Network Working Group
Request for Comments: 3570
Category: Informational

P. Rzewski
Media Publisher, Inc.
M. Day
Cisco
D. Gilletti
July 2003

Content Internetworking (CDI) Scenarios

Status of this Memo

Copyright Notice

Abstract

In describing content internetworking as a technology targeted for use in production networks, it is useful to provide examples of the sequence of events that may occur when two content networks decide to interconnect. The scenarios presented here seek to provide some concrete examples of what content internetworking is, and also to provide a basis for evaluating content internetworking proposals.

Table of Contents

1. Introduction....2
   1.1. Terminology....3
2. Special Cases of Content Networks....3
   2.1. Publishing Content Network....3
   2.2. Brokering Content Network....3
   2.3. Local Request-Routing Content Network....4
3. Content Internetworking Arrangements....5
4. Content Internetworking Scenarios....5
   4.1. General Content Internetworking....6
   4.2. BCN providing ACCOUNTING INTERNETWORKING and REQUEST-ROUTING INTERNETWORKING....9
   4.3. BCN providing ACCOUNTING INTERNETWORKING....11
   4.4. PCN ENLISTS multiple CNs....12
   4.5. Multiple CNs ENLIST LCN....13
5. Security Considerations....15
   5.1. Threats to Content Internetworking....15
      5.1.1. Threats to the CLIENT....15

5.1.2. Threats to the PUBLISHER.....17
5.1.3. Threats to a CN.....17
6. Acknowledgements.....18
7. References.....18
8. Authors' Addresses.....19
9. Full Copyright Statement.....20

1. Introduction

In [1], the concept of a "content network" is introduced and described. In addition to describing some general types of content networks, it also describes motivations for allowing content networks to interconnect (defined as "content internetworking").

In describing content internetworking as a technology targeted for use in production networks, it's useful to provide examples of the sequence of events that may occur when two content networks decide to interconnect. Naturally, different types of content networks may be created due to different business motivations, and so many combinations are likely.

This document first provides detailed examples of special cases of content networks that are specifically designed to participate in content internetworking (Section 2). We then discuss the steps that would be taken in order to "bring up" or "tear down" a content internetworking arrangement (Section 3). Next we provide some detailed examples of how content networks (such as those from Section 2) could interconnect (Section 4). Finally, we describe any security considerations that arise specifically from the examples presented here (Section 5).

The scenarios presented here answer two distinct needs:

1. To provide some concrete examples of what content internetworking is, and

2. To provide a basis for evaluating content internetworking proposals.

A number of content internetworking systems have been implemented, but there are few published descriptions. One such description is [2].

1.1. Terminology

Terms in ALL CAPS are defined in [1] except for the following terms defined below in this document: PCN, BCN, and LCN. Additionally, the term SLA is used as an abbreviation for Service Level Agreement.

2. Special Cases of Content Networks

A CN may have REQUEST-ROUTING, DISTRIBUTION, and ACCOUNTING interfaces. However, some participating networks may gravitate toward particular subsets of the CONTENT INTERNETWORKING interfaces. Others may be seen differently in terms of how they relate to their CLIENT bases. This section describes these refined cases of the general CN case so they may be available for easier reference in the further development of CONTENT INTERNETWORKING scenarios. The special cases described are the Publishing Content Network, the Brokering Content Network, and the Local Request-Routing Content Network.

2.1. Publishing Content Network

A Publishing Content Network (PCN), maintained by a PUBLISHER, contains an ORIGIN and has a NEGOTIATED RELATIONSHIP with two or more CNs. A PCN may contain SURROGATES for the benefit of serving some CONTENT REQUESTS locally, but does not intend to allow its SURROGATES to serve CONTENT on behalf of other PUBLISHERS.

Several implications follow from knowing that a particular CN is a PCN. First, the PCN contains the AUTHORITATIVE REQUEST-ROUTING SYSTEM for the PUBLISHER's CONTENT. This arrangement allows the PUBLISHER to determine the distribution of CONTENT REQUESTS among ENLISTED CNs. Second, it implies that the PCN need only participate in a subset of CONTENT INTERNETWORKING. For example, a PCN's DISTRIBUTION INTERNETWORKING SYSTEM need only be able to receive DISTRIBUTION ADVERTISEMENTS, it need not send them. Similarly, a PCN's REQUEST-ROUTING INTERNETWORKING SYSTEM has no reason to send AREA ADVERTISEMENTS. Finally, a PCN's ACCOUNTING INTERNETWORKING SYSTEM need only be able to receive ACCOUNTING data, it need not send it.

2.2. Brokering Content Network

A Brokering Content Network (BCN) is a network that does not operate its own SURROGATES. Instead, a BCN operates only CIGs as a service on behalf other CNs. A BCN may therefore be regarded as a "clearinghouse" for CONTENT INTERNETWORKING information.

For example, a BCN may choose to participate in DISTRIBUTION INTERNETWORKING and/or REQUEST-ROUTING INTERNETWORKING in order to aggregate ADVERTISEMENTS from one set of CNs into a single update stream for the benefit of other CNs. To name a single specific example, a BCN could aggregate CONTENT SIGNALS from CNs that represent PUBLISHERS into a single update stream for the benefit of CNs that contain SURROGATES. A BCN may also choose to participate in

ACCOUNTING INTERNETWORKING in order to aggregate utilization data from several CNs into combined reports for CNs that represent PUBLISHERS.

