Centro Estadual de Educação Tecnológica Paula Souza

Faculdade de Tecnologia de Americana

Curso Superior de Tecnologia em Segurança da Informação

RAQUEL FERRAZ CUNHA SANTOS

GERÊNCIA E MONITORAMENTO DE REDES

Americana, SP

2011

Centro Estadual de Educação Tecnológica Paula Souza

Faculdade de Tecnologia de Americana

Curso Superior de Tecnologia em Segurança da Informação

RAQUEL FERRAZ CUNHA SANTOS

GERÊNCIA E MONITORAMENTO DE REDES

Trabalho de Conclusão de Curso apresentada à Faculdade de Tecnologia de Americana como parte das exigências do curso de Análise de Sistemas e Tecnologia da Informação para obtenção do título de Tecnólogo em Segurança da Informação, sob orientação do Professor Rogério Nunes de Freitas.

Americana, SP

2011

RAQUEL FERRAZ CUNHA SANTOS

0822334

GERÊNCIA E MONITORAMENTO DE REDES

Trabalho de Conclusão de Curso aprovada como requisito parcial para obtenção do título de Tecnólogo em Segurança de Informação no curso de Análise de Sistemas e Tecnologia da Informação da Faculdade de Tecnologia de Americana.

Banca Examinadora:

Professor Rogério Nunes de Freitas
(Orientador)

Professor Marcus Vinicius Lahr Giraldi
(Convidado)

Professor Mestre Wladimir da Costa
(Convidado)

Americana (SP), 08 de dezembro de 2011

DEDICATÓRIA

Dedico este trabalho a minha mãe Rita de Cássia Ferraz Cunha Santos e ao meu pai Valdir da Cunha Santos (em memória) pela paciência e ensinamentos. Aos familiares, amigos e colegas pelo companheirismo e a todos os professores pelos conhecimentos transferidos para a minha formação acadêmica ser concretizada.

AGRADECIMENTOS

Primeiramente a Deus que é o nosso pai, fonte de vida e sabedoria. Que nos proporciona todos os dias o milagre da vida e conhecimento, que me concedeu a maravilhosa família que tenho.

Aos meus pais, Rita de Cássia Ferraz Cunha Santos e Valdir da Cunha Santos (em memória), que sempre me apoiaram em cada etapa da minha vida, me ajudando e incentivando em tudo.

Ao meu orientador Professor Rogério Nunes de Freitas pela paciência, dedicação e incentivo que muito me ajudou.

A todos os professores da Faculdade de Tecnologia de Americana pela contribuição na minha formação das mais diferentes maneiras (aulas, conversas, exemplos de vida, entre outros).

Aos amigos e amigas pelas horas de trabalho em grupo, pelas companhias em festas, pelas reuniões semanais, pelos bate-papos, entre outros.

Aos colegas da graduação que estiveram juntos comigo nessa caminhada acadêmica de lutas e vitorias, pela convivência e amizade sempre com palavras de incentivo.

“A primeira regra de qualquer tecnologia utilizada nos negócios é que a automação aplicada a uma operação eficiente aumentará a eficiência. A segunda é que a automação aplicada a uma operação ineficiente aumentará a ineficiência” (Bill Gates).

RESUMO

Com a globalização o mundo vem passando por grandes e intensas transformações em termos de TI (Tecnologia da Informação), com isso, surge à necessidade do uso de ferramentas que nos auxiliam na manutenção dos grandes fluxos de informações de forma constante, segura e veloz.

Para controlar esses grandes fluxos de informações podemos utilizar ferramentas que gerenciam satisfatoriamente os recursos e serviços em ambientes de redes.

Com base nessas informações esse TCC (Trabalho de Conclusão de Curso) foi desenvolvido, com a finalidade de se obter mais conhecimento em como gerenciar e monitorar as redes de computadores.

Palavras Chave: Rede, Gerenciamento, Monitoramento, Tecnologia, Internet, Segurança, Computadores.

ABSTRACT

With globalization the world has been undergoing major transformations and intense in terms of IT (Information Technology), with this comes the need to use tools that assist us in maintaining major information flows steadily, safe and fast.

To control these large flows of information we can use tools to successfully manage the resources and services in network environments.

Based on this information the CBT (Completion of Course Work) was developed in order to obtain more knowledge on how to manage and monitor computer networks.

Keywords: Network, Management, Monitoring, Technology, Internet, Security, Computers.

LISTA DE FIGURAS

Figura 1. Exemplo de uma rede LAN 15
Figura 2. Exemplo de uma MAN 16
Figura 3. Exemplo uma WAN 17
Figura 4: Arquitetura do TCP/IP 20
Figura 5: Topologia em anel 23
Figura 6: Topologia em barramento 24
Figura 7: Topologia em estrela 25
Figura 8: Topologia em árvore 26
Figura 9: Topologia hibrida 27
Figura 10: Hub 8 portas 10/100Mbps 28
Figura 11: Switch 24 portas 10/100Mbps 29
Figura 12: Roteador Wirelles 150/Mbps 30
Figura 13: Access Point WAP4410N 31
Figura 14: Gerenciamento de redes 33
Figura 15: Arquitetura de gerenciamento 38
Figura 16: Estação de monitoramento de redes 41
Figura 17: Monitoramento do nagios via web 45
Figura 18: Fedora com servidor nagios monitorando um Windows XP 46
Figura 19: Nagios monitorando uma sobrecarga de CPU no Windows XP 46
Figura 20: Monitoramento com the dude 53
Figura 21: Monitoramento the dude via web 54
Figura 22: Tela de implantação do dude 55
Figura 23: Tela de implantação do dude 56
Figura 24: Tela de implantação do dude 56

LISTA DE ABREVIATURAS E SIGLAS

AP	Access Point
ARP	Address Resolution Protocol
DNS	Domain Name Server
FTP	File Transfer Protocol
HTML	Hiper Text Markup Language
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
MAN	Metropolitan Area Network
MIB	Management Information Base
NE	Network Elements
NETBIOS	Network Basic Input
NNTP	Network News Transfer Protocol
NOC	Network Operation Center
OSI	Open System Interconnection
PDA	Personal Digital Assistants
PDU	Protocol Data Unit
POP3	Post Office Protocol
RMON	Remote Network Monitoring
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCC	Trabalho de Conclusão de Curso
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
UDP	User Datagram Protocol
WAN	Wilde Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WWW	World Wide Web

SUMÁRIO

INTRODUÇÃO 13

1. REDES DE COMPUTADORES 14
   1.1. REDES LOCAIS (LOCAL AREA NETWORKS – LAN'S) 14
   1.2. REDES METROPOLITANAS (METROPOLITAN AREA NETWORKS – MAN'S) 16
   1.3. REDES GEOGRAFICAMENTE DISTRIBUÍDAS (WIDE AREA NETWORKS – WAN'S) 17
2. PROTOCOLOS DE REDES 18
   2.1. INTERNET PROTOCOL (IP) 19
   2.2. TRANSMISSION CONTROL PROTOCOL (TCP) 19
   2.3. USER DATAGRAM PROTOCOL (UDP) 20
   2.4. SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) 21
3. TOPOLOGIA DE REDES 22
   3.1. TOPOLOGIA EM ANEL 23
   3.2. TOPOLOGIA EM BARRAMENTO 24
   3.3. TOPOLOGIA EM ESTRELA 25
   3.4. TOPOLOGIA EM ÁRVORE 26
   3.5. TOPOLOGIA HÍBRIDA 26
4. EQUIPAMENTOS DE REDES 28
   4.1. HUB 28
   4.2. SWITCH 29
   4.3. ROTEADOR 30
   4.4. ACCESS POINT 31
5. GERÊNCIA DE REDES 32
   5.1. COLETA DE DADOS 33
   5.2. DIAGNÓSTICOS 34
   5.3. AÇÃO 34
   5.4. AS CINCO ÁREAS DE GERENCIAMENTO DE REDES 34
      5.4.1. Gerenciamento de Falhas 34
      5.4.2. Gerenciamento de Desempenho 35
      5.4.3. Gerenciamento de Configuração 36
      5.4.4. Gerenciamento de Contabilização 36

5.4.5. Gerenciamento de Segurança 37
5.5. ARQUITETURA DE GERENCIAMENTO DE REDES 37
5.6. ENTIDADE GERENCIADORA 38
5.7. DISPOSITIVOS GERENCIADOS 39
5.8. PROTOCOLO DE GERENCIAMENTO DE REDE 39
5.9. GERENTE 39
5.10. AGENTE 40
5.11. MIB (MANAGEMENT INFORMATION BASE) 40
5.12. FERRAMENTAS DE INSPEÇÃO E MONITORAMENTO DE REDES 40
5.13. CONFIGURANDO UM SISTEMA DE GERENCIAMENTO 41
5.13.1. Informações de Gerência de Redes 42
6. MONITORAMENTO DE REDES 43
6.1. NAGIOS 44
6.1.1. Nagios em Funcionamento na Virtualização 46
6.1.2. Processo de Instalação do Nagios no Linux 47
6.1.3. Processo de Instalação do Nagios no Windows 50
6.2. THE DUDE 52
6.2.1. Instalação do Dude 54

CONCLUSÃO 57

BIBLIOGRAFIA 58

INTRODUÇÃO

Uma rede de computadores possui partes complexas de *hardware* e *software*, tais como todos os seus equipamentos, por isso, pode-se esperar que ocorram problemas de funcionamento, onde os elementos da rede poderão perder a configuração por um ou outro motivo. Por essa razão é necessário o uso de algumas ferramentas que auxiliam em um melhor desempenho, gerenciamento e confiabilidade da rede.

Realizar um melhor gerenciamento dos processos ativos, agregando o monitoramento constante dos recursos, faz com que se evitem grandes perdas de informações que são necessárias para o desenvolvimento e tomadas de decisões de uma organização, por exemplo. Por esse motivo, as organizações têm buscado soluções no mercado de TI (Tecnologia da Informação) que sejam capazes de suprir a suas necessidades e deficiências na gestão tecnológica, resultando em um melhor produto no mercado, com processamento ideal das informações e segurança nos processos de negócios dentro das organizações.

Sendo assim, a cada dia aumenta a necessidade de aplicação de recursos e pessoal qualificado na gerência de rede, proporcionando em melhor desempenho de rede nos fluxos das informações para conduzir a complexidade de informações e a segurança das mesmas com eficiência, já que elas estão associadas ao bom desempenho da rede.

Com o intuito de estabelecer melhorias na qualidade de serviço e garantir confiabilidade e segurança nos grandes fluxos de informações que trafegam na rede, esse TCC (Trabalho de Conclusão de Curso) propõe a explicação de ferramentas de gerenciamento e monitoramento de redes, a fim de melhorar a vida dos usuários através de informações de gerenciamento dos dispositivos de redes.

1. REDES DE COMPUTADORES

Neste capítulo, serão abordados alguns conceitos gerais relacionados a redes de computadores, tipos de redes existentes tais como: LAN, MAN e WAN e sua arquitetura. Serão apresentadas definições e características de algumas topologias de redes tais como: anel, estrela, barramento, híbrida e árvore. Complementando o conteúdo serão abordados estudos dos protocolos IP, TCP, UDP e SNMP, suas definições, juntamente com suas características e funcionalidades. Assim como a importância e os tipos de equipamentos de redes.

Redes de computadores podem ser definidas como um conjunto de computadores, interligados por um sistema de comunicação, capazes de se comunicar entre si e obter respostas das mesmas, podendo então compartilhar informações e recursos [1]. Este sistema de comunicação irá depender de um arranjo topológico (que é estrutura da rede).

1.1. REDES LOCAIS (*LOCAL AREA NETWORKS* – LAN'S)

Redes locais (LAN) são redes de computadores concentradas em uma área geograficamente agrupada [2]. Geralmente projetadas para operar em redes de pequenas distâncias que pertencem à mesma organização ou território geográfico. São pequenas redes de computadores que na maioria das vezes é de uso privado e são utilizados para conexão de computadores pessoais ou estação de trabalho, permitindo o compartilhamento dos recursos e informações.

Na figura 1 a seguir, têm-se uma estrutura de uma rede local de computadores (LAN) que tem como função interligar esses dispositivos (equipamentos) por intermédio de enlaces físicos, ou seja, meios de transmissão de dados juntamente com um conjunto de regras, que tem por finalidade organizar o meio de comunicação (protocolos).

