Unidade III

5 PADRÕES PARA O GERENCIAMENTO

Existem diversas soluções de gerenciamento de rede, desde soluções proprietárias – as quais atendem somente os equipamentos de um fornecedor particular – até soluções abertas e ambientes multiplataforma. Há soluções gratuitas e pagas.

O Laboratório Nacional de Aceleração (SLAC, em inglês) da Universidade de Stanford realizou um levantamento das ferramentas existentes no mercado americano e gerou uma lista com centenas de ferramentas para monitoramento e gerenciamento de redes separadas por ano de lançamento.

Saiba mais

A listagem completa está disponível no *site*:

<http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html>.

Por exemplo, somente no ano de 2008, foram lançadas cinquenta ferramentas diferentes, entre elas: AutoMate, BGPlay, BGPmon, BreakingPoint, Capsa, Collectl, DopplerVue, Eddie, EffeTech, EtherDetect, Ethergrouik, ElvinRRD, FlowMon, FreeNats, GNetWatch, InterMapper Flows, Inventory Genie, IPAudit, IPHost Network Monitor, Labtech Software, LANSurveyor, Lemon, NetaNAV, monitis, Monitoring Genie, MTD Sentry, Opnet nCompass, NetGong, NetInfo, NetMRI, NetScope, Network Miner, Network Performance Daily, nfdump, NfSen, Opnet Modeler, Opsview, Osmius, PacketTrap, Panopta, PC Inventory Advisor, Q3ADE, Remote Asset Tracker, Sentinel, Server Supervisor, Splunk, Tembria, tcpillust, The Dude, Total network monitor, ZettaView e Zyrion Traverse.

Existem sistemas de gerenciamento EMS e NMS. Um Sistema de Gerenciamento de Elemento (Element Management System – EMS) é o nome dado para os *softwares* gerentes que conseguem gerenciar apenas um tipo de agente. Neste tipo de *software* a MIB (Base de Informações Gerenciáveis) já é reconhecida por ele. Já o Sistema de Gerenciamento de Rede (Network Management System – NMS) é o nome dado para o *software* gerente que consegue gerenciar qualquer agente simultaneamente. Neste tipo de *software* é necessário compilar a MIB dos objetos que se deseja gerenciar.

Deve-se também diferenciar os alertas dos *logs*. Um alerta indica que uma operação fora do normal está ocorrendo. Já um *log*, normalmente um arquivo-texto, ajuda a identificar a causa desse acontecimento. Existem sistemas gerenciadores de *logs* que podem utilizar as informações gravadas para descobrir o que ocorreu no sistema.

Lembrete

Alertas indicam quando algo fora do normal está acontecendo. Já os *logs* ajudam a identificar a causa desse acontecimento.

5.1 Protocolos de monitoramento

Além do protocolo SNMP, utilizado em redes TCP/IP, e do protocolo CMIP, utilizado em redes no padrão OSI, existem outros protocolos de monitoramento de rede, como o ICMP, o Syslog e o NetFlow.

5.1.1 ICMP

O Protocolo de Controle de Mensagem de Internet (Internet Control Message Protocol – ICMP) opera na camada da rede e é utilizado para gerenciar as informações relativas aos erros nas máquinas conectadas, realizando *debug* da rede, através de comandos como *ping* e *traceroute*.

Uma das informações de *ping* e *traceroute* é o TTL (Time To Live), que define o número máximo de roteadores pelos quais o pacote pode trafegar. Essa informação é definida para evitar, por exemplo, que um pacote fique indefinidamente circulando pela rede antes de encontrar seu endereço destino.

O tempo necessário para o pacote ir e voltar do seu destino é conhecido como RTT (Round Trip Time).

O *ping*, por sua vez, é um aplicativo que usa o protocolo ICMP e possibilita ao usuário verificar a conectividade entre dois servidores. Este comando envia pacotes ICMP (*echo request*) para uma determinada máquina e aguarda uma mensagem ICMP de resposta (*echo reply*).

Com o comando *traceroute*, o usuário pode descobrir o caminho percorrido pelo pacote até seu destino. O *traceroute* envia três pacotes UDP com a porta de destino que não seja usada por nenhuma aplicação, inicialmente com TTL igual a um.

Ao passar pelo primeiro roteador, esse tempo se tornará zero e uma mensagem ICMP tempo excedido retornará. Com isso, obtêm-se as informações sobre o primeiro roteador no meio do caminho e o RTT da fonte até este roteador. Em seguida, o TTL é aumentado para dois e novamente são enviados três pacotes UDP. Entretanto, a mensagem ICMP ocorrerá somente no segundo roteador. O processo irá se repetir até que se conheça cada roteador no meio do trajeto, entre a origem e o destino. Quando o destino for alcançado, a mensagem ICMP tempo excedido não será mais retornada, mas sim uma mensagem ICMP porta inacessível.

Lembrete

O comando *ping* utiliza o ICMP para verificar a acessibilidade de equipamentos.

O comando *traceroute* permite a verificação do caminho feito por um pacote para chegar ao destino, retornando a sequência de saltos que o pacote atravessou.

5.1.2 Syslog

O Syslog é um serviço que registra os eventos e as ações dos processos em qualquer dispositivo que adote o padrão de mensagem definido pela IETF (Internet Engineering Task Force) na RFC 3164. Os dispositivos gerenciados podem ser *hosts* Linux, servidores Unix, roteadores, servidores de impressão e qualquer outro dispositivo que siga o padrão da IETF.

Os *logs* salvos possuem as informações da mensagem emitida, do *host*, data e hora e podem ser configurados para registro somente de eventos críticos ou de praticamente todos os eventos do sistema. Assim, será no *log* em que um administrador da rede irá encontrar informações sobre o funcionamento do sistema, que auxiliem na correção de erros e em verificações de rotina.

O Syslog pode informar sobre tentativas de acesso ao sistema ou a recursos do sistema e ajudar na prevenção e na solução de problemas de funcionamento, segurança, confiabilidade das informações, integridade e disponibilidade da rede.

5.1.3 NetFlow

Fluxo indica uma taxa de entrada/saída de um determinado objeto dentro de uma referência fixa. Em um contexto de redes de computadores, o fluxo é uma sequência unidirecional ou bidirecional de pacotes com características em comum entre uma origem e um destino.

É utilizado para mensuração das informações sobre o uso da rede. Alguns analisadores tradicionais, como o MRTG, informam apenas o tráfego total da rede.

