Direct Cloud Access

The Direct Cloud Access IWAN 2.3 feature enables users at branch sites to have best application experience to SaaS applications, such as, Office 365, Google services, with reduced cost. This feature helps in constantly monitoring network and application performance and select the optimized paths (usually local break out from branch to Cloud SaaS applications instead of back-haul to the data center). Non-SaaS traffic still back-haul to data center for further inspection.

Feature Information for Configuring Direct Cloud Access

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Direct Cloud Access IWAN 2.3

Feature Name	Releases	Feature Information
Direct Cloud Access IWAN 2.3	Cisco IOS XE Fuji 16.8.1	The Direct Cloud Access (DCA) feature allows traffic from trusted applications, part of well-trusted domains, to pass the local Internet security check because traffic from these trusted applications have a lower security risk than untrusted Internet sites. The following commands were introduced or modified: **domain path**, **path-preference**, **show domain dca-status**, **show domain default border**, **show domain default policy**, **show domain vrf border channels**, **show domain vrf master channels**.

Prerequisites for Configuring Direct Cloud Access

- NAT:

  To enable a host that typically operates in a private network directly communicate with a SaaS application in a public network, use a NAT. Enable NAT on the same router that has DCA enabled or other devices in the path.

- Firewall security:

  To improve security, you can enable a firewall, such as a zone-based firewall (ZBFW), in the path.

Note By default OpenDNS is used as DNS resolver for SaaS traffic, but you can choose to use other DNS resolver such as Google DNS resolver 8.8.8.8. OpenDNS license/registration is not a must if you don't need OpenDNS security services.

Restrictions for Configuring Direct Cloud Access

- IPv6 address is not supported.
- DCA is not supported if the DNS traffic does not pass through the router which is enabled with DCA.
- DCA does not work if SaaS applications use proxy. All traffic going to proxy server as DCA may not classify these applications and cannot perform local breakout for traffic that is bound to proxy.
- Applications that directly access the content and not through DNS resolution, NBAR may fail to classify as SaaS and cannot provide local break-out.
- DCA may not work on a device when NBAR classification results are not available on the device. You must customize NBAR to classify the results to support DCA.
- This feature depends on applications classification. SD-AVC helps in better classification with NBAR.
- To access SaaS applications, a public IP address is required. NAT helps translate the user’s private IP address to a public IP address. Configure NAT on the border router that has DCA enabled, or on other internet-facing devices.

Information About Configuring Direct Cloud Access

Direct Cloud Access Overview

The infrastructure of cloud-hosted services, such as Microsoft Office 365 and Google Apps, is in the cloud. Back-hauling traffic from remote users and sites through the private WAN to the data center via Internet imposes additional bandwidth requirements on the private WAN and may add latency to each connection. Moreover, private WAN connectivity is more expensive than direct Internet connections, which could add a tremendous amount of cost to the equation.

The Direct Cloud Access IWAN 2.3 feature implements direct cloud access (DCA) on Cisco IWAN networks and allows trusted SaaS traffic to be forwarded out over the optimized path (directly local break out) while other traffic still back-haul to headquarters over VPN. DCA monitors the candidate path (DCA path, back-haul path to headquarter) performance and chooses the optimized path in policy to get the best SaaS application performance. While adding direct Internet connectivity to the branch site without back hauling to data center, IWAN DCA provides the security capability at branch site by enabling security features like NAT and Firewall (Zone-based Firewall, Snort IPS, etc.) at branch sites.

Features

DCA features include:

- Automatic configuration of Cisco Umbrella Connector (supported from Cisco IOS XE Gibraltar 16.10.1)
- Support for policy configured on a centralized hub, or per-site customized local policy
  - Customized local policy overrides global plicy.
  - If a hub connection goes down, local policy remains in effect.
- Support for P2P interface, such as dialer interface, as DCA interface

Benefits of Direct Cloud Acces

- Reduced operation cost as SaaS traffic no longer needs to go to headquarters which consume additional headquarter network bandwidth.
- Business processes run faster through direct network access to the major cloud providers. A traffic classification mechanism is required in order to achieve direct Internet access for selected cloud applications.