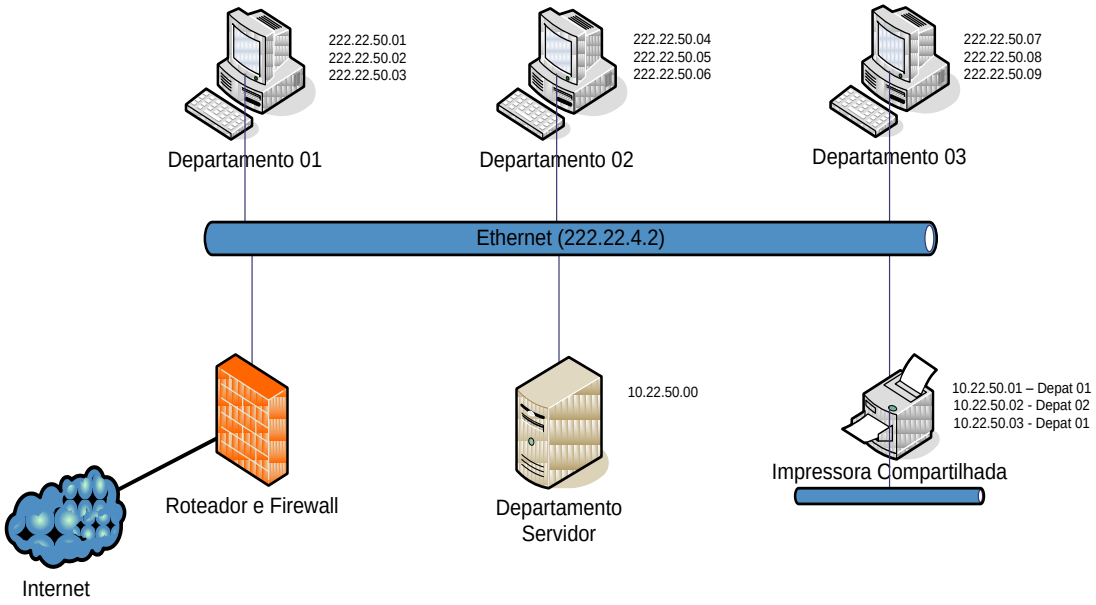

Figura 1. Exemplo de uma rede LAN [12]

As redes LAN pertencem a uma mesma organização e abrangência geográfica territorial, sendo que os dispositivos nelas conectados (computadores, *switch* e *hubs*) são os responsáveis pela transmissão de sinais de comunicação ou ampliações do mesmo, interligando e comunicando-se entre si dentro dessas pequenas distâncias.

Esta distância pode variar de alguns poucos metros a alguns quilômetros, sendo que as proporções físicas de uma de uma LAN têm uma abrangência bem menor se comparada a uma rede geograficamente distribuída (WAN).

Seu tamanho é limitado, o que permite o conhecimento e controle do tempo de transmissão, antecedências das detecções de falhas, permitindo um gerenciamento simplificado da rede. Algumas das características favoráveis desse tipo de rede são as altas taxas de transmissão e baixa taxas de erro.

Portanto, estas características transcorrem de acordo com a evolução da tecnologia empregada e a escolha de equipamentos necessários para um bom funcionamento da rede.

1.2. REDES METROPOLITANAS (*METROPOLITAN AREA NETWORKS* – MAN'S)

As redes Metropolitanas (MAN - *Metropolitan Area Networks*) são conexões entre os dispositivos de redes para atingirem distâncias ainda maiores de que uma rede LAN, ou seja, é praticamente uma versão modificada e ampliada de uma LAN, pois utilizam tecnologia semelhante [1].

As redes MAN podem ser formadas por conjuntos de escritórios vizinhos ou ter capacidade de abrangência territorial de uma cidade inteira. Podem possuir domínio de redes publicas ou privadas. As redes metropolitanas são inferiores às redes locais em nível de capacidade de transmissão, devido aos dispositivos de conexão utilizados e a distância entre os nós.

Em medidas de comparação entre uma LAN e MAN a principal diferença está no alcance de maior abrangência, onde as redes metropolitanas destacam-se por cobrir um perímetro um pouco maior. Uma rede metropolitana opera em uma velocidade maior, onde essa velocidade está associada à sua estrutura. Na figura 2 ilustra um exemplo de uma estrutura MAN.

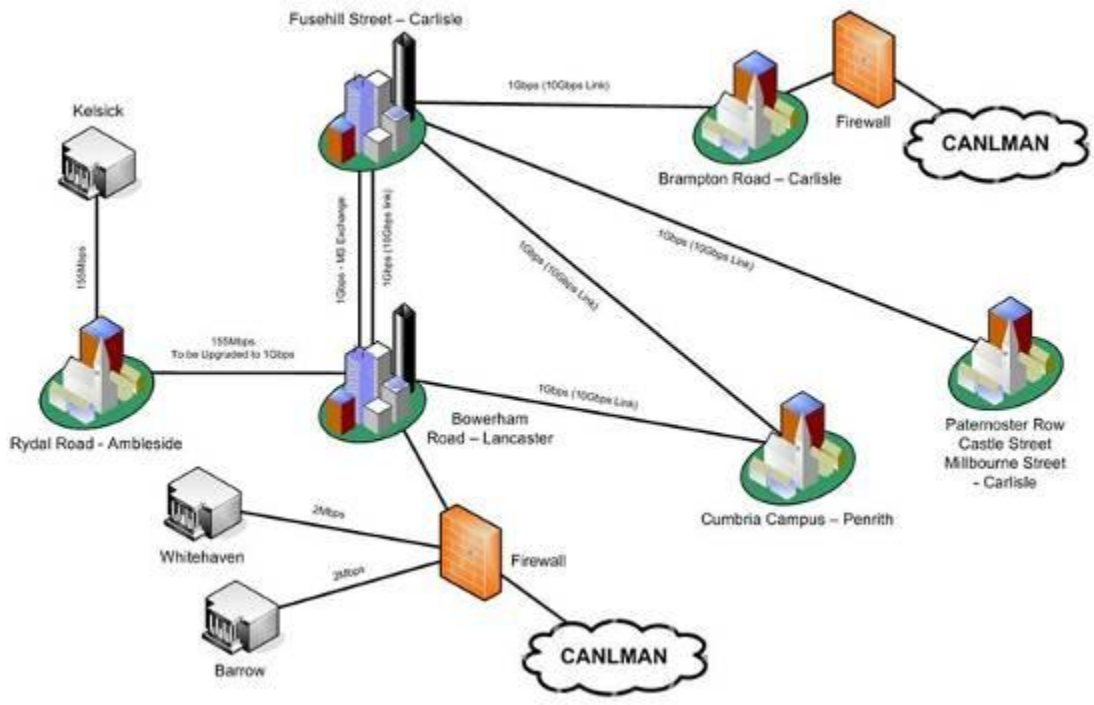

Figura 2. Exemplo de uma MAN [12]

1.3. REDES GEOGRAFICAMENTE DISTRIBUÍDAS (*WIDE AREA NETWORKS* – WAN'S)

As redes Geograficamente Distribuídas (WAN - *Wide Area Networks*) surgiram devido à necessidade de compartilhar recursos especializados com um maior número de comunidades e usuários. Localizados em regiões dispersas geograficamente, têm um índice de abrangência muito maior e bem mais preparado em se tratando de distâncias geográficas longínquas [1].

Neste tipo de rede sua cobertura torna-se maior, com taxas de velocidades altas no envio e recebimentos de pacotes.

Os custos tornam-se elevados por motivo de abrangência e complexidade de serviços, por exemplo: circuitos para satélite e enlaces de microondas, que nesse caso envolve custos elevados e grande disponibilidade de recursos e tecnologia. Tais redes geralmente são públicas. O sistema de comunicação e a maneira de como as operações serão gerenciados é administrada por grandes operadoras telefônicas (públicas ou privadas), e provedores de acesso à internet, responsáveis por tornar a conexão disponível a todos.

Diferente das outras distribuições geográficas (LAN, MAN) a interligação e comunicação entre os diversos dispositivos (equipamentos), determinarão o uso de um arranjo topológico específico e diferente daqueles utilizados em redes locais. Pode-se observar uma rede WAN e sua abrangência de cobertura, como ilustra a figura 3.

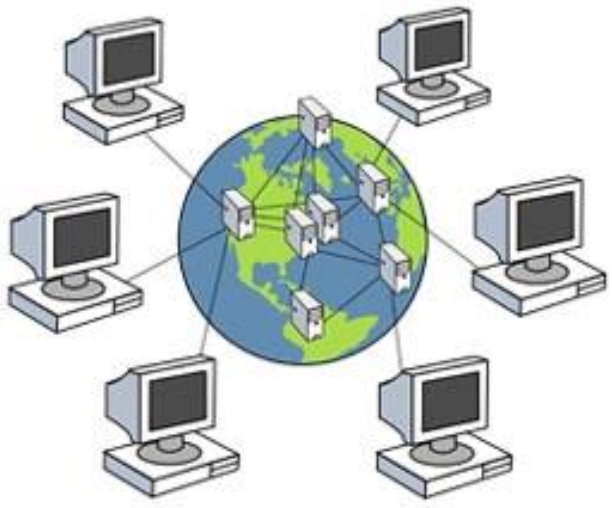

Figura 3. Exemplo uma WAN [13]

2. PROTOCOLOS DE REDES

Um protocolo de rede é semelhante ao sistema de comunicação humana, exceto pelo fato de que as entidades que irão trocar as mensagens e quem realizará as ações são os componentes de *hardware* e *software* [2].

Os protocolos de redes são artefatos de extrema importância para a comunicação entre as máquinas, afinal, se uma rede compartilhada não falar a mesma língua torna-se difícil à comunicação entre elas.

Os protocolos são responsáveis por esta comunicação, constituídos de um conjunto de padrões bem definidos (regras que determinam o modo de comunicação) que atuam nas diversas camadas de comunicação. Na falta desses padrões seria necessária a criação de *softwares,* que permitissem a comunicação de redes distintas com sistemas operacionais distintos.

> *"Um protocolo define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações realizadas na transmissão e/ou recebimento de uma mensagem ou outro evento" (KUROSE, F. James, Lemos & Ross, W.Keith; 1995).*

Necessita-se então que todas as estações de trabalho estejam configuradas de acordo com esses padrões. Sem eles, seria impossível o funcionamento da internet e redes comerciais. Os protocolos trabalham com camadas que interagem e desempenham uma ou mais funções específica na comunicação, controlando erros e tornando o canal lógico mais confiável entre as camadas.

Com o controle dos fluxos de informações, evita-se o congestionamento dos PDUs (*Protocol Data Unit*) que na verdade é uma unidade de dados, passados de uma camada de protocolos a outra. Sendo que cada uma dessas camadas, em que os protocolos empilhados em camadas será adicionada informações de cabeçalho PDUs. Cada camada de cima sofrerá esse processo de encapsulamento juntamente com as informações que ela adiciona.

As informações com essas segmentação e remontagem, que no lado transmissor consiste em dividir grandes blocos de informações em pequenas partes, e logo em seguida remontando-as e recuperando o bloco original entre outras tarefas.

2.1. *INTERNET PROTOCOL* (IP)

O *Internet Protocol* (IP) é o principal protocolo de comunicação utilizado para transmissão de dados chamados datagramas (pacotes) através de uma rede interna usando o *Internet Protocol Suite*. É responsável pelo roteamento de pacotes através dos limites da rede onde é o principal protocolo para estabelecer a Internet.

IP é o protocolo primário na camada de Internet do conjunto de protocolos de Internet e tem a tarefa de entregar pacotes da fonte do remetente para o host de destino apenas com base em seus endereços, para isso, o IP é definido abordando métodos e estruturas de pacotes encapsulados.

O IP foi o serviço de datagrama sem conexão no programa original de controle de transmissão, sendo assim necessário o outro serviço de datagrama orientado a conexão *Transmission Control Protocol* (TCP). O *Internet Protocol Suite*, portanto, é muitas vezes referido como TCP/IP.

A primeira versão de IP é conhecida como *Internet Protocol Version* 4 (IPv4) onde atualmente é o protocolo dominante da Internet, embora o sucessor, *Internet Protocol Version* 6 (IPv6) está com uma crescente implantação mundial.

2.2. *TRANSMISSION CONTROL PROTOCOL* (TCP)

O *Transmission Control Protocol* (TCP) é um dos principais protocolos da *Internet Protocol Suite* e um dos dois componentes originais do conjunto, complementando o *Internet Protocol* (IP), portanto, todo o conjunto é comumente referindo como TCP/IP.

TCP é um serviço confiável e ordenado de um fluxo de *bytes* que garante a entrega de um fluxo de dados enviados de um host para outro sem duplicação ou perda de dados. É o protocolo de aplicações utilizado extensivamente por muitos dos aplicativos populares da Internet, como a World Wide Web (WWW), E-mail, File Tranfer Protocol (FTP), administração remota e transferência de arquivos confiável.

O TCP consiste de um conjunto de regras: para os protocolos que são usados com o IP, para enviar dados “em uma forma de unidades de mensagem” entre computadores pela Internet. Enquanto o IP lida com a entrega real dos dados, o TCP controla as unidades individuais de transmissão de dados, chamadas segmentos, que uma mensagem é dividida para roteamento eficiente através da rede. Por exemplo, quando um arquivo HTML (*Hiper Text Markup Language*) é enviado de um servidor Web, a camada de *software* TCP desse servidor divide a seqüência de octetos do arquivo em segmentos e encaminha-os individualmente para a camada de *software* IP (camada de Internet). A camada de Internet encapsula cada segmento TCP em um pacote IP, adicionando um cabeçalho que inclui (entre outros dados) o destino de endereço IP. Mesmo que cada pacote tenha o mesmo endereço de destino, eles podem ser encaminhados por caminhos diferentes através da rede. Quando o programa de cliente no computador de destino recebê-los, a camada TCP (camada de transporte) reagrupa os segmentos individuais e garante que eles estão corretamente ordenados e livre de erros, uma vez que os reproduzem para um aplicativo. A figura 4 ilustra o modelo das camadas TCP/IP.

