CDN INTEROPERABILITY
DEFINING STANDARDS THAT CAN INCREASE MARKET REACH AND UNLOCK NEW MONETIZATION OPPORTUNITIES
STRATEGIC WHITE PAPER

The rapid growth of over-the-top (OTT) video and multiscreen pay TV services has prompted network service providers to make significant investments in their infrastructure. Increasingly, these investments include deployment of content delivery networks (CDNs) that can take advantage of service providers’ vital network assets. These on-net CDNs push content closer to subscribers, helping service providers optimize bandwidth usage, improve quality of experience (QoE) and gain access to new revenue opportunities.

With the rise of on-net CDNs, CDN interoperability has emerged as a strategically important concept and topic of discussion for service providers and the larger content industry. CDN interoperability offers a means for service providers to expand their CDN footprint to reach new markets and regions and support nomadic users. Interoperability can also enable them to offload traffic to cover demand surges, peak periods and service outages, or to add functionality to a less capable existing CDN.

This white paper explores the important aspects of CDN interoperability, focusing on key concepts relating to CDN federation and interconnection. It describes key use cases, technical requirements and standardization efforts that are driving progress toward fully interoperable on-net CDNs.
# TABLE OF CONTENTS

Introduction / 1  
The challenges of CDN ownership / 1  
The quest for interoperability / 3  

Use cases and scenarios / 3  
Footprint extension / 3  
Traffic offload / 5  

Requirements for CDN interconnection / 7  
Building blocks and functions / 7  
CDNI touch points / 8  

Standards organizations and CDNI / 11  
Internet Engineering Task Force (IETF) / 11  
Other standards organizations / 12  

Alcatel-Lucent and CDN interoperability / 12  
Velocix shared CDN / 12  
Velocix APIs / 13  
Real-world experience in CDN interoperability / 14  

Conclusion / 14  

Acronyms / 15
INTRODUCTION

Consumers are hungry for more media content on every device. But growing consumption is raising pressure on service providers’ fixed and wireless networks. To ensure network performance and maintain an effective network cost base, service providers are deploying content delivery networks (CDNs).

On-net CDNs offer scalable, cost-effective support for a broad range of content delivery capabilities. For example, they can deliver high-volume video traffic, distribute software updates that involve a large number of transactions and accelerate the performance of Web sites and applications. By creating their own CDNs, service providers can minimize the distance that content travels over the network and deliver it more quickly and reliably. As shown in Figure 1, on-net CDNs originate content at the edge of fixed and mobile networks, bringing it closer to consumers. This proximity to consumers helps service providers reduce congestion and disruptions and deliver a consistently superior quality of experience (QoE) to subscribers.

Figure 1. On-net CDNs bring content closer to consumers

CDNs also offer new monetization opportunities to service providers. With their own CDNs in place, service providers can expand and diversify their content offers within unified infrastructures. For example, they can use their own CDNs to deliver licensed content to connected devices. They can generate new revenue by using their CDNs to support wholesale business models. Or they can offer premium content delivery services that make it easy for content providers to publish content directly to their networks.

The challenges of CDN ownership

The prospect of owning and operating CDNs presents compelling opportunities and benefits to service providers. But service providers need to address some key challenges so that they can use their CDNs to make the most of their content delivery opportunities.
For example, today’s on-net CDNs exist as standalone solutions and offer coverage that is typically limited to the service provider’s network footprint. Limited coverage can hinder a service provider’s ability to partner with large content providers and maximize return on CDN assets. Many content providers view on-net CDNs as a means to extend their reach while delivering an assured QoE, as shown in Figure 2A. But they often have to implement complex methods to work with CDNs that expose reporting, billing and control capabilities in different ways. This sort of complexity may prompt content providers to work with a single third-party CDN service instead of working with multiple service provider CDNs — even if it means accepting a best-effort approach to QoE (Figure 2B).

