SNMP Proxy CCN: Uma proposta de arquitetura para gerência de redes orientadas a conteúdo interoperável com sistemas legados

Marciel de Lima Oliveira[1], Christian Esteve Rothenberg[1]

[1]Departamento de Engenharia da Computação e Automação Industrial (DCA)
Faculdade de Engenharia Elétrica e de Computação (FEEC)
Universidade Estadual de Campinas (UNICAMP)
Av. Albert Einstein 400, 13083-852 Campinas, SP, Brasil.

marciel.oliveira@gmail.com, chesteve@dca.fee.unicamp.br

Abstract. *Research efforts on Information-Centric Networking (ICN) mainly focus on the "data and control plane" challenges compared to the efforts devoted so far on "management plane". Aiming at addressing this gap, this paper presents some mapping mechanisms and a proxy tool in order to enable the management and monitoring of CCN nodes through legacy SNMP-based systems. This work is a first step towards exploring the management of content-oriented (name/data) networks that promise better performance compared to traditional architectures based on addressing network interfaces.*

Resumo. *Pesquisas voltadas as Redes Orientadas a Conteúdo (ROCs) tem maior foco nos "planos de dados e controle" em comparação ao "plano de gerência". Como contribuição para suprir essa carência, este artigo apresenta uma proposta de arquitetura NONM (Name-Oriented Network Management) baseada em mecanismos de mapeamento e uma ferramenta proxy que permite o gerenciamento e monitoramento de nós de rede CCN nativas através de sistemas de gerência de redes SNMP legadas. Desta forma é possível explorar o conceito de gerencia orientada ao conteúdo (nomes/dados), que promete melhor desempenho quando comparado com arquiteturas tradicionais baseadas no endereçamento de interfaces dos nós.*

1. Introdução

Com o surgimento de grandes redes de transporte e equipamentos complexos construídos para tratar diversos serviços como dados, voz e vídeo, surge também o interesse de monitorar e otimizar o uso destas redes (equipamentos e serviços). Esse monitoramento é classificado como "plano de gerência" como forma de diferenciá-lo dos "planos de dado e de controle" responsáveis pela implementação efetiva dos

serviços oferecidos aos usuários. Parte da instanciação do plano de gerência se dá através da ideia do centro de operações de redes (NOC) que atua em um regime 24/7 para a operação, manutenção e análise do desempenho das redes e dos respectivos equipamentos.

O plano de gerência geralmente conta com um sistema de gerência de rede NMS (Network Management System) central que atua no monitoramento e operação das três grandes divisões das redes (plano de dados) de equipamentos de telecomunicações, núcleo (ex.: DWDM), agregação (ex.: MPSL-TP, Metro-Ethernet) e acesso (exe.: LTE/4G, xDSL, xFTTH). A comunicação entre os sistemas de gerência e os equipamentos no plano de dados é feita através de uma rede dedicada chamada DCN (Data Communication Network) e os protocolos de rede TCP/IP são adotados como padrão para uso nos equipamentos que compõem a DCN (roteadores L3/IP/MPLS e switches L2/Ethernet/Metro).

O surgimento de recentes trabalhos em Redes Orientadas a Conteúdo (ROCs) representa um novo paradigma onde o foco das redes é baseado no conteúdo e não mais na sua localização [1]. As ROCs propõem que o conteúdo seja o elemento central das redes, independente de sua localização, substituindo o foco de "onde" para "o quê". Nas ROCs, a infraestrutura da rede participa ativamente no armazenamento (caching) e na distribuição dos conteúdos visando um aumento na eficiência da busca e na disponibilidade dos conteúdos na rede.

As ROCs têm despertado grande interesse no meio acadêmico e dentre várias empresas e institutos relacionados às pesquisas na área das novas arquiteturas de rede abrindo espaço para novas aplicações, pesquisas e experimentos, tais como: CCN [2], que apresenta uma estrutura hierárquica para nomes semelhante às URLs; DONA [3], que utiliza o mecanismo de nomeação plana e funções de *hash* criptográfico e LIPSIN [4] que possui uma arquitetura que identifica os enlaces pelo nome ao invés dos pares de endereços fim a fim.

O novo paradigma proposto pelas ROCs traz consigo inúmeros desafios [5]. Esse trabalho foca no ponto de vista de gerência de redes orientadas a conteúdo levando em consideração a carência, tanto no nível de mecanismos adequados, como na definição de um plano de gerência para estas redes. O artigo apresenta uma proposta de arquitetura NONM (Name-Oriented Network Management) que tem como principais destaques a modelagem da MIB CCN para identificação dos objetos do nó CCN e o mecanismo SCNAT que converte as mensagens das redes legadas para interação com elementos nativos da rede CCN.

2. Motivação e Objetivo

A motivação principal deste artigo deve-se à percepção da carência de paradigmas adequados à gerência de redes orientadas ao conteúdo. Consideramos a possibilidade de experimentar gerência de redes orientadas a conteúdo com o uso de protocolos e arquiteturas de gerência utilizados nas redes tradicionais, como por exemplo; TL1, REST, NETCONF, SNMP, CLI e WEB UI [9, 10, 11], transformando-as em ferramentas eficientes para a gerencia de redes CCN.

