UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

WILLIAM SILVEIRA SIPRIANO

ANÁLISE LÓGICA DE REDE: ESTUDO DE CASO NA SATC

CRICIÚMA

2014

WILLIAM SILVEIRA SIPRIANO

ANÁLISE LÓGICA DE REDE: ESTUDO DE CASO NA SATC

Trabalho de Conclusão de Curso apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. Msc. Rogério Antônio Casagrande

CRICIÚMA

2014

WILLIAM SILVEIRA SIPRIANO

ANÁLISE LÓGICA DE REDE: ESTUDO DE CASO NA SATC

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel, no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Redes de Computadores.

Criciúma, 24 de Junho de 2014.

BANCA EXAMINADORA

Prof. Rogério Antônio Casagrande - MSc. - (UNESC) - Orientador

Prof. Paulo João Martins - MSc. - (UNESC)

Prof. Sérgio Coral - Esp. - (UNESC)

Dedico este trabalho a minha família, cuja educação e incentivo me tornaram o que sou. Dedico também aos meus amigos e namorada que sempre me apoiaram e aconselharam a tomar as decisões corretas.

AGRADECIMENTOS

Agradeço primeiramente a Deus por me dar saúde, confiança e determinação.

Agradeço também aos meus pais, Rudnei e Sandra, que fizeram tudo o que estava ao alcance deles para eu chegar até aqui, sem dúvida não mediram esforços para proporcionar o melhor a mim. Este trabalho, entrego-lhes como gratidão por toda educação que me deram e tudo o que me ensinaram. Sei que estarão sempre ao meu lado aconteça o que acontecer, sempre terei o apoio deles.

A minha amiga e namorada Morgana por toda força que me deu e paciência por ter me aturado, muitas vezes nervoso, e também pelo tempo em que queria e não podia estar em sua companhia.

Ao orientador Rogério Antônio Casagrande pelo incentivo e contribuições a pesquisa.

Não posso deixar de agradecer a SATC por permitir que o trabalho fosse realizado dentro da instituição.

Enfim, a todos que de alguma forma contribuíram para a execução deste trabalho.

"A mente que se abre a uma nova ideia jamais voltará ao seu tamanho original."

Albert Einstein

RESUMO

Este trabalho foi realizado no ambiente da instituição de ensino SATC. Tem como objetivo identificar a importância da segmentação de redes para maior controle e segurança. E também identificar a importância da gerência através de softwares de monitoramento, mais precisamente o MRTG e o Nagios. Continuou-se a criação de segmentos com VLAN, utilizando a técnica de VLAN baseada em pontos. Com a rede segmentada, verificou-se os serviços realmente necessários a cada segmento, criando-se então uma ACL para filtragem dos pacotes. Com a ACL o tráfego da rede diminui e a segurança aumenta, pois os pacotes dos serviços não liberados são descartados. Após a segmentação e filtragem dos pacotes fez-se a instalação dos softwares de gerenciamento. O MRTG foi implantado para monitorar o tráfego das principais portas dos switches gerenciáveis e também as interfaces do firewall. O Nagios monitora os pontos de acesso sem fio e os switches gerenciáveis, através do protocolo ICMP verifica a comunicação destes equipamentos com a rede. Apresenta-se o conceito e funcionalidade de cada uma destas ferramentas, bem como seus processos de instalação e configuração. Através do monitoramento com o MRTG descobriu-se um gargalo de rede que foi solucionado e o Nagios possibilitou a resolução de muitos problemas de forma ágil. O estudo de caso foi positivo, pois a segmentação realizada propiciou uma rede menos suscetível a problemas e sem gargalos e as ferramentas de monitoramento proporcionaram melhorias na questão de prevenção de problemas e agilidade na resolução destes.

Palavras-chave: ACL. Ferramentas de monitoramento de rede. Nagios. MRTG. VLAN.

ABSTRACT

This work was conducted in the educational environment of SATC institution. It has as a goal to identify the importance of networks segmentation in order to obtain a wider control and security. Also, it is expected the importance of management by softwares of monitoring, more specifically the MRTG and the Nagios. The VLAN segments continued, using the VLAN technique based in points. With the segmented network, the really necessary services were checked by each segment, resulting in the creation of an ACL for package filtering. With the ACL, the network's traffic diminished and the security improved because the service packages not unleashed are discarded. After the segmentation and packages filtering the softwares for management were installed. The MRTG was implanted to monitor the traffic of the main manageable switches ports likewise the firewall's interfaces. The Nagios monitor the wireless access points and the manageable switches, through the ICMP protocol that verifies the communication of such equipments with the network. The concept and the functionality of each one of these mentioned tools are presented as well theirs installation and configuration processes. Through the monitoring with MRTG was discovered a network's bottleneck which was solved and Nagios made possible to solve several problems in an agile way. The case study was positive because the segmentation enforced a lesser susceptible network to problems and free of bottleneck. The tools for monitoring also proportionated improvents in what refers to avoiding problems and agility for solving them.

Keywords: ACL, Network monitoring tools, Nagios, MRTG, VLAN.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
ARP	Address Resolution Protocol
ASCII	American Standard Code Information Interchange
ASN1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DVR	Digital Video Recorder
FDDI	Fiber Distributed Data Interface
Gbps	Giga Bits por Segundo
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISS	Internet Information Services
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
LED	Light-Emitting Diode
MAC Address	Media Access Control Address
MAN	Metropolitan Area Network
Mbps	Mega Bits por Segundo
MIB	Management Information Base
MPLS	Multi-Protocol Label Switching
MRTG	Multi Router Traffic Grapher
NAT	Network Address Translation
NIC	Network Interface Card
OSI	Open Systems Interconnection
PAN	Personal Area Network

POS	Point of Sale
RFC	Request for Comments
SAN	Storage Area Network
SLA	Service Level Agreements
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
UDP	User Datagram Protocol
UTP	Unshielded Twist Pair
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WWAN	Wireless Wide Area Network

SUMÁRIO

1 INTRODUÇÃO

Nos dias atuais os novos equipamentos, computadores, *smartphones*, *tablets*, enfim, a tecnologia está cada vez mais fazendo o uso das redes de computadores. A mais utilizada que se conhece é a Internet.

Conforme Comer (2007) há duas décadas poucas pessoas tinham acesso à rede, agora já é algo essencial. Sejam para os negócios, produção, ensino, atividades militares, governos ou uso pessoal, as redes de computadores estão presentes em todos os campos.

E no campo corporativo as redes de computadores crescem a passos largos. A medida que crescem os nós da rede e consequentemente esta rede, problemas podem surgir, principalmente quando a rede não é planejada para tal evolução.

Em redes grandes o tráfego pode ser lento, haver perdas de pacotes. Isto, devido ao domínio de *broadcast*, que pode ser resolvido segmentando a rede em Virtual LAN (VLAN) (TORRES, 2008).

A técnica de VLAN é utilizada com o uso de *switches* camada 3 ou roteadores. Além de dividir o domínio de *broadcast,* esta técnica proporciona também uma gerência mais apurada e fácil de se implementar.

Softwares de gerência de redes auxiliam o administrador a descobrir problemas e a isolar sua causa. Com eles o gerente pode monitorar e controlar todos os equipamentos da rede, como *switches*, roteadores, *hosts*, verificando seus *status* e obtendo estatísticas das redes as quais eles ligam (COMER, 2007).

O Nagios e o Multi Router Traffic Grapher (MRTG) são softwares de gerenciamento e monitoramento. Com eles monitora-se o tráfego de rede e todos os equipamentos, através do protocolo Simple Network Management Protocol (SNMP). O MRTG monta gráficos com as informações do tráfego que é visualizado em um navegador.

Uma rede com bom desempenho depende também da tecnologia com a qual foi construída e o meio de transmissão que utiliza. Podem operar utilizando-se de cabos ou até mesmo o ar e ter taxas de transmissão que variam de 10 Mega bits por segundo (Mbps) a dezenas de Giga bits por segundo (Gbps).

Além de possuir um bom desempenho uma rede também precisa

apresentar segurança. A segurança em redes pode ser aplicada em todas as camadas, utilizando-se de firewalls, codificações, criptografias e autenticações. Filtrando os pacotes, pode-se permitir que somente determinadas portas e aplicações possam trafegar na rede.

Aborda-se neste trabalho, uma análise lógica de rede, segmentando-a em VLAN, aplicando Access Control List (ACL) para filtragem de pacotes e o gerenciamento da rede, monitorando o tráfego e os equipamentos da mesma, obtendo-se assim um bom desempenho e também segurança.

1.1 OBJETIVO GERAL

Analisar a estrutura de rede e por meio de um estudo de caso, propor e implantar soluções que visem melhoria de desempenho e segurança.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos abordados são:

a) coletar informações necessárias sobre a estrutura da rede que será utilizada como base para a elaboração da pesquisa através do estudo de caso;
b) compreender o conceito e descrever sobre a importância da segmentação de Redes;
c) prosseguir com a segmentação da rede em VLAN;
d) compreender o uso de portas em Redes e criar listas controles de acesso entre as VLAN criadas;
e) compreender o protocolo SNMP;
f) monitorar o tráfego de rede com o MRTG;
g) verificar outras formas de monitoramento de tráfego.

1.3 JUSTIFICATIVA

Uma rede bem planejada e estruturada precisa definir no mínimo três fatores: largura de banda de rede desejada, número de usuários e *hosts* na rede e

inclusão ou exclusão de equipamentos de tecnologia antiga. Esses fatores determinarão o funcionamento da rede e possibilitarão o crescimento futuro desta. (DIMARZIO, 2001).

Um problema comum em grandes redes é a presença de apenas um domínio de *broadcast*, podendo tornar a rede lenta. Um *switch* cria domínios de colisão individuais para cada porta, mas continua existindo ainda apenas um domínio de *broadcast* (TORRES, 2009).

O principal problema de *switches* de camada 2 é o *broadcasting*, pois não verificam o protocolo da camada de rede. O *broadcasting* é uma mensagem utilizada na comunicação entre os nós da rede que todo o sistema da rede recebe (VERAS, 2009).

Segmentando a rede, divide-se o domínio de colisão, fazendo com que aumente a largura de banda disponível para as estações individuais. Mas para que não estejam no mesmo domínio de *broadcast*, utiliza-se roteadores ou *switches* camada 3, criando-se redes virtuais (BIRKNER, 2003).

Utilizar-se de VLAN para segmentação da rede física em diversas redes lógicas resulta em uma performance mais apurada, pois o domínio de *broadcast* é quebrado (CALDAS FILHO; FERREIRA, 2013).

As principais razões para utilizar VLAN são: segurança, gerenciamento, desempenho e controle de fluxo. Aumenta a segurança pelo fato de poder separar da rede sistemas com dados sigilosos, impedindo acesso não autorizado. Melhora o gerenciamento e mobilidade, pois ao deslocar um nó da rede precisa-se apenas alterar a configuração do *switch* (BARROS, 2007).

Sub-redes também têm sido utilizadas para limitar os tamanhos dos domínios de *broadcast* da rede, oferendo vantagens significativas no desempenho (NORTHCUTT et al, 2002).

Uma forma de aumentar a segurança e também o desempenho é usando filtragem de pacotes. Uma ACL tem essa função. Ela é uma lista de instruções, que podem permitir ou negar endereços ou protocolos da camada superior, aumentando assim a segurança e mantendo o controle de tudo que está trafegando na rede. A ACL retira do cabeçalho do pacote alguns dados e os compara com suas regras configuradas, tomando as decisões corretas (JUNG; PELLIS, 2013).

Gerenciar a rede traz vários benefícios ao administrador, pois pode-se gerenciar o desempenho do ambiente, encontrar e resolver problemas e fornecer informações para o planejamento de capacidade. Para gerenciar a rede é necessário utilizar um protocolo de comunicação, sendo o SNMP o mais comum (VERAS, 2009).

Dentre os fatores que levaram a escolha de fazer um estudo e análise utilizando-se de VLAN e ACL está o fato de os *switches* da instituição suportarem esses recursos. E o monitoramento de tráfego entre as VLAN com o MRTG por ser totalmente gratuito e trazer informações precisas do tráfego de rede.

1.4 ESTRUTURA DO TRABALHO

Esta pesquisa está dividida em quatro capítulos, sendo no primeiro destacado o tema proposto, os objetivos e a justificativa para a realização desta pesquisa.

O capítulo 2 apresenta os conceitos fundamentais de redes de computadores necessários para a compreensão do estudo, como a classificação das redes, tipos de topologias, meios de transmissão, dispositivos, tecnologias, da arquitetura TCP/IP e suas camadas, protocolos e portas, tipos de segmentação de rede e, métodos de segurança e gerência de redes.

Os trabalhos que auxiliaram na realização desta pesquisa, com estudos que foram e estão sendo realizados nesta área de redes de computadores encontram-se no capítulo 3.

Toda a implantação da pesquisa, destacando a descrição do ambiente, a maneira com que a rede foi segmentada, os pacotes filtrados e os softwares de gerenciamento e monitoramento instalados e configurados são descritos no capítulo 4.

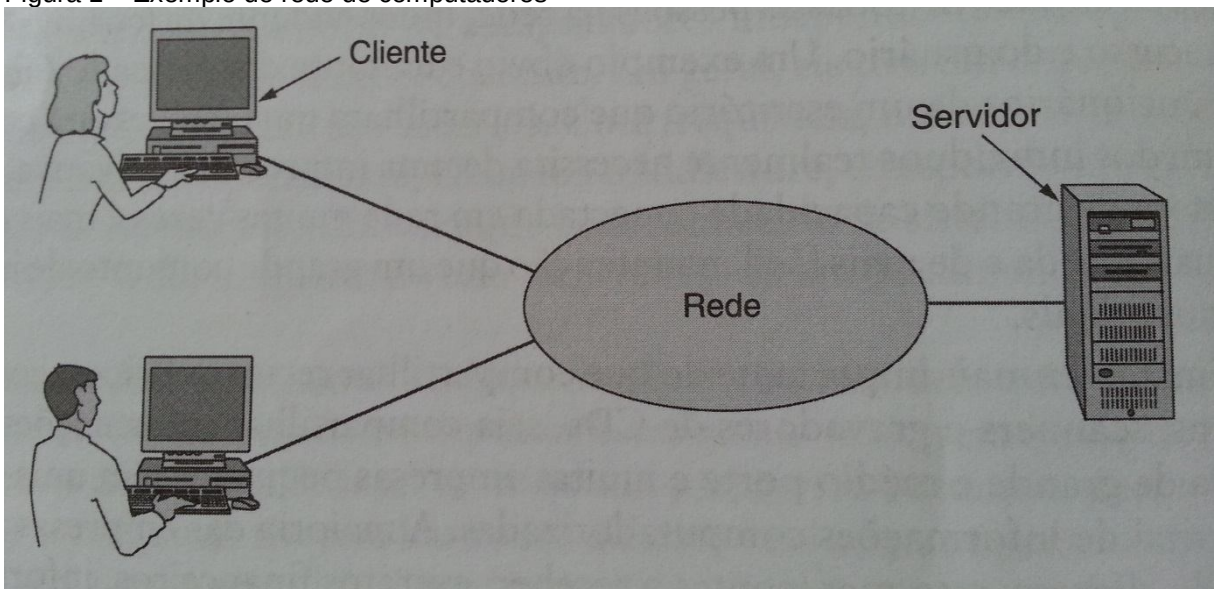
Por fim, tem-se a conclusão desta pesquisa, onde são apresentados também algumas sugestões para trabalhos futuros.

2 REDES DE COMPUTADORES

Rede de computadores é um conjunto de computadores interconectados no qual se pode trocar informações. Esta conexão pode ser por vários modos: fibra óptica, fio de cobre, micro-ondas, entre outros. Existem redes de diferentes tamanhos, modelos e formas (TANENBAUM, 2003).

As redes possibilitam o acesso a informações e recursos mesmo estando-se a quilômetros da origem destes dados, de forma transparente, como se estivesse numa rede local. O local onde os dados, geralmente, são armazenados, ou seja, em poderosos computadores, chama-se servidor. Já os computadores dos usuários que acessam esses dados recebem o nome de clientes. A figura 1 mostra uma rede de computadores.

Figura 1 – Exemplo de rede de computadores



Fonte: Tanenbaum (2003).

Segundo Comer (2007) as redes inicialmente eram utilizadas para compartilhar algum recurso, um periférico geralmente, entre os computadores. Este periférico era conectado à rede e assim os computadores poderiam utilizá-lo. Nos dias atuais o uso das redes está mais amplo. Empresas se comunicam umas com as outras e com os clientes através das redes.

Além da vantagem de compartilhar recursos, tem-se a facilidade de trocar informações e o acesso à Internet, reduzindo os custos com equipamentos e serviços (TORRES, 2009).

Tanenbaum (2003) ainda destaca que as redes de computadores otimizaram a comunicação entre as pessoas, tanto para uso doméstico quanto para uso comercial. Elas proporcionam o fácil acesso a e-mail, áudio e videoconferência, serviços e negócios online.

Com as redes os usuários podem acessar seus dados de diferentes locais com diferentes dispositivos.

2.1 CLASSIFICAÇÃO DAS REDES

Baseando-se na área geográfica ou organizacional, ou seja, em escalas, as redes podem ser classificadas principalmente em Local Area Network (LAN), Metropolitan Area Network (MAN) e Wide Area Network (WAN) (TANENBAUM, 2003).

Mas existem também outras classificações como a Wireless Local Area Network (WLAN), Wireless Metropolitan Area Network (WMAN), Wireless Wide Area Network (WWAN), Storage Area Network (SAN) e Personal Area Network (PAN).

As principais classificações são citadas a seguir.

2.1.1 Local area network

Uma LAN ou rede local, é o tipo mais comum de rede, abrange um espaço limitado, geralmente uma sala ou prédio (TORRES, 2009).

Para Tanenbaum (2003) as LAN são redes privadas de um edifício ou campus universitário, com até alguns quilômetros de extensão. Conectam computadores pessoais e estações de trabalho em escritórios e empresas, permitindo o compartilhamento de recursos e troca de informações. As LAN tradicionais operam com velocidade de cerca de 100 Mbps, já as mais modernas chegam a 10 Gbps.

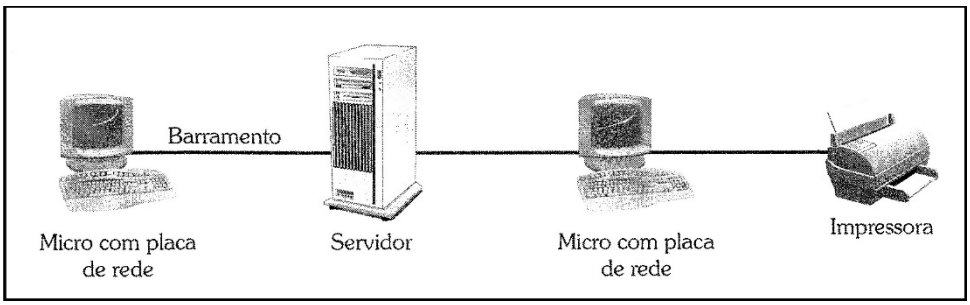
Tanenbaum ainda afirma que este tipo de rede se difere das demais por três motivos: tamanho, tecnologia de transmissão e topologia.

Como a distância da LAN não é muito extensa sua velocidade é maior que as demais classificações de rede e também seu atraso, que não passa de 10 milissegundos (COMER, 2006).

As LAN surgiram na década de oitenta, segundo os padrões IEEE 802.3, IEEE 802.4 e IEEE 802.5 (CARISSIMI; ROCHOL; GRANVILLE, 2009).

Uma LAN (figura 2) é composta por placas de rede, sistemas operacionais, meio de transporte, equipamentos de concentração e servidor (MORAES, 2008).

Figura 2 – LAN



Fonte: Moraes (2008).

2.1.2 Metropolitan area network

Quando a rede atinge maiores proporções, abrangendo um grupo de escritórios ou mesmo uma cidade inteira, ela recebe o nome de Metropolitan area network. Esta pode ser privada ou pública (TANENBAUM, 2003).

Torres (2009) destaca que a conexão entre as redes locais que compõe a rede metropolitana é alugada de uma concessionária de telecomunicações ou feita utilizando-se da Internet com o uso de uma técnica chamada Virtual Private Network (VPN), rede privada virtual, reduzindo os custos de conexão. Em relação as redes locais, as redes metropolitanas têm a desvantagem de desempenho e segurança, pois não estão mais centralizadas para uma fácil gerência.

As MAN surgiram na década de noventa com o padrão IEEE 802.6 e o Fiber Distributed Data Interface (FDDI). Atualmente a tecnologia MAN mais representativa é a Asymmetric Digital Subscriber Line (ADSL) (CARISSIMI; ROCHOL; GRANVILLE, 2009).

2.1.3 Wide area network

Quando uma rede abrange uma ampla área geográfica, como um país ou um continente ela é chamada de Wide area network ou rede geograficamente distribuída (TANENBAUM, 2003).

Tanenbaum ainda diz que em uma WAN há um conjunto de *hosts* que são conectados por uma sub-rede. Os *hosts* pertencem a usuários em geral e a sub-rede pertence e é operada por uma empresa de telefonia ou provedor de serviços da Internet.

Segundo Moraes (2008) uma WAN trabalha com velocidades inferiores a das LAN. Estas redes possuem protocolos específicos e os meios de transmissão mais comuns são: cabo de cobre, satélite, micro-ondas e fibra óptica.

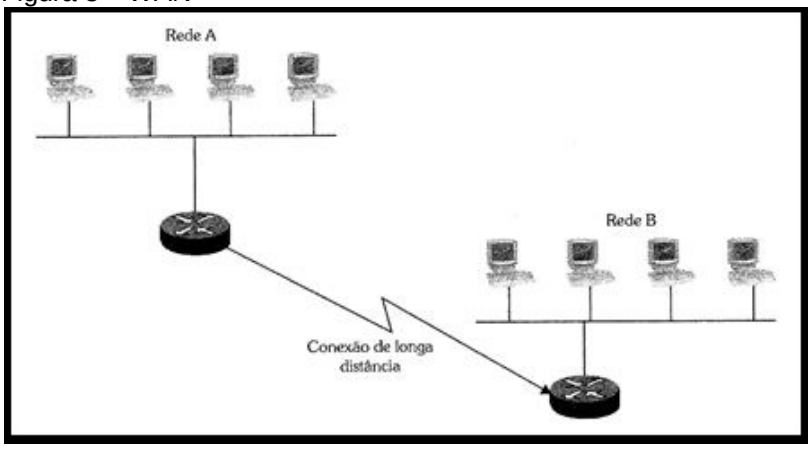
Um bom exemplo de WAN seria uma empresa conectando suas diversas filiais e escritórios (TORRES, 2009).

Comer (2006) afirma que a velocidade típica de uma WAN é de 1,5 Mbps a 2,4 Gbps, velocidades bem inferiores que de uma LAN. Os atrasos através de uma WAN podem variar de milissegundos a dezenas de segundo, quando a WAN envia sinais para satélites na órbita da Terra.

