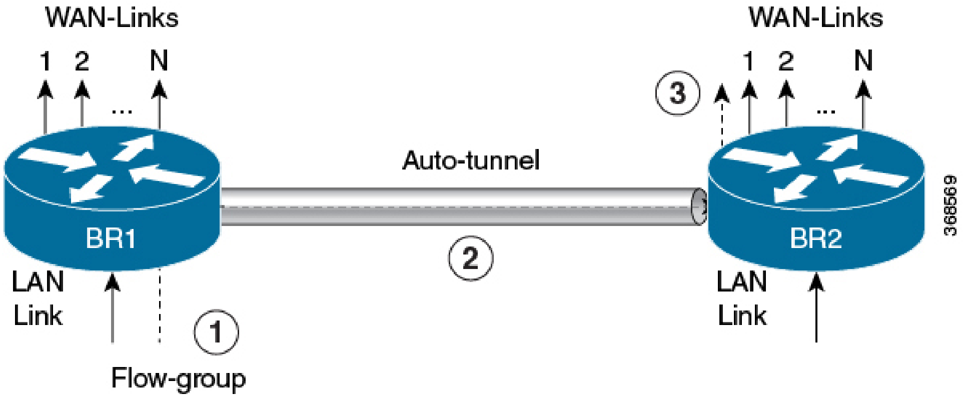

Border-Routers
Router-Manager
opt
[Event processing]
Notify events (link, prefix delete, etc)
Re-compute routes to relocate impacted flow-groups
Push re-computed routes for enforcement
Enforce flow-group routes using pre-routing and inter-BR forwarding
368568

Inter BR Forwarding

BRs create IP/GRE tunnels (referred to as auto-tunnels) to neighbor-BRs learnt from the RM. The inter-BR auto-tunnels are between the BR loopback IP addresses.

With site-wide policy routing, ingress BR for a flow-group and the egress BR can be different and this requires forwarding of traffic between BRs. DAPR uses auto-tunnels for loop-free forwarding of traffic between BRs.

Figure 8: Auto-tunnel based Inter-BR Forwarding



DAPR Operations

DAPR operation is based on three key building blocks:

- Monitoring
- Flow Route Computation
- Flow Route Enforcement

Monitoring

DAPR monitoring involves BRs monitoring and exporting the following information to RM for the flow route computation based on the site-wide visibility:

- Bandwidth and utilization of DAPR egress interfaces (DAPR-enabled WAN links)
- Prefixes learned through the DAPR egress interfaces
- Application flow-groups egressing the DAPR egress interfaces
- Inter-BR availability through the auto-tunnels

Flow Route Computation

Flow Route Computation Logic:

Invokes DAPR RM route-compute logic to compute routes for newly discovered flow-groups. It also re-computes routes for existing flow-groups to re-locate either due to events impacting current routes or current routes being not the best routes. Invokes route-compute on a per flow-group basis and involves following steps:

1. Create a list of viable egress interfaces that meet all the following criteria.
   - Egress interface has the flow destination availability.
   - Egress interface bandwidth is above the specified minimum-bandwidth.
   - Egress interfaces have the headroom for the flow.
   - Egress BR has the bidirectional inter-BR reachability to ingress-BR.
2. Select the best egress interface which is based on the following parameters as tie breakers:
   - Egress that has the higher specified preference for the flow-group.
   - Egress that has higher projected percentage-headroom (projected remaining link utilization).
   - Egress that has the lesser number of flows.
   - Egress link stickiness.

Flow-group Selection Logic for Re-location:

When an egress interface exceeds the specified link thresholds, some of the flow-groups re-locates to other egress interfaces. Flow-groups are selected in the following order for re-location:

- Flow-groups that have no preference for the current egress interface (pref-level = none).
- Flow-groups for which the current egress interface has third preference (pref-level = 3).
- Flow-groups for which the current egress interface has second preference (pref-level = 2).

- Flow-groups for which the current egress interface has first preference (pref-level = 1).
- If there are multiple flow-groups that have the same preference level for the current egress, any of the flow-groups can be selected for the re-location (indeterminate).

Flow States

The following table lists the DAPR flow-group states:

Table 1: DAPR flow-group States

State Transition	Description
Unmanaged (U)	Newly discovered flow-group by RM.
Managed (M)	• For the flow-group with preference policy, flow-group assigned to its most preferred interface • For the flow-group with no preference policy, flow-group assigned to any viable interface
Out-of-policy (O)	• For the flow-group with preference policy, flow-group assigned to its lesser/non-preferred interface. • For the flow-group with no preference policy - NA.
Deleted (D)	Flow-group that was in M/O state and is marked for deletion.

The following lists lifecycle of a flow-group that does not have a preference policy.

State Transition	Description
U ⇨ M	Flow-group assigned to any viable egress
U ⇨ D	• Flow-group discovered from non-DAPR ingress • Flow-group discovered from multiple BRs/egresses • No viable egress available for the flow-group
M ⇨ M	Flow-group relocated due to events
M ⇨ D	• Flow-group expiry - not seen for multiple cycles • Flow-group discovered from invalid egress/ingress • Flow-group could not be relocated as part of event processing

The following lists the lifecycle of a flow-group that has a preference policy.

State Transition	Description
U ⇨ M	Flow-group assigned to its most preferred egress
U ⇨ O	Flow-group assigned to lesser or non-preferred egress
U ⇨ D	• Flow-group discovered from non-DAPR ingress • Flow-group discovered from multiple BRs/egresses • No viable egress available for the flow-group
M ⇨ O	Flow-group re-located to lesser/non-preferred egress as part of event processing.
O ⇨ M	Flow-group relocated to its most preferred egress as part of event or periodic OOP flow processing.
O ⇨ O	Flow-group re-located to lesser/non-preferred egress as part of event or periodic OOP flow processing.
M ⇨ M	Flow re-located to another most-preferred egress as part of processing an event where current egress is no longer viable.
M/O ⇨ D	• Flow-group expiry that is not seen for multiple cycle. • Flow-group discovered from invalid egress or ingress. • Flow-group that are part of event processing cannot be relocated.

Flow Route Enforcement

Flow-group route enforcement involves the following steps:

1. RM pushes the computed route for a flow-group to its ingress-BR. For example, the BR that is currently receiving this flow-group from LAN. The flow-group route consist of (Egress-BR, Egress-interface, Next-hop-IP).
2. Ingress BR enforces the flow-group route as follows:
    - If the egress BR is same as the ingress BR, pre-routing bypasses the routing.
    - If the egress BR is not same as ingress BR, pre-routing forwards traffic to egress BR over the auto-tunnel. The auto-tunnel carries metadata specifying the egress interface to use on the egress-BR.

DAPR Features

DAPR supports the following key features:

1. Link preference
2. Link load balancing
3. Application flow-group whitelisting
4. RM redundancy

Link Preference

This feature ensures application performance by dynamically steering application flows to the specified preferred WAN links.

Link Load Balancing

This feature ensures uniform utilization of the DAPR-enabled WAN links by dynamically steering application flows across WAN links based on changing link bandwidth or utilization and flow rates.

Application Flow-group Whitelisting

This feature allows flow-groups egressing DAPR egress interfaces are not managed by DAPR. Such flows takes the paths as determined by regular routing. Currently, the whitelisted flow-groups are reported by BRs to RM and are ignored by RM.

One of the use cases where this feature is useful is for DAPR to bypass and not manage traffic that is required for its operation such as routing protocol traffic.

RM Redundancy

DAPR supports stateless RM redundancy using anycast-IP with no state synchronization between the RMs. In case the current RM goes down or becomes unreachable, the TCP control connection keepalives detect this and reset the connection, and the new connection goes to the other RM.

Like with any other anycast based redundant setup, routing must be setup to ensure that only one of the RMs is reachable from all the BRs at any time.

DAPR Scalability and Responsiveness

DAPR supports the following scaling numbers:

Table 2: Standalone RM and BR

RM Scale	
Description	**Scaling Numbers: Cisco IOS XE Release 16.11.1**
Maximum number of BRs	20
Maximum number of WAN links per BR	20
Maximum number of WAN links across all BRs	400

RM Scale	
Description	**Scaling Numbers: Cisco IOS XE Release 16.11.1**
Maximum number of destination prefixes	525/2100
Maximum number of application flow-groups	33,600
BR Scale	
Maximum number of destination prefixes	175/700
Maximum number of application flow-groups	11,200

Table 3: Co-located RM and BR Scale

Description	Scaling Numbers: Cisco IOS XE Release 16.11.1
Maximum number of BRs	1
Maximum number of WAN links per BR	8
Maximum number of WAN links across all BRs	8
Maximum number of destination prefixes/routes	35/140
Maximum number of application flow-groups	3600

DAPR Responsiveness

The DAPR responsive time includes:

1. DAPR response-time to critical events = ~5 seconds.
    - WAN link down, route deletion, WAN link hard threshold exceed

2. DAPR response-time to non-critical events = ~30 seconds
    - WAN link soft threshold exceed, out-of-policy flows.

Benefits of DAPR

DAPR offers the following benefits compared to other solutions:

1. DAPR has no overlay dependency: DAPR does not require an overlay and it can manage the overlay or underlay traffic.

2. Synchronized and predictable system: RM performs a synchronized collection of monitoring information from all the BRs. RM performs the flow route computation and route push at designated periodic that intervals based on the latest monitoring information. BRs use an on-demand flow export that is triggered by periodic requests from the RM for the synchronized flow export from all the BRs.

