Portanto, o gerente SNMP deverá localizar-se na máquina servidora que também executará o processo agendador de tarefas e eventualmente o HTTP server. Assim, por exemplo, a execução desse gerente SNMP poderá ser agendada no crontab (Linux) através do script PHP que executa quando, através de uma página HTML, o "principal" (usuário) clica no botão agendar.

Além do software desenvolvido será necessária a entrega de um artigo no formato IEEE, com no mínimo 5 e no máximo 6 páginas, especificando na seção de Introdução o problema do controle de acesso a Internet (em um ambiente de ensino, por exemplo), a motivação para sua resolução, a proposta de solução apresentada pelo trabalho, e a contribuição dada pelo trabalho no campo da gerência de redes. Na seção Trabalhos Relacionados deverá constar uma revisão bibliográfica sobre o SNMP, bem como o levantamento e descrição de outras ferramentas/trabalhos que também atacam o problema do controle de acesso à Internet no ambiente de ensino. Na seção desenvolvimento, deverá constar a descrição do que foi desenvolvido, as ferramentas utilizadas, eventualmente algoritmos, figuras explicando a interação entre as partes do sistema, etc... Na seção Resultados, deverá constar uma avaliação de desempenho básica do sistema. Por exemplo, para um agendamento de bloqueio e desbloqueio de acesso à Internet de todas as máquinas da sala, quantas mensagens SNMP foram trocadas, quanto tempo demorou para isso, etc...

Além desse artigo é necessária a elaboração de uma espécie de manual de configuração/utilização do sistema. A escrita do manual deve ser pensada tendo em vista que os leitores do mesmo serão o administrador do sistema/rede, e o professor que será o usuário final do sistema. O administrador estará preocupado com a configuração e manutenção do sistema. Portanto, para ele será importante conhecer a fundo o banco de dados e o que cada tabela e coluna quer dizer, bem como o que ele deve fazer em caso de alterações na infraestrutura da rede ou das salas de aula. Assim, entre outras coisas, é importante informar no manual que o sistema está preparado para ter uma (ou mais) máquinas autorizadas a usar o sistema, e sempre que a máquina autorizada mudar, deve ser alterado, no banco de dados, o MAC da máquina (computador) autorizado. Já o professor, estará interessado em saber como funciona a utilização do sistema. Ou seja, o que cada página disponibiliza em termos de funcionalidades; como ele deve agir para agendar um bloqueio, atual ou futuro, de todas ou de apenas uma ou algumas das máquinas existentes na sala; como ele desbloqueia o acesso a essas máquinas, etc... Nesse sentido, dois documentos podem ser produzidos: um para o administrador e outro para o usuário (aquele que pode agendar o bloqueio do acesso à Internet por meio do "desligamento"da porta física do switch).

2 Prazos

1. Apresentação para o professor do sistema funcionando: 27/06/2024
2. Entrega do artigo (impresso e digital): 27/06/2024
3. Entrega do código fonte: 27/06/2024

Managing Internet Access

Prof. Adriano Fiorese

1 Caracterização do Sistema

Um trabalho por equipe deverá ser desenvolvido. Cada trabalho consiste na implementação de um sistema de controle de acesso à Internet utilizando técnicas de gerência de redes.

Para a implementação deverá ser considerado um cenário de rede local cuja interconexão se dá através de switch. Esta rede local conterá uma série de máquinas (computadores) com acesso cabeado (ex: laboratório de ensino do DCC). O acesso à Internet deverá ser controlado para todas as máquinas (em nível de portas RJ45 do switch) com exceção da máquina do professor que fará o papel de acionador do gerente de rede por meio da interface web (*front end*), da porta que conecta o *switch* ao *data center* onde estará o servidor web (rede local) e eventualmente da porta física do switch que conecta o switch de uma sala com outra. A máquina do professor é a única autorizada que poderá acessar uma interface gráfica (web) via browser que agendará/executará imediatamente a negação do acesso à Internet por um determinado período de tempo, das demais máquinas. Apenas o "principal" (usuário) autorizado poderá executar esse agendamento/execução imediata. Para tanto a interface web só deverá ser apresentada caso a invocação tenha partido da única máquia autorizada a utilizá-la, e nesse caso, deverá requisitar login e senha do usuário para liberar o acesso a aplicação de controle de acesso à Internet (*front end*).

O agendamento da negação de acesso a Internet (por meio do desligamento da porta física do switch) deverá ser executado pelo *crontab* (linux). Isso significa que haverá a necessidade de um processo gerente responsável pela emissão de mensagens SNMP, que será acionado pelo agendamento, para desfazer a negação do acesso à Internet no final do período de tempo solicitado no início do processo. Além disso, o agendamento/execução somente poderá ser realizado a partir da máquina que será a única autorizada a ter acesso à Internet e que necessariamente deverá estar dentro da rede local gerenciada. Ou seja, por exemplo, se a máquina que está acessando a aplicação de controle de acesso à Internet estiver na sala F203, somente poderá ser controlado o acesso (bloqueadas ou desbloqueadas portas no switch) das máquinas que pertencerem à sala F203.

