

# SNMP Gateway CCN: Software de gerência de redes orientadas a conteúdo interoperável com sistemas legados

Marciel de Lima Oliveira<sup>1</sup>, Christian Esteve Rothenberg<sup>1</sup>

<sup>1</sup> 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, Cidade Universitária Zeferino Vaz, Campinas, SP, Brasil

{marciel, chesteve}@dca.fee.unicamp.br

**Abstract.** *Research on Information-Centric Networking (ICN) mainly focuses on the data and control plane design and implementation challenges compared to the efforts devoted on the management plane. Aiming at addressing this gap, this paper presents some mapping mechanisms and the SNMP Gateway CCN tool, enabling the management and monitoring of CCN nodes through legacy SNMP-based systems. The tool allows exploring the concept of content-oriented management (name/data) in emulated environments.*

**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 alguns mecanismos de mapeamento e a ferramenta SNMP Gateway CCN, que permite o gerenciamento e monitoramento de nós CCN através de sistemas de gerência de redes legadas baseados no protocolo SNMP (Simple Network Management Protocol). A ferramenta possibilita explorar o conceito de gerência orientada a conteúdo (nomes/dados) em ambientes emulados.*

## 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 dados 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 redes central NMS (*Network Management System*), que atua no monitoramento e operação das três grandes divisões das redes (plano de dados) de equipamentos de telecomunicações, núcleo (ex.: DWDM), agregação (ex.: MPLS-TP, Metro-Ethernet) e acesso (ex.: LTE/4G, xDSL, FTTH). 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 [de Brito et al. 2012]. 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 [Jacobson et al. 2009], que apresenta uma estrutura hierárquica para nomes semelhante às URLs; DONA [Koponen et al. 2007], que utiliza o mecanismo de nomeação plana e funções de hash criptográfico e LIPSIN [Jokela et al. 2009] 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 [Xylomenos et al. 2014]. 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.

## 2. Motivação e Objetivo

A motivação principal deste artigo deve-se à percepção da carência de paradigmas adequados à gerência de redes orientadas a conteúdo [Kutscher et al. 2016]). 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, SNMP, CLI, WEB UI e NETCONF/YANG [web 2014, Nunes and David 2005, James and ROSS 2006, Mauro and Schmidt 2005, net 2014, Schonwalder et al. 2010], transformando-as em ferramentas eficientes para a gerência de redes CCN [Oliveira and Rothenberg 2014].

A arquitetura CCN (*Content-Centric Networking*) [Jacobson et al. 2009] adotada como referência nesse trabalho é reconhecidamente uma das propostas mais relevantes na literatura relativamente às redes orientadas a 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 do label/nome como identificador único de um nó na rede CCN e o mapeamento de mensagens através de um gateway. Essa estratégia é denominada NONM (*Named-Oriented Network Management*) [Oliveira and Rothenberg 2014], tem como principal tarefa compatibilizar a gerência tradicional baseada no protocolo SNMP (*Simple Network Management Protocol*), com o modelo CCN, dessa forma permitir a gerência de elementos de rede CCN nativos.

### 3. Projeto e arquitetura para gerência de redes orientada a conteúdo

A modelagem de uma ferramenta SNMP Gateway CCN é o primeiro passo em direção à adoção de mecanismos para gerência de redes CCN, sejam nativas ou overlay. Para gerenciar elementos das redes orientadas a conteúdo, optamos pelo SNMP por se tratar de um protocolo largamente conhecido, que se mostra mais eficiente do ponto de vista de monitoramento e alarmes, em relação a outros protocolos que tem maior destaque na configuração. A ferramenta SNMP Gateway CCN tem como uma de suas principais características o uso de uma arquitetura de gerência de redes *in-band*, que atua em conjunto com o plano de dados para monitoramento dos elementos de rede. Neste contexto o pacote de interesse (requisição) é formado pelo nome do conteúdo monitorado que deseja consultar e o *payload* do pacote de dados (resposta) carrega o valor do objeto consultado.

