LARCES_PBM: Uma Ferramenta de Gerenciamento Baseado em Políticas para prover QoS*

Ana Luiza B. de P. Barros, André Luís de O. Campos, Daniel Pereira, Felipe Colares, Fernanda Lígia R. Lopes, Francisco Wagner C. Aquino, Joaquim Celestino Júnior, Laure W. N. Mendouga, Marcel M. de Alencar, Marcial P. Fernandez, Rafael R. Soares

[1]Departamento de Estatística e Computação – Universidade Estadual do Ceará (UECE)
Av. Paranjana, 1700 – Fortaleza – CE – Brasil

{analuiza, andre, daniel, felipecolares, fernanda, wagner,

celestino, marcel, marcial, laure, rafael}@larces.uece.br

Abstract. *Policy-Based Management has been a widely used architecture to configure and to provide QoS in networks build through different devices from varied manufacturers. This paper presents LARCES_PBM, a policy-based generic framework designed to provide QoS in any networks types. As study case, an prototype has been developed to WLAN wireless network management. From a considered testbed it was proved the correct policies application in this network type, which has demonstrated the architecture functionalities.*

Resumo. *O gerenciamento baseado em políticas tem sido uma arquitetura muito utilizada para configurar e oferecer QoS em redes construídas com diferentes equipamentos e de fabricantes diversos. Nesse artigo é apresentado o LARCES_PBM, um framework genérico de gerenciamento baseado em políticas implementado para oferecer QoS em quaisquer tipos de rede. Como estudo de caso, foi implementado um protótipo de gerenciamento de redes sem fio WLAN. A partir de um cenário de testes proposto comprovou-se a aplicação correta de políticas neste tipo de rede, o que demonstrou as funcionalidades da arquitetura.*

1. Introdução

Desde o surgimento das redes de comunicação propostas para o seu gerenciamento têm surgido. As soluções iniciais, voltadas para monitoramento e configuração individual de cada dispositivo, foram se tornando impraticáveis ou altamente exaustivas devido ao crescimento das redes e à conseqüente diversificação dos tipos de dados trafegados, os quais possuem diferentes exigências em termos de QoS. Administradores de redes e operadores de telecomunicações, desde então, desejam automatizar o processo de configuração dos nós da rede. Esta automatização visa de controlar o fluxo de dados que transitam, tentando prover a QoS necessária e facilitar a gerência dos equipamentos.

Devido a essas necessidades, foi padronizado pelo IETF/DMTF (*Internet Engineering Task Force* e *Distributed Management Task Force*) uma nova forma de definir o comportamento de redes, altamente aceito e reconhecido, denominado Gerenciamento de Redes Baseado em Políticas (*Policy-Based Network Management* - PBNM).

*Trabalho realizado com recursos da HP Brasil P&D referentes à Lei nº 10.176 (Lei de Informática).

O LARCES desenvolveu um *framework* genérico denominado LARCES_PBM, baseado no modelo padronizado pelo IETF/DMTF, para gerenciamento baseado em políticas envolvendo qualidade de serviço em diversos tipos de redes, cabeadas ou sem fio, bastando apenas que o mesmo seja adaptado para cada tipo. Como estudo de caso, foi desenvolvido um protótipo voltado a redes sem fio WLAN, tendo em vista as dificuldades encontradas no gerenciamento de redes deste tipo.

O artigo é organizado da seguinte forma: na seção 2 é apresentado o modelo teórico proposto pelo IETF/DMTF. A arquitetura do *framework* desenvolvido é apresentada na seção 3. Testes realizados para validação da ferramenta e seus resultados são descritos na seção 4. A seção 5 apresenta a conclusão geral do trabalho e os possíveis trabalhos futuros.

2. Modelo Teórico

A arquitetura padronizada pelo IETF/DMTF é baseada no uso de políticas para o gerenciamento de redes. Segundo Moore et al. [Moore 2001], , políticas são um conjunto de regras para administrar, gerenciar e controlar o acesso a recursos da rede. A arquitetura consiste em quatro elementos básicos (Figura 1): uma ferramenta para gerenciamento de políticas (*Policy Decision Point* - PDP) e pontos para aplicações de políticas (*Policy Enforcement Points* - PEPs) [Verma 2000].

