A survey into CDNs Security

Lucas Begnini Costa[1], **Carlos A. Maziero**[1]

[1]LARSIS - Departamento de Informatica – Universidade Federal do Paraná (UFPR)
Curitiba – PR – Brazil

lucasbegnini@gmail.com,

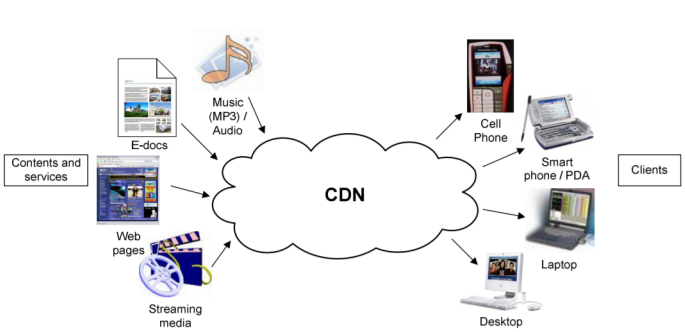
Abstract. *This meta-paper describes the style to be used in articles and short papers for SBC conferences. For papers in English, you should add just an abstract while for the papers in Portuguese, we also ask for an abstract in Portuguese ("resumo"). In both cases, abstracts should not have more than 10 lines and must be in the first page of the paper.*

Resumo. *Este meta-artigo descreve o estilo a ser usado na confecção de artigos e resumos de artigos para publicação nos anais das conferências organizadas pela SBC. É solicitada a escrita de resumo e abstract apenas para os artigos escritos em português. Artigos em inglês deverão apresentar apenas abstract. Nos dois casos, o autor deve tomar cuidado para que o resumo (e o abstract) não ultrapassem 10 linhas cada, sendo que ambos devem estar na primeira página do artigo.*

1. Introdução

All full papers and posters (short papers) submitted to some SBC conference, including any supporting documents, should be written in English or in Portuguese. The format paper should be A4 with single column, 3.5 cm for upper margin, 2.5 cm for bottom margin and 3.0 cm for lateral margins, without headers or footers. The main font must be Times, 12 point nominal size, with 6 points of space before each paragraph. Page numbers must be suppressed.

Full papers must respect the page limits defined by the conference. Conferences that publish just abstracts ask for **one**-page texts.



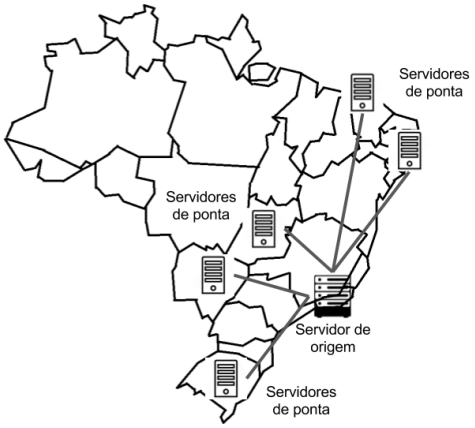
2. Composição de uma CDN

Uma CDN pode ser definida segundo os seguintes pontos:

- Organização;
- Servidores;
- Relacionamentos;
- Protocolos de iterções;
- E tipos de conteúdo.

2.1. Tipos de servidores

Figura 1. Tipos de servidores



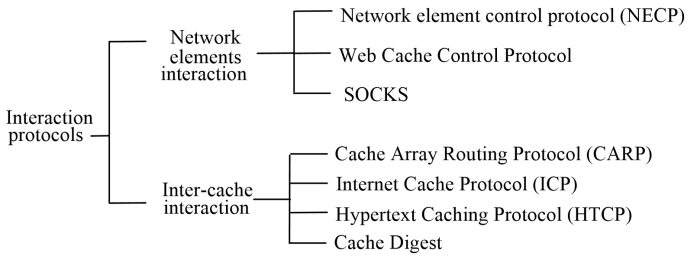
Os servidores são definidos dos seguintes modos:

- Servidor de origem
- Servidor de ponta

Podemos ilustrá-los conforme a figura 1.