Direct Cloud Access Architecture

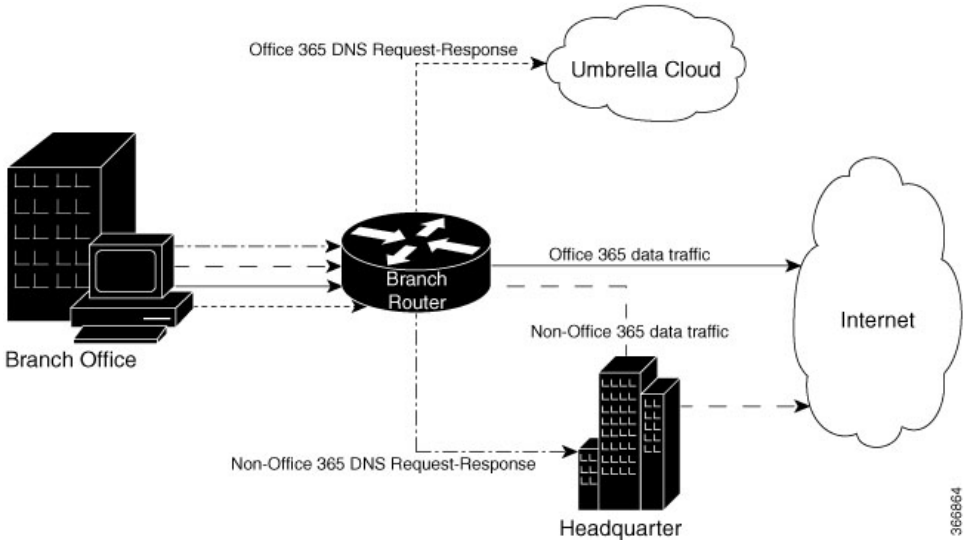
The overlay DMVPN WAN tunnels on a branch router are configured to dynamically learn the service provider they are connected to. An underlay interface is identified as a direct access interface via configuration.

Packets from the LAN side on a branch site are sent over the overlay when packets do not match the criteria of the configured application. When a flow matches the DCA criteria, the packets are directed to the DCA interface that is specified in the path preference. DCA interfaces can be listed in the order of priority in the path preference configuration of the policy for the application. The DCA interfaces are evaluated in the order of the configured path preference priority.

NBAR classification occurs at LAN ingress. NBAR provides the application ID, which is exported by the border router. If a match occurs on the Master Controller for an application, the policy for the application is applied to the traffic class for the specific flow.

The following figure explains the DCA functionality for Office365 application:

Figure 1: DCA for Office365



The following actions are performed to achieve DCA functionality:

- Classify all the cloud applications based on the DNS.
- Intercept DNS traffic and make decisions based on the classification.
  - If the traffic is from a trusted application, direct Internet access is provided. Ensure that security concerns are addressed for the breakout traffic, which include, constant application monitoring, choosing network performance over candidate paths (DCA path, back-haul path), selecting the optimized path according to policy (if DCA path is not good), back-hauling SaaS traffic to data center and reverting back if DCA path recovered.
  - If the traffic is not from a trusted application, the traffic is passed it to the Headquarter for further security inspection and processing.
- Route HTTP, HTTPS data traffic to Internet or Headquarter depending on the above decision.

Designate an Underlay Interface as Direct Access Interface

An interface of the border router must be designated as direct access interface. **domain path** *path-name* **direct-cloud-access** command to specify the direct access interface. A service provider may have multiple links of direct access and each of the direct access interface is measured independently.

When an interface is selected to be the direct access interface, all traffic to the whitelisted applications is directed through the direct access interface. If there are multiple direct access interfaces, the traffic is directed on one direct access interface depending on the performance metrics and policy.

Direct Cloud Access Components

Direct Cloud Access functionality has the following components:

Cisco Umbrella Connector

To achieve location proximity, the SaaS server must be closer to the branch router to achieve better application performance. Generally, DNS requests for a SaaS application are destined to an enterprise DNS resolver. However, the DNS request must be changed from enterprise DNS resolver to a public DNS resolver, such as, OpenDNS resolver or Google DNS resolver. The public DNS resolver helps in placing the SaaS server closer to the branch router by using Cisco Umbrella connector. OpenDNS account and registration is not mandatory.

DNS requests must be unencrypted traffic from the endpoint to the DNS server. Each direct access interface must be configured with Open DNS.

NBAR Classification

Network Based Application Recognition (NBAR) is a classification engine that recognizes and classifies a wide variety of protocols and applications. NBAR uses several classification information metadata such as application name, ID, traffic class, business relevance, and so on.

For Direct Cloud Access functionality, once NBAR recognizes the DNS traffic as belonging to interesting cloud application, it attaches this information to DNS packet in a way so that the umbrella connector feature can extract and use the information.

Cisco NBAR provides the first packet classification for some applications. Cisco NBAR uses DNS learning for application recognition of user defined and predefined domains, Once the server is learned from the DNS response, traffic going to this server can be classified as FIFO. SD-AVC also improves the first packet classification result.

Performance Routing Version 3

Performance Routing version 3 (PfRv3) delivers intelligent path control for application-aware routing across the WAN. Once a DNS response is received, the data traffic (HTTP, HTTPS etc.) from cloud application is provided direct Internet access (local break-out) or is sent to the headquarter for further security inspection.

IPSLA

IPSLA is enabled automatically by PfRv3 to probe each SaaS application over candidate paths by using IPSLA HTTP operation. PfRv3 leverages the metrics reported by IPSLA to select the optimized path.

SaaS Reachability and Performance Management

Performance and reachability of each whitelisted application determines the path that an application takes. PfR measures the reachability and performance of all VRFs and enables and shares one measurement across multiple VRFs.

Next-Hop Reachability

One DSCP-agnostic channel is created as the next-hop for the direct access interface. The DSCP of DCA channel is configured as FF. The routing protocol configured on the direct access interface determines the next hop for the channel.

