Dimension Data Peering Policy

AS3471 – Private & Public Peering

peering@dimensiondata.com

2022

Introduction

This document describes the peering relationship between the applicant and Dimension Data (DD) so that the applicant can connect between their network and DD's backbone. This document has set rules for peering connections.

Dimension Data contact details

All peering-related queries can be directed at the Core Infrastructure team by emailing peering@dimensiondata.com

Parties who do not meet any of the peering requirements can become a client of Dimension Data by emailing sales@dimensiondata.com

Table of Contents

General Peering Policy Statement

Dimension Data (DD) will peer directly or through an Internet Service Providers Association (ISPA) - managed Internet Exchange ("INX") with any Internet Protocol (IP) based service provider in a peering arrangement where traffic exchanged meets the levels and ratios specified below. Whenever possible, DD will implement multiple peering links with a peer, to avoid the loss of a single connection.

All peering partners must meet the criteria defined below and agree that the bandwidth of the peering connection will be determined by current and periodic reviews of traffic exchange. Peering will be done on a negotiated basis, with location and cost as agreed to by both parties. Parties who peer with DD will need to complete a written Peering Agreement with DD. The contractual relationship between DD and its peering partner, including all the respective parties' rights and obligations, will be constituted solely by the Peering Agreement. No rights or obligations are intended to arise out of or be conferred through the Peering Policy.

In addition to the criteria below, DD's willingness to enter into peering arrangements with a particular peer will be subject to generally accepted commercial and technical considerations, including but not limited to the applicant's financial stability, the availability of peering ports and DD's backbone capacity in particular locations.

It should be noted that the Peering Policy contains the general guidelines which will determine DD's peering relationships. In all circumstances, irrespective of compliance with the Peering Policy, the decision on whether or not to peer with any particular party will be in DD's sole and unfettered discretion.

Amendments to DD's Peering Policy

DD conducts periodic internal reviews of the Peering Policy to ensure that the criteria for the peering eligibility are consistent with DD's network growth and expansions. DD reserves the right to modify the Peering policy at any time at its sole and unfettered discretion. Based on such modifications, existing peering partners may be asked at times to re-qualify for continued peering.

Peering Criteria

Section one contains the interconnection requirements which the network of a Peering Applicant must-have for the applicant to be eligible for peering with DD. Section two contains the technical and operational requirements that the network of the Peering Applicant must comply with in order to peer with DD. Section three outlines any other general notices.

1. Interconnection Requirements

To determine whether bilateral peering is mutually beneficial in a particular case, the extent of the geographic distribution of the Peering Applicant's network and the volume of traffic to be exchanged between the networks will be the key indicators.

Geographic Scope: The Peering Applicant must operate its own facilities capable of terminating IP connections onto a device in two of IS' nodes, namely Johannesburg, Cape Town. In other words, the Peering Applicant must have a geographically dispersed network.

As an example, any of the following will be accepted:

- NapAfrica JNB and CINX — Johannesburg and Cape Town
- NapAfrica JNB and DINX — Johannesburg and Durban
- NapAfrica CTN and JINX — Cape Town and Johannesburg
- NapAfrica CTN and DINX — Cape Town and Durban

- NapAfrica JNB and NapAfrica CTN — Johannesburg and Cape Town
- NapAfrica JNB and NapAfrica DBN — Johannesburg and Durban
- NapAfrica CTN and NapAfrica DBN — Cape Town and Durban

- JINX and DINX — Johannesburg and Durban
- JINX and CINX — Johannesburg and Cape Town
- DINX and CINX — Durban and Cape Town

NapAfrica - https://www.napafrica.net/

INX - https://ispa.org.za/inx/

The Peering Applicant must be in possession of its own international IP transit bandwidth i.e., it does not get its international IP transit bandwidth from upstream South African providers.

Traffic Exchange Ratio: The ratio of the aggregate amount of traffic to be exchanged between the Peering Applicant and IS shall be balanced and shall not exceed the ratio of 1.5:1.

Backbone Capacity: The Peering Applicant must have a fully redundant backbone network with sufficient bandwidth to carry its own national traffic, which is delivered on an ECNS-provided telco infrastructure and not through a virtual connection with another ISP.

Traffic Volume: The total amount of traffic exchanged in each direction over all interconnection links between the Peering Applicant and IS will equal or exceed 600 Mbps of traffic for either private or public peering.

ISPA Membership: The Peering Applicant must preferably be a member of the Internet Service Providers Association (ISPA).

