Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: January 8, 2012

G. Bertrand
E. Stephan
France Telecom - Orange
G. Watson
T. Burbridge
P. Eardley
BT
K. Ma
Azuki Systems

July 7, 2011

Use Cases for Content Delivery Network Interconnection
draft-bertrand-cdni-use-cases-02

Abstract

Content Delivery Networks (CDNs) are commonly used for improving the footprint and the end-user experience of a content delivery service, at a reasonable cost. This document outlines real world use-cases (not technical solutions) for interconnecting CDNs. It provides the business motivations for CDNI Working Group, which can be used to validate different interconnection arrangements, and requirements of the various CDNI interfaces.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 8, 2012.

Table of Contents

1. Introduction

This document now merges input from [I-D.watson-cdni-use-cases] and [I-D.ma-cdni-publisher-use-cases].

Content Delivery Networks (CDNs) are commonly used for improving the footprint and the end-user experience of a content delivery service, at a reasonable cost. This document outlines real world use-cases (not technical solutions) for interconnecting CDNs. It provides the business motivations for CDNI Working Group, which can be used to validate different interconnection arrangements, and requirements of the various CDNI interfaces.

There are many possible combinations for the relationships between the different parties (Network Service Provider (NSP), CDN Provider, Content Service Provider (CSP) and End User) involved in end-to-end content delivery. However, in the context of interconnecting CDNs the key relationships are listed below.

- How the CSP interacts with the CDN provider, so that the CDN delivers content in a manner compliant with CSP's distribution policies.
- How the End User interacts with the CSP and one or more CDNs to request and receive content.
- How the different CDN providers, operating their CDNs, interact with one another to deliver the CSP's content to the End User while continuing to enforce the CSP's distribution policies.

This document describes a number of use cases that motivate CDN Interconnection.

1.1. Terminology

We adopt the terminology described in [I-D.jenkins-cdni-problem-statement], [RFC3466], and [RFC3568], except for the terms defined below.

CDN Provider:

An administrative entity who operates a CDN over a NSP or over the Internet.

Authoritative CDN (aCDN):

A CDN provider contracted by the CSP for delivery of content by its CDN or by its downstream CDNs.

Downstream CDN (dCDN):

A CDN provider which is contracted by an uCDN to achieve the delivery of content to users.

Access CDN:

A CDN that is connected to the end-user's access and has information about the end-user's profile and access capabilities.

Delivering CDN:

The CDN that delivers the requested content asset to the end-user. In particular, the delivering CDN can be an access CDN.

CDN Interconnection (CDNI):

Relationship between two CDNs that enables a CDN to provide content delivery services on behalf of another CDN. It relies on a set of interfaces over which two CDNs communicate in order to achieve the delivery of content to end-users by one CDN (the downstream CDN) on behalf of another CDN (the upstream CDN).

CDN peering: A business relation between two CDN providers based on one or more CDN interconnections.

Recursive request routing:

Recursive: Where a process is repeated, but embedded within the original process. In the case of Request Routing, this means that the initial request received by the Authoritative CDN is processed downstream from one CDN to another and that the responses are send back upstream to the Authoritative CDN which then replies to the initial request.

Iterative request routing

Iterative: Where a process is repeated multiple times to make progress towards a goal. In the case of Request Routing, this means that the initial request is received by the Authoritative CDN, which replies it with a redirection directive to a downstream CDN. When the end-user sends its request to the downstream CDN, the same process is repeated, until the request arrives to the delivering CDN.

Asymmetric Distribution:

A distribution scenario where different NSPs have distribution rights to the same content, but at different levels of quality (e.g., high

definition vs. low definition video), which places restrictions on delivery delegation.

1.2. Abbreviations

[Ed. Note: List of abbreviations to be updated later]

- CSP: Content Service Provider
- dCDN: downstream CDN
- ISP: Internet Service Provider
- NSP: Network Service Provider
- PC: Personal Computer
- QoE: Quality of Experience
- QoS: Quality of Service
- SLA: Service Level Agreement
- STB: Set-Top-Box
- uCDN: upstream CDN
- UA: User Agent
- UE: User Equipment
- VoD: Video on Demand
- WiFi: Wireless Fidelity

1.3. High Level Use Cases for Multi-CDN Systems

Content Delivery Networks (CDNs) are used to deliver content because they can:

- improve the experience for the End User; for instance delivery has lower latency and better robustness,
- reduce the operator's costs; for instance lower delivery cost (reduced bandwidth usage) for cacheable content,
- reduce the Content Service Provider costs, such as datacenter capacity, space, and electricity consumption.