Performance Measurement

After the channel next hop is up, the service is reached via next hop by using the following steps:

Application Domain Mapping

Application to domain URL and Differentiated Services Code Point (DSCP) mapping must be configured on the master controller of each branch router so that IPSLA can measure the SaaS application using right domain and DSCP.

Reachability and Performance Probing

Measuring network characteristics is performed using IPSLA. IPSLA probes are not sent per VRF, instead, PFR creates a probing layer for all the VRFs and path preferences in the VRFs in a domain. Reachability and performance can be verified per application by using the **show domain** *domain-name* **border dca** command. This command provides information per application, per interface for a border router.

Traffic Steering and Flow Stickiness

When DCA is implemented on a network, traffic classes are automatically created for interested applications. The applications configured in the policy includes path preferences, which corresponds to the respective DSCP configured per application.

When selecting a path, PfR assigns a path to a flow that is destined to a service, for example, Offic365. These flows might traverse a NAT device or a firewall device that maintains the state for the flow sequence numbers. Changing the flow during packet traversal may lead to flow reset. Therefore, when a path is selected, flows must align to that path only. If a path is unreachable, the flow is reset by the client and retried. If the path experiences packet loss but still usable, new flows are routed via alternate paths.

Local Policy Configuration

Direct Cloud Access (DCA) policy can be configured on a centralized hub, or it can be configured on any individual site as a customized local policy. To configure local DCA policy, use the **policy local type DCA** command.

- Customized local policy overrides global policy.
- If a hub connection goes down, local policy remains in effect.

Example of Local Policy Configuration

```
policy local type DCA
  class DCA sequence 4
    match application ms-cloud-group saas-dca
      path-preference DCA1 fallback DCA2
```

How to Configure Direct Cloud Access

Assign an Underlay Interface as Direct Access Interface

The following configuration snippet explains how to assign an Ethernet interface as direct access interface.

```
Router(config)# interface Ethernet 0/1
Router(config-interface)# domain path ATT-DCA direct-cloud-access
```

Define PfR Policy for SaaS Application on Hub Master Controller

The following configuration snippet explains how SaaS application policies are defined on hub master controller at a central point and published to all branch sites. There is no need to define policies at each branch sites because branch sites still have the capability to customize the interested SaaS.

```
Router(config)# domain iwan Router
Router(config-domain)# vrf green
Router(config-domain-vrf)# master hub
Router(config-domain-vrf-master)# class BUSINESS-CRITICAL sequence 10
Router(config-domain-vrf-master-class)# match app-group ms-cloud-group policy custom
Router(config-domain-vrf-master-class-match)# priority 1 delay 500 ms
Router(config-domain-vrf-master-class-match)# exit
Router(config-domain-vrf-master-class)# path-preference ATT-DCA fallback ATT next-fallback
 INET
```

Define SaaS Application Mapping on Branch Master Controller

To measure the SasS application's reachability and performance, the domain URL and DSCP must be specified for IPSLA probing for each SaaS application.

Use HTTP ping to probe a specific SaaS to determine reachability and performance. The system has built-in default URL domains for popular SaaS applications. For a complete list, use **show domain xxx master dca domain-map**.

Note If there are multiple VRFs, IP SLA probing is performed for all domains defined for each VRF and the same IP SLA ID is used for each domain group in the VRF.

If a desired SaaS is not included in the list, create a domain map for the service in PfRv3. For example, to add Servicenow:

```
master branch
 domain-map
 application servicenow-group domain http://www.servicenow.com dscp af21
```

Configure a DNS Resolver

By default, DNS requests for white-listed SaaS are intercepted by Umbrella, and the OpenDNS resolver is used to achieve location proximity.

Optionally, configure a specific DNS resolver, either on a hub master controller or on an specific branch master controller. Configuring a DNS resolver on a specific branch overrides, for that branch, the DNS resolver configured on the hub.

Hub

Use the following on a hub master controller to configure a DNS resolver for all DCA branches.

```
domain default
  master hub
    advanced
      dns-redirect dns-server-address
```

Example:

```
domain default
  master hub
    advanced
      dns-redirect 8.8.8.8
```

Branch

Use the following on a branch master controller to configure a DNS resolver for the branch, overriding the hub setting.

```
domain default
  master branch
    dns-redirect dns-server-address
```

Example:

```
domain default
  master branch
    dns-redirect 8.8.8.8
```

Configure the HTTP Ping Probe Interval

The HTTP ping probe uses a default probe interval of 30 seconds.

Optionally, you can configure a specific interval on the hub master controller, which applies the change to all DCA branches, or to a branch master controller, to change the interval for a specific branch.

Hub

Use the following on a hub master controller to configure the interval for all DCA branches.

```
domain default
  master hub
    advanced
      dca-probe-http-interval interval-in-seconds
```

Example:

```
domain default
  master hub
    advanced
      dca-probe-http-interval 20
```

Branch

Use the following on a branch master controller to configure the interval for a specific branch. The branch setting overrides a setting made at the hub.

```
domain default
  master branch
    dca-probe-http-interval interval-in-seconds
```

Example:

```
domain default
  master branch
    dca-probe-http-interval 20
```

Verify and Monitor Direct Cloud Access Configuration

Use the following commands to verify and monitor DCA configuration.