A arquitetura CCN (Content-Centric Networking) [2] adotada como referência nesse trabalho é reconhecidamente uma das propostas mais relevantes na literatura relativamente às redes orientadas ao conteúdo. As redes CCN utilizam uma estrutura de nomes hierárquicos e legíveis (formados por sequências de caracteres e números) para identificar os conteúdos. Tais nomes possuem características semânticas, ou seja, os componentes hierárquicos utilizados na identificação trazem algum tipo de informação sobre o conteúdo como, por exemplo, versão, formato ou propriedade.

Para tornar os sistemas de gerência compatíveis esta proposta define como estratégia a utilização de *label* (nome) como identificador único de um nó na rede CCN e o mapeamento através de um *SNMP Proxy* [7] entre a arquitetura de gerência da rede atual com a arquitetura da gerência da rede CCN. A arquitetura *NONM* (Named-Oriented Network Management), tem como principal tarefa compatibilizar a gerência tradicional baseada no protocolo SNMP (Simple Network Management Protocol*)* [12, 13] com a gerência de redes CCN.

3. Fundamentos teóricos: CCN e SNMP

Nesta seção são apresentados de forma breve os fundamentos teóricos da arquitetura CCN e do protocolo SNMP, os principais componentes explorados neste trabalho.

3.1 Características do modelo CCN

O CCN utiliza basicamente dois tipos de pacotes: *Interest* e *Data*. O consumidor expressa seu interesse inserindo o nome do conteúdo desejado em uma mensagem do tipo *Interest* e a envia para rede. O produtor, ou algum *caching* no interior da rede, que possui tal conteúdo receberá essa mensagem e enviará de volta ao consumidor uma mensagem do tipo *Data* como resposta. Ou seja, essas mensagens possuem uma relação um para um onde um pacote de interesse satisfaz um de dados se o nome de conteúdo em ambos os pacotes são equivalentes. A Figura 1 mostra uma representação gráfica dos pacotes do modelo CCN. O pacote *Interest* pode possuir alguns parâmetros opcionais como seletores de escopo, preferência de ordem e filtro de exclusão. Um valor aleatório *nonce* é utilizado para descartar o recebimento de mensagens duplicadas por interfaces diferentes, eliminando assim *loops* da rede. O pacote *Data*, além do nome e do conteúdo, também carrega a assinatura e algumas informações opcionais como identificador do publicador e localização da chave para auxiliar na verificação da assinatura.

O mecanismo de nomeação permite ao requisitante buscar o conteúdo posicionado em uma estrutura hierárquica. Caso o conteúdo corresponda a uma versão posterior, basta solicitá-lo através do identificador, por exemplo: *br.youtube/video/filme.avi/1/anterior*. Se o conteúdo corresponder a uma versão posterior basta acessar o próximo "pedaço" denominado *chunk*, por exemplo: *br.youtube/video/filme.avi/1//1/posterior*.

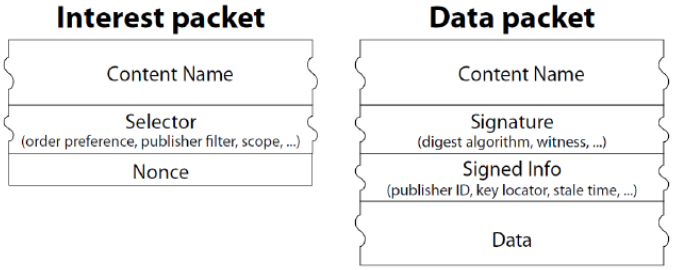

Figura 1. Pacote do CCN (reproduzido de [2]).

Os nós CCN possuem um buffer de memória para *cache* que busca armazenar os pacotes de dados o maior tempo possível em uma estrutura denominada CS (Content Store), uma vez que o mesmo conteúdo pode ser compartilhado por muitos consumidores. Quando um pacote de interesse chega ao nó, se o conteúdo requisitado estiver armazenado no *cache* o pacote de dados é imediatamente encaminhado na direção onde foi recebido o pacote *Interest*. Caso contrário, o nó insere o nome do conteúdo desejado e a interface pela qual o pacote *Interest* foi recebido na PIT (Pending Interest Table). A PIT registra, portanto, todos os interesses que passaram pelo nó em busca do conteúdo para que, quando o pacote de dados for recebido ele possa ser encaminhado corretamente em direção ao(s) consumidor(es). Apenas interesses são roteados no CCN; os pacotes de dados simplesmente seguem as entradas na PIT deixadas no caminho de volta ao consumidor. Estas entradas são apagadas assim que o pacote de dados correspondente é encaminhado ao consumidor ou por temporização, no caso em que o interesse não encontra o pacote de dados correspondente. Após registro na PIT, o pacote de *Interest* é encaminhado pela FIB (Forwarding Information Base) do nó através de uma busca de prefixo-mais-longo (*longest-prefix match*) indicando por qual interface enviar o pacote de *Interest*. Caso não haja uma entrada correspondente na FIB, o *Interest* é descartado.

A Figura 2 apresenta a estrutura do nó CCN e a dinâmica de encaminhamento.