This definition of a BCN implies that a BCN's CIGs would implement the sending and/or receiving of any combination of ADVERTISEMENTS and ACCOUNTING data as is necessary to provide desired services to other CONTENT NETWORKS. For example, if a BCN is only interested in aggregating ACCOUNTING data on behalf of other CNs, it would only need to have an ACCOUNTING INTERNETWORKING interface on its CIGs.

2.3. Local Request-Routing Content Network

Another type of CN is the Local Request-Routing CONTENT NETWORK (LCN). An LCN is defined as a type of network where CLIENTS' CONTENT REQUESTS are always handled by some local SERVER (such as a caching proxy [1]). In this context, "local" is taken to mean that both the CLIENT and SERVER are within the same administrative domain, and there is an administrative motivation for forcing the local mapping. This type of arrangement is common in enterprises where all CONTENT REQUESTS must be directed through a local SERVER for access control purposes.

As implied by the name, the LCN creates an exception to the rule that there is a single AUTHORITATIVE REQUEST-ROUTING SYSTEM for a particular item of CONTENT. By directing CONTENT REQUESTS through the local SERVER, CONTENT RESPONSES may be given to CLIENTS without first referring to the AUTHORITATIVE REQUEST-ROUTING SYSTEM. Knowing this to be true, other CNs may seek a NEGOTIATED RELATIONSHIP with an LCN in order to perform DISTRIBUTION into the LCN and receive ACCOUNTING data from it. Note that once SERVERS participate in DISTRIBUTION INTERNETWORKING and ACCOUNTING INTERNETWORKING, they effectively take on the role of SURROGATES. However, an LCN would not intend to allow its SURROGATES to be accessed by non-local CLIENTS.

This set of assumptions implies multiple things about the LCN's CONTENT INTERNETWORKING relationships. First, it is implied that the LCN's DISTRIBUTION INTERNETWORKING SYSTEM need only be able to send DISTRIBUTION ADVERTISEMENTS, it need not receive them. Second, it is implied that an LCN's ACCOUNTING INTERNETWORKING SYSTEM need only be able to send ACCOUNTING data, it need not receive it. Finally, due to the locally defined REQUEST-ROUTING, the LCN would not participate in REQUEST-ROUTING INTERNETWORKING.

3. Content Internetworking Arrangements

When the controlling interests of two CNs decide to interconnect their respective networks (such as for business reasons), it is expected that multiple steps would need to occur.

The first step would be the creation of a NEGOTIATED RELATIONSHIP. This relationship would most likely take the form of a legal document that describes the services to be provided, cost of services, SLAs, and other stipulations. For example, if an ORIGINATING CN wished to leverage another CN's reach into a particular country, this would be laid out in the NEGOTIATED RELATIONSHIP.

The next step would be to configure CONTENT INTERNETWORKING protocols on the CIGs of the respective CNs in order to technically support the terms of the NEGOTIATED RELATIONSHIP. To follow our previous example, this could include the configuration of the ENLISTED CN's CIGs in a particular country to send DISTRIBUTION ADVERTISEMENTS to the CIGs of the ORIGINATING CN. In order to configure these protocols, technical details (such as CIG addresses/hostnames and authentication information) would be exchanged by administrators of the respective CNs.

Note also that some terms of the NEGOTIATED RELATIONSHIP would be upheld through means outside the scope of CDI protocols. These could include non-technical terms (such as financial settlement) or other technical terms (such as SLAs).

In the event that the controlling interests of two CNs no longer wish to have their networks interconnected, it is expected that these tasks would be undone. That is, the protocol configurations would be changed to cease the movement of ADVERTISEMENTS and/or ACCOUNTING data between the networks, and the NEGOTIATED RELATIONSHIP would be legally terminated.

4. Content Internetworking Scenarios

This section provides several scenarios that may arise in CONTENT INTERNETWORKING implementations.

Note that we obviously cannot examine every single permutation. Specifically, it should be noted that:

- Any one of the interconnected CNs may have other CONTENT INTERNETWORKING arrangements that may or may not be transitive to the relationships being described in the diagram.

- The graphical figures do not illustrate the CONTENT REQUEST paths. It is assumed that a REQUEST-ROUTING SYSTEM eventually returns to the CLIENT the IP address of the SURROGATE deemed appropriate to honor the CLIENT's CONTENT REQUEST.

The scenarios described include a general case, two cases in which BCNs provide limited interfaces, a case in which a PCN enlists the services of multiple CNs, and a case in which multiple CNs enlist the services of an LCN.

4.1. General Content Internetworking

This scenario considers the general case where two or more existing CNs wish to establish a CONTENT INTERNETWORKING relationship in order to provide increased scale and reach for their existing customers. It assumes that all of these CNs already provide REQUEST-ROUTING, DISTRIBUTION, and ACCOUNTING services and that they will continue to provide these services to existing customers as well as offering them to other CNs.