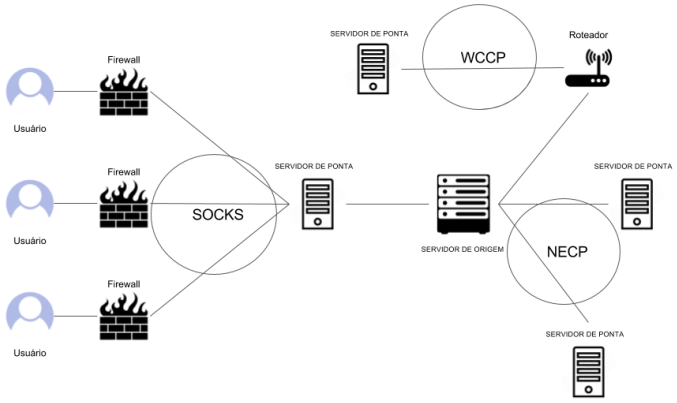
2.2. Protocolos de interações

Figura 2. Tipos de relacionamentos



Os protocolos de interações podem ser divididos em duas partes: Protocolos de interações de elementos da rede e Protocolos de interações entre os servidores de cache da CDN.

Figura 3. Tipos de protocolos de iterações



2.2.1. Interações dos elementos da rede

Dentro dos protocolos de interações dos elementos de rede podemos verificar que cada um possui sua especificidade e funcionalidade bem definida, como podemos ver na figura 3 , tentando proteger o não só a rede mas também o usuário, o servidor, os roteadores e a comunicação entre os mesmos.

2.2.2. Interações de cache

Os protocolos de interações de cache são protocolos que organizam as trocas de informações entre os servidores, ou seja, é ele que dita como irá funcionar a distribuição da informação dentro da rede.

Conforme vimos na figura 2, e segundo [Pathan and Buyya 2007], existem 4 tipos de protocolos aplicados nessa circunstância, que são:

- HTCP - Hypertext Caching Protocol
- ICP - Internet Cache Protocol

Ambos são concorrentes entre sí e tem como funcionalidade controlar o fluxo de informação entre os caches. Sendo através deles que se controla o que irá para um determinado servidor de ponta, por exemplo. Falaremos mais sobre ambos em 2.2.3 e 2.2.4 respectivamente.

Existe também os protocolos:

- CARP - Cache Array Routing Protocol
- Cache Digest

Esses dois protocolos, também concorrentes entre sí, servem para controlar o conteúdo existente dentro de cada servidor e saber onde estão os outros conteúdos. Falaremos mais sobre ambos em 2.2.6 e 2.2.7 respectivamente.

2.2.3. HTCP

Como dito anteriormente o HTCP, Hypertext Caching Protocol, é um protocolo de interação entre os caches, suas principais caracteristícas são:

- Protocolo para descobri Caches HTTP;
- Suporte ao HTTP 1.0;
- Permite incluir cabeçalhos nas respostas;
- Podem ser enviados via TCP/UDP;
- Devem ser resilientes à falhas.

2.2.4. ICP

Já o ICP, Internet Cache Protocol, é um protocolo muito mais leve que possui as seguintes caracteristícas:

- Protocolo de mensagem leve;
- Utilizado para comunicação de Caches;
- Utiliza consultas para determinar localização mais apropriada;
- Suporte ao HTTP 0.9;
- Comunica-se com caches vizinhos;
- recebe MISS ou HIT como resposta;
- Enviado via UDP;
- Falha por timeout indica caminho quebrado;
- Fornece informações para balanceamento através das medidas de perda.

2.2.5. HTCP x ICP

Analisando os dois protocolos,HTCP e ICP, podemos fazer um quadro comparativo entre os e colocá-los da seguinte maneira(figura 4):

Figura 4. HTCP x ICP

Serviços	HTCP	ICP
Envio TCP	✓	✓
Envio UDP	✓	
Suporte HTTP 1.0	✓	
Permite enviar apenas cabeçalho	✓	
Monitora caches remotos	✓	
Permite monitoramento de falhas		✓

2.2.6. CARP

CARP - Cache Array Routing Protocol

Protocolo de armazenamento distribuído baseado em uma lista conhecida de proxies suavemente acoplada e uma função hash para dividir o espaço URL entre esses proxies.

- Cliente HTTP pode enviar requisição à qualquer proxy da lista.

2.2.7. Cache Digest

Cache Digest

Protocolo de intercâmbio e formato de dados entre caches.