Uma demanda que surgiu foi a análise eficiente de coleta de dados, pois não era viável a pesquisa pacote a pacote. Em vez de armazenar as informações pacote a pacote, os pacotes foram agrupados por características semelhantes, como origem e destino, porta de origem e destino ou protocolo de camada de transporte.

Tal abstração de dados é útil em situações como engenharia de tráfego, *top talker*, para descobrir quem são os usuários mais ativos e quais recebem mais atividades, monitoramento de redes ocultas, lista de IPs maliciosos, verificando se algum computador da rede está conectando a um IP conhecido como malicioso, violações da política de uso e análise de dados históricos. Ao analisar dados históricos, é possível verificar as razões pelas quais ocorreu um determinado incidente na rede.

A IETF propôs a criação de uma arquitetura padrão para análise de tráfego. Um dos protocolos que surgiram foi o NetFlow (RFC 3954), desenvolvido pela Cisco Systems. O grupo de trabalho escolheu o NetFlow como protocolo a ser aperfeiçoado e implementado.

Com a utilização do NetFlow, é possível possuir o cache para acelerar os *lookups* nas tabelas de roteamento, dispensar a verificação de tabelas de *access-list* toda vez que um pacote chega, ficando mais eficiente o processo de roteamento, além de exportar as informações de fluxo utilizadas pelo cache do NetFlow, facilitando a coleta de dados para futuras análises sem a necessidade de colocar um analisador em cada enlace.

A Cisco define um fluxo como uma sequência unidirecional de pacotes entre máquinas de origem e destino, e o NetFlow permite a agregação das informações de tráfego sobre um roteador ou *switch*. Fluxos de rede são altamente granulares e identificados por ambos os endereços IP (da origem e do destino) e pelo número das portas da camada de transporte na origem e no destino. O NetFlow também utiliza, para identificar unicamente um fluxo, os campos Protocol Type e Type of Service (ToS) do IP e a interface lógica de entrada do roteador ou *switch*.

Os fluxos mantidos no cache do roteador/*switch* são enviados para um coletor nos seguintes casos: quando o elemento permanece ocioso por mais de 15 segundos, sua duração excede 30 minutos, uma conexão TCP é encerrada com a *flag* FIN ou RST, a tabela de fluxos está cheia ou o usuário redefine as configurações de fluxo. O tempo máximo que um fluxo permanece no dispositivo antes de ser exportado é de 30 minutos. A figura a seguir mostra como criar um fluxo pelo NetFlow.

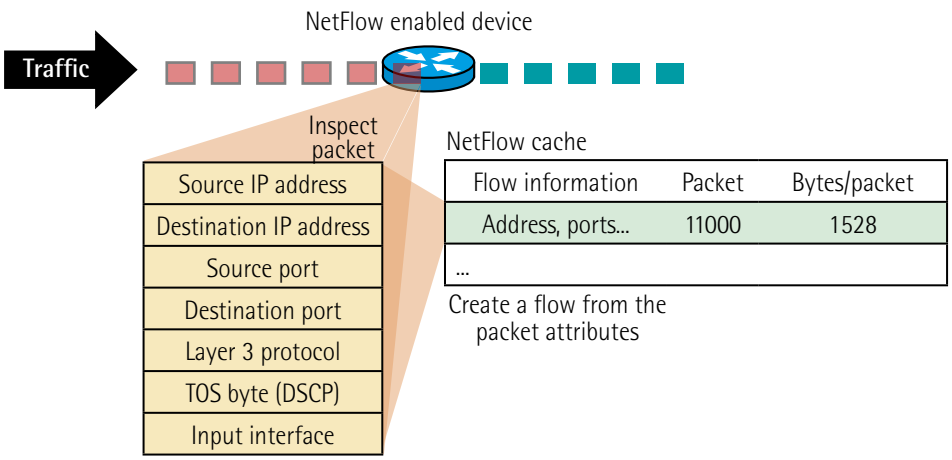

Figura 26 – Criação de um fluxo no NetFlow

Observação

O NetFlow identifica unicamente um pacote pelos endereços IP de origem e de destino e pelo número das portas da camada de transporte na origem e no destino, pelos campos Protocol Type e Type of Service (ToS) do IP e pela interface lógica de entrada do roteador ou *switch*.

5.2 Classificações de ferramentas de gerenciamento

Uma classificação inicial das ferramentas irá dividi-las em dois grupos: as ferramentas ativas e as passivas.

Ferramentas ativas são aquelas que geram interferência no sistema visando alcançar as informações necessárias. São exemplos de ferramentas ativas: snmpwalk, *ping* e *traceroute*. Analisando com mais detalhe o *traceroute*: este comando envia pacotes de pesquisa UDP, denominados *UDP probe packets*, com um pequeno TTL máximo e, então, espera por pacotes de resposta ICMP TIME_EXCEEDED dos *gateways* que estão no caminho. Como ele envia pacotes, está causando interferência na rede.

As ferramentas passivas, por sua vez, são aquelas que se limitam a coletar os dados já existentes. São exemplos dessas ferramentas: AWStats e nfdump. AWStats é a abreviação de Advanced Web Statistics; é uma ferramenta gratuita que gera relatórios gráficos estatísticos avançados de acesso em um servidor *web*.

Podem-se separar as ferramentas de gerenciamento de rede em diferentes tipos:

- Coletores.
- Sistemas de detecção de invasão (IDS).
- Sistemas de análise de *performance*.
- Sistemas de gerenciamento de alarme.
- Sistemas de *tickets*.
- Ferramentas de acesso.
- Ferramentas de depuração.
- Gerenciamento de configurações.
- Ferramentas de *log*.
- *Performance*.
- Gerenciamento de endereços.

Uma mesma ferramenta pode apresentar características de mais de um tipo.

Os **coletores** são ferramentas utilizadas para colher e guardar diferentes tipos de informação de rede. Por exemplo, para redes TCP/IP, é utilizada a ferramenta tcpdump. Quando se usa o protocolo NetFlow, a ferramenta utilizada é a nfdump.

Na nfdump, o objetivo é ser capaz de analisar um dado NetFlow do passado tão bem quanto encontrar padrões de tráfego continuamente. A quantidade de tempo que se pode retroagir é limitada pelo espaço em disco disponível. A figura seguinte mostra o princípio de operação da nfdump.