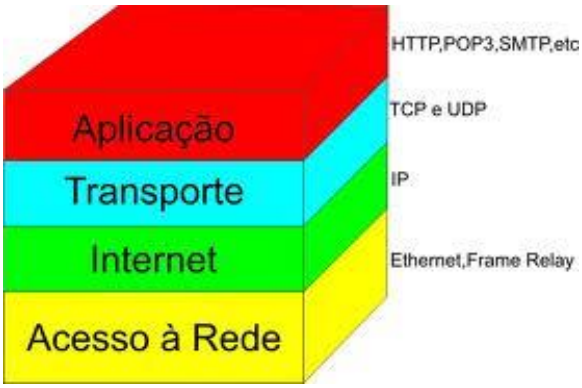

Figura 4: Arquitetura do TCP/IP [14]

2.3. *USER DATAGRAM PROTOCOL* (UDP)

O *User Datagram Protocol* (UDP) é um protocolo simples da camada de transporte, ele permite que a aplicação escreva um datagrama encapsulado num pacote IPv4 ou IPv6, e enviar ao destino. Mas não há qualquer tipo de garantia que o pacote irá chegar ou não.

O protocolo UDP não é confiável, então caso haja necessidade de garantias, é preciso implementar uma série de estruturas de controle, tais como *timeouts*, retransmissões, controle de fluxo, entre outros. Cada datagrama UDP tem um tamanho e pode ser considerado como um registro indivisível, diferentemente do TCP, que é um protocolo orientado a fluxos de *bytes* sem início e sem fim.

O UDP é um serviço sem conexão, pois não há necessidade de manter um relacionamento longo entre cliente e o servidor. Ele fornece os serviços de *broadcast* e *multicast*, permitindo que um único cliente envie pacotes para vários outros na rede.

2.4. *SIMPLE NETWORK MANAGEMENT PROTOCOL* (SNMP)

O protocolo SNMP (*Simple Network Management Protocol*) existente na arquitetura TCP/IP é o grande responsável pelo gerenciamento de uma rede, operando na camada de aplicação [7]. No gerenciamento SNMP ele atua como gerente e agente. Na estação gerente é realizado o envio de comandos através do SNMP ao agente, esse comando recebe o nome de *Get (*requisição*)* obtendo assim um *Get Response (*resposta*).*

O SNMP define e administra a forma de execução dos intercâmbios de informações de gerenciamento. As operações *traps* (alarmes) são definidas pelo SNMP. Os objetos de gerenciamento são armazenados na MIB (*Management Information Base*) espécie de banco de dados onde são armazenadas as informações sobre o funcionamento dos *hosts, gateways* e protocolos de comunicação (IP, TCP, ARP entre outros).

3. TOPOLOGIA DE REDES

Uma topologia de rede é uma espécie de mapa que irá indicar os segmentos de redes, verificando onde há pontos de interconexão e comunidades de usuários [1].

Uma topologia de rede serve para descrever como será o *layout* físico e também a maneira de como as informações irão trafegar na rede através dos dispositivos, com destino aos computadores.

É um dos pontos mais importantes referentes à comunicação, nos quais diferentes dispositivos se interligam, de forma a se comunicarem nas diferentes plataformas de comunicação e serviços.

Estas plataformas são conhecidas como topologias e todos os dispositivos de rede, são conhecidos como nós que compõem as características dessa rede. Esses módulos processadores utilizam protocolos de comunicação que auxiliam na organização das informações através de padrões estabelecidos de comunicação. Sua finalidade é prover um melhor arranjo de recursos e economia [2].

Uma vez conectados em rede, sua capacidade de processamento individual será compartilhada com todos os outros dispositivos, tornando esses dados acessíveis a todos os usuários conectados a rede. Há várias formas de se organizar uma rede, devido aos diferentes tipos de topologias existentes que podem ser definidas em dois tipos: fisicamente e logicamente.

A descrita fisicamente trata-se da verdadeira aparência visual da rede (*layout*) onde é analisada de forma estratégica a disposição física dos micros, a maneira exata de sua distribuição e sua finalidade no espaço. Já a logicamente analisa e descreve os fluxos de dados que trafegarão na rede, como os nós de comutação estão organizados e preparados para interagir em determinados caminhos físicos, utilizáveis entre qualquer estação que irá ser servir de ponto de comunicação, assim como o trajeto desses sinais na rede.

Mas tudo isso irá depender da arquitetura do projeto, do grau de confiabilidade esperado, sem contar no custo operacional dessa rede onde muitos fatores são considerados. Mas a maneira como os nós se comporta é um dos fatores mais importantes nesse aspecto.

3.1. TOPOLOGIA EM ANEL

Uma rede em anel consiste em estações conectadas através de um caminho fechado [1]. Não há ligação alguma entre as estações de forma direta. Para isso seria necessária uma série de repetidores, que são equipamentos que permitem uma espécie de união com redes idênticas, nas quais iria receber todos os pacotes de cada uma dessas redes interligada. As informações circulariam dentro da rede, sempre em um mesmo sentido repassando assim os sinais através dos repetidores, traçando os caminhos de um computador para o outro em um mesmo sentido.

Na figura 5 apresenta uma topologia anel, onde é possível observar as informações (representadas pelas setas) partindo de um ponto de origem e trafegando na rede em um único sentido continuo até chegar ao destinatário. Ressaltando que, os repetidores operam em um nível físico na rede.

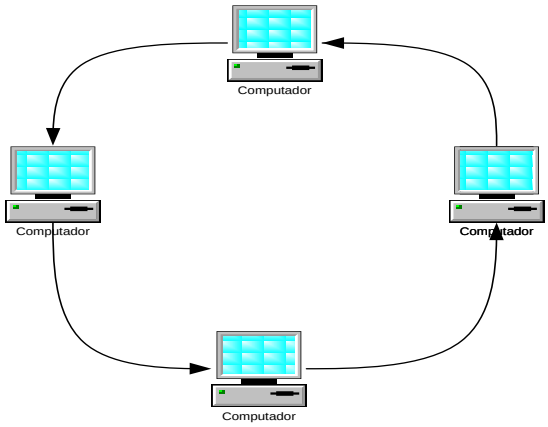

Figura 5: Topologia em anel [15]

A função específica desses repetidores consiste em verificar o endereçamento dos pacotes enviado pela estação origem, onde deverão ser analisados e verificados se o mesmo pertence à estação destino. No caso de não pertencer a essa estação, o repetidor reenvia novamente esses pacotes dentro da rede, dando continuidade no sentido de tráfego das informações no ciclo dentro do nó, onde só poderão ser retirados os pacotes pelo repetidor pertencente à estação destino. Esta topologia possui alguns aspectos negativos tais como:

a) Vulnerabilidade de erros na comunicação e entrega de dados;

b) Pouca tolerância de falhas, onde um equipamento desativado na rede pode determinar a falta de comunicação geral da rede.

3.2. TOPOLOGIA EM BARRAMENTO

A topologia em barramento é onde todos os clientes são anexados a um cabo, em geral utilizando um cabo coaxial [1]. Esta é uma topologia física utilizada por rede *Ethernet*. Nesse tipo de rede um computador é interligado ao outro por meio de cabos e conectores, na qual uma ponta é ligada na placa de rede e as outras duas são ligadas às estações vizinhas.

Conforme ilustrado na figura 6 tem-se uma topologia em barramento e suas respectivas conexões em um mesmo meio.

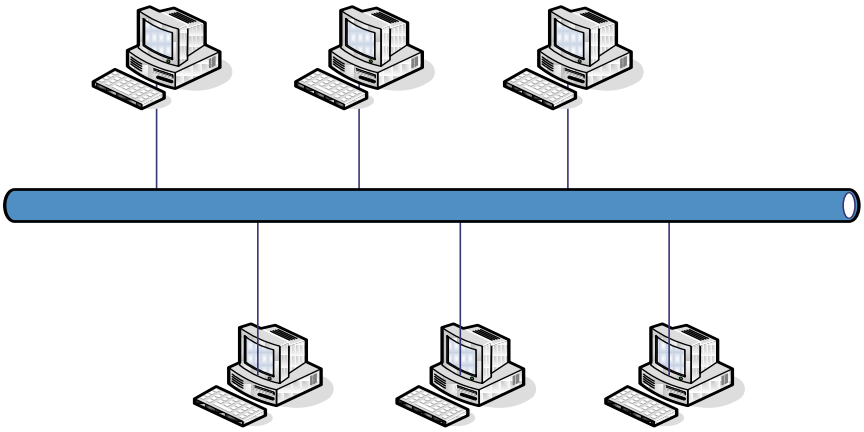

Figura 6: Topologia em barramento [15]

Nesta topologia os diversos computadores conectados à rede, compartilham o mesmo meio de comunicação. O fluxo de informações é bidirecional, ou seja, o direcionamento de tráfego das informações é indiferente, pois pode partir de qualquer ponto da rede. Esse compartilhamento de informações se dá paralelamente em tempo e frequência.

Cada equipamento conectado à rede possui um único endereço que irá indentificá-lo, sem margem de erro na rede. Os dados que trafegam na rede são detectados por todos os computadores interligados nessa rede, no entanto, essas informações só serão recebidas e interpretadas apenas pelos computadores que possuírem o endereço especificado de destino.

3.3. TOPOLOGIA EM ESTRELA

Em uma topologia estrela cada nó é interligado a um nó central (mestre) através dos quais todas as mensagens deverão passar [1]. É no caminho especificado que passarão todas as informações centrais interligadas e conectadas a cada estação da rede. Tendo por finalidade distribuir todas as informações de forma que uma estação não receba os dados que serão destinados a outra estação. Essa topologia só pode ser aplicada em pequenas redes de computadores, pois as maiorias dessas redes só possuem *hubs* com entrada de 8 a 16 portas.

Em redes maiores utiliza-se topologia em árvore, que é composta de vários *hubs* interligados através de um *switch.* Pode-se observar um exemplo de uma topologia estrela conforme figura 7.

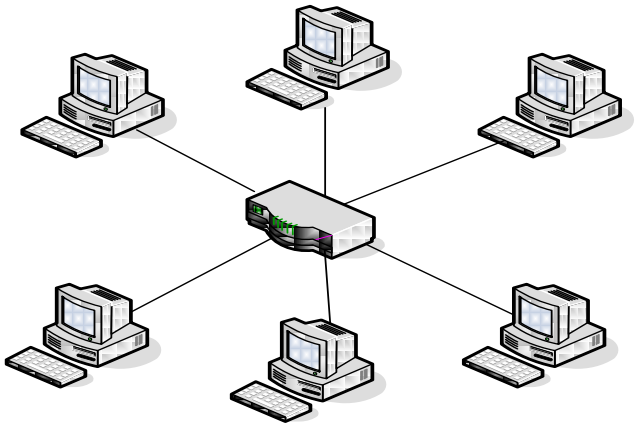

Figura 7: Topologia em estrela [15]

Na topologia estrela conforme figura 7, cada computador está ligado a um dispositivo central (*hub*) onde toda a informação recebida deverá passar pela estação central que será retransmitida as demais estações. Essa topologia é uma das mais comuns encontradas hoje em dia, pois possibilita aplicação em redes pequenas sem grandes complexidades.

3.4. TOPOLOGIA EM ÁRVORE

A topologia em árvore possui uma característica física semelhante a uma árvore. Nela existe uma barra central onde outro componente menor pode ser conectado a ela [1].

Alguns cuidados devem ser tomados nesse tipo de topologia, já que o sinal pode se espalhar bidirecionalmente, ou seja, podem tomar dois caminhos distintos. No entanto se esses caminhos estiverem protegidos, os sinais enviados têm a velocidade de transmitir e refletir os sinais de diferentes maneiras nessa rede, trabalhando com taxas de transmissão menor do que as redes de barra comum. Conforme a figura 8 pode-se observar uma rede de topologia em árvore.

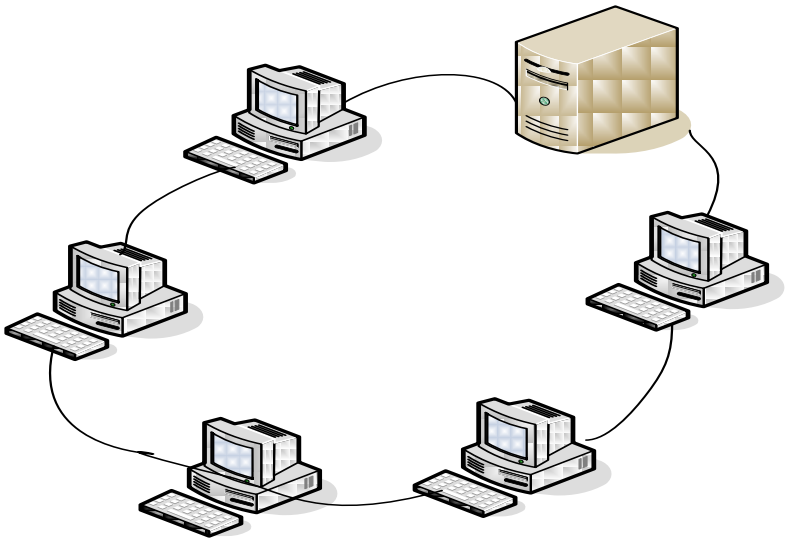

Figura 8: Topologia em árvore [16]

3.5. TOPOLOGIA HÍBRIDA

Com freqüência, em uma topologia híbrida é permitido que a área de uma rede continue em operação mesmo se o *backbone* (equipamento que interliga diversas redes num único ponto) [11].

