Implantação do Sistema de Registro de Estações da UFRGS

Caciano Machado, Daniel Soares, Leandro Rey
João Ceron, Arthur Júnior

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

{caciano,daniel,leandro,ceron,boos}@cpd.ufrgs.br

Resumo. *O Sistema de Registro de Estações da UFRGS foi desenvolvido com o objetivo de facilitar a gerência das estações de trabalho na universidade. Problemas como os conflitos de IP, a crescente utilização de redes sem fio e a falta de administradores de rede em algumas unidades da universidade foram os fatores que motivaram o desenvolvimento desse sistema. No presente trabalho apresentaremos as suas novas funcionalidades e a implantação do sistema na UFRGS.*

1. Introdução

O controle da alocação dos IPs das estações de trabalho, servidores e equipamentos de rede é fundamental para organizar a segmentação da rede presente nas unidades da universidade. Além disso, auxilia no tratamento de incidentes de segurança, conflitos de IP e identificação de usuários dos dispositivos. O Sistema de Registro de Estações permite associar a cada dispositivo um usuário responsável e um IP sem a necessidade de mediação do gerente de rede. Isso é feito delegando a tarefa de registro para os próprios usuários. Desonerar os gerentes de rede desse trabalho permite que eles se preocupem com tarefas de maior prioridade e ameniza um problema bastante comum que é a falta de gerentes em determinadas unidades.

No último Workshop de TI das IFES foram apresentados o sistema de registro [Machado et al. 2008] e o sistema de gerenciamento de redes *wireless* [Tonin et al. 2008] em fase inicial de implantação. Mostraremos, no presente trabalho, a evolução dos sistemas, as novas funcionalidades e a experiência da migração das redes das unidades da UFRGS.

2. Sistema de Registro de Estações

O Sistema de Registro de Estações desenvolvido na UFRGS herda algumas características de sistemas conhecidos como NAC [Conover 2006] (*Network Access/Admission Control*). As implementações de NAC têm como foco permitir o ingresso e permanência apenas de máquinas que estejam em conformidade com especificações mínimas de configuração e segurança estabelecidas pela organização. Após o estudo de ferramentas comerciais e abertas optou-se por desenvolver um novo sistema que se adequasse à realidade da universidade.

A Figura 1 permite uma visão geral do sistema desenvolvido. No lado esquerdo estão os usuários, conectados via rede cabeada e via rede sem fio. No lado direito estão