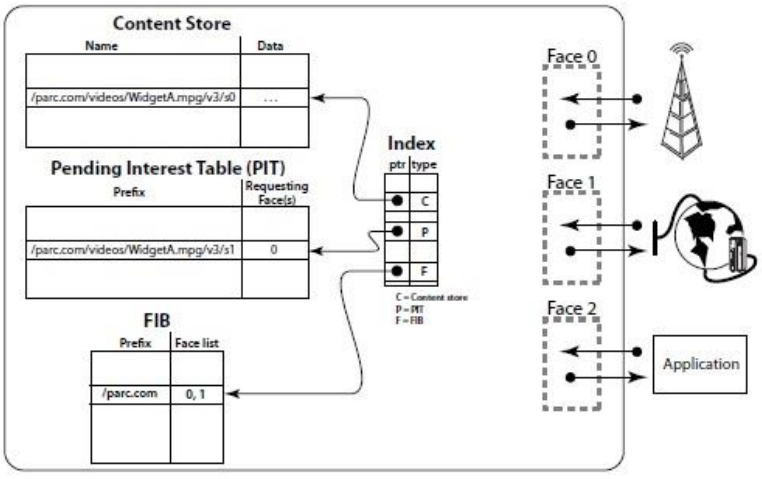

Figura 2: Arquitetura de roteamento do nó CCN (reproduzido de [2]).

3.2 Características do SNMP

O protocolo SNMP [12, 13] faz parte da infraestrutura de gerência baseada em três componentes básicos: *entidade gerenciadora*, *dispositivo gerenciado* e o *próprio protocolo de gerência*.

1- *Entidade gerenciadora ou Gerente NMS*. É uma aplicação que controla e coleta as informações de gerenciamento de uma rede. Um *NMS* é responsável pelo *pooling* e recebimento de *traps* dos agentes. As solicitações de informação enviadas pelo gerente na forma de *pooling* são requisições feitas para um agente por informações gerenciáveis. A mensagem de *trap* é enviada pelo agente para o gerente para informar a ocorrência de eventos relevantes na operação do dispositivo de rede.

2- *Dispositivo ou elemento gerenciado*. Elemento de rede que faz parte da rede gerenciada. Neste elemento podem existir diversos objetos gerenciados que são partes físicas do dispositivo, como uma interface de rede de um roteador, ou mesmo partes do software como, por exemplo, informações relativas à operação do protocolo de roteamento. Em cada dispositivo gerenciado existe um agente de gerenciamento que se comunica com a entidade gerenciadora (gerente) e executa ações específicas de acordo com solicitações dos gerentes. Para organização dos objetos gerenciados existe uma base de informação de gerenciamento MIB (Management Information Base) que disponibiliza para a entidade gerenciadora o conteúdo dos objetos gerenciáveis disponibilizados pelo dispositivo de rede. Os objetos da MIB são nomeados e organizados de forma hierárquica de acordo com a estrutura de nomeação da ISO, onde cada ramo da árvore possui um nome e um número OID (Object Identifier).

3 - *Protocolo de gerenciamento de rede*. Atua entre o gerente e o agente, permitindo que o gerente consulte informações do dispositivo gerenciado e execute ações sobre eles mediante seus agentes, como alteração de valores.

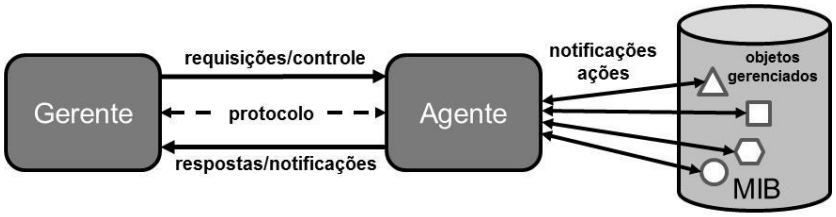

Figura 3: Arquitetura genérica de gerência SNMP.

O protocolo SNMP é utilizado para transportar informações da MIB entre *gerentes* e *agentes*, neste contexto são permitidas operações de consulta *GET* e modificação *SET* para valores de objetos da MIB associados a um elemento gerenciado. O SNMP também é utilizado para permitir que os agentes enviem mensagens (não solicitadas) caracterizadas como *eventos*, mensagens estas chamadas de *TRAPs*. A figura 3 apresenta a arquitetura genérica da gerência SNMP.

3.3 Trabalhos relacionados

Como trabalho relacionado, a proposta definida em [6] utiliza uma rede IP (Internet Protocol) convencional para transportar os pacotes *Interest* e *Data* entre os nós CCN. Neste cenário o protocolo IPFIX foi estendido para criar um *agente IPFIX* que captura

os pacotes na rede IP (porta fixa UDP 9695) e converte para um formato XML (Extensible Markup Language) com os atributos relacionados ao CCN. Para os pacotes *Interest* são considerados como atributos; *message type, content name, chunk number, timestamp* e *address*. De forma similar para os pacotes *Data* são considerados como atributos; *content name* e informações de performance como; *bytes*, *packets* ou *data rate*. Com essas informações, o *agente IPFIX* cria um novo fluxo de dados que é encaminhado para um servidor central denominado *CCN Collector/Visualizer*, esse servidor tem o papel de analisar as estatísticas do tráfego.

Cada nó CCN também possui um agente SNMP que coleta diversas informações a respeito das características físicas do nó como; *CPU*, *memória*, *HDD*, *interfaces de rede* e também informações a respeito das tabelas; *CS*, *PIT* e *FIB*. O agente SNMP utiliza uma *MIB CCN* definida para coletar ou alterar dados dos objetos, assim como para o envio de mensagens de notificação ao Servidor SNMP.

