SUMÁRIO

APRESENTAÇÃO DO PROJETO

1. INTRODUÇÃO

Os avanços tecnológicos exercem hoje um grande impacto na sociedade. A informação tem-se tornado cada vez mais uma vantagem competitiva para as empresas e organizações em investimentos futuros.

O fato é que, cada vez mais, as empresas, para se tornarem competitivas e sobreviverem no mercado, têm investido em tecnologia de informação, como a única forma de tornar seguro o processo decisório. E é nesse quadro que as redes de computadores se proliferam, encurtando as distâncias e diminuindo o tempo de resposta entre as transações entre as organizações de todo o mundo.

Em decorrência das vantagens que as redes de computadores oferecem, o número e a extensão dessas estão em expansão continua. À medida que as redes crescem em escala e extensão, dois fatores vão ficando mais evidentes: as redes, juntamente com seus recursos e aplicações, tornam-se cada vez mais indispensáveis para as organizações que as utilizam, e uma maior possibilidade de ocorrerem problemas, o que pode levar as redes a um estado de inoperância ou a níveos inaceitáveis de desempenho.

A fim de garantir certa qualidade dos serviços a seis usuários, é que as redes de computadores devem ser gerenciadas. Este gerenciamento envolve o monitoramento e o controle de recursos distribuídos em redes. Em essência, o gerenciamento de redes busca assegurar que sistemas de informação, disponíveis em redes, estejam operacionais e eficazes a todo instante.

No entanto, o gerenciamento de redes de computadores é por si só complexo. Na proporção que as redes tornam-se maiores (extensão), complexas (tecnologia) e heterogêneas (plataformas de hardware e software distintas), tornam o gerenciamento em si mais complexo ainda. Conseqüentemente o gerenciamento não pode ser realizado somente pelo esforço humano. A complexidade do gerenciamento de redes impõe o uso de soluções automatizadas de gerenciamento de redes.

Procurando cumprir objetivos de gerenciamento da rede e agilidade de acesso aos dados, nós, da HELPNET.COM, apresentamos uma proposta de implantação de software de gerenciamento Whats UP Gold (plataforma Windows) ou MRTG (Plataforma Linux), conforme veremos a seguir.

2. PROBLEMÁTICA

Sem um software de gerenciamento da rede, é impossível minimizar o tempo de parada da rede, pois não permite que algumas falhas da mesma possam ser previamente apontadas.
Hoje na empresa UNINOVE, não possui gerenciamento da rede, o que não permite aos administradores de redes a capacidade de monitorar, mapear, ser notificado quando ocorre algo anormal na rede, bem como analisar o status da rede em tempo real, monitoramento de hardware, software de rede, impressoras, repetidores, concentradores LAN e dispositivos de usuário final; além de serviços como SNMP, POP3, FTP, Telnet, WWW e NNTP.

3. OBJETIVO

Realizar a instalação e configuração de sistema de gerenciamento da rede, baseado na plataforma Microsoft ou Linux.
Trazendo melhorias, de forma fácil de mapear a rede, monitorar dispositivos e serviços, receber notificação de problemas, gerar de relatórios, gerenciamento remoto, entre outros, além de fornecer treinamento para a equipe de administração da rede.

4. PORQUE MRTG?

MRTG consiste em um script em Perl que usa SNMP para ler os contadores de tráfego de seus roteadores e um rápido programa em C que loga os dados do tráfego e cria belos gráficos representando o tráfego da conexão de rede monitorada. Estes gráficos são incluídos em páginas web que podem ser visualizadas de qualquer Browser moderno.
Somadas a detalhada visão diária o MRTG também cria representações visuais do tráfego durante os últimos 7 dias, das últimas 4 semanas e dos últimos 12 meses. Isto é possível porque o MRTG mantém um log de todos os dados que ele conseguiu do roteador. Este log é automaticamente consolidado, e com isso ele não cresce com o tempo, mas ainda contém todos os dados relevantes de todo o tráfego dos últimos 2 anos. Isto tudo é realizado de uma maneira muito eficiente. Então você pode monitorar mais de 200 links de rede de qualquer estação UNIX decente.
O MRTG não se limita a monitorar somente tráfego, é possível monitorar qualquer variável SNMP que você escolher. Você pode até usar um programa externo para pegar os dados que você deve monitorar via MRTG. As pessoas usam o MRTG, para monitorar coisas como

Carga do Sistema, Sessões Logadas, Disponibilidade de Modens e muito mais. O MRTG ainda permite a você acumular 2 ou mais fontes de dados em um único gráfico.
MRTG é disponível sem custo sob os termos da GNU Licença Pública Universal.

5. PORQUE WHATS UP GOLD?

WhatsUp Gold é uma solução simples de mapeamento de rede, monitoramento, notificação e de relatório de desempenho que ajuda os administradores de rede e engenheiros a detectarem e consertarem os problemas da rede - rapidamente. É um monitorador / gerenciador gráfico de redes multi-protocolo, monitora seus dispositivos críticos e serviços através de alarmes visuais e auditivos quando um problema é detectado, ajudando gerenciar sua rede e deixá-la mais tempo online. O WhatsUp irá notificá-lo através de beeper, pager, e-mail ou telefone. Pode ser instalado em sistemas operacionais como Windows 2000, Windows NT com SP 6 ou posterior, Windows ME ou Windows XP.
Além disso, não exisge a máquina robusta para trabalhar, evitando gastos com equipamentos inicialmente.

6. PREMISSAS E RISCOS

6.1 Premissas

- Local para desenvolvimento do projeto
- Equipamentos conforme descritos no item 7 deste capítulo.

6.2 Riscos

- Paralisação total ou parcial da rede
- Falha na energia elétrica
- Defeito de Hardware
- Política fiscal
- Atraso na entrega do software (no caso da ferramenta Whats UP Gold)

7. DESCRIÇÃO DAS ATIVIDADES

Será instalado o software Whats UP Gold ou MRTG (conforme escolha do cliente), onde será de responsabilidade da HELNET.COM a instalação e configuração do software, bem como os testes e treinamento os administradores da rede.

8. DETALHES DAS CONFIGURAÇÕES MÍNIMAS DOS EQUIPAMENTOS REQUERIDOS

8.1 Para software Whats UP Gold

- Intel Pentium ou equivalente
- 30 MB de espaço em disco (100 MB recomendado)
- 64 MB de RAM (256 MB recomendado)
- Windows NT 4.0 SP6 ou superior, Windows 2000, Windows 98, Windows ME, Windows XP, Windows Server 2003
- Utilização do protocolo TCP/IP

8.2 Para software MTRG

8.2.1 Hardware Mínimo Necessário:

- Pentium II 400Mhz
- 128Mb de memória
- HD 10Gb

8.2.2 Softwares Necessários:

- Servidor Web
- GCC (Compilador C)
- Perl
- biblioteca gd
- biblioteca zlib
- biblioteca libpng

9. ANÁLISE DE CUSTO E ORÇAMENTO

Os valores descritos na tabela abaixo são apenas um demonstrativo de impacto de custos/ orçamentos do projeto, uma vez que todos envolvidos são profissionais da HELPNET.COM.

9.1 Custos

Recursos Humanos				
Cargo/função	**Salário/Mês**	**Custo/Hora**	**Total Hora**	**Custo do Projeto**
Gerente Comercial	R$ 5.000,00	R$ 28,41	6	R$ 170,45
Analista Pleno	R$ 3.000,00	R$ 17,05	6	R$ 102,27
Analista Sênior	R$ 4.000,00	R$ 22,73	38	R$ 863,64
Analista Junior	R$ 2.000,00	R$ 11,36	8	R$ 90,91

9.2 Orçamento

9.2.1 Orçamento MRTG

Recursos Humanos			
Cargo/função	**Valor/Hora**	**Total Hora**	**Orçamento do Projeto**
Gerente Comercial	R$ 56,82	6	R$ 340,92
Analista Pleno	R$ 34,10	6	R$ 204,60
Analista Sênior	R$ 45,46	38	R$ 1.727,48

A tabela abaixo é referente ao orçamento do PDI com suas dependências custos e viabilidade de implantação do MRTG.

Tabela de Atividades - MRTG					
Atividade	**Descrição**	**Dependência**	**Valor/hora**	**Horas Trabalhadas**	**Custo Total**
1	Visita ao Local	inicio	R$ 56,82	3	R$ 170,46
2	Levantamento de inventário e necessidades	1	R$ 34,10	6	R$ 204,60
3	Aquisição do Software de gerenciamento	2	-	-	-
4	Implantação do Software de gerenciamento	3	R$ 45,46	32	R$ 1.454,72
5	Treinamento a equipe de administradores da rede	4	R$ 45,46	6	R$ 272,76
6	Entrega e Aceite	5	R$ 56,82	3	R$ 170,46
7	Fim	6	-	-	
				Total	**R$ 2273,00**

9.2.2 Orçamento Whats UP Gold

Recursos Humanos			
Cargo/função	**Valor/Hora**	**Total Hora**	**Orçamento do Projeto**
Gerente Comercial	R$ 56,82	6	R$ 340,92
Analista Pleno	R$ 34,10	6	R$ 204,60
Analista Sênior	R$ 45,46	8	R$ 1.727,48
Analista Junior	R$ 22,72	8	R$ 181,76

A tabela abaixo é referente ao orçamento do PDI com suas dependências custos e viabilidade de implantação do Whats Up Gold.

Tabela de Atividades – Whats Up Gold					
Atividade	**Descrição**	**Dependência**	**Valor/hora**	**Horas Trabalhadas**	**Custo Total**
1	Visita ao Local	inicio	R$ 56,82	3	R$ 170,46
2	Levantamento de inventário e necessidades	1	R$ 34,10	6	R$ 204,60
3	Implantação do Software de gerenciamento	2	R$ 45,46	8	R$ 363,68
4	Configuração e testes nos equipamentos clientes	3	R$ 22,72	8	R$ 181,76
5	Treinamento a equipe de administradores da rede	4	R$ 45,46	6	R$ 272,76
6	Entrega e Aceite	5	R$ 56,82	3	R$ 170,46
7	Fim	6	-	-	
				Total	**R$ 1363,72**

10 – CUSTO DO SOFTWARE

MRTG – software de distribuição livre.

Whats UP Gold

Custo: R$ 4.500,00

Forma de pagamento: faturamento 07 dias após entrega

Complemento: 01 ano de suporte e atualização, com utilização ilimitada de dispositivos.

Proposta valida até 15/12/2005.

11. ESTRUTURA ANALÍTICA DO PROJETO

Nível 0	Nível 1	Nível 2
Implantação do software de gerenciamento de rede	Levantamento de inventário	
	Implantação das tecnologias	Instalação e configuração do software de gerenciamento
		Treinamento fornecido aos administradores de rede

12. CRONOGRAMA

12.1 Implantação MRTG

	Dezembro							
Tarefas	**01/12**	**02/12**	**05/12**	**06/12**	**07/12**	**08/12**	**09/12**	**12/12**
Visita ao Local	X							
Levantamento de inventário e necessidades		X						
Implantação do Software de gerenciamento			X	X	X	X		
Treinamento a equipe de administradores da rede							X	
Entrega e Aceite								X
Fim								X

12.1 Implantação Whats UP Gold

	Dezembro				
Tarefas	**01/12**	**02/12**	**12/12**	**13/12**	**14/12**
Visita ao Local	X				
Levantamento de inventário e necessidades		X			
Aquisição do Software de gerenciamento		X*			
Implantação do Software de gerenciamento			X		
Configuração e testes nos equipamentos clientes			X		
Treinamento a equipe de administradores da rede				X	
Entrega e Aceite					X
Fim					X

** prazo de entrega do software Whats UP Gold é de 07 dias úteis*

13. EQUIPE DE GERENCIAMENTO DO PROJETO

O gerente do projeto indicado pela HELPNET.COM e que coordenará todos os trabalhos e recursos envolvidos será o Sr. Adriano Santos, seguido abaixo a listagem de todos envolvidos no projeto.

Nome	Cargo
Adriano Pereira Santos	Gerente Comercial
Vinicius de Lima	Analista Pleno
Leonardo da Costa Santos	Analista Sênior
Viviane Pereira Santos	Analista Sênior
Fernanda Freitas	Analista Junior (Microsoft)
Cássia Silva	Analista Junior (Linux)

14. PROPOSTA DE CONTRATO DE MANUTENÇÃO

Conforme levantamento realizado, foram avaliadas quais soluções oferecidas pela Helpnet.com se aplicam as necessidade de Contrato de Suporte da empresa UNINOVE e temos a certeza de que essas soluções poderão contribuir para integrar o processo e atender as expectativas de resultados dentro do prazo estipulado. A proposta de contrato está disponível no ANEXO A.

HISTÓRICO SOBRE REDES GERENCIADAS

1. RESUMO

O continuo crescimento em número e diversidades dos componentes das redes de computadores tem tornado a necessidade de gerenciamento de redes cada vez mais complexa. Por menor e mais simples que seja uma rede de computadores, precisa ser gerenciada, a fim de garantir, aos seus usuários, a disponibilidade de serviços a um nível de desempenho aceitável. O gerenciamento de rede foi estudo por 20 pessoas pela primeira vez em 1986. A abordagem clássica para integrar o gerenciamento de redes era, pois, baseada em arquitetura proprietárias. Os requisitos de gerenciamento foram levantados na metade de 1990 em uma pesquisa realizada pelo NIST e indicaram que o gerenciamento de redes locais, bem como as pontes que as interconectam, constituem em quesito básico. Em 30 de julho de 1992, o resultado de um grande trabalho, o surgimento do GNMP (Government Network Management Profile), cuja versão 1, constitui a referência que todas as agências do governo federal dos Estados Unidos devem usar ao adquirir funções e serviços de gerenciamento de rede. Novos produtos surgem dia a dia, cujo gerenciamento é indispensável.

2. INTRODUÇÃO

Os avanços tecnológicos exercem hoje um grande impacto na sociedade. A informação tem-se tornado cada vez mais uma vantagem competitiva para as empresas e organizações em investimentos futuros.

O fato é que, cada vez mais, as empresas, para se tornarem competitivas e sobreviverem no mercado, têm investido em tecnologia de informação, como a única forma de tornar seguro o processo decisório. E é nesse quadro que as redes de computadores se proliferam, encurtando as distâncias e diminuindo o tempo de resposta entre as transações entre as organizações de todo o mundo.

Gerenciar uma Rede é uma atividade complexa. Nos últimos anos o tráfego de informações dentro das redes corporativas aumentou exponencialmente devido ao surgimento de novas aplicações. Concorrentemente, novas tecnologias e padrões proporcionaram uma grande proliferação de dispositivos heterogêneos conectados à rede.

Este trabalho tem a finalidade apresentar o histórico das redes gerenciadas. Inicia-se com a descrição do que vem a ser gerenciamento de redes e os protocolos usados. Em seguida, descrevemos a necessidade do gerenciamento de redes, quando surgiu, e sua finalidade. Finalizando, apresentamos o histórico, o surgimento do gerenciamento de redes, o surgimento, as pessoas envolvidas do seu desenvolvimento.

3. GERENCIAMENTO DE REDES

A área de gerencia as redes, foi inicialmente impulsionada pela necessidade de monitoração e controle do universo de dispositivos que compõem as redes de comunicação. Com esta crescente necessidade de gerenciamento, fez-se necessário que padrões para ferramentas fossem estabelecidos.

Em resposta a esta necessidade surgiram dois padrões:

- Família de Protocolos SNMP: o protocolo SNMP (Simple Network Management Protocol) refere-se a um conjunto de padrões para gerenciamento que inclui um protocolo, uma especificação de estrutura de dados, e um conjunto de objetos de dados. Este protocolo hoje já está na sua segunda versão oficial, chamada de SNMPv2. E já existem estudos para o desenvolvimento do SNMPv3. Este é o protocolo de gerencia adotado como padrão para redes TCP/IP.
- Sistemas de gerenciamento OSI: este termo refere-se a um grande conjunto de padrões de grande complexidade, que definem aplicações de propósito gerais para gerencia de redes, um serviço de gerenciamento e protocolo, uma especificação de estrutura de dados, e um conjunto de objetos de dados. Este conjunto de protocolos é conhecido como CMIP [ISO 1991] [Stallings 1993]. Pela sua complexidade, e pela lentidão do processo de padronização, este sistema de gerenciamento não e muito popular.

O gerenciamento da rede realizado pelo protocolo Simple Network Management Protocol (SNMP), permite que uma ou mais de uma máquina na rede sejam designadas gerentes da rede. Esta máquina recebe informações de todas as outras máquinas da rede, chamadas agentes, e através do processamento destas informações pode gerenciar toda a rede e detectar facilmente problemas ocorridos.

As informações coletadas pela máquina gerente estão armazenadas nas próprias máquinas da rede, em uma base de dados conhecida como Management Information Base (MIB). Nesta base de dados estão gravadas todas as informações necessárias para o gerenciamento deste dispositivo, através de variáveis que são requeridas pela estação gerente.

Entretanto, em uma interligação de diversas redes locais, pode ser que uma rede local esteja funcionando perfeitamente, mas sem conexão com as outras redes, e, conseqüentemente, sem conexão com a máquina gerente. O ideal é implementar em alguma máquina, dentro desta rede local, um protocolo para gerenciamento que permita um trabalho off-line, isto é, que a rede local possa ser gerenciada, ou pelo menos tenha suas informações de gerenciamento coletadas, mesmo que estas informações não sejam enviadas instantaneamente a estação gerente.

O protocolo Remote Monitoring (RMON) permite uma implementação neste sentido, devendo ser implementado em diversas máquinas ao longo da rede. É possível, ainda, que uma estação com implementação RMON, envie dados à estação gerente apenas em uma situação de falha na rede. Isto contribuiria para redução do tráfego de informações de controle na rede (overhead).