Moraes (2008) também ressalta que existem diferentes técnicas de comutação em uma WAN. Essas técnicas podem ser baseadas em circuitos, pacotes e células. E também, conforme a necessidade, seja a banda disponibilizada, a qualidade de serviço, a disponibilidade e a confiabilidade do serviço, a análise de custo x benefício e os meios de transmissão, diferentes tecnologias podem ser utilizadas. As tecnologias mais importantes são: Linhas discadas e privativas, Integrated Services Digital Network (ISDN), E-1, X.25, Frame Relay, Asynchronous Transfer Mode (ATM), Internet Protocol (IP), Point of Sale (POS) e Multi-Protocol Label Switching (MPLS).

A figura 3 mostra uma rede WAN.

Figura 3 – WAN



Fonte: Moraes (2008).

2.2 TOPOLOGIAS

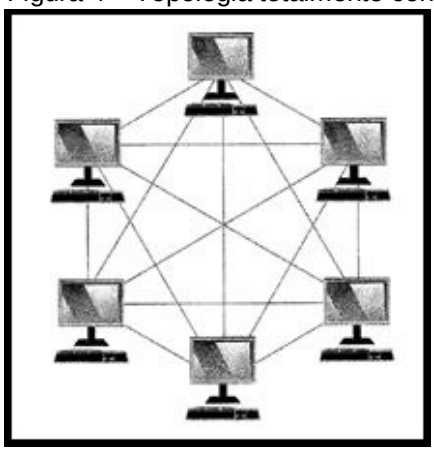
A topologia física descreve o *layout* dos hardwares na rede, ou seja a maneira com que os computadores de uma rede local estão conectados (TORRES, 2009).

De acordo com a topologia empregada os protocolos utilizados diferem, assim como a sinalização, endereçamento, velocidade, banda e performance (MORAES, 2008).

2.2.1 Totalmente conectada

Na topologia totalmente conectada (figura 4) cada computador possui uma conexão individual com todos os outros computadores da rede. Apesar de ser uma rede com um alto nível de redundância ela é inviável devido ao alto custo na infraestrutura (TORRES, 2009).

Figura 4 – Topologia totalmente conectada

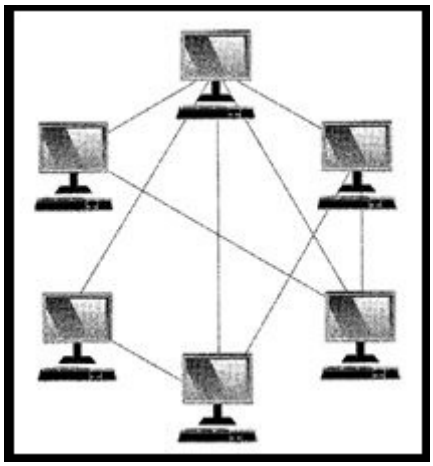


Fonte: Torres (2009).

2.2.2 Em malha

Similar a totalmente conectado, porém nem todos os computadores tem conexões individuais com todos os outros computadores. Oferece alto nível de redundância, mas também necessita de muitos cabos. Mostra-se na figura 5 uma topologia em malha (TORRES, 2009).

Figura 5 – Topologia em malha



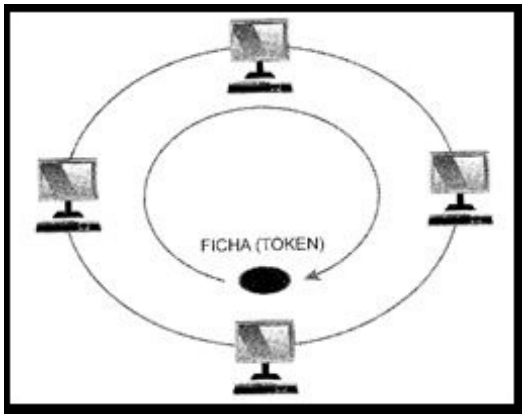
Fonte: Torres (2009).

2.2.3 Em anel

Cada computador possui duas conexões, uma com o computador anterior e outra com o próximo, formando um círculo. Caso algum pare de funcionar ou um cabo partir a rede deixa de funcionar. Mas na prática utiliza-se um dispositivo concentrador, cuja função é criar internamente um anel, funcionando de forma similar a topologia estrela (TORRES, 2009).

A topologia em anel (figura 6) possui a vantagem de nunca haver colisões, pois somente uma mensagem por vez trafega no anel. Uma estação é responsável por gerenciar a rede, que geralmente funciona em um único sentido. Este sentido pode alterar quando a rede é quebrada, retornando a mensagem para a origem (MORAES, 2008).

Figura 6 – Topologia em anel



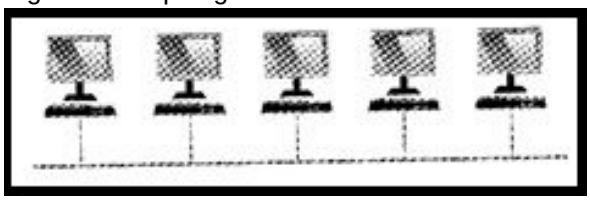
Fonte: Torres (2009).

2.2.4 Linear

Conhecida também como barramento. Nela todos os computadores são ligados a um elemento central. A rede deixa de funcionar se este elemento parar de funcionar (TORRES, 2009).

O desempenho da rede linear (figura 7) varia de acordo com a quantidade de equipamentos, do tipo de cabo e da utilização da rede pelos equipamentos e aplicações (MORAES, 2008).

Figura 7 – Topologia linear



Fonte: Torres (2009).

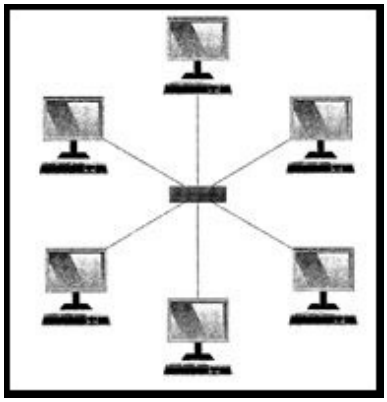
2.2.5 Em estrela

Os computadores são conectados a um periférico concentrador. Ocorrendo um problema em uma conexão, somente o computador pertencente a esta conexão deixa de ter acesso a rede, facilitando a manutenção (TORRES, 2009).

Por outro lado se ocorrer uma falha no concentrador toda a rede para de funcionar. A performance da rede fica limitada a capacidade deste equipamento comutar os pacotes (MORAES, 2008).

Uma rede em estrela pode ser identificada pela figura 8.

Figura 8 – Topologia em estrela

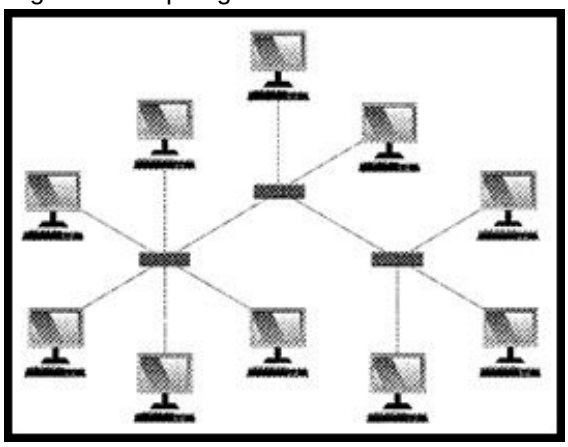


Fonte: Torres (2009).

2.2.6 Em árvore

Na topologia em árvore (figura 9), duas ou mais redes estrelas são ligadas juntas, ou seja, é uma rede estrela com mais periféricos concentradores (TORRES, 2009).

Figura 9 – Topologia em árvore



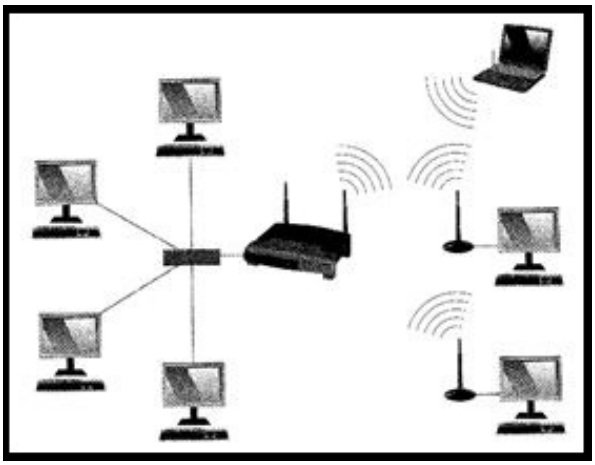
Fonte: Torres (2009).

2.2.7 Sem fio

Os computadores se ligam a rede sem a necessidade de cabos. Para esta ligação, entre a rede sem fio e a rede física, necessita-se de um equipamento chamado ponto de acesso (TORRES, 2009).

Topologia sem fio pode ser exemplificada pela figura 10.

Figura 10 – Topologia sem fio



Fonte: Torres (2009).

2.2.8 Híbrida ou mista

Redes que usam mais de uma topologia ao mesmo tempo (TORRES, 2009).

2.3 MEIOS DE TRANSMISSÃO

Meios de transmissão são os canais físicos utilizados para a comunicação de dados. E se diferem por: velocidades suportadas, taxa de erros, disponibilidade, confiabilidade, atenuação, limitação geográfica, imunidade a ruído e suporte a conexões ponto a ponto ou ponto multiponto (MORAES, 2008).

Ainda segundo Moraes, as mídias de comunicação utilizadas são par de cobre trançado, usado em redes locais; cabos coaxiais, usados em links de comunicação de dados E1/E3; fibras ópticas, mais utilizadas em redes de longa distância; radiodifusão, transmissão por ondas de rádio; enlaces de micro-ondas, onde não existe possibilidade de cabeamento; infravermelho, usada principalmente para conectar edifícios próximos ou ambientes internos; transmissão de ondas via satélite, usados como redundância dos sistemas de comunicação ou em localidades remotas.

Os meios mais utilizados são: par de cobre trançado e fibra óptica.

2.3.1 Par de cobre trançado

Para Kurose e Ross (2010) esse é o meio de transmissão mais comumente utilizado nos dias atuais. Mais de noventa e nove por cento de toda fiação que conecta os equipamentos é de par de cobre trançado.

Os cabos Unshielded Twist Pair (UTP), muito utilizados em redes locais podem ser classificados em: categoria 3, para uso em Ethernet na velocidade máxima de 10 Mbps; categoria 4, para uso em redes Token Ring com velocidade máxima de 16 Mbps; categoria 5, para uso em redes Fast Ethernet com velocidade de até 100 Mbps; e categoria 6, usada em redes Gigabit Ethernet com velocidade máxima de 1 Gbps (MORAES, 2008).

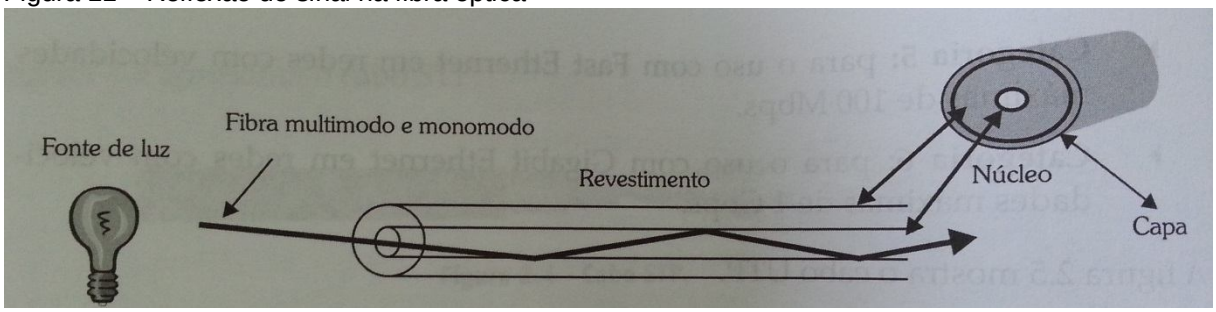
Moraes ainda afirma que as principais características do uso deste tipo de cabo são o baixo custo, a fácil conectorização, a flexibilidade e fácil instalação, velocidade variada e alcance máximo entre as estações de cem metros.

2.3.2 Fibras ópticas

A fibra óptica conduz pulsos de luz. São imunes a interferência eletromagnética, tem baixíssimas atenuações de sinal e são muito difíceis de derivar. Porém suportam taxas de transmissão elevadíssimas e por longas distâncias. São utilizadas inclusive em cabos submarinos. Não são utilizadas em LAN devido ao alto custo de equipamentos óticos (KUROSE; ROSS, 2010).

Segundo Moraes (2008) as fibras ópticas são compostas por fios muito finos de sílica, vidro ou até plástico e revestidas com um material com índice de refração diferente do miolo da fibra. O raio de luz é refletido na casca da fibra e fica confinado em seu núcleo. A figura 11 mostra este funcionamento.

Figura 11 – Reflexão do sinal na fibra óptica



Fonte: Moraes (2008).

Moraes ainda diz que as fibras podem ser classificadas em mono ou multimodo. As fibras monomodo alcançam até cem quilômetros e possuem velocidade máxima de 100 Gbps. Utiliza laser como fonte de luz e sua conectorização é mais complexa. Já as fibras multimodo alcançam até dois quilômetros e possuem velocidade máxima de 1.2 Gbps, utiliza Light-Emitting Diode (LED) como fonte de luz e sua conectorização é mais simples.

2.4 EQUIPAMENTOS DE INTERCONEXÃO

Os equipamentos de interconexão são equipamentos obrigatórios para a comunicação entre os computadores, cada um executa uma função específica. Estes dispositivos se diferem em tecnologia e podem ser classificados em inteligentes, como roteadores e *switches* e não inteligentes, como os *hubs* (DIMARZIO, 2001).

Dimarzio diz que os dispositivos inteligentes possuem processador e sistema operacional. São utilizados para funções específicas e executam tarefas complexas. Já os dispositivos não inteligentes não possuem capacidade de processamento ou sistema operacional. Executam tarefas mais simples e não obedecem qualquer critério de rede.

2.4.1 *Switch*

Conforme Dimarzio (2001) um *switch* pode ser considerado um *hub* inteligente. Os *switches* entregam os dados diretamente as estações através das portas.

Dimarzio ainda descreve que os *switches* não difundem informações, ou seja, garantem a largura de banda por porta. São capazes de consultar as estações conectadas a cada porta, colocando estas informações em *cache*, armazenando o Media Access Control Address (MAC Address) de todas as estações. Recebendo os dados o *switch* abre o pacote e lê o destino, comparando estas informações aos endereços em seu *cache*, roteando os dados para a porta correta, eliminando a difusão de dados.

Moraes (2008) informa que existem também *switches* multicamada, ou seja, não operam somente na camada 2 do modelo Open Systems Interconnection (OSI), como os tradicionais, mas também na camada 3. São capazes de examinar o pacote IP e tomar decisões de comutação baseadas nestas informações. Estes tipos de *switches* são capazes de priorizar o tráfego de determinados serviços, trabalhar como servidores Dynamic Host Configuration Protocol (DHCP) e executar a função Network Address Translation (NAT).

Moraes ainda comenta que existem *switches* que suportam a criação de links redundantes entre os *switches*, através do algoritmo de *spanning tree*. Quando

um link falha o outro é automaticamente acionado. Isto de forma transparente e dessa forma evita-se *loops*. O *spanning tree* é padronizado pela norma IEEE 801.2d.

Para Torres (2009) utilizando *switches* de camada 3, cria-se domínios de broadcast separados, ligando-se várias redes distintas. Com isso melhora-se o desempenho.

2.4.2 Roteador

Os roteadores possuem processador e sistemas operacionais que lhes permitem tomar decisões complexas baseadas em vários critérios. O roteador entrega os dados ao destino específico através de alguns percursos, podendo usar o roteamento estático, em que é definido qual o melhor caminho, ou roteamento dinâmico, em que são verificados um número de critérios para descobrir o melhor caminho. O roteamento dinâmico é mais complexo de ser implementado, exigindo maior administração e configuração (DIMARZIO, 2001).

Segundo Moraes (2008) os roteadores são equipamentos essenciais também para garantir a segurança das redes, pois atuam como filtro de pacotes indesejáveis. Também executam uma função muito importante na rede que é o NAT, ou seja, ele converte endereços IP válidos em endereços IP inválidos, possibilitando o uso de IP internos a serem utilizados na Internet.

2.4.3 Placa de rede

A placa de rede, também conhecida como Network Interface Card (NIC), é responsável por ligar os dispositivos a rede. Ela, através do *driver* da placa, recebe os dados a serem transmitidos, monta-os no *frame* correspondente ao protocolo de rede e envia pelo meio de transmissão (MORAES, 2008).

Moraes também ressalta que cada placa de rede possui um endereço único, chamado de MAC Address. Este endereço é formado por um identificador do fabricante, seguido por um sufixo de identificação da placa.

Atualmente existem placas de rede de diferentes tecnologias, Ethernet, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, dentre outras.

2.5 TECNOLOGIAS

A tecnologia de rede mais conhecida e utilizada é a Ethernet ou uma de suas variantes. A Ethernet é baseada na norma IEEE 802.3 e é formalmente conhecida como 10Base-T, operando a 10 Mbps. Mas com o passar dos anos essa taxa de transmissão acabou tornando-se um gargalo, necessitava-se de taxas maiores. Foi então projetada a Fast Ethernet, conhecida como 100Base-T e a Gigabit Ethernet, conhecida como 1000Base-T, ambas operando respectivamente a 100 Mbps e 1 Gbps (COMER, 2006).

Kurose e Ross (2010) informam que em 2007 um novo padrão foi disponibilizado, chamado de 10 Gigabit Ethernet ou 10GBase-T, operando a 10 Gbps.

2.6 ARQUITETURA TCP/IP

Este modelo recebe este nome devido aos seus dois principais protocolos: Transmission Control Protocol (TCP) e o Internet Protocol (IP) (MURHAMMER et al, 2000).

A ARPANET, rede de pesquisa criada pelo Departamento de Defesa dos Estados Unidos e antecessora da Internet, estava em expansão. Várias universidades e repartições públicas estavam sendo ligadas a ela. Com isso, quando as redes de rádio e satélites foram criadas houveram problemas com os protocolos existentes. Forçando a criação de um novo modelo de referência. Este ficou conhecido como TCP/IP, cujo objetivo era conectar várias redes ao mesmo tempo (TANENBAUM, 2003).

Com a popularização da Internet, a capacidade do TCP/IP de ser roteável e o fato de possui uma arquitetura aberta, ou seja, qualquer fabricante pode adotar sua versão do TCP/IP em seu Sistema Operacional, tornando-o um protocolo universal. Estes motivos contribuíram para este ser o modelo mais utilizado em redes atualmente (TORRES, 2009).

Segundo Murhammer et al (2000) o TCP/IP é modelado em camadas, podendo ser representado por uma pilha de protocolos ou um conjunto de protocolos.

2.6.1 Camadas

2.6.1.1 Camada de aplicação

Para Torres (2009), esta é a camada de comunicação, ela “conversa” com os softwares contidos no computador. Existem vários protocolos nesta camada, cada um responsável por um serviço diferente, como o Domain Name System (DNS), HyperText Transfer Protocol (HTTP), SNMP, Telnet, dentre muitos outros.

Através de uma porta essa camada se comunica com a camada de transporte.

2.6.1.2 Camada de transporte

A camada de transporte é composta por dois protocolos, o TCP e o User Datagram Protocol (UDP) (MURHAMMER et al, 2000).

A função da camada de transporte é fornecer a transferência de dados de uma ponta a outra, da origem ao destino, ou seja, recebe os dados da camada de aplicação e transforma-os em pacotes, que são enviados para a camada de Inter-Redes (TORRES, 2009).

2.6.1.3 Camada inter-redes

Torres (2009) ainda afirma que a camada de Inter-Redes também conhecida como camada de redes é responsável por receber os pacotes oriundos da camada de transporte e dividi-los em datagramas, juntamente com os endereços lógicos de origem e destino.

Torres informa também que o principal protocolo desta camada é o IP, mas ela abrange outros protocolos como o Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP), Address Resolution Protocol (ARP), dentre outros.

2.6.1.4 Camada de interface de rede

Para Murhammer et al (2000) a camada de interface de rede ou camada de enlace é a interface com o próprio hardware de rede. Esta camada pode ser orientada para pacotes ou fluxo e pode ou não fornecer uma entrega confiável.

2.6.2 Protocolos

“Protocolos são regras e procedimentos de comunicação” (MORAES, 2008, p. 124). Existem vários tipos de protocolos, cada um com uma vantagem e propósitos distintos.

Moraes ainda informa que alguns protocolos podem operar em mais de uma camada, sendo que a camada que ele trabalha descreve a sua função e muitos dos protocolos podem trabalhar em pilha, ou seja, conjuntamente.

Para Comer (2007) este conjunto de regras, denominado protocolos, especifica o formato e as ações a serem tomadas em cada mensagem. Estes protocolos são divididos em camadas, dividindo-se as tarefas e facilitando sua utilização, análise e teste.

Em redes têm-se três espécies de protocolos: protocolos de aplicação, transporte e de rede.

Comer (2006) diz que os protocolos são divididos em camadas para que um problema maior possa ser dividido em várias partes, facilitando também para os projetistas de software, que podem se importar apenas com a camada para qual o software é destinado.

2.6.2.1 Telnet

É um protocolo de aplicação que trabalha sobre o TCP na porta 23 e permite a criação de um terminal remoto de uma estação (MORAES, 2008).

Conforme Torres (2009) o Telnet é um terminal do qual o cliente Telnet se conecta em um servidor Telnet, o qual pode manipulá-lo. O Telnet usa o código American Standard Code Information Interchange (ASCII) para transmissão de dados. O seu maior problema é não criptografar os dados na transmissão.

Ao estabelecer uma conexão com o servidor Telnet o cliente aceita toques de tecla do teclado do usuário e os envia ao servidor, que simultaneamente envia informações que são mostradas na tela do usuário (COMER, 2006).

2.6.2.2 SNMP

Segundo Moraes (2008) o SNMP é um protocolo de gerenciamento, com o objetivo de monitoração e configuração de equipamentos em rede.

O SNMP é um protocolo de solicitação e resposta que atua sobre o UDP. Tem duas operações. GET, que informa o estado de algum nó e SET, que armazena um novo estado para algum nó (PETERSON; DAVIE, 2004).

Uma entidade gerenciada possui um conjunto de variáveis que são mantidas pelo SNMP. Esse conjunto de variáveis constitui uma base de informações de gerenciamento, chamada de Management Information Base (MIB). As variáveis MIB são descritas usando codificação Abstract Syntax Notation One (ASN.1), uma linguagem formal (COMER, 2006).

Para Peterson e Davie (2004) as variáveis da MIB trazem informações de sistema, como nome, tempo em que esteve ligado; de interfaces, como endereço físico, quantidade de pacotes trafegados; de IP, como a tabela de roteamento; de TCP, UDP, dentre outras.