- **show domain iwan master traffic-classes summary**
- **show domain iwan master traffic-classes detail**
- **show domain iwan master traffic-classes dca detail**
- **show domain iwan master traffic-classes dca application**
- **show domain** *domain-name* **border dca**

  Displays information about reachability and metrics collected for all paths towards a service. This command helps in understanding the behavior of various paths for a service and how PFR is selecting the best paths depending on the metrics.

```
Device# show domain iwan border dca

[*] PFR created IP SLA entry ID
IPSLA DNS Resolver:208.67.220.220

App    DSCP  RTT/ms  DCA2   MPLS1
        thresh  Gi0/0/2   Tu10 (0:1)
           RTT/ms[*]   RTT/ms[*]
share-point    default  1000  7 [31]   --
youtube    default  1000  78 [33]   --
box    default  1000  7 [39]   --
dropbox    default  1000  3 [41]   --
google-services default     1000  108 [49]   --
google-group    default  1000  109 [51]   --
gtalk-group    default  1000  112 [53]   --
hangouts-group    default  1000  115 [55]   --
ms-lync-group    default  1000  6 [57]   --
ms-cloud-group    default  1000  7 [59]   --
```

- **show domain default policy**

  Displays the default policy on the master controller.

```
Device# show domain default master policy
       No Policy publish pending
-------------------------------------------------------------------------------
  class SOCIAL-NETWORKING sequence  11
        class type: Application Based
             match application skype policy custom
                   priority 1 delay threshold 500 msec
```

- To troubleshoot, use **debug domain default master dca** and *debug domain default border dca* commands.

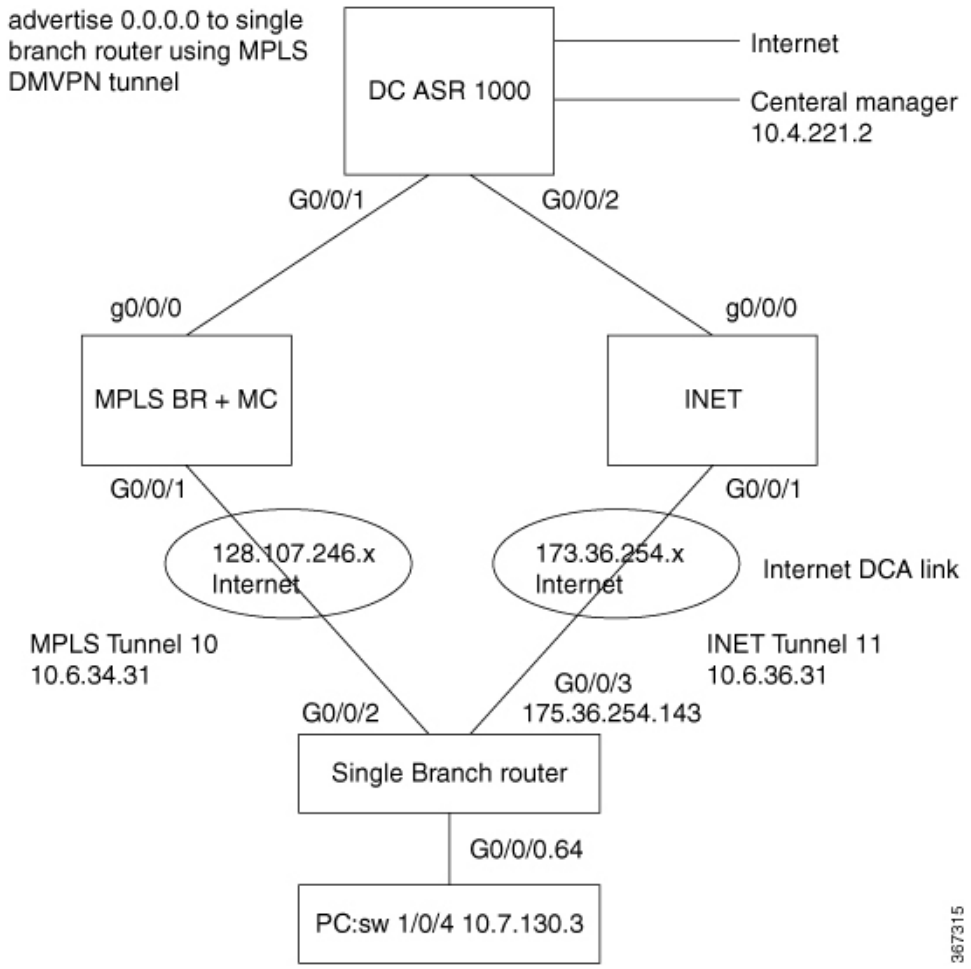
Configuration Examples for Configuring Direct Cloud Access

Example: Configure DCA Link on a Single Branch Router

Overview

In this example, DCA is configured on Cisco IWAN network with a single branch router as shown in the following topology.

