UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

ILDEBRANDO TADEU ANDREATTA JUNIOR

MÉTODOS E TÉCNICAS DE BOA PRÁTICA PARA IMPLEMENTAÇÃO DE UM NETWORK OPERATION CENTER (NOC)

MONOGRAFIA

CURITIBA
2011

ILDEBRANDO TADEU ANDREATTA JUNIOR

MÉTODOS E TÉCNICAS DE BOA PRÁTICA PARA IMPLEMENTAÇÃO DE UM NETWORK OPERATION CENTER (NOC)

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná
Orientador: Prof. M.Sc. Fabiano Scriptore de Carvalho

CURITIBA
2011

AGRADECIMENTOS

Agradeço primeiramente a Deus pela oportunidade de estar fazendo este curso e realizando esse estudo.

Ao meu orientador Prof. M.Sc. Fabiano Scriptore de Carvalho pela paciência e pelo alto grau de conhecimento no assunto que muito auxiliou no processo de desenvolvimento e qualidade deste trabalho.

Aos meus pais Ildebrando T. Andreatta, Sandra Andreatta e minha namorada Cibeli Barsh Fagundes Cellarius pela compreensão e pela força que sempre me estimulou para o andamento deste trabalho.

A Profa. Dra. Faimara do Rocio Strauhs

Aos meus colegas de sala.

Os problemas significativos que enfrentamos não podem ser resolvidos no mesmo nível de pensamento em que estávamos quando os criamos.

(EINSTEIN, Albert, s.d.)

RESUMO

ANDREATTA JUNIOR, Ildebrando Tadeu. **Métodos e técnicas de boas práticas para a implantação de um Network Operation Center (NOC)**. 2011. 40.folhas. Monografia (Especialização em Configurações e Gerenciamento de Servidores e Equipamentos de Redes) - Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

Este projeto tem por intuito definir maneiras de implementar um centro de gerenciamento de redes, onde tem como atores: computadores, ISPs, equipamentos de rede e afins. Está contido nesse projeto também as melhores práticas e técnicas a serem utilizadas em uma gerência de redes, tem também o objetivo de gerenciar SLAs, ajudar a identificar falhas, e ter um controle em tempo real de todos os equipamentos contidos nesta gerência. Dissertar de forma clara e simples as melhores técnicas de implementação de um NOC, para que de fato esta gerência seja confiável e ágil. Hoje existem diversas ferramentas e muitas maneiras de se fazer este controle. O objetivo deste trabalho é mostrar de forma detalhada e exemplificada as diversas opções de ambientes simples até ambientes mais críticos, mostrando os resultados obtidos com cada ferramenta para comprovar que o estudo tem efeito de mostrar qual a melhor ferramenta versus técnica para cada tipo de ambiente.

Palavras-chave: Gerenciamento de redes. Melhores práticas. *Network Operation Center* (NOC).

ABSTRACT

ANDREATTA Junior, Ildebrando Tadeu**. Methods and techniques of good practice for the implementation of a network operation center (NOC)**. 2011. 40 pages. Monograph (Specialization in Settings and Server Management and Network Equipment) - Federal Technological University of Paraná. Curitiba, 2011.

This project is meant to identify ways to implement a network management center, which features actors: computers, ISPs, network equipment and the like. Is contained in this project also the best practices and techniques to be used in a network management, also has the objective of managing SLAs, help identify gaps, and have a real-time control of all equipment contained in this management. Lecture clearly and simply the best technical implementation of a NOC, that in fact it manages to be reliable and agile. Today there are many tools and many ways to do this control, the aim of this paper is to show in detail and exemplified the various options for simple environments to more critical environments, showing the results obtained with each tool to prove that the study has the effect of show what the best tool versus technique for each type of environment.

Keywords: Network management. Best practices. NOC.

LISTA DE SIGLAS

CMIP	Common Management Information Protocol
CMOT	CMIP Over TCP/IP
CORBA	Common Object Request Broker Architecture
CPU	Central Processing Unit
DEC	Digital Equipment Corporation
GPL	General Public License
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	Provider International Organization for Standardization
ISP	Internet Service
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
MIB	Management Information Base
NOC	Network Operation Center
OMG	Object Management Group
OSI	Open Systems Interconnection
RMON	Remote Network Monitoring
RRD	Round-Robin Database
RRD Tool	Round-Robin Database Tool
SLA	Service Level Agreement
SMI	Structure of Management Information
SMS	Short Message Service
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
UDP	User Datagram Protocol
WAN	Wide Area Network

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A internet é um amplo sistema de redes interconectadas, que forma um sistema de comunicação a nível mundial. Existem muitos equipamentos e várias formas dos mesmos serem interligados e compartilhados, dentre diversos meios de acesso, protocolos e níveis de segurança. (MENDES, 1.ed,2008).

Como toda conexão, independente da distância está suscetível a falhas por inúmeros fatores, será abordado as formas de prever falhas em um sistema de comunicação e de como implementar uma gerência de redes. (MENDES, 1.ed,2008).

1.1 TEMA

Em meados da década de 1960, onde houve as primeiras conexões entre computadores por meio de redes com diferentes meios físicos, foi o inicio de uma história em busca da eterna evolução e expansão deste conceito (MENDES, 1.ed,2008).

As décadas se passaram e cada vez mais o homem ficou dependente dos serviços disponibilizados por dispositivos pessoais, logo houve a ampla ascensão no mundo tecnológico e novos equipamentos são lançados no mercado a fim de suprir a grande demanda tecnológica da época, e como um grande sucesso, que acabou tornando os dispositivos em objetos de uso essencial em todo o mundo tudo em uma grande rede, onde estão interligados diretamente com todo o mundo.

Sob esta facilidade de se conectar e estabelecer contato entre computadores em diversos pontos remotos espalhados por um determinado espaço físico existe uma gama de equipamentos e meios físicos que interligam os mesmos para obter a conexão entre um dispositivo e outro. Escalonado em grandes proporções, começou a se perceber que tal quantidade de equipamentos era suscetível a falhas, causando grandes transtornos e prejuízos pelas falhas na rede ou indisponibilidades, foi então que administradores destes sistemas começam a perceber que existe uma grande

dificuldade de gerenciar todos os equipamentos e ter informações em tempo real da rede (TANENBAUM, 4.ed, 2003).

Em ambientes grandes e distribuídos, tais como operadoras de telecomunicações, e grandes *backbones*[1] como fazer esse controle?

A idéia foi criar um conceito de administração de rede centralizado, onde envolveria uma equipe e *softwares* especializados que fazem todo este controle em tempo real. Mas, como todo princípio, ainda não havia nada concretizado, e nem uma fórmula para a criação desta gerência, vieram então os primeiros passos para um controle de redes, as primeiras empresas a adotarem uma equipe de monitoramento de redes, eram os fornecedores de mainframes também na década de 1960 quando as conexões eram de banda insuficiente entre terminais e *mainframes*.

No decorrer deste trabalho estarão enfatizadas as técnicas, os diferentes protocolos e as formas de gerência de redes.

1.2 PROBLEMAS E PREMISSAS

Atualmente as redes de computadores são ambientes suscetíveis a expansões, essa malha de telecomunicação passou a exigir mais do profissional que gerência e mantém esta estrutura, esse agravante impossibilita que o gestor tenha o controle em tempo real de sua infra-estrutura.

Com um ambiente cada vez maior, as falhas são mais difíceis de serem identificadas, sendo necessário implementar um modelo de gerência para cada ambiente de rede.

Para auxiliar nesse processo existem padrões e *softwares* que fazem em conjunto uma gerência de rede, possibilitando ao gestor manter o seu ambiente controlado com status em tempo real e notificações dos eventos da rede, tais como indisponibilidades de servidores, falhas em segmentos distribuídos, gerência de

---

[1] *Backbone* si*gnifica rede de transporte,* designa o esquema de ligações centrais de um sistema mais amplo, tipicamente de elevado desempenho.

hosts remotos entre outros incidentes de rede comuns ocorridos em redes de computadores.

Para profissionais de Tecnologia de Informação (TI), é de fato um grande apoio a gestão do seu ambiente, podendo evitar, prevenir e localizar falhas na rede.