#### 3.1. Mecanismo de tradução SCNT

O método SCNT (*SNMP Content Network Translation*) tem como principal objetivo permitir a utilização do campo *ContextName* (string formada em texto plano) da mensagem PDU do protocolo SNMPv3, como meio para passagem de parâmetro para informar ao gateway qual elemento deseja consultar na rede CCN. O campo *Community* existente nas versões SNMPv1 e SNMPv2 do protocolo também poderia ser usado para esse propósito, porém a funcionalidade do campo teria que ser redefinida. Por tanto, a ferramenta *SNMP Gateway CCN* não possui suporte para as versões 1 e 2 do protocolo. O valor do campo *Object-Name* que representa o OID (*Object identifier*), é utilizado em conjunto com o valor do campo *contextName*, para formar a mensagem *Interest* no processo de consulta. Após a entrega da mensagem *Interest* do *SNMP Gateway CCN* para a rede CCN, formada pelo mapeamento descrito anteriormente, a rede deve retornar como resposta um pacote *Data*, levando em consideração a arquitetura do modelo CCN. Quando o *SNMP Gateway CCN* recebe o pacote *Data* de volta como resposta, a mensagem *PDU Response* é formada de acordo com o conteúdo recebido e é encaminhada de volta para o Gerente (NMS) que fez a solicitação no início no processo.

#### 3.2. MIB CCN

Neste trabalho definimos uma MIB (*Management Information Base*) [Walsh 2008] para a rede CCN com o mesmo propósito da MIB apresentada em [Kang et al. 2012], que se diferencia nos aspectos relativos à gerência de objetos refletidos em um agente CCN nativo, ao contrário de um agente SNMP convencional, e posicionamento sob o ramo da MIB-2 com OID 100, ao invés do ramo *private*, desta forma podemos utilizar a filosofia de extensibilidade da mib padrão. A MIB CCN é apresentada de forma resumida na Figura 1.

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 fica sob hierarquia da MIB-2 e está classificada em duas partes, a primeira parte representa objetos de *ccnSystem* que tratam informações do próprio nó, e a segunda parte trata objetos específicos para monitoramento de protocolo CCN através da coleta de dados da daemon *ccndStatus*. O nó CCN possui características que o torna único em relação à arquitetura de outros elementos das redes, pois possui tabelas de controle diferenciadas para tratamento e roteamento de pacotes/conteúdo.

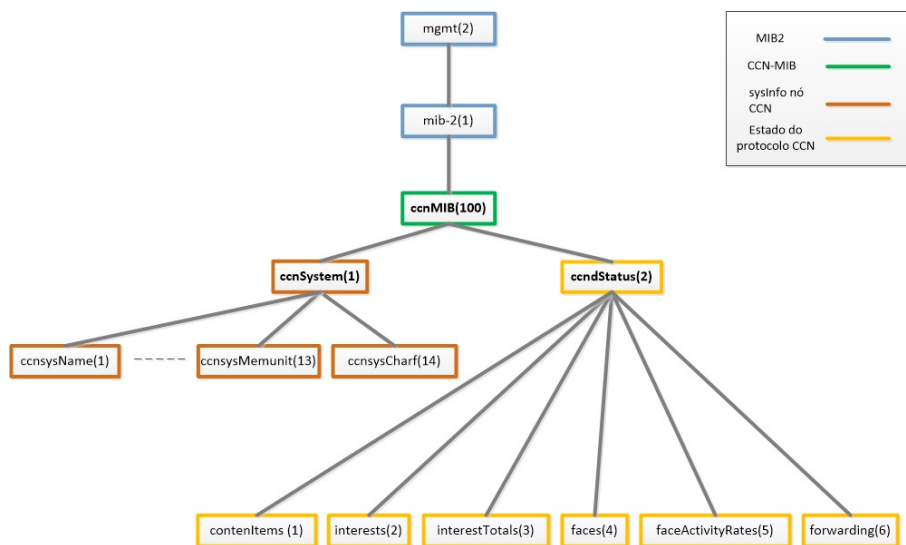


Figura 1. A MIB CCN e sua sub-árvore.

### 3.3. Visão geral da ferramenta

A ferramenta *SNMP Gateway CCN* foi implementada tendo como foco a operação *GET*, levando em consideração as garantias das funcionalidades mínimas. A plataforma *MiniCCNx* [Cabral et al. 2013] foi utilizada como ambiente para troca de mensagens entre o *gerente IP* e o *Agente CCN*, que também compõe a rede de elementos CCN. A plataforma *MiniCCNx* foi escolhida por ser considerada robusta e confiável para coleta de evidências que comprovem o funcionamento e eficácia dos experimentos. Do ponto de vista de um ambiente CCN nativo, a plataforma *MiniCCNx* possui características de um emulador que permite executar aplicações reais, necessárias para auxiliar na interação do *SNMP Gateway CCN*, com o agente nativo do ambiente emulado.