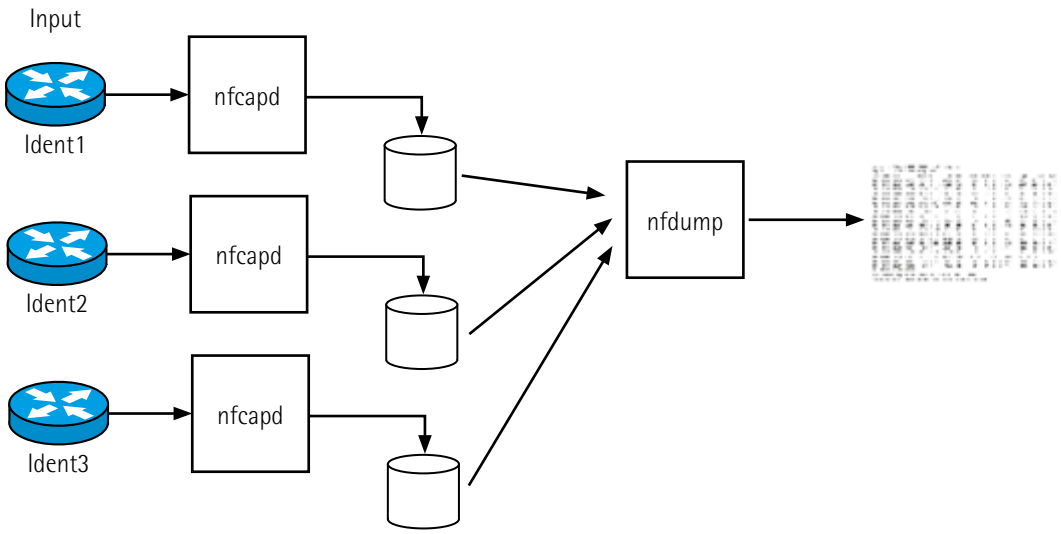

Figura 27 – Princípio de operação da nfdump

Já os **sistemas de detecção de invasão (IDS)** são responsáveis por detectar padrões suspeitos que são característicos de comportamento malicioso na rede. Para isso, o sistema pode analisar o tráfego da rede, alarmes e *logs*. Adicionalmente, este sistema toma ações para mitigar os efeitos dessa invasão.

Um exemplo desse tipo de sistema é o Snort, que é um sistema *open source* capaz de analisar o tráfego e capturar pacotes em tempo real em redes que utilizam o protocolo IP. O *software* pode analisar protocolos, procurar por conteúdo específico e ainda ser usado para detectar uma variedade de ataques e sondas, como *buffer overflows*, *portscans* e tentativas de identificação de sistema operacional.

Os **sistemas de análise de *performance*** são aqueles que permitem a análise de dados de tráfego e *performance*. Frequentemente os dados são plotados em gráficos, possibilitando o acompanhamento dos resultados. Adicionalmente, permitem o planejamento de novos recursos e a identificação de gargalos na rede. São exemplos desse tipo de ferramenta: Cacti e Zabbix.

Os **sistemas de gerenciamento de alarmes** são responsáveis pela coleta e monitoramento dos alarmes da rede. Entre seus objetivos estão uma melhor visualização dos alarmes do ponto de vista dos usuários e a realização de um diagnóstico inicial. São exemplos desse tipo de ferramenta: Nagios, Icinga e Zabbix.

Os **sistemas de *tickets*** são capazes de rastrear como os problemas estão sendo resolvidos. Além disso é possível fazer cadastro dos problemas, alocação de recursos e estatísticas de resolução. Como exemplos desse tipo de solução, podemos citar: Redmine e Trac.

As **ferramentas de acesso** são aquelas que permitem o uso de máquinas remotas, possibilitando a troca de informação entre a ferramenta de gerenciamento e os dispositivos. São exemplos as ferramentas OpenSSH e PuTTy.

A ferramenta PuTTy é um terminal de simulação *open source* que foi desenvolvido para o estabelecimento de conexões seguras entre um cliente e um servidor remoto.

As **ferramentas de depuração** possuem funções bastante específicas. A ferramenta *ping* ou latência é um utilitário do protocolo ICMP que verifica a conectividade entre as máquinas.

O aplicativo *traceroute* verifica as rotas feitas por um pacote até o destino. Os comandos ps/top monitoram os processos da máquina. Já o comando nmap verifica quais portas estão habilitadas em certo *host*. O aplicativo Wireshark analisa pacotes da rede em tempo real e o protocolo da rede.

Saiba mais

Para mais informações sobre o aplicativo Wireshark, acesse o *site*:

<http://www.wireshark.org>.

As **ferramentas de *log*** auxiliam na gestão dos arquivos *log* criados no sistema. Diversas ferramentas utilizam o padrão Syslog, que foi estabelecido pela IETF.

As ferramentas syslog-ng e rsyslog implementam o protocolo Syslog. Já o Log Analyzer permite visualizar o conteúdo dos *logs* de maneira inteligível. As ferramentas tenshi e swatch permitem a criação de filtros para os *logs*.

Entre as **ferramentas de *performance***, destaca-se a IPerf, que mede ativamente a máxima banda possível e a vazão ou *throughput* na rede IP. A ferramenta não possui interface gráfica.

Outra ferramenta de *performance* é a Ntop, ou Network Top, que mostra o uso atual de uma interface de rede, discriminando qual programa está gerando o tráfego no computador analisado. O seu nome é uma derivação de Top, o utilitário tradicional que exibe os principais usuários (*top users*) de ciclo da CPU, e é adaptada para vários sistemas operacionais.