3. Predictable route enforcement: DAPR uses policy routing (PBR) on the BRs to enforce flow routes from the RM. BRs use PBR batching feature to push the updated flow routes that are received from the

RM to the data plane. This avoids chattiness between the control and data plane, and ensures predictable dynamic flow route enforcement.

4. Inter-BR availability tracking: DAPR monitors the state of the auto-tunnels and thus the reachability between BRs. RM maintains the inter-BR reachability matrix and uses it for the route computation.
5. Simplified forwarding state distribution: RM pushes the flow routes only to the ingress-BR. Ingress-BR enforces the flow routes using policy routing (PBR) and inter-BR forwarding over auto-tunnels for the route enforcement.
6. Loop-free inter-BR forwarding: Forwarding of the inter-BR traffic over auto-tunnels ensures that traffic does not loop between BRs.
7. No restriction that BRs must be a L2-adjacent: The inter-BR IP or GRE auto-tunnels remove the restriction that BRs at a site be L2 adjacent.
8. Inter-BR resiliency with multiple LANs: The inter-BR auto-tunnels provide the resiliency when BRs are interconnected over multiple LANs.
9. Supports variable-BW Radio WAN links.
10. Supports virtual-access interfaces as WAN interfaces.
11. Simplified and reduced configuration: DAPR has simplified and reduced configuration by avoiding any BR-specific configuration on the RM.

Prerequisites for DAPR Solution

To configure the DAPR solution:

1. Configure DAPR RM and BRs with a loopback interface with a host IP address.
   - Use the RM or BR loopback IPs for RM-BR control communications, and for the inter-BR auto-tunnels.
2. RM-BR availability (between RM and BR loopback IPs).
   - RM is purely a control plane entity and does not participate in data plane forwarding. Therefore, keep the availability between BRs and RM separate from the BR availability to remote-sites. In other words, do not extend the BR WAN-side routing to RM, which would load the RM unnecessarily.
   - We recommended to use either a separate routing protocol instance between BR and RMs or static routes.
   - RM must not be reachable from the BRs through DAPR egresses.
3. Inter-BR availability (IP or GRE auto-tunnels between BR loopback IPs).
   - Like BR-RM availability, it is preferable to keep the inter-BR availability separate from the BR availability to remote-sites.
   - As the DAPR tracks the inter-BR availability (and the auto-tunnel UP/DOWN status) and uses this in route computations, it is recommended to use dynamic routing protocol instead of static routes for availability between BR loopbacks.

- If the RM-BR availability is using a separate routing protocol instance, use the same instance for inter-BR loopback availability as well.

- Inter-BR availability must NOT be through DAPR egresses.

- Avoid static routes for inter-BR availability, as there are no tunnel keepalives to monitor availability.

4. All possible paths (not just the best path) to remote sites that are reachable through DAPR egress interfaces (DAPR-enabled WAN links) must be available in the routing table either as equal cost or unequal cost routes. This requires tuning of routing protocols metrics.

Restrictions for DAPR

The following restrictions apply to DAPR:

- DAPR supports only IPv4.
- DAPR is supported on RAR and PPPoE interfaces only in RAR bypass mode.
- DAPR identifies application flow groups that are based on a 3-tuple of {source IP-address, destination IP-address, DSCP} where the source and destination IP addresses are host addresses. This means DAPR flow-group currently consists of a single flow with a unique source-IP, destination-IP, and DSCP value.
- DAPR does not support identification of application flow groups using NBAR or 5-tuple (source-prefix, destination-prefix, protocol, source-ports, destination-ports).
- DAPR does not use probes and hence does not support monitoring of delay, jitter, and packet loss on WAN links.

Supported Platforms for DAPR

The following table provides the supported platforms for DAPR.

Table 4: Supported Platforms for DAPR

DAPR Components	Cisco 4000 Series ISRs with Cisco IOS-XE Release 16.11.1 Onwards	Cisco ASR 1000 with Cisco IOS XE Release 16.11.1 Onwards	Cisco CSR 1000v with Cisco IOS XE Release 16.11.1 Onwards	ISRv with Cisco IOS XE Release 16.11.1 Onwards
Route-Manager (RM)	Yes	Yes	Yes	No
Border-Router (BR)	Yes	No	No	No
Co-located BR and RM	Yes	No	No	No

Note DAPR is supported only on Cisco 4451, 4300 ISR, and ASR 1001-X routers.

How to Configure DAPR

To configure DAPR, follow these steps:

1. Configure the loopback interfaces on BRs and RM.
    - Establish the RM-BR reachability between BR and RM loopbacks.
    - Establish the inter-BR reachability between BR loopbacks.
2. Ensure that all paths to remote destinations are in the routing table (RIB).
3. Configure the RM.
4. Configure the BR.

Configuring DAPR instance

DAPR instance is a container for DAPR RM and/or BR configuration. Currently, only a single DAPR instance is supported. DAPR instance is identified by a user-defined string or by the string *default*.

Note There are multiple instances where the interface utilization or bandwidth may be inaccurate. This can cause undesirable Traffic Class movements even for very small changes (or inaccuracies). To avoid the undesirable flow movements, route-manager allows 5% margin in inaccuracies and to flow stickiness even when there are changes upto 5%.

```
Device(config)#?
  Dapr    Dynamic Application Policy Routing (DAPR)
               configuration

DAPR(config)#dapr ?
  WORD     Instance Name
  default    Default DAPR Instance

Device(config)#dapr default
DAPR(config-dapr-instance)#
DAPR(config)#dapr dapr-instance-1
 DAPR instance 'default' exits. Single instance allowed.

Device(config-dapr-instance)#?
DAPR Instance Configurations commands:
  border-router  DAPR border router (BR) configuration
  route-manager  DAPR route manager (RM) configuration
```

Configuring Route Manager

Configure the DAPR RM within the DAPR instance as show in this example:

```
Device(config-dapr-instance)#route-manager
Device(config-dapr-route-manager)#?
Router manager configuration commands:
  authentication    Authentication parameters
  border-routers    Authorized border routers
  class             Application class parameters
  link-thresholds   BR egress link thresholds
  shutdown          Disable route manager instance
  source-interface  Route manager address source
```

Shutdown the RM before creating or modifying any RM configuration.

```
Device(config-dapr-route-manager)#link-thresholds
 RM should be in shutdown mode for any config change

Device(config-dapr-route-manager)#shutdown
 %DAPR_RM-5-RM_STATUS: Shutdown
 %DAPR_RM-5-RM_STATUS: Inactive

Device(config-dapr-route-manager)#link-thresholds
Device(config-dapr-rm-link-thresholds)#

Device(config-dapr-route-manager)#no shutdown
%DAPR_RM-5-RM_STATUS: Active
```

Configure the following mandatory parameters to RM to start listening to BR connections:

- RM source interface (loopback interface) with a valid IP-address
- Authentication password
- List of authorized BRs, with at least one entry

```
Device#show running-config | section dapr
dapr default
 route-manager
 ! Config incomplete
```

Configuring the RM Source Interface

RM uses the source interface IP address for control communication with BRs. RM source interface can only be a loopback interface.

```
Device(config-dapr-route-manager)#?
Router manager configuration commands:
  source-interface  Route manager address source
Device(config-dapr-route-manager)#source-interface ?
  Loopback  Loopback interface
```

Example

```
dapr default
 route-manager
  source-interface Loopback0
interface Loopback0
 description RM-loopback
 ip address 11.0.0.1 255.255.255.255
```

Configuring DAPR Authentication

RM uses passwords to authenticate BRs. Note that DAPR authentication is unidirectional in that it is only for BR authentication to RM and not vice versa. The password is carried in plaintext over the BR-RM TCP-based control connection.

Use IKE/IPsec for more secure and mutual authentication of RM and BRs. For more information, see the IOS IKE/IPsec configuration guide for configuring IKE/IPsec.