Figure 2. Content providers can extend their audience by working with individual service providers (A) or a third-party CDN service (B)

Service providers also face the challenge of having to offer seamless next-generation digital entertainment services to subscribers across a plethora of connected devices. Increasingly, service providers also feel pressure to offer these services within and beyond their own CDN footprint. Service providers have nomadic users who try to access content and services using other service provider networks. Without agreements, service providers have no way to guarantee QoE outside their own footprint (Figure 3). Service providers need CDN strategies and technologies that can enable them to work together to extend an assured QoE to a larger and more nomadic subscriber base.
The quest for interoperability

The CDN industry has begun exploring strategies to address some of these challenges. In particular, CDN interoperability has emerged as a topic of strategic interest among CDN vendors, third-party CDN services and service providers. This paper explores various aspects of CDN interoperability. It describes some of the key use cases, technical requirements and standardization efforts that are being evaluated and pursued by the CDN industry.

In this paper, the term CDN interconnection (CDNI) refers to the technical aspects of interconnecting two or more CDNs in a single-vendor or multi-vendor environment. The term CDN federation refers to the non-technical business relationships that govern the interconnected CDN. Both terms fall within the broader subject of CDN interoperability.

USE CASES AND SCENARIOS

There are many reasons why a service provider may want to interconnect its CDN with that of another provider. This section examines some of the key use cases and scenarios associated with CDNI. In each instance, the CDNs may operate within single-vendor or multi-vendor network environments. More discrete use cases are possible. These use cases are likely to be functionally or topologically equivalent to those described in this section.

Footprint extension

A service provider can use CDNI to extend its service reach beyond its CDN footprint. This CDN footprint typically maps to the provider’s network footprint. However, the term footprint does not apply solely to physical geography. It can also refer to the reach of a CDN’s content or functionality.
The following examples show how a service provider can use CDNI to increase a CDN’s physical, functional or content footprint. They describe two different bilateral federation use cases, one between two service providers and one between a service provider and a third-party CDN service.

**Bilateral federation — On-net CDN to on-net CDN**

In Figure 4, Service Provider A offers a pay TV service featuring content for which it has distribution rights for a region larger than its CDN footprint. By interconnecting its CDN with that of Service Provider B, Service Provider A can extend its addressable market and offer pay TV services to broadband subscribers outside its own network footprint.

![Figure 4. Using CDNI to reach new or nomadic subscribers](image)

A service provider can also use bilateral federation with other on-net CDNs to ensure a seamless user experience for nomadic subscribers who roam beyond the reach of its network or CDN footprint. In the example shown in Figure 4, Service Provider A can work with Service Provider B to enable subscribers with tablets and smartphones to access digital entertainment assets from public Wi-Fi hotspots and mobile networks.

**Bilateral federation — On-net CDN to third-party CDN service**

Third-party CDN services typically have worldwide content distribution agreements with content providers. However, their CDNs do not offer coverage that extends deep into service provider networks. The traffic sourced from third-party CDN services is served over the top of service provider networks and CDNs.
Figure 5 shows how a third-party CDN service can use interconnection to access the delivery capacity offered by service provider CDNs in specific regions. This added capacity can enable the third-party CDN service to deliver the superior QoE associated with on-net CDNs. It can also reduce the CDN provider’s CAPEX and OPEX by limiting its need for OTT capacity, caches and network connectivity.

Figure 5. A third-party CDN service can improve QoE by caching content in a service provider CDN

Service providers can also benefit from bilateral federation with third-party CDN services. Through interconnection, they can save network costs by reducing the amount of OTT traffic flowing across their backhaul, core network and Internet peering points. In addition, they can protect content providers from the complexity of having to integrate with and choose between several service provider CDNs. This makes them more attractive partners for content providers.