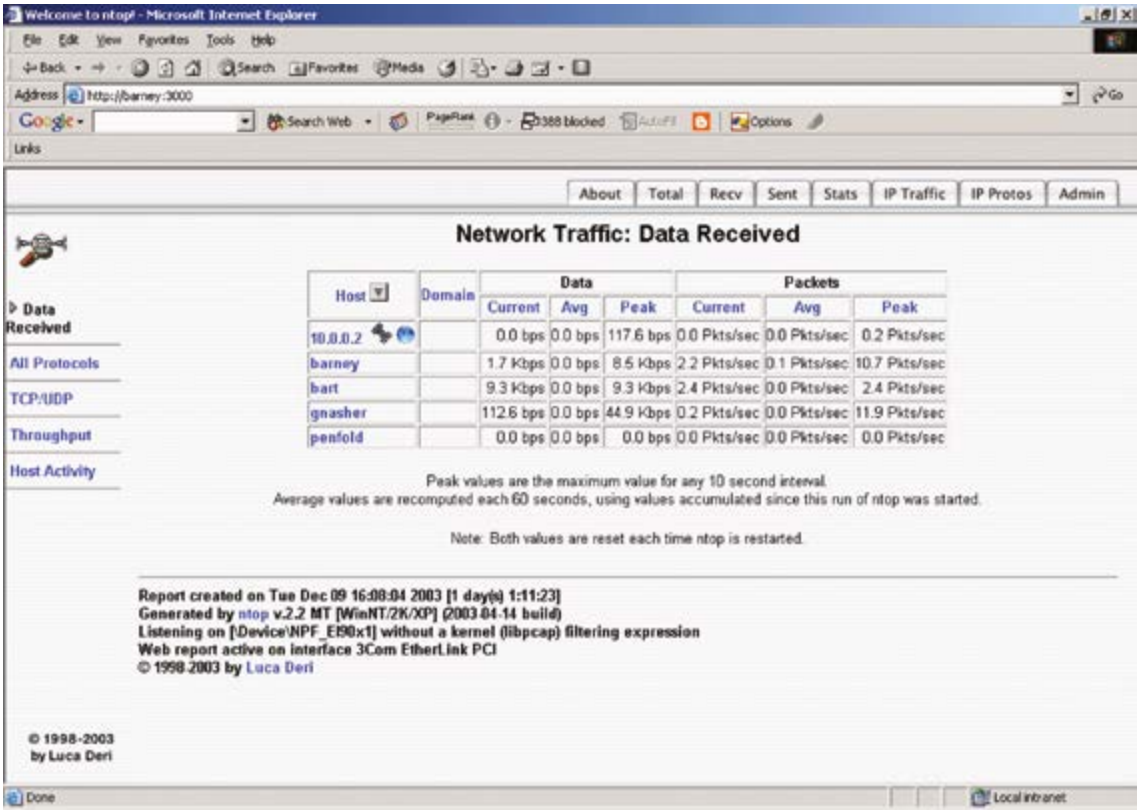

Figura 28 – Tráfego da rede, exemplo do Ntop

As **ferramentas de gerenciamento de configurações** podem ser executadas de forma manual ou automática. Na forma manual, destacam-se as ferramentas CVS, SVN e Mercurial. Já em sistemas automáticos, destaca-se a Rancid (Really Awesome New Cisco conflg Differ), aplicada aos roteadores.

O programa Rancid realiza *backups* e controle de versões de configuração de forma simplificada e eficiente, e não somente de equipamentos Cisco, apesar do nome. O Rancid pode ser executado em FreeBSD, Linux ou Mac OS X. A ferramenta Rancid conecta o roteador ao servidor remoto via SSH ou Telnet. Em seguida, executa e coleta dados de comandos, e com isso salva os dados em uma base de controle de versões CVS/SVN. Posteriormente, a mesma ferramenta cria um *diff* entre a configuração anterior e a atual. Por fim, envia um *e-mail* com o *diff* das configurações aos interessados.

Em relação a **ferramentas de gerenciamento de endereços**, pode-se destacar a IPPlan, uma ferramenta *web* para gerenciamento do endereçamento IP de uma rede. Foi projetada como uma ferramenta de fácil utilização e instalação, mas a última atualização foi feita em 2010. Outra característica dessa plataforma é o suporte a IPv6 somente na versão beta.

Outra ferramenta para gerenciamento de endereço é a phpIPAM, uma ferramenta *open source*. Ela possui suporte a IPv6 e interface amigável.

Saiba mais

Para ambas as ferramentas de gerenciamento de endereço mencionadas, foram desenvolvidos *sites* com suas devidas especificações:

<http://iptrack.sourceforge.net/>.

<https://phpipam.net/>.

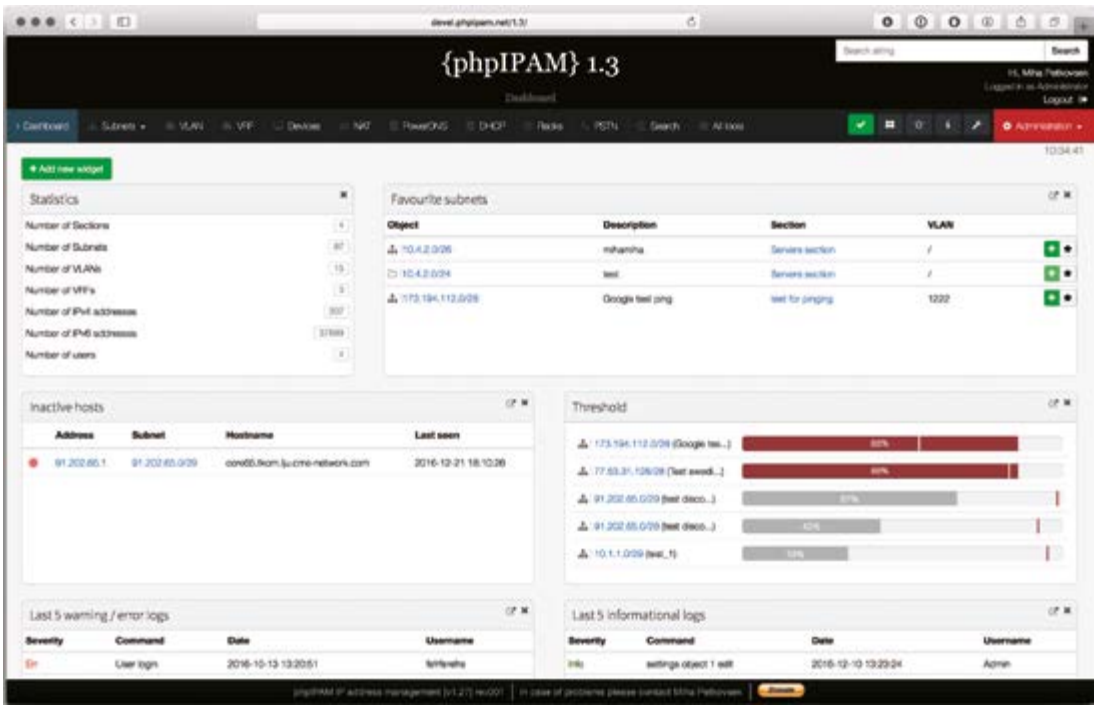

Figura 29 – Exemplo das telas do phpIPAM

A ferramenta Netdot realiza a descoberta de dispositivos via SNMP e possui gerenciamento de endereços IPv4 e IPv6. Também implementa a geração de arquivos de configuração para outras ferramentas, como Nagios, Rancid e Cacti.

O *software* GestióIP é uma ferramenta automática baseada na *web*, com gerenciamento de endereços IPv4 e IPv6. Possui funções de descoberta de rede e calcula as sub-redes.

