SABRE - Sistema Aberto de Registro de Estações

**Caciano Machado, Daniel Soares, Francisco Fialho,
Leandro Rey, Rafael Silveira, Rui Ribeiro**

Universidade Federal do Rio Grande do Sul
Centro de Processamento de Dados
Rua Ramiro Barcelos, 2574 – Portão K – Porto Alegre – RS

{caciano,daniel,francisco,leandro,rafaelsm,rui_ribeiro}@cpd.ufrgs.br

O Sistema de Registro de Estações da UFRGS foi desenvolvido com o objetivo de facilitar a gerência das estações de trabalho na universidade. No presente trabalho, apresentamos as experiências e resultados parciais da implementação de um sistema aberto de registro de estações (SABRE), utilizável por qualquer instituição que busque uma solução automatizada para o gerenciamento do seu bloco de endereços IP.

1. Introdução

O controle da alocação de cada bloco IP utilizado por estações de trabalho, servidores e equipamentos de rede é indispensável, dentro das universidades, para organizar e documentar a segmentação da rede. Além disso, auxilia no tratamento de incidentes de segurança, conflitos de IP e identificação dos usuários dos dispositivos conectados à rede. O Sistema de Registro de Estações da UFRGS [3][4][5] permite associar a cada um destes dispositivos um usuário responsável e um número IP sem a necessidade de configurações manuais, mediadas ou efetuadas por um gerente de rede. Este objetivo é alcançado através da delegação deste papel para os próprios usuários. Desonerar os gerentes de rede desse trabalho também permite que eles se preocupem com outras tarefas e ameniza um problema bastante comum que é a falta de gerentes em determinadas unidades.

Algumas limitações da versão atual do sistema e o interesse demonstrado por outras instituições motivaram o projeto de uma versão aberta. A seguir, será explicada brevemente a situação do Sistema de Registro de Estações atualmente implantado na UFRGS. Depois abordaremos as motivações para o desenvolvimento do novo sistema aberto, as suas principais funcionalidades e as novas funcionalidades implementadas.

2. A versão atual Sistema de Registro de Estações da UFRGS

O Sistema de Registro de Estações apresenta características de sistemas de NAC (*Network Access Control*) [1][2] e IPAM (*IP Address Management*) [7]. Atualmente, a UFRGS já possui 8768 IPs registrados no sistema, de um total de 13030 IPs em funcionamento na rede da universidade. A implantação do sistema em 70% da rede da UFRGS proporcionou o amadurecimento do mesmo e de várias extensões que auxiliam desde o tratamento de incidentes de segurança até o gerenciamento de tickets de acesso à rede sem fio. Apesar do sistema estar sendo continuamente adotado nas diversas unidades da UFRGS existem algumas limitações que motivaram a criação de uma nova versão do sistema.

3. SABRE - Sistema Aberto de Registro de Estações

Algumas decisões de projeto durante o desenvolvimento do Sistema de Registro de Estações atualmente implantado na UFRGS impossibilitam sua utilização de forma simples em outras

instituições. Componentes como a gerência de listas de discussão, o sistema de patrimônio e a autenticação de usuários foram implementados de acordo com os sistemas da universidade, sem preocupação com a possível implantação do sistema em outros ambientes.

Estes fatos, somados ao interesse de outras instituições no sistema, levaram a UFRGS a implementar uma versão aberta do mesmo. Nesta versão, funcionalidades como a autenticação de usuários foram substituídas por alternativas padronizadas, como LDAP com o esquema *brEduPerson* [6]. Além disso, foram mantidas apenas funcionalidades consideradas fundamentais para o sistema.

Outra preocupação no projeto da versão aberta é a de viabilizar a implementação de suporte ao registro de endereços IPv6. A versão atual do sistema não oferece esse suporte e seu desenvolvimento não foi planejado para prever esta facilidade, tornando a implementação de IPv6 uma tarefa muito difícil. Em contrapartida, na versão aberta, o suporte a IPv6 está sendo considerado desde o início do projeto para futura implementação.

