actas da V Conferência da APSI – CAPSI2004, Lisboa, Portugal, 3-5 Novembro de 2004

Utilização de Políticas em Gestão de Redes e Sistemas de Informação

Vitor Roque
Instituto Politécnico da Guarda, ESTG, Guarda – Portugal
email: vitor.roque@ipg.pt

Rui P. Lopes
Instituto Politécnico de Bragança, ESTiG, Bragança – Portugal
email: rlopes@ipb.pt

José Luís Oliveira
Universidade de Aveiro, DET, Aveiro – Portugal
email: jlo@det.ua.pt

Palavras chave: Sistemas de Informação, Gestão de Redes, Gestão de Redes por Políticas, Especificação de Políticas.

Resumo

A gestão das redes tornou-se, nos últimos anos, um tema de máxima importância para as empresas dado que a sua organização, os fluxos de informação e métodos de trabalho, quer interna quer externamente, estão cada vez mais dependente do bom funcionamento de redes de comunicação. Esta dependência faz com que a *disponibilidade* e *desempenho* destas infra-estruturas e serviços sejam actualmente factores determinantes para o seu sucesso.

Tem-se assistido também a um aumento quer a nível de tamanho, quer a nível de complexidade das redes, o que implica o desenvolvimento rápido de mecanismos de configuração normalizados para que a sua gestão seja feita de uma forma eficaz e rápida.

O conceito de gestão por políticas surgiu nos últimos anos como o paradigma "ideal" para tratar este tipo de necessidades.

Tendo em consideração que a maioria dos actuais sistemas de informação tem uma interdependência quase total com a rede de comunicação que lhe dá suporte, é importante que esta mesma rede esteja a funcionar correctamente, isto é exiba os comportamentos adequados, pois uma sua eventual falha pode levar, em casos extremos, à inoperabilidade total ou parcial do próprio sistema de informação.

A Gestão Baseada em Políticas (PBM – *Policy Based Management*) apresenta-se como um paradigma adequado quer para gerir estas novas redes de comunicação quer para garantir segurança e, genericamente, definir as politicas de utilização dos sistemas e infra-estrutura de comunicações de uma organização. Este artigo visa expor esta metodologia, o estado de normas e de desenvolvimentos, e discutir a sua utilização nos

sistemas de informação actuais de forma a garantir uma administração coordenada e consistente.

1. Introdução

A evolução das redes de comunicação veio criar novas oportunidades e novas perspectivas de exploração dos SI (Sistema de Informação). Sendo a informação o principal componente dos sistemas de informação, é necessário que esta esteja disponível em qualquer hora e em qualquer lugar (*any time, any place*). No entanto, esta disponibilidade só é possível se houver uma infraestrutura de comunicação robusta que a suporte.

Se os sistemas de informação são cada vez mais eficientes são-o também cada vez mais complexos. A eficiência e a complexidade reflectem-se também na rede de comunicação, sendo imperioso geri-la de forma eficiente e em tempo útil para garantir a operacionalidade e estabilidade dos sistemas de informação. Pode afirmar-se que um bom desempenho do sistema de informação está relacionado directamente com o bom desempenho da rede de comunicação e vice-versa, isto é, um mau desempenho da rede de comunicação implica obrigatoriamente um mau desempenho do sistema de informação.

Relativamente às redes de comunicação, tem-se verificado nos últimos anos um grande crescimento em diferentes sentidos:

- *Escala* – as redes possuem cada vez mais elementos, cada vez há maior diversidade de elementos e estes requerem cada vez mais recursos dos sistemas que os gerem.
- *Funcionalidade* – os elementos de rede têm cada vez maior capacidade para desempenhar mais funções. Cada vez mais protocolos e níveis de rede são necessários para o desenvolvimento de novos serviços.
- *Intervalo de alteração* – a natureza dos actuais serviços de rede requer intervalos de alteração (actualização, adição, remoção) da configuração da rede mais pequenos que num passado recente. Não é possível actualmente fazer-se a configuração da rede e pensar que a mesma se vai manter por muito tempo. Esta deverá ser alterada de acordo com as necessidades dos seus utilizadores.
- *Complexidade* – devido à crescente complexidade dos equipamentos e respectiva gestão, novas tecnologias e novos serviços de rede, a gestão da rede é cada vez mais complexa.
- *Eficiência/Desempenho* – novas tecnologias aplicadas a novos equipamentos de rede tornam as redes mais eficientes em termos de desempenho e fiabilidade.