As informações coletadas dos nós CCN pelos agentes IPFIX (tabelas de fluxos) e SNMP (tabelas de objetos monitorados) são exibidas em uma interface Web para o usuário.

4. NONM: Projeto e arquitetura para gerência de redes orientadas a conteúdo

Nesta seção apresentamos a proposta de arquitetura NONM (Named-Oriented Network Management) a partir da utilização do SNMP como protocolo inicial a ser utilizado na arquitetura.

4.1 Protocolo SNMP como primeira proposta NONM

A modelagem de uma ferramenta SNMP Proxy CCN é o primeiro passo em direção à adoção de mecanismos para gerência de redes CCN, sejam nativas ou overlay, outro protocolo convencional (mais antigo ou mais moderno) também poderia ser traduzido para gerenciar elementos nativos das redes orientadas a conteúdo, optamos pelo SNMP apenas por se tratar de um protocolo largamente conhecido como primeira aproximação para suprir a necessidade. Um modelo de mapeamento das funcionalidades mínimas de arquiteturas de gerência tradicionais para uso em CCN tornará possível a coexistência de ferramentas *gerentes* de redes legadas interoperáveis com *agentes* em redes CCN nativas.

4.2 MIB CCN

Neste trabalho definimos uma MIB para a rede CCN com o mesmo propósito da MIB apresentada em [6], que se diferencia nos aspectos relativos à gerência de objetos refletidos em uma gente CCN *nativo* ao contrário de um agente SNMP *convencional*.

Tabela 1: Características das ferramentas de monitoramento CCN

	Trabalho relacionado	SNMP Proxy CCN
Define uma MIB CCN	SIM	SIM
Agente CCN nativo	NÃO	SIM
Gerencia de nós CCN nativos	NÃO	SIM
Mapeamento das operações básicas do SNMP para CCN	NÃO	SIM

A MIB CCN tem como objetivo criar novos ramos na árvore com a identificação de objetos exclusivos (OIDs) para monitoramento de elementos de rede CCN em redes nativas. A MIB CCN proposta neste trabalho fica no mesmo nível de hierarquia da MIB2 e está classificada em duas partes, uma parte reflete objetos adotados no padrão da MIB2 e a outra parte trata objetos específicos para monitoramento de nós CCN.

Objetos relacionados com a MIB padrão. Propomos manter a relação de objetos já adotados na MIB para manter um padrão de arquitetura uma vez que estes objetos estão relacionados à gerência do elemento de rede propriamente dito, como exemplo, "System" para "ccnSystem", "Interfaces" para "ccnInterfaces" e demais objetos.

Objetos exclusivos para tratar características do nó CCN. O nó CCN possui características que o torna único em relação à arquitetura de outros elementos das redes legadas, pois ele possui tabelas de controle diferenciadas para tratamento e roteamento de pacotes/conteúdo. Pensando nesta tratativa especificamos alguns grupos de objetos para monitorar estas tabelas, como por exemplo: *ccnStatus*, *ccnFace*, *ccnCS*, *ccnPTI* e *ccnFIB*. A MIB CCN é apresentada na Figura 4.

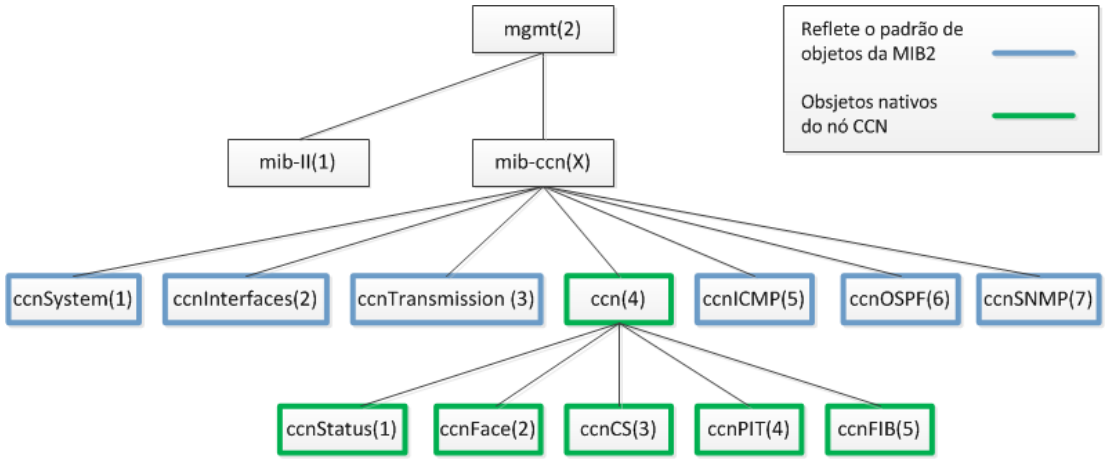

Figura 4: A MIB CCN e sua sub-árvore.

4.3 Estratégias para mapeamento das operações básicas do SNMP

Levando em consideração que os elementos da rede CCN não suportam o protocolo SNMP, é necessário o uso de um mecanismo *SNMP Proxy* [7] que permite o mapeamento das operações básicas do protocolo SNMP para monitoramento dos elementos nativos da rede CNN. Neste contexto um *sub-agente* (executado no proxy) deve conhecer os objetos da MIB CCN para estabelecer a interface de comunicação entre as redes IP e CCN. Com esse propósito, adotamos um mecanismo de mapeamento denominado SCNAT (SNMP Content Network Address Translation) que faz o papel de "tradutor" da arquitetura utilizada na ferramenta SNMP Proxy CCN, apresentada na figura 5.