**Traffic offload**

Interconnection can enable service providers to extend their CDN footprint as a means to offload traffic (partially or fully) from their own CDNs. Service providers can use offloading for a variety of reasons — for example, to augment capacity, increase resilience or provide additional functionality to a less capable existing CDN.
Offload for dimensioning
The unpredictable nature of video consumption and usage patterns makes it hard for service providers to scale their networks to address peak demand for unplanned events. Scaling delivery capacity to cope with demand for large sports events, popular live broadcasts and new film releases can be particularly challenging. In service provider networks, it is typically very difficult to deploy high volumes of CDN capacity at short notice or on demand. But deploying high volumes of capacity far in advance of when it is needed skews the CAPEX and OPEX models of service provider CDNs.

Service providers can address these challenges by interconnecting their CDNs with those of other CDN providers. Through interconnection, service providers can seamlessly scale to address very high and potentially unexpected peaks in subscriber demand by offloading traffic to other CDNs as required.

Offload for resilience
CDN availability underpins the user experience for digital entertainment services. Service provider CDNs need the ability to scale so that they can transparently cope with failure scenarios. Although rare, network outages or system failures can reduce the overall delivery capacity of the CDN or make some or all services entirely unavailable. In failure scenarios, service providers can use CDNI to offload delivery to an alternate CDN. Offloading allows service providers to seamlessly (or almost seamlessly) recover from catastrophic failures within their own platforms (Figure 6).

Figure 6. Using CDNI to ensure service and system resilience

Offload for functionality
Many service providers offer digital entertainment services based on their own content or content they distribute on behalf of content providers. These service providers have to cope with a diverse geographic and network footprint to provide access to digital assets wherever subscribers want them. In addition, they need to offer functionality that facilitates delivery to subscribers’ devices or applications of choice.
Service providers may not always have or wish to develop a given delivery technology. A service provider may be constrained by a chosen CDN vendor or technology or may not view the technology as a worthy investment, perhaps because the volume of traffic is too low to justify it. However, a rich depth of functionality and breadth of delivery technology is critical to content providers and has a heavy influence on their CDN partner choices. If a service provider does not offer a specific delivery technology, it can use CDNI to offload certain traffic types or delivery technologies to a CDN that is equipped to support them. For example, a service provider can delegate the delivery of encrypted content to another service provider that supports HTTP Secure (HTTPS) technology.

**REQUIMENTS FOR CDN INTERCONNECTION**

Before adopting strategies that involve CDNI, service providers must ensure that their CDNs include key building blocks and meet key technical requirements.

**Building blocks and functions**

A typical on-net CDN solution includes building blocks that cover functions such as service, storage and delivery. Figure 7 illustrates these key functions.

**Figure 7. The key functions of an on-net CDN**

Service
The CDN’s service function includes management, routing and monitoring components that support the following capabilities:

- Request Routing and Cache Selection: The service function selects the delivery appliance that is most appropriate for delivering a given asset to a given consumer.
- Management: The service function supports management activities that concern content owners. These activities typically relate to services that are directly available to content owners, including reporting, billing and content management.
• Monitoring: The service function monitors the physical aspects of the CDN solution, including the hardware and services that are used to deliver content services.
• Configuration and Deployment: The service function manages the configuration of services within the CDN. It may be responsible for deploying new routing rules, for managing, configuring and setting up accounts for content owners, or for configuring and deploying new CDN appliances and services.

Storage
The storage function provides mechanisms that enable the CDN to ingest or register content. It may include the following components:
• An origin server that packages, stores and originates copies of media objects so that they can be delivered over the CDN
• A shield cache that keeps the origin server from overloading
• Publishing and storage appliances that ingest and store pre-published content

Delivery
The CDN’s delivery function handles the physical delivery of managed or OTT content to consumers. Delivery is typically performed by a caching device or streaming server that supports one or more delivery protocols.

CDNI touch points
To establish and maintain successful interconnections, service providers need to support touch points that can link their key CDN functions with those of other CDNs. These touch points typically take the form of application programming interfaces (APIs), as shown in Figure 8.

Figure 8. CDNI touch points
This section describes some of these touch points and illustrates how they can be used to deliver content from interconnected CDNs. In this section, the term upstream CDN, or uCDN, refers to a CDN that has a relationship with a content provider. The term downstream CDN, or dCDN, refers to a CDN to which a uCDN has elected to redirect end-user requests.

