Universidade Federal de Pernambuco
Centro de Informática
Trabalho de Graduação

PMT - UMA FERRAMENTA PARA EDIÇÃO E MONITORAMENTO DE POLÍTICAS EM REDES DE AMBIENTE USANDO XML

Aluno: Ernani Madureira de Azevêdo
Orientador: Djamel Fawzi Hadj Sadok
Co-orientador: Carlos Alberto Kamienski

Janeiro de 2008

Ernani Madureira de Azevêdo

PMT – UMA FERRAMENTA PARA EDIÇÃO E MONITORAMENTO DE POLÍTICAS EM REDES DE AMBIENTE USANDO XML

Trabalho de Graduação correspondente ao Curso de Ciências da Computação, apresentado ao Centro de Informática da Universidade Federal de Pernambuco, como parte dos requisitos para obtenção do título de Bacharel em Ciências da Computação.

Orientador: Prof. Djamel Fawzi Hadj Sadok, PhD
Co-orientador: Prof. Carlos Alberto Kamienski, PhD

Recife, janeiro de 2008

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA - CIn

PMT – UMA FERRAMENTA PARA EDIÇÃO E MONITORAMENTO DE POLÍTICAS EM REDES DE AMBIENTE USANDO XML

Ernani Madureira de Azevêdo

Trabalho de Graduação referente ao Curso de Ciências da Computação, apresentado para avaliação ao Centro de Informática da UFPE:

Orientador: _____
Djamel Fawzi Hadj Sadok

Aluno: _____
Ernani Madureira de Azevêdo

Dedicatória

Dedico a meus pais e a todos os que me apoiaram, compreenderam e ajudaram a completar esta etapa importante da minha vida.

Agradecimentos

Agradeço primeiramente aos meus pais. Meu pai é um exemplo de inteligência que eu procuro seguir. Sempre me mostrou que com paciência e dedicação tudo pode ser conseguido. Minha mãe é uma mulher maravilhosa que, incrivelmente, sempre está certa. Agradeço a eles por tudo que eu sou.

Obrigado a meus tios, tias, primos, primas, avós, avô e irmão - pessoas que compreendiam minhas ausências e sempre torceram pelo meu sucesso e comemoram minhas conquistas como se fossem deles mesmos.

Agradeço a minha namorada Lívia pelo apoio e incentivo constantes, sem falar na força dada para alcançar mais um objetivo.

Aos professores Djamel Sadok e Judith Kelner, por proporcionar a oportunidade de trabalhar com pesquisa e desenvolvimento numa área tão instigante, bem como por fazer parte do Grupo de Pesquisa em Redes e Telecomunicações.

Aos amigos e colegas da turma – a união e amizade ao longo da graduação foram cruciais para que eu atingisse minhas metas sem esquecer dos valores básicos.

A Érico Guedes, Leonardo Arcanjo, Jennifer Lima, Fabrício Cabral, Joseane Fidalgo e Ramide Dantas - equipe que me ajudou a entender do projeto *Ambient Networks* tudo o que eu precisava para desenvolver a ferramenta aqui tratada, bem como sugeriram e criticaram, me direcionando para uma solução cada vez melhor.

A Carlos Kamienski por acompanhar este trabalho e ter ajudado sempre que necessário. Mostrou-me como trabalhar para que tudo saia de maneira perfeita e dentro dos prazos.

Agradeço a Ericsson pelo financiamento deste Trabalho de Graduação dentro do projeto *Ambient Networks*.

Por fim, agradeço a Deus por colocar todas essas pessoas na minha vida.

Resumo

Dado o crescimento na escala dos sistemas em rede e a amplitude ganha pela disseminação da internet, conceitos-chave de Redes de Computadores, Web e o ambiente de Tecnologia da Informação em geral tiveram que ser revistos, uma vez que surgiu a necessidade de prover serviços de TI que satisfaçam a demanda do novo contexto da informação, de compartilhamento de recursos, disponibilidade de serviços e cooperação entre redes – ações realizadas através de contratos. Os acordos realizados atualmente exigem quase sempre configuração manual, o que é pouco proveitoso e pouco performático, uma vez que a heterogeneidade dos dispositivos e a diversidade dos serviços disponíveis, dentre outros fatores, inviabilizam tais operações.

Com as redes de ambiente não é diferente. O gerenciamento destas é extremamente importante para seu correto funcionamento. Sem uma infra-estrutura de gerenciamento adequada fica impossível dar suporte a tudo o que as Redes de Ambiente exigem. O controle das redes de ambiente através de políticas se mostrou ser o mais aplicável ao escopo e às idéias do projeto. Entretanto, o uso do padrão escolhido gera problemas no sentido de ser pouco usável para o padrão humano. Uma ferramenta para criação e gerenciamento de redes de ambiente controladas por políticas foi necessária para dar um bom andamento ao projeto em termos de viabilidade cronológica e técnica.

O objetivo deste trabalho é apresentar conceitos sobre redes de ambiente e gerenciamento das mesmas, baseados em políticas. Tais conceitos serão úteis para o entendimento do uso da ferramenta de edição e monitoramento de Redes de Ambiente Gerenciadas por Políticas. Um objetivo secundário do documento é relatar estudos sobre conceitos utilizados para tornar a ferramenta genérica para qualquer aplicação baseada em políticas e demonstrar a facilidade adquirida com recursos da ferramenta que facilitam o desenvolvimento e evitam falhas.

Sumário

Lista de Ilustrações

1. Introdução

1.1 Contexto

Com a evolução da Internet e o crescimento na escala dos sistemas, Redes de Computadores, Web e o ambiente de Tecnologia da Informação em geral, evidenciou-se a necessidade de prover serviços de TI que satisfaçam a necessidade de compartilhamento de recursos, disponibilização de serviços e cooperação entre redes – o que pode ser realizado através de contratos. Os acordos realizados atualmente exigem extensiva configuração manual, bem como um conhecimento prévio do comportamento das redes em que vão atuar [2]. Entretanto, a heterogeneidade dos dispositivos, a diversidade dos serviços disponíveis, a dinamicidade, a mobilidade e a natureza assíncrona dos dispositivos e serviços torna inviável a complexa tarefa de gerenciamento centralizado e a predição de seu estado ou contexto de operação de momento a momento [2].

Visando facilitar o envolvimento de recursos e serviços descritos no contexto acima, foi proposta a criação das Redes de Ambiente [6]. Estas representam uma nova visão na área de redes, com o objetivo de habilitar a criação de uma série de soluções para redes móveis e sem fio que permitam o provimento de serviços de comunicação de boa qualidade, escaláveis, e ao alcance de todos. O projeto Redes de Ambiente (*Ambient Networks – AN*) é parte integrante do *World Wireless Initiative* (WWI) [3], uma iniciativa mantida pelo programa europeu IST *(Information Society Technologies*) [1].

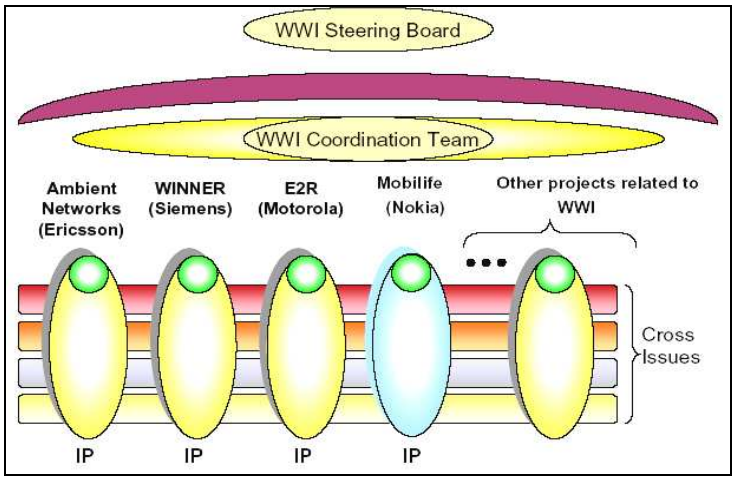

Ilustração 1: Estrutura da WWI [11]

Como se pode observar na ilustração acima, a WWI é composta por diversos projetos que são auto-contidos em cada área de pesquisa proposta, porém são complementares entre si, ou seja, os resultados encontrados em cada projeto se unem para formar um solução mais completa [9].

O gerenciamento das Redes de Ambiente é extremamente importante para o funcionamento das mesmas. Sem uma infra-estrutura de gerenciamento adequada, todos os conceitos vislumbrados para Redes de Ambiente se tornam meros exercícios de futurologia [7]. Sistemas auto-gerenciáveis escaláveis e eficientes irão permitir a implantação de Redes de Ambiente. Tendo esse problema como foco será proposta a utilização de novas tecnologias de gerenciamento tais como P2P e controle baseado em políticas [7], [8], [10].

Uma proposta para o controle de acesso a serviços e recursos é o uso de políticas. Uma alternativa encontrada foi o gerenciamento de Redes de Ambiente baseado em políticas, fundado sobre uma infra-estrutura Peer-to-Peer e com o objetivo de prover características de escalabilidade e auto-contimento [8]. Para tal, foi escolhida uma linguagem sobre a qual o PBMAN (*Policy-Based Management of Ambient Networks* – tópico 3.3) [9] iria funcionar, e a linguagem selecionada foi um padrão definido pelo Comitê Técnico da Oasis, o *eXtensible Access-Control Markup Language* (XACML) [5]. O controle de acesso baseado em políticas escritas em XML apresenta ser uma solução prática e viável, uma vez que o XML está inserido em muitos contextos da Web e facilita a compreensão humana [4].

Contudo, por ter sido definida numa instituição ligada a padrões Web, o XACML apresenta bastante dificuldade para a definição de políticas. Apesar de herdar a simplicidade da semântica do XML, a sintaxe padronizada é uma barreira que vai de encontro à produtividade no desenvolvimento de políticas de controle de acesso e, consequentemente, um percalço no avanço das pesquisas em redes de ambiente.

1.2 Objetivos

Este trabalho de graduação tem como objetivo apresentar conceitos sobre redes de ambiente e gerenciamento de redes de ambiente baseados em políticas que serão úteis para o entendimento do uso da ferramenta de edição e monitoramento de Redes de Ambiente Gerenciadas por Políticas. O objetivo do trabalho também é relatar estudos sobre conceitos utilizados para tornar a ferramenta genérica para qualquer aplicação baseada em políticas, demonstrar a facilidade adquirida com recursos da ferramenta que facilitam o desenvolvimento e evitam falhas e discorrer sobre utilidades práticas do monitoramento de redes de ambiente através do PMT.

Os objetivos específicos são os seguintes:

- Estudo geral e direcionado sobre Redes de Ambiente, focando no projeto *Ambient Networks*, e o uso de políticas para gerenciar tais redes.
- Estudo e representação de políticas e entidades de redes de ambiente (usuários, grupos de usuários, serviços, etc) usando XACML/XML
- Descrição dos conceitos de projeto local (armazenamento local) e projeto remoto (P2P) utilizados na ferramenta para armazenamento e recuperação de políticas em Redes de Ambiente.
- Uso da ferramenta para geração de códigos de cenários recorrentes e complexos.
- Relato sobre geração e interpretação genérica de código XACML/XML, com foco na unificação de modelos de representação em árvores de dados.
- Apresentação da Interface Gráfica genérica para sistemas que envolvam redes de ambiente.
- Estudo do ganho de produtividade obtido quando a ferramenta detecta erros e verifica consistência das informações.
- Descrição da utilidade de uma ferramenta de monitoramento.

1.3 Estrutura do Trabalho

Além deste capítulo introdutório sobre contextualização e objetivos, a seção 2 apresenta os conceitos básicos e as características das Redes de Ambiente (dentro do projeto *Ambient Networks*) e na seção 3 iremos mostrar conceitos de gerenciamento por políticas e

ressaltar o caso específico de gerenciamento e controle de redes de ambiente através de políticas, dentro do contexto do projeto PBMAN. Estes conceitos serão úteis para uma melhor compreensão do problema em questão e justificarão o uso da ferramenta. No capítulo 4 apresentaremos uma visão geral o PMT, sua arquitetura, interações com outros componentes, especificações técnicas e possíveis usos. A seção 5 apresenta os principais aspectos envolvidos na escolha do padrão XACML para controle de acesso e a definição da arquitetura criada para geração e interpretação de XML, bem como aborda conceitos utilizados na ferramenta para geração e leitura do XML para todas as entidades de uma rede de ambiente proposta no projeto *Ambient Networks*. A seção 6 apresenta as abordagens de armazenamento de dados utilizados e entendidos pela ferramenta. Na seção 7 serão vistas aplicações e usos práticos da ferramenta – a geração de códigos para cenários complexos e a criação e relacionamento de entidades da rede.A seção 8 descreve um estudo detalhado sobre os aspectos atuais do gerenciamento e monitoramento de redes e a sua adequação ao conceito de Redes de Ambiente, bem como apresenta a abordagem utilizada pela ferramenta. Por fim, na seção 9, alguns comentários e considerações para o desenvolvimento de trabalhos futuros.

2 Redes de Ambiente

O futuro da humanidade está caminhando para se tornar um mundo sem-fio. Será composto por inúmeros dispositivos pessoais e sistemas inteiramente ligados a tecnologias livres de cabos [11]. Redes de acesso fáceis de usar a qualquer hora e qualquer lugar e acessíveis a qualquer um são conceitos vistos necessários na sociedade eletrônica e provavelmente em 2012, o usuário terá a sua disposição um conjunto rico de serviços de comunicação, independentemente da forma de conexão usada. O desenvolvimento de tecnologias para a real integração *plug-and-play*, uso eficiente de todos os investimentos em infra-estrutura e a competição pelo acesso são as carências técnicas que mais desafiam a realização prática desta visão.

2.1 Cenário

Um cenário que pode descrever bem o ganho de poder e autonomia adquiridos com o uso das redes de ambiente será descrito abaixo:

Os jogos Olímpicos vão começar em dois dias e Alice foi contratada para fazer a cobertura do canal de notícias olímpicas de uma conhecida rede de imprensa. Ela voa para Pequim e encontra com sua equipe. Como houve pouco tempo para se preparar Alice permite que sua rede pessoal (*Personal Area Network* – PAN) se conecte às redes pessoais dos seus colegas sem maiores inconvenientes. A equipe agora tem uma pequena rede local móvel através da qual eles podem cooperar entre si.

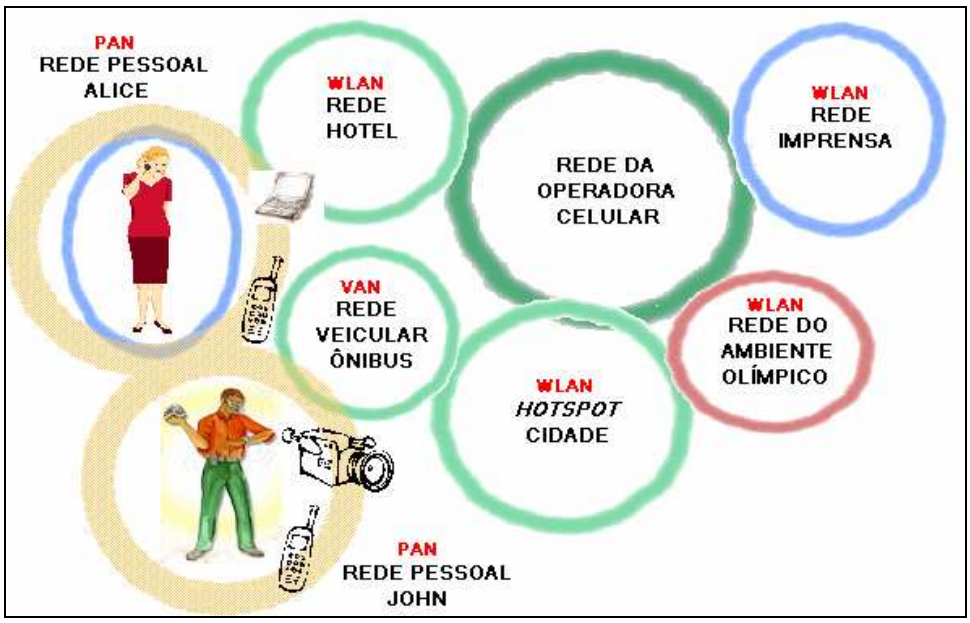

Ilustração 2: Cenário das redes que podem interagir e compartilhar dados

Considerando que existem muitas redes locais e provedores de serviços espalhados por toda a vila olímpica, Alice precisa manter conexões com muitas destas redes, inclusive

quando ela estiver em movimento. Por exemplo, Alice e sua equipe podem se informar a respeito dos acontecimentos da vila olímpica e receber roteiros turísticos da rede veicular do ônibus da vila olímpica, podem acessar seus emails através de uma conexão com o *hot spot* da rede da cidade e podem obter informações sobre as próximas provas a serem disputadas, locais, horário e classificação dos atletas através de uma conexão com a rede da vila olímpica. Sem que Alice perceba, sua Rede de Ambiente negocia participação dentro dessas redes, operadores e provedores de serviços. Quando os serviços fornecidos pelas redes às quais Alice se conectou não forem mais requisitados ou a conexão for perdida, os contratos feitos entre as redes serão desfeitos sem a necessidade da intervenção de Alice.

A equipe então prepara uma entrevista para a televisão. A rede local detecta a necessidade de garantia de qualidade de conexão para a transmissão televisiva e a ajusta. Um canal de contingência é organizado através de outro provedor de serviços (disponibilização de banda) para uma rápida recuperação, no caso do primeiro canal sofrer alguma queda.