Figure 2: DCA Link on a Single Branch Router



Umbrella Service

Beginning with Cisco IOS XE Gibraltar 16.10.1, the Umbrella service configuration is automatic.

Underlay Interface

DCA is configured on WAN underlay interface in order to distinguish tunnel WAN interface.

```
interface GigabitEthernet0/0/3  ! INET branch WAN DCA interface
domain iwan path DCA1 direct-cloud-access
umbrella out
```

Optionally, a second DCA can be created as WAN underlay interface.

```
interface GigabitEthernet0/0/2  ! INET branch DCA2 interface
 domain iwan path DCA2 direct-cloud-access
 umbrella out
```

Create Domain Map

Optionally, create a domain map for a specific SaaS not included by default.

```
master branch
 domain-map
 application servicenow-group domain http://www.servicenow.com dscp af21
```

Hub Master Controller Configuration

The policy can be local or from a centralized hub master controller. Configure a hub master controller as follows:

Note Configure only one master controller, either at a hub site or a branch site.

```
domain default
vrf default
  master hub

  class DCA sequence 4
    match application ms-cloud-group saas-dca
    path-preference DCA1 fallback DCA2
```

Branch 1 and Master Controller Configuration

A branch site can serve as master controller instead of a hub site. In this example, Branch 1 serves as master conroller. The configuration includes LAN interface and WAN (DCA) interface.

Note Configure only one master controller, either at a hub site or a branch site.

```
domain default
  vrf default
    border
      master local
    master branch
      source-interface Loopback0
      hub 100.20.1.1
```

LAN interface configuration:

```
interface GigabitEthernet3.30
  description B1MCBR-LAN
  encapsulation dot1Q 30
  ip address 10.20.0.1 255.255.255.0
  ip nat inside
```

Assigning the DCA to a WAN interface:

```
interface GigabitEthernet2.30
  encapsulation dot1Q 30
    ip vrf forwarding fvrf
    ip address 10.20.1.1 255.255.255.0
    ip nat outside
    domain path DCA1 direct-cloud-access
```

Branch 2 Configuration

This branch configuration includes LAN interface and WAN (DCA) interface.

```
domain default
  vrf default
     border
       source-interface Loopback0
       master 192.168.3.22
```

LAN interface configuration:

```
interface GigabitEthernet3.30
  description B1MCBR-LAN
  encapsulation dot1Q 30
  ip address 10.20.0.1 255.255.255.0
  ip nat inside
```

Assigning the DCA to a WAN interface:

```
interface GigabitEthernet2.30
  encapsulation dot1Q 30
    ip vrf forwarding fvrf
    ip address 10.20.1.1 255.255.255.0
    ip nat outside
    domain path DCA2 direct-cloud-access
```

Verifying the Configuration

The following commands are used to verify the configuration. To verify OpenDNS configuration, use the **show umbrella deviceid** and **show umbrella configuration** commands.

```
router# show umbrella deviceid

Device registration details
Interface Name                    Tag                   Status                 Device-id
GigabitEthernet3.64     inside-network   200 SUCCESS     010a3d458c172b8b

router# show umbrella configuration
Umbrella Configuration
========================
   Token: 7772166EF2E473ADE8FA2204B37D0BD7001FE4F5
   OrganizationID: 2090229
   Local Domain Regex parameter-map name: dns_bypass
   DNSCrypt: Enabled
   Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

   UDP Timeout: 5 seconds
   Resolver address:
       1. 208.67.220.220
       2. 208.67.222.222
       3. 2620:119:53::53
```

```
       4. 2620:119:35::35
Umbrella Interface Config:
       Number of interfaces with "umbrella out" config: 2
         1. GigabitEthernet0/0/0
             Mode     :  OUT
             VRF      : IWAN-TRANSPORT-2(Id: 3)
         2. GigabitEthernet0/0/1
             Mode     :  OUT
             VRF      : IWAN-TRANSPORT-1(Id: 2)
       Number of interfaces with "umbrella in" config: 1
         1. GigabitEthernet3.64
             Mode       : IN
             DCA        : Enabled
             Policy Name: umbrella-direct-access
             Tag        : lan064
             Device-id  : 010a3d458c172b8b
             VRF        : global(Id: 0)
```

To verify the DCA configuration, use the following commands:

- **show domain iwan border dca**
- **show domain iwan master dca status**
- **show domain iwan master traffic-classes summary**
- **show domain iwan master traffic-classes detail**
- **show ip sla summary**
- **show ip sla configuration**
- **show ip sla statistics**
- **show flow monitor name flow-monitor cache format table**

Use the **show ip sla summary**, **show ip sla configuration**, and **show ip sla statistics** commands to verify the probe functions.