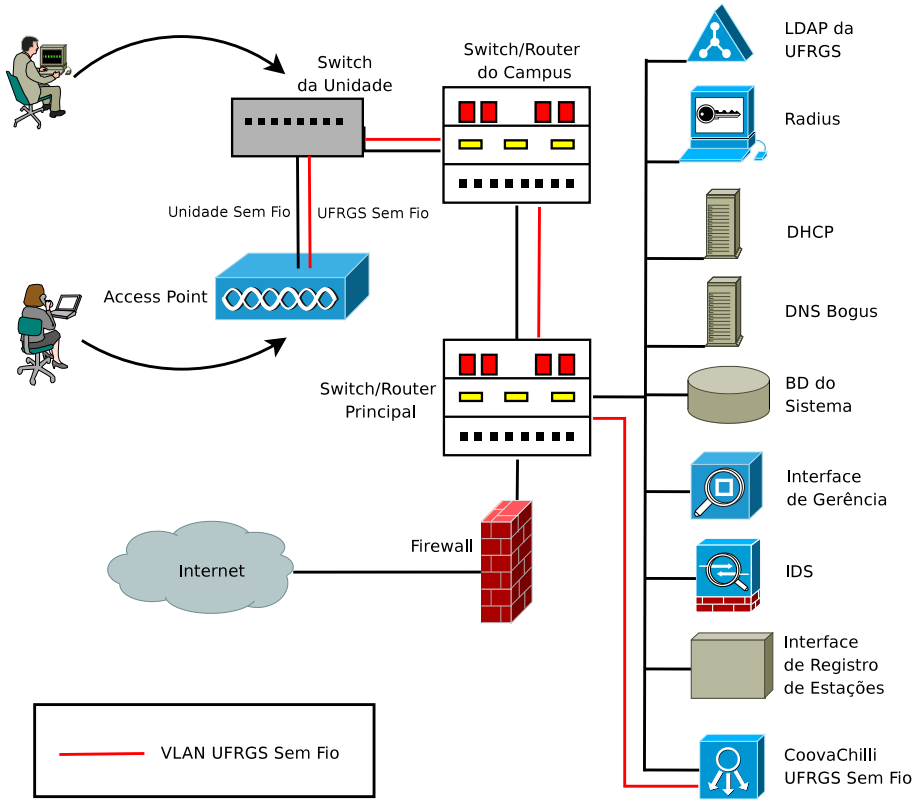

Figura 1. Elementos do Sistema de Registro de Estações

os serviços envolvidos no sistema. A seguir, nessa seção, veremos a Interface de Registro de Estações, Interface de Gerência, DHCP, Expiração de Registros e Detecção de Rogue Users.

2.1. Interface de Registro de Estações

O método normal de registro de estações parte dos próprios usuários. Quando um usuário liga um computador não registrado na rede da sua unidade, esse deve ser configurado para obter endereço IP e de DNS automaticamente via DHCP. O procedimento de registro de estação típico pode ser encontrado em [Machado et al. 2008]

As páginas de registro foram aprimoradas e na nova versão o registro é efetuado em seis passos. A seguir, estão apresentados esses passos juntamente com algumas das telas de maior importância.

1. Instalação dos certificados da UFRGS no navegador (Figura 2).
2. Autenticação do usuário com as credenciais institucionais da UFRGS.
3. Verificação de dispositivo (Figura 3).[1]
4. Nºde patrimônio, hostname, bloco de subrede e usuário da estação (Figura 4). [2]
5. Confirmação dos dados informados.
6. Apresentação do IP registrado e solicitação de reinicialização da estação.

[1]O sistema solicita ao usuário se esse IP é de um dispositivo já registrado no sistema. É permitido que um mesmo dispositivo possua vários IPs registrados, inclusive em subredes diferentes.

[2]É possível cadastrar os órgãos e unidades da universidade que estão associados com cada bloco de subrede para permitir registros apenas de usuários com vínculo nos órgãos.

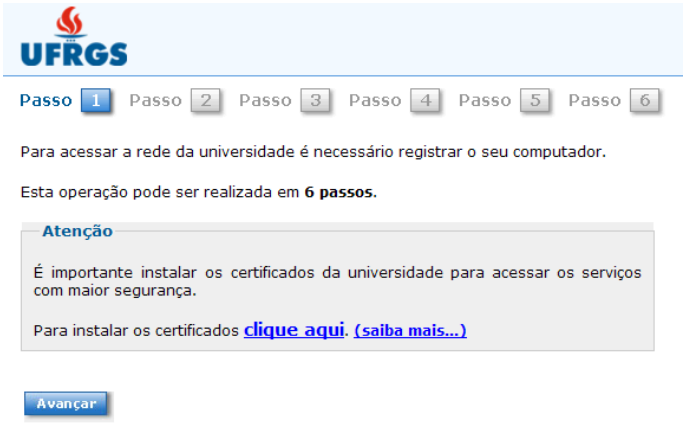

Figura 2. Interface de Registro de Estações. Passo 1.

Figura 3. Interface de Registro de Estações. Passo 3.

Atualmente, somente servidores da UFRGS podem registrar IPs. Esse não é o único meio de registrar IPs. A Interface de Gerência de Estações, apresentada a seguir, também permite fazer o registro, entre várias outras operações.

2.2. Interface de Gerência de Estações

A Interface de Gerência de Estações é um dos principais elementos do sistema. O acesso à interface é feito através do Portal da UFRGS. As funcionalidades implementadas no sistema fornecem aos gerentes de rede, central de atendimento, grupo de segurança e outros operadores um maior controle da rede. A seguir estão listadas algumas das principais funcionalidades implementadas.

- Criação, remoção e alteração de enlaces, subredes, blocos de subrede, registros de IP e dispositivos.
- Configuração de DHCP para subredes, blocos de subrede e IPs específicos.
- Bloqueio de IPs no *firewall* integrado com o tratamento de incidentes d.
- Requisição de abertura de portas no *firewall* para serviços que necessitem de acesso externo à universidade.
- Autorizações e bloqueios de usuários nos SSIDs das bases *wireless*.