2.2 Conceitos

Seguem alguns conceitos indispensáveis para o bom entendimento de redes de ambiente e conseqüente compreensão da abordagem utilizada pelo PMT para gerenciar tais redes.

O principal foco das Redes de Ambiente é permitir a cooperação e comunicação de redes heterogêneas pertencentes a diferentes domínios administrativos ou tecnológicos. Tal comunicação deve acontecer totalmente entre as redes, sem que haja necessidade de configuração prévia ou intervenção de administradores de rede e que aconteça apenas quando requisitada por dispositivos das redes. Para alcançar este objetivo, as Redes de Ambiente serão construídas sobre conectividade e funções de rede abertas, objetivando permitir que qualquer rede que queira se compor possa fazê-lo e removendo assim as restrições de negócios. O auto-gerenciamento e auto-composição, permitirão que a composição de redes de ambiente seja feita da maneira mais transparente aos usuários.

Uma Rede de Ambiente pode ser caracterizada pela publicidade das suas interfaces de controle a outras Redes de Ambiente, plataformas e aplicações, bem como pela sua capacidade de fornecer funções de controle de gerenciamento e da possibilidade de composição dinâmica com outras redes para formar uma nova rede de ambiente.

2.2.1 Propostas básicas

Alguns conceitos-chave das Redes de Ambiente podem ser destacados, como:

1. Suporte a Heterogeneidade: uma vez que as redes de ambiente são baseadas em um conjunto de múltiplas redes com diferentes tecnologias, deverá ser fornecido um mecanismo para comunicação entre elas independente da tecnologia utilizada.
2. Mobilidade Integrada: deve acontecer de maneira efetiva interagindo com as interfaces de controle necessárias ao fornecimento de qualidade de serviço e roteamento, fazendo com que os *hand-offs* de rede sejam imperceptíveis.
3. Composição de Redes: o mecanismo básico de composição das redes de ambiente deve ser dinâmico e instantâneo e será melhor abordado adiante.

2.2.2 Composição

Composição de Redes é um novo conceito introduzido pelas Redes de Ambiente para o compartilhamento de funções de controle e serviços entre redes heterogêneas que pertencem a diferentes domínios administrativos e tecnológicos, como dito anteriormente [11]. A idéia da composição de redes é facilitar o uso da rede por parte de algum usuário e qualquer lugar, como se a rede o estivesse envolvendo (daí surgiu o conceito de redes de "ambiente", uma rede que circunda o usuário). Vistos os conceitos fica clara a intenção do PMT no sentido de visualizar e gerenciar também as redes compostas.

2.2.2.1 Conceitos básicos

Uma composição de Redes resultará em uma nova Rede de Ambiente com um novo identificador, ou em uma extensão de uma Rede de Ambiente já existente com o identificador desta rede. O ponto crucial das composições reside no fato de que os ACSs (*Ambient Control Spaces*), ou planos de controle das redes, interagem entre si, fazendo com que as Redes de Ambiente compostas aparentem ser uma rede a parte para o mundo exterior. São os ACSs os responsáveis por decidir quais serviços ou dispositivos serão compartilhados entre os elementos da rede.

Existem duas interfaces externas que provêem acesso ao ACS: ASI (*Ambient Service Interface*) e a ANI (*Ambient Network Interface*). A ASI é utilizada pelos usuários para acessar os serviços e a ANI é uma interface utilizada pelos ACSs para a troca de informações de gerenciamento e para a tomada de decisões relacionadas a composição.

Para que aconteça uma composição é preciso que todas as entidades envolvidas em algum tipo de negociação possuam um identificador que será utilizado para acessar esta entidade e este identificador deve poder ser traduzido em um endereço de um ponto final de comunicação, quando necessário. Para que se estabeleça o acordo de composição as ANIs devem permitir a comunicação entre ACSs de redes diferentes e entre ACSs de redes compostas.

O Acordo de Composição é um contrato estabelecido entre as Redes de Ambiente envolvidas na composição. Ele é criado e negociado pelas áreas funcionais do ACS, e pode ser modificado sempre que todos os membros da composição concordem em modificá-lo. A composição se resumirá, portanto, na concordância do acordo e na sua realização.

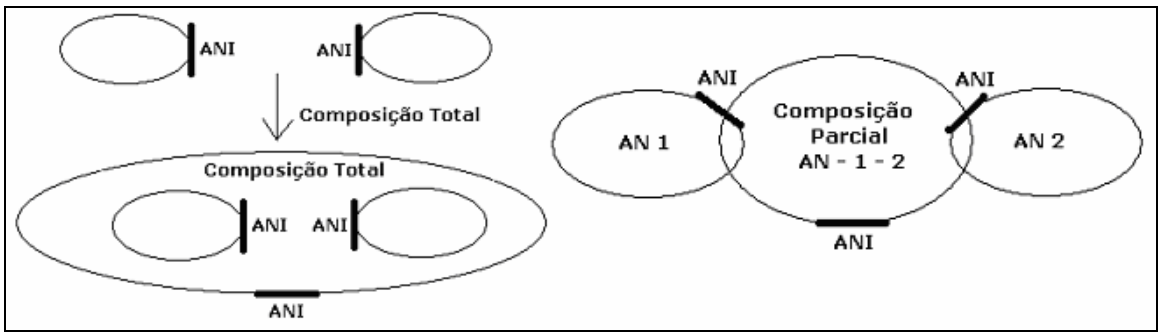

Ilustração 3: Exemplos de composição total e parcial. Observe que na composição parcial a rede composta recebe uma identificação que poderá ser usada por sua ACS para novas composições.

2.2.2.2 Características

A composição consiste em uma operação realizada entre Redes de Ambiente e possui aspectos como generalidade, onde o processo de composição é independente da presença de uma funcionalidade de controle em particular e não é específico a nenhum tipo de rede, conseqüentemente, serve muito bem a ambientes heterogêneos onde existem tipos diferentes de rede; escalabilidade, segundo a qual a composição fornece compatibilidade tanto para pequenos dispositivos quanto para grandes redes; extensibilidade, dado que a composição pode ser facilmente estendida para incorporar novos tipos de funções de controle; automaticidade, uma vez que a composição é uma operação que funciona com o mínimo ou nenhuma interação humana.

A realização da composição também deve ser ajustável, para que seu comportamento possa ser configurado baseado em preferências do usuário, e controlável, consioderando-se que a operação pode ser limitada e controlada por políticas que são tidas como um método genérico onde preferências são utilizadas como parâmetros de controle de operação.

As composições podem pertencer a três tipos de grau:

1. Total, quando os ACSs de todos os membros das Redes de Ambiente precisam concordar em participar da composição. Estas ANs se fundem totalmente e a rede composta consiste de todos os recursos lógicos e físicos dos seus membros. O ACS da rede composta possui controle total desses recursos, desde que as ANs constituintes abram mão deste controle. Outras redes não podem identificar as Redes de Ambiente que constituem a AN composta diretamente, pois o ACS comum é o único que pode ser visto pelas outras redes.

2. Parcial, quando as redes envolvidas fazem um acordo de composição e contribuem para a composição com um subconjunto dos seus recursos lógicos e físicos. O ACS da rede composta não é único e é responsável apenas pelos recursos compartilhados. As redes participantes da composição mantêm seus próprios identificadores e podem participar de outras composições em paralelo, ao contrário do que acontece na composição total.

3. Não ocorre composição, onde há uma mínima cooperação (por isso é considerado um grau de composição), baseada na troca de pacotes de dados, para permitir que as redes vizinhas a AN se comuniquem. Este tipo de composição é muito usado na telefonia móvel e objetiva apenas oferecer conectividade.

2.3 Projeto Ambient Networks

Visualizando estes conceitos foi criado o projeto Redes de Ambiente, que é um projeto integrado cujo objetivo é criar soluções para sistemas móveis sem fio além da 3ª geração. O projeto faz parte da WWI, a Iniciativa para um Mundo Sem Fios, que é composta por várias empresas do ramo, cada um com seu projeto específico, conforme pode ser observado na Ilustração 1 acima. Os objetivos específicos da WWI são fornecer sistemas de comunicação de alta performance que permitam acesso ubíquo a uma variedade de novos serviços e fornecer sistemas sem fio confiáveis. Numa primeira estimativa, previu-se a possibilidade de quatro milhões de pessoas e quarenta milhões de dispositivos possam se conectar uns aos outros em meados de 2020.

A preocupação da WWI não se resume apenas a garantir a definição de soluções completas para Redes de Ambiente baseadas em uma grande variedade de cenários, mas também em assegurar que as soluções propostas estabeleçam novos padrões e protocolos, bem como assegurar a viabilidade comercial da proposta.

O projeto Redes de Ambiente está reconhecendo estes desafios através do desenvolvimento de soluções de redes móveis inovadoras para aumentar a competição e cooperação em um ambiente com múltiplas tecnologias de acesso, operadores de rede e modelos de negócios [11]. O projeto oferece uma solução completa e coerente para redes sem fio baseada na composição dinâmica de redes que provêem acesso para qualquer rede através do estabelecimento imediato de acordos entre redes. Este conceito oferece funções de controle comuns a uma ampla gama de aplicações e tecnologias de acesso, o que habilita o controle integrado, escalável e transparente das capacidades da rede.

O projeto reúne um conglomerado de fortes empresas do ramo de redes, líderes de mercado, fabricantes de dispositivos sem fio, sociedades de engenharia e organizações de pesquisa e desenvolvimento com determinação, qualidade e capacidade para criar consensos multi-industriais para sistemas móveis e sem fio para tecnologias além da 3G. Os resultados vão facilitar o crescimento do mercado e a introdução de novos serviços, bem como vai estimular o crescimento sustentável no setor de comunicação móvel.

Mais informações sobre o projeto *Ambient Networks* podem ser encontradas em [1].

3 Gerenciamento e Uso de Políticas

Gerenciamento Através de Políticas objetiva simplificar a administração de uma infra-estrutura complexa de rede estabelecendo políticas para tratar de situações prováveis de ocorrer em larga escala [12]. Uma das principais características de Redes de Ambiente é a capacidade de mudar dinamicamente a sua topologia através de composições e decomposições para suportar diferentes tipos de usuários, incluindo os das redes móveis. Novos conceitos de gerenciamento de redes serão necessários para lidar tanto com os problemas atuais quanto com os novos problemas de gerenciamento trazidos pela introdução deste tipo de rede.

O gerenciamento para essas redes compostas deve ser simples, de baixo custo, escalável e robusto. Para atingir estes objetivos, os componentes de um sistema de gerenciamento de redes devem ser mais dinâmicos, autônomos e devem participar mais ativamente da rede.

Quando duas Redes de Ambiente se compõe, um desafio crucial é transformar o sistema de gerenciamento de ambas as redes em um único sistema de gerenciamento consistente para a rede composta. De maneira similar, quando as redes se decompõem este sistema de gerenciamento único deve ser separado. Uma das propostas é a utilização de *self-management* [11], uma técnica permite a redução do custo de distribuição e operação da rede e aumenta a escalabilidade das Redes de Ambiente.

3.1 Self-Management

Atualmente, se faz necessário que os procedimentos de operação de redes (instalação ou remoção de elementos de rede, reconfiguração) sejam realizados por administradores de rede experientes em lidar com mudanças. Estas operações de gerenciamento e configuração são custosas, suscetíveis a erros e podem resultar em falhas inesperadas. Em particular, redes ativas envolvem rápidas mudanças que não podem depender dos operadores e precisam ser automatizadas [11].

Auto-gerenciamento é considerado a essência da computação autonômica. Fazem parte desta técnica as tecnologias de auto-configuração (*self-configuration*), auto-otimização (*self-optimization*), auto-conserto (*self-healing*) e auto-proteção (*self-protection*). Auto-configuração consiste na capacidade de configurar automaticamente os componentes do sistema e o próprio sistema seguindo políticas de alto nível definidas pelo administrador do sistema. Na auto-otimização os componentes procuram oportunidades para melhorar seu próprio desempenho e eficiência. Auto-conserto consiste em automaticamente detectar, diagnosticar e reparar problemas no sistema. A auto-proteção permite que o sistema se defenda automaticamente contra ataques maliciosos.

As tecnologias de auto-gerenciamento aumentam a autonomia de elementos individuais da rede ou de grupos pequenos, firmemente conectados mudando o papel das entidades controladas de passivo para ativo ou mesmo pró-ativo. Os elementos da rede são responsáveis por uma quantidade significativa de funções de gerência, reduzindo as interações requeridas do gerente, ou seja, o gerente divide as responsabilidades de gerência com os próprios elementos da rede.

3.2 Gerenciamento por Políticas

Gerenciamento por políticas (*Policy-Based Network Management* – PBMN) possui muitos significados dependendo da organização envolvida no conceito. A princípio, o gerenciamento por políticas servia para fornecer às empresas que disseminam informação habilidades de controlar a qualidade de serviço (*Quality of Service* – QoS) experimentada por usuários e aplicações de rede [14]. Na verdade, o conceito ideal de gerenciamento de políticas vai além disso e diz que os executivos deveriam ser capazes de controlar políticas através de interfaces gráficas simples em seus computadores, e por trás das interfaces as instruções seriam traduzidas em ajustes específicos de controle de tráfego, em detrimento das operações tradicionais de controle de tráfego. Foi sobre este princípio que foi cunhada a idéia do PMT.

3.2.1 Políticas

Diversas tentativas para o desenvolvimento de novos métodos de gerenciamento de redes vêm sendo desenvolvidas ao longo dos últimos anos com objetivos como o de simplificar e automatizar o processo de gerenciamento ou suportar dinamicamente a adaptabilidade de comportamento através da mudança de políticas sem recodificar ou parar o sistema. Dessa forma, políticas podem ser vistas como regras que governam as escolhas no comportamento de um sistema, podendo ser derivadas e/ou influenciadas por objetivos e metas de negócios, acordos a nível de serviços ou relacionamentos de confiança [11]. Em Redes de Computadores, estas se referem à habilidade de administrar, gerenciar e controlar acesso aos recursos dos seus elementos para fornecer um conjunto de serviços aos seus clientes, que podem ser vistos como usuários, aplicações e serviços.

O objetivo a atingir com o gerenciamento por políticas é a especificação de um conjunto de regras genéricas que podem ser aplicadas a um ou vários equipamentos de rede. Com as ferramentas apropriadas, estas regras genéricas, ou políticas, podem ser criadas, instaladas, monitoradas, modificadas ou ainda eliminadas dos diversos equipamentos da rede com um pequeno custo operacional independentemente do tipo de equipamento ou fabricante dos equipamentos que constituem a rede.

3.2.1.1 Arquitetura Geral

O *framework* desenvolvido pela *Internet Engineering Task Force* (IETF) é um modelo para gerenciamento de políticas compreendido por Pontos de Decisão de Políticas (*Policy Decision Points* – PDPs), Pontos de Execução de Políticas (*Policy Enforcement Points* – PEPs), um repositório de políticas e uma Ferramenta de Gerenciamento de Políticas (*Policy Management Tool* – PMT) [13].

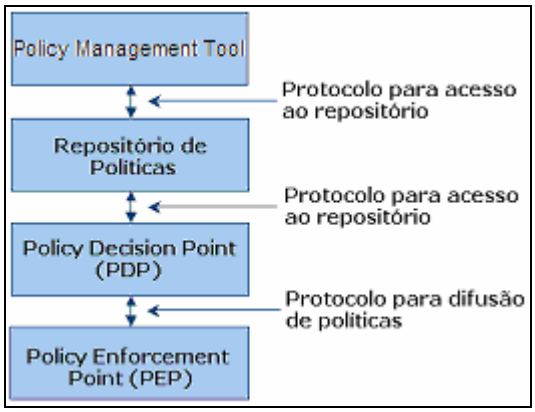

Ilustração 4: Arquitetura geral do *framework* [11]

O nível mais superior da arquitetura permite a edição, tradução e validação das políticas definidas de modo a poderem ser armazenadas no repositório de políticas e posteriormente postas em prática. Este console de políticas poderia ser uma interface gráfica, um *script* ou uma interface de linha de comando. Assim, a tradução consiste no mapeamento de formas abstratas para a sintaxe do modelo de informações do repositório de políticas e a validação consiste na checagem sintática e semântica básicas. O PMT representa esta camada mais alta, e suporta a especificação do modelo de informação da rede, edição e gerenciamento de políticas através de uma interface gráfica amigável ao administrador da rede [13].

O Repositório de Políticas é o local onde as políticas associadas a um determinado domínio estão armazenadas, ou seja, é a base de dados das informações sobre as políticas. Exemplos deste nível são servidores de diretórios e banco de dados.

O Ponto de Decisão de Políticas (*Policy Decision Point* – PDP) é responsável por efetuar o processamento de políticas definidas para a rede, juntamente com outros dados relevantes para a administração da rede. Ele adquire, distribui e opcionalmente traduz regras em mecanismos de políticas do alvo. O PDP toma as decisões posteriormente transformadas em novas configurações para os PEPs consultando o repositório de políticas.

O Ponto de Execução de Políticas (*Policy Enforcement Point* – PEP) funciona normalmente nos equipamentos ativos de uma rede realizando as ações impostas pelas regras de políticas. O PEP é responsável por gerenciar cada equipamento de acordo com as instruções recebidas pelo PDP. Possui também a responsabilidade de traduzir e instalar as políticas nestes equipamentos.

Para a troca de informação ser efetuada com sucesso entre os vários componentes da arquitetura existe a necessidade da utilização de protocolos normalizados. Assim, estes protocolos permitirão a comunicação sem restrições entre produtos de vários fabricantes assegurando assim o caráter geral da solução.