- Fornecem um resumo dos conteúdos na resposta;
- Soluciona os problemas de congestionamento e timeout;
- Torna possível determinar se um servidor possui em cache um conteúdo;
- Executado via HTTP ou FTP;
- Contém tempo de expiração na resposta;
- Podem ser utilizados para eliminar redundância.

2.3. Seleção e entrega de conteúdo

Dentro de uma CDN temos que nos preocupar com a forma como esse conteúdo vai catalogado, armazenado e distribuído dentro da rede, o que vimos no item 2.2, como também temos que nos preocupar como esse conteúdo vai chegar até o cliente (usuário) da forma mais otimizada possível, ou seja, o servidor o qual vai fornecer as informações para ele será o mais perto ou mais rápido.

Temos que destacar também a importância da otimização do fluxo de informação pela rede. Visto que quanto maior o tráfico de informação pela rede significa que a informação está mais distante do usuário e também que vai ter um custo maior pela troca intensa de informação.

Segundo [Krishnamurthy et al. 2001], na tentativa de otimizar o redirecionamentos de URL para o usuário se sacramentou dois tipos de técnicas de redirecionamentos:

- Full - site
- Partial - site

2.3.1. Full - site

Na técnica de Full-site todo o conteúdo é entregado ao usuário de um servidor ponta único. Ou seja, o usuário faz uma requisição ao servidor principal, onde o mesmo processa um algoritmo de roteamento para encontrar o servidor ponta que melhor se enquadra como resposta, e então retorna ao usuário o endereço onde então será consumido por fim todas as informações requisitadas.

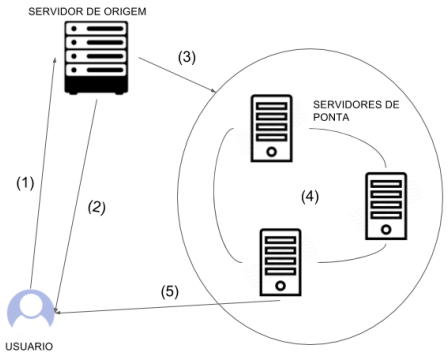
É importante salientar que essa técnica é amplamente utilizada por serviços que fazem pouco uso de dados da rede. Uma página estática da web, por exemplo, se encaixaria perfeitamente nesse contexto. Visto que possui baixo grau de modificações e seu tamanho é pequeno perto de outros tipos de mídias que circulam na web.

2.3.2. Partial - site

Já redirecionamentos do tipo Partial-sites os servideores principais retornam para o usuário uma parte do conteúdo e disparam, automaticamente, um algoritmo de roteamento para encontrar o restante da informação e retornar ao usuário. Conforme podemos ver na figura 5

Figura 5. Entrega de conteúdo

(1)	Requista rota
(2)	Retorna um index.html
(3)	redireciona a requisição para o provedor de CDN
(4)	Acha o melhor servidor de ponta
(5)	Envia o conteúdo ao usuário



Nela podemos ver que todo o processo acontece em, basicamente, 5 etapas. (1) o usuário faz uma requisição ao servidor principal, depois, em (2) o servidor principal retornar um html com as principais informações e dispara automaticamente (3) um processo de roteamento (4) para buscar o melhor servidor e retornar (5) para o usuário os conteúdos.

Entretanto há em (4) diversas formas de fazer esse roteamento quanto a distribuição do conteúdo pela rede e quanto a aglomeração desse conteúdo dentro do servidores de cache.

Tipo de distribuição nada mais é do que a forma como o conteúdo vai ser disperso na rede, como esse conteúdo vai se aproximar do nó que está mais perto do usuário.

Os tipos de distribuição mais frequentemente utilizados são:

- Empírico
- Popularidade

Empírico trata, como o próprio nome diz, de uma forma de distribuição sem nenhum conhecimento específico a respeito, utilizando-se apenas um conhecimento experimental de onde seria melhor posicionado o conteúdo.

Em um esquema baseado em popularidade a distribuição é feita conforme a notoriedade. Ou seja, quanto mais a requisição do conteúdo mais ele vai ficar nos servidores de ponta perto do usuário.

Ambos esquemas não são necessariamente excludentes, pode-se inicialmente aplicar a forma empiríca para gerar dados a respeito da distribuição e depois utilizar esses dados para aplicar o modo de popularidade.