Request routing API
A CDN must have the ability to direct end users to the right delivery appliances in the right locations. Likewise, an interconnected CDN needs a component that can reroute end-user requests from a uCDN to a dCDN if the uCDN elects to do so.

In most CDNs, request routers use Domain Name System (DNS) or application redirection methods (for example, HTTP 302 or RTMP 302) to route end-user content requests to delivery appliances. An interconnected CDN must maintain support for these methods to ensure that its connections with other CDNs remain transparent to end-user devices and clients.

A uCDN can delegate responsibility for delivery based on a variety of different factors. For example, if the end user is outside its network footprint, the uCDN may lack the capacity or ability to deliver content using the requested delivery technology. The uCDN’s decision to reroute to another CDN relies on the ability to share information between CDNs. Once the uCDN has elected to delegate a request to the dCDN, the uCDN must also ask the dCDN what action it would like to take. For example, the uCDN can ask whether the dCDN is able to accept the request. If so, the uCDN can then ask whether to pass the request to the request router within the dCDN or directly to a delivery appliance within the dCDN.

Metadata
Most CDNs are configured with information that enables them to respond to end-users’ requests for content. In an interconnected CDN, the uCDN and dCDN need to be able to share this information so that the dCDN can respond properly to content requests. This information is stored and shared as metadata. It can be shared between CDNs using an API based on standards and protocols such as a Simple Object Access Protocol (SOAP) or Representational State Transfer (REST). The types of information shared between a uCDN and dCDN include:

- Territories or geographies to which the content can be delivered (geo-blocking)
- Signing or tokenization processes that should be applied to the content
- Delivery technologies that should be used to deliver the content (for example, RTMP, RTSP or HTTP)
- Details on where the dCDN should go to acquire the content (for example, the location of the origin server)
- Information on time-based delivery restrictions
Figure 9 shows how request routing and metadata APIs are used in a typical scenario. Here, a subscriber of Service Provider A requests content through a content provider portal. The content provider has an agreement to distribute content using Service Provider B’s CDN. It asks Service Provider B to deliver the content. Since the end user is not one of Service Provider B’s subscribers, the request is passed to Service Provider A. The content is then delivered using Service Provider A’s CDN, ensuring that the end user enjoys a superior QoE.

Logging
The collection of logging data is very important to CDN operators. Logging data provides a detailed record of content delivery, including information on where content was delivered, which content was delivered, what delivery technology was used, how much content was delivered, and how long it took to deliver the content.

Logging data is used for operational and analytical purposes, and to produce accurate billing data. To enable a uCDN to fulfill its operational, analytical and billing requirements, a dCDN must be able to provide accurate logging data in a timely fashion.
Control

Today’s CDNs expose functionality that allows content providers to control what content is stored within the CDN. Many content providers want to be able to purge content from caches, delete content from storage and push content to the CDN, as shown in Figure 10. They view these capabilities as key requirements for working with CDNs.

In an interconnected CDN, the dCDN must provide the uCDN with equivalent control functionality. This functionality can be provided by a control API.

Figure 10. At the content provider’s request, a uCDN asks a dCDN to purge content from caches

STANDARDS ORGANIZATIONS AND CDNI

The growing interest in CDNI has inspired several industry standards organizations to form efforts to solve some of the important technical challenges associated with interoperating CDNs.

Internet Engineering Task Force (IETF)

In 2010, the IETF held a “Birds of a Feather” (BoF) meeting to explore proposals for work on the CDNI concept. With the support of over 100 attendees from service provider and CDN equipment vendor organizations, the IETF formed a CDNI Working Group in June 2011. This working group is focused on creating a CDNI protocol specification.