3.2.1.2 Linguagens para especificação de políticas

A especificação de políticas pode ser efetuada através do uso de uma linguagem e um conjunto de acessórios que permitam manipular esta linguagem. A criação de uma interface gráfica permitindo ao administrador uma maior abstração desta linguagem é de grande importância.

Procurar um meio de controlar o acesso à qualidade para alguns serviços foi o que impulsionou o começo do gerenciamento por políticas [14]. A razão do uso de políticas,

obviamente, foi poder configurar qualidade de serviço em redes grandes e heterogêneas e com tantos requisitos diferentes. Desta forma fica claro perceber que PBMN demanda muito tempo, é caro e complexo. As primeiras soluções para PBMN apresentaram algumas características que destacam a dificuldade de implementar uma solução ótima de controle por políticas [14]:

- Maioria das primeiras abordagens para PBMN eram muito ligadas ao contratante, e desta forma podia controlar apenas seus dispositivos. Como resultado, diversas incompatibilidades em soluções de gerenciamento por políticas foram lançadas, o que gerou inúmeros problemas de compatibilidade;
- As soluções eram focadas em poucas funcionalidades de alguns aparelhos de alguns fabricantes que tinham adotado PBMN, e desta forma as mesmas não poderiam controlar problemas que funcionassem sobre outras tecnologias;
- PBMN era focado em um contexto de IP, o que inviabilizaria seu uso por empresas que usassem outras tecnologias;
- Soluções PBMN eram incompreensíveis e brotavam sob demanda, sem necessariamente serem padronizadas.

Foi principalmente por causa do último fator que as soluções PBMN não puderam cumprir seu objetivo em larga escala, como era proposto. Além disso, dois outros problemas impediram a adoção ampla dos modelos: As soluções inicialmente disponíveis não eram muito escaláveis, e consequentemente não poderiam ser facilmente implantadas em qualquer rede existente; e as soluções para monitoramento de redes estavam muito atrasadas em relação ao PBMN, desta forma, ficava difícil descobrir como as políticas estavam funcionando de fato. O monitoramento do funcionamento das políticas também é coberto pela proposta do PMT.

3.3 Projeto PBMAN

Conforme visto na introdução deste documento, vários projetos existem com a finalidade de viabilizar o cenário de mobilidade proposto pela WWI. Uma das abordagens é o projeto *Ambient Networks*, que ao ser adaptado à realidade do PBMN se tornou um novo projeto cujo objetivo é reproduzir o cenário descrito no capítulo 2, usando políticas para prover o controle de recursos: *Policy-Based Management of Ambient Networks* – PBMAN.

O foco do PBMAN é projetar e implementar uma estrutura de gerenciamento para Redes de Ambiente. Um princípio básico do PBMAN é manter a arquitetura genérica e simples, e melhorias irão sendo realizadas com o ganho de experiência através de projeção e implementação do *framework* com novas características e funcionalidades [9].

A arquitetura geral do PBMAN é focada na definição e implementação do espaço de controle de acesso (*Access Control Space* – ACS). Na figura abaixo pode-se claramente diferenciar três tipos de implementação de ACSs, a rede de decisão de políticas (*Policy Decision Network* – PDN), os usuários dos recursos e os PEPs.

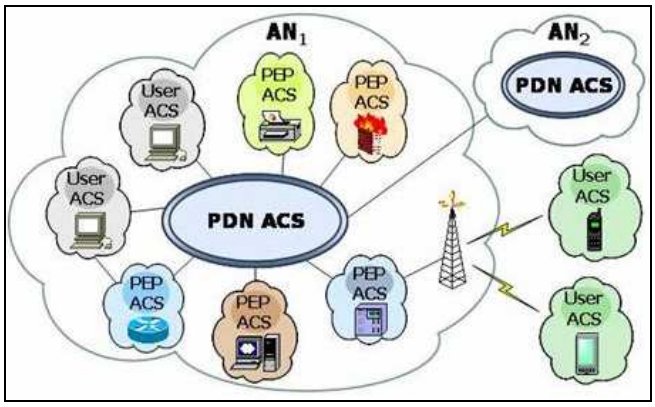

Ilustração 5: Arquitetura geral do PBMAN [9].

3.3.1 Policy Decision Networks

As PDNs são o coração do PBMAN, responsáveis por implementar maioria de suas funcionalidades, grande parte delas relacionadas a PBMN e P2P tais como gravação e recuperação de políticas e tomada de decisões relativas a requisições. As PDNs são compostas de duas entidades principais: os já mencionados PDPs e os repositórios. Uma Ferramenta de Gerenciamento de Políticas imersa no contexto do PBMAN deve funcionar numa camada superior à destas duas entidades, gerando, atualizando e monitorando dados presentes no repositório e interagindo com os PDPs (ou P-Nodes) para tratar informações referentes a políticas, bem como para monitorar o correto funcionamento das PBMNs.

4 Policy Management Tool

A ferramenta de gerenciamento de políticas (*Policy Management Tool* - PMT) foi a solução encontrada dentro do projeto PBMAN para administrar a criação de Redes de Ambiente.

Um ambiente de desenvolvimento que aumente a produtividade dos administradores é um fator a ser considerado para a adoção de sistemas controlados por políticas. Tal ambiente deve prover uma linguagem de políticas de alto nível para especificação de processos de negócio de forma direta e intuitiva. O ato de prover serviços de rede requer configuração de uma grande diversidade de equipamentos, bem como de muitos sistemas operacionais de suporte diferentes (por exemplo sistemas de cobrança e relacionamento com os clientes). A realidade atual define que a configuração (usualmente manual) de sistemas de suporte e redes é trabalhosa e custosa, o que acaba sendo o gargalo que evita um tempo de resposta mais hábil para o mercado. O ponto principal então é como suportar as futuras demandas de serviços de alta distribuição, dinâmicos, móveis e com múltiplos domínios – conforme é esperado que aconteça para Redes de Ambiente – sem ser impedido por este gargalo.

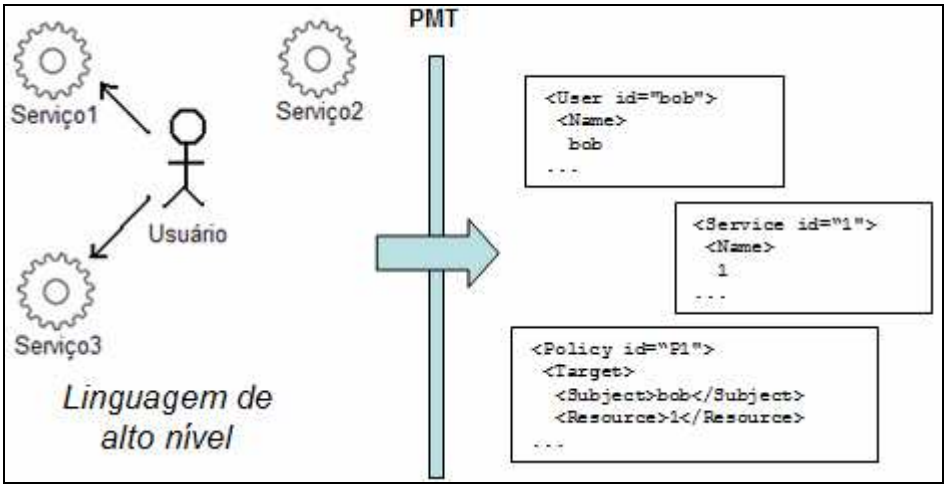

Ilustração 6: Conversão de uma linguagem de alto nível (gráfica) para uma linguagem de configuração de tecnologia.

Apesar de PMTs corresponderem a uma parte muito importante de uma arquitetura baseada em políticas completa, geralmente se dá pouca atenção ao seu projeto e implementação, uma vez que são apenas programas simples que permitem ações básicas de manipulação de políticas [13]. Uma das tarefas mais importantes associadas ao PMT é a habilidade de suportar níveis diferentes de políticas, como políticas de negócio de alto nível ou políticas de baixo nível, ligadas à tecnologia [12]. A maioria das implementações baseadas em políticas suportam políticas a nível de pseudo-código, com controles de fluxo e variáveis, o que não deve ser apropriado para definir processos de negócio. Empresários precisam de uma linguagem (preferencialmente gráfica) através da qual eles possam descrever como os negócios funcionam, que possa prover às empresas a capacidade de ser mais eficiente em desenvolvimento, produção, venda e divulgação de seus produtos. A solução para este problema é implementar um sistema que permita aos gerentes de negócios descreverem seus

processos em um modelo de alto nível que possa ser traduzido para um modelo de nível mais baixo, focado em regras e rotinas ligadas à tecnologia usada. Com todos os recursos envolvidos em seus lugares (PEPs, PDPs, repositórios), esta linguagem deve permitir fácil manipulação e reconfiguração flexível da rede.

Geralmente algumas características associadas ao PMT são: interface gráfica, descoberta de recursos, lógica de transformação de políticas, validação de políticas e análise e resolução de conflitos. A interface gráfica permite ao administrador inserir no sistema políticas de negócio e tecnologia. A descoberta de recursos é o componente que determina a topologia de rede e informações sobre suas entidades. A lógica de transformação de políticas pode ser descrita como um componente muito amplo podendo incluir até outros componentes, como um componente para mapeamento de modelos, um para validação de políticas e outro para resolução de conflitos. Mapeamento de modelos é o componente que traduz políticas escritas de acordo com um modelo de negócio (alto nível) para um nível mais baixo, mais apropriado para configurar redes e serviços de acordo com as regras do negócio. Validação de políticas é um componente que checa se estas são consistentes de acordo com as regras. Análise e resolução de conflitos é o processo de identificar se um grupo de políticas tem regras que vão de encontro a outras e tomar as atitudes necessárias para sanar o problema.

A habilidade de monitorar um sistema gerenciado e reportar os dados obtidos a um administrador é uma característica muito importante presente em uma ferramenta de monitoramento de sistemas baseados em políticas. Entretanto, esta característica por muitas vezes é negligenciada nesses sistemas. Uma ferramenta de gerenciamento de políticas deveria ser capaz de monitorar o processo de decisão de políticas nos PDPs e também o de execução de políticas nos PEPs. A ferramenta para gerenciamento de políticas em redes de ambiente – que ficou simplesmente denominado PMT – é uma ferramenta que contém algumas das características descritas acima e também a capacidade de monitorar as ações e decisões do PDP, bem como os serviços providos pela rede.

Para desenvolver a ferramenta foi usada a linguagem de programação Java, da Sun, que não exige uso de licenças para desenvolvimento e possui características úteis para o projeto como uma biblioteca gráfica expansível de simples uso e com muitas referências na literatura, portabilidade entre sistemas operacionais e fácil integração com outras bibliotecas. Por ser uma linguagem *free*, um grande número de usuários desenvolve e libera suas soluções em Java para a comunidade científica, e este tipo de colaboração também gerou conteúdo de grande utilidade para a implementação bem sucedida da ferramenta.

4.1 Arquitetura do PMT

A arquitetura do software é dividida em três camadas, como ilustrado abaixo. A camada central contém as principais funções do PMT. Seu modelo básico é composto da Visão de Árvore, que contem a representação interna da Rede de Ambiente, e o Mapeamento de Modelos, que funciona como uma camada de abstração para simplificar a modificação dos dados da estrutura de árvore. A camada mais superior é composta dos módulos da interface gráfica. As interfaces desenvolvidas para esta camada visam facilitar a interação do administrador da rede com a árvore – estrutura central das Redes. A camada de armazenamento pode ser dividida em duas partes, uma delas trata do armazenamento local no sistema de arquivos e outra que armazena os dados da Árvore de forma distribuída (ambas as abordagens serão detalhadas no capítulo 6).

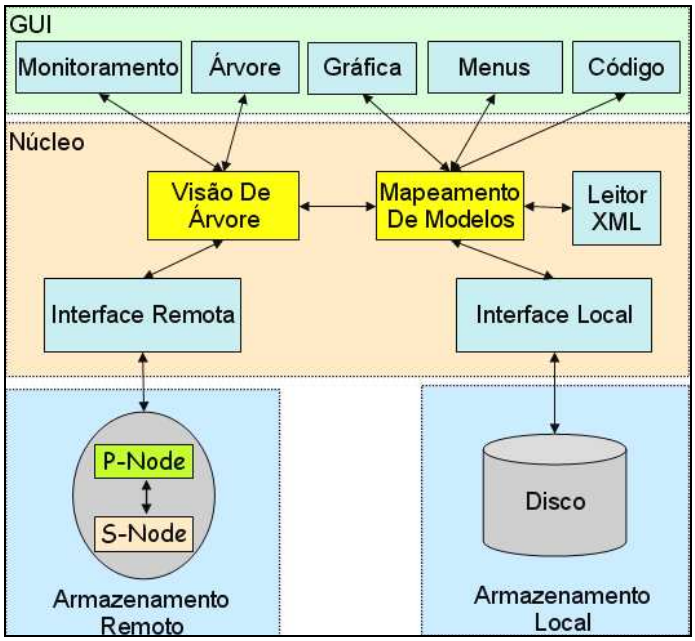

Ilustração 7: Arquitetura do PMT.

Os módulos da camada central do PMT são:

- Visão de Árvore: Contem uma representação baseada em XML de toda a estrutura da Rede, suas entidades, atributos, relacionamentos e políticas, representados em XML (políticas em XACML). A estrutura também provê uma interface de acesso aos dados (*get/set*) para modificação e recuperação dos dados dos ramos e folhas da árvore. Esta estrutura é navegável a partir de uma nomenclatura hierárquica baseada em pontos (por exemplo: raiz.ramo1.ramoFilho.entidade);
- Mapeamento de Modelo: A manipulação da estrutura da Visão de Árvore é trabalhosa e por vezes até perigosa, por comprometer a estrutura básica das Redes de Ambiente. O Mapeamento de Modelo provê uma camada de abstração que torna mais simples e seguro para o PMT manipular as informações da Visão de Árvore, uma vez que os relacionamentos entre entidades ficam consistentes quando estas são modificadas. Este recurso de abstração é usado pelas interfaces gráficas da camada GUI;
- Leitor XML: Este é o módulo responsável por interpretar e validar uma estrutura XML usada para representar uma entidade. Será melhor detalhado no capítulo 5;
- Interfaces Remota e Local: Estes módulos são usados para armazenar e recuperar toda informação contida na Visão de Árvore em um sistema específico de armazenamento, podendo este ser local ou remoto (centralizado ou distribuído). Mais detalhes sobre este módulo encontram-se no capítulo 6.

Os módulos da camada superior (interface gráfica) são a visão de Monitoramento, visão de Árvore, visão de Menus, visão de Edição Gráfica e visão de Código. Os cinco módulos que serão explanados mais adiante provêem as duas principais características do PMT para administradores: edição de políticas (e gerenciamento de informação) e monitoramento em tempo real.

Os módulos da camada inferior, de fato, não fazem parte da arquitetura física do PMT, mas por interagir diretamente com suas funcionalidades, vale a ressalva. Estes módulos são responsáveis pela gravação e recuperação da informação a partir das interfaces de armazenagem de dados para fornecer valores à Visão de Árvore. Uma das formas de armazenar os dados é usar o sistema de arquivos local da estação de trabalho do

administrador, onde o PMT está funcionando, o que pode ser útil para testar o funcionamento da rede num contexto *offline*.

O administrador fica ciente sobre a forma como sua informação foi armazenada remota ou localmente através do uso de projetos diferentes (projeto local ou remoto). Contudo para fazer uso do PMT, o projetista precisa ou criar um projeto, ou abrir um já existente, remoto ou local. Para abrir o projeto remoto é preciso usar a Interface Remota que vai interagir com um P-Node usando os protocolos apropriados, definidos em XACML. Para que isso aconteça, o administrador precisa fornecer informações de acesso aos dados do P-Node: um ou mais endereços de IP, que definem em quais nós da rede os dados podem estar armazenados, uma porta de comunicação, um *login* e uma senha de um usuário com acesso às informações. No caso do projeto local, o caminho até o diretório onde os dados estão armazenados deve ser inserido. Ambos os casos serão vistos graficamente no capítulo 7.

4.2 Interface Gráfica

A camada superior da arquitetura do PMT provê a interface gráfica de usuário (*Graphical User Interface* – GUI) para a interação com a Árvore através de cinco módulos: Menus, Edição Gráfica, visão de Árvore, visão de Código e Monitoramento.

Para o desenvolvimento da interface com o usuário foi utilizada a biblioteca Swing, de Java. A escolha da biblioteca facilitou o desenvolvimento de componentes criados exclusivamente para a ferramenta e mostrou uma boa performance em todos os aspectos.

4.2.1 Menus

O uso de Menus fornece diferentes telas para prover ao projetista a capacidade de adicionar, remover, editar e visualizar todas as entidade e atributos do modelo de informação, tais como usuários, serviços e políticas. Para acessar estas telas o usuário pode abri-las a partir de um menu simples ou através de um menu de contexto, exibido a partir da interface de Árvore.

Um destaque para o módulo dos Menus é o uso de guias (ou *wizards*) para a criação e edição de elementos complexos da rede (políticas e modelos de rede). O ponto forte destas interfaces é criar entidades grandes e que exigem muita informação de forma mais eficiente e rápida, e sem demandar um grande nível de informação do projetista (como conhecimento muito específico da linguagem).

4.2.2 Edição gráfica

O módulo responsável pela edição gráfica corresponde à parte que mais será desenvolvida e pesquisada, uma vez que será o trunfo do PMT se comparado a outros editores de redes. A idéia principal de interação através da *Graphical View* é o uso de ícones e conexões entre estes para gerar políticas de controle de acesso e configuração de recursos.