Uma diminuição do tráfego na rede, facilitando seu gerenciamento, pode ser propiciada pela instalação de um servidor proxy, que , além de servir como cache dos documentos acessados por uma rede local, pode também restringir o acesso a alguns documentos ou a utilização de algum protocolo, garantindo segurança à rede.

4. NECESSIDADES DO GERENCIAMENTO DE REDES

Por menor e mais simples que seja uma rede de computadores, precisa ser gerenciada, a fim de garantir, aos seus usuários, a disponibilidade de serviços a um nível de desempenho aceitável.

À medida que a rede cresce, aumenta a complexidade de seu gerenciamento, forçando a adoção de ferramentas automatizadas para a sua monitoração e controle.

A adoção de um software de gerenciamento não resolve todos os problemas da pessoa responsável pela administração da rede. Geralmente o usuário de um software de gerenciamento espera muito dele e, conseqüentemente, fica frustrado quanto aos resultados que obtém. Por outro lado, esses mesmos softwares quase sempre são sub-utilizados, isto é, possuem inúmeras características inexploradas ou utilizadas de modo pouco eficiente. Para gerenciar um recurso, é necessário conhecê-lo muito bem e visualizar claramente o que este recurso representa no contexto da rede.

O investimento em um software de gerenciamento pode ser justificado pelos seguintes fatores:

- As redes e recursos de computação distribuídos estão se tornando vitais para a maioria das

organizações. Sem um controle efetivo, os recursos não proporcionam o retorno que a corporação requer.

- O contínuo crescimento da rede em termos de componentes, usuários, interfaces, protocolos e fornecedores ameaçam o gerenciamento com perda de controle sobre o que está conectado na rede e como os recursos estão sendo utilizados.
- Os usuários esperam uma melhoria dos serviços oferecidos (ou no mínimo, a mesma qualidade), quando novos recursos são adicionados ou quando são distribuídos.
- Os recursos computacionais e as informações da organização geram vários grupos de aplicações de usuários com diferentes necessidades de suporte nas áreas de desempenho, disponibilidade e segurança. O gerente da rede deve atribuir e controlar recursos para balancear estas várias necessidades.
- À medida que um recurso fica mais importante para a organização, maior fica a sua necessidade de disponibilidade. O sistema de gerenciamento deve garantir esta disponibilidade.
- A utilização dos recursos deve ser monitorada e controlada para garantir que as necessidades dos usuários sejam satisfeitas a um custo razoável.

Além desta visão qualitativa, uma separação funcional de necessidades no processo de gerenciamento foi apresentada pela ISO (International Organization for Standardization), como parte de sua especificação de Gerenciamento de Sistemas OSI. Esta divisão funcional foi adotada pela maioria dos fornecedores de sistemas de gerenciamento de redes para descrever as necessidades de gerenciamento: Falhas, Desempenho, Configuração, Contabilização e Segurança.

5. HISTÓRICO DO GERENCIAMENTO DE REDES

Quando em 1986 reuniu-se, pela primeira vez, o Grupo de Trabalho sobre gerenciamento de Redes do Comitê Técnico em Comunicação de dados IFIP (International Federation for Information Procesing) havia apenas o consenso sobre a necessidade de gerenciamento. Cerca de 20 pessoas reunidas em Dallas, provenientes de diversos países, sequer concordavam sobre o escopo do gerenciamento de rede. Enquanto representantes incorporasse apenas as três camadas inferiores da arquitetura OSI – Open System Interconnection (pois era com o que estavam acostumados a trabalhar), para os outros o gerenciamento de redes devia englobar as sete camadas. Percebia-se claramente que cada fornecedor tinha construído uma arquitetura proprietária de gerenciamento para seus produtos e tinha dificuldade de impingi-la aos

clientes, ao lado de outros fornecedores. Já se falava na oportunidade sobre o gerenciamento OSI, embora muitos tenham encarado com certo ar de dúvida aquela alternativa.

A abordagem clássica para integrar o gerenciamento de redes era, pois, baseada em arquitetura proprietárias. Para que pudessem funcionar como elemento de integração, os arquitetos de tais soluções incorporaram nelas uma abertura para agregar a informação de gerenciamento de sistema de outros fornecedores. A IBM, por exemplo, com o conceito de focal point abriu esta porta para integrar outros sistemas de gerenciamento ao Netview, principalmente por interesse próprio, uma vez que a aquisição da RDLM (fabricante PABX) levou a esta necessidade. Módulos para traduzir o fluxo de informação de gerenciamento de um esquema para outros tinham de ser constituídos e podiam ser implantados em vários pontos, como mostra a Figura 1.

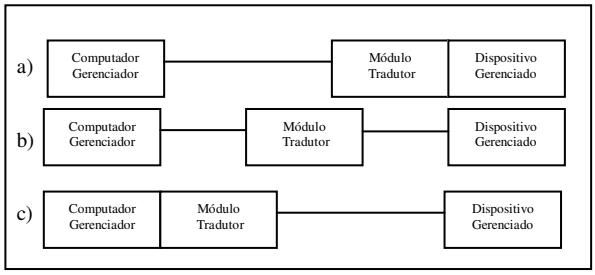


Figura 1 – Formas de Implantação do Módulo Tradutor.

Na figura 1, a) poderia ser um servidor de rede Novell, com um módulo interno capaz de gerar os "vetores de alerta" esperados pelo Netview. O caso b) poderia ser a solução para integrar o gerenciamento de um PABX digital em que a tradução seria feita em um PC que receberia as mensagens de gerenciamento de um lado e as traduziria, quando possível, para o outro. A terceira abordagem seria para o caso em que um roteador fosse o diagnostico gerenciado e que usasse um protocolo padrão de fato na indústria, tal como o SNMP (Simple Network Management Protocol da arquitetura Internet), com a conversão feita internamente no computador gerenciador.

Dentro dos problemas decorrentes desta solução, pode-se destacar principalmente a limitação imposta pelo fato de somente usar opções gerenciamento (dados recebidos e comandos veiculáveis) que tinham similar na arquitetura proprietária do fornecedor do computador gerenciador. Opções de interação propiciadas pelos dispositivos gerenciados podiam não ser aproveitadas simplesmente pela falta de condições de mapeá-las para uma forma passível de reconhecimento pelo computador gerenciador. Em decorrência, os dispositivos gerenciados providos pelo mesmo fornecedor do computador gerenciador "pareciam" mais facilmente

gerenciáveis. Para não parecerem diminuídos sob este prima, muitos fornecedores não se mostravam entusiasmados em cooperar para tornar seus produtos gerenciáveis por um computador gerenciador de outro fabricante.

Esta abordagem foi adotada por alguns fornecedores no mercado, como a IBM e a DEC, mas cada vez mais crescida o desejo por um sistema de gerenciamento independente de fornecedor que pudesse rodar numa máquina dedicada, de modo a não sobrecarregar nem prejudicar o atendimento dos serviços normais a serem executados no mainframe. A AT&T também entrou o cenário, definindo uma arquitetura de gerenciamento e se propondo a gerenciar as redes de seus clientes de telecomunicações.

Criando o impasse, uma solução alternativa teria de ter buscada, implicando a agregação de esforços que levassem a uma solução mais universal e padronizada. Obviamente, tal solução deveria englobar is serviços de gerenciamento mais importantes e relevantes, além de formalizar a interação entre os dispositivos gerenciados e os gerenciadores. A ISO tomou a bandeira e o esquema básico da arquitetura de gerenciamento de rede foi adicionado ao modelo de referência ISO/OSI em 1989.

A colaboração entre a ISO/IEC (International Organization for Standardization / International Eletrotechnical Committee) resultou na série de documentos X.700, cujo objetivo maior é criar condições para o desenvolvimento de produtos de gerenciamento de redes de computadores e sistema de comunicações heterogêneos.

Todavia, o embate das forças dominantes no cenário internacional dificultou a estabilização dos detalhes operacionalizastes do modelo de gerenciamento. Anos se passaram sem que os documentos atingissem o estágio do padrão ISO internacional. As implantações, baseadas em interpretações da documentação disponível, começaram a aparecer e, em 1989, percebendo a necessidade de acordos que assegurassem a interoperabilidade das implementações, os fornecedores começaram a reunir-se em associações como a ISO/NM Fórum, para buscar um acordo que viabilizasse a definição de um conjunto de opções de implantação capaz de assegurar a interoperabilidade dos sistemas de gerenciamento. Outro grupo foi criado sob a tutela do NIST (National Institute of Standards and Technology) dos Estados Unidos para atender às necessidades do governo americano, que já havia determinado, através de seu documento GOSIP (Government OSI Profile), que as soluções de redes a serem adquiridas deveriam atender às recomendações ISO/IEC. Este trabalho resultou no GNMP (Government Network Management Profile), cuja versão 1, de 30 de julho de 1992, constitui a referência que todas as agências do governo federal dos Estados Unidos devem usar ao adquirir funções e serviços de gerenciamento de rede.

O primeiro dos protocolos de gerência de rede foi o SGMP (Simple Gateway Monitoring Protocol) que surgiu em novembro 1987. Entretanto, o SGMP era restrito à monitoração de gateways. A necessidade crescente de uma ferramenta de gerenciamento de rede mais genérica fez emergirem mais algumas abordagens:

High-Level Entity Management System – HEMS – generalização do HMP – Host Management Protocol;

SNMP – Simple Network Management Protocol – um melhoramento do SGMP;

CMOT – (CMIP over TCP/IP) uma tentativa de incorporar o máximo possível o protocolo (CMIP), serviços e estrutura de base de dados que estava sendo padronizada pela ISO para gerenciamento de redes.

No início de 1988 a IAB (Internet Architecture Board) revisou os protocolos e escolheu o SNMP como uma solução de curto prazo e o CMOT como solução de longo prazo para o gerenciamento de redes. O sentimento era que, em um período de tempo razoável, as instalações migrariam do TCP/IP para protocolos baseados em OSI. Entretanto, como a padronização do gerenciamento baseado no modelo OSI apresentava muita complexidade de implementação e o SNMP, devido à sua simplicidade, foi amplamente implementado nos produtos comerciais, o SNMP tornou-se um padrão de fato. Posteriormente, pela existência de lacunas funcionais (devido exatamente à simplicidade do SNMP), foram definidas novas versões do protocolo SNMP chamadas de SNMPv2 e SNMPv3, e o SNMP original ficou conhecido como SNMPv1.

A primeira versão da arquitetura de gerenciamento SNMP foi definida no RFC 1157 de maio de 1990.

O RFC 1157 define ainda três objetivos a serem alcançados pelo SNMP: minimizar o número e complexidade das funções de gerenciamento, ser flexível o suficiente para permitir expansões futuras e ser independente da arquitetura e mecanismo dos dispositivos gerenciados.

A definição das informações de gerenciamento requer não apenas profundo conhecimento da área específica em foco, mas também do modelo de gerenciamento.

6. CONCLUSÃO

Com o crescimento e evolução das redes de computadores têm se tornado fundamental a área de gerência de redes agregar as necessidades de monitoramento e controle, assim, podemos concluir que é muito importante dentro de uma organização a implementação de um gestor de

redes, bem como as ferramentas de monitoramento para controlar e monitorar uma rede evitando assim ocorrer os riscos de falhas.

Novos produtos surgem dia a dia, cujo gerenciamento é indispensável. A definição dos objetos gerenciados que os representem é necessária e precisa ser continuamente realizada. Neste sentido, torna-se importante à capacitação para usar todas as ferramentas inerentes à estrutura de gerenciamento de rede. Adicionalmente, aplicações precisam ser escritas, para usar as interfaces pelo sistema de gerenciamento de modo a propiciar os serviços considerados importantes em cada organização.

REFERÊNCIAS

http://www.rnp.br/newsgen/9708/n3-2.html
http://www.inf.pucrs.br/~gustavo/rici/Redes.pdf
Apostila de TCP/IP(Entidade ACR-Informática)
http://www.projetoderedes.com.br/tutoriais
http://www.buscaki.com.br/links/redes.html
http://www.getronics.com.br
http://www.aldemario.adv.br/infojur/conteudo4texto.htm
http://www.multirede.com.br/pagina.php?codigo=10
http://www.teleco.com.br/emdebate/quadros02.asp
http://www.absoluta.org/tcp/tcp_per_hist.htm#2.3
http://www.lol.com.br/conectividade/redes/ger%EAncia_de_rede.php
http://www.vision.ime.usp.br/~mehran/ensino/ger.html

CARVALHO, Tereza Cristina Melo de Brito. **Gerenciamento de redes: uma abordagem de sistemas**. São Paulo: Makron Books,1993, 364 p.

ESTUDO SOBRE SNMP

1. RESUMO

Este trabalho tem como objetivo principal abordar as características e recursos do protocolo de gerenciamento conhecido como SNMP. Para atingir este objetivo descreveremos a arquitetura, o gerenciamento e a utilização do SNMP. Com a finalidade de poder utilizar o máximo de recursos possíveis deste protocolo.

2. INTRODUÇÃO

Até o início 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 da gerência de tais redes, a situação ainda favorecia arquiteturas proprietárias, devido à 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. No final da década de 1990, a solução SNMP já era tão difundida que se estabelecera como padrão de gerência de redes de computadores. 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 bancos de dados etc.).

3. OS PRINCIPAIS OBJETIVOS DO PROTOCOLO SNMP

- ✓ Reduzir o custo da construção de um agente que suporte o protocolo;
- ✓ Reduzir o tráfego de mensagens de gerenciamento pela rede necessárias para gerenciar dos recursos da rede;

- ✓ Reduzir o número de restrições impostas as ferramentas de gerenciamento da 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 a somente a algumas implementações particulares.

4. AGENTE DE GERENCIAMENTO

O agente de gerenciamento é o componente contido nos dispositivos que devem ser gerenciados. Bridges, roteadores, hubs e switches podem conter agentes SNMP que permitem que eles sejam controlados pela estação de gerenciamento. O agente de gerenciamento responde à estação de gerenciamento de duas maneiras:

2.1- Polling -A estação de gerenciamento solicita dados ao agente e o agente responde com os dados solicitados.

2.2 - Interceptação - É um método de reunião de dados projetado para reduzir o tráfego na rede e para o processamento nos dispositivos que estão sendo monitorados. Em vez da estação de gerenciamento fazer polling nos agentes em intervalos determinados e contínuos, são definidos limites (superiores e inferiores) no dispositivo de gerenciamento. Se esses limites forem ultrapassados no dispositivo, o dispositivo de gerenciamento enviará uma mensagem de alerta à estação de gerenciamento. Isso elimina a necessidade de fazer polling em todos os dispositivos gerenciados na rede. A interceptação é muito útil em redes com muitos dispositivos que precisem ser gerenciados. Ela reduz a quantidade de tráfego SNMP na rede para fornecer mais largura de banda para a transferência de dados.

O mundo SNMP está baseado em três documentos:

- ✓ Structure of Management Information (SMI). Definido pela RFC 1155, a SMI traz essencialmente, a forma pela qual a informação gerenciada é definida.
- ✓ Management Information Base (MIB) principal. Definida na RFC 1156, a MIB principal do mundo SNMP (chamada MIB-2) define as variáveis de gerência que todo elemento gerenciado deve ter, independentemente de sua função particular. Outras MIBs foram posteriormente definidas para fins particulares, tais como MIB de interfaces Ethernet, MIB de nobreaks, MIB de repetidores etc.

- ✓ Simple Network Management Protocol (SNMP). Definido pela RFC 1157, é o protocolo usado entre gerente e agente para a gerência, principalmente trocando valores de variáveis de gerência.

5. MENSAGENS NO PROTOCOLO SNMP

Ao contrário de muitos outros protocolos TCP/IP, as mensagens no protocolo SNMP além de não apresentarem campos fixos, são codificadas usando a sintaxe ASN.1 (tanto a mensagem de pedido, como a de resposta) o que dificulta o entendimento e a decodificação das mensagens.

Os cinco tipos de mensagens SNMP são:

- ✓ get-request-PDU: mensagem enviada pelo gerente ao agente solicitando o valor de uma variável;
- ✓ get-next-request-PDU: mensagem utilizada pelo gerente para solicitar o valor da próxima variável depois de uma ou mais variáveis que foram especificadas;
- ✓ set-request-PDU: mensagem enviada pelo gerente ao agente para solicitar que seja alterado o valor de uma variável
- ✓ get-response-PDU: mensagem enviada pelo agente ao gerente, informando o valor de uma variável que lhe foi solicitado;
- ✓ trap-PDU: mensagem enviada pelo agente ao gerente, informando um evento ocorrido.

As partes mais importantes de uma mensagem são: as operações (GET, SET e GET-NEXT) e a identificação, no formato ASN.1, dos objetos em que as operações devem ser aplicadas. Deve existir um cabeçalho que informe o tamanho da mensagem, que só será conhecido após a representação de cada campo ter sido computada. Na verdade, o tamanho da mensagem depende do tamanho de sua parte remanescente (que contém os dados), portanto o tamanho só poderá ser computado após a construção da mensagem. Uma maneira de evitar este problema é construir a mensagem de trás para frente.

Uma mensagem SNMP deve definir o servidor do qual obtemos ou alteramos os atributos dos objetos, e que será responsável por converter as operações requisitadas em operações sobre as estruturas de dados locais. Após verificar os campos de uma mensagem, o servidor deve usar as estruturas internas disponíveis para interpretar a mensagem e enviar a resposta da operação ao cliente que requisitou o pedido. Uma mensagem é constituída por três partes principais:

- ✓ A versão do protocolo;

- ✓ A identificação da comunidade, usada para permitir que um cliente acesse os objetos gerenciados através de um servidor SNMP;
- ✓ A área de dados, que é dividida em unidades de dados de protocolo (Protocol Data Units - PDUs). Cada PDU é constituída ou por um pedido do cliente, ou por uma resposta de um pedido (enviada pelo servidor).