Use the **show flow monitor** command to verify that the flow is passes through the DCA path.

```
Router# show domain iwan master traffic-classes summary

APP - APPLICATION, TC-ID - TRAFFIC-CLASS-ID, APP-ID - APPLICATION-ID
Current-EXIT - Service-Provider(PFR-label)/Border/Interface(Channel-ID)
UC - UNCONTROLLED, PE - PICK-EXIT, CN - CONTROLLED, UK - UNKNOWN

Dst-Site-Pfx      Dst-Site-Id       State DSCP        TC-ID      APP-ID    APP
Current-Exit

DCA               Internet          CN    default[0]  30         9424      ms-cloud-group
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  29         4478      ms-lync-group
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  28         8388      hangouts-group
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  27         4692      gtalk-group
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  26         4456      google-group
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  25         218104328 google-service
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  21         50349148  dropbox
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
```

```
DCA               Internet          CN    default[0]  20         218104882 box
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  17         218103890 youtube
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)

Router# show domain iwan border dca

[*] PFR created IP SLA entry ID
IPSLA DNS Resolver:208.67.220.220

App    DSCP  RTT/ms  DCA2   MPLS1
        thresh  Gi0/0/2   Tu10 (0:1)
           RTT/ms[*]   RTT/ms[*]
share-point    default  1000  7 [31]   --
youtube    default  1000  78 [33]   --
box    default  1000  7 [39]   --
dropbox    default  1000  3 [41]   --
google-services default     1000  108 [49]   --
google-group    default  1000  109 [51]   --
gtalk-group    default  1000  112 [53]   --
hangouts-group    default  1000  115 [55]   --
ms-lync-group    default  1000  6 [57]   --
ms-cloud-group    default  1000  7 [59]   --

Router# show domain iwan master traffic-classes detail

 Dst-Site-Prefix: DCA               Application: ms-cloud-group   DSCP: default [0] Traffic
 class id:30 app_id:9424
  Clock Time:                 22:13:32 (UTC) 01/17/2018
  TC Learned:                 4d23h ago
  Present State:              CONTROLLED
  Current Performance Status: not monitored (internet)
  Current Service Provider:   DCA1 since 4d23h
  Previous Service Provider:  Unknown
  BW Used:                    0 bps
  Present WAN interface:      GigabitEthernet0/0/3 in Border 10.255.241.31
  Present Channel (primary):  6 DCA1 pfr-label:0:0 | 0:0 [0x0]
  Backup Channel:             4 DCA2 pfr-label:0:0 | 0:0 [0x0]
  Destination Site ID:        Internet
  DNS Primary Channel:        6 DCA1 pfr-label:0:0 | 0:0 [0x0]
  DNS Backup Channel:         4 DCA2 pfr-label:0:0 | 0:0 [0x0]
  Class-Sequence in use:      55
  Class Name:                 saasapp using policy User-defined
    priority 1 one-way-delay threshold 500 msec
  BW Updated:                 - ago
  Method for choosing channel: Random
  Reason for Latest Route Change:    Uncontrolled to Controlled Transition
  Route Change History

Router# show ip sla sum

ID           Type        Destination       Stats       Return      Last
                                                       Code        Run
---------------------------------------------------------------------------

*1255        http        216.58.217.164    RTT=198     OK          30 seconds ago
*1256        http        216.58.217.164    RTT=184     OK          30 seconds ago
*1257        http        216.58.217.164    RTT=219     OK          30 seconds ago

*1258        http        216.58.217.164    RTT=219     OK          30 seconds ago

*1259        http        13.107.7.190      RTT=76      Http Error  30 seconds ago
```

```
Router# show ip sla config 1255

Entry number: 1255
Type of operation to perform: http
Target address/Source address: 216.58.217.164/172.16.1.1
Target port/Source port: 80/0
Type Of Service parameters: 0x0
Vrf Name: IWAN-TRANSPORT-2
HTTP Operation: get
HTTP Server Version: 1.0
URL: http://www.google.com
Proxy:
Raw String(s):
Cache Control: enable
Owner:
Tag:
Operation timeout (milliseconds): 30000
Schedule:
   Operation frequency (seconds): 60  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 20000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
History Statistics:
   Number of history Lives kept: 0
   Number of history Buckets kept: 15
   History Filter Type: None

Router# show ip sla statistics 1255

IPSLA operation id: 1255
        Latest RTT: 179 milliseconds
Latest operation start time: 19:09:14 UTC Fri Jan 26 2018
Latest operation return code: OK
Latest DNS RTT: 6 ms
Latest TCP Connection RTT: 62 ms
Latest HTTP Transaction RTT: 111 ms
Number of successes: 29
Number of failures: 0
Operation time to live: Forever

Router# show flow monitor Monitor-FNF-IWAN cache format table | i office
54.209.129.73    172.31.1.2                80          62102  Gi0/0/0               Input
            6  layer7 ms-office-365             0.0.0.0                        /30  Null
                          4                   0x00
172.31.1.2       52.109.2.14              5110           443  Gi0/0/2.101           Output
           6  layer7 ms-office-web-apps         172.31.1.1                     /0  Gi0/0/0
                          7                   0x00
10.30.32.200     104.91.217.163           50319           443  Gi0/0/2.101           Input
            6  layer7 ms-office-365             172.31.1.1                     /0  Gi0/0/0
                          9                   0x00
172.31.1.2       208.67.222.222           52262            53  Null                  Output
          17  layer7 ms-office-365             172.31.1.1                    /30  Gi0/0/0
                          1  www.office.com   0x00
10.30.32.200     104.91.188.182           50341           443  Gi0/0/2.101           Input
            6  layer7 ms-office-365             172.31.1.1                     /0  Gi0/0/0
```

```
                    11                    0x00
10.30.32.200     104.91.188.182          50310           443  Gi0/0/2.101          Input
           6  layer7 ms-office-365              172.31.1.1                    /0  Gi0/0/0
                    11                    0x00
172.31.1.2       52.109.2.14             5108            443  Gi0/0/2.101          Output
           6  layer7 ms-office-web-apps         172.31.1.1                    /0  Gi0/0/0
                    8                     0x00
```