2.6.2.3 DNS

O DNS é um protocolo de aplicação, ele resolve nomes na Internet. Trabalha sobre o UDP, na porta 53 (MORAES, 2008).

Segundo Torres (2009) o DNS possui duas funções: converter endereços IP em endereços nominais e vice-versa.

O DNS pode ser referenciado como um serviço de rede, já que auxilia outros protocolos de aplicação, agindo de maneira transparente aos usuários (CARISSIMI; ROCHOL; GRANVILLE, 2009).

2.6.2.4 TCP

Para Carissimi, Rochol e Granville (2009) o TCP é o protocolo de transporte mais importante, devido a sua grande disseminação e utilização.

O TCP oferece conexão confiável entre pares de processos e também: transferência em fluxo de dados, confiabilidade, controle de fluxo, multiplexação, conexões lógicas e *full-duplex* (MURHAMMER et al, 2000).

Segundo Tanenbaum (2003), o TCP oferece um fluxo de bytes fim a fim confiável em uma inter-rede não confiável, sendo que este foi projetado para se adaptar a inter-rede e ser robusto diante das falhas que possam ocorrer.

O TCP conta com princípios de detecção de erros, retransmissão, reconhecimentos cumulativos, temporizadores, entre outros. Ele está definido no Request For Comments (RFC) 793, 1122, 1323, 2018 e 2581 (KUROSE; ROSS, 2010).

O TCP coloca em ordem os datagramas IP recebidos, verificando se todos chegaram corretamente através de uma confirmação de reconhecimento enviada pelo receptor. Empacota os dados recebidos da camada de aplicação, adicionando a porta de origem e destino, dentre outros, repassando para o protocolo IP (TORRES, 2009).

As conexões TCP são identificadas por quatro parâmetros distintos: endereço da rede de origem, porta de transporte da origem, endereço de rede de destino e porta de transporte de destino (CARISSIMI; ROCHOL; GRANVILLE, 2009). A tabela 1 mostra um exemplo de conexões TCP e também que um servidor pode se conectar com mais de um cliente utilizando a mesma porta.

Tabela 1 – Exemplo de conexão TCP

	Endereço Origem	Porta Origem	Endereço Destino	Porta Destino
Cliente 1	143.54.47.253	3345	200.132.73.9	80
Cliente 2	200.19.179.139	7002	200.132.73.9	80
Cliente 3	200.19.179.139	3345	200.132.73.9	80

Fonte: Carissimi, Rochol e Granville (2009).

Carissimi, Rochol e Granville ainda afirmam que o TCP é utilizado quando a integridade dos dados transmitidos é importante.

> O TCP fornece um serviço de transporte de *stream* orientado a conexão, *full-duplex* e completamente confiável (nenhuma duplicação ou perda de dados), o que permite a dois programas

> aplicativos formarem uma conexão. Cada conexão de TCP é iniciada confiavelmente e terminada graciosamente, com todos os dados sendo entregues antes de a terminação acontecer (COMER, 2007, p. 348).

2.6.2.5 UDP

Segundo Murhammer et al (2000) o UDP funciona simplesmente para o envio e recebimento de datagramas, utilizando-se de portas para direcionar estes datagramas. Não oferece confiabilidade, controle ou recuperação de erros ao IP, ficando a aplicação com esta responsabilidade.

Como o UDP não oferece confiabilidade, ele é mais utilizado em um ambiente local, onde a conexão é melhor e a perda de pacotes é mais difícil (COMER, 2006).

Para Kurose e Ross (2010) algumas aplicações utilizam o UDP por: melhor controle no nível da aplicação sobre quais dados são enviados e quando, não estabelecer conexão nem estados de conexão e pela pequena sobrecarga de cabeçalho de pacote. O UDP é definido pelo RFC 768.

A vantagem do UDP sobre o TCP é principalmente pela rápida transmissão de dados. Pois o cabeçalho do UDP é menor e também não existe um mecanismo de confirmação de entrega (TORRES, 2009).

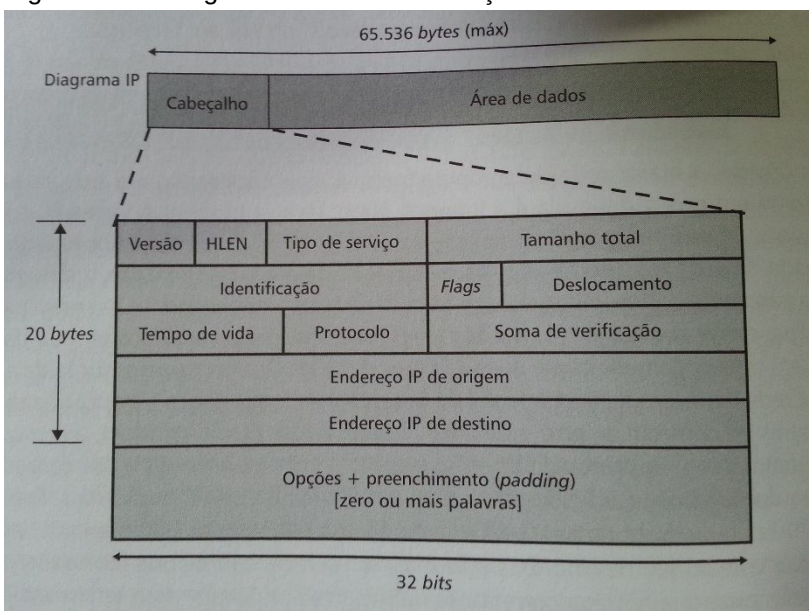
2.6.2.6 IP

O IP tem a função de enviar para a camada de interface de rede os dados vindos da camada de transporte (TORRES, 2009).

O protocolo IP não garante a entrega e a ordem de datagramas ao destino final, podendo ainda duplica-los. Esta tarefa de garantir a entrega e a ordem cabem as camadas superiores de transporte ou aplicação (CARISSIMI; ROCHOL; GRANVILLE, 2009).

Carissimi, Rochol e Granville ainda mostram que a unidade básica de transmissão de dados, ou seja, o datagrama IP é composta por um cabeçalho e uma área de dados. A figura 12 mostra um datagrama de um IPV4 e seu cabeçalho, com todos os campos que formam o mesmo.

Figura 12 – Datagrama IPV4 e seu cabeçalho

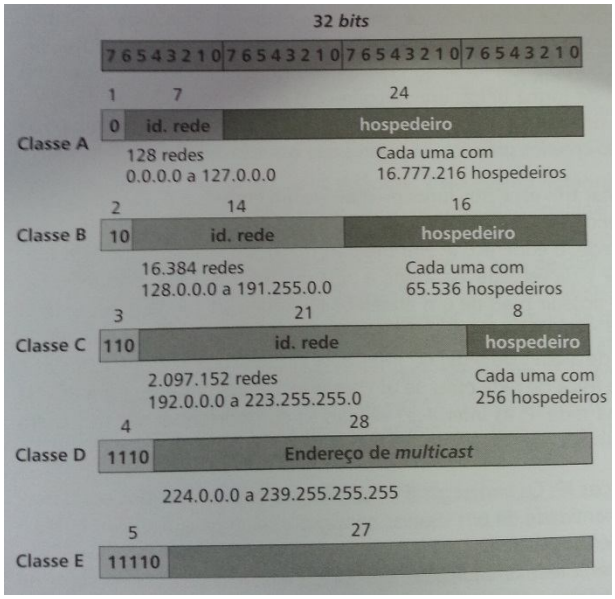


Fonte: Carissimi, Rochol e Granville (2009).

Ainda segundo os autores, o IP é composto de duas partes, um prefixo, que indica de forma única uma rede, e um sufixo, que também indica de forma única um equipamento dentro da rede.

Os autores ainda relatam que os endereços IP foram divididos em cinco classes: A, B, C, D e E. As classes A, B e C definem redes e equipamentos dentro dessas redes. A classe D é de *multicast*, ou seja, de suporte a comunicação em grupo e a classe E é reservada para o futuro. Respectivamente os endereços de classe A empregam 8, 16 e 24 bits para o prefixo, ou seja, para o endereço de rede, conforme figura 13.

Figura 13 – Classes de endereço IP



Fonte: Carissimi, Rochol e Granville (2009).

Há também um conjunto de IP privativos, definidos na RFC 1918, mostrados na tabela 2. Estes endereços não precisam ser únicos, por isso também são chamados de inválidos.

Tabela 2 – Endereços IP privativos

Classe	Inicial	Final	Qtde. máquinas*
A	10.0.0.0/8	10.255.255.255/8	16.777.216
B	172.16.0.0/12	172.31.255.255/12	1.048.576
C	192.168.0.0/16	195.168.255.255/16	65.536

* descontar os endereços especiais

Fonte: Carissimi, Rochol e Granville (2009).

Segundo Kurose e Ross (2010), atualmente há duas versões do IP em uso. O IPv4, RFC 791 e o IPv6, RFCs 2460 e 4291.

2.6.3 Portas

Portas são um sistema de endereçamento. Permitem a comunicação entre a camada de aplicação e a camada de transporte. Tornando possível saber a qual protocolo de aplicação a camada de transporte deve entregar um pacote (TORRES, 2009).

Torres ainda diz que as portas usam um endereçamento de 16 bits, ou seja, são numeradas de 0 a 65535, podendo ser associada ao TCP e ao UDP. Estas portas são padronizadas por um órgão responsável, a Internet Assigned Numbers Authority (IANA), para que não existam aplicações diferentes utilizando a mesma porta, já que somente uma única aplicação pode escutar uma porta.

Segundo Murhammer et al (2000) há dois tipos de portas, as bem conhecidas e as efêmeras.

As portas do tipo bem conhecidas pertencem a servidores padrão e são controladas pela IANA. Variam de 1 a 1023. Já as portas do tipo efêmeras não são controladas pela IANA e podem ser utilizadas por aplicações comuns desenvolvidas pelo próprio usuário. Variam de 1024 a 65535.

2.7 SEGMENTAÇÃO DE REDES

Segmentando a rede, divide-se o domínio de colisão, fazendo com que aumente a largura de banda disponível para as estações individuais (BIRKNER, 2003).

As redes podem ser segmentadas utilizando sub-redes ou VLAN.

2.7.1 Sub-redes

Sub-redes têm sido utilizadas para limitar os tamanhos dos domínios de *broadcast* da rede, oferendo vantagens significativas no desempenho (NORTHCUTT et al, 2002).

A máscara de rede é um valor de 32 bits, dividido em 4 bytes. Cada bit que indica rede é colocado em nível lógico 1 e cada bit que indica *host* é colocado em nível lógico 0. As máscaras padrão em redes são: para classe A 255.0.0.0, para classe B 255.255.0.0 e para classe C 255.255.255.0. Para criar uma sub-rede é preciso quebrar estas máscaras, ou seja, alterar o endereçamento da rede, mudar os bits do endereço utilizado para identificar a rede e os bits usados para identificar os *hosts*. Sub-redes podem ser criadas em qualquer classe de rede (TORRES, 2009).

O administrador pode definir um número grande de sub-redes com poucos *hosts* ou um número menor de sub-redes com muitos *hosts* (MURHAMMER et al, 2000).

2.7.2 VLAN

Para montar uma rede em um edifício necessitava-se de muitos cabos, e em resposta dos usuários que queriam maior flexibilidade, os fornecedores de redes começaram a buscar um novo meio de recompor a parte física para uma parte lógica. Com isso surgiu o conceito de VLAN (TANENBAUM, 2003).

Uma VLAN, segundo Veras (2009), é um domínio de *broadcast* criado por um ou mais *switches*. Fazendo uso destas, o administrador tem controle sobre portas e usuários.

Utilizar-se de VLAN para segmentação da rede física em diversas redes lógicas resulta em uma performance mais apurada, pois o domínio de *broadcast* é quebrado (CALDAS FILHO; FERREIRA, 2013).

Além de concentrar melhor o tráfego, diminuindo o domínio de *broadcast*, as VLAN também resolvem outras dificuldades, como o uso ineficiente de comutadores e o gerenciamento de usuários, pois se um usuário se locomove entre os grupos todo cabeamento físico deve ser revisto, no caso de LAN (KUROSE; ROSS, 2010).

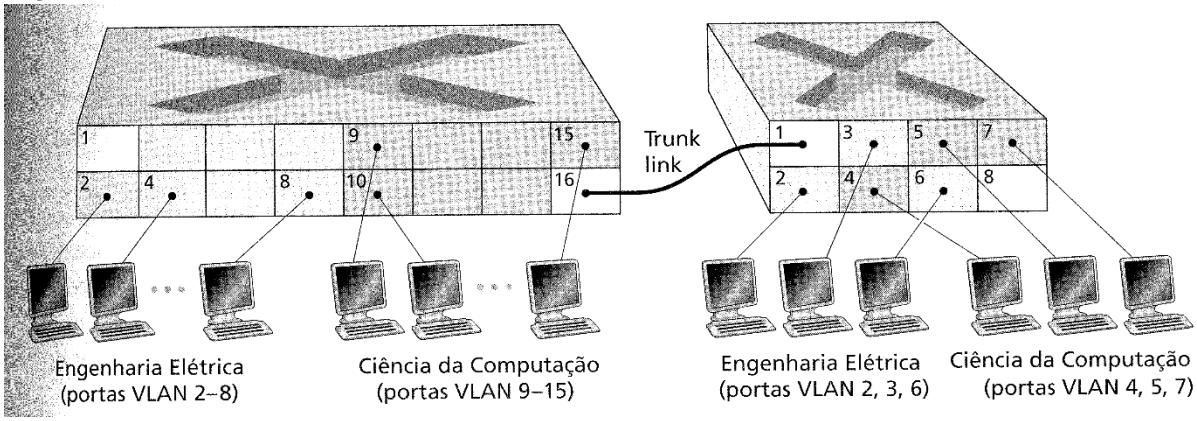
Ainda segundo Kurose e Ross um comutador que suporta VLAN permite que várias redes locais virtuais sejam implementadas através de uma única infraestrutura física. Em uma VLAN baseada em pontos, as interfaces do comutador são divididas em grupos, ou seja, em VLAN, e cada uma possui o seu domínio de *broadcast*.

Para Kurose e Ross existem também outras formas de VLAN, como a baseada em MAC, no qual o administrador pode dividir os dispositivos em VLAN através de seu MAC Address. Quando o dispositivo for conectado ao comutador, a porta se conecta na VLAN específica.

Para interconectar os comutadores das VLAN utiliza-se de uma abordagem chamada de entroncamento (figura 14). Em cada comutador uma porta é configurada

como porta de tronco, que pertence a todas as VLAN. E os quadros enviados a uma VLAN são encaminhados através do enlace tronco para o outro comutador.

Figura 14 – Entroncamento de VLAN



Fonte: Kurose e Ross (2010).

Este recurso é muito importante pois se a rede na empresa for separada por setores, os funcionários podem estar em locais distintos, mas fazendo parte da mesma VLAN (MORAES, 2008).

Ainda segundo Moraes as vantagens de se usar VLAN são muitas. Dentre elas destacam-se o aumento da performance, pois o domínio de *broadcast* é menor, facilidade de gerenciamento, que torna-se mais simples e muito mais rápido, topologia de rede independente, ou seja, a rede lógica fica completamente independente da rede física, tornando a rede bastante flexível a modificações e aumento da segurança, pois pode-se separar da rede sistemas como dados sigilosos, impedindo o acesso não autorizado.

2.8 SEGURANÇA EM REDES

Assim que as redes de computadores surgiram estas eram usadas por pesquisadores, universitários para o envio de mensagens de correio eletrônico e por empresas para o compartilhamento de recursos. Diante disto, não havia necessidade de muitos cuidados. Mas com o uso cada vez maior das redes, seja para acesso bancário, compras, dentre outras utilidades, cresceu também os problemas relacionados com a segurança das mesmas (TANENBAUM, 2003).

Tanenbaum ainda destaca que a segurança em redes é algo bastante abrangente, incluindo vários problemas. Na camada de enlace os pacotes podem ser

codificados ao saírem da máquina e decodificados quando entram em outro sistema. Na camada de rede firewalls podem ser instalados para filtrar os pacotes. Na camada de transporte conexões fim-a-fim podem ser criptografadas inteiras e por fim, na camada de aplicação podem ser tratados a autenticação do usuário e o não-repúdio. Com exceção da camada física, quase toda a segurança envolvida nas outras camadas é baseada em criptografia.

A segurança em redes não depende somente da tecnologia envolvida mas de um conjunto de etapas que devem ser seguidas. O acesso físico, as senhas, os equipamentos, devem ser levados em conta, bem como a prevenção (TORRES, 2009).

Para Kurose e Ross (2010) uma rede segura deve proporcionar: confidencialidade, autenticação, integridade e segurança operacional.

A confidencialidade consiste no fato de somente o remetente e o destinatário poderem entender o conteúdo da mensagem enviada, estando esta cifrada para os demais não a compreenderem. A mensagem é protegida para que usuários não autorizados não possam ter acesso a ela.

Confirmar a identidade dos envolvidos na comunicação, ou seja, confirmar realmente se é quem se alega ser, dá-se o nome de autenticação.

A integridade garante que os dados envolvidos na comunicação não sejam alterados sem a autorização do autor da mensagem, o conteúdo da comunicação permanece íntegro. Já a segurança operacional é composta por mecanismos como firewalls e sistemas de detecção de invasão.

Outra forma de aumentar a segurança e também o desempenho é usando filtragem de pacotes. Uma ACL tem essa função. Ela é uma lista de instruções, que podem permitir ou negar endereços ou protocolos da camada superior, aumentando assim a segurança e mantendo o controle de tudo que está trafegando na rede. A ACL retira do cabeçalho do pacote alguns dados e os compara com suas regras configuradas, tomando as decisões corretas (JUNG; PELLIS, 2013).

Um filtro de pacotes é composto por um IP de origem e destino, um datagrama e um número de porta de protocolo. Desta forma somente os serviços especificados pelas portas de protocolo no filtro de pacotes estarão disponíveis entre os dispositivos (COMER, 2007).

Para Murhammer et al (2000) o filtro de pacotes é aplicado, geralmente, em roteadores, que envia os pacotes de acordo como as regras de filtragem. Ao chegar no roteador são extraídas algumas informações do cabeçalho do pacote e de acordo com as regras do filtro o roteador toma as decisões, como por onde o pacote passará ou se será descartado.

2.9 GERÊNCIA DE REDES

Segundo Comer (2007) a gerência de redes é fundamental, pois falhas de hardware e software que compõe a rede poderão causar problemas, devido a isto há necessidade de monitorá-la.

Comer ainda destaca que essa administração não é simples. Muitas redes são heterogêneas, ou seja, possuem componentes de hardware e software de diferentes fabricantes e, também muitas das redes são extensas, sendo partes delas remota, tornando mais difícil sua administração. Outro fator que dificulta a administração é o fato de as redes serem projetadas para se recuperarem de erros automaticamente.

Um gerenciamento de rede é capaz de prever e agilizar a correção de vários problemas, como a detecção de falha em uma placa de rede em um dispositivo, monitoração de um dispositivo, monitoração de tráfego, detecção de mudanças em tabelas de roteamento, monitoração de Service Level Agreements (SLA), Acordos de Nível de Serviço e detecção de intrusos (KUROSE; ROSS, 2010).

Kurose e Ross indicam também que são definidas cinco áreas de gerenciamento de rede, segundo a International Organization for Standardization (ISO), do qual deu-se o nome de FCAPS (Fault, Configuration, Accounting, Performance and Security) em português, Falha, Configuração, Contabilidade, Desempenho e Segurança.

O gerenciamento de desempenho, que quantifica, mede, analisa e controla o desempenho dos vários dispositivos da rede. O gerenciamento de falhas registra, detecta e reage às condições de falhas na rede, sendo um tratamento imediato. Com o gerenciamento de configuração o administrador pode saber quais dispositivos fazem parte da rede, bem como suas versões de hardware e software. Especificar, registrar e controlar o acesso de usuários e dispositivos a determinados recursos da rede faz-

se por meio do gerenciamento de contabilização. O gerenciamento de segurança tem o objetivo de controlar o acesso aos recursos da rede seguindo alguma política definida, como os firewalls.

> Gerenciamento de rede inclui o oferecimento, a integração e a coordenação de elementos de hardware, software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer às exigências operacionais, de desempenho e de qualidade de serviço em tempo real a um custo razoável. (SAYDAM, 1996 apud KUROSE; ROSS, 2010, p. 556).

2.9.1 Softwares de gerência de redes

As ferramentas de gerenciamento visam facilitar, auxiliar o gerente na descoberta de problemas para que este esteja a par do que está ocorrendo na rede.

2.9.1.1 MRTG

MRTG é um software livre bastante utilizado para análises estatísticas em redes. Ele pode ser executado em sistemas Unix, Linux, Windows e incorporado em softwares de terceiros. Os seus gráficos são derivados das informações provenientes do SNMP. O MRTG é feito em Perl, uma linguagem de programação multiplataforma mais utilizada em desenvolvimento web (SEAGREN, 2007, tradução nossa).

Com um *script* Perl, usando o SNMP os contadores de tráfego são lidos nos equipamentos e um programa em linguagem C registra este tráfego e cria os gráficos da conexão monitorada. Os gráficos são incorporados em páginas web, podendo ser visualizado em qualquer navegador (OETIKER, 2002, tradução nossa).

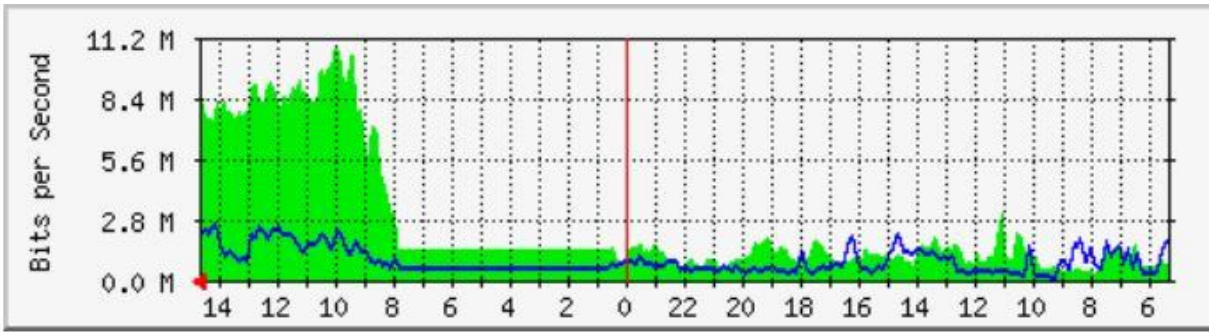
Oetiker relata também que o MRTG proporciona uma visão detalhada do tráfego de rede diária, dos últimos sete dias, das últimas cinco semanas e dos últimos doze meses.

E ainda como este monitoramento é visualizado em páginas web, esta pode ser totalmente configurada.

O MRTG é uma ferramenta bastante útil quando se quer apresentar a evolução temporal de um valor monitorado via SNMP, podendo assim, ser utilizado não somente para monitorar o tráfego de rede de uma interface, mas tendo outras opções de configuração (CONTESSA; POLINA, 2013).