1.3 OBJETIVOS

1.3.1 OBJETIVO GERAL

Mensurar as diferentes formas de gerência de redes e identificar qual a melhor forma de gerência para cada tipo de rede e as melhores práticas para a implementação.

1.3.2 OBJETIVOS ESPECÍFICOS

- Avaliar a viabilidade técnica para implementar um *network operation center* em cada tipo de ambiente;
- Definir quais as melhores ferramentas e suas combinações em cada tipo de rede;
- Mostrar a melhor forma de implementação, detalhando as técnicas utilizadas para cada tipo de gerência;
- Comprovar a eficiência da aplicação dos métodos e técnicas implantados;
- Detalhar as formas de gerência de rede e seus modelos;

1.4 JUSTIFICATIVA

Desenvolver um estudo que demonstre e cite os métodos e técnicas para a implementação de uma gerência de redes usando o conceito de *network operation center*.

Este estudo foi iniciado pelo fato de ser usado além de um trabalho de conclusão de curso de especialização, é também um material de referência voltado para profissionais da área de TI e empresas especializadas para detalhamento e embasamento em cada técnica descrita neste trabalho.

Outro grande motivo do desenvolvimento deste trabalho de pesquisa foi a ausência deste tipo de referencial teórico para este assunto, que se faz a cada dia mais importante o seu uso nas diversas empresas e todo tipo de rede presente no nosso dia a dia.

1.5 MÉTODOS DE PESQUISA

Fazer uma revisão bibliográfica a respeito dos principais tipos de gerência de redes. O método de pesquisa será de caráter exploratório experimental cujo objetivo é reunir informações aplicáveis a este trabalho, utilizando livros, artigos, revistas, internet, catálogos de fabricantes, softwares, análise em ambientes em produção e outros.

Serão avaliadas as mais diversas estruturas de rede, tanto em redes com aplicações reais como em ambientes de simulação.

Para realizar os testes de campo, serão utilizadas algumas ferramentas de monitoramento de rede, como por exemplo, o *software* Nagios e algumas ferramentas de medição de tráfego: Cacti, Zabbix.

As ferramentas utilizadas serão de natureza *freeware*, *open source* e *software* livre. O sistema operacional do servidor onde as ferramentas serão hospedadas é um ambiente Linux Debian 6.0.

As medições comparativas de campo serão feitas periodicamente, durante o período de um mês. As medições serão tabeladas em planilhas.

Após a coleta de dados, serão gerados gráficos com os dados das planilhas. Serão então, comparados os melhores resultados de cada ambiente, sob qual ferramenta está, e cada gráfico representará a prática utilizada, por fim, a conclusão do presente.

1.6 ***ESTRUTURA***

A monografia é composta basicamente por 4 capítulos. O capítulo 1 tratará da parte introdutória sobre redes e gerência, sendo apresentado o tema, os objetivos a serem atingidos, a justificativa que motivou o inicio do estudo, e os problemas a serem resolvidos. Ainda neste capítulo apresentam-se os métodos de pesquisa utilizados na produção deste trabalho e a estrutura da monografia.

O capítulo 2 tratará do referencial teórico, que é composto pela apresentação básica do conceito de redes e gerência, modelo OSI (*Open System Connection*), explanando de forma clara sobre os protocolos de gerência de redes, modelos de gerência de redes, diferenciando os tipos de gerência de redes, métodos e melhores práticas de gerência de redes.

Iniciando a parte prática do trabalho, o capitulo 3 fará referência nos cenários que serão estudados, apresentando de forma clara e simplificada as ferramentas disponíveis que serão trabalhadas para realizar a análise contextual deste trabalho. Tratará as principais técnicas para implementação do gerenciamento de rede com um determinado modelo de gerência.

Para finalizar a monografia, o capítulo 4 trará as conclusões obtidas com base no estudo teórico descrito nos capítulos anteriores, bem como as referências do conteúdo geral.

2 REFERENCIAL TEÓRICO

A cada ano, novas aplicações e novos usuários impulsionam o crescimento das redes de computadores internas (*intranets*) e externas (*extranets e Internet*) tanto em escala como em complexidade. A necessidade de monitorar essas redes diante desse crescimento impulsiona também o desenvolvimento de *softwares* cada vez mais aprimorados tecnicamente e abrangendo uma gama maior de características, adaptando-se às novas tecnologias lançadas ao mercado anualmente. Neste ínterim, o gerenciamento de tais redes tornou-se uma tarefa indispensável para manter o correto funcionamento.

Para se realizar a tarefa de gerenciar redes de computadores é necessário o uso de *softwares* específicos (aqui chamadas de ferramentas), dado o notório aumento do número de dispositivos a serem gerenciados, o que impede um tratamento individualizado de cada um, bem como dado a necessidade de procedimentos automatizados, de configurações, monitoração, entre outros.

A adoção de um *software* de gerenciamento não resolve todos os problemas da equipe responsável pela administração da rede. Geralmente o usuário de uma ferramenta de gerenciamento espera muito dela e, consequentemente, fica frustrado quanto aos resultados que obtém. Por outro lado, essa mesma ferramenta é subutilizada, isto é, possui inúmeras características inexploradas, ou utilizadas de forma pouco eficiente. Para gerenciar um recurso é necessário conhecê-lo e visualizar claramente o que este recurso representa no contexto da rede. (COMER, 4ª ed., 2007).

2.1 *MODELOS DE GERÊNCIA*

Para gerenciar uma rede é essencial levar em conta os *softwares*, os padrões e principalmente os modelos que garantem ao administrador de redes a eficiência e a confiabilidade sob a gerência aplicada. Os modelos são diferentes na questão de sua organização, no que se refere à disposição dos administradores de rede, é levado em conta também a distribuição dos gerentes na rede.

Existem dois modelos usados para a gerência de rede:

- Modelo Internet;
- Modelo OSI

2.1.1 **MODELO INTERNET**

O modelo de gerenciamento Internet aborda tanto o agente quanto o gerente, o qual os agentes correspondem às informações sobre os recursos locais, e o papel do gerente é apenas requisitar as informações contidas nos agentes.

O padrão utilizado pelo modelo Internet é o SMI (*Structure of Management Information*) que tem como especificação a metodologia de definição da informação de gerenciamento armazenada na MIB. É pela MIB que são definidos os elementos e as informações de gerenciamento e também variáveis e tabelas de variáveis. O modelo SMI usa o subconjunto de dados do tipo ASN.1. (LOPES, 2003).

2.1.2 **MODELO OSI**

O gerenciamento através do modelo OSI que é mantido pela ISO, é baseado na teoria da orientação a objetos. O sistema trata os recursos gerenciados através de entidades lógicas que recebem a rotulação de objetos gerenciados.

Este modelo delega funções de monitoração para os seus agentes, porém as funções de controle ficam sob responsabilidade do gerente, pois não há como adaptar a codificação em classes de objetos, portanto o conhecimento e as tomadas de decisões ficam sob responsabilidade do gerente, o oposto do conhecimento que se refere a monitoração que por sua vez é mais simples e normalmente é estático e periódico. (LOPES, 2003).

As áreas funcionais do modelo OSI são subdivididas da seguinte forma:

- Gerência de configuração (gerência o estado da rede);
- Gerência de desempenho (tráfego de rede e taxas de erro);
- Gerência de falhas (notificação de comportamento anormal da rede);
- Gerência de contabilidade (consumo de recursos de rede);
- Gerência de segurança (trata questões de acesso e permissões);

Os aspectos mais importantes que devem ser considerados no modelo de gerenciamento OSI é o fato de que o modelo possui agentes mais complexos de serem desenvolvidos, o que consome mais recursos dos elementos de rede, devido a diminuição dos pedidos de dados (*pollings*) necessários para obter esta informação dos objetos gerenciados, cabendo ao gerente a alocação de tarefas mais "inteligentes".