Caso seja solicitado o bloqueio do acesso, deverá ser especificado o prazo (minutos ou horas, ou dias) para desbloqueio (via browser), para evitar que as portas permaneçam desabilitadas indefinidamente. Portanto, o desbloqueio pode ocorrer por ação do usuário ou por agendamento.

Assim, o sistema deverá permitir o bloqueio de todas as portas pertencentes a um ambiente físico particular, por exemplo uma sala servida por um switch. Assim, hipoteticamente, se o switch tem 24 portas e atende duas salas com um conjunto de equipamentos em cada sala, então com apenas um clique deverá ser possível selecionar todas as portas a serem bloqueadas que correspondem aos equipamentos da sala em que se encontra a única máquina autorizada a executar o bloqueio. Ainda, a atualização da interface gráfica (por exemplo mudança de ícone mostrando porta aberta ou fechada) a respeito das portas atualmente bloqueadas deve ser feita automaticamente, sem a necessidade do usuário (ex: professor) solicitar.

Lembrem-se, o sistema deverá levar em conta a possibilidade de uma sala ser atendida por mais de um switch.

Quaisquer informações, devidamente documentadas, (ex: IP, MAC, número de portas, etc...) necessárias à correta implementação, implantação e operação da referida solução deverá estar em base de dados de configuração. Recomenda-se a utilização de uma base de dados *freeware* como MySQL por exemplo, onde ficarão armazenadas as informações. O responsável por alimentar essa base, ou seja, preencher para cada sala, qual é o IP do(s) switch(es) que a atende(m), o endereço MAC da única máquina autorizada a usar o web browser para controle do acesso à Internet daquela sala, login, senha, etc..., é o administrador do sistema. Portanto, ele deverá alimentar a base de dados com as ferramentas próprias disponibilizadas pelo banco de dados em questão (ex: PHPadmin do MySQL), ou por sistema apropriado desenvolvido além deste trabalho solicitado.

Ainda, a interface web deverá exibir o status de cada máquina (bloqueada ou liberada). Para tanto é necessário que:

1. O usuário ("principal" autorizado) possa se valer de dados específicos do host (nome, IP, MAC) para bloquear, desbloquear ou consultar o status. Isso significa que a aplicação deverá manter o mapeamento entre um ou mais desses dados e a porta correspondente do switch; até por razões de depuração, seria útil que a porta acompanhasse o identificador do host na interface web.

2. É importante lembrar que cada porta no switch está associada a uma máquina host; ou a uma porta de outro equipamento de interconexão (ex: switch, roteador, etc...). Assim, não deverão ser bloqueadas as portas que ligam a máquina autorizada ao switch, nem a porta que liga o switch a outro equipamento de interconexão (e por consequência ao servidor web onde está hospedada a aplicação de controle de acesso à Internet, ou seja, ao *front end*).

A Fig. 1 procura demonstrar a arquitetura do sistema proposto.

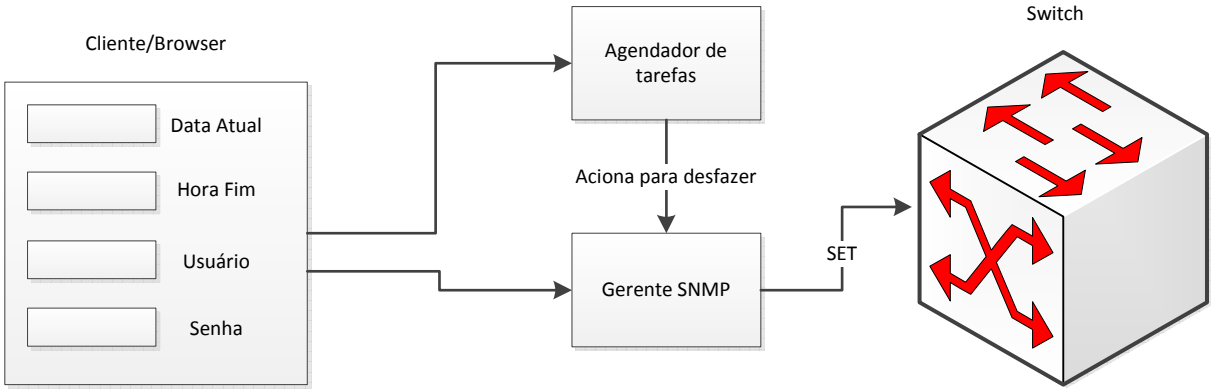

Figura 1: Arquitetura do Sistema Proposto

O gerente de rede de que trata o terceiro parágrafo da Seção 1 é o gerente SNMP que deverá ser desenvolvido utilizando a API WebNMS SNMP, ou API SNMP4J disponíveis no moodle da disciplina OGMR0001. A responsabilidade do gerente é justamente enviar os pacotes SNMP SET com os valores adequados (para bloqueio ou desbloqueio da porta) para a variável gerenciada adequada mantida pelo agente SNMP que executa no switch. Assim, o agendamento de bloqueio serve para ativar o gerente em determinado instante de tempo para que envie a mensagem SNMP SET adequada ao agente executando no switch adequado. Já o desbloqueio executa o SNMP SET contrário. A variável gerenciada em questão faz parte da MIB II, que deve ser carregada (*loaded*) no gerente SNMP para que seja possível enviar mensagens SNMP SET.