Se tivermos em consideração o dinamismo actual das redes de comunicação/sistemas de informação e das empresas necessitarem cada vez mais, de novos e melhores serviços de comunicação, a gestão de redes assume um papel fundamental no sentido de reduzir ao mínimo o tempo que a mesma se encontra inoperacional e consequentemente, de forma total ou parcial, o sistema de informação que sobre ela assenta.

Na Figura 1 pode visualizar-se o impacto no tempo dos factores instalação e administração/gestão de uma rede de comunicações.

A administração de redes deu inicialmente origem a sistemas de gestão proprietários para de seguida se passar a sistemas de gestão com base em normas, portanto abertos, promovidos por diferentes entidades de normalização – ISO (*International Organization for Standardization*), IETF (*The International Organization for Standardization*) e outras. Isto acontece no início da década de 90 e desde então diversas têm sido as propostas neste domínio: SNMP (*Simple Network Management Protocol*) [1], CMIP (*Common Management Information Protocol*) [2], CORBA (*Common Object Request Broker Architecture*) [3], WBEM (*Web-Based Enterprise Management Initiative)* [4], COPS (*Common Open Policy Service*) [5], entre outros.

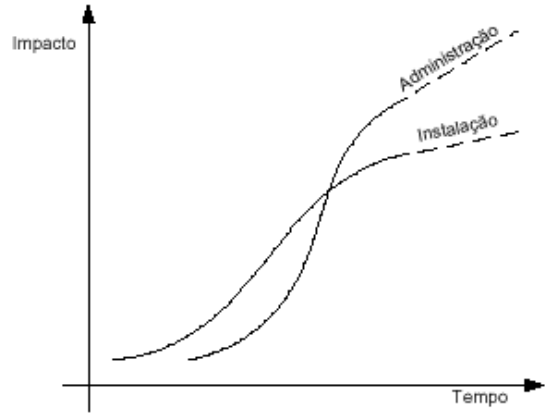

Figura 1 – Impacto relativo Instalação/Administração [6].

Apesar desta diversidade a grande maioria dos sistemas de gestão continua bastante dependente de esforço humano. E duas abordagens têm sido privilegiadas. Uma, muito ligada às operações de monitorização, é efectuada essencialmente por SNMP. Outra, mais ligada a operações de configuração, baseia-se na intervenção directa no equipamento de rede, por CLI (*Command Line Interface*) por exemplo, ou através de interfaces baseadas em tecnologia Web. Este cenário, devido à forte dependência do operador, faz com que seja extremamente sensível a erros e consequentemente poder por em causa o correcto funcionamento da rede. Por outro lado a gestão dos SI tem sido arredada destas estratégias dando origem a diferentes soluções para diferentes operações (rede e sistemas) que, em muitos casos, são realizadas pelas mesmas pessoas.

Tendo em conta este conjunto de requisitos e problemas, urge definir mecanismos de configuração que garantam uma gestão eficiente e homogénea dos diferentes equipamentos que fazem parte da rede de comunicação. Uma possível resposta a este problema é a Gestão Baseada em Políticas *(PBM – Policy-Based Management).*

2. Gestão Baseada em Políticas

Os gestores de redes têm tipicamente de configurar e manipular manualmente os elementos da rede através de um processo que é atrito a erros e consome muito tempo. Esta abordagem, traz também dificuldades ao nível do ajuste dos parâmetros da rede, mesmo se os padrões de utilização da rede forem razoavelmente previsíveis no tempo. Devido a estas complexidades, a configuração dinâmica da rede baseada nos requisitos de utilização pode ser obtida com a ajuda de PBM. A gestão por políticas fornece a capacidade de definir e distribuir políticas para gerir redes heterogéneas. Estas políticas controlam recursos críticos da rede tais como largura de banda, segurança, controlo de acessos, entre outros.

