CORDENA – UM FRAMEWORK PARA GESTÃO DE REDES BASEADA EM POLÍTICAS

Guilherme Teixeira
guilherme.teixeira@sonaeindustria.com
Dept. de Informática – Escola Engenharia
Universidade do Minho

Paulo Carvalho
pmc@di.uminho.pt
Dept. de Informática – Escola Engenharia
Universidade do Minho

A Gestão de Redes baseada em Políticas (PBNM) tem tido nos últimos anos um novo alento em virtude de tematicamente apresentar um grande potencial de aplicação. No entanto, são ainda poucas as implementações concretas que poêm à prova esta abordagem, tirando dela partido no que o IETF e o DMTF defendem principalmente na abstracção da gestão da complexidade das tecnologias de rede.

O ambiente CORDENA aqui descrito, um framework de Gestão de Redes baseado em Políticas concretiza a abordagem PBNM perseguindo a autosuficiência e a inteligência das redes, usando para isso o modelo provisioning com o qual potencía a autonomia nos nós da rede, de acordo com as políticas definidas.

Preve-se no decurso dos trabalhos dar destaque a algumas questões específicas, nomeadamente, a definição e controlo de SLA/SLS, a tolerância a falhas, a resiliência da rede e a gestão de conflitos na aplicação de políticas, assim como a aplicação da tecnologia a alguns casos reais onde a tecnologia poderá representar benefícios.

I. INTRODUÇÃO

O alargamento das redes, o aumento da sua complexidade, assim como a heterogeneidade dos equipamentos a elas ligados têm dificultado de uma forma geral a sua gestão e monitorização.

Garantir uma determinada qualidade de serviço fim-a-fim, ou disponibilizar de uma forma controlada serviços de valor para suportar processos de negócio críticos, são objectivos complexos a que a área da gestão de redes tem tentado dar resposta mas evidenciando uma clara falta de integração. Geralmente os administradores de rede, vêm-se obrigados a gerir uma amálgama de equipamentos baseados em diferentes tecnologias, obrigando a controlar vários domínios de conhecimento diferentes, em áreas tão separadas como a gestão de um sistema operativo de rede, ou a configuração de um router, frequentemente sem qualquer tipo de integração.

Assim, o interesse em uniformizar a gestão destes recursos, é claramente importante e permite definir a um nível de abstracção superior, as políticas de gestão da rede e as definições concretas dos serviços pretendidos, ocultando o detalhe técnico prescindível.

A Gestão de Redes baseada em Políticas (PBNM) é uma evolução nos princípios de Gestão de Redes ao favorecer a visão global dos sistemas, de modo a controlar eficazmente as infraestruturas de uma forma integrada com todas as políticas guardadas e geridas em entidades centrais.

A definição de políticas na rede a um nível superior de abstracção, além de afastar o detalhe técnico não nuclear, abre simultaneamente a porta a várias vantagens indirectas, nomeadamente aumentos de produtividade, reduções significativas no "time-to-deploy", etc.

Apesar de ainda se encontrar numa fase precoce, esta tecnologia já provou que poderá resolver muitos dos problemas que hoje em dia existem em gestão de redes [4] [6] [11]. No entanto, muito trabalho está ainda em desenvolvimento, nomeadamente na definição de normas e interoperacionalidade entre o que, de facto, é a realidade hoje [6].

É neste cenário que surge o framework CORDENA, tendo como pedras basilares a Gestão da Redes baseada em Políticas e a criação de redes inteligentes autosuficientes com capacidade para se autoconfigurar de acordo com os níveis de serviço definidos e traduzidos em políticas transversais, divulgadas à priori à rede por mecanismos de Policy Provisioning.

Para o seu desenvolvimento foram especificadas juntamente com o framework, uma organização empresarial e uma infraestrutura virtual, à qual este trabalho entende dar algum destaque pelas vantagens que incutiu no trabalho. Estas traduzem-se na facilidade de executar testes e na portabilidade de todo o ambiente, abrindo caminho a uma possível resposta às questões relativas aos métodos de teste e desenvolvimento de políticas.

A implementação em curso inclui as entidades descritas na Tabela 1, implementadas com as tecnologias referidas.

Entidade PBNM	Descrição	Tecnologia empregue
Policy Repository (PR)	Guarda todos os objectos da organização, inclusivamente as políticas.	OpenLDAP
Policy Management Tool (PMT) & *Policy* Console	*Frontend* de interacção com o utilizador.	C, Tcl-Tk, MySQL, IDE
Pol. Decision Point (PDP)	Servidor de políticas. Comunica com os layers inferiores de rede as políticas a aplicar.	C, Intel COPS-PR Sdk
Policy Enforcement Point (PEP)	Onde as políticas são aplicadas e traduzidas para as configurações específicas dos equipamentos. Podem coexistir no próprio equipamento.	Routers Linux c/ kernel 2.4.26 (c/ iproute2) C, Intel COPS-PR Sdk

Tabela 1 – Principais entidades e respectivas tecnologias usadas.

Embora a implementação se devenvolva com o intuito de ser abrangente, para efeitos de definição de âmbito concentrar-se-á na Gestão de Serviços Diferenciados (*DiffServ*). Dentro do âmbito do trabalho, pretende-se ainda destacar e testar algumas questões importantes, nomeadamente a definição de *Service Level Agreements e Service Level Specifications* (SLA e SLS) apoiada por PBNM, a tolerância a falhas, a resiliência da rede e a gestão de conflitos.

A implementação culminará com a integração destas tecnologias num ambiente prático empresarial definido com base numa infraestrutura que pretende ser representativa dos problemas e necessidades verificadas em contexto profissional nas empresas, como a própria implementação tentará exemplificar.

Apenas para simplificar a leitura deste documento, indica-se de seguida um breve resumo da sua organização.

A Secção 2 apresenta noções sobre PBNM, seguida da Secção 3 onde se apresenta o modelo "humanizado" da rede, via *policy provisioning*. A Secção 4 detalha as principais especificações e definições levantadas no desenho do *framework*. Apesar de se tratar de um trabalho em concepção sem resultados finais apurados, a Secção 5 fará um resumo do estado do projecto, das fases já finalizadas e dos proximos passos, seguida finalmente pela Secção 6 onde se levantam desde já algumas perspectivas futuras na aplicação destes desenvolvimentos enumerando alguns exemplos práticos.

II. Gestão de Redes Baseada em Políticas

A. Definições

A Gestão de Redes Baseada em Políticas, é antes de mais, uma mudança na forma como as redes são mantidas hoje em dia. O sistema baseia-se num conjunto de entidades em rede que dinamicamente fazem associações e mapeiam, por exemplo, os utilizadores aos equipamentos e serviços de acordo com as politicas definidas, desviando da visão do administrador da rede o detalhe técnico destes mapeamentos, nomeadamente as configurações subjacentes.

Este modelo não é apenas uma substituição do que já existe, mas uma importante extensão aos métodos de gestão existentes, como veremos ao longo deste trabalho.

O modelo PBNM apresenta algumas vantagens importantes, entre elas destacam-se as seguintes:

a) Permite ao administrador da rede mapear recursos de rede com necessidades de negócio, definindo uma qualidade de serviço garantida para processos críticos de negócio (QoS);
b) simplifica, de uma forma geral, a gestão da rede tornando os operadores mais produtivos ao simplificar a gestão e a configuração dos equipamentos de rede, assim como o desenvolvimento de novos serviços para produção;

c) ao permitir um controlo central relativamente a segurança, prioridades de tráfego, acessos VPN, etc, garante-se que todas estas políticas são aplicadas de uma forma consistente por todo o domínio de gestão, mantendo a rede mais consistente e sob controlo.
d) de uma forma geral, a configuração dos equipamentos de rede, como routers e switches, pode ser automatizada, facultando às organizações uma ferramenta indispensável para aplicar QoS, por exemplo;
e) este modelo prevê ou incorpora a integração de serviços de directório, de onde pode adquirir conhecimento de utilizadores, postos de trabalhos, impressoras, etc.