6 UTILITÁRIOS GRATUITOS

Quantos aos **utilitários gratuitos**, existem diversos *softwares* distribuídos livremente com funções específicas no gerenciamento de redes. Muitos desses *softwares* são auxiliados por comunidades que criam *plugins* para a melhoria dessas ferramentas. Assim, esses *softwares* podem ser utilizados sozinhos ou incorporados a outras ferramentas de gerenciamento mais completas.

6.1 RRDtool

A ferramenta RRDtool (Round-Robin Database tool) é baseada em uma técnica de dados denominada *round-robin*, a qual mantém uma quantidade fixa de dados e um ponteiro que indica o elemento atual.

Figura 30 – Logotipo da ferramenta RRDtool

Para entender o princípio de funcionamento da RRDtool, considere um círculo com dados plotado nas bordas. Quando se representa uma flecha direcionada para um dos pontos do círculo, obtém-se o ponteiro. Quando se lê ou se escreve o dado atual, o ponteiro se move para a próxima posição. Como não há início nem fim no círculo, após diversas leituras ou gravações, o processo irá reutilizar automaticamente posições antigas. Dessa forma, o conjunto de dados não irá crescer em tamanho e, então, não vai requerer manutenção, porque dados gravados são sobrescritos, mantendo apenas os últimos observados.

O tipo de informação colocada na RRDtool é normalmente uma série de dados temporais, sendo necessário realizar uma tomada de medidas no tempo e informar a ferramenta RRDtool.

Observação

Uma ferramenta RRDTool é um sistema de base de dados *round-robin*. Esse sistema foi desenvolvido por Tobias Oetiker sob Licença Pública Geral GNU (General Public Licence GNU – GNU GPL). Nele, é possível armazenar séries de dados numéricos sobre o estado de redes de computadores.

Uma das utilidades da RRDtool é armazenar e processar os dados coletados via SNMP. Além da informação do tráfego na rede ou em um computador em *bytes* por segundo, é possível exibir informações como nível de consumo de energia, radiação solar, número de visitantes em uma exibição, nível de ruído em um aeroporto, a temperatura na praia de Copacabana ou qualquer outra informação desejada.

Para isso, somente é necessário que um sensor realize a mensuração e seja capaz de alimentar os dados na RRDtool. A ferramenta cria o banco de dados, atualiza os dados e gera gráficos no formato Gráfico Portátil de Rede (Portable Network Graphic – PNG) para exibir no navegador. As imagens PNG são dependentes dos dados coletados, que podem representar métricas como eventos por segundo (como na figura a seguir), tráfego da rede e nível de ocupação de um recurso da rede.

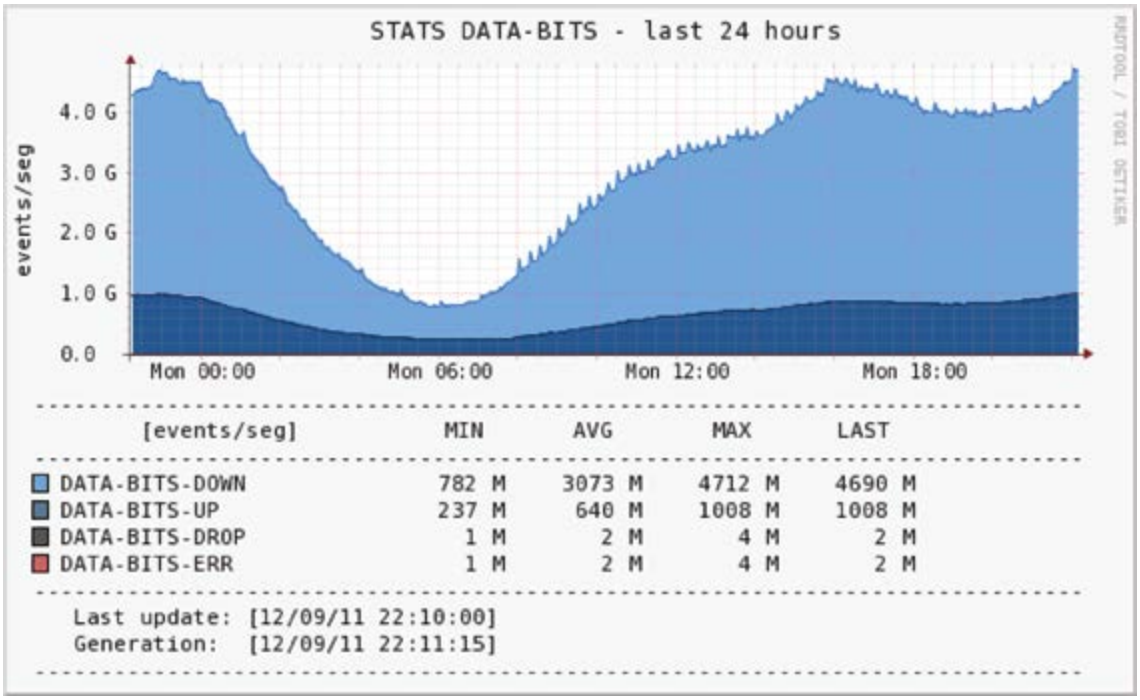

Figura 31 – Gráfico do tráfego da rede PS

6.2 MRTG

Grande parte das ferramentas de gerenciamento de redes é oriunda ou baseada na técnica Multi Router Traffic Grapher (MRTG). Esta técnica utiliza um *script* em linguagem Perl que usa SNMP para a leitura dos contadores de tráfego dos roteadores e um programa eficiente em C que compila os dados de tráfego e apresenta gráficos com destacada qualidade visual, representando o tráfego da rede que está sob monitoramento. Tais gráficos podem ser facilmente disponibilizados em páginas *web* para serem visualizados em navegadores comerciais.

O freeware MRTG foi desenvolvido pelo suíço Tobias Oetiker e licenciado por GNU GPL. A primeira versão foi desenvolvida em 1995. O *software* roda tanto em sistemas Unix e Linux como em sistemas Windows.

Figura 32 – Logotipo e rodapé do MRTG

Além de uma visão diária em detalhes, é possível o MRTG criar representações visuais históricas do tráfego para comparação – por exemplo, nos últimos 7 dias, no último mês, nos últimos 12 meses. Tal fato ocorre pela existência de um arquivo *log* contendo todos os dados obtidos com o roteador. Este

arquivo é consolidado automaticamente e não cresce com o tempo, já que irá, por padrão, manter todos os dados relevantes relacionados ao tráfego nos últimos 24 meses.