De uma forma simplista, pode dizer-se que os gestores de redes criam políticas para definir como os recursos ou serviços na rede podem ou não ser utilizados. Os sistemas PBM transformam as políticas em instruções de configuração e aplicam essas mesmas instruções de configuração à rede (Figura 2). Desta forma, os sistemas PBM vão permitir que a configuração da rede seja feita de uma forma "automática" com base em regras de alto-nível [7]. Por exemplo, o sistema de gestão deverá ser capaz de, para uma determinada situação, oferecer facilidades para reconfiguração do sistema na sua totalidade, se necessário, sem que o gestor da rede tenha que se preocupar com os detalhes de configuração dos diferentes equipamentos que constituem a rede.

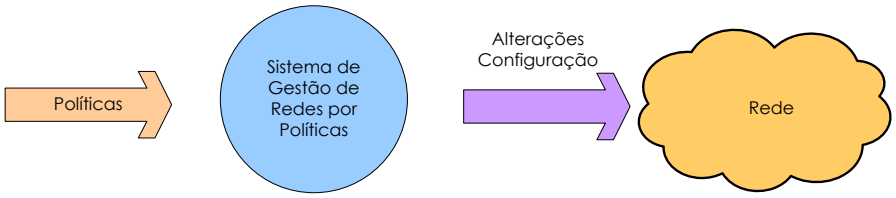

Figura 2 – Funcionamento básico de Sistemas de Gestão por Políticas.

Se se tiver em consideração que o termo "política" pode ser utilizados nas mais diversas áreas de actividade, podemos defini-lo no seu sentido mais abrangente como planos de uma organização para alcançar objectivos e metas. De uma forma geral, as políticas podem ser consideradas como uma ou mais regras que descrevem as acções que devem ocorrer quando se verificam determinadas condições específicas [8]. É também possível que a aplicação de políticas dependa de acontecimentos, sob a forma de eventos. Neste caso, as regras poderão incluir uma parte associada a eventos [9]:

(policyEvent) causes *(policyAction)* if *(policyCondition)*

Assim, as políticas são constituídas por regras que gerem a forma como os recursos podem ser utilizados, ou como as aplicações e utilizadores devem ser tratados. Estas regras especificam um conjunto de condições, que quando se verificam, provocam que sejam executadas acções. As soluções de PBM permitem criar, manter e aplicar estas regras na rede.

Uma analogia possível de comparação entre PBM e a gestão tradicional de redes é a comparação de uma linguagem de alto nível com uma linguagem de baixo nível. Quer na PBM quer numa linguagem de alto nível, o mais importante é o resultado final e não os mecanismos que produzem esse resultado. Nos dispositivos actuais a informação de alto nível é traduzida em instruções de baixo nível para que os dispositivos as consigam interpretar e executar.

Assim, a gestão baseada em políticas apresenta várias vantagens nomeadamente:

- Redução do tempo, custo e problemas associados à configuração/gestão individual de dispositivos, redes, sistemas e serviços. A rede passa a ser gerida de forma centralizada.
- Definição do comportamento da rede como um todo.
- Utilização de linguagem não técnica para a definição das políticas.
- Utiliza a visão de objectivos e metas de negócio para a configuração da rede.

Políticas, Regras, Grupos e Papeis

Como definido anteriormente, política é uma ou mais regras que descrevem as acções a ocorrer quando determinadas condições se verificam. As políticas podem ser simples ou resultarem da composição de duas ou mais regras ou mesmo da composição de várias políticas (política de políticas). As regras são os elementos mais simples (elementos atómicos) que constituem as políticas [8, 10].

Regras simples, são regras que são constituídas por duas expressões lógicas binárias. A primeira define o domínio de aplicabilidade da regra e a segunda o domínio de aceitabilidade da regra.

