Universidade Federal do Piauí
Centro de Educação Aberta e a Distância

GERÊNCIA DE REDES

José Valdemir dos Reis Junior

Ministério da Educação - MEC
Universidade Aberta do Brasil - UAB
Universidade Federal do Piauí - UFPI
Universidade Aberta do Piauí - UAPI
Centro de Educação Aberta e a Distância - CEAD

Gerência de Redes

José Valdemir dos Reis Junior

UFPI
2012

Apresentação

Segundo Andrew S. Tanenbaum, importante pesquisador e autor de diversos livros técnicos de informática, uma rede de computadores consiste de dois ou mais computadores e outros dispositivos conectados entre si de modo a poderem compartilhar seus serviços, que podem ser: dados, impressoras, mensagens (*e-mails*), etc. A *Internet* é um amplo sistema de comunicação que conecta muitas redes de computadores. Existem várias formas e recursos de vários equipamentos que podem ser interligados e compartilhados, mediante meios de acesso, protocolos e requisitos de segurança.

Desde a década de 70 que a introdução das redes de computadores tem contribuído para facilitar o compartilhamento de dispositivos, periféricos e equipamentos caros como impressoras, dispositivos de armazenamento em massa, modens de alta velocidade, *scanners*, etc.

No entanto, o crescimento natural na quantidade de usuários e o constante surgimento de novas aplicações, cada vez mais complexas, tornaram o compartilhamento de recursos computacionais um aspecto secundário. As redes de computadores passaram a ser compreendidas pelas organizações e empresas como uma ferramenta imprescindível para o aumento de produtividade e para a economia de seus recursos bem como para dar suporte e facilitar a comunicação entre as pessoas.

Com a intensificação da utilização das redes de computadores nas diversas corporações, instituições públicas e privadas o gerenciamento de rede tornou-se indispensável.

Do ponto de vista interno das organizações, é difícil mensurar, com precisão, o impacto que a Tecnologia da Informação (TI) traz sobre a corporação, pois tem se verificado que a infraestrutura de TI tem se tornado uma parte inseparável dos processos e da estrutura da organização, de modo que se torna difícil separar o impacto proporcionado pela TI das demais

atividades da organização. Do ponto de vista histórico, no que corresponde à evolução do uso da tecnologia pelas empresas, pode-se ter alguns parâmetros que revelam um impacto no gerenciamento e adaptações das atividades da empresa perante o uso de recursos tecnológicos, muitas vezes impostos por fatores externos.

A intensa evolução tecnológica no meio empresarial desencadeou um conjunto de consequências. Inicialmente, do ponto de vista corporativo, pode se classificar as consequências desta evolução em dois principais focos: (a) Consequências Externas – as quais variam desde mudanças no hábito dos seus clientes até na própria forma que a empresa se relaciona com seus clientes, parceiros, concorrentes e fornecedores; (b) Internas – que caracterizam o impacto da tecnologia no âmbito interno da empresa como, por exemplo, a necessidade de investimento em capacitação para os funcionários, recursos tecnológicos e de gerenciamento das redes.

Nas redes de computadores, principalmente nas corporativas, é de fundamental importância que a equipe de gerenciamento de rede conheça e compreenda suas principais responsabilidades. Neste contexto pode-se, inicialmente, apresentar algumas perguntas a serem respondidas ao longo desta apostila:

- É de responsabilidade da equipe de rede diagnosticar os problemas no computador do usuário ou é, simplesmente, determinar se o problema do usuário não está relacionado com setor de redes (relacionado à comunicação de dados)?
- A responsabilidade da equipe de rede limita-se apenas até o ponto de conexão, relacionado ao cabeamento horizontal, ou aborda até a placa de rede?
- O problema de rede pode estar ocorrendo em função de cabo rompido ou danificado ou simplesmente é um conector defeituoso ou mal instalado?
- Qual equipamento de rede (por exemplo, um roteador) pode estar gerando um problema em um determinado segmento da rede de computadores?
- Qual a importância do gerenciamento da rede?
- Quais são as melhores práticas para a gerência de redes de computadores?
- A gerência de redes também está relacionada à segurança das informações que trafegam nesta?

Essas respostas são muito importantes para um departamento de

rede e consequentemente para as instituições que dependem dentre outros, do bom funcionamento, da disponibilidade e da segurança destas redes de computadores.

Adicionalmente com a globalização, principalmente das informações, tem-se exigido que a comunicação através dos elementos de rede seja ampliada além da intensa necessidade de que as informações e serviços estejam disponíveis em tempo real, vinte quatro horas durante os sete dias da semana. Neste contexto, faz-se necessária a aplicação de técnicas diversas de gerenciamento de rede capazes de manter o índice de qualidade necessária para a disponibilidade contínua dessas informações.

O gerenciamento de redes envolve o monitoramento (isto é, supervisão) e o controle de recursos distribuídos em redes bem como a identificação e a solução de eventuais falhas. Em essência, o gerenciamento visa garantir certa qualidade de serviços a usuários de redes.

Contudo, é importante mencionar que o gerenciamento de redes de computadores é, essencialmente, uma atividade extensa e complexa o que a impossibilita de ser exercida unicamente pelo esforço humano. O grau de complexidade presente nestas exige o uso de soluções automatizadas nas ferramentas de administração e gerenciamento de redes de computadores.

Deste modo, as ferramentas de administração e gerenciamento de redes acabam sendo importantes artifícios utilizados pelos administradores na execução de suas atividades principais.

Neste contexto, esta apostila apresenta os principais conceitos e terminologias relacionados à administração e o gerenciamento de redes, bem como apresenta as principais metodologias de gerenciamento e uso do sistema e ferramentas para aplicações de gerenciamento de redes.

Esta apostila é baseada em notas de aula do autor nas disciplinas de Redes de Computadores I e II, ministrada no curso Técnico em Informática da Universidade Federal do Piauí, bem como faz referências a livros clássicos de Redes e Gerenciamento de Redes de Computadores, como “Melhores Práticas para Gerência de Redes de Computadores” de Raquel V. Lopes, Jaqueline P. Sauvé e Pedro S. Nicolletti (referência principal), “Planejamento e Gerenciamento de Redes” de Steve Rigney e “Redes de Computadores” de Andrew S. Tanenbaum. Outros materiais que foram levados em consideração na elaboração dessa apostila são publicações de pesquisas e relatórios técnicos sobre ferramentas de gerenciamento de redes, sites especializados, bem como trabalhos de conclusões de pós-graduações, devidamente

referenciados em cada um das unidades descritas a seguir.

Conteúdo desta Apostila

Na Unidade I é apresentado o conceito de gerenciamento de redes, bem como a importância do gerenciamento. Além deste são apresentados os principais componentes dos modelos de redes OSI e TCP/IP, bem como os principais elementos ativos de uma rede de computadores.

Na Unidade II são apresentados os principais problemas relacionados à camada física, enlace, rede e aplicação. Vale ressaltar que os casos aqui apresentados não representam toda a totalidade dos que normalmente acontecem no âmbito das redes de computadores.

Na Unidade III é apresentado o gerenciamento de uma rede TCP/IP que se baseia no protocolo SNMP - *Simple Network Management Protocol*. Apresenta-se à sua arquitetura, componentes e versões dos protocolos e do monitoramento remoto (RMON).

Na Unidade IV é apresentada a gerência de redes baseada no modelo de Referência OSI. Este modelo identificou a gerência OSI como uma importante área de trabalho e forneceu definições iniciais. Serão descritos os seus principais componentes e funcionalidades.

Na Unidade V são apresentadas as principais ferramentas de gerenciamento de redes, tais como: *Nagios, Cacti, Zabixx, NetWare Management System, Open*NMS e NTOP. Adicionalmente, será feito um comparativo entre as principais ferramentas utilizadas.

Sumário

UNIDADE 01

Introdução a Gerência de Redes de Computadores

Resumindo

Na primeira unidade é apresentada uma breve introdução à gerência de redes. Embora existam muitas razões para a administração e o monitoramento de rede, duas razões principiais seriam prever mudanças para crescimento futuro e detectar mudanças inesperadas no *status* da rede. Mudanças inesperadas podem incluir: falha em um roteador ou *switch*, a tentativa de acesso ilegal de um invasor à rede ou a falha de um *link* de comunicação. Sem habilidade de monitorar a rede, um administrador poderá apenas reagir a problemas quando eles acontecerem, ao invés de impedir antecipadamente que eles ocorram.

1 INTRODUÇÃOA GERÊNCIA DE REDES DE COMPUTADORES

As redes de computadores foram concebidas, inicialmente, como meio para compartilhar dispositivos periféricos tais como impressoras, scanners, entre outros, existindo apenas em ambientes acadêmicos, governamentais e algumas empresas de grande porte. Entretanto, a rápida evolução das tecnologias de redes, aliada à grande redução de custos dos recursos computacionais, motivou a proliferação das redes de computadores por todos os segmentos da sociedade.

À medida que essas redes foram crescendo e tornando-se integradas às organizações, o compartilhamento dos dispositivos tomou aspecto secundário em comparação às outras vantagens oferecidas. As redes passaram então a fazer parte do cotidiano das pessoas como uma ferramenta que oferece recursos e serviços que permitem uma maior interação entre os usuários e um consequente aumento de produtividade.

Também ocorreu uma grande mudança nos serviços oferecidos. Além do compartilhamento de recursos, novos serviços, tais como correio eletrônico, transferência de arquivos, Internet, aplicações multimídia, dentre outras, foram acrescentadas, aumentando ainda mais a complexidade das redes. Não bastassem esses fatos, o mundo da interconexão de sistemas ainda passou a conviver com a grande heterogeneidade de padrões, sistemas operacionais, equipamentos etc.

Considerando este quadro, torna-se cada vez mais necessário o gerenciamento do ambiente de redes de computadores para mantê-lo funcionando corretamente. Surge então a necessidade de buscar uma maneira consistente de realizar o gerenciamento de redes para, com isso, manter toda a estrutura funcionando de forma a atender as necessidades dos usuários e às expectativas dos administradores.

Figura 1 - Exemplo de Sala de Gerência de Rede de Computadores

A NECESSIDADE DE GERÊNCIA

O aumento da complexidade das redes de computadores, pelo seu crescimento numérico e pela diversidade dos componentes envolvidos, tem dificultado a atividade de gerência do sistema.

Neste ambiente há dificuldade pela diversidade de formas de controle e monitoração visto que, embora os produtos envolvidos na rede se tornem gradativamente mais inteligentes, cada fornecedor oferece ferramentas próprias de controle para monitorar seus produtos.

Esse cenário exige um grande esforço do administrador da rede, levando a uma busca pela automatização do processo com o objetivo de reduzir ao máximo o esforço humano e, também, prover um método de gerenciamento mais seguro e confiável. O objetivo final é zelar pelo bom funcionamento e desempenho da rede de computadores e seus serviços.

As redes de computadores atuais são compostas por uma grande variedade de dispositivos que devem se comunicar e compartilhar recursos. Na maioria dos casos, a eficiência dos serviços prestados está associada ao bom desempenho dos sistemas da rede. Para gerenciar esses sistemas e as próprias redes, um conjunto eficiente de ferramentas de gerenciamento automatizadas é necessário, sendo fundamental a utilização de técnicas padronizadas para a correta representação e o intercâmbio das informações obtidas.

Figura 2 – Diversos equipamentos envolvidos no gerenciamento

Neste contexto, o gerenciamento de rede pode ser definido como a coordenação (controle de atividades e monitoração de uso) de recursos materiais (modens, roteadores, etc.) e ou lógicos (protocolos), fisicamente distribuídos na rede, assegurando, na medida do possível, confiabilidade, tempos de resposta aceitáveis e segurança das informações.

Pode-se elencar um conjunto de itens que justificam a necessidade gerenciamento, tais como:

- As redes estão ficando cada vez mais importantes para as empresas;
- Não é mais infraestrutura dispensável, é missão crítica;
- As redes são cada vez maiores;
- Atingem mais gente na empresa;
- Atingem mais lugares físicos da empresa;
- Atingem mais parceiros da empresa;
- Atingem até os clientes da empresa;
- As redes são cada vez mais heterogêneas;
- Apresentam uma mistura de tecnologias;
- Apresentam uma mistura de fornecedores de equipamentos e serviços;
- As tecnologias são cada vez mais complexas;

Da mesma forma, um sistema de telecomunicações precisa ser gerenciado. Centrais telefônicas, equipamentos SDH, roteadores, sistema de

rádio enlace, etc. necessitam de monitoramento com o objetivo de alcançar os requisitos de desempenho operacional e de qualidade de serviço, que muitas vezes estão especificados em contratos através de um SLA (Service Level Agreemment).

MODELO CLÁSSICO DO GERENCIAMENTO DE REDE

O modelo clássico de gerenciamento pode ser sumarizado em três etapas:

- Coleta de dados: um processo, em geral automático, que consiste de monitoração sobre os recursos gerenciados;
- Diagnóstico: consiste no tratamento e análise realizados a partir dos dados coletados. O computador de gerenciamento executa uma série de procedimentos (por intermédio de um operador ou não) com o intuito de determinar a causa do problema representado no recurso gerenciado;
- Ação ou controle: Uma vez diagnosticado o problema, cabe uma ação ou controle sobre o recurso, caso o evento não tenha sido passageiro (incidente operacional).

Figura 3 – Modelo Clássico do Gerenciamento de Rede

Um sistema de gerência de rede pode ser considerando como um conjunto de ferramentas que trabalham de forma integrada para permitir o monitoramento e controle, que disponha de interface de controle de dados da rede e que traga informações sobre o status da rede (por exemplo) podendo oferecer ainda um conjunto de comandos que visam executar praticamente todas as atividades de gerenciamento sobre o sistema em questão.

Os modelos de gerência se diferenciam nos aspectos organizacionais envolvendo a disposição dos gerentes na rede, bem como no grau da distribuição das funções de gerência. Cada gerente local de um domínio

pode prover acesso a um gerente responsável (pessoa que interage com o sistema de gerenciamento) local e/ou ser automatizado para executar funções delegadas por um gerente de mais alto nível, geralmente denominado de Centro de Operações da Rede (NOC – *Network Operation Center*). O NOC é responsável por gerenciar os aspectos interdomínios, tal como um enlace que envolva vários domínios ou aspectos específicos de um domínio, devido à inexistência de gerente local.

Na figura a seguir tem-se a representação da arquitetura básica de um sistema de gerenciamento de rede. Cada nó da rede possui uma coleção de *softwares* dedicados à tarefa de gerenciamento da rede.

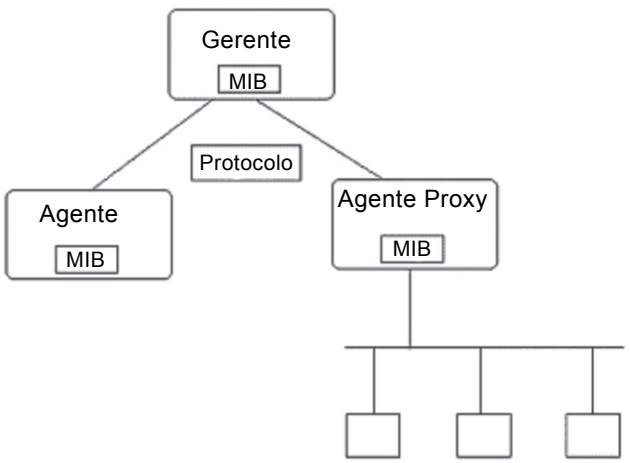

Figura 4 – Arquitetura básica de um sistema de gerenciamento de rede.

Pelo menos um servidor da rede é designado para exercer a função de servidor de gerenciamento da rede. O servidor de gerenciamento da rede possui uma coleção de softwares denominados de *Network Management Application* (NMA). A NMA inclui uma interface de operador para permitir que um usuário autorizado gerencie a rede. A NMA responde aos comandos do operador, mostrando informações e/ou enviando comandos para os agentes através da rede. Essa comunicação é realizada usando um protocolo da camada de aplicação específica para o gerenciamento de redes.

Outros nós que fazem parte do sistema de gerenciamento de rede incluem um módulo agente que responde às solicitações do servidor de gerenciamento. Os agentes são implementados em sistemas finais que

suportam aplicações de usuários finais, bem como em nós que fornecem serviços de comunicação, tais como roteadores e controladores de acesso remoto.

Para manter a alta disponibilidade de gerenciamento, dois ou mais servidores são usados. Em condições normais, um deles é usado para o controle, enquanto os outros ficam coletando estatísticas ou em estado de espera. No caso de falha daquele que está sendo utilizado para controle, outro poderá substituí-lo.

ARQUITETURA DE GERENCIAMENTO DE REDE

A arquitetura geral dos sistemas de gerenciamento de redes apresenta quatro componentes básicos: os elementos gerenciados, as estações de gerência, os protocolos de gerenciamento e as informações de gerência.

Os elementos gerenciados são dotados de um *software* chamado agente, que permite o monitoramento e controle do equipamento através de uma ou mais estações de gerência. A princípio, os principais fabricantes de qualquer dispositivo de rede, (impressoras, roteadores, repetidores, *switches*, etc.) procuram habilitar seus equipamentos para terem um agente instalado.

Dependendo da topologia da rede será necessária uma ou mais estações de gerência para obter informações desses agentes. Um sistema de gerência centralizado deve possuir pelo menos uma estação de gerência e os sistemas distribuídos em duas ou mais estações de gerência.

Nas estações de gerência encontramos o *software* gerente, responsável pela comunicação direta desta estação com os agentes nos elementos gerenciados. Claro que para que aconteça a troca de informações entre o gerente e os agentes é necessário ainda um protocolo de gerência que será o responsável pelas operações de monitoramento e de controle.

Gerentes e agentes podem trocar tipos específicos de informações conhecidas como informações de gerência. Tais informações definem os dados que podem ser utilizados nas operações do protocolo de gerenciamento.

O sistema de gerenciamento de uma rede é integrado e composto por uma coleção de ferramentas para monitorar e controlar seu funcionamento. Uma quantidade mínima de equipamentos separados é necessária, sendo que a maioria dos elementos de *hardware* e *software* para gerenciamento está incorporada aos equipamentos já existentes.

Representado pelo atual ITU-T, o mundo das telecomunicações iniciou em 1985 a definição de um sistema básico de gerenciamento para a indústria do setor.

Juntamente com a definição de um conjunto de informações de gerenciamento, a expressão *Telecommunications Management Network* - TMN foi estabelecida para designar a arquitetura de gerenciamento para a indústria de telecomunicações.

O QUE SE DEVE GERENCIAR?

Como mencionado, um sistema de gerenciamento consiste de alguns itens de hardware e software adicionais, implementados entre os equipamentos de rede existentes.

O software usado para auxiliar o gerenciamento da rede é instalado em servidores, estações e processadores de comunicação, tais como: roteadores, concentradores de acesso e *switches*. Ele é projetado para oferecer uma visão de toda a rede como uma arquitetura unificada, com endereços e rótulos associados a cada ponto da rede e atributos específicos de cada elemento e *link* conhecido do sistema de gerenciamento.

Com o crescimento das redes de computadores, em tamanho e complexidade, sistemas de gerência baseados em um único gerente são inapropriados devido ao volume das informações que devem ser tratadas e que podem pertencer a localizações geograficamente distantes do gerente. Evidencia-se, então, a necessidade da distribuição da gerência na rede, através da divisão das responsabilidades entre gerentes locais que controlem domínios distintos e da expansão das funcionalidades dos agentes.

Dependendo da ênfase atribuída aos investimentos realizados no ambiente de rede, as funções de gerência podem ser centralizadas nos servidores ou distribuídas em diversos ambientes locais.

Como o gerenciamento de rede implica na utilização de várias ferramentas inseridas em uma estrutura, de certa forma complexa, com os limites de atuação definidos, se possível padronizado, entre os componentes envolvidos, é importante definir aspectos como a estratégia que será usada no atendimento dos usuários, atuação do pessoal envolvido nas tarefas de gerenciamento, supridores de serviços, etc.

Os tipos mais básicos de tarefas de gerenciamento de uma rede são: monitoração e controle. A monitoração consiste na observação periódica dos

objetos gerenciados, importantes para a política de gerenciamento. A partir da monitoração, o gerente tem conhecimento do estado da rede e, desta forma, pode efetuar operações de controle sobre a mesma.

A distribuição das funções de monitoramento é ser mais detalhista em relação às funções de controle, pois a monitoração consome mais recursos da rede, bem como a atenção do gerente, pois através dela é que se obtém o estado da rede em relação ao tempo, enquanto que as funções de controle são invocadas em menor número, geralmente com objetivos de alteração de configuração e erradicação de problemas.

O limite de atuação desta gerência, ou seja, o controle deve levar em conta a amplitude desejada pelo modelo implantado na instalação que, além de operar a rede, deve envolver tarefas como:

- Controle de acesso à rede;
- Disponibilidade e desempenho;
- Documentação de configuração;
- Gerência de mudanças;
- Planejamento de capacidade;
- Auxílio ao usuário;
- Gerência de falhas;
- Controle de inventário.

Os benefícios da integração dos sistemas computacionais como forma de distribuir tarefas e compartilhar recursos disponíveis é uma realidade. Junto a esse fato temos o contínuo crescimento em número e diversidade de componentes das redes de computadores que tem contribuído decisivamente para que a atividade de gerenciamento de rede se torne cada vez mais imprescindível.

As grandes redes corporativas, que são inter-redes formadas pela interconexão de pequenas redes locais, assumiram um papel fundamental para os negócios das empresas que delas se utilizam. Por este motivo, estas redes requerem um sistema de gerenciamento eficiente para que as informações da corporação estejam sempre disponíveis no local e no momento onde forem requisitadas.

O crescimento das redes de computadores, juntamente com a integração de serviços como voz, vídeo e dados, introduzem a necessidade de um controle sobre o desempenho dos recursos, tornando-se de vital importância para garantia de qualidade dos serviços prestados. Assim, torna-

se necessário lançar mão de recursos computacionais que proporcionem um gerenciamento mais eficaz e preciso.

Para conseguir gerenciar sistemas eficientemente e planejar inteligentemente um sistema de gerenciamento de redes, o profissional necessita conhecer os conceitos fundamentais e as tecnologias de gerência de redes, tornando possível atingir os seus objetivos, monitorando e controlando os elementos da rede (sejam eles físicos ou lógicos) e assegurando um determinado nível de qualidade dos serviços oferecidos aos usuários.

Concluindo, a gerência de redes está associada não somente ao controle de atividades e ao monitoramento do uso de recursos da rede, como também às necessidades atuais e futuras de toda a infraestrutura da rede, consoante às necessidades estratégicas de seus usuários. As atividades da gerência de redes são complexas e interdependentes, requerendo um fluxo de informações eficaz e contínuo para sua realização.

Alguns administradores de redes comparam a Gerência de Redes com a Medicina na medida em que o gerente de redes pode ser considerado o médico da rede, capaz de tratar as possíveis doenças (diversos problemas apresentados pela rede) que possam surgir.