Indeed, many network service providers and enterprise service providers are deploying or have deployed their own CDNs. Despite the potential benefits of interconnecting CDNs, today each CDN is a standalone network. The objective of CDN interconnection is to overcome this restriction: the interconnected CDNs should be able to collectively behave as a single delivery infrastructure.

Let's take an example, as depicted in Figure 1. Two CDN Providers establish a CDN Interconnect. The Content Service Provider CSP-1 reaches an agreement with CDN Provider A for the delivery of its content. CDN Provider A and CDN Provider B agree to interconnect their CDNs. When a User Agent that is connected to CDN Provider B's network requests Content from CSP-1, the Content is actually delivered from CDN-B, because handling of requests for CSP-1's Content has been delegated as part of the CDN Interconnect agreement. The End User benefits through a better quality of experience, because the Content is delivered from a nearby Surrogate. CDN Provider A benefits because it doesn't need to deploy such an extensive CDN, whilst CDN Provider B receives some compensation for the delivery. CSP-1 benefits because it only needs to make one business agreement and one physical connection, with CDN Provider A, but its End Users get a service quality as though it had also gone to the trouble of making a business agreement with CDN Provider B.

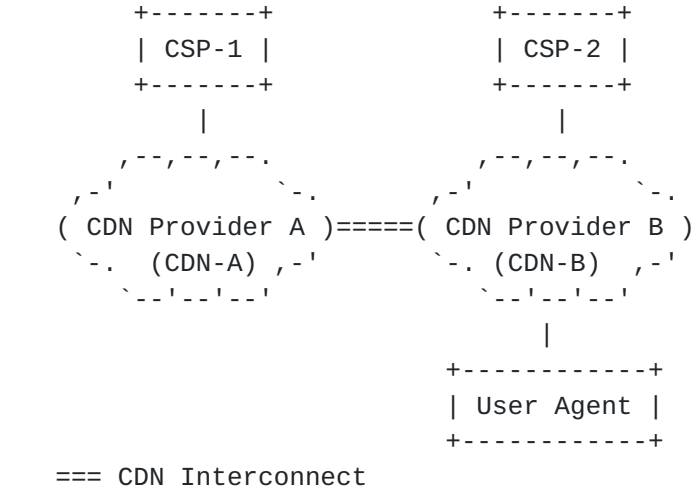

Figure 1

To extend the example, another Content Service Provider, CSP-3, may also reach an agreement with CDN Provider A. But it does not want its Content to be distributed by CDN Provider B, for example, CSP-3 may not have distribution rights in the country where CDN Provider B operates. This example illustrates that policy considerations are an

important part of CDNI.

This document identifies three main motivations for a CDN Provider to interconnect its CDN:

- CDN Footprint Extension Use Cases (Section 2)
- CDN Offload Use Cases (Section 3)
- CDN Capability Use Cases (Section 4)

1.4. The Need for CDNI Standards

Existing CDN interfaces are proprietary and an external CDN typically cannot use them, especially if the two CDNs rely on different solutions. Nevertheless, [I-D.bertrand-cdni-experiments] shows that some level of CDN interconnection can be achieved experimentally without standardized interfaces between the CDNs. The methods used in these experiments are hardly usable in an operational context, because they suffer from several limitations in terms of functionalities, scalability, and security level.

The aim of the CDNI standards work is therefore to overcome such shortcomings; a full list of requirements is being developed in [I-D.lefaucheur-cdni-requirements].

2. Footprint Extension Use Cases

Footprint extension is expected to be a major use case for CDN interconnection.

2.1. Geographic Extension

In this use case, the CDN Provider wants to extend the geographic distribution that it can offer CSPs, without

- compromising the quality of delivery
- attracting transit and other network costs by serving from geographically or topologically remote surrogates.