Regras compostas, são regras resultantes da composição de regras simples ou regras compostas. As operações lógicas podem ser utilizadas na composição de regras nomeadamente as operações conjunção *(and)*, disjunção *(or)* e negação *(not)*. A definição de políticas simples e compostas é idêntica à definição de regras simples e compostas, isto é, uma política composta é o resultado da composição de políticas simples ou compostas.

Grupos de políticas são a agrupamentos de políticas, podendo ter-se "grupos dentro de grupos dentro de grupos". Como exemplo, um grupo de políticas que se aplicam a "Alunos" pode ser constituído por outros grupos "Alunos 1º ano", "Alunos 2º ano", ..., "Alunos 5º ano".

O conceito de papel/role é utilizado para a selecção de políticas. Assim, é atribuído um papel/role a cada recurso e depois utilizado como selector do tipo: o *router* X é do tipo *access router*; aplicar a política Y a todos os *access router*.

Quer em regras compostas, quer em políticas compostas, as regras ou políticas não devem entrar em conflito umas com as outras. Não deve ser possível, por exemplo, ter políticas a autorizar o acesso a um recurso e outra, na mesma política geral, a negar o acesso a esse mesmo recurso.

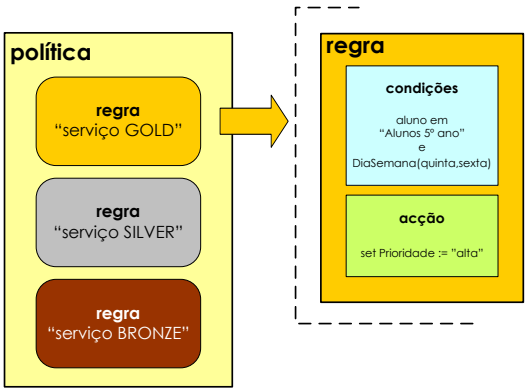

Figura 3 – Exemplo de uma política de QoS.

Tradução das Políticas

As políticas no seu sentido mais abrangente podem ser definidas como planos de uma organização para alcançar objectivos e metas. São portanto definições de alto nível que necessitam ser traduzidas para instruções de baixo nível compreensíveis pelos dispositivos de rede. Este processo de tradução é denominado por *policy continuum* [11], onde os vários níveis de abstracção definem como a política é representada desde

o nível de negócio até ao nível de dispositivo. Na Figura 4 pode ser visualizado o resultado da aplicação ao *policy continuum* das normas definidas no IETF.

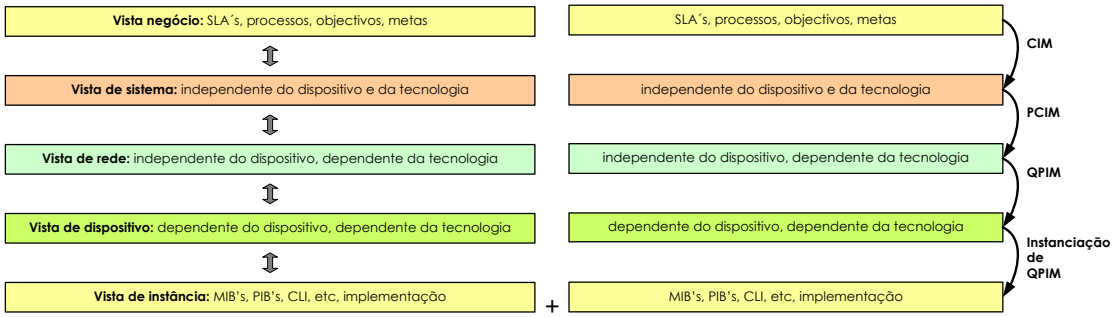

Figura 4 – *Policy Continuum* + Modelos IETF.

Do ponto do utilizador, todo este processo de tradução deverá ser automático permitindo desta forma que a configuração da rede seja feita com base em regras de alto-nível.

Arquitectura dos Sistemas PBM para Redes

O esforço de normalização da gestão por políticas parte principalmente de organizações como o IETF e o DMTF (*Distributed Management Task Force*) tendo resultado propostas como: COPS (*Common Open Policy Service*) [5] e SNMP *for Configuration* [12] no âmbito do IETF, e CIM (*Common Information Model*) [13] e PCIM (*Policy Core Information Model*) [8] dentro do DMTF (*Distributed Management Task Force*) (na realidade, o PCIM é resultado de ambas as organizações).