O passo atual da edição gráfica é um protótipo para teste de interfaces para criação de regras através de ícones, e por este motivo, abrange apenas um cenário simples de edição: criação de políticas de controle de acesso para ambientes locais. Este cenário comporta apenas usuários, grupos de usuários e serviços a serem acessados. Em ambientes mais adiantados será possível controlar o acesso para usuários pertencentes a outras redes, bem como configurar dispositivos de rede e PEPs através de políticas geradas graficamente.

O modelo de edição gráfica foi pensado no sentido de permitir a exibição de muitas entidades sem perda de usabilidade, visualizando um cenário complexo com milhares de unidades presentes numa rede. Foi usado o conceito de agrupamento de entidades ordenadas, comum em grandes cadastros, para que se pudesse representar muitas entidades em uma

interface simples e pouco poluída. O desenho atual das interfaces de edição gráfica é fixo, não é possível redimensionar ou mover os ícones. O modelo primou pela simplicidade e não pela interação, vista como desnecessária para casos simples. As entidades-sujeito das ações (usuários e grupos) ficam localizadas numa metade da janela, enquanto os recursos ficam na outra metade.

À medida que entidades surgem na visão gráfica, o módulo verifica a necessidade de agrupar ou não as mesmas. O usuário poderá navegar por entre as entidades ordenadas lexicograficamente até encontrar o elemento-alvo de sua ação. Para definir uma regra de controle de acesso basta ligar um objeto atingido pela política (sujeito) a um recurso. Este tipo de interação para criação de políticas, com o mínimo de conhecimento do administrador das redes e pouca entrada de dados, é a base ideológica de funcionamento do editor gráfico.

O protótipo atual apenas permite a criação de políticas sobre entidades já existentes. A versão em estudo e desenvolvimento vai possibilitar a criação, remoção e edição de entidades e políticas tanto de controle de acesso quanto de configuração, sempre com foco na simplicidade.

4.2.3 Visão de Árvore e Código

Os módulos de Árvore e Código, apesar de interagirem com entidades diferentes na camada central do PMT, são exibidos juntos na interface gráfica e possuem suas funcionalidades conectadas, por isso é válido listar seu funcionamento num tópico apenas.

Na visão de Árvore e Código, a janela da interface fica dividida de forma que possa fornecer visualização e navegação por toda a estrutura da árvore usada pela rede para manter as informações e ainda permitir a edição direta de código para pequenos ajustes. Na área da esquerda (Visão de Árvore), o usuário tem acesso rápido a qualquer elemento da Rede de Ambiente, representado por uma estrutura de árvore de dados no PBMAN. O mesmo também acontece para uma rede composta, mesmo quando esta é acessada através de um P-Node diferente, ou outra tecnologia de armazenamento (este comportamento será ilustrado mais adiante).

Uma decisão de projeto importante foi tomada para que o PMT se tornasse um cliente da camada de políticas do PBMAN, isto é, que ele pudesse ver a árvore que armazena os dados da Rede de Ambiente acessando diretamente os P-Nodes através de um protocolo específico. Também com o objetivo de melhorar a navegabilidade pelas Redes de Ambiente, o PMT permite que o usuário navegue por qualquer Rede composta à Rede que está sendo trabalhada de forma análoga a um projeto criado. Através do editor é possível mudar o contexto da árvore de uma rede simples para sua composição com outra rede. Isso significa que a “raiz” da visão de Árvore será mudada para um novo ponto dentro desta Árvore.

Através da árvore na esquerda, o usuário pode ver o código das entidades que o possuem através da parte direita da janela. A área de trabalho para a edição de código é simplificada para evitar que o projetista faça mudanças que comprometam a consistência dos dados. A ferramenta provê um recurso de verificação simples de erros para que o usuário tenha noção do impacto de suas alterações diretas no código.

4.2.4 Monitoramento

Uma grande vantagem de ter todo o modelo de informação mapeado numa árvore de dados é que uma única ferramenta de gerenciamento pode ser usada para administrar todos os serviços e ações da Rede. Dado o fato de que interfaces apropriadas são providas entre os P-Nodes, que são capazes de atualizar a árvore, e os serviços, na maioria dos casos, ferramentas proprietárias são desnecessárias. Geralmente o administrador deverá ser capaz de ter uma

visão integrada de todas as entidades gerenciadas. A habilidade de editar e visualizar os atributos das entidades torna isso possível.

Um dos recursos interessantes da visão de monitoramento é a possibilidade de analisar a execução e decisão das políticas através dos históricos de execução das Redes. O histórico (ou *log*) poderá ser armazenado localmente (independente do tipo de projeto) para posterior verificação. Novas abordagens para monitoramento de atributos estão sendo estudadas (capítulos 8 e 9).

5 Uso de XML e Padrão XACML

Insatisfeitos com os formatos descritivos existentes (padronizados ou não), um grupo de empresas e organizações que se autodenominou *World Wide Web Consortium* (W3C) começou a trabalhar em meados da década de 1990 em uma linguagem de marcação que combinasse a flexibilidade da SGML (*Standart Generalized Markup Language*), uma linguagem capaz de descrever diversos tipos de dados, com a simplicidade da HTML (*HyperText Markup Language*). O princípio do projeto era criar uma linguagem que pudesse ser lida por *software*, e integrar-se com as demais linguagens. Sua filosofia seria incorporada por vários princípios importantes [15].

XML é um acrônimo para *EXtensible Markup Language* (linguagem extensível de marcação). Trata-se de uma linguagem que é considerada uma grande evolução na internet. A linguagem XML é definida como o formato universal para dados estruturados na Web. Esses dados consistem em tabelas, desenhos, parâmetros de configuração, etc. A linguagem então trata de definir regras que permitem escrever esses documentos de forma que sejam adequadamente visíveis ao computador [16].

XML é simples porque possui a mesma estrutura de *tags* comumente encontrada em linguagens recorrentes de marcação, como o próprio HTML, e é extensível e maleável o bastante para suportar modificações que se adaptem a qualquer modelo de informação. Não obstante, o XML se tornou o padrão universal para comunicação de dados em aplicações orientadas a objetos. Uma ilustração é o uso da linguagem em conceitos que se propõem a ser comunicadores universais, como *Universal Plug-and-Play* (UPnP) e *Webservices*.

Por estas razões, a equipe técnica do projeto PBMAN decidiu adotar o XML como linguagem de comunicação de entidades, visto que esta propõe unificar e uniformizar as mensagens que trafegarão por meios tão distintos, seja uma antena de grande alcance ou um telefone celular, além de ser baseada no paradigma usado de orientação a objetos e por corresponder a um padrão internacionalmente utilizado.

5.1 XACML

Redes de Ambiente impõem novos desafios em matéria de gerenciamento, e políticas, conforme visto no capítulo 3, são consideradas uma solução adequada para prover flexibilidade, controle distribuído e auto-gerenciamento. Entretanto, os modelos de políticas correntemente usados pela IETF não foram desenhados para os desafios encontrados pelas tecnologias 3G e 4G, como o uso de Redes de Ambiente.

Uma vez que o padrão escolhido é muito flexível e passível de confusão e ambigüidade, um novo padrão, originado a partir do XML foi selecionado para representar o comportamento das políticas.

A princípio foi elaborada uma linguagem própria de descrição de políticas, facilmente compilável por uma máquina, e ainda compreensível ao entendimento humano, uma vez que se aproxima muito da linguagem natural. Mais adiante a equipe decidiu escolher o XACML (*eXtensible Access-Control Markup Language*), uma linguagem definida pela organização de padronização OASIS (*Organization for the Advancement of Structured Information Standard*), e ficando a primeira linguagem elaborada usada para demonstrações visualmente mais agradáveis e definições de modelo de negócio. A razão da transição se fez devido às

conhecidas vantagens de se usar padrões, tais como substituir muitas linguagens específicas, evitando que a políticas precisem ser reescritas em diversas linguagens diferentes. Uma outra vantagem de se usar padrões reconhecidos é a disponibilidade de ferramentas de edição, e da criação de uma comunidade de discussão para assuntos relacionados. O PMT só foi viável graças ao enorme volume abrangendo políticas em XACML encontrado na literatura.

```
<Policy PolicyId="P21" RuleCombiningAlgId="priority-combining">
    <Target>
        <Subjects>
            <Subject>
                <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">any-subject</AttributeValue>
                    <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </SubjectMatch>
            </Subject>
        </Subjects>
        <Resources>
            <Resource>
                <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">vpn-pep</AttributeValue>
                    <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </ResourceMatch>
            </Resource>
        </Resources>
        <Actions>
            <Action>
                <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">start</AttributeValue>
                    <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </ActionMatch>
            </Action>
        </Actions>
    </Target>
    <Rule RuleId="R1" Priority="1" Effect="Permit">
        <Processing FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
            <Apply FunctionId="perform-configuration">
                <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                    <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </Apply>
                <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                    <Apply FunctionId="get-context-variable">
                        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">clientAddress</AttributeValue>
                    </Apply>
                </Apply>
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">start</AttributeValue>
            </Apply>
        </Processing>
    </Rule>
</Policy>
```

Ilustração 8: Exemplo de política de controle de acesso.

5.1.1 Vantagens do XACML

O XACML se propunha a padronizar o gerenciamento de políticas e decisões de acesso. A linguagem se tornou um padrão da OASIS em fevereiro de 2003 [17], e define uma linguagem genérica de políticas usada para proteger recursos bem como uma linguagem para decisão de acesso.

A linguagem extensível de marcação para controle de acesso é um padrão baseado em XML que provê uma linguagem de políticas e um protocolo de requisições e respostas para controle de acesso, úteis para gerenciar o uso dos recursos. Ela foi projetada para ser uma linguagem universal de políticas de autorização, no sentido de permitir interoperabilidade com uma grande gama de ferramentas restritivas e administrativas.

Além das definições já bem compreendidas na área de gerenciamento, tais como as de PDP e PEP, XACML usa outras definições e conceitos importantes, como:

- Requisição de decisão (*Decision request*): o pedido lançado de um PEP a um PDP, que pode fazer estes gerarem uma decisão (resposta) de autorização;

- Efeito (*Effect*): A conseqüência pretendida por uma regra satisfeita (efeitos normalmente são permitir ou negar);
- Decisão de autorização (*Authorization decision*): O resultado da avaliação de uma política aplicável, isto é, a resposta retornada de um PDP a um PEP. Seus valores são de simples permissões e negações de acesso a exceções sobre regras não aplicáveis ou decisões não determinadas ou conjuntos de obrigações a serem cumpridas;
- Alvo (*Target*): Uma parte em comum entre as políticas de acesso e requisições de acesso, composto de um recurso (*Resource*), um sujeito (*Subject*) e uma ação (*Action*). A partir da combinação dos alvos que se descobre a aplicabilidade de uma política;
- Obrigação (*Obligation*): Uma operação especificada na política que pode ser executada pelos PEPs;
- Condição (*Condition*): Uma expressão booleana que sempre terá como resultado "verdadeiro" ou "falso". As condições são usadas para verificar o casamento de regras dentro das políticas.

```
<Request>
    <Subject>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>Alice
      </Attribute>
    </Subject>
    <Resource>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                 DataType="http://www.w3.org/2001/XMLSchema#anyURI">
        <AttributeValue>video-service
      </Attribute>
    </Resource>
    <Action>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>start
      </Attribute>
    </Action>
  </Request>
```

Ilustração 9: Exemplo de política de requisição.

5.1.2 Limitações do XACML

A principal limitação do XACML na condição de linguagem genérica de políticas para Redes de Ambiente está justamente no seu nome, destaque para "controle de acesso". O controle de acesso é focado apenas em limitar a atividade de usuários legítimos de certos recursos que foram devidamente autenticados [17].

Dada uma requisição para acesso a um recurso, o PDP avalia todas as políticas e retorna um resultado, que pode ser uma permissão ou negação ao recurso. A necessidade de dois novos tipos de política foi identificada a partir da avaliação de gerenciamento de Redes de Ambiente. Políticas de configuração são necessárias para a configuração de alguns serviços como resultado do processamento de uma requisição de autorização. Por outro lado, RA precisam de políticas para gerenciar o processo de composição.

5.1.3 Extensões do XACML no Projeto PBMAN

Para o projeto PBMAN, foram necessárias várias extensões ao XACML, para que as políticas deste suportassem configuração de recursos e composição de redes e agentes. Algumas das modificações feitas para que o XACML suportasse funções mais avançadas foram: inserção da capacidade de execução de uma função localmente, atribuição de prioridades às políticas e regras para resolução simples de conflitos, acesso direto ao repositório de dados, para a obtenção de informação extra das entidades, e uso de um novo atributo para combinação das requisições com as políticas.

5.2 XML / XACML no PMT

Inicialmente o *Policy Management Tool* foi idealizado para ser uma ferramenta que editasse as complexas políticas XACML de uma forma mais simplificada e amigável aos usuários, evitando a confusão de usar inúmeras *tags* e tipos em sua representação. O projeto PBMAN precisava de algo que adiantasse a criação de políticas, uma vez que a fase de prototipação precisava ser iniciada, e desde então o PMT começou a ser desenvolvido. A partir deste desenvolvimento orientado a prototipagem, e através das pesquisas realizadas, foi visto que o PMT poderia adquirir mais propriedades de ferramenta avançada de edição e monitoramento das redes de ambiente, e os recursos hoje existentes na ferramenta foram idealizados, pesquisados e implementados.

Atualmente o PMT conta com três visões (ou *Views*) para permitir uma maior flexibilidade e poder de decisão ao administrador da rede ou responsável por criá-la, modificá-la ou monitorá-la. Uma destas visões, a *General View* (Ilustração 17: Visão dividida e uso de abas.), corresponde a uma representação em árvore da estrutura de armazenamento que será discutida mais adiante, e da possibilidade de visualizar e editar o código para cada entidade. Todas as entidades presentes numa rede de ambiente possuem uma representação em XML, para que seus dados possam ser mantidos através da estrutura de armazenamento utilizada (capítulo 6). Usuários, Grupos, Serviços, Nós da rede e Modelos de Rede têm seus atributos guardados de forma estruturada em um arquivo XML, enquanto as políticas são representadas por códigos definidos pelo padrão XACML.

A ferramenta permite que o código seja gerado de duas formas, e modificado de três formas:

- A primeira interface desenvolvida no editor com o intuito de facilitar a criação de código foi a edição por menus/*wizards*. Através de guias passo-a-passo é possível tanto criar quanto modificar as entidades sem interagir diretamente com XML / XACML. Através da interação direcionada os complexos códigos XACML são gerados para as políticas desenvolvidas a partir do *Policy Creation Wizard*;
- Uma outra abordagem para criação e edição de código é a abordagem gráfica, através da qual é possível "arrastar" ícones que representam entidades e descrever apenas seus atributos. Seus relacionamentos com outras entidades se dão por conexões no próprio modelo gráfico. Esta visão, no futuro, terá recursos para gerar qualquer tipo de código XACML, já que atualmente o PMT gera apenas código para políticas de controle de acesso, em detrimento dos outros tipos de política mencionados;
- O modo de edição textual pode ser usado apenas para edição, uma vez que a idéia da ferramenta é evitar que o usuário desta precise escrever códigos a partir "do zero". Apesar de dar maior autonomia e poder de modificação, este recurso abre espaço para que ocorram falhas humanas. Desta forma, um suporte primário a erros (Ilustração 21: Edição de código com destaques de

linha e suporte a erros simples.) foi desenvolvido para evitar que o usuário cometa deslizes graves.

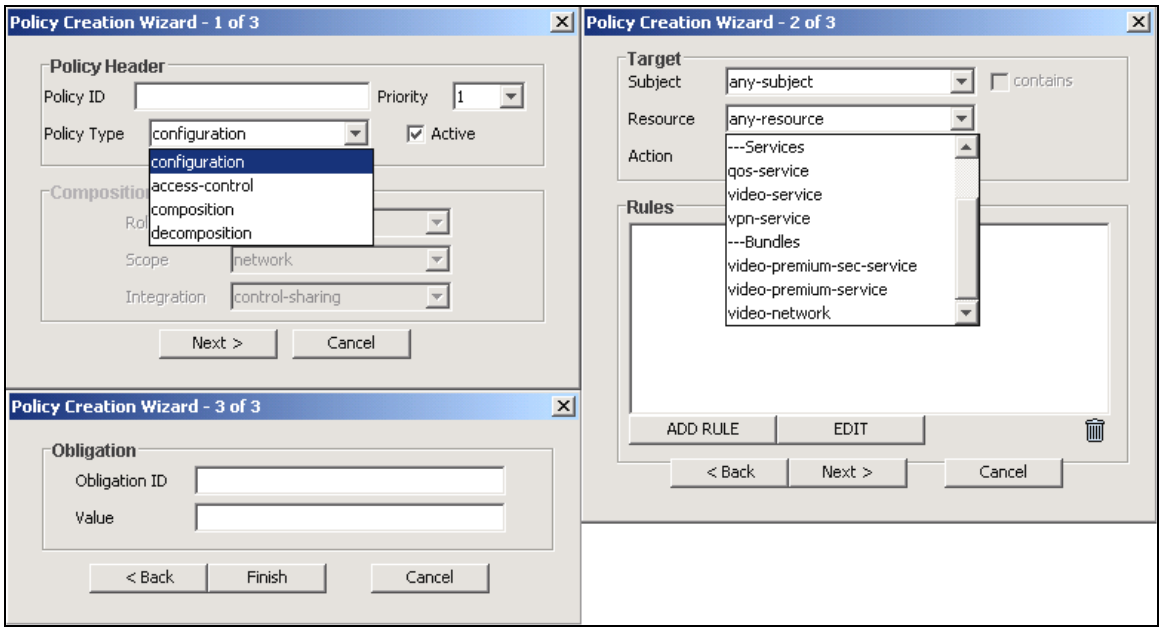

Ilustração 10: Passo-a-passo do *Policy Creation Wizard*.