A seguir são mostrados, a título de exemplo, os gráficos diário, semanal, mensal e anual. É medido o tráfego em *bits* por segundo, verificando-se na cor verde o tráfego de dados que entram na rede e em azul o tráfego de dados que saem da rede.

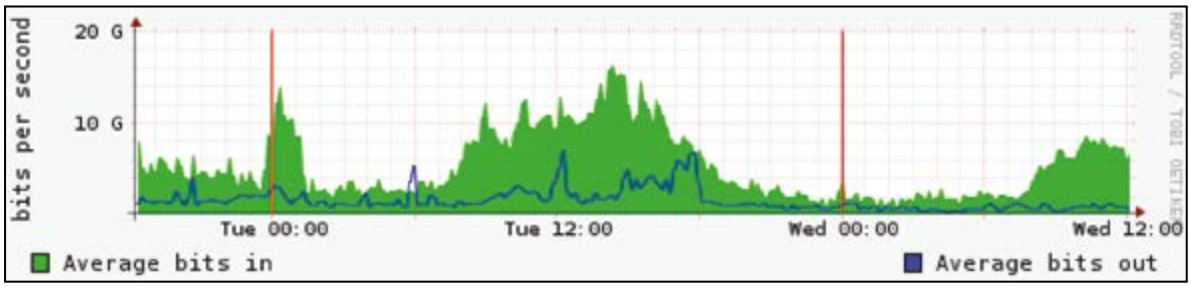

Figura 33 – Exemplo de gráfico de tráfego diário gerado pela ferramenta MRTG

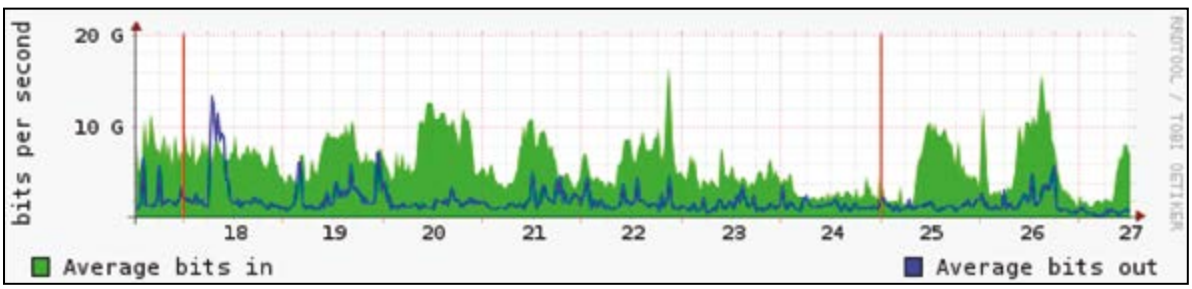

Figura 34 – Exemplo de gráfico de tráfego semanal gerado pela ferramenta MRTG

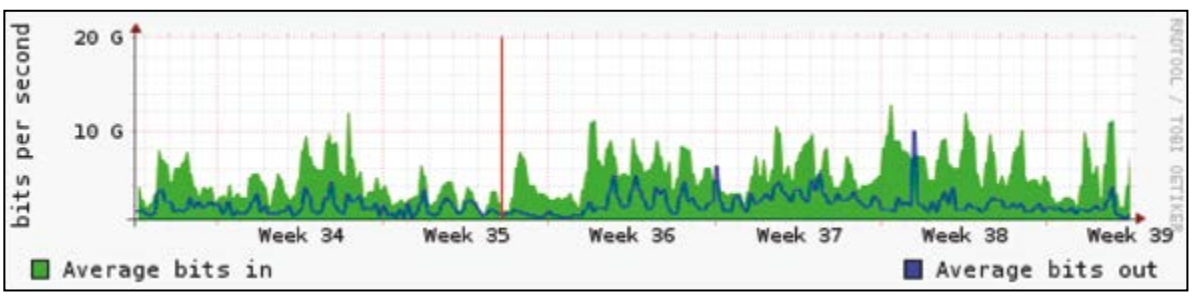

Figura 35 – Exemplo de gráfico de tráfego mensal gerado pela ferramenta MRTG

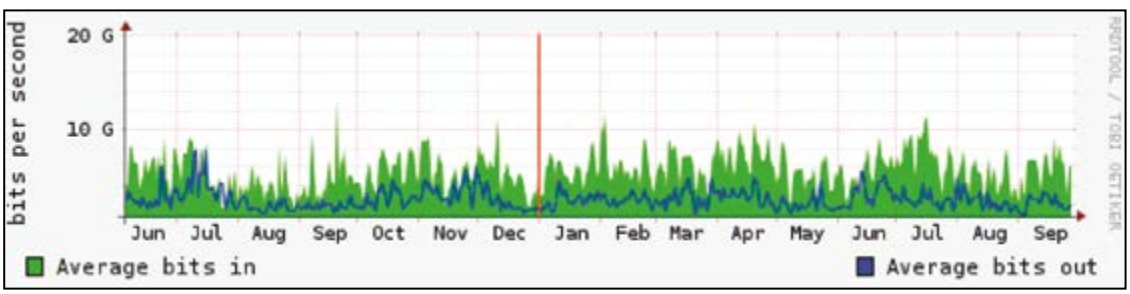

Figura 36 – Exemplo de gráfico de tráfego anual gerado pela ferramenta MRTG

6.3 Cacti

Outra ferramenta gráfica gratuita é a Cacti, uma solução de gerenciamento de rede gráfica desenhada para aproveitar as funcionalidades gráficas e o armazenamento de dados da ferramenta RRDTool.

Figura 37 – Logomarca da ferramenta Cacti

A Cacti oferece um rápido *polling*, múltiplos métodos para aquisição de dados, geração de gráficos predefinidos e diversas propriedades para gerenciamento de usuário. Apesar de lidar com toda a complexidade da informação, a interface é de fácil utilização, tanto para redes pequenas (redes LANs locais) como para redes com milhares de dispositivos.

A Cacti é uma interface *front-end* que armazena todas as informações necessárias para a criação e o preenchimento de gráficos com os dados em um banco de dados MySQL, um dos sistemas de gerenciamento de banco de dados mais populares do mercado e desenvolvido pela Oracle. O *front-end* é construído baseado inteiramente em PHP (Hypertext Preprocessor), uma linguagem de programação muito aplicada para a geração de conteúdo *web*. Além de ser capaz de manter gráficos, fontes de dados e arquivos *round-robin* em um banco de dados, o Cacti lida com a coleta de dados. É também possível utilizar suporte SNMP para a criação de gráficos de tráfego com o *software* MRTG.