Os principais objetivos da Gerência de Redes é monitorar e controlar os elementos da rede (sejam eles físicos ou lógicos), assegurando certo nível de qualidade de serviço.

Para viabilizar a realização destas tarefas, os gerentes de redes são geralmente auxiliados por um sistema de gerência de redes. Este sistema pode ser definido como uma coleção de ferramentas integradas para a monitoração e controle da rede, onde oferecem, geralmente, uma interface única, com informações sobre a rede que podem oferecer também um conjunto poderoso e amigável de comandos os quais são usados para executar quase todas as tarefas da gerência da rede

PROTOCOLOS DE GERENCIAMENTO

Desde a década de 1980, vários grupos têm trabalhado para definir arquiteturas padronizadas (e abertas) para o gerenciamento de redes heterogêneas, ou seja, redes compostas por equipamentos de diferentes fabricantes.

As principais arquiteturas abertas de gerenciamento de redes são relacionadas às tecnologias TCP/IP e OSI da ISO e estas são conhecidas

mais facilmente pelos nomes dos protocolos de gerenciamento utilizados: Simple Network Management Protocol (SNMP), do TCP/IP e o Common Management Information Protocol (CMIP), do modelo OSI. Muitos produtos de gerenciamento já foram desenvolvidos obedecendo estes padrões. Por razões históricas, os primeiros produtos seguiram o padrão SNMP e até hoje este é o protocolo que possui o maior número de implementações.

Embora atualmente existam algumas aplicações de gerenciamento muito sofisticadas, a maioria destas aplicações possibilita apenas o monitoramento dos nós de uma rede e não possui "inteligência" para auxiliar os administradores de rede na execução de sua tarefa. Por exemplo, a arquitetura de gerenciamento SNMP, adotada na tecnologia TCP/IP, supõe a existência de estações de gerenciamento, onde são executados as aplicações de gerenciamento e os nós gerenciados, que são os elementos da rede (estações, roteadores e outros equipamentos de comunicação), que desempenham funções de comunicação na operação normal da rede, através dos chamados protocolos úteis. Estes protocolos são instrumentados para permitir o monitoramento e controle do seu funcionamento.

Uma parte significativa do processo de gerenciamento baseia-se na aquisição de informações sobre a rede, sendo as mais importantes àquelas relativas a erros, falhas e outras condições excepcionais. Tais dados devem ser armazenados em forma bruta, sendo importante definir os valores aceitáveis como limiares de tolerância que, quando ultrapassados, determinam uma sinalização para pedir intervenção de um operador ou o início de uma operação corretiva.

Tais limites não são necessariamente absolutos, tais como a taxa de erros num enlace de dados, sendo necessário dispor de estatísticas de erros em função do tráfego existente. Um determinado limiar pode ser aceitável numa situação de carga leve na rede, mas intolerável numa outra situação, de carga mais intensa, no qual o número de retransmissões faria com que o tráfego total excedesse a capacidade do enlace, afetando seriamente o tempo de resposta.

A gerência em redes de computadores torna-se tarefa complexa em boa parte por consequência do crescimento acelerado das mesmas, tanto em desempenho, quanto em suporte a um grande conjunto de serviços. Além disso, os sistemas de telecomunicações, parte importante e componente das redes, também adicionam maior complexidade, estando cada vez mais presentes, mesmo em pequenas instalações.

Para resolver os problemas associados à gerência em redes a ISO, através do modelo de referência OSI, propôs as estruturas: Modelo Organizacional, Modelo Informacional, Modelo Funcional e de Comunicação.

PRINCIPAIS COMPONENTES ATIVOS DE REDES

Se o sistema de cabeamento são as artérias e veias de sua rede, os componentes de rede ativos são o coração. Sozinho, o sistema de cabeamento é apenas uma fiação inativa. Os componentes de rede ativos trazem aquela fiação à vida, colocando-lhe dados e permitindo que várias partes da rede se comuniquem entre si.

Para uma boa gerência de redes é primordial o conhecimento dos principais elementos da rede bem como suas funcionalidades, descritas a seguir.

Placas de Redes

A placa de rede é o hardware que permite aos micros conversarem entre sí através da rede. Sua função é controlar todo o envio e recebimento de dados através da rede. Cada arquitetura de rede exige um tipo específico de placa de rede; você jamais poderá usar uma placa de rede *Token Ring* em uma rede *Ethernet*, pois ela simplesmente não conseguirá comunicar-se com as demais.

Além da arquitetura usada, as placas de rede à venda no mercado diferenciam-se também pela taxa de transmissão, cabos de rede suportados e barramento utilizado.

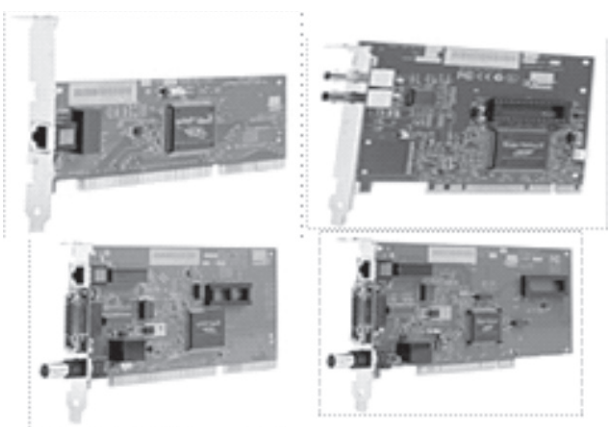

Figura 5 – Placas de rede

Estações de Trabalho ou Clientes (*Hosts*)

São as estações de trabalho dos clientes, geralmente destinada aos usuários finais.

Repetidores

Dispositivo que opera apenas na camada física recebendo um sinal de entrada, regenerando-o e enviando para a porta de saída. Com o objetivo de manter a inteligibilidade dos dados, o repetidor é um regenerador de sinais (não um amplificador), pois refaz os sinais originais (deformados pela atenuação/ruído) tentando anular a interferência do ruído. Por definição, não efetua nenhum tipo de filtragem.

Hubs

Um hub consiste num repetidor multiportas, ou seja, ao receber a informação de uma porta, ele distribui por todas as outras. Com um hub é possível fazer uma conexão física entre diversos computadores com a topologia estrela. Assim, um Hub permite apenas que os utilizadores compartilhem *Ethernet* e todos os nós do segmento *Ethernet* irão partilhar o mesmo domínio de colisão.

Um domínio simples de colisão consiste em um ou mais *Hubs* Ethernet e nós conectados entre eles. Cada aparelho dentro do domínio de colisão partilha a banda de rede disponível com os outros aparelhos no mesmo domínio. *Switches* e *Bridges* são utilizados para separar domínios de colisão que são demasiado grandes de forma a melhorar a performance e a estabilidade da rede.

Ponte (Bridge)

Este dispositivo trabalha na camada física e na camada de enlace, agregando a função de verificar o MAC address, endereço física da placa de rede, da estação que receberá o quadro (*frame*). Com a bridge é possível fazer uma filtragem de entrega, pois ao verificar o MAC *address*, ela determina que interface receba o *frame* enviado.

O ideal é que as estações não tomem conhecimento da existência da

bridge para que as configurações de rede se tornem mais simples.

Switchs

No mercado de telecomunicações é possível adquirir *switches* industriais gerenciáveis (*managed*) e os *switches* não-gerenciáveis (*unmanaged*), numa aplicação do tipo industrial em que os parâmetros deverão ser analisados em tempo real (real time) deveremos especificar os *switches* gerenciáveis.

Figura 6 – Exemplo de um Switch com 24 portas

Nos switches gerenciáveis poderemos através de inúmeras funções terem um controle do gerenciamento dos pacotes, informações trocadas entre os equipamentos do chão de fábrica. Cada porta singular poderá ser analisada, dados recebidos e enviados, erros, otimizando assim a largura de banda da devida aplicação. Sendo assim, quando adquirir um switch industrial gerenciável, seu custo será mais elevado quando comparado a um switch não-gerenciável, visto a enorme diversidade de funções de controle de um switch gerenciável.

Roteadores

Geralmente, é um equipamento utilizado para fazer a comutação de protocolos, a comunicação entre diferentes redes. Ele também provê a comunicação entre computadores. O roteador deve escolhe a melhor rota por onde irão passar as informações de um ponto a outro.

São considerados equipamentos extremamente variáveis se quantificarmos as funcionalidades adicionais que pode ser agregada ao equipamento. Por exemplo:

- Possui frequentemente uma grande variedade de interfaces *LAN* (rede local) e *WAN* (para longo alcance);

• Normalmente, dão suporte a uma variedade de protocolos de roteamento, tais como *Border Gateway Protocol* (BGP), *Intermediate System-to-Intermediate System* (IS-IS), *Open Shortest Path First* (OSPF), etc.;
• Normalmente, dão suporte a diversos protocolos de multicast, tais como PIM, IGMP, CGMP, DVMRP, etc.;
• São frequentemente multiprotocolo (conseguem rotear tráfego de vários protocolos de rede, tais como IP, IPX, etc.);
• Frequentemente incluem um filtro de pacotes (ou até um *firewall* completo), permitindo estabelecer regras de segurança sobre que tipo de tráfego pode ser roteado pelo equipamento;
• Devido a sua criticalidade, roteadores frequentemente possuem recursos especiais para aumentar a disponibilidade da rede ou melhorar a manutenibilidade. Exemplos de tais recursos incluem suporte ao *Hot Standby Routing Protocol* (HSRP), módulo redundante (módulos de processamento, fontes de alimentação, ventiladores, etc.) e hot swappable;
• Podem ter recursos especiais para priorizar o tráfego roteado ou, de forma geral, dividir os recursos disponíveis, principalmente, a banda passante dos enlaces, entre várias classes de tráfego. Podemos chamar esses recursos de "Orientados à Qualidade de Serviço" Esses recursos incluem *Weighted Fair*
• *Queuing* (WFQ) e roteamento baseado em políticas administrativas (*Policy Based Routing*);
• Suporte a uma vasta gama de recursos e protocolos adicionais tais como: MPLS, VPN, tunelamento GRE;
• Suporte à gerência via protocolo SNMP.

Servidores

O uso das redes de computadores se dá em grande parte entre clientes e servidores, onde estes estabelecem uma conexão para a troca das informações desejadas. Estas informações percorrem as diversas redes que os separam, e somente o cliente e o servidor deveria ter acesso às informações trafegadas. Este tipo de comunicação é chamado de unicast. Este tipo de tráfego domina quase a totalidade dos tráfegos das redes locais.

Porém, em algumas circunstâncias, o cliente precisa descobrir quem

é o servidor ou como encontrá-lo. Como nestas situações ele não sabe como encontrá-lo, ele envia quadros para todos os computadores do seu segmento e aguarda uma resposta. Esta situação também ocorre quando um computador recém-ligado deseja acesso à rede. O computador envia, neste caso, uma requisição de endereço IP para todos os computadores do seu segmento. Aquele computador que tiver como atender a requisição vai responder diretamente para o solicitante. Este tipo de comunicação, o qual um computador envia um quadro para todos os computadores do mesmo segmento é chamado de Broadcast.

PADRÕES DO MODELO DE REFERÊNCIA OSI DA ISO E TCP/IP

No modelo tradicional, as redes são compostas por múltiplos componentes. Além das máquinas em que as aplicações estão efetivamente executando, roteadores, pontes (*bridges*), *gateways* e *modens* são componentes importantes. No tocante ao *software*, vários outros componentes estão envolvidos, especialmente em ambientes multifornecedores e, em alguns casos, seria extremamente confortável que componentes de software pudessem ser gerenciados. A tarefa de gerenciamento deve, então, ser resolvida por uma combinação entre entidades chamadas de gerentes e agentes.

O código de um agente é constituído por uma função de gerenciamento - contadores, rotinas de teste, temporizadores, etc. - que permite o controle e gerenciamento do objeto gerenciado. Já a instrumentação de gerenciamento está tipicamente associada a uma estrutura particular de gerenciamento, que especifica as regras empregadas para definir a informação referente a um objeto referenciado, assim que este possa ser monitorado e gerenciado.

A ISO especifica o CMIPi e o CMIS (*Commom Management Information Services*) como protocolo e serviço de gerenciamento de rede do nível de aplicação do modelo OSI.

A utilização dos padrões da ISO para gerenciamento tem sido ampliada (além dos méritos técnicos) em boa parte pela OSF, que está comprometida, através do OSF/DME (*Open Software Foundation/Distributed Management Environment*), em suportar os padrões OSI de gerenciamento.

A necessidade de mecanismos de gerenciamento nas redes baseadas em TCP/IP é atendida pelo SNMP (*Simple Network Management Protocol*) em associação com o esquema de MIB (*Management Information Base*), que

também é suportado pelo padrão OSF/DME. Uma das vantagens do SNMP é a simplicidade e facilidade de implementação, e com isso a grande maioria dos problemas de gerenciamento de rede podem ser contornados com TCP/IP

No gerenciamento SNMP, é adicionado um componente ao hardware (ou software) que estará sendo controlado que recebe o nome de agente. Este agente é encarregado de coletar os dados dos dispositivos e armazená-los em uma estrutura padrão (denominada MIB, como mencionado anteriormente e que será vista em detalhes na Unidade III). Além desta base de dados, normalmente é desenvolvido um *software* aplicativo com a habilidade de sumarizar estas informações e exibi-las nas estações encarregadas das tarefas de monitorar a rede.

Os pioneiros na implantação dos protocolos SNMP foram os fornecedores de *gateways*, pontes (*bridges*) e roteadores. Normalmente, o fornecedor desenvolve o agente SNMP e posteriormente desenvolve uma interface para a estação gerente da rede. Em geral, estes produtos funcionam para vários sistemas operacionais, como VMS, SUN-OS, DOS e outros, e é muito comum que estes fornecedores incluam bibliotecas e utilitários que permitam a criação de aplicações de gerenciamento com características específicas para alguns componentes da rede.

As implementações básicas do SNMP permitem monitorar e isolar falhas, já as aplicações mais sofisticadas permitem gerenciar o desempenho e a configuração da rede. Estas aplicações, em geral, incorporam menus e alarmes para facilitar a interação com o profissional que está gerenciando a rede.

O esquema dos produtos desenvolvidos com o protocolo SNMP é um pouco diferente dos produtos que utilizam o protocolo CMIP. Os fornecedores de produtos que utilizam o protocolo CMIP pressupõem que os fabricantes possuam algum tipo de gerenciamento em seus equipamentos, portanto estas informações podem ser disponibilizadas para um integrador via protocolo CMIP. O conceito de integrador foi definido em três níveis: o mais baixo, que contém os agentes e os elementos gerenciadores, o intermediário, que consiste em elementos do sistema de gerenciamento, e finalmente, o nível mais alto, que consiste no integrador dos sistemas de gerenciamento.

A dificuldade maior para uma aplicação integradora é que os fornecedores não têm as mesmas variáveis de gerenciamento e as mesmas operações em seus servidores de objetos.

A escolha entre um ou outro protocolo de gerenciamento deve recair sobre o tipo de rede e dos produtos a ela agregados, sendo que podem ser mesclados os dois protocolos.

O SNMP e seu *Internet Standard Network Management Framework* são adequados a agentes simples e fáceis de implementar, enquanto o CMIP e o seu *framework Network Management Forum Release* 1.0 são adequados para agentes com um ou mais servidores de objetos dentro da modalidade cliente-servidor orientado para objeto, dentre os quais incluem-se o RPC.

EXERCÍCIOS

1 - Defina o que é gerenciamento de redes. O que se deve Gerenciar? Exemplifique.

2 - Qual a importância e áreas de atuação da gerencia de redes?

3 - Detalhe quais são os principais elementos ativos de rede. Qual a diferença entre *Hub e Switch*? O que é um domínio de colisão?

4 - Quais os principais elementos nas arquiteturas de gerenciamento? Descreva e elenque uma de aplicação de cada um destes elementos.

5 - Comente sobre os padrões do modelo de referência OSI da ISO e TCP/IP.

WEB-BIBLIOGRAFIA

http://www.intragov.sp.gov.br/manuais/Manual%20de%20Gerenciamento%20e%20Monitoramento%20da%20Rede%20v1%20(04.12.07).pdf

http://www.gta.ufrj.br/~alexszt/ger/snmpcmip.html

http://www.projetoderedes.com.br/artigos/artigo_gerenciamento_de_redes_de_computadores.php

http://www.teleco.com.br/tutoriais/tutorialmodelotmn/pagina_1.asp

[http://www.malima.com.br/article_read.asp?id=52]

http://andredeo.blogspot.com/2010/09/conceitos-de-gerencia-de-redes_30.html

[http://im.ufba.br/pub/MATA67/TrabalhosSemestre20081/Monografia_Jeronimo_Bezerra.pdf

http://www.shitsuka.net/materialdidatico/cisco/Ap_FundRd3.pdf

UNIDADE 02

Problemas mais comuns nas redes de computadores

Resumindo

Nesta unidade serão apresentados os principais problemas das redes de computadores relacionados à camada física, de enlace, de rede e de aplicação. Vale ressaltar que os casos aqui apresentados não representam a totalidade dos problemas que normalmente acontecem no âmbito das redes de computadores. Um material excelente que serviu de base para esta unidade é o livro de "Melhores Práticas para Gerência de Redes de Computadores" de Raquel V. Lopes, Jaqueline P. Sauvé e Pedro S. Nicolletti.

2 PROBLEMAS MAIS COMUNS NAS REDES DE COMPUTADORES

Problemas de rede podem aparecer e exigir consertos diretamente, como um cabo com conector frouxo ou uma configuração errada de um roteador. Sintomas de rede lenta, por exemplo, não é necessariamente um problema, pois não se conserta a lentidão da rede de modo direto. Rede lenta pode ser considerada um sintoma de um problema. Possivelmente, ao consertar o problema, os sintomas não mais devem ser percebidos.

Com base nesta afirmação, antes do administrador da rede dominar e conhecer as técnicas de gerenciamento faz-se necessário conhecer os principais problemas que podem ocorrer na rede e para tal propor a melhor alternativa para contornar o devido problema.

OS PRINCIPAIS PROBLEMAS DAS REDES DE COMPUTADORES RELACIONADAS À CAMADA FÍSICA

Nos seguintes subtópicos são apresentados os principais problemas que podem ocorrer em uma rede relacionada à camada física: cabo rompido ou danificado, conectores defeituosos ou instalado erroneamente, equipamento de interconexão defeituoso, placa de rede ou porta de equipamento de interconexão defeituosa.

Cabo rompido ou danificado

A maioria dos enlaces de clientes nas redes de computadores é formada por três componentes de *hardware*: uma placa de rede no cliente, uma porta em um equipamento de interconexão e um cabo conectando os dois primeiros componentes. Um cabo de rede, portanto, interliga dois ou mais componentes da rede. O rompimento de um cabo, consequentemente,

impossibilita a comunicação entre os dispositivos da rede interligados por ele. Da mesma forma, cabos de redes danificados dificultam a comunicação entre os equipamentos unidos por ele.

Dentre os principais tipos de cabos de redes destacam-se os cabos de pares trancados e as fibras ópticas. No caso dos primeiros, podem ter sua capacidade de transmissão prejudicada devido a torções, curvas muito acentuadas e nós apertados, pois estas formas de disposição do cabo alteram sua geometria. As alterações na geometria do cabo podem causar prejuízos permanentes cuja gravidade depende da categoria do cabeamento utilizada. Quanto ao segundo, pode-se afirmar que são muito mais sensíveis, quando flexionados além de certo limite sofrem pequenas fraturas, que não são visíveis externamente. Estas causam uma maior perda de sinais no enlace. Curvas mais fechadas ou os impactos fortes podem quebrar a fibra completamente. O processo de tração ou torção excessiva da fibra durante a instalação também podem causar o seu rompimento.

Figura 7 – Exemplo de cabos. À esquerda cabo par trançado e à direita cabos de fibras ópticas

Como os fios de fibra são muito finos, é possível incluir um grande volume deles em um cabo de tamanho modesto, o que é uma grande vantagem sobre os fios de cobre, o caso dos pares trançado. Como a capacidade de transmissão de cada fio de fibra é bem maior que a de cada fio de cobre e eles precisam de um volume muito menor de circuitos de apoio, como repetidores, usar fibra em *links* de longa distância acaba saindo mais barato. Outra vantagem é que os cabos de fibra são imunes a interferência eletromagnética, já que transmitem luz e não sinais elétricos, o que permite que sejam usados mesmo em ambientes onde o uso de fios de cobre é problemático.

Criar *links* de longa distância cavando valas ou usando cabos submarinos é muito caro, sendo normal usar um volume de cabos muito maior que o necessário. Os cabos adicionais são chamados de fibra escura

(*dark fiber*) ou fibras apagadas, não por causa da cor, mas pelo fato de não serem usadas. Elas ficam disponíveis para expansões futuras e substituição de cabos rompidos ou danificados. Quando ouvir falar em padrões "para fibras escuras", tenha em mente que são justamente padrões de transmissão adaptados para uso de fibras antigas ou de baixa qualidade, que estão disponíveis como sobras de instalações anteriores.

Uma notícia veiculada por John Ribeiro (2008), editor do IDG *News Service*, relata um caso de rompimento de uma destes cabos bem como suas consequências, leia:

> O *Flag Telecom Group* enviará, na próxima semana, um navio próximo a Alexandria, no Egito, onde a âncora de um navio rompeu um cabo de rede submarino, revelou o grupo nesta sexta-feira (01/02/ 2008). O rompimento deste cabo e de outro do consórcio de empresas SEA-ME-WE4 gerou quedas de conexão e problemas nas telecomunicações em algumas áreas do Oriente Médio e da Índia na quarta-feira (30/01/2008).
>
> Mesmo com a nova rota de tráfego estabelecida para contornar o problema, o tempo de resposta em chamadas telefônicas de longa distância aumentou e as conexões no Reino Unido e na Costa Leste dos Estados Unidos ficaram lentas, revelou o presidente da Associação de Provedores de Serviços de Internet da Índia, Rajesh Chharia. O governo da Índia anunciou na quinta-feira (31/01) que os provedores indianos, incluindo integrantes do consórcio dono do cabo, estão em contato com a Telecom Egypt para se certificar do conserto. Reparos em cabos de fibra óptica submarinos costumam levar 15 dias, mas o Ministro das Comunicações da Índia espera que a conexão seja restabelecida em 10 dias. Outro cabo submarino de internet, o Falcon, também do Flag Telecom, foi rompido nesta sexta-feira (01/02/08), a 56 quilômetros de Dubai, revelou o grupo. Um navio para reparo deve chegar ao local nos próximos dias.

Logo, se conclui que cabos de fibra ótica quebrados completamente não possibilitam a passagem de sinais de uma extremidade à outra, inibindo o funcionamento da rede. As microfraturas tornam a rede lenta, uma vez que causam um aumento significativo na quantidade de erros na rede.