In this scenario, these CNs would interconnect with others via a CIG that provides a REQUEST-ROUTING INTERNETWORKING SYSTEM, a DISTRIBUTION INTERNETWORKING SYSTEM, and an ACCOUNTING INTERNETWORKING SYSTEM. The net result of this interconnection would be that a larger set of SURROGATES will now be available to the CLIENTS.

Figure 1 shows three CNs which have interconnected to provide greater scale and reach to their existing customers. They are all participating in DISTRIBUTION INTERNETWORKING, REQUEST-ROUTING INTERNETWORKING, and ACCOUNTING INTERNETWORKING.

As a result of the NEGOTIATED RELATIONSHIPS it is assumed that:

1. CONTENT that has been INJECTED into any one of these ORIGINATING CNs may be distributed into any other ENLISTED CN.

2. Commands affecting the DISTRIBUTION of CONTENT may be issued within the ORIGINATING CN, or may also be issued within the ENLISTED CN. The latter case allows local decisions to be made about DISTRIBUTION within the ENLISTED CN, but such commands would not control DISTRIBUTION within the ORIGINATING CN.

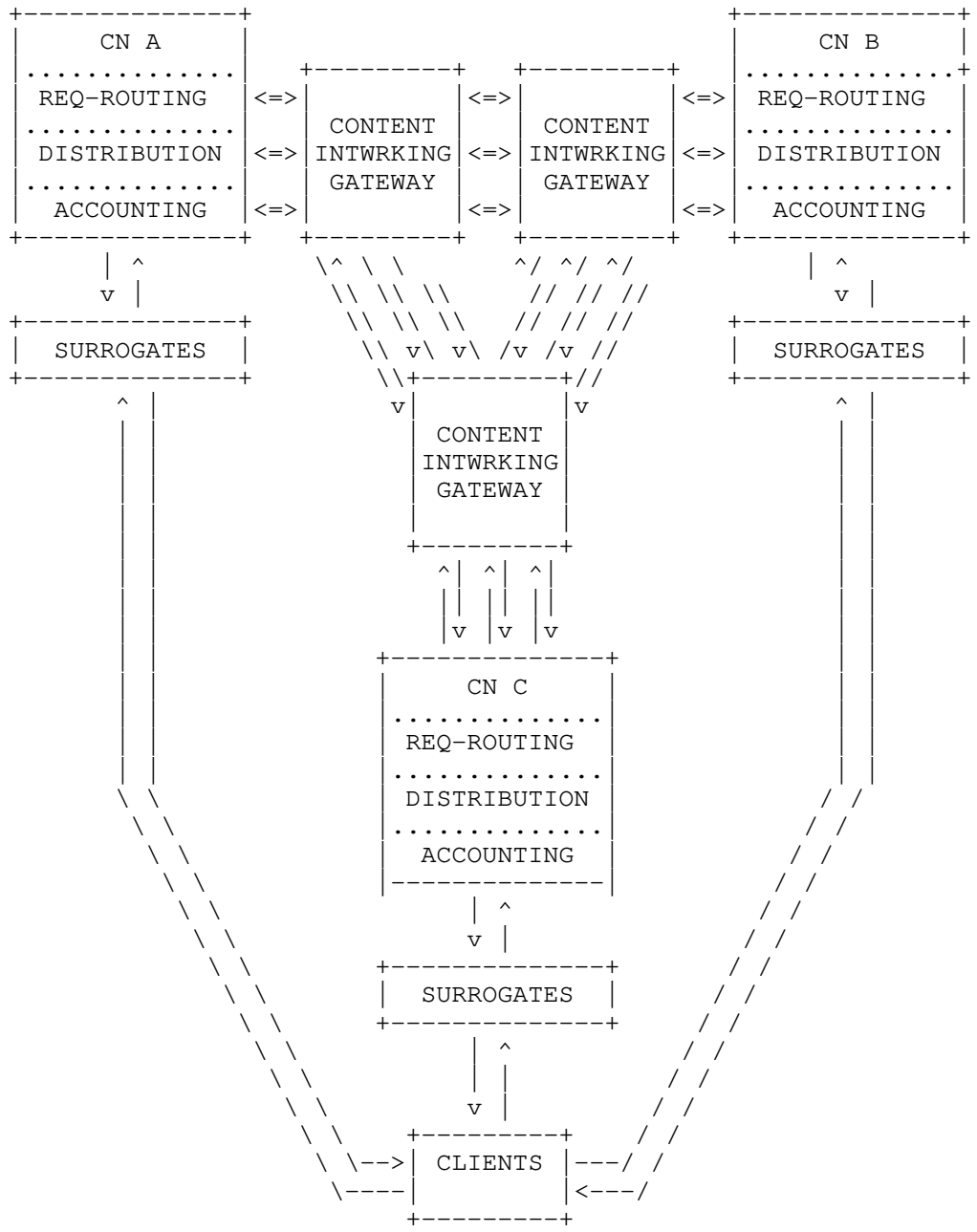
3. ACCOUNTING information regarding CLIENT access and/or DISTRIBUTION actions will be made available to the ORIGINATING CN by the ENLISTED CN.

4. The ORIGINATING CN would provide this ACCOUNTING information to the PUBLISHER based on existing Service Level Agreements (SLAs).