Estes desenvolvimentos conduziram à definição de uma arquitectura para PBNM (PBM para redes) composta por quatro entidades funcionais (Figura 5): a *Policy Management Tool* ou *Policy Console*, o *Policy Repository*, o *Policy Server* ou *Policy Decision Point (PDP)* e o *Policy Enforcement Point (PEP)*. Este modelo descreve os componentes chave mas não faz qualquer referência a detalhes de implementação como por exemplo distribuição, plataforma ou linguagem. Como consequência, a *Policy Console* é de todos os componentes o menos definido e as suas funcionalidades dependem grandemente das opções assumidas pelos programadores.

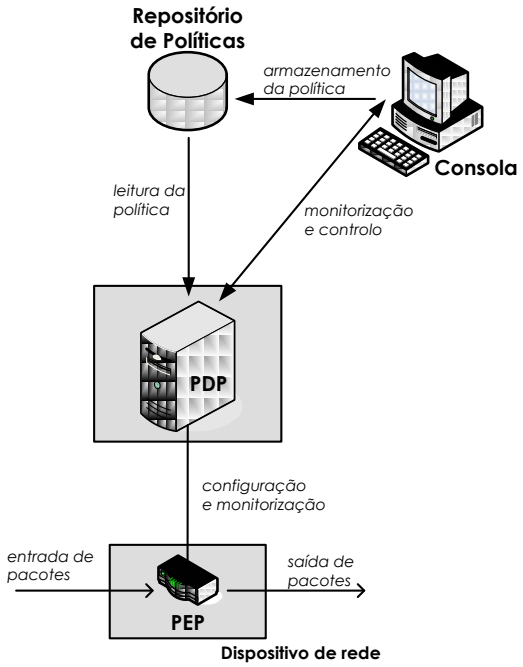

Figura 5 – Arquitectura PBM para Redes.

O PDP é a entidade responsável pela verificação de quando e como as políticas podem ser aplicadas. Valida as decisões com base em medições de tráfego, análise da contabilidade, perfis de utilizadores, detecção de eventos e trata também da determinação e validação de aplicabilidade de regras a nível de recursos específicos e funções de adaptação dos dispositivos. Do outro lado, o PEP é o elemento onde as decisões são aplicadas quando as condições devolvem o valor lógico "verdade". São os responsáveis pela execução das acções podendo realizar operações adicionais como a verificação e a validação de condições. Como exemplos de PEP's temos routers, servidores, sistemas, genericamente qualquer entidade passível de ser gerida. O Repositório de Políticas é o local onde toda a informação relacionada com políticas é guardada. A informação aqui guardada descreve, entre outra informação, utilizadores autorizados, aplicações, computadores e serviços e os seus relacionamentos.

A transferência de informação entre PDPs e PEPs é efectuada por intermédio de um protocolo de políticas. Uma das opções actualmente disponíveis é o COPS [5, 14].

3. Caso Prático: PBM na Gestão de Sistemas

Políticas genéricas

O cenário aqui apresentado como exemplo de aplicação tem por base a ESTiG (Escola Superior de Tecnologia e de Gestão) do IPB (Instituto Politécnico de Bragança). Os recursos actuais em termos de salas de formação incluem 4 salas de 12 PCs cada uma e 1 sala de 45 PCs, para apoio aos diversos planos de estudo (8 Licenciaturas bietápicas), com um total aproximado de 2000 alunos.

Considerando a diversidade de sistemas operativos e de conhecimentos informáticos dos utilizadores foram considerados os seguintes objectivos e que vão de encontro à regra do Conselho Directivo:

- Todo o software, incluindo os SO (Sistema Operativo), deve ser obtido de um servidor de forma a facilitar a instalação e actualização.
- A configuração dos clientes deve ser mínima. Estes devem obter o IP e outros parâmetros de configuração do servidor e esta residir num único ficheiro comum a todos os SO.
- Os utilizadores devem ser identificados por intermédio de um nome e de uma palavra-chave e ter acesso a uma área de trabalho comum a todos os SO.
- Os computadores devem ser limpos e reinicializados no arranque.
- Todos os computadores devem estar protegidos de vírus informáticos.

