



## 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, on page 1](#)
- [Prerequisites for Configuring Direct Cloud Access, on page 2](#)
- [Restrictions for Configuring Direct Cloud Access, on page 2](#)
- [Information About Configuring Direct Cloud Access, on page 2](#)
- [How to Configure Direct Cloud Access, on page 6](#)
- [Configuration Examples for Configuring Direct Cloud Access, on page 7](#)
- [Additional References for Configuring Direct Cloud Access, on page 17](#)

## 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](http://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	<p>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.</p> <p>The following commands were introduced or modified: <b>domain path</b>, <b>path-preference</b>, <b>show domain dca-status</b>, <b>show domain default border</b>, <b>show domain default policy</b>, <b>show domain vrf border channels</b>, <b>show domain vrf master channels</b>.</p>

## Prerequisites for Configuring Direct Cloud Access

- Cisco Umbrella Branch must be enabled to intercept DNS to public DNS resolver.

**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.

## Benefits of Direct Cloud Access

- 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

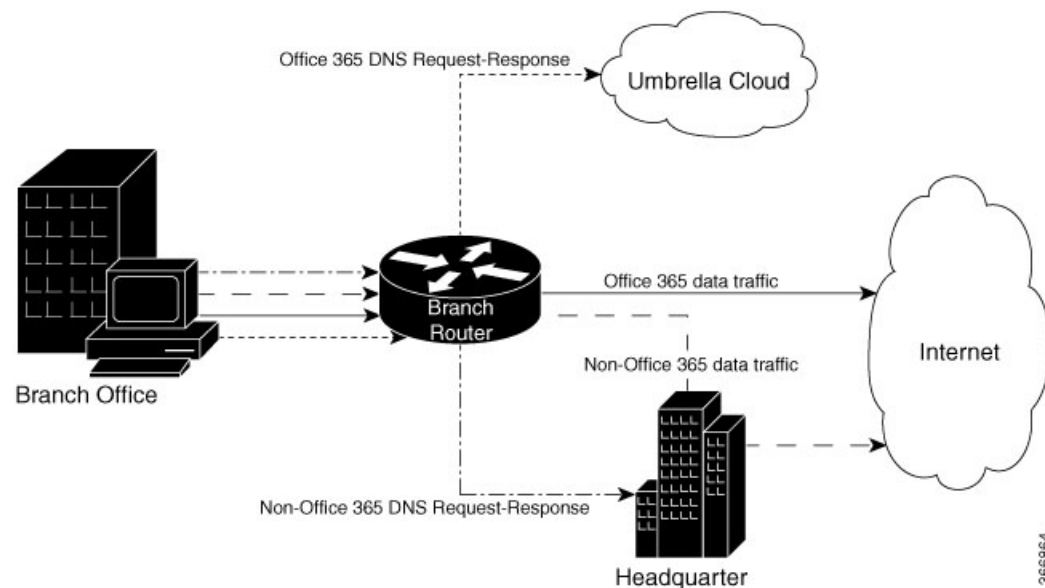
The overlay DMVPN WAN tunnels on a branch router are configured to dynamically learn the service provider they are connected to. An underlay interface is identified as a direct access interface via configuration.

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.

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

```
master branch
domain-map
application ms-lync-group domain http://www.office.com dscp default
application ms-cloud-group domain http://www.office.com dscp default
application ms-lync- group domain http://www.office.com dscp default
application box domain http://www.box.com dscp default
application dropbox domain http://www.dropbox.com dscp default
application google-services domain http://www.google.com dscp default
application google- group domain http://www.google.com dscp default
application hangouts-group domain http://www.google.com dscp default
application gtalk-group domain http://www.google.com/ dscp default
```