2.2 ***PROTOCOLOS DE GERÊNCIA***

2.2.1 **PROTOCOLO SNMP**

Até o inicio da década de 1980, redes de computadores eram baseadas em arquiteturas e protocolos patenteados, a exemplo de *System Network Architecture* (SNA) da IBM e DECNET da Digital Equipment Corporation. Já no final da década de 1980, redes interconectadas baseadas na arquitetura e protocolos TCP/IP estavam em franca ascensão. Porém do ponto de vista de gerência de tais redes a situação ainda favorecia arquiteturas proprietárias, devido a inexistência de soluções de gerência de redes TCP/IP. Com o crescimento das redes TCP/IP, aumentaram consideravelmente as dificuldades de gerência. A demora no aparecimento de soluções abertas baseadas no modelo OSI fez com que um grupo de engenheiros decidisse elaborar uma solução temporária baseada num novo protocolo: *Simple*

Network Management Protocol (SNMP). A simplicidade do SNMP facilitou sua inclusão em equipamentos de interconexão.

Hoje praticamente todos os equipamentos de interconexão dão suporte a SNMP, bem como muitos outros dispositivos (*nobreaks*, modems, etc.), e sistemas de *software* (servidores Web, sistemas de banco de dados, etc.).

Os principais objetivos do protocolo SNMP são:

- Reduzir o custo da construção de um agente que suporte o protocolo;
- Reduzir tráfego de mensagens de gerenciamento pela rede necessárias para gerenciar os recursos de rede;
- Reduzir o número de restrições impostas às ferramentas de gerenciamento de rede, devido ao uso de operações complexas e pouco flexíveis;
- Apresentar operações simples de serem entendidas, sendo facilmente usadas pelos desenvolvedores de ferramentas de gerenciamento;
- Permitir facilmente a introdução de novas características e novos objetos não previstos ao se definir o protocolo;
- Construir uma arquitetura que seja independente de detalhes relevantes e algumas implementações particulares;

O protocolo SNMP comumente utilizado para a gerência de redes UDP é referenciado no modelo OSI na camada de aplicação. (FARREL, 2003).

Camada	Protocolo
5.Aplicação	HTTP, SMTP, FTP, SSH, Telnet, SIP, RDP, IRC, **SNMP**, NNTP, POP3, IMAP, BitTorrent, DNS, Ping ...
4.Transporte	TCP, UDP, RTP, SCTP, DCCP ...
3.Rede	IP (IPv4, IPv6) , ARP, RARP, ICMP, IPsec ...
2.Enlace	Ethernet, 802.11 WiFi, IEEE 802.1Q, 802.11g, HDLC, Token ring, FDDI, PPP,Switch ,Frame relay,
1.Física	Modem, RDIS, RS-232, EIA-422, RS-449, Bluetooth, USB, ...

Tabela 1 – Protocolos comuns no modelo OSI. Fonte: (MENDES, 2008).

Uma rede gerenciada pelo protocolo SNMP é formada por três componentes principais:

- Dispositivos geridos (objeto gerenciado);
- Agentes (hospedado no objeto gerenciado);
- Aplicação de Gerenciamento;

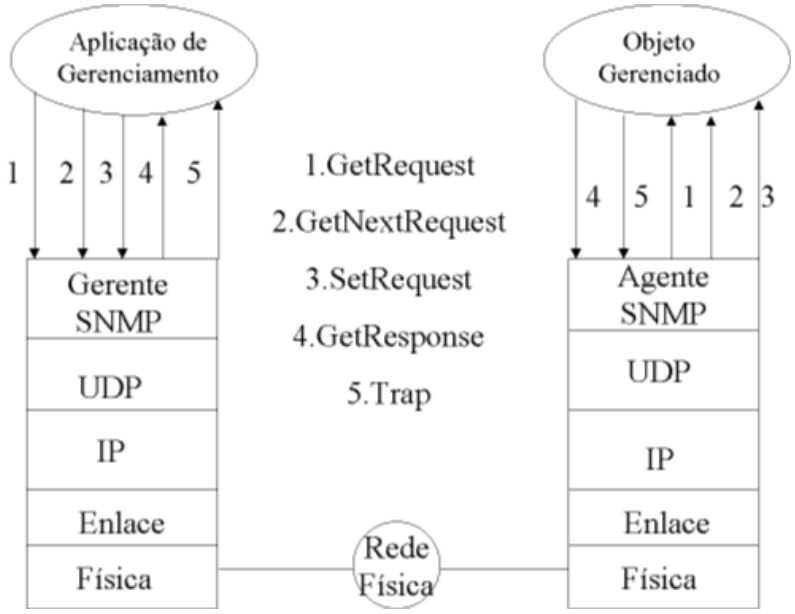

Figura 1 – Esquema de funcionamento protocolo SNMP. Fonte: (TANENBAUM, 2003).

O agente gerenciado é considerado um nó de rede que possui um agente SNMP instalado e se encontra na rede gerenciada.

Os agentes são módulos de *software* de gestão que ficam armazenados em um dispositivo e tem o conhecimento das informações de gestão local que traduz esses dados para o padrão do protocolo SNMP.

O sistema de gestão de redes é um sistema responsável pela aplicação que controlam e gerenciam os dispositivos mantidos pelo sistema, normalmente é instalado em um servidor dedicado a este tipo de aplicação.

2.2.2 **PROTOCOLO RMON**

O *Remote Network Monitoring MIB* (RMON) é um protocolo de gerência de redes no padrão IETF, portanto não é uma solução proprietária. A solução é completa e ao mesmo tempo complexa, onde dificilmente um fabricante irá implementar a solução por completa. (TANENBAUM,2003).

Em um ambiente de gerenciamento *RMON*, os dispositivos de rede carregam as *MIBs RMON*, um sistema de gerenciamento que trabalha com este protocolo permite alarmes e notificações ao usuário, também pode utilizar-se dos dados para a análise que interage com os grupos *RMON*.

Entre os principais protocolos de gerência o *RMON*, é um dos primeiros a permitir a gerência proativa, certamente esta a grande vantagem em relação aos demais protocolos na mesma arquitetura de gerência.

Este trabalho de gerência é simplificado, algo que facilita a resolução dos problemas, sempre visando manter a alta disponibilidade da rede com uma diminuição de custos de forma significativa.

Em contrapartida toda esta vantagem torna o *RMON* um protocolo que atua apenas na camada *MAC* do modelo de referência *OSI*. O gerenciamento em camadas superiores permite um protocolo de gerenciamento ponto-a-ponto do tráfego. (FARREL, 2003).

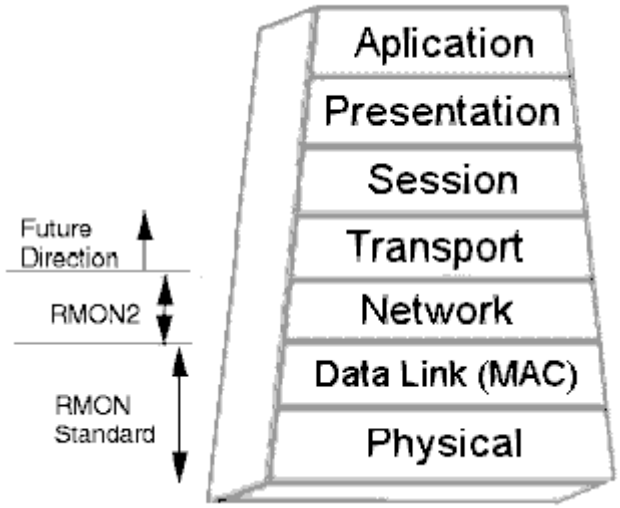

Figura 2 – Representação do RMON no modelo OSI. Fonte: (FARREL,2003)

Sendo assim pode-se afirmar que os objetivos do RMON são:

- Reduzir o volume de informação trocada entre a rede local gerenciada, e a estação remota do gerente;
- Fazer com que seja possível a gerência contínua de segmentos de redes locais, mesmo quando a conexão com o elemento RMON esteja temporariamente indisponível;
- Possibilitar a gerência proativa da rede, diagnosticar e registrar os eventos que possibilitem detectar uma falha e até mesmo prevenir um incidente que evite o seu funcionamento.

2.2.3 **PROTOCOLO PROXIES**

O proxies é um protocolo simples que utiliza dos padrões do SNMP, bem como as estações de gerência com o mesmo padrão, o protocolo permite conexões TCP quanto UDP, fato esse de que limita o gerenciamento direto para dispositivos e não permite a outros como, modems e bridges que não dão suporte a pilha de protocolos TCP/IP.