5.2.1 Geração de Código

Nesta seção serão ilustradas as abordagens utilizadas para geração de código a partir da representação central das entidades usadas na ferramenta. Na arquitetura (capítulo 4) vimos como o módulo de geração de código se relaciona com outros módulos nesta abordagem encontrada para trabalhar com Redes de Ambiente e Orientação a Objetos.

5.2.1.1 Código das entidades

As entidades que interagem entre si numa Rede de Ambiente possuem apenas alguns atributos e relacionamentos a serem representados através do XML, de forma que se optou por não usar biblioteca ou padrão de projeto para a geração de código das entidades. Cada entidade possui uma rotina responsável por gerar um código XML, no esquema definido para o projeto, contendo suas entidades e com uma formatação textual amigável à compreensão humana.

5.2.1.2 Código das políticas

As políticas em XACML possuem *tags* e estruturas que, em respeito aos padrões definidos pela OASIS, tornam-se enfadonhos de ser representados ou gerados manualmente. Tendo isso em vista, a *Sun Microsystems* desenvolveu uma biblioteca utilitária de código aberto contendo uma implementação do padrão XACML da OASIS em Java, a SunXACML. O código fornecido pela Sun precisou ser estendido para ser usado no PMT, uma vez que o projeto PBMAN propôs alterações ao padrão XACML. As modificações permitiram que as classes da biblioteca suportassem mais atributos e, consequentemente, que as rotinas de geração de código da SunXACML comportassem esses novos atributos e gerassem o código aplicável para o projeto em questão.

```
<Policy PolicyId="P1" RuleCombiningAlgId="priority-combining">
...
<Rule RuleId="R2" Effect="Permit">
```

```
<Policy PolicyId="P1" RuleCombiningAlgId="priority-combining" Priority="2" Type="access-control" Active="true">
...
<Rule RuleId="R2" Priority="1" Effect="Permit">
```

Ilustração 11: Acima o XACML definido pela OASIS, abaixo algumas das modificações feitas para dar suporte ao projeto PBMAN.

5.2.2 Leitura de Código

Para realizar o caminho inverso, isto é, a geração de uma entidade de Orientação a Objetos a partir da interpretação do código foram usadas algumas bibliotecas e camadas de código.

Para que o código seja transformado de uma seqüência de caracteres em uma estrutura orientada a objetos, o PMT usa classes da biblioteca DOM da W3C (*World Wide Web Consortium* – consórcio da rede de alcance mundial) e da extensão de Java para tratar XML. Estas bibliotecas geram um modelo de informação que pode ser mais facilmente manipulado pelo PMT. Todavia, a restituição deste modelo resulta numa estrutura deveras fragmentada, o que prejudica sua interpretação e posterior conversão para o objeto usado pela ferramenta para representação interna. Para contornar este problema é gerada uma segunda estrutura de dados mais simples que a primeira, e desta forma os interpretadores específicos para cada entidade ficam responsáveis apenas por restaurar seus devidos atributos e relacionamentos.

Esta divisão em camadas de complexidade de estruturas foi o trunfo que permitiu ao PMT "entender" qualquer espécie de XML, bem como facilitou a validação das informações contidas no código interpretado (tópico 5.3).

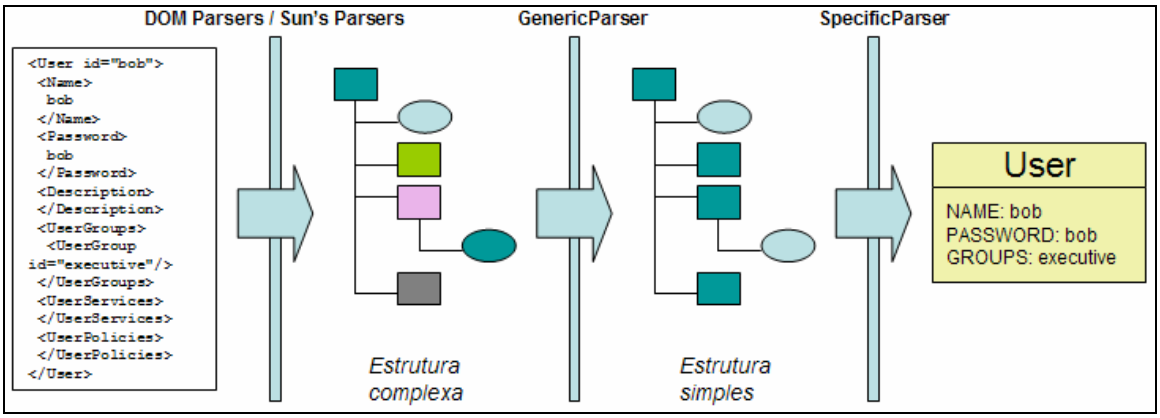

Ilustração 12: Processo de interpretação de código.

5.3 Validação de código

Comumente para validar a estrutura (*schema*) de um arquivo XML são usados os DTDs (*Document Type Definition* – definição de tipo de documento). DTDs são documentos que contêm as regras que definem quais as *tags* que devem ser usadas num XML e quais valores serão aceitos. Apesar de ser um padrão internacional, os *doctypes* representam um custo computacional extra para validação, sem falar que são uma barreira que dificulta a realização de requisitos da ferramenta, tais como estensibilidade das entidades e genericidade da ferramenta (isto é, seria necessário modificar os DTDs sempre que uma entidade fosse estendida, ou gerar uma DTD nova para cada entidade implementada).

Apesar do uso de DTDs possuir grande reconhecimento e não apresentar tanta dificuldade de implementação, foi preferível, por motivos de custo computacional e agilidade de implementação, usar uma abordagem mais genérica, capaz de abranger de forma mais facilitada conceitos como estensibilidade, flexibilidade e genericidade.

Por este motivo, foi implementada uma abordagem baseada em árvores de dados, que permitirá o uso de uma estratégia recursiva para busca e validação das informações contidas no XML. O esquema de interpretação de código descrito acima é bastante útil, uma vez que fica mais fácil navegar numa estrutura simples e de domínio bem conhecido em vez de iterar sobre uma estrutura complexa.

No terceiro estágio da Ilustração (Estrutura simples) a aplicação já sabe qual estrutura de dados está processando – uma vez feita a interpretação genérica o interpretador terá informações sobre qual entidade está interpretando, e consequentemente quais campos devem ter valores aceitáveis. Desta forma, cada entidade tem um conjunto atributos e valores possíveis e obrigatórios, para que o interpretador possa analisar a Estrutura simples e permitir sua conversão em um objeto ou não.

6 Abordagens para Armazenamento de Dados

A criação de uma Rede de Ambiente demanda estudo corporativo e entendimento aprofundado do modelo de negócio. Por esta razão, se faz necessário o uso de um conceito que permita armazenar as entidades e políticas de uma Rede de Ambiente de forma que seja possível desenvolver parcialmente e portar a solução ou testá-la num contexto pormenorizado. Também será necessário abordar uma forma de publicar os dados da Rede no ambiente onde esta funcionará. Este capítulo irá abordar estes conceitos e vai apresentar a forma como eles são usados no PMT.

6.1 Projeto Local

Em ferramentas onde os dados podem ser divididos em várias ópticas, e geralmente se usa mais um arquivo para representar estas informações, é comum encontrar o conceito de projeto. Um projeto – neste sentido – é um conglomerado de documentos relacionados de forma que o conjunto apresente um comportamento esperado por quem o desenvolveu. Este conceito foi usado para que os desenvolvedores dos projetos pudessem fazê-lo em partes, sempre verificando seu modelo de informação e realizando testes de validação e verificação sem ter que implantá-lo em seu ambiente de uso final.

Normalmente os ambientes integrados de desenvolvimento (IDE - *Integrated Development Environment*) usados para desenvolver programas utilizam este conceito, já que um software é intrinsecamente um projeto. O desenvolvimento de uma aplicação envolve vários arquivos ligados de forma estruturada para cumprir um objetivo de funcionamento.

Tendo em vista que o *Policy Management Tool* é uma ferramenta de desenvolvimento, ou "uma IDE para Redes de Ambiente", foi necessário implementar neste alguns artifícios que tornassem possível aos projetistas desenvolver as Redes em um ambiente mais simples e rápido, e que estas soluções temporárias pudessem ser compartilhadas entre projetistas sem envolver o uso de muitos recursos computacionais.

O projeto local do PMT consiste de um diretório contendo um arquivo de especificação de projeto, opcionalmente, um arquivo com o histórico da rede local (será discutido no capítulo 8) e subdiretórios que englobam vários arquivos XML. Cada arquivo corresponde a uma entidade ou política da RA, os quais contêm toda informação necessária para seu reconhecimento e comportamento dentro da rede (conforme visto no capítulo 5).

Quando o usuário do PMT opta por criar um projeto local, a ferramenta armazena todas as modificações feitas nas entidades e políticas em disco, num local escolhido pelo mesmo. Este local simula uma Rede funcional para que o usuário possa desenvolver em um ambiente próximo do real. Quando o projeto for validado e verificado, o mesmo pode ser publicado através da ferramenta, para passar a ter uso prático. O projeto publicado passa a funcionar como um projeto remoto, ou uma rede em funcionamento.

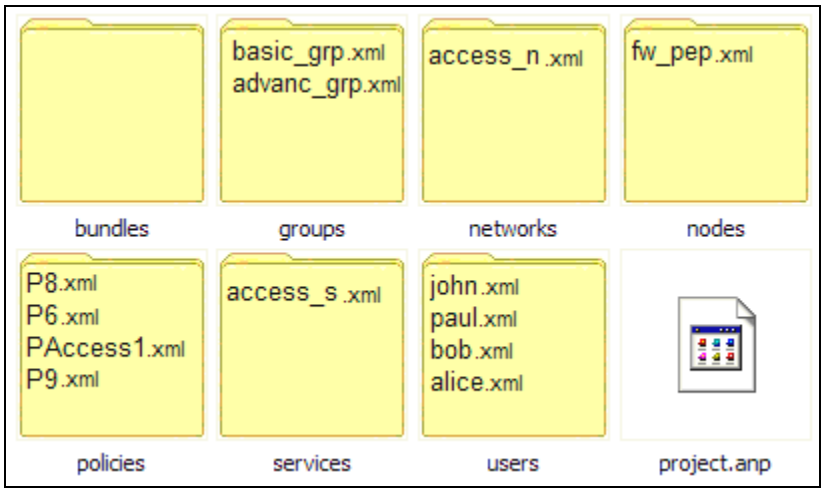

Ilustração 13: Estrutura de um projeto local, armazenado em disco.

6.1.1 Interface Local

A fim de prover um meio único capaz de interagir com o sistema de arquivos da máquina foi criado o módulo Interface Local. Apenas através dele, a ferramenta pode armazenar ou recuperar dados referentes ao projeto do sistema de arquivos.

A solução foi pensada para ser uma camada de abstração para o núcleo do PMT. Enquanto comandos simples a nível de ferramenta de edição são passados para a interface, esta gera comandos específicos de sistema operacional para gravação e leitura do disco, funcionando também como uma camada única de suporte a erros e exceções.

A Interface Local possui rotinas que recuperam todo um projeto do sistema de arquivos, realizam cópias de segurança de um projeto remoto para o disco e rotinas que movimentam unicamente cada arquivo. É na recuperação de arquivos XML que acontece a interpretação de código através do esquema descrito na Ilustração 12: Processo de interpretação de código. Entretanto, a Interface Local, a exemplo do próprio nome, é apenas um meio de comunicação entre o sistema de arquivos e o PMT, de forma que a interpretação e geração de código acontecem fora deste módulo.

6.2 Projeto Remoto

Visando pôr em execução as entidades relacionadas e aplicar as regras definidas num contexto real, as entidades e políticas precisam ser publicadas em redes para acesso de todos os dispositivos que a alcancem. Para cumprir este objetivo dentro do projeto PBMAN foi decidido o uso de redes *peer-to-peer*.

O conceito de projeto remoto foi explorado neste sentido porque possibilita ao administrador da rede realizar modificações em sua estrutura e comportamento diretamente no seu ambiente de execução através da ferramenta, contudo, a rede de ambiente publicada não é praticamente um projeto, e sim o resultado da conclusão de um projeto, uma vez que as ações esperadas já estão sendo executadas. Já que o PMT deveria permitir este tipo de alteração, a rede já publicada teria que ser visualizada de uma forma intuitiva e de fácil modificação, por esta razão foi desenvolvida a idéia de projeto remoto.

O projeto remoto é visto exatamente como um projeto local, a visualização de sua estrutura de árvore, do código das entidades e políticas, a possibilidade de edição gráfica e o monitoramento através dos históricos. Já que a Rede de Ambiente depois de publicada se torna acessível a várias partes que possuam permissão para tal, existe a possibilidade de haver acesso concorrente à Rede. Desta forma, no projeto remoto, acontece uma atualização periódica dos dados contidos na árvore, numa tentativa mínima de se manter a consistência das informações. A verificação de integridade das informações para acessos múltiplos a uma árvore de dados é ainda um ponto a ser resolvido pelo PMT.

Para se acessar um projeto remoto, é necessário que o administrador possua um *login* e senha, verificados pelo PDP, um endereço IP do nó de acesso (ou uma lista de possíveis endereços) e a porta pela qual os dados devem trafegar. Por questão de simplicidade de operação, a ferramenta oferece a opção de salvar um arquivo-chave contendo estas informações, o que agiliza o processo de abertura de um projeto remoto.

Todas as entidades ficam armazenadas em nós especiais que pertencem a redes X-Peer, os *storage nodes* (SNodes). Os PDPs carregam estas informações sob demanda para poder realizar as tarefas sobre os dados e políticas relacionados.

6.2.1 P2P

Redes *peer-to-peer* (P2P) são redes virtuais que funcionam na Internet com o objetivo de compartilhar recursos entre os participantes, sendo que por princípio não existe diferenciação entre eles [11]. Este novo paradigma promoveu uma grande modificação nos padrões de uso da Internet, uma vez que possibilita a colaboração direta entre os usuários.

A natureza descentralizada e distribuída dos sistemas P2P os torna robustos e tolerantes a falhas, uma vez que acontecendo a queda de um dos *peers* os outros dão o suporte necessário para manter o sistema em funcionamento. Esta arquitetura também é útil para economizar os recursos de *hardware*, sem falar que permite o uso do processamento de máquinas ociosas da rede para operar sobre grandes volumes de dados.

Um ponto de destaque do modelo P2P é sua capacidade para controlar crescimentos incontroláveis a respeito do número de entidades acessando a rede, quantidade de dispositivos conectados, número de nós da rede, capacidade da rede, aplicações e capacidade de processamento. Em um sistema cliente/servidor, os servidores são os únicos responsáveis por suprir todas as necessidades dos clientes, o que inviabiliza as operações em horários de pico. Já nos sistemas P2P, quando o número de clientes cresce, aumenta também o número de servidores, mantendo uma proporção de um para um e sustentando o equilíbrio da rede. Dessa forma, o sistema aumenta de tamanho sem perder escalabilidade [11]. Todas estas características são úteis para Redes de Ambiente.

6.2.2 X-Peer

O X-Peer é um *middleware* para a construção de aplicações P2P que utiliza o conceito de super-nós que se comunicam através de uma rede estruturada baseada em tabelas de código distribuídas (*distributed hash tables* - DHT), o que lhe permite recuperar todas as informações disponíveis na rede X-Peer [21]. O fato de redes X-Peer garantirem a localização dos dados em um contexto hierarquicamente distribuído é um grande diferencial da solução utilizada. Além disso, o X-Peer é capaz de suportar várias aplicações P2P em uma única infra-estrutura de rede [21]

Na rede X-Peer, qualquer informação em qualquer nível de representação precisa ser vista como um tipo de dado aceito pelo X-Peer, isto é, um conjunto campo + valor. Desta forma, toda informação, inclusive partes de conjuntos de dados maiores, pode ser facilmente armazenada e recuperada da rede. Essas informações são armazenadas de forma distribuída entre os super-nós que compõem a rede X-Peer e são categorizadas em campos (tipos) e valores. Os campos são utilizados pelo DHT para indicar o local (nó) em que as informações referentes a esse campo estarão armazenadas.

Ainda referente aos campos utilizados pelo DHT, é justamente a granularidade do campo escolhido para ser aplicada a função *hash* que irá determinar o grau de distribuição de informações na rede X-Peer. A escolha do campo para a função *hash* constitui um *trade-off* entre o grau de distribuição e a eficiência da busca. O diferencial do X-Peer nesse aspecto é permitir ao desenvolvedor de aplicações a flexibilidade em refletir em suas aplicações a avaliação desse *trade-off* de acordo com suas necessidades reais.

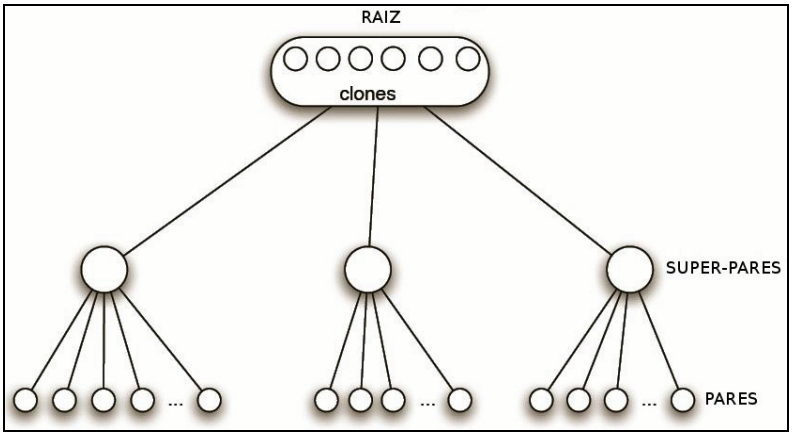

Ilustração 14: Níveis de arquitetura de rede X-Peer [18].