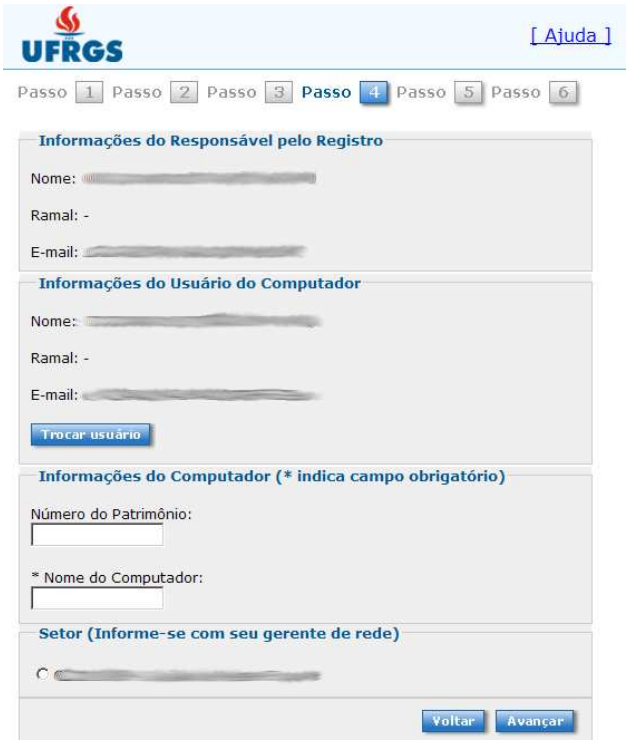

Figura 4. Interface de Registro de Estações. Passo 4.

- Autorizações de usuários de órgãos e unidades da universidade nos SSIDs das bases *wireless*.
- Atualização dos registros de estações dos usuários.
- Transferência de responsabilidade de registro.

O esquema de permissões da interface de gerência é baseado em papéis (Figura 6). Os papéis podem ser criados e atribuídos aos usuários cadastrados no sistema. Cada papel é associado um conjunto de funcionalidades que poderão ser acessadas pelos usuários vinculados. Assim é possível criar papéis para os gerentes de rede, central de atendimento ao usuário, grupo de segurança de rede, etc.

2.3. DHCP

A distribuição da configuração de rede dos IPs registrados e dos IPs temporários da rede bogus é feita através de 4 servidores DHCP. Os servidores estão configurados com *failover* e estão distribuídos geograficamente entre os três campi da universidade (Figura 7).

Essa configuração oferece tolerância a falhas através de redundância. No caso de segmentação da rede entre os campi ou queda do servidor primário os servidores secundários assumem a entrega de configurações das estações registradas no sistema. Durante o período que o servidor secundário assume o trabalho não é possível registrar estações.

2.4. Detecção de Rogue Users

Rogue User é o usuário que utiliza IPs indevidamente da rede, ocasionando conflitos de IP e dificultando o tratamento de incidentes. O objetivo da Detecção de Rogue Users é