Estes objectivos contribuem para que todos os PCs estejam em boa condição de funcionamento. Para responder a estes requisitos, o pessoal do CRi decide, de forma técnica, implementar um mecanismo de *remote boot*, o que vem resolver os seguintes problemas:

if [(ficheiro corrompido) or (virus detectado) or (configuração inexistente)] then (restaurar todos os ficheiros)

Além disso, foi também implementado um mecanismo de autenticação centralizado que pretende responder ao requisito de que todos os utilizadores devem ser reconhecidos antes de poderem ter acesso aos recursos:

if (utilizador faz login) then (autenticar utilizador)

Remote Boot

Talvez o maior obstáculo à implementação de um sistema deste tipo seja a diversidade de computadores numa única rede. No caso presente da ESTiG esta situação normalmente não se coloca, uma vez que o concurso de aquisição de material incide sobre uma quantidade suficiente para equipar uma ou mais salas de aula e do qual resulta todas as máquinas serem iguais. O processo de *remote booting* segue três fases:

- Obtenção da configuração do cliente. Nesta fase o cliente estabelece uma ligação com o servidor por intermédio de BOOTP/DHCP (*Bootstrap Protocol /Dynamic Host Configuration Protocol*) de forma a obter a informação necessária para as fases seguintes. A informação contém o endereço IP, máscara de sub-rede, o encaminhador por defeito e o nome do programa de bootstrap.
- Carregamento do programa de bootstrap. Este programa é o núcleo da operação de remote boot. É permanentemente armazenado no servidor e transferido para o cliente por TFTP (*Trivial File Transfer Protocol*). Tem a responsabilidade de preparar o cliente para executar o SO.
- Execução do programa de bootstrap. Este passo leva à definição de partições e formatação do disco, à obtenção e execução do SO.

Estas fases são dirigidas por uma ROM (*Read-Only Memory*) instalada na placa de rede. A ROM interage directamente com a BIOS (*Basic Input/Output System*) e providencia a conectividade IP/UDP (*Internet Protocol/User Datagram Protocol*) necessária para concretizar os diversos passos.

A norma PXE (*Preboot Execution Environment*) para *boot roms* também conhecido por LanDesk Service Agent [15] é a mais utilizada actualmente. Praticamente todas as placas de rede do mercado têm ROMs compatíveis com esta norma.

Para desempenhar funções de *bootstraping*, Rembo é um programa bastante versátil e poderoso (http://www.rembo.com). Ele assume o controlo do arranque do computador praticamente no início do processo ainda antes do sistema operativo. Este facto permite manipular qualquer ficheiro sem restrições de utilização.

Em termos práticos, o DHCP indica à *bootrom* o nome do *bootfilename*. Este usa, posteriormente, o TFTP para carregar o Rembo directamente do servidor.

Quando o Rembo é executado, este procura no servidor um script que será interpretado no cliente. É neste script que se encontram definidas as operações a realizar no cliente e que permitem definir qual a imagem a carregar localmente. O funcionamento do sistema é apresentado passo por passo em [16]. Depois disto o cliente dispõe de sistema operativo pronto a utilizar.

Actualmente esta metodologia suporta a instalação remota de três tipos de sistemas operativos: Linux, Windows 98 e Windows NT. A infra-estrutura de rede é baseada em Fast Ethernet.

Autenticação

O processo de autenticação assenta num servidor de directoria com base no LDAP (*Lightweight Directory Access Protocol*). Este armazena os atributos correspondentes a todos os utilizadores, incluindo o nome, passwords, endereço de correio electrónico, etc.

O servidor de LDAP, instalado com base em OpenLDAP (http://www.openldap.org), responde a pedidos de um servidor SAMBA (http://www.samba.org) quando o utilizador recorre a uma estação de trabalho Windows. Se a estação de trabalho for Linux, o servidor de LDAP comunica directamente com os módulos PAM (*Pluggable Authentication Modules*) correspondentes (http://www.kernel.org/pub/linux/libs/pam/).