E quanto aos pares trançados, com geometria alterada, verifica-se que podem ocasionar a falta ou instabilidade na conectividade e ainda conexões mais lentas.

Conectores defeituosos ou instalados erroneamente

Considerando que um conector é uma peça responsável pela ligação entre o cabo de rede e o equipamento de interconexão ou hospedeiro, verifica-se que é possível que conectores mal instalados ou defeituosos possam ser a causa de problemas na rede que, em primeira análise, podem ter aparência de mais complexos.

Problemas em conectores do tipo RJ-45, utilizados em cabos de pares trançados, são os mais comuns. As causas são diversas: a crimpagem, nome dado ao processo de conexão dos cabos ao conector, pode ter sido mal feita, os quais podem existir pares separados, etc.

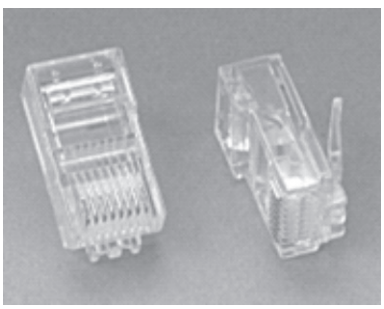

Figura 8 – Exemplo de conector do tipo RJ-45

Detalhando os fios responsáveis pelo processo de transmissão e recepção nos cabos pares trancados verifica-se que existem 4 pares de fios condutores. Os fios de cada par estão trançados entre si para tentar reduzir a interferência elétrica entre os fios condutores. Ou seja, o fio 1 está trançado com o 2, o 3 com o 4 e assim, sucessivamente.

Quando cabos de pares trançados são utilizados para transmissão de dados apenas os fios 1, 2, 3 e 6 são utilizados. Para evitar a interferência troca-se, em cada extremidade do cabo, a posição do fio 4 com o fio 6.

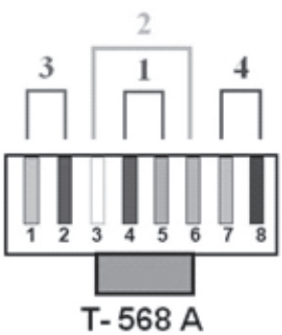

Figura 9 – Exemplo da sequência de cabos para o padrão T-568-A

Para testar o cabo par trançado após a crimpagem nos conectores de rede recomenda-se utilizar os testadores de cabos disponíveis no mercado, vide:

Figura 10– Exemplo de equipamento para teste de cabo de rede

Normalmente, esses testadores são compostos de duas unidades independentes. A vantagem disso é que o cabo pode ser testado no próprio local onde fica instalado, muitas vezes com as extremidades localizadas em recintos distintos. Denominaremos os dois componentes do testador: um de testador e o outro de terminador. Uma das extremidades do cabo deve ser ligada ao testador, no qual pressionamos o botão Liga/Desliga (ON/OFF). O terminador deve ser levado até o local onde está a outra extremidade do cabo, e nele encaixamos o outro conector RJ-45.

Uma vez estando pressionado o botão ON/OFF no testador, um LED (diodo emissor de luz) irá piscar. No terminador, quatro LEDs piscarão em sequência, indicando que cada um dos quatro pares está corretamente ligado. Observe que este testador não é capaz de distinguir ligações erradas quando são feitas de forma idêntica nas duas extremidades. Por exemplo, se o fio azul e verde for ligado em posições invertidas em ambas as extremidades do cabo, o terminador apresentará os LEDs piscando na sequência normal. Cabe ao usuário ou técnico que monta o cabo conferir se os fios em cada conector estão ligados nas posições corretas.

Equipamento de Interconexão Defeituoso

Equipamentos de interconexão, tais como roteadores, switchs, pontes podem deixar de realizar sua tarefa e não mais ser capaz de interconectar

dispositivos dentre as redes. É possível que equipamentos que costumavam funcionar normalmente, de repente, passem a apresentar um comportamento atípico.

Muitas vezes, os equipamentos que aparentam estar com defeito, após uma reinicialização, desligar e ligar novamente podem voltar a restabelecer sua operação normal. Estas instabilidades podem ser causadas, por exemplo, por oscilações de energia ou erros de programação do sistema operacional do equipamento que não foram tratados pelo fabricante.

Uma avaliação inicial pode ser feita ao analisar os LEDs indicativos do equipamento, pois o manual pode informar que o LED *status* sempre deve estar aceso na cor verde. Por exemplo, se ele tiver piscando e apresentar cor laranja é sinal de que muitos quadros/pacotes estão sendo descartados devido a erros, ou se ficar vermelho é sinal de que existe um problema grave no equipamento, etc.

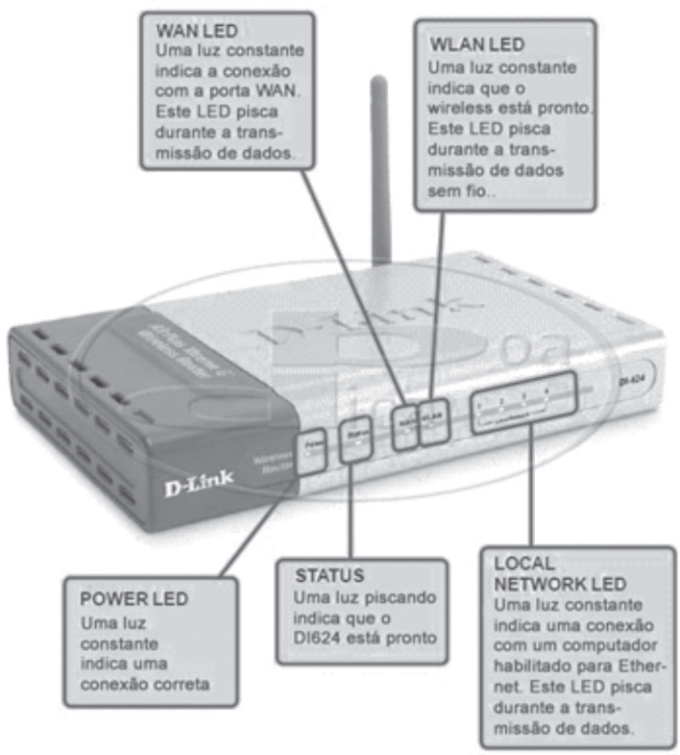

Figura 11– Explicação das luzes de um roteador do modelo D-LINK

Muitas vezes, solucionamos problemas em equipamentos simplesmente reiniciando-os. Se após a reinicialização, o problema persistir, a sugestão é estudar os manuais do equipamento em busca de dicas para

este problema ou entrar em contanto com a assistência técnica especializada.

Problemas em equipamentos de rede que requeiram sua reinicialização não devem ser observados frequentemente para o mesmo equipamento.

Por precaução, recomenda-se ter sempre equipamentos de reserva (repetidores, comutadores, roteadores, conversores, etc.) para substituir equipamentos danificados enquanto são submetidos à manutenção.

Placa de Rede ou Porta de Equipamento de Interconexão defeituosa

Uma placa de rede que não está funcionando apropriadamente pode ser a causa de falta de conectividade ou de rede lenta.

Alguns exemplos de defeitos em placas de rede *Ethernet* são: a placa não consegue ouvir a portadora (*Carrier sense*) apropriadamente, causando um número excessivo de colisões, inclusive colisões tardias; a placa começa a gerar quadros inúteis. Dentre os quadros inúteis gerados, coincidentemente, pode haver tráfego de *broadcast/multicast* (tráfego para todas as máquinas da rede e para um grupo de máquinas respectivamente), que, em excesso, satura os processadores dos equipamentos de rede, os quais devem processar todos os quadros de broadcast recebidos, causando a lentidão da rede.

Interfaces de equipamentos de alguns equipamentos de interconexão (portas de repetidores, comutadores e roteadores) também podem apresentar defeitos e causar os mesmos sinais e efeitos de placas de rede defeituosas.

OS PRINCIPAIS PROBLEMAS DAS REDES DE COMPUTADORES RELACIONADAS À CAMADA DE ENLACE

Nestes subtópicos são apresentados alguns problemas que podem ocorrer em uma rede relacionada à camada de enlace: Interface desabilitada, Saturação de recursos devido ao excesso de quadros de difusão, Tempo de envelhecimento de tabelas de endereços inadequados.

Interface Desabilitada

A partir de uma estação de gerência, por exemplo, é possível desabilitar administrativamente uma interface de um equipamento de interconexão que dê suporte a atividade gerenciamento. Com isso, uma interface ficará inativa

até que ela seja novamente habilitada. Tal procedimento só é possível em equipamentos que suportem as funcionalidades de gerenciamento, dentre elas o controle por portas ou interfaces de conexão.

Uma das utilidades deste procedimento é para que os gerentes da rede desabilitem interfaces que não estão sendo utilizadas no momento para evitar que usuários realizem modificações topológicas sem o conhecimento da equipe de gerência. Ao desabilitar interfaces que não estão em uso você impede que usuários introduzam novas máquinas ou equipamentos de interconexão, por exemplo, ou passem a utilizar portas que não estão sendo monitoradas.

Deve-se controlar esta prática, pois pode gerar confusão. Por exemplo, o gerente pode esquecer que as interfaces vagas estão desativadas. Ele pode adicionar novas máquinas e esquecer habilitá-las novamente. Para os desavisados, talvez haja perda de tempo tentando descobrir porque a rede não funciona para a nova máquina antes de lembrar-se de habilitar a interface. Outro caso é quando a equipe de gerência venha a ser alterada e os novos integrantes não sabem que as portas vagas estão desabilitadas.

É um problema relativamente simples, mas quando a rede está funcionando, ninguém se lembra de olhar se a interface está ou não habilitada.

Ao decidir que as interfaces que não estão sendo utilizadas devem ficar administrativamente desabilitadas para evitar problemas, é recomendado que os cabos de rede estejam devidamente identificados, como descrito em e que a documentação da rede seja suficiente para a detecção de mudanças realizadas por usuários.

Saturação de recursos devido a excesso de quadros de difusão

Um quadro de difusão é endereçado a todas as estações que participam do mesmo domínio de difusão do emitente. Muitos protocolos de rede e aplicações em uma rede local dependem do envio de quadros de difusão para funcionar apropriadamente, por exemplo, o DHCP.

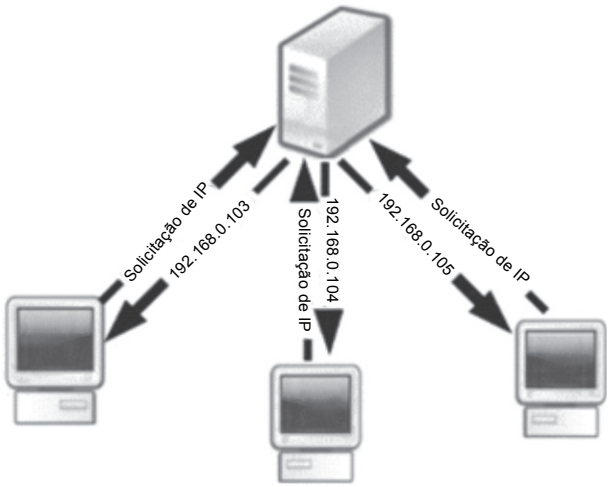

Figura 12– Funcionamento do servidor DHCP

Um excesso de quadros de difusão ocorre quando um grande número de quadros de difusão está trafegando na rede. Em um domínio de difusão, quanto maior o número de estações e a quantidade de protocolos e aplicações que dependem do envio de quadros de difusão, maior a quantidade desses quadros e maior a probabilidade da ocorrência do excesso de quadros de difusão.

Normalmente, com os dados atuais, uma máquina envia em média um quadro de difusão a cada 10 segundos. Considerando um domínio de difusão com 1600 máquinas, por exemplo, seria normal um tráfego de difusão em torno de 160 quadros por segundo. Quando este número cresce para milhares de quadros de difusão por segundo, uma tempestade de quadros de difusão está ocorrendo. Os equipamentos com processadores mais atualizados conseguem processar alguns milhares de quadros de difusão por segundo sem comprometer o desempenho da rede.

Para amenizar o problema, recomenda-se utilizar comutadores, como switchs, que possuem a funcionalidade de suprimir o tráfego de difusão. Eles podem ser configurados para aceitar uma determinada quantidade de quadros de difusão por segundo e descartar os demais quadros. Importante para o gerenciamento da rede é observar se a quantidade de quadros estabelecidos está sendo constantemente alcançado.

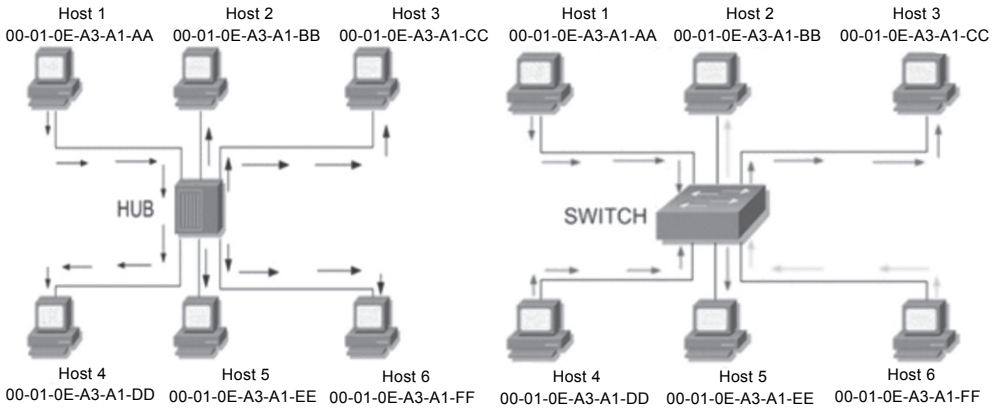

Figura 13 – Diferença entre *Hub e Switchs* (domínio de colisão)

Uma rede montada apenas com repetidores forma um único domínio de colisão. Com um grande acréscimo no número de computadores querendo conversar no meio compartilhado, a probabilidade de colisão aumenta até inviabilizar o uso da rede.

Tempo de envelhecimento de tabelas de endereços inadequado

Um comutador mantém uma tabela, denominada tabela de endereços que informa através de qual de suas portas uma máquina (identificada pelo seu endereço físico) pode ser alcançada. Esta tabela inicia-se vazia, e à medida que as máquinas se comunicam através do comutador, ela vai sendo preenchida, através de uma técnica chamada backward learning. Ou seja, ao receber um quadro na porta P com endereço origem Eo e endereço destino Ed, o comutador, embora talvez não saiba como alcançar o destino Ed, sabe que a origem Eo é alcançada pela porta P (já que o quadro veio de lá). Portanto, o comutador coloca o par (Eo, P) na tabela de encaminhamento. Num momento futuro, quando chegar um quadro endereçado a Eo, o comutador o encaminhará diretamente à porta P sem usar uma flooding (enchete de quadros).

Detalhadamente, cada entrada na tabela de endereços informa à porta que dá acesso a certa máquina da rede. Quando o comutador recebe um quadro de uma máquina, a entrada correspondente na tabela de endereços é atualizada. Se uma maquina da rede não se comunica através do comutador durante certo tempo (chamado tempo de envelhecimento), a entrada na tabela de endereços correspondente à máquina em questão é retirada.

Ao receber um quadro destinado a certo endereço físico, o comutador

procurará em sua tabela de endereços através de que porta o quadro deverá ser enviado. Se não encontrar esta informação na tabela de endereços, o quadro será enviado para todas as portas do comutador.

No caso de uma rede comutada com muitas máquinas, quando o tempo de envelhecimento configurado em um comutador for muito pequeno, enchentes serão realizadas com bastante frequência, gastando largura de banda da rede desnecessariamente. Já quando o tempo de envelhecimento for muito grande, as entradas na tabela de endereços podem se tornar obsoletas. Por conseguinte, algumas máquinas podem ficar incomunicável por certo período de tempo, até que a tabela de endereços seja reajustada. A tabela de endereços é ajustada quando a máquina que sofreu modificação se comunica através do comutador ou quando acaba o tempo de envelhecimento. Veja o exemplo de uma tabela de roteamento na Figura 14.

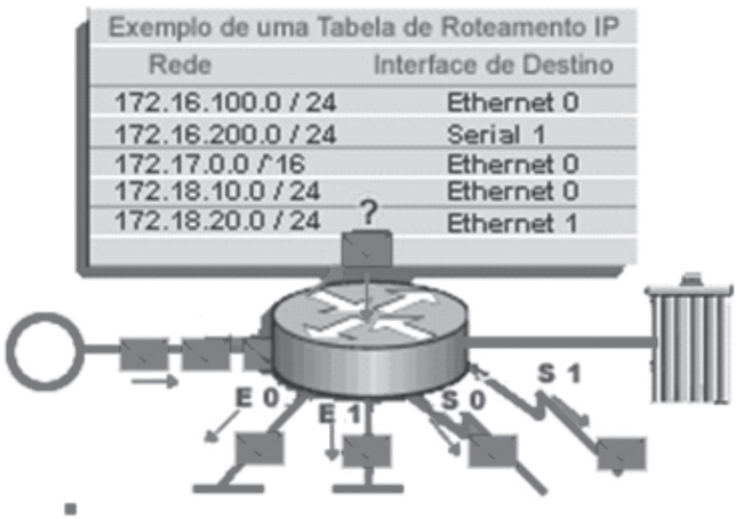

Figura: 14 – Exemplo de uma tabela de Roteamento

OS PRINCIPAIS PROBLEMAS DAS REDES DE COMPUTADORES RELACIONADAS À CAMADA DE REDE

Neste tópico são apresentados alguns problemas que podem ocorrer em uma rede relacionada à camada de rede, tais como: Tabela de rotas de hospedeiros incorretas e cliente DNS mal configurado.

Tabela de rotas de hospedeiros incorretas

Estatiscamente ou dinamicamente, um roteador padrão deve ser configurado em máquinas clientes, geralmente denominado gateway da rede. Quando o hospedeiro deseja se comunicar com outra máquina que não faz parte de sua rede local (não tem mesmo prefixo e máscara de rede que ele), os dados desta comunicação devem ser entregues ao este roteador.

Se o mesmo estiver sendo configurado manualmente, erros de digitação podem ocorrer e causar o problema. Pode-se ainda, equivocadamente, não configurar o roteador padrão de um hospedeiro, o que também é bastante problemático.

Se o roteador padrão estiver sendo configurado dinamicamente, através de um servidor DHCP, a configuração do escopo no servidor pode estar incorreta, causando o problema. Veja figura a seguir.

Figura 15 – Propriedades para configuração do endereço IP e DNS, respectivamente

Quando a tabela de rotas de uma máquina cliente estiver com rota padrão incorreta ou inexistente, a consequência para os usuários é que só haverá conectividade com máquinas da mesma subrede. Os usuários de máquinas com este problema apresentarão o problema para o administrador da rede, geralmente relatando que a rede só funciona internamente, que eles não conseguem navegar em sites fora da organização.

Cliente DNS mal configurado

Considerado um dos mais importantes serviços existentes na Internet, o DNS (*Domain Name Service*) ou Serviço de nome de domínio ou ainda, Servidor de nome de domínio é de fundamental importância para a facilidade no acesso as páginas da internet.

Quando usamos o browser para navegar, e ao consultar os inúmeros sites, vemo-nos sempre clicando na barra de endereços do mesmo e digitando algo como www.ufpi.br. Como após alguns segundos este site é exibido em nossa máquina, onde ele está fisicamente, como ele sabe que alguém fez uma solicitação pra que ele fosse exibido.

Ao digitar o endereço no *browser*, o mesmo se encarrega de iniciar um trabalho para que esse nome possa ser traduzido (resolvido) em um número IP. Os responsáveis por essa tradução são os servidores DNS. Este serviço não só atua apenas quando digitamos algo do tipo www. Há outros serviços em que o trabalho de um DNS é fundamental. O envio de mensagens eletrônicas (*e-mail*) e a transferência de arquivos na Internet (FTP) são outros exemplos.

Quando o endereço do servidor de nomes não é especificado ou está incorreto, o serviço de nomes não funcionará para a máquina em questão. Como grande parte dos serviços de rede é acessada através de nomes de máquinas, o usuário da máquina com configuração de cliente DNS incorreta não conseguirá acessar vários serviços de rede.

OS PRINCIPAIS PROBLEMAS DAS REDES DE COMPUTADORES RELACIONADAS À CAMADA DE APLICAÇÃO

Nos subtópicos seguintes serão abordados os principais problemas das redes de computadores relacionados à camada de aplicação, tais como: O Tempo de Vida (TTL) de uma zona DNS não está configurado e filtro IP barrando tráfego DNS.

Tempo de Vida (TTL) de uma zona DNS não está configurado

Considere, por exemplo, os servidores de nomes do domínio ufpi.br e do domínio cnpq.com. Eles serão denominados aqui de ns.ufpi.br e ns.cnpq.com. Quando um usuário do domínio ufpi.br deseja visitar a página www.

cnpq.com, o servidor de nomes ns.ufpi.br é consultado: “ns.ufpi.br, qual é o endereço IP correspondente ao nome www.cnpq.com?”. Como ns.ufpi.br não sabe resolver este nome localmente e esta resolução também não se encontra em sua cache, memória adotada para armazenamento, ele consulta um dos servidores na hierarquia superior a sua ou seja a raiz (root) configurado em seu arquivo de busca.

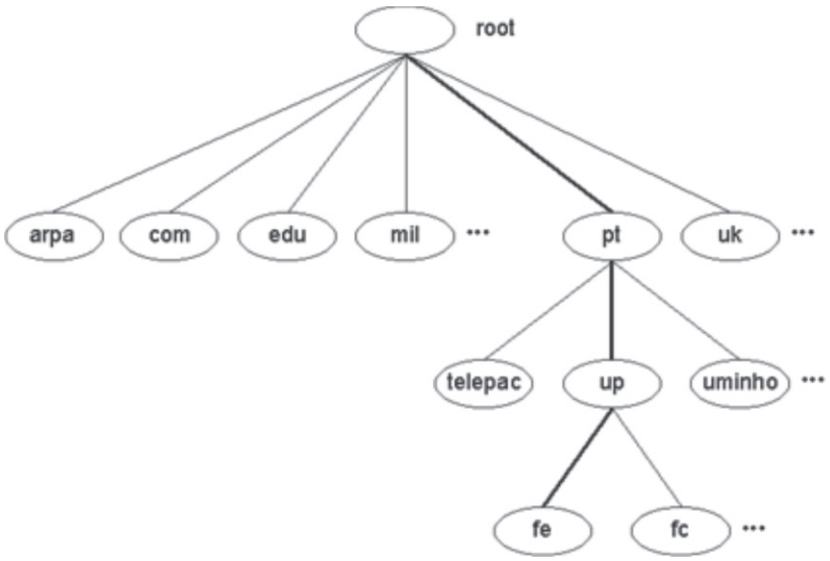

Figura16 – Exemplo da hierarquia nos servidores de DNS

O servidor raiz também não sabe quem é www.cnpq.com, mas ele sabe quem é o servidor do domínio.com e fornece esta informação para ns.ufpi.br, que em seguida, consulta um dos servidores ns.com. Este servidor informa a ns.ufpi.br que não sabe quem é www.cnpq.com, mas sabe quem é o servidor do domínio cnpq.com. Ao consultar ns.cnpq.com, o servidor de nomes ns.ufpi.br pode obter uma resposta positiva ou uma resposta negativa.