O primeiro campo de uma mensagem SNMP é um operador seqüencial, seguido por um campo com o tamanho total da mensagem (se este tamanho não for igual ao do datagrama, será retornado um código de erro). O próximo campo é um número inteiro que identifica a versão do protocolo SNMP, seguido por um campo usado para a autentificação, indicando a comunidade que o cliente pertence (a comunidade public permite a qualquer cliente acessar os objetos, não precisando o servidor verificar se o cliente pode ou não acessar o objeto). O quarto campo contém a operação que será executada, devendo ser um GET, SET ou GET-NEXT pois a operação de TRAP só é gerada pelo servidor. O quinto campo é usado para o servidor ter certeza de que o valor deste campo é igual ao tamanho da parte da mensagem que contém os dados. O sexto campo é uma identificação para o pedido, e o sétimo e o oitavo campos são flags que indicam erros quando estão setadas (campos de status e de índice de erro).

Na definição de uma mensagem, cada uma das PDUs são constituídas ou por um dos cinco tipos de PDUs para as operações ou por uma PDU para a resposta. Na definição da mensagem SNMP, deve-se ter uma sintaxe individual para cada um das cinco operações da PDU. Alguns termos encontrados nas sintaxes das PDUs das operações são:

- ✓ O campo RequestID é um inteiro de 4 bytes (usado para identificar as respostas);
- ✓ Os campos ErrorStatus e ErrorLevel são inteiros de um byte (sendo nulos em um pedido de um cliente);
- ✓ O campo VarBindList é uma lista de identificadores de objetos na qual o servidor procura os nomes dos objetos, sendo definida como uma sequência de pares contendo os nomes dos objetos (em ASN.1 este par é representado como uma sequência de dois itens). Na sua forma mais simples (com um objeto) apresenta dois itens: o nome do objeto e um ponteiro nulo.

6. LIMITAÇÕES DE SNMP

- ✓ Falta de segurança
  - ➢ Esquema de autenticação trivial

- Limitações no uso do método SET

- ✓ Ineficiência
  - Esquema de eventos limitado e fixo
  - Operação baseada em pooling
  - Comandos transportam poucos dados

- ✓ Falta de Funções Específicas
  - MIB com estrutura fixa
  - Falta de comandos de controle
  - Falta de comunicação entre gerenciadores

- ✓ Não Confiável
  - Baseado em UDP/IP
  - Trap sem reconhecimento

7. SNMPV2 E SNMPV3

Visando obter melhorias com relação aos aspectos de segurança foram desenvolvidas novas versões do SNMP. A segunda versão, o SNMPv2 contém mecanismos adicionais para resolver os problemas relativos á segurança como: privacidade de dados, autenticação e controle de acesso.

A terceira versão, o SNMPv3 tem como objetivo principal alcançar a segurança, sem esquecer-se da simplicidade do protocolo, através de novas funcionalidades como:

- ✓ Autenticação de privacidade
- ✓ Autorização e controle de acesso
- ✓ Nomes de entidades
- ✓ Pessoas e políticas
- ✓ Usernames e gerência de chaves
- ✓ Destinos de notificações
- ✓ Relacionamentos proxy
- ✓ Configuração remota

8. CONCLUSÃO

Como o protocolo SNMP é amplamente utilizado, seria impossível imaginar uma referência rede sem o uso de ferramenta que o implementa. Os mecanismos oferecidos pelo protocolo SNMP permitem efetuar tarefas de monitoração; além da possibilidade de efetuar configuração nos equipamentos gerenciados.

Com o surgimento das novas versões o SNMPv2 e SNMPv3, foram realizadas alterações na especificação do protocolo, tais como a forma de representação das variáveis, e inclusão de novos tipos de PDUs e o retorno dos tipos de erros, que acabaram por tirar a simplicidade do protocolo. Entretanto, o SNMP é amplamente usado, sendo que, a maioria dos fabricantes de hardware para internet (como bridges e roteadores) projetam seus produtos para suportar o SNMP.

REFERÊNCIAS

http://www.teleco.com.br/tutoriais/tutorialsnmp/pagina_2.asp
http://www.inf.ufrgs.br/gpesquisa/tf/estudantes/trabalhos/peres.html
http://www.gta.ufrj.br/~alexszt/ger/snmpcmip.html
<http://mesonpi.cat.cbpf.br/naj/snmp_color.pdf>. Acessado em 22/08/2005.
http://www.malima.com.br/article_read.asp?id=50. Acessado em 22/08/2005.
Net academy cisco network
http://www.rnp.br/newsgen/9708/n3-2.html
http://www.cbpf.br/~sun/pdf/snmp.pdf
http://www.inf.furb.br/~pericas/orientacoes/JDMK2000.pdf
http://www.rnp.br/newsgen/9708/n3-2.html
http://www.cbpf.br/~sun/pdf/snmp.pdf
http://www.inf.furb.br/~pericas/orientacoes/JDMK2000.pdf

ESTUDO SOBRE CMIP

1. RESUMO

Os modelos predominantemente usados no gerenciamento de redes são o SNMP e o CMIP. Entretanto, o SNMP foi proposto para gerenciamento de redes internet, mas não vem suportando a complexidade que as redes atuais vem exigindo. E o CMIP proposto pela ISO é muito complexo e seu processo de padronização é muito lento, por isso ele não tem a mesma aceitação do SNMP.

2. INTRODUÇÃO

O CMIP é um protocolo de gerenciamento definido segundo o padrão 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 de Gerenciamento, ou seja, com o primeiro acessando e mudando informações que se encontram na MIB. Os tipos de informação a serem trocadas levam em conta o CMIS (Common management information service), que especifica o conjunto de serviços a que os sistemas gerenciador e gerenciado 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 e uma aplicação da camada 7 do RM-OSI.

O CMISE utiliza duas aplicações de serviço comuns (São aplicações de serviço comum àquelas aplicações que oferecem serviços não só as aplicações de gerenciamento, bem como a todas as outras.), 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.

O CMIP possui onze informações para a troca de mensagens. São elas: m-event-report, m-event-report-confirmed, m-get, m-linked-reply, m-cancel-get-confirmed, m-set, m-set-confirmed, m-actin, m-action-confirmed, m-create e m-delete.

3. O PROTOCOLO CMIP

Num ambiente de gerenciamento OSI, o protocolo CMIP é utilizado para definir as regras de comunicação entre os processos gerente e agente. Este protocolo trabalha no Nível de

Aplicação e é orientado a conexão utilizando os serviços providos pelo ASCE (Association Control Service Element), ROSE (Remote Operations Service Element) e pelo serviço de apresentação.

A utilização dos padrões da ISO para gerenciamento tem sido sustentada 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 e flexibilidade.

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 de Gerenciamento, ou seja, com o primeiro acessando e mudando informações que se encontram na Mib. Os tipos de informação a serem trocadas levam em conta o serviço do CMIS (Common management information service), que especifica o conjunto de serviços a que os sistemas gerenciador e gerenciado poderão acessar para que seja realizado o gerenciamento.

Juntos CMIS e CMIP formam o que é chamado de CMISE (Common Management information Service Element). Os serviços do CMIS e o protocolo CMIP são usados para implementar sistemas desenvolvidos para vários propósitos, como o gerenciamento de desempenho, de nível de falhas, de segurança, de configuração e de contabilidade, usando os recursos de uma rede baseada no modelo de comunicação OSI.

3.1 CMIS

Como já foi dito, o CMIS é uma norma que define o conjunto de serviços oferecidos às aplicações de gerenciamento (software do gerente e software do agente).

O conjunto de serviços oferecidos se enquadram em três categorias. São eles:

***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 CMISE 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.

3.2 Relação de Serviços e PDU's do CMIS/P:

Cada serviço, além de estar enquadrado em uma categoria, está associado a um conjunto de PDU's, exceto os serviços de associação. Abaixo a lista de serviços de acordo com a categoria, ou seja, as 11 PDUs que o CMIP utiliza:

***Serviços de Associação*:**
A-ASSOCIATE:
A-RELEASE:
A-ABORT :

***Serviços de Notificação*:**
M-EVENT-REPORT:

***Serviços de Operação*:**
M-GET
M_CANCEL-GET
M-SET
M-ACTION
M-CREATE
M-DELETE:
M-CANCEL-GET-CONFIRMED

Além das funções apresentadas o CMIS apresenta facilidades adicionais que permitem selecionar um conjunto de objetos sobre o qual pode-se aplicar a mesma operação, e também a existência de respostas múltiplas para cada requisição (uma para cada objeto gerenciado). São três as facilidades adicionais:
1. Scopping - permite selecionar um grupo de instâncias de objetos gerenciados sobre o qual será aplicada uma única operação;

2. Filtro - dá a possibilidade de definir um conjunto de testes que serão aplicados a um grupo de instâncias de um objeto, selecionado por uma operação de *scopping* anterior, permitindo formar um grupo menor a partir deste, sobre o qual as operações de gerenciamento devem ser aplicadas;

3. Sincronização permite sincronizar várias operações de gerenciamento a serem aplicadas a instâncias de objetos gerenciados, obtidos através do uso das operações de scopping e de filtragem.

4. CMISE

O CMISE (Common Management Information Service Element) implementa os serviços definidos pelo CMIS, executando o protocolo CMIP. É correspondente ao mecanismo SASE (*Special Application Service Element*) da camada de aplicação, e utiliza os elementos ACSE (*Association Control Service Element*) e ROSE (*Remote Operations Service Element*) que juntos correspondem ao mecanismo de CASE (*Common Application Service Element*) também da camada de aplicação.

Os serviços oferecidos pelo CMISE ao protocolo CMIP podem ser confirmados ou não confirmados. A tabela mostra a relação entre os serviços CMISE e as classes de operação do protocolo CMIP. Estes serviços serão mapeados em operações aplicadas sobre os objetos gerenciados, que representam os recursos da rede a serem gerenciados.

SERVIÇO	TIPO	CLASSE DE OPERAÇÃO
M-EVENT-REPORT	confirmado/não-confirmado	2 ou 1/5
M-GET	confirmado	2 ou 1
M-CANCEL-GET	confirmado	2 ou 1
M-SET	confirmado/não-confirmado	2 ou 1/5
M-ACTION	confirmado/não-confirmado	2 ou 1/5
M-CREATE	confirmado	2 ou 1
M-DELETE	confirmado	2 ou 1

5. CMOT

Existe uma terceira proposta chamada de CMOT (*CMIP Over TCP/IP*) cujo objetivo é permitir o uso do CMIP em redes com o protocolo TCP/IP.

CMOT (CMIP over TCP/IP) e a utilização do protocolo CMIP dentro da arquitetura internet. Para que isto seja realizado se faz necessária a implantação do protocolo LPP na camada apresentação da Arquitetura Internet. Este protocolo soluciona eventuais incompatibilidades

entre as duas arquiteturas (OSI x INTERNET) no que diz respeito a gerenciamento.

5.1 Conceitos básicos

O gerenciamento no modelo OSI da ISO baseia-se na teoria da orientação a objetos. O sistema representa os recursos gerenciados através de entidades lógicas chamadas de objetos gerenciados. Ao desenvolver uma aplicação de gerenciamento, usamos processos distribuídos conhecidos como gerentes (os quais gerenciam) e agentes (os que realizam as ações). Além de definir um modelo informacional, define-se também um modelo funcional em que para cada área é definido um conjunto de funções, que ao serem implementadas, serão usadas para gerenciar a rede. Existem cinco áreas funcionais no gerenciamento num ambiente OSI:

- Gerência de configuração (estado da rede);
- Gerência de desempenho (vazão e taxa de erros);
- Gerência de falhas (comportamento anormal);
- Gerência de contabilidade (consumo de recursos);
- Gerência de segurança (acesso);

5.2 Gerentes, agentes e objetos gerenciados

Num ambiente de gerenciamento OSI, usa-se o protocolo CMIP para definir as regras de comunicação entre os processos gerente e agente. O protocolo CMIP implementa as primitivas oferecidas pelo serviço de informação de gerenciamento CMIS. Este ambiente também propõe uma estrutura de gerenciamento para permitir a definição dos conceitos necessários à construção de classes de objetos gerenciados, os princípios necessários à nomeação dos objetos e dos seus componentes, e como é definido o inter-relacionamento entre os objetos. Para descrever a estrutura, são usadas a Hierarquia de Herança, a Hierarquia de Nomeação e a Hierarquia de Registro.

a. Na Hierarquia de Herança a modelagem é realizada com base nas classes de objetos. Para se obter sub-classe com um comportamento mais particular, deve-se detalhar uma superclasse, gerando a partir destas subclasses para um propósito mais particular do que esta classe.

b. Na Hierarquia de Nomeação é descrita a relação de composição entre os objetos, ou seja, a relação de subordinado x superior entre estes objetos, além de serem definidas as regras

usadas para nomear os objetos (*name binding*), de forma que este seja univocamente determinado.

c. Na Hierarquia de Registro são registradas as definições das classes dos objetos, os atributos dos objetos, as ações que podem ser aplicadas, as notificações geradas e os pacotes, seguindo as regras definidas pela notação ASN.1.

6. SNMP X CMIP

Uma comparação entre o SNMP e o CMIP demonstra que o SNMP é excessivamente simples quando usado em aplicações que não foram previstas quando foi definido, e que apresenta deficiências em relação a segurança ao ser usado em aplicações mais críticas. Já o CMIP é um protocolo poderoso e abrangente que foi concebido com o objetivo de adequar-se à complexidade das redes. Mas apesar desta característica, ainda não alcançou um grau de estável de aceitação pela comunidade. As projeções de mercado demonstram que o SNMP continuará sendo muito usado em pequenas redes, enquanto que o CMIP deve dominar o mercado composto pelas grandes redes corporativas e redes públicas de telecomunicações.

7. CONCLUSÃO

Tanto o SNMP como o CMIP suporta a mesma idéia de troca de mensagens entre gerente e agente e armazenamento das informações na MIB.

O SNMP é simples e mais fácil de ser implementado. Em compensação, possui limitações de desempenho que o CMIP não possui. Principalmente na área de segurança. Portanto o SNMP se adequa mais a sistemas de pequeno porte, pois se pode exigir menos de um sistema de gerenciamento. Devido o CMIP ser bem completo e projetado é mais útil em sistemas de comunicação de grande porte onde existem grandes quantidades de recursos a serem gerenciados. Em contraposição, em sistemas de pequeno porte, ele não se torna adequado devido a sua complexidade.

REFERÊNCIAS

http://www.projetoderedes.com.br

http://www.rnp.br/newsgen/9805/metricas.html

http://penta2.ufrgs.br/gere96/cmipXsnmp/snmpcmipf.htm - acessado em 02/09/2005

http://penta2.ufrgs.br/gere96/cmipXsnmp/cmip_stra.htm - acessado em 02/09/2005
http://www.gta.ufrj.br/grad/cmip.html#cmip - acessado em 02/09/2005

ESTUDO SOBRE SMI

1. RESUMO

A SMI descreve o cenário no qual a Base de Informação Gerencial pode ser definida. A SMI, baseada na abordagem orientada a objetos, introduz os conceitos de hierarquia, herança, nomeação e registros usados na caracterização e identificação de objetos gerenciados. Além disso, ela define o conjunto de operações que pode ser realizado sobre os objetos gerenciados da MIB e o comportamento desses objetos mediante a execução destas operações.

2. INTRODUÇÃO

A SMI (Structure of Management Information), como é chamada esta instrumentação, é análoga à linguagem de programação usada para construir estruturas de dados e permitir operações que possam ser executadas sobre essas estruturas. A combinação de uma SMI com um protocolo particular é denominada ***framework***. Tem por finalidade ser um padrão da MIB e pode ser definida e construída na RFC 1511. Ela identifica os tipos de dados que podem ser utilizados na MIB e especifica como os recursos são reapresentados e nomeados. A SMI procura a simplicidade e a escalabilidade.

3. DEFINIÇÕES PARA SMI

Um objeto gerenciador não tem apenas que estar definido mas identificado também. Isto é feito usando o Identificador de Objetos como um número de telefone, reservando um grupo de números para diferentes localizações. No caso do TCP/IP - baseado em gerenciamento de rede, o número alocado é 1.3.6.1.2 e a SMI usa isto como uma base para definir novos objetos. Abaixo está um exemplo que mostra a definição de um objeto contido em uma MIB. Seu nome é sysDescr e faz parte do grupo System.

OBJETO

sysDescr { system 1 }
Sintaxe STRING de OCTETOS

Os tipos de dados SMI são divididos em três categorias:

- ✓ tipo simples

- ✓ tipo de grandes aplicações
- ✓ tipo construtor simples

Os tipos simples incluem quatro tipos ASN. 1 primitivos:

- ✓ Inteiros - valores negativos ou positivos de todos os números, inclusive o zero
- ✓ Cadeia de octetos - seqüência ordenada de zero ou mais octetos
- ✓ Identificadores de objetos - conjunto de todos os identificadores de objetos alocados de acordo com as regras especificadas pelo ASN.1.

Tipos de dados de grandes aplicações referem-se aos tipos de dados especiais definidos pelo SMI:

- ✓ Endereços de rede - representam um endereço de uma família particular de protocolos
- ✓ Contadores - inteiros não negativos são incrementados de um em um até atingirem um valor máximo, quando eles são resetados e voltam a zero. O número total de bits recebidos em uma interface é um exemplo de contador
- ✓ Medidas - inteiros não negativos que são incrementados ou decrementados, porém atrelados a um valor máximo. O tamanho da fila de saída de pacotes é um exemplo
- ✓ Checagem de tempo - o tempo de um evento. O tempo necessário para uma interface chegar ao estado corrente é um exemplo
- ✓ Opaco - representa uma codificação arbitrária. Este tipo de dados é usado para passar uma cadeia de informações arbitrárias que não está de acordo com a tipagem de dados usada no SMI
- ✓ Inteiros - representa uma informação com valores inteiros sinalizados. Este tipo de dados redefine o tipo de dados simples "inteiro" do ASN.1, que tem uma precisão arbitrária no ASN.1, porém uma precisão determinada no SMI
- ✓ Inteiros sem sinal - representa uma informação com valores inteiros não sinalizados. Ele é útil quando os valores são sempre não negativos. Este tipo de dados redefine o tipo de dados simples "inteiro" do ASN.1, que tem uma precisão arbitrária no ASN.1, porém uma precisão determinada no SMI.