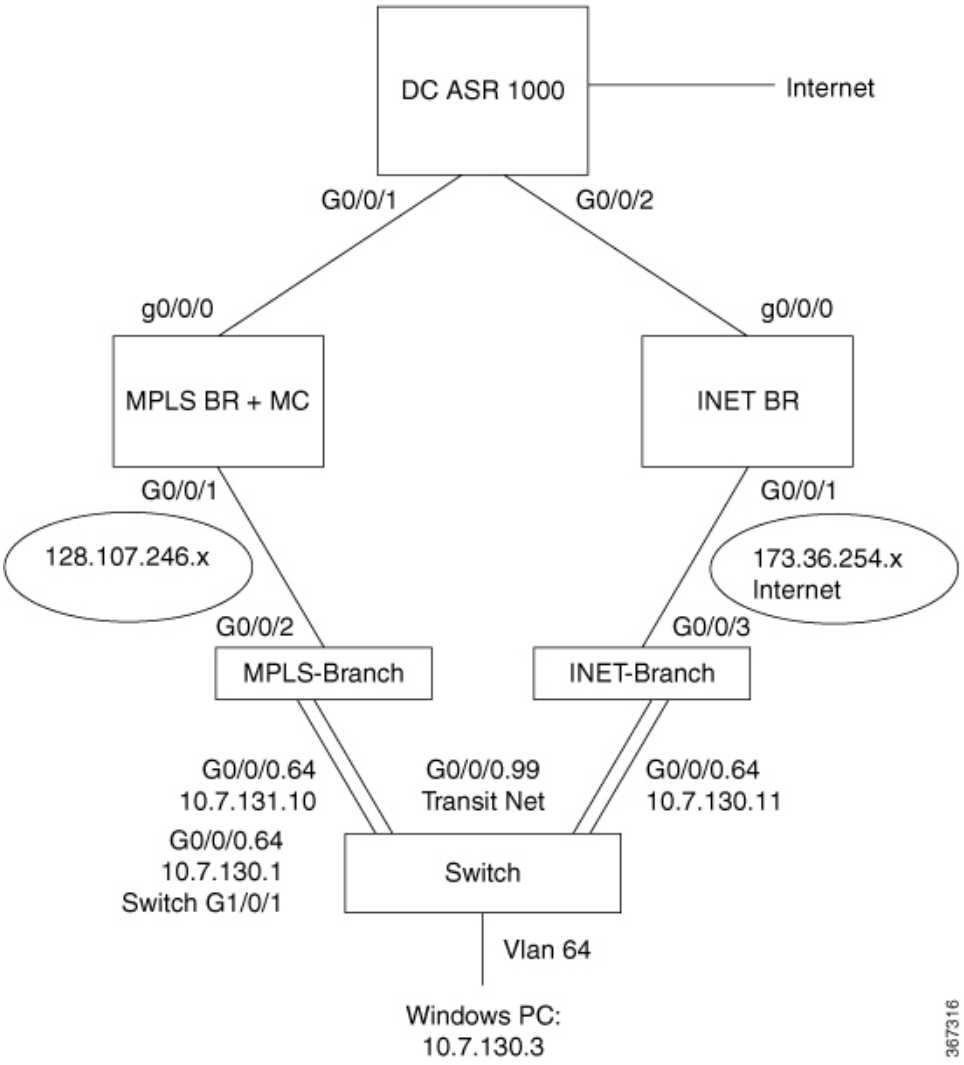
Example: Configure DCA Link on a Dual Branch Router

Overview

In this example, DCA is configured on Cisco IWAN network with a dual branch router as shown in the following topology.

The policy can be local or from a centralized hub. This example illustrates the use of a local policy in a non-IWAN scenario.

Figure 3: DCA Link on a Dual Branch Router



Branch 1 and Master Controller Configuration

A branch site can serve as master controller instead of a hub site. In this example, Branch 1 serves as master conroller. The configuration includes LAN interface and WAN (DCA) interface.