Para dispositivos que não há suporte à SNMP, foi criado o conceito de proxy, no caso deste protocolo, o SNMP atua como proxy para um ou mais dispositivos. (FARREL, 2003).

2.2.4 **PROTOCOLO CMIP**

O CMIP é um protocolo que é gerenciado e mantido sob os padrões de gerenciamento OSI, o qual especifica quais os elementos de protocolo que serão utilizados para prover os serviços de notificações.

Sua arquitetura é implementada usando o conceito de orientação a objetos e se baseia em eventos, sua aplicabilidade é usada em diferentes camadas do modelo

OSI, incluindo a camada de aplicação e seu uso é restrito devido a sua aplicabilidade. (FARREL, 2003).

2.2.5 **PROTOCOLO CMOT**

O protocolo CMOT surgiu com o objetivo prover a convivência das arquiteturas do modelo Internet e do protocolo de gerenciamento OSI, este modelo tem referência de estrutura de gerenciamento OSI, nos modelos protocolos e serviços desenvolvidos pela ISO para a gerência de redes. O CMOT pode ser aplicado com sua estrutura gerencial OSI sobre objetos gerenciados de uma rede TCP/IP. (FARREL, 2003).

2.2.6 **PROTOCOLO CORBA**

CORBA (*Common Object Request Broker Arquitecture*) é um protocolo que atualmente está em desenvolvimento pelo OMG (*Object Management Group*), que visa oferecer mecanismos para que de forma transparente possa enviar e receber solicitações e respostas.

Este protocolo fornece uma estrutura de interoperabilidade entre objetos, como linguagens diferentes, máquinas diferentes e até mesmo em ambientes heterogêneos distribuídos. (FARREL, 2003).

2.3 ***TIPOS DE GERÊNCIA***

2.3.1 **Gerência centralizada**

Uma gerência centralizada é definido por um único gerente que controla todo o processo da rede. Na existência de um problema é mais crítico gerenciar o incidente devido à gerência ser feita por um individuo apenas, podendo depender das

características de cada incidente. Também deve ser considerado que a cada crescimento da rede, torna-se mais difícil fazer uma gerência centralizada devido ao crescimento da estrutura de rede. Um ambiente que pode ser gerenciado por este modelo é uma empresa de pequeno ou médio porte, onde a rede não é consideravelmente grande, mas que sofre crescimento em determinado período, se tornando cada vez mais critico uma gerência centralizada, considerando o número de ativos a serem monitorados na rede. (TORRES,2009).

2.3.2 **Gerência descentralizada**

Na gerência descentralizada a distribuição das atividades são feitas por vários nós, ou seja, permite a gerência de forma hierárquica, onde cada nó é responsável por gerenciar o seu ambiente. Uma forma de exemplificar a gerência descentralizada em um ambiente de um banco, onde tem a gerência de matrizes, cada uma com seus responsáveis pela gerência, e com as agências, que também exigem uma gerência pelo fato que, independente do tamanho do segmento, um ponto de falha considerado crítico. (LOPES,2003).

2.3.3 **Gerência reativa**

Numa gerência reativa, os administradores da rede são alertados dos seus problemas ocorridos na sua infra-estrutura, e o grande diferencial das outras gerências é que o mesmo administrador que recebe o evento ou notificação, é quem vai estar atuando na solução do incidente. Esta gerência é muito comum em empresas de pequeno e médio porte, onde existe um número de pessoas relativamente pequeno para gerenciar e atuar na prevenção e solução de incidentes. (LOPES,2003).

2.3.4 **Gerência proativa**

Uma gerência proativa consiste em um aumento em larga escala das redes de computadores e que a cada passo do seu crescimento exige uma gerência mais eficaz, sempre com o intuito de evitar e tratar preventivamente futuras falhas e interrupção do serviço. Um exemplo prático de gerência proativa é a rede de uma operadora de telecomunicações, onde a cada dia são formados novos enlaces com outras redes, até mesmo novas redes, expandindo exponencialmente em um curto período. (LOPES, 2003).

2.4 ***MELHORES PRÁTICAS PARA GERÊNCIA DE REDES***

Melhores práticas para uma gerência de redes é baseado em falhas e problemas ocorridos em redes de telecomunicação. Com base no ocorrido são criados os padrões, modelos e técnicas para evitar que tais incidentes ocorram e ainda facilitem o gerenciamento do escopo da infraestrutura.

2.4.1 **Gerência de rede e gerência de sistema**

Na gerência de uma infraestrutura organizacional podemos dividir em duas situações de gerência, uma são os dispositivos em sua forma física, avaliando seu comportamento e sua atividade na rede, outra questão é a gerencia de sistema, que consiste em coletar dados específicos de processos existentes dentro de dispositivos gerenciados fisicamente na rede. (COSTA, 2008).

2.4.1.1 Elementos a serem gerenciados na rede:

- Roteadores;
- Modems;
- Switches;
- Hubs
- Servidores;
- Multiplexadores;
- Enlaces.

Tarefas padrões de gerenciamento desses elementos:

- Configurações dos dispositivos;
- Administração dos endereços IPs;
- Serviços de diretório;
- Monitoramento de tráfego;
- Diagnóstico de faltas;
- Tratamento de alarmes;
- Restauração de serviços;
- Segurança de rede;
- Inventário.

2.4.1.2 Elementos a serem gerenciados em sistemas:

- Servidores de arquivos;
- Servidores de impressão;
- Servidores de banco de dados;
- Servidores de aplicação;
- Servidores de correio eletrônico.

Tarefas padrões de gerenciamento desses elementos:

- Monitoramento de desempenho;
- Inventário;
- Controle de licença de *software*;
- Gerência de contas de usuários;

- Backup;
- Segurança de sistemas.

2.4.2 **Desempenho**

O desempenho no quesito de gerência de redes, é algo fundamental, e seu histórico de informação é de grande utilidade para previsões de falhas, esses dados são usados para que exista a garantia que a rede opere em conformidade com a qualidade e disponibilidade de serviços acordados com os usuários.

Pontos que devem ser avaliados no quesito desempenho são:

- Caracterizar o tempo de latência;
- Tempo de espera em fila;
- Utilização do meio físico e do equipamento.

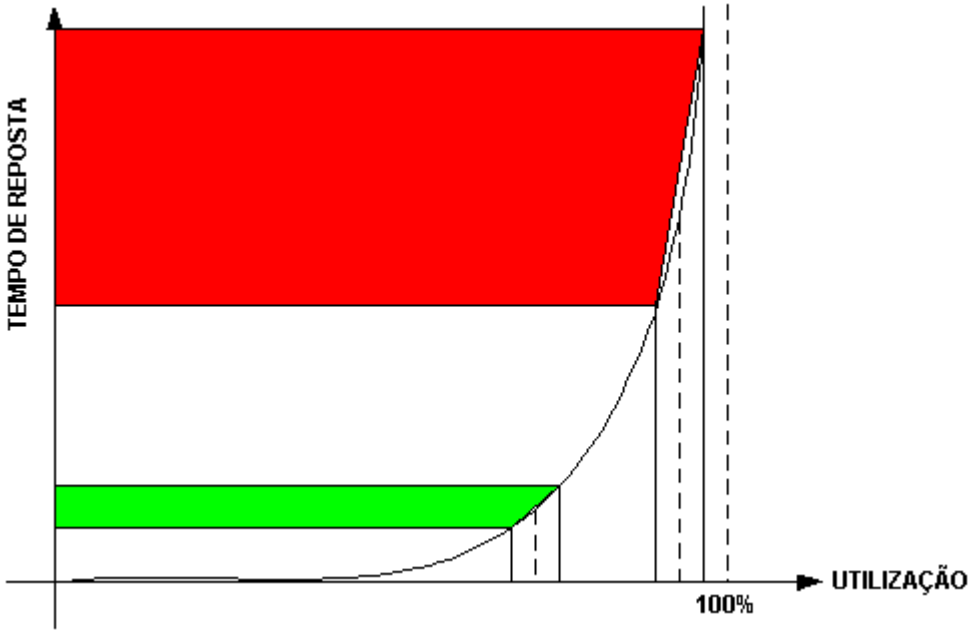

Figura 3 - Gráfico representativo de tempo de latência. Fonte: (BLACK, 2008).