O tipo construtor simples inclui dois tipos ASN.1 que definem múltiplos objetos em tabelas e listas:

- ✓ Linha - referência a uma linha de uma tabela. Cada elemento de uma linha pode ser um tipo simples ou um tipo de grandes aplicações
- ✓ Tabela - referência a uma tabela com zero ou mais linhas. Cada linha pode ter um número qualquer de colunas

A especificação BER, definida por [8825,*Specification of Basic Encoding Rules for* ASN.1] citado por [Cisco96], permite que máquinas diferentes troquem informações de gerenciamento especificando a posição de cada bit nos octetos transmitidos e a estrutura dos bits. A estrutura de bits é definida pela descrição do tipo de dados, tamanho e valor.

4. CONCLUSÃO

Concluímos que a SMI descreve o cenário no qual a Base de Informação Gerencial pode ser definida. A SMI, baseada na abordagem orientada a objetos, introduz os conceitos de hierarquia, herança, nomeação e registros usados na caracterização e identificação de objetos gerenciados. Além disso, ela define o conjunto de operações que pode ser realizado sobre os objetos gerenciados da MIB e o comportamento desses objetos mediante a execução destas operações. A MIB é uma base de dados, cuja estrutura é especificada pelo padrão SMI, como já descrito anteriormente. Ela pode ser caracterizada como um banco de dados ativo, o que possibilita que os valores das suas variáveis sejam, não só recuperados,como também alterados. Cada agente deve manter sua própria instancia da MIB, relacionada com os objetos que estão sendo gerenciados sob o seu domínio. O RFC 1213 define um conjunto de variáveis utilizadas para a monitoração e o controle de redes TCP/IP.

REFERÊNCIAS

http://www.apostilando.com/download.php?cod=252&categoria=Redes.
http://www.gta.ufrj.br/~alexszt/ger/compact.html
http://www.rnp.br/newsgen/9708/n3-2.html
http://www.malima.com.br/article_read.asp?id=50
http://www.redes.unb.br/PFG.092004.pdf
http://www.mcc.ufc.br/disser/ErnestoVasconcelos.pdf.

ESTUDO SOBRE MIB

1. RESUMO

O conhecimento das MIB's (Base de Informações Gerenciáveis), e principalmente, o conhecimento de como utilizar estas informações são de fundamental importância na Gerência de Redes.

2. INTRODUÇÃO

Este hiperdocumento procura introduzir o conceito de MIB e apresentar os dois principais padrões de MIB, a MIB da OSI e a MIB da Internet, aprofundando mais neste último, no qual serão apresentados todos os objetos gerenciados e suas possíveis utilizações. Dentro deste contexto, a MIB é definida como um conjunto de objetos gerenciados dentro de um Sistema Aberto, na qual um objeto gerenciado é a visão abstrata de um recurso real dentro deste sistema.

3. DEFINIÇÃO DE MIB

Antes de definir o que é uma MIB, introduziremos 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.

3.1 O que é a MIB ?

A MIB é o conjunto dos objetos gerenciados, que procura abranger todas as informações necessárias para a gerência da rede, possibilitando assim, a automatização de grande parte das tarefas de gerência.

4. MIB DA OSI

O padrão OSI define três modelos para gerência de redes: o modelo organizacional, o modelo informacional e o modelo funcional. O modelo organizacional descreve a forma pela qual a gerência pode ser distribuída entre domínios e sistemas dentro de um domínio. O modelo funcional descreve as áreas funcionais e seus relacionamentos. Já o **modelo informacional** provê a base para a definição de **objetos gerenciados** e suas relações, classes atributos, ações e nomes.

Na definição de objetos gerenciados é utilizada a orientação a objetos. Objetos com características semelhantes são agrupados em classes de objetos. Uma classe pode ser uma subclasse de outra, e a primeira herda todas as propriedades da segunda. Uma classe é definida pelos atributos da classe, pelas ações que podem ser invocadas, pelos eventos que podem ser relatados, pela subclasse a qual ela deriva e pela superclasse na qual ela está contida.

Para a definição dos objetos gerenciados deve-se considerar três hierarquias: hierarquia de herança, de nomeação e de registros usados na caracterização e identificação de objetos gerenciados.

A seguir descreveremos cada uma das hierarquias mencionadas acima.

a) Hierarquia de Herança

Também denominada hierarquia de classe, tem como objetivo facilitar a modelagem dos objetos.

b) Hierarquia de Nomeação

descreve a relação de "estar contido em" aplicado aos objetos. Um objeto gerenciado está contido dentro de um e somente um objeto gerenciado.

Um objeto gerenciado existe somente se o objeto que o contém existir, e dependendo da definição, um objeto só pode ser removido se aqueles que lhe pertencerem forem removidos primeiro.

c) Hierarquia de Registro

é usada para identificar de maneira universal os objetos, independentemente das hierarquias de heranças e nomeação.

5. MIB DA INTERNET

A MIB II usa uma arquitetura de árvore, definida na ISO ASN.1, para organizar todas as suas informações. Cada parte da informação da árvore é um **nó rotulado** que contém:

- um identificador de objetos (OID): seqüência de números separados por pontos.
- uma pequena descrição textual: descrição o nó rotulado

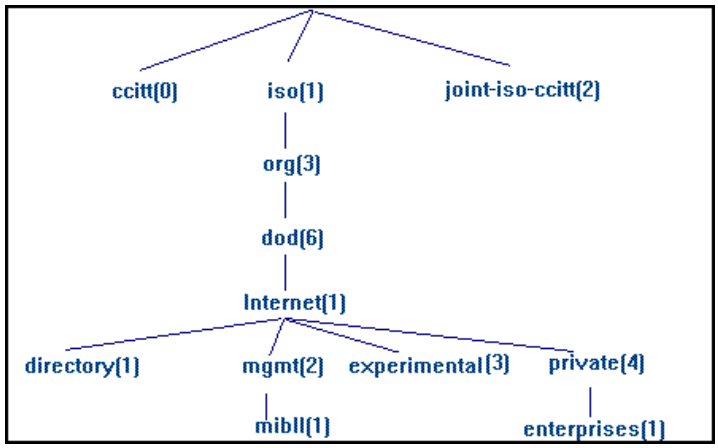
Exemplo:

directory(1)

identificador de objetos: 1.3.6.1.1

descrição textual: {internet 1}

Um **nó rotulado** pode ter árvores contendo outros **nós rotulados**. Caso não tenha árvores, ou nós folhas, ele conterá um valor e será um **objeto**.



O nó raiz da árvore MIB não tem nome ou número, mas tem três árvores:

1. **ccitt(0)**, administrada pelo CCITT
2. **iso(1)**, administrada pela ISO
3. **joint-iso-ccitt(2)**, administrada pela ISO juntamente com o CCITT.

Sob o nó iso(1), estão outras árvores, como é o caso da árvore **org(3),** definida pela ISO para conter outras organizações. Uma das organizações que está sob a árvore **org(3)** é o Departamento de Defesa dos EUA (DOD), no nó **dod(6).** A Internet(1) está sob o **dod(6),** e possui quatro subárvores:

- **directory(1)**: contém informações sobre o serviço de diretórios OSI (X.500)
- **mgmt(2)**: contém informações de gerenciamento, é sob esta subárvore que está o nó da mibII, com o identificador de objeto 1.3.6.1.2.1 ou { mgmt 1 }.
- **experimental(3)**: contém os objetos que ainda estão sendo pesquisados pela IAB.
- **private(4)**: contém objetos definidos por outras organizações.

Abaixo da subárvore mibII estão os objetos usados para obter informações específicas dos dispositivos da rede. Esses objetos são divididos em 11 grupos, que são apresentados na tabela abaixo.

Grupo	Informação
system (1)	informações básicas do sistema
interfaces (2)	interfaces de rede
at (3)	tradução de endereços
ip (4)	protocolo ip
icmp (5)	protocolo icmp
tcp (6)	protocolo tcp
udp (7)	protocolo udp
egp (8)	protocolo egp
transmission (10)	meios de transmissão
snmp (11)	protocolo snmp

Exemplos

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 re-inicialização 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 erro.

- ipInHdrErrors (1.3.6.1.2.1.4.4): Número de datagramas que foram recebidos e descartados devido a 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.

6. COMPARAÇÃO ENTRE A MIB DA OSI E A MIB DA INTERNET

A diferença entre estas duas MIB's reside nas hierarquias usadas para representar os objetos. Na MIB da ISO são definidas três hierarquias: hierarquia de herança, hierarquia de nomeação e hierarquia de registro.

A hierarquia de herança ou de classes está relacionada às propriedades associadas a um determinado objeto. .Dentro desta hierarquia diz-se que objetos da mesma classe possuem propriedades similares.

No caso da Internet não são usados os conceitos de classes de objetos e seus respectivos atributos. São definidos tipos de objetos. A definição de tipo de objetos contém cinco campos: nome textual com o respectivo identificador de objeto (OBJECT IDENTIFIER), uma sintaxe ASN.1, uma descrição do objeto, o tipo de acesso e o status.

A hierarquia de nomeação ou de *containment* é usada para identificar instâncias de objetos. Este tipo de hierarquia não é definido no caso da Internet. Finalmente tem-se a hierarquia de registro que é especificada em ambos padrões.

7. CONCLUSÃO

Tanto o SNMP como o CMIP suportam a mesma idéia de troca de mensagens entre gerente e agente e armazenamento das informações na MIB.

O SNMP devido a sua simplicidade e mais fácil de ser implementado. Em compensação, possui limitações de desempenho que o CMIP não possui. Principalmente na área de segurança. Portanto o SNMP se adequa mais a sistemas de pequeno porte, onde se pode exigir menos de um sistema de gerenciamento.

O CMIP, devido a ser bem completo e bem projetado, e mais útil em sistemas de comunicação de grande porte, onde existem grandes quantidades de recursos a serem gerenciados. Em contraposição, em sistemas de pequeno porte, ele não se torna adequado devido a sua complexidade.

REFERÊNCIAS

http://penta.ufrgs.br/gere96/cmipXsnmp/cmip_stra.htm

http://penta2.ufrgs.br/gere96/cmipXsnmp/snmpcmipf.htm

http://www.gta.ufrj.br/grad/cmip.html

http://www.rnp.br/newsgen/9805/metricas.html

http://penta.ufrgs.br/gr952/trab1/z_cmip.html

ESTUDO SOBRE RMON

1. RESUMO

Redes cliente/servidor estão, RMON – Remote Network Monitoring é um protocolo derivado do protocolo SNMP, foi criado pelos mesmos criadores do TCP/IP e do próprio SNMP.
Tecnologias como RMON pode dar ao administrador uma possibilidade maior de trabalhar proativamente quanto aos problemas da rede ao invés da reativa(atual) onde o problema ocorre para após isso corrigi-lo. Isto se torna possível devido ao suporte de estatísticas e dados em tempo-real. RMON2 (RMON versão2) permite um monitoramento até o nível de aplicação (RMON versão 1 permitia monitoramente somente até a camada MAC) possibilitando coletar informações como a banda usada por uma determinada aplicação. Possui, além dessa, muitas outras vantagens.
O padrão RMON foi desenvolvido no intuito de resolver questões que outros protocolos de gerenciamento não eram capazes. Com base nestas questões, a RFC 1757 define objetivos gerenciais que o padrão RMON deve observar, abaixo listado.

2. INTRODUÇÃO

O RMON é um padrão IETF. Portanto, não é uma solução proprietária. Na realidade, um só fabricante dificilmente irá implementar a solução RMON completa. No cenário do gerenciamento RMON, os equipamentos de rede carregam MIBs RMON, a rede transporta os dados, um sistema de gerenciamento aceita alarmes e notifica usuários, e uma ferramenta de análise RMON interage com os grupos RMON e seus dados

3. RMON

Os dispositivos de gerenciamento remoto de redes, normalmente chamados de monitores ou sondas (*probes*), são instrumentos cuja existência é dirigida exclusivamente ao gerenciamento de redes. Geralmente, são independentes (*standalone*) e direcionam boa parte de seus recursos internos ao gerenciamento da rede a qual estão conectados.
Uma organização pode empregar vários destes dispositivos para o gerenciamento de sua rede- um por segmento. Adicionalmente, os monitores podem ser utilizados para que um provedor

de serviços de gerenciamento de rede possa acessar uma rede cliente, normalmente separada geograficamente.

Os objetos definidos na RFC 1757 são objetos de interface entre agentes RMON e aplicações de gerenciamento RMON. Ainda que a maioria desses objetos sirva a qualquer tipo de gerenciamento de redes, alguns são específicos às redes Ethernet. A estrutura desta MIB permite que outros objetos sejam desenvolvidos para outros tipos de redes. Há uma expectativa de que futuras versões da RFC 1757 ou outros documentos definam extensões para outros tipos de redes, como FDDI ou Token Ring.

3.1 Operação *Off-line*

Existem situações em que uma estação de gerenciamento não estará em contato contínuo com seus dispositivos de gerenciamento remoto. Esta situação pode ocorrer como conseqüencia de projeto, a fim de que se reduzam os custos de comunicação, ou por falha da rede, quando a comunicação entre a estação de gerenciamento e o monitor fica comprometida em sua qualidade.

Por esta razão, a MIB RMON permite que um monitor seja configurado para realizar suas atividades de diagnóstico e coleta de dados estatísticos continuamente, mesmo quando a comunicação com a estação de gerenciamento seja impossível ou ineficiente. O monitor poderá então comunicar-se como a estação de gerenciamento quando uma condição excepcional ocorrer.

Assim, mesmo em circunstâncias em que a comunicação entre monitor e estação de gerenciamento não é contínua, as informações de falha, desempenho e configuração podem ser acumuladas de forma continua, e transmitidas à estação de gerenciamento conveniente e eficientemente quando necessário.

3.2 Monitoramento Proativo

Dados os recursos disponíveis no monitor, é normalmente desejável e potencialmente útil que ele execute rotinas de diagnóstico de forma contínua e que acumule os dados de desempenho da rede. O monitor estará sempre disponível no início de uma falha; assim, ele poderá notificar a estação de gerenciamento da falha, assim como armazenar informações estatísticas a seu respeito. Esta informação estatística poderá ser analizada pela estação de gerenciamento numa tentativa de diagnosticar as causas do problema.

3.3 Detecção e Notificação de Problemas

O monitor pode ser configurado para reconhecer condições, que, normalmente, são de erro e verificar pelas mesmas continuamente. No advento de uma destas condições, o evento pode ser registrado e as estações de gerenciamento notificadas de várias formas.

3.4 Valor Agregado aos Dados

Considerando o fato de que os dispositivos de gerenciamento remoto representam recursos dedicados exclusivamente a funções de gerenciamento, e considerando também que os mesmos localizam-se diretamente nas porções monitoradas da rede, pode-se dizer que estes dispositivos permitem a agregação de valor aos dados coletados. Por exemplo, indicando quais os *hosts* que geram a maior quantidade de tráfego ou erros, um dispositivo pode oferecer (à estação de gerenciamento) informações preciosas para a resolução de toda uma classe de problemas.

3.5 Gerenciamento Múltiplo

Uma organização pode ter mais de uma estação de gerenciamento para as várias unidades da empresa, para funções distintas, ou como tentativa de proporcionar recuperação em caso de falha (*crash recovery*). Como tais ambientes são comuns na prática, um dispositivo de gerenciamento de rede remoto deverá ser capaz de lidar com múltiplas estações de gerenciamento concorrendo para a utilização de seus recursos.

4. CONCLUSÃO

O RMON (Remote Monitoring Network) é um protocolo que tem muito a prometer, ele é baseado na definição de limites de tolerância para a rede, é praticamente o snmp porém muito melhorado, com novas características e funções, o snmp só ia até o MAC Address da máquina, já o RMON continua e vai até a camada de aplicação do MIB, é muito importante pois possui mecanismos muito interessante para administrar a rede com uma melhor eficiência, possui atividades de diagnóstico e estatística quando uma estação estiver offline ou incomunicável enviando a informação a máquina gerenciadora que esta pode identificar as

causas do problema ocorrido e proporcionar recuperação em casos de falha, chamados de crash recovery.

REFERÊNCIAS

http://penta.ufrgs.br/gere96/rmon2/rmon2.html
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rmon.htm
http://www.rnp.br/newsgen/9901/r.html
http://penta.ufrgs.br/gr952/trab1/rmon.html
http://www.rnp.br/newsgen/9901/rmon.html
http://www.rnp.br/newsgen/9712/gerencia.html
http://www.apostilando.com.br

ESTUDO SOBRE FERRAMENTAS DE MONITORAMENTO DE REDES

1. TIVOLI

1.1 Conceitos Básicos do Tivoli

O gerenciamento de uma rede através do Tivoli esta baseado no conceito de regiões de policiamento (Policy Region ou TMR – Tivoli Management Region). Uma região de policiamento abrange um conjunto de recursos gerenciados, como contas de usuários, estações de trabalho, roteadores. Em uma rede podem ser definidas mais de uma região de policiamento. Cada região possuindo suas próprias políticas de controle de acesso e gerenciamento.

Em uma região de policiamento existem os seguintes elementos que auxiliam no gerenciamento dos recursos [framework/98]: TMR Server – É responsável pela gerência de determinada região de policiamento. No TMR Server são definidas e controladas as políticas utilizadas e os recursos gerenciados. O TMR Server mantém uma base de dados e coordenadas de comunicação com os Managed Nodes, desempenhando a verificação e autenticação necessária para a segurança dos dados.

Managed Node – Um Managed Node, em princípio, pode atuar como Endpoint. Mas com a instalação de outras funções, como Endpoint Gateway, pode atuar como intermediário na execução de determinadas tarefas de gerenciamento a pedido do TMR Server.