DAPR authentication is a mandatory configuration.

```
Device(config-dapr-route-manager)#?
Router manager configuration commands:
  authentication    Authentication parameters

Device(config-dapr-route-manager)#authentication ?
  password  assign password (Max of 25 characters)
Device(config-dapr-route-manager)#authentication password ?
  0     Specifies an UNENCRYPTED password will follow
  4     Specifies an SHA256 HASHED password will follow
  LINE  The UNENCRYPTED (cleartext) 'password' string
```

Note that even if the authentication password is entered in plaintext, encrypted password is displayed in the running-config.

```
Device(config-dapr-route-manager)#authentication password dapr123
Device#show running-config | section dapr
dapr default
 route-manager
  authentication password 4 U28mHpS4suXM7r6q3U3E.oDXKCESijH3TSF6FHKrYHA
```

Example

```
dapr default
 route-manager
  authentication password 4 U28mHpS4suXM7r6q3U3E.oDXKCESijH3TSF6FHKrYHA
```

Configuring DAPR Authorization

DAPR authorization consists of a list of BR IP addresses that are authorized to register with the RM. The list can have a maximum of 20 entries for a standalone RM and a single entry for a co- located RM and BR. You must configure DAPR authorization with at least one entry.

```
Devic(config-dapr-route-manager)#?
Router manager configuration commands:
  border-routers    Authorized border routers

Device(config-dapr-route-manager)#border-routers ?
  <cr>

Device(config-dapr-rm-brs)#?
RM border router configuration commands:
  A.B.C.D  Border router address
```

Example

```
dapr default
 route-manager
  border-routers
   10.0.0.2
```

Configuring DAPR Thresholds

DAPR thresholds specify the thresholds for DAPR egress interfaces on the BRs. RM pushes the thresholds to BRs in the registration response on a successful registration. BRs enforce the thresholds by monitoring the DAPR egress interfaces and reporting any threshold violation to the RM. RM re-computes routes in order to relocate the application flow groups impacted by the threshold violations.

Following are the currently supported thresholds:

- Minimum bandwidth - Specifies the minimum bandwidth (in kbps) in order for DAPR egress interfaces to be considered viable and used in route computations. The default value is 500kbps.
- Maximum percent utilization - Specifies the maximum utilization (in percentage) beyond which DAPR egress interfaces would be considered out-of-policy. The default value is 50%.
- Configuring DAPR thresholds is optional and there are default values for thresholds.

```
Devcie(config-dapr-route-manager)#?
Router manager configuration commands:
  link-thresholds   BR egress link thresholds

Device(config-dapr-route-manager)#?
Router manager configuration commands:
  class             Application class parameters

Device(config-dapr-route-manager)#link-thresholds
Device(config-dapr-rm-link-thresholds)#?
RM link threshold configuration commands:
  max-utilization  Maximum % utilization (default = 50)
  min-bandwidth    Minimum bandwidth (kbps) for viability (default = 500)
```

Example

```
dapr default
 route-manager
  link-thresholds
   max-utilization 50
   min-bandwidth 500
```

Configuring DAPR Preference Policy

DAPR preference policy allows specifying a list of preferred links for a set of flow-groups. DAPR preference policy is an ordered sequence of DAPR application classes. Each class specifies match criteria for flow-groups using an access-list and the first, second and third preferred link-groups. .

Link-group is an arbitrary group of DAPR egress interfaces that is referenced in preference policy. Configure link-group membership on the BR egress interfaces. BRs communicate the membership information to RM in the registration request. A DAPR egress interface can be part of a single link-group.

DAPR application classes are processed in the order of class sequence number and first match is used. Up to 255 classes can be configured. Each class must have a unique combination of class name and sequence number. Configuring DAPR preference policy is optional.

```
Device(config-dapr-route-manager)#?
Router manager configuration commands:
  class             Application class parameters

Device(config-dapr-route-manager)#class ?
  WORD  Application class name
```

Up to 255 application classes can be configured.

```
Device(config-dapr-route-manager)#class class1 ?
  <1-255>  Application class processing sequence

Device(config-dapr-route-manager)#class class1 1 ?
  <cr>  <cr>
```

Each class must have a unique combination of class name and sequence number.

```
Device(config-dapr-route-manager)#class class2 1
 Class 'class1 1' exists.
 Changing class name or sequence number not allowed.

Device(config-dapr-route-manager)#class class1 2
 Class 'class1 1' exists.
 Changing class name or sequence number not allowed.

Device(config-dapr-rm-class)#?
RM application class configuration commands:
  match            Match criteria
  path-preference  Specify path preference
```

Application flow-group matching is based on extended ACL and using only source, destination and dscp.

```
Device(config-dapr-rm-class)#match ?
  access-list  Specify access-list

Device(config-dapr-rm-class)#match access-list ?
  WORD  IP Named Extended Access list name

Device(config-dapr-rm-class)#match access-list access-list1
 Note: DAPR Flow match based on source, destination and dscp only.
       Other ACL fields ignored.
Device(config-dapr-rm-class)#
```

Up to 3 link-groups can be specified as path preference.

```
Device(config-dapr-rm-class)#path-preference
Device(config-dapr-rm-class-path-pref)#?
RM class path preference configuration commands:
  <1-255>  Path preference sequence number

Device(config-dapr-rm-class-path-pref)#1 ?
  WORD  Link group name (max 50 characters)

Device(config-dapr-rm-class-path-pref)#1 link-group1
Device(config-dapr-rm-class-path-pref)#2 link-group2
Device(config-dapr-rm-class-path-pref)#3 link-group3
Device(config-dapr-rm-class-path-pref)#4 link-group4
 Max 3 path preferences allowed in a class.
```

Example

```
dapr default
 route-manager
  class class1 1
   match access-list access-list1
   path-preference
    1 link-group1
    2 link-group2
    3 link-group3

ip access-list extended access-list1
 permit ip any any
```

Configuring DAPR Whitelisting

DAPR whitelisting policy allows specifying a set of flow-groups egressing DAPR egress interfaces that must not be managed by DAPR. Such flow-groups would take regular routing paths.

DAPR whitelist policy can be configured using a DAPR application class of type *bypass*. The bypass application class specifies match criteria for flow-groups using an access-list. Only a single DAPR whitelist policy can be configured. Configuring DAPR whitelist policy is optional.

```
Device(config-dapr-route-manager)#class ?
  WORD  Application class name

Device(config-dapr-route-manager)#class class2 ?
  <1-255>  Application class processing sequence
  type     Application class type

Device(config-dapr-route-manager)#class class2 type ?
  bypass  Application class type bypass

Device(config-dapr-route-manager)#class class2 type bypass

Device(config-dapr-rm-class)#class class3 type bypass
Class 'class2 type bypass' exists. Only one bypass class allowed.
```

```
Device(config-dapr-rm-class)#

Device(config-dapr-rm-class)#?
RM application class configuration commands:
  match  Match criteria

Device(config-dapr-rm-class)#match ?
  access-list  Specify access-list

Device(config-dapr-rm-class)#match access-list ?
  WORD  IP Named Extended Access list name

Device(config-dapr-rm-class)#match access-list access-list2
Note: DAPR Flow match based on source, destination and dscp only. Other ACL fields ignored.
```

```
Example
dapr default
 route-manager
  class class2 type bypass
   match access-list access-list2

ip access-list extended access-list2
 permit ip any any dscp ef
```

Verifying RM

Verify RM configuration and operation using the following show commands.

```
Device#show dapr route-manager ?
  border-router    Border router information
  flow-groups      Flow-group learnt from BRs
  link-groups      Link-group membership information
  route-table      Prefixes/routes learnt from BRs
  summary          RM Summary information

Device#show dapr route-manager border-router ?
  A.B.C.D    BR address
  neighbors  BR neighbor connectivity information
  summary    BR summary information
  |        Output modifiers
  <cr>       <cr>

Device#show dapr route-manager link-groups ?
  WORD  link-group name
  |        Output modifiers
  <cr>  <cr>

Device#show dapr route-manager route-table ?
  A.B.C.D  BR address - routes learnt from this BR
  |        Output modifiers
  <cr>     <cr>

Device#show dapr route-manager flow-groups ?
  detail      flow-groups detail
  egress-br   flow-groups ingressing this BR
  ingress-br  flow-group ingressing this BR
  match       flow-group match criteria
  |           Output modifiers
  <cr>        <cr>

Device#show dapr route-manager flow-groups match ?
  destination  flow-groups matching this destination prefix
  dscp         flow-groups matching this dscp
  source       flow-groups matching this source prefix
  |            Output modifiers
  <cr>         <cr>
```

Configuring Border Router

DAPR BR is configured under DAPR instance.

```
Device(config-dapr-instance)#border-router
Device(config-dapr-border-router)#?
Border router configuration commands:
  authentication    Authentication parameters
  route-manager     Route manager address
  shutdown          Disable border router instance
  source-interface  Border router address source
```

Shutdown BR before creating or modifying any BR configuration.

```
Device(config-dapr-border-router)#source-interface loopback 1
 BR should be in shutdown mode for any config change

Devcie(config-dapr-border-router)#shutdown
%DAPR_BR-5-STATUS: shutdown

Device(config-dapr-border-router)#source-interface loopback 1
Device(config-dapr-border-router)#no shutdown
```

```
Device#show running-config | section dapr
dapr default
 border-router
  ! Config incomplete
```

DAPR BR Mandatory Configuration

Configure the BR with the following mandatory parameters for a BR to start TCP control connection and registration with RM

- BR source interface (loopback interface) with a valid IP-address.