If there are several CDN Providers that have a geographically limited footprint (e.g., restricted to one country), or do not serve all end-users in a geographic area, then interconnecting their CDNs enables CDN Providers to provide their services beyond their own footprint.

As an example, suppose a French CSP wants to distribute its TV

programs to End Users located in various countries in Europe and North Africa. It asks a French CDN Provider to deliver the content. The French CDN Provider's network only covers France, so it makes an agreement with another CDN Provider that covers North Africa. Overall, from the CSP's perspective the French CDN Provider provides a CDN service for both France and North Africa.

In addition to video, this use case applies to other types of content such as automatic software updates (browser updates, operating system patches, virus database update, etc).

2.2. Region to Region Interconnection

In the previous section, we have described the case of geographic extension between CDNs operated by different entities. A large CDN Provider may also operate CDNs from several subsidiaries (which may rely on different CDN solutions, see Section 4.2). In certain circumstances, the CDN Provider needs to make its CDNs interoperate to provide a consistent service to its customers on its whole footprint.

2.3. Nomadic Users

In this scenario a CSP wishes to allow users who move to other geographic regions to continue to access their content. The motivation in this case is to allow nomadic users to maintain access, rather than to allow all residents within a region access to the content.

This use case covers situations like users moving between different CDN Providers within the same geographic region, or users switching between different devices, as discussed in Section 4.

2.4. Delivery Restrictions

The content distribution policies that a CSP attaches to a content asset depend on many criteria. Distribution rights for audiovisual content are often negotiated using a combination of temporal licensing (e.g., available for 24 hours, available 28 days after DVD release, etc.), resolution-based licensing (e.g., high definition vs. standard definition), and geo- location-based licensing (e.g., per country).

"Geo-blocking" rules may specify:

- the geographic regions where content can be delivered from (i.e. the location of the Surrogates), or

- geographic locations where content can be delivered to (i.e., the location of the End Users).

Hence, the exchange through the CDN interconnection of information for controlling the footprint of the delivery is an important use case.

The delivery of content may be further influenced by policies which may include time-based rules that specify:

- an activation time (i.e., the time when the content should become available for delivery),
- a deactivation time (i.e., time after which the content should no longer be delivered), or
- an expiration time (i.e., the time at which the content files should be expunged from all CDN storage).

The delivery of content may be further influenced by policies which may include quality of service rules that specify:

- the maximum resolution deliverable to specific devices,
- the maximum resolution deliverable though a specific NSP, or
- the maximum resolution deliverable to users based on their subscription levels.

The enforcement of CSP licensing rules when making CDN delegation decisions is another important use case for CDN interconnection.

3. Offload Use Cases

3.1. Overload Handling and Dimensioning

A CDN is likely to be dimensioned to support the prime-time traffic. However, unexpected spikes in content popularity may drive load beyond the expected peak. The prime recurrent time peaks of content distribution may differ between two CDNs. Taking advantage of the different traffic peak times, a CDN may interconnect with another CDN to increase its effective capacity during the peak of traffic. This brings dimensioning savings to the CDNs as they can use the resources of each other during their peaks of activity.

Offload also applies to planned situations where a CDN Provider needs CDN capacities in a particular region during a short period of time.

For example, a CDN can offload traffic to another CDN during a specific maintenance operation or for covering the distribution of a special event. For instance, consider a TV-channel which has exclusive distribution rights on a major event, such as a celebrities' wedding, or a major sport competitions. The CDNs that the TV-channel uses for delivering the content related to this event are likely to experience a flash crowd during the event and to need offloading traffic, while other CDNs will support a more usual traffic load and be able to handle the offloaded traffic load.

3.2. Resiliency

3.2.1. Failure of Content Delivery Resources

It is important for CDNs to be able to guarantee service continuity during partial failures (e.g., failure of some Surrogates). In partial failure scenarios, a CDN Provider could redirect some requests towards another CDN, which must be able to serve the redirected requests or, depending on traffic management policies, to forward these requests to the CSP's origin server.

3.2.2. Failure of Content Acquisition

Source content acquisition is typically handled in one of two ways:

- CDN origin, where a downstream CDN acquires content from an upstream CDN, and the authoritative CDN acquires content from an origin server of the CSP, or

- CSP origin, where the CDNs acquire content directly from an origin server of the CSP.