Alcatel-Lucent has been heavily involved in the IETF’s work on CDNI. Its involvement has included lobbying IETF leadership, playing an integral role in forming the CDNI Working Group and submitting the first proposals for protocol specifications. In addition, Alcatel-Lucent is openly and actively working with operators and competitors to produce interoperability standards. Documents authored by Alcatel-Lucent include:

- CDNI Problem Statement
- CDNI Metadata
- CDNI Control Triggers
- Framework for Naming and Referencing of Data Objects in CDNI
- CDNI Use Cases
Other relevant and notable documents include:
- CDNI Framework
- CDNI Requirements

Further information about the IETF CDNI Working Group and its associated documentation can be found at the following locations:
- IETF CDNI Documents: http://datatracker.ietf.org/wg/cdni/

Other standards organizations

Other standards organizations are researching and authoring proposals for standardized CDNI technology. These organizations include the Alliance for Telecommunications Industry Standards (ATIS) IPTV Interoperability Forum (IIF), the ATIS Cloud Services Forum (CSF) and the European Technical Standards Institute (ETSI). These organizations are focusing on authoring architectural proposals for CDNI. The IETF specifications are generally referenced wherever detailed protocol specifications are required.

ALCATEL-LUCENT AND CDN INTEROPERABILITY

With the Velocix CDN, Alcatel-Lucent is leading the CDN industry toward broader adoption of the CDN interoperability concept. For example, Alcatel-Lucent is already leveraging Velocix CDN features and APIs to provide customers with shared CDN deployments that support technical interconnection and business model federation.

Velocix shared CDN

Alcatel-Lucent has deployed shared CDNs in a commercial production environment. This deployment scenario, illustrated in Figure 11, leverages multi-tenancy capabilities already provided by the Velocix solution. Alcatel-Lucent can supply all service functions — request routing, cache selection, management, monitoring, configuration and deployment — as an optional managed service. Alternatively, these service functions can be provided by one of the service providers. Storage functions (origin server, storage and publishing) can be hosted by Alcatel-Lucent or the service providers. Each service provider has control of its own CDN customer base and all delivery functions. At the same time, each service provider can share the benefits of content delivery that is common to all.

Figure 11. The Velocix shared CDN in a production environment
The Velocix CDN uses multiple administrative layers to support a flexible approach to a shared CDN. As shown in Figure 12, the solution can establish a scheme to generate virtual CDNs that share the same delivery appliances. Each virtual CDN can configure separate accounts for different customers. Each customer, in turn, can configure separate accounts for different services. These flexible hierarchies can scale readily to support scenarios that include many virtual CDNs, customers, services, publishers and objects.

![Figure 12. Velocix shared CDN hierarchy](image)

The Velocix CDN offers a rich role-based administrative model that complements support for shared virtual CDN, customer and service hierarchies. This model allows service providers to control administrative access between virtual CDN domains, customers and services.

**Velocix APIs**

The Velocix CDN offers a broad range of extensible, flexible and openly available APIs. Service providers can use these APIs to support many different use cases, including the shared CDN scenario described in the preceding section, and to gain experience with the principles of CDN interconnection and federation. The Velocix CDN includes the following APIs:

- **Velocix Server Side Cache Selection API**: This API enables external systems to request cache selection information. Systems can receive request routing information from this API by passing it a parameter such as an end-user IP address. The response includes the best cache to use. Content providers and service providers can use this API in a variety of ways — for example, to build applications that construct playlists or to provide a CDN selector with request routing instructions.

- **Velocix Provisioning API**: This API enables external systems to manage (create, delete and modify) resources such as Web sites, origins and users within the CDN. In shared CDN deployments, it allows content and service providers to use their own management systems to provision services on the Velocix CDN.

- **Velocix Publishing & Acquisition API**: This API enables content and service providers to publish assets directly to the CDN using a broad range of industry-standard publishing protocols. Supported protocols include Aspera, rsync, FTP, SFTP, HTTP PUT/PUSH, XML-RPC pre-publish over SSL, and reverse proxy to external origin servers.