Topologia híbrida é uma topologia de rede local, onde poderá haver vários tipos distintos de topologias na rede.

Essa topologia é usada em redes de grande porte, que se adaptam perfeitamente com as topologias da rede já utilizadas. Nesse tipo de rede, às vezes pode acontecer altas demandas de conexão e nem sempre há recursos suficientes de atendimento no momento. Para adquirir produtos de montagem na rede é necessário que o administrador dessa rede utilize os equipamentos que estão disponíveis na topologia da mesma.

Na figura 9 apresenta-se uma topologia híbrida utilizando os recursos de rede já existente. Notam-se várias ramificações de redes interligadas entre si juntamente com os nós de comutação que permite a comunicação.

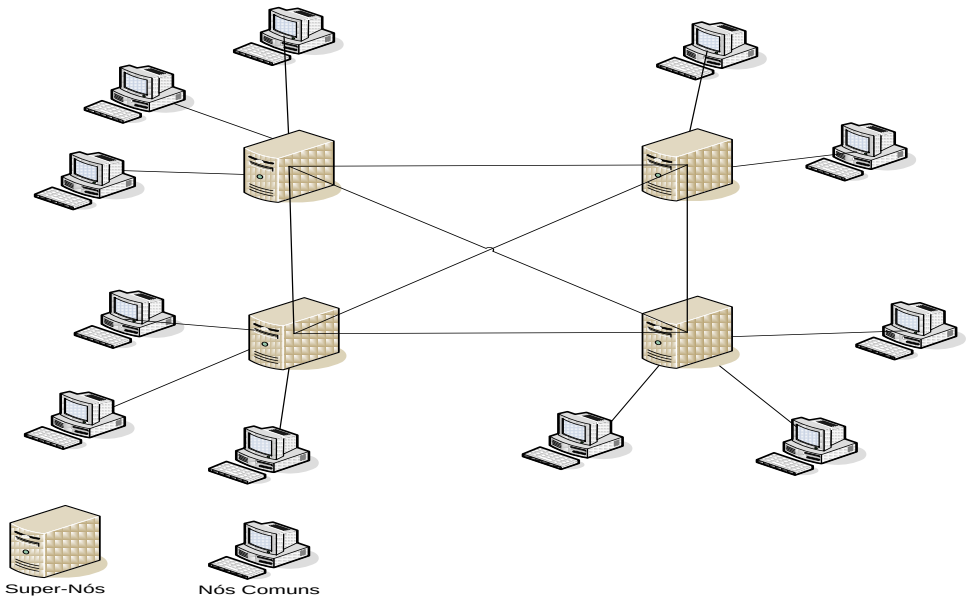

Figura 9: Topologia hibrida [17]

4. EQUIPAMENTOS DE REDES

Neste capítulo serão abordados alguns conceitos relacionados a equipamentos de redes de computadores, suas funcionalidades, características e importância em uma rede de computadores.

Os equipamentos de redes são dispositivos necessários para a montagem de uma estrutura de rede, podendo assim controlar a comunicação dos diferentes tipos de dispositivos, que também são conhecidos como elementos de rede (*Network Elements* - NE) [2].

4.1. HUB

Os *hubs* podem ser interconectados como uma forma de expansão do tamanho da rede [3]. É um aparelho que faz com que as máquinas se comuniquem, promovendo pontos de conexões físicas entre computadores interligados, ajudando os usuários a se comunicar com outras maquinas existente na mesma rede. No envio de pacotes, as informações são distribuídas para todos os componentes da rede, o *hub* tem a função de interligar os computadores, e são mais utilizados em redes locais.

O *hub* possui dispositivos que são utilizados para distribuir os cabos ligados aos computadores da rede. Os sinais dos cabos transmitem as distribuições de carga de tráfego pela rede. Em uma única rede pode existir vários *hubs.* Geralmente no mercado encontra-se aparelho com 8, 16,24 e 32 porta. A figura 10 apresenta um *hub* de 08 portas.

Figura 10: Hub 8 portas 10/100Mbps [23]

4.2. SWITCH

O *switch* é um equipamento necessário para regular os acessos aos meios físicos compartilhados [3]. É um equipamento que permite a comunicação dos computadores na rede. Diferentemente dos *hubs*, os *switch* permite que a comunicação tenha maior nível de velocidade, agindo como comutadores que aliviam assim o congestionamento de informações nas redes LAN *Ethernet* com redução de tráfego, possibilitando o aumento da largura de banda.

Possui barramentos internos para que as conexões sejam mais utilizadas pelo meio físico existente.

O *switch* pode facilmente substituir os *hubs*, uma vez que aproveita a infra-estrutura já existente da rede local *Ethernets,* outrora conectadas por *hubs.*

Os cabos dos computadores são ligados ao *switch*, com a finalidade de direcionar os dados enviados de uma máquina para a outra. Eles trocam grandes fluxos de informações de forma contínua, compartilhando meios para isso.

Já o *hub* não tem essa capacidade de direcionar informações de um computador para o outro. O *hub* envia mensagens para todas as máquinas da rede ao mesmo tempo, no recebimento das informações que foram disponibilizadas a todas as máquinas, a máquina de origem recebe essas informações e as outras maquinam ignoram essas informações que não foram a elas destinadas.

Existe *switch* com vários números de portas com: 4, 8,12, 24, 32,36 e 48... assim por diante. A figura 11 apresenta a imagem de um equipamento *switch*.

Figura 11: Switch 24 portas 10/100Mbps [24]

4.3. ROTEADOR

Todos os seguimentos da rede devem ser capazes de se comunicar com outro seguimento de rede. Essa comunicação só é possível com o uso de um roteador [17].

É através dos roteadores/ou routers que passam todas as informações adequadas para seu endereçamento, fazendo com que seus pacotes sejam encaminhados como o TCP/IP, possuindo assim um roteamento que compartilhe as rotas de endereçamento.

Os roteadores são usados para que os protocolos passem a se comunicar. Essa comunicação pode ocorrer em redes de computadores distintas, permitindo que uma rede LAN se comunique com outra rede que pertença à mesma rede LAN.

É como se essas redes fossem uma só, não levando em conta o fator da distância entre elas. Como por exemplo, *a* matriz de uma empresa pode ter suas filiais localizadas em outras cidades, fazendo uso de uma mesma rede de comunicação.

Os roteadores operam em camadas especificamente. Ele seleciona a melhor rota disponível para encaminhar seus pacotes recebidos, para que chegue com sucesso até seu destino. A figura 12 apresenta um roteador D-Link.

Figura 12: Roteador Wirelles 150/Mbps [25]

4.4. ACCESS POINT

Access Point (AP) ou em português Ponto de Acesso é um dispositivo em uma rede sem fio que realiza a interconexão entre todos os dispositivos móveis. Em geral se conecta a uma rede cabeada servindo de ponto de acesso para uma outra rede, como por exemplo a Internet. Esta ligado a camada de enlace.

Pontos de acesso Wi-Fi estão se tornando populares, muitos estabelecimentos comerciais que oferecem o acesso a internet através de um ponto de acesso como serviço ou cortesia aos clientes, tornando-se *hotspots*. Também é prático, pois a implantação de uma rede sem fio interligada por um ponto de acesso economiza o trabalho de instalar a infra-estrutura cabeada.

Vários pontos de acesso podem trabalhar em conjunto para prover um acesso em uma área maior. Esta área é subdividida em áreas menores sendo cada uma delas coberta por um ponto de acesso, provendo acesso sem interrupções ao se movimentar entre as áreas através de *roaming*. Também pode ser formada uma rede *ad hoc* onde os dispositivos móveis passam a agir intermediando o acesso dos dispositivos mais distantes ao ponto de acesso caso ele não possa alcançá-lo diretamente.

Estes pontos de acesso precisam implementar a segurança da comunicação entre eles e os dispositivos móveis que estão em contato. No caso do Wi-Fi, isso foi inicialmente tentado com o WEP (*Wired Equivalent Privacy*) que atualmente é comprometido facilmente. Surgiram então o WPA (*Wi-Fi Protected Access*) e o WPA2 que são considerados seguros caso seja utilizada uma senha. A figura 13 apresenta a imagem de um equipamento *access point*.

Figura 13: Access Point WAP4410N [26]

5. GERÊNCIA DE REDES

Abordam-se aqui conceitos de gerência de rede, seu funcionamento e arquitetura. O foco, no entanto, consistirá no estudo do gerenciamento de redes, incluindo elementos gerenciados, estações de gerência, protocolos de informações e gerência.

> *"Gerenciamento de redes inclui a disponibilização, a integração e a coordenação de elementos de hardware. Software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos de rede, de elementos para, satisfazer as exigências operacionais de desempenho e juntamente a qualidade de serviço em tempo real e a um custo razoável" (KUROSE, F. James, Lemos & Ross, W.Keith; 1995).*

Na gerência de redes é possível desempenhar várias atividades dentro de uma estrutura de rede. Não se torna necessária a limitação da área de atuação exclusiva em serviços a ser gerenciado, mas sim executar um conjunto de funções que permita tornar acessível às metas, princípios e metodologias, que mantenham a rede em perfeito funcionamento. Por essa razão o gerenciamento de redes, é vista como uma aplicação distribuída, composta de multitarefa paralelas. Seu papel consiste na comunicação e acompanhamento dos acontecimentos dos processos em rede, entre o gerente e agente.

Tem-se então uma troca de informação entre eles, com intuito de monitorar e controlar todos os dispositivos e comportamento em que a rede possa estar apresentando. As informações não só para observação, mas sim para possíveis tomadas de ações, conforme os problemas afetem de alguma maneira o desempenho da rede.

Na figura 14 apresenta uma rede constituída de três roteadores, alguns terminais e servidores. Têm-se uma rede tipo LAN em que o administrador pode se beneficiar com o uso de ferramentas de gerenciamento adequados a necessidade da rede. Esta figura ilustra uma rede simples, de tamanho pequeno, onde há troca de informação entre os dispositivos de rede, independente da sua complexidade (tamanho da estrutura). Há uma interação entre os ambientes a serem monitorados.

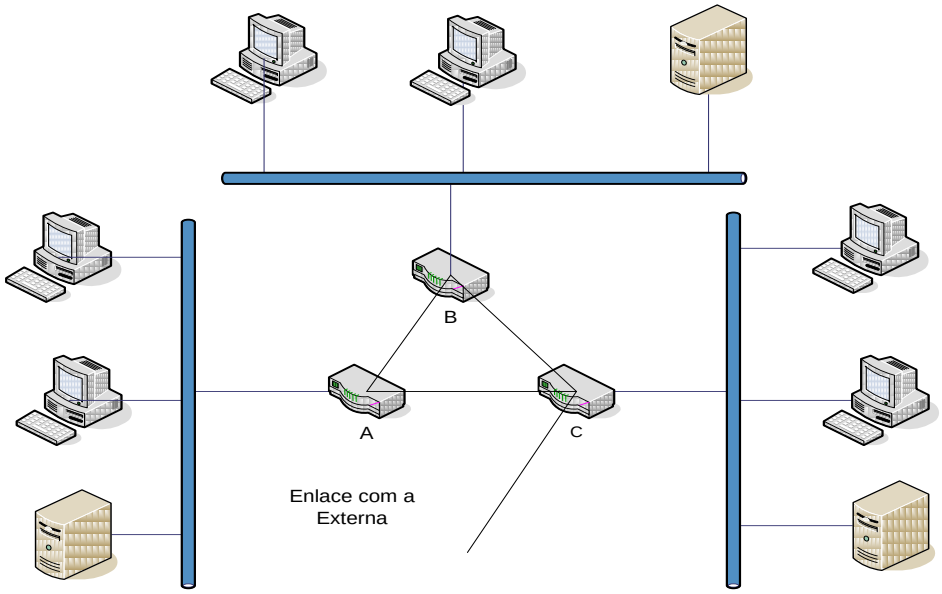

Figura 14: Gerenciamento de redes [1]

Garantir e assegurar o perfeito funcionamento dos diferentes objetos na rede é o foco principal a ser gerenciado, evitando altos índices de incidentes de falhas na rede.

Usualmente a gerência de redes se divide em três aspectos que facilitam a coordenação da rede [2]. Estes aspectos são: coleta de dados, diagnósticos e ação.

5.1. COLETA DE DADOS

Coleta de dados é um processo realizado na rede, que consiste em atividades de monitoramento dos dispositivos da rede a serem gerenciados. Observar e registrar o comportamento desses dispositivos, observando como se comportam em rede, os níveis de falhas e sua freqüência ocorrida, e se esse comportamento ocorre de forma esperada durante a sua execução. Toda informação coletada é armazenadas em arquivos logs, para possíveis medidas de ação.