- Authentication password.
- RM IP address (must be reachable through non DAPR-egress interfaces).
- At least one interface configured as DAPR egress.

```
Device#show running-config | section dapr
dapr default
 border-router
  ! Config incomplete
```

Configuring the BR Source Interface

BRs use the source interface IP address for control communication with RM as well as for the inter-BR auto-tunnels(IP/GRE). RM source interface can only be a loopback interface. Configuring BR source interface is mandatory.

```
Device(config-dapr-route-manager)#?
Router manager configuration commands:
  source-interface  Route manager address source

Device(config-dapr-route-manager)#source-interface ?
  Loopback  Loopback interface
```

Example

```
dapr default
 border-router
  source-interface Loopback0

interface Loopback0
 description BR-loopback
 ip address 10.0.0.1 255.255.255.255
```

Configuring DAPR Authentication

BRs use passwords to authenticate to RM. Note that DAPR authentication is unidirectional in that it is only for BR authentication to RM and not vice versa. The password is carried in plain text over the BR-RM TCP-based control connection.

Use IKE/IPsec for more secure and mutual authentication of RM and BRs. For more information, see the IOS IKE/IPsec configuration guide for configuring IKE/IPsec.

DAPR authentication is a mandatory configuration.

```
Device(config-dapr-border-router)#?
Border router configuration commands:
  authentication    Authentication parameters
  route-manager     Route manager address
  shutdown          Disable border router instance
  source-interface  Border router address source

Device(config-dapr-border-router)#authentication ?
  password  Specify the password (Max of 25 characters)

Device(config-dapr-border-router)#authentication password ?
  0     Specifies an UNENCRYPTED password will follow
  4     Specifies an SHA256 HASHED password will follow
  LINE  The UNENCRYPTED (cleartext) 'password' string
```

Note that even if the authentication password is entered in plaintext, encrypted password is displayed in the running-config.

```
Device(config-dapr-border-router)#authentication password dapr123
Device#show running-config | section dapr
dapr default
 border-router
  authentication password 4 U28mHpS4suXM7r6q3U3E.oDXKCESijH3TSF6FHKrYHA
```

Example

```
dapr default
 border-router
  authentication password 4 U28mHpS4suXM7r6q3U3E.oDXKCESijH3TSF6FHKrYHA
```

Configuring DAPR Egress Interfaces and Link-group Membership

Configure at least one interface (WAN facing interface) as a DAPR egress interface. This is required for a BR to start initiating TCP connection and registration to RM. DAPR manages only the flow-groups egressing DAPR egress interfaces.

Optionally configure a DAPR egress interface with link-group membership. A DAPR egress interface can only be part of a single link-group. BR reports DAPR egress interfaces along with any link-group membership information to the RM in registration request.

DAPR egress and link group membership can only be configured on the following interfaces types:

- PPPoE/RAR virtual-template interface
- PPPoE/RAR virtual-access interface
- Serial interface
- Ethernet main and sub-interface

Note An interface can be configured as either DAPR egress or ingress but you cannot configure not both.

Configuring at least one DAPR egress interface is mandatory. Configuring link-group membership is optional.

```
Devcie(config)#interface Loopback 0
Device(config-if)#dapr ?
  egress   dapr egress interface
  ingress  dapr ingress interface
Device(config-if)#dapr egress
% ERROR: Interface not supported as DAPR Egress

Device(config)#interface Serial2/00
Device(config-if)#dapr ?
  egress   dapr egress interface
  ingress  dapr ingress interface

Device(config-if)#dapr egress ?
  link-group  specify link group name (max 50 characters)
  <cr>        <cr>

Device(config-if)#dapr egress link-group ?
  WORD  link group name

Device(config-if)#dapr egress link-group LG1
```

Example

```
interface Serial2/0
 dapr egress link-group LG2
```

Configuring DAPR Ingress Interfaces

At least one interface (LAN facing interface) must be configured as a DAPR ingress interface. Configuring DAPR ingress interface is not mandatory for a BR to start registration. However, only the flow-groups entering a BR through DAPR ingress interfaces (DAPR-enabled LAN interfaces) are managed by DAPR. .

Note An interface can be configured as either DAPR egress or ingress but not both.

DAPR ingress only be configured on Ethernet main and sub-interfaces.

```
Device(config)# interface Loopback 0
Device(config-if)#dapr ingress
% ERROR: Interface not supported as DAPR Ingress

Device(config)# interface Ethernet0/0
Device(config-if)#dapr ingress
```

Example

```
interface Ethernet0/0
 dapr ingress
```

Verifying BR

Verify BR configuration and operation using the following show commands:

```
Device#show dapr border-router ?
  interfaces  BR interface information
  neighbors   BR neighbor information
  summary     BR status information

Device#show dapr border-router neighbors ?
  |     Output modifiers
  <cr>  <cr>

Device#show dapr border-router interfaces ?
  metrics  Egress interface metrics
  |        Output modifiers
  <cr>     <cr>
```

Configuring DAPR Co-located RM and BR

DAPR RM and BRs would be commonly configured on separate routers. For single edge router sites, RM and BR can be configured on the same router under the same DAPR instance, which is referred to as co-located RM/BR.

Following restrictions apply to co-located RM/BR:

- Co-located RM and BR must use different source interfaces (different loopback interfaces).
- Co-located RM supports a single BR.
- Co-located RM does not support external BRs.
- Co-located BR supports a maximum of 8 DAPR egress interfaces and 3360 flow-groups.

DAPR Yang Model

YANG data model is defined for DAPR feature which allows user to add, modify, and delete configuration programmatically using NETCONF.

To make any programmatical changes, use the **shutdown** RPC command first and followed by configuration changes including **no shutdown** command. Operational yang model is currently not supported.

Troubleshooting DAPR

To troubleshoot the DAPR configuration, use the debug commands or the syslog messages.

DAPR RM and BR Syslogs

The following table provide the syslog for RM and BR:

Table 5: RM Syslog

Syslog	Severity Level	Description
BR_REG_FAILED	Error(3)	BR Registration failed
BR_RESET	Error(3)	RM reset the BR
FLOW_EXP_PKTS_MISSED	Error(3)	Flow export packets missed
FLOW_INVALID_EGRESS	Error(3)	Flow discovered from unexpected egress
APP_RT_COMPUTE_FAILED	Error(3)	App route compute failed for flow-group
NO_VIABLE_PATH	Warning(4)	No viable path found for flow-group
APP_REROUTE_FAILED	Warning(4)	App route re-compute failed for flow-group
FLOW_EXP_PKT_INVALID_SEQ	Warning(4)	Unexpected sequence number in flow export packet
FLOW_DATA_RECS_IGNORED	Warning(4)	Flow data records ignored
FLOW_INVALID_INGRESS	Warning(4)	Flow discovered from unexpected ingress
FLOW_MULTI_EGRESS	Warning(4)	New flow discovered from multiple egresses
INTERNAL_ERROR	Warning(4)	Internal error

Syslog	Severity Level	Description
RIB_MISMATCH	Warning(4)	Mismatch of RIB database between BRs and RM
BR_STATUS	Notification(5)	Border-Router status on RM
RM_STATUS	Notification(5)	RM status changed
APP_RT_INSTALL	Informational(6)	App route installed for flow-group
APP_RT_DEL	Informational(6)	App route deleted for flow-group
BR_EVENT	Informational(6)	RM received event from BR
RM_RESET	Informational(6)	RM reset

Table 6: DAPR BR Syslogs

Syslog	Severity Level	Description
PREFIX_LIMIT_EXCEEDED	Warning(4)	DAPR RIB prefixes exceeded
FLOW_LIMIT_EXCEEDED	Warning(4)	DAPR Flows exceeded
RMAP_LIMIT_EXCEEDED	Warning(4)	DAPR route-map entries exceeded max allowed
INTERNAL_ERROR	Warning(4)	Internal error
STATUS	Notification(5)	BR status changed
RESET	Notification(5)	Border-Router reset
RM_ROUTE_INVALID	Notification(5)	Invalid route from BR to RM
NBR_ROUTE_INVALID	Notification(5)	Invalid route to neighbor BR
NBR_TUNNEL_UPDOWN	Notification(5)	Status of tunnel to neighbor BR changed
EGRESS_INTF_THRESHOLD_EXCEED	Notification(5)	DAPR egress interface utilization threshold exceeded
EGRESS_INTF_NOT_VIABLE	Notification(5)	DAPR egress interface not viable
EGRESS_INTF_UPDOWN	Notification(5)	DAPR egress interface status
INGRESS_INTF_UPDOWN	Notification(5)	DAPR ingress interface status