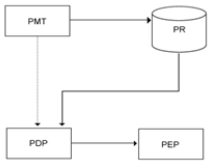

Figura 1. Arquitetura proposta pelo IETF

O PMT é utilizado pelo administrador para inserir as diferentes políticas a serem aplicadas à rede. O PR é um repositório de dados específico, que armazena regras (condições e ações) de políticas e os dados relacionados às políticas [Westerinen 2001]. As informações armazenadas no repositório devem seguir convenções. Estas convenções são especificadas como modelo de informações. O PDP é a entidade lógica responsável por tomar decisões sobre políticas para ele próprio ou para outros elementos que requisitem tais decisões [Yavatkar 2000]. Os PEPs são entidades lógicas que aplicam as decisões tomadas pelo PDP. Enquanto PMT e PDP são módulos genéricos, o PEP é específico para um certo tipo de dispositivo, ou seja, para cada tipo de dispositivo é necessário um PEP. Assim, vários dispositivos semelhantes podem ser submissos às ordens de um único PEP.

3. Arquitetura LARCES_PBM

O *framework* LARCES_PBM (Figura 2) possui todos os módulos da arquitetura padronizada pelo IETF/DMTF. O PMT, o PDP e o PEP foram desenvolvidos em Java e, conseqüentemente, são multi-plataforma.

Para se obter maior escalabilidade e reforçar seu caráter genérico, o framework é customizado a partir de arquivos XML. Alterando os parâmetros destes arquivos, é

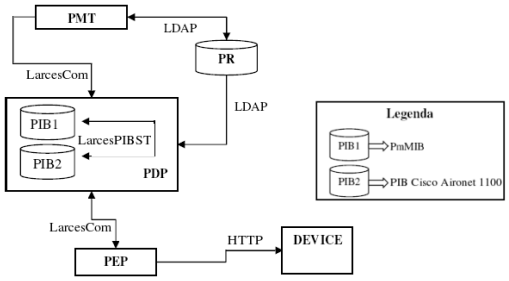

Figura 2. Arquitetura do Framework LARCES_PBM

possível, entre outras coisas, modificar o tipo de comunicação entre os módulos, modificar a base de dados utilizada, facilitar possíveis modificações no modelo de informações, adaptar o framework aos diferentes tipos de dispositivos e modificar as informações referentes à validação das políticas. A vantagem dessa abordagem é a não modificação do código-fonte.

3.1. Policy Management Tool (PMT)

O PMT consiste de uma interface onde o administrador (Figura 3) da rede insere acordos de serviço (*Sevice Level Agreements* - SLAs), que são traduzidas para políticas segundo um modelo de informações utilizado e, então, mapeadas para o formato compatível com o esquema de armazenamento utilizado pelo PR. O SLA é composto de condições e ação. Os elementos condicionais são aqueles que determinam sobre quais condições a regra será aplicada. São eles: cliente, destino, aplicação e período de validade. O serviço a ser provido é o elemento resultante (ação).

Antes do cadastro de SLAs algumas configurações e outros cadastros precisam ser realizados. Primeiramente, é preciso que seja definida a topologia da rede, inserindo os nós existentes na rede e as ligações entre eles. Também é necessário o cadastro de clientes, onde são indicados os dispositivos pertencentes a estes, e de aplicações, onde é indicado a porta e o protocolo desta. Também devem ser configurados os serviços que serão providos e seus parâmetros de QoS. Qualquer informação inserida, removida ou modificada é atualizada no PR. O conteúdo deste é apresentado através de um *browser*.

Visando garantir que o SLA seja cumprido, as políticas devem passar por processos um processo de validação. A validação sintática é responsável por verificar os dados quanto à sintaxe antes que estes sejam traduzidos para o nível de política. A validação semântica é dividida em duas partes: estática e dinâmica. A primeira verifica se os dados estão de acordo com as capacidades da rede. A segunda coleta os dados da situação real do sistema, no momento da aplicação da política, para verificar se esta pode ser aplicada. O PMT realiza a validação sintática, a validação semântica estática e a detecção estática de conflitos.