Endpoint Gateway - controla as comunicações e operações com os Endpoints. Basicamente, um Endpoint Gateway envia os métodos necessários (instruções de como realizar determinadas operações) para os Endpoints realizarem funções de gerenciamento requisitadas.

Endpoint – É o agente encarregado de executar as operações de gerenciamento nos recursos finais. O código inicial do Endpoint é pequeno, mas pode crescer assim que novos métodos são carregados.

1.1 Módulos do Tivoli

O Tivoli Management Environment (TME10) é um ambiente de gerenciamento de sistemas distribuídos. Os principais módulos são brevemente descritos a seguir, de acordo com [Hawes/98].

Framework – é o componente base do TME, produz capacidades de administração de sistemas básicos, bem como serviços fundamentais para aplicações de gerenciamento. Estas capacidades e serviços incluem facilidades na administração do Tivoli, facilidades no policiamento de sistemas e facilidades nas notificações.

User Administration – Permite o gerenciamento de grupos e contas de usuários nos sistemas operacionais Windows, NetWare, e UNIX(AIX, HP-UX, Solaris e SunOS) em uma arquitetura distribuída.

Distributed Monitoring – Verifica o status de uma variedade de recursos da rede, tais como, sistemas, aplicações e processos. Esta aplicação é usada para monitorar de recursos locais ou remotos e apresentar eventos e alarmes da rede. Seus Componentes são: TME 10 DM profiles; TME 10 DM engine e Indicator collections.

Inventory - O Inventário procura e mantém informações sobre o inventário em um ambiente distribuído de modo rápido e fácil. Suas principais funções são: Manter e atualizar regularmente softwares e hardwares; Monitorar e registrar mudanças nas configurações de 3 hardware e software; Gerenciar todos os sistemas da empresa a partir de um ponto central; Disponibilizar informações de inventário para realizar funções de auditoria de sistemas.

Software Distribution – A Distribuição de Software permite a distribuição e instalação de softwares em máquinas de uma rede heterogênea de forma eficiente.

Enterprise Console - A Console é uma aplicação de gerenciamento de eventos baseada em regras. Seus componentes são: Central Event Server, Distributed Event Console; Central Event RDBMS (RIM); Distributed Event Adapters.

1.2 Principais Produtos

- ✓ **IBM Tivoli Storage Area Network Manager**
  Descobre, monitora e gerencia componentes de estrutura da SAN
- ✓ **IBM Tivoli Storage Manager**
  Automatiza as funções de backup e de restauração, suporta uma ampla faixa de plataformas e dispositivos de armazenamento e centraliza operações de gerenciamento de armazenamento.
- ✓ **IBM Tivoli Storage Manager para Application Servers**
  Protege ambientes do WebSphere banco de dados de administração, dados de configuração e aplicativos implementados sem afetar a disponibilidade do aplicativo
- ✓ **IBM Tivoli Storage Manager para Databases**
  Protege dados do Informix, Oracle e Microsoft® SQL, independentemente de onde estejam e de como estão armazenados.
- ✓ **IBM Tivoli Storage Manager para Enterprise Resource Planning**
  Protege dados vitais do sistema SAP R/3 de formas mais eficiente, consistente e confiável.
- ✓ **IBM Tivoli Storage Manager para Hardware**
  Elimina virtualmente o impacto no desempenho relacionado a backup em bancos de dados de missão crítica que requerem disponibilidade por 24 horas e 7 dias por semana.
- ✓ **IBM Tivoli Storage Manager para Mail**
  Protege dados do Lotus Domino e do Microsoft® Exchange, independentemente de onde estejam ou de como estão armazenados.
- ✓ **IBM Tivoli Storage Manager para Space Management**
  Move automaticamente dados inativos para liberar espaço em disco on-line para dados ativos importantes.
- ✓ **IBM Tivoli Storage Manager para Backup e Recuperação do Sistema**
  Oferece uma ferramenta abrangente de backup, restauração e reinstalação do sistema que fornece recursos de restauração básicos.
- ✓ **IBM Tivoli Storage Resource Manager**
  Monitora e faz relatórios sobre recursos de armazenamento heterogêneos em toda a empresa para aumentar a utilização do armazenamento, identificar e resolver possíveis

problemas e assegurar disponibilidade do aplicativo através da automatização baseada em critérios.

- ✓ **IBM Tivoli Storage Resource Manager para Databases**

  Permite a você descobrir problemas em aplicativos críticos de bancos de dados, apontando rapidamente o problema principal, seja ele um usuário individual ou um espaço de tabelas de aplicativo específico.

- ✓ **Tivoli SANergy**

  Unifica o compartilhamento de administração fácil e heterogênea, para várias plataformas do Network Attached Storage com a grande largura de banda, escalabilidade e eficiência de CPU do Storage Area Networks

REFERÊNCIAS

http://www.magnasistemas.com.br/magnasistemas/sbs1_3p.nsf/pages/tectivoli?OpenDocument&Click=
http://www.rnp.br/wrnp2/2000/posters/tivoli.pdf

2. SUÍTE TRAUMA ZER0

2.1 Diferenciais

A Suíte Trauma Zer0 consolida-se no mercado como a melhor solução em custo-benefício para gerenciamento de redes. Além de sua alta tecnologia para o Gerenciamento do Ciclo de vida de TI, proporcionando significativo retorno e redução dos investimentos nas empresas, seus principais diferenciais são:

Descobrimento de Software	Um módulo único de reconhecimento de software identifica positivamente mais aplicações, reduzindo drasticamente o custo e o tempo de gerenciamento de softwares na rede.
Descobrimento de tipos de arquivos	Identificação de arquivos não autorizados e potencialmente perigosos na rede (mp3, mpg, jpg, etc), para ajudar a cumprir as políticas, segurança e planejamento da rede.
Rastreamento de Localização Física	Monitorar a localização de cada recurso de hardware na organização e alertar o Administrador automaticamente de movimentação, inclusões e remoções.
Suporte a multiplataforma	Opções de implementação para cobrir todos os ambientes e sistemas operacionais: Windows 3.11, 95, 98, Me, NT, XP, 2000, 2003, CE, Novell Linux Desktop, Redhat 8.0 ou superior, Fedora Core 1 e 2, Mandrake 8.0 ou superior, Slackware 8.0 ou superior, Suse 9.0 ou superior, Debian 3.0 ou superior, Conectiva 7.0 ou superior,, Freedows. MuLinux, OS2-Warp, MS-DOS, Caldeira DR-Dos, Novell Dos, IBM PC-Dos e FreeDos.
Amigável à rede	Comunicação baseada em IP para máxima performance e com portas configuráveis, controla nativamente de 10 a 20 % o tráfego de rede (Tráfego estimado de até 60 Kb)
Categorização de Utilização de Software	Categorizar a utilização individual das aplicações de software fornece informação de gerenciamento e controle de custo de alto valor.
Gerenciamento de Mudanças	Rastreia e registra automaticamente tanto mudanças de localização como de configuração para dispositivos com Alertas de Mudanças selecionáveis, criando um rastro completo e preciso.
Auditoria Remota	Audita a máquina de usuários remotos através de qualquer conexão IP (conexão remota à rede, VPN, internet discada, etc.)
Tz0 Agent	Tamanho do arquivo de instalação de 500 Kb, hardware mínimo 486 DX33, 8 Mb de memória Ram e 1Mb livre em disco, não requer outro requisito (como DCOM) para os Sistemas Windows 9X.
Comunicação Segura	Implantação dos agentes nos clientes de modo seguro, comunicação encriptada entre os agentes e centro de controle com tecnologia 3DES de 192bits nativo. Conexão única com autenticação Unique ID.
Acesso Console Seguro	Oferece acesso para múltiplos usuários autorizados (local e remoto) com senhas de acesso seguras.
Integração fácil	Banco de dados aberto compatível com ODBC permite fácil exportação dos dados de auditoria para outras soluções complementares. Permite a instalação em bancos como MS-SQL, Oracle, My SQL, DB2-IBM, Postgre e Interbase.
Distribuição de Softwares	A criação e distribuição de aplicativos ou de processos (macros) são simples e fáceis de aplicar, podendo configurar a utilização da rede para a distribuição.
Bloqueio de Aplicações	A criação de bloqueios de aplicações é pelo nome da janela que essa aplicação apresenta. É possível simplesmente parar a aplicação ou desinstalar a mesma.
Bloqueio de URL	A criação de bloqueios de URL facilita o uso da internet; esta configuração aplica-se aos agentes, permanecendo ativo mesmo com o servidor desligado. Independe do tipo e versão do browser do computador cliente.
Regras de Segurança para os computadores	Você pode criar diversas políticas para limitar o usuário na utilização do uso das funcionalidades do computador, tais como mudanças no papel de parede. Aplicável para Windows 95, 98, Me, NT, XP, 2000 e 2003.
Violação do Sistema	Criação de regras de notificação para quando o sistema de um computador com agente for alterado, tanto na parte de Hardware quanto de Software
Utilização do Computador	Acesso a relatórios que mostram o nível de acesso aos computadores, tais como horários de logins e logouts.

Utilização de Aplicação	Acesso a relatórios que mostram o nível de utilização dos aplicativos em rede ou local nos computadores
Gerenciamento de Licenças	Você pode associar valores e prazos para cada produto encontrado na rede. Ainda sem notificação para o vencimento das licenças, porém, existe a previsão de que até o fim do 4º trimestre deste ano esta funcionalidade estará operacional.
Utilização de URLs	Você pode ter acesso a relatórios que mostram as URLs mais acessadas na sua rede ou local nos computadores
Controle Remoto	O controle remoto é muito simples, bastando apenas selecionar o computador e conectar. Com esta funcionalidade você pode ter acesso a transferências de arquivos com o computador alvo, interagir com o vídeo, parar ou iniciar serviços, iniciar uma sessão de Chat por texto.
Help Desk Console	Com esta console você pode criar e administrar novos chamados, associar os computadores com o inventário, criar notificações para chamados SLA, associar com o controle remoto de maneira muito simples.
Help Desk Web	Com esta sessão de web você pode criar e acompanhar os chamados, não tendo o direito de administrar os mesmos.
Rápido Retorno	O Trauma Zer0 é reconhecido por seu baixo custo, por ser em português e com fábrica localizada no Brasil; seu agente é extramente leve e não causa paradas críticas nos computadores clientes; para todos os módulos disponíveis pela iVirtua é utilizado o mesmo agente cliente nos computadores, facilitando a distribuição e o uso imediato das soluções.

2.2 O que é o Tz0?

O Trauma Zer0 é um software que revolucionou os conceitos de administração de ambientes de TI. Desenvolvido no Brasil com modernas tecnologias que possibilitam o controle centralizado da utilização de recursos de TI, aumentam a performance e disponibilidade de recursos de softwares e hardwares, proporcionam uma visão completa de segurança, níveis de satisfação e garantem o retorno de investimento para sua empresa. Desenhado para prover informações diretas e precisas, auxilia a tomada de decisões e o correto dimensionamento da utilização dos recursos tecnológicos e humanos da sua empresa.

Com o Trauma Zer0 você consegue obter de maneira simples e rápida:

Controle de Produtividade - Tz0 Productivity
Inventário de Hardware e Software - Tz0 Asset Inventory
Controle Remoto - Tz0 Remote Control
Distribuição de Software - Tz0 Software Delivery and Deploy
Controle e Aplicação de Diretrizes de Segurança - Tz0 Network Security
Monitor de Performance - Tz0 Performance Monitor
Análise e Reconstrução de Pacotes - Tz0 Sniffer Rescue
Compactação de Anexos de E-Mail - Tz0 Email Warp
Controle da informação (HelpDesk/ServiceDesk/Workflow) - Tz0 Support Cycle

2.3 Por que inventário é importante para o meu negócio?

Quanto mais controle você tiver dos seus bens, mais controle você terá dos custos associados a harware, software, help desk, suporte e gerenciamento de desktop. Quanto mais informações sua equipe de TI tiver sobre cada sistema, mais eficientes eles serão – as ligações ao suporte diminuirão e serão mais breves, up grades de software e hardware serão mais rápidos e fáceis, o controle sobre licenças será preciso, sobrando assim mais tempo para sua equipe buscar novos projetos que contribuam para o crescimento da sua empresa.

2.4 Como funciona o Tz0?

O Tz0 Server é instalado em Windows NT, 2000 Server ou 2003 Server.
O Tz0 Agent pode ser instalado via login script, intranet ou diretamente nas estações (Windows 95/98/Me/NT/2000/XP).
Uma vez que o Tz0 Agent esteja instalado nas estações, o Tz0 Manager será usado para centralizar e gerenciar todas as informações e resultados coletados.

2.5 O que faz do Tz0 único?

O Tz0 incorpora várias tecnologias únicas. Tecnologias essas que foram desenvolvidas e patenteadas pela iVirtua. Permite acompanhar e armazenar tudo o que acontece em todos os computadores da sua rede em tempo real sem que afete a performance da mesma. Determinar onde se encontra fisicamente uma máquina, obter um inventário detalhado do seu patrimônio de hadware e software. O Tz0 rastreia todas instalações, movimentos, ou qualquer tipo de alteração nas suas estações e mantém um completo histórico. Essas informações auxiliam o help desk na solução de problemas.

Outro fator que faz do Tz0 único é a velocidade e facilidade de implementação em qualquer tipo e tamanho de rede, e o conceito "plug and get it" desenvolvido pela iVirtua, em dois dias se instala o produto em centenas de máquinas e automaticamente se obtem um inventário detalhado de hardware, software e licenças. Além de permitir todas as funcionalidades em máquinas que não estejam na rede corporativa da empresa.

2.6 Quais as plataformas que o Tz0 suporta?

O Tz0 service suporta hoje os seguintes sistemas operacionais:

Windows 95,98 & Millennium Edition.
Windows NT 3.5,4.0, 2000, XP, .NET & 2003
Windows 3.1, 3.11, DOS
OS2
Linux

2.7 Quais os ambientes de rede que o Tz0 suporta?

O Trauma Zer0 funciona nos seguintes ambientes de rede:
Microsoft Active Directory, LanManager, NT/2000/2003/.NET ou XP.
Novell Netware 3.11 ou superior, Intranetware, Unixware

2.8 Quais os Bancos de Dados que o Trauma Zer0 suporta?

O Trauma Zer0 suporta de forma nativa, os principais Bancos de Dados do mercado:
Oracle, Microsoft SQL Server, Sybase, DB2, Postgre, My SQL, Firebird e Interbase.

2.9 Quais os requerimentos do sistema necessários para o funcionamento do Trauma Zer0?

Os requerimentos mínimos para o Trauma Zer0 Server são:
Microsoft Windows 2000 Professional, Server ou Advanced Server

Numero de PCs	Memória	Disco Rígido	Processador
Até 250	256Mbytes	1GB	Pentium III 500Mhz
250- 500	512Mbytes	1GB	Pentium III 800Mhz
500- 2000	1024Mbytes	1GB	Pentium III 800Mhz
2000-5000	2048MBytes	2GB	2 x Pentium IV 1Ghz
5000-10000	2048Mbytes	2GB	3 x Pentium IV 1Ghz
10000-20000	4096Mbytes	2GB	4 x Pentium IV 1Ghz

2.10 Como é licenciado o Trauma Zer0?

A licença é necessária para cada computador que tiver o Tz0 Agent instalado. Não é necessário licenças para nenhum outro tipo de equipamentos da sua rede.

2.11 Como é oferecido Suporte Técnico?

Depende da necessidade do cliente, temos disponíveis opções de contratos 8x5 e 24x7, com diversos níveis de SLA. O suporte pode ser feito por telefone, email, site, ou podemos disponibilizar um técnico para ficar dentro do cliente por tempo indeterminado.

2.12 Qual o impacto que o Trauma Zer0 terá no tráfego da rede?

O Trauma Zer0 não causa impacto no tráfego da sua rede, toda informação trafega compactada e criptografada com 3DES. Nossos cases vão de 100 a 10.000 computadores interligados a um único servidor

2.13 Gerenciamento de Ciclo de Vida de TI

A **iVirtua Solutions** desenvolve a Suite de aplicativos **Trauma Zer0** buscando suprir a crescente demanda das empresas pela harmonização da tecnologia aos seus objetivos de negócio. O Trauma Zer0 proporciona um Gerenciamento do Ciclo de Vida de TI de forma prática e centralizada, cobrindo todos os aspectos de seus três pilares: **Infra-Estrutura de TI, Segurança da Rede e Serviços e Informações.**

REFERÊNCIAS

http://www.ivirtua.com.br/index.php?conteudo=solutions&pg=dif
http://www.ivirtua.com.br/index.php?conteudo=solutions&pg=faq

3. NAGIOSTM

3.1 Introdução

O Nagios™ é um aplicativo de monitoramento de sistemas e de redes. Ele checa clientes e serviços, especificados, alertando quando as coisas estão indo mal ou se restabelecendo.
O Nagios™ foi originalmente desenhado para rodar no Linux, apesar dele poder funcionar na maioria dos unices. Para mais informações sobre qual sistema operacional o Nagios irá, ou não, funcionar, veja a página de portabilidade em sistemas operacionais, acessível em http://www.nagios.org/ports.shtml.
Algumas das várias ferramentas do Nagios ™ incluem:

- Monitoramento de rede e serviços (SMTP, POP3, HTTP, NNTP, PING, etc.)
- Monitoramento dos recursos de clientes (carga de processador, uso de disco, etc.)
- Organização simples de plugins que permite aos usuários facilmente desenvolverem seus próprios serviços de checagem
- Checagem paralela de serviços
- Habilidade para definir hierarquia de redes de clientes usando clientes pais (parent hosts), permitindo a detecção e distinção entre clientes que estão desativados e aqueles que estão inalcançáveis
- Notificação de contatos quando problemas em serviços e clientes ocorrerem ou forem resolvidos (via email, pager, ou métodos definidos pelo usuário)
- Habilidade para definir tratadores de eventos (event handlers) que serão executados durante eventos de serviços ou clientes na tentativa de resolução de problemas.
- Rotatividade automática de arquivos de logs
- Suporte para implementação de clientes de monitoramento redundantes
- Interface web opcional para visualização do status atual da rede, histórico de notificações e problemas, arquivos de log, etc.