Em caso de resposta positiva, ns.cnpq.com informa para ns.ufpi.br o endereço IP de www.cnpq.com e informa também por quanto tempo esta informação pode ser utilizada com segurança por ns.ufpi.br. A este tempo dá-se o nome de Tempo de Vida (TTL) *default*. O servidor ns.ufpi.br irá armazenar esta resolução positiva em uma cache durante o tempo correspondente ao TTL default fornecido. Durante este tempo, sempre que um cliente do servidor ns.ufpi.br consultá-lo para resolver o nome www.cnpq.com, o servidor utilizará a informação que está em sua cache.

Quando o servidor de nomes interno estiver sem a configuração do TTL default, os usuários podem reclamar que não conseguem acessar os serviços locais, mas conseguem acessar a Internet e quando o servidor de nomes externo está com este problema, usuários externos à organização podem reclamar que os serviços oferecidos pela sua organização não estão funcionando, por exemplo, não conseguiriam acessar a página do cnpq.com.

Filtro IP barrando tráfego DNS

Um filtro pode estar barrando o tráfego entre seu servidor DNS e os clientes DNS deste servidor, entre servidor primário e servidores secundários ou entre servidores DNS internos de sua organização e servidores DNS que não pertencem a sua organização. O primeiro caso é bastante raro, pois não é comum que exista um filtro IP entre os clientes DNS e o servidor destes clientes. Mas, se existir e não estiver permitindo a passagem do tráfego DNS, o resultado drástico: os clientes DNS não conseguirão se comunicar com o servidor e nenhum nome será resolvido para os clientes.

Servidores secundários precisam se comunicar com os servidores primários de tempos em tempos em busca de modificações nos arquivos de zonas. Se modificações foram realizadas no servidor primário, uma transferência das zonas modificadas é feita. Além disso, alguns servidores DNS estão configurados para notificar os servidores secundários quando modificações em zonas forem realizadas. Se um filtro IP barra a comunicação entre servidores primários e secundários, os secundários não conseguirão se comunicar com o primário e após algum tempo deixarão de ter autoridade para resolver nomes do domínio que não pode ser atualizado, até que a comunicação seja novamente possível.

EXERCÍCIOS

1 - Qual a importância do conhecimento dos principais problemas que ocorrem em redes para o seu administrador? Há como prevê-los e antecipar soluções?

2 - Comente sobre pelo menos 6 (seis) dos principais problemas das Redes de Computadores relacionadas à Camada Física? Faça pesquisas complementares.

3 - Comente sobre pelo menos 7 (sete) dos principais problemas das Redes de Computadores relacionadas à Camada de Enlace?
4 - Comente sobre pelo menos 4 (quatro) dos principais problemas das Redes de Computadores relacionadas à Camada de Rede?
5 - Comente sobre pelo menos 6 (seis) dos principais problemas das Redes de Computadores Relacionadas à Camada de Aplicação?

WEB-BIBLIOGRAFIA

http://www.malima.com.br/article_read.asp?id=51
http://imasters.com.br/artigo/2660/cisco/roteamento_e_distance_vector_parte_01/
http://www.marceloeiras.com.br/linux/tutorial/dns/dns.htm

UNIDADE 03

Gerência de Redes TCP/IP

Resumindo

Nesta unidade é apresentado o modelo de gerenciamento de redes baseado no TCP/IP, incluindo as especificações do protocolo Simple Network Management Protocol - SNMP, nas versões 1, 2 e 3, como suas principais operações e mensagens disponibilizadas pelos agentes e gerentes do sistema de gerenciamento. O sistema de monitoramento remoto RMON, a estrutura de gerenciamento da informação e a base de informações gerenciais também são apresentadas.

3 GERENCIAMENTO DE ENTRADA E SAÍDA

MODELO DE GERÊNCIA TCP/IP

Com a disseminação das redes de computadores necessitou-se a monitoração e controle do universo de dispositivos e recursos que compõem as redes de comunicação.

Atualmente, as redes de computadores e os seus recursos associados, além das aplicações distribuídas, tem se tornado fundamental e de tal importância para uma organização que elas basicamente “não podem parar/falhar”. Ou seja, o nível de falhas e de degradação de desempenho considerado aceitáveis está cada vez mais reduzido, sendo este nível igual ate a zero, dependendo da importância da rede para uma instituição.

Um breve histórico da evolução da gerência de redes nas ultimas décadas até os dias atuais:

1970: Os computadores eram centralizados, com terminais conectados a mainframes em baixa velocidade de transmissão. O gerenciamento era inexistente ou quando muito fornecido pelos fabricantes de mainframes.

1980: Com o surgimento das redes locais de computadores, aumentou-se a velocidade das conexões. Surgiram os primeiros sistemas de gerenciamento voltados para redes distribuídas.

1990: Com o advento da *Internet*, o gerenciamento passa a ser feito através de Navegador *Web*, acompanhando o avanço da tecnologia de interconexão de redes como ATM e *Frame Relay* das redes de longa distância.

Hoje: O aumento do grau de complexidade das redes e do seu tamanho exige o emprego de sistema de gerenciamento que proporcionem qualidade de serviço, proatividade, integração com processo de serviços e negócios.

Considerando que esses equipamentos não podem falhar nunca

ou que o seu nível de falhas seja reduzido juntamente com a perda de informações e a degradação do desempenho a monitoração e controle desses processos são feito por meio de ferramentas que auxiliam os profissionais tanto na identificação dos problemas quanto na orientação para as soluções dos mesmos.

As principais arquiteturas abertas de gerenciamento de redes são relacionadas às tecnologias TCP/IP e OSI da ISO e estas são conhecidas mais facilmente pelos nomes dos protocolos de gerenciamento utilizados: *Simple Network Management Protocol* (SNMP), do TCP/IP e o *Common Management Information Protocol* (CMIP), do modelo OSI. Muitos produtos de gerenciamento já foram desenvolvidos obedecendo estes padrões. Por razões históricas, os primeiros produtos seguiram o padrão SNMP e até hoje é o protocolo que possui o maior número de implementações.

ARQUITETURA DE GERENCIAMENTO TCP/IP

No modelo de gerência de redes baseado em TCP/IP temos uma arquitetura de gerenciamento composta por uma ou mais estações de gerenciamento, agente de gerenciamento, base de informações gerenciais (MIB) e o protocolo de gerenciamento de redes.

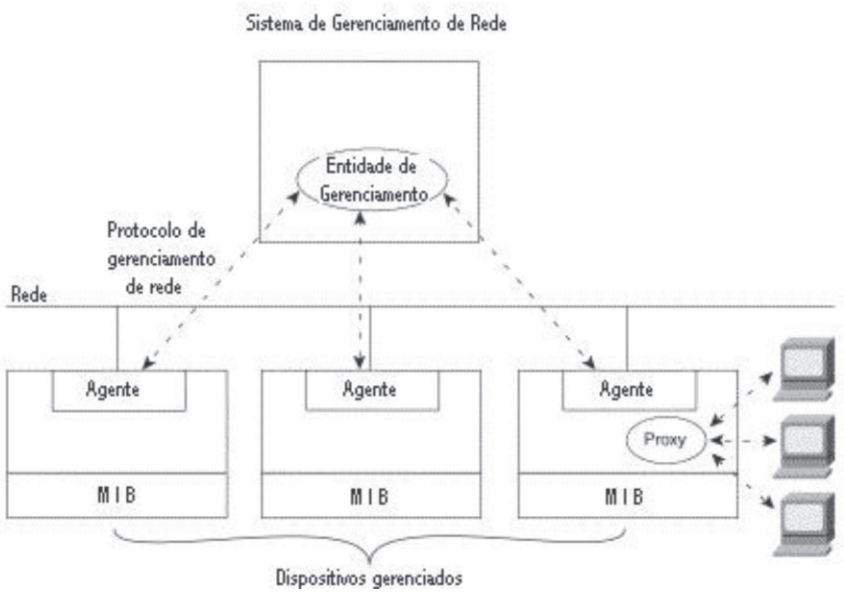

Figura 17 – Modelo de gerência de redes

Uma estação de gerenciamento é um meio de acesso que servirá como interface de comunicação para o gerente humano em um sistema de gerenciamento de rede.

Já o agente de gerenciamento é o responsável pela comunicação com a estação de gerenciamento e fornece informações assíncronas importantes que não foram requisitadas por esta estação.

O que será gerenciado, sejam recursos ou não, será representado como objetos e a sua coleção é conhecida como MIB (Base de informações gerenciais).

O SNMP (*Simple NetworkManagement Protocol*) é o protocolo de gerência recomendado para o gerenciamento de redes TCP/IP, definido à nível de aplicação, utilizando os serviços do protocolo de transporte UDP(*User Datagram Protocol*) para enviar suas mensagens através da rede. Sua especificação está contida no RFC 1157. Este protocolo é o centro do desenvolvimento do gerenciamento SNMP.

O AGENTE

É um processo executado na máquina gerenciada, responsável pela manutenção das informações de gerência da máquina. As funções principais de um agente são:

• Atender as requisições enviadas pelo gerente;

• Enviar automaticamente informações de gerenciamento ao gerente, quando previamente programado;

O agente utiliza as chamadas de sistema para realizar o monitoramento das informações da máquina e utiliza as RPC (*Remote Procedure Call*) para o controle das informações da máquina.

GERENTE

É um programa executado em uma estação servidora que permite a obtenção e o envio de informações de gerenciamento junto aos dispositivos gerenciados mediante a comunicação com um ou mais agentes.

O gerente fica responsável pelo monitoramento, relatórios e decisões na ocorrência de problemas enquanto que o agente fica responsável pelas funções de envio e alteração das informações e também pela notificação da ocorrência de eventos específicos ao gerente.

PROTOCOLO SNMP

Este protocolo tem como premissa à flexibilidade e a facilidade de implementação, também em relação aos produtos futuros. Sua especificação está contida no RFC 1157.

O SNMP é um protocolo de gerência definido ao nível de aplicação, é utilizado para obter informações de servidores SNMP - agentes espalhados em uma rede baseada na pilha de protocolos TCP/IP. Os dados são obtidos através de requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte UDP - *User Datagram Protocol* para enviar e receber suas mensagens através da rede. Dentre as variáveis que podem ser requisitadas utilizaremos as MIBs podendo fazer parte da MIB II, da experimental ou da privada.

O gerenciamento da rede através do SNMP permite o acompanhamento simples e fácil do estado, em tempo real da rede, podendo ser utilizado para gerenciar diferentes tipos de sistemas.

Este gerenciamento é conhecido como modelo de gerenciamento SNMP ou simplesmente gerenciamento SNMP. Por tanto, o SNMP é o nome do protocolo no qual as informações são trocadas entre a MIB e a aplicação de gerência como também é o nome deste modelo de gerência.

Os comandos são limitados e baseados no mecanismo de busca/alteração. No mecanismo de busca/alteração estão disponíveis as operações de alteração de um valor de um objeto, de obtenção dos valores de um objeto e suas variações.

A utilização de um número limitado de operações, baseadas em um mecanismo de busca/alteração, torna o protocolo de fácil implementação, sendo simples, estável e flexível. Como consequência reduz o tráfego de mensagens de gerenciamento através da rede e permite a introdução de novas características.

O funcionamento do SNMP é baseado em dois dispositivos: o agente e o gerente. Cada máquina gerenciada é vista como um conjunto de variáveis que representam informações referentes ao seu estado atual, as quais ficam disponíveis ao gerente através de consulta e podem ser alteradas por ele. Cada máquina gerenciada pelo SNMP deve possuir um agente e uma base de informações MIB.

Os agentes se comunicam com os gerentes através de um protocolo de gerenciamento de redes ao nível de aplicações, que utiliza a arquitetura

de comunicação da rede. Protocolos de gerenciamento de redes descrevem um formato para o envio de informações de gerenciamento.

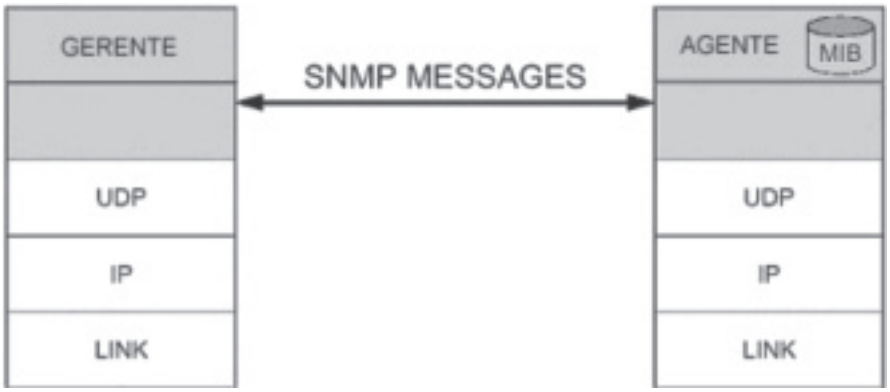

Figura 18 – Modelo de gerência de redes

Para que seja possível a comunicação entre um gerente e um agente, é necessário que ambos compartilhem o mesmo esquema conceitual de informações. O gerente deve ter então uma visão conceitual dos elementos gerenciados que o agente interage.

O sucesso do SNMP baseia-se no fato de ter sido ele o primeiro protocolo de gerenciamento não proprietário, público, fácil de ser implementado e que possibilita o gerenciamento efetivo de ambientes heterogêneos. Geralmente, estes produtos de gerenciamento de redes incorporam funções gráficas para o operador de centro de controle.

No gerenciamento SNMP, é adicionado um componente ao *hardware* (ou *software*) que estará sendo controlado que recebe o nome de agente. Este agente é encarregado de coletar os dados dos dispositivos e armazená-los em uma estrutura padrão. Além desta base de dados, normalmente é desenvolvido um software aplicativo com a habilidade de sumarizar estas informações e exibi-las nas estações encarregadas das tarefas de monitorar a rede.

Basicamente, são definidos quatro tipos de MIBs: MIB I, MIB II, MIB experimental e MIB privada.

Os pioneiros na implantação dos protocolos SNMP foram os fornecedores de gateways, bridges e roteadores. Normalmente, o fornecedor desenvolve o agente SNMP e posteriormente desenvolve uma interface para a estação gerente da rede.

As implementações básicas do SNMP permitem monitorar e isolar

falhas, já as aplicações mais sofisticadas permitem gerenciar o desempenho e a configuração da rede. Estas aplicações, em geral, incorporam menus e alarmes para facilitar a interação com o profissional que está gerenciando a rede.

Informações úteis para o monitoramento de redes são coletadas e armazenadas por agentes e disponibilizadas para um ou mais gerentes.

São utilizadas duas técnicas para disponibilizar tais informações: polling e event report (relato de eventos ou notificações).

- Polling: é uma interação do tipo pergunta– reposta entre gerente e agente. É utilizada para se obter periodicamente informações armazenadas nas MIBs associadas aos agentes pelos gerentes.
- Relato de Eventos: é uma interação em que agentes enviam informações a gerentes. O gerente aguarda até que tais informações cheguem.

Operações do Protocolo SNMP

Existem duas operações básicas (*SET e GET*) e suas derivações (*GET-NEXT, TRAP*).

- A operação SET é utilizada para alterar o valor da variável; o gerente solicita que o agente faça uma alteração no valor da variável;
- A operação GET é utilizada para ler o valor da variável; o gerente solicita que o agente obtenha o valor da variável;
- A operação de GET-NEXT é utilizada para ler o valor da próxima variável; o gerente fornece o nome de uma variável e o cliente obtém o valor e o nome da próxima variável; também é utilizado para obter valores e nomes de variáveis de uma tabela de tamanho desconhecido;
- A operação TRAP é utilizada para comunicar um evento; o agente comunica ao gerente o acontecimento de um evento, previamente determinado. São sete tipos básicos de TRAP determinados:

- *coldStar*t: a entidade que a envia foi reinicializada, indicando que a configuração do agente ou a implementação pode ter sido alterada;
- *warmStart*: a entidade que a envia foi reinicializada, porém a configuração do agente e a implementação não foram alteradas;
- *linkDown*: o enlace de comunicação foi interrompido;
- *linkUp*: o enlace de comunicação foi estabelecido;
- *authenticationFailure*: o agente recebeu uma mensagem SNMP do

gerente que não foi autenticada;

- *egpNeighborLoss*: um par EGP parou;
- *enterpriseSpecific*: indica a ocorrência de uma operação TRAP não básica.

Mensagem no Protocolo SNMP

Uma mensagem SNMP deve definir o servidor o qual vai obter ou alterar os atributos dos objetos e que será o responsável pela conversão das operações requisitadas em operações sobre a MIB. Após verificar os campos de uma mensagem, o servidor deve utilizar as estruturas internas disponíveis para interpretar a mensagem e enviar a resposta da operação ao cliente que a solicitou.

As mensagens no protocolo SNMP não possuem campos fixos e por isso são construídas de trás para frente.

A mensagem possui três partes principais: *version, community*, SNMP PDU:

- A version contém a versão do SNMP. Tanto o gerente como o agente devem utilizar a mesma versão. Mensagens contendo versões diferentes são descartadas.
- A *community* identifica a comunidade. Ela é utilizada para permitir acesso do gerente as MIBs;
- A SNMP PDU é a parte dos dados, possui PDU (*Protocol Data Units*) que são constituídas ou por um pedido ou por uma resposta a um pedido.

Existem cinco tipos de PDUs: *GetRequest, GetNextRequest, GetResponse, SetRequest e Trap*.

SNMPv2

O SNMPv2 foi desenvolvido com base nas especificações do Secure SNMP e do SMP *Simple Management Protocol*) . Seu propósito era remover muitas das deficiências do SNMP e aumentar sua aplicabilidade para incluir redes baseadas no modelo OSI bem como no modelo TCP/IP. Contudo, só as duas primeiras deficiências citadas acima foram solucionadas por esta versão.

SNMPv3

É uma versão do SNMP que apresenta uma proposta de solução para o problema de segurança encontrado nas versões anteriores do protocolo. As propriedades de segurança abordadas são:

- Autenticação: Permite a um agente verificar se uma solicitação está vinda de um gerente autorizado e observar a integridade do seu conteúdo.
- Criptografar: Permite gerentes e agentes a criptografarem mensagens para evitar invasão de terceiros
- Controle de Acesso: Torna possível configurar agentes para oferecerem diferentes níveis de acesso a diferentes gerentes.

RMON

O protocolo SNMP não é adequado para ambientes de redes corporativas e constituído de diversas redes locais conectadas através de outra de longa distância. Esses enlaces de rede de longa distância, por operarem as taxas de transmissão inferiores às *LAN*s que a interconectam, passam a ter grande parte da sua banda de transmissão ocupada para informações de gerenciamento. Uma solução encontrada para dirimir este problema foi o *Remote MONitoring* (RMON).

RMON é uma capacidade de gerenciamento remoto do SNMP. A especificação RMON é uma definição de uma MIB. Seu objetivo, contudo, é definir padrões de monitoração e interfaces para a comunicação entre agentes/gerentes SNMP.

RMON dá ao gerente da rede a habilidade para monitorar subredes como um todo, ao invés de apenas dispositivos individuais na subrede.

O protocolo 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 monitorar remotamente. Cada elemento RMON tem como tarefas: coletar, analisar, tratar, filtrar informações de gerenciamento da rede e apenas notificar à estação gerente os eventos significativos e situações de erro.

No caso de existirem múltiplos gerentes, cada elemento RMON deve determinar quais informações de gerenciamento devem ser encaminhados

para cada gerente.

Sendo assim, os objetivos do protocolo RMON são:

• Reduzir a quantidade de informações trocadas entre a rede local gerenciada e a estação gerente conectada a uma rede local remota;

• Possibilitar o gerenciamento contínuo de segmentos de redes locais, mesmo quando a comunicação entre o elemento RMON e a estação gerente estiver temporariamente interrompida.

• Permitir o gerenciamento pró-ativo da rede, diagnosticando e registrando eventos que possibilitem detectar o mau funcionamento e prever falhas que interrompam sua operação.

• Detectar, registrar e informar à estação gerente condições de erro e eventos significativos da rede.

• Enviar informações de gerenciamento para múltiplas estações gerentes, permitindo, no caso de situações críticas de operação da rede gerenciada, que a causa da falha ou mau funcionamento da rede possa ser diagnosticada a partir de mais de uma estação gerente.

Dois padrões básicos de protocolo RMON são especificados: RMON1 e RMON2, funcionalmente complementares.

RMON1

O RMON1 opera somente na camada *Media Access Control* (MAC) oferecendo recursos ao administrador da rede para monitorar o tráfego e coletar informações e estatísticas da operação de um segmento de rede local, além de realizar o diagnóstico remoto de falhas e erros ocorridos no segmento de rede a partir de funcionalidades de um analisador de protocolo suportadas pelo correspondente elemento RMON.

Porém, o fato do RMON1 só trabalhar na camada MAC, significa que este somente apresenta estatísticas para tráfego agregado – porém não apresenta estatísticas para camadas diferentes de várias pilhas de protocolos (ex: IP, FTP, IPX). Isto também significa que, por não serem capazes de monitorar a camada de rede, os dispositivos RMON1 não distingue o tráfego originado através de um roteador, o que é uma grande deficiência.

RMON2

O RMON2, por sua vez, opera no nível da camada de rede e camadas superiores, complementando, portanto o RMON1, possibilitando coletar informações estatísticas e monitorar a comunicação fim-a-fim e o tráfego gerado por diferentes tipos de aplicação.

ESTRUTURA DE INFORMAÇÃO – SMI

As regras de construção das estruturas da MIB são descritas através da SMI - Structure of Management Information. A SMI define com exatidão como os objetos gerenciados são nomeados e especifica os respectivos tipos de dados associados.

Os objetos são organizados em uma hierarquia em árvore e são reconhecidos por um OID (*object identifier*). Essa estrutura é base do esquema de atribuição de nomes do SNMP.

Um OID de objeto é formado por uma sequência de inteiros baseada nos nós das árvores, separada por pontos (.). Por exemplo, o objeto internet pode ser referenciado como isso.org.dod.internet ou 1.3.6.1 como é mostrado na árvore de objetos da SMI.

BASE DE INFORMAÇÕES DE GERÊNCIA – MIB

Antes de conhecer a definição do que é uma MIB, será apresentado o conceito de objetos gerenciados.

Um objeto gerenciado é a visão abstrata de um recurso real do sistema. Assim, todos os recursos da rede que devem ser gerenciados são modelados e as estruturas dos dados resultantes são os objetos gerenciados. Os objetos gerenciados podem ter permissões para serem lidos ou alterados, sendo que cada leitura representará o estado real do recurso e cada alteração também será refletida no próprio recurso.