5.2. DIAGNÓSTICOS

O diagnóstico consiste no tratamento e análise de todas as informações anteriormente coletadas, porém, nesse meio tempo é feito juntamente um levantamento das causas problemáticas nos recursos gerenciados. A central responsável pelo gerenciamento executa uma série de procedimentos manuais, podendo ser também feito de forma automática (por intermédio de um operador ou não) com intuito de determinar a causa do problema.

5.3. AÇÃO

Na ação, uma vez diagnosticados os problemas detectados na rede, propõem-se etapas de procedimentos a serem realizados, que resultem na solução do problema ou o controle dos recursos.

5.4. AS CINCO ÁREAS DE GERENCIAMENTO DE REDES

A International Organization for Standardization (ISO) criou um modelo de gerenciamento de rede que é útil para situar os cenários apresentados em um quadro mais estruturados [2].

Para gerenciar uma rede existem cinco áreas funcionais definidas pelo modelo OSI, onde seu objetivo é criar um modelo que estruturasse os ambientes de funcionamento da rede em uma estrutura lógica e mais organizada. Um ponto ativo direcionado para uma solução mais ágil no setor de gerenciamento. Essas cinco áreas são:

5.4.1. Gerenciamento de Falhas

Na área de gerenciamento de falhas o objetivo é detectar se há falhas de operação dos dispositivos (por exemplo, roteadores, hospedeiros e cabos) na rede [7].

Tem como meta medir, analisar e quantificar controlando assim seu desempenho assegurando o funcionamento da rede e identificando quais são áreas mais críticas para uma possível intervenção. Há então uma coleta dos acontecimentos apresentados na rede, registrando - os para que seja possível ser acompanhado juntamente com a execução de teste para análise de resultado. Um mau gerenciamento resultará em má utilização de dispositivos afetando diretamente as outras quatro áreas de gerenciamento já que todas elas têm relações entre si. Exemplo de gerenciamento de falhas: perdas de pacotes de dados no funcionamento da rede.

5.4.2. Gerenciamento de Desempenho

Na área de gerenciamento de desempenho é onde se controla todo o comportamento e desempenho da rede. Monitorando todas as atividades realizadas em rede, os desempenhos de todos os dispositivos relacionados ao seu funcionamento [6].

Durante o processo ocorrerá monitoramento diário da rede, já que é possível ter as informações de toda a rede, devido o seu mapeamento e controle de dispositivos podendo então manter um registro desses acontecimentos.

Possíveis soluções dos problemas poderão ser tomadas ou direcionadas a outra área relacionada à do desempenho, nesse caso seria na detecção de falhas, já que ambas estão relacionadas.

Observando que há uma diferença importante entre o gerenciamento de desempenho, em relação ao gerenciamento de falhas. O gerenciamento de falhas é voltado para a solução imediata das falhas na rede (falha de funcionamento de roteadores, problemas com hardware e software dos dispositivos).

Já o gerenciamento de desempenho é uma área mais ampla que mede o desempenho dos equipamentos mediante a quantidade de serviços podendo ocasionar lentidão no fluxo de informações, acarretando congestionamento de informação na rede, ocasionando falhas. Já que o protocolo SNMP (*Simple Network Management Protocol*) tem um papel de grande importância no gerenciamento de falhas.

Exemplo de gerenciamento de desempenho: Lentidão na rede, devido ao alto fluxo de informação, onde equipamentos não suportam elevadas quantidades de informações.

5.4.3. Gerenciamento de Configuração

Na área do Gerenciamento de configuração de rede é possível acompanhar as relações e interações dos componentes em rede, permitindo que os administradores saibam quais dispositivos fazem parte dessa rede e quais são as suas configurações. Tem-se então um sistema ágil na rede que sempre se modifica, possibilitando o acompanhamento dos componentes de configurações [9].

O nível apropriado para as relações, os requisitos estabelecidos de funcionamento, status desses componentes, execução de alterações do sistema com isolamento de erros e falhas, possibilitando mandar avisos de erros de execução para o administrador, registrando-os para possível controle e análise. Uma gerência de configuração deficiente reflete diretamente no gerenciamento de desempenho e no gerenciamento de falha, onde resultará na falha do planejamento e na área de gerenciamento de contabilização. Exemplo de gerenciamento de configuração: equipamentos com configurações desatualizadas ou configurações incorretas [2].

5.4.4. Gerenciamento de Contabilização

Na área do gerenciamento de contabilização, mantém-se um limite pré - definidos de consumo direcionando essa necessidade ás áreas mais importantes e com maior índice de utilização, que possa ser controlado e direcionado as demais áreas especificando o registro de controle de acesso de usuários e dispositivos [2].

Têm-se então, uma melhor definição e distribuição de recursos que acarretará em um trabalho bem planejado, onde as tarifas serão aplicadas aos recursos de rede com alguns arquivos remotos e serviços de telecomunicação, melhorando assim os serviços prestados com maior nível de qualidade e planejamento. Exemplo de gerenciamento de contabilização: é a identificação dos

departamentos ou setores que utilizam mais os recursos da rede, ou seja, um departamento que utiliza mais a impressora que outro, deve ter prioridade ou o caso de acrescentar mais impressoras no local [6].

5.4.5. Gerenciamento de Segurança

Na área de gerenciamento de segurança, têm-se o processo de proteção e distribuição das informações em seus eventos, registrando-o de forma relativa à segurança e garantindo as aplicações de políticas de segurança.

Algumas ferramentas (como os *firewalls* que controlam e monitoram pontos externos de acesso à rede) de gerenciamento de segurança autorizam o administrador a ter algum domínio nas atividades de gerenciamento [7].

Nas redes de computadores tem-se um arranjo bem complexo nas conexões do sistema de software de protocolos, podendo tornar-se uma rede mais completa no seu desenvolvimento de gerenciamento, para que seus componentes desenvolvam na sua complexidade física e técnica. Exemplo de gerenciamento de segurança: identificar os acessos na rede, elaboração de permissões, onde é definido o acesso de cada usuário na rede [6].

5.5. ARQUITETURA DE GERENCIAMENTO DE REDES

Na sessão anterior foram citados alguns aspectos e funções, em que gerenciamento de redes é responsável e capaz de realizar dentro da estrutura de uma rede o que torna bem mais fácil caracterizar e dividir essas funções em uma estrutura. Na figura 15 tem-se uma arquitetura de gerenciamento de rede e seus vários componentes, tornando-se mais fácil a compreensão e visualização da arquitetura de uma rede [2].

Arquitetura de Gerência de rede é um conjunto de camadas e protocolos que atuam entre si, em um meio lógico de funcionamento das informações e solicitações dos dados nessa arquitetura, permitindo assim a troca dessas informações e interação dos componentes [7].

Neste tipo de arquitetura algumas funcionalidades de gerenciamento ocorrem no setor gerenciador, onde contém informações suficientes que permita o

desenvolvimento necessário de software e hardware em cada uma dessas camadas. É definida pelo alto índice na demanda no mercado de serviços de TI.

Conforme figura 15, há 3 tipos de componentes que tem função primordial em uma arquitetura de gerenciamento de rede:

1º. É uma entidade gerenciadora (onde contém todas as informações de controle nessa arquitetura),

2º. São os dispositivos gerenciados (tipos de dispositivos ou equipamentos a serem gerenciados),

3º. Seriam os protocolos de gerenciamento (permitem a transmissão de relatórios, dados padronizados e comunicação).

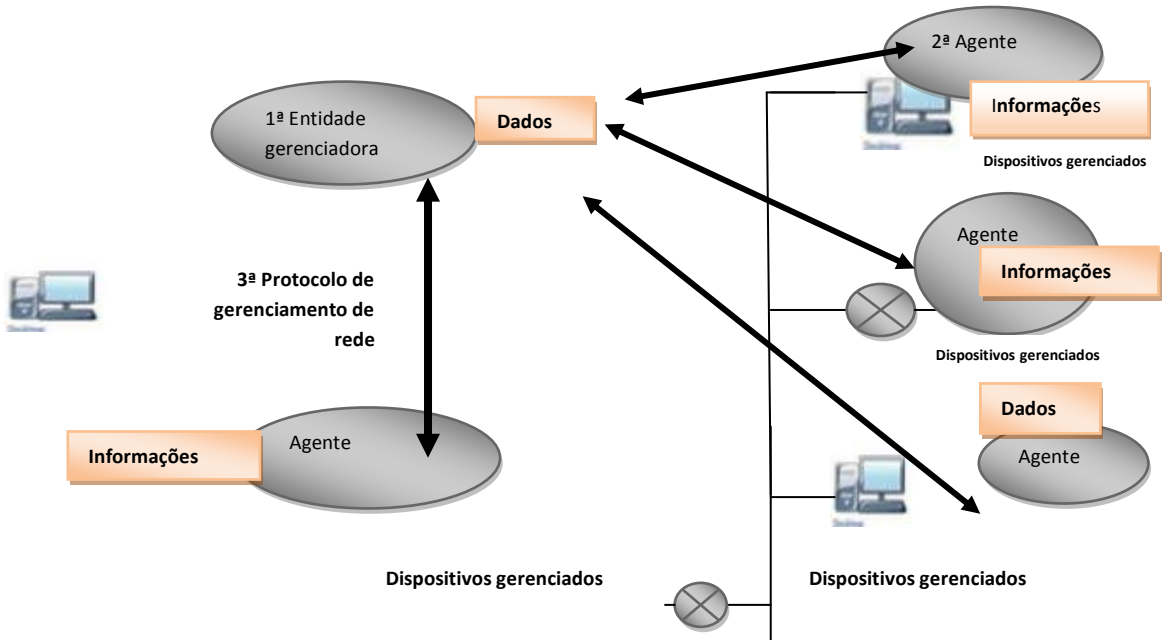

Figura 15: Arquitetura de gerenciamento [1]

5.6. ENTIDADE GERENCIADORA

Entidade gerenciadora são aplicações onde geralmente há pessoas (com recursos manuais) envolvidas nos processos de execução [9]. Nesta fase há responsáveis em executar as funções no circuito das operações, que são executadas de uma central de gerência de redes chama NOC. A NOC é o núcleo vivo das atividades de gerenciamento que tem por responsabilidade controlar e processar a coleta de dados, e também em analisar e/ou representar essas informações de gerenciamento de rede.

5.7. DISPOSITIVOS GERENCIADOS

Dispositivos gerenciados são todos os equipamentos de redes existentes na rede gerenciada, incluindo também os softwares relacionados aos dispositivos que reside em uma estação gerenciada [6].

É o conjunto de equipamentos que serão monitorados dentro de todo o contexto, sendo que através deles serão acompanhados os padrões de funcionamentos e parâmetros de configurações para os dispositivos de hardware.

Todas essas informações são coletadas e direcionadas para uma base de informações denominadas MIB (*Managemet Information Base-MIB*).

5.8. PROTOCOLO DE GERENCIAMENTO DE REDE

Protocolo de Gerenciamento de rede é o fornecimento de meios e mecanismo de comunicação entre o agente e gerente. Eles trocam informações usando protocolos de gerenciamento, onde são incluídas operações de monitoramento e controle de equipamentos a eles ligados.

As informações serão enviadas através do roteador que está na rede, informando erros que estão acontecendo nos fluxos durante o processo de gerenciamento**.**

5.9. GERENTE

O gerente é um computador conectado a rede que executa um conjunto de *softwares* de protocolos de gerenciamento, requisitando informações do agente [7].

Ele então faz a coleta de todas as informações junto ao agente e depois as processa. Se for necessário solicita aos sistemas agentes que executem operações de gerenciamento a fim de controlar o funcionamento dos objetos gerenciados.

5.10. AGENTE

O agente é um software que roda em um recurso de elementos ou sistemas gerenciados exportados de uma base de dados MIB (*Management Information Base*) [5].

Passa então a realizar operações de gerenciamento sobre os dispositivos gerenciados, atendendo requisições enviadas pelo gerente. Contudo o agente envia ao gerente notificações que serão geradas pelos objetos gerenciados, ou notificações sobre ocorrência de falhas no funcionamento desses dispositivos**.**

5.11. MIB (*MANAGEMENT INFORMATION BASE*)

A MIB é uma base de dados de gerenciamento, em que estão alocadas todas as informações decorrentes da rede. São responsáveis por armazenar todas essas informações gerenciais das estações de trabalho e ativos de redes [7].

Com base nos dados da MIB é possível visualizar toda parte operacional do equipamento, se existe ou não perdas de pacotes, erros de transmissões, índice de tráfego e muitos outros dados que contribuem para o gerenciamento de rede. Para se coletar os dados relacionados à MIB uma estação gerente utiliza protocolos SNMP citado no capitulo 2. Todos os equipamentos possuem uma MIB com dados de fabricante relacionados a máquina.

5.12. FERRAMENTAS DE INSPEÇÃO E MONITORAMENTO DE REDES

São equipamentos com softwares que é utilizado para monitoramento de redes *LAN*. Trata-se de algo muito flexível, que permite o monitoramento de um trabalho para os equipamentos e serviços, gerando um relatório de alerta que pode ser enviado por e-mail ou através de mensagem instantânea ao administrador da rede [4]. Também são utilizados para armazenamentos de dados que foram coletados durante todo o processo. O monitoramento envia um alerta sonoro, ou envio de mensagens de *traps* (envio de mensagens

instantâneas), ou seja, notificação que é enviada sempre que alguns problemas atinjam a rede de acordo com as especificações. Estas notificações são enviadas pelo protocolo SNMP para que se tenha um controle durante o processo.