### 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
```

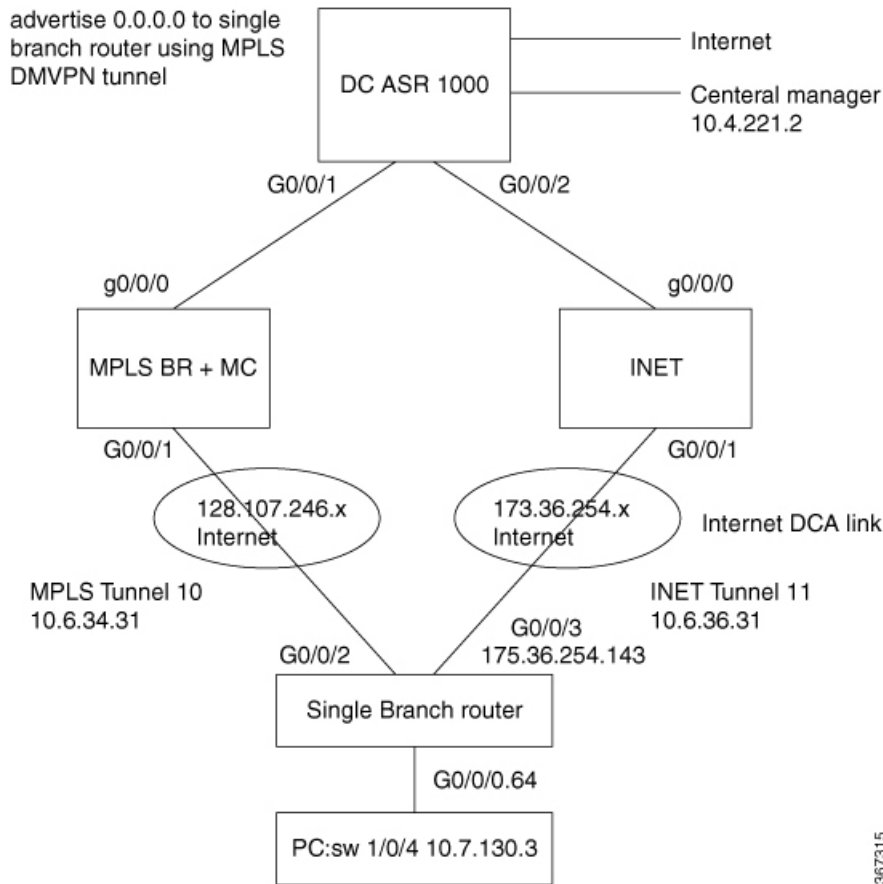
- To troubleshoot, use **debug domain default master dca** and **debug domain default border dca** commands.

## Configuration Examples for Configuring Direct Cloud Access

### Example: Configure DCA Link on a Single Branch Router

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



The following configuration pertains to configuring Umbrella branch.

```
ip domain lookup vrf IWAN-TRANSPORT-2 source-interface GigabitEthernet0/0/3
ip domain name cisco.com /*This step is not required if OpenDNS Server is not used to
resolve dns request or if other DNS server is configured for DNS resolution or registration
with DNS is not required*/
ip host api.opendns.com 67.215.92.210 /*This step is not required if OpenDNS Server is not
used to resolve dns request*/
ip name-server 8.8.8.8
ip name-server vrf IWAN-TRANSPORT-2 8.8.8.8
```



**Note** You need not specify the default static route if you have multi-VRF or if LAN is in different VRF. Pfrv3 will automatically forward the whitelisted traffic to DCA interface.

The commands **ip domain name cisco.com** and **ip host api.opendns.com 67.215.92.210** are not required if OpenDNS Server is not used to resolve dns request or if another DNS server is configured for DNS resolution or registration with DNS is not required

Navigate to this link to log in to the OpenDNS portal ([https://login.opendns.com/?return\\_to=https://dashboard2.opendns.com](https://login.opendns.com/?return_to=https://dashboard2.opendns.com)) to obtain API token and import the certificate on the device.