Dessa forma, a MIB é o conjunto dos objetos gerenciados que procura abranger todas as informações necessárias para a gerência da rede.

O RFC - *Request For Comment* 1066 apresentou a primeira versão da MIB, a MIB I. Este padrão explicou e definiu a base de informação necessária para monitorar e controlar redes baseadas na pilha de protocolos TCP/IP. A evolução aconteceu com o RFC 1213 que propôs uma segunda MIB, a MIB

II, para uso baseado na pilha de protocolos TCP/IP.

Basicamente, são definidos três tipos de MIBs: MIB II, MIB experimental, MIB privada. A MIB II, que é considerada uma evolução da MIB I, fornece informações gerais de gerenciamento sobre um determinado equipamento gerenciado. Através das MIB II podemos obter informações como: número de pacotes transmitidos, estado da interface, entre outras. A MIB experimental é aquela em que seus componentes (objetos) estão em fase de desenvolvimento e teste, em geral, eles fornecem características mais específicas sobre a tecnologia dos meios de transmissão e equipamentos empregados. MIB privada é aquela em que seus componentes fornecem informações específicas dos equipamentos gerenciados, como configuração, colisões e também é possível reinicializar, desabilitar uma ou mais portas de um roteador.

A árvore hierárquica abaixo foi definida pela ISSO. Representa a estrutura lógica da MIB e mostra o identificador e nome de cada objeto.

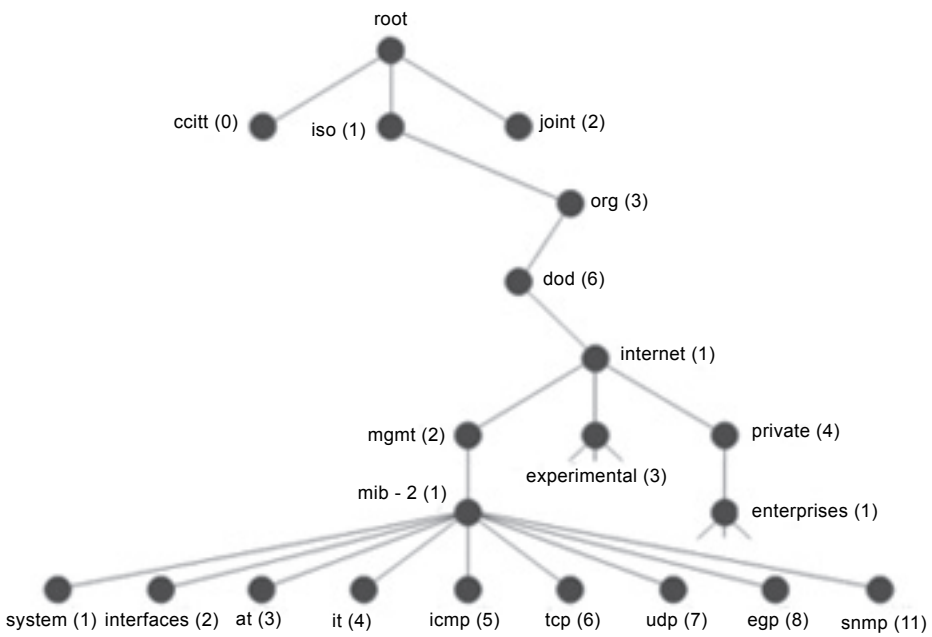

Figura 19 – A árvore hierárquica para a MIB definida pelo ISSO

O nó raiz da árvore não possui rótulo, mas possui pelo menos três subníveis, sendo eles:

- nó 0 que é administrado pela Consultative Committe for International Telegraph and Telephone - CCITT;
- nó 1 que é administrado pela International Organization for

Standartization - ISO;

• o nó 2 que é administrado em conjunto pela CCITT e pela ISO. Sob o nó ISO fica o nó que pode ser utilizado por outras instituições: o org (3), abaixo dele fica o dod (6) que pertence ao departamento de defesa dos EUA. O departamento de defesa dos EUA alocou um subnó para a comunidade internet, que é administrado pela International *Activities Board* - IAB e abaixo deste nó temos, entre outros, os nós: *management*, experimental, *private*.

Sob o nó management ficam as informações de gerenciamento. É sob este nó que está o nó da MIB II.

Sob o nó experimental estão as MIBs experimentais.

Sob o nó private fica o nó enterprises e sob este nó ficam os nós das indústrias de equipamentos.

As regras de construção das estruturas da MIB são descritas através da SMI – *Structure of Management Information*. A estrutura de informações de gerência SMI é um conjunto de documentos que definem:

• Forma de identificação e agrupamento das informações;

• Sintaxes permitidas;

• Tipos de dados permitidos.

Os objetos de uma MIB são especificados de acordo com a ASN.1 - *Abstract Syntax Notation One*. A notação sintática abstrata é uma forma de descrição abstrata dos dados com o objetivo de não se levar em consideração a estrutura e restrições do equipamento no qual está sendo implementada. Para cada objeto são definidos: nome, identificador, sintaxe, definição e acesso. As instâncias do objeto são chamadas de variáveis.

• O *Object Name* é o nome do objeto que é composto por uma string de texto curto.

• O *Object Identifier* é o identificador do objeto e é formado por números que são separados por pontos.

A *Sintax*, sintaxe do objeto, descreve o formato ou o valor da informação. Ela pode ser:

• Uma sintaxe do tipo simples, que pode ser um inteiro, uma string de octetos, um *Object Identifier* ou nulo;

• Pode ser também uma sintaxe de aplicação, o qual pode ser um endereço de rede, um contador, uma medida, um intervalo de tempo ou incompreensível.

A definição é uma descrição textual do objeto.

O acesso é o tipo de controle que se pode ter sobre o objeto, podendo ser: somente leitura, leitura e escrita ou não acessível.

Como exemplo de um objeto citaremos o *ipInReceives* do grupo IP:

ipInReceives Object Type

Object Identifier: 1.3.6.1.2.1.4.3

Access: read-only

*Syntax: Counter*32

Description: O número total de datagramas que chegam às interfaces, incluindo aquelas com erros.

MIB II

Abaixo da subárvore MIB II estão os objetos usados para obter informações específicas dos dispositivos da rede. Por exemplo:

Figura 20 – Exemplo da localização do objeto SysDescr

Alguns dos objetos pertencentes aos grupos da MIB II são:

Grupo *System* (1.3.6.1.2.1.1)

• *sysDescr* (1.3.6.1.2.1.1.1): Descrição textual da unidade. Pode incluir o nome e a versão do *hardware*, sistema operacional e o programa de rede.

• *sysUpTime* (1.3.6.1.2.1.1.3): Tempo decorrido (em milhares de segundos) desde a última reinicialização do gerenciamento do sistema na rede.

• *sysContact* (1.3.6.1.2.1.1.4): Texto de identificação do gerente da máquina gerenciada e como contatá-lo.

Grupo *Interfaces* (1.3.6.1.2.1.2)

• *ifNumber* (1.3.6.1.2.1.2.1): Número de interfaces de rede (não importando seu atual estado) presentes neste sistema.

• *ifOperStatus* (1.3.6.1.2.1.2.2.1.8): Estado atual da interface.

• *ifInOctets* (1.3.6.1.2.1.2.2.1.10): Número total de octetos recebidos pela interface.

Grupo IP (1.3.6.1.2.1.4)

• *ipForwarding* (1.3.6.1.2.1.4.1): Indica se esta entidade é um *gateway*.

• *ipInReceives* (1.3.6.1.2.1.4.3): Número total de datagramas recebidos pelas interfaces, incluindo os recebidos com erros.

• *ipInHdrErrors* (1.3.6.1.2.1.4.4): Número de datagramas que foram recebidos e descartados devido aos erros no cabeçalho IP.

Grupo ICMP (1.3.6.1.2.1.5)

• *icmpInMsgs* (1.3.6.1.2.1.5.1): Número total de mensagens ICMP recebidas por esta entidade. Incluindo aquelas com erros.

• *icmpOutMsgs* (1.3.6.1.2.1.5.14): Número total de mensagens ICMP enviadas por esta entidade. Incluindo aquelas com erros.

Grupo TCP (1.3.6.1.2.1.6)

• *tcpMaxConn*(1.3.6.2.1.6.4): Número máximo de conexões TCP que esta entidade pode suportar.
• *tcpCurrentEstab* (1.3.6.2.1.6.9): Número de conexões TCP que estão como estabelecidas ou a espera de fechamento.
• *tcpRetransSegs* (1.3.6.2.1.6.12): Número total de segmentos retransmitidos.

Grupo UDP (1.3.6.1.2.1.7)

• *udpInDatagrams* (1.3.6.1.2.1.7.1): Número total de datagramas UDP entregues aos usuários UDP.
• *udpNoPorts* (1.3.6.1.2.1.7.2): Número total de datagramas UDP recebidos para os quais não existia aplicação na referida porta.
• *udpLocalPort* (1.3.6.1.2.1.7.5.1.2): Número da porta do usuário UDP local.

Grupo SNMP (1.3.6.1.2.1.11)

• *snmpInPkts* (1.3.6.1.2.1.11.1): Número total de mensagens recebidas pela entidade SNMP.
• *snmpOutPkts* (1.3.6.1.2.1.11.2): Número total de mensagens enviadas pela entidade SNMP.
• *snmpInTotalReqVars* (1.3.6.1.2.1.11.13): Número total de objetos da MIB que foram resgatados pela entidade SNMP.

EXERCÍCIOS:

1 - Caracterize o Modelo de Gerência TCP/IP. Exemplifique.
2 - Quais os principais componentes da arquitetura de gerenciamento TCP/IP? Descreva seus elementos.
3 - O que é o protocolo SNMP? Qual a sua importância? O que ele possibilita para um administrador de rede?
4 - Descreva o que é o RMON? Quais suas vantagens e desvantagens?
5 - O que é uma MIB? Qual a sua importância? Como é organizada?

WEB-BIBLIOGRAFIAS

http://www.shitsuka.net/materialdidatico/cisco/ap_agr_cisco1.pdf
http://pontoderedes.blogspot.com/2010/04/protocolo-de-gerenciamento-snmp.html
http://www.oocities.com/siliconvalley/network/7460/tcpip.htm
http://www.gta.ufrj.br/~rezende/cursos/eel879/trabalhos/gerenciamento/
http://artigos.netsaber.com.br/resumo_artigo_15934/artigo_sobre_gerenciamento_de_redes_tcp/ip
http://www.gta.ufrj.br/grad/04_1/snmp/mib.htm
http://www.cin.ufpe.br/~flash/ais98/gerrede/gerrede.html

UNIDADE 04

Gerência de Redes OSI

Resumindo

Nesta unidade é apresentado o modelo de gerenciamento de redes baseado nas especificações da ISO, desde 1989, ou seja, baseado no modelo de referência OSI. As especificações funcional, organizacional, informacional e de comunicação serão especificados. Os protocolos CMIP (*Common Management Information Protocol*) e o CMIS (*Commom Management Information Services*) como protocolo e serviço de gerenciamento de rede do nível de aplicação do modelo OSI são abordados, bem como sua comparação com o protocolo SNMP.

4 GERENCIAMENTO DE REDES OSI

MODELO DE GERENCIAMENTO DE REDES OSI

O modelo de redes OSI é um padrão ISO e tem colaborado amplamente para a padronização das redes. O seu modelo de gerenciamento é fundamental para que se possam compreender de maneira abrangente os aspectos fundamentais dos Sistemas de Gerenciamento de Redes. Ele é estruturado e referencia todos os aspectos de gerenciamento. A figura abaixo mostra um modelo de gerenciamento OSI que agrega 4 modelos: modelo organizacional, modelo de informação, modelo de comunicação e modelo funcional.

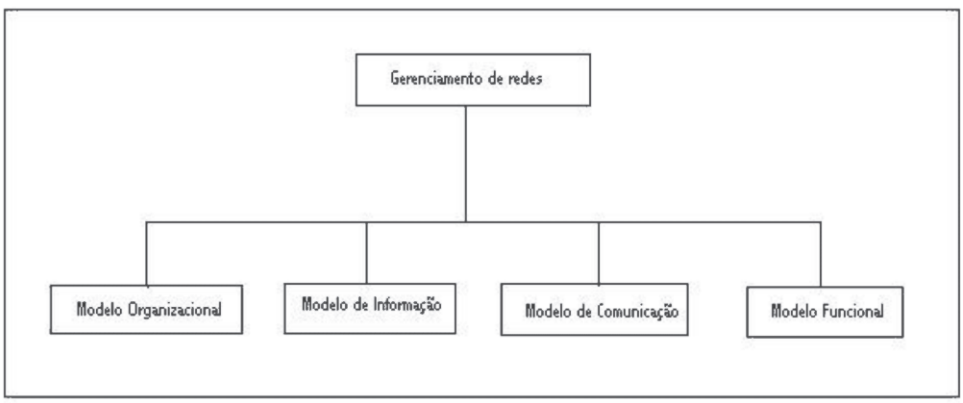

Figura 21 – Modelo de gerenciamento OSI

Modelo Informacional

O Modelo de Informação lida com o armazenamento de informações, definindo a estrutura e organização de gerenciamento da informação. Neste

especifica a Estrutura de Gerenciamento de Informação (SMI – *Struct Management Information*) e o bando de dados MIB (*Management Information Base*). SMI descreve como o gerenciamento de informação é estruturado, ou seja, a sintaxe (formato) e a semântica (significado) das informações armazenadas na MIB, que por sua vez trata das relações e armazenamento das informações gerenciadas. A MIB é usada por ambos os processos, agente e gerente, para armazenar e trocar informações de gerenciamento. Cada agente possui uma MIB com as informações locais e a plataforma de gerenciamento possui as informações de todos os componentes da rede gerenciados.

O gerente possui 2 bancos de dados: MDB (*Management Data Base*) e MIB. Veja:

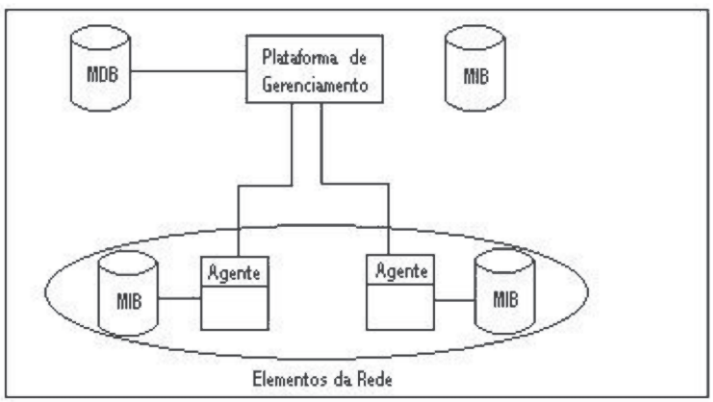

Figura 22 – Modelo Informacional

A plataforma de gerenciamento irá perguntar a MIB de um dispositivo recém-instalado, que é diferente de todos os outros da rede, quais são as variáveis e valores associados, através do agente que reside no componente. Essa pergunta será feita durante o reconhecimento da rede que é feito de tempos em tempos através do protocolo de gerenciamento. Esse reconhecimento também é usado na monitoração de falhas, pois caso um elemento que anteriormente havia sido reconhecido na rede não responda ao ping, pode caracterizar alguma falha.

Modelo Organizacional

O modelo organizacional descreve os componentes do Sistema de Gerenciamento de Redes com suas funções, relações e infraestruturas. Ele define os termos objeto, agente e gerente. Objetos de rede consistem em elementos de rede, tais como *hubs, switches, bridges, gateways*, etc. Eles podem ser classificados como objetos gerenciáveis ou não gerenciáveis. Os elementos gerenciáveis possuem um processo de gerenciamento sendo executado internamente, chamado agente.

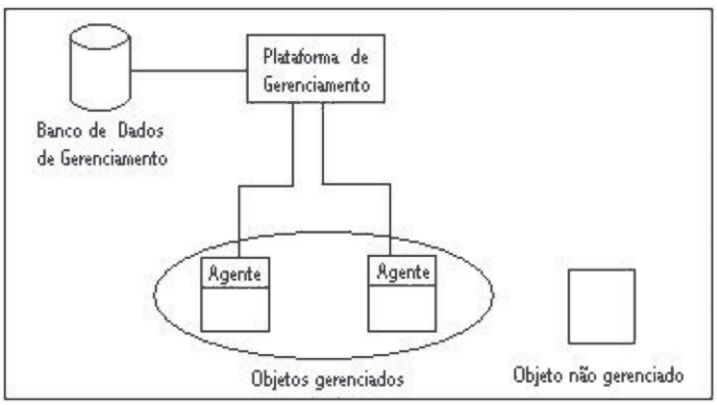

Figura 23 – Modelo Organizacional

A plataforma de gerenciamento solicita e recebe dados de gerenciamento do agente para processá-los e armazená-los em seu banco de dados.

Modelo Funcional

O Modelo Funcional lida com os requerimentos de gerenciamento orientado ao usuário. No sentido de definir um escopo para a gerência de redes o Modelo de Referência OSI definiu cinco áreas funcionais:

- Gerenciamento de Configuração;
- Gerenciamento de Desempenho;
- Gerenciamento de Falhas;
- Gerenciamento de Segurança;
- Gerenciamento de Contabilização.

Esta subdivisão é normalmente usada na área de gerência independente do tipo de protocolo e é importante para a compreensão do assunto.

Muitas vezes, as áreas funcionais possuem funções de gerenciamento que se sobrepõem, isto é, são utilizadas não somente em uma, mas até mesmo em várias áreas de gerenciamento, apesar de terem finalidades diferentes em cada uma. Por outro lado, algumas funções servem de suporte para as funções das outras áreas, vejamos.

Gerenciamento de Falhas

A gerência de falhas tem a responsabilidade de monitorar os estados dos recursos, dar manutenção a cada um dos objetos gerenciados e tomar decisões para restabelecer as unidades do sistema que venham a dar problemas.

As informações que são coletadas sobre os vários recursos da rede podem ser usadas em conjunto com um mapa desta rede para indicar quais elementos estão funcionando, quais estão em mau funcionamento e quais não estão funcionando.

Opcionalmente, pode-se gerar um registro das ocorrências na rede, um diagnóstico das falhas ocorridas e uma relação dos resultados deste diagnóstico com as ações posteriores a serem tomadas para o reparo dos objetos que geraram as falhas.

O ideal é que as falhas que possam vir a ocorrer em um sistema sejam detectadas antes que os efeitos significativos decorrentes desta falha sejam percebidos. Pode-se conseguir este ideal através do monitoramento das taxas de erros do sistema e da evolução do nível de severidade gerado pelos alarmes (função de relatório de alarme), que permitem a emissão das notificações de alarme ao gerente, que pode definir as ações necessárias para corrigir o problema e evitar as situações mais críticas.

Entre as funções de gerência destacam-se:

- Manter e examinar registros (“logs”) de erros;
- Aceitar e agir sobre notificações de erros;
- Traçar e identificar falhas;
- Realizar testes de diagnóstico;
- Corrigir falhas.

Gerenciamento de Contabilidade

O gerenciamento de contabilidade possibilita estabelecer taxas a serem utilizadas pelos recursos no ambiente OSI e os custos a serem identificados na utilização daqueles recursos. Outras considerações incluem informações dos custos dos usuários e recursos gastos, estipulando limites e incorporando informações de tarifas em todo o processo de contabilidade.

No mundo de hoje, contabilidade significa tratar com pessoas usando os reais recursos de rede com despesas de operação real. Exemplos desses custos incluem uso do espaço em disco e dados armazenados, despesas de telecomunicação para acesso a dados remotos e taxas de envio de *e-mail*.

Pode-se também usar o gerenciamento de contabilidade para determinar se a utilização do recurso da rede está aumentando com o crescimento, o que deve indicar a necessidade de adições e reajustamentos num futuro próximo

Gerenciamento de Configuração

O objetivo da gerência de configuração é o de permitir a preparação, a iniciação, a partida, a operação contínua e a posterior suspensão dos serviços de interconexão entre os sistemas abertos, tendo então, a função de manutenção e monitoramento da estrutura física e lógica de uma rede, incluindo a verificação da existência dos componentes e a verificação da interconectividade entre estes componentes.

A gerência de configuração é, portanto, correspondente a um conjunto de facilidades que permitem controlar os objetos gerenciados, identificando-os, coletando e disponibilizando dados sobre estes objetos para as seguintes funções:

- Atribuição de valores iniciais aos parâmetros de um sistema aberto;
- Início e encerramento das operações sobre os objetos gerenciados;
- Alteração da configuração do sistema aberto;
- Associação de nomes a conjuntos de objetos gerenciados.

Entre as funções desta área destacam-se:

- Registrar a atual configuração;
- Registrar alterações quando realizadas;
- Identificar todos os componentes da rede endereçando os pontos

de acesso à rede;

• Realizar reinicializações quando ocorrer queda nos sistemas;

• Realizar trocas nas tabelas de roteamento.

Gerenciamento de Desempenho

Na gerência de desempenho tem-se a possibilidade de avaliar o comportamento dos recursos num ambiente de gerenciamento OSI verificando se este comportamento é eficiente, ou seja, preocupa-se com o desempenho corrente da rede, através de parâmetros estatísticos como atrasos, vazão, disponibilidade e o número de retransmissões realizadas.

O gerenciamento de desempenho é um conjunto de funções responsáveis por garantirem que não ocorram insuficiências de recursos quando sua utilização se aproximar da capacidade total do sistema.

Para atingir estes objetivos, devem-se monitorar as taxas de utilização dos recursos, as taxas em que estes recursos são pedidos e as taxas em que os pedidos a um recurso são rejeitados. Para cada tipo de monitoramento, define-se um valor máximo aceitável (*threshold*), um valor de alerta e um valor em que se remove a situação de alerta.

Definem-se três modelos para atender os requisitos de monitoramento de uso dos recursos do sistema:

• Modelo de Utilização: Provê o monitoramento do uso instantâneo de um recurso.

• Modelo de Taxa de Rejeição: Provê o monitoramento da rejeição de um pedido de um serviço.

• Modelo de Taxa de Pedido de Recursos: Provê o monitoramento dos pedidos do uso de recursos.

Os registros de desempenho podem ser utilizados em outras áreas tais como para:

• Auxiliar a detectar falhas na rede;

• Auxiliar a determinação quando serão necessárias alterações na configuração da rede;

Gerenciamento de Segurança

O objetivo do gerenciamento de segurança é o de dar subsídios às aplicações de políticas de segurança, que são os aspectos essenciais

para que uma rede baseada no modelo OSI seja operada corretamente, protegendo os objetos gerenciados e o sistema de acessos indevidos. Deve-se providenciar um alarme ao gerente da rede sempre que se detectarem eventos relativos à segurança do sistema.