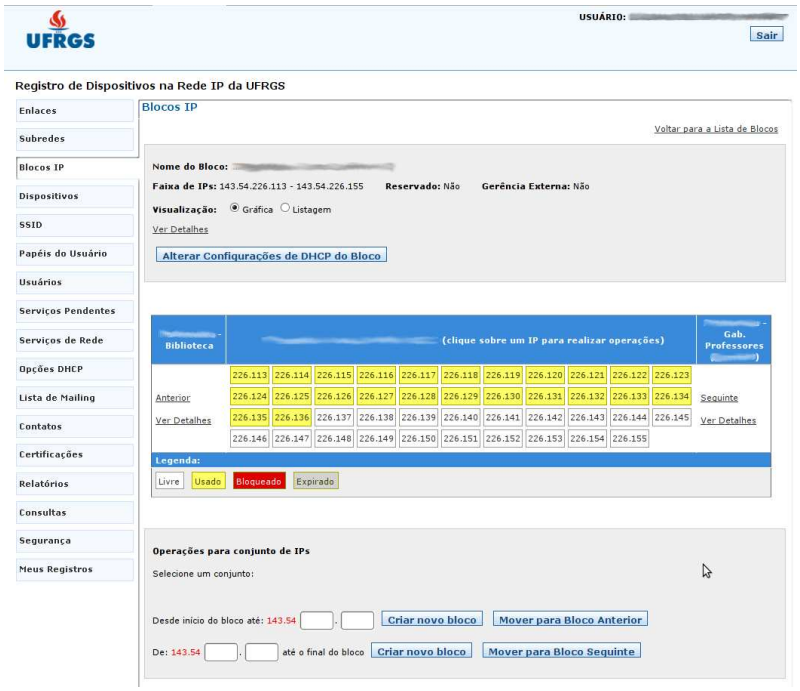

Figura 5. Interface de Gerência de Estações

Figura 6. Papéis de Usuário

bloquear automaticamente eventuais usuários que não estejam devidamente cadastrados no sistema. Atualmente, o procedimento de detecção é automatizado mas a tarefa de bloqueio ainda necessita da interferência de um operador. Existem dois *script*s que dividem a tarefa de detecção:

snatch Cria uma base de dados com todos os endereços MAC utilizados na rede da universidade. Os dados são capturados das tabelas ARP dos roteadores do *backbone* via SNMP.

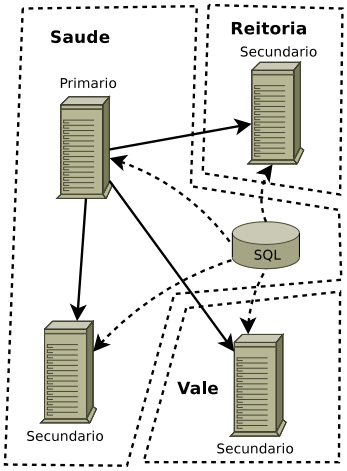

Figura 7. Redundância de servidores DHCP

rogueusers Compara os endereços MAC capturados pelo snatch com os endereços registrados no sistema. Se houver incongruências são gerados alertas informando o MAC que está utilizando o IP indevidamente.

Os alertas gerados pelo *script rogueusers* são enviados via email para o time de resposta a incidentes. O tratamento padrão para esses casos é o bloqueio do IP no *firewall* de borda.

2.5. Expiração de Registros

Os registros de IP possuem um tempo de validade. O tempo de validade foi estipulado para evitar o desperdício de IPs que poderia ocorrer com registros alocados e não utilizados. O tempo de expiração pode ser definido na interface de gerência para cada subrede, bloco e IP registrado[3].

A expiração dos IPs é feita automaticamente pelo sistema. São gerados alertas para o usuário avisando sobre a data da expiração dos seus registros de IP com antecedência de três mês, um mês, uma semana e um dia. Assim o usuário tem tempo suficiente para atualizar seus registros de IP.

2.6. Redes sem fio

A universidade implantou uma infraestrutura de rede *wireless* que permite que tanto usuários visitantes acessem a internet quanto usuários das unidades acessem a rede local de dados. São as redes UFRGS Sem Fio e Unidade Sem Fio, respectivamente.

A rede UFRGS Sem Fio permite autenticação via *tickets* ou pelo número do cartão da universidade. Essa é uma rede aberta, sem criptografia. Para habilitar o acesso à Internet é necessário que o usuário se autentique em uma página HTTP. Qualquer servidor pode gerar *tickets* para a rede *wireless* no portal da universidade e distribuí-los para usuários que não tenham vínculo com a universidade. Cada *switch* de unidade transporta uma *vlan* para o *backbone* da UFRGS. A saída dessa *vlan* se dá através de um servidor que funciona como *gateway* da rede wireless.

[3]Prioridade para os valores de IP, bloco e subrede, nessa ordem.

A rede Unidade Sem Fio, por sua vez, permite que usuários acessem a rede local se autenticando com o número do cartão, e utilizem recursos compartilhados, assim como usuários da rede cabeada. Essa rede possui criptografia WPA2 com certificados. Após autenticar-se a estação obtém acesso seguro ao nível de enlace da subrede da unidade, assim como uma máquina cabeada. Para finalizar a configuração da estação é necessário executar os mesmos passos de registro de estação da rede cabeada.

Cada SSID de Unidade Sem Fio precisa ser configurado no Sistema de Gerência de Estações. O sistema permite cadastrar órgãos no SSID da mesma forma que o bloco de subrede. Também é possível autorizar ou bloquear usuários individuais no SSID.