```

crypto pki trustpool import terminal
% Enter PEM-formatted CA certificate.
-----BEGIN CERTIFICATE----- MIEI1DCCA3ygAwIBAgIQAf2j627KdciIQ4tys8+8kTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLEExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDEXdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAEFw0xMzAzMDgxMjAwMDEwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
MRUwEwYDVQQKEwEaWdpQ2VydCBHbG9iYWwgUm9vdCBHbG9iYWwgUm9vdCBHbG9i
U2VjdXJlIFNlcnZlcjBDQTCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCgggEB
ANYuWJBNwCQwFZA1W248ghX1LFy949v/cUP6ZCWA104Yok3wZtAKc24RmDYXZK83
nf36QYSvx6+M/hpzTc8z15CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXu3R0bDK
pPDkC55gIDvEwRqFDulm5K+wgdlTvza/P96rtxcflUxDOg5B6TXvi/TC2rSsd9f
/l0Uzs1gN2ujkSYs58009rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdRrdNzGX
kujNVA075ME/OV4uuPncfhC0hkeAjUVmR7ChZc6gqikJTVOX6+guqw9ypzAO+sf0
/RR3w6RbKfCs/mC/bdFWJscAwEAAOCAVowggFWMBIGA1UdEwEB/wQIMAYBaf8C
AQAwDgYDVROPAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCCgwJjAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMMh0dHA6
Ly9jcmwzLmRpZ21jZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwzLmRp
oDOGMMh0dHA6Ly9jcmw0LmRpZ21jZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD
QS5jcmwzLmRpZ21jZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwzLmRp
d3d3LmRpZ21jZXJ0LmNvbS9DUFMwHQYDVRO0BBYEFa+AYRyCMWHVlyjnjUY4tCzh
xtniMB8GA1UdIwQYMBaFAFAPEUDVW0Uy7Zvcj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFS+S+JtZLHg14+mUwnNqip1
5T1Pho0lblyYoiQm5vuh7ZPHLgLGtUq/sELfeNqzqPlt/yGFUzZgTHb07Djc1lGA
8MXW5dRNJ2Srm8c+cftI17gzbcTB+6WohsYFFZcTEDts8Ls/3HB40f/1LkAtDdC
2iDJ6m6K7hQGrn2iWziIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rAhaPit
c+LJMto4JQtV05od8GiG7S5BN098pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0
j6tJLp07kzQoH3j0lOrHvdPjBzRzeXDLz-----END CERTIFICATE-----

```

Optionally, the local domains and the token can be configured. DNS queries destined to local domain will remain untouched and will not be redirected to OpenDNS cloud.

```

parameter-map type umbrella global
token F3F195ADD8160A3A4E42BB6B3722A5770022BF2F
no dnscrypt
udp-timeout 5

```

You may include the **resolver ipv4 dns-server IP address** command, if you are not registering with the OpenDNS server or using another DNS server.

The hub master controller configuration is as follows:

```

domain iwan
vrf default
master hub
class saasapp sequence 55
match application share-point policy custom ! For Office 365 Application
priority 1 one-way-delay threshold 500
match app-group ms-lync-group policy custom ! For Office 365 Application
priority 1 one-way-delay threshold 500
match app-group ms-cloud-group policy custom ! For Office 365 Application
priority 1 one-way-delay threshold 500
match application google-services policy custom ! For google Application
priority 1 one-way-delay threshold 1000
match app-group google-group policy custom ! For google Application
priority 1 one-way-delay threshold 500
match app-group gtalk-group policy custom ! For google Application
priority 1 one-way-delay threshold 500
match app-group hangouts-group policy custom ! For google Application
priority 1 one-way-delay threshold 500
match application youtube policy custom ! For youtube Application
priority 1 one-way-delay threshold 500
match application box policy custom
priority 1 one-way-delay threshold 500
match application dropbox policy custom

```

```

priority 1 one-way-delay threshold 500
path-preference DCA1 fallback DCA2 next-fallback MPLS1

```

The configuration for class-map and policy for umbrella branch on the branch master controller is as follows:

```

class-map match-any umbrella-direct-access
match protocol share-point
match protocol attribute application-group ms-lync-group
match protocol attribute application-group ms-cloud-group
match protocol skype
match protocol dropbox
match protocol google-services
match protocol attribute application-group google-group
match protocol attribute application-group gtalk-group
match protocol attribute application-group hangouts-group
match protocol youtube
policy-map type umbrella umbrella-direct-access
class umbrella-direct-access
direct-cloud-access

```

The above created policy is assigned to an LAN interface.