Debug Commands

The following are the DAPR debug commands:

```
Device#debug ?
  dapr                     Enable Dapr debugs

Device#debug dapr ?
  border-router  Enable Border Router debugs
  packet         Enable Packet debugs
  route-manager  Enable Route Manager debugs
  socket         Enable Socket debugs

Device#debug dapr route-manager ?
  all             Enable RM RIB/Flow-Collector/Route-Compute/Events debugging
  events          Enable RM Events debugging
  flow-collector  Enable RM Flow-Collector debugging
  rib             Enable RM RIB debugging
  route-compute   Enable RM Route-Compute debugging

Devie#debug dapr border-router ?
  all          Enable BR RIB/Flow-Export/Flow-Route/Inter-BR/Wan-Metric/Events
               debugging
  events       Enable BR Events debugging
  flow-export  Enable BR Flow-Export debugging
  flow-route   Enable BR Flow-Route debugging
  inter-br     Enable BR Inter-BR Tunnel debugging
  rib          Enable BR RIB debugging
  wan-metric   Enable BR Wan-Metric debugging

Device#debug dapr packet ?
  detail  Enable Packet detail debugging
  dump    Enable Packet dump debugging
  error   Enable Packet error debugging
  <cr>    <cr>

Device#debug dapr socket ?
  detail  Enable Socket detail debugging
  error   Enable Socket error debugging
  <cr>    <cr>
```

DAPR Conditional Debug Commands

Conditional debug commands are supported only on RM.

```
Device#debug dapr route-manager ?
  condition       Enable RM Conditional debugging
```

Conditional debugging can be based on BR IP address and the flow-group parameters.

```
Device#debug dapr route-manager condition ?
  br-ip        Enable RM Condition based on the BR ip address
  flow-groups  Flow-group learnt from BRs
  unmatched    Output debugs even if no context available

Device#debug dapr route-manager condition flow-groups ?
  destination  flow-groups matching this destination prefix
  dscp         flow-groups matching this dscp
  egress-br    flow-groups egressing this BR
  ingress-br   flow-group ingressing this BR
  source       flow-groups matching this source prefix
  <cr>         <cr>
```

DAPR conditional debugging status can be checked using the below command.

```
Device#show dapr route-manager debug-condition
BR addresses under debug are:
```

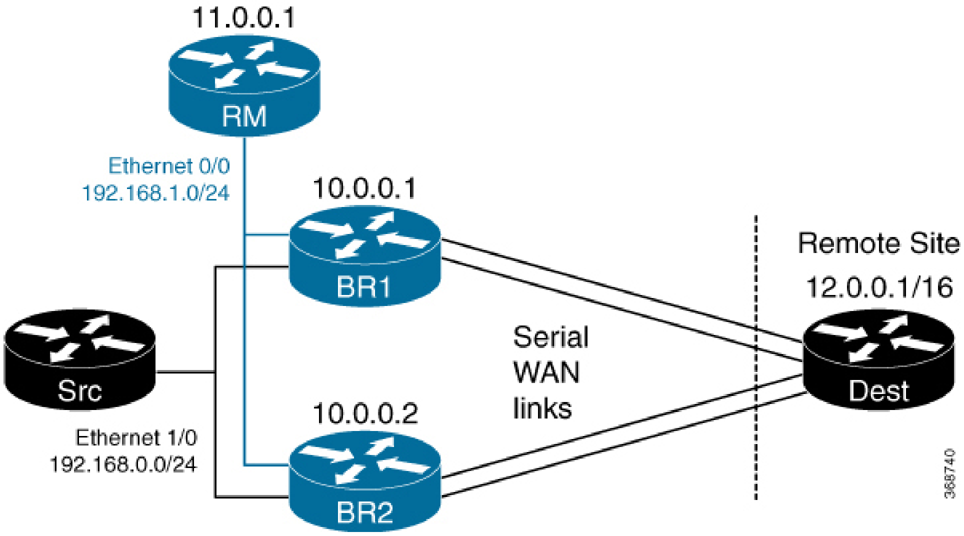
```
10.0.0.1,
Flow-groups under debug are(SRC(mask)/DST(mask)/DSCP/Egress/Ingress):

DAPR RM Conditional debug context unmatched flag: OFF
Device#
```

Configuration Examples

Example for DAPR Standalone RM and BR

This configuration example is based on a sample DAPR topology shown in the figure below. The topology consists of a standalone RM, 3 BRs, traffic source, and destination.

Figure 9: DAPR Topology



Configuring Route-Manager

The following example shows how to configure a RM:

```
dapr default
 route-manager
  source-interface Loopback0
  authentication password 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
  link-thresholds
   max-utilization 50
   min-bandwidth 500
  border-routers
   10.0.0.2
   10.0.0.1
  class whitelist type bypass
   match access-list access-list2
  class class1 1
   match access-list access-list1
   path-preference
    10 LG1
    20 LG2
!
```

```
interface Loopback0
 description RM-loopback
 ip address 11.0.0.1 255.255.255.255
!
interface Ethernet0/0
 description RM-BR LAN
 ip address 192.168.0.1 255.255.255.0
!
ip route 10.0.0.1 255.255.255.255 192.168.0.2
ip route 10.0.0.2 255.255.255.255 192.168.0.3
ip route 192.168.1.0 255.255.255.0 Ethernet0/0
!
ip access-list extended access-list1
 permit ip any any
ip access-list extended access-list2
 permit ip any any dscp ef
!
```

Configuring Border-Router 1

```
dapr default
 border-router
  source-interface Loopback0
  route-manager 11.0.0.1
  authentication password 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
!
interface Loopback0
 description BR-loopback
 ip address 10.0.0.1 255.255.255.255
!
interface Ethernet0/0
 description To-RM
 ip address 192.168.0.2 255.255.255.0
!
interface Ethernet1/0
 description To-Src-Host
 ip address 192.168.1.2 255.255.255.0
 dapr ingress
!
interface Serial2/0
 description WAN link
 ip address 192.168.10.2 255.255.255.0
 ip ospf cost 100
 serial restart-delay 0
 dapr egress link-group LG1
!
!
interface Serial3/0
 description WAN link
 ip address 192.168.11.2 255.255.255.0
 ip ospf cost 100
 dapr egress link-group LG1
!
router ospf 1
 network 10.0.0.1 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
ip route 11.0.0.1 255.255.255.255 Ethernet0/0 192.168.0.1
```

Configuring Border-Router 2

```
dapr default
 border-router
  source-interface Loopback0
  route-manager 11.0.0.1
  authentication password 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
!
interface Loopback0
 description BR-loopback
 ip address 10.0.0.2 255.255.255.255
!
interface Ethernet0/0
 description To-RM
 ip address 192.168.0.3 255.255.255.0
!
interface Ethernet1/0
 description To-Src-Host
 ip address 192.168.1.3 255.255.255.0
 dapr ingress
!
interface Serial2/0
 ip address 192.168.12.2 255.255.255.0
 ip ospf cost 100
 dapr egress link-group LG2
!
interface Serial3/0
 ip address 192.168.13.2 255.255.255.0
 ip ospf cost 100
 dapr egress link-group LG2
!
router ospf 1
 network 10.0.0.2 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.255 area 0
 network 192.168.13.0 0.0.0.255 area 0
!
ip route 11.0.0.1 255.255.255.255 Ethernet0/0 192.168.0.1
```

Show Commands for Route-Manager

```
Device#show dapr route-manager summary
Legend: BR - Border Router, RM - Route Manager
        U - Unmanaged, M - Managed, O - Out of policy, D - Marked for deletion
        R - Re-compute pending

  RM Status                       :  ACTIVE
  RM Address                      :  11.0.0.1
  BRs Registered/Configured       :  2/2
  Prefixes Learnt                 :  5
  Flow-groups Learnt (U/M/O/D/R)  :  4 (0/4/0/0/0)
  Thresholds (Min-BW, Max-Util)   :  500 kbps, 50%
  Flow-group Template             :  Source, Destination, DSCP

Device#show dapr route-manager border-router summary
Legend: S - Status
          D - Disconnected, C - Connected, R - Registered
        Nbr - Neighbor

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

```
Address         S  Egress/  Nbr  Prefixes  Ingress App      Up-time
                   Ingress  BRs  Learnt    Flows   Routes
                   Intfs                   Learnt  Pushed
---------------------------------------------------------------------------
10.0.0.1        R  2/1      1    3         2       2        8m 24s
10.0.0.2        R  2/1      1    3         2       2        8m 23s

Device#show dapr route-manager border-router neighbors
Legend: C - Connected, . - Disconnected
        1 - 10.0.0.2, 2 - 10.0.0.1

Inter BR Connectivity Matrix:
    1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20
1   C  C  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
2   C  C  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
3   .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
4   .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
5   .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
6   .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
7   .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
8   .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
9   .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
10  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
11  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
12  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
13  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
14  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
15  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
16  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
17  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
18  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
19  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
20  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .


Device#show dapr route-manager border-router 10.0.0.1
Legend: BR - Border Router, BW - Bandwidth in kbps, SIdx - SNMP Ifindex

BR: 10.0.0.1
  Status                   :  REGISTERED
  Table Id                 :  0
  Egress/Ingress Intfs     :  2/1
  Neighbor BRs             :  1
  Prefixes Learnt          :  3
  Ingress Flows Learnt     :  2
  App/Flow-group Routes    :  2
  Up-time                  :  00:08:34
  Last FNF Template Rcvd   :  00:00:28
  Last RIB Update Rcvd     :  00:03:54
  FNF Export Seq Num       :  10
  FNF Export Pkts Missed   :  0
  Last Reset Reason        :  Reset RM

Ingress Interfaces:
  Interface-Name  SIdx  State
  Et1/0           5     UP

Egress Interfaces:
  Interface-Name  SIdx  State    BW(Cur/Avg) %Util(Cur/Avg) Link-Group
  Se2/0           9     UP        1544/1544     0/0         LG1
  Se3/0           13    UP        1544/1544     0/0         LG1

Neighbor BRs:
  Addresss        Tunnel      SIdx   State
  10.0.0.2        Tu0         19     UP


Device#show dapr route-manager border-router 10.0.0.2
Legend: BR - Border Router, BW - Bandwidth in kbps, SIdx - SNMP Ifindex

BR: 10.0.0.2
  Status                   :  REGISTERED
  Table Id                 :  0
  Egress/Ingress Intfs     :  2/1
  Neighbor BRs             :  1
  Prefixes Learnt          :  3
  Ingress Flows Learnt     :  2
  App/Flow-group Routes    :  2
  Up-time                  :  00:08:39
  Last FNF Template Rcvd   :  00:00:33
  Last RIB Update Rcvd     :  00:03:59
  FNF Export Seq Num       :  10
  FNF Export Pkts Missed   :  0
  Last Reset Reason        :  Reset RM

Ingress Interfaces:
  Interface-Name  SIdx  State
  Et1/0           5     UP

Egress Interfaces:
  Interface-Name  SIdx  State    BW(Cur/Avg) %Util(Cur/Avg) Link-Group
  Se2/0           9     UP        1544/1544     0/0         LG2
  Se3/0           13    UP        1544/1544     0/0         LG2


Device#show dapr route-manager link-groups
Legend: BR - Border Router

----------------------------------------------
Link-group
   Members (BR, Egress Interface)
----------------------------------------------
LG1
    10.0.0.1, Se2/0
    10.0.0.1, Se3/0
LG2
    10.0.0.2, Se2/0
    10.0.0.2, Se3/0


Device#show dapr route-manager route-table
Legend: BR - Border Router

---------------------------------------
Prefix
 BR  Next-Hop
---------------------------------------
12.0.0.0/16
  10.0.0.1 192.168.11.1, Se3/0
  10.0.0.2 192.168.12.1, Se2/0
  10.0.0.2 192.168.13.1, Se3/0
  10.0.0.1 192.168.10.1, Se2/0
192.168.10.0/24
  10.0.0.2 192.168.13.1, Se3/0
  10.0.0.2 192.168.12.1, Se2/0
192.168.11.0/24
  10.0.0.2 192.168.13.1, Se3/0
  10.0.0.2 192.168.12.1, Se2/0
```

```
192.168.12.0/24
  10.0.0.1 192.168.11.1, Se3/0
  10.0.0.1 192.168.10.1, Se2/0
192.168.13.0/24
  10.0.0.1 192.168.11.1, Se3/0
  10.0.0.1 192.168.10.1, Se2/0


Device#show dapr route-manager flow-groups
Legend: BR - Border Router, Rate - Flow rate(current) bps
        S - Status
          U - Unmanaged, M - Managed, O - Out of policy, D - Marked for deletion

Source           Destination     DSCP Rate    Up-time  S Egress-BR        Next-hop
13.0.0.1         12.0.0.1        def  0K      00:00:38 M 10.0.0.1         192.168.10.1,
Se2/0
13.0.0.1         12.0.0.2        def  0K      00:00:38 M 10.0.0.1         192.168.11.1,
Se3/0
13.0.0.1         12.0.0.3        def  0K      00:00:38 M 10.0.0.1         192.168.11.1,
Se3/0
13.0.0.1         12.0.0.4        def  0K      00:00:38 M 10.0.0.1         192.168.10.1,
Se2/0


Device#show dapr route-manager flow-groups detail
Legend: BR - Border Router, Rate - Flow rate(curr/avg) bps
        S - Flow State
          U - Unmanaged, M - Managed, O - Out of policy, D - Pending deletion
        Reason codes
         N - New flow-group, X - Expired, E - Invalid Egress
         I - Invalid Ingress, U - Path unreachable, NV - No viable path
         LO - Link out of policy, FO - Flow-group out of policy
         A - Admin deleted, IB - Ingress BR disconnected

--------------------------------------------------------------------------------
Flow-group(Source Destination DSCP):
 Attr:   IngressBR       Rate                           Up-time
 Curr: S EgressBR        Rate    Next-hop               Duration  Reason
 Prev: S EgressBR                Next-hop
--------------------------------------------------------------------------------
13.0.0.1, 12.0.0.1, def:
         10.0.0.1        0K/0K                          00:00:42
       M 10.0.0.1        0K      192.168.10.1, Se2/0    00:00:38  N
       U 10.0.0.1                -
13.0.0.1, 12.0.0.2, def:
         10.0.0.2        0K/0K                          00:00:42
       M 10.0.0.1        0K      192.168.11.1, Se3/0    00:00:38  N
       U 10.0.0.2                -
13.0.0.1, 12.0.0.3, def:
         10.0.0.1        0K/0K                          00:00:42
       M 10.0.0.1        0K      192.168.11.1, Se3/0    00:00:38  N
       U 10.0.0.1                -
13.0.0.1, 12.0.0.4, def:
         10.0.0.2        0K/0K                          00:00:42
       M 10.0.0.1        0K      192.168.10.1, Se2/0    00:00:38  N
       U 10.0.0.2
```

Show Commands for Border-Router

```
Device#show dapr border-router summary
Legend: BR - Border Router, RM - Route Manager
```

```
  BR Status                        : REGISTERED
  Local Address                    : 10.0.0.1
  RM Address                       : 11.0.0.1
  Egress Interfaces                : 2
  Ingress Interfaces               : 1
  Neighbor BRs                     : 1
  Last Successful Registration     : 00:15:10
  Last Stats Pull Request Rcvd     : 00:00:05
  Last RIB Pull Request Rcvd       : 00:00:35
  Last Flow Route Policy Rcvd      : 00:05:30
  Last Reset Reason                : Conn-Down
  Route-map Flows                  : 0
  Route-map Entries (Local/InterBR): 0 (0/0)
  Flow Record                      : dapr-flow-record
  Flow Exporter                    : dapr-flow-exporter
  Flow Monitor                     : dapr-flow-monitor
  Route Map                        : dapr-routemap


Device#show dapr border-router neighbors
Legend: SIdx - SNMP Ifindex

  Neighbor-BR      Tunnel       SIdx  Status
  10.0.0.2         Tunnel0      19    UP


Device#show dapr border-router interfaces
Legend: SIdx - SNMP Ifindex

Ingress Interfaces:
  Interface-Name   SIdx
  Et1/0            5

Egress Interfaces:
  Interface-Name   SIdx  Link-Group
  Se2/0            9     LG1
  Se3/0            13    LG1

Device#show dapr border-router interfaces metrics
Serial2/0
   Bandwidth kbps (Cur/Avg/Min/Max)  : 1544/1544/1544/1544
   % Utilization (Cur/Avg)           : 0/0
   Count (Pkt/Byte)                  : 0/0
Serial3/0
   Bandwidth kbps (Cur/Avg/Min/Max)  : 1544/1544/1544/1544
   % Utilization (Cur/Avg)           : 0/0
   Count (Pkt/Byte)                  : 0/0
Device#
```

Example for Configuring DAPR Co-located RM and BR

The following example show how to configure co-located RM and BR.

```
dapr default
 route-manager
  source-interface Loopback1
  authentication password 4 U28mHpS4suXM7r6q3U3E.oDXKCESijH3TSF6FHKrYHA
  link-thresholds
   max-utilization 50
   min-bandwidth 500
  border-routers
```

```
    10.0.0.2
  border-router
   source-interface Loopback0
   route-manager 10.0.0.100
   authentication password 4 U28mHpS4suXM7r6q3U3E.oDXKCESijH3TSF6FHKrYHA

interface Loopback0
 description BR-loopback
 ip address 10.0.0.2 255.255.255.255
end

interface Loopback1
 description RM-loopback
 ip address 10.0.0.100 255.255.255.255
end

Device#show dapr border-router summary
Legend: BR - Border Router, RM - Route Manager
  BR Status                         : REGISTERED
  Local Address                     : 10.0.0.2
  RM Address                        : 10.0.0.100
  RM Co-located                     : TRUE
```

Example for Configuring DAPR on RAR and PPPoE interfaces

DAPR is supported on RAR interfaces only in RAR bypass mode. Following is an example of RAR bypass mode configuration. For more information on RAR configuration, see the RAR Configuration Guide.