3.2 Configuração mínima

A única exigência para rodar o Nagios é ter um computador rodando Linux (ou variantes do UNIX) e um compilador C. Você provavelmente necessitará ter o TCP/IP configurado já que a maioria das checagens de serviços serão feitas através da rede.

Você *não é* obrigado a usar os CGIs incluídos com o Nagios. No entanto, se você optar por usá-los, você precisará dos seguintes programas instalados...

1. Um servidor WEB (de preferência Apache)
2. gd library de Thomas Boutell versão 1.6.3 ou superior (exigido pelos CGIs statusmap e trends)

3.3 Licença

Nagios™ é distribuído sob os termos da GNU General Public License Versão 2 como foi publicado pela Free Software Foundation. Isto lhe garante permissão de copiar, distribuir e modificar o Nagios sob certas condições. Leia o arquivo 'LICENSE' que veio na distribuição do Nagios ou leia a versão online da licença para maiores detalhes.
Nagios™ é fornecido SEM QUALQUER GARANTIA DE QUALQUER TIPO, INCLUINDO A GARANTIA DE DESENHO, MECANTIBILIDADE E ADEQUAÇÃO PARA UM PROPÓSITO PARTICULAR.

3.4 Visão da configuração

Existem muitos arquivos de configurações que você precisará criar ou editar antes de iniciar o monitoramento de qualquer coisa. Eles serão descritos abaixo...

3.4.1 Arquivo de configuração principal

O arquivo de configuração principal (comumente */usr/local/nagios/etc/nagios.cfg*) contem várias diretivas que afetam como o Nagios opera. Este arquivo de configuração é lido pelo processo do Nagios e pelos CGIs. Este será o primeiro arquivo de configuração que você vai querer criar ou editar.
Um exemplo de arquivo de configuração é gerado automaticamente quando você executa o script **configure** antes de compilar os binários. Procure por ele no diretório da distribuição ou no subdiretório etc/ de sua instalação. Quando você instala os exemplos de arquivos de configuração usando o comando **make install-config**, um exemplo de arquivo de configuração principal será colocado no seu diretório de configuração (geralmente /usr/local/nagios/etc). O nome padrão para o arquivo de configuração principal é **nagios.cfg**.

3.4.2 Arquivo(s) de recurso(s)

Arquivos de recurso são usados para armazenar macros definidas por usuários. Arquivos de recursos podem também conter outras informações (como configurações de conexão a banco de dados), apesar disto depender de como você compilou o Nagios. O ponto principal de ter arquivos de recurso é usá-los para armazenar informações de configuração sensitivas e não para torná-las disponíveis aos CGIs.
Você pode especificar um ou mais arquivos de recursos opcionais usando a diretiva resource_file no arquivo de configuração principal.

3.4.3 Arquivos de configuração de objetos

Arquivos de configuração de objetos (historicametne chamados de arquivos de configuração de "clientes") são usados para definir clientes, serviços, grupos de clientes, contatos grupos de contatos, comandos, etc. Aqui é onde você define as coisas que você quer monitorar.

3.4.4 Arquivo de configuração de CGI

O arquivo de configuração de CGI (geralmente */usr/local/nagios/etc/cgi.cfg*) contém numerosas diretivas que afetam a operação dos CGIs.
Um exemplo de arquivo de configuração de CGI é gerado automaticamente quando você executa o script **configure** antes de compilar os binários. Quando você instala os exemplos de arquivos de configuração usando o comando **make install-config**, um arquivo de configuração de CGI será colocado no mesmo diretório que o arquivo de configuração de clientes e o arquivo de configuração principal (geralmente /usr/local/nagios/etc). O nome padrão para o arquivo de configuração de CGI é **cgi.cfg**.

3.4.5 Arquivos de configuração de informações estendidas

Arquivos de configuração de informações estendidas são usados para definir informações adicionais para serviços e clientes que devem ser usados pelo CGI. Aqui é onde você definir coisas como coordenadas de desenho, belos ícones, etc.

3.5 Segurança

A intenção deste texto é fornecer uma rápida visão sobre alguns aspectos que você deve ter em mente quando instalar o Nagios de forma a não configurá-lo de forma insegura. Este documento é novo, portanto se alguém tiver alguma sugestão ou comentário sobre segurança com Nagios, me mande uma mensagem em nagios@nagios.org

3.5.1 Não execute o Nagios como Root!

Nagios não precisa rodar como root, logo não faça isso. Mesmo se você iniciar o Nagios no boot com um script, você pode forçá-lo a largar seus previlegios após a inicialização e rodar como outro usuário/grupo usando as diretivas nagios_user e nagios_group no arquivo de configuração principal.
Se você precisar executar event handlers ou plugins que requerem acesso de root, você poderá tentar usar o comando sudo.

3.5.2 Habilite comandos externos somente quando necessário

Por padrão, comandos externos são desabilitados. Isto é feito para previnir que um administrador ao configurar o Nagios deixe desprevinidamente a interface de comandos aberta para "outros usuários" ... Se você planeja usar event handlers ou executar comandos através da interface web, você deverá habilitar comandos externos. Se você não planeja usar event handlers ou executar comandos via web, eu recomendo manter comandos externos desabilitados.

3.5.3 Configurando permissões apropriadas no Arquivo de Comandos Externos

Se você habilitar comandos externos, certifique-se de configurar as permissões apropriadas no diretório */usr/local/nagios/var/rw*. Você somente precisa que o usuário Nagios (geralmente *nagios*) e o usuário do servidor web (usually *nobody*) tenham permissão para escrever no arquivo de comando. Se você instalou o Nagios em uma máquina dedicada a monitorar e administrar tarefas e que não é usada para contas publicas, isto seria suficiente.
Se você instalar em uma máquina pública ou multi-usuário, permitir que o usuário do servidor web escreva no arquivo de comando poderá ser um problema de segurança. Apesar de tudo,

você não quer que qualquer usuáio de seu sistema controle o Nagios via arquivo de comando externo. Neste caso, eu sugeriria apenas garantir acesso de escrita ao arquivo de comando para o usuário *nagios* e usar algo como CGIWrap para executar os CGIs como usuário *nagios* ao invés de *nobody*.

3.5.4 Requerer Autenticação nos CGIs

Eu sugiro fortemente a requisição de autenticação para acessar CGIs. Após fazer isto, leia a documentação sobre as permissões padrões que contatos autenticados terão e somente autorize contatos específicos para permissões adicionais se isto for necessário. Instruções de como configurar autenticação e autorização de permissões podem ser encontradas aqui. Se você desabilitar aos opções de autenticação de CGI usando a diretiva use_authentication no arquivo de configuração de CGI, o comando CGI recusará escrever qualquer comando no arquivo de comando externo.

Use caminho completo na definição de comandos

Quando você definir comandos, certifique-se de especificar o *caminho completo* para qualquer script ou binário que você for executar.

Esconda informações sensíveis com a macro $USERn$

Os CGIs lêm o arquivo de configuração principal e o(s) arquivo(s) de configuração de objeto, logo você não vai querer guardar qualquer informação sensível (nomes, senhas, etc) lá. Se você precisar especificar nomes e/ou senhas em uma definição de comando use a macro $USERn$ para ocultá-los. Macros $USERn$ são definidas em um ou mais arquivos de recurso (resource files). Os CGIs não tentarão ler o conteúdo dos arquivos de recursos, logo você poderá colocar permissões mais restritivas (600 ou 660) neles. Veja o arquivo *resource.cfg* de exemplo na distribuição base do Nagios para ter um noção de como definir macros $USERn$.

Remova caracteres perigosos das Macros

Use a diretiva illegal_macro_output_chars para remover caracteres perigosos das macros $OUTPUT$ e $PERFDATA$ antes de elas serem usadas em notificações, etc. Caracter perigoso é qualquer coisa que pode ser interpretado pelo shell, portanto abrindo um brecha na segurança. Um exemplo disto e a presença de crase (`) nas macros $OUTPUT$ e/ou $PERFDATA$, que pode permitir que um atacante execute um comando arbitrário como o usuário nagios (uma boa razão para não executar o Nagios como usuário root).

CONCLUSÃO

O *Nagios* é uma das ferramentas mais poderosas para gerenciar uma rede de computadores. Com ele você consegue tirar relatórios de acesso, status das máquinas, problemas que podem estar ocorrendo na sua máquina antes que eles afetem gravemente o sistema.

REFERÊNCIAS

http://www2.dcc.ufmg.br/~leoh/nagios/docs/toc.html

4. MRTG

4.1 História da criação do MRTG

Em 1994 eu, Tobias Oetiker, estava trabalhando para um site onde nós tínhamos um link de 64kbit para o mundo externo. Obviamente todos estavam interessados em saber como estava a utilização do link. Então eu escrevi um rápido programa que constantemente atualizava um gráfico na web, mostrando a utilização do nosso link de Internet. Isso finalmente tornou-se um script configurável em Perl chamado MRTG-1.0 que foi lançado na primavera de 1995.
Depois de poucas atualizações eu deixei meu trabalho na DMU, para começar a trabalhar no (SFIT) Swiss Federal Institute of Technology. Devido à falta de tempo eu tive que deixar o MRTG de lado.
Certo dia em Janeiro de 1996, eu recebi um e-mail de Dave Rand perguntando se eu tinha idéia do porquê o MRTG era tão lerdo. Atualmente eu sei. A programação do MRTG não era muito eficiente e eu havia escrito inteiramente em Perl. Depois de uma semana, Dave escreveu-me novamente e disse que ele havia tentado o que eu havia sugerido para melhorar a velocidade do MRTG. Já que as alterações não ajudaram muito, ele havia decidido reescrever as sessões que demoravam mais tempo do MRTG em C. O código veio anexo ao seu e-mail. A ferramenta que ele desenvolveu melhorou a velocidade do MRTG em 40 vezes! Isto me tirou do meu esquecimento do MRTG e eu comecei a gastar tempo vago no desenvolvimento do MRTG-2.
Logo depois do desenvolvimento MRTG-2 ter começado eu passei a distribuir cópias Beta para pessoas interessadas. Passei a receber muitas contribuições, muitos retornos de usuários e correção de bugs. O produto que você pode utilizar hoje não seria como é, se não fossem as contribuições e suporte que recebi de muitas pessoas.

4.2 Conceito do MRTG

MRTG consiste em um script em Perl que usa SNMP para ler os contadores de tráfego de seus roteadores e um rápido programa em C que loga os dados do tráfego e cria belos gráficos representando o tráfego da conexão de rede monitorada. Estes gráficos são incluídos em páginas web que podem ser visualizadas de qualquer Browser moderno.
Somadas a detalhada visão diária o MRTG também cria representações visuais do tráfego durante os últimos 7 dias, das últimas 4 semanas e dos últimos 12 meses. Isto é possível porque o MRTG mantém um log de todos os dados que ele conseguiu do roteador. Este log é

automaticamente consolidado, e com isso ele não cresce com o tempo, mas ainda contém todos os dados relevantes de todo o tráfego dos últimos 2 anos. Isto tudo é realizado de uma maneira muito eficiente. Então você pode monitorar mais de 200 links de rede de qualquer estação UNIX decente.

O MRTG não se limita a monitorar somente tráfego, é possível monitorar qualquer variável SNMP que você escolher. Você pode até usar um programa externo para pegar os dados que você deve monitorar via MRTG. As pessoas usam o MRTG, para monitorar coisas como Carga do Sistema, Sessões Logadas, Disponibilidade de Modens e muito mais. O MRTG ainda permite a você acumular 2 ou mais fontes de dados em um único gráfico.

4.3 Características e funcionalidades

- ✓ **Portabilidade**
  MRTG trabalha na maior parte das plataformas UNIX e Windows NT.
- ✓ **Perl**
  MRTG é escrito em Perl e vem com todo o código fonte.
- ✓ **Portabilidade SNMP**
  MRTG usa uma implementação SNMP de alta portabilidade escrita toda em Perl graças a Simon Leinen. Não é necessário instalar qualquer pacote SNMP externo.
- ✓ **Suporte a SNMPv2c**
  MRTG pode ler os novos contadores de 64 bits do SNMPv2c. Os contadores não serão mais problema.
- ✓ **Interface de Identificação Confiável**
  As interfaces dos roteadores podem ser identificadas pelo Endereço IP, Descrição e Endereço Ethernet em adição ao número da interface normal.
- ✓ **Tamanho dos arquivos de Log Fixos**
  Os arquivos de log do MRTG NÃO crescem. Graças ao uso de um algoritmo de consolidação de dados único.
- ✓ **Configuração Automática**
  MRTG vem com um conjunto de ferramentas de configuraçao que fazem a configuração muito simples.

- ✓ **Desempenho**

  As rotinas mais críticas foram escritas em C graças a iniciativa de Dave Rand meu Co-Autor.
- ✓ **Livre de Gráficos GIF**

  Os gráficos são gerados diretamente no formato PNG, usando a biblioteca GD de Thomas Boutell.
- ✓ **Customizável**

  A aparência das páginas produzidas pelo MRTG são altamente configurável.
- ✓ **RRDtool**

  MRTG foi construído para ser compatível com RRDtool. Se você precisa de performance isso pode ajudar.

REFERÊNCIAS

Tobias Oetiker <oetiker@ee.ethz.ch> e muitos colaboradores
http://people.ee.ethz.ch/~oetiker/webtools/mrtg/pt/mrtg.htm

5. WHATS UP GOLD

Esta ferramenta é fabricada pela empresa IPSwitch, cujo site é http://www.ipswitch.com. A sua plataforma de utilização é baseada em MS Windows. Com respeito ao licenciamento, a sua utilização requer pagamento de aproximadamente U$ 700,00. Toda a documentação do software está em língua inglesa.

WhatsUp Gold é uma solução simples de mapeamento de rede, monitoramento, notificação e de relatório de desempenho que ajuda os administradores de rede e engenheiros a detectarem e consertarem os problemas da rede - rapidamente. É um monitorador / gerenciador gráfico de redes multi-protocolo, monitora seus dispositivos críticos e serviços através de alarmes visuais e auditivos quando um problema é detectado, ajudando gerenciar sua rede e deixá-la mais tempo online. O WhatsUp irá notificá-lo através de beeper, pager, e-mail ou telefone. Pode ser instalado em sistemas operacionais como Windows 2000, Windows NT com SP 6 ou posterior, Windows ME ou Windows XP.

5.1 Qual seu propósito

Mapear sua rede: escolha algumas opções automáticas de mapeamento para criar um mapa com seus devices como por exemplo: roteadores, switches, servidores, estações na sua rede. Automapeamento para monitorar serviços como web, e-mail ou servidores FTP de cada device.

Monitorar Dispositivos e Serviços: use os protocolos TCP/IP, SNMP, NetBIOS e IPX para mapear e monitorar sua rede. O WhatsUp continuamente monitora seus devices mapeados e serviços nos mesmos. Ele inicia os alarmes audíveis e visíveis quando os devices e os serviços estão com problemas.

Receber notificação de problemas: quando detecta um problema, você pode receber uma mensagem por beeper, pager, som, WinPopup, e-mail, mensagens de voz e outros.

Geração de relatórios: para ajudar você analisar o tempo que sua rede fica online, capacidade de utilização e tempo de resposta.

Gerenciamento remoto: utiliza servidor de Internet para visualização e configuração dos mapas em qualquer equipamento remoto.

5.2 Fácil de configurar e usar

WhatsUp Gold é tão fácil de instalar e operar que você não vai precisar de qualquer treinamento especializado. Em poucos minutos você será capaz de monitorar toda a rede e as aplicações críticas.

REFERÊNCIAS

PEREIRA, Jeziel Torres. **Modelo de Gerenciamento baseado em Ferramentas de Baixo Custo para Redes de Pequeno Porte**. Florianópolis, 2002. Monografia (para a obtenção do grau de Mestre em Ciência da Computação) – PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO, Universidade Federal de Santa Catarina.

Disponível em: <http://www.netprofit.com.br/whatsup.htm> acessado em: 03/11/2005.

6. ADVENTNET V5 MONITOR

Esta ferramenta é fabricada pela Advent, cujo site é http://www.adventnet.com e foi analisada na versão 2.4. A sua plataforma de utilização é baseada em MS Windows, nas versões 9X, NT e 2000, além do Linux. Com respeito ao licenciamento, a sua utilização requer pagamento de aproximadamente U$ 7500,00. O software é do tipo *AS IS*[1], sendo que o seu código fonte não está disponível. Toda a documentação do software está em língua inglesa.

A instalação do mesmo pode ser considerada fácil, ocupa pouco espaço em disco e não requer grande capacidade computacional para executar, sendo que o hardware mínimo recomendado é computador com processador Pentium 166 MHz, 64 Mb de memória RAM e 10 MB de espaço disponível em disco.

O AdventNet V5 Monitor possui interface gráfica, possibilitando a geração de gráficos representando a utilização dos recursos gerenciados. O software também pode ser usado para a criação de *applets java*, que podem ser visualizados em um WEB Browser e permitem a troca de informações de gerenciamento com agentes SNMP. Sua principal característica é o monitoramento das variáveis SNMP, que são obtidas através de varredura (*polling*) entre as sessões de monitoramento. Permite a geração de páginas web, dependendo de servidor WWW para tanto.

A ferramenta provê flexibilidade fixando filtros, baseados em condições sobre as variáveis SNMP obtidas e ativando ações baseadas nos dados apanhados, podendo ser a geração de arquivos do tipo log ou envio de e-mail.