Quando algum equipamento não estiver funcionando corretamente, ele possui uma independência quando se trata de falha no gerente, não parando com os dados até volta à operação.

O monitoramento de rede permite também o acompanhamento em algumas redes distintas que são interligadas entre elas, permitindo a comunicação no envio de dados e pacotes. Pode-se observar uma estação de monitoramento de rede na figura 16.

Figura 16: Estação de monitoramento de redes [20]

5.13. CONFIGURANDO UM SISTEMA DE GERENCIAMENTO

> ***"****Assim a arquitetura de gerenciamento de redes da internet é modular por projeto, com uma linguagem de definição de dados independente de protocolos, e um protocolo indenpedente de MIBs. Sendo que essa arquitetura modular foi primeiramente disponibilizada para facilitar a transição de um gerenciamento de redes baseado em SNMP para uma estrutura de gerenciamento de rede que está sendo desenvolvida pela ISO e que era arquitetura de gerenciamento que concorreria com o SNMP quando foi projetado. Ou seja, uma transição que nunca aconteceu." (KUROSE, F. James, Lemos & Ross, W.Keith; 1995).*

Os sistemas de gerenciamento de redes devem receber configurações dos administradores para que monitorem e coletem os dados de forma adequada. Considerando os tipos de pacote, a maneira como os dados serão coletados e definição do tempo de resposta para cada verificação na rede. Existem

basicamente algumas formas para determinar cada tipo de dados estatísticos que vão ser coletados durante o andamento do processo. Para cada estatísticas existem algumas normas como: O intervalo e a medição, que são definidos por tabelas de controles e resultado do monitoramento.

Algumas estações de gerenciamento exigem estatísticas de dados na rede, para que o gerente possa configurar os pedidos pela tabela de controle. Para cada tabela existe uma identificação como se fosse um RA, que será usado para ter acesso aos resultados da tabela, podendo surgir alguns problemas, tais como:

- Muitos pedidos que tendam a se encontrar com outros gerentes, podendo sobrecarregar a capacidade do monitor numa única estação do gerente.
- Podem ser alocados vários recursos, podendo mantê-los sobrecarregados por algum tempo.

5.13.1. Informações de Gerência de Redes

A estação gerente pode receber alerta de problemas através de protocolos RMON (*Remote Network Monitoring*) que é uma extensão do SNMP, onde acrescenta funções de gerenciamento da rede oferecendo informações vitais para gerenciamento [2].

Com o agente RMON é possível criar interfaces que permitem o recebimento de alertas, para que o gerente possa tomar medidas e ações pró-ativas, resultando em uma rede com um índice menor de falhas e evitar problemas futuros com as informações coletadas através das MIB sobre tráfego e desempenho. *O* RMON utiliza de alertas chamados *traps* (mensagens que identificam anormalidade na rede). Tem como vantagem o uso do RMOM*,* que independente da estaco gerente está ligada e operando, o RMON permanece coletando informações gerenciais da rede.

Neste capítulo foram apresentados assuntos relacionados à definição de gerência de redes de computadores e seus aspectos funcionais juntamente com a sua arquitetura. Estudaram-se os aspectos das cinco áreas de gerenciamento e sua arquitetura. Foram apresentados conceitos ferramenta de inspeções monitoramento de redes e a configuração de sistema, juntamente com as informações de gerencia de redes.

6. MONITORAMENTO DE REDES

Este capítulo apresenta ferramentas de monitoramento de redes, nos próximos tópicos, serão relacionadas duas ferramentas de monitoramento de rede e ativos de rede. As ferramentas são: NAGIOS e DUDE.

Neste capítulo também serão apresentadas às características de cada ferramenta que as torna distintas uma das outras, visto que cada uma possui um serviço diferenciado, mas com um mesmo objetivo de monitorar e gerenciar redes de computadores.

Para um monitoramento correto da rede, é necessário ter todos os serviços configurados, estabelecendo comunicação com as estações gerentes. Alguns desses serviços foram relacionados nos capítulos anteriores, como por exemplo: SNMP, MIB entre outros. Com todos estes serviços é preciso ferramentas que tratem todas as informações gerenciais da rede disponível, e que organize de um modo que o gerente possa ter ações gerenciais de prevenção, manutenção, projetos estratégicos de mudanças na rede entre outros.

Estas ferramentas, denominadas “ferramentas de monitoramento de rede” possuem interfaces customizadas ao cliente, de um modo facilitado para o gerente visualizar, monitorar, em alguns casos, dependendo da ferramenta utilizada, pode-se ter um acompanhamento em tempo real. Algumas ferramentas possuem interfaces Web capazes de disponibilizar dados estatísticos, com gerações de gráficos para adquirir informações gerenciais, de um modo organizado, contribuindo assim essencialmente em uma tomada de decisões ágil, preventiva e corretiva na rede.

Cada ferramenta possui um foco diferenciado de gerenciamento, algumas semelhantes e outras mais complementadas e diversificadas. Exemplificando algumas ferramentas que são caracterizadas pela capacidade de gerarem alertas em tempo real, com planos de ações para estabelecer um trabalho pró-ativo, que resulte em uma rede com menor índice de falhas e com disponibilidade de rede elevada.

Existem ferramentas que auxiliam o gerente a obter informações do tráfego da rede de um modo gráfico, onde ilustra os problemas de comunicação e utilização do link de dados.

6.1. NAGIOS

O Nagios é uma ferramenta de monitoramento de rede com ativos de rede pertencente a determinada rede. Utiliza-se a ferramenta Nagios para automatizar *os acontecimentos* de rotina, verificando e monitorando serviços do tipo SMTP, POP3, HTTP, NNTP, ICMP, SNMP e equipamentos pertencentes uma determinada rede. Esta característica por sua vez, proporciona ao administrador da rede obter ações de manutenção preventiva e ativa, estabelecendo um funcionamento de rede com eficiência e evitando quedas na comunicação que possa vir a prejudicar os fluxos de informação na rede.

O Nagios é um *software* livre, sem custo de aquisição da ferramenta. Possui interface web onde os grupos de monitoramento e gerenciamento da rede têm a possibilidade de customizar e otimizar sua interface, de acordo com as suas necessidades e seu fluxo de trabalho.

A vantagem de utilização dessa ferramenta é exatamente essa, a possibilidade de alteração em seu código, pois o mesmo é aberto, livre para ser feito as alterações necessárias em seu código.

Com o uso do Nagios têm-se níveis e tipos de alertas diferentes, relacionados à coleta das informações em relação ao cliente, onde seus alertas são: *Ok*, *Unknown, Warning* e *Critical.* Os alertas do Nagios são coletados por conexão fim-a-fim.

A gestão de monitoramento do Nagios possibilita ao usuário, definir subgrupos de trabalho e determinar ações para cada subgrupo. Os alertas gerados pela ferramenta também podem ser definidos e configurados para os subgrupos que irá pertencer ao monitoramento do Nagios, ou seja, para cada subgrupo, tem-se um alerta de equipamento diferente, exemplo: o Grupo que monitores servidores irá receber somente alertas relacionados a quedas e problemas de servidores. E o segundo grupo monitora o funcionamento de equipamentos, irão receber somente alertas relacionados a esses equipamentos.

Pode-se afirmar que a ferramenta Nagios possui como característica principal, sua capacidade de promover alertas as estações gerentes, proporcionando ao gerente uma visão geral e mais abrangente da situação, e tipos de problemas que estão ocorrendo na rede.

Este serviço contribui ao gerente os aspectos relacionados à tomada de ações imediatas em relação à manutenção e cuidados com a rede.

Os alertas gerados pelo Nagios são enviados e recebidos em tempo real, através das varreduras das informações feitas constantemente. Estes alertas podem ser configurados para serem recebidos através de e-mail, sinais sonoros na estação gerente, ou até mesmo em aparelhos móvel PDAs *(Personal Digital assistants)* e celulares.

Conforme figura 17 segue o exemplo do uso real do Nagios durante um monitoramento e sua interface Web. O conteúdo exibido na página relaciona-se a problemas gerais que estão ocorrendo, e são registrados pela ferramenta em tempo real na rede, facilitando assim a vida do gerente responsável pelo acompanhamento e monitoramento dessas informações na rede.

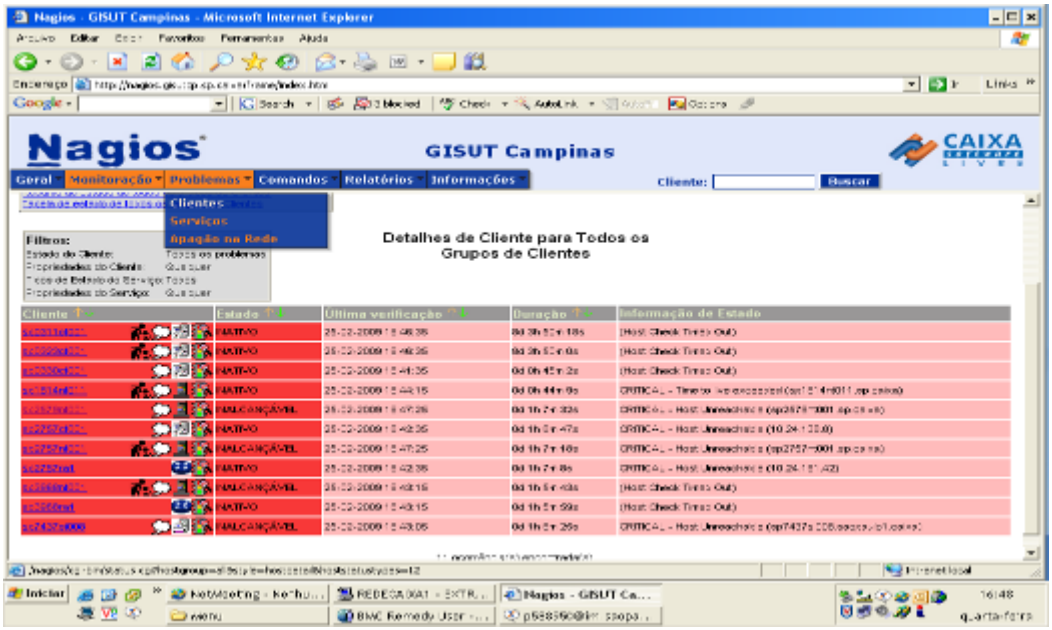

Figura 17: Monitoramento do nagios via web.

Fonte: imagem da tela de monitoramento cedida pela empresa Caixa Econômica Federal

6.1.1. Nagios em Funcionamento na Virtualização

Nas figuras 18 e 19 são exibidas as mensagens de monitorameto com o equipamento em uso normal e com uma sobre carga dada ao equipamento.