Resiliency may be required against failure to ingest content from the CSP. If a CDN is unable to retrieve the content, it may be that the CSP's origin server is inaccessible to only this CDN, in which case redirection of the end-users to an alternative CDN may circumvent the problem. A CSP may also choose to specify one or more backup origin servers.

3.3. Branding Consideration

There are situations where one CDN Provider cannot or does not want to operate all the functions of a CDN. For instance, it always acts as an uCDN and offloads the content delivery to dCDNs, i.e., it uses the surrogates of other CDSPs. In this model, the uCDN acquires content and receives the initial routing requests from the user agent; whereas, the dCDNs operate the content delivery functions. The uCDN also retrieves and presents the logging for the CSP.

Preserving branding elements could interest the CSP or CDSPs. The CSP might desire to offer content services under its name, even if the associated CDN service involves other organizations. Therefore, the CSP could request that the name of the CDSPs does not appear in the URLs. Similarly, in offload situations, the uCDN might want to offer CDN services under its own branding. This highlight a requirement for exchanging branding related constraints over a CDNI.

4. CDN Capability Use Cases

4.1. Device and Network Technology Extension

In this use case, the CDN Provider may have the right geographic footprint, but wishes to support the delivery of content to alternative devices, such as smartphones connected to a mobile network. In this case, the CDN Provider may federate with another CDN Provider that offers service to these devices.

Consider the scenario shown in Figure 2. In this example, a nomadic user switches from a TV going through a cable provider to a smartphone going through a mobile operator. The CDN Provider on the cable network may wish to delegate delivery of Content to the CDN Provider on the mobile network. There are several possible differences that may arise in this use case compared with the ones discussed earlier, for example:

- the phone may require the Content at lower resolution than the TV;
- the CSP may want to license only lower resolution Content to CDN Provider 2;
- the CSP may not want CDN Provider 2 to deliver Content if the connection quality is below some threshold;
- the CSP may want to tailor the Content in some special way depending on whether the End User is on cable or mobile, for example, different adverts / DRMs / codecs / container formats / delivery protocols...

These examples suggest the requirement for Asymmetric Distribution of Content across the CDN interconnect. In the nomadic scenario, the switch of CDN should be as seamless as possible from the End User's perspective.

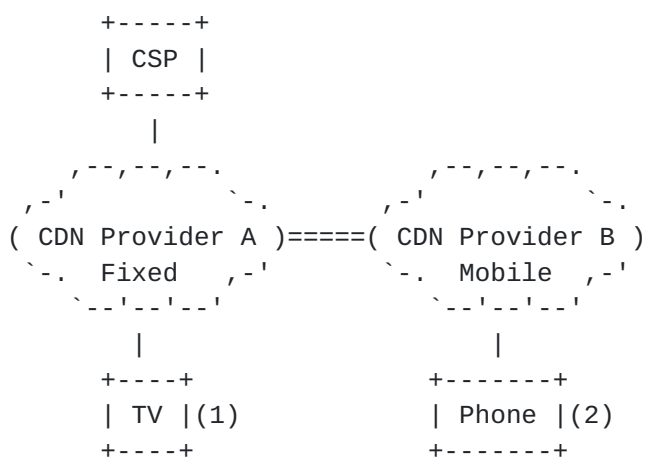

Figure 2

4.2. Technology and Vendor Interoperability

A CDN Provider may deploy a new CDN to run alongside its existing CDN, as a simple way of migrating its CDN service to a new technology. A CDN Provider may have a multi-vendor strategy for its CDN deployment. A CDN Provider may want to deploy a separate CDN for a particular CSP or a specific network. In all these circumstances, CDNI benefits the CDN Provider, as it simplifies or automates some inter-CDN operations (e.g., migrating the request routing function progressively).

4.3. QoE and QoS Improvement

Some CSPs are willing to pay a premium for enhanced delivery of Content to their End Users. In some cases, even if the CDN Provider could deliver the content to the end users, it cannot meet the CSP's service level agreement. So, it makes a CDN Interconnect agreement with another CDN Provider that can meet the SLA, for instance an Access CDN, which is able to deliver content from Surrogates located closer to the end-user.