Também existe as formas de aglomerações de conteúdo. Isso existe porque os conteúdos podem ser conjuntos de objetos ou objetos independentes. As formas de aglomerações são:

- Objeto
- Conjunto de objetos

Aglomeração por objeto vai juntar os objetos mais selecionados e distribui-los individualmente entre os servidores. Já por conjunto de objetos ele vai separa-los em grupos e distribui-los em conjuntos.

Podemos exemplicar da seguinte forma: Em um site temos vários elementos, temos o HTML, temos o CSS e temos a media de um vídeo qualquer. Podemos separar da seguinte forma temos 3 elementos onde 2 deles são altamente dependentes(HTML e CSS) e temos u que pode ser diferente em cada região do país que é o vídeo. Então podemos misturar as formas de aglomerações, para o HTML e para o CSS agrupamos em conjuntos de objetos, e para o vídeo fazemos a aglomeração por objeto, já que será distribuído de maneira independente nos servidores.

Analisando os tipos se perceber que nenhuma das opções são excludentes entre sí. Pode-se combinar quaisquer tipo de distribuição e aglomeração e também. As escolhas vão depender das necessidades de cada aplicação.É necessário uma análise minuciosa de cada aplicação para chegar em um veredito da melhor abordagem.

2.3.3. VOD

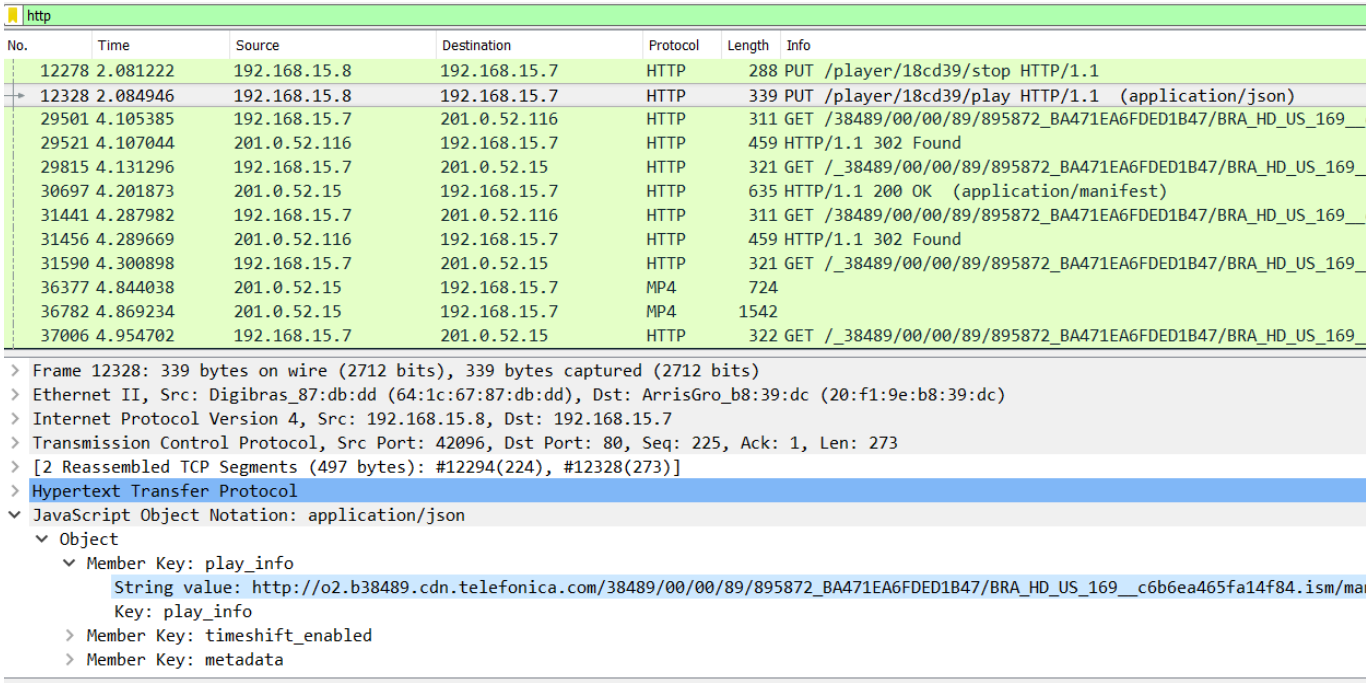
2.3.4. Exemplo

Agora vamos ilustrar com um exemplo mais prático. Utilizaremos uma requisição de uma URL de um VOD(Video On Demand) onde a parte de roteamento é feita no usuário. A aplicação do usuário faz uma requisição à CDN e enquanto o

cabeçalho da resposta não for 200 ele vai ler um campo dentro do cabeçalho de resposta e fazer uma nova requisição. A figura (FAZER A FIGURA) ilustra a situação.