A seguir, mostraremos as características básicas, novidades e dificuldades do sistema aberto que de agora em diante chamaremos de SABRE. Todas as funcionalidades da primeira versão do SABRE já estão implementadas no Sistema de Registro de Estações da UFRGS atual, e foram atualizadas para fazer parte do sistema aberto. Além delas, já existem projetos para adicionar novas funcionalidades ao SABRE. O novo sistema aproveita o crescimento da equipe tanto no entendimento do problema quanto no domínio das tecnologias envolvidas na solução. O código do sistema original foi totalmente reescrito, já que modificá-lo seria mais trabalhoso. A seguir, mostraremos as principais funcionalidades oferecidas e as novidades implementadas.

3.1. Registro de Estações

A interface de registro é possivelmente a mais importante do sistema. Através dessa tela os usuários comuns conseguem efetuar o registro de suas próprias máquinas. No SABRE esses usuários são professores e funcionários da universidade, que ao conectar seus computadores na rede pela primeira vez conseguem informar dados básicos do mesmo, sem a necessidade da intervenção de um técnico.

O registro ficou mais simples e existe apenas uma tela no lugar das cinco anteriores, conforme mostra a Figura 1. Qualquer usuário registrado no sistema pode efetuar registros de novas estações. Alguns dados ainda precisam ser informados pelo usuário, começando pelos dados do dispositivo: nome, um texto descritivo da localização do computador, um comentário livre e o tipo de uso que o dispositivo terá na instituição (Acadêmico, Administrativo, Infraestrutura). Um outro usuário pode ser cadastrado como usuário que utilizará o dispositivo, mas por padrão, o usuário que efetuou o registro é considerado o usuário do dispositivo. Por fim, um dos setores cadastrados na subrede deve ser escolhido, sendo esse setor o bloco onde o novo dispositivo ficará registrado.