Conforme Dias e Alves Júnior (2006) para o MRTG funcionar, precisa-se ter instalado um interpretador Perl. Após configurações das variáveis a serem monitoradas o MRTG fornece gráficos semelhantes a figura 15, que mostra um gráfico diário do MRTG, sendo traçado a cada cinco minutos.

Figura 15 – Gráfico diário do MRTG



Fonte: Dias e Alves Júnior (2006).

2.9.1.2 Nagios

O Nagios é um software de gerenciamento de rede que permite identificar e resolver problemas de infraestrutura de Tecnologia da Informação (TI) antes que estes se tornem mais críticos.

Segundo Andrade (2006) o Nagios foi criado e ainda é mantido por Ethan Galstad e sua equipe. Originalmente tinha o nome de *Netsaint*. É um software distribuído livremente.

Andrade ainda afirma que apesar de o Nagios ser projetado para redes de grande porte, ele apresenta bom desempenho em redes pequenas.

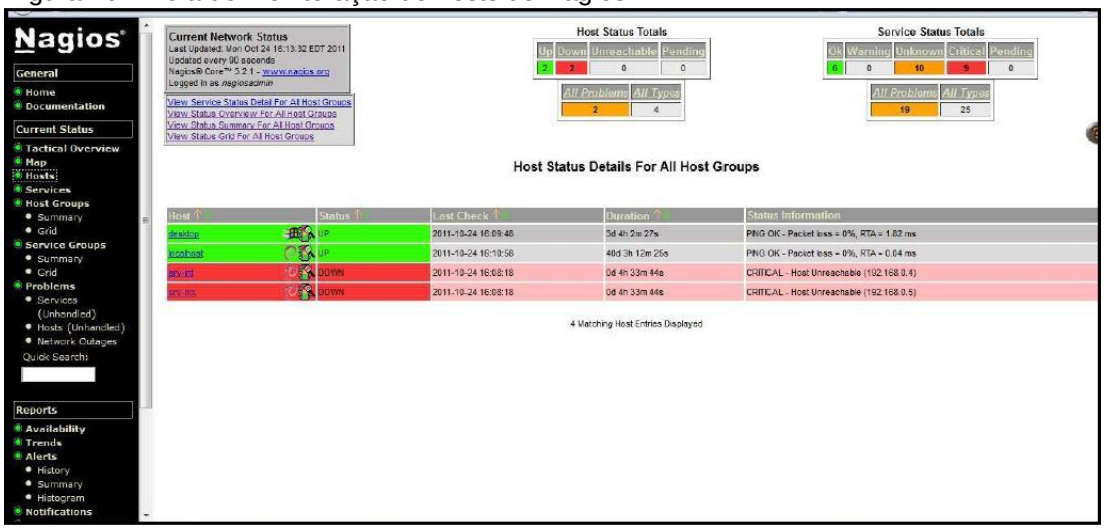
Para torná-lo ainda mais eficaz, o Nagios conta com expansão através de *plug-ins*, que são complementos. Estes complementos podem ser desenvolvidos por diferentes programadores, mas também tem-se vários *plug-ins* oficiais (ANDRADE, 2006).

O Nagios é uma ferramenta que possui vários *plug-ins*, cada um com uma função específica. Com ele o desempenho e a agilidade na correção de falhas é muito rápido. Erros e defeitos em hardwares podem ser notificados com antecedência, de forma que possa ser resolvido sem maiores problemas (SALKYS et al, 2007).

O Nagios gerencia equipamentos de rede, serviços e hardwares com o objetivo de detectar falhas, gerando alertas e notificações de eventos (DIAS et al, 2009).

Para Cardoso (2011) a interface do Nagios é disposta de forma simples, facilitando ao administrador verificar os erros e tomar as providencias necessárias com agilidade. Na figura 16 pode-se observar a tela do Nagios com alguns *hosts* monitorados.

Figura 16 – Tela de monitoração de hosts do Nagios



Fonte: Cardoso (2011).

As notificações de falhas podem ser enviadas ao administrador por e-mail, mensagens instantâneas, Short Message Service (SMS), dentre outras e em tempo real. Possui interface web (BITTENCOURT JUNIOR; OE; SANTANNA, 2005).

Andrade (2006) diz que o Nagios é composto de três partes: um *scheduler*, que é parte do servidor e verifica os *plug-ins* em intervalos de tempo, executando ações; um Graphical User Interface (GUI), ou seja, interface do Nagios, que é exibido em páginas web; e pelos *plug-ins*, que conferem os serviços e são configurados pelo usuário.

3 TRABALHOS CORRELATOS

Esta seção traz alguns trabalhos científicos semelhantes a esta pesquisa.

3.1 DETECÇÃO E CLASSIFICAÇÃO DE ANOMALIAS NO TRÁFEGO DE REDES DE COMPUTADORES

Trabalho de Conclusão de Curso de Guilherme Fernandes Raphanelli, para obtenção do grau de Bacharel em Ciência da Computação, em 2008, pela Universidade Federal de Santa Catarina – UFSC.

O trabalho desenvolve um estudo sobre anomalias de rede, ressaltando a importância da monitoração e gerenciamento das redes. Fez-se um algoritmo que realiza a detecção e classificação automatizada das anomalias do tráfego de rede.

Como resultado, o trabalho proporcionou a diferenciação de diferentes tipos de anomalias de forma bem expressiva.

3.2 SEGMENTAÇÃO DE REDES COM VLAN

Artigo desenvolvido por Leonardo Haffermann para a Pós Graduação em Redes e Segurança de Sistemas da Pontifícia Universidade Católica do Paraná, em 2009.

No trabalho é feito um estudo das diferentes características e configurações das VLAN e com isso, pode-se comparar as diversas formas de implantação, observando sua flexibilidade e versatilidade.

Conclui-se que não há um modo geral de aplicar as VLAN, deve-se levar em conta o ambiente, as tecnologias e as necessidades e assim aplicar uma de suas formas. Ressaltando-se que os resultados são promissores, principalmente na questão de melhoria de trafegabilidade de dados na rede.

3.3 GERENCIAMENTO DE REDES

Trabalho de Conclusão de Curso de Wamilson Luiz Candido do Curso de Técnico em Manutenção e Suporte em Informática do Instituto Federal do Paraná, em 2011.

No trabalho é descrito a importância do gerenciamento da rede, bem como a necessidade de um software que faça este procedimento, detecte os problemas para auxiliar o gerente de informática a solucioná-los o mais rápido possível.

Tem-se com um software de gerenciamento um aumento da eficiência da equipe de Informática na resolução de problemas, pois estes são detectados com mais rapidez. Com o gerenciamento pode-se aumentar a qualidade no serviço.

3.4 REESTRUTURAÇÃO DAS CAMADAS 2 E 3 (ENLACE E REDE) DA UTFPR CAMPUS CURITIBA

Trabalho de Conclusão de Curso desenvolvido por Pedro Henrique Modesto Deguchi e Francisco Bittencourt dos Santos para obtenção do título de Tecnólogo em Desenvolvimento de Sistemas Distribuídos pela Universidade Tecnológica Federal do Paraná – UTFPR, em 2012.

No trabalho é descrito como a rede da UTFPR estava estruturada e que vinha enfrentando alguns problemas como um grande domínio de *broadcast*, descentralização da rede, criação de gargalos e baixa disponibilidade.

Com a aquisição de novos *switches* de camada 2 e 3 e a utilização de VLAN pode-se segmentar a rede, mudando sua estrutura lógica e assim, resolvendo os problemas que a rede enfrentava.

3.5 IMPLANTAÇÃO DA FERRAMENTA NAGIOS PARA MONITORAÇÃO DE REDE E ANÁLISE E TRATAMENTO DOS EVENTOS POR MEIO DE SOFTWARES DE APOIO

Trabalho de Conclusão de Curso de Leandro Koehler Cardoso para obtenção do Grau de Bacharel no Curso de Ciência da Computação pela Universidade do Extremo Sul Catarinense – UNESC, em 2011.

No trabalho é descrito a importância do gerenciamento e monitoração das redes. Buscou-se verificar o comportamento do software livre Nagios, juntamente com a ferramenta de apoio Cacti, para monitoração de uma rede.

Com a implantação das ferramentas conclui-se que são de grande utilidade e importância para o gerenciamento de rede. Elas auxiliam o administrador no seu trabalho, tendo este, uma rede estável e confiável, pois problemas podem ser solucionados com mais antecedência, evitando danos maiores.

4 ANÁLISE, GERENCIAMENTO E MONITORAMENTO DA REDE NA SATC

Apresenta-se os dados pertinentes ao estudo deste trabalho. Em um primeiro momento se descreve o ambiente da instituição onde foi aplicado o estudo de caso e também motivo pelo qual se optou realizar este estudo.

Sequencialmente descreve-se sobre o método de segmentação e controle de acessos implantados, juntamente com softwares de monitoramento e gerenciamento que passaram a auxiliar a equipe de TI.

4.1 DESCRIÇÃO DO AMBIENTE

Este trabalho tem como escopo a rede da instituição SATC. Atualmente a SATC dispõe de 22 laboratórios de informática com acesso à rede, com cerca de 480 computadores. Além disso tem-se ainda os setores corporativos, servidores, salas de pesquisa, rede *wireless* que é disponível a alunos, professores, colaboradores e a visitantes em geral, com aproximadamente 350 dispositivos conectados diariamente, equipamentos destinados a segurança eletrônica, como centrais de câmeras, alarmes e controles de acesso e também os geradores de energia elétrica. Ao todo, os dispositivos conectados à rede chegam em torno de mil.

A rede provê serviços de e-mail, terminal *server*, Internet, entre outros e todos os dispositivos são executados sobre o protocolo TCP/IP.

A rede possui um design hierárquico, ou seja, ela é dividida em camadas: núcleo, distribuição e acesso.

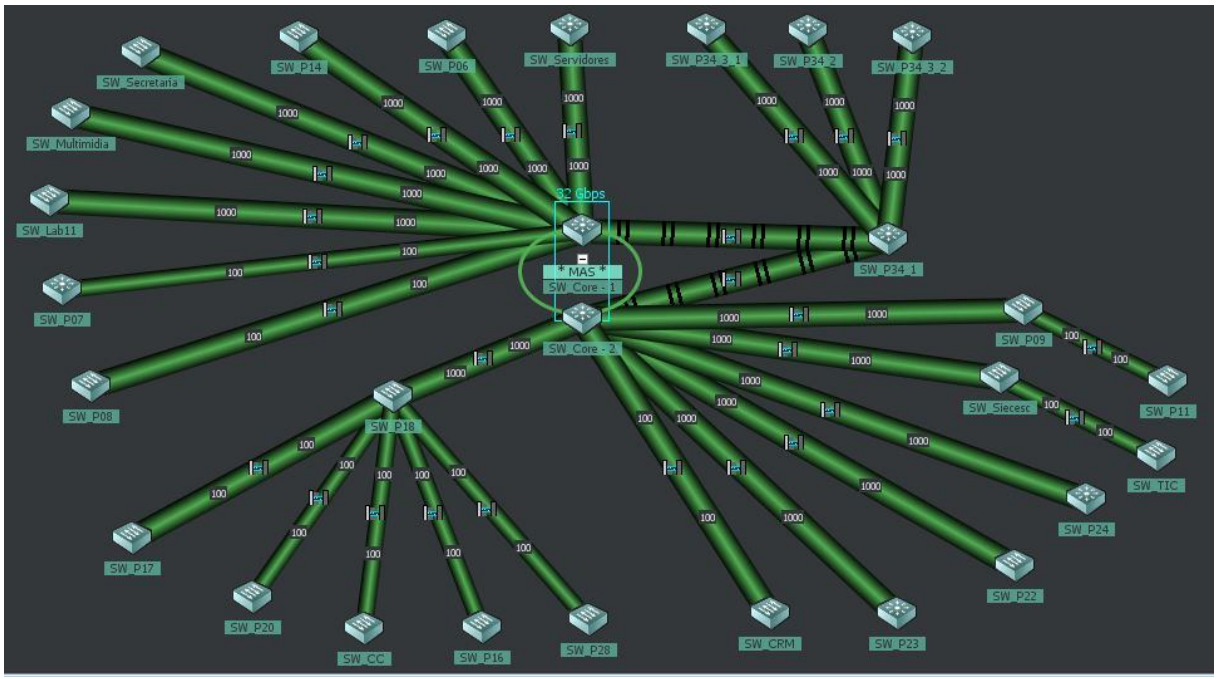
A camada de núcleo é onde os dispositivos da camada de distribuição são conectados, necessitando de maior velocidade e disponibilidade, para tal tem-se dois *switches* Cisco Catalyst 3750G-24T conectados a 32 Gbps.

A camada de distribuição recebe os dados da camada de acesso antes de serem transmitidos para o núcleo. Na instituição tem-se 26 *switches* Cisco de diferentes modelos que operam nesta camada: Cisco Catalyst 2950-24, 2960-24TT, 2960-24TC, 2960S-24PS-L, 2960S-24TS-L, 29060G-24TC e 3560-24+2. Alguns são conectados ao núcleo a Gigabit Ethernet e outros a Fast Ethernet. E também há uma conexão a 4GB, utilizando o recurso de *PortChannel*, que utiliza 4 portas Gigabit Ethernet do *switch*, criando uma espécie de link agregado e redundante.

A camada de acesso conecta os dispositivos finais, como computadores, impressoras, telefones. Os *switches* que atuam nesta camada não são gerenciáveis.

A estrutura da rede, com os 28 *switches* gerenciáveis, da camada de núcleo e distribuição, pode ser observada na figura 17.

Figura 17 – Estrutura da rede gerenciada



Fonte: Do autor.

4.1.1 Sistemas operacionais

Nos servidores têm-se o sistema operacional Microsoft Windows 2008 R2 Server, Windows 2012 Server, Windows 2003 Server e GNU/Linux Debian 6 e 7. Os computadores de laboratórios e corporativos possuem Microsoft Windows XP, Windows 7, Windows 8 e Windows 8.1, Apple Mac OS X Mavericks. No acesso à rede *wireless* tem-se diferentes sistemas operacionais, com diferentes versões do Android, IOs, Windows Phone, Microsoft Windows, Linux, entre outros.

4.1.2 Serviços

Há vários serviços disponibilizados na rede corporativa, como DHCP, DNS, serviços de impressão, de terminal, de arquivos, de e-mail, Internet, que atendem uma gama de usuários.

O objetivo principal é de que estes serviços estejam disponíveis a todo momento, funcionando de forma eficaz e segura, afim de não desagradar aos usuários da rede. Por isso algumas soluções são necessárias para nortear o administrador quando algum problema está para acontecer ou surge repentinamente. Dividir a rede em segmentos e gerenciá-los é o que se recomenda.

Numa rede com centenas ou milhares de estações é impossível gerenciar e prever problemas manualmente. Com uma rede segmentada e monitorada torna-se muito mais fácil e eficaz o trabalho do administrador, que com alertas pode resolver determinado problema de forma muito mais ágil.

4.2 SEGMENTAÇÃO E FILTRAGEM DE PACOTES

Com o objetivo de tornar a rede mais estável, rápida e fácil de gerenciar, descartando o tráfego de pacotes não essenciais, através da filtragem dos mesmos, deu-se sequência a segmentação da rede.

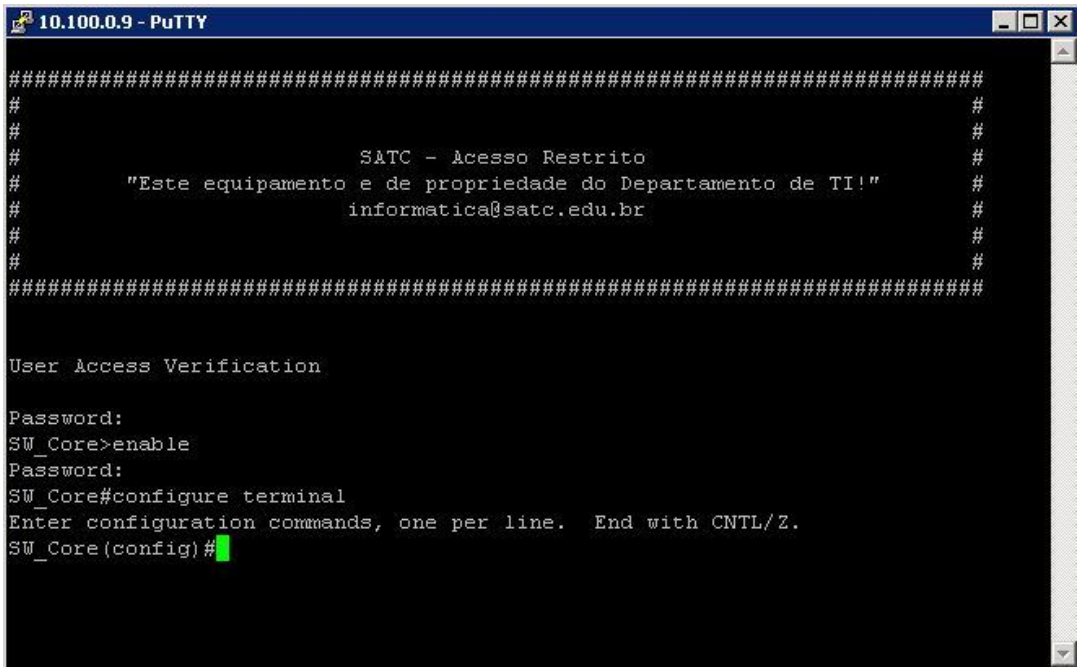
4.2.1 Implantação da segmentação

A instituição dispõe de 22 laboratórios, salas de pesquisa, rede *wireless*, corporativa e serviços de segurança e controle. Para tal, tinha-se algumas VLAN. Depois de analisada a rede foi segmentada da seguinte forma: uma VLAN para cada laboratório, uma para segurança eletrônica, cinco para *Wireless*, sendo estas de gerência, administrativa, para alunos, para professores e de testes, uma para serviços, que inclui os geradores de energia elétrica, uma para pesquisas, uma para uma rede ADSL externa, uma corporativa e uma de servidores. Separando logicamente toda a rede.

Estas VLAN foram criadas no *switch* do núcleo da rede e seu acesso pode ser feito via console, diretamente conectado no mesmo com cabo serial ou via IP com telnet. Para ambos utilizou-se do software Putty, que permite ambas conexões.

A tela de configuração do *switch* através do software Putty pode ser observada na figura 18.

Figura 18 – Tela de configuração do *switch*



Fonte: Do autor.

Em cada *switch*, basicamente foram configuradas as senhas de acesso, habilitado o SNMP e criado um segmento de gerência, a qual fornecerá o seu IP. As portas foram configuradas de acordo com a utilização a que se referem, seja para uso corporativo, em laboratório ou tronco, conexão entre *switches* em que mais de uma VLAN é utilizada, ou seja, utilizou-se da técnica de VLAN baseada em pontos.

Estas VLAN foram criadas cada uma com uma configuração, com nomes, IP, *gateways* e classes diferentes, de forma que atendam às necessidades. Foram criadas no *switch core*, do núcleo da rede, e os *switches* de distribuição passaram a entender as mesmas. As VLAN criadas, seus nomes e máscaras de rede podem ser vistos na figura 19.

Figura 19 – VLAN da instituição

VLAN	Nome	Máscara
100	Gerencia SW	255.255.0.0
101	Servidores	255.255.255.0
102	P10_L04	255.255.255.0
103	P22_L18-19	255.255.255.0
104	P07_L05	255.255.255.0
105	P18_L18	255.255.255.0
106	P07_L06	255.255.255.0
107	P10_L24-25	255.255.255.0
108	P10_L11	255.255.255.0
109	P09_L07	255.255.255.0
110	P20_L10	255.255.255.0
111	P23_L33	255.255.255.0
112	P17_L03	255.255.255.0
113	P24_L25	255.255.255.0
114	P23_L22	255.255.255.0
115	P10_L23	255.255.255.0
116	P20_L01	255.255.255.0
117	P10_L10	255.255.255.0
118	P08_L01	255.255.255.0
119	P13_L01	255.255.255.0

VLAN	Nome	Máscara
120	Wifi	255.255.255.0
121	Ilhas	255.255.255.0
122	SSE-CFTV	255.255.255.0
123	P14_L07	255.255.255.0
124	P10_L13-14	255.255.255.0
125	Administrativo	255.255.254.0
126	P07_L16	255.255.255.0
127	P14_LB	255.255.255.0
128	P34_CTCL	255.255.255.0
129	Telefonia	255.255.255.0
130	P17_L10	255.255.255.0
131	Serviços	255.255.255.0
132	Wireless-Aluno	255.255.0.0
133	Wireless-Visitante	255.255.255.0
134	Wireless-Professor	255.255.0.0
135	Wireless-Administrativo	255.255.0.0
136	Wireless-Gerencia	255.255.255.0
137	P17_L03	255.255.255.0
138	SSE-Alarme	255.255.255.0
1256	ADSL	255.255.255.0

Fonte: Do autor.

No tronco de cada *switch* passa somente as VLAN necessárias, utilizando o recurso *trunk allowed vlan* dos *switches*.

Criou-se as VLAN no *switch* e após criou-se também o escopo de cada rede no servidor DHCP, fazendo reserva dos *hosts* que não mudam, computadores dos laboratórios, por exemplo. Foi criado a reserva de cada máquina e excluído os IP não utilizados.

Nos *switches* também se configurou o protocolo *spanning tree*, que resolve problemas de *loop* na rede, auxiliando em melhor performance.

4.2.2 Implantação da filtragem de pacotes

A fim de diminuir o tráfego da rede, foram liberados somente os pacotes essenciais a cada serviço. Foi criado uma ACL no *switch core* da rede, a qual descarta todo o tráfego para as portas não contidas na lista.

Com o auxílio do software gratuito Windump diagnosticou-se quais portas os serviços estavam utilizando. Em cada setor, segmento, foi analisado os serviços que seriam necessários e liberados somente as portas destes.

Uma única ACL, na entrada do *switch*, faz o controle de acesso das VLAN.

Esta ACL, além de tornar a rede mais segura, colabora para o desempenho, pois diminui o tráfego de pacotes na rede. A rede pode ser utilizada por qualquer usuário, tornando-a mais suscetível a ataques, mas bloqueando o acesso a portas desnecessárias para utilização em geral, isto fica mais difícil.

Na ACL foi liberado para toda a rede os serviços de DNS e DHCP. Para os *hosts* da TI foi concedido acesso liberado a tudo. Liberou-se também o acesso remoto aos servidores de terminal, o acesso ao compartilhamento das pastas do servidor de arquivos, o acesso as impressoras do servidor de impressão e acesso a licenças no servidor de licenças. Na rede de segurança é liberado somente o acesso a transmissão de imagens.

A ACL contendo todas as regras aplicadas é listada na figura 20. Destaca-se que a última linha da ACL é implícita e contém o comando: *deny ip any any*, que bloqueia tudo o que não foi permitido nas linhas acima.