Como podemos observar na figura 6 a aplicação manda para o player a url associada ao VOD que é responsável por responder com o caminho oficial, ou intermediário, do manifesto. Na figura 6 ele está localizado no campo ”play_info”da requisição.

Figura 6. exemplo VOD



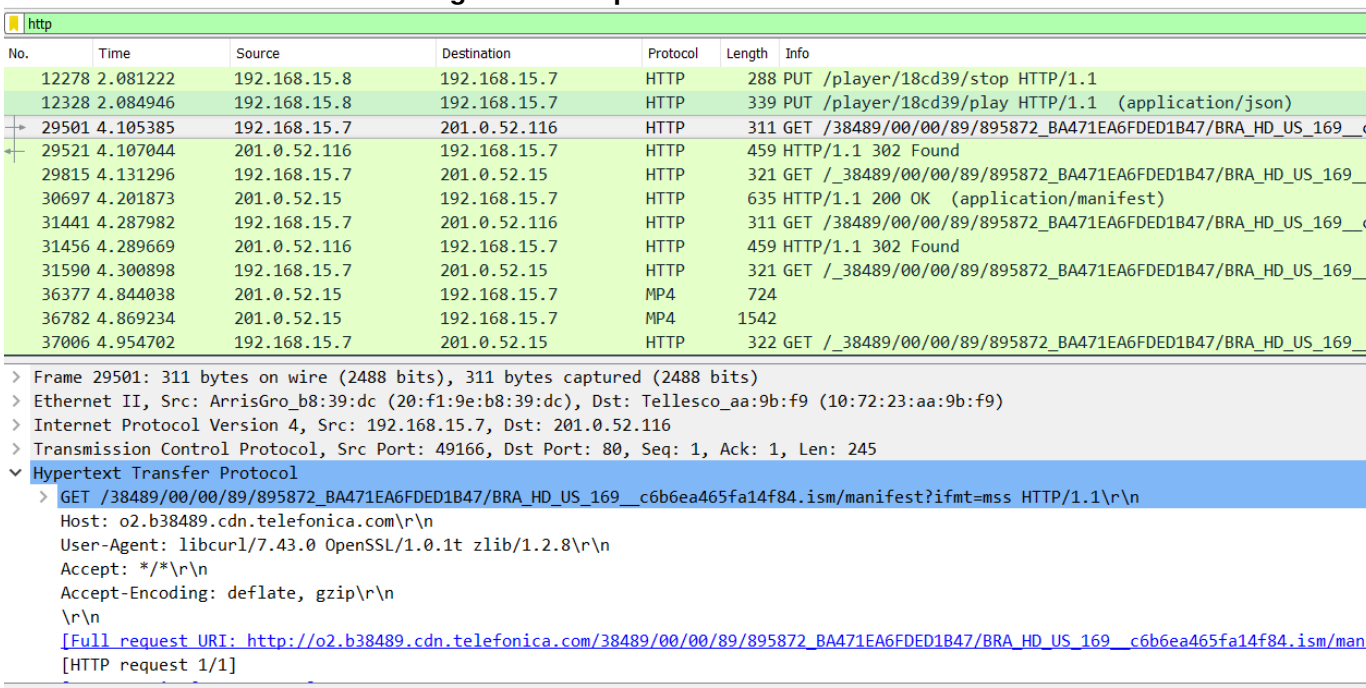
O player, por sua vez, como responsável por enviar as requisições, envia ao servidor principal a requisição do manifest do VOD que ele quer tocar. Figura 7.