Para implementação dos mecanismos de validação, foram utilizados arquivos XML. Os dados a serem tratados no modelo de informações são definidos em XML e, caso ocorra alguma alteração no modelo ou na forma da política ser aplicada, não será necessária a modificação do código-fonte [Celestino 2006].

A seqüência de ações executadas no cadastro de informações é mostrada na Figura 4. Inicialmente, é construído um formulário de acordo com o tipo de informação

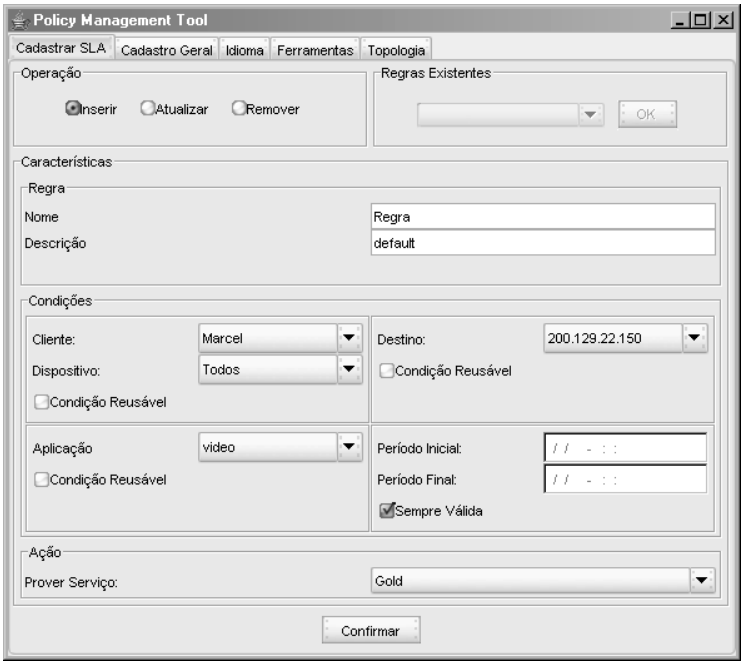

Figura 3. Tela para cadastro de SLAs

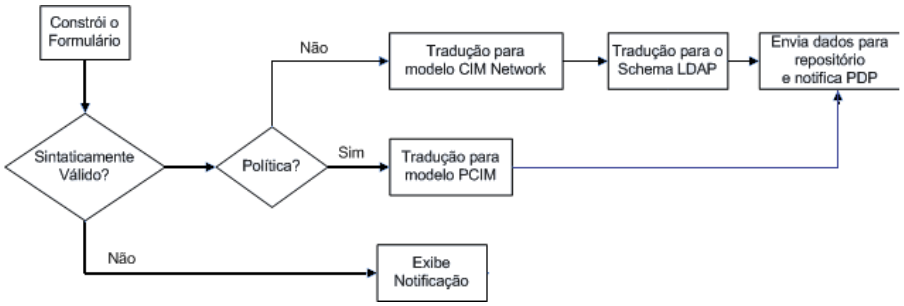

Figura 4. Fluxograma do cadastro de informações

cadastrada. Em seguida, é realizada a validação sintática e a tradução para o modelo de informações. Caso a informação seja uma política, é realizada a validação semântica estática. Ao final deste processo, é realizada a tradução do modelo de informações para o esquema de armazenamento do repositório, ocorre a atualização das informações do PR e o posterior envio de uma notificação ao PDP.

3.2. Policy Repository (PR)

O PR utilizado é responsável pelo armazenamento de informações dos recursos da rede, além das políticas. Ele providencia um ponto central de onde são tiradas as informações de gerenciamento de toda a rede. No *framework* foi utilizado um servidor LDAP pois, além de recomendado pelo IETF, sua padronização tem sido o foco de vários grupos de trabalho, como o DMTF. Outra característica relevante é a disponibilidade de um servidor de diretório livre, o OpenLDAP [OpenLDAP 2002], o qual foi utilizado no trabalho.