Esta abordagem permite que os utilizador tenham o mesmo *username* e *password* independentemente do SO e da estação de trabalho que ocupem.

4. Conclusões

A gestão por políticas é uma metodologia em que a informação de configuração é especificada segundo regras e objectivos que depois de distribuídos pelos diferentes elementos de rede irão assegurar um comportamento consistente da rede de comunicação e dos sistemas de informação.

Esta forma de gerir a rede traz várias vantagens que indirectamente vão condicionar o desempenho do sistema de informação que nela assenta, nomeadamente:

- *Simplificação da gestão de dispositivos, redes e serviços* - possibilidade de rapidamente alterar as características da rede de forma a suprir necessidades imediatas do sistema de informação. Como exemplo, é facilmente alterável o comportamento da rede para que o tráfego de um determinado grupo tenha prioridade sobre o de outros.

- *Redução no esforço de configuração* - permite que com pouco esforço possam ser efectuadas as modificações solicitadas, possibilitando desta forma tornar o sistema de informação mais dinâmico.
- *Definição do comportamento da rede como um todo* - sabe-se à partida qual vai ser o comportamento da rede no final da aplicação da(s) política(s). Se algo correr mal, o sistema PBM faz com que a rede volte ao seu estado anterior. Garante-se desta forma a operacionalidade da rede e consequentemente do sistema de informação, pois mesmo no caso de uma eventual falha, os mecanismos de recuperação disponibilizados pelo sistema PBNM fazem com que a mesma volte ao seu estado de funcionamento anterior, não havendo portanto quebras no seu funcionamento e consequentemente dos serviços de sistema de informação dela dependentes.

5. Referências bibliográficas

1. Case, J., et al., *A Simple Network Management Protocol (SNMP) - RFC 1157*. 1990, The Internet Engineering Task Force (IETF).
2. *Common Management Information Protocol: Specification. Recommendation X.711*. 1997, International Telecommunication Union (ITU-T).
3. *CORBA Specification*. 2004, Object Management Group (OMG).
4. *Web-Based Enterprise Management (WBEM) Initiative*. 2004, Distributed Management Task Force, Inc. (DMTF).
5. Durham, D., et al., *The COPS (Common Open Policy Service) Protocol - RFC2748*. 2000, The Internet Engineering Task Force (IETF).
6. Lopes, R., *Instalação e Administração de uma Rede Local de Comunicação de Dados*, in *Departamento de Electrónica e Telecomunicações*. 1998, Universidade de Aveiro.
7. Sloman, M., *Policy driven management for distributed systems.* Journal of Management Information Systems, 1994. **2**(4): p. 333-360.
8. Moore, B., et al., *Policy Core Information Model Specification v1 - RFC3060*. 2001, The Internet Engineering Task Force (IETF).
9. Naqvi, S., J. Chomicki, and J. Lobo, *Conflict resolution using logic programming.* IEEE Transactions on Knowledge and Data Engineering, 2003. **15**(2).
10. Moore, B., *Policy Core Information Model (PCIM) Extensions - RFC3460*. 2003, The Internet Engineering Task Force (IETF).
11. Strassner, J., *Policy-Based Network Management: Solutions for the Next Generation*. 2003: Morgan Kaufmann.
12. MacFaden, M., et al., *Configuring Networks and Devices With SNMP - RFC3512*. 2003, The Internet Engineering Task Force (IETF).
13. *Common Information Model (CIM) Specification – Version 2.7*. 2003, Distributed Management Task Force, Inc.
14. Chan, K., et al., *COPS Usage for Policy Provisioning (COPS-PR) - RFC3084*. 2001, The Internet Engineering Task Force (IETF).
15. *Preboot Execution Environment (PXE) Specification version 2.1*. 1999, Intel Corp.
16. Stückelberg, M. and D. Clerc, *Linux Remote-Boot mini-HOWTO*. 2000.