Na figura 8 vemos a CDN, que já fez um roteamento para uma outra rede(ou servidor), que retornou com um código 302 indicando que o retorno da requisição não é a resposta final. Dentro do cabeçalho da resposta tem um campo chamado ”location”o qual é responsável por retornar o endereço final (ou intermediário) para nova requisição. Esse processo será repetido até o código de retorno da requisição for 200.

Ainda na figura 8 podemos observar que ele recebe um 200 OK da requisição em seguida do 302 Found. O que simboliza que aquela URL é a URL final e o player pode utiliza-la como base do manifesto.

Em 9 vemos o player começando a consumir os ”chuncks”e por consequência tocando o vídeo.

Figura 7. exemplo VOD



3. Segurança de uma CDN

3.1. Autenticação de usuário

3.2. Autenticação de conteúdo

3.3. Modelos de ataques à uma CDN

4. References

Referências

Krishnamurthy, B., Wills, C., and Zhang, Y. (2001). On the use and performance of content distribution networks. In *Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement*, pages 169–182. ACM.

Pathan, A.-M. K. and Buyya, R. (2007). A taxonomy and survey of content delivery networks. *Grid Computing and Distributed Systems Laboratory, University of Melbourne, Technical Report*, 4.

Figura 8. exemplo VOD

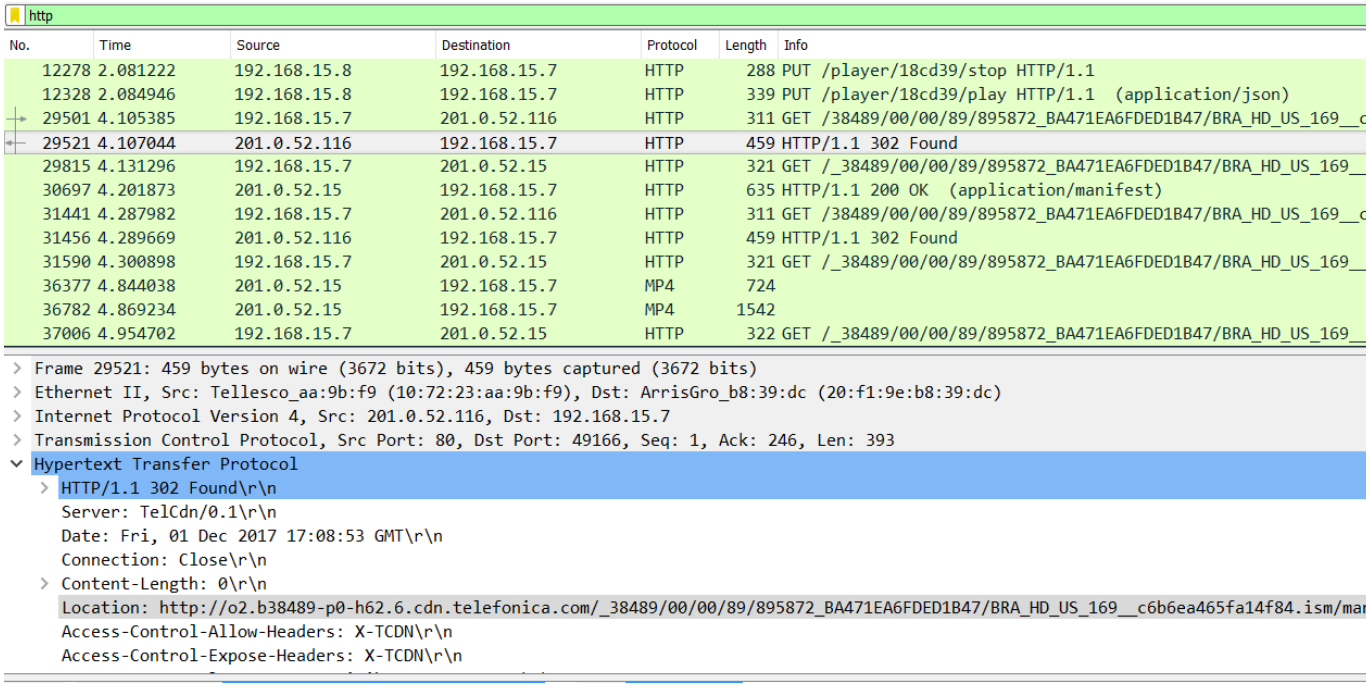


Figura 9. exemplo VOD