Figura 38 – Interface da ferramenta Cacti

Para lidar com a coleta de dados, pode-se alimentar o Cacti com os caminhos para algum comando ou *script* externo junto com qualquer dado que o usuário preencher. A ferramenta então irá coletar este dado em uma tarefa e preencher o banco de dados MySQL e os arquivos *round-robin*.

As fontes de dados também podem ser criadas, as quais correspondem a dados reais no gráfico. Por exemplo, no caso de um usuário querer um gráfico dos tempos de *ping*, ele pode criar uma fonte de dados utilizando um *script* que realiza um *ping* em um servidor e retorna o tempo decorrido em milissegundos (após a definição das opções para a RRDTool de como armazenar o dado que ele criou e qualquer outra informação adicional que a fonte de dados precise, no caso o serviço que terá o *ping*). Criada a fonte de dados, ela é automaticamente atualizada em intervalos de cinco minutos.

Uma das funções da ferramenta é o gerenciamento dos direitos dos usuários em relação a certas áreas. Alguns usuários poderão apenas visualizar gráficos; outros poderão alterar parâmetros dos gráficos.

Por fim, uma das facilidades da ferramenta Cacti é o uso de *templates* que permitem trabalhar com um elevado número de fontes de dados e gráficos. Isto possibilita a criação de um gráfico ou de uma fonte de dados que define qualquer gráfico ou fonte de dados associada a ele.

Com o Cacti, é possível gerar gráficos referentes a uso de memória física e virtual, tráfego de rede, quantidade de espaço em disco ou quantidade de processos. Por meio do SNMP, ele permite o acesso a gráficos de sistemas operacionais Linux e Windows, de dispositivos de rede como roteadores e *switches* ou de qualquer outro elemento da rede que suporte o protocolo SNMP. Existem três opções de como o Cacti busca a informação no SNMP, como mostra o quadro a seguir.

Quadro 5 – Meios de obter dados do SNMP no Cacti

Tipo	Descrição	Opções (suporte)	Local de utilização
SNMP Externo	Chama os binários net-snmp snmpwalk e snmpget que estão instalados no sistema	Todas as opções de SNMP	Interface *web* e *poller* PHP (poller.php)
SNMP Interno (php-snmp)	Usa as funções de SNMP do PHP que estão ligadas à net-snmp ou ucd-snmp durante o tempo de compilação	Versão 1 apenas	Interface *web* e *poller* PHP (poller.php)
Spine SNMP	Liga-se diretamente com net-snmp ou ucd-snmp e chama API diretamente	Todas as opções de SNMP	*Poller* baseado em linguagem C (*spine*)

A arquitetura do *software* permite a expansão deste por meio de *plugins* desenvolvidos pela comunidade, que o incrementam e adicionam novas funcionalidades. Um exemplo de *plugin* é o PHP Network Weathermap, no qual se visualiza um mapa da rede e o *status* de cada elemento.

A ferramenta permite o agendamento de serviços em intervalos predeterminados, gerando gráficos, e a partir dos resultados é possível tratar com múltiplos usuários ao mesmo tempo, ainda que com consultas diferentes.

É possível utilizar duas categorias de agente remoto no Cacti: um *script* PHP previsto para pequenas redes, por meio do arquivo cmd.php, ou um pequeno agente escrito em C chamado de *poller spine*, o qual é escalável para grandes redes de computadores.

As informações capturadas por esse tipo de ferramenta são de um volume muito elevado. Assim, não se recomenda visualizar um grande número de gráficos, pois isso irá gerar uma série de parâmetros a monitorar, tornando a tarefa de administração muito mais complexa.

Um ponto benéfico do Cacti é que ele não demanda muitos recursos do servidor em que está executando. Como foi escrito em PHP sobre plataforma *web*, ele tem como característica ser uma ferramenta ágil. Também é possível criar outros usuários no Cacti. Adicionalmente, a ferramenta é escalável, sendo de certa forma previsível o desempenho com o aumento da rede e dos recursos.

Entretanto, não existe um agente de descoberta automático. Assim, toda a rede deve ser adicionada manualmente. Alguns *plugins* incorporaram essa melhoria na ferramenta, mas o ideal é que o próprio desenvolvedor do *software* realize essa inclusão, para não tornar o trabalho do administrador da rede muito adverso.

Resumo

Nesta unidade Vimos que existem centenas de soluções focadas no gerenciamento de redes. Essas soluções podem ser proprietárias, as quais atendem somente os equipamentos de um fornecedor particular, podem ser abertas (ambientes multiplataforma) ou, ainda, podem ser gratuitas e/ou pagas por licença.

Estudamos também que os *softwares* podem geram alertas ou *logs*. Alertas indicam quando algo fora do normal está acontecendo. Por sua vez, os *logs* ajudam a identificar a causa desse acontecimento.

Já o protocolo ICMP opera na camada de rede e é utilizado para gerenciar as informações relativas aos erros nas máquinas conectadas, realizando *debug* da rede, através de comandos como *ping* e *traceroute*. O comando *ping* verifica a acessibilidade de equipamentos. O comando *traceroute* permite a verificação do caminho feito por um pacote para chegar ao destino, retornando a sequência de saltos que o pacote atravessou.

Vimos, igualmente, alguns sistemas de serviços, entre eles o Syslog e o NetFlow. O Syslog é um serviço que registra os eventos e as ações dos processos em qualquer dispositivo que adote o padrão de mensagem definido pela IETF.

O NetFlow, criado pela Cisco, identifica unicamente um pacote pelos endereços IP de origem e de destino e pelo número das portas da camada de transporte na origem e no destino, pelos campos Protocol Type e Type of Service (ToS) do IP e pela interface lógica de entrada do roteador ou *switch*.

Estudamos que existem diversos tipos de ferramenta de gerenciamento de rede, como: coletores; sistemas de detecção de invasão (IDS); sistemas de análise de *performance*; sistemas de gerenciamento de alarme; sistemas de *tickets*; ferramentas de acesso; ferramentas de depuração; gerenciamento de configurações; ferramentas de *log*; *performance* e gerenciamento de endereços.

Por fim, vimos que a ferramenta RRDTool é um sistema de base de dados *round-robin*, e que algumas ferramentas são baseadas na técnica Multi Router Traffic Grapher (MRTG). Esta técnica concatena as informações de tráfego e gera gráficos que demonstram o tráfego da rede monitorada.

A ferramenta Cacti é uma solução de gerenciamento de rede gráfica desenhada para aproveitar as funcionalidades gráficas e o armazenamento de dados da ferramenta RRDTool.