Através de análises de performance em [21] foi possível comprovar que X-Peer é escalável, oferecendo tempo de resposta aceitável com crescimento linear à carga submetida à rede, onde as operações mais custosas são realizadas com baixa freqüência.

6.2.2.1 Funcionamento

Os dados em formato XML (ou XACML, no caso das políticas) não chegam a ser transmitidos entre os pares da rede X-Peer em nenhum momento. A Visão de Árvore, responsável por montar a estrutura básica a ser manipulada pelo PMT, já é em si uma visão adaptada da hierarquia XML em forma de ramos e folhas de uma árvore lógica. No módulo Interface Remota, localizado logo abaixo da Visão de Árvore, acontece a abstração da estrutura de árvore para um conjunto de estruturas do tipo campo-valor. Estas novas estruturas serão transmitidas aos pares X-Peer através da rede.

Vale salientar que os pares da rede podem armazenar informações com a mesma função *hash*, o que vem a ser uma replicação de segurança da informação. O objetivo de se usar tabelas de código distribuídas é dividir a carga proveniente do acesso em vários nós da rede e ainda assim prover um acesso rápido a todos os dados.

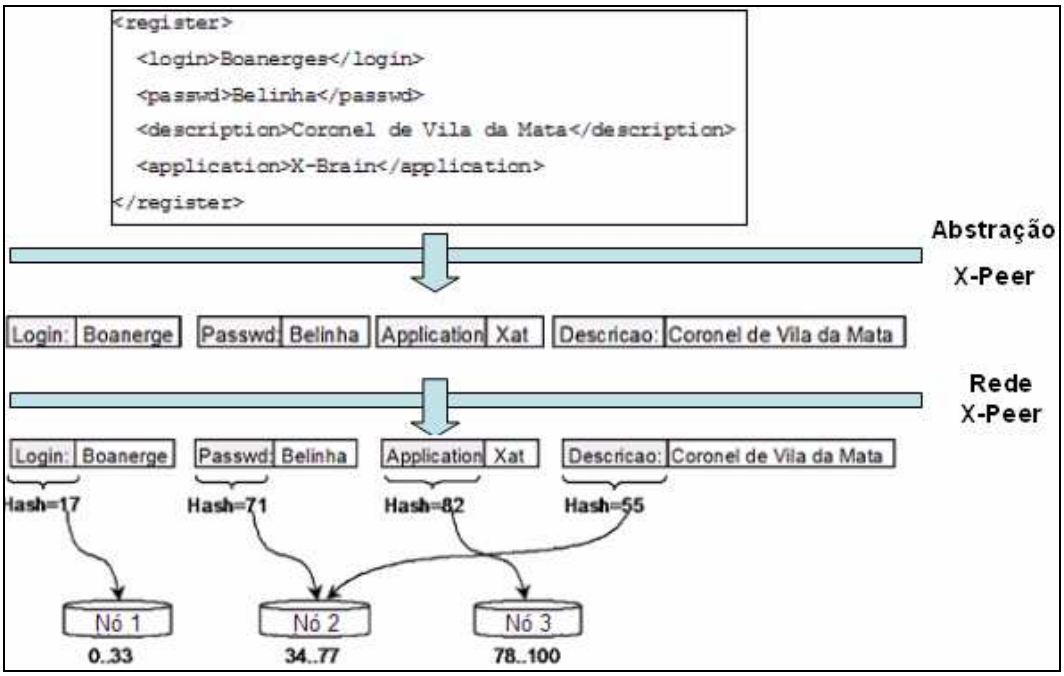

Ilustração 15: Funcionamento do armazenamento X-Peer.

6.2.3 Interface Remota

Visto que os projetos remotos (ou redes publicadas) estão armazenados em um conjunto de computadores (rede X-Peer), foi necessário que houvesse uma entidade responsável por unificar o acesso do PMT a esta rede, visando evitar ambiguidade e inconsistências. Esta entidade, capaz de recuperar os dados de vários pontos e uni-los em uma estrutura de árvore para posterior acesso é a Visão de Árvore (seção 4.1).

A Visão de Árvore se comunica com o PDP onde as políticas estão armazenadas e através destes recupera informações a respeito dos SNodes nos quais os dados das entidades se encontram. Conforme visto anteriormente, o Mapeamento de Modelos se liga à Visão de Árvore para acessar as informações de forma centralizada, uma vez que este é o módulo responsável por manter a integridade da árvore que representa uma Rede de Ambiente, uma vez que ele verifica toda a estrutura da árvore antes de fazer qualquer alteração na mesma. Desta forma, a rede publicada pode ser modificada como se ainda fosse um projeto, sem que haja o risco de deturpação da estrutura ou geração de erros e inconsistências.

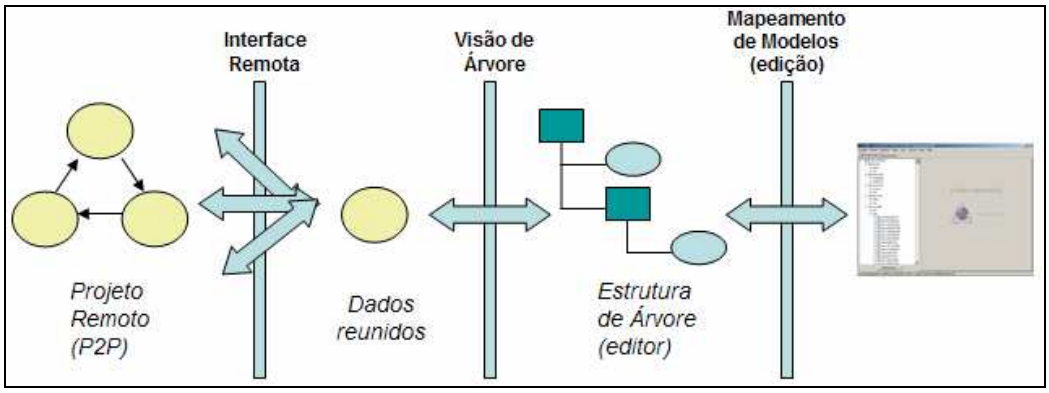

Ilustração 16: Detalhamento da Ilustração 14 mostrando interação dos módulos internos do PMT com o projeto remoto (Rede publicada).

7 Uso da Ferramenta

Até este ponto foram vistos conceitos utilizados, pesquisas realizadas e metodologias e protocolos implementados para que a ferramenta proposta cumprisse seu papel dentro do contexto de edição e observação das Redes de Ambiente controladas por Políticas. A base teórica dada foi essencial para o entendimento da utilidade do PMT, entretanto, uma visão prática de suas capacidades é imprescindível para que haja uma melhor compreensão de sua criação.

Este capítulo mostra as abordagens e casos de uso idealizados para que se encontrassem na literatura recursos tecnológicos os quais possibilitassem a implementação da ferramenta. A maioria das interações possíveis entre administrador e editor foram discutidas em reuniões, de forma que apenas recursos interessantes e viáveis foram aproveitados para o desenvolvimento da ferramenta. Abaixo será demonstrada a conformidade da aplicação implementada com a proposta feita para a mesma.

7.1 Interface gráfica

Por ser uma ferramenta de edição de ambientes complexos e até em grande escala, a simplicidade na apresentação visual é um ponto crucial para este o editor. Da mesma forma, ações intuitivas e comportamentos transparentes precisaram ser pensados durante a implementação.

Visando a maior clareza visual possível sem perda de espaço de trabalho, a interface foi dotada de muitas abas. A navegação através de abas se mostrou uma tendência promissora, não obstante é aproveitada em várias aplicações como editores de texto, navegadores e IDEs. Assim sendo, todas as visões do PMT, bem como a visualização dos seus códigos estão em interfaces navegáveis através de abas.

A abordagem inicial da ferramenta tinha como objetivo apenas navegar por todas as entidades e poder validar seus respectivos códigos. Levando isso em consideração foi usado o paradigma de visão dividida, recorrente em IDEs.

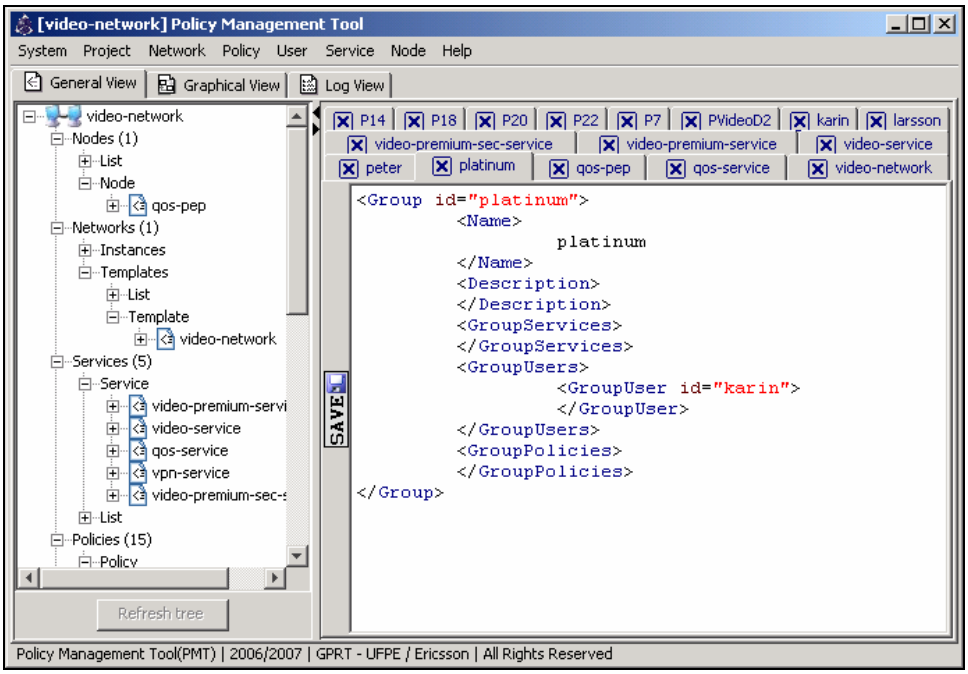

Ilustração 17: Visão dividida e uso de abas.

O PMT possui recursos de integração com uma rede de computadores responsáveis por armazenar informações e executar tarefas. Por este motivo ocorre atraso de algumas tarefas, o que pode acarretar uma falsa impressão de pane no sistema. Por este motivo, a interface gráfica é dotada de uma barra de progresso a qual é exibida sempre que uma atividade de longa duração não tiver sido concluída.

Ilustração 18: Barras de progresso.

7.2 Visões da ferramenta

O PMT possui diferentes visões cujo objetivo é fornecer diferentes ópticas ao administrador, entrar em determinados níveis de detalhe, a depender a atividade a ser executada, e controlar degraus de permissão de modificação da rede, ou seja, gerenciar o poder do usuário da ferramenta. Atividades simples podem ser mais facilmente aplicadas através uma determinada visão, e tarefas que exigem mais poder e conhecimento do nível de tecnologia podem ser executadas através de outra visão.

Por questão de clareza visual e facilidade de uso, as visões foram separadas por abas, a exemplo do paradigma gráfico que foi pensado para o editor. Abaixo, algumas características das visões existentes.

7.2.1 Visão geral

A visão geral (ou *General View*) permite a total navegação pela árvore que representa a Rede de Ambiente, bem como a visualização e edição textual de suas entidades e a edição através de menus. A visualização da estrutura da Rede através da árvore também permite realizar as mesmas tarefas que os menus, através de menus de contexto – um atalho bastante útil para editores deste tipo. As maneiras através das quais o administrador pode interagir diretamente com a estrutura da Rede nesta visão seguem abaixo.

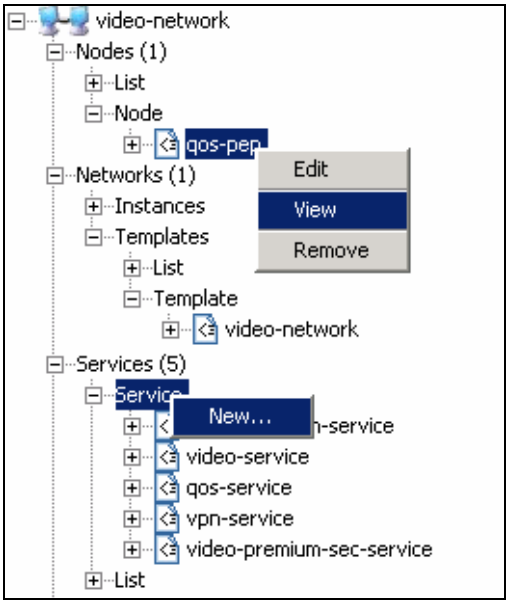

Ilustração 19: Menus de contexto na Visão de Árvore possuem as mesmas funcionalidades do menu da ferramenta.

7.2.1.1 Edição por menus

A primeira interface desenvolvida, por ser intuitiva e mais simples de implementar, foi o uso de menus e guias de desenvolvimento. Menus, a exemplo dos comumente encontrados nas aplicações de escritório atuais, fornecem acesso à criação, edição, visualização e remoção de entidades e políticas. A interação do usuário com a ferramenta passa a ser o uso de formulários com os campos necessários à construção de uma entidade ou política, fazendo-se uso de guias (ou *wizards*) para os casos mais complexos, como o guia de criação de políticas (Ilustração 10: Passo-a-passo do *Policy Creation Wizard*.).

Os menus também apresentam recursos extras como a remoção de todos os dados da árvore e a exportação e importação consistente de qualquer entidade ou política (possuidores de código representativo).

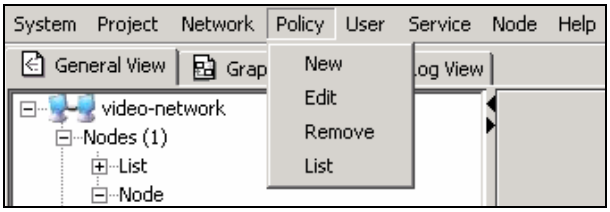

Ilustração 20: Menus.

7.2.1.2 Edição textual

O PMT foi desenvolvido com o intuito de evitar o custo de trabalho necessário para se desenvolver uma representação textual das entidades e as regras em forma de políticas. Contudo, esta abstração dada ao projetista de rede acaba tirando um pouco de seu poder de modificar a árvore diretamente no código XML.

Algumas alterações em políticas consistem de simples modificações de valores em atributos, e usar uma interface gráfica baseada em menus e formulários pode ser uma tarefa desnecessariamente desgastante. Neste sentido, a edição manual do código facilita a modificação e devolve o poder aos administradores. O PMT possui um recurso de auto-identação do código, para que a boa legibilidade seja mantida, destaque de trechos em edição, para facilitar a visualização e um suporte a erros simples para evitar o comprometimento da estrutura da árvore.

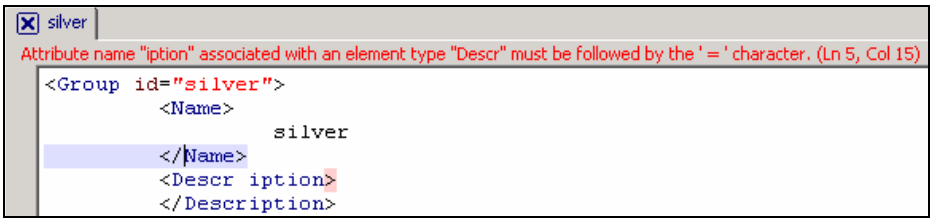

Ilustração 21: Edição de código com destaques de linha e suporte a erros simples.

7.2.2 Visão gráfica

A representação gráfica de cenários e regras de negócio é, de longe, a abordagem de mais alto nível idealizada para um editor. É uma linguagem simples e intuitiva que pode ser compreendida por executivos, e não necessariamente por projetistas com conhecimento específicos em linguagem de marcação e da estrutura da Rede.

Atualmente, o PMT não dá suporte a todos os cenários, apenas aos mais simples casos de controle de acesso. O aumento desta capacidade de edição gráfica é um passo importante para tornar a ferramenta perfeitamente compatível com qualquer organização baseada em Redes de Ambiente.