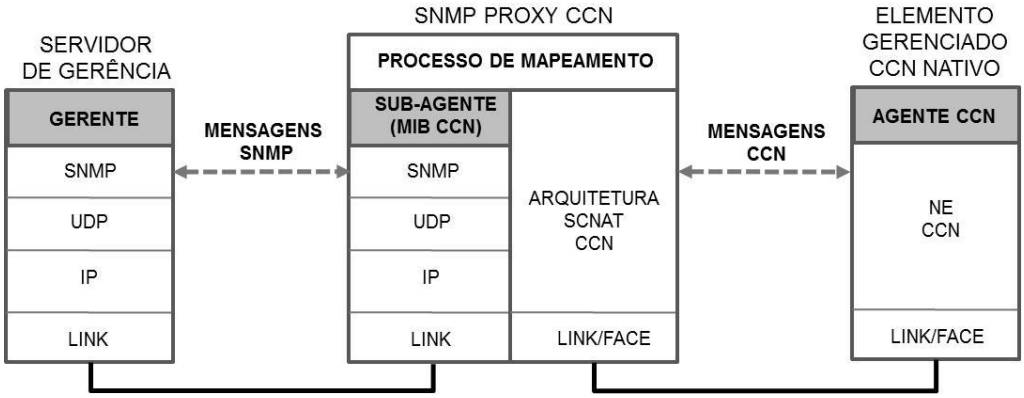

Figura 5: Arquitetura do SNMP Proxy CCN.

A arquitetura utilizará dois tipos de agentes, um *sub-agente* e um *agente ccn* nativo, como descritos abaixo:

Sub-agente: Responsável por mapear as consultas SNMP feitas aos objetos (OIDs) da MIB CCN para pacotes *Interest* que serão encaminhados para a rede CCN.

Agente CCN: Responsável por gerar os conteúdos mapeados de acordo com a MIB CCN, que serão encaminhados para o SNMP Proxy CCN no formato de pacotes *Data* (nativo CCN) como resposta às solicitações dos pacotes *Interest*.

5. Mapeamento das operações básicas do SNMP através do SCNAT

5.1 Nomeação e descoberta dos nós

Antes do processo de mapeamento das operações básicas do SNMP para CCN, é necessário conhecer os elementos existentes na rede CCN. A descoberta dos *nomes* ou *labels* destes elementos pode ser feita de forma hierárquica durante o *processo de troca de mensagens de controle* do protocolo de roteamento adotado, desta forma o *nome ou label* se torna um identificador exclusivo de cada elemento na rede CCN, por exemplo; */<network>/site/<ne>/* [8].

Descoberta de nomes. Do lado da interface com a rede CCN, o SNMP Proxy CCN manterá uma tabela dinâmica com os nomes dos nós conhecidos na rede.

5.2 Mecanismo de tradução SCNAT

O Proxy SNMP CCN deve ter um *sub agente* implementado com uma imagem da MIB CCN de modo que ele possa acessar os objetos definidos para gerenciamento dos nós CCN, e utilizará o campo "*Community*" (string formada em texto plano) da PDU do SNMPv1 e SNMPv2 como parâmetro para informar com qual *Label/NE* deseja se comunicar. O campo "*ContextName*" terá a função do "*Community*" para o protocolo SNMPv3.

Consulta: Do lado da interface com a rede IP, o SNMP Proxy CCN mantém uma tabela correspondente ao *OID* e o campo "*Community*" da mensagem que será usado para identificar o *nome* ou *label* do nó de destino. A tabela é formada pelos campos; *IP de origem*, *Porta de origem*, *IP de destino*, *Porta de destino*, *RequestID* e *OID* (MIB CCN) de acordo com a consulta feita pelo Gerente (NMS).

Neste caso, a ferramenta Proxy saberá que a mensagem recebida trata-se de uma mensagem que deve ser mapeada para o mundo CCN com a definição de valor de porta diferente da porta 161 (ex.: uma porta alta qualquer), que servirá como um indicador na mensagem GET do SNMP informando que se trata de uma mensagem para ser mapeada para CCN e não de uma mensagem para um agente SNMP no próprio Proxy, sendo assim uma porta específica do SNMP, de modo que o Proxy saiba que aquela mensagem é para ser convertida e encaminhada a um nó CCN.

O campo *RequestID* do protocolo SNMP é utilizado para identificar as mensagens de requisição geradas pelo processo gerente, uma vez que um gerente pode fazer múltiplas requisições SNMP para o mesmo agente.

O campo *OID* será mapeado para o campo "*Conteúdo*" que juntamente com a informação do campo "*Community*" formará o pacote de interesse contido no campo "*Pacote de interesse"* que finalmente será encaminhado para a rede CCN.

Tabela 2: A string do campo "*Community*" será utilizada para identificar o NE que deseja se comunicar.