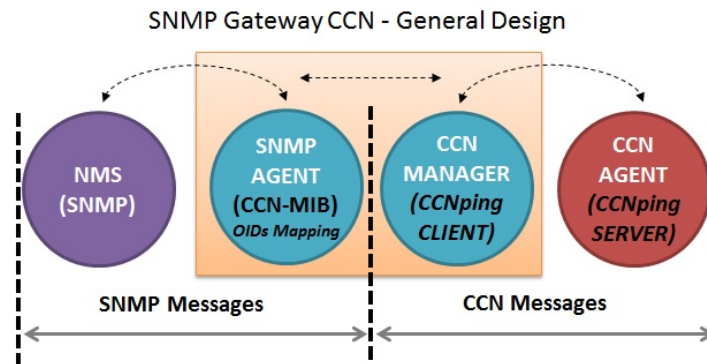
A ferramenta *SNMP Gateway CCN* é composta basicamente das partes; *MIB CCN*, *Agente SNMP* e as ferramentas *ccnmanager* e *ccnagent* (Agente CCN nativo) que compõem a arquitetura *SCNT*.

**MIB CCN.** A MIB CCN deve implementar todos os objetos (OIDs) definidos para gerência e monitoramento dos elementos CCN nativos. A implementação da MIB segue as especificações da RFC 3418, definida com base no padrão SMI (*Structure of Management Information*).

**Agente SNMP.** O Agente SNMP é capaz de interpretar as consultas SNMP feitas para o objetos mapeados na MIB CCN da hierarquia, em seguida traduz as mensagens que são encaminhadas para rede de elementos CCN nativos.

**Agente CCN.** O agente CCN nativo, tem como principal objetivo fornecer conteúdo em resposta às requisições originadas do gateway, os conteúdos devem refletir exatamente cada objeto do elemento de rede gerenciado, que estão diretamente relacionados com os OIDs especificados na MIB CCN.

Conforme ilustrado na Figura 2, a ferramenta *SNMP Gateway CCN* é capaz de receber mensagens SNMP do tipo *Request* e traduzi-las para mensagens CCN do tipo



**Figura 2. Visão geral da ferramenta *SNMP Gateway CCN***

*Interest*, o mesmo processo deve ocorrer no sentido inverso, ou seja, receber mensagens CCN do tipo *Data* e convertê-las para mensagens SNMP do tipo *Response*, o mecanismo de tradução atua de forma totalmente transparente do ponto de vista do NMS.

#### 4. Plano de demonstração da ferramenta

Os principais componentes da ferramenta serão apresentados inicialmente, assim como as configurações necessárias para preparação do ambiente emulado. O MIB Browser *Snmplib* deve ser utilizado para carregar a MIB CCN que por sua vez será responsável por gerar as mensagens de consulta SNMP encaminhadas ao Agente SNMP executado no gateway, por tanto, terá o papel do NMS (vide Figura 3 ilustrativa).

A ferramenta será demonstrada em duas etapas, na primeira etapa o funcionamento da operação *SNMP GET* será avaliado passo a passo, na segunda etapa devemos exercitar o funcionamento da operação *SNMP WALK*, que tem o objetivo de consultar todos os objetos da MIB CCN.

A topologia de referência adotada para validação da prova de conceito, apresenta um cenário com 10 elementos de rede CCN, pré-configurado no ambiente MiniCCNx. Com a auxílio da ferramenta *MiniccnxEdit*, a topologia foi construída em anel, com alguns elementos ramificados no formato linear. Por fim, todas as configurações da topologia foram armazenadas no arquivo *r1-r10.mnccnx* para facilitar a restauração do ambiente quando necessário. Para nomeação dos elementos de rede, adotamos o prefixo *r* que representa a inicial da palavra *router*, seguido de um número de 1 até 10.

Para verificar a troca de mensagens SNMP e CCN, adotamos o analisador de protocolos de rede *Wireshark* juntamente com um plugin<sup>1</sup> específico para suporte à análise de mensagens do protocolo CCNx.