O modelo de informações utilizado foi o CIM [DMTF 2005], devido a este descrever as informações relevantes a gerência de redes. Este modelo é composto por vários sub-modelos como, por exemplo, o de redes (CIM_Network) e o de políticas

(PCIM). São utilizadas duas RFCs, PCIM [Moore 2001] e PCIMe [Moore 2003], para a padronização do sub-modelo PCIM. Entretanto, este sub-modelo não é suficiente para descrever políticas que visam obter QoS. Desta forma, foi necessária a extensão desses modelos para o *framework*.

Para que as informações possam ser armazenadas é necessário que seja feita a tradução do modelo de informações para o esquema de armazenamento do repositório. Moore et al. [Strassner 2004] e Burnner et al. [Burnner 2005] definem o mapeamento dos sub-modelos PCIM e PCIMe, respectivamente, para o equema de armazenamento do LDAP. Este mapeamento foi implementado no *framework*. Também foi realizado o mapeamento dos modelos estendidos para o esquema do LDAP.

3.3. Policy Decision Point (PDP)

O PDP é o bloco que se pode chamar de núcleo de todo o *framework* e, por essa razão, o mais complexo. Este bloco é responsável por interpretar as políticas armazenadas no repositório, tomar decisões acerca dessas políticas e enviá-las ao PEP para que possam ser executadas.

As principais funções do PDP são: tradução de políticas, configuração das PIBs (*Policy Information Bases*), detecção dinâmica de conflitos, validação dinâmica e distribuição de políticas aos PEPs subordinados, além da descoberta de recursos.

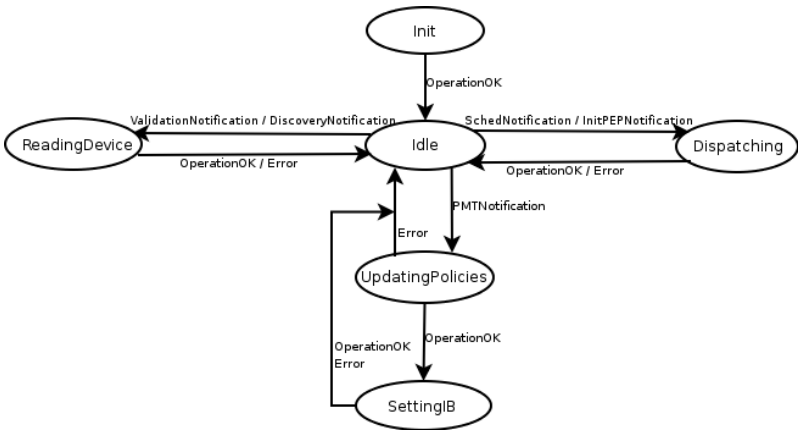

Figura 5. Diagrama de estados do PDP

O PDP possui seis estados (Figura 5). *Init* é o estado de inicialização do PDP, no qual são obtidas de arquivos XML as configurações iniciais necessárias. Outra função de *Init* é simular uma mensagem do PMT ao PDP para que este obtenha as políticas presentes no PR. O estado *Idle* é responsável por escutar e tratar as diferentes notificações já enfileiradas ou vindouras. *UpdatingPolicies* é o estado responsável pela atualização das políticas. As políticas tratadas no estado *UpdatingPolicies* devem ser atualizadas nas PIBs. SettingIB é o estado que realiza esta atualização. O estado de distribuição de políticas é o *Dispatching*É nesse estado que o PDP envia ao PEP os OIDs (*Object Identifiers*) que contêm informações das políticas que devem ser aplicadas. ReadingDevice é o estado em que o PDP acessa as MIBs (*Management Information Bases*)dos dispositivos gerenciados pelos PEPs.

As notificações do PMT ao PDP contêm os identificadores das políticas que foram adicionadas, removidas ou modificadas pelo administrador. Em caso de adição ou modificação, é preciso que sejam feitas consultas ao repositório para a obtenção dos novos valores. Após obtidas as políticas, estas são traduzidas para o formato de PIBs e armazenadas pelo agente manipulador de PIBs.