5. CONTENT REQUESTS by CLIENTS may be directed to SURROGATES within any of the ENLISTED CNs.

The decision of where to direct an individual CONTENT REQUEST may be dependent upon the DISTRIBUTION and REQUEST-ROUTING policies associated with the CONTENT being requested as well as the specific algorithms and methods used for directing these requests. For example, a REQUEST-ROUTING policy for a piece of CONTENT may indicate multiple versions exist based on the spoken language of a CLIENT. Therefore, the REQUEST-ROUTING SYSTEM of an ENLISTED CN would likely direct a CONTENT REQUEST to a SURROGATE known to be holding a version of CONTENT of a language that matches that of a CLIENT.

Figure 1 - General CONTENT INTERNETWORKING



4.2. BCN providing ACCOUNTING INTERNETWORKING and REQUEST-ROUTING INTERNETWORKING

This scenario describes the case where a single entity (BCN A) performs ACCOUNTING INTERNETWORKING and REQUEST-ROUTING INTERNETWORKING functions, but has no inherent DISTRIBUTION or DELIVERY capabilities. A potential configuration which illustrates this concept is given in Figure 2.

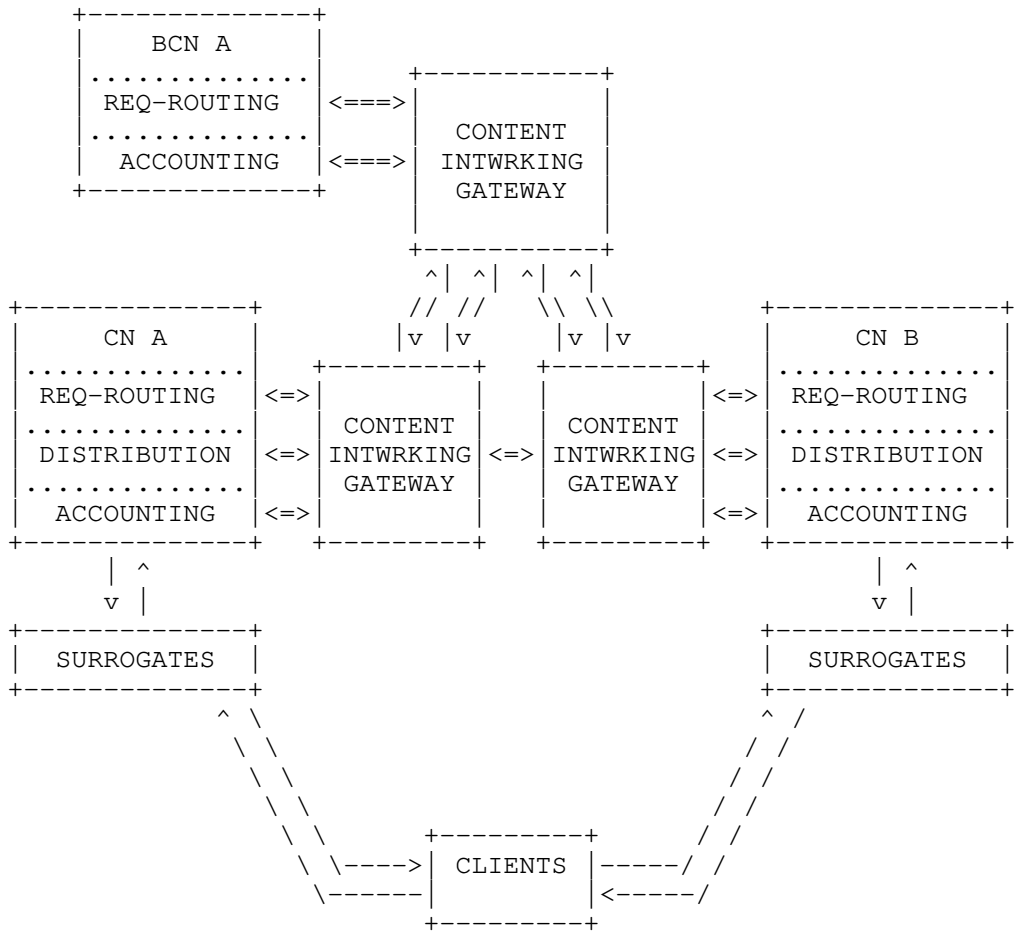
In the scenario shown in Figure 2, BCN A is responsible for collecting ACCOUNTING information from multiple CONTENT NETWORKS (CN A and CN B) to provide a clearinghouse/settlement function, as well as providing a REQUEST-ROUTING service for CN A and CN B.

In this scenario, CONTENT is injected into either CN A or CN B and its DISTRIBUTION between these CNs is controlled via the DISTRIBUTION INTERNETWORKING SYSTEMS within the CIGs. The REQUEST-ROUTING SYSTEM provided by BCN A is informed of the ability to serve a piece of CONTENT from a particular CONTENT NETWORK by the REQUEST-ROUTING SYSTEMS within the interconnected CIGs.

BCN A collects statistics and usage information via the ACCOUNTING INTERNETWORKING SYSTEM and disseminates that information to CN A and CN B as appropriate.