A automação ao nível do inventário é logo à partida outra vantagem bastante importante, quer para o administrador de rede, quer para o gestor de sistemas de informação.

Com esta integração, a criação de políticas adquire uma nova dimensão, por ser possível a conjugação de variáveis muito importantes em termos de negócio.

Os objectivos são nobres, e evidenciam a importância do esforço de normalização, compatibilização e mapeamento entre toda a gama de serviços de informação e equipamentos existentes no mercado. Esforço esse, neste momento em evolução pela acção das entidades referidas anteriormente, o IETF e o DMTF, juntamente com outras subentidades, empresas, utilizadores, etc.

B. Arquitectura de base

A Figura 1 ilustra os componentes principais que constituem esta arquitectura.

O ponto central de onde são controladas todas as políticas aplicadas no sistema é a *Policy Console*, podendo ser mais do que uma, dependendo da dimensão da rede. A consola é onde o administrador da rede aplica, altera e define todas as políticas, juntamente com a visualização do estado da rede e toda a monitorização possível.

Eventualmente coexistente com a consola, temos o *Policy Management Tool* do qual a consola é o seu *frontend*.

Esta ferramenta pode inclusivé fazer validações em relação às entradas efectuadas pelo administrador e controlar automaticamente a ocorrência de conflitos entre políticas, quando diferentes políticas tentam aplicar diferentes acções aos mesmos objectos, com condições igualmente válidas.

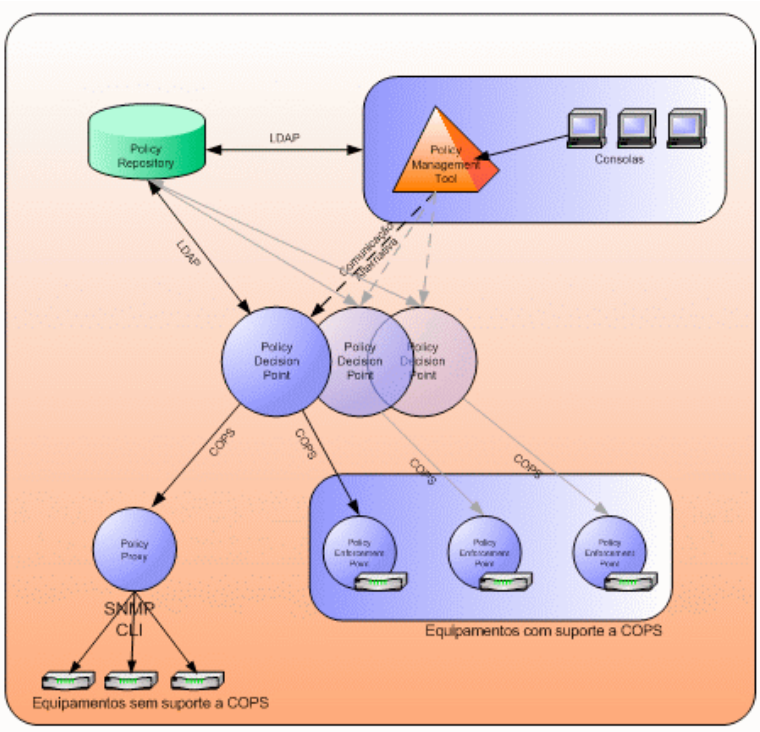

Figura 1 – Arquitectura geral para PBNM.

O *Policy Repository* é onde as políticas são guardadas e de onde são consultadas e actualizadas, juntamente com os restantes objectos da organização ou não, dependendo da implementação. Estes repositórios podem ser baseados em bases de dados relacionais, ou em directórios. Ambas as abordagens têm vantagens e desvantagens, embora o bom desempenho da leitura hierarquizada nos serviços de directório sejam uma das razões porque estes serviços se baseiam tipicamente em directórios.

O *Policy Decision Point* tem como função principal aceder ao repositório de políticas e decidir quais aplicar. O PDP é onde as políticas são convertidas para um nível de abstracção inferior, ainda não com as configurações detalhadas ao nível de um equipamento específico, mas por exemplo mapeando determinadas políticas para o *Policy Information Base* (PIB) respectivo que será posteriormente aplicado nos elementos de rede. Os PDP deverão basear as suas decisões nos pedidos da rede, nas políticas do repositório e na monitorização da rede.[3]

No final da cadeia aparecem os *Policy Enforcement Points*, responsáveis por aplicar as políticas nos equipamentos específicos e garantir que são correctamente e consistentemente aplicadas nos equipamentos terminais de rede.

É provavelmente aqui que reside uma das variáveis mais importantes de toda a arquitectura, pois são os PEP's que deverão integrar os mecanismos de transformação das políticas recebidas em

configurações e alterações de estado das interfaces, dispositivos, etc.

Existem ainda os *Policy Proxies*, cuja função visa integrar na rede equipamentos que não estão preparados para interpretar políticas, ou dito de outra forma não suportam nenhum protocolo de transporte de políticas, como COPS, COPS-PR para *Provisioning*, etc...

Isto é conseguido através do uso de outros protocolos auxiliares de gestão de redes como o SNMP, CLI, etc.

III. Modelo Proposto

Entende-se com o modelo proposto potenciar o cumprimento de dois objectivos primordiais da Gestão de Redes. Assim para uma qualquer estrutura de rede, heterogénea ou não, é de primeira importância a necessidade de:

- disponibilizar os serviços definidos necessários e suficientes às aplicações e utilizadores;
- usar para isso os recursos disponíveis da forma mais eficiente;

Estes dois objectivos são obviamente a base de uma gestão eficiente. Apesar da sua simplicidade, garantem a clarificação das metas que devemos perseguir. Neste sentido, pretende-se antes de mais o contributo da rede ao nível do SLA definido e do seu correspondente SLS, ou ainda de uma forma mais informal, que simplesmente garanta o funcionamento de uma determinada aplicação de negócio de acordo com os requisitos definidos.

Por outro lado, é importante salvaguardar que são mobilizados os recursos da forma mais eficiente possível, rentabilizando o seu uso, e garantindo sempre o nível de serviço pretendido pela entidade cliente.

PBNM serve neste contexto como a base para implementar os dois objectivos mencionados de uma forma inovadora porque permite gerir os recursos sem nunca perder estes objectivos de vista, recorrendo também a todo um leque de políticas, regras e acções as quais terão que estar em primeira mão correctamente definidas de acordo com os objectivos identificados ou acordados.

No entanto, constata-se que existem alguns pontos merecedores de atenção, nomeadamente no que respeita à escalabilidade [15], desempenho e capacidade de resposta a eventos inesperados, entre outros pontos. [12]

Face a estas limitações, o presente trabalho defende um modelo baseado na delegação de funções para os elementos inferiores da arquitectura PBNM, como forma de diminuir o tempo de resposta na aplicação das políticas à rede e de tornar tais componentes chave da arquitectura mais autónomos, retirando daí também uma diminuição de alguns riscos inerentes à diminuição da dependência das comunicações com os PDP's, repositórios LDAP e melhorias na utilização eficiente da rede. [3]

Ao autonomizar mais os PEP's, pretende-se capacitá-los não apenas com acções, mas também com regras, tal como defendido nos trabalhos sobre "*MetaPolicies*" [3], aumentando o espectro de acção destes pontos da rede, e diminuindo em grande medida as necessidades de controlo via PDP das decisões a aplicar. Estas podem ser fruto eventualmente de funções de monitorização existentes nos próprios PEP's.