Abaixo a tabela que representa a disponibilidade por ano levando em consideração as horas de *downtime*:

% disponível	Descrição	Tempo em downtime
95%	Testes ou protótipos	438 horas por ano
99,50%	Baixa disponibilidade	44 horas por ano
99,95%	Boa disponibilidade	4 horas por ano
99,98%	Alta disponibilidade	2 horas por ano
99,99%	Limite superior	50 minutos por ano

Tabela 2 – Demonstrativos de disponibilidade. Fonte: (ALVES, 2009).

2.4.3 **Aplicações**

A gerência de aplicações é feita por *softwares* especializados, que frequentemente executa testes programados para verificar problemas comuns, como segurança da aplicação, localizadores de falhas, e ferramentas que reportam comportamentos anormais. (COSTA, 2008).

Os principais componentes que devem ser monitorados são:

- Vazão de informação na conexão;
- Taxa de erros;
- Tempo de resposta obtido;
- Recursos utilizados;
- Uso de memória;
- Contabilidade de acessos.

2.4.4 **Configurações**

Em ambientes gerenciados é de extrema importância manter controle das configurações. São consideradas configurações elementos de rede como topologia, configurações administrativas, configurações de serviço, conectividade lógica e física. Abaixo um pouco mais sobre cada uma delas:

- Topologia:

  Na visão de topologia é necessário mostrar qual equipamento esta interligado com o outro, devendo ser levado em conta domínios de colisão dessas áreas.

- Administrativas:

  Deve conter os dispositivos envolvidos no agrupamento, sem necessidade de existir relação com os aspectos físicos e de conectividade física e lógica.

- Serviços:

  Busca evidenciar os dispositivos de rede que são utilizados por vários serviços, como por exemplo, um servidor de e-mail que deva ser monitorado o serviço da ferramenta de e-mail, e em casos de falha na aplicação, que seja emitida uma notificação apenas que o serviço inoperante mas que o servidor esta íntegro.

- Conectividade Física:

  Faz relação com os equipamentos, é exibido graficamente as interfaces e portas dos dispositivos, mostrando o status de cada componente, possibilitando a execução de comandos remotos, tais como o reset de uma porta, mudar o status do equipamento, e até mesmo alterar configurações, conforme ilustração abaixo.

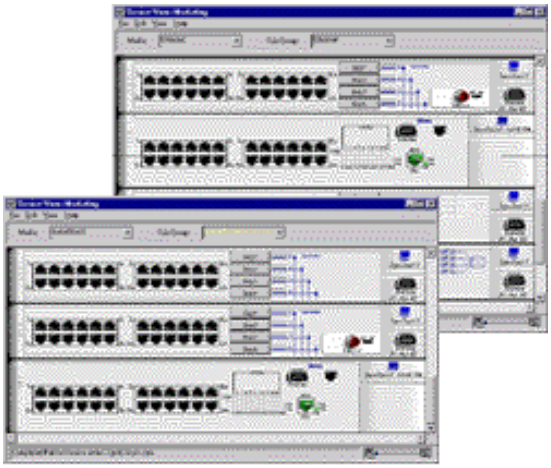

Figura 4 – Interface que exemplifica configurações físicas. Fonte: (CISCO, 2009)

- Conectividade lógica:

  É importante que seja exibido as informações entre redes de endereçamento TCP/IP, onde exista roteamento, evidenciando os domínios de *broadcast*. Nesta visão não deverá aparecer equipamentos como hubs, modems e switches.

3 DESENVOLVIMENTO

Este capítulo tratará os cenários que serão avaliados e apresentação das principais ferramentas de gerenciamento de redes. Com os cenários abaixo apresentados são descritos os ambientes de redes que foram realizados os testes com as ferramentas de gerência.

3.1 *CENÁRIOS*

Os cenários usados para avaliação e demonstração das técnicas e melhores práticas serão divididos basicamente e generalizado nas situações mais comuns nos ambientes de rede, tais como um ambiente de grande, médio e pequeno porte.

3.1.1 **GRANDE PORTE**

Um ambiente de grande porte pode ser considerado uma rede com mais de 500 computadores interligados, entre diversos dispositivos de rede. Basicamente, este ambiente pode ser local ou distribuído em outros locais (LAN, WAN e MAN).

É muito comum encontrar este cenário em empresas com diversas filiais, bancos e operadoras de telecomunicações.

A análise será realizada com o seguinte escopo:

Quantidade	Descrição
80	Servidores
6	Links de comunicação
5	Roteadores
4	Switches
2	PABX com ramais IP
20	Serviços diversos customizados
1	Firewall

Tabela 3 – Escopo de rede grande porte. Fonte: (O Autor).

3.1.2 **MÉDIO PORTE**

Médio porte, é de fato o ambiente mais comum encontrado na maioria das empresas, pode ser considerado de médio porte uma rede que possui de 100 até 500 computadores e dispositivos interconectados.

A análise será realizada com o seguinte escopo:

Quantidade	Descrição
40	Servidores
3	Links de comunicação
2	Roteadores
3	Switches
1	PABX com ramais IP
15	Serviços diversos customizados
1	Firewall

Tabela 4 – Escopo de rede médio porte. Fonte (O Autor).

3.1.3 **PEQUENO PORTE**

Uma rede de pequeno porte com modelo de gerência pode ser considerada incialmente de 5 a 100 computadores e alguns poucos dispositivos interconectados, é comum em pequenas empresas ou de pequeno enfoque na comunicação digital, serão consideradas e avaliadas redes de pequeno porte as corporativas, não serão mensuradas redes residenciais.

A análise será realizada com o seguinte escopo:

Quantidade	Descrição
5	Servidores
1	Links de comunicação
1	Switches
3	Serviços diversos customizados
1	Firewall

Tabela 5 – Escopo de rede pequeno porte. Fonte: (O Autor).

3.2 *FERRAMENTAS DE GERÊNCIA*

Com um número cada vez maior de equipamentos e recursos de rede, 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.

Algumas ferramentas como Nagios, CACTI e Zabbix são exemplos de *softwares* de gerência e monitoramento de rede, e técnicas de gerenciar estes ambientes foram sendo criadas e evoluídas com o passar do tempo assim como as ferramentas de gerência. (ALVES, 2009).

3.2.1 **NAGIOS**

Nagios é uma ferramenta bem comum no quesito monitoração de rede, sua concessão de uso é pela licença GPL, e de código aberto. Ele pode monitorar tanto *hosts* quanto dispositivos de rede e até mesmo serviços, alertando ao responsável quando ocorrem problemas e também quando os incidentes foram resolvidos.

Originalmente o Nagios foi criado com o nome de Netsaint. Foi desenvolvido e é atualmente mantido por Ethan Galstad, junto de uma grande quantidade de desenvolvedores que criam e atualizam *plugins* oficiais e não oficiais. Inicialmente o Nagios foi desenvolvido para trabalhar em plataforma Linux, mas pode ser encontrado no site do desenvolvedor o aplicativo para outras plataformas, até mesmo para o Microsoft Windows. (COSTA, 2008).

3.2.1.1 **Apresentação**

O Nagios é considerado uma das ferramentas mais comuns encontradas nos ambientes de gerência, suas versões são muito bem documentadas e altamente disponíveis para consultas no site da comunidade do projeto.

Nagios é uma ferramenta abrangente e experiente com várias funcionalidades que despertam a atenção nos profissionais, com algumas particularidades em relação a segurança, traz suporte a todas as tecnologias padrões de mercado, e várias configurações específicas para o seu código que são encontradas nas documentações. O foco do projeto é o monitoramento dos dispositivos de rede com diversas opções distribuídas em *plugins*.

Os gráficos não são o seu ponto forte, o qual o destaque vai para o Cacti, mas toda a informação disponibilizada é coerente e atualizada, para manter o quesito disponibilidade, podendo monitorar plataformas como Windows, Unix e Linux.