Figura 20 - ACL

```
permit udp any 10.1.1.254 0.0.0.255 eq 53
permit tcp any host 10.255.255.254 eq 8080
permit tcp any host 10.255.255.254 eq 88
permit udp any host 10.1.1.179 eq 1812
permit udp any host 10.1.1.179 eq 1813
permit udp any host 10.1.1.102 eq 1812
permit udp any host 10.1.1.102 eq 1813
permit tcp any host 10.1.1.21 eq 3389
permit tcp any host 10.1.1.23 eq 3389
permit tcp any host 10.1.1.170 eq 3389
permit udp any any eq 67
permit tcp any any eq 80
permit tcp any any eq 443
permit udp any any eq 123
permit tcp any host 10.1.1.179 eq 389
permit tcp any host 10.1.1.179 eq 445
permit tcp any host 10.1.1.179 eq 135
permit tcp any host 10.1.1.179 range 1024 65535
permit udp any host 10.1.1.179 range 49152 65535
permit tcp any eq 389 host 10.1.1.179
permit tcp any eq 445 host 10.1.1.179 eq 135
permit tcp any range 1024 65535 host 10.1.1.179
permit udp any range 49152 65535 host 10.1.1.179
permit tcp any host 10.1.1.102 eq 389
permit tcp any host 10.1.1.102 eq 445
permit tcp any host 10.1.1.102 eq 135
permit tcp any host 10.1.1.102 range 1024 65535
permit udp any host 10.1.1.102 range 49152 65535
permit tcp any eq 389 host 10.1.1.102
permit tcp any eq 445 host 10.1.1.102 eq 135
permit tcp any range 1024 65535 host 10.1.1.102
permit udp any range 49152 65535 host 10.1.1.102
permit icmp any host 10.1.1.10
permit tcp 10.9.0.0 0.0.0.255 eq 5800 10.1.2.0 0.0.1.255
permit tcp 10.9.0.0 0.0.0.255 eq 11400 10.1.2.0 0.0.1.255
permit tcp 10.9.0.0 0.0.0.255 eq 11100 10.1.2.0 0.0.1.255
permit tcp 10.9.0.0 0.0.0.255 eq 9100 10.1.2.0 0.0.1.255
permit tcp 10.9.0.0 0.0.0.255 host 10.1.3.138 eq 135
permit udp 10.9.0.0 0.0.0.255 host 10.1.3.138 eq 137
permit udp 10.9.0.0 0.0.0.255 host 10.1.3.138 eq 138
permit tcp 10.9.0.0 0.0.0.255 host 10.1.3.138 eq 139
permit udp 10.9.0.0 0.0.0.255 host 10.1.3.138 eq 389
permit tcp 10.9.0.0 0.0.0.255 host 10.1.3.138 eq 445
permit tcp 10.20.0.0 0.0.0.255 10.22.0.0 0.0.0.255 eq 37777
permit tcp 10.22.0.0 0.0.0.255 eq 80 any
permit tcp 10.22.0.0 0.0.0.255 eq 37777 any
permit tcp any any eq 4060
permit tcp any any eq 1720
permit udp any any eq 4061
permit udp any any eq 5010
permit udp any any eq 1300
permit tcp any any eq 21
permit tcp any any eq 443 any
permit udp any any eq 1720 any
permit tcp any any eq 1720 any
permit tcp any any eq 4060 any
permit udp any any eq 4061 any
permit udp any any eq 5010 any
permit udp any any eq 1300 any
permit tcp any any eq 21 any
permit tcp any host 10.1.1.168 eq 135
permit udp any host 10.1.1.168 eq 137
permit udp any host 10.1.1.168 eq 138
permit tcp any host 10.1.1.168 eq 139
permit tcp any host 10.1.1.168 eq 389
permit udp any host 10.1.1.168 eq 445
permit tcp any host 10.1.1.168 eq 445
permit tcp any host 10.1.1.167 eq 80
permit tcp any host 10.1.1.167 eq 443
permit tcp any host 10.1.1.167 eq 445
permit tcp any host 10.1.1.167 eq 1433
permit tcp any host 10.1.1.167 eq 3268
permit tcp any host 10.1.1.167 eq 3269
permit tcp any host 10.1.1.167 eq 10123
permit tcp any host 10.1.1.167 eq 3389
permit tcp any host 10.1.1.167 eq 135
permit tcp any host 10.1.1.167 eq 2701
permit udp any host 10.1.1.167 eq 2701
permit udp any host 10.1.1.161 eq 65450
permit udp any host 10.1.1.167 eq 67
permit udp any host 10.1.1.167 eq 68
permit udp any host 10.1.1.167 eq 69
permit udp any host 10.1.1.167 eq 4011
permit udp any host 10.1.1.167 eq 135
permit udp any host 10.1.1.167 range 63000 64000
permit tcp any eq 80 host 10.1.1.167
permit tcp any eq 443 host 10.1.1.167
permit tcp any eq 445 host 10.1.1.167
permit tcp any eq 1433 host 10.1.1.167
permit tcp any eq 3268 host 10.1.1.167
permit tcp any eq 3269 host 10.1.1.167
permit tcp any eq 10123 host 10.1.1.167
permit tcp any eq 3389 host 10.1.1.167
permit tcp any eq 135 host 10.1.1.167
permit tcp any eq 2701 host 10.1.1.167
permit udp any eq 67 host 10.1.1.167
permit udp any eq 68 host 10.1.1.167
permit udp any eq 69 host 10.1.1.167
permit udp any eq 4011 host 10.1.1.167
permit udp any eq 135 host 10.1.1.167
permit udp any range 63000 64000 host 10.1.1.167
permit tcp 10.20.0.0 0.0.0.255 range 50000 55000 host 10.1.1.5
permit tcp 10.20.0.0 0.0.0.255 eq 8080 any
permit ip any host 10.1.2.3
permit ip any host 10.1.2.6
permit ip any host 10.1.2.7
permit ip any host 10.1.2.8
permit ip any host 10.1.2.12
permit ip any host 10.1.2.84
permit tcp 10.1.2.0 0.0.1.255 eq 9100 10.15.0.0 0.0.0.255
permit tcp 10.15.0.0 0.0.0.255 host 10.1.1.2 eq 135
permit udp 10.15.0.0 0.0.0.255 host 10.1.1.2 eq 137
permit udp 10.15.0.0 0.0.0.255 host 10.1.1.2 eq 138
permit tcp 10.15.0.0 0.0.0.255 host 10.1.1.2 eq 139
permit tcp 10.15.0.0 0.0.0.255 host 10.1.1.2 eq 389
permit udp 10.15.0.0 0.0.0.255 host 10.1.1.2 eq 389
permit tcp 10.15.0.0 0.0.0.255 host 10.1.1.2 eq 445
permit tcp 10.15.0.0 0.0.0.255 host 10.1.1.165 eq 135
permit udp 10.15.0.0 0.0.0.255 host 10.1.1.165 eq 137
permit udp 10.15.0.0 0.0.0.255 host 10.1.1.165 eq 138
permit tcp 10.15.0.0 0.0.0.255 host 10.1.1.165 eq 139
permit tcp 10.15.0.0 0.0.0.255 host 10.1.1.165 eq 389
permit udp 10.15.0.0 0.0.0.255 host 10.1.1.165 eq 389
permit tcp 10.15.0.0 0.0.0.255 host 10.1.1.165 eq 445
permit tcp 10.15.0.0 0.0.0.255 host 10.1.1.165 eq 1935
permit tcp any any eq 1935
permit tcp any host 10.50.0.1 eq 8080
permit tcp any host 10.50.0.1 eq 88
permit tcp any any eq 2900
permit ip any host 177.54.52.203
permit ip any host 177.54.52.204
permit tcp 10.26.0.0 0.0.0.255 range 40000 60000 host 10.1.1.181
permit tcp 10.4.0.0 0.0.0.255 range 40000 60000 host 10.1.1.181
permit tcp 10.3.0.0 0.0.0.255 range 40000 60000 host 10.1.1.181
permit tcp 10.6.0.0 0.0.0.255 range 40000 60000 host 10.1.1.181
permit tcp 10.14.0.0 0.0.0.255 range 40000 60000 host 10.1.1.181
permit tcp 10.30.0.0 0.0.0.255 range 40000 60000 host 10.1.1.181
permit tcp 10.12.0.0 0.0.0.255 range 40000 60000 host 10.1.1.181
permit tcp any any eq 3128
permit tcp any any eq 3456
```

Fonte: Do autor.

4.3 FERRAMENTAS DE MONITORAMENTO

Neste trabalho foram estudadas e implantadas duas ferramentas de monitoramento, o MRTG, que monitora o tráfego de rede das portas dos *switches* e do firewall, e o Nagios que verifica se os equipamentos estão acessando a rede, como *switches*, pontos de acesso *wireless* e pontos de acesso do tipo *bullets*, que são antenas de links sem fio de linha empresarial.

4.3.1 Implantação do MRTG

A ferramenta de monitoramento, MRTG, foi instalada em um servidor com sistema operacional Windows Server 2008 R2 Standard. Os passos para a sua instalação e configuração são descritos no apêndice A deste trabalho.

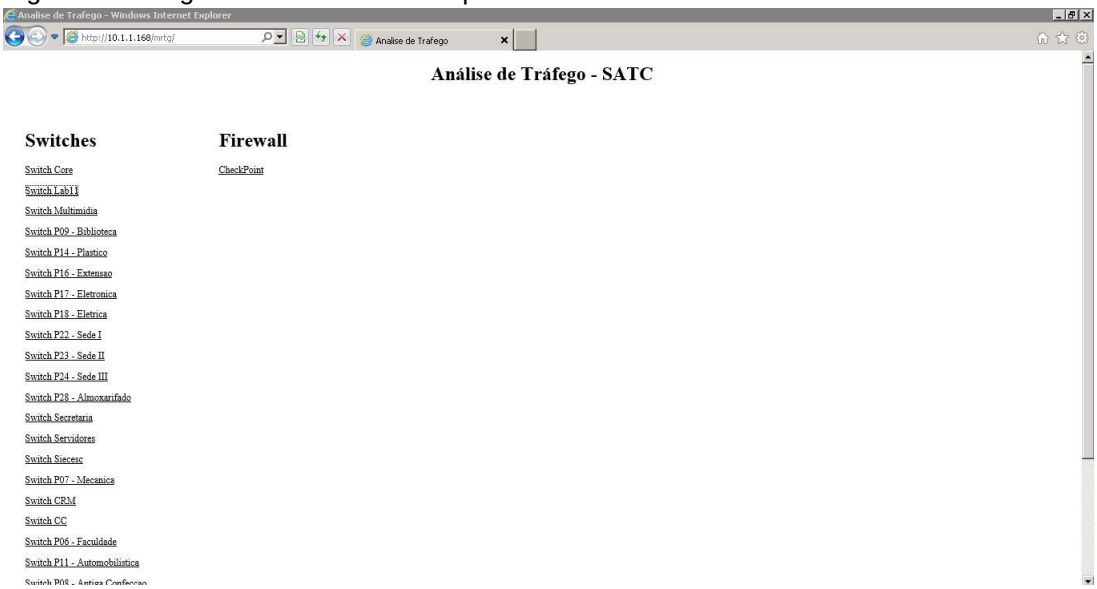
O MRTG é um software que faz o monitoramento de tráfego da rede, gerando gráficos que são visualizados via web, para tal, necessita-se, no servidor onde o mesmo está instalado de um servidor web. Como servidor web utilizou-se o Microsoft Internet Information Services (IIS), na versão 7. Além do servidor web, para o MRTG funcionar necessita-se também da linguagem de programação *perl*, que é uma linguagem multiplataforma. Foi instalado então o software ActivePerl na versão 5.16.3.1604.

O requisito para que os equipamentos possam ser monitorados pelo MRTG é de que o SNMP esteja instalado e configurado. Após este processo, o tráfego de rede do equipamento pode ser analisado e visualizado, podendo ser dividido em diferentes páginas web, conforme necessidade do administrador.

Neste trabalho o MRTG é a ferramenta principal para análise da rede. Através das informações geradas e dos históricos armazenados o administrador poderá verificar em quais segmentos o tráfego de rede é maior, qual o horário de maior pico, além de diagnosticar possíveis gargalos. Estas informações também servirão economicamente, pois com dados precisos não haverá desperdício de recursos para aquisição de equipamentos mais robustos, por exemplo.

O MRTG foi colocado para monitorar as portas mais importantes de todos os *switches* gerenciáveis da instituição e também as interfaces do firewall. Criou-se uma página inicial (figura 21), que contém os links para cada equipamento monitorado.

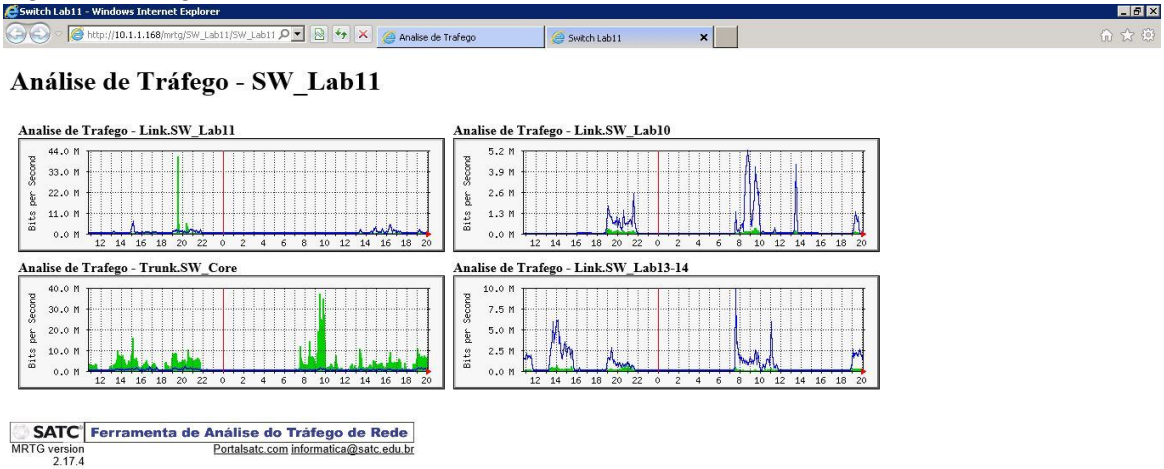
Figura 21 – Página inicial do MRTG implantado



Fonte: Do autor.

A página de monitoramento específica de um *switch*, contendo as portas monitoradas pode ser vista na figura 22, sendo este *switch* do laboratório 11 da instituição.

Figura 22 – Página de monitoramento do *switch* do Laboratório 11



Fonte: Do autor.

O MRTG tornou-se um aliado no monitoramento da rede, auxiliando a equipe na descoberta e soluções de problemas. Após implantá-lo, a equipe de TI passou a acessá-lo todos os dias, a fim de prevenir possíveis problemas, ficando atentos caso alguma mudança ocorra na rede.

4.3.2 Implantação do Nagios

O Nagios foi instalado no Linux/GNU Debian na versão 7, Wheezy. Os passos para sua instalação e configuração são descritos no apêndice B deste trabalho. Alguns requisitos são necessários para sua instalação, bibliotecas e também o servidor HTTP Apache, para poder visualizar via web.

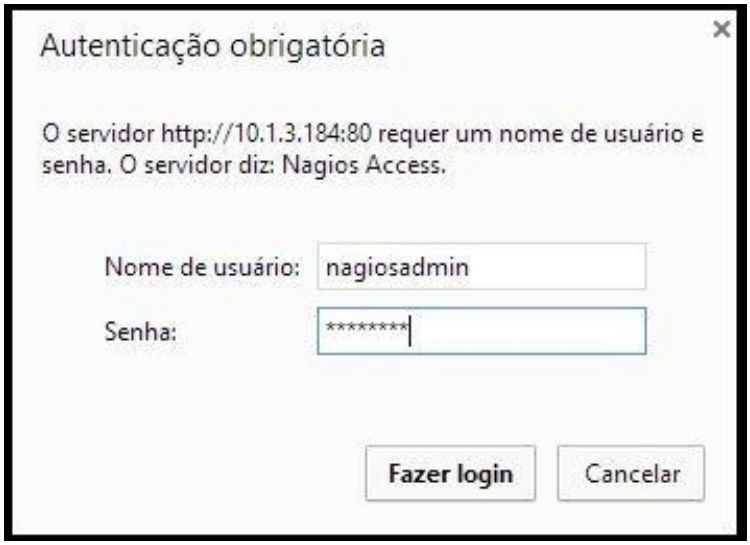
É uma aplicação de monitoramento de rede que pode monitorar *hosts*, serviços e até recursos. Gerando alertas quando surgirem problemas e também quando estes problemas são resolvidos.

Neste trabalho o Nagios foi configurado para fazer o monitoramento de *hosts* através do utilitário *ping*, que usa o protocolo ICMP para testar a conectividade dos equipamentos, ou seja, verifica se o *host* está se comunicando com a rede. Os *hosts* monitorados são visualizados em um navegador.

Para monitorar um *host* o processo feito foi adicioná-lo no arquivo de configuração, especificando o seu IP. Depois de adicioná-lo, também foi necessário definir alguns parâmetros, como o tempo de checagem do equipamento, por exemplo.

Durante a instalação do Nagios é solicitado um usuário e senha, que são utilizados para o acesso via web do mesmo. A tela de *login* pode ser vista na figura 23.

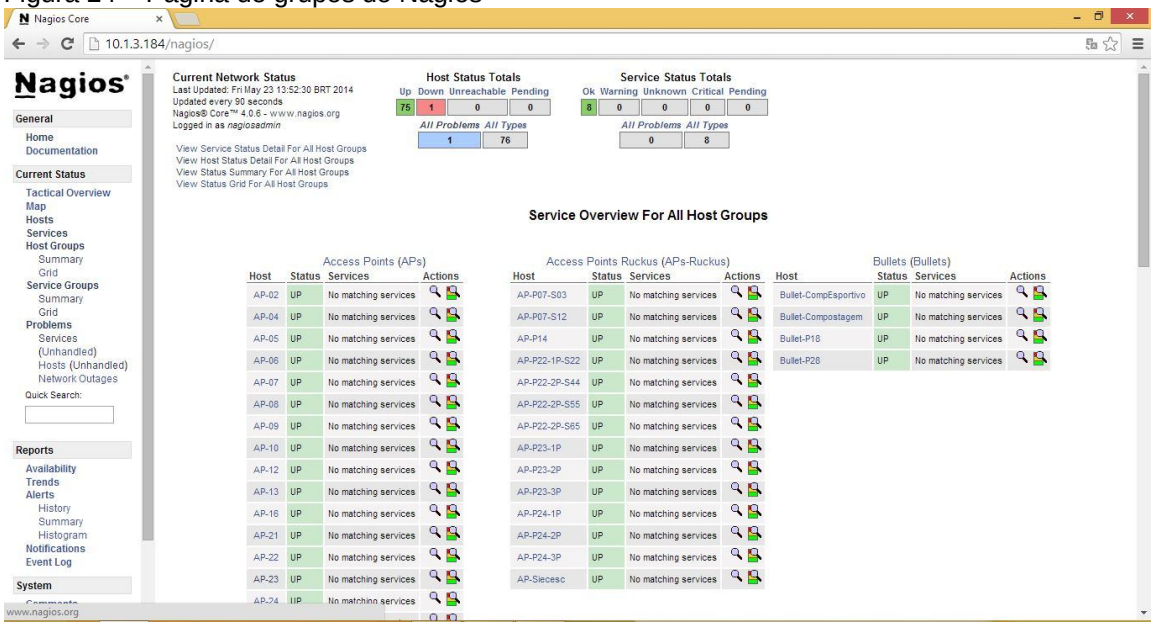
Figura 23 – Tela de login do Nagios



Fonte: Do autor.

Ao fazer *logon* no Nagios, abre-se a tela inicial, onde se tem acesso a todos os menus, no qual se pode prosseguir para a tela de *hosts*, de grupos (figura 24), de serviços, de problemas, de relatórios, dentre outros.

Figura 24 – Página de grupos do Nagios

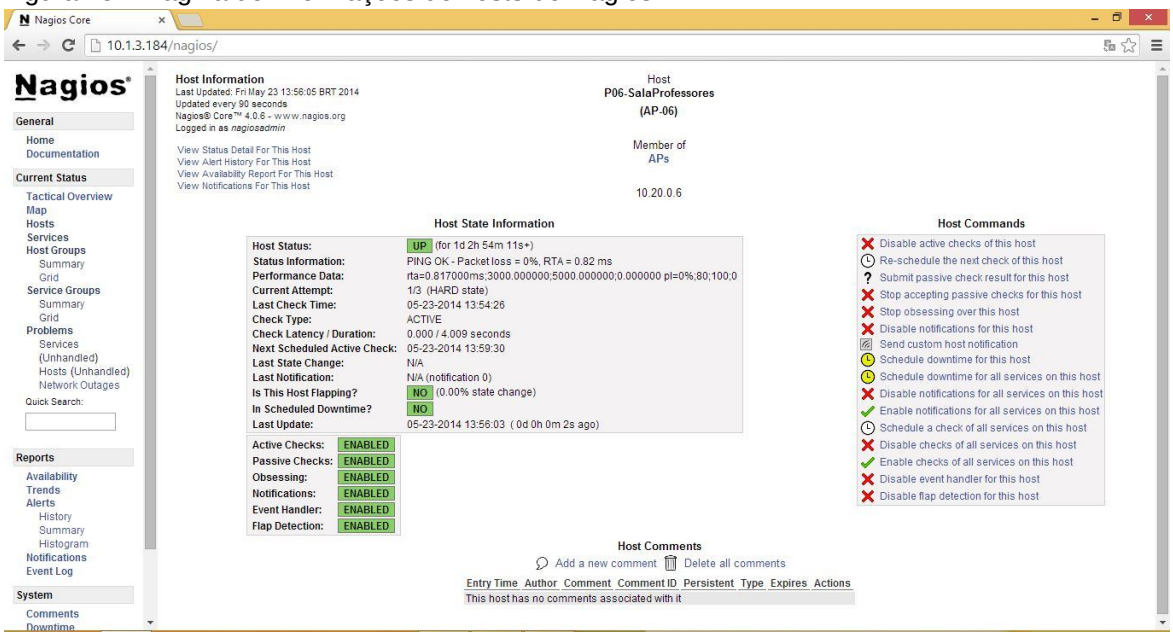


Fonte: Do autor.

No trabalho foram definidos quatro grupos de *hosts.* Um grupo de pontos de acesso *wireless (Acess Points)*, um grupo de *access points* da linha Ruckus, um grupo de *switches* e um grupo de *bullets*. Por padrão o Nagios também cria um grupo chamado Linux Servers, no qual o próprio servidor do Nagios está incluso.

Através da página de grupos ou da própria página de *hosts* se tem acesso a algumas informações deste equipamento, como sua descrição, grupo a que pertence, IP, seu *status*, data e horário da última checagem, dentre outros. A página de informações de *hosts* é vista na figura 25.