3. Migração de Rede da Unidade

Cada unidade migrada foi precedida por uma reunião com os responsáveis pela subrede para explicar as bases do sistema e coletar informações que pudessem ser importantes durante a migração. Para realizar a migração das redes das unidades optamos pela estratégia de manter provisioriamente o endereçamento em uso na unidade migrada. Assim, os usuários poderiam se adaptar gradualmente ao novo sistema, minimizando as eventuais indisponibilidades de rede.

Foi estabelecido um prazo de um mês dentro do qual o endereçamento IP novo compartilha o nível de enlace (mesma *vlan*) com o endereçamento IP antigo da unidade (rede legada). Expirado esse prazo a rede legada é removida dos roteadores. Para definir o tamanho do bloco da subrede nova utilizamos o histórico de MACs presentes na subrede obtido nas tabelas ARP dos roteadores do *backbone*.

A Tabela 1 apresenta a quantidade de equipamentos registrados em cada unidade da universidade que já foi migrada. As redes sem fio (UFRGS e Unidades) já estão instaladas em algumas unidades da universidade e a demanda pelo serviço está crescendo. Existem 52 bases configuradas para UFRGS Sem Fio e 13 para Unidade Sem Fio.

Algumas subredes que foram migradas eram palco constante de incidentes de trocas de IP indevidas e conflitos de IP, muitas vezes não tratados. Após a migração pudemos observar um aumento significativo no número de tratamentos de incidentes desse tipo. Isso se deve à maior visibilidade proporcionada pelo *script* de detecção de *rogue users*. A associação de usuário e MAC com o IP, no sistema de registro, foi fundamental para o tratamento mais adequado desse tipo de incidente.

Outro benefício imediato do sistema foi a alocação de IPs automática, sem necessidade de intervenção de gerentes de rede. Algumas subredes da universidade nem mesmo possuem gerentes disponíveis para realizar a alocação do espectro de IPs da unidade. Com o sistema essa alocação de IPs é feita automaticamente, de acordo com a disponibilidade de IPs na rede.

4. Conclusão e Considerações Finais

O Sistema de Registro de IPs está prestes a completar um ano de funcionamento na rede da UFRGS. Durante esse período, amadureceu consideravelmente com melhorias, novas funcionalidades e correções de bugs. Atualmente, existem mais de 3300 dispositivos registrados no sistema, o que equivale a aproximadamente 30% do total de dispositivos presentes na universidade. As redes sem fio do sistema também estão se espalhando pela universidade.

Unidade	Estações
Psicologia	83
FABICO	57
Reitoria - Anexo II	10
Reitoria	19
Arquitetura	181
ICBS	182
Matemática	256
Direito	80
Economia	260
CPD	231
Agronomia	387
Veterinária	243
Bioquímica	129
Enfermagem	151
Engenharia Química	181
Geociências	583
Farmácia	172
Odontologia	179
Total	3384

Tabela 1. Estações registradas pelas unidades da UFRGS migradas para o Sistema de Registro de Estações

As unidades migradas puderam se beneficiar com a alocação automática dos IPs, configuração automática das estações através de DHCP, desoneração dos gerentes de rede e gerenciamento do acesso às redes sem fio. Outro grande benefício está associado a um melhor tratamento dos conflitos de IP e outros incidentes de segurança.

Pretende-se dar continuidade na implantação do sistema nas demais unidades da universidade, conforme a demanda. Quanto ao desenvolvimento, estão sendo criadas extensões para auxiliar no trabalho do time de resposta a incidentes e grupo de gerenciamento de rede. Para a parte de segurança estão sendo aprimorados a integração com o firewall, sistema de *tickets* e histórico de ARP. A gerência de rede irá ser integrada com a documentação da configuração dos ativos de rede (*switches* e roteadores) no sistema.

Referências

Conover, J. (2006). NAC Vendors Square Off. In *Network Computing*, pages 55–64.

Machado, C., Marquezan, C., Rey, L., Soares, D., Postal, E., Horowitz, E., and Ziulkoski, L. (2008). Sistema de Registro de Estações da UFRGS. In *II Workshop de Tecnologia da Informação das IFES*, Gramado, RS, Brazil.

Tonin, R., Machado, C., Postal, E., Rey, L., and Ziulkoski, L. (2008). Sistema de Gerenciamento de Redes Wireless da UFRGS. In *II Workshop de Tecnologia da Informação das IFES*, Gramado, RS, Brazil.