As illustrated in Figure 2, there are separate REQUEST-ROUTING SYSTEMS employed within CN A and CN B. If the REQUEST-ROUTING SYSTEM provided by BCN A is the AUTHORITATIVE REQUEST-ROUTING SYSTEM for a given piece of CONTENT this is not a problem. However, each individual CN may also provide the AUTHORITATIVE REQUEST-ROUTING SYSTEM for some portion of its PUBLISHER customers. In this case care must be taken to ensure that the there is one and only one AUTHORITATIVE REQUEST-ROUTING SYSTEM identified for each given CONTENT object.

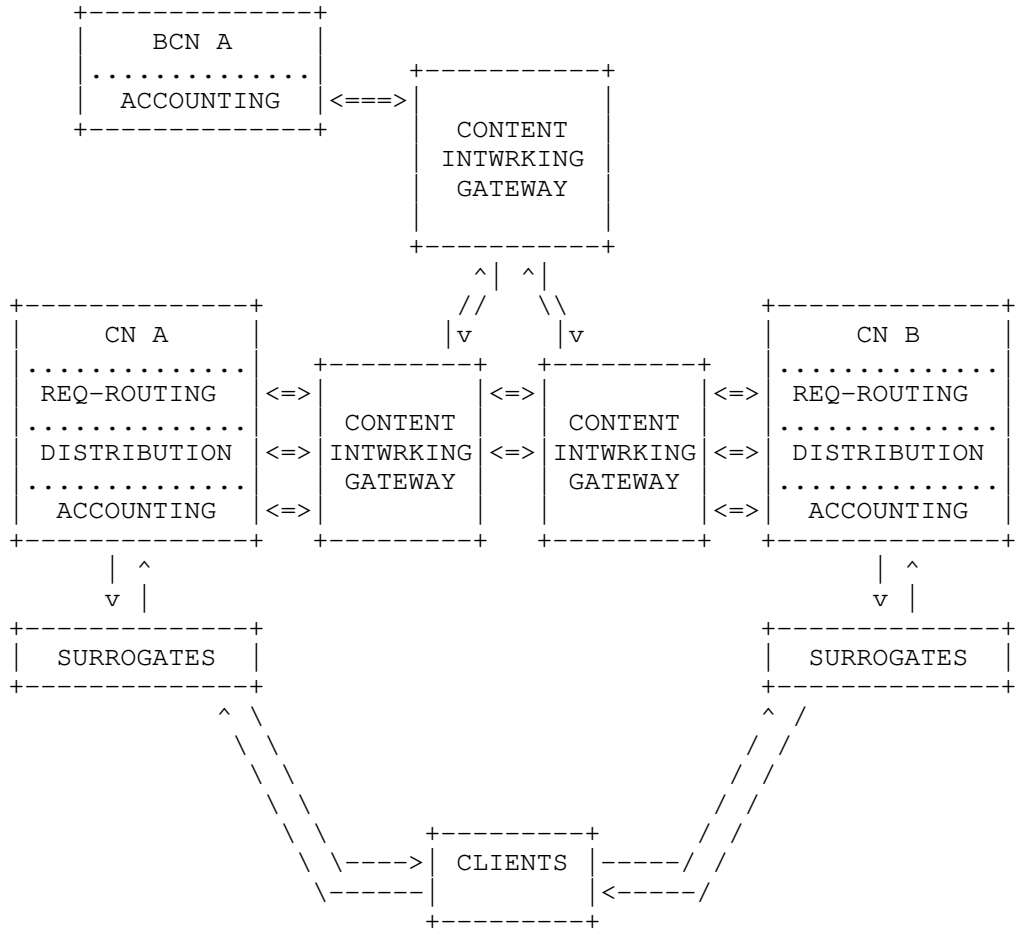
Figure 2 - BCN providing ACCOUNTING INTERNETWORKING and REQUEST-ROUTING INTERNETWORKING



4.3. BCN providing ACCOUNTING INTERNETWORKING

This scenario describes the case where a single entity (BCN A) performs ACCOUNTING INTERNETWORKING to provide a clearinghouse/ settlement function only. In this scenario, BCN A would enter into NEGOTIATED RELATIONSHIPS with multiple CNs that each perform their own DISTRIBUTION INTERNETOWRKING and REQUEST-ROUTING INTERNETWORKING as shown in FIGURE 3.