Note Configure only one master controller, either at a hub site or a branch site.

```
domain default
  vrf default
    border
      master local
    master branch
      source-interface Loopback0
            hub l00.20.1.1

  policy local type DCA
    class DCA sequence 4
      match application ms-cloud-group saas-dca
        path-preference DCA1 fallback DCA2
```

LAN interface configuration:

```
interface GigabitEthernet3.30
  description B1MCBR-LAN
  encapsulation dot1Q 30
  ip address 10.20.0.1 255.255.255.0
  ip nat inside
```

Assigning the DCA to a WAN interface:

```
interface GigabitEthernet2.30
  encapsulation dot1Q 30
    ip vrf forwarding fvrf
    ip address 10.20.1.1 255.255.255.0
    ip nat outside
    domain path DCA1 direct-cloud-access
```

Branch 2 Configuration

This branch configuration includes LAN interface and WAN (DCA) interface.

```
domain default
  vrf default
    border
      source-interface Loopback0
      master 192.168.3.22
```

LAN interface configuration:

```
interface GigabitEthernet3.30
  description B1MCBR-LAN
  encapsulation dot1Q 30
  ip address 10.20.0.1 255.255.255.0
  ip nat inside
```

Assigning the DCA to a WAN interface:

```
interface GigabitEthernet2.30
  encapsulation dot1Q 30
  ip vrf forwarding fvrf
  ip address 10.20.1.1 255.255.255.0
  ip nat outside
  domain path DCA2 direct-cloud-access
```

Example: Configuring Umbrella Branch for OpenDNS

Overview

Beginning with Cisco IOS XE Gibraltar 16.10.1, DCA configures the Cisco Umbrella Connector automatically on the router. However, it is still possible to configure Umbrella manually.

For example, if it is necessary to validate OpenDNS, you must configure Cisco Umbrella Connector on the branch, as shown in the example below.

Procedure

1. Configure the DNS server, setting the router's clock and time zone correctly.

```
ip domain name cisco.com
ip host api.opendns.com 67.215.92.210
```

2. Log into the OpenDNS portal to get an API token.

   https://login.opendns.com/?return_to=https://dashboard2.opendns.com

3. Import the certificate, entering a PEM-formatted CA certificate.

   (config)#**crypto pki trustpool import terminal**

   Enter a PEM-formatted CA certificate.

```
(config)#crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIElDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaME0xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxJzAlBgNVBAMTHkRpZ2lDZXJ0IFNIQTIg
U2VjdXJlIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANyuWJBNwcQwFZA1W248ghX1LFy949v/cUP6ZCWA1O4Yok3wZtAKc24RmDYXZK83
nf36QYSvx6+M/hpzTc8zl5CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bd
KpPDkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDOg5B6TXvi/TC2rSsd9f
/ld0Uzs1gN2ujkSYs58O09rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdRrdNzGX
kujNVA075ME/OV4uuPNcfhCOhkEAjUVmR7ChZc6gqikJTvOX6+guqw9ypzAO+sf0
/RR3w6RbKFfCs/mC/bdFWJsCAwEAAaOCAVowggFWMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHA6
Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwN6A1
oDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD
QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v
d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh
xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl
5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/sELfeNqzqPlt/yGFUzZgTHbO7Djc1lGA
8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC
2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit
c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0
j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLz-----END CERTIFICATE-----
```

Note This is the PEM-formatted version. Keep the "END CERTIFICATE" portion. Without this, the certificate will be lost after a router reloads.

4. (Optional) Configure local domains.

DNS queries directed to a local domain will remain untouched and will not be redirected to OpenDNS cloud.

```
parameter-map type regex dns_bypass
pattern www.cisco.com
pattern .*eisg.cisco.*
```

5. Configure the token.

```
parameter-map type umbrella global
token 0F32C32FEC26991C2B562D3C7FF844E0001C70E7
local-domain dns_bypass
```

Note Cisco OpenDNS is used by default. To use a different DNS resolver, add the following line:

resolver ipv4 *DNS-server- IP*

Note Enter a fake token for this step if you are using another DNS server or do not want to register with OpenDNS server.

6. Assign the above policy to a LAN interface.

```
GigabitEthernet0/0/0.100  ! INET branch LAN interface
umbrella in direct-cloud-access default lan100
```

7. Assign the Umbrella to a WAN interface.

```
interface GigabitEthernet0/0/3  ! INET branch WAN DCA interface
domain iwan path DCA1 direct-cloud-access
umbrella out
```

8. Apply **umbrella out** on all DCA interfaces. This includes the MPLS branch of a dual branch if the MPLS branch has a DCA interface.

```
interface GigabitEthernet0/0/2  ! MPLS branch WAN DCA interface
domain iwan path DCA2 direct-cloud-access
umbrella out

interface GigabitEthernet0/0/0.100  ! MPLS branch LAN interface
umbrella in direct-cloud-access default lan100
```

Additional References for Configuring Direct Cloud Access

Related Documents

Related Topic	Document Title
Performance Routing Version 3 commands	Cisco IOS Performance Routing Version 3 Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html