As informações de gerenciamento de segurança são armazenadas numa MIB especial, a qual deve dar apoio as três categorias de atividades de gerenciamento de segurança existentes. Esta MIB é chamada de SMIB (*Security Management Information Base*).

Ou seja, a gerência de segurança é o processo que controla o acesso às informações disponíveis na rede. Existem informações armazenadas em computadores ligados à rede que são impróprias a todos os usuários. O grupo de informações mais conhecido em que não fica disponível para evitar ações impróprias que prejudiquem os usuários é o conjunto de senhas que permitem o acesso à rede. A gerência de segurança permite que o administrador monitore as tentativas de entrada na *red*.

Modelo de Comunicação

O Modelo de Comunicação define a maneira como as informações são trocadas entre os sistemas. Dados de gerenciamento são trocados entre os agentes e os processos gerentes, bem como entre um processo gerente com outro. Há três aspectos que devem ser abordados na comunicação entre duas entidades: o meio de mensagem da troca de informação (protocolo de mensagem), formato da mensagem de comunicação (protocolo de aplicação) e mensagem propriamente dita (comandos e respostas). A figura abaixo apresenta o modelo de comunicação.

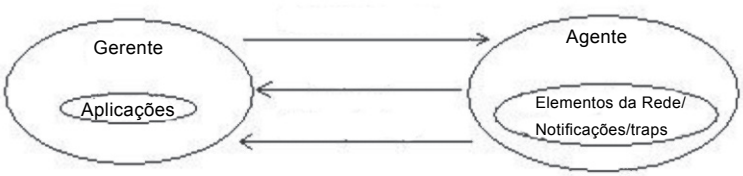

Figura 24 – Modelo de Comunicação

As aplicações no módulo gerente iniciam pedidos ao agente no modelo da Internet. O agente executa o pedido no elemento de rede, que é o objeto gerenciável, e retorna a resposta ao gerente. As notificações/*traps* são

mensagens não solicitadas, como alarmes, geradas pelo agente.

O modelo OSI usa Protocolo Comum de Gerenciamento da Informação (CMIP – *Common Management Information Protocol*) juntamente com os Serviços Comuns de Gerenciamento da Informação (CMIS – *Common Management Information Services*).

PROTOCOLOS DE GERÊNCIA DE REDES – CMIP E CMIS

A utilização dos padrões da ISO para gerenciamento tem sido ampliada (além dos méritos técnicos) em boa parte pela OSF, que está comprometida, através do OSF/DME (Open Software Foundation/Distributed Management Environment), em suportar os padrões OSI de gerenciamento. A função do DME é fornecer facilidades que permitam integrar o gerenciamento de sistemas em ambientes heterogêneos, satisfazendo três requisitos básicos:

- Interoperabilidade;
- Consistência;
- Flexibilidade.

A ISO especifica o CMIP (*Common Management Information Protocol*) e o CMIS (Commom Management Information Services) como protocolo e serviço de gerenciamento de rede do nível de aplicação do modelo OSI.

Da mesma maneira que o SNMP, o CMIP especifica como vai ser realizada a troca de informações entre o gerente e o agente no sistema e gerenciamento, ou seja, com o primeiro acessando e mudando informações que se encontram na MIB.

Os tipos de informações a serem trocadas levam em conta o CMIS (Common Management Information Service), que especifica o conjunto de serviços a que os sistemas gerenciadores e gerenciados poderão acessar para que seja realizado o gerenciamento. Juntos CMIS e CMIP formam o que é chamado de CMISE (*Common Management information Service Element*), que é uma aplicação da camada 7 do modelo de rede OSI.

O CMISE utiliza duas aplicações de serviço comuns, ACSE e ROSE. A primeira trata do estabelecimento e liberação de conexões entre um equipamento e outro. A segunda oferece serviços de requisição de operações remotas.

Os conjuntos de serviços oferecidos se enquadram em três categorias:

- Serviços de Associação: São utilizados para que os usuários do CMIS possam estabelecer as associações necessárias para a

realização da comunicação entre si. Para que isso ocorra, no entanto, o CMIS precisa dos serviços oferecidos pela aplicação ACSE.

• Serviços de Notificação: Os serviços de notificação de gerenciamento são utilizados para que o agente sinalize sobre a ocorrência de eventos nos dispositivos gerenciados.

• Serviços de Operação: Os serviços de operação de gerenciamento são utilizados para que o gerente possa obter informações ou alterar as variáveis do MIB.

Os serviços podem ser confirmados ou não-confirmados. Serviço confirmado significa que quem começou a comunicação (gerente ou agente) deve receber uma resposta vinda do outro lado sobre o sucesso ou o erro da requisição.

Quanto aos serviços de operação de gerenciamento, são fornecidos três mecanismos de seleção de objetos gerenciados (variáveis do MIB). São eles:

• Escopo: É um parâmetro da mensagem passada do gerente para o agente, através do protocolo CMIP, que possibilita a seleção de um grupo de objetos que serão submetidos a operações de gerenciamento;

• Filtragem: É outro parâmetro que aplica testes em cima do conjunto selecionado pelo escopo para eliminar a possibilidade de certos objetos sofrerem operações de gerenciamento sem necessidade.

• Sincronismo: É o parâmetro que de acordo com seu valor passado na mensagem, ou exigirá que os objetos só sofram operações, caso todos os que forem selecionados pelo escopo passem pelo processo de filtragem ou exigirá que o maior número possível de objetos selecionados e aprovados sofra operações de gerenciamento.

Quando o serviço de operação de gerenciamento exige confirmação, para cada objeto selecionado (caso possua), pelo escopo e pela filtragem haverá uma resposta. Este processo é chamado de respostas múltiplas. Caso o serviço seja não-confirmado não há sentido em se falar de respostas múltiplas.

COMPARAÇÕES ENTRE O CMIP E SNMP

Atualmente, quando se fala em gerenciamento de redes, dois protocolos se destacam:

SNMP: *Simple Network Management Protocol*.

CMIP: *Common Management Information Service Over TCP*.

Uma das diferenças fundamentais entre os dois protocolos é o fato de o primeiro ser baseado no modelo de gerenciamento TCP/IP. Já o segundo é baseado no modelo de gerenciamento OSI.

Além destas diferenças algumas outras são:

- O CMIP possui uma quantidade bem menor de produtos que o implementam;
- O CMIP possui uma quantidade maior de operações, permitindo uma maior versatilidade no controle exercido sobre os elementos da rede (por exemplo, as operações CREATE e DELETE permitem que objetos sejam criados e eliminados dinamicamente);
- O CMIP é mais rico, apresentando uma melhor qualidade de informação;

Uma implementação CMIP tende a ser mais lenta e maior, uma vez que requer maior capacidade de processamento e memória.

Sabendo-se agora as diferenças básicas entre estes dois protocolos, sabe-se que atualmente vários produtos têm surgido com a finalidade de gerenciar a rede, quase que em sua totalidade baseados no padrão SNMP e CMIP.

O esquema dos produtos desenvolvidos com o protocolo SNMP são um pouco diferente dos produtos que utilizam o protocolo CMIP. Os fornecedores de produtos que utilizam o protocolo CMIP pressupõem que os fabricantes possuam algum tipo de gerenciamento em seus equipamentos, portanto estas informações podem ser disponibilizadas para um integrador via protocolo CMIP. O conceito de integrador foi definido em três níveis: o mais baixo, que contém os agentes e os elementos gerenciadores, o intermediário, que consiste em elementos do sistema de gerenciamento, e finalmente o nível mais alto, que consiste no integrador dos sistemas de gerenciamento. Produtos como o *NetView* da IBM, *Accumaster* da AT& T, *Allink* da *Nynex* e o *SunNet Manager da Sun Microsiytems*, dentre outros, são exemplos deste tipo de implementação.

A dificuldade maior para uma aplicação integradora é que os fornecedores não têm as mesmas variáveis de gerenciamento, tão pouco as mesmas operações em seus servidores de objetos.

A escolha entre um ou outro protocolo de gerenciamento deve recair sobre o tipo de rede e dos produtos a ela agregados, sendo que podem ser mesclados os dois protocolos.

EXERCÍCIOS

1 - Caracterize o Modelo de Gerência OSI. Exemplifique.
2 - Quais os principais componentes da arquitetura de gerenciamento OSI? Descreva seus elementos.
3 - Quais são as cinco áreas funcionais da gerência de rede? Descreva cada uma delas.
4 - Pensando em algum serviço específico, é possível que uma área funcional seja considerada em maior importância? Por quê?
5 - Caracterize CMIP e CMIS. Em seguida, faça a comparações entre CMIP e SNMP.

WEB-BIBLIOGRAFIA

http://www.shitsuka.net/materialdidatico/cisco/
http://www.gta.ufrj.br/grad/cmip.html#cmip

UNIDADE 05

Plataformas e Aplicações de Gerenciamentos

Resumindo

Nesta unidade são apresentadas as principais características de algumas ferramentas de gerenciamento de rede, tais como *Nagios, Cacti, Zabixx, NetWare Management System, OpenNMS* e NTOP. Adicionalmente, é apresentado o processo de instalação básica das ferramentas NAGIOS, Cacti e NTOP. Por fim, é apresentado um quadro comparativo de diversas funcionalidades de algumas destas ferramentas.

5 PLATAFORMAS E APLICAÇÕES DE GERENCAMENTOS

INTRODUÇÃO AS FERRAMENTAS DE GERENCIAMENTO

Considerando que servidores são máquinas que hospedam softwares e uma destas finalidades é administrar serviços de redes de computadores. Para montar um ambiente tecnológico de confiança é preciso investir em *hardware* e *software*. E não só isso, como também mão-de-obra especializada para que os serviços sigam um alto padrão de confiabilidade.

Monitorar redes é um trabalho feito na maioria das organizações e existem soluções pagas e gratuitas que ajudam os analistas de redes fazer tal trabalho. Uma rede pode oferecer variados tipos de trabalhos que, com o uso de ferramentas, é diminuído com a monitoração. Por exemplo, o NAGIOS é um ótimo monitor para redes. Com ele, é possível monitorar e atestar o funcionamento correto dos equipamentos e serviços. É possível também criar grupos de usuários para receber relatórios e alertas do sistema.

Com o aumento cada vez mais do uso de equipamentos em conexão nas redes das empresas e a criação e utilização de aplicações baseadas na web, ficar sem conectividade, ou seja, sem rede, deixando indisponível o serviço, é algo que as empresas têm evitado ao máximo. Atualmente, ficar fora do ar sem sistema, mesmo que por pouco tempo.

Para atividade de gerenciamento, pode-se denominar de ferramentas mais simples, aquelas ferramentas que não dão uma visão geral da rede, mas que muitas vezes ajudam a descobrir características mais internas de determinados elementos da rede. Essas ferramentas são geralmente oferecidas junto com o sistema operacional de rede dos próprios hospedeiros.

Como exemplo das principais ferramentas mais simples tem: *traceroute* (*tracert*), *ping*, *route*, *netstat*, e *ipconfig*. Em muitas situações, faz-se o uso dessas ferramentas, no entanto, elas isoladamente não são suficientes para

realizar bem a tarefa de gerência. Em geral, estas ferramentas são utilizadas como apoio depois de termos descoberto que um problema ocorre ou ocorreu.

Por exemplo, com o comando tracert, podemos descobrir onde o problema está localizado. Ao usar o auxílio de uma estação de gerência onde o mapa da rede é apresentado e alarmes são gerados automaticamente quando limiares ou mudanças de estado operacional são detectados, certamente o problema seria detectado com maior rapidez e precisão.

Quando se utiliza apenas essa instrumentação mais simples, pode-se caracterizar com a técnica da porta aberta. Ou seja, é um tipo de gerência totalmente reativo (em que se reage aos problemas, que não podem ser previstos). Esse tipo de gerência não tem escala. Não é possível gerenciar uma rede com milhares de elementos dessa forma.

Já uma estação de gerência é normalmente construída usando uma plataforma de gerência. Para compreender o que é uma plataforma de gerência, é necessário entender que a gerência de redes é uma atividade complexa e o software que executa numa estação de gerência não é uma aplicação única e monolítica. A solução de gerência é montada modularmente usando várias aplicações, à semelhança do que ocorre num hospedeiro em que várias aplicações são instaladas para formar o conjunto de software disponível. Portanto, pode-se comparar a plataforma de gerência ao “sistema operacional de gerência”.

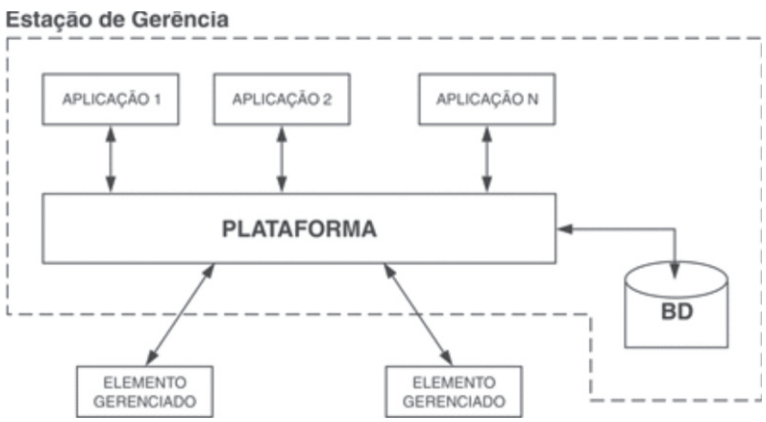

Figura 25 – Modelo de estação de Gerência

Com base nas principais ferramentas de monitoramento de redes ou plataformas de gerência, que são desenvolvidos com a filosofia dos softwares livres foi montada um árvore de dependências entre os principais projetos, apresentados na figura a seguir.

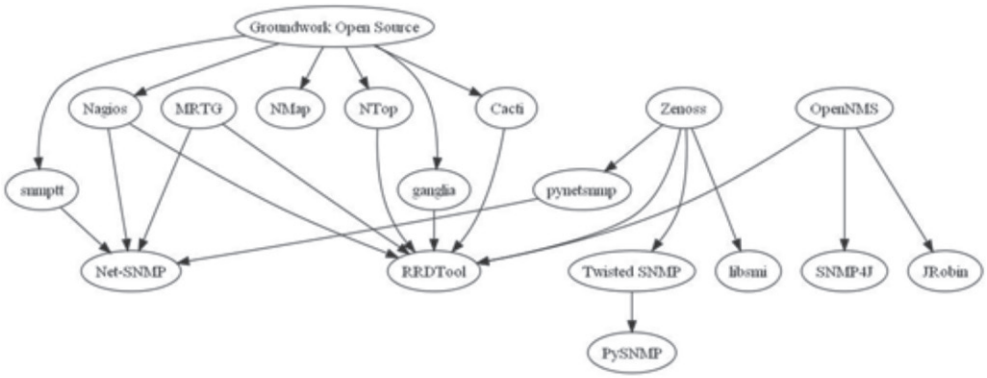

Figura 26 – Árvore de relacionamento entre os projetos de ferramentas de gerenciamento de código aberto (*Open Source*).

Nos tópicos seguintes serão apresentadas algumas das principais ferramentas de monitoramento de redes.

FERRAMENTA NAGIOS

O Nagios é um sistema de monitoramento de rede licenciado sob os termos da GNU (*General Public License*) e que tem a capacidade de monitorar toda a infraestrutura de tecnologia da informação com o objetivo de garantir o bom funcionamento de servidores, aplicativos, processos, serviços e ativos de rede. Originalmente, criado sob o nome de *Netsaint*, foi escrito e é atualmente mantido por Ethan Galstad, junto com um exército de desenvolvedores que ativamente mantém plugins oficiais e não-oficiais. O NAGIOS tem sua estrutura formada por plugins, sendo todo o serviço feito através de deles. *Plugins* são pequenas partes de programas e para o NAGIOS foram escritas em Perl e C e são incorporados a estrutura do *software* para executar uma tarefa especifica. Com ele é possível emitir alertas ao pessoal técnico de uma falha ocorrida ou que possa ocorrer, para que não afete os clientes ou comprometa os processos de negócios dos utilizadores finais.

Com o NAGIOS pode-se monitorar impressoras de rede, roteadores/ switches e servidores e alguns serviços como tráfego de *e-mail*, por exemplo, sob as plataformas *Windows*, *Linux*, *Unix* e *Netware*. Ele pode monitorar tanto hosts quanto serviços, alertando-o quando ocorrerem problemas e também quando os problemas forem resolvidos.

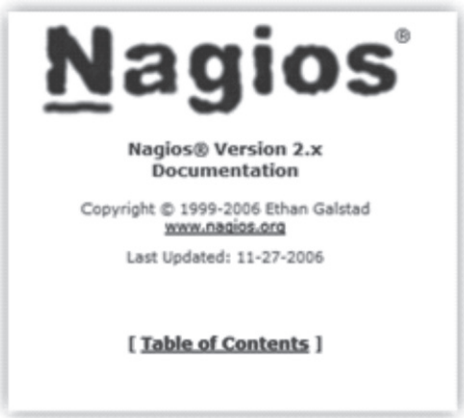

Figura 27 – Tela com informações da versão do Nagios

Sem dúvidas é um dos sistemas de monitoramento mais populares que se tem atualmente e com características muito apropriadas e usuais para a maioria dos gerentes de redes, como:

- Monitoramento de serviços de rede como SMTP, POP3, HTTP, ICMP, etc.;
- Monitoramento dos recursos de computadores ou outros equipamentos de rede como carga do processador, uso da memória, uso do disco, tráfego de rede, dentre outros itens;
- Rotação automática do log;
- Capacidade de definir hierarquicamente a rede permitindo detectar e diferenciar quando um cliente está inalcançável ou desativado;
- Capacidade de definir tratadores de eventos, que são ações pré-definidas para tentar solucionar um problema detectado;
- Suporte para implementação de monitoramento redundante.

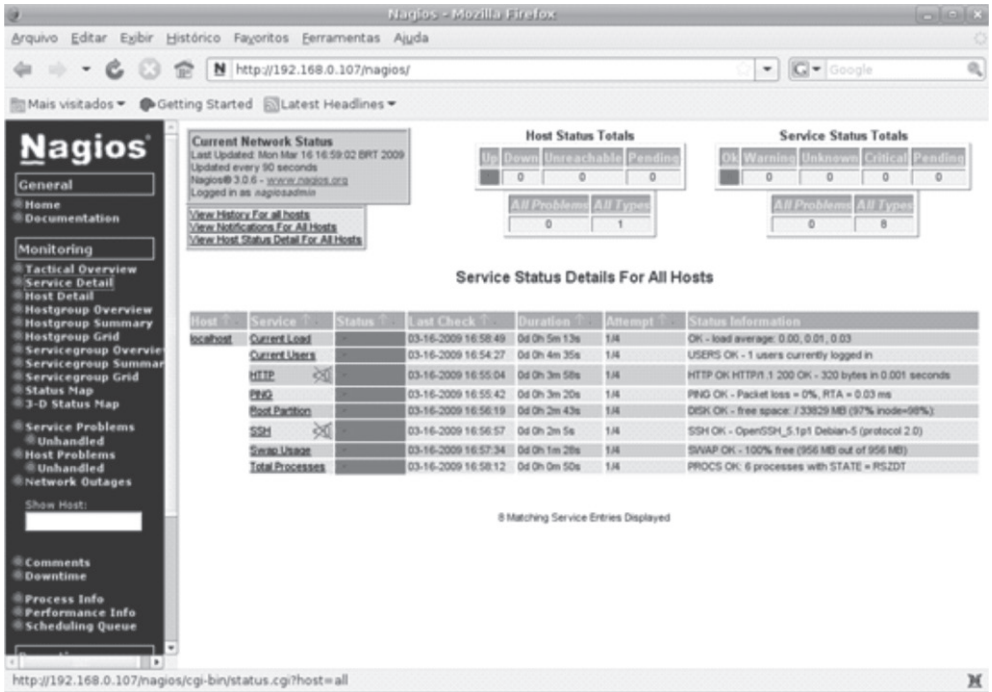

Figura 28 – Tela principal do Nagios

Ele é responsável por realizar checagem de tempos em tempos dos equipamentos monitorados, bem como alguns serviços nestes. O monitoramento é feito através de um conjunto de *Plugins* responsáveis por informar ao servidor do Nagios o *status* dos *hosts* (computadores) e serviços monitorados. Caso ocorra algum problema em cada um dos host ou serviço, o Nagios enviará informações alertando-o. Essas informações podem ser enviadas de diferentes formas (*e-mail*, mensagens instantâneas, SMS, etc.).

Instalação do sistema Nagios

A versão do Nagios utilizada nesse material é a 3.2.3 e do Nagios Plugins 1.4.15. Para iniciar a instalação do Nagios, baixe-o em http://www.nagios.org/download ou via comando wget no GNU/*Linux*, no caso deste material adotamos a distribuição *Ubuntu*.

```
# wget http://heanet.dl.sourceforge.net/sourceforge/nagios/nagios-3.2.3.tar.gz
# wget http://sourceforge.net/projects/nagiosplug/files/nagiosplug/1.4.15/nagios-plugins-1.4.15.tar.gz
```

Para compilar os pacotes do Nagios e seus plugins é preciso instalar as bibliotecas, compiladores e os headers do kernel do GNU/Linux, além de satisfazer as dependências para instalação correta do sistema, que são: o Apache, a biblioteca de desenvolvimento GD e o compilador. As bibliotecas requeridas são libgd e openssl.

```
# apt-get install build-essential linux-headers-`uname -r`
```

O build-essential é o conjunto de pacotes e bibliotecas de compilação, ele instala o GCC, G++ e os demais integrantes do kit básico.

O pacote "*linux-headers*" inclui os *headers* do *kernel*, o conjunto de arquivos e ponteiros necessários para que o compilador seja capaz de gerar módulos adequados ao kernel em uso. Existem várias versões do pacote, uma para cada versão do kernel disponível nos repositórios (como em "linux-headers-2.6.26-1-686"); por isso, para facilitar, usamos o "*linux-headers-`uname -r`*" (o ` é o símbolo de crase) que faz com que o apt descubra sozinho qual versão deve instalar a partir do comando "uname -r". Com isso, a casa fica pronta para a instalação dos *drivers*.