Figure 3 - BCN providing ACCOUNTING INTERNETWORKING

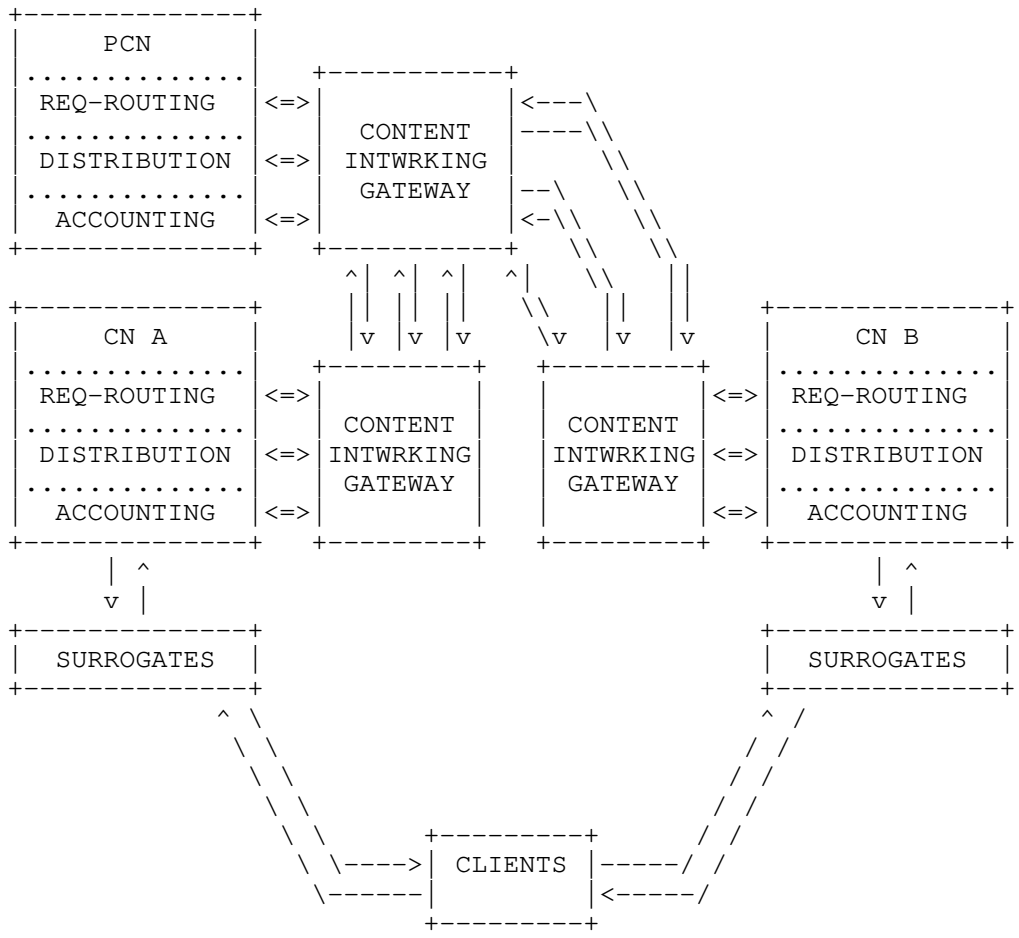


4.4. PCN ENLISTS multiple CNs

In the previously enumerated scenarios, PUBLISHERS have not been discussed. Much of the time, it is assumed that the PUBLISHERS will allow CNs to act on their behalf. For example, a PUBLISHER may designate a particular CN to be the AUTHORITATIVE REQUEST-ROUTING SYSTEM for its CONTENT. Similarly, a PUBLISHER may rely on a particular CN to aggregate all its ACCOUNTING data, even though that data may originate at SURROGATES in multiple distant CNs. Finally, a PUBLISHER may INJECT content only into a single CN and rely on that CN to ENLIST other CNs to obtain scale and reach.

However, a PUBLISHER may wish to maintain more control and take on the task of ENLISTING CNs itself, therefore acting as a PCN (Section 2.1). This scenario, shown in Figure 4, describes the case where a PCN wishes to directly enter into NEGOTIATED RELATIONSHIPS with multiple CNs. In this scenario, the PCN would operate its own CIG and enter into DISTRIBUTION INTERNETWORKING, ACCOUNTING INTERNETWORKING, and REQUEST-ROUTING INTERNETWORKING relationships with two or more CNs.