Customer Relationship: No Peering Applicant who is an IS transit customer and maintains transit connections with IS at one or more locations shall be entitled to enter into a peering relationship with IS while maintaining such transit connections to IS.

DD will not peer with customers of any of its current peering partners.

2. Technical and Operational Requirements

The following operational requirements apply both to the Peering Applicant and DD:

2.1 Infrastructure and Reporting Requirements

Each Party must operate a fully redundant network, capable of handling a simultaneous single-node outage in each network without significantly affecting the performance of the traffic being exchanged.

Both the Peering Applicant and DD are responsible for monthly graphing and reporting on utilisation. Where average utilisation is measured in excess of 75%, for more than 25 periods of one hour over a period of 5 consecutive days, this will automatically lead to the upgrading of the interconnection bandwidth.

For the purposes of the Traffic Exchange Ratio and Traffic Volume requirements of the Peering Policy, all traffic is to be measured over interconnection links. The traffic to be measured will include only what is being exchanged by the two Parties and their respective customers (excluding any transit traffic) in the specific geographic region for which settlement-free interconnection has been requested.

To troubleshoot routing problems, the peering partner must either provide a "traceroute" gateway and preferably a looking glass or must grant DD Network Operations Engineers telnet (read-only) access to its peering router. This will be used for confirmation of traffic flows, troubleshooting of interconnection-related issues, and auditing purposes

2.2 Routing Requirements

Each Party must set the next hop to be itself, the advertising router of the network.

Each Party will circulate such routes to its transit customers with its own router as the next hop.

Each Party will implement "shortest exit routing" and advertise routes consistent with that policy unless both parties mutually agree otherwise based on special circumstances.

Each Party will restrict its advertisements to non-transit routes originating within the geographic region in which peering has been established and will not announce the received route outside of the region.

DD requires consistent route advertisements at all peering locations.

DD requires that all the BGP peering sessions have the MD5 checksum/ password configured.

All traffic exchanged between DD and the Peering Applicant will occur over the peering connection.

Under normal operating conditions no traffic will be directed via another provider (a third party).

No traffic manipulations (including North-South tunnels) will be permitted. Should such traffic manipulations occur this will constitute a material breach of the Peering Policy and will result in immediate termination.

Parties cannot connect a customer line directly to the peering router.

2.3 General Requirements

Each Party must maintain a fully functional 24x7 Network Operations Centre (NOC) with qualified operations engineers available to address problems, with a defined escalation path.

Both Parties are to take all reasonable steps necessary to limit or stop Denial of Service attacks identified from their respective networks to any customer or other peering partner where this Denial-of-Service traffic passes through or touches the interconnect point(s) between DD and its peering partner.

Both parties must implement reasonable filtering methods to prohibit routing instabilities from leaking out of their respective network.

Each Party must be responsive to unsolicited email and network abuse complaints, as well as routing and security issues, and should provide responses from a knowledgeable operations engineer within two hours.

3. General Policy Notices

As stated under section one the Peering Applicant is required to complete a written Peering Agreement with DD.

The requirements in section one (Interconnection Requirements) must be met before completing the Peering Agreement. The Peering Applicant will provide DD with an official letter confirming that these requirements are met before a Peering Agreement is completed and before DD activates the peering connection.

To be eligible for peering with DD, the Peering Applicant will need to provide DD (subject to the execution of a mutual confidentiality agreement) with:

- A copy of its network topology including its backbone capacity
- A technical specification of its peering interconnection points of presence
- Average utilisation patterns

All requirements of the Peering Policy must continue to be met to continue a settlement-free interconnection relationship. The peering partner's status under this Peering Policy will be evaluated periodically. In the case of a change in ownership or control of a Peering Partner, the status of the peering relationship in terms of the Peering Policy will be evaluated within 30 days of such change.

DD reserves the right to terminate any peering relationship, for violations of the Peering Policy, or as a result of a breach of the Peering Agreement. The Peering Agreement will provide that DD may terminate peering with a Peering Partner with immediate effect for non-compliance with the Peering Policy.

Peering with DD will be subject to DD's Acceptable Use Policy ("AUP").

http://dimensiondata.com/-/media/dimensiondata/pdfs/dimension-data-acceptable-use-policy.pdf

DD reserves the right to terminate any peering relationship, for violations of its AUP by a Peering Partner or any of its customers.

DD reserve the right to set, and/or convert any, and all route filters, and filter types at its sole discretion, to preserve network stability and route sanity. A reasonable effect will be made to notify the peer of the change.