5. Acknowledgments

The authors would like to thank Francois Le Faucheur and Ben Niven-Jenkins for lively discussions.

They also thank the contributors of the EU FP7 OCEAN and ETICS projects for valuable inputs.

6. IANA Considerations

This memo includes no request to IANA.

7. Security Considerations

CDN interconnect, as described in this document, has a wide variety of security issues that should be considered. The security issues fall into three general categories:

- CSP Trust: where the CSP may have negotiated service level agreements for delivery quality of service with the uCDN, and/or configured distribution policies (e.g., geo-restrictions, availability windows, or other licensing restrictions), which it assumes will be upheld by dCDNs to which the uCDN delegates requests. Furthermore, billing and accounting information must be aggregated from dCDNs with which the CSP may have no direct business relationship. These situtations where trust is delegated must be handled in a secure fashion to ensure CSP confidence in the CDN interconnection.

- Client Transparency: where the client device or application which connects to the CDN must be able to interact with any dCDN using its existing security and DRM protocols (e.g., cookies, certificate-based authentication, custom DRM protocols, URL signing algorithms, etc.) in a transparent fashion.

- CDN Infrastructure Protection: where the dCDNs must be able to identify and validate delegated requests, in order to prevent unauthorized use of the network and to be able to properly bill for delivered content. A dCDN may not wish to advertise that it has access to or is carrying content for the uCDN or CSP, especially if that information may be used to enhance denial of service attacks. In general, CDNI interfaces and protocols should minimize overhead for dCDNs.

This document focuses on the motivational use cases for CDN interconnect, and does not analyze these threats in detail.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2. Informative References

[I-D.bertrand-cdni-experiments]
Bertrand, G., Faucheur, F., and L. Peterson, "Content Distribution Network Interconnection (CDNI) Experiments", draft-bertrand-cdni-experiments-00 (work in progress), February 2011.

[I-D.jenkins-cdni-problem-statement]
Niven-Jenkins, B., Faucheur, F., and N. Bitar, "Content Distribution Network Interconnection (CDNI) Problem Statement", draft-jenkins-cdni-problem-statement-02 (work in progress), March 2011.

[I-D.lefaucheur-cdni-requirements]
Faucheur, F., Viveganandhan, M., Watson, G., and Y. Lee, "Content Distribution Network Interconnection (CDNI) Requirements", draft-lefaucheur-cdni-requirements-01 (work in progress), March 2011.

[I-D.ma-cdni-publisher-use-cases]
Nair, R. and K. Ma, "Content Distribution Network Interconnection (CDNI) Publisher Use", draft-ma-cdni-publisher-use-cases-00 (work in progress), March 2011.

[I-D.watson-cdni-use-cases]
Watson, G., "CDN Interconnect Use Cases", draft-watson-cdni-use-cases-00 (work in progress), January 2011.

[RFC3466] Day, M., Cain, B., Tomlinson, G., and P. Rzewski, "A Model for Content Internetworking (CDI)", RFC 3466, February 2003.

[RFC3568] Barbir, A., Cain, B., Nair, R., and O. Spatscheck, "Known Content Network (CN) Request-Routing Mechanisms", RFC 3568, July 2003.

Authors' Addresses

Gilles Bertrand
France Telecom - Orange
38-40 rue du General Leclerc
Issy les Moulineaux, 92130
FR

Phone: +33 1 45 29 89 46
Email: gilles.bertrand@orange-ftgroup.com

Stephan Emile
France Telecom - Orange
2 avenue Pierre Marzin
Lannion F-22307
France

Email: emile.stephan@orange-ftgroup.com

Grant Watson
BT
pp GDC 1 PP14, Orion Building, Adastral Park, Martlesham
Ipswich, IP5 3RE
UK

Email: grant.watson@bt.com

Trevor Burbridge
BT
B54 Room 70, Adastral Park, Martlesham
Ipswich, IP5 3RE
UK

Email: trevor.burbridge@bt.com

Philip Eardley
BT
B54 Room 77, Adastral Park, Martlesham
Ipswich, IP5 3RE
UK

Email: philip.eardley@bt.com

Kevin Ma
Azuki Systems
43 Nagog Park
Acton, MA 01720
USA

Phone: +1 978 844 5100
Email: kevin.ma@azukisystems.com