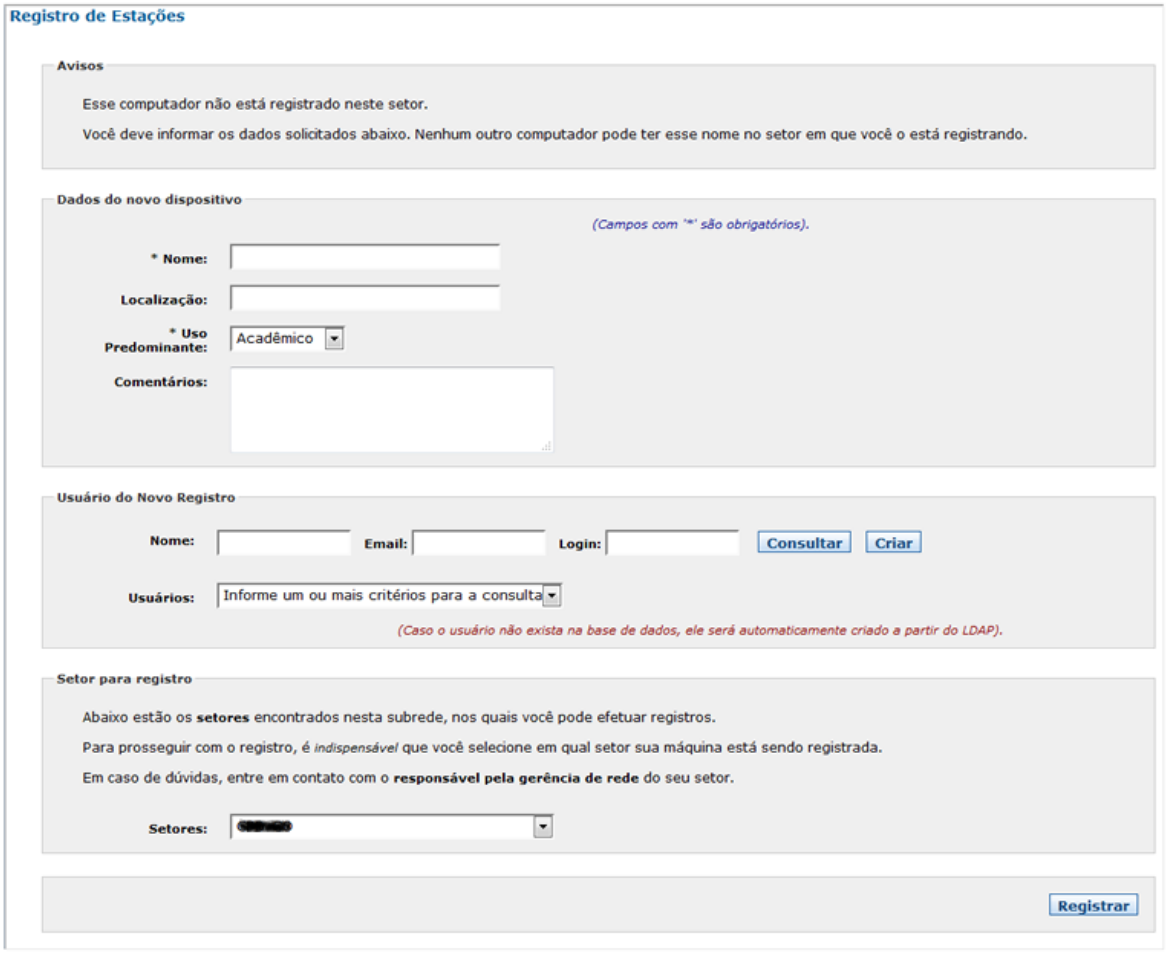

Figura 1: Tela de registro de máquinas do sistema aberto

Como o sistema foi desenvolvido pensando num futuro suporte a IPv6, foi utilizada versão 4 do ISC DHCP. Porém, durante os primeiros testes foi encontrado um bug no OMAPI, utilizado para recuperar o endereço MAC de máquinas não registradas no sistema, que impossibilitou o uso de ambos. A solução foi manter a escolha da versão 4 do DHCP e desenvolver um protocolo alternativo que faz a comunicação entre a página de registro e os servidores de DHCP, em substituição ao OMAPI, para captura do MAC.

3.2. DHCP

O DHCP é o protocolo de base do sistema. A configuração automática dos computadores é feita por um conjunto de servidores de DHCP trabalhando com tolerância a falhas e redundância. Isso é feito utilizando a configuração de *failover*, com um servidor centralizado primário e servidores local secundários.

A configuração que o projeto propõe, e que já está implantada atualmente na versão não aberta do sistema, é a de um servidor primário no Datacenter da instituição e um conjunto de servidores secundários, cada qual em um campus remoto. Dessa forma, o servidor primário atenderá as requisições enquanto não houver problema e, se houver segmentação da rede de algum campus ou falha do servidor primário, o servidor secundário correspondente atenderá as requisições de DHCP dos clientes locais.

3.3. Gerenciamento de DNS

Uma das últimas funcionalidades adicionadas ao Sistema de Registro de Estações da UFRGS, foi escolhida como uma das primeiras disponibilizadas na primeira versão do SABRE. Ainda em fase final de testes, o gerenciamento de arquivos de DNS permite adicionar blocos de registros do sistema para dentro de arquivos de zona previamente criados, sendo toda a configuração de registros transparente para o gerente.

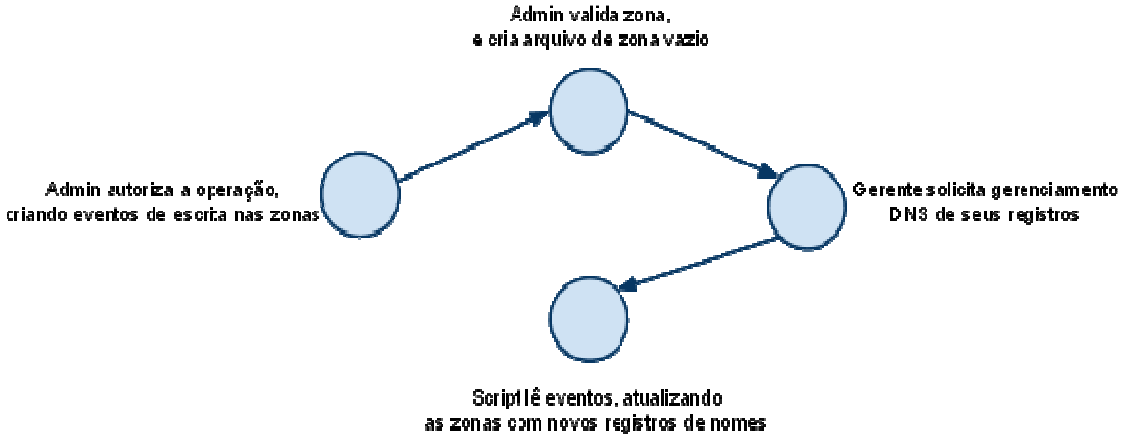

Figura 2: Fluxo base de mudanças de DNS

Todo o tratamento de conflitos de nomes e de validação dos mesmos são feitos pelo sistema, de forma que nomes são únicos no mesmo nível de enlace. Dispositivos que possuem serviços disponíveis para a internet (e não somente na rede interna), tem seus registros adicionados automaticamente ao arquivo de *visão externa*, que permite a resolução de seus nomes fora da rede gerenciada.