Os PDP's serão retirados do intercâmbio com os PEP's nos casos em que estes não apresentam valor acrescentado ao processo. Nesta arquitectura, a função dos PDP's fica assim, mais focada nas funções de "*Policy Proxy*", nomeadamente (i) compatibilizando políticas com equipamentos que não apresentam suporte nativo a protocolos de controlo de políticas (e.g. COPS); (ii) na resolução de conflitos aquando da aplicação de políticas divergentes, e finalmente (iii) na função de integração das funções de monitorização e controlo da rede.

Como em qualquer hierarquia funcional, a função de delegação trás consigo a necessidade de reporte periódico. Neste modelo a função de reporte é indexada à periodicidade de controlo operacional nos períodos mínimos definidos no SLA ou SLS, adicionando a essa métrica o tempo de resposta necessário para a correcção de eventuais desvios.

Não deixa de ser interessante neste momento, fazer uma breve comparação com a gestão de equipas no nosso mundo real. Tendo como base os PEP's como membros de uma equipa que executa as tarefas planeadas pelo seu coordenador – o PDP.

Vejamos brevemente onde nos leva tal comparação:

Tal coordenador terá como missão executar com a sua equipa os objectivos que lhe foram propostos (SLA), garantindo sempre que os diversos membros da mesma, executam as tarefas que lhes são atribuídas dentro dos prazos acordados (SLS) e com os recursos que têm disponíveis para o efeito (REDE), alocando a quantidade de recursos necessária e suficiente (QoS). No caso de existir um excesso de recursos, estes poderão sempre ser canalizados para outros serviços que têm de ser da mesma forma garantidos (outras aplicações ou SLA sobre a mesma estrutura), ou então servem simplesmente como alternativa para o caso de indisponibilidade de alguns dos membros principais (Backups, redundância), embora possam ser usados para outros fins durante os períodos em que não são necessários - *over provisioning*.

De seguida, pensando um pouco no processo de distribuição de funções, repare-se no modelo de delegação. Inicialmente, o coordenador atribui determinada acção ao seu colaborador (REQ msg). Tal

acção pressupõe o cumprimento com sucesso do trabalho executado, momento em que o resultado final da acção deve ser reportado ao seu coordenador (REP msg). Por outro lado, objectivos que se estendem no tempo, como por exemplo, a manutenção de um orçamento anual (SLS; *Policy*), implicam mais do que um único reporte no final do período, nomeadamente uma periodicidade mensal para verificar desvios e accionar correcções enquanto é tempo. Por outro lado, um acompanhamento diário neste caso parecerá certamente exagerado, a tal ponto que poderá inclusivamente diminuir a capacidade dos recursos em executar as tarefas que lhe foram confiadas, por diminuir o tempo disponível para a execução das suas funções – *sobrecarga de recursos.*

Por outro lado, a tendência para capacitar cada vez mais os elementos da equipa a agirem autonomamente e de forma correcta, é importante no sentido em que potencia o desempenho do elemento e o seu conhecimento para ultrapassar situações novas e não previstas, quer em capacidade e rapidez de resposta - *resiliência da rede.*

Situando obviamente cada abordagem dentro do seu próprio mundo, não podemos deixar de reparar nas semelhanças e no que pode ser transferido para o modelo PBMN da experiência do quotidiano que vivemos.

Adicionalmente, os elementos da arquitectura descritos na secção anterior, a sua existência puramente material e a sua repetibilidade de conduta, em certa medida potenciam esta abordagem de delegação e autosuficiência, desde que a robustez e fiabilidade das partes constituintes esteja garantida.

Em resumo, pretende-se apenas com esta breve comparação, ilustrar as razões de base do modelo proposto.

O quadro seguinte resume as comparações entre a gestão das equipas e a abordagem em PBNM.

Gestão RH's	**PBNM**
Coordenador	PDP
Objectivo a cumprir	SLA
Colaboradores	PEP's
Recursos	Rede
Gestão de Recursos	QoS, Over*provisioning*
Autonomia	Via *Policy Provisioning* - Decisões tomadas no PEP de acordo com as políticas recebidas.
Relatórios	COPS REP msg
Capacidade de resolução de situações novas	Resiliência
Experiência	Acções via uso de métodos de IA, Data Mining ou consulta de histótico
Tarefas atribuidas	COPS REQ msg
Gestão de Conflitos	Arbitragem no PDP, ou gestão por prioridades
Períodicidade de envio de relatórios	Definido nas tarefas específicas, ou de acordo com o SLS, SLA ou preferências de gestão.

Tabela 2 – Comparação entre a Gestão de RH's e PBNM.

Esta abordagem conjunta define assim uma linha de pensamento do que se entende que deve ser a PBNM, potenciando a delegação para os PEP's das políticas, suas condições, regras e acções, de forma a melhorar a qualidade do serviço prestado pela rede, e optimizando a utilização dos recursos disponíveis.

IV. Desenho e Especificação

Tratando-se de um trabalho em curso, destacamos de seguida as linhas orientadoras mais importantes incluídas nas especificações técnica e funcional do projecto.

A. Organização

A primeira definição importante é sem dúvida a organização empresarial de base que serve de laboratório ao presente desenvolvimento.

De forma a conseguir percorrer os objectivos expostos nas contribuições científicas previstas, entendeu-se que seria imprescindível ter um ambiente de teste completo com as diversas componentes infraestruturais que veremos de seguida, mas também, e principalmente, a existência de uma organização

empresarial fictícia com os seus tradicionais departamententos, localizações, utilizadores, etc, de forma a adequar o *framework* à real envolvente de uma empresa, com as quais se pretende compatibilizar este trabalho.

Assim, sob a actual envolvente é crucial que sejam garantidos os seguintes requisitos de tal organização:

- representar em termos organizacionais o tecido empresarial;
- incluir obrigatoriamente grupos de utilizadores com perfis de acesso diferenciados, nomeadamente grupos departamentais com perfil operacional (logística, produção, etc), e também de administração e controlo;
- ser uma organização descentralizada por várias localizações geograficamente dispersas;
- usar sistemas de informação para gerir os seus negócios, quer os operacionais relaccionados com o seu core business (por exemplo produção), quer também para administração, gestão e controlo financeiro;
- deter sistemas acessíveis via Internet para consulta de informação, acesso a serviços de Internet Banking, e para gerir e aprovisionar stocks junto dos seus fornecedores;
- disponibilizar um ambinte de e-business para gerir a relação comercial com alguns dos seus parceiros, nomeadamente clientes e distribuidores;
- ser uma empresa jovem e dinâmica que aposte nas tecnologias e sistemas de informação como factor de diferenciação para criar vantagens competitivas no mercado em que opera.

São estas as características seleccionadas na definição do perfil da organização de base.

Justamente por se entender que tal definição deve conter um nível de abstracção tal que permita equacionar a aplicação deste modelo a várias topologias de empresas distintas, a definição não contemplou outras dimensões de detalhe, como por exemplo: volume de negócios, capitais próprios, mercados alvo, número concreto de colaboradores, previsões de evolução, tecnologia disponível nos mercados em que opera, know-how interno e nível de serviços contratados, estratégia, etc.

Muitas mais haveria para citar e analisar, no entanto tal matéria ultrapassa o âmbito deste documento, embora em qualquer solução real, sejam variáveis a ter em conta.

B. Laboratório

Uma vez que o objectivo núclear do laboratório de testes é aferir um Sistema de Gestão de Redes baseado em Políticas numa organização, deverá existir uma determinada base técnica que represente as infraestruturas de uma organização com as características enumeradas no ponto anterior.