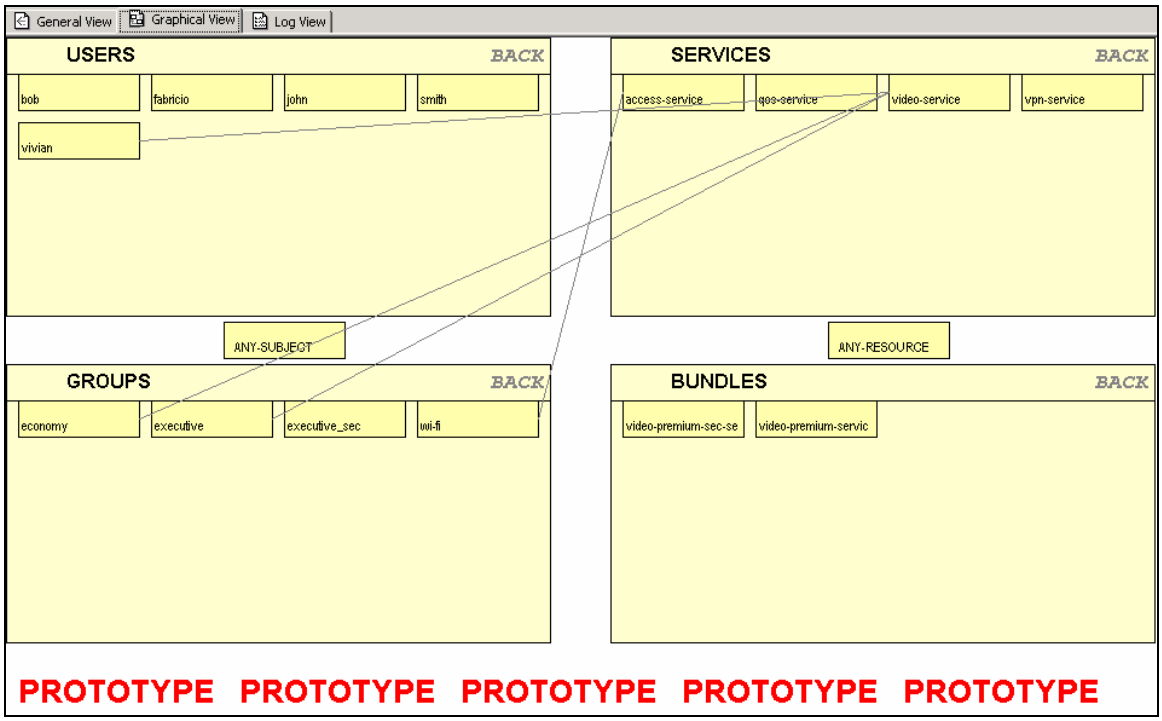

Ilustração 22: Protótipo da edição gráfica via ícones.

7.2.3 Visão de monitoramento

Conforme descrito no capítulo 8, o monitoramento provido pelo PMT ainda é simplório, e é utilizando para simples verificação e correção de erros (*debug*). Abordagens mais avançadas voltadas para cenários maiores e mais complexos estão sendo estudadas.

A ferramenta fornece recursos para aprimorar a capacidade monitorar o funcionamento das políticas. Os filtros de tipo de política, rotinas em execução e data inicial de exibição do histórico permitem ao administrador focar apenas certos comportamentos de políticas, determinados comandos em execução e limpar a visão do *log* a partir de uma certa data, respectivamente. Também é possível selecionar um trecho do histórico e salvá-lo no disco, para avaliação posterior.

Um recurso igualmente digno de destaque é a localização de textos, também presente nos códigos da *General View*, e necessária para agilidade de identificação do trecho em questão ou *debug*.

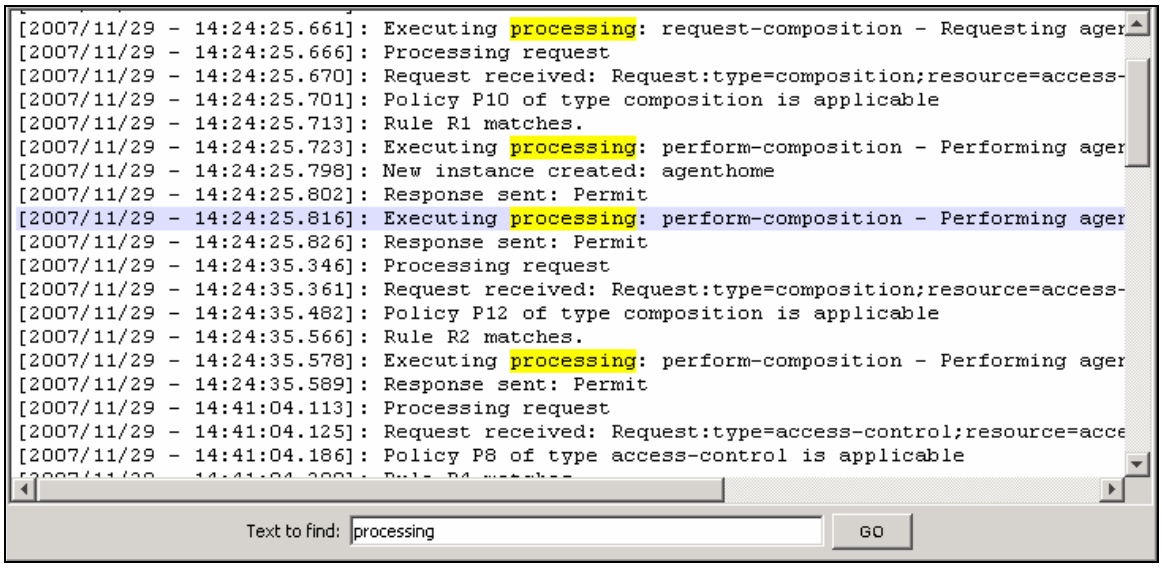

Ilustração 23: Parte da visão do histórico (*Log View*) com destaque para a localização de texto.

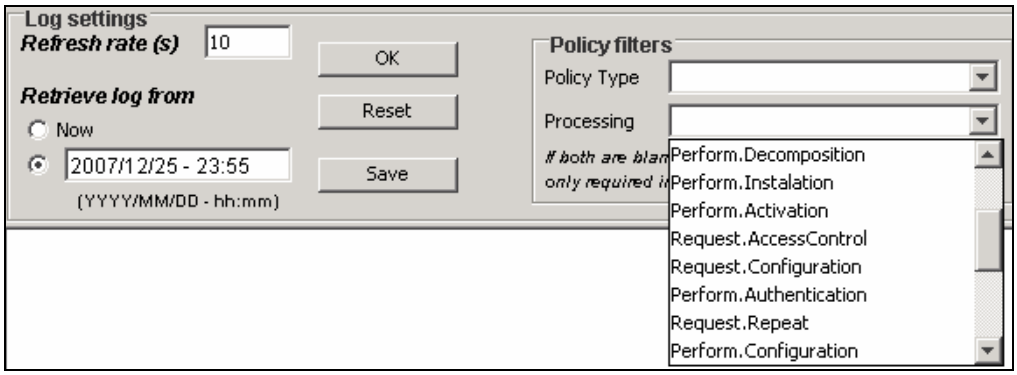

Ilustração 24: Filtros de data, tipo de política e tipo de função executada.

7.3 Importação e Exportação de projetos

Através dos menus é possível criar um novo projeto local, identificando uma localização no disco onde o mesmo deve ser armazenado; abrir um projeto local a partir de sua localização no disco ou abrir um projeto remoto, através de informações de localização em rede como um conjunto de possíveis endereços IP, a porta de dados, um *login* e uma senha. Para se criar um projeto remoto (teoricamente, uma rede publicada) é necessário que se tenha um PNode rodando, isto é, não depende unicamente da ferramenta, mas também da pré-configuração de uma aplicação servidor em algum nó da rede.

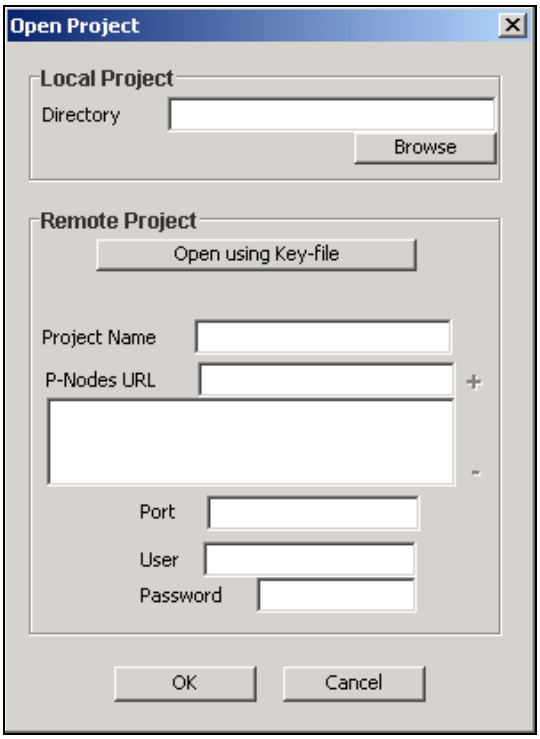

Ilustração 25: Possibilidades de recuperação de um projeto.

Uma vez que se tem uma Rede de Ambiente em forma de projeto é possível realizar duas atividades que envolvem toda a rede: fazer uma cópia de segurança da rede publicada ou publicar uma rede em forma de projeto local. Para fazer um *backup* de uma Rede publicada basta escolher o caminho no disco local onde o projeto deve ser salvo. Já para publicar um projeto local é preciso definir um endereço IP cuja estação possua um servidor funcionando, a porta de dados, e um conjunto de *login* e senha para verificação de acesso.

7.4 Observações de desempenho

7.4.1 Otimização no desenvolvimento

Após o uso da ferramenta no desenvolvimento de Redes de Ambiente para alguns cenários foi observado um bom ganho de produtividade, uma vez que uma tarefa manual de edição de texto passou a ser evitada pelo editor, restringindo a intervenção do administrador apenas ao fornecimento de informações essenciais para cada caso. O uso de um meio automatizado para geração de código também se mostrou interessante no aspecto de eliminar erros de digitação, os quais poderiam gerar falhas de interpretação de código ou falta de consistência na estrutura.

7.4.2 Performance da ferramenta

O PMT mostrou robustez para suportar grandes cargas geradas numa Rede de Ambiente. A Visão de Árvore deu um bom suporte a todas as entidades e políticas presentes na rede.

Contudo, uma vez que a abordagem de recuperação da informação das Redes de Ambiente é atômica, qualquer tarefa executada em sua estrutura demanda muito tempo, pois

todos os nós da rede X-Peer envolvidos na Rede em questão são acionados. Uma melhora na performance neste aspecto é um trabalho a ser desenvolvido na ferramenta.

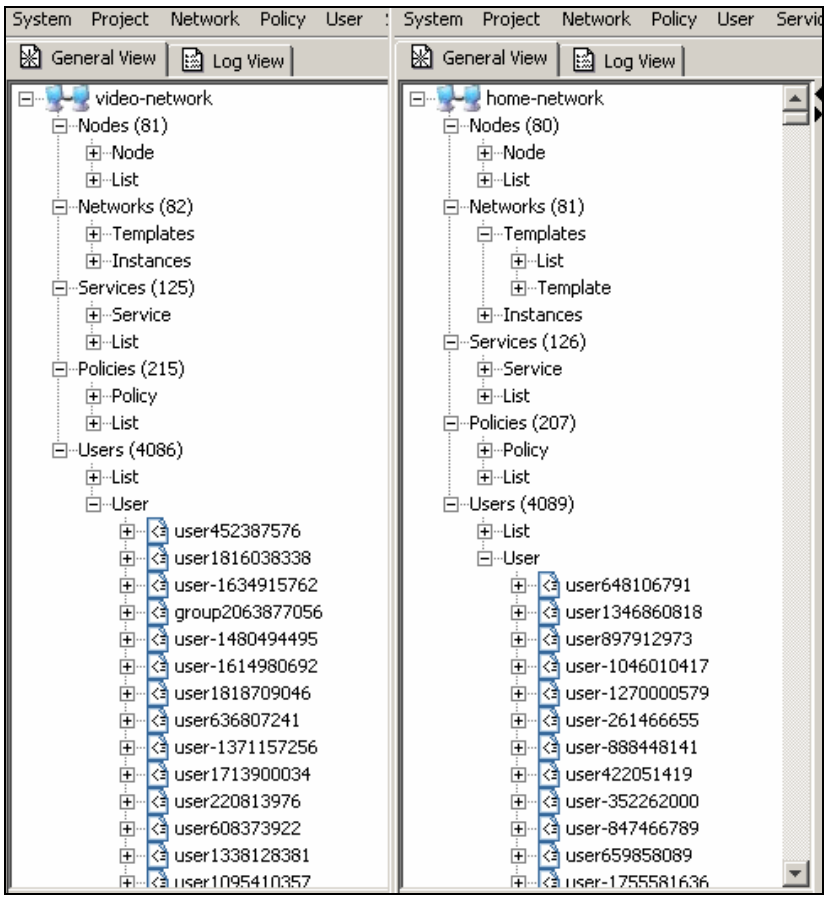

Ilustração 26: Duas Redes diferentes abertas como projeto no PMT com grande carga de entidades (entre parênteses).

8 Monitoramento de Redes de Ambiente

Gerenciar consiste em tomar decisões baseadas em resultados obtidos a fim de melhorar o desempenho das atividades executadas. Uma vez que é necessário verificar valores para avaliar resultados, uma ferramenta de monitoramento de políticas para Redes de Ambiente deve possuir a capacidade de monitorar uma Rede e a execução das políticas presentes nesta.

Redes de Ambiente são auto-gerenciáveis, contudo esta nomenclatura se dá em referência a um nível mais baixo de gerenciamento, isto é, uso de recursos computacionais, necessidade de composição ou não, configuração de nós da Rede, etc. Entretanto, gerenciamento de comportamento das entidades sob uma óptica mais abrangente envolve não apenas as permissões a nível de tecnologia, mas também macro-modelos de negócios, as regras de funcionamento das políticas. Visto que as Redes tem capacidade de tomar decisões próprias a nível de ajustes e configurações, apenas é possível gerenciar as regras de negócio, ou se as políticas estão sendo executadas de acordo com o esperado. O acompanhamento das Redes e políticas se torna um meio importante de verificação de aplicabilidade das regras definidas (em linguagem natural pelos executivos da empresa responsável pela Rede), e uma importante ferramenta de verificação e correção de erros.

8.1 Métodos de monitoramento

A tentativa mais simples de verificar o funcionamento e aplicabilidade das políticas é analisar um histórico de movimentação da Rede e conferir se as políticas e regras sendo aplicadas a cada cenário correspondem ao que era esperado. Na fase de experimentação que o projeto PBMAN se encontrava a única prioridade relacionada a gerenciamento era a verificação de conformidade das políticas, a solução de verificação de histórico foi a única abordagem de monitoramento implementada. Mais adiante, dado o sucesso da fase inicial, surgiram mais alternativas e demandas de monitoramento para ajudar na administração de Redes de Ambiente e suas políticas.

Os PNodes (ou PDPs) foram implementados de forma que adicionem na árvore informações de decisão e execução de políticas. Esta solução foi tomada para que qualquer PMT com acesso ao nó pudesse ter ciência do que foi feito pelo mesmo até o momento, ou seja, para que o histórico do ponto não ficasse restrito a uma máquina, mas a todo administrador com acesso à informação. Também visando simplicidade e esperando atingir o princípio da unicidade da informação, não foi criada uma nova estrutura para armazenar os *log*s, foi usada a única estrutura existente para tal dentro do X-Peer.

O PMT filtra as informações que recuperam da Árvore de dados de uma Rede de forma que o histórico não seja desnecessariamente exibido em forma de hierarquia em árvore (4.2.3), mas em forma de lista de texto (4.2.4, Ilustração 23: Parte da visão do histórico (*Log View*) com destaque para a localização de texto.). Através de um recurso de localização de texto (comum em editores) o administrador pode localizar os trechos do histórico que lhe convém e verificar a exatidão de sua execução.

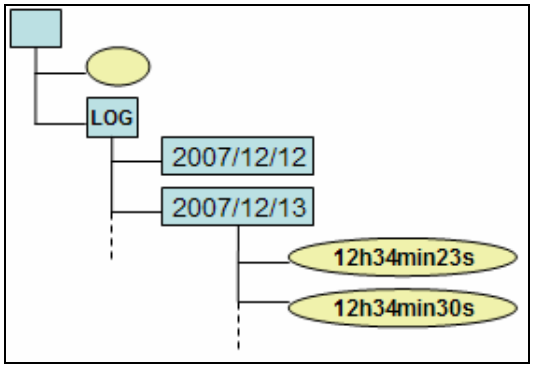

Ilustração 27: Forma como o histórico é armazenado na Árvore.

O histórico do PMT é orientado por uma linha do tempo onde cada entrada é devidamente separada em ramos diferentes da árvore de dados para uma posterior recuperação facilitada pelo editor. Cada entrada do histórico recebe uma descrição textual apropriada para o acontecimento documentado, de forma que o PMT não precisa dedicar processamento à sua interpretação. Para cada atividade executada pelo PNode o gerador de histórico captura a data do sistema em milisegundos. Após as devidas conversões, o gerador de *log*s encontra um ramo apropriado para a data (ano, mês e dia) do acontecimento do evento, ou cria um ramo caso não exista, e insere um novo atributo indexado pela hora do acontecimento (horas, minutos, segundos e milisegundos). Caso hajam dois eventos acontecidos no mesmo instante, ambos recebem o mesmo índice, uma vez que não ocorrerá inconsistência neste nível de informação.

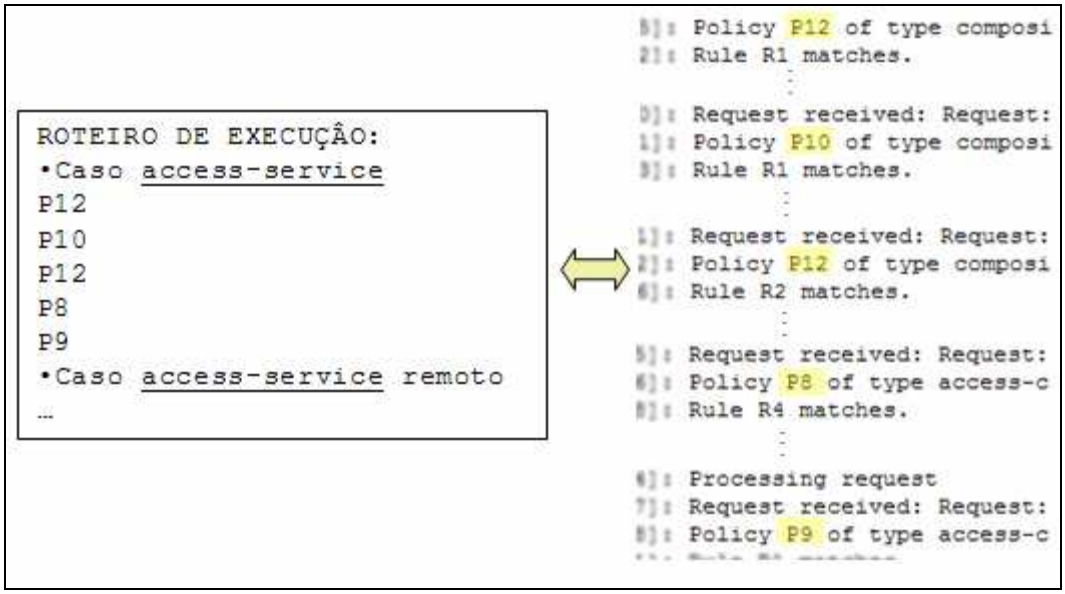

Ilustração 28: Verificação de histórico realizada pelo projetista da rede.