REFERÊNCIAS

PEREIRA, Jeziel Torres. **Modelo de Gerenciamento baseado em Ferramentas de Baixo Custo para Redes de Pequeno Porte**. Florianópolis, 2002. Monografia (para a obtenção do grau de Mestre em Ciência da Computação) – PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO, Universidade Federal de Santa Catarina.

[1] AS IS (Como é) – Tipo de software cujo código fonte não é fornecido com o produto.

ESTUDO SOBRE A FERRAMENTA ESCOLHIDA PARA WINDOWS WHATS UP GOLD

1. INTRODUÇÃO

Não importa o tamanho ou complexidade que tenham, as redes têm o desafio diário de entregar máxima confiabilidade e desempenho.
Falhas das aplicações ou do equipamento podem paralisar totalmente a produtividade e causar forte impacto no lucro de um negócio. Empresas médias, assim como grandes corporações, têm redes de complexidade crescente, mas prescindem de soluções práticas para alcançar o monitoramento de redes ideal. Em um mercado asfixiado com soluções de administração complexas e caras, existe a necessidade para gerência de redes que seja escalável, utilizável e elástica, em combinação com baixo custo de compra. O Ipswitch WhatsUp® Professional isola os problemas de sua rede e lhe proporciona informação e compreensão do rendi- mento e da disponibilidade.

2. WhatsUp Professional Oferece

Monitoramento de Rede Extenso — acompanhe a disponibilidade e o rendimento de sistemas de negócio críticos. O WhatsUp Professional oferece monitoramento em tempo-real e alertas relativos aos serviços da rede, eventos de Windows e Syslog, utilização dos recursos do sistema e mais.

Rastreamento e Mapeamento Intuitivos da Rede — Identificação automática de todos os dispositivos de sua rede, utilizando capacidades de rastreamento inteligente. O administrador pode criar definições lógicas de sua rede diretamente desde o interior da completamente redesenhada interface estilo-Explorer do WhatsUp Professional.

Armazenamento de Dados Escalável — Uma base de dados relacional e compatível com o servidor SQL armazena o status compreensível das até mais extensas redes, de modo a dar flexibilidade de gerência e capacidade de relatórios desde o WhatsUp Professional.

Relatórios Integrados — O administrador pode analisar tendências que se estão desenvolvendo em sua rede, utilizando relatórios, baseados em HTML, sobre os dispositivos,

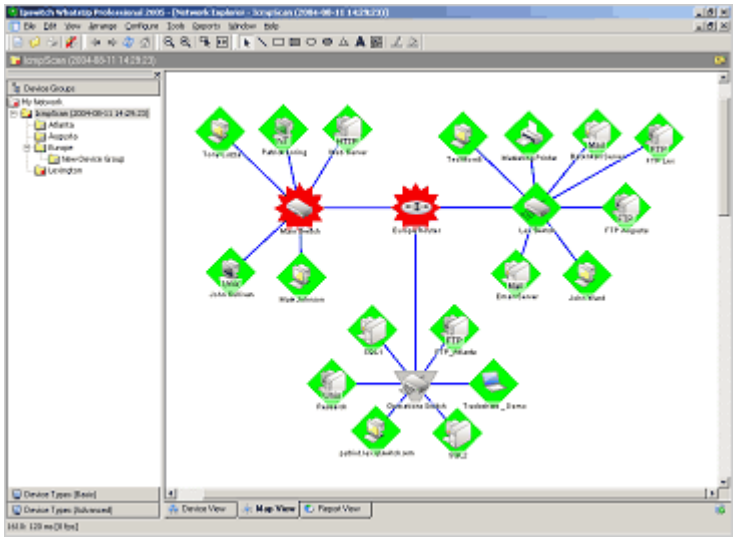
disponibilidade dos serviços e rendimento. Relatórios importantes são gerados sobre a rede inteira, grupos de dispositivos e serviços individuais.

Acesso Remoto Seguro — O administrador pode visualizar dados de sua rede e fazer mudanças de configuração desde qualquer lugar e a qualquer hora, com o servidor web que está construído desde dentro do WhatsUp Professional, ou via Microsoft® IIS. A codificação SSL assegura que os dados de sua rede estejam sempre protegidos.

3. Monitoramento de Rede Poderoso

Ipswitch WhatsUp Professional proporciona monitoramento detalhado de disponibilidade da rede e do rendimento. A pesquisa pró-ativa dos dispositivos, desde uma lista centralizada dos mesmos, auxilia o administrador a acompanhar o estado de sua rede. Políticas alteráveis sob medida e alarmes ajudam a administrar qualquer situação imaginável. Entre as capacidades de monitoramento estão:

- Serviços Windows (em sistemas NT® , 2000, XP®)
- Monitoramento de Portas TCP/UDP
- Monitoramento dos limites de recursos como o CPU, espaço de disco e memória
- Logs de Eventos Windows e Syslog
- Informações de SNMP
- Status dos dispositivos pode ser codificado por cor, ajudando a que o administrador se informe de algum problema com una simples olhada no monitor



Apresente corretamente a infra-estrutura de sua rede com a nova dinâmica interface estilo-Explorer do WhatsUp Professional.

4. Rápida Resolução de Problemas

Informe-se imediatamente das falhas em sua rede ou da degradação de rendimento, com alertas alteráveis sob medida e políticas de ação. Envie alertas quando surgem problemas ou acelere ainda mais a resolução dos mesmos, com opções como "reiniciar um dispositivo" ou "lançar um programa automaticamente". Maximize o tempo que sua rede está totalmente disponível, das seguintes formas:

- Receba alertas via e-mail, Pager, celular, SMS o alertas de áudio
- Alertas na bandeja das Tarefas do Sistema
- Reenvio/Redirecionamento de informações de SNMP
- Reinicio automático do serviço
- Visualize o status ou faça mudanças desde qualquer navegador de web (acesso remoto seguro tem codificação SSL 128-bit)

5. Rastreamento e Mapeio Dinâmicos

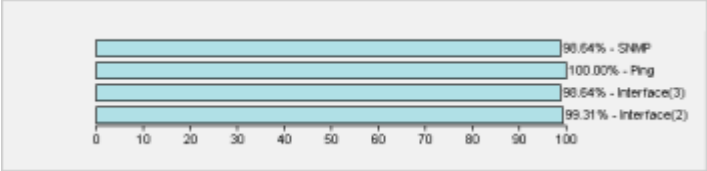
Rastreie a sua rede em minutos, utilizando assistentes de instalação intuitivos, os quais ativam o WhatsUp Professional a procurar, por toda a rede, routers, switches, servidores, impressoras e qualquer outro dispositivo. Toda esta informação é, então, armazenada dentro de uma base de dados relacional, para habilitar fácil administração dos dispositivos e a criação dos relatórios.

- O administrador pode criar grupos lógicos dos dispositivos e redes, para assim ajudar no monitoramento de áreas específicas de sua rede
- O administrador pode visualizar a topologia de sua rede em uma lista ou em um mapa, através do novo interface estilo-Explorer do WhatsUp Professional
- O administrador pode alterar a maneira em que visualiza sua rede, sob medida, com "drag and drop", múltiplos grupos de dispositivos e opções de desenho

6. Revele Tendências

WhatsUp Professional proporciona relatórios em tempo-real e com opções de formato histórico HTML, para fácil acesso e customização. O administrador pode compartilhar relatórios detalhados de disponibilidade ou rendimento para grupos de dispositivos ou dispositivos específicos. Relatórios flexíveis podem mostrar dados por mês, semana, dia ou hora. Entre as opções de relatórios estão:

- Relatório de Disponibilidade (porcentagem de tempo de resposta)
- Relatório de Desempenho (atraso em serviço ou dispositivo)
- Relatório de Saúde (relatório-resumo do status atual)
- Cronologia de Mudanças de Estado (histórico recente de mudanças nos dispositivos)



Entenda tendências de sua rede que se estejam desenvolvendo historicamente, com relatórios HTML dos dispositivos e serviços.

7. Requerimentos de Sistema

- Servidor Windows 2003, Windows XP SP1 ou posterior, ou Windows 2000
- 260 MB de espaço de disco
- 256 MB RAM
- Para utilizar a opção de notificação/alerta via beeper ou pager, um modem local e linha telefônica são necessários (WhatsUp Professional não suporta pool de modems)

8. Nova Versão 2006 - Principais características e Benefícios/ Novidades

Características	Benefícios
Melhoria nos relatórios, incluindo: - Relatório estatístico de desempenho - Relatórios padrões em tempo real - Relatórios recorrentes	Mostra como um dispositivo esta se comportando através do tempo e quais os dispositivos que tem um desempenho abaixo do esperado ou tem seus recursos super utilizados no decorrer do tempo.
Melhoria na capacidade de monitoramento incluindo a possibilidade de adaptação através de Monitoração ativa por scripts (VBscript ou Javascript)	Usuários podem criar sua própria estatística de monitoramento SNMP ou WMI e também coletar dados e produzir relatórios e estatísticas através de qualquer monitoramento adaptado (customizado).
Monitoramento HTTPS	Permite o monitoramento de conteúdo web seguro através de conexões SSL.
Monitoramento SNMP3	Permite o rastreamento de valores SNMP de um dispositivo com SNMPv3.
Ações recorrentes para Pagers	Configure mensagens que podem ser enviadas para um pages com o status corrente de uma situação.
Grupos de Dispositivos Dinâmicos	Cria grupos de dispositivos dinâmicos com características específicas para um gerenciamento mais conveniente. Fornece uma forma mais flexível e compreensiva de agrupar dispositivos dinamicamente facilitando a produção de relatórios e alertas.
Encontra e reporta MAC Address	Mapeia e descobre MAC addresses para endereços de IP. Mostra a conectividade entre portas de um switch e dispositivos.
Alarms pela Web	Permite a um operador ser notificado colocando um alerta audível na console WEB.
Monitoramento de banda de passagem em router	Mostra a utilização de banda de passagem e acompanha a utilização dentro de espaços de tempo.
Biblioteca de credenciamento	Permite o gerenciamento centralizado das credenciais de conexão para SNMPv1, SNMPv2 e SNMPv3 como também para WMI.

REFERÊNCIAS

Documentação impressa fornecida pela Ipswitch “Ipswitch WhatsUp Professional - Conheça a sua Rede”

ESTUDO SOBRE A FERRAMENTA ESCOLHIDA PARA LINUX MRTG

1. INTRODUÇÃO

O MRTG acompanha o tráfego de pacotes em sua rede e cria páginas HTML contendo imagens GIF que fornecem um acompanhamento ao vivo do que está acontecendo em uma rede local.

MRTG foi escrito em PERL e C e roda sob sistemas Unix e Windows NT. As informações utilizadas para construir os gráficos são obtidas a partir do protocolo SNMP (Simple Protocol Network Management).

O MRTG é um dos softwares mais utilizados e mais, além de relatórios diários, o MRTG cria também relatórios semanais, mensais e anuais, que permitem visualizar a evolução do tráfego em sua rede.

Com o MRTG você pode ter uma boa idéia de como anda sua rede local e também consegue descobrir a origem de problemas.

2. SISTEMAS QUE RODA O MRTG:

- Linux 1.2.x, 2.0.x, 2.2.x, 2.4.x (Intel and Alpha and Sparc and PowerPC)
- Linux MIPS, Linux S/390
- SunOS 4.1.3
- MacOS X 10.3 with Fink or DarwinPorts
- Solaris 2.4, 2.5, 2.5.1, 2.6, 7, 8, 9, 10
- AIX 4.1.4, 4.2.0.0, 4.3.2
- HPUX 9,10,11
- WindowsNT 3.51, 4.0, 2k, XP, 2003 (95, 98 and ME too, but only for die-hards)
- IRIX 5.3, 6.2, 6.5
- BSDI BSD/OS 2.1, 4.x, 3.1
- NetBSD 1.5.x 1.6.x
- FreeBSD 2.1.x, 2.2.x, 3.1, 3.4, 4.x
- OpenBSD 2.x, 3.x
- Digital Unix 4.0
- SCO Open Server 5.0
- Reliant UNIX

- NeXTStep 3.3
- OpenStep 4.2
- Mac OS X 10.1 or greater
- And about any other sensible Unix

3. CARACTERÍSTICAS E FUNCIONALIDADES

Portabilidade

MRTG trabalha na maior parte das plataformas UNIX e Windows NT.

Perl

MRTG é escrito em Perl e vem com todo o código fonte.

Portabilidade SNMP

MRTG usa uma implementação SNMP de alta portabilidade escrita toda em Perl graças a Simon Leinen. Não é necessário instalar qualquer pacote SNMP externo.

Suporte a SNMPv2c

MRTG pode ler os novos contadores de 64 bits do SNMPv2c. Os contadores não serão mais problema.

Interface de Identificação Confiável

As interfaces dos roteadores podem ser identificadas pelo Endereço IP, Descrição e Endereço Ethernet em adição ao número da interface normal.

Tamanho dos arquivos de Log Fixos

Os arquivos de log do MRTG NÃO crescem. Graças ao uso de um algoritmo de consolidação de dados único.

Configuração Automática

MRTG vem com um conjunto de ferramentas de configurações que fazem à configuração dele simples.

Desempenho

As rotinas mais críticas foram escritas em C graças a iniciativa de Dave Rand.

Livre de Gráficos GIF

Os gráficos são gerados diretamente no formato PNG, usando a biblioteca GD de Thomas Boutell.

Customizável

A aparência das páginas produzidas pelo MRTG são altamente configurável.

RRDtool

MRTG foi construído para ser compatível com RRDtool. Se você precisa de performance isso pode ajudar.

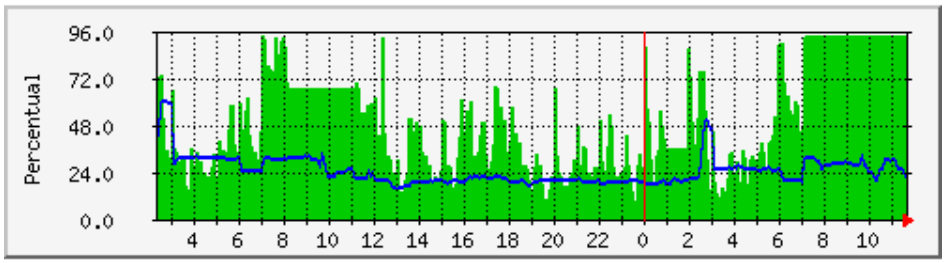
4. MRTG SEM SNMP

O MRTG pode também ser utilizado sem a necessidade do protocolo snmp, O MRTG (www.mrtg.org) é um software livre que facilita enormemente a tarefa de acompanhar o funcionamento do seu sistema. Embora o seu foco seja o acompanhamento de componentes de rede através do protocolo SNMP, você pode muito bem utilizar este software para verificar o funcionamento do seu computador doméstico ou estação de trabalho mesmo sem instalar o suporte a SNMP - basta usar a sua interface com scripts shell.

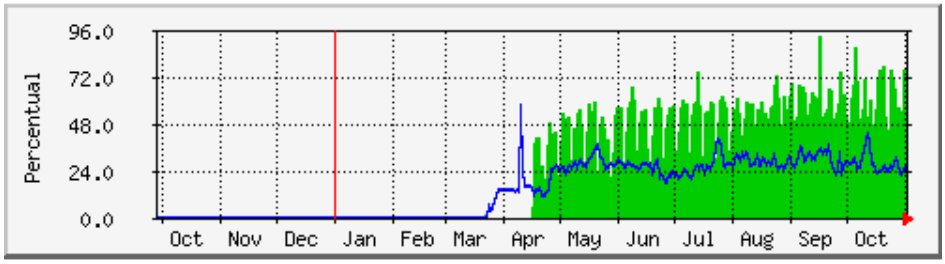
As imagens que coloquei abaixo é do conjunto de gráficos *default* gerados para acompanhar a utilização da CPU e memória e também uma interface de rede mostrando a quantidade de bytes transmitida e recebida na última semana e no último mês.

O site do MRTG tem muitos exemplos de como monitorar roteadores e outros equipamentos de rede com suporte a SNMP, mas muita gente procura informações sobre a interface do MRTG com programas externos, sem precisar de protocolos especializados em monitoramento nem de alterações na configuração de seus equipamentos. E isso se explica pela simplicidade com que é possível construir um script de monitoramento de qualquer coisa (uso de banda de rede, uso do disco, quantidade de usuários conectados a um sistema, etc.) e integrá-lo ao MRTG.

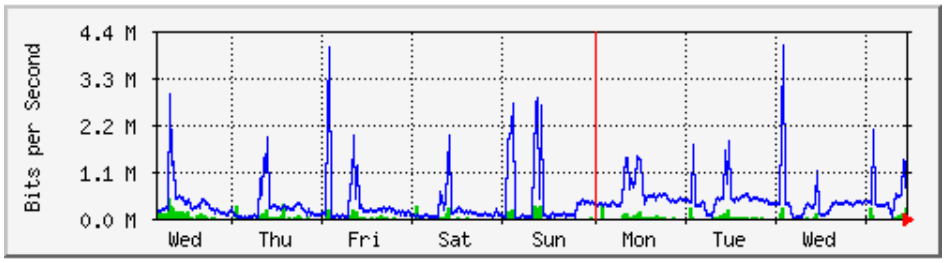
Um exemplo dos gráficos e dos tipos de dispositivos que o MRTG pode monitorar:



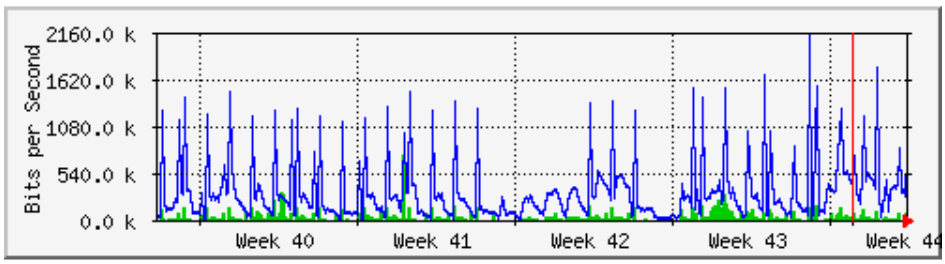
(Uso da Memória e CPU nas últimas 24hs, em verde: CPU ocupada. Em azul: memória ocupada)



(Uso da Memória e CPU no ano, em verde: CPU ocupada. Em azul: memória ocupada)



(Uso da Placa de rede na semana, em verde: tráfego recebido. Em azul: tráfego enviado)



(Uso da Placa de rede no mês, em verde: tráfego recebido. Em azul: tráfego enviado)

5. EXEMPLO DE IMPLEMENTAÇÃO DO MRTG

Demonstraremos abaixo um exemplo de scripts para geração de gráficos para utilização da CPU, uso da memória e tráfego de dados em uma conexão PPP(conexão discada). Com uma pequena noção de programação Shell não haverá muita dificuldade em alterar os exemplos e monitorar o que quiser e puder.