Assim de acordo com o ponto anterior, salientam-se os seguintes requisitos técnicos:

- deve existir um sistema de directório que guarde de forma unívoca os utilizadores, grupos de utilizadores e se possível restantes recursos tecnológicos de forma a gerir autenticação e acesso nos sistemas de rede e aplicações, sempre de acordo com os respectivos níveis de acesso autorizados;
- deve existir uma qualquer rede de comunicações WAN que ligue as várias delegações;
- cada delegação deve ter uma infraestrutura de rede local responsável por conectar os postos clientes aos sistemas de gestão da empresa;
- devem existir sistemas de informação para todas as áreas da empresa. (produção, logística, financeira, administrativa, etc) usados por todos os colaboradores da empresa, como por exemplo um Enterprise Resource Planning (ERP);
- a empresa necessita de uma ligação estável e fluente à Internet para satisfazer alguns processos de negócio críticos, nomeadamente para acesso a bancos, sistemas de aprovisionamento, etc;
- da mesma forma deve existir uma área reservada e de acesso externo controlado para aceder ao sistema de e-Business da empresa, nomeadamente uma *Desmilitarized Zone* (DMZ);
- a existência dos dois últimos pontos, dita a existência obrigátoria de uma *firewall* para controlar e proteger o acesso à Internet.

Adicionalmente, existem alguns requisitos técnicos relativos à natureza de investigação associada ao trabalho e não pelo perfil da organização em teste.

Esses requisitos são os seguintes:

Uso de soluções Open Source: Por permitir a exploração total das soluções em estudo e de todas as suas componentes, além de conter os custos associados ao desenvolvimento. Além disso tratam-se de sistemas em produção e com fiabilidade e robustez bem confirmada ao longo dos últimos quase 15 anos de existência.

Representatividade da tecnologia real: As soluções encontradas devem reflectir as preocupações reais, os dimensionamentos aproximados e as soluções técnicas mais usadas na realidade.

Portabilidade do ambiente: Um tal sistema de testes, obriga naturalmente a um conjunto de equipamentos de teste razoável, desde equipamentos terminais, routers, switches, servidores, etc. O desafio lançado como requisito técnico não crítico, foi tornar tal ambiente portátil por questões de produtividade e facilidade para a execução de todo o desenvolvimento e testes.

C. Fluxo de Processos e Operações

Uma boa parte da especificação funcional do *framework* está patente nos RFC publicados pelos *Working Groups Policy Framework* (*policy*), e *Resource Allocation Protocol* (rap) do IETF, nomeadamente no modelo de dados [1], na sua implementação em LDAPv3 [2] e as extensões posteriores, assim como pelo conjunto de normas definidas pelo *framework* de *Policy Provisioning* via COPS-PR especificado nos RFC's 2748, 3084, 3159, 3318, 3438, 3317, entre outros.

Para lá das normas definidas, há ainda questões de carácter mais operacional e que fazem parte do conjunto de requisitos e especificações do *framework*.

De forma a materializar as vantagens até agora levantadas por este *framework*, vejamos que operações ou processos devem ser garantidos ou aconselhados. O diagrama da Figura 2 apresenta o fluxo de processos, destacando os processos pelo *tier* em que ocorrem, desde o *frontend*, *layer* de rede (PDP e PEP), e o PMT. O diagrama serve de base para a especificação e definição de todo o ambiente do *framework*, no que respeita às operações a suportar, desde a configuração inicial até à gestão e manutenção quotidiana do ambiente, cujas fases são resumidamente descritas de seguida.

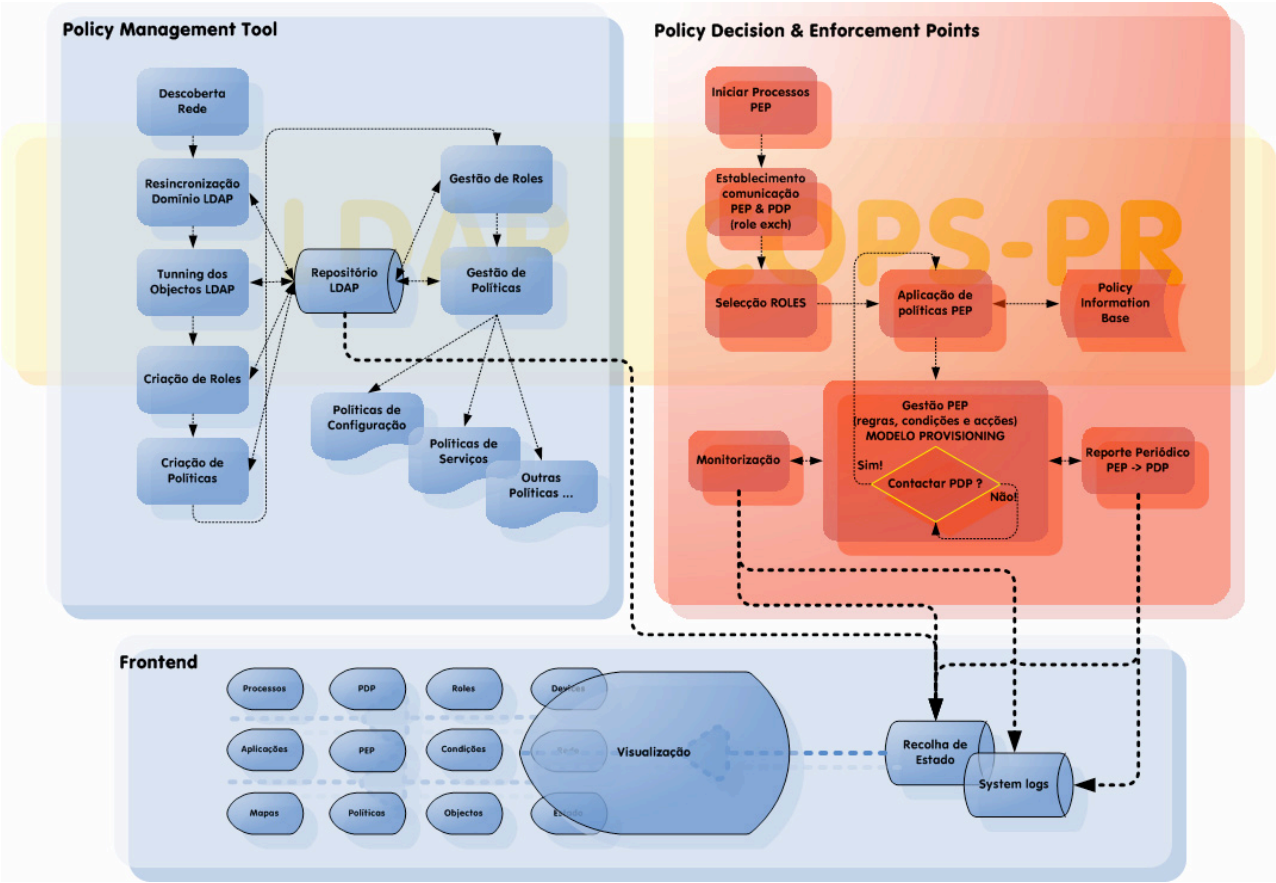

Figura 2 – Diagrama geral do fluxo de operações do framework

C.1 Objectos

Os objectos sobre os quais o *framework* deve permitir a criação e gestão de políticas, são os indicados no RFC 3060 começando pelas dimensões de tempo indicadas de seguida,

- Hora
- Dia da semana
- Dia do mês
- Mês do ano
- Duração

São também necessários objectos para a construção das *policy rules* e *policy conditions*, dos quais se indicam como exemplo os seguintes:

- Equipamentos terminais
- Redes
- Postos de trabalho (por nome)
- Grupos de postos de trabalho
- Servidores
- Aplicações (layer 4 e superiores)

- Grupos de aplicações
- Utilizadores
- Grupos de utilizadores
- Localizações
- Grupo de localizações

Convém salientar que quanto mais extensível for o modelo, maior será a sua aplicabilidade, e assim para este ponto específico, lançemos o atrevido desafio de implementar algo que permita o uso de todos os objectos presentes no directório da empresa. Como sabemos, o directório pode ter mais ou menos objectos e ser mais ou menos extensível de acordo com os *schemas* que implementa e os objectos que guarda, e que amanhã podem naturalmente ser mais do que hoje.