##### 4.1. Teste funcional da operação *SNMP GET*

Tendo como base a topologia de referência, o elemento de rede CCN *r1* foi escolhido como gateway de rede. O objetivo inicial é consultar o valor de um objeto qualquer em um elemento de rede distante do gateway, deste modo, uma mensagem de consulta *SNMP*

<sup>1</sup>O plugin de CCNx para *Wireshark* foi compilado e instalado conforme instruções do projeto abaixo. <https://github.com/ProjectCCNx/ccnx/blob/master/apps/wireshark/README-wireshark-1.6.txt>

*GET Request* deve partir do elemento *r1* e alcançar o elemento alvo, uma mensagem *SNMP GET Response* deve retornar ao gateway em resposta à requisição. A interface de rede *lo* (loopback/IP 127.0.0.1) será monitorada no elemento de rede gateway para captura das mensagens SNMP. As interfaces *eth-0* e *eth1* serão monitoradas para captura das mensagens CCN. Abaixo seguem os passos e o comportamento esperado como resultado para o teste funcional da operação SNMP GET:

**Passos:**

- O *Mib Browser SnmpB* deve ser configurado para preencher o campo *contextName* do protocolo SNMPv3 conforme o nome do elemento de rede que deseja consultar.
- Executar o *Wireshark* para monitorar as interfaces de rede *lo*, *eth0* e *eth1* do elemento gateway *r1*.
- A partir do *Mib Browser*, iniciar uma consulta *SNMP GET Request* para uma OID da MIB CCN.
- Na captura realizada na interface *lo* do gateway *r1*, deve ser possível verificar a existência de uma mensagem de requisição *SNMP GET* na versão 3, o campo *contextName* preenchido com o label definido no *Mib Browser*, e na sequência uma mensagem de resposta *SNMP GET Response* com o valor solicitado.
- Nas capturas realizadas nas interfaces *eth0* e *eth1* do gateway, deve ser possível verificar a existência de uma mensagem CCN de requisição *Interest* e na sequência uma mensagem de resposta *Data* com o valor solicitado.

#### 4.2. Teste funcional da operação SNMP WALK

O principal objetivo deste experimento é percorrer todos os 280 objetos da MIB CCN. Mensagens *Interest* de requisição devem partir do elemento *r1* e alcançar os elementos alvo, uma mensagem de resposta *Data* deve retornar ao gateway em resposta à cada requisição. As interfaces *eth-0* e *eth1* serão monitoradas para captura das mensagens CCN. Abaixo seguem os passos e o comportamento esperado como resultado para o teste funcional da operação SNMP WALK:

**Passos:**

- O *Mib Browser SnmpB* deve ser configurado com o valor do campo *contextName* do elemento de rede que deseja consultar, podemos exercitar a consulta para qualquer um dos elementos da topologia de referência.
- Executar o *Wireshark* para monitorar apenas as interfaces de rede *eth0* *eth1* do elemento gateway *r1*.
- A partir do *Mib Browser*, iniciar uma consulta *SNMP WALK Request* a partir do OID principal da MIB CCN.
- Nas capturas realizadas nas interfaces *eth0* e *eth1* do gateway, deve ser possível verificar a existência de uma mensagem CCN de requisição *Interest*, e na sequência uma mensagem de resposta *Data* para cada valor solicitado.

O código fonte aberto da ferramenta *SNMP Gateway CCN* está disponível online<sup>2</sup>

---

<sup>2</sup><https://github.com/marcieloliveira/snmp-gateway-ccn>

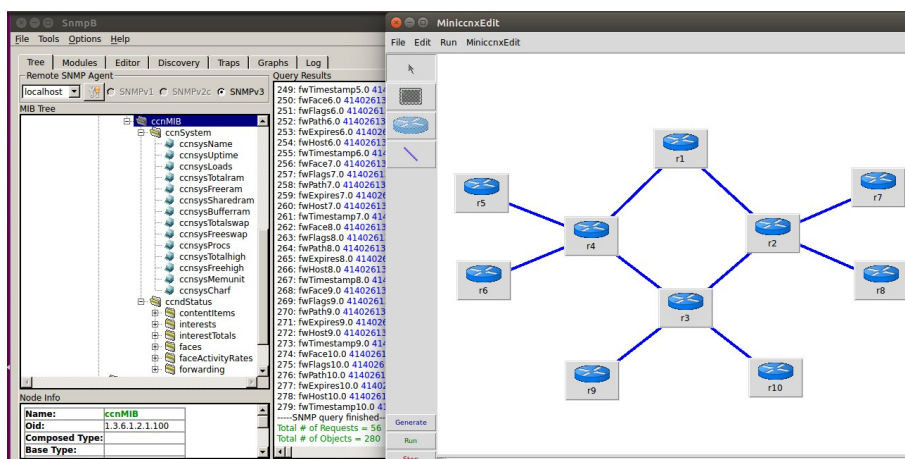


Figura 3. Ferramenta *SNMP Gateway CCN* em funcionamento.

juntamente com um tutorial para utilização, uma imagem da máquina virtual do ambiente completo e um vídeo<sup>3</sup> com a demonstração funcional da ferramenta.