```
subscriber authorization enable
!
policy-map type service RAR-SERVICE1
 pppoe service manet_radio //pppoe service name must be manet_radio
```

Configure BBA Goup and Apply on the WAN Interface:

```
bba-groupGpppoe BBA-GROUP1
 virtual-template 1
 service profile RAR-SERVICE1
!
interface GigabitEthernet0/0/1
 ip address 22.23.23.1 255.255.0.0
 negotiation auto
 pppoe enable group BBA-GROUP1
```

Configure a Unique Loopback Interface for each Virtual-template:

```
interface Loopback1
 ip address 22.81.4.1 255.255.255.255
 ip ospf 100 area 0
 ip ospf cost 1000
```

Enable DAPR on the Virtual-template:

```
interface Virtual-Template1
 ip unnumbered Loopback1
 ip ospf 100 area 0
 ip ospf cost 1000
 no peer default ip address
 dapr egress link-group LG_1
```

Configure a VMI interface in Bypass Mode:

```
interface vmi1
 ip address 22.4.71.1 255.255.255.0
 physical-interface GigabitEthernet0/0/1
 mode bypass
```

Configure OSPF and Enable it on the Virtual-template:

```
router ospf 100
router-id 22.1.1.6
maximum-paths 20
```

Simulating RAR Radio Modem

RAR Radio modem can be simulated using a directly connected peer router. The following is an example of configuration required on the peer router to simulate an RAR Radio modem and the test commands to initiate a PPPoE session and change Radio bandwidth.

Note that the simulator only has RAR/PPPoE configuration and does not have any DAPR configuration.

```
subscriber authorization enable
!
policy-map type service RAR-SERVICE1
pppoe service manet_radio //pppoe service name must be manet_radio
```

Configure BBA Group and Apply on the WAN Interface:

```
bba-group pppoe BBA-GROUP1 virtual-template 1
service profile RAR-SERVICE1
!
interface GigabitEthernet0/0/3
ip address 22.39.39.1 255.255.0.0 negotiation auto
pppoe enable group BBA-GROUP1
```

Configure a Unique Loopback Interface for each Virtual-template:

```
interface Loopback1
ip address 22.81.7.3 255.255.255.255
ip ospf 100 area 0 ip ospf cost 1000
interface Virtual-Template1 ip unnumbered Loopback1
ip ospf 100 area 0 ip ospf cost 1000
no peer default ip address
```

Configure a VMI Interface in Bypass Mode:

```
interface vmi1
ip address 22.7.6.1 255.255.255.0
physical-interface GigabitEthernet0/0/3 mode bypass
```

Configure OSPF and Enabling it on the Virtual-template:

```
router ospf 100
router-id 22.1.1.7
```

Test Command on Simulator to Initiate a RAR/PPPoE Session

```
Simulator#test pppoe 1 1 g0/0/3
TEST: MAX: 1, CPS: 1
BRSR3#show pppoe session
     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st      Type
    N/A      2  00fc.ba05.c273  Gi0/0/3                  1  Vi2.1      PTA
                00fc.ba3a.d3b1                              UP
```

Test Command on Simulator to Change RAR Link Bandwidth

```
Simulator#test pppoe session 2 padq mdr-scalar 1 max-data-rate 55 cdr-scalar 1 cur-data-rate
 55
```

Verifying the PPPoE Session

```
Device# show pppoe session
     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st      Type
     46     37  00fc.ba05.c273  Gi0/0/1                  1  Vi1.1      PTA
                00fc.ba3a.d3b1                              UP


Device#show derived-config interface Vi1.1
Building configuration...

Derived configuration : 156 bytes
!
interface Virtual-Access1.1
ip unnumbered Loopback1
 ip ospf 100 area 0
 ip ospf cost 1000
 no peer default ip address
 dapr egress link-group LG_1
end

Device1#show int vi1.1
Virtual-Access1.1 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback3 (22.81.7.3)
  MTU 1492 bytes, BW 100000 Kbit/sec, DLY 100000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP
  PPPoE vaccess, cloned from Virtual-Template3
  Vaccess status 0x0
  Keepalive set (10 sec)
     89 packets input, 4706 bytes
     89 packets output, 4806 bytes
  Last clearing of "show interface" counters never
```

Debug Logs

Debug Logs for RM

The following are the debug logs for RM:

```
Device#debug dapr route-manager all
Device# debug dapr route-manager route-compute detail
debug dapr route-manager flow-collector detail

Device#show debugging
DAPR RM:
  DAPR RM Route-Compute debugging is on
  DAPR RM Route-Compute error debugging is on
  DAPR RM Route-Compute detail debugging is on
  DAPR RM Flow-Collector debugging is on
  DAPR RM Flow-Collector error debugging is on
  DAPR RM Flow-Collector detail debugging is on
  DAPR RM Events debugging is on
  DAPR RM Events error debugging is on
Device#

Device#configure terminal
DAPR-RM(config-dapr-instance)#route-manager
DAPR-RM(config-dapr-route-manager)#no shut
*Mar  6 11:09:14.174: %DAPR_RM-5-RM_STATUS: Active
Device#
```

Registration:

```
*Mar  6 11:09:36.445: DAPR-RM-EV: New BR connection, addr:10.0.0.1 port:45608
*Mar  6 11:09:36.445: %DAPR_RM-5-BR_STATUS: BR 10.0.0.1 CONNECTED
*Mar  6 11:09:36.445: DAPR-RM-EV: Received message from 10.0.0.1(fd:1)
*Mar  6 11:09:36.445: DAPR-RM-EV: Send message Registration Response to BR 10.0.0.1
*Mar  6 11:09:36.445: DAPR-RM-EV: Sent complete message to 10.0.0.1(fd:1)
Device#
*Mar  6 11:09:36.445: %DAPR_RM-5-BR_STATUS: BR 10.0.0.1 REGISTERED
DAPR-RM#
*Mar  6 11:09:37.446: DAPR-RM-EV: Received message from 10.0.0.1(fd:1)
*Mar  6 11:09:39.174: %DAPR_RM-6-BR_EVENT: BR Inter BR state event: 10.0.0.1
Device#
```

Periodic Information Pull:

```
*Mar  6 11:09:44.175: DAPR-RM-EV: Send message Pull Request to BR 10.0.0.1
*Mar  6 11:09:44.175: DAPR-RM-EV: Sent complete message to 10.0.0.1(fd:1)
*Mar  6 11:09:44.175: DAPR-RM-EV: Received message from 10.0.0.1(fd:1)

*Mar  6 11:10:14.174: DAPR-RM-EV: Send message Pull Request to BR 10.0.0.1
*Mar  6 11:10:14.174: DAPR-RM-EV: Sent complete message to 10.0.0.1(fd:1)
*Mar  6 11:10:14.174: DAPR-RM-EV: Received message from 10.0.0.1(fd:1)
```

Route-compute for Discovered Flow-group:

```
*Mar  6 11:10:49.175:   Viable paths:
*Mar  6 11:10:49.175:           Path:{10.0.0.1, [0]192.168.10.1, 9}, Pref:1, BW:1544,
Hr:1544, Util:0, TCC: 0
*Mar  6 11:10:49.175:           Path:{10.0.0.1, [0]192.168.11.1, 13}, Pref:1, BW:1544,
Hr:1544, Util:0, TCC: 0
*Mar  6 11:10:49.175: %DAPR_RM-6-APP_RT_INSTALL: TC[P]:{192.168.1.1/32, 12.0.0.1/32, default}
 on 10.0.0.1[0] (BW:0) Path:{10.0.0.1, [0]192.168.10.1, 9}
*Mar  6 11:10:49.175: DAPR-RM-EV: Send message FG Route Push to BR 10.0.0.1
*Mar  6 11:10:49.175: DAPR-RM-EV: Sent complete message to 10.0.0.1(fd:1)
```

Route-delete on Flow Expiry:

```
*Mar  6 11:12:16.922: DAPR-RM-FC-DETAIL: delete flow - reason 2
*Mar  6 11:12:19.176: %DAPR_RM-6-APP_RT_DEL: FG[D]:{192.168.1.1, 12.0.0.1, default} on
10.0.0.1 (BW:0)
*Mar  6 11:12:19.176: DAPR-RM-EV: Send message FG Route Push to BR 10.0.0.1
*Mar  6 11:12:19.176: DAPR-RM-EV: Sent complete message to 10.0.0.1(fd:1)
```

Debug Logs for BR

The following are the debug logs for BR:

```
Device#show debugging
Device:
DAPR BR All debugging is on DAPR BR Events debugging is on
DAPR BR Events Error debugging is on DAPR BR Flow-Route debugging is on
DAPR BR Flow-Route Error debugging is on DAPR BR RIB debugging is on
DAPR BR RIB Error debugging is on DAPR BR Flow-Export debugging is on
DAPR BR Flow-Export Error debugging is on DAPR BR Inter-BR Tunnel debugging is on
DAPR BR Inter-BR Tunnel Error debugging is on DAPR BR WAN-Metric debugging is on
DAPR BR WAN-Metric Error debugging is on
```

BR Shutdown:

```
Device#conf t
Device (config)#dapr default
Device(config-dapr-instance)#border-router Device(config-dapr-border-router)#shudown

*Mar 6 11:08:03.003: %DAPR_BR-5-STATUS: shutdown
*Mar 6 11:08:03: DAPR-BR-EV: Handle config shutdown notification
*Mar 6 11:08:03: DAPR-BR-EV: Enqueue Connection Close Request
*Mar 6 11:08:03: DAPR-BR-EV: Handle BR-RM event for disconnect
*Mar 6 11:08:03: DAPR-BR-EV: Received BR-RM Connection Close, reason: Config shutdown
*Mar 6 11:08:03: DAPR-BR-EV: Cleanup BR info
*Mar 6 11:08:03: DAPR-BR-EV: BR-RM Connection Closed by BR DAPR-BR1#
```

TCP Control Connection to RM:

```
Device#configure terminal
Device(config)#dapr default
Device(config-dapr-instance)#border-router
Device(config-dapr-border-router)#no shudown

*Mar 6 11:09:36: DAPR-BR-EV: Handle config criteria met notification
*Mar 6 11:09:36: DAPR-BR-EV: Enqueue Connection Request
*Mar 6 11:09:36: DAPR-BR-FR: Handle config criteria met Notification
*Mar 6 11:09:36: DAPR-BR-EV: Handle BR-RM event for connect
*Mar 6 11:09:36: DAPR-BR-EV: Received BR-RM Connection Request
*Mar 6 11:09:36: DAPR-BR-RIB: Check RM route validity
*Mar 6 11:09:36: DAPR-BR-RIB: lookup returned out_idb:Ethernet0/0 for tableid:0
rm_addr:11.0.0.1
*Mar 6 11:09:36: DAPR-BR-RIB: rm route is via Ethernet0/0
*Mar 6 11:09:36: DAPR-BR-RIB: Route to RM is VALID
*Mar 6 11:09:36: DAPR-BR-EV: Connect to RM, local: 10.0.0.1(0), remote: 11.0.0.1(17749),
idb:Loopback0
*Mar 6 11:09:36: DAPR-BR-EV: Set tableid 0
*Mar 6 11:09:36: DAPR-BR-EV: socket 0 connect status: -1 errno: 11
*Mar 6 11:09:36: DAPR-BR-EV: Connect to RM PENDING on fd 0
*Mar 6 11:09:36: DAPR-BR-EV: BR-RM Connection IN PROGRESS
*Mar 6 11:09:36: DAPR-BR-EV: Handle BR-RM Connection Pending Request
*Mar 6 11:09:36: DAPR-BR-EV: BR-RM(11.0.0.1) channel progress->connected, make connection
UP
*Mar 6 11:09:36: DAPR-BR-EV: BR-RM Connection SUCCESSFUL
*Mar 6 11:09:36.445: %DAPR_BR-5-STATUS: CONNECTED
*Mar 6 11:09:36: DAPR-BR-FR: Handle connection UP
```

Registration:

```
*Mar 6 11:09:36: DAPR-BR-EV: Send message Registration Request to RM 11.0.0.1(fd:0)
*Mar 6 11:09:36: DAPR-BR-EV: Sent complete message to 11.0.0.1(fd:0)
*Mar 6 11:09:36: DAPR-BR-EV: Registration request sent to RM
*Mar 6 11:09:36: DAPR-BR-EV: Received message from 11.0.0.1(fd:0)
*Mar 6 11:09:36: DAPR-BR-EV: Received msg Registration Response from RM
*Mar 6 11:09:36.445: %DAPR_BR-5-STATUS: REGISTERED
```

Inter-BR Tunnel Creation:

```
*Mar 6 11:09:36: DAPR-BR-RIB: Check Inter-BR route validity for 10.0.0.2
*Mar 6 11:09:36: DAPR-BR-RIB: lookup returned out_idb:Ethernet1/0 for tableid:0
br_addr:10.0.0.2
*Mar 6 11:09:36: DAPR-BR-RIB: inter-br route is via Ethernet1/0
*Mar 6 11:09:36: DAPR-BR-INTER-BR: Tunnel ceate to 10.0.0.2: Succefully created inter BR
tunnel Tunnel0
Enabling egress Netflowv9 on DAPR egress interfaces:
Mar 6 11:09:36: DAPR-BR-FLOW-EXP: Created Flow record dapr-flow-record
*Mar 6 11:09:36: DAPR-BR-FLOW-EXP-ERR: Flow exporter create: Exporter mtu 16384
*Mar 6 11:09:36: DAPR-BR-FLOW-EXP: Created DAPR owned fnf exporter dapr-flow-exporter
(11.0.0.1:9995)
*Mar 6 11:09:36: DAPR-BR-FLOW-EXP: Flow monitor create sucess: Monitor name dapr-flow-monitor
*Mar 6 11:09:36: DAPR-BR-FLOW-EXP: Attached monitor dapr-flow-monitor on interface Serial2/0:
*Mar 6 11:09:36: DAPR-BR-FLOW-EXP: Attached monitor dapr-flow-monitor on interface Serial3/0:
```

Start Monitoring DAPR Egress Interfaces:

```
Mar 6 11:09:44: DAPR-BR-EV: Received message from 11.0.0.1(fd:0)
*Mar 6 11:09:44: DAPR-BR-EV: Received msg Pull Request from RM
*Mar 6 11:09:44: DAPR-BR-RIB: RIB walk and populate
*Mar 6 11:09:44: DAPR-BR-RIB: Total prefixes:3 max:1000
*Mar 6 11:09:44: DAPR-BR-RIB: RIB walk and populate SUCCESS, prefixes 3 routes 6
*Mar 6 11:09:44: DAPR-BR-EV: Send message Pull Response to RM 11.0.0.1(fd:0)
*Mar 6 11:09:44: DAPR-BR-EV: Sent complete message to 11.0.0.1(fd:0)
```

Periodic Information Pull Request from RM:

```
Mar 6 11:09:44: DAPR-BR-EV: Received message from 11.0.0.1(fd:0)
*Mar 6 11:09:44: DAPR-BR-EV: Received msg Pull Request from RM
*Mar 6 11:09:44: DAPR-BR-RIB: RIB walk and populate
*Mar 6 11:09:44: DAPR-BR-RIB: Total prefixes:3 max:1000
*Mar 6 11:09:44: DAPR-BR-RIB: RIB walk and populate SUCCESS, prefixes 3 routes 6
*Mar 6 11:09:44: DAPR-BR-EV: Send message Pull Response to RM 11.0.0.1(fd:0)
*Mar 6 11:09:44: DAPR-BR-EV: Sent complete message to 11.0.0.1(fd:0)
```

Periodic Sampling of DAPR Egress Bandwith and Utilization:

```
*Mar 6 11:09:46: DAPR-BR-WAN-METRIC: Current Sample: (max samples = 3, curr_idx = 0,
next_idx = 1)
*Mar 6 11:09:46: DAPR-BR-WAN-METRIC: Current sample utilization 0 (index 0)
*Mar 6 11:09:46: DAPR-BR-WAN-METRIC: Utilization Samples Collected:
*Mar 6 11:09:46: DAPR-BR-WAN-METRIC: Average Utilization of collected samples: 0
*Mar 6 11:09:46: DAPR-BR-WAN-METRIC: Current Sample: (max samples = 3, curr_idx = 0,
next_idx = 1)
*Mar 6 11:09:46: DAPR-BR-WAN-METRIC: Current sample utilization 0 (index 0)
*Mar 6 11:09:46: DAPR-BR-WAN-METRIC: Utilization Samples Collected:
*Mar 6 11:09:46: DAPR-BR-WAN-METRIC: Average Utilization of collected samples: 0
```

Periodic Information Pull Request from RM:

```

Periodic information pull request from RM:
*Mar 6 11:10:14: DAPR-BR-EV: Received message from 11.0.0.1(fd:0)
*Mar 6 11:10:14: DAPR-BR-EV: Received msg Pull Request from RM
*Mar 6 11:10:14: DAPR-BR-EV: Send message Pull Response to RM 11.0.0.1(fd:0)
*Mar 6 11:10:14: DAPR-BR-EV: Sent complete message to 11.0.0.1(fd:0)
```

Route Push Message from RM to BR:

```
Mar 6 11:14:19: DAPR-BR-EV: Received message from 11.0.0.1(fd:0)
*Mar 6 11:14:19: DAPR-BR-EV: Received msg FG Route Push from RM
*Mar 6 11:14:19: DAPR-BR-FR: ***BEGIN***
*Mar 6 11:14:19: DAPR-BR-FR: Remove route map entries, total: 1
*Mar 6 11:14:19: DAPR-BR-FR: No new entries received
*Mar 6 11:14:19: DAPR-BR-FR: calling rmap batch commit
```

```
*Mar 6 11:14:19: DAPR-BR-FR: ***END:SUCCESS***
Device#
```