Para manipulação das PIBs, segundo [Verma 2000], é recomendado um agente que utilize o protocolo SNMP. Porém, buscando uma forma mais simples, rápida, com baixo consumo de memória e que melhor se adaptasse à arquitetura, a manipulação das PIBs do LARCES_PBM é feita por um agente desenvolvido, chamado de LarcesPIBST (*LARCES Policy Information Base Storage Tree*). A estrutura do LarcesPIBST é baseada em árvore e possui apenas os comandos *GET* e *SET*. Testes de desempenho temporal e espacial demonstraram as vantagens da utilização LarcesPIBST em relação a um agente SNMP ou um banco de dados. Os resultados destes testes fogem ao escopo desse trabalho, mas podem ser encontrados em [Aquino].

A validação dinâmica é realizada no momento de distribuição da política. Ao distribuir políticas ao PEP, é necessário verificar se as condições atuais do ambiente permitem que estas sejam aplicadas. Somente após esse processo pode-se considerar que a política estará apta a ser aplicada no sistema.

Para distribuição de políticas aos PEPs, o método utilizado foi o de provisionamento, ou seja, o PDP envia ou remove as políticas a serem aplicadas. Tais eventos podem ocorrer na iniciação do PEP ou caso uma nova política entre ou saia de seu período de validade.

Por ser descrita no PMT, a atualização de topologia é algo trivial para equipamentos cabeados. Contudo, para dispositivos wireless, tal atualização é impraticável. Para solucionar esse problema, o PDP é encarregado da descoberta desses dispositivos wireless. A descoberta é feita acessando as MIBs dos Aps (*Access Points*) presentes na rede e descobrindo quantos e quais equipamentos wireless estão associados a cada AP.

3.4. Policy Enforcement Point (PEP)

Tendo em vista as dificuldades encontradas em redes sem fio WLAN, como estudo de caso, o LARCES desenvolveu um PEP voltado a esse tipo de rede, específico para APs do modelo *Cisco Aironet 1100*.

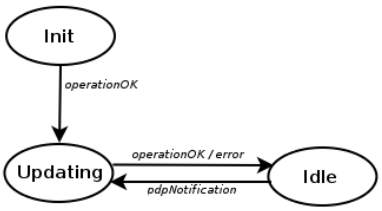

Figura 6. Diagrama de estados do PEP

O PEP possui três estados (Figura 6). *Init*. é o estado onde são feitas as configurações iniciais, obtendo os parâmetros necessários de arquivos XML. Ao final da configuração, é enviada uma mensagem ao PDP, informando que o PEP está ativo.*Updating*é o estado em que o PEP aplica as políticas aos dispositivos. Também é o

estado responsável pela tradução dos OIDs genéricos, recebidos do PDP, para o formato necessário à comunicação com os Aps. O estado *Idle* é onde o PEP espera novas mensagens do PDP. Também é o responsável por receber notificações, verificar o remetente, analisar e tratar o tipo de notificação.

3.5. Comunicação entre os Módulos

Para integração entre os módulos da arquitetura, é evidente a necessidade de comunicação entre eles. Por ser um *framework* genérico, os protocolos de comunicação não são fixos e podem ser alterados facilmente, utilizando arquivos XML.

Procurando uma forma mais simples, veloz, de fácil implementação e que melhor se adequasse às necessidades do LARCES_PBM, foi desenvolvida uma forma de comunicação, chamada LarcesCom (LARCES *Communication*). Esta forma de comunicação utiliza TCP como protocolo de transporte e é baseado no envio de mensagens simples por um módulo (emissor) e o envio de uma mensagem de confirmação de recebimento pelo outro módulo (receptor). O este protocolo de comunicação é apresentado mais detalhadamente em [Celestino Jr]. Esta é a forma de comunicação utilizada nas comunicações entre PMT e PDP e entre PDP e PEP.

As comunicações com o PR são realizada utilizando o protocolo LDAP. PMT e PDP fazem armazenamentos e buscas no servidor de diretório utilizando esse protocolo.