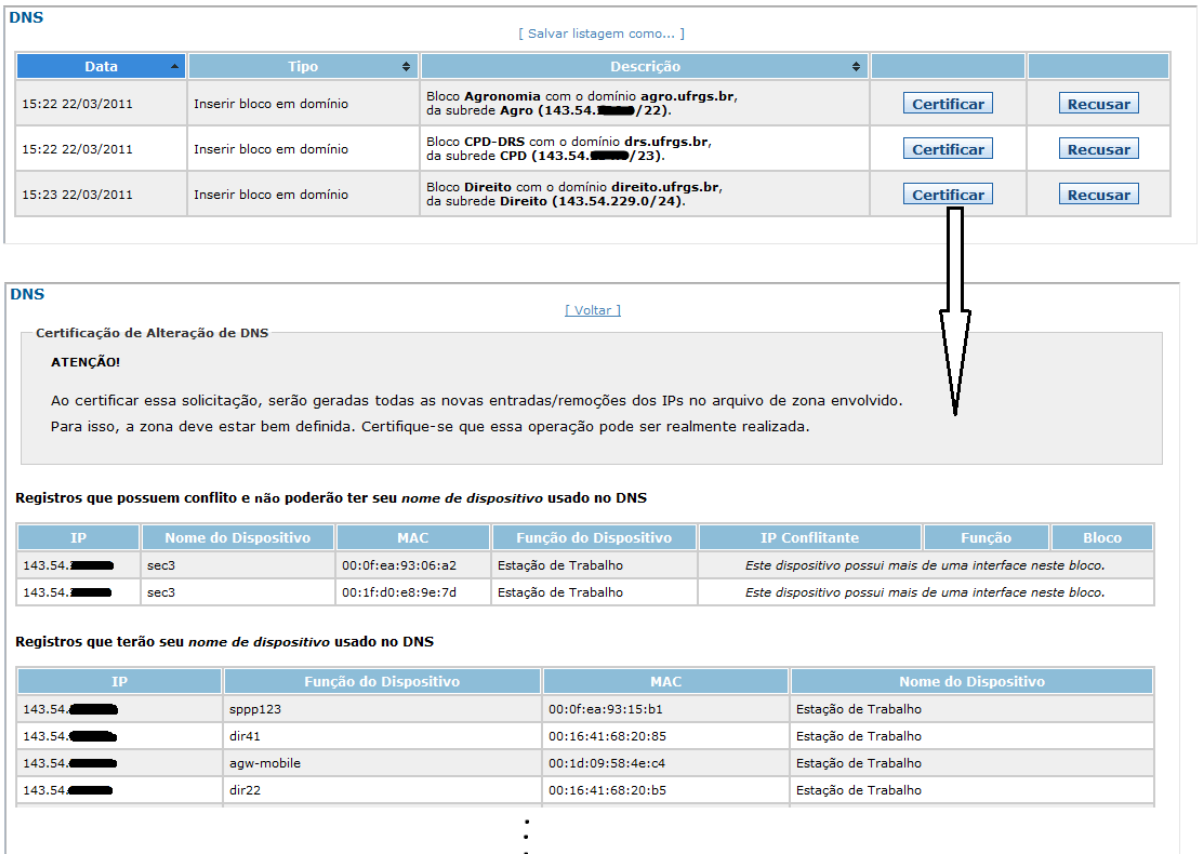

Figura 3: Telas de pendências e de certificação de mudanças nas configurações de DNS

O processo de solicitação é simples, mas necessita da autorização e da atuação do administrador, já que ainda é necessário criar os arquivos de zona vazios. Autorizando a operação (que pode ser de solicitação, troca de domínio, ou remoção), são gerados todos os eventos necessários para cada dispositivo. De minuto em minuto um script agendado coleta estes eventos para escrever/remover os registros necessários dos arquivos de zona.