Desta forma estamos a capacitar o *framework* para evoluir na mesma medida que toda a estrutura evolui, o que embora pareça à partida utópico, pode ser possível, obrigando necessariamente a um enquadramento mais abstracto e provavelmente ao ajuste de alguns schemas conforme o caso.

De qualquer forma, como base, o conjunto de objectos indicados é suficiente para testar o modelo. Os atributos de cada um deles são descritos [1], e implementados em [2] e posteriores extensões.

C.2 Configurações iniciais

Por mais automático que seja o ambiente, haverá sempre que proceder à preparação do *framework* e à sua instalação inicial, assim requere-se que esta fase seja o mais transparente possível fazendo um equilíbrio entre a complexidade inevitável, o conhecimento necessário para a execução das tarefas e a simplicidade, tentando sempre manter a operação o mais expedita possível.

C.3 Descoberta da rede

Uma das funcionalidades que esta ferramenta prevê, é a descoberta automática dos nós da rede, e que embora não seja um requisito crucial no âmbito deste trabalho, poderá ser interessante.

Desta forma coleccionar-se-iam todos os objectos da infraestrutura numa primeira fase e posteriormente procedia-se à sua limpeza e ajuste de propriedades, a atribuição de *roles*, etc.

No entanto, dado o carácter limitado da rede de teste, esta função não é essencial.

C.4 Ajuste e verificação dos objectos LDAP

Este ponto refere-se ao possível ajuste de algumas informações dos objectos contidos no repositório LDAP. Esta operação visa limpar o diretório de informação sem qualidade, e acrescentar os atributos necessários, para a correcta administração quer das políticas, quer do próprio repositório. Exemplos disto, podem ser a atribuição das *roles* a todos os objectos.

Funcionalidades como selecção simultânea de vários objectos, e processos automatizados de gestão devem ser usados.

Muitas das melhores funcionalidades de gestão do directório LDAP, encontram-se em *frontend*s próprios para o efeito.

De forma a acelerar o desenvolvimento da aplicação, as partes respeitantes à gestão pura e simples de informação do direcório poderão ser baseadas em aplicações externas já existentes.

C.5 Criação e gestão de roles

A criação de *roles* parte muito da própria visão do administrador de rede. Para evitar ter a sensibilidade como mais uma variável de utilização do ambiente, vão ser criadas algumas *roles* iniciais para garantir o uso de um conjunto inicial de funcionalidades importantes.

O conjunto sugerido será o seguinte:

Roles de Infraestrutura: WAN; LAN; DMZ; Centro de Dados; Gateway Internet; Routers; Servidores; Postos de trabalho.

Roles Organizacionais: Todos os utilizadores; Utilizadores do Dept. Financeiro; Utilizadores do Dept. Produção; Utilizadores do Dept. Logística; Administração.

Roles por Criticidade de Processo de Negócio: Processos críticos; Processos prioritários; Processos normais; Processos de baixa prioridade.

As *roles* por processos de negócio podem ser bastante importantes na definição de acções decorrentes de um Plano de Continuidade de Negócio, ou de Recuperação de Desastre, algo que na maior parte dos casos obriga a uma fastidiosa inventariação e classificação dos processos de negócio e respectivas infraestruturas envolvidas nesses processos de acordo com a criticidade para a empresa.

Posteriormente, as *roles* poderão ser usadas para os mais variados fins, podendo ter aplicação temporária para determinado projecto finito no tempo, bastando para isso fazer as respectivas atribuições de objectos, dispositivos, etc às *roles* pretendidas.

C.6 Criação e gestão de políticas

A criação de Políticas tem subjacente a criação de Regras, Condições e Acções, podendo ser todas elas reutilizáveis ou não. Este trabalho de criação pode ser

gradual começando pelas políticas de configuração, as quais permitirão pôr o ambiente a trabalhar de uma forma normal, em tudo idêntica à anterior.

Posteriormente, avança-se para a criação de políticas mais avançadas e mais complexas, partindo sempre do simples para o complexo, preferencialmente por reutilização de políticas mais abrangentes. Um ponto muito importante e aqui subjacente, diz respeito aos elementos constituintes das condições e acções, pois na sua quase totalidade dependem da fase de ajuste e verificação dos objectos LDAP descrita acima. Quanto mais detalhada e correcta for a caracterização dos objectos do directório, maiores serão obviamente as capacidades do *framework* na gestão da infraestrutura.

A manutenção das políticas deve ser auxiliada pela visualização, e pela verificação do que está ou não aplicado à rede, assim como o efeito real das políticas aplicadas, com a identificação dos possíveis conflitos e resultados alcançados.

C.7 Gestão dos processos de rede

Uma vez tendo todo o *framework* estabelecido, é útil deter alguma forma de controlo sobre os processos de rede que ocorrrem nos PDP's e nos PEP's. Valorizaram-se as seguintes funcionalidades:

Arranque de processos: Tarefas de arranque do *framework* de forma explícita por questões de segurança. A passagem para a Gestão pelas políticas deve ser clara e facilmente constatável.

Sincronização de políticas: Face a uma grande alteração de políticas, ou porventura a uma dúvida generalizada acerca do que está ou não em funcionamento, ou ainda face a algum tipo de incidência no sistema, é importante deter uma forma de sincronização da infraestrutura com as políticas estabelecidas. Dependendo da dimensão da rede, esta actualização pode ser controlada eventualmente pela aplicação parcial e sequencial baseada nas *roles* da infraestrutura definidas. Não deve ter qualquer implicação em termos de *downtime* ou falha de qualquer ordem para os utilizadores finais.

Modos de Espera: Se por qualquer motivo, nomeadamente falha, determinada política apresenta um comportamento *Bizantino*, ou antes, as acções e condições que a constituem provocaram por exemplo implicações graves numa parte substancial da rede, deverá haver possibilidade de regredir ao estado imediatamente anterior, e de colocar as políticas em causa num estado latente de espera, até se apurar a causa do problema.

Monitorização: Os processos de monitorização são essenciais para se verificar se o sistema está em funcionamento pleno, e se não está, apurar onde reside o problema principal. Para isso é necessário monitorizar uma série de itens, processos, dispositivos, equipamentos, etc, assim como que políticas estão a ser aplicadas, se com sucesso ou não, etc.

Relatórios Periódicos: Com uma periodicidade que faça sentido, levando em linha de conta os ciclos de análise dos administradores de rede e essencialmente de acordo com os SLS/SLO ou SLA definidos com os respectivos clientes. Exemplos de relatórios adicionais poderão incluir informações estruturadas ou ad-hoc retiradas do repositório LDAP; Relatórios das Políticas em uso e em que objectos e *roles*; Relatório de Políticas inactivas; Relatórios de Actividade por PDP, PEP; Relatórios de Erros, etc.

Muitas outras funcionalidades poderão fluir do uso do *framework*, no entanto estas são o conjunto inicial definido para permitir a gestão básica do ambiente.

C.8 Visualização

Embora não seja crítico o seu apuro, uma vez que não está no âmbito deste trabalho desenvolver o ambiente de trabalho em profundidade, será dado algum tratamento às questões de *frontend.*

É necessário distinguir que a visualização e percepção dos efeitos da aplicação das políticas poderão ser vistos com outras ferramentas externas de monitorização, pois estas através de SNMP permitem colher uma imagem online do estado da rede, em termos das larguras de banda usadas, estado dos principais serviços e processos, etc.

Assim, haverá ainda que acrescentar técnicas de visualização próprias para Gestão de políticas e verificação de estado no que ao *Framework* de Gestão de Políticas diz respeito.