3.2.1.2 **Funcionalidades**

Com o Nagios podemos obter as mais diversas funcionalidades de monitoramento de rede e gerência de incidente tais como:

- Monitoramento de infraestrutura da rede;
- Detectar problemas, antes mesmo que eles ocorram;
- Receber notificação no momento em que aconteceu um incidente;
- Compartilhar dados sobre a disponibilidade com as partes envolvidas;
- Detectar e notificar falhas, graficamente ou através mensagens customizadas;
- Possibilidade de prever e um plano para upgrade de equipamentos necessários;
- Reduzir o tempo de indisponibilidade;
- Identificar pontos hierárquicos que foram afetados.

3.2.2 **CACTI**

Cacti é uma ferramenta desenvolvida com a finalidade de administrar um ambiente de rede, utiliza por padrão o protocolo SNMP para coletar os dados dos equipamentos de rede. Sua principal característica é coletar e armazenar estas informações em um banco de dados e exibir em forma de um gráfico gerencial. (COSTA, 2008).

3.2.2.1 **Apresentação**

O CACTI permite através das informações coletadas o gerenciamento e monitoramento de redes simples e até mesmo de redes mais complexas com a possibilidade de gerenciar na sua base centenas de dispositivos.

Seu projeto teve por intuíto em criar uma ferramenta flexível de forma que possa facilmente se adaptar às diversas necessidades, pode ser considerado como uma ferramenta robusta por conter uma interface Web muito intuitiva e fácil de trabalhar.

Os principais dados utilizados pelo CACTI através do protocolo SNMP são:

- Largura de Banda;
- Monitora o status de cada elemento na rede;
- Uso de CPU em um determinado periodo;
- Monitoramento de disco.

Um dos recursos que desperta um grande interesse em administradores de redes é a possibilidade de criação de hierarquias gráficas, desta forma tornando mais dinâmico à gerência através dos gráficos.

3.2.2.2 **Funcionalidades**

Podemos obter uma grande quantidade de recursos com o Cacti, a cada dia novos *plugins* são liberados para aperfeiçoar a administração e gerência através da ferramenta. As principais funcionalidades por padrão são:

3.2.2.2.1 Gráficas

- Números ilimitados de itens de gráfico podem ser definidos para cada gráfico ou fontes de dados de dentro do Cacti;
- Agrupamento automático de itens para permitir o rápido re-seqüenciamento de ítens gráfico;
- Dados do gráfico podem ser manipulados usando as funções matemáticas;
- Suporte para todos os tipos de *RRDTool* de ítem gráfico.

Figura 5 – Exemplos de funcionalidades gráficas do CACTI. Fonte: (COSTA, 2008).

3.2.2.2.2 Base de dados

- Bases de dados podem ser criadas com funções padrões como “*create*” e “*update*” direto no banco de dados;
- Suporte a arquivos *RRD* com mais de uma base de dados que podem ser armazenadas em qualquer lugar do sistema local;
- Configurações de *Round Robin* podem ser feitas para personalizar a coleta de dados do gráfico;

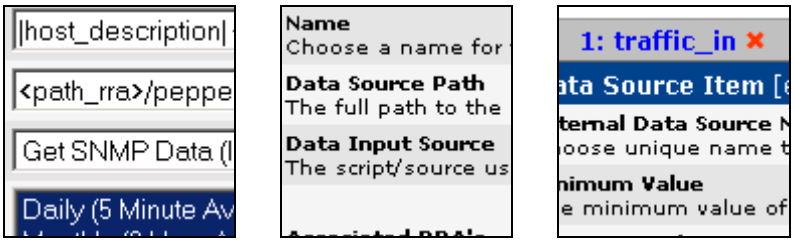

Figura 6 – Exemplo de conexões com banco de dados. Fonte: (COSTA, 2008).

3.2.3 **ZABBIX**

A ferramenta de gerência Zabbix é a ferramenta mais completa entre as GPL, seu grande diferencial é unir as outras funções das demais ferramentas analisadas, sob uma interface robusta e amigável, os gráficos e mapas são gerados e acessados facilmente e os recursos remotos promovem um levantamento em tempo real do ambiente gerido. (COSTA, 2008.)

3.2.3.1 **Apresentação**

Um dos grandes aspectos importantes que destaca o Zabbix das demais ferramentas é a sua documentação muito completa e que facilita bastante a vida do administrador da rede devido as constantes atualizações da versão do *software*, destaca-se também pela grande quantidade de banco de dados que podem se conectar com a aplicação do Zabbix.

3.2.3.2 **Funcionalidades**

Como uma das ferramentas mais recentes lançadas no mercado, com uma grande aceitação dos profissionais de TI, o Zabbix oferece um grande número de funcionalidades e podem ser destacadas como as principais:

- Controle de *Service Level Agreement* (SLA);
- Função *auto-discovery*, que localiza novos recursos e interconexões;

- Disponibiliza um agente que habilita mais funções monitoráveis;
- Suporte ao protocolo *SNMP*;
- Armazena dados de *syslog* interno;
- Permite a execução de scripts externos;
- Adição de funcionalidades através de *plugins*;
- Emissão de alertas;
- Controle completo em *um front-end web*;
- Realiza monitoramento distribuído;
- Permite fazer inventário;
- Licença de uso *GPL*;
- Emissão de eventos;
- Gera gráficos, mapas e relatórios.

3.3 *TÉCNICAS*

Em redes de computadores além de ser empregados modelos de gerência de redes deve ser consideradas algumas técnicas que sejam empregadas junto ao modelo que melhor se adapta ao ambiente de rede, para garantir que todos os contextos sejam avaliados de forma correta. As principais técnicas a serem empregadas estão abaixo relacionadas. (TANENBAUM, 4.ed, 2003).

3.3.1 **Configuração**

A técnica de configuração é responsável pela descoberta, manutenção e monitoração de mudanças ocorridas na infra-estrutura física e lógica na rede.

Devem ser consideradas básicas as seguintes funções:

- Coleta de informações de configuração;
- Descoberta de novos elementos na rede;
- Descoberta de interconectividade entre elementos na rede;

- Geração de eventos;
- Emitir eventos quando recursos são adicionados ou removidos;
- Manter um inventário atualizado;
- Atribuir parâmetros a cada elemento monitorado;
- Alteração de elementos gerenciados.

3.3.2 **Faltas**

É responsável pela detecção e isolamento de falhas na rede. Esta técnica tem por objetivo perceber que está havendo um problema na rede, uma falta pode gerar uma falha, que então gera um evento e testes de diagnóstico.

Como a técnica de falta tem por objetivo antecipar falhas, os monitores de indicadores podem prever a ocorrência de falhas, taxas crescentes de erro e atrasos de transmissão, fazendo o uso de *tresholds* é possível gerar alarmes na interface do usuário indicando quais elementos estão funcionando e quais estão fora de operação. Algo que deve ser considerado nos alarmes é o nível de severidade de cada evento, dependendo da sua importância deve ser enviado uma notificação por *e-mail*, *pager* ou até mesmo por *SMS*.

3.3.3 **Desempenho**

Técnicas de desempenho são responsáveis pela monitoração dos recursos envolvidos. O desempenho atual da rede deve se basear em indicadores como: atraso, disponibilidade, utilização, taxas de erro, etc.

Um *baseline* pode ser estabelecido com base nos dados de comportamento individual de cada recurso, outro fator que deve ser considerado são os registros de histórico para permitir uma análise de diversos pontos dos recursos para um planejamento futuro, isso pode ser realizado através da análise de desempenho e planejamento de capacidade.

Para um planejamento real da infraestrutura a técnica de desempenho empregada na gerência de rede é muito útil para prever gastos e mensurar a

utilização de cada recurso na rede, com uma análise do histórico de despenho de um dispositivo é possível compreender o seu uso na rede e verificar se o mesmo está operando de forma esperada ou está suscetível à falha pelo fato de estar sobrecarregado.

3.3.4 **Segurança**

Técnicas de segurança são responsáveis pela proteção dos elementos da rede, monitorando e detectando violações da política de segurança estabelecida. Voltada a proteção dos elementos da rede, deve apoiar a política de segurança, e tem por objetivo prover mecanismos para criar, remover e controlar os serviços de segurança, além de monitorá-los.

Com o uso de ferramentas de gerência de redes pode-se disparar alarmes ao detectar violações de segurança, responsável também por fazer a manutenção e armazenamento de log de auditoria de segurança.