IP origem (NMS)	Porta Origem (NMS)	IP destino (Proxy)	Porta Destino (Proxy)	Community (Proxy)	ResquestID (NMS)	OID (MIB CNN)
10.0.0.100/24	20000	10.0.0.1/24	64000	Label-NE1	0	1.3.6.1.2.x.1.1
10.0.0.100/24	20000	10.0.0.1/24	64000	Label-NE2	1	1.3.6.1.2.x.1.2
10.0.0.200/24	30000	10.0.0.1/24	64000	Label-NE2	0	1.3.6.1.2.x.1.3

Tabela 3: Formação do pacote de interesse de acordo com o conteúdo das colunas "Community" e "Conteúdo"

Community (Proxy)	**OID (MIB CNN)**	**Conteúdo**	**Pacote de Interesse**
Label-NE1	1.3.6.1.2.x.1.1	**ccnSystem/sysDesc**	/Label-NE1/**ccnSystem/sysDesc**
Label-NE2	1.3.6.1.2.x.1.2	**ccnSystem/sysObjectID**	/Label-NE2/**ccnSystem/sysObjectID**
Label-NE2	1.3.6.1.2.x.1.3	**ccnSystem/sysUpTime**	/Label-NE3/**ccnSystem/sysUpTime**

Resposta: Após a entrega do pacote *Interest* do SNMP Proxy CCN para a rede CCN nativa formado pelo mapeamento descrito anteriormente, a rede deve retornar como resposta um pacote *Data* levando em consideração a arquitetura do modelo CCN. Quando o SNMP Proxy CCN receber o pacote *Data* de volta como resposta, a mensagem *PDU Response* será formada de acordo com o conteúdo da tabela que mantém o mapeamento do campo *IP origem* e *Porta de origem*, na volta os valores serão utilizados agora como *destino,* para identificação do Gerente (NMS) que fez a solicitação no início.

Tabela 4: Formação da "PDU Request", para entrega do conteúdo solicitado de volta ao Servidor Gerente (NMS).

IP destino (NMS)	**Porta destino (NMS)**	**ResquestID (NMS)**	**IP origem (Proxy)**	**Conteúdo**
10.0.0.100/24	20000	0	10.0.0.1/24	**ccnSystem/sysDesc**
10.0.0.100/24	20000	1	10.0.0.1/24	**ccnSystem/sysObjectID**
10.0.0.200/24	30000	0	10.0.0.1/24	**ccnSystem/sysUpTime**

6. Mapeamento das operações básicas do SNMP para CCN

6.1 Operação GET

Com uso da arquitetura SCNAT será possível iniciar uma consulta ao nó CCN nativo através da operação *GET* do SNMP. Como exemplo, podemos usar uma consulta feita para o objeto "*sysUptime"* (sob o objeto *ccnSystem*) do elemento "*NE1"*. O servidor de gerência "*Host Gerente"* inicia uma consulta SNMP "*GET Request"* para o OID "*1.3.6.1.2.x.1.3"*, que reflete o objeto "*ccnSystem/sysUpTime"* (**1**), o campo "*Community"* deve ser preenchido com o "*label/nome"* do nó que deseja consultar, como exemplo, "*label_NE1"*. O SNMP Proxy CCN converte a mensagem para um pacote de interesse mapeado como "*Interest /NE1/ccnSystem/sysUpTime*" e envia o pacote para a rede de elementos CCN (**2**). Se o elemento "*NE1"* tem o conteúdo *"/NE1/ccnSystem/sysUpTime*" (como objeto do nó label_NE1 mapeado da MIB CCN),

ele responde a requisição imediatamente com a mensagem de dados, exemplo "*Data /NE1/ccnSystem/sysUpTime*". O SNMP Proxy CCN converte a mensagem de dados "*/NE1/System/sysUpTime*" para uma mensagem padrão SNMP "*GET Response*". Se a consulta fosse feita para outro elemento da rede mais distante, "*NE2*" por exemplo, o "*NE1*" armazena o interesse em sua tabela "*PIT*" e encaminha a mensagem para os próximos nós na rede até que o conteúdo seja localizado (**3**). Por fim, o conteúdo localizado é armazenado no "*cache*" de cada *NE* para satisfação das pendências do pacote de interesse (**4**). Como grande parte dos objetos gerenciáveis na MIB CCN são objetos dinâmicos (ex.: informação sobre o número de pacotes de interesse), é recomendado que apenas alguns valores de objetos sejam armazenados no cache dos nós intermediário na rede CCN (ex.: número de interface de rede físicas de um elemento). Após a entrega do conteúdo finalmente para o SNMP Proxy CCN (**5**), o mesmo é encaminhado para o Host Gerente que a solicitou no início da consulta (**6**). Os passos descritos acima são apresentados na figura 6.

As demais operações básicas do SNMP tais como: "*GET-NEXT*", "*GET-BULK*" e "*SET*" embora mais complexas, podem ser mapeadas seguindo o mesmo princípio, com a diferença que a operação "*GET-NEXT*" consulta o próximo OID na hierarquia e o "*GET-BULK*" consulta um número maior de OIDs, de acordo com o valor do parâmetro *max-repetitions*. A operação "*SET*" tem como objetivo alterar o valor de um objeto.