Após etapa de *download* dos pacotes, deve-se criar um usuário "nagios" no sistema, pois o O Nagios utiliza um usuário do sistema para sua execução.

```
# adduser nagios
```

Para executar comandos externos via interface web é preciso que o servidor web esteja instalado. Para instalar o servidor *web Apache* na distribuição *GNU/Linux Ubuntu*, deve-se executar:

```
# apt-get install apache2
```

Durante a instalação do apache, automaticamente é criado o usuário www-data. Esse usuário, por padrão é quem executa o apache. Criaremos um grupo chamado "*nagcmd*" para que possam ser realizados os external commands através da interface web, posteriormente adicionaremos o usuário nagios e o www-data a este grupo.

```
# usermod -a –G nagcmd nagios
# usermod -a –G nagcmd www-data
```

O *Nagios* deverá instalado no diretório /usr/local/nagios. Extraia os arquivos do *Nagios* utilizando o comando:

```
# tar -xvzf nagios-3.2.3.tar.gz
```

Acesse o diretório *nagios*-3.2.3/:

```
# cd nagios-3.2.3
```

Execute o *scritp*, conjunto de comandos, de configuração:

```
#  ./configure --with-command-group=nagcmd
(Observe que o início do comando é ponto e barra)
```

Em seguida, compile o *Nagios* e seus complementos:

```
#  make all
```

Instale os binários:

```
#  make install
```

Instale os scripts de inicialização:

```
#  make install-init
```

Instale os arquivos de configuração:

```
#  make install-conf
```

Crie o diretório que será utilizado para a inserção de comandos externos:

```
#  make install-commandmode
```

Arquivo de configuração do apache para ser configurada a interface web:

```
# make install-webconfig
```

Após estas etapas, o Nagios já estará instalado em seu computador. Você encontrará no diretório do Nagios outros seis subdiretórios. Abaixo uma breve explicação de cada um deles:

- *bin* - Contém os arquivos binários do *Nagios*;
- *etc* - Contém os arquivos de configuração do *Nagios*;
- *libexec* - Contém os *plugins do Nagios*;
- *sbin* - Contém os CGI script que será usado na interface *web*;
- *share* – Contém os arquivos HTHML para a interface *web* e a documentação.

Após a instalação do Nagios, devem-se instalar os plugins, logo: Decompacte os plugins e mude o diretório referente:

```
# tar zfxv nagios-plugins-1.4.15.tar.gz
# cd nagios-plugins-1.4.15
```

Realize a configuração dos *plugins*:

```
# ./configure --with-nagios-user=nagios --with-nagios-group=nagios
(Observe que o início do comando é ponto e barra)
```

Em seguida, realize a compilação dos plugins. Verifique se não está faltando algum componente. Caso esteja faltando algum irá aparecer uma mensagem para realizar a instalação:

```
# make all
# make install
```

Para acessar o *Nagios* via *web*, é necessário adicionar a seguinte configuração no arquivo de configuração do *Apache*, httpd.conf :

ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin/

<Directory "/usr/local/nagios/sbin/">
AllowOverride AuthConfig
Options ExecCGI
Order allow,deny
Allow from all
</Directory>

Alias /nagios /usr/local/nagios/share/

<Directory "/usr/local/nagios/share">
Options None
AllowOverride AuthConfig
Order allow,deny
Allow from all
AuthName "Nagios Access"
AuthType Basic
AuthUserFile /usr/local/nagios/etc/htpasswd.users
require valid-user
</Directory>

Depois é necessário criar o arquivo com usuário e senha, para isso faça uso dos comandos:

```
# htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
# chown apache:apache /usr/local/nagios/etc/htpasswd.users
(verifique o grupo do apache)
```

Será solicitada uma senha para acesso ao Nagios via navegador (*browser*):

login: nagiosadmin
senha: a definir
Após todo processo, reinicie o apache:

```
# etc/init.d/apache2 restart
```

Após a instalação do Nagios e seus *Plugins* é necessário configurar os arquivos de configuração conforme sua rede. Iremos mostrar algumas etapas para um exemplo de configuração.

Recomenda-se por segurança realizar uma cópia dos arquivos originais antes de alterar a configuração, para tal:

```
# cd /usr/local/nagios/etc
# mkdir original
# mv *.cfg-sample original
for i in *cfg-sample; do mv $i `echo $i|sed -e s/cfg-sample/cfg/`; done;
# cd /usr/local/nagios/etc/original
# cp cgi.cfg checkcommands.cfg misccommands.cfg nagios.cfg
resource.cfg timeperiods.cfg ../
```

Principais Arquivos de configuração

CGI.CFG

Nele ficam as configurações de utilização de arquivos CGI usadas pelo Nagios. Devem ser configurados os parâmetros de autorização de utilização da interface *web*. Altere os campos para o nome do usuário cadastros no arquivo /usr/local/nagios/etc/htpasswd.users e assim permitirá que estes tenham acesso ao sistema. Tais parâmetros são:

authorized_for_system_information=usuario1, usuario2
authorized_for_configuration_information=usuario1, usuario2
authorized_for_system_commands= usuario1, usuario2
authorized_for_all_services=usuario1, usuario2
authorized_for_all_hosts=usuario1, usuario2
authorized_for_all_service_commands=usuario1, usuario2
authorized_for_all_host_commands=usuario1, usuario2

CHECKCOMMANDS.CFG

Configuração dos plugins que estão no diretório */usr/local/nagios/libexec*, deve-se efetuar a adição do *plugin* e seus parâmetros.

MISCCOMMANDS.CFG

Definição de alguns comandos, tais como envio de *e-mail* e envio de Pager.

NAGIOS.CFG

Arquivo com as configurações principais. O padrão é bem completo, pode-se, inicialmente, alterar os parâmetros de checagem de comandos externos e formatação da data:

check_external_commands=0 -> check_external_commands=1

date_format=us -> date_format=euro

RESOURCE.CFG

Configuração de parâmetros de recursos. Por padrão vem definido qual o caminho os *plugins* podem ser setados as variáveis para serem utilizadas nos arquivos *CHECKCOMMANDS.CFG* e *MISCCOMMANDS.CFG.*

TIMEPERIODS.CFG

Arquivo com os horários pré-definidos para checagem de serviços e/ou servidores.

Para a configuração dos usuários e de grupos de usuários no sistema deve-se manipular dois arquivos contacts.cfg e contactgroups.cfg, respectivamente.

O escopo do arquivo *contacts*.cfg é :

contacts.cfg

define contact{

contact_name login

alias Nome do Usuario

service_notification_period Periodos definidos em *TIMEPERIODS*.CFG

host_notification_period Periodos definidos em TIMEPERIODS.CFG

service_notification_options w,u,c,r (w=*warning* / u=*unknown* / c=*critical* / r=*recoveries* / n=*none*)

host_notification_options d,u,r (d=*down* / u=*notify* / r=*recoveries* /

n=none)

service_notification_commands notify-by-email
host_notification_commands host-notify-by-email
email root@dominio.com.br
}
contactgroups.cfg
define contactgroup{
contactgroup_name grupo
alias Nome do Grupo
members Logins definidos no arquivo contacts.cfg
}

Configurando *hosts* e grupos de *hosts*

Existem dois arquivos que possuem a configuração dos hosts e dos grupos de hosts a serem manipulados, hostgroups.cfg e hosts.cfg.

hosts.cfg
define host{
event_handler_enabled 1
flap_detection_enabled 1
max_check_attempts 5
name generic-host
notification_interval 20
notification_options d,u,r
notification_period 24x7
notifications_enabled 1
process_perf_data 1
retain_status_information 1
retain_nonstatus_information 1
register 0
}

Definicao do 'servidor1'

define host{
use generic-host
address IP do Servidor
alias Nome do Servidor

check_command Comando a ser efetuado (funcao do services.cfg)
*host_name Host_Name*_do_servidor
}

hostgroups.cfg

define hostgroup{
hostgroup_name nome_do_grupo
alias Descricao do Grupo
contact_groups grupos_que_fazem_parte
members membros_que_fazem_parte
}

Utilize os comandos a seguir para criar os dois arquivos pela primeira vez. É necessário para iniciar o *Nagios*:

```
# touch /usr/local/nagios/etc/dependencies.cfg
# touch /usr/local/nagios/etc/escalations.cfg
```

Também é necessário criar o diretório abaixo:

```
# mkdir -p /usr/local/nagios/var/rw
# chown nagios:nagios -R /usr/local/nagios/var/rw
```

Após as configurações, é necessário iniciar o Nagios. Utilize o comando a seguir para verificar se está correto os arquivos de configuração:

```
# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

Se tudo estiver certo, inicie o Nagios com o comando:

```
# /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
```

Assim será iniciado como daemon. Não esqueça que foi criado o arquivo de inicialização no diretório /etc/rc.d/init.d/nagios.

FERRAMENTA CACTI

O Cacti é uma ferramenta gráfica de gerenciamento de dados de rede desenvolvido por *Ian Berry* em linguagem de programação PHP que utiliza scripts em BASH, PEARL e XML para coletar dados localmente ou SNMP para coletar dados remotamente. Seu funcionamento depende da instalação do RRDTOOL, conjunto de ferramentas desenvolvido por Tobias Oeticker que gera e interpreta informações em arquivos de dados do Apache, servidor de aplicação web e se apresenta em forma de gráficos. Possui uma interface web e armazena todos os seus dados em um banco de dados *MySql*.

RRD é a abreviação de Round Robin Database, sistema cujo objetivo é armazenar e monitorar dados em série obtidos durante um período de tempo pré determinado. Esses dados não aumentam com o decorrer do tempo e nem com a quantidade de dados já armazenados. Entretanto, o RRDTOOL não é capaz de gerar páginas html ou produzir gráficos, fato que torna necessário a sua comum utilização associada a um interface ou front-end. usar.

Esta ferramenta permite fazer o controle de acesso por nível de usuário, ou seja, pode configurar o acesso a certas informações apenas por determinados usuários. Além disso, adicionar novos equipamentos para serem monitorados no mapa da rede no sistema é uma tarefa menos complicada como em outras ferramentas, como o MRTG.

Para a instalação do *Cacti* necessita que alguns pacotes estejam instalados, tais como:

- *Apache* (ou outro servidor web);
- PHP (versão superior a 4) e extensões php-snmp e php-gd2;
- Banco de dados MySQL;
- *net-snmp*;
- RRDtool.

Instalação do *Cacti*

Para a instalação destes pacotes pode-se utilizar os seguintes comandos:

```
# apt-get install apache2
# apt-get install php5
# apt-get install mysql-server
# apt-get install rrdtool
```

Após a instalação dos pacotes dependentes, faça o *download* da última versão estável do *cacti* 0.8.7g, em http://www.cacti.net/download_cacti.php e o descompate dentro do diretório dos arquivos do servidor web, no caso do apache, em "/var/www":

```
# tar xzvf cacti-version.tar.gz
# mv cacti-version.tar.gz cacti
```

Após a descompactação do pacote do cacti, é necessário criar o mapa da base de dados do Cacti no MySQL:

```
# mysqladmin --user=root create cacti
```

Após a etapa anterior, deve-se importar a base de dados padrão do cacti, cacti.sql. Para tal faremos o uso do "<" (menor que), conforme comando a seguir:

```
# mysql cacti < cacti.sql
```

Defina no banco de dados MySQL um usuário e uma senha para Cacti:

```
# mysql --user=root mysql
```

Dentro do *prompt* de comando do mysql, defina o usuário e a senha, conforme procedimento:

```
mysql> GRANT ALL ON cacti.* TO cactiusuario@localhost IDENTIFIED BY 'suasenha';
 mysql> flush privileges;
```

Após a definição do usuário, definido no exemplo como cactiusuario, e a senha, definido no exemplo como suasenha, deve-se editar o arquivo de configuração, no caminho "/include/config.php", localizado dentro da pasta *Cacti* previamente descompactada e especifique o usuário MySQL, senha e a base de dados de configuração do cacti. Para executar este procedimento pode-se utilizar um dos editores de texto do Linux, no caso o denominado de nano, conforme:

```
# nano /www/var/cacti/include/config.php
```

Localize as linhas de configuração neste arquivo e os edite conforme:
$database_default = “cacti”;
$database_hostname = “localhost”;
$database_username = “cactiusuario”;
$database_password = “suasenha”;

Com esta configuração definiu-se a base de dados a ser utilizada, no caso cacti, o nome de identificação da localização desta base de dados, no caso o servidor local definido como localhost, o nome do usuário cadastrado no banco de dados para a manipulação dos dados, no caso o cactiusuario e finalmente a senha, definida no exemplo como suasenha.

Deve-se ajustar as permissões apropriadas aos diretórios dos Cacti para permitir a geração do gráfico. Execute o comando abaixo para mudança do proprietário dos arquivos no sistema dentro do diretório do *Cacti*, conforme:

```
# chown -R cactiusuario rra/ log/
```

Para acessar a tela inicial do cacti é preciso usar o endereço de acesso local no seu navegador web (browser), no caso definido como localhost:

http://localhost/cacti/

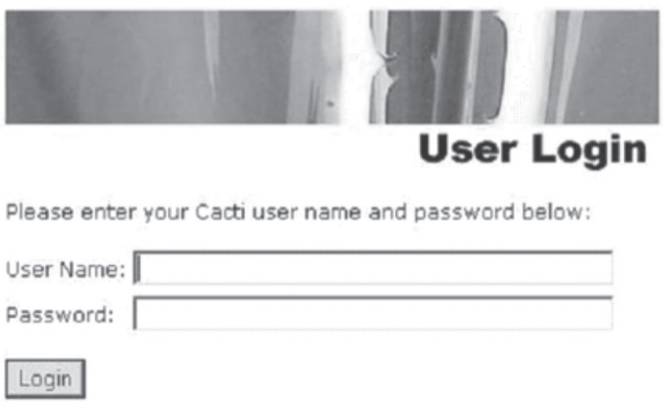

Figura 29 – Tela de autenticação do Cacti

Irá aparecer outra tela para você informar nova senha de acesso e aparecerão outras telas de configuração, responda-as de acordo com seus parâmetros escolhidos e clique em NEXT (avançar).

Na etapa de autenticação utilize com user name, a palavra admin, e como password, novamente a palavra admin. Esta definição de senha pode ser alterada posteriormente.

A ferramenta Cacti possibilita personalizar os gráficos, como por

exemplo, mudar as cores dos gráficos, cores de áreas específicas, largura e altura dos gráficos, escala, dentre outros requisitos. Para realizar estas configurações, utilize o menu da esquerda da página, clicando em Graph Templates (gráficos dos modelos ou templates).

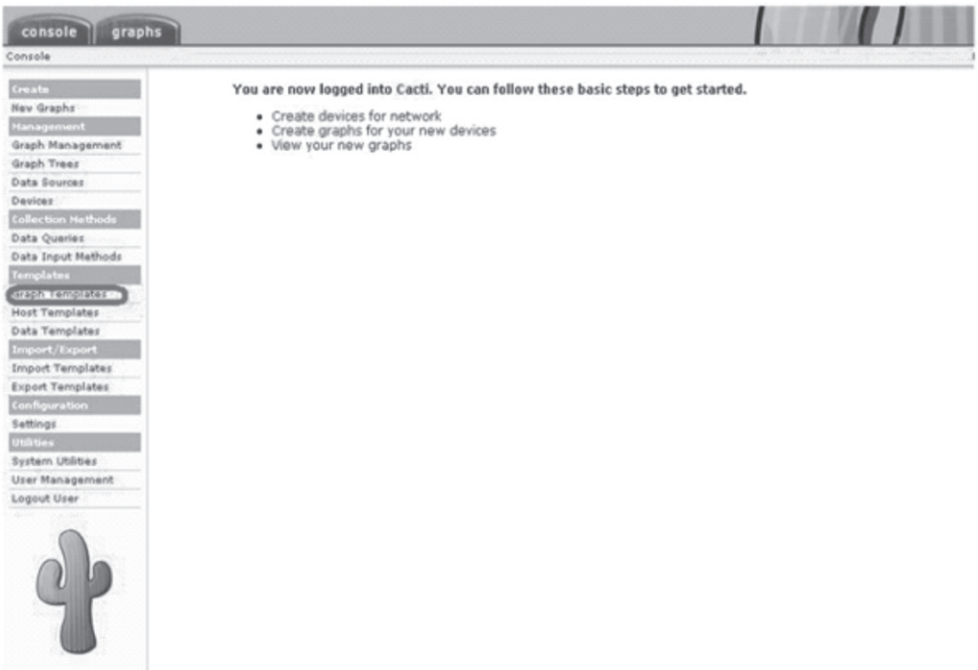

Figura 30 – Tela com as configurações de Templates do sistema Cacti

Além desta funcionalidade, permite a definição de configurações personalizadas para cada usuário, permitindo que este visualize somente o que realmente for permitido. É possível adicionar novos usuários, bem como alterar permissões de usuários já existentes. Para realizar estas configurações, utilize o menu da esquerda da página, clicando em *User Management* (gerenciador de usuário). Após a adição de novos usuários é possível alterar os dados, atribuir uma nova senha e modificar as permissões para esses usuários, além de permitir alterar também as permissões de cada gráfico utilizando a aba *Graph Permissions* (permissões dos gráficos) e as configurações dos gráficos clicando em *Graph settings*.

Figura 31 – Configurações de gráficos do sistema Cacti.

FERRAMENTA ZABIXX

O Zabbix é um software de código aberto que monitora vários parâmetros da rede de computadores bem como a integridade de serviços e ativos. Ele possui um mecanismo de alerta que permite o recebimento de *e-mails* e/ou mensagens de texto no celular, quando qualquer evento ocorrer com algum equipamento monitorado pelo Zabbix, o que permite uma rápida reação para solucionar o problema.

Figura 32 – Tela principal do Zabixx.

A facilidade da customização é sua maior característica na coleta de dados, pois as informações são coletadas por itens cadastrados em um *host* ou grupo de *hosts* sendo que cada item é uma variável SNMP. Além de gráficos estáticos, é possível mapear uma rede inteira mostrando todos os elementos ativos. Seu principal desenvolvedor é Alexei Vladishev no ano 2000.

Ele tem seu funcionamento baseado no servidor-agente e permite que mais de um servidor execute ao mesmo tempo, ou seja, redundante.

Algumas características interessantes também são:

- Utiliza SGBD (Sistema de Gerenciamento de Banco de Dados) para armazenar as configurações, dados coletados, tendências, etc.;
- Detalhamento em tempo-real do status do serviço de TI e dos *hosts*, histórico, dados estatísticos e gráficos;
- SLAs de serviços de TI bem como garantir a monitorização durante todo o período estipulado;
- Agente com suporte em praticamente todas as plataformas, além da facilidade de configuração e instalação;
- Capacidade de realizar alertas via SMS, *e-mail*, jabber ou até mesmo ligação telefônica;
- Controle de usuários por grupos e privilégios de acesso a determinadas funcionalidades.

FERRAMENTA NETWARE MANAGEMENT SYSTEM (NMS)

O sistema de gerenciamento Netware é a solução de gerenciamento da Novell que habilita os supervisores de rede e ajuda o pessoal de assistência técnica a monitorar e controlar redes heterogêneas de um ponto central. Projetado para proporcionar uma plataforma modular, aberta e com base em padrões para gerenciamento empresarial, o *NetWare Management System* otimiza recursos em um ambiente de rede com diversos fornecedores.

Operando em uma única estação de trabalho de gerência centralizada rodando o *MS Windows, o NetWare Management System* integra o gerenciamento de todos os dispositivos e serviços na rede.

O NMS lhe permite gerenciar os recursos de rede de forma eficiente possibilitando a redução do custo operacional de sistemas de cliente-servidor. Através da monitoria constante das mudanças na rede, o NMS identifica problemas em potencial e ajuda a resolvê-los antes que eles interrompam o funcionamento da rede. Centralizando os recursos de gerenciamento da rede, ele permite o gerenciamento eficaz de redes maiores e mais complexas, com menos pessoal. Com o NMS é possível maximizar a performance e disponibilidade da rede empresarial e otimizar o investimento em computação.

A plataforma NMS proporciona muitos serviços centrais, como a identificação e mapeamento automáticos de dispositivos na rede, monitoração de mudanças na rede, gerenciamento de informações de alarme e suporte SNMP. Os serviços da plataforma NMS facilmente acomodam aplicativos

de gerenciamentos criados por clientes e outros fabricantes. Combinando a funcionalidade e serviços fornecidos pelo NMS com outros aplicativos de gerenciamento, pode ser criado um único sistema de gerenciamento empresarial para redes de vários vendedores de modo simples, eficiente e econômico.

Além dos serviços de plataforma, a versão, NMS 2.0 inclui aplicativos para gerenciar os seguintes recursos de rede:

- Servidores de *NetWare* 3 e *NetWare* 4;
- *NetWare LANanlyzer Agent* para análise de rede distribuída;
- Todos os dispositivos SNMP;
- Monitoramento de roteadores;
- Hubs em conformidade com o *Hub Management Interface* (HMI);
- Monitoramento de endereços de rede.

O NMS proporciona um amplo gerenciamento de recursos, incluindo as seguintes funções:

- Identifica e exibe todos os dispositivos na rede através do *NetExplorer*;
- Mapeia objetos identificados em seus locais físicos;
- Possibilita a configuração de mapas para atender requisitos específicos;
- Mantém registros completos sobre informações de configuração para cada dispositivo;
- Possibilita a associação de imagens com informações de configuração;
- Proporciona vistas de mapa que permitem o recebimento de alarmes e a iniciação de tarefas;
- Proporciona proteção por senha para evitar mudanças não autorizadas;

O NMS proporciona um amplo gerenciamento de falhas, incluindo as seguintes funções:

- Oferece monitoria contínua de mudanças nos dispositivos da rede;
- Oferece monitoria em *background* quando outros aplicativos MS *Windows* estão ativos;
- Exibe a localização de eventos da rede e os registra sem intervenção;
- Oferece notificação imediata sobre a ocorrência de problemas em

potencial através de alarmes em tempo real;

• Inicializa programas baseado em entradas de alarmes;

• Gera relatórios de alarmes e sugere possíveis soluções;

• Possibilita a personalização de notificação e filtragem de alarme;

• Mantém um histórico de problemas da rede;

• Testa a conectividade de dispositivos IP e IPX.

O NMS proporciona uma ferramenta SNMP MIB Browser, incluindo as seguintes funções:

• Monitora e controla dispositivos gerenciáveis por SNMP, tais como hubs e roteadores;

• Recebe alarmes de qualquer dispositivo SNMP na rede.

O NMS proporciona gerenciamento de endereços e monitoria de dispositivos críticos, incluindo as seguintes funções:

• Determina automaticamente todos os endereços IPX e IP na rede e os armazena no seu banco de dados;

• Permite que se vejam quem está usando determinado endereço e atribuem endereços exclusivos a novos usuários;

• Detecta endereços IP duplicados, assim que eles são colocados em uso;

• Permite selecionar dispositivos críticos e monitorá-los quanto a problemas.

O NMS proporciona gereciamento de roteadores para qualquer roteador que suporte MIB II, incluindo as seguintes funções:

• Monitora todos os roteadores na rede;

• Proporciona estatísticas de interface de roteadores;

• Exibe endereços IP e IPX da rede em forma tabular;

• Diagrama e compara a utilização de portas.

O NMS proporciona uma fácil manutenção de registros para planejamento e análise, incluindo as seguintes funções:

• Armazenam dados em um banco de dados central;

• São exportados dados para planilhas eletrônicas padrão para análise posterior;

• Possibilita imprimir a configuração da rede;

• Armazena informações de configuração de estação de trabalho introduzidas pelo usuário para fins de visualização e edição.

Quando usado com o *NetWare Management Agent*, o NMS proporciona um eficiente gerenciamento de servidor *NetWare*, incluindo as seguintes funções:

• Proporciona gerenciamento centralizado de múltiplos servidores NetWare;

• Monitora continuamente eventos de servidor;

• Notifica sobre problemas em potencial usando alarmes em tempo real;

• Proporciona gerenciamento de desempenho com gráficos em tempo real;

• Apresenta uma visão gráfica completa e intuitiva da configuração de servidores;

• Restringe acesso através de senhas de servidores.

O NMS é integrado ao *NetWare LANanaLyzer Agent* para proporcionar análise de rede distribuída a nível de segmento, incluindo as seguintes funções:

• Coleta remota informações de tráfego da rede em tempo real e em longo prazo;

• Proporciona um sumário instantâneo do estado de um segmento através do painel de controle da rede;

• Coleta informações em tempo real e em longo prazo para cada estação de trabalho e comunicação;

• Captura tráfego da rede e totalmente descodifica protocolos IP, IPX, SNA e *AppleTalk*;

• Oferece alarmes para condições de erro de tráfego;

• Suporta *Ethernet e token-ring*.

Quando usado com o *NetWare Hub Services Agent*, o NMS proporciona um eficiente gerenciamento de hub conforme ao HMI, incluindo as seguintes funções:

• Apresenta estatística tabular e gráfica da rede em tempo real;

• Proporcionam estatísticas do sistema, tais como condição, uso, fluxo de informações e colisões;

• Proporciona recursos de ativação e desativação de portas;

• Indica mudança de estado de porta;
• Inclui um utilitário de nomeação para personalizar *hubs* e portas de *hubs*.

FERRAMENTA OPENNMS

O openNMS é um software livre(open source) para gerenciamento de redes, desenvolvido em linguagem JAVA e utiliza banco de dados postgresql. Atualmente está na versão estável 1.8.9, conforme site do projeto, vide http://www.opennms.org/, que possui pacotes para os seguintes sistemas operacionais: *Linux, Solaris, Mac OS* X e *Windows* 2000, XP e vista.

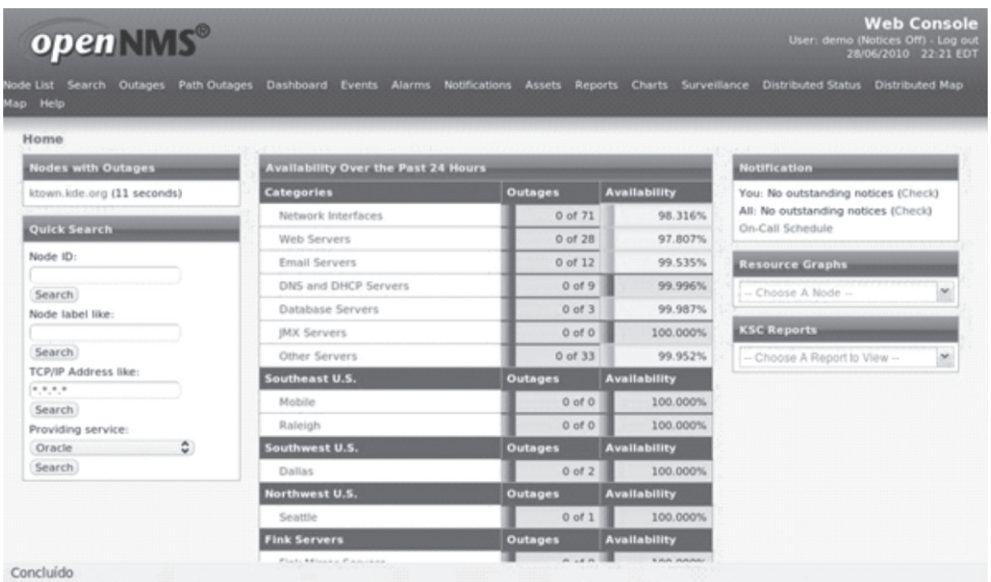

Figura 33 – Tela principal do OpenNMS.

Resumidamente, possui as seguintes características:
• Descoberta de dispositivos na rede e serviços;
• Monitoração e coleta de dados;
• Gráficos estatísticos e relatórios;
• Base dados para inventários.

FERRAMENTA NTOP

Ntop é um *software* livre, desenvolvido com a finalidade para monitoramento e análise de tráfego de rede, bem como atividades de gerência como: otimização da rede, planejamento e detecção de violações

de segurança são algumas características oferecidas por este aplicativo. Este também tem se mostrado uma ferramenta com grande simplicidade por possuir um rápido acesso para monitoramento de redes (baseado em interface *web*).

A grande vantagem de utilizar o *ntop* é devido a pouca necessidade de esforço e custo (para instalação e aprendizado) comparado a outras complexas e caras (apesar de sofisticados e flexíveis) plataformas de gerência.

Na página oficial do NTOP (http://www.ntop.org/) há documentações, binários, códigos fonte.

Possui como características e funcionalidades:

- Analisa os pacotes que trafegam na rede;
- Lista e ordena o tráfego de rede de acordo com vários protocolos;
- Exibe estatísticas de tráfego;
- Armazena estatísticas de forma permanentemente em bancos de dados;
- Identifica passivamente várias informações obre os hosts da rede, incluindo o sistema operacional executado e endereço de e-mail do usuário da estação;
- Exibe a distribuição do tráfego IP entre vários protocolos da camada de aplicação;
- Decodificam vários protocolos da camada de aplicação, inclusive os encontrados em *softwares* do tipo P2P;
- Atua como coletor de fluxos gerados por roteadores e switches através da tecnologia NETFLOW;
- Possui um *WebServer* integrado que permite consultas às informações através de um *browser*.

Instalação do NTOP

Para instalar o Ntop no sistema operacional Linux Ubuntu, utilize o *apt-get*:

```
# apt-get install ntop
```

Além da instalação do programa, outras operações foram efetuadas no seu servidor, tais como:

• O usuário "*Ntop*" foi adicionado ao sistema e será usado para executar o processo *Ntop*;
• O arquivo de inicialização foi instalado em /etc/init.d/ntop (Ubuntu) e configurado para ser iniciado no *boot*.

Deve-se criar após a instalação uma senha para o usuário que administrará o *Ntop*. Para fazê-lo, pode-se utilizar:

```
# /usr/sbin/ntop -P /var/lib/ntop -U ntop -A
```

Dentre as funcionalidades, a medição do tráfego consiste em ilustrar a utilização da rede por atividades relevantes. O *Ntop* acompanha a utilização da rede gerando uma série de estatísticas para cada "*host*" (cliente) em sua subrede e também por todas as outras subredes. Sendo assim, as informações que se desejam ser adquiridas, são coletadas pelo "*host*" (cliente com o ntop ativo) simplesmente observando o tráfego da rede. O modelo centrado no cliente favorece uma diminuição das necessidades para processar e adquirir dados de outros nós (computadores) ativos. Todos os pacotes da subrede são capturados e associados a uma dupla "remetente/destinatário", deste modo, é possível acompanhar todas as atividades de um host conectado a uma rede.

Quando uma violação de segurança ou má configuração da rede é detectada, *Ntop* oferece facilidades para gerar alarmes para o gerente de rede (via *email*, SNMP traps ou pequenos sistemas de envio de mensagem) e também de executar determinadas ações (se possível) com o objetivo de bloquear o ataque. Isso também possibilita manter a informação do tráfego armazenada em um banco de dados, esses registros podem ser usados para entender o ataque e prevenir futuros acontecimentos semelhantes.

O *Ntop* não é um *software* que possui arquivos de configurações editáveis. Alguns parâmetros podem ser setados pela interface web, mas a maioria deles são opções passadas pela linha de comando, no momento da inicialização. A tabela abaixo apresenta os principais parâmetros para o comando.

TABELA I – PARÂMETROS UTILIZADO PELA FERRAMENTA NTOP

Parâmetro	Descrição
- A	Define ou altera a senha do usuário administrador
- a <arquivo>	Habilitar logs no servidor *web*: Por padrão o *Ntop* não gera logs das requisições que seu servidor web recebe. Para habilitar, use esta opção acompanhada pelo nome do arquivo onde serão armazenadas as logs.
- b	Desabilita decodificadores de Protocolos: Os decodificadores examinam e coletam informações sobre vários tipos de protocolos das pilhas *NetBIOS, Netwares* e TCP/IP.
- d	Inicia o Ntop em modo *deamon* (*backgroud*): Este parâmetro é sempre incluído pelo script de inicialização.
- i <nome>	Nome da interfaces que são monitoradas
- K	Habilita o modo de depuração: útil para diagnosticar problemas do serviço.
- M	Não une o tráfego das interfaces de rede. Por padrão a Ntop une os dados coletados de todas as interfaces em um único conjunto de contadores. Em uma rede pequena local isto é interessante, pois gera uma imagem melhor de rede como um todo.
- m	Redes que serão consideradas locais.
- n	Não resolve endereços nome.
- p <caminho>	Caminho do diretório que contém os banco de dados do programa.
- p <arquivo>	Substitui os protocolos que o *Ntop* analisa por padrão pelos contidos no arquivo. Esta opção será vista em detalhes a seguir.
- u <usuário>	Usuário que executará o processo *Ntop*. Por padrão "*ntop*".
- W <porta>	Porta do servidor *Web* (HTTPS).Por padrão o servidor web não responde https, é necessário especificar a porta para habilitar o suporte. Um endereço pode ser especificado também no fomrmato "endereço: porta".
- w <porta>	Porta do servidor *Web* (HTTPS).Por padrão o *WebServer* escuta na porta 3000. Um endereço pode ser especificado também no formato: "endereço: porta".

Um exemplo de uso do ntop com um parâmetro, -i, definindo o monitoramento nas interfaces eth0 e eth1 da sua máquina:

```
# ntop –i eth0, eth1
```

Quanto ao modo web (ativado por padrão), o Ntop inicia seu próprio servidor (definido geralmente para executar via porta 3000 ou via porta 3001, caso tenha habilitado HTTPS). Para acessar o aplicativo via web, do seu servidor localhsot, abra seu browser e digite na barra de endereço a seguinte URL:

http://localhost:3000

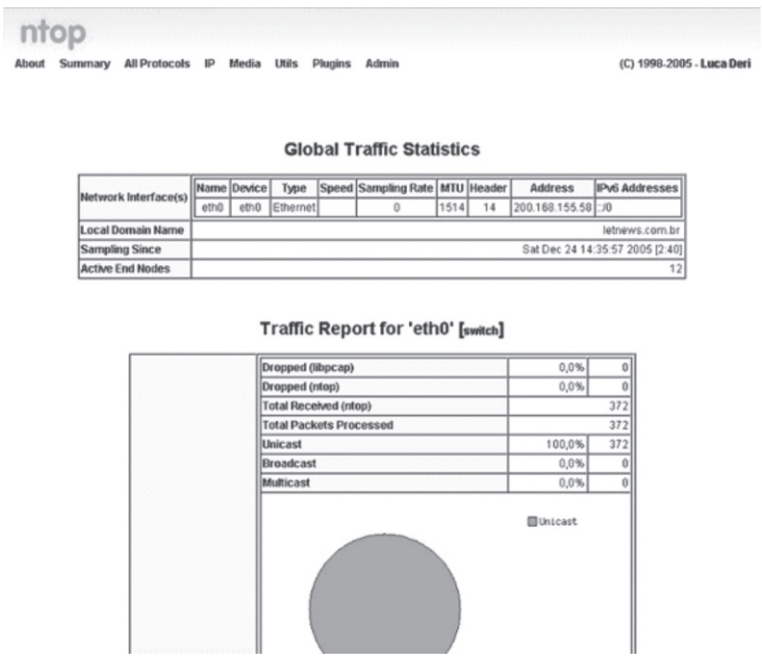

Figura 34 – Tela inicial do Ntop via interface *web*.

O Ntop monitora apenas um conjunto reduzido de protocolos, listados na tabela abaixo:

TABELA II – LISTA DE PROTOCOLOS E PORTAS MONITORADOS PELA FERRAMENTA NTOP

Protocolo	**Portas**
FTP	20 21
HTTP	80 443 3128
DNS	53
Telnet	23 513
NBios - IP	137 138 139
Mail	25 109 110
DHCP/BOOTP	67 68
DNMP	161 162
NNTP	119
NFS/AFS	2049 7000-7009
X11	6000-6010
SSH	22
Kazaa	1214
WinMX	6699 7730
eDonkey	4661-4665
Bit Torrent	6881-6999 6969
Messenger	1863 5000 5001

O NTOP monitora e gera relatórios sobre o tráfego e suporte dos hosts por estes protocolos.

Os relatórios do NTOP aparentam simplicidade no acesso, mas através deles é capaz de encontrar grande um volume informações da rede e dos hosts e seus detalhes. Acessando a seção "*All Protocols* > *Traffic*", você tem acesso a um relatório dos *hosts* de *internet* que foram acessados através da conexão, organizados de acordo com o volume de dados transferidos.

Os *hosts* recebem um ícone de classificação de acordo com o tipo de tráfego predominante. Uma bandeira verde indica um site que hospeda arquivos legítimos, enquanto um "K" indica um servidor do *Kazaa* ou um *tracker* Bittorrent. Clicando sobre os *hosts*, você tem acesso a um relatório detalhado com o tipo de tráfego, horários de maior acesso e, o mais importante, uma lista dos endereços IP da rede que acessaram o servidor, o que permite localizar estações rodando programas P2P ou outros aplicativos que consomem muito tráfego da rede.

A figura abaixo apresenta um relatório de uso de um conjunto de

protocolos, demonstrando os horários de picos na rede (maior quantidade de tráfego).

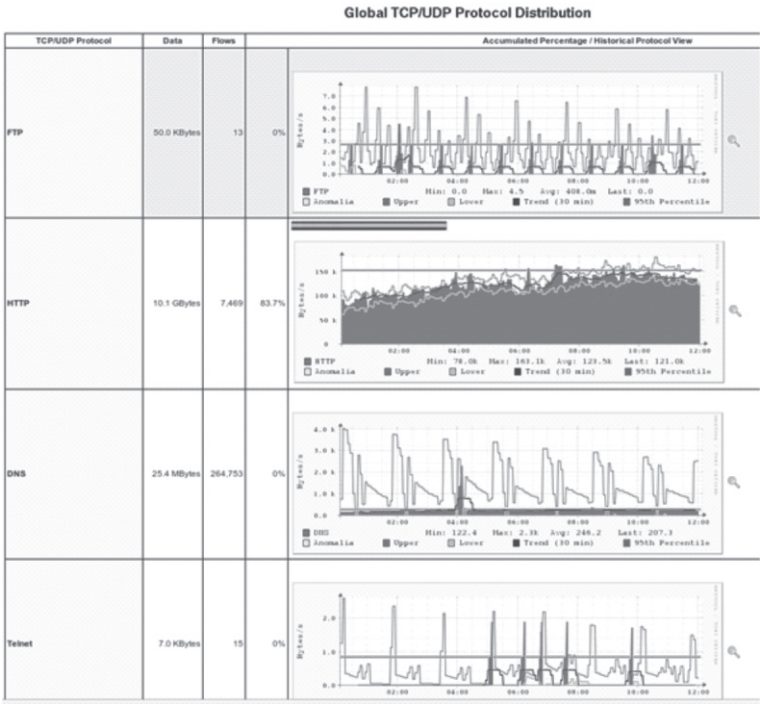

Figura 35 – Tela de relatórios de rede do NTOP.

COMPARANDO AS PRINCIPAIS FERRAMENTAS

Após apresentar um conjunto de ferramentas, a tabela abaixo apresenta os principais sistemas de gerenciamento, dentre eles o Cacti, Nagios e Zabixx, listando suas principais funcionalidades e características.

TABELA III – COMPARAÇÃO ENTRE AS PRINCIPAIS FERRAMENTAS DE MONITORAMENTO

	Cacti	Nagios	ZenOSS	Op Manager	BigBrother4	Spice works	Look@ LAN	Zabbix
SLA *Reports*	Não	Através de *Plugin*	Não	Em desenvol-vimento	Sim	Sim	Não	Sim
Auto *Discovery*	Através de *Plugin*	Através de *Plugin*	Sim	Sim	Sim	Sim	Sim	Sim
Agente	Não	Sim	Não	Não	Sim	Sim	Não	Sim
SNMP	Sim	Através de *Plugin*	Sim	Sim	Sim	Sim	Sim	Sim
Syslog	Não	Através de *Plugin*	Sim	Sim	Sim	Sim	Não	Sim
Permite Scripts Externos	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim
Plugins	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Linguagem que foi escrito	PHP	Perl	Python e Zope	Perl e Python	C	Ruby	C	C e PHP
Gatilhos/ Alertas	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Front end Web	C o n t r o l e Completo	Controle Parcial	Controle Completo	Controle Completo	Controle Completo	Controle Completo	Não	Controle Completo
Monitoramento Distribuído	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Inventário	Através de *Plugin*	Através de *Plugin*	Sim	Sim	Sim	Sim	Não	Sim
Método de Armazenamento de Dados	RRDTool, MySQL. PostgreSQL em desenvolvi-mento	MySQL, MSSQL	RRDTool para dados de performan-ce MySQL para eventos	MySQL, MSSQL	Oracle, MSSQL, MySQL	MySQL e SQLite	Não	Oracle, MSSQL, Postgree SQL e SQLite
Licenciamento	GPL	GPL	Core: GPLPro: Comercial Enterprise: comercial	Comercial 30 dias para testar o produto	Comercial	GPL	*Freeware*	GPL
Geração/ Gráficos/ Mapas	Sim/ Através de *Plugin*	Sim/ Sim	Sim/ Sim	Sim/ Não	Sim/ Sim	Sim/ Parcial	Sim/ Sim	Sim/ Sim
Eventos	Através de *Plugin*	Sim	Sim	Não	Sim	Sim	Não	Sim

EXERCÍCIOS

1 – Quais as principais ferramentas de código aberto adotadas para gerenciamento? Exemplifique.
2 – Quais as principais vantagens e desvantagens da ferramenta *Nagios*?
3 - Quais as principais vantagens e desvantagens da ferramenta *Cacti*?
4 - Comparado ao seu ambiente de trabalho, liste quais as funcionalidades que o NTOP pode prover a sua gerência de redes?
5 – Configurem e façam uso de uma das ferramentas descritas na unidade.

WEB-BIBLIOGRAFIA

http://aptlinux.blogspot.com/2010/04/instalando-o-nagios-3-no-debian.html
http://eng.registro.br/gter17/videos/02-Nagios.pdf
http://leandrotoledo.com.br/2010/10/02/utilizando-o-nagios-parte-i/
http://www.dicas.com.br/arquivo/configurando_o_nagios_no_debian_lenny__atualizado_.php
http://www.hss.blog.br/arquivos/nagios.pdf
http://fr34kz0id.blogspot.com/2010/12/monitorando-servicos-e-recursos-oracle.html
http://under-linux.org/wiki/Tutoriais/Monitoramento/cacti
http://www.cacti.net/
http://www.brainwork.com.br/blog/2010/04/04/instalando-e-configurando-o-cacti/
http://wiki.ubuntu-br.org/Cacti
http://wmunguiam.blogspot.com/2009/01/howto-install-cacti-ubuntu.html
http://pt.kioskea.net/faq/6353-instalacao-do-cacti-no-windows
http://commons.wikimedia.org/wiki/File:Zabbix_1.6.7_Dashboard.png
http://zabbixbrasil.org
http://br-linux.org/2010/tutorial-gerenciamento-de-redes-com-opennms/
http://www.opennms.org/get-opennms/
http://imasters.com.br/artigo/6498/redes/monitorando_redes_utilizando_ntop/
http://www.drsolutions.com.br/exemplos/ntop.pdf
http://www.jffnms.org/docs/HowTO_JFFNMS_on_sarge-1.2.pdf
http://www.jffnms.org/docs/JFFNMS_Installation_Guide_for_Windows_XP_Pro_SP2.pdf

http://www.mar.mil.br/sdms/artigos/6951.pdf
http://www.slackware-brasil.com.br/web_site/downloads/ artigos/ monitoramento _redes.pdf
http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Alex%20Martins%20Garcia%20-%20Artigo.pdf
http://www.ppgia.pucpr.br/~jamhour/Download/pub/RSS/MTC/referencias/TCC-2009.pdf
http://www.openxtra.co.uk/blog/hub-projects-in-open-source-network-management/
http://www.malima.com.br/article_read.asp?id=49

Referências

SZTAJNBERG, Alexandre, Gerenciamento de Redes. COPPE-UFRJ.

DIAS, Beethovem Zanella, ALVES JR, Nilton. **Protocolo de Gerenciamento** SNMP. CBPF-NT-006/01.

SANTOS, Eduardo Erlê dos (UFSC), KOCH, Fernando Luiz (Univ Utrecht), ASSUNÇÃO, Marcos Dias de (UFSC), WESTPHALL, Carlos Becker (UFSC). **Agentes Coletores na Gerência de Redes de Computadores.**

WAGNER, Hélcio e EDUARDO, Iguatemi. Gerência de Redes de Computadores – UERN.

HUNT, Craig. Linux Servidores de Rede. Rio de Janeiro: **Ciência Moderna**. 2004

SANTOS, Madson da Silva. **Estudo de Gerenciamento da Rede de Distribuição com o Protocolo SNMP e Tutorial para Implantação de Ferramentas de Gerência**. CET, 2006.

RIBEIRO, John. IDG News Service.Local, 30 de jan, e 01 fev. 2008.Disponível em:
<http://idgnow.uol.com.br/telecom/2008/02/01/flag-telecom-enviara-navio-para-consertar-cabo-de-rede-rompido/>.

JUNQUEIRA, Wagner Ribeiro, DÉO, André Luis Boni, **Implementando gerenciamento de redes de computadores usando Nagios e Zabbix**. Universidade Estadual de Campinas (UNICAMP), Campinas – SP, Brasil.

Minicurrículo

JOSÉ VALDEMIR DOS REIS JUNIOR

Possui graduação em Bacharelado em Ciência da Computação pela Universidade Federal do Piauí (2006) e mestrado em Engenharia Elétrica, subárea Telecomunicações, na Universidade de São Paulo em São Carlos (2009). Tem experiência na área de Ciência da Computação, com ênfase em Redes de Computadores, Sistemas Operacionais Linux, Técnicas de Correção e Detecção de Erros e Segurança da Informação. Na área de Engenharia Elétrica, ênfase em Modelagem de Redes Ópticas Baseada na Técnica de Acesso Múltiplo por Divisão de Códigos (O-CDMA) e Redes Ópticas Passivas - PON.

Atualmente, é Professor e Coordenador do Curso Técnico em Informática do Colégio Técnico de Teresina, vinculado a Universidade Federal do Piauí, bem como professor conteudista, na área de Informática, da E-Tec vinculada ao Colégio Agrícola de Floriano – CAF/UFPI e da Universidade Aberta do Piauí – UAPI.

Currículo Lattes: http://lattes.cnpq.br/5892952730297435

www.uapi.ufpi.br