3.3.5 **Contabilidade**

Para a contabilidade de cada recurso na rede é empregada uma técnica que é responsável pela contabilização e verificação de limites da utilização de recursos da rede, pela divisão de contas distribuídas entre usuários ou grupos de usuários.

Basicamente, a técnica provém da coleta de informações de utilização, monitora quais recursos e quanto destes recursos estão sendo utilizados por qual entidade, estabelecendo assim cotas de utilização. Pode oferecer também limites de recursos por usuários, estabelecendo escalas de tarifação para dividir o custo entre usuários e departamentos de uma empresa. As informações extraídas podem ser utilizadas para fins de estatísticas ou para previsão para novos investimentos em recursos de rede.

4 ANÁLISE DE RESULTADOS

Este capítulo tem por objetivo descrever resultados analisados, com base nos três tipos de redes, pequeno, médio e grande porte, com a teoria contida neste trabalho.

Os resultados obtidos nesse capítulo são baseados em ambientes diferentes, onde uma empresa foi utilizada para a análise de uma rede real de médio porte, e em ambientes de testes em máquinas e equipamentos virtuais.

Para simulações de rede e tráfego foram utilizados os seguintes softwares:

- Cisco *Packet Tracer* 5.3.2;
- Oracle Virtual *Box* 4.1;
- GNS3 v0.8.1

Abaixo um detalhamento de cada comparativo realizado.

4.1 *REDE DE PEQUENO PORTE*

Os resultados obtidos no ambiente de rede de pequeno porte foram divididos e classificados respectivamente em melhor forma de gerência, melhor modelo de gerência e melhor ferramenta.

Abaixo a classificação:

4.1.1 **Fator “Tipo de Gerência”**

Em um ambiente de rede de pequeno porte o modelo que mais se adapta ao cenário é o Modelo de Gerência Centralizada. Esta conclusão é dada pelo fato de equipes de gerência ou até mesmo equipes de infraestrutura ser relativamente reduzidas, podendo ser gerenciado por apenas um administrador de rede.

Com apenas um ou um número bem reduzido de administradores de rede, a gerência não trabalhará com hierarquia nem com ambientes de segmentos distribuídos. Todos os eventos e ações sobre um determinado incidente será destinado a um único usuário de gerência que fará não só o monitoramento mas também tomará as devidas medidas para a resolução do problema.

Ao validar os demais tipos de gerencia deve-se levar em consideração a gerencia reativa, o ponto que se adaptou foi que o mesmo administrador que é notificado do incidente tomará as devidas medidas para atuar na correção do mesmo.

4.1.2 **Fator “Modelo de Gerência”**

Ao analisar um ambiente com poucas estações e pequena quantidade de recursos de rede foi notável que o modelo de gerência OSI foi o que melhor geriu as necessidades de administração, monitoramento e notificação para o gerente. Sua escolha de implementação foi correlacionada com a existência das 5 gerências contidas no modelo OSI, que asseguram ao gerente sua eficiência e confiabilidade para atender o gestão de todos os dispositivos e sistemas presentes no segmento de rede.

O modelo Internet não foi a melhor opção a ser implantada por se tratar de uma gerência mais complexa de implantação que oferecem recursos que não serão utilizados pelo administrador devido a grande quantidade de informação produzida, uma vez que sua equipe é reduzida ou até mesmo é mantida por um único administrador.

4.1.3 **Fator “Melhor Ferramenta”**

Foram testadas as três ferramentas abordadas neste trabalho (Cacti, Nagios e Zabbix), a que melhor atendeu as necessidades com uma interface mais organizada com a quantidade de informação necessária para uma equipe reduzida foi o Zabbix, o qual gerencia e monitora os recursos de rede em tempo real, envia notificações e

alertas ao administrador, e conta com a geração de relatório e gráficos de consumo por período de cada recurso gerenciado.

O Zabbix se mostrou como uma ferramenta unificada e centralizadora, o que para uma rede com poucos recursos atende em todos os quesitos sem a necessidade de implementar outra ferramenta para auxilia-lo.

4.2 *REDE DE MÉDIO PORTE*

4.2.1 **Fator “Tipo de Gerência”**

O ambiente mais comum nas empresas, se mostrou fortemente tendencioso para o tipo de gerencia descentralizado, onde geralmente a equipe possui pelo menos um gerente, que é a pessoa responsável por monitorar e analisar os eventos e notificações provindas da ferramenta de gerencia. Por sua vez deve ser levado em consideração que uma rede de médio porte pode possuir mais de um segmento ou hierarquia a ser gerenciada, o qual a gerência descentralizada possibilita usar as técnicas de gerencia de nos remotos e delegando quais recursos serão a ele subordinado, tornando mais simples o controle de cada vez mais equipamentos.

O principal fator que considerado foi que este ambiente é muito suscetível a mudanças de escopo e sofrer crescimentos.

4.2.2 **Fator “Modelo de Gerência”**

Ao implementar os modelos no ambientes de teste com monitoramento de serviços e equipamentos ambos os modelos de gerencia supriram a necessidade para uma gerencia confiável da rede, mas com menor volume de dados e informações sobre a rede o modelo OSI superou expectativas em monitoramento

remoto, o consumo de banda pelo modelo internet é bem superior que o modelo OSI.

Embora para redes locais onde a largura de banda é consideravelmente maior o modelo internet foi o mais completo em nível de informações contidas e sua gerência serem estruturadas com o uso de MIBs.

4.2.3 **Fator “Melhor Ferramenta”**

Ao eleger a ferramenta de gerência de rede para um segmento de médio porte deve ser levado em consideração o seu crescimento futuro, em nível de perspectiva consideramos o mesmo principio de um segmento de grande porte, para suportar futuras expansões.

Dois diferentes esquemas de configurações foram avaliados que atendem perfeitamente a demanda do gerente deste segmento.

A primeira configuração foi realizada com um servidor com a ferramenta de gerencia CACTI, juntamente com o Nagios, ambos fazendo atividades distintas em nível de aperfeiçoar a visualização do status da rede.

A segunda configuração foi realizada no servidor de gerência a ferramenta Zabbix, que engloba as atividades de monitoramento contidas no Nagios e o histórico e análise de desempenho contida no CACTI.

É notória que a segunda configuração é recomendada a ambientes que não sejam suscetíveis a crescimento futuro, sendo que a gerencia do Zabbix é centralizada, na primeira configuração temos um ambiente descentralizado mas considerado especializado pelo fato de cada ferramenta exercer o seu papel distinto uma da outra.

4.3 *REDE DE GRANDE PORTE*

4.3.1 **Fator “Tipo de Gerência”**

O tipo de gerência que melhor representa tanto na teoria quanto na prática um ambiente de grande porte é o modelo de gerência proativo, que se mostrou robusto ao ponto de ser empregado em redes de operadoras de telecomunicações, e grandes empresas, que a cada dia sofre grandes expansões e modificações no seu escopo, tornando esse o único modelo flexível a ajustes e que atende as necessidades de gerência de grandes redes com segurança, performance e eficiência, fatores o qual se tornam indispensável em segmentos em que o tempo de *downtime* seja o mínimo possível acordado em uma SLA.

4.3.2 **Fator “Modelo de Gerência”**

O modelo aplicado em simulação de um ambiente de grande porte foi o modelo Internet, que por sua vez oferece suporte aos mais diversos tipos de equipamentos de rede, e que na teoria é o único modelo que atende redes com diversos segmentos distribuídos, e na prática é utilizado em fornecedores de soluções ISP e operadoras de telecomunicações, portanto sua avaliação foi empregada apenas com o intuito de teste de implementação como descrito no cenário, uma vez que não houve possibilidade de simulação de tal ambiente devido a complexidade e disponibilidade de recursos de rede.

4.3.3 **Fator “Melhor Ferramenta”**

A melhor ferramenta avaliada tanto em simulação quanto em pesquisas realizadas em operadoras de telecomunicações foi a combinação de duas ferramentas de gerência, o CACTI e o Nagios.

Cada uma apresenta sua especialidade específica, o Nagios no quesito monitoramento e notificações de incidentes, e o CACTI com os dados gráficos e estatísticas de cada recurso de rede armazenada e listada conforme customização do gerente.