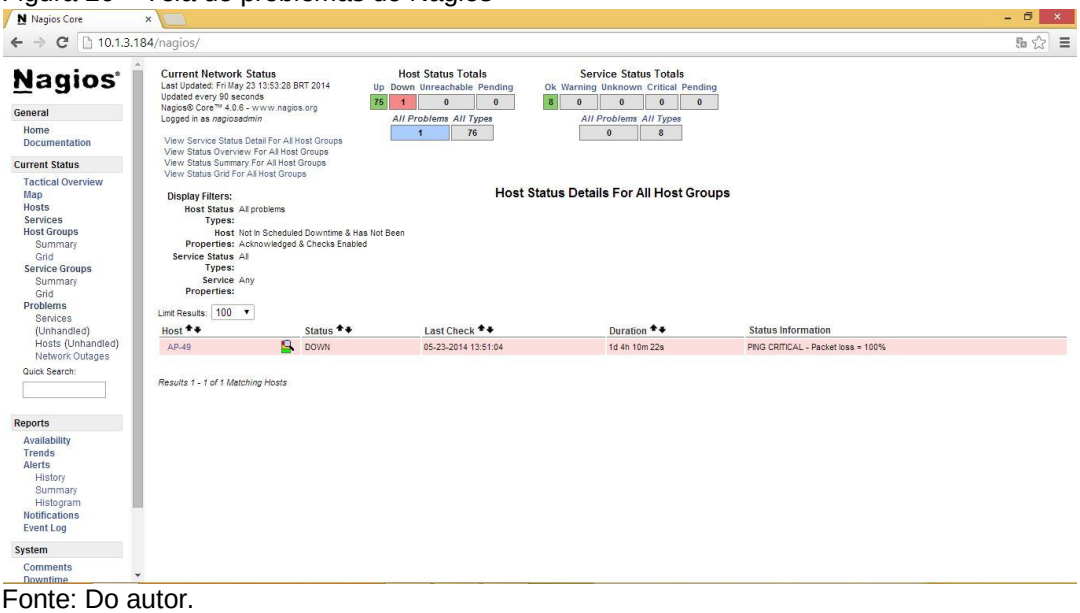
Figura 25 – Página de informações de *hosts* do Nagios



Fonte: Do autor.

A página de maior importância para o monitoramento da rede é a página de problemas (figura 26). Nesta página todos os *hosts* que não estão se comunicando com a rede são destacados. Foi deixado um monitor na sala da TI nesta página, onde os profissionais podem saber em tempo real se algum equipamento parou de funcionar e procurar solucionar o problema o mais rápido possível.

Figura 26 – Tela de problemas do Nagios

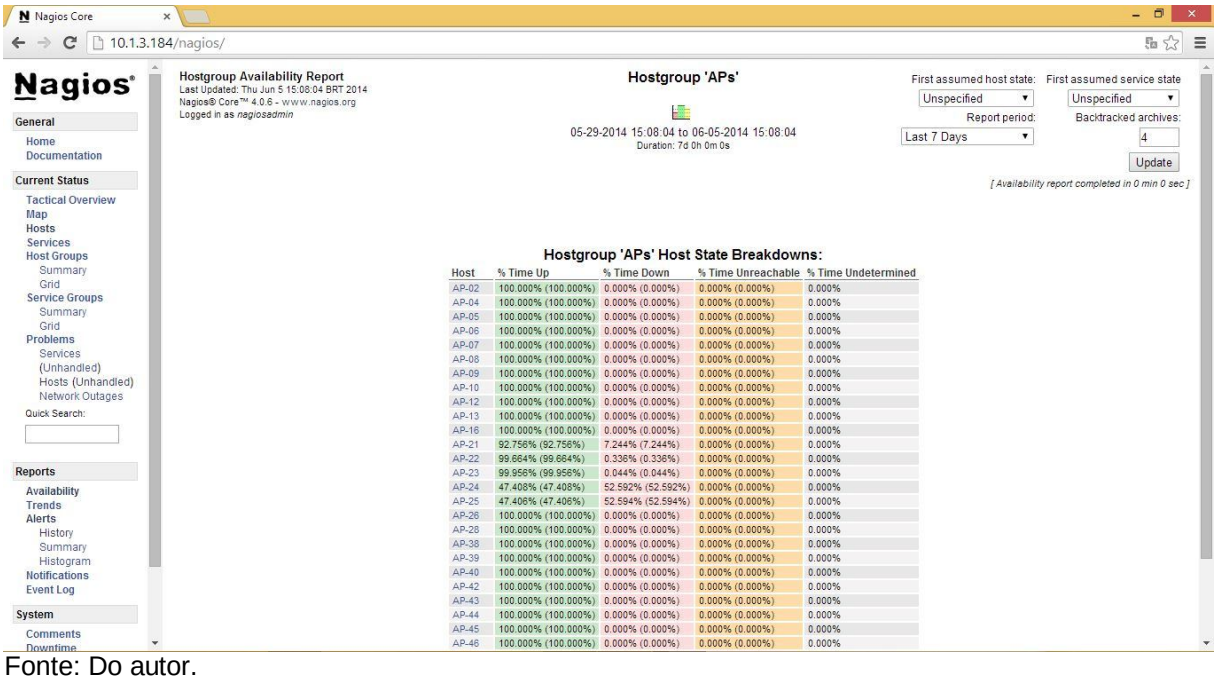


Fonte: Do autor.

Outra informação importante que pode ser observada nesta tela é o tempo em que o equipamento deixou de funcionar. Podendo caber até ao administrador cobrar da equipe de TI pelo tempo de resposta caso um evento ocorra e demore a ser solucionado.

No Nagios também pode-se obter relatórios. Nestes relatórios é possível saber, por exemplo, qual o *host* que mais ficou sem acesso a rede num determinado período, possibilitando um histórico dos acontecimentos. A figura 27 mostra um relatório gerado por grupo, no caso o grupo de *access points*, em um período de sete dias.

Figura 27 – Relatório por grupo do Nagios



Fonte: Do autor.

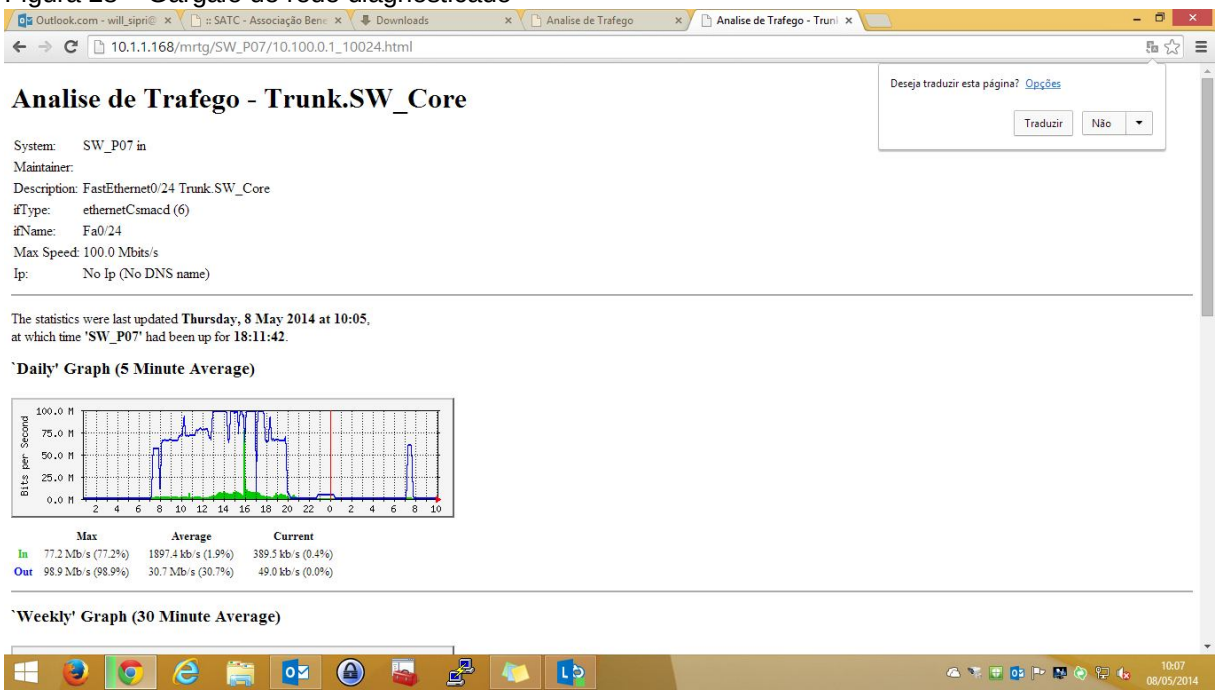
4.4 RESULTADOS OBTIDOS

Muito se pensou e por análises, como número de estações, dependência de recursos, dentre outros, decidiu-se segmentar a rede da forma apresentada, podendo-se perceber que esta ficou mais organizada.

Com a utilização dos softwares de monitoramento, problemas que antes não se conheciam, agora tornam-se visíveis em tempo real. E alguns que levariam um tempo maior para serem resolvidos hoje são identificados e solucionados mais facilmente, tornando o usuário final mais satisfeito e a equipe de TI mais segura.

Um caso que aconteceu, foi a descoberta de um gargalo de rede, através do MRTG. Percebeu-se que havia um gargalo em um dos troncos de um *switch* com o *switch* core. Neste *switch*, que é do Prédio 07 da instituição, havia quatro equipamentos de Digital Video Recorder (DVR) e links de alguns laboratórios. Os DVR são equipamentos que gravam as imagens das câmeras da instituição. O tronco entre estes *switches* é feito através de portas Fast Ethernet e em momentos em que os vigilantes acessavam as imagens dos DVR se percebeu que o tráfego entre os mesmos chegava a borda dos 100 Mbps. Isto estava onerando a rede nos laboratórios e deixando a visualização de imagens das câmeras lentas. Observando cada porta do *switch* para ver o consumo de link diagnosticou-se que este consumo foi devido aos DVR. Tinha-se então, duas alternativas. Ou colocava-se outro *switch* que fosse Gigabit Ethernet, o que exigiria custos, pois não se tinha para repor, ou retirava-se o tráfego de um desses DVR e colocava-se em outro *switch* disponível no mesmo ambiente, não havendo custo algum. Optou-se pela segunda opção. Monitorou-se o funcionamento por um tempo e tudo estava funcionando satisfatoriamente. O gargalo diagnosticado pode ser visto na figura 28.

Figura 28 – Gargalo de rede diagnosticado



Fonte: Do autor.

Ficou bastante claro que com o MRTG um problema que poderia ter durado dias e até semanas para ser descoberto e depois ainda para ser resolvido, foi solucionado em poucas horas.

O Nagios também proporcionou a resolução de muitos problemas de forma ágil, pois assim que surgiam alertas gerados quando um equipamento deixava de comunicar com a rede, a equipe de TI já o verificava, não necessitando ser avisada por algum usuário. Isso é bastante promissor, pois muitas vezes o problema foi solucionado sem que o usuário final o percebesse.

Define-se como positiva a avaliação destes softwares de monitoramento, apesar de o Nagios ser de complexa implantação, caso configurado para todas as funções que pode exercer, como monitoramento de serviços, recursos, alertas via e-mail, entre outros. Enfim, é uma poderosa ferramenta, mas que exige pessoas especializadas para sua completa implantação. O MRTG é simples, de fácil configuração e muito útil para monitoração do tráfego da rede.

Não pode-se comparar a rede antes de toda segmentação com a rede já segmentada. Por se tratar de uma rede em produção, maiores testes não foram executados para não correr o risco de tornar indisponíveis alguns dos recursos. O objetivo com que este trabalho foi executado é de prevenção.

5 CONCLUSÃO

Conclui-se como positivo o desfecho deste trabalho, tendo ficado a rede de fácil entendimento e gerenciamento. Com os segmentos, esta ficou menos suscetível a problemas. A segurança com a segmentação também aumentou. O ponto mais importante foi separar a parte administrativa da educacional, isolando cada segmento e dando acesso somente aos recursos necessários a cada um, obtendo maior controle sobre a rede.

Com as VLAN tornou-se claro o conceito de segmentação de redes e sua importância numa rede de médio e grande porte. Dividindo-se a rede, separou-se também as necessidades, ou seja, nem todos os recursos disponíveis em uma rede precisam estar na outra. Com a filtragem de pacotes, compreendeu-se o uso das portas nos serviços de rede. E pensando em segurança e desempenho, muitas portas, que seriam desnecessárias a algumas VLAN, foram bloqueadas, diminuindo o tráfego entre os *switches* da rede, possibilitando maior banda para os recursos realmente necessários.

A gerência de redes corporativas torna-se mais simples e fácil com o uso de ferramentas auxiliares. Considerando o ambiente corporativo com inúmeros usuários, equipamentos e acessos a rede, o uso destas ferramentas traz vantagens no diagnóstico de problemas aos administradores.

Este trabalho fundamentou-se no entendimento e utilização de segmentação de redes, uso de portas e controles de acesso, de ferramentas para o monitoramento de tráfego na rede e de equipamentos, objetivando prevenção.

Utilizando-se das ferramentas problemas foram identificados em tempo real. Com a ferramenta de monitoramento de tráfego na rede, MRTG, foi possível a verificação de gargalo na rede em determinado momento. Monitorando os equipamentos, por meio do Nagios, verificou-se inúmeras vezes o não funcionamento principalmente de *access points*.

Portanto, o uso de ferramentas de monitoramento, MRTG e Nagios, servem para monitoramento do que está ocorrendo na rede. Desta forma a equipe de TI pode tomar precauções mais rapidamente caso algum problema seja diagnosticado.

Pode-se avaliar o uso destas ferramentas como eficientes e bastante satisfatórias. Os objetivos com o uso destas foram alcançados. Que eram de auxiliar

a equipe de TI na questão de gerência da rede, prevendo e tendo conhecimento de eventos que ocorrem.

Alguns problemas foram encontrados para a elaboração deste trabalho, devido ao fato de estar lidando com um ambiente grande e em produção. A criação das VLAN para segmentação foi feita tomando cuidados para que não influenciasse na disponibilidade dos serviços. Da mesma maneira a criação da ACL, que em alguns casos se acabou bloqueando portas que eram utilizadas e serviços deixaram de funcionar. Na questão das ferramentas de monitoramento, o maior problema foi com o Nagios, que foi difícil encontrar documentação para configuração da nova versão do software, que difere um pouco das versões anteriores, tornando-se complexo a sua implantação. Para a implantação do MRTG foi necessário criar um modelo para descrição das portas nos *switches* para facilitar no entendimento da equipe de TI. Isto não é considerado um problema, mas é um processo trabalhoso, visto que são 28 equipamentos para mudar a configuração.

Superadas as dificuldades, os objetivos específicos deste trabalho foram atingidos e destaca-se também que o uso das ferramentas não supre a necessidade de um administrador, estas servem para auxiliar o mesmo e não tomar o seu lugar.

Com os fundamentos aplicados neste trabalho, bem como os resultados obtidos, algumas sugestões de trabalhos futuros podem ser descritas. Outras implantações poderiam ser feitas com o Nagios, que é bastante abrangente, como monitoramento de servidores, com os serviços e recursos de cada um, implementar para que o Nagios envie e-mails quando determinados eventos ocorrerem. O MRTG também poderia ser colocado para monitorar o tráfego de rede de cada servidor, possibilitando diagnosticar se o hardware do mesmo está atendendo. Ou também monitorar algum *host* que suspeita-se estar com largura de banda acima do normal. Pode-se criar e verificar o funcionamento de VLAN baseada em MAC Address e também ACL aplicadas a portas do *switch*.

REFERÊNCIAS

ANDRADE, Hetty Alves de. **Nagios como Solução de Monitoramento de Rede**. Disponível em: <http://www.ginux.ufla.br/files/mono-HettyAndrade.pdf> Acesso em: 15 nov. 2013.

BARROS, Soares Odair. **Segurança de Redes Locais com a Implementação de VLAN's:** O Caso da Universidade Jean Piaget de Cabo Verde. 2007. 67 f. Monografia (Graduação) - Universidade Jean Piajet de Cabo Verde, Cabo verde.

BIRKNER, Matthew H. **Projeto de interconexão de redes:** Cisco internetwork Design. São Paulo: Pearson Education do Brasil, 2003.

BITTERCOURT JUNIOR, Benedito Rodrigues; OE, Robson Hirohito; SANTANNA, João. **Gerência e Monitoramento de Redes de Computadores com o software livre Nagios.** Belém, PA: IESAM, 2005.

CARDOSO, Leandro Koehler. **Implantação da ferramenta Nagios para monitoração de rede e análise e tratamento dos eventos por meio de softwares de apoio**. 2011.

CARISSIMI, Alexandre da Silva; ROCHOL, Juergen; GRANVILLE, Lisandro Zambenedetti. **Redes de computadores.** 2. ed. Porto Alegre: Bookman, 2009.

CONTESSA, Diego Fraga; POLINA, Everton Rafael. **Gerenciamento de Equipamentos Usando o Protocolo SNMP.** Disponível em: <http://www.cp.com.br/upl/artigo_3.pdf>. Acesso em: 18 nov. 2013.

COMER, Douglas. **Interligação em rede com TCP/IP.** Rio de janeiro: 1999. Elsevier, 2006.

COMER, Douglas. **Redes de computadores e internet.** 4. ed. Porto Alegre: Bookman, 2007.

CALDAS FILHO, Francisco Lopes; FERREIRA, Pedro Ernesto. **Projeto e Implantação de uma Nova Topologia de Rede de Computadores para o Laboratório de Informática LINF/CIC/UnB.** 2013. 69 f. Monografia (Graduação) - Universidade de Brasília, Brasília.

DIAS, Dagoberto et. al. Redes Monitoradas com Cacti e Nagios. **Engenharia de Computação em Revista**, Nazaré, 2009.

DIAS, Beethovem Zanella; ALVES JÚNIOR, Nilton. **Protocolo de Gerenciamento SNMP.** Disponível em: <http://www.rederio.br/downloads/pdf/nt00601.pdf>. Acesso em: 18 nov. 2013.
DIMARZIO, J. F. **Projeto e Arquitetura de Redes:** Um guia de campo para profissionais de TI. Rio de Janeiro: Elsevier, 2001.

JUNG, Edson Venicius; PELLIS, Ricardo Rafael. **Aplicando Segurança em Redes Locais Através de Gerenciamento de Ativos de Rede.** 2013. 10 f. Pós Graduação - Pontifícia Universidade Católica do Paraná, Curitiba.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet:** uma abordagem top-down. 5. ed. São Paulo: Pearson Addison Wesley, 2010.

MORAES, Alexandre Fernandes de. **Redes de computadores:** fundamentos. 6. ed. rev. e ampl. São Paulo: Érica, 2008.

MURHAMMER, Martin W. **TCP/IP:** tutorial e técnico. São Paulo: Makron Books, 2000.

NORTHCUTT, Stephen et. al. **Desvendando:** segurança em redes. Rio de Janeiro: Campus, 2002.

OETIKER, Tobias. **MRTG:** The Multi Router Traffic Grapher. Proceedings of the 12th Systems Administration Conference (LISA '98), 3 abr. 2002.

PETERSON, Larry L.; DAVIE, Bruce S. **Redes de computadores:** uma abordagem de sistemas. Rio de Janeiro: Elsevier, 2004.

SALKYS, Paulo Henrique Bessani et. al. Gerência e Monitoramento de Redes de Computadores: uma introdução ao Nagios. **Revista Varia Scientia**, Cascavel, v.07, n. 13, p.149-152, 2007.

SEAGREN, Eric. **Secure your network for free:** using nmap, wireshark, snort, nessus, and MRTG. Rockland: Syngress, 2007.

TANENBAUM, Andrew S.; SOUZA, Vandenberg D. **Redes de computadores**. 4. ed. Rio de Janeiro: Campus, 2003.

TORRES, Gabriel. **Redes de computadores.** Rio de Janeiro: Novaterra, 2009.

VERAS, Manoel. **Datacenter:** componente central da infraestrutura de TI. Rio de Janeiro: Brasport, 2009.

ANEXO (S)

ANEXO A – DOCUMENTO ASSINADO PELA COORDENAÇÃO DA SATC

Termo de Responsabilidade

Os dados apresentados pelo Trabalho estão de acordo com o que é necessário para uma melhor gerência de rede da Instituição. Desta forma declaro para os devidos fins que autorizou-se o desenvolvimento do trabalho na SATC.

Izes Ester Machado Beloli
Coordenadora de Informática

APÊNDICE (S)

APÊNCICE A – INSTALANDO E CONFIGURANDO O MRTG

1 OBTENDO OS ARQUIVOS DE INSTALAÇÃO

Antes de configurar o MRTG, deve se instalar a linguagem *perl*, através do software gratuito ActivePerl, que pode ser obtido pelo link: http://downloads.activestate.com/ActivePerl/releases/5.16.3.1604/ActivePerl-5.16.3.1604-MSWin32-x64-298023.msi.

Os arquivos do MRTG estão disponíveis no link: http://oss.oetiker.ch/mrtg/pub/mrtg-2.17.4.zip.

2 INSTALAÇÃO E CONFIGURAÇÃO

Primeiramente deve-se instalar o *perl*. Após baixar o arquivo de instalação, execute-o.

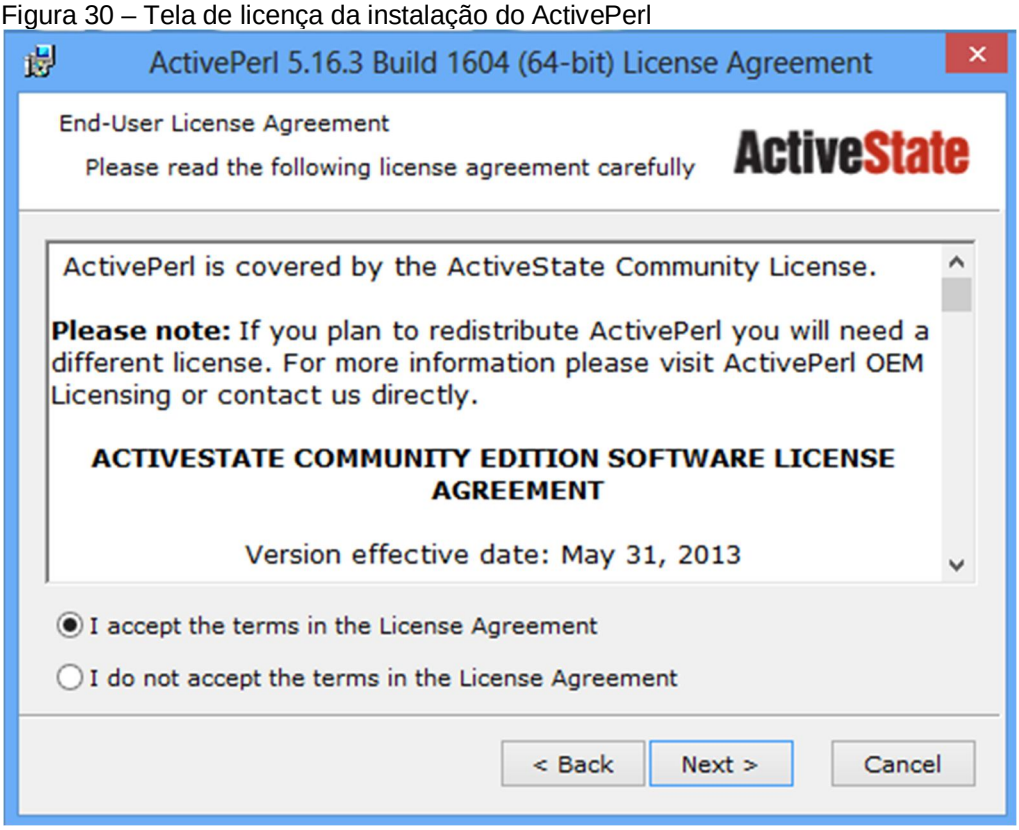
A seguinte janela se abrirá (figura 29):

Figura 29 – Tela incial de instação do ActivePerl

Fonte: Do autor.