```

interface GigabitEthernet0/0/0.64 ! INET branch LAN interface
 umbrella in direct-cloud-access umbrella-direct-access lan064

```

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

```

The following configuration creates domain map, which must match the hub configuration.

```

domain iwan
master branch
domain-map
 application ms-lync-group domain http://www.office.com dscp default
 application ms-cloud-group domain http://www.office.com dscp default
 application ms-lync-group domain http://www.office.com dscp default
 application box domain http://www.box.com dscp default
 application dropbox domain http://www.dropbox.com dscp default
 application google-services domain http://www.google.com dscp default
 application google-group domain http://www.google.com dscp default
 application hangouts-group domain http://www.google.com dscp default
 application gtalk-group domain http://www.google.com/ dscp default

```



**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.

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
DNSEncrypt: 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 DCA configuration, use the following commands:

- **show domain iwan border dca**
- **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
```

## Example: Configure DCA Link on a Single Branch Router

```

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 Code	Last 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**

### Example: Configure DCA Link on a Dual Branch Router

```

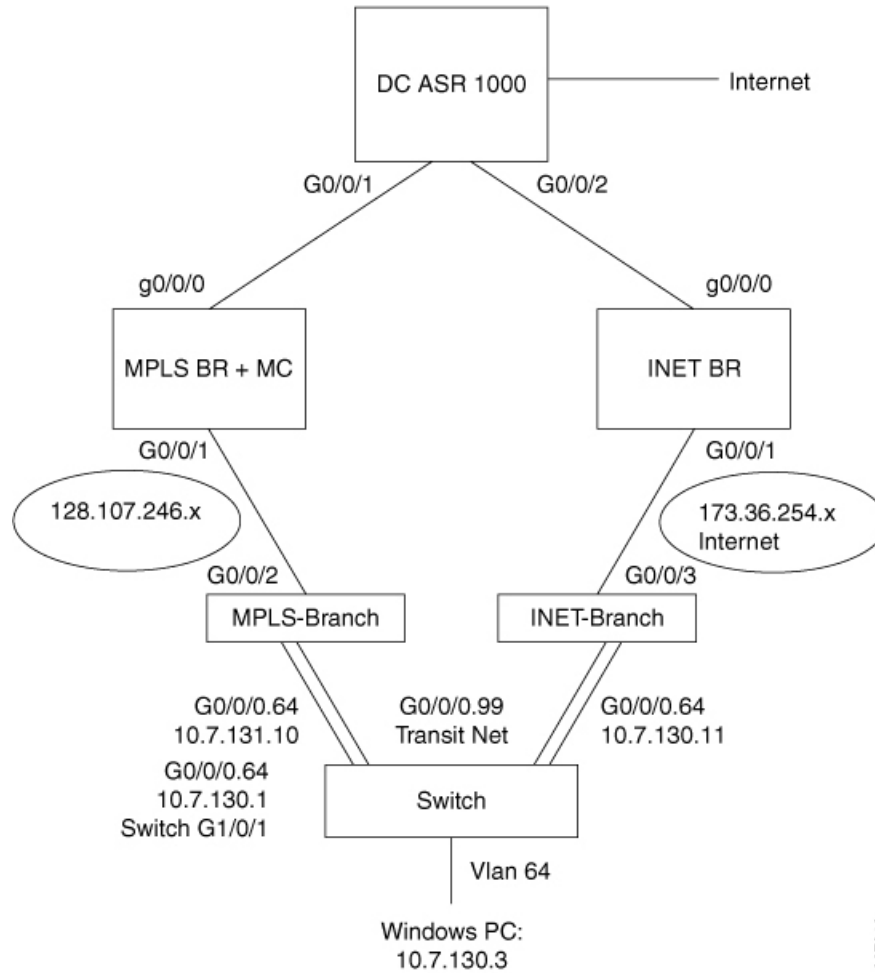
54.209.129.73 172.31.1.2 80 62102 Gi0/0/0 Input
6 layer7 ms-office-365 0.0.0.0 /30 Null
4 0x00
172.31.1.2 52.109.2.14 5110 443 Gi0/0/2.101 Output
6 layer7 ms-office-web-apps 172.31.1.1 /0 Gi0/0/0
7 0x00
10.30.32.200 104.91.217.163 50319 443 Gi0/0/2.101 Input
6 layer7 ms-office-365 172.31.1.1 /0 Gi0/0/0
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

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

Figure 3: DCA Link on a Dual Branch Router



The following is the hub master controller configuration.