3.4. Perfis de Usuário

Organizar as permissões em grupos de funcionalidades - chamados de *perfis* como pode ser visto na Figura 4 - se mostrou muito eficiente para atribuir permissões a usuários semelhantes. Dessa forma, gerentes não precisam ter cada uma de suas permissões especificadas manualmente: basta atribuir a eles um perfil com as permissões de gerente. Essa organização de perfis e funcionalidades utilizada no Sistema de Registro de Estações da UFRGS foi mantida no sistema aberto, porém muito foi alterado quanto ao gerenciamento de usuários.

O Sistema de Registro de Estações da UFRGS é baseado no número do cartão de identificação da UFRGS, código único que identifica cada pessoa com algum tipo de vínculo com a universidade. Para a versão aberta, implementamos uma solução diferente. O registro de usuários do sistema pode ter duas origens: um LDAP que utilize o esquema *brEduPerson* [6] ou o cadastro manual de usuários locais.

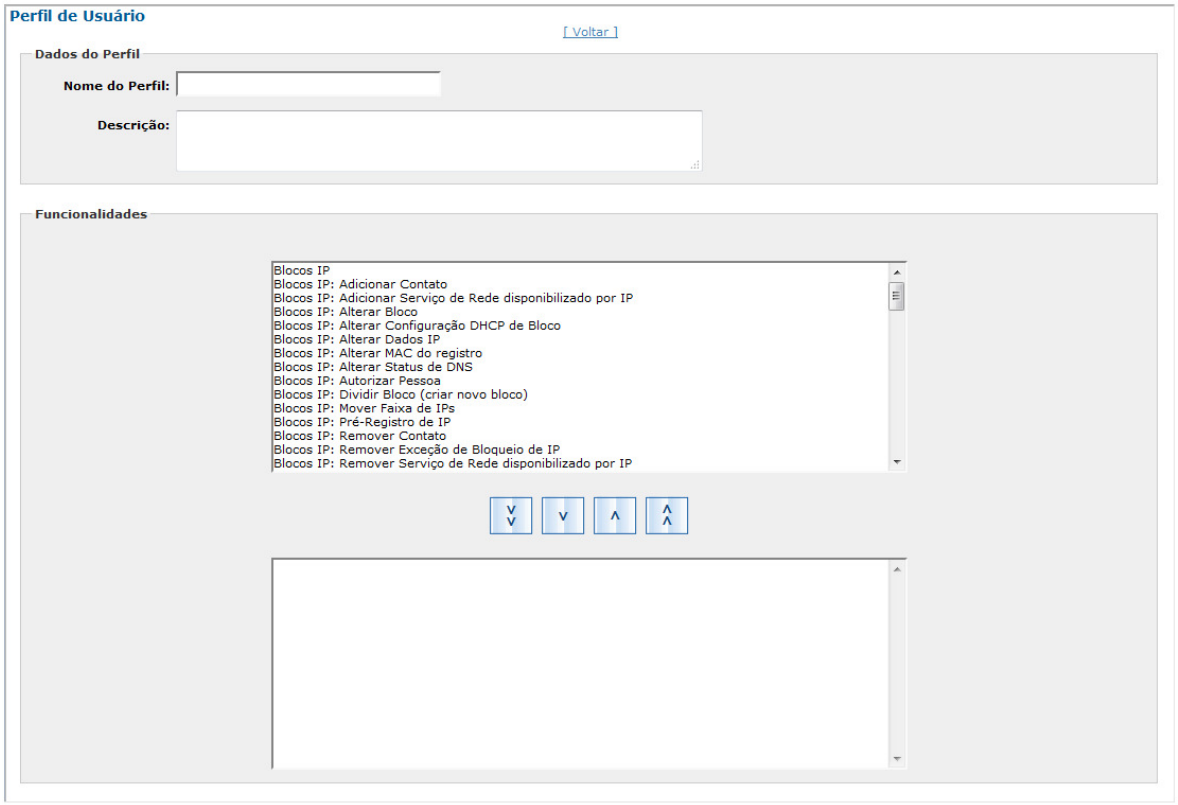

Figura 4: Tela de criação de Perfil de Usuário

O esquema *brEduPerson* para LDAP foi projetado para instituições de educação e possui informações de usuário que são necessárias para o sistema. O *uid* (identificador de usuário) passa a ser o login do usuário para o sistema, e sua senha pode ser validada pela interface de LDAP no PHP. Para usuários locais, todos os dados são informados manualmente, inclusive a senha, que é armazenada de forma encriptada. Para qualquer tipo de usuário, deve ser informada uma data de expiração de conta a partir da qual ele perderá o acesso ao sistema.