Esta é a janela de apresentação do software, clique em *next*. A próxima janela será a do contrato de licença (figura 30).

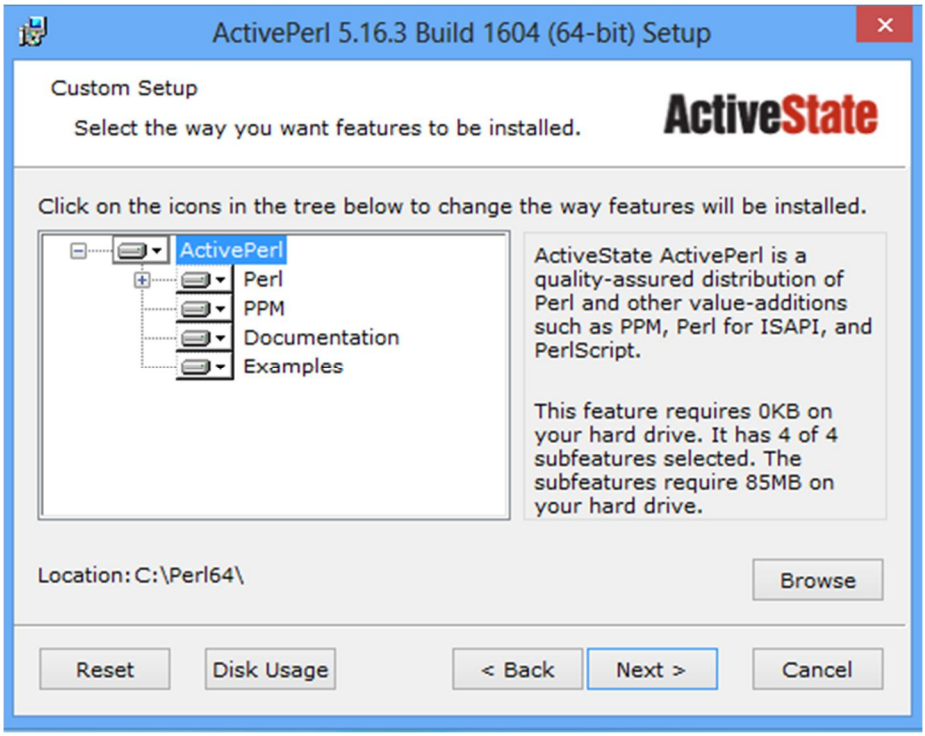
Figura 30 – Tela de licença da instalação do ActivePerl



Fonte: Do autor.

Selecione a opção *I accept the terms in the License Agreement* e clique em *next*. Após virá a tela de recursos (figura 31) que poderão ser instalados.

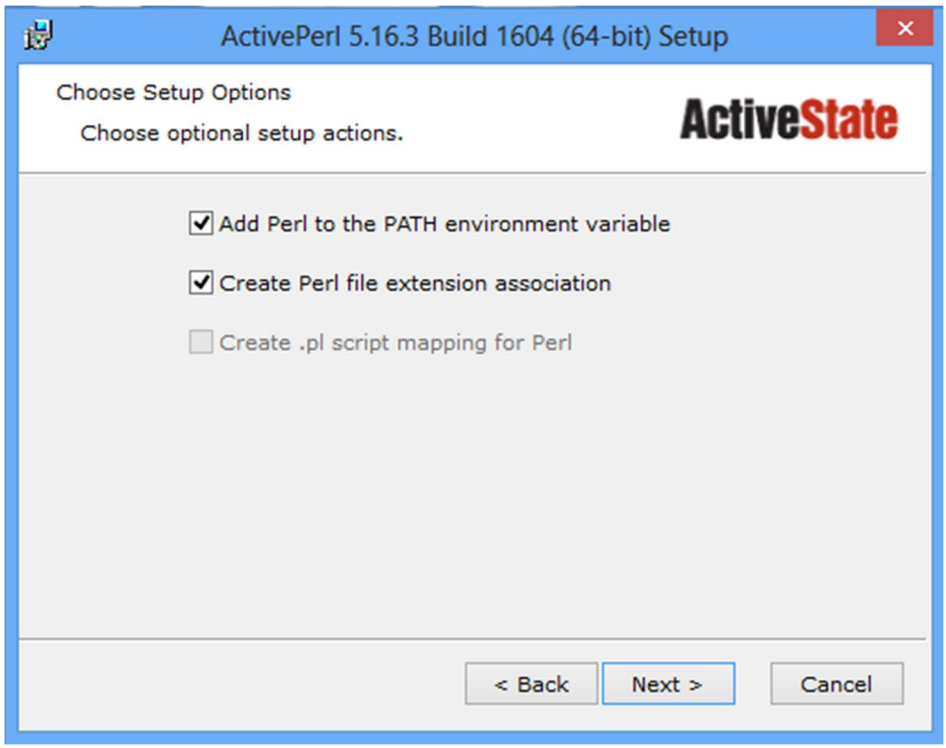
Figura 31 – Tela de recursos da instalação do ActivePerl



Fonte: Do autor.

Apenas clique em *next*, deixando todos os recursos disponíveis. A próxima tela será de ações (figura 32).

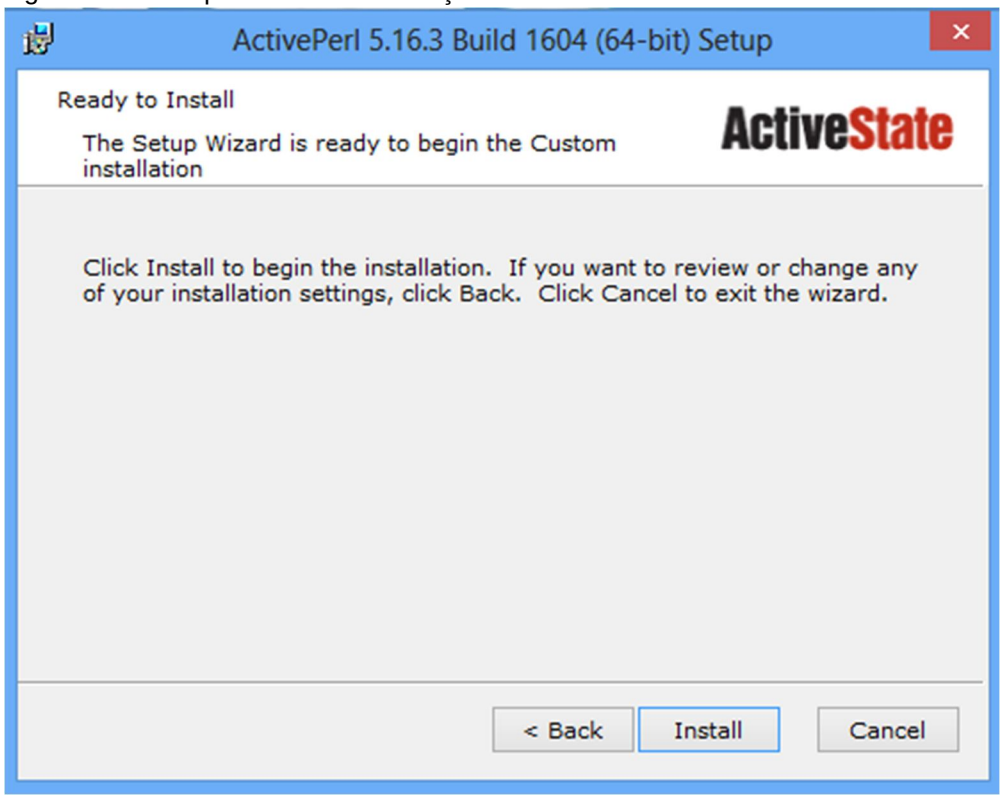
Figura 32 – Tela de ações da instalação do ActivePerl



Fonte: Do autor.

Deixe como padrão e clique em *next*. A penúltima tela será para iniciar a instalação (figura 33).

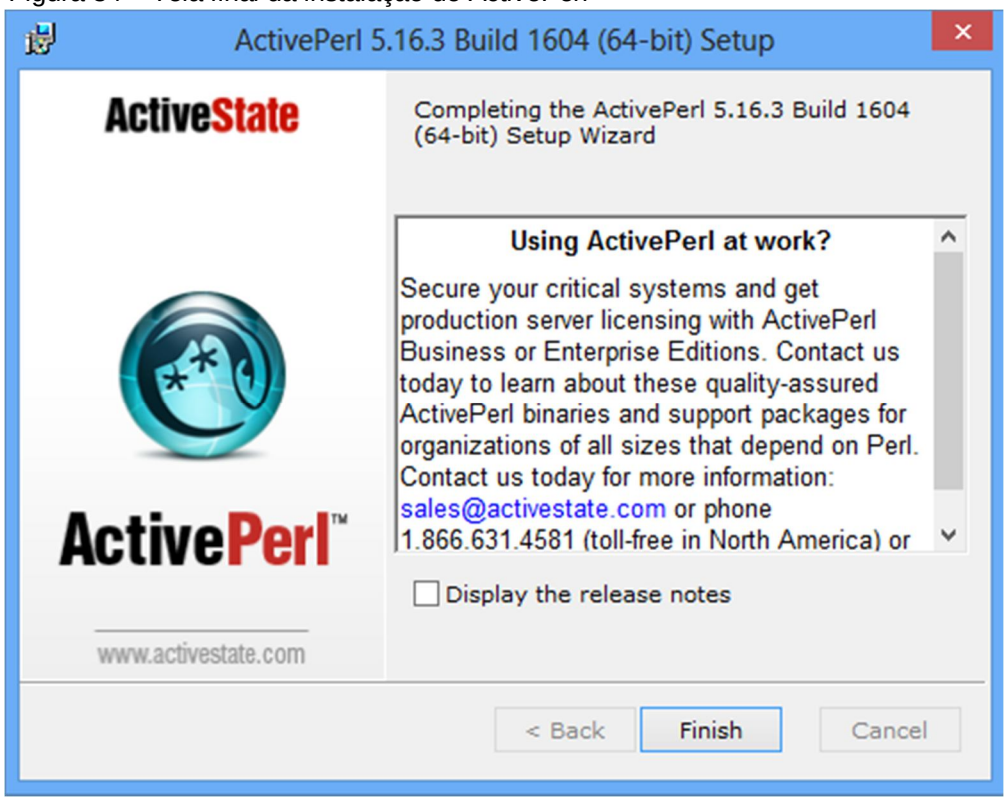
Figura 33 – Tela para iniciar a instalação do ActivePerl



Fonte: Do autor.

Clique em *Install* e aguarde até o final da instalação. Ao término da instalação (figura 34) clique em *Finish*. Pronto, o ActivePerl já está instalado.

Figura 34 – Tela final da instalação do ActivePerl



Fonte: Do autor.

O próximo passo é descompactar a pasta baixada do MRTG. Descompacte-a em um local, de preferência na raiz da unidade C:.

Com o MRTG descompactado a primeira coisa a se fazer é criar um arquivo de configuração padrão, utilizando o *cfgmaker* do MRTG.

O arquivo de configuração padrão pode ser criado através do comando:

C:\MRTG\mrtg-2.17.4>perl bin\cfgmaker --output conf\Nome.cfg --global "Options[_]: bits,growright" --global "WorkDir: C:/inetpub/wwwroot/mrtg" satc@x.x.x.x

Onde:

conf é a pasta onde o arquivo será criado;

Nome.cfg é o nome do arquivo de configuração;

WorkDir: C:/inetpub/wwwroot/mrtg é o local onde o arquivo será atualizado;

satc é o nome da comunidade SNMP;

x.x.x.x é o IP do equipamento a ser monitorado.

Depois de criar o arquivo de configuração padrão, o próximo procedimento é criar um *index* para ser acessado pela web, utilizando o *indexmaker* do MRTG. O *index* pode ser criado através do comando:

C:\MRTG\mrtg-2.17.4>perl bin\indexmaker --output=c:\inetpub\wwwroot\mrtg\index.html conf\core.cfg

Onde:

c:\inetpub\wwwroot\mrtg\nomeindex.html é o local no servidor web e o nome do arquivo de *index*;

conf\nome.cfg é a pasta e o nome do arquivo de configuração padrão.

Por fim, cria-se um arquivo com a extensão .bat com o comando para executar a varredura no equipamento.

Este arquivo deve conter o comando:

c:\Perl64\bin\perl.exe c:\MRTG\mrtg-2.17.4\bin\mrtg c:\MRTG\mrtg-2.17.4\conf\nome.cfg

Somente os arquivos de configuração padrão irão mudar, caso tenha mais de um. Salvando este comando em um arquivo com extensão .bat, deve-se criar uma tarefa para executá-lo em um determinado intervalo de tempo, a cada 5 minutos por exemplo, para o MRTG ir montando o gráfico.

Pode-se também fazer uma página inicial, espécie de menu, para facilitar o acesso aos equipamentos.

Uma página inicial básica pode ser feita através do código abaixo:

```
<HTML>
<BODY bgcolor="#ffffff" text="#000000" link="#000000" vlink="#000000" alink="#000000">
<center>
        <H1>Análise de Tráfego - MRTG</H1>
```

```
</center>
<TABLE BORDER=0 CELLPADDING=0 CELLSPACING=30>
        <td>
                <a href="pasta\nomedoarquivo.html"target="_blank">Nome do Equipamento</a></p>
        </td>
</TABLE>
</BODY>
</HTML>
```

APÊNDICE B – INSTALANDO E CONFIGURANDO O NAGIOS

1 INSTALAÇÃO

O Nagios deve ser instalado em um sistema operacional Linux. Utilizou-se o Debian GNU/Linux na versão 7 (Wheezy) para tal.

Após o sistema operacional estar devidamente instalado, atualiza-se o repositório através do comando:

#apt-get update

1.1 Instalação dos Pré-Requisitos

Depois de atualizado, começa-se a instalação dos pré-requisitos, que são: o apache, biblioteca de execução Joint Photographic Experts Group (JPEG), biblioteca SNMP, biblioteca de desenvolvimento e documentação da Secure Sockets Layer (SSL), *shell* para conexões remotas, linguagem de *script* HyperText Markup Language (HTML) e por fim uma biblioteca de autenticação. Os comandos para instalação desses requisitos seguem abaixo:

 # apt-get -y install apache2 build-essential libgd2-xpm-dev
 # apt-get -y install libjpeg62 libjpeg62-dev libpng12-dev
 # apt-get -y install snmp libsnmp-base
 # apt-get -y install libssl-dev openssl
 # apt-get -y install mc rsh-server openssh-server
 # apt-get -y install php5 php-pear libsnmp9-dev rcconf
 # apt-get -y install libsasl2-2 libsasl2-modules sasl2-bin mutt postfix

1.2 Criação do Usuário

Deve-se criar um usuário e um grupo para o Nagios. Para criar o usuário *nagios* com a senha:

 # useradd -m -s /bin/bash nagios

 # passwd nagios

1.3 Obtenção dos Arquivos de Instalação

O próximo passo é criar um diretório e baixar os arquivos de instalação.

#mkdir /etc/nagios

Foi criada pasta “nagios” dentro do diretório /etc. Agora deve-se baixar os arquivos de instalação. Primeiro o Nagios Core, depois os *Plug-ins* do Nagios.

#wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.6.tar.gz

#wget http://nagios-plugins.org/download/nagios-plugins-2.0.2.tar.gz

A versões baixadas são as mais recentes, sendo a do Nagios Core a versão 4.0.6 e a dos *Plug-ins* a versão 2.0.2.

1.4 Extração dos Arquivos de Instalação

Os arquivos baixados devem ser descompactados. O comando para descompactar o Nagios Core é o seguinte:

#tar xzf nagios-4.0.6.tar.gz

Para descompactar os *Plug-ins* utilize o comando:

#tar -xvf nagios-plugins-2.0.2.tar.gz

1.5 Compilação e Instalação do Nagios Core

Para compilar e iniciar a instalação segue-se os comandos:

 # ./configure --with-command-group=nagios

 # make all

 # make install

 # make install-init

 # make install-config

 # make install-commandmode

 # make install-webconf

1.5.1 CRIAÇÂO DO USUÁRIO WEB

Deve se criar o usuário “*nagiosadmin”* para acesso *web*.

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

Com o usuário criado, reinicia-se o serviço do *apache.*

 # /etc/init.d/apache2 restart

Logo pode-se acessar o Nagios com um navegador com o usuário e senha criados acima.

http://IP_DO_SERVIDOR/nagios

1.6 Compilação e Instalação dos *Plug-ins*

Segue os comandos para compilar e iniciar a instalação dos *plug-ins*:

 # ./configure --prefix=/usr/local/nagios --with-nagios-user=nagios --with-nagios-group=nagios

 # make

 # make install

1.7 Permissões no Diretório

Por fim, altera-se as permissões no diretório do Nagios e reinicia-se os serviços do apache e nagios.

 # chown nagios.nagios -R /usr/local/nagios
 # /etc/init.d/apache2 restart
 # /etc/init.d/nagios restart

Acessando o Nagios pela web, pode-se notar que a máquina local já estará sendo monitorada.

1.8 Adicionando *Hosts*

Para adicionar *hosts* para serem monitorados por *ping* o ideal é criar arquivos de configuração. Isto pode ser feito assim:

#vim /usr/local/nagios/etc nomearquivo.cfg

Criando-se este arquivo basta informar algumas informações sobre o *host*, como nome, descrição e IP, e opções de monitoramento, como intervalo e período de checagem, quantidade de tentativas até gerar notificação de erro, intervalo e período destas notificações e tipos de notificações, ou seja, quando o estado do *host* mudar de *down* para *up* ou estar inativo, por exemplo.

define host {
host_name NOMEHOST1
alias DESCRIÇÃO
address IPDOHOST
check_command check-host-alive
check_interval 5
retry_interval 1
check_period 24x7

```
        max_check_attempts 3
        notification_interval 30
        notification_period 24x7
        notification_options d,u,r
}
```

Neste mesmo arquivo, pode-se criar também um grupo para os *hosts*.

```
define hostgroup{
        hostgroup_name  NOMEDOGRUPO
        alias           DESCRIÇÃO
        members         NOMEHOST1, NOMEHOST2
}
```

Com o arquivo criado, para o Nagios fazer o monitoramento destes *hosts*, deve-se acrescentar o caminho do arquivo no arquivo nagios.cfg, que fica no mesmo diretório.

```
cfg_file=/usr/local/nagios/etc/NOMEDOARQUIVO.cfg
```

Feito isto, reinicia-se o serviço do Nagios e este deve passar a monitorar o *host* ou grupo de *hosts* adicionados.

```
#service nagios restart
```

Sempre que houver alguma mudança nos arquivos, para adicionar, alterar ou remover algumas configurações, o serviço do nagios deve ser reiniciado para funcionar.

APÊNCICE C – ARTIGO CIENTÍFICO

Análise Lógica de Rede: Estudo de Caso na SATC

William Silveira Sipriano[1], Rogério Antônio Casagrande[1]

[1]Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC)
Criciúma – SC – Brasil

will_sipri@hotmail.com, roc@unesc.net

Abstract. *The following article describes the course conclusion work presented for the obtention of the degree of Bachelor in Computer Science of the University of Extreme Catarinense South (UNESC), which goal was to analyze the SATC institution's network and then present and implant solutions which aim the improvement on performance and security. For such effort, a study was conducted about the kinds of network segmentation Packages filtering, as well of softwares for management. As a result, the implantation of segmentation through VLAN was performed with the filtering of packages by ACL between the segments created and the managed network by the MRTG and Nagios softwares.*

Resumo. *O presente artigo descreve o trabalho de conclusão de curso apresentado para obtenção do grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense, cujo objetivo foi analisar a estrutura da rede da instituição SATC e por meio de um estudo de caso, propor e implantar soluções que visassem melhoria de desempenho e segurança. Para a realização do mesmo efetuou-se um estudo sobre tipos de segmentação de rede e filtragem de pacotes, e também de softwares de gerenciamento. Como resultado teve-se a implantação de segmentação por VLAN, com filtragem de pacotes por ACL entre os segmentos criados e a rede gerenciada pelos softwares MRTG e Nagios.*

1. Introdução

Nos dias atuais com o aumento do uso de tecnologias como smartphones, tablets, notebooks, entre outros, está crescendo muito o uso das redes de computadores.

E no campo corporativo as redes de computadores também crescem a passos largos. A medida que crescem os nós da rede e consequentemente esta rede, problemas podem surgir, principalmente quando a rede não é planejada para tal evolução.

Em redes grandes o tráfego pode ser lento, haver perdas de pacotes. Isto, devido ao domínio de broadcast, que pode ser resolvido segmentando a rede em Virtual LAN (VLAN) (TORRES, 2008).

A técnica de VLAN é utilizada com o uso de switches camada 3 ou roteadores. Além de dividir o domínio de broadcast, esta técnica proporciona também uma gerência mais apurada e fácil de se implementar.

Softwares de gerência de redes auxiliam o administrador a descobrir problemas e a isolar sua causa. Com eles o gerente pode monitorar e controlar todos os equipamentos da rede,

como switches, roteadores, hosts, verificando seus status e obtendo estatísticas das redes as quais eles ligam (COMER, 2007).

Além de possuir um bom desempenho uma rede também precisa apresentar segurança. A segurança em redes pode ser aplicada em todas as camadas, utilizando-se de firewalls, codificações, criptografias e autenticações. Filtrando os pacotes, pode-se permitir que somente determinadas portas e aplicações possam trafegar na rede.

Com o desenvolvimento do trabalho fez-se a implantação de softwares de gerenciamento e monitoramento da rede, o Nagios e o MRTG. Com o propósito de prevenção, a rede foi então segmentada e monitorada. E pensando-se também em segurança se fez a filtragem de pacotes com ACL.

2. Redes de Computadores

Rede de computadores é um conjunto de computadores interconectados no qual se pode trocar informações. Esta conexão pode ser por vários modos: fibra óptica, fio de cobre, micro-ondas, entre outros. Existem redes de diferentes tamanhos, modelos e formas (TANENBAUM, 2003).