Vejamos alguns exemplos de ferramentas de visualização que se recomenda que sejam integradas:

- Mapa da rede com indicações visuais da atribuição de políticas.
- Ferramenta de frontend gráfica baseada em janelas, e também em texto.
- Listagem das politicas em cada PEP
- Mapa de apresentação visual e online dos PEP's e dos respetrivos PDP com que interagem.

A Figura 3 apresenta um protótipo gráfico do *frontend* deste ambiente, onde se incluem os requisitos aqui indicados.

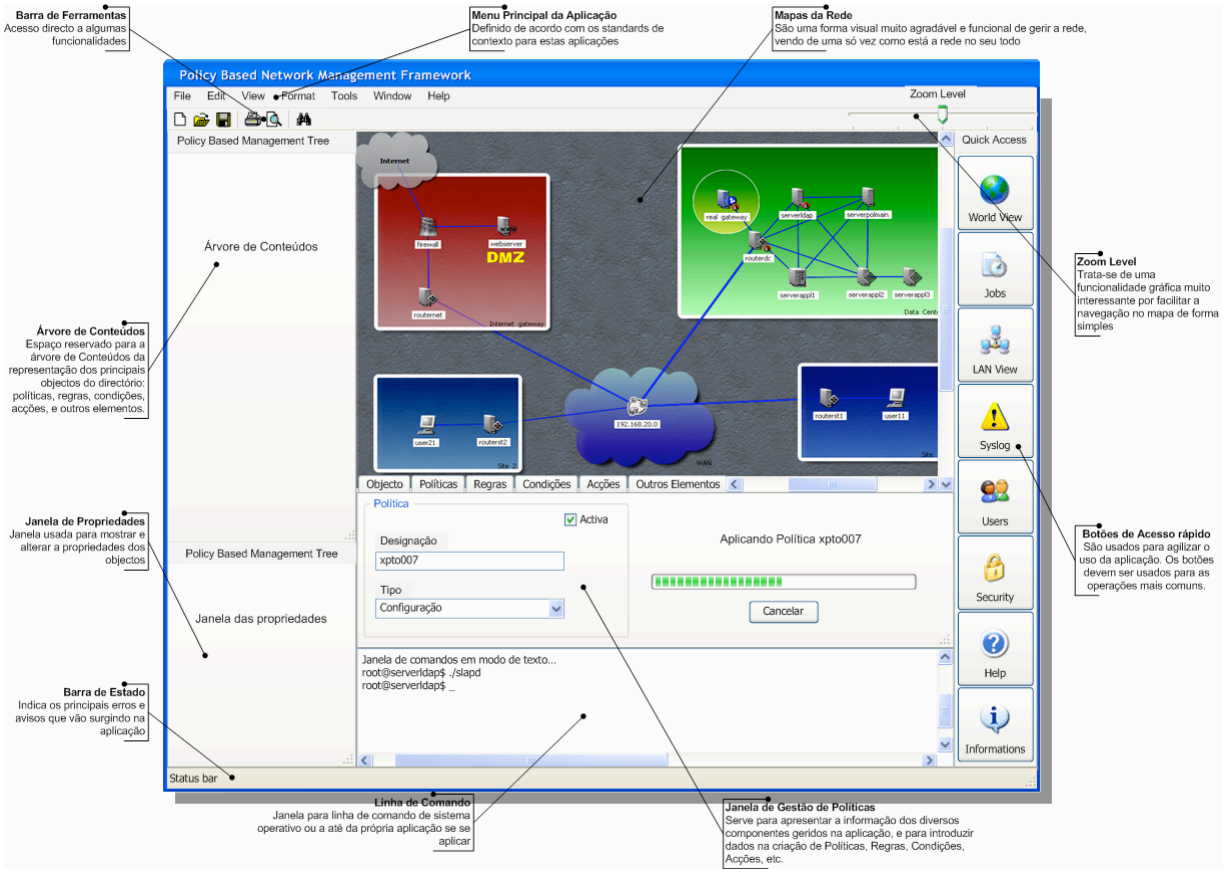

Figura 3 – Protótipo gráfico do frontend

D. Modelos de Informação

O *framework* deve garantir a implementação dos seguintes RFC no que respeita ao modelo de informação usado:

- RFC 3060 - *Policy* Core Information Model
- RFC 3703 - *Policy* Core LDAP Schema
- RFC 3644 - *Policy* Quality of Service (QoS) Information Model

Implicitamente no que se refere ao repositório LDAP, os seguintes RFC's são também validados:

- RFC 2251 - LDAP v3
- RFC 2252 - LDAP v3 - Attibute Syntax Definitions
- RFC 2377 - Naming Plan for Internet Directory-Enabled Applications (***)
- RFC 2798 - Definition of the inetOrgPerson LDAP Object Class
- RFC 2829 - Authentication Methods for LDAP
- RFC 2849 - The LDAP Data Interchange Fornat (LDIF) - Technical Speficication.
- RFC 3045 - Storing Vendor Information in the LDAP root DSE.
- RFC 3112 - LDAP Authentication Password Schema
- RFC 3377 - LDAP v3 Techincal Specification
- RFC 3383 - Internet Assigned Numbers Authority (IANA) Considerations for LDAP.

Ainda relativamente à informação que é passada dos PDP's para os PEP's, esta deverá estar de acordo com os seguintes RFC's:

- RFC 3159 - Structure of *Policy* Provisining Information Base
- RFC 3318 - *Framework Policy* Information Base
- RFC 3317 - Differentiated Services Quality of Service *Policy* Information Base
- RFC 3571 - *Framework Policy* Information Base for Usage Feedback

E. Comunicação PEP-PDP

Ao nível de rede, nomeadamente no que diz respeito à comunicação entre as instâncias PDP e as PEP, devem ser suportados os seguintes RFC's:

- RFC 2748 - The COPS (Common Open *Policy* Service Protocol)
- RFC 3084 - COPS usage for *Policy Provisioning* (COPS-PR)
- RFC 3483 - *Framework* for *Policy* Usage Feedback for COPS- PR

F. Frontend

Muitas das funcionalidades desenvolvidas no âmbito deste *framework* baseiam-se em comandos em texto analisados por *parsers* e executados com o respectivo resultado também em texto. Sejam ao nível do sistema operativo (Linux), sejam das aplicações que correm sobre ele.

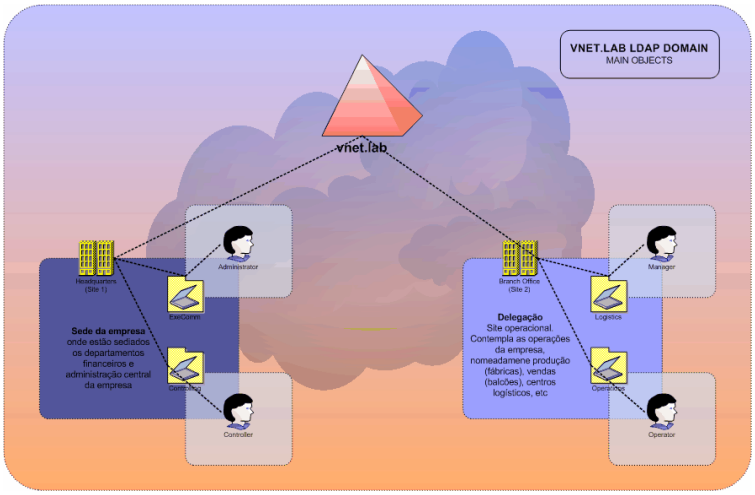

Figura 4 – Organização de base

De qualquer forma, entende-se crucial a integração visual de todas as componentes em especificação sob um ambiente integrado de gestão.