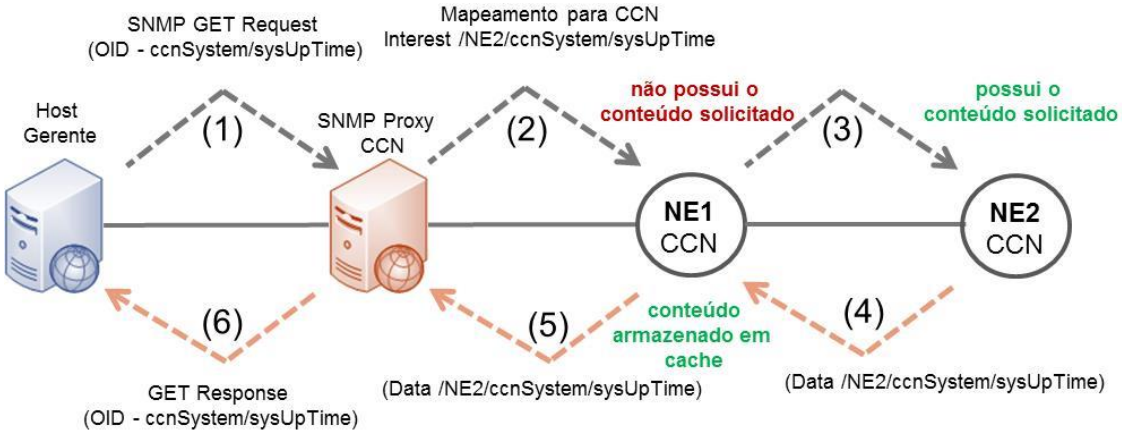

Figura 6: Passos para mapeamento da consulta da operação "GET".

6.2 Uso do Publishe/Subscribe para mapeamento da TRAP

Com base no modelo de comunicação Publishe/Subscribe [14, 15, 16], temos como proposta inicial o uso do mecanismo "*Publishe/Subscribe Event Notification*" para tratar a notificação de eventos na plataforma SNMP Proxy CCN. A ferramenta SNMP Proxy CCN deve implementar o processo "*Forwarding Tables/Notification Service*" que fará o gerenciamento das mensagens de publicação e assinaturas de eventos, também deverá implementar o processo "*Sub-agente Consumer*" que deve agir como *Consumer/Subscriber* do sistema. O Agente CCN deve implementar o processo "*Producer/Publisher*" que fornecerá a publicação dos eventos relacionados aos objetos gerenciados que podem mudar o seu estado (ex.: linkDown, linkUP).

Os processos no SNMP Proxy CCN e nó CCN estão classificados abaixo:

SNMP Proxy CCN

- Forwarding tables/Notification Service
- Consumer/Subscriber

Nó CCN

- Producer/Publisher

6.3 Mapeamento da operação "TRAP" do SNMP para CCN

O *sub-agente* da ferramenta *Proxy* deve cadastrar os servidores gerentes que receberão as *TRAPs*, como é feito no modo convencional (**1**). A ferramenta SNMP Proxy CCN deve implementar os processos "*Consumer*" e "*Notification Service*", o processo *Consumer* expressará ao processo *Notification Service* o interesse em eventos específicos que deseja monitorar, como por exemplo; "*Interest/label_NE/ccnSystem/linkDown*" e "*Interest /label_NE/ccnSystem/linkUP*" (**2**). O processo "*Producer*" implementado no elemento CCN deve informar ao *Proxy* a publicação dos conteúdos "*/NE1/ccnSystem/linkDown*" e "*NE1/ccnSystem/linkUP*" (**3**). Se o conteúdo/estado do "*Interest /label_NE/ccnSystem/linkUP*" é alterado para "*Interest /label_NE/ccnSystem/linkDown*", o mesmo é encaminhado para o *Proxy* (**4**). Em seguida o pacote é convertido para o formato de uma *TRAP SNMP* e encaminhado para os servidores gerentes cadastrados para receber as *TRAPs* (**5**).

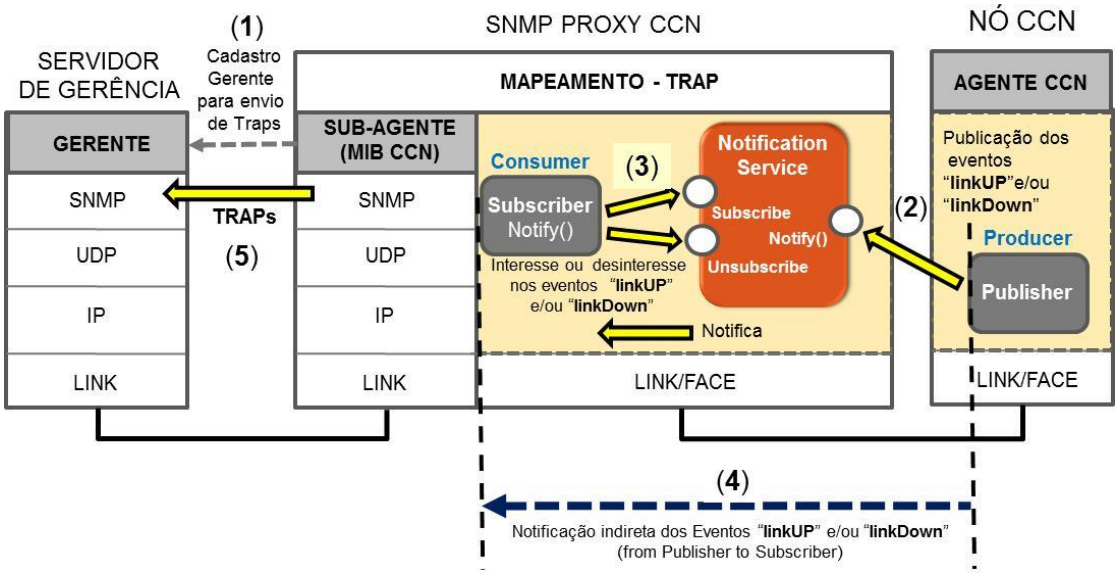

Figura 7: Arquitetura "Publishe/Subcribe Event Notification" para o SNMP Proxy CCN.