3.5. Instalação Automatizada do Sistema

Para automatizar a implantação do sistema nas instituições está em desenvolvimento um script para instalação dos servidores. Esse script prevê a configuração inicial dos servidores Linux, instalação e configuração dos serviços de DHCP, DNS, Apache, carga inicial do banco de dados PostgreSQL e agendamento dos scripts do SABRE.

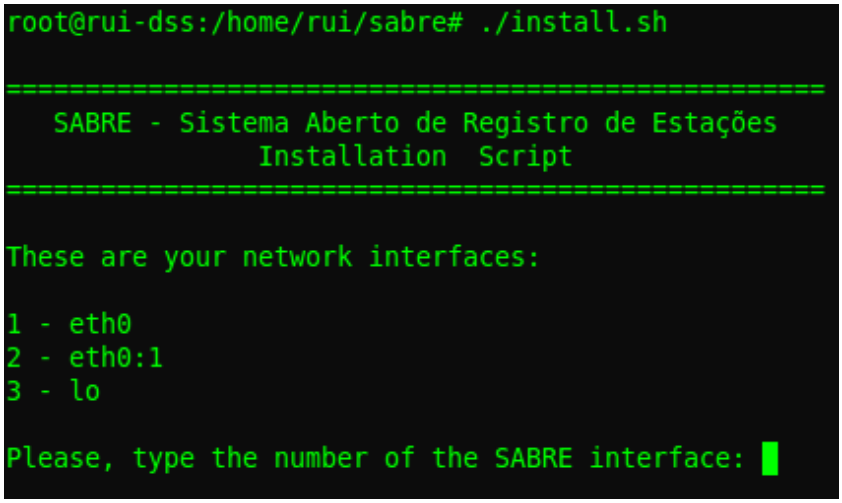

Figura 5: Início da instalação do sistema - escolha da interface de rede do SABRE

A interface de instalação coleta os dados necessários para configurar o estado inicial do SABRE, simplificando a implantação do sistema. Na Figura 5, está ilustrado o início da execução do script de instalação, na etapa na qual o script solicita em qual interface de rede que deverá atender os serviços do SABRE. Entre os dados coletados estão a interface de rede que será utilizada para o serviço, o IP do servidor de DHCP e as senhas de acesso.

3.6 Configuração

O SABRE possui uma interface para configuração dos parâmetros globais do sistema. As configurações dessa interface estão classificadas em Sistema, Rede e DHCP. As configurações de Rede se referem às informações do sistema autônomo (AS) e prefixos IP da instituição. As de Sistema definem parâmetros de estilo e aparência da interface Web. Nas configurações de DHCP, conforme mostra a Figura 6, a interface permite configurar os parâmetros da rede real e também da rede bogus que é utilizada durante o processo de registro das estações.