## 5. Conclusão e Trabalhos Futuros

Uma solução eficiente para gerência 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/YANG 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 Gateway 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.

A ferramenta *SNMP Gateway CCN* atualmente se limita a algumas funcionalidades, dentre elas, as operações básicas do protocolo SNMP (*GET*, *GET-NEXT*, *GET-BULK* e *WALK*) e apresenta uma topologia de referência estática com apenas 10 elementos de rede, que tem como objetivo principal, experimentar a gerência de redes CCN e demonstrar a prova de conceito. Tais limitações demonstram lacunas a serem ocupadas do ponto de vista funcional, como por exemplo, a operação *SET* do SNMP. Deste modo, novas pesquisas também podem ser conduzidas para a criação de um *Gerente CCN* nativo além do *Agente CCN* já proposto neste trabalho, que permitiria desacoplar o ambiente legado (NMS SNMP/IP) do ambiente CCN e experimentar a relação *gerente/agente* em um cenário baseado apenas no modelo CCN.

<sup>3</sup><https://youtu.be/vIfCsDhPoSO>

## References

- (2014). *Netconf Central - Network Configuration Protocol*. URL: [www.netconfcentral.org](http://www.netconfcentral.org).
- (2014). *Webnms - Introdução ao protocolo TL1*. URL: [www.webnms.com](http://www.webnms.com).
- Cabral, C., Rothenberg, C. E., and Magalhães, M. F. (2013). Mini-ccnx: Fast prototyping for named data networking. In *Proceedings of the 3rd ACM SIGCOMM workshop on Information-centric networking*, pages 33–34. ACM.
- de Brito, G. M., Velloso, P. B., and Moraes, I. M. (2012). Redes orientadas a conteúdo: Um novo paradigma para a internet. *Minicursos do Simpósio Brasileiro de Redes de Computadores-SBRC*, 2012:211–264.
- Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., and Braynard, R. L. (2009). Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, pages 1–12. ACM.
- James, F. and ROSS, K. W. (2006). Redes de computadores e a internet: uma abordagem topdown.
- Jokela, P., Zahemszky, A., Esteve Rothenberg, C., Arianfar, S., and Nikander, P. (2009). Lipsin: Line speed publish/subscribe inter-networking. In *Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication, SIGCOMM '09*, pages 195–206, New York, NY, USA. ACM.
- Kang, W., Sim, B., Kim, J., Paik, E., and Lee, Y. (2012). A network monitoring tool for ccn. In *World Telecommunications Congress (WTC), 2012*, pages 1–3. IEEE.
- Koponen, T., Chawla, M., Chun, B.-G., Ermolinskiy, A., Kim, K. H., Shenker, S., and Stoica, I. (2007). A data-oriented (and beyond) network architecture. In *ACM SIGCOMM Computer Communication Review*, volume 37, pages 181–192. ACM.
- Kutscher, D., Eum, S., Pentikousis, K., Psaras, I., Corujo, D., Saucez, D., Schmidt, T., and Waehlich, M. (2016). Information-centric networking (icn) research challenges. Technical report.
- Mauro, D. and Schmidt, K. (2005). *Essential SNMP: Help for System and Network Administrators*. "O'Reilly Media, Inc."
- Nunes, S. and David, G. (2005). Uma arquitetura web para serviços web. *XATA 2005-XML: Aplicações e Tecnologias Associadas*.
- Oliveira, M. and Rothenberg, C. E. (2014). Snmp proxy ccn: Uma proposta de arquitetura para gerência de redes orientadas a conteúdo interoperável com sistemas legados.
- Schonwalder, J., Bjorklund, M., and Shafer, P. (2010). Network configuration management using netconf and yang. *IEEE communications magazine*, 48(9).
- Walsh, L. (2008). *SNMP MIB Handbook: essential guide to MIB development, use and diagnosis*. Wyndham.
- Xylomenos, G., Ververidis, C. N., Siris, V. A., Fotiou, N., Tsilopoulos, C., Vasilakos, X., Katsaros, K. V., and Polyzos, G. C. (2014). A survey of information-centric networking research. *IEEE Communications Surveys & Tutorials*, 16(2):1024–1049.