Figure 4 - PCN ENLISTS multiple CNs

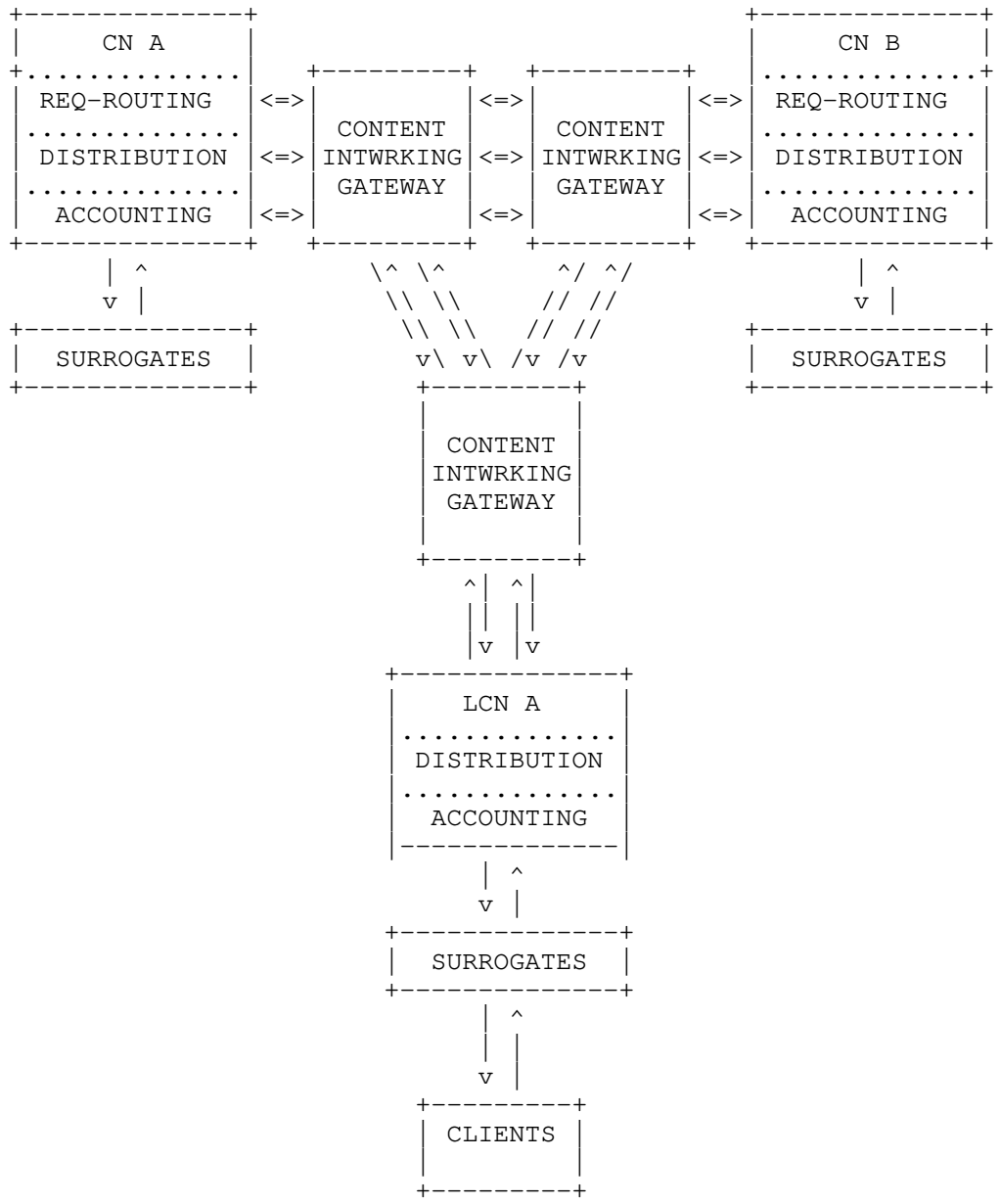


4.5. Multiple CNs ENLIST LCN

A type of CN described in Section 2.3 is the LCN. In this scenario, we imagine a tightly administered CN (such as within an enterprise) has determined that all CONTENT REQUESTS from CLIENTS must be serviced locally. Likely due to a large CLIENT base in the LCN, multiple CNs determine they would like to engage in DISTRIBUTION INTERNETWORKING with the LCN in order to extend control over CONTENT objects held in the LCN's SURROGATES. Similarly, the CNs would like to engage in ACCOUNTING INTERNETWORKING with the LCN in order to receive ACCOUNTING data regarding the usage of the content in the local SURROGATES. This scenario is shown in Figure 5. Although this diagram shows a DISTRIBUTION INTERNETWORKING connection between CN A

and CN B, it should be recognized that this connection is optional and not a requirement in this scenario.

Figure 5 - Multiple CNs ENLIST LCN



5. Security Considerations

Security concerns with respect to Content Internetworking can be generally categorized into trust within the system and protection of the system from threats. The trust model utilized with Content Internetworking is predicated largely on transitive trust between the ORIGIN, REQUEST-ROUTING INTERNETWORKING SYSTEM, DISTRIBUTION INTERNETWORKING SYSTEM, ACCOUNTING INTERNETWORING SYSTEM, and SURROGATES. Network elements within the Content Internetworking system are considered to be "insiders" and therefore trusted.

5.1. Threats to Content Internetworking

The following sections document key threats to CLIENTs, PUBLISHERs, and CNs. The threats are classified according to the party that they most directly harm, but, of course, a threat to any party is ultimately a threat to all. (For example, having a credit card number stolen may most directly affect a CLIENT; however, the resulting dissatisfaction and publicity will almost certainly cause some harm to the PUBLISHER and CN, even if the harm is only to those organizations' reputations.)

5.1.1. Threats to the CLIENT

5.1.1.1. Defeat of CLIENT's Security Settings

Because the SURROGATE's location may differ from that of the ORIGIN, the use of a SURROGATE may inadvertently or maliciously defeat any location-based security settings employed by the CLIENT. And since the SURROGATE's location is generally transparent to the CLIENT, the CLIENT may be unaware that its protections are no longer in force. For example, a CN may relocate CONTENT from a Internet Explorer user's "Internet Web Content Zone" to that user's "Local Intranet Web Content Zone". If the relocation is visible to the Internet Explorer browser but otherwise invisible to the user, the browser may be employing less stringent security protections than the user is expecting for that CONTENT. (Note that this threat differs, at least in degree, from the substitution of security parameters threat below, as Web Content Zones can control whether or not, for example, the browser executes unsigned active content.)

5.1.1.2. Delivery of Bad Accounting Information

In the case of CONTENT with value, CLIENTs may be inappropriately charged for viewing content that they did not successfully access. Conversely, some PUBLISHERs may reward CLIENTs for viewing certain

CONTENT (e.g., programs that "pay" users to surf the Web). Should a CN fail to deliver appropriate accounting information, the CLIENT may not receive appropriate credit for viewing the required CONTENT.