Para completar, nós demonstraremos uma página HTML bastante interessante para organizar os gráficos gerados.

Em primeiro lugar, é preciso ter o pacote MRTG instalado (todas as diostribuições comerciais de Linux o incluem), e o seu kernel deve ter suporte ao pseudo-filesystem /proc habilitado e em operação, pois iremos coletar dados diretamente de seus componentes.

Nossos arquivos de exemplo serão instalados no diretório /home/leonardo/mrtg, mude de acordo com a sua conveniência.

Os scripts para interface com o MRTG se caracterizam por sempre retornarem dois valores, um em cada linha, na saída padrão a cada vez que são executados. Estes valores correspondem às variáveis (sempre duas) monitoradas pelo script.

O script abaixo, extrai dados sobre o tráfego na sua interface ppp0. Grave-o com o nome de pppstats, e torne-o executável com o comando ("chmod 755 /home/leonardo/mrtg/pppstats"). Se quiser que ele grave os dados de sua placa de rede, ao invés do modem, substitua o ppp0 por eth0, eth1, eth2...(de acordo com a placa que deseja monitorar)

```
#!/bin/awk -f
/ppp0:/ { $0=substr($0,index($0,":")+1);
        print $1;print $9}
```

Este segundo script extrai informações sobre o uso da CPU e da memória, transforma em percentual e repassa ao MRTG. Grave-o com o nome de cpustats, e torne-o executável com o comando "chmod 755 /home/leonardo/mrtg/cpustats")

```
#!/bin/sh
mem=$(/usr/bin/free|grep ^-)
cpu=$(grep '^cpu ' /proc/stat)
/bin/awk -v cpu="$cpu" -v mem="$mem" '
BEGIN {
  split(cpu,cpustats)
  print 100-int(100*cpustats[4]/(cpustats[1]+\
       cpustats[2]+cpustats[3]+cpustats[4]))
  split(mem,memstats);
  print int(100*memstats[3]/(memstats[3]+\
       memstats[4]));
}'
```

Agora, trate de criar um arquivo de configuração para o MRTG, e grave-o com o nome de mrtg.conf:

```
WorkDir: /home/leonardo/mrtg
Target[ppp0]: `/home/leonardo/mrtg/pppstats /proc/net/dev`
Title[ppp0]:"Tráfego na interface PPP0"
PageTop[ppp0]: <h1>Tráfego de dados no modem local</h1>
MaxBytes[ppp0]:7168
Options[ppp0]: growright,bits,noinfo
#Unscaled[ppp0]:ymwd

Target[perf]:`/home/leonardo/mrtg/cpustats`
```

```
Title[perf]:"CPU e memória"
PageTop[perf]:"<h1>Uso de CPU e memória</h1>"
MaxBytes[perf]:100
Unscaled[perf]:ymwd
Options[perf]: growright,noinfo,gauge
YLegend[perf]: Percentual
ShortLegend[perf]: %
Legend1[perf]: Uso de tempo da CPU
Legend2[perf]: Uso da memória real
LegendI[perf]: CPU
LegendO[perf]: Mem
```

Tudo está pronto! Agora inclua na sua crontab a linha para executar o mrtg a cada 5 minutos, passando como parâmetro o nome do arquivo de configuração que você criou, conforme o exemplo:

```
*/5 * * * * /usr/bin/mrtg /home/leonardo/mrtg/mrtg.conf
```

Após 5 minutos você poderá ver o início dos seus gráficos se formando nos arquivos em formato html que serão criados no diretório /home/leonardo/mrtg. Antes de 5 minutos, os dados aparecerão zerados, mesmo que você execute várias vezes o mrtg manualmente - isto é uma consequência do modo como ele calcula suas estatísticas.

No diretório do MRTG (/home/Leonardo/mrtg) crie uma página html e cole o código abaixo, isto é só um exemplo, irá apresentar os gráficos das últimas 24 horas do uso de cpu e memória e outro gráfico das últimas 24 horas do uso do modem, cada gráfico possui sua devida legenda:

```
<head> <title>M.R.T.G</title> </head>
<!--by Leonardo Artware-->
<body bgcolor=black text=yellow link=white vlink=white>
<table border=0 width=100%>
   <tr><td colspan=2>
      <center> <p><h1>Uso da CPU e memória nas últimas 24 horas</h1> <img src=perf-day.png> <br>(em
verde: CPU ocupada. Em azul: memória ocupada)
<h1>Uso do modem nas últimas 24 horas</h1> <img src=ppp0-day.png> <br>(em verde: tráfego recebido. Em
azul: tráfego enviado)
      </center>
    </td></tr> </table>
  </body>
```

REFERÊNCIAS

http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
http://www.linux-sottises.net/en_mrtg.php

REFERÊNCIAS GERAIS

http://www.rnp.br/newsgen/9708/n3-2.html

http://www.inf.pucrs.br/~gustavo/rici/Redes.pdf

Apostila de TCP/IP(Entidade ACR-Informática)

http://www.projetoderedes.com.br/tutoriais

http://www.buscaki.com.br/links/redes.html

http://www.getronics.com.br

http://www.aldemario.adv.br/infojur/conteudo4texto.htm

http://www.multirede.com.br/pagina.php?codigo=10

http://www.teleco.com.br/emdebate/quadros02.asp

http://www.absoluta.org/tcp/tcp_per_hist.htm#2.3

http://www.lol.com.br/conectividade/redes/ger%EAncia_de_rede.php

http://www.vision.ime.usp.br/~mehran/ensino/ger.html

CARVALHO, Tereza Cristina Melo de Brito. **Gerenciamento de redes: uma abordagem de sistemas**. São Paulo: Makron Books,1993, 364 p.

http://www.teleco.com.br/tutoriais/tutorialsnmp/pagina_2.asp

http://www.inf.ufrgs.br/gpesquisa/tf/estudantes/trabalhos/peres.html

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

http://mesonpi.cat.cbpf.br/naj/snmp_color.pdf. Acessado em 22/08/2005

http://www.malima.com.br/article_read.asp?id=50 Acessado em 22/08/2005

Net academy cisco network

http://www.rnp.br/newsgen/9708/n3-2.html

http://www.cbpf.br/~sun/pdf/snmp.pdf

http://www.inf.furb.br/~pericas/orientacoes/JDMK2000.pdf

http://www.rnp.br/newsgen/9708/n3-2.html

http://www.cbpf.br/~sun/pdf/snmp.pdf

http://www.inf.furb.br/~pericas/orientacoes/JDMK2000.pdf

http://www.projetoderedes.com.br

http://www.rnp.br/newsgen/9805/metricas.html

http://penta2.ufrgs.br/gere96/cmipXsnmp/snmpcmipf.htm - acessado em 02/09/2005

http://penta2.ufrgs.br/gere96/cmipXsnmp/cmip_stra.htm - acessado em 02/09/2005

http://www.gta.ufrj.br/grad/cmip.html#cmip - acessado em 02/09/2005

http://www.apostilando.com/download.php?cod=252&categoria=Redes

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

http://www.rnp.br/newsgen/9708/n3-2.html

http://www.malima.com.br/article_read.asp?id=50

http://www.redes.unb.br/PFG.092004.pdf

http://www.mcc.ufc.br/disser/ErnestoVasconcelos.pdf

http://penta.ufrgs.br/gere96/cmipXsnmp/cmip_stra.htm

http://penta2.ufrgs.br/gere96/cmipXsnmp/snmpcmipf.htm

http://www.gta.ufrj.br/grad/cmip.html

http://www.rnp.br/newsgen/9805/metricas.html

http://penta.ufrgs.br/gr952/trab1/z_cmip.html

http://penta.ufrgs.br/gere96/rmon2/rmon2.html

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rmon.htm

http://www.rnp.br/newsgen/9901/r.html

http://penta.ufrgs.br/gr952/trab1/rmon.html

http://www.rnp.br/newsgen/9901/rmon.html

http://www.rnp.br/newsgen/9712/gerencia.html

http://www.apostilando.com.br

http://www.magnasistemas.com.br/magnasistemas/sbs1_3p.nsf/pages/tectivoli?OpenDocument&Click=

http://www.rnp.br/wrnp2/2000/posters/tivoli.pdf

http://www.ivirtua.com.br/index.php?conteudo=solutions&pg=dif

http://www.ivirtua.com.br/index.php?conteudo=solutions&pg=faq

http://www2.dcc.ufmg.br/~leoh/nagios/docs/toc.html

Tobias Oetiker <oetiker@ee.ethz.ch> e muitos colaboradores

http://people.ee.ethz.ch/~oetiker/webtools/mrtg/pt/mrtg.htm

PEREIRA, Jeziel Torres. **Modelo de Gerenciamento baseado em Ferramentas de Baixo Custo para Redes de Pequeno Porte**. Florianópolis, 2002. Monografia (para a obtenção do grau de Mestre em Ciência da Computação) – PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO, Universidade Federal de Santa Catarina.

http://www.netprofit.com.br/whatsup.htm Acessado em: 03/11/2005

PEREIRA, Jeziel Torres. **Modelo de Gerenciamento baseado em Ferramentas de Baixo Custo para Redes de Pequeno Porte**. Florianópolis, 2002. Monografia (para a obtenção do grau de Mestre em Ciência da Computação) – PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO, Universidade Federal de Santa Catarina.

Documentação impressa fornecida pela Ipswitch “Ipswitch WhatsUp Professional - Conheça a sua Rede”

http://people.ee.ethz.ch/~oetiker/webtools/mrtg/

http://www.linux-sottises.net/en_mrtg.php

ANEXO A – CONTRATO DE MANUTENÇÃO

Proposta contratual a UNINOVE

Nº da Proposta PSS-01/135/04-1

São Paulo, 27 de Novembro de 2005.

Prezado Sr(a).

Gostaríamos de agradecer a atenção dedicada a **HelpNet.com** e a oportunidade oferecida pela Universidade Nove de Julho para apresentação desta proposta.

Conforme levantamento realizado, pudemos avaliar quais de nossas soluções se aplicam em sua necessidade de Contrato de Suporte e temos a certeza de que a HelpNet.com poderá contribuir para integrar o processo e atender as expectativas de resultados dentro do prazo estipulado.

Adriano Santos
Gerente de Projetos
Tel (11) 0000000
Celular (11) 00000
E-mail: adrianoaps@hotmail.com

Índice da Proposta Comercial

Apresentação HelpNet.com

Quem Somos:

Integradora de Soluções desde Janeiro de 2000, a HelpNet.com atende seus clientes através de suas áreas de negócios: Soluções Corporativas, Soluções Integradas e Assistência Técnica, contando com profissionais treinados, de larga experiência e competência.

Um dos principais desafios das empresas é comunicar-se com seus clientes de maneira ágil, oportuna e a um baixo custo, e a tecnologia da informação é o instrumento que permite o desenvolvimento das estratégias de negócios destas organizações.

Voz, Dados e Imagem convergem em um único sistema lógico e físico, formando uma verdadeira rede de comunicação interativa, possibilitando redução de custos e aumento de resultados.

É com este foco que a HelpNet.com se posiciona no mercado.

Trabalhar para que nossos clientes possam disponibilizar suas informações de negócios.

MISSÃO:

"Disponibilizar as informações de nossos clientes, agregando segurança e velocidade para criar oportunidades de negócios."

Certificações Genéricas

MBA em Gestão Estratégica da Tecnologia da Informação

Bacharelado em Ciências da Computação

Engenharia Eletrônica

Tecnólogos em Redes

Certificação Cisco

Cisco CCNA e CCNP

Certificações Microsoft

MCP

MCSE

Especialidades

Especialista em Segurança da Informação

Parceiros Corporativos

Trend Micro	*Checkpoint*
Cisco	*IBM*
Microsoft	*C.A. Computer Associates*
Cconectiva	*Softium*

Clientes Corporativos

Johnson & Johnson	*Unicsul*
LG Philips	*Mondial Assistance*
Audi	*Nec*
Vunesp	*Volkswagen*
Blue Life	*Net Serviços*
Bovespa	*Nissin*

Responsabilidades da Helpnet.com

Garantir a equipe de profissionais especializados, tanto em quantidade quanto em qualificação profissional, de forma a assegurar a realização com alta qualidade nos trabalhos.

A Helpnet.com responsabiliza-se por todos os ônus e encargos trabalhistas e previdenciários resultantes da contratação e emprego das pessoas para a realização dos serviços objeto desta proposta.

A Helpnet.com obriga-se a executar os serviços, dentro das técnicas e dos costumes usuais em trabalho deste gênero, bem como a utilização de mão-de-obra qualificada.

Todos os tributos (impostos, taxas e contribuições) de natureza federal, estadual e municipal, incidentes ou que venham a incidir sobre contrato fruto desta proposta.

Responsabilidades do Cliente

Garantir aos profissionais envolvidos, de acordo com o nível de atuação de cada um, o acesso às informações necessárias para o desenvolvimento dos trabalhos, dentro dos prazos constantes no cronograma a ser definido de comum acordo.

A Helpnet.com deverá designar um profissional, que será responsável pelo contato e relacionamento com os profissionais da UNINOVE durante o desenvolvimento das atividades previstas nos serviços.

Esse profissional da Helpnet.com deverá ter disponibilidade de agenda para prestar, no menor prazo possível, quaisquer esclarecimentos ou buscar dentro da própria empresa decisões que, do contrário, possam afetar o andamento do projeto. Esses contatos podem ser feitos por telefone, e-mail ou através de reuniões nas instalações do cliente, de acordo com a sua conveniência.

A UNINOVE deverá permitir e facilitar o ingresso dos profissionais da Helpnet.com às suas instalações, assim como prover informações corretas e precisas, que se julgarem necessárias para o desenvolvimento adequado das atividades profissionais previstas nos serviços, objeto desta proposta. Se ao final da leitura desta proposta, ainda persistir qualquer dúvida ou mesmo falta de alguma informação, solicitamos entrar em contato conosco.

Responsabilidades Mútuas

Manter registro sobre etapas do processo de trabalho, através de documentos específicos de conhecimentos gerais, devidamente assinados pelas partes interessadas e pessoais envolvido.

Quando necessário, convocar e realizar revisões gerais ou específicas do projeto, visando redefinir recursos e prazos.

As alterações e/ou redefinições que configurem mudança do escopo do projeto poderão gerar negociações de prazos e custos referentes ao projeto como um todo.

Proposta

Serviços Oferecidos

Suporte Técnico

Categoria	*Serviços*
Suporte Local, Telefônico e Remoto	Instalação e Configuração; Manutenções Corretivas e Preventivas; Relatórios Gerenciais e de Controle.

Horário de Atendimento

Turno	*Horário*	*Tipo*
Normal	8x5 (8:00Hs às 18:00Hs)	Suporte a Software fornecido pela Helpnet.com
Normal	8x5 (8:00Hs às 18:00Hs)	Suporte ao Sistema Operacional Windows 2003 / Linux

Condições Comerciais

- O serviço será desenvolvido nas instalações da UNINOVE em São Paulo – SP;
- Os atendimentos serão realizados na modalidade 8x5 (oito horas por dia / cinco dias da semana);
- A proposta preve o fornecimento de serviços de Suporte, Manutenção Corretiva e Preventiva nas seguintes condições:
  - Servidores (Contido o Software Ger. Redes): atendimento em até 4h úteis;
  - Servidores com Part Number: XXXX;
  - Sistema Operacional Windows 2003 / Linux.
- Está previsto no contrato um total de 12 (doze) horas mensais de suporte local;
- Esta previsto no contrato que suporte telefônico e remoto, não será descontado as horas de créditos pré estabelecidas na cláusula a cima;
- As horas previstas no contrato serão acumulativas por 03 meses e poderão ser utilizadas para manutenções, instalações e treinamentos/consultorias, que serão sempre fornecidos por um profissional da Helpnet.com;
- As horas acumuladas, que não forem utilizadas no final do período de 03 meses serão zeradas, passando a valer o número de horas previstas no contrato (12 horas);
- Caso seja utilizado um número de horas superior ao que está previsto no contrato mensal, essas horas serão cobrados como excedentes e seus valores estarão pré-estabelecidos no contrato;
- O transporte dos Técnicos / Analistas serão de inteira responsabilidade da Helpnet.com;
- Valores em reais com impostos já inclusos;
- Valores para pagamento mensal;
- Os valores do contrato serão reajustados anualmente pelo índice do IGP-m;
- Contrato com validade de 12 (doze) meses com renovação automática, não podendo ser cancelado antes do 6º (sexto) mês;

Proposta Comercial

Suporte local, telefônico e remoto:

Qtde.	Produto / Serviço	Vl. Unitário	Vl. Mensal
12 hs/mês	Suporte Local, Telefônico e remoto (8x5)	R$ 0	**R$ 0**
01 hora	Hora Excedente (8x5)	R$ 0	**R$ 0**

Especificação

- Serviços especializados de Suporte para:
  - Microsoft Windows Server 2000;
  - Linux;
  - Software Gerenciamento de Redes fornecido pela Helpnet.com (MRTG e Whats UP Gold).