O Zabbix não foi cogitado pelo fato de não ter confiabilidade e performance para atender funcionalidades específicas apresentadas no Nagios e no CACTI, como uma única solução de gerência de rede.

REFERÊNCIAS

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 10520: informação e documentação: citações em documentos: apresentação**. Rio de Janeiro, 2002.

ALVES, Maicon Melo. **Linux: Performance e Monitoramento.** 1ª ed. São Paulo: Editora Brasport, 2009.

BLACK, Tomas Lovis. **Comparação de Ferramentas de Gerenciamento de Redes.** Porto Alegre, 2008. Disponível em: < http://www.lume.ufrgs.br/bitstream /handle/10183/15986/000695315.pdf?sequence=1 > Acesso em 05/10/2011. 23:36.

CARMONA, Tadeu. **Universidade Redes.** 1ª ed. São Paulo: Editora Universo dos Livros, 2004.

CISCO, **Network Academy. CCNA Exploration – Fundamentos de Redes.** Cisco Systems, Inc., 2007-2009.

COMER, Douglas E. **Redes de Computadores e Internet.** 4ª ed. São Paulo: Editora Bookman, 2007.

COSTA, Felipe. **Nagios e Cacti – Monitoramento de redes**. 1ª ed. Rio de Janeiro: Editora Ciência Moderna, 2008.

EINSTEIN, Albert, s.d. Disponível em: **< http://pensador.uol.com.br/nem_tudo_ que_enfrentamos_pode_ser_mudado/ >.** Acesso em: 1 ago. 2011.

FARREL, Adrian. **A Internet e seus Protocolos**. São Paulo: Editora Elsevier, 2005.

FOROUZAN, Behrouz A**. Comunicação de dados e redes de computadores.** 3ª ed. Porto Alegre: Editora Bookman, 2004.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa.** 4ª ed. São Paulo: Atlas 2002.

LOPES, Raquel V. **Melhores Práticas para Gerência de Redes de Computadores.** Rio de Janeiro: Editora Campus, 2003.

MENDES, Douglas Rocha. **Redes de Computadores.** 1ª ed. Paraná, Curitiba: Editora Novatec, 2008.

ROSS, Julio. **Redes de Computadores.** 1ª ed. São Paulo: Editora Antenna Edições técnicas, 2008.

SCRIMGER ,Rob. **TCP/IP - A BIBLIA.** 3ª ed. Rio de Janeiro: Editora Campus, 2002.

TANENBAUM, Andrew S. **Redes de Computadores.** 4ª ed . São Paulo: Editora Campus, 2003.

TORRES, Gabriel. **Redes de computadores Curso completo.** 1ª ed. São Paulo: Editora Axcel Books, 2001.

TORRES, Gabriel. **Redes de computadores – Versão Revisada e Atualizada.** 2ª ed. São Paulo: Editora Nova Terra, 2009.

APÊNDICE – A

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Pró-Reitoria de Graduação e Educação Profissional
Pró-Reitoria de Pesquisa e Pós-Graduação

DECLARAÇÃO DE AUTORIA

Autor[1]: Ildebrando Tadeu Andreatta Junior

CPF[1]: 066.282.409-16 **Código de matrícula**[1]**:** 01222694

Telefone[1]**:** (41) 8444-0840 **e-mail**[1]**:** ildebrandojunior@hotmail.com

Curso/Programa de Pós-graduação: CURSO DE ESPECIALIZACÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES.

Orientador: Fabiano Scriptore de Carvalho.

Co-orientador: Não possui.

Data da defesa: 26/11/2011

Título/subtítulo: MÉTODOS E TÉCNICAS DE BOA PRÁTICA PARA IMPLEMENTAÇÃO DE UM NETWORK OPERATION CENTER (NOC)

Tipo de produção intelectual: ( ) TCC[2] (X) TCCE[3] ( ) Dissertação ( ) Tese

Declaro, para os devidos fins, que o presente trabalho é de minha autoria e que estou ciente:

- dos Artigos 297 a 299 do Código Penal, Decreto-Lei nº 2.848 de 7 de dezembro de 1940;
- da Lei nº 9.610, de 19 de fevereiro de 1998, sobre os Direitos Autorais,
- do Regulamento Disciplinar do Corpo Discente da UTFPR; e
- que plágio consiste na reprodução de obra alheia e submissão da mesma como trabalho próprio ou na inclusão, em trabalho próprio, de idéias, textos, tabelas ou ilustrações (quadros, figuras, gráficos, fotografias, retratos, lâminas, desenhos, organogramas, fluxogramas, plantas, mapas e outros) transcritos de obras de terceiros sem a devida e correta citação da referência.

Assinatura do Autor[1] Local e Data

[1] Para os trabalhos realizados por mais de um aluno, devem ser apresentados os dados e as assinaturas de todos os alunos.
[2] TCC – monografia de Curso de Graduação.
[3] TCCE – monografia de Curso de Especialização.

APÊNDICE – B

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Pró-Reitoria de Graduação e Educação Profissional
Pró-Reitoria de Pesquisa e Pós-Graduação

TERMO DE AUTORIZAÇÃO PARA PUBLICAÇÃO DE TRABALHOS DE CONCLUSÃO DE CURSO DE GRADUAÇÃO E ESPECIALIZAÇÃO, DISSERTAÇÕES E TESES NO PORTAL DE INFORMAÇÃO E NOS CATÁLOGOS ELETRÔNICOS DO SISTEMA DE BIBLIOTECAS DA UTFPR

Na qualidade de titular dos direitos de autor da publicação, autorizo a UTFPR a veicular, através do Portal de Informação (PIA) e dos Catálogos das Bibliotecas desta Instituição, sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9.610/98, o texto da obra abaixo citada, observando as condições de disponibilização no item 4, para fins de leitura, impressão e/ou *download*, visando a divulgação da produção científica brasileira.

1. Tipo de produção intelectual: ( ) TCC[1] (X) TCCE[2] ( ) Dissertação ( ) Tese
2. Identificação da obra:

Autor[3]: Ildebrando Tadeu Andreatta Junior

RG[3]: 8060172-7 **CPF**[3]: 066.282.406-16 **Telefone**[3]: (41) 8444-0840

e-mail[3]: ildebrandojunior@hotmail.com

Curso/Programa de Pós-graduação: CURSO DE ESPECIALIZACÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES.

Orientador: Fabiano Scriptore de Carvalho.

Co-orientador: Não possui.

Data da defesa: 26/11/2011

Título/subtítulo (português): MÉTODOS E TÉCNICAS DE BOA PRÁTICA PARA IMPLEMENTAÇÃO DE UM NETWORK OPERATION CENTER (NOC).

Título/subtítulo em outro idioma: METHODS AND TECHNIQUES OF GOOD PRACTICE FOR THE IMPLEMENTATION OF A NETWORK OPERATION CENTER (NOC).

Área de conhecimento do CNPq: 10304045 - TELEINFORMÁTICA

Palavras-chave: Gerenciamento de redes. Melhores práticas. Network Operation Center (NOC).

Palavras-chave em outro idioma: Network management. Best practices. NOC.

3. Agência(s) de fomento (quando existir):

4. Informações de disponibilização do documento:

Restrição para publicação: ( ) Total[4] ( ) Parcial[4] (X) Não Restringir
Em caso de restrição total, especifique o por que da restrição: _____
Em caso de restrição parcial, especifique capítulo(s) restrito(s): _____

_____
Local e Data

_____ _____
Assinatura do Autor[3] Assinatura do Orientador

[1] TCC – monografia de Curso de Graduação.
[2] TCCE – monografia de Curso de Especialização.
[3] Para os trabalhos realizados por mais de um aluno, devem ser apresentados os dados e as assinaturas de todos os alunos.
[4] A restrição parcial ou total para publicação com informações de empresas será mantida pelo período especificado no Termo de Autorização para Divulgação de Informações de Empresas. A restrição total para publicação de trabalhos que forem base para a geração de patente ou registro será mantida até que seja feito o protocolo do registro ou depósito de PI junto ao INPI pela Agência de Inovação da UTFPR. A íntegra do resumo e os metadados ficarão sempre disponibilizados.