5.1.1.3. Delivery of Bad CONTENT

A CN that does not deliver the appropriate CONTENT may provide the user misleading information (either maliciously or inadvertently). This threat can be manifested as a failure of either the DISTRIBUTION SYSTEM (inappropriate content delivered to appropriate SURROGATEs) or REQUEST-ROUTING SYSTEM (request routing to inappropriate SURROGATEs, even though they may have appropriate CONTENT), or both. A REQUEST-ROUTING SYSTEM may also fail by forwarding the CLIENT request when no forwarding is appropriate, or by failing to forward the CLIENT request when forwarding is appropriate.

5.1.1.4. Denial of Service

A CN that does not forward the CLIENT appropriately may deny the CLIENT access to CONTENT.

5.1.1.5. Exposure of Private Information

CNs may inadvertently or maliciously expose private information (passwords, buying patterns, page views, credit card numbers) as it transmits from SURROGATEs to ORIGINs and/or PUBLISHERs.

5.1.1.6. Substitution of Security Parameters

If a SURROGATE does not duplicate completely the security facilities of the ORIGIN (e.g., encryption algorithms, key lengths, certificate authorities) CONTENT delivered through the SURROGATE may be less secure than the CLIENT expects.

5.1.1.7. Substitution of Security Policies

If a SURROGATE does not employ the same security policies and procedures as the ORIGIN, the CLIENT's private information may be treated with less care than the CLIENT expects. For example, the operator of a SURROGATE may not have as rigorous protection for the CLIENT's password as does the operator of the ORIGIN server. This threat may also manifest itself if the legal jurisdiction of the SURROGATE differs from that of the ORIGIN, should, for example, legal differences between the jurisdictions require or permit different treatment of the CLIENT's private information.

5.1.2. Threats to the PUBLISHER

5.1.2.1. Delivery of Bad Accounting Information

If a CN does not deliver accurate accounting information, the PUBLISHER may be unable to charge CLIENTs for accessing CONTENT or it may reward CLIENTs inappropriately. Inaccurate accounting information may also cause a PUBLISHER to pay for services (e.g., content distribution) that were not actually rendered. Invalid accounting information may also effect PUBLISHERs indirectly by, for example, undercounting the number of site visitors (and, thus, reducing the PUBLISHER's advertising revenue).

5.1.2.2. Denial of Service

A CN that does not distribute CONTENT appropriately may deny CLIENTs access to CONTENT.

5.1.2.3. Substitution of Security Parameters

If a SURROGATE does not duplicate completely the security services of the ORIGIN (e.g., encryption algorithms, key lengths, certificate authorities, client authentication) CONTENT stored on the SURROGATE may be less secure than the PUBLISHER prefers.

5.1.2.4. Substitution of Security Policies

If a SURROGATE does not employ the same security policies and procedures as the ORIGIN, the CONTENT may be treated with less care than the PUBLISHER expects. This threat may also manifest itself if the legal jurisdiction of the SURROGATE differs from that of the ORIGIN, should, for example, legal differences between the jurisdictions require or permit different treatment of the CONTENT.

5.1.3. Threats to a CN

5.1.3.1. Bad Accounting Information

If a CN is unable to collect or receive accurate accounting information, it may be unable to collect compensation for its services from PUBLISHERs.

5.1.3.2. Denial of Service

Misuse of a CN may make that CN's facilities unavailable, or available only at reduced functionality, to legitimate customers or the CN provider itself. Denial of service attacks can be targeted at a CN's ACCOUNTING SYSTEM, DISTRIBUTION SYSTEM, or REQUEST-ROUTING SYSTEM.

5.1.3.3. Transitive Threats

To the extent that a CN acts as either a CLIENT or a PUBLISHER (such as, for example, in transitive implementations) such a CN may be exposed to any or all of the threats described above for both roles.

6. Acknowledgements

The authors acknowledge the contributions and comments of Fred Douglis (AT&T), Raj Nair (Cisco), Gary Tomlinson (CacheFlow), John Scharber (CacheFlow), Nalin Mistry (Nortel), Steve Rudkin (BT), Christian Hoertnagl (IBM), Christian Langkamp (Oxford University), and Don Estberg (Activate).

7. References

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

[2] Biliris, A., Cranor, C., Douglis, F., Rabinovich, M., Sibal, S., Spatscheck, O. and W. Sturm, "CDN Brokering", Proceedings of the 6th International Workshop on Web Caching and Content Distribution, Boston, MA, June 2001.

8. Authors' Addresses

Mark S. Day
Cisco Systems
1414 Massachusetts Avenue
Boxborough, MA 01719
US

Phone: +1 978 936 1089
EMail: mday@alum.mit.edu

Don Gilletti
21 22nd Ave.
San Mateo, CA 94403
US

Phone +1 408 569 6813
EMail: dgilletti@yahoo.com

Phil Rzewski
30 Jennifer Place
San Francisco, CA 94107
US

Phone: +1 650 303 3790
EMail: philrz@yahoo.com

9. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.