```

domain iwan
vrf default
master hub
class saasapp sequence 55
  match application share-point policy custom      ! For Office 365 Application
  priority 1 one-way-delay threshold 500
  match app-group ms-lync-group policy custom      ! For Office 365 Application
  priority 1 one-way-delay threshold 500
  match app-group ms-cloud-group policy custom     ! For Office 365 Application
  priority 1 one-way-delay threshold 500
  match application google-services policy custom  ! For google Application
  priority 1 one-way-delay threshold 1000
  match app-group google-group policy custom      ! For google Application
  priority 1 one-way-delay threshold 500
  match app-group gtalk-group policy custom       ! For google Application
  priority 1 one-way-delay threshold 500
  match app-group hangouts-group policy custom    ! For google Application
  priority 1 one-way-delay threshold 500
  match application youtube policy custom         ! For youtube Application
  priority 1 one-way-delay threshold 500
  match application box policy custom

```

```

priority 1 one-way-delay threshold 500
match application dropbox policy custom
priority 1 one-way-delay threshold 500
path-preference DCA1 fallback DCA2 next-fallback MPLS1

```

The following is the domain map configuration on the MPLS branch master controller. The domain map must match the hub configuration.

```

domain iwan
master branch
  domain-map
    application ms-lync-group domain http://www.office.com dscp default
    application ms-cloud-group domain http://www.office.com dscp default
    application ms-lync-group domain http://www.office.com dscp default
    application box domain http://www.box.com dscp default
    application dropbox domain http://www.dropbox.com dscp default
    application google-services domain http://www.google.com dscp default
    application google-group domain http://www.google.com dscp default
    application hangouts-group domain http://www.google.com dscp default
    application gtalk-group domain http://www.google.com/ dscp default

```

The following is the configuration on INET branch router to create class-map and policy for umbrella branch.

```

class-map match-any umbrella-direct-access
  match protocol share-point
  match protocol attribute application-group ms-lync-group
  match protocol attribute application-group ms-cloud-group
  match protocol skype
  match protocol dropbox
  match protocol google-services
  match protocol attribute application-group google-group
  match protocol attribute application-group gtalk-group
  match protocol attribute application-group hangouts-group
  match protocol youtube
policy-map type umbrella umbrella-direct-access
class umbrella-direct-access
  direct-cloud-access

```

The policy created above is assigned to a LAN interface.

```

GigabitEthernet0/0/0.64 ! INET branch LAN interface
  umbrella in direct-cloud-access umbrella-direct-access lan064

```

The DCA is assigned to WAN interface as follows:

```

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

```

Optionally, a second DCA (on another WAN interface) can be configured as follows:

```

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

```

The following adds the interface to IWAN border source-interface configuration and enables the feature.

```

interface Virtual-Template1 type tunnel
  ip unnumbered Loopback0
  ip nat inside
  umbrella in direct-cloud-access umbrella-direct-access inetAT
domain iwan
vrf default
  border

```



```
source-interface Loopback0 virtual-template 1
shut
no shut
```

In DCA dual branch scenario, to apply features like NAT or Umbrella on PfR auto-tunnel interface, a virtual template is configured and bound to IWAN domain configuration.

To effect configuration changes on virtual template interface, you must execute the **shut** or **no shut** command on the branch router.

## Additional References for Configuring Direct Cloud Access

### Related Documents

Related Topic	Document Title
Performance Routing Version 3 commands	<a href="#">Cisco IOS Performance Routing Version 3 Command Reference</a>

### 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