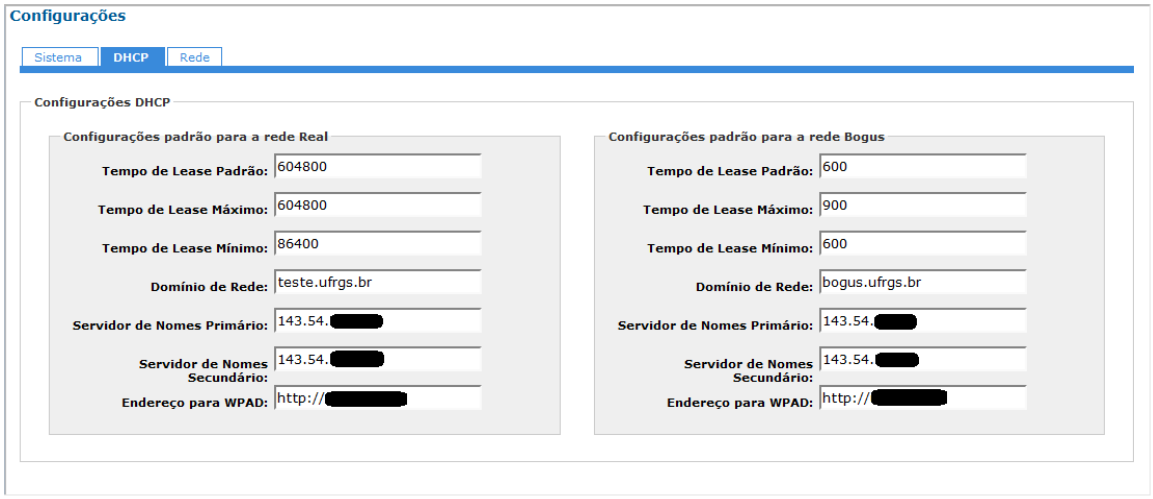

Figura 6: Configuração de opções de DHCP padrão para as redes Real e Bogus

Além dessa interface, cada subrede, bloco e IP também podem ter suas próprias configurações específicas de DHCP, que se sobrepõem às configurações globais. Especificando vários níveis de configurações, as válidas serão as do próprio registro ou as de um nível superior (um IP usa as suas configurações, ou as de seu bloco caso as suas não sejam especificadas) até se chegar nas globais.

3.7. Personalização

Outro ponto que não pode ser deixado de lado no sistema aberto foi a personalização do sistema, algo que não era tratado no Sistema de Registro de Estações da UFRGS. O sistema foi reescrito em inglês. Além disso, a base de dados possui toda uma estrutura modelada para armazenar as mensagens do sistema. Isso permite uma outra mudança: um sistema multilinguagem. Cadastradas todas as mensagens em uma nova língua, basta alterar a língua no próprio sistema, sem necessidade de uma nova instalação.

Os dados de configuração, além de informações para funcionamento do sistema web (formato de datas e grupos de permissões para operações especiais) também estão armazenadas no banco, reduzindo a necessidade de alterar código fonte para determinadas mudanças de comportamento do sistema.

4. Conclusões e Considerações Finais

Atualmente o SABRE está em testes de instalação, implantação e carga de dados, todos executados no CPD/UFRGS. Alguns erros do sistema utilizado atualmente pelos gerentes de rede da UFRGS foram corrigidos na versão aberta, assim como a incompatibilidade com algumas ferramentas.

A meta é fornecer uma versão com as funcionalidades escolhidas do sistema anterior até a metade de 2011. Além disso, o projeto continuará contando com atualizações frequentes para adicionar mais funcionalidades que já estão presentes no Sistema de Registros da UFRGS. Os próximos passos são: atualização dos scripts para coleta de MACs utilizados, tratamento de incidentes de segurança, suporte a redes sem fio e auditoria das operações realizadas no sistema. A primeira versão será implantada em uma unidade piloto da UFRGS. Posteriormente disponibilizaremos o código e desejamos implantar em uma instituição piloto.

5. Referências

[1] RFC 5209 - **Network Endpoint Accessment: Overview and Requirements**

[2] Conover, J. **NAC Vendors Square Off**. Revista Network Computing, Julho de 2006.

[3] Machado, C.; Marquezan, C.; Rey, L.; Soares, D.; Postal, E., Horowitz; E.; Ziulkoski, L. **Sistema de Registro de Estações da UFRGS**. No II Workshop de Tecnologia da Informação das IFES, Gramado, RS - Brasil, Maio de 2008

[4] Machado, C.; Rey, L.; Soares, D.; Ceron, J; Júnior, A. **Implantação do Sistema de Registro de Estações da UFRGS**. No III Workshop de Tecnologia da Informação das IFES, Belém, PA - Brasil, Maio de 2009.

[5] Ceron, J; Rey, L; Boos Jr, Arthur; Machado, C.; Macedo, F; Brighenti, F; Pohlmann, M. (2010). **Sistema de Registro de Estações da UFRGS como Ferramenta de Segurança**. No IV Workshop de Tecnologia da Informação das IFES, Rio de Janeiro, RJ - Brasil, Maio de 2010.

[6] **Esquema brEduPerson - versão 1.0.** Federação Café. Disponível em http://wiki.rnp.br/display/cafewebsite/brEduPerson e acessado em Março de 2011.

[7] Rooney, T. **IP Address Management Principles and Practice.** IEEE Press Series on Network Management. Janeiro de 2011.