A comunicação entre os PEP e os APs é feita com o protocolo HTTP, devido à facilidade e à simplicidade de utilização deste protocolo nesse tipo de dispositivo. Assim, os OIDs que são enviados do PDP ao PEP precisam ser traduzidos para URLs. A configuração é feita utilizando comandos *GET* ou *POST*, dependendo da URL.

Para a comunicação entre o PDP e os dispositivos subordinados ao PEP, é utilizado o protocolo SNMP. O objetivo dessa comunicação é monitorar o estado da rede. Para isso, é necessária a leitura da MIB dos dispositivos através do comando *GET*.

4. Testes

Para validar a arquitetura foram realizados testes em uma rede sem fio WLAN, que analisaram os comportamentos de diferentes tipos de tráfego com e sem o uso de políticas aplicadas a estes. Os testes consistiram de diversos cenários com objetivos difersos, como, por exemplo, comprovar a aplicação das políticas ou comparar o comportamente de tráfegos com e sem políticas aplicadas. Uma descrição mais detalhada dos testes, incluindo a plataforma de teste, gráficos e resultados mais detalhados, pode ser encontrada em [Celestino Jr].

O resultado dos testes comprovaram que as políticas foram corretamente aplicadas, mostraram que os tráfegos se comportam melhor com aplicação de políticas e que quanto melhor o serviço utilizado, melhor o comportamento do tráfego. Também foi demonstrado que as configurações de políticas são respeitadas tanto quando não há disputa pelo meio sem fio quanto quando existe disputa.

5. Conclusão e Trabalhos Futuros

Nesse artigo foi apresentado e avaliado o *framework* genérico LARCES_PBM, baseado na arquitetura proposta pelo IETF/DMTF, para gerenciamento baseado em políticas de

QoS em redes de comunicação. Este *framework* é aplicável a quaisquer tipos de rede, bastando que seja adaptado a cada tipo.

Tendo em vista as dificuldades encontradas em redes sem fio, como estudo de caso foi desenvolvido um PEP específico para gerenciamento de redes WLAN. A funcionalidade da arquitetura desenvolvida foi demonstrada a partir de testes realizados com objetivo de obter QoS nesse tipo de rede. Os testes comprovaram a aplicação correta de políticas, demonstraram que o comportamento dos tráfegos gerados foi melhor com uso de políticas e que as configurações das políticas são respeitadas também quando ocorre disputa pelo meio de transmissão entre dispositivos *wireless*.

Trabalhos futuros são relacionados à implementação de um mecanismo para detecção dinâmica de conflitos, ao desenvolvimento de PEPs para outros tipos de rede e à realização de testes de desempenho do *framework*.

Referências

Aquino, F., M. L. B. A. e. a. Technical report.

Burnner, M., M. D. B. A. e. R. A. (2005). *Policy Core Extension Lightweight Directory Access Protocol Schema (PCELS)*. RFC 4104.

Celestino, J., M. F. A. L. B. e. A. (2006). Validation de politiques et détection de conflits pour la gestion par politiques de réseaux: Une implémentation customisé. In *GRES*. a publicar.

Celestino Jr, J., L. B. A. T. F. e. a. Technical report.

DMTF (2005). *Common Information Model (CIM) Standards*. http://www.dmtf.org/standards/cim, acessado em 22/12/2005.

Moore, B. (2003). *Policy Core Information Model (PCIM) Extensions*. RFC 3460.

Moore, B., E. E. S. J. (2001). *Policy Core Information Model*. RFC 3060.

OpenLDAP (2002). *Página Oficial do OpenLDAP*. http://www.openldap.org, acessado em 11/4/2006.

Strassner, J., M. B. M. R. e. E. E. (2004). *Policy Core Lightweight Directory Access Protocol (LDAP) Schema*. RFC 3703.

Verma, D. C. (2000). *Policy-Based Networking - Architecture and Algorithms*. New Riders.

Westerinen, A., S. J. S. J. e. a. (2001). *Terminology for Policy-Based Management*. RFC 3198.

Yavatkar, R., P. D. e. G. R. (2000). *A Framework for Policy-based Admission Control*. RFC 2753.