- **Velocix Authorization API**: This API allows service providers to use an external authorization server to authorize requests for content and influence how the content is delivered. In a shared CDN scenario, for example, the dCDN may make requests to an authorization server to understand how it should respond to requests delegated by the uCDN, such as requests for encryption keys.
• Velocix Control API: This API allows a content or service provider to control Web site objects by way of a programmatic interface. For example, a content provider can flush or delete objects from the Velocix CDN, either to remove invalid objects or to ensure that the CDN has the most current version of a given object.

• Velocix Reporting API: This API provides an Atom-based interface that gives service and content providers programmatic access to CDN logging data and event-based reporting capabilities. Reports can be filtered in the Velocix CDN to provide output relevant to specific users within service or content provider organizations.

These APIs provide a foundation for meeting the requirements set out by the CDN interoperability standards. They will achieve full alignment with these requirements once the standards are finalized. Alcatel-Lucent offers detailed documentation for all of the Velocix APIs.

**Real-world experience in CDN interoperability**

Alcatel-Lucent has wide-reaching real-world experience with CDN interoperability. The company has worked with service providers to establish federated CDN solutions in a variety of scenarios, including:

- Shared Velocix CDN deployment: Alcatel-Lucent uses the Velocix CDN’s rich multi-tenant functionality to support CDN federation between two major North American cable service providers. These service providers use multi-tenant functions such as granular role-based access and logical customer separation to deliver video to subscribers. Both providers have benefited from reduced CAPEX and OPEX.

- Velocix single-vendor CDN interoperability: Alcatel-Lucent has successfully demonstrated its ability to support CDN interconnection between two autonomous Velocix CDNs deployed in a trial environment for two tier 1 service providers with global operations.

- Velocix multi-vendor CDN interoperability: Alcatel-Lucent has successfully demonstrated its ability to support CDN interconnection between two autonomous CDNs from different vendors in a trial environment. This trial used a Velocix deployment as the dCDN. For the uCDN, it used a live production environment owned by a tier 1 service provider with global operations. The Velocix CDN was able to accept delegated content requests and acquire content from the uCDN.

**CONCLUSION**

The market for CDN interoperability is still in the early stages of development. Service providers’ strategies for CDN federation and interconnection are not yet fully formed. However, increasing interest across the industry — from service providers, third-party CDN services, CDN equipment vendors and standards organizations — makes it clear that CDN interoperability could have a positive effect on the CDN market. By deploying their own on-net CDNs, service providers can capitalize on this growing momentum.

CDN interoperability enables service providers to leverage standardized interfaces as a means to work with other CDN operators and expand their CDN footprint. Greater interoperability will help make service provider-owned CDNs more attractive and easier to manage for content providers.
By leveraging new CDNI technologies, service providers will be able to build highly scalable federated CDNs with broad-ranging feature sets, device support capabilities and geographic footprints. This will enable service providers to leverage new wholesale business models, either through federation with one or many service provider CDNs or through federation with traditional third-party CDN services. As technologies and standards advance and become available for wider multi-vendor deployments, the mutual benefit of forming federated CDN businesses between service and content providers will drive development of increasingly mature interoperability strategies.

ACRONYMS

API Application programming interface
ATIS Alliance for Telecommunications Industry Solutions
CDN Content delivery network
CDNI CDN interconnection
CSF Cloud Services Forum
dCDN Downstream CDN
DNS Domain Name System
ETSI European Telecommunications Standards Institute
FTP File Transfer Protocol
HDTV High-definition television
HTTP Hypertext transfer protocol
HTTPS HTTP Secure
IETF Internet Engineering Task Force
IIF IPTV Interoperability Forum
IPTV Internet Protocol Television
OTT Over the top
QoE Quality of experience
REST Representational state transfer
RTMP Real Time Messaging Protocol
RTSP Real Time Streaming Protocol
SFTP SSH File Transfer Protocol
SSH Secure Shell protocol
SOAP Simple Object Access Protocol
uCDN Upstream CDN
XML-RPC XML remote procedure call protocol