O protótipo gráfico apresentado na Figura 3 é apenas uma apresentação esquemática para efeitos de análise gráfica dos vários componentes do *frontend*. A Figura apresenta as notas acerca das principais componentes e a sua utilização em cada secção. Resumem-se nesta imagem os principais requisitos do *frontend* com o utilizador.

Não se especificam cada uma das componentes em detalhe desde o menu, árvore de conteúdos, etc, deixando tais definições ao critério da fase de desenvolvimento da aplicação. O único ponto que se realça é a importância de seguir as regras e definições para o desenvolvimento de interfaces gráficas de acordo com os ambientes gráficos seleccionados em que a aplicação irá correr, nomeadamente, Gnome, KDE, MS Windows, GNUStep, etc...

V. Trabalho em curso

Após o necessário aprofundamento técnico em algumas das tecnologias envolvidas, o trabalho em curso situa-se, à data da redacção deste documento, no início do desenvolvimento aplicacional para os processos de rede, baseado do SDK COPS-PR disponibilizado pela Intel [5]. Entre as fases concluídas, incluem-se as seguintes:

- Desenho e Especificações técnicas e funcionais
- Organização de base
- Infraestruturas virtuais
- Serviços de rede

A. Organização de base

A topologia lógica do ambiente é baseada numa empresa fictícia com uma distribuição de acordo com a organização ilustrada na Figura 4.

A organização definida *(Vnet.Lab)* detem um local como sendo a sua sede onde residem habitualmente utilizadores com perfis administrativos nas diversas áreas funcionais da empresa. Para lá da sede, existem várias localizações distribuídas geograficamente onde são executadas as operações de negócio, logísticas, de vendas e distribuição ou até de produção. Entende-se que de uma forma ou de outra, com as devidas variantes, esta estrutura é representativa de uma grande parte do tecido empresarial.

O organigrama da Figura 5, ilustra a organização de pessoas e departamentos da organização fictícia que será mapeada sob o modelo proposto.

Funcionalmente, poderia ter mais ou menos departamentos, entende-se no entanto que os indicados são os núcleares em qualquer empresa e representam os principais níveis de criticidade e importância no seio das empresas.

A empresa está distribuída entre três localizações, sendo uma a sede, e duas delegações operacionais. Poderá facilmente ter mais de duas delegações, sendo as restantes instâncias do modelo actual.

Caso a empresa cresca com mais delegações, as adicionais serão sempre uma "cópia" das existentes no que respeita ao âmbito do presente trabalho.

B. Infraestrutura

A infraestrutura resultante de todas as especificações e requisitos levantados anteriormente é a apresentada na Figura 6.

A ilustração é uma cópia do ecrã de uma ferramenta de monitorização via SNMP do laboratorio virtual acessível através do router referenciado no diagrama como "real gateway", o qual é a interface de rede real sob a qual existe uma bridge virtual de acesso ao data center virtual.

Por motivos de direitos de autor, e da impossibilidade de desenvolver implementações sob sistemas proprietários, o que seria representativo de uma fatia dominante de mercado, são usadas componentes Open Source para as implementações dos routers.

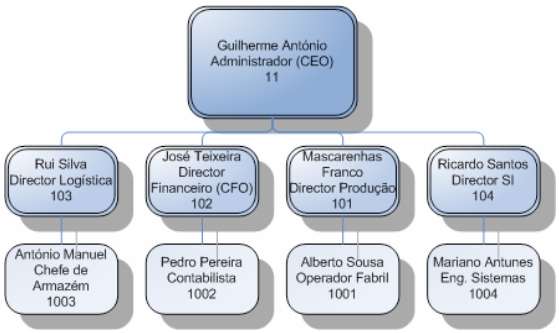

Figura 5 – Organigrama da empresa

No entanto, apesar dessas limitações que poderão ser minorizadas pelo uso de equipamentos que

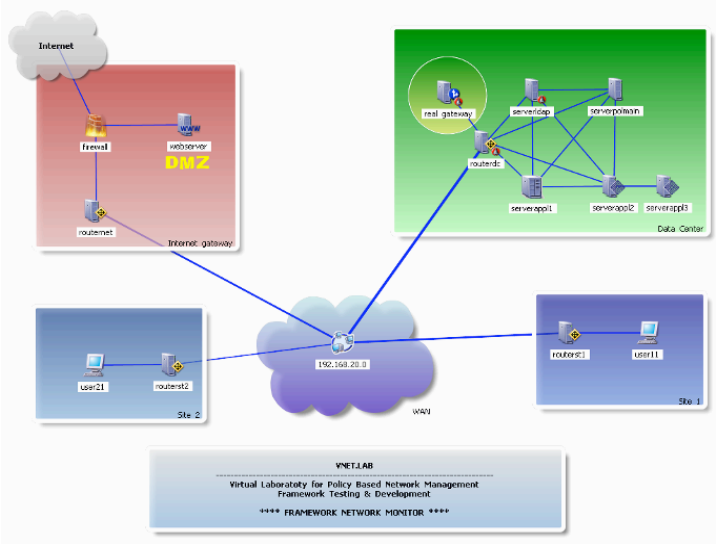

Figura 6 – Laboratório Virtual

implementem COPS-PR e implementem os processos necessários para traduzir políticas DiffServ nos mecanismos próprios do equipamento terminal (PEP), esta implementação pode facilmente ser extendida pela integração de vários directórios proprietários, desde que implementem a norma LDAP, como sejam por exemplo a Active Directory da Microsoft ou o NDirectory da Novell.

A Tabela 3 detalha as características de cada máquina virtual dentro do laboratório. O ambiente descrito encontra-se implementado sob *VMware GSX Server 3.2* numa estação de trabalho Intel Pentium Mobile 1.6Mhz com 1Gb RAM e 80Gb de disco rígido sob *Windows XP Professional*.

Sobre esta infraestrutura foram configurados os serviços normais de uma infraestrutura técnica, nomeadamente o serviço de directório OpenLDAP, DNS, serviços de routing via iproute2 já incluido no kernel 2.4.26 e serviços de autenticação via LDAP.

VI. Perspectivas de Aplicação

Se a abordagem PBNM permite gerir de uma forma integrada redes de comunicações pelo "click de um botão", certamente que sem grande margem de dúvida serão os fornecedores de serviços de comunicações os grandes beneficiados pela tecnologia, pela simples razão de que esse é seu negócio central.

No entanto, contrapondo esta perspectiva um tanto redutora da aplicabilidade da Gestão baseada em Políticas, o horizonte de aplicação desta tecnologia pode ser vertiginosamente alargado se for explorada a forma como é aplicada, levando em consideração questões como:

- transparência da instalação e exploração do middleware necessário;
- total integração com as tecnologias existentes;
- ambiciosas funcionalidades aplicacionais e de *frontend*, com mecanismos amigáveis capazes por exemplo de automatizar e distribuir políticas via "macros" para necessidades e problemas habituais.

Estes três pontos destacam a necessidade de explorar as vantagens da tecnologia mais do que para o óbvio negócio de telecomunicações, onde a tecnologia se justifica por si só.

No entanto para que efectivamente haja um contágio generalizado de Gestão baseada em Políticas, tem que ser acelerado o processo de adopção pelo mercado e pelos principais fabricantes de soluções, principalmente no que respeita à integração do transporte e tradução de políticas para os equipamentos activos de rede, e da integração nos vários serviços comerciais de directório.

Vejamos a título de ilustração alguns exemplos de aplicação de PBNM.