Exercícios

Questão 1. (TER-RR 2015) Considere as características dos protocolos de Gerenciamento de Redes.

I – As principais vantagens de utilização deste protocolo são: funciona como cache para acelerar os *lookups* nas tabelas de roteamento; dispensa a verificação de tabelas de *access-list* (apenas de entrada) toda vez que um pacote chega, deixando mais eficiente o processo de roteamento; permite a exportação das informações de fluxo utilizadas pelo *cache*, facilitando a coleta de dados para futuras análises sem a necessidade de colocar um analisador em cada enlace.

II – Tem como base o modelo de gerência OSI, sendo um protocolo não orientado a conexão. Os gerentes são *softwares* executados em uma ou mais estações capazes de realizar tarefas de gerenciamento da rede, sendo responsáveis por enviar *requests* às estações agentes e receber as *responses*, podendo ainda acessar (*get*) ou modificar (*set*) informações nos agentes e receber, mesmo sem requisição, informações relevantes ao gerenciamento (*traps*).

III – Dois padrões básicos deste protocolo, funcionalmente complementares, são especificados. O primeiro opera somente na camada MAC, oferecendo recursos ao administrador da rede para monitorar o tráfego e coletar informações estatísticas da operação de um segmento de rede local, não permitindo, porém, obter estatísticas com relação às camadas de rede e superiores. A necessidade de um melhor tratamento do tráfego de protocolos para a gerência da rede fez com que uma extensão deste protocolo fosse criada.

Os protocolos caracterizados em I, II e III, são, correta e respectivamente:

A) SNMP – Netflow – RMON.

B) Netflow – SNMP – RMON.

C) SNMP – RMON – Netflow.

D) RMON – SNMP – Netflow.

E) Netflow – RMON – SNMP.

Resposta correta: alternativa B.

Análise da resposta

Netflow: é uma ferramenta que contém variações como *netstreams low*, *ipfix* etc. É uma tecnologia que é parte integral do IOS da Cisco que considera os pacotes como parte de um fluxo, ao invés de simplesmente contá-los. Um fluxo, como significa o nome, tem um princípio, meio e fim. Quando pacotes de dados são agrupados como fluxos, administradores são capazes de entender as aplicações que estão utilizando a rede de forma mais abrangente. Isto naturalmente permite um melhor gerenciamento e uma melhor qualidade de serviço. Os administradores também são capazes de identificar as áreas de problemas e tomarem uma ação preventiva.

O Netflow agora foi adotado por vários fabricantes além da Cisco, já que se tornando um padrão de-facto. Juniper, Extreme Vanguard, Huawei e muitos outros fabricantes incorporaram em seus roteadores e *switches* funcionalidade similares (Fonte: <https://www.telcomanager.com/pt-br/o-que-e-netflow>).

Simple Network Management Protocol (SNMP): é um protocolo da camada aplicação criado para transportar informações de gerência de rede entre os dispositivos gerenciados e os sistemas de gestão de redes, ele possibilita que administradores de rede gerenciem o desempenho de uma rede monitorando interfaces, processadores, memórias de equipamentos como roteadores, *switches*, dispositivos *wireless* e servidores.

O SNMP utiliza na camada de transporte o UDP(User Datagram Protocol, não é um protocolo orientado a conexão) com as portas 161 e 162, para realizar a comunição entre NMS e os dispositivos gerenciados.

Existem três tipos de mensagem comuns durante o processo de gerenciamento:

Get – permite que a estação de gerenciamento recupere o valor de objetos MIB do agente.

Set – permite que a estação de gerenciamento defina o valor de objetos MIB do agente

Trap – permite que o agente notifique a estação de gerenciamento sobre eventos significativos (Fonte: <http://www.ti-redes.com/gerenciamento/snmp/intro/>).

Remote Monitoring (RMON) – oferece suporte à implementação de um sistema de gerenciamento distribuído. Nele fica atribuída aos diferentes elementos, tais como estações de trabalho, *hubs*, *switches* ou roteadores, das redes locais remotas a função de monitor remoto.

O RMON1 opera somente na camada Media Access Control (MAC).

O RMON2 opera no nível da camada de rede e camadas superiores complementando portanto o RMON1 (Fonte: <http://www.oocities.org/siliconvalley/vista/5635/cap5.html>).

Questão 2. (UFRJ 2012) Sobre os aplicativos web Nagios, Cacti e MRTG, é correto afirmar que:

A) o Nagios é uma ferramenta para monitoramento puramente SNMP de redes e serviços, capaz de gerar apenas alertas de sobrecarga; o Cacti é uma ferramenta de monitoramento SNMP que usa o RRDTool para gerar diversos tipos de alarmes, mas que não provê visualização; o MRTG é uma ferramenta para monitoramento SNMP como o Cacti, porém com interface web de configuração e com uma visualização mais simples.

B) o Nagios é uma ferramenta para monitoramento puramente ICMP de redes e serviços, capaz de gerar apenas alertas de falha; o Cacti é uma ferramenta de monitoramento SNMP capaz de gerar alertas de sobrecarga e de visualização simples; o MRTG é uma ferramenta para monitoramento SNMP como o Cacti, porém com interface web de configuração e que usa o RRDTool para exibir os dados monitorados.

C) o Nagios é uma ferramenta para monitoramento puramente SNMP de redes e serviços, capaz de gerar alertas de falha e sobrecarga; o Cacti é uma ferramenta de monitoramento ICMP capaz de gerar alertas de falha e de visualização simples; o MRTG é uma ferramenta para monitoramento SNMP como o Nagios, porém sem interface web de configuração e que usa o RRDTool para exibir os dados monitorados.

D) o Nagios é uma ferramenta para monitoramento ICMP e SNMP de redes e serviços, capaz de gerar apenas alertas de falha; o Cacti é uma ferramenta de monitoramento SNMP que usa o RRDTool para gerar diversos tipos de alarmes, mas que não provê visualização; o MRTG é uma ferramenta para monitoramento SNMP como o Cacti, porém com interface web de configuração e com capacidade para exibir os dados monitorados.

E) o Nagios é uma ferramenta para monitoramento ICMP e SNMP de redes e serviços, capaz de gerar alertas de falha ou de sobrecarga; o Cacti é uma ferramenta de monitoramento SNMP que usa o RRDTool para exibir os dados monitorados; o MRTG é uma ferramenta para monitoramento SNMP como o Cacti, porém sem interface web de configuração e com uma visualização de dados mais simples.

Resolução desta questão na plataforma.