7. Conclusão e Trabalhos Futuros

Uma solução eficiente para gerencia de elementos CCN nativos com uso de gerentes SNMP em redes IP, abre espaço para novas discussões sobre a interoperabilidade entre redes legadas e redes orientadas a conteúdo.

Entre as vantagens da arquitetura proposta, é apresentada a possibilidade de tornar os sistemas convencionais (SNMP, NETCONF ou outros) compatíveis com novos sistemas e paradigmas (ex.: CCN), uma vez que a migração destas arquiteturas pode ser feita de forma gradual sem a necessidade de grandes alterações na infraestrutura já existente. Desta forma podemos afirmar que a ferramenta SNMP Proxy CCN serve como um facilitador no processo de migração das plataformas legadas.

Outro ponto a se observar é a possível diminuição de custos de operação das redes de telecomunicações, uma vez que o elemento gerenciado passa a ser localizado através do seu "*label/nome*" que se mostra totalmente desacoplado do endereçamento IP convencional, no que se refere ao controle destes endereços em grandes redes (centenas e milhares de elementos) devido a sua arquitetura mais complexa de planejamento.

Como trabalhos futuros inclui-se o desenvolvimento de uma prova de conceito da arquitetura para avaliação experimental no Mini-CCNx [17] e a inclusão dos resultados como contribuição para futuras discussões. Existe também a possibilidade de novas pesquisas para a criação de um gerente CCN nativo além do agente CCN já proposto neste trabalho.

Referências

[1] de Brito, G. M., Velloso, P. B., and Moraes, I. M. (2012). "Redes Orientadas a Conteúdo: Um Novo Paradigma para a Internet", In Minicursos SBRC 2012.

[2] Jacobson, V., Smatters, D. K., Thornton, J, D., Plass, M, F., N, H., Briggs, R, L., Braynard, "Networking Named Content". Palo Alto Research Center. Palo Alto, CA, USA. 2009.

[3] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica: "*A Data-Oriented (and Beyond) Network Architecture*", In ACM SIGCOMM 2007.

[4] Jokela, P., Zahemszky, A., Rothenberg, C., Arianfar, S., Nikander, P.: "*LIPSIN: Line Speed Publishe/Subscribe Inter-Networking*", In ACM SIGCOMM 2009.

[5] Xylomenos, G. and *et al*..: "*A Survey of Information-Centric Networking Research*", Communications Surveys & Tutorials, IEEE, 2013

[6] Kang, W., Sim B., Kim, J., Paik, E., Lee, E.: "*A Network Monitoring Tool for CCN"*, Daejeon, Seoul, Korea 2012

[7] Chavan, S. S. and *et al*..: " *Generic SNMP Proxy Agent Framework Management of Heterogeneous Network Elements*", Communication Systems and Networks and Workshops, IEEE, 2009

[8] A, K, M, Mahmudul Hoque, Syed Obaid Amin, Adam Alyyan, Beichuan Zhang, Lixia Zhang, Lan Wang, "*NLSR: Named-data Link State Routing Protocol*", In ACM SIGCOMM Workshop on ICN, Aug. 2013.

[9] Webnms (2014) – Introdução ao protocolo TL1. Disponível *online*:

http://www.webnms.com/webnms/help/developer_guide/management_protservices/mgmnt_protocols/tl1/proto_tl1_intro.html

[10] Nunes, S., David, G.: "*Uma Arquitectura Web para Serviços Web*", in XATA 2005.

[11] Netconf Central (2014) – Acesso: Marc/2014, Disponível *online*:

http://www.netconfcentral.org/netconf_docs

[12] Kurose, J. F, Ross, K. W: "*Redes de Computadores e a Internet – Uma abordagem top-down*", 3 Edição, 2005

[13] Mauro, R. D, Schmidt, K. J: "*Essential SNMP, Second Edition*", 2005

[14] Virgillito, A., "*Publishe/Subscribe Communication Systems: from Models to Applications*", Phd Thesis, Universita "La Sapienza", Aug. 2003

[15] Eugster, P., Felber P. A., Guerraoui, R., Kermarrec, A., "*The Many Faces of Publishe/Subscribe"*, *ACM Comput. Surv.* 35, 2 (June 2003) Jun. 2003

[16] Carzaniga, A., Palpaline, M., Wolf, L. A., "*Content-Based Publishe/Subscribe Networking and Information-Centric Networking"*, ACM SIGCOMM Workshop on ICN, Aug. 2011

[17] Cabral, C., Rothenberg, C., Magalhães, M.: "*Mini-CCNx: prototipagem rápida para Redes Orientadas a Conteúdo baseadas em CCN*", In Salão de Ferramentas do SBRC 2013.