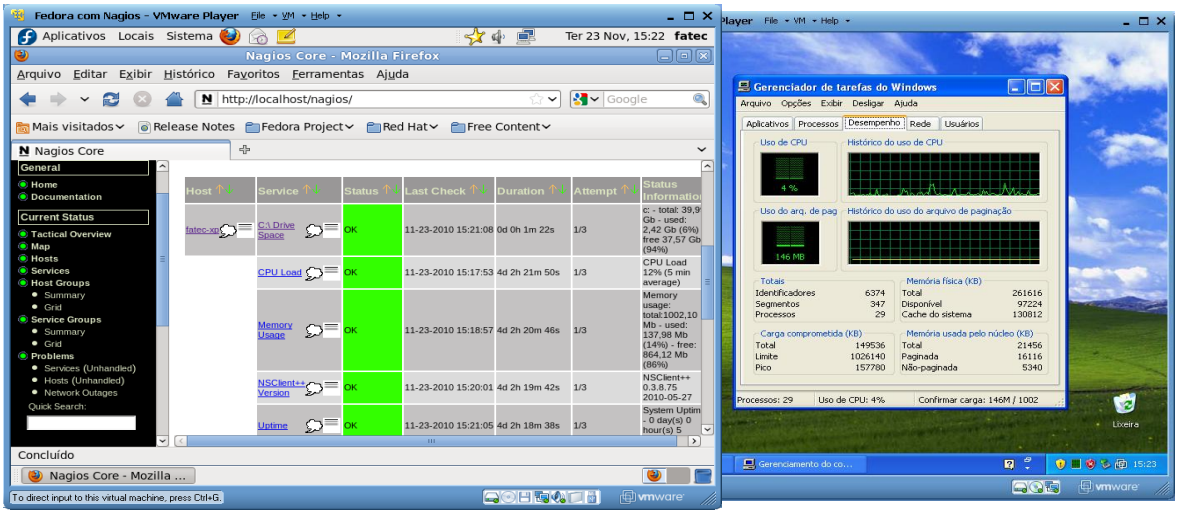

Figura 18: Fedora com servidor nagios monitorando um Windows XP

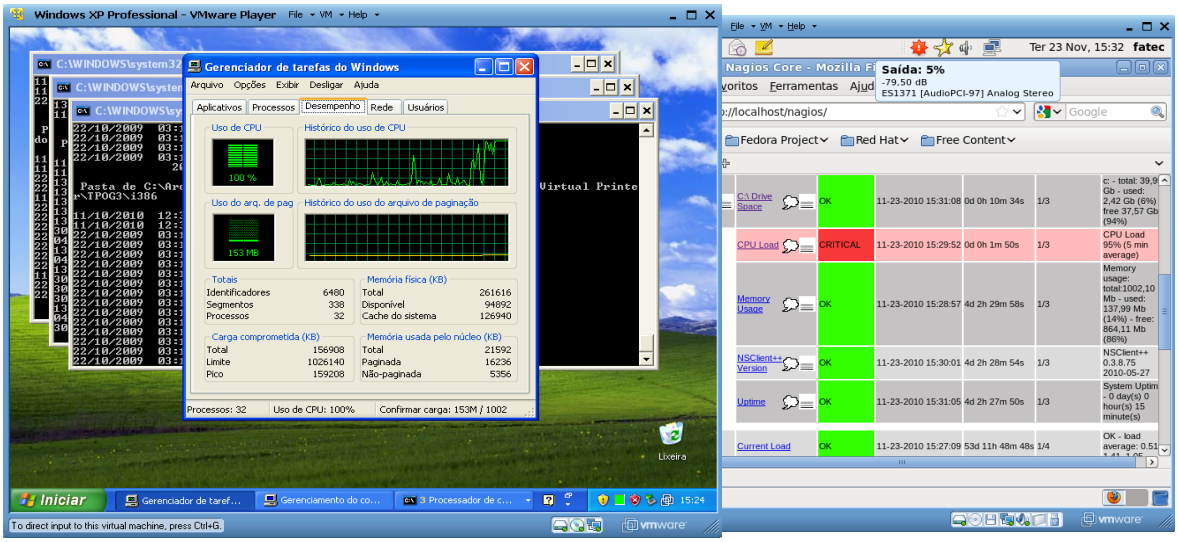

Figura 19: Nagios monitorando uma sobrecarga de CPU no Windows XP

6.1.2. Processo de Instalação do Nagios no Linux

1º Criação da conta

- Se autentique como root:

  su –

- Crie uma conta de usuário chamada nagios e atribua uma senha:

  /usr/sbin/useradd –m nagios

  passwd nagios

- Crie um grupo chamado nagcmd para permitir que comandos externos enviados pelo navegador sejam submetidos ao nagios. O grupo nagcmd deve conter os usuários nagios e apache:

  /usr/sbin/groupadd nagcmd

  /usr/sbin/usermod -a -G nagcmd nagios

  /usr/sbin/usermod -a -G nagcmd apache

2º Download do nagios e do plugin para linux

- Crie um diretório chamado download no seu perfil:

  mkdir ~/downloads

- Acesse o diretório:

  cd ~/downloads

- Os links abaixo são versões da aplicação, utilizados na instalação do aplicativo:

  wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-3.2.3.tar.gz

  wget http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.11.tar.gz

3º Compilação e instalação do nagios

- Extrai os arquivos de instalação e acesse a pasta com o conteúdo extraído:

  tar xzf nagios-3.2.3.tar.gz

  cd nagios-3.2.3

- Execute o script de configuração, passando o nome do grupo que você criou anteriormente como parâmetro:

```
./configure --with-command-group=nagcmd
```

- Compile o código fonte do nagios:

```
make all
```

- Instale os binaries, script init, scripts de exemplo de configuração e atribua a permissão para aceitar comandos externos:

```
make install
make install-init
make install-config
make install-commandmode
```

4º Customizando as configurações

- Os arquivos de configuração foram instalados em /usr/local/nagios/etc. Estes exemplos já contem as informações necessárias para executar com sucesso o servidor e monitorar os recursos do servidor. A única configuração necessária é alterar o email de envio dos alertas de monitoramento. Para isto basta modificar esta informação dentro do arquivo /usr/local/nagios/etc/objects/contacts.cfg:

```
vi /usr/local/nagios/etc/objects/contacts.cfg
```

5º Configurar a Interface Web

- Instale o arquivo de configuração do nagios no diretório do apache conf.d:

```
make install-webconf
```

- Crie a conta nagiosadmin para acessar a interface web:

```
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

- Reinicie o servidor apache para que as alterações se tornem efetivas:

```
service httpd restart
```

6º Compilar e instalar o plugin do nagios

- Acesse a pasta onde você baixou o plugin, o extraia e acesse a pasta criada:

```
cd ~/downloads
```

```
tar xzf nagios-plugins-1.4.11.tar.gz
cd nagios-plugins-1.4.11
```

- Compile e instale o plugin:

```
./configure --with-nagios-user=nagios --with-nagios-group=nagios
make
make install
```

7º Inicie o Nagios:

- Adicione o nagios na lista de serviços que são carregados automaticamente quando o sistema operacional é iniciado:

```
chkconfig --add nagios
chkconfig nagios on
```

- Verifique a integridade dos arquivos de configuração:

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

- Caso não seja apresentado algum erro inicie o serviço:

```
service nagios start
```

8º Modifique as configurações do SELinux

- O fedora vem por padrão com o módulo de segurança SELinux (*Security Enhanced Linux*) habilitado, o que pode gerar erros como "*Internal Server Error*" quando o usuário tentar acessar as configurações web da ferramenta. Foi escolhido, para evitar qualquer tipo de conflito, desabilitar o SELinux. Para isto basta editar o arquivo /etc/selinux/config:

```
vi /etc/selinux/config
```

9ª Acesso a interface

- Para realizar o acesso basta abrir um navegador no servidor da aplicação e digitar o endereço HTTP://localhost/nagios inserindo posteriormente o usuário e senha cadastrados no apache. Como o Nagios realiza o monitoramento de serviços e atributos de máquinas, utilizaremos como exemplo o sistema operacional Windows.

6.1.3. Processo de Instalação do Nagios no Windows

1º Instalação agente

- O primeiro passo para você configurar o monitor do nagios em máquinas Windows é habilitar este recurso no servidor nagios. Obs.: este processo é realizado apenas uma vez.
- Como root, edite o arquivo de configuração do nagios:

  vi /usr/local/nagios/etc/nagios.cfg
- Encontre a linha abaixo e remova o sinal de Sharp (#) para habilitar o monitoramente:

  #cfg_file=/usr/local/nagios/etc/objects/windows.cfg
- Salve o arquivo.
- Com este procedimento você habilita o nagios a procurar dentro do arquivo /usr/local/nagios/etc/objects/windows.cfg por estações e objetos Windows que devem ser monitorados.
- Antes de realizar o monitoramento é necessário acessar o site http://sourceforge.net/projects/nscplus e realizar o download do aplicativo NSClient++.

2º Configuração do Nagios

- Agora é necessário definir quais são os objetos a serem monitorados em cada máquina Windows. Abaixo será demonstrado como foi realizado a configuração da estação Windows utilizada no projeto.
- Abra o arquivo de configuração das estações Windows:

  vi /usr/local/nagios/etc/objects/windows.cfg
- O primeiro passo é definir qual será os valores dos campos host_name, alias e address. “Logo após cada um dos campos, separados pelo caractere de ‘;’ constará a explicação do atributo”:

```
define host
{
use windows-server ; Herda valores padrões vindos de um template
host_name    Windows-XP ; Este é o nome da estação monitorada
```

alias Estação Windows XP ; Aqui pode ser inserido um comentário sobre a estação

address 192.168.1.2 ; Este é o endereço IP da estação

}

- Após esta configuração basta definir quais serão os objetos a serem monitorados.
- Foi realizado o monitoramento dos seguintes objetos (em ordem): Versão da aplicação NSClient, Tempo que a estação esta ligada, Carga da CPU, Uso da Memória, Espaço em Disco. Abaixo segue os parâmetros de configurações:

```
define service
{
use generic-service ; Carrega o template
host_name Windows-XP ; estação windows
service_description NSClient++ Version ; Descrição do objeto
check_command     check_nt!CLIENTVERSION ; commando check_nt que realiza o monitoramento do objeto
}
define service
{
use generic-service
host_name Windows-XP
service_description Uptime
check_command     check_nt!UPTIME
}
define service
{
use generic-service
host_name Windows-XP
service_description CPU Load
check_command     check_nt!CPULOAD!-l 5,80,90
}
define service
{
use generic-service
```