8.2 Abordagens futuras

É visto que a metodologia usada para monitoramento de funcionamento adequado das Redes é bastante simplória, e que exige grandes atualizações para realizar bem seu papel de ajuda aos administradores e projetistas das Redes de Ambiente. Visto que ocorreram

progressos na forma como as entidades da Rede interagem, melhoras precisam ser feitas na maneira como se monitoram as mesmas. Esta seção aborda algumas destas maneiras.

A verificação de histórico para cenários simples como os de teste é humanamente possível, porém, uma vez que cenários envolvendo cada vez mais dispositivos e regras começam a surgir, o PMT precisa automatizar suas verificações de conformidade nas políticas. Uma abordagem automatizada para verificação de integridade e exatidão na execução das políticas é o uso de modelos de verificação que possam ser validados pela própria ferramenta. Apenas para fins de teste seriam definidos *scripts* de execução em uma linguagem própria e o editor verificaria a conformidade do histórico a este roteiro depois da execução. Este modelo é usado com sucesso em *frameworks* automatizados de teste, como o JUnit [20].

A definição de políticas através de interfaces gráficas avançadas evitaria a necessidade deste tipo de observação da rede, uma vez que apenas as políticas necessárias, consistentes e não-conflitantes seriam geradas pela ferramenta e sua validação diante de cenários de teste seria desnecessária. Sendo assim, uma abordagem futura para o monitoramento das políticas seria não monitorá-las neste aspecto, e sim garantir que a ferramenta de criação dê suporte para criar políticas sempre corretas. Esta abordagem, entretanto, seria útil apenas para mostrar conformidade das regras de negócio com as políticas. Fatores externos poderiam fazer políticas indevidas serem executadas durante um caso de uso, por este motivo, um monitoramento paralelo tem que ser feito.

Independente da abordagem utilizada é primordial o desenvolvimento de um módulo que verifique a integridade das políticas, avaliando sua única representação (não-ambigüidade) e verificando possíveis conflitos. Este módulo aparenta ser uma parte importante de uma ferramenta avançada para edição de políticas. Idealmente o módulo deve executar as políticas para alguns cenários automaticamente gerados e checar se seus comportamentos conflitam ou se são idênticos. A construção gráfica das políticas vai evitar que tais problemas ocorram, mas visto que vários administradores podem interferir numa mesma Rede de Ambiente este tipo de verificação é sempre necessário.

Um outro aspecto do monitoramento é a possibilidade de se verificar a carga de usuários e serviços nos nós da rede. Esta capacidade é útil para que as regras de negócio definidas pelas políticas sejam reavaliadas e alteradas a ponto de evitar congestionamentos, quebra de segurança e falta de qualidade mínima nos serviços prestados. Um recurso que permita verificar valores presentes na Árvore que representa a Rede está sendo estudado para implementações futuras do PMT. A abordagem em pesquisa consiste do uso de gráfico temporais atualizados constantemente. O gráfico seria uma curva representando o valor de um atributo (folha da Árvore) ou conjunto de atributos (ramos) de uma entidade em função do tempo. O modelo idealizado permitirá aos administradores verificar picos de acesso a nós da Rede para adaptar recursos de computadores e políticas que suportem os acessos através da simples observação do gráfico em períodos regulares de experimentação. Outra facilidade da ferramenta será a notificação dos administradores a respeito de valores atingindo picos ou máquinas sobrecarregadas.

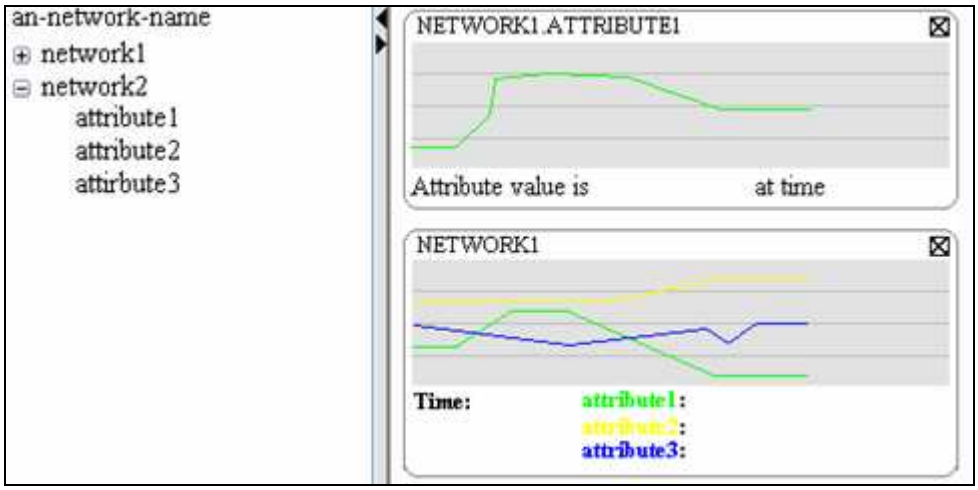

Ilustração 29: Abordagem para monitoramento de atributos da Rede por um administrador.

Já se sabe que as Redes de Ambiente precisam ser auto-configuráveis a nível de tecnologia, esta versão de monitoramento do PMT, que seria executada em um servidor, poderia enviar comandos de reconfiguração de recursos aos PNodes visando diminuir sua carga ou aumentar sua performance. Talvez um novo nível de políticas de controle tenha que ser definido para controlar a autonomia dos nós da Rede.

8.3 Cenário ilustrativo

Na fase de testes, quando foi necessário verificar se as políticas cumpriam com o esperado e se as mesmas eram executadas em ordem, foi necessário criar cenários de validação, cujos casos de uso incluíam ambientes críticos. O foco do projeto PBMAN para usar Redes de Ambiente na fase passada foi um serviço de fornecimento de vídeo e acesso à Internet.

O serviço de vídeo permite que usuários pertencentes à rede de Vídeo ou de outras redes, porém pertencentes ao grupo de acesso ao serviço de vídeo possam visualizar clipes através da internet. O serviço de acesso permite que usuários inscritos em grupos de acesso sem-fio à internet tenham este acesso, podendo inclusive visualizar os vídeos da Rede de Vídeo.

Usuários, Grupos e Serviços adequados foram criados para tal. As políticas foram definidas em três níveis: acesso geral, onde uma classe de entidades é envolvida; acesso por grupos, onde grupos de usuários ou usuários inscritos em determinados serviços são atingidos, e políticas de acesso específico, cujas ações foram desenhadas para uma entidade específica. A nomenclatura das políticas foi dada por sua ordem de criação.

Um exemplo de roteiro de caso de uso pode ser visto como:

Serviço de Acesso Remoto:

1. Verificar que a Árvore da Rede de Acesso não possui um usuário Alice
2. Verificar que o usuário Alice está na árvore da Rede Local e pertence ao grupo WiFi, também da Rede Local
3. Verificar as configurações dos Pontos de Acesso
    a. Verificar que não há configuração para usuários acessarem a rede sem-fio
    b. Verificar que não há usuários usando a rede sem-fio (Rede de Acesso)
4. Checar no histórico se a política de composição de um usuário a uma rede é executada (P12)
5. Checar no histórico se a política de composição de Redes envolvidas (Local e de Acesso) é executada (P10)
6. Checar se a política de composição de um usuário à rede composta é executada (P12)
7. Acessar o serviço de Rede sem-fio através do usuário Alice
8. Checar no histórico se a política de controle de acesso para Alice é executada (P8)

A verificação de execução das políticas em ordem acontece visualmente. Eis a saída do histórico durante a experimentação deste cenário.

```
...24:25.306]: Processing request
...24:25.384]: Request received: Request:type=composition;resource=access-service;subject=a...
...24:25.525]: Policy P12 of type composition is applicable
...24:25.642]: Rule R1 matches.
...24:25.661]: Executing processing: request-composition - Requesting agent startup composi...
...24:25.666]: Processing request
...24:25.670]: Request received: Request:type=composition;resource=access-service;subject=a...
...24:25.701]: Policy P10 of type composition is applicable
...24:25.713]: Rule R1 matches.
...24:25.723]: Executing processing: perform-composition - Performing agent startup composi...
...24:25.798]: New instance created: agenthome
...24:25.802]: Response sent: Permit
...24:25.816]: Executing processing: perform-composition - Performing agent node compositio...
...24:25.826]: Response sent: Permit
...24:35.346]: Processing request
...24:35.361]: Request received: Request:type=composition;resource=access-service;subject=f...
...24:35.482]: Policy P12 of type composition is applicable
...24:35.566]: Rule R2 matches.
...24:35.578]: Executing processing: perform-composition - Performing agent node compositio...
...24:35.589]: Response sent: Permit
...41:04.113]: Processing request
...41:04.125]: Request received: Request:type=access-control;resource=access-service;subjec...
...41:04.186]: Policy P8 of type access-control is applicable
...41:04.208]: Rule R4 matches.
...41:04.211]: Executing processing: add-subject
...41:04.214]: Executing processing: get-user-attribute
...41:04.221]: Executing processing: request-repeat
```

Ilustração 30: Histórico gerado pelo PMT durante a execução do cenário acima.

9 Conclusões

Neste trabalho de graduação foram apresentados conceitos relacionados a uma nova visão na área de redes, denominada Redes de Ambiente. O conceito mais importante das Redes de Ambiente é o de composição, pois permite a cooperação, disponibilização de serviços e compartilhamento de recursos entre redes de domínios administrativos e tecnológicos diferentes. Este conceito é essencial para tornar as Redes autônomas o suficiente para lidar com o ambiente de computação e conectividade ubíquas, no qual as empresas estão se esforçando para explorar.

É visto que as máquinas não podem possuir autonomia total, de forma que é necessário definir regras através das quais os dispositivos devem interagir. Este documento também apresentou uma abordagem inovadora utilizada por várias corporações em todo o mundo: o gerenciamento baseado em políticas. Além disso, foram apresentados os conceitos de gerenciamento que foram e continuam sendo estudados para tratar os problemas das Redes de Ambiente, o que inclui o armazenamento remoto de informação via P2P, e o uso de XML.

Após a demonstração das definições introdutórias foi apresentado um arcabouço de conceitos úteis para o desenvolvimento de uma ferramenta que permita a criação, edição e acompanhamento de entidades presentes no novo ambiente de redes descrito e foi introduzida a ferramenta-tema deste trabalho, o PMT. Por ser o alvo do documento, os vários módulos da arquitetura do editor foram detalhados, de forma a detalhar o uso dos conceitos anteriormente mencionados.

Devido à natureza recente das pesquisas propostas apenas resultados sobre casos de teste foram apresentados. Toda referência de uso do PMT se deu após pesquisa de casos críticos e verificação de utilidade da ferramenta.

A implementação do *Policy Management Tool* teve como principal objetivo acelerar o estudo de Redes de Ambiente em contextos reais e mais plausíveis para verificação e desenvolvimento.

9.1 Contribuições do trabalho

Este trabalho de graduação teve como principal objetivo realizar estudos sobre aspectos essenciais sobre Redes de Ambiente e o auto-gerenciamento das mesmas para poder relacionar estes estudos ao uso de uma ferramenta que facilitasse sua criação e acompanhamento.

Estudos relacionados a interfaces gráficas para computadores de mesa e áreas correlatas foram desenvolvidos, bem como aprofundamento nos conceitos de projetos na condição de agrupamentos de arquivos de definição.

Para unir todos os conceitos necessários, foram imprescindíveis pesquisas relacionadas à interpretação e geração de código para entidades e cenários complexos, cuja solução encontrada se apresentou uma boa nova abordagem para manipulação de XML. Além de também ter sido idealizada uma nova proposta de armazenamento de projetos, o que acarretou pesquisas aprofundadas em P2P.

9.2 Trabalhos futuros

É possível notar que a ferramenta, apesar de possuir recursos avançados, ainda se encontra em fase de aprimoramento e alguns estudos para novas capacidades ainda precisam ser desenvolvidos. Algumas características descritas na proposta não foram aprofundadas o suficiente, de forma que precisam de mais pesquisa relacionada. Entre alguns trabalhos futuros, estão:

1. Ferramentas mais avançadas de monitoramento, que precisam ser estudadas para permitir mais integração do administrador com os recursos administrados;
2. Edição gráfica para cenários mais complexos, uma vez que atualmente o PMT dá suporte a cenários simples e recorrentes. A edição através de gráficos corresponde ao mais alto nível de definição de regras de negócios. Também é necessário um estudo de eficiência e usabilidade de interfaces de edição gráfica para os cenários futuros;
3. Módulo para verificar consistência e analisar conflitos entre políticas, visto que os ambientes e cenários se tornam cada vez mais complexos e maiores;
4. Recursos que permitam à ferramenta ser mais inteligente para tomar decisões importantes de manutenção e gerenciamento básico. Outro nível de Políticas (para controle de autonomia do PMT) precisa ser estudado nesse sentido;
5. Uma noção mais ampla de projeto, isto é, módulos que permitam ao PMT "entender" mais tipos de projeto, o que vai colaborar para direcionar o PMT no sentido de se tornar uma ferramenta completamente genérica para ser usada em qualquer rede de ambiente. A ferramenta atual está ligada a cenários existentes até o momento, é preciso deixá-la maleável para aceitar novos ambientes e novas entidades. Muitos estudos precisam ser realizados neste sentido para prover um editor ideal a todos os casos possíveis;
6. Uma nova abordagem para recuperação de informação da árvore de dados, uma vez que o modelo atual demanda muito tempo para recuperar de forma atômica todos os dados da árvore. O conceito de requisições *ad-hoc* da informação parece ser um bom ponto de partida.

Referências

1. Ambient Networks Project, http://www.ambient-networks.org
2. Oasis XACML 2.0 Specification Document, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
3. Wireless World Initiative – WWI, http://www.wireless-world-initiative.org
4. ARMSTRONG M. W. "An Introduction To XACML". GIAC Security Essentials Practical Assignment, SANS Institute. Junho de 2003.
5. MERRELLS J. "XACML: XML Access Control".
6. NIEBERT N.; SCHIEDER A.; ABRAMOWICZ H.; MALMGREN G.; SACHS J.; HORN U. "Ambient Networks: An Architecture For Communication Networks Beyond 3G". Ericsson Research. Abril de 2004.
7. VERMA D. C. "Simplifying Network Administration Using Policy-Based Management". IBM Thomas J Watson Research Center. Abril de 2002.
8. KAMIENSKI C.; FIDALGO J.; SADOK D.; LIMA J.; PEREIRA L. "On the Use Of Policies For Ambient Networks Management". Universidade Federal de Pernambuco.
9. Projeto PBMAN, Grupo de Pesquisa em Redes e Telecomunicações, http://www.gprt.ufpe.br/projetos/pbman .
10. KAMIENSKI, C., FIDALGO, J., et. al. "A Policy-Based Management Framework for Ambient Networks – PBMAN Framework Specification", Deliverable D05, Grupo de Pesquisa em Redes e Telecomunicações, Março de 2005.
11. LIMA, J. "Gerenciamento de Redes de Ambiente". Trabalho de Graduação – Centro de Informática – UFPE, orientado pela professora doutora Judith Kelner. Março de 2005.
12. VERMA, D. C., "Simplifying Network Administration using Policy-Based Management", IEEE Network, March/April 2002.
13. KAMIENSKI, C., DANTAS, R., AZEVEDO, E. "A Policy-Based Management Framework for Ambient Networks – A Policy Management Tool for PBMAN", Deliverable D09, Grupo de Pesquisa em Redes e Telecomunicações, Novembro de 2007.
14. STRASSNER, J.C. Policy-Based Network Management – Solutions for the next generation. Colorado, EUA, 2004. 1ª Edição. 516 p.
15. XML – Wikipedia. http://pt.wikipedia.org/wiki/XML, visitado em 16/12/2007.
16. Linguagem XML. http://www.infowester.com/lingxml.php, visitado em 16/12/2007.
17. KAMIENSKI, C, FIDALGO, J. et al. "XACML-Based Composition Policies for Ambient Networks". Grupo de Pesquisa em Redes e Telecomunicações, Março de 2007.
18. GHELLI, G. et al. "Scalable query dissemination in XPeer ". Departamento de Informática, Universidade de Pisa, Itália. Disponível em http://www.di.unipi.it/~manghi/XPeerWeb/homexpeer.htm, acesso em 28/12/2007.

19. ROCHA, J. “XPeer : Policy Based Management Group”. Grupo de Pesquisa em Redes e Telecomunicações, Setembro de 2005.
20. Junit.org. http://www.junit.org, visitado em 6/1/2008.
21. DANTAS, R. et al. “XPeer : Avaliações de desempenho”.Centro de Informática – UFPE. Julho de 2006.