- gestão de acessos à Internet durante horas de expediente;
- gestão dinâmica de prioridades no tráfego aplicacional em função do dia do mês, para salvaguardar situações típicas de fechos de período;
- gestão de largura de banda "a pedido" para fazer videoconferência multiponto ou *webcasting* sob linhas de comunicação tipicamente alocadas apenas a dados;

Código	Nome	Função	Sistema Oper.	Aplicações	Kernel	Interface Primário (LAN)	Vmnet	RAM	Disco	CPU
R1	routerdc	Router de acesso ao data center	Linux Slack. 10.1	iproute2	2.4.26	LAN 10.10.1.1	3	16 Mb	128 Mb	Intel Pentium Mobile 1,6Mhz i686
R2	routerst1	Router de acesso ao site 1	Linux Slack. 10.1	iproute2	2.4.26	LAN 10.10.2.1	6	16 Mb	128 Mb	Intel Pentium Mobile 1,6Mhz i686
R3	routerst2	Router de acesso ao site 2	Linux Slack. 10.1	iproute2	2.4.26	LAN 10.10.3.1	7	16 Mb	128 Mb	Intel Pentium Mobile 1,6Mhz i686
R4	routernet	Router de acesso ao gateway internet	Linux Slack. 10.1	iproute2	2.4.26	LAN 10.10.4.1	8	16 Mb	128 Mb	Intel Pentium Mobile 1,6Mhz i686
Sdev1	serverdev	Servidor de desenvolvimento	Linux Slack. 10.1	--	2.4.26	LAN 10.10.1.49	3	16 Mb	128 Mb	Intel Pentium Mobile 1,6Mhz i686
S1	serverldap	Servidor de Directório e DNS Primário	Linux Slack. 10.1	OpenLDAP, Bind 9	2.4.26	LAN 10.10.1.50	3	128 Mb	1024 Mb	Intel Pentium Mobile 1,6Mhz i686
S2	serverpmt	Gestor do Framework CORDENA	Linux Slack. 10.1	MySQL + openLDAP	2.4.26	LAN 10.10.1.51	3	128 Mb	1024 Mb	Intel Pentium Mobile 1,6Mhz i686
S3	serverapp1	Servidor aplicacional simples	Linux Slack. 10.1	Geração tráfego simul	2.4.26	LAN 10.10.1.52	3	128 Mb	1024 Mb	Intel Pentium Mobile 1,6Mhz i686
S4	serverapp21	Servidor aplicacional em cluster - 1º nó	Solaris 10 Zone 1	Geração tráfego simul	5.1	LAN 10.10.1.53	3	256 Mb	6144 Mb	Intel Pentium Mobile 1,6Mhz i686
S5	serverapp22	Servidor aplicacional em cluster - 2º nó	Solaris 10 Zone 2	Geração tráfego simul	5.1	LAN 10.10.1.54	3			Intel Pentium Mobile 1,6Mhz i686
S6	serverweb	Servidor web	Linux Slack. 10.1	Apache Web Server	2.4.26	LAN 10.10.5.50	1	64 Mb	256 Mb	Intel Pentium Mobile 1,6Mhz i686
S7	serverfrw	Firewall + proxy corporativa	Linux Slack. 10.1	iptables	2.4.26	LAN 10.10.4.50	8	64 Mb	256 Mb	Intel Pentium Mobile 1,6Mhz i686
W1	wsuser11	estação de trabalho	Linux Slack. 10.1		2.4.26	LAN 10.10.2.x (via DHCP)	6	8 Mb	128 Mb	Intel Pentium Mobile 1,6Mhz i686
W2	wsuser21	estação de trabalho	Linux Slack. 10.1		2.4.26	LAN 10.10.3.x (via DHCP)	7	8 Mb	128 Mb	Intel Pentium Mobile 1,6Mhz i686
TOTAIS								864 Mb	10624 Mb	

Tabela 3 – Especificações técnicas do ambiente virtual de testes

- alocação de recursos para alterações esperadas na rede, nomeadamente fluxos de dados em "avalanche";
- usar aplicações secundárias até ao limite sob o qual as aplicações críticas de negócio não são afectadas, nomeadamente *downloads*, transferências via FTP ou instalação de software a pedido;
- atribuir limites de largura de banda, ou *plafond* de tráfego diário por utilizador de acordo com as suas funções, para o centro de dados, internet, etc;
- desviar instantaneamente acesso de grandes grupos de utilizadores a diferentes nós de clusters, a diferentes troços de rede, por motivos de manutenções programadas, evitando quebras de serviço de uma forma totalmente transparente;
- gerir o acesso a infraestruturas de teste permitindo sob os mesmos recursos programar acções de formação, em detrimento de acções de desenvolvimento, e vice-versa de acordo com as necessidades, evitanto neste caso a duplicação de investimentos (assumindo os níveis de serviço correspondentes).

VII. Conclusões

Apresentou-se ao longo deste trabalho, o *framework* CORDENA, um ambiente para Gestão de Redes baseada em Políticas, do qual foram destacados os requisitos técnicos e funcionais mais relevantes na sua definição e actual implementação. Salientaram-se as vantagens da criação de políticas a um nível de abstracção superior, gerindo objectos de negócio, e ocultando a complexidade das configurações de rede não nucleares.

O trabalho descreveu também algumas considerações relativas a redes inteligentes e autosuficientes, sobre as quais se enquadra. Relativamente a este ponto, foi apresentada uma descrição do modelo, baseada numa comparação quotidiana com a Gestão de Recursos Humanos.

Relataram-se os trabalhos em curso, com especial relevo para o laboratório de infraestrutura criado para o desenvolvimento do *framework*, baseado inteiramente em tecnologias de virtualização de hardware.

Finalmente, perspectivou-se a aplicabilidade desta tecnologia, exemplificando possíveis aplicações num contexto prático empresarial.

References

[1] IETF *policy* working group, RFC 3060 – *Policy* Core Information Model – Version 1 Specification, Morr et al., February 2001

[2] IETF *policy* working group, RFC 3703 - *Policy* Core Lightweight Directory Access Protocol (LDAP) Schema

[3] Polyrakis, A., Boutaba, R, "The Meta-*Policy* Information Base", IEEE Network, March/April 2002

[4] Kosiur, D. et al., Understanding *Policy*-Based Networking, Wiley

[5] Intel(R) COPS (Common Open Policy Service) Client Software Development Kit, Ver. 3.1, http://www.intel.com

[6] Rocha, F., "PBNM volta a dar cartas", Revista REDES nº 84, pág. 58-61, Abril 2002

[7] Barhamj, P., et al, Xen and the Art of Virtualization, University of Cambridge, ACM SOSP'03

[8] Waldspurger, C., Memory Resource Management in VMware ESX Server, Vmware Inc., Proceedings of the 5th Symposium on Operating Systems Design and Implementation, Boston, USA, Dec 2002

[9] Carvalho, P., Lima, S., Parada, C., Fontes, F., Carapinha, J., Comparação de Plataformas para Suporte de Serviços Diferenciados em Redes IP, Universidade do Minho, Portugal Telecom Inovação

[10] Hubert, Bert, Linux Advanced Routing & Traffic Control How-to (iproute2), Linux Documentation Project, 2002

[11] Sheridan-Smith, N, A Distributed Policy-based Netowrk Management (PBNM) system for Enriched Experience Networks (EENs), Doctoral Assessment, University of Technology, Sydney, Nov 2003

[12] Schonwalder, J. et al, On the future of the Internet Management Technologies, IEEE Communications Magazine, Oct 2003

[13] Flegkas, Paris et al, A Policy-Based Quality of Service Management System for IP Diffserv Networks, IEEE Network, March/April 2002

[14] Tsarouchis, C et al, A Policy-Based Management Architecture for Active and Programmable Networks, IEEE Network, May/June 2003

[15] Eddie Law et al, Scalable Design of a Policy-Base Management System and its Performance, University of Toronto, IEEE Communications Magazine, June 2003

[16] Trimintzios, P. et al, Policy-Based Network Dimensioning for IP Differentiated Services Networks, University of Surrey, University of Thessaloniki, University College London