```
host_name Windows-XP
service_description Memory Usage
check_command     check_nt!MEMUSE!-w 80 -c 90
}
define service
{
use generic-service
host_name Windows-XP
service_description C:\ Drive Space
check_command     check_nt!USEDDISKSPACE!-l c -w 80 -c 90
}
```

3º Reinicie o nagios

- Após a configuração basta verificar a existência de algum erro no arquivo e caso não encontre reiniciar o serviço do nagios.

6.2. THE DUDE

O The Dude é uma ferramenta de monitoramento de rede, onde seu foco é facilitar as rotinas de trabalho do administrador. O The Dude foi desenvolvido pela empresa MikroTik [10]. A instalação do The Dude é simples e suas configurações são de simples customização, pois o *software* busca os componentes de rede automaticamente.

Após a instalação do aplicativo na estação de trabalho gerente onde vão ser monitorados os periféricos pertencentes à rede, o The Dude realiza o trabalho de busca automaticamente dos equipamentos e serviços encontrados na rede. O funcionamento da busca na rede é realizado através de serviços e protocolos como, SNMP, IP, NETBIOS e DNS. O mapeamento realizado pelo The Dude possibilita identificação através de informações contidas nas MIBs. As MIBs contêm as informações do fabricante, versão de software e muitas outras informações adicionais contidas em cada equipamento.

Após todo o trabalho de identificação da rede realizado pela ferramenta de monitoramento, o The Dude cria um esqueleto graficamente visível de toda rede, facilitando em muito as tarefas de monitoramento do administrador.

Na figura 20 tem se uma tela do Dude em funcionamento, já com o mapeamento de toda rede definida e identificada. O Dude identifica os IP das máquinas no ar. Reler para ver se ficou bom o comentário da figura.

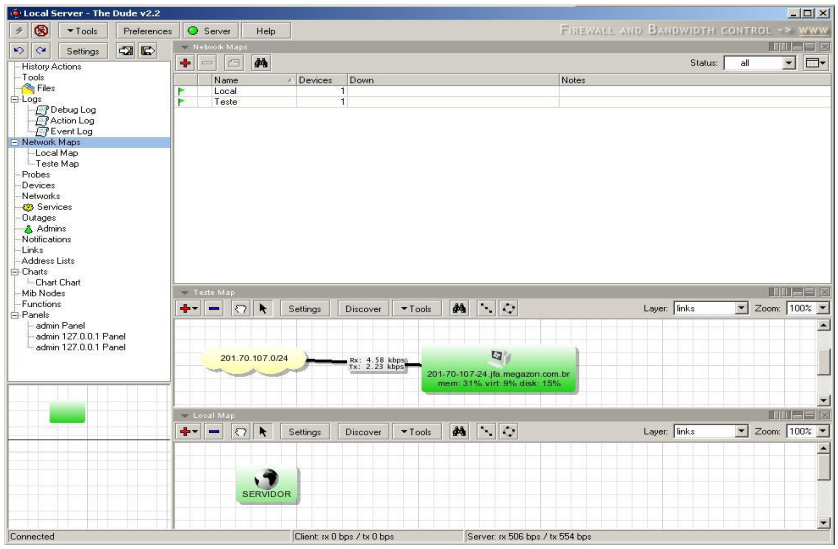

Figura 20: Monitoramento com the dude

As configurações das visualizações gráficas da ferramenta são customizadas de acordo com a preferência do administrador. É possível inserir informações adicionais sobre os equipamentos onde o administrador possa configurar a velocidade de cada enlace, podendo posicionar as figuras conforme suas necessidades.

Com essa ferramenta o administrador possui um monitoramento em tempo real, trazendo informações recentes da situação da rede, possibilitando um trabalho de monitoramento eficiente, em que o índice de disponibilidade da rede é mais elevado e com menos falhas de comunicação. Através do monitoramento realizado nos serviços da rede o The Dude captura informações sobre o link de dados, perda de pacotes, problemas de comunicação em determinados enlaces.

Essa ferramenta possui uma interface Web sendo possível a outros usuários administradores visualizar toda rede, porem, o mesmo não vem ativo em sua instalação padrão, mas basta ativá-lo e possuir um servidor Web para hospedá-lo.

É possível observar na figura 21 o The Dude em uma interface Web.

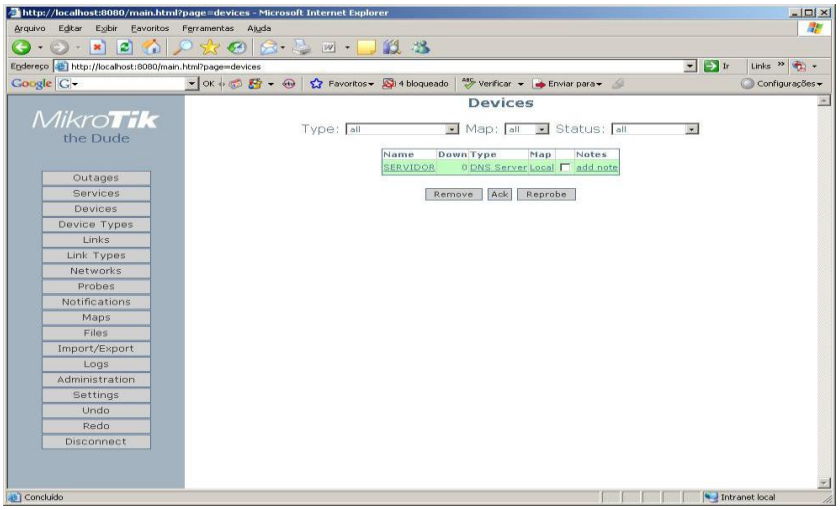

Figura 21: Monitoramento the dude via web

6.2.1. Instalação do Dude

O Dude tem a capacidade de 4,53 MB e tem como finalidade executar um scaneamento nos dispositivos na rede. Sua função é monitorar as máquinas mapeadas, coletando os dados disponíveis em rede. A taxa de avaliação e monitoramento na instalação foi de 5 dias.

Nas figuras 22, 23 e 24 ilustram os equipamentos sendo mapeados pela ferramenta DUDE, em que se podem observar as máquinas que estão inativas representadas pela cor vermelha, os equipamentos funcionando ativamente na rede na cor verde, os servidores ativos representados pela cor laranja, mas que não são utilizados. O Dude também diferencia os tipos de equipamentos, como: servidores máquinas, *hub, switch* entre outros.

Todas as máquinas na rede foram mapeadas pelo Dude de forma que cada máquina é diferenciada por cores. O Dude passa uma descrição total das máquinas, o que torna fácil a visualização e compreensão dos dados.

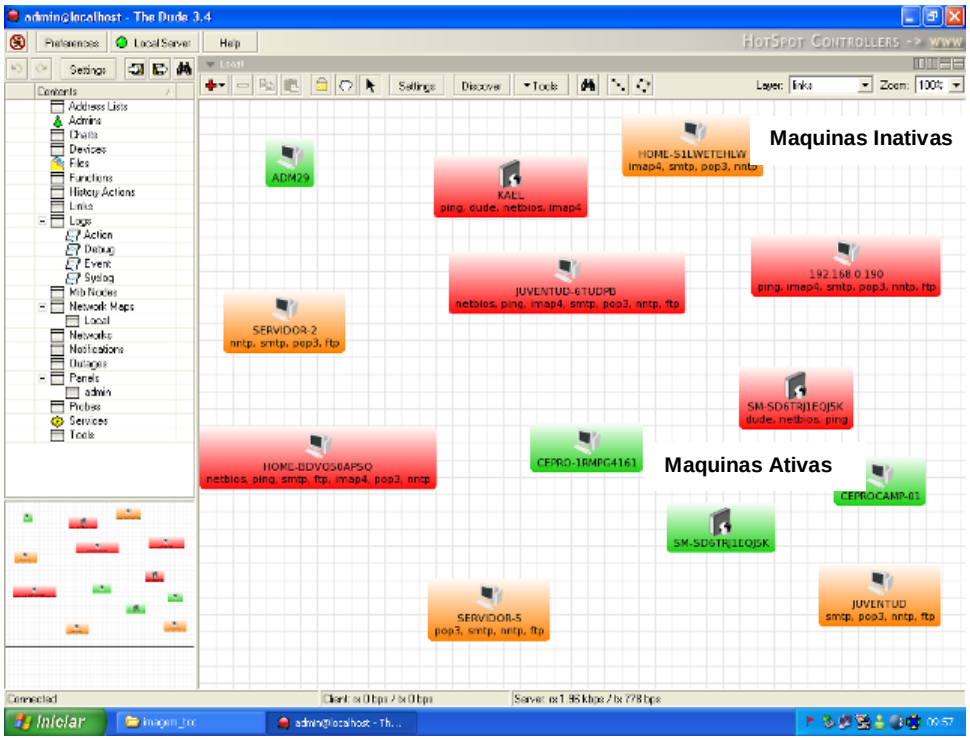

Figura 22: Tela de implantação do dude

O Dude é de fácil compreensão, pois sua interface é totalmente Web. Por ter um mapeamento gráfico interpretado por cores torna-se fácil a identificação das máquinas e servidores. O painel possui diversas ferramentas conforme a necessidade de operação.

Na figura 22 apresenta a visualização de uma rede mapeada pela ferramenta, com máquinas inativas na rede, e dois servidores ativos na rede.

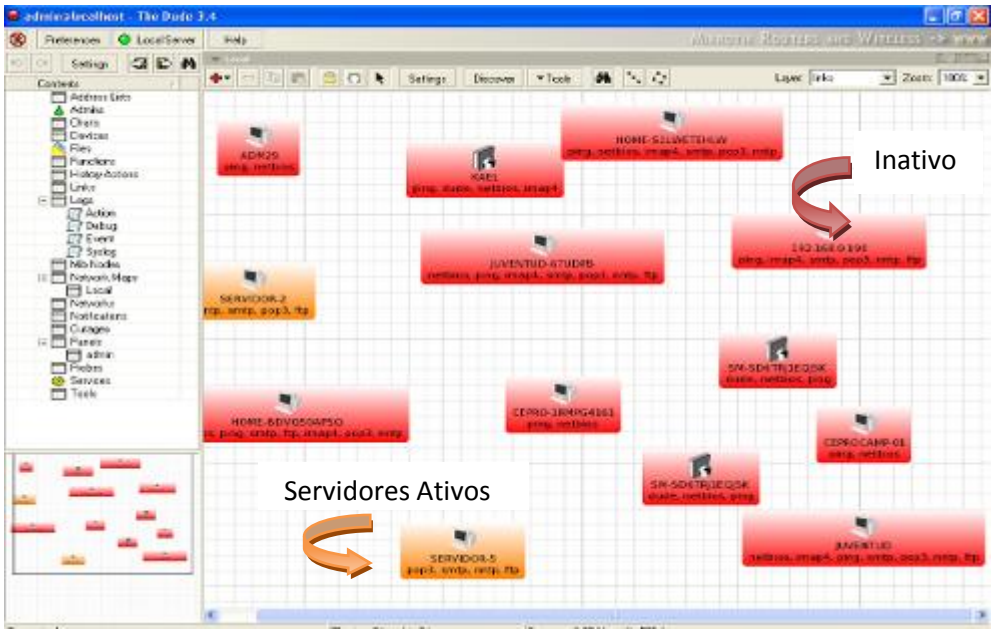

Figura 23: Tela de implantação do dude

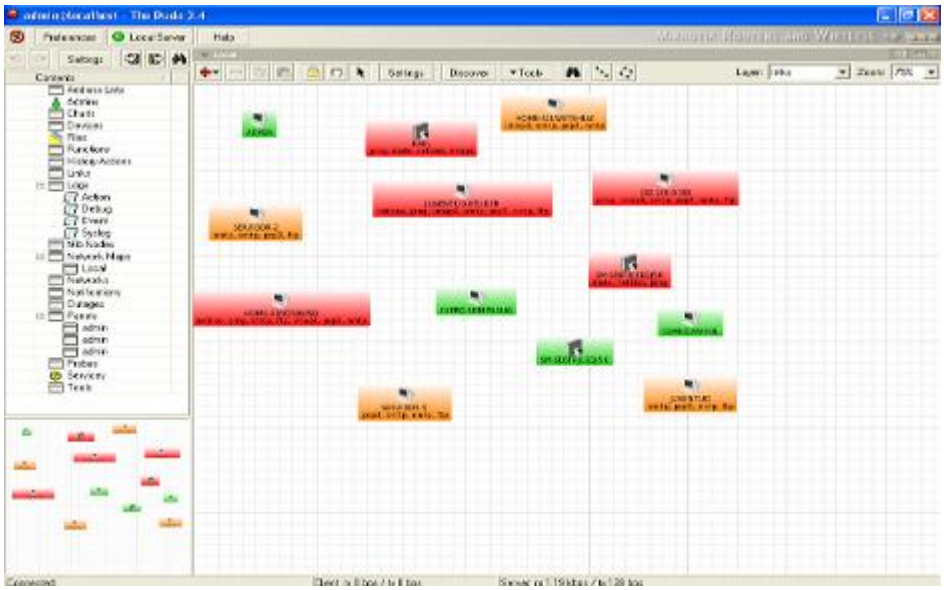

Figura 24: Tela de implantação do dude

CONCLUSÃO

O presente trabalho apresenta uma metodologia de gerência e monitoramento de redes, que seja capaz de facilitar o fluxo de informações, garantindo assim a integridade das informações nas redes interligadas com um acompanhamento constante dos acontecimentos e funcionamento dos dispositivos e configurações estabelecidas a cada tipo de rede.

A contribuição de modo geral desse trabalho tem como principal objetivo, facilitar as rotinas de trabalho do administrador de rede, a forma de organizar e registrar informações estabelecendo prazos de prioridade sem que cause danos ao funcionamento da rede, registrando tais problemas encontrados em tabelas, podendo assim gerar gráficos comparativos de funcionamento.

Um dos fatores de grande importância são os critérios para organizar melhor as prioridades e os trabalhos que devem ser realizado para manutenção. Tem-se então uma rede com fácil interação das informações, um gerenciamento com visão bem definidas e delimitadas do que gerenciar, e um monitoramento capaz de prever falhas de funcionamento dessas redes, facilitando assim a tomada de decisão e intervenção sem que danifique o funcionamento da mesma, sem que haja grandes perdas de informações.

BIBLIOGRAFIA

[1] SOARES, L. F; Lemos, G. & Colcher, S. **Redes de Computadores das LAN's, MAN's e WAN's ás Redes ATM**. Rio de Janeiro: Editora Campus, 1995.

[2] KUROSE, F. James, Lemos & Ross, W.Keith. **Redes de Computadores e a Internet - Uma Nova Abordagem**. São Paulo: Editora Pearson, 1995.

[3] FURMANKIEVICZ, Edson. **TCP/IP: a Bíblia**. Rio de Janeiro: Editora Campus, 2002.

[4] GIL, Antonio Loureiro. **Segurança em Informática**. São Paulo: Editora Atlas, 1994.

[5] Fontes, Edson. **Segurança da Informação**. São Paulo: Editora Saraiva, 2006.

[6] CARVALHO, Luciano Gonçalves. **Segurança de Redes**. Rio de Janeiro: Editora Ciência Moderna LTDA, 2005.

[7] TANENBAUM, A. S. **Redes de Computadores**. Rio de Janeiro: Editora Campus, 2003.

[8] WADLOW, Thomas. **Segurança de Redes - Projeto e Gerenciamento de Redes Seguras**. São Paulo: Editora Campus, 2000.

[9] MORIMOTO, Carlos E. **Redes Guia Prático**. 1ª Edição. Editora: GDH Press e Sul Editores, 2008.

[10] DAIBERT, Marcelo Santos & SILVA, João Carlos da. **Análise Comparativa de Sistemas de Gerência SNMP WhatsUP e The Dude**, Universidade Federal de Viçosa-Centro de Ciências Exatas e tecnologias departamento de informática.

[11] OLIVEIRA, Rodrigo Andrade de. **Desenvolvimento de uma Estrutura de Resposta Ativa Utilizando IDS SNORT**. Universidade do Oeste Paulista.

[12] Disponível em http://www.byfiles.storage.live.com. Acesso em 10/09/2011.

[13] Disponível em http: //www.felinux.com.br. Acesso em 11/09/2011.

[14] Disponível em http://rafaelpinto1995.blogspot.com/2011/02/modelo-tcpip.html. Acesso em 12/11/2011.

[15] Disponível em http://www.projetosderedes.com.br. Acesso em 11/09/2011.

[16] Disponível em http://www.lia.ufc.br. Acesso em 18/09/2011.

[17] Disponível em http://www.gta.ufrj.br. Acesso em 17/09/2011.

[18] Disponível em http://www.wonderware.com. Acesso em 17/09/2011.

[19] Disponível em http://www.images.google.com.br/imagem. Acesso em 25/09/2011.

[20] Disponível em http://images.google.com.br. Acesso em 24/09/2011.

[21] Disponível em http://nagios.sourceforge.net/docs/3_0/quickstart-fedora.html. Acesso em 11/09/2011.

[22] Disponível em http://nagios.sourceforge.net/docs/3_0/monitoring-windows.html. Acesso em 11/09/2011.

[23] Disponível em http://www.informaticagames.com.br/produto/Hub-8-Portas-10%7B47%7D100Mbps-Enh908%252dNWY-%252d-Encore.html. Acesso em 19/11/2011.

[24] Disponível em http://www.lojamegabrasil.com.br/switch-d-link-des-1024a.html. Acesso em 19/11/2011.

[25] Disponível em https://www.balaodainformatica.com.br/Site/index.asp?prod_id=26392&Promocao=roteador_d_link_di_524_150_wireless_150_mbps_dlink. Acesso em 20/11/2011.

[26] Disponível em https://www.balaodainformatica.com.br/Site/index.asp?prod_id=12582&Promocao=access_point_cisco_wap4410n_access_point_wireless_n_poe_cisco. Acesso em 20/11/2011.