Segundo Comer (2007) as redes inicialmente eram utilizadas para compartilhar algum recurso, um periférico geralmente, entre os computadores. Este periférico era conectado à rede e assim os computadores poderiam utilizá-lo. Nos dias atuais o uso das redes está mais amplo. Empresas se comunicam umas com as outras e com os clientes através das redes.

Além da vantagem de compartilhar recursos, tem-se a facilidade de trocar informações e o acesso à Internet, reduzindo os custos com equipamentos e serviços (TORRES, 2009).

2.1. Arquitetura TCP/IP

Este modelo recebe este nome devido aos seus dois principais protocolos: Transmission Control Protocol (TCP) e o Internet Protocol (IP) (MURHAMMER et al, 2000).

A ARPANET, rede de pesquisa criada pelo Departamento de Defesa dos Estados Unidos e antecessora da Internet, estava em expansão. Várias universidades e repartições públicas estavam sendo ligadas a ela. Com isso, quando as redes de rádio e satélites foram criadas houveram problemas com os protocolos existentes. Forçando a criação de um novo modelo de referência. Este ficou conhecido como TCP/IP, cujo objetivo era conectar várias redes ao mesmo tempo (TANENBAUM, 2003).

Segundo Murhammer et al (2000) o TCP/IP é modelado em camadas, podendo ser representado por uma pilha de protocolos ou um conjunto de protocolos.

2.1.1. Protocolos

“Protocolos são regras e procedimentos de comunicação” (MORAES, 2008, p. 124). Existem vários tipos de protocolos, cada um com uma vantagem e propósitos distintos.

Moraes ainda informa que alguns protocolos podem operar em mais de uma camada, sendo que a camada que ele trabalha descreve a sua função e muitos dos protocolos podem trabalhar em pilha, ou seja, conjuntamente.

Para Comer (2007) este conjunto de regras, denominado protocolos, especifica o formato e as ações a serem tomadas em cada mensagem. Estes protocolos são divididos em camadas, dividindo-se as tarefas e facilitando sua utilização, análise e teste.

Em redes têm-se três espécies de protocolos: protocolos de aplicação, transporte e de rede.

2.1.2. Portas

Portas são um sistema de endereçamento. Permitem a comunicação entre a camada de aplicação e a camada de transporte. Tornando possível saber a qual protocolo de aplicação a camada de transporte deve entregar um pacote (TORRES, 2009).

Torres ainda diz que as portas usam um endereçamento de 16 bits, ou seja, são numeradas de 0 a 65535, podendo ser associada ao TCP e ao UDP. Estas portas são padronizadas por um órgão responsável, a Internet Assigned Numbers Authority (IANA), para que não existam aplicações diferentes utilizando a mesma porta, já que somente uma única aplicação pode escutar uma porta.

2.2. Segmentação de Redes

Segmentando a rede, divide-se o domínio de colisão, fazendo com que aumente a largura de banda disponível para as estações individuais (BIRKNER, 2003).

As redes podem ser segmentadas utilizando sub-redes ou VLAN.

2.2.1. VLAN

Uma VLAN, segundo Veras (2009), é um domínio de broadcast criado por um ou mais switches. Fazendo uso destas, o administrador tem controle sobre portas e usuários.

Utilizar-se de VLAN para segmentação da rede física em diversas redes lógicas resulta em uma performance mais apurada, pois o domínio de broadcast é quebrado (CALDAS FILHO; FERREIRA, 2013).

Além de concentrar melhor o tráfego, diminuindo o domínio de broadcast, as VLAN também resolvem outras dificuldades, como o uso ineficiente de comutadores e o gerenciamento de usuários, pois se um usuário se locomove entre os grupos todo cabeamento físico deve ser revisto, no caso de LAN (KUROSE; ROSS, 2010).

Para Kurose e Ross existem também outras formas de VLAN, como a baseada em MAC, no qual o administrador pode dividir os dispositivos em VLAN através de seu MAC Address. Quando o dispositivo for conectado ao comutador, a porta se conecta na VLAN específica.

Segundo Moraes (2008) as vantagens de se usar VLAN são muitas. Dentre elas destacam-se o aumento da performance, pois o domínio de broadcast é menor, facilidade de gerenciamento, que torna-se mais simples e muito mais rápido, topologia de rede independente, ou seja, a rede lógica fica completamente independente da rede física, tornando a rede bastante flexível a modificações e aumento da segurança, pois pode-se separar da rede sistemas como dados sigilosos, impedindo o acesso não autorizado.

2.3. Segurança em Redes

A segurança em redes não depende somente da tecnologia envolvida mas de um conjunto de etapas que devem ser seguidas. O acesso físico, as senhas, os equipamentos, devem ser levados em conta, bem como a prevenção (TORRES, 2009).

Para Kurose e Ross (2010) uma rede segura deve proporcionar: confidencialidade, autenticação, integridade e segurança operacional.

A confidencialidade consiste no fato de somente o remetente e o destinatário poderem entender o conteúdo da mensagem enviada, estando esta cifrada para os demais não a compreenderem. A mensagem é protegida para que usuários não autorizados não possam ter acesso a ela.

Confirmar a identidade dos envolvidos na comunicação, ou seja, confirmar realmente se é quem se alega ser, dá-se o nome de autenticação.

A integridade garante que os dados envolvidos na comunicação não sejam alterados sem a autorização do autor da mensagem, o conteúdo da comunicação permanece íntegro. Já a segurança operacional é composta por mecanismos como firewalls e sistemas de detecção de invasão.

2.3.1. Filtragem de Pacotes

Outra forma de aumentar a segurança e também o desempenho é usando filtragem de pacotes. Uma ACL tem essa função. Ela é uma lista de instruções, que podem permitir ou negar endereços ou protocolos da camada superior, aumentando assim a segurança e mantendo o controle de tudo que está trafegando na rede. A ACL retira do cabeçalho do pacote alguns dados e os compara com suas regras configuradas, tomando as decisões corretas (JUNG; PELLIS, 2013).

Um filtro de pacotes é composto por um IP de origem e destino, um datagrama e um número de porta de protocolo. Desta forma somente os serviços especificados pelas portas de protocolo no filtro de pacotes estarão disponíveis entre os dispositivos (COMER, 2007).

Para Murhammer et al (2000) o filtro de pacotes é aplicado, geralmente, em roteadores, que envia os pacotes de acordo como as regras de filtragem. Ao chegar no roteador são extraídas algumas informações do cabeçalho do pacote e de acordo com as regras do filtro o roteador toma as decisões, como por onde o pacote passará ou se será descartado.

2.4. Gerência de Redes

Segundo Comer (2007) a gerência de redes é fundamental, pois falhas de hardware e software que compõe a rede poderão causar problemas, devido a isto há necessidade de monitorá-la.

Kurose e Ross (2010) indicam que são definidas cinco áreas de gerenciamento de rede, segundo a International Organization for Standardization (ISO), do qual deu-se o nome de FCAPS (Fault, Configuration, Accounting, Performance and Security) em português, Falha, Configuração, Contabilidade, Desempenho e Segurança.

O gerenciamento de desempenho, que quantifica, mede, analisa e controla o desempenho dos vários dispositivos da rede. O gerenciamento de falhas registra, detecta e reage às condições de falhas na rede, sendo um tratamento imediato. Com o gerenciamento de configuração o administrador pode saber quais dispositivos fazem parte da rede, bem como suas versões de hardware e software. Especificar, registrar e controlar o acesso de usuários e dispositivos a determinados recursos da rede faz-se por meio do gerenciamento de contabilização. O gerenciamento de segurança tem o objetivo de controlar o acesso aos recursos da rede seguindo alguma política definida, como os firewalls.

Os softwares de gerenciamento visam facilitar, auxiliar o gerente na descoberta de problemas para que este esteja a par do que está ocorrendo na rede.

2.4.1. MRTG

MRTG é um software livre bastante utilizado para análises estatísticas em redes. Ele pode ser executado em sistemas Unix, Linux, Windows e incorporado em softwares de terceiros. Os seus gráficos são derivados das informações provenientes do SNMP. O MRTG é feito em Perl, uma linguagem de programação multiplataforma mais utilizada em desenvolvimento web (SEAGREN, 2007, tradução nossa).

Com um script Perl, usando o SNMP os contadores de tráfego são lidos nos equipamentos e um programa em linguagem C registra este tráfego e cria os gráficos da conexão monitorada. Os gráficos são incorporados em páginas web, podendo ser visualizado em qualquer navegador (OETIKER, 2002, tradução nossa).

Oetiker relata também que o MRTG proporciona uma visão detalhada do tráfego de rede diária, dos últimos sete dias, das últimas cinco semanas e dos últimos doze meses.

O MRTG é uma ferramenta bastante útil quando se quer apresentar a evolução temporal de um valor monitorado via SNMP, podendo assim, ser utilizado não somente para monitorar o tráfego de rede de uma interface, mas tendo outras opções de configuração (CONTESSA; POLINA, 2013).

2.4.2. Nagios

O Nagios é um software de gerenciamento de rede que permite identificar e resolver problemas de infraestrutura de Tecnologia da Informação (TI) antes que estes se tornem mais críticos.

Andrade (2006) afirma que apesar de o Nagios ser projetado para redes de grande porte, ele apresenta bom desempenho em redes pequenas.

Para torná-lo ainda mais eficaz, o Nagios conta com expansão através de plug-ins, que são complementos. Estes complementos podem ser desenvolvidos por diferentes programadores, mas também tem-se vários plug-ins oficiais (ANDRADE, 2006).

O Nagios é uma ferramenta que possui vários plug-ins, cada um com uma função específica. Com ele o desempenho e a agilidade na correção de falhas é muito rápido. Erros e defeitos em hardwares podem ser notificados com antecedência, de forma que possa ser resolvido sem maiores problemas (SALKYS et al, 2007).

3. Metodologia

A rede foi analisada, com os meios de transmissão, topologias e equipamentos. Como já haviam algumas VLANS optou-se por seguir esta forma de segmentação.

Após foi verificado quais serviços seriam permitidos em cada VLAN, bloqueando os demais. Os softwares de gerenciamento foram então instalados e a rede passou a ser monitorada.

3.1. Implantação da Segmentação

Conforme seguiu-se com a segmentação que se tinha, foi criado uma VLAN para cada laboratório, duas para segurança eletrônica, cinco para a rede wireless, sendo uma de gerência, uma administrativa, uma para alunos, uma para professores e uma de testes. Também criou-se uma para serviços, que inclui os geradores de energia elétrica, uma para salas de pesquisa, uma para a parte corporativa, uma para os servidores e uma para uma rede ADSL externa. Toda a rede foi separa logicamente.

Estas VLAN foram criadas no switch núcleo da rede, verificando o número de hosts de cada uma para determinar a classe. Em cada switch foram configuradas as senhas de acesso, habilitado o SNMP e criado uma VLAN de gerência, a qual fornecerá o seu IP. Utilizou-se a técnica de VLAN baseada em pontos, ou seja, as portas do switch foram configuradas de acordo com a utilização a que se referem.

Com estas VLAN criadas no switch núcleo da rede, os switches de distribuição passaram a entender as mesmas.

Cada VLAN foi criada e configurada com um nome, IP, gateways e classes diferentes, de forma que atendesse as necessidades.

3.2. Implantação da Filtragem de Pacotes

Com o objetivo de diminuir o tráfego na rede, foram liberados somente os serviços realmente necessários.

Para descobrir quais portas bloquear foi instalado o software Windump em um notebook. Com este software foi possível saber quais portas eram utilizadas por cada protocolo. Assim com a rede sem nenhum bloqueio foi analisado quais serviços seriam necessários. Separados os protocolos e portas criou-se as linhas da ACL.

Na ACL foi liberado para toda a rede os serviços de DNS, DHCP, HTTP e HTTPS para navegação na internet. Para os hosts da TI foi concedido acesso liberado a todos os serviços. Liberou-se também o acesso remoto aos servidores de terminal, o acesso ao compartilhamento das pastas no servidor de arquivos, o acesso as impressoras no servidor de impressão, acesso as licenças de software no servidor de licenças. E na rede de segurança foi liberado também o acesso a visualização de imagens das centrais de câmera e comunicação com os alarmes.

Criou-se apenas uma ACL, que controla toda a rede e descarta todo o tráfego das portas não contidas na lista.

Com a ACL a rede torna-se mais segura, pois os pacotes não necessários e que possivelmente serviriam para um ataque, por exemplo, são descartados. Colabora também para o desempenho, pois diminui o tráfego na rede.

3.3. Implantação do MRTG

O MRTG foi instalado e configurado para monitorar o tráfego na rede. Ele gera gráficos que são visualizados na web. Foi colocado para monitorar as principais portas de cada um dos switches gerenciáveis e também as interfaces do firewall, possibilitando visualizar o tráfego da Internet.

Para instalar o MRTG precisou-se instalar um servidor web. Como o MRTG foi instalado em um servidor com Windows 2008 R2 Standard, utilizou-se do Microsoft IIS como servidor web. Outro requisito também é a linguagem Perl, foi instalado então o software ActivePerl para tal. Requisito no host a ser monitorado é somente um: que o protocolo SNMP esteja ativado e configurado. Em cada switch e também no firewall foram configurados uma comunidade SNMP.

Criou-se os arquivos de configuração de cada equipamento a ser monitorado, um script para executar o comando de leitura do MRTG e uma tarefa para executar este script a cada 5 minutos, o que montava os gráficos.

Foi feito também uma página inicial, espécie de menu, onde se separou cada equipamento.

3.4. Implantação do Nagios

O Nagios foi instalado e configurado para a verificação da comunicação de alguns equipamentos com a rede. Foi instalado no Linux Debian na versão 7 e assim como o MRTG também precisa de alguns requisitos, como servidor web, no qual foi instalado o Apache e algumas bibliotecas.

Neste trabalho o Nagios foi configurado para monitorar através de Ping os switches, Access Points e Bullets, que são antenas de link sem fio de linha empresarial. Através do Ping, que utiliza o protocolo ICMP para testar a conectividade dos equipamentos, pode-se verificar se o equipamento está se comunicando com a rede.

Depois de instalado e configurado, para adicionar um host para monitoração adicionou-se o seu IP, sua descrição e definiu-se alguns parâmetros de checagem dos eventos.

Os hosts adicionados foram separados em 4 grupos, um grupo de pontos de acesso wireless (Access Points), um grupo de Access Points da linha Ruckus, um grupo de switches e um grupo de bullets. Por padrão o Nagios também cria um grupo chamado Linux Servers, no qual o próprio servidor do Nagios está incluso.

A tela de maior importância é a de problemas, nela todos os hosts que não estão se comunicando com a rede são destacados. Outro ponto importante desta tela é que indica quanto tempo o equipamento deixou de comunicar com a rede.

Outra tela que merece destaque é a de relatórios. Pode-se obter relatórios de determinado host ou grupo, possibilitando um histórico dos acontecimentos.

4. Resultados Obtidos

Com a utilização dos softwares de monitoramento, problemas que antes não se conheciam, agora tornam-se visíveis em tempo real. E alguns que levariam um tempo maior para serem resolvidos hoje são identificados e solucionados mais facilmente, tornando o usuário final mais satisfeito e a equipe de TI mais segura.

Um caso que aconteceu, foi a descoberta de um gargalo de rede (figura 1), através do MRTG. Percebeu-se que havia um gargalo em um dos troncos de um switch com o switch de núcleo. Neste switch, que é do Prédio 07 da instituição, havia quatro equipamentos de Digital Video Recorder (DVR) e links de alguns laboratórios. Os DVR são equipamentos que gravam as imagens das câmeras da instituição. O tronco entre estes switches é feito através de portas Fast Ethernet e em momentos em que os vigilantes acessavam as imagens dos DVR se percebeu que o tráfego entre os mesmos chegava a borda dos 100 Mbps. Isto estava onerando a rede nos laboratórios e deixando a visualização de imagens das câmeras lentas. Observando cada porta do switch para ver o consumo de link diagnosticou-se que este consumo foi devido aos DVR. Tinha-se então, duas alternativas. Ou colocava-se outro switch que fosse Gigabit Ethernet, o que exigiria custos, pois não se tinha para repor, ou retirava-se o tráfego de um desses DVR e colocava-se em outro switch disponível no mesmo ambiente, não havendo custo algum. Optou-se pela segunda opção. Monitorou-se o funcionamento por um tempo e tudo estava funcionando satisfatoriamente.

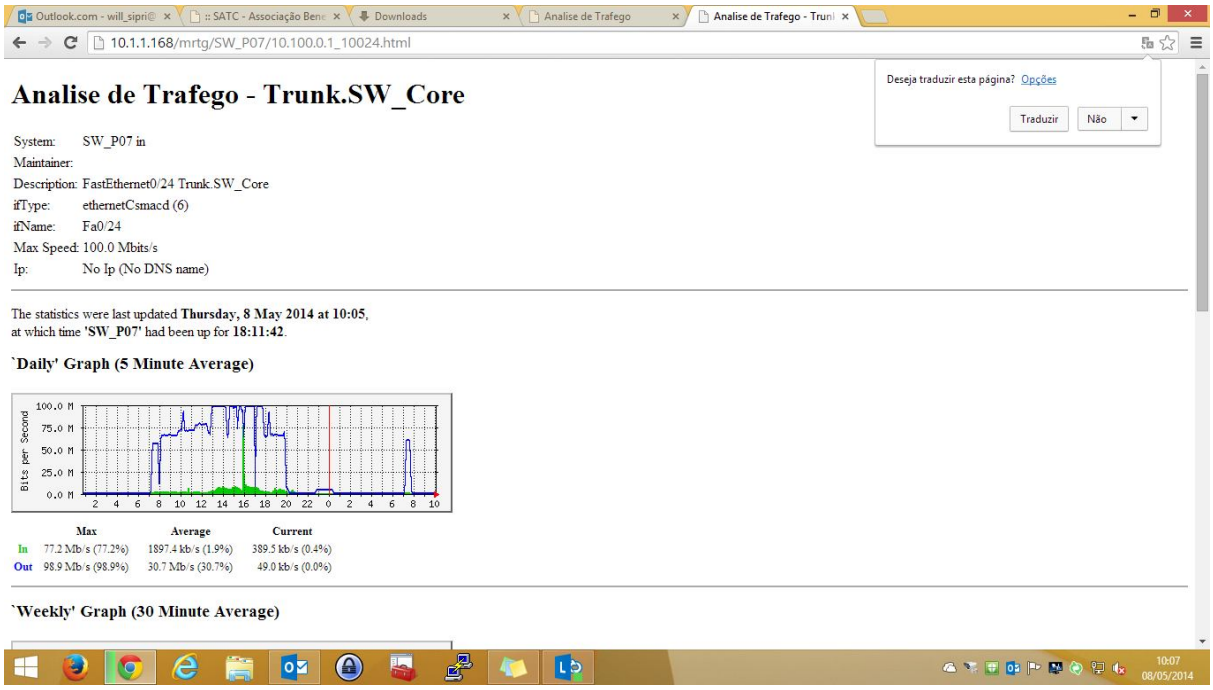


Figura 1. Gargalo de rede diagnosticado pelo MRTG

Ficou bastante claro que com o MRTG um problema que poderia ter durado dias e até semanas para ser descoberto e depois ainda para ser resolvido, foi solucionado em poucas horas.

O Nagios também proporcionou a resolução de muitos problemas de forma ágil, pois assim que surgiam alertas gerados quando um equipamento deixava de comunicar com a rede, a equipe de TI já o verificava, não necessitando ser avisada por algum usuário. Isso é bastante promissor, pois muitas vezes o problema foi solucionado sem que o usuário final o percebesse.

5. Conclusão

Com as VLAN tornou-se claro o conceito de segmentação de redes e sua importância numa rede de médio e grande porte. Dividindo-se a rede, separou-se também as necessidades, ou seja, nem todos os recursos disponíveis em uma rede precisam estar na outra.

Com a filtragem de pacotes, compreendeu-se o uso das portas nos serviços de rede. E pensando em segurança e desempenho, muitas portas, que seriam desnecessárias a algumas VLAN, foram bloqueadas, diminuindo o tráfego entre os switches da rede, possibilitando maior banda para os recursos realmente necessários.

A gerência de redes corporativas torna-se mais simples e fácil com o uso de ferramentas auxiliares. Considerando o ambiente corporativo com inúmeros usuários, equipamentos e acessos a rede, o uso destas ferramentas traz vantagens no diagnóstico de problemas aos administradores.

Utilizando-se das ferramentas problemas foram identificados em tempo real. Com a ferramenta de monitoramento de tráfego na rede, MRTG, foi possível a verificação de gargalo na rede em determinado momento. Monitorando os equipamentos, por meio do Nagios, verificou-se inúmeras vezes o não funcionamento principalmente de Access Points.

Referências

ANDRADE, H. A. (2006) "Nagios como Solução de Monitoramento de Rede", http://www.ginux.ufla.br/files/mono-HettyAndrade.pdf.

BIRKNER, M. H. (2003) "Projeto de interconexão de redes: Cisco internetwork Design", São Paulo: Pearson Education do Brasil.

CALDAS FILHO, F. L.; FERREIRA, P. E. (2013) "Projeto e Implantação de uma Nova Topologia de Rede de Computadores para o Laboratório de Informática LINF/CIC/UnB", Monografia (Graduação) - Universidade de Brasília, Brasília.

COMER, D. (2007) "Redes de computadores e internet", 4. ed. Porto Alegre: Bookman.

CONTESSA, D. F.; POLINA, E. R. (2013) "Gerenciamento de Equipamentos Usando o Protocolo SNMP", http://www.cp.com.br/upl/artigo_3.pdf.

JUNG, E. V.; PELLIS, R. R. (2013) "Aplicando Segurança em Redes Locais Através de Gerenciamento de Ativos de Rede", Pós Graduação - Pontifícia Universidade Católica do Paraná, Curitiba.

KUROSE, J. F.; ROSS, K. W. (2010) "Redes de computadores e a internet: uma abordagem top-down", 5. ed. São Paulo: Pearson Addison Wesley.

MORAES, A. F. (2008) "Redes de computadores: fundamentos", 6. ed. rev. e ampl. São Paulo: Érica.

MURHAMMER, M. W. (2000) "TCP/IP: tutorial e técnico", São Paulo: Makron Books.

OETIKER, T. (2002) "MRTG: The Multi Router Traffic Grapher", Proceedings of the 12th Systems Administration Conference (LISA '98).

SALKYS, P. H. B. et al (2007) "Gerência e Monitoramento de Redes de Computadores: uma introdução ao Nagios", Revista Varia Scientia, Cascavel, v.07, n. 13, p.149-152.

SEAGREN, E. (2007) "Secure your network for free: using nmap, wireshark, snort, nessus, and MRTG", Rockland: Syngress.

TANENBAUM, A. S.; SOUZA, V. D. (2003) "Redes de computadores", 4. ed. Rio de Janeiro: Campus.

TORRES, G. (2009) "Redes de computadores", Rio de Janeiro: Novaterra.

VERAS, M. (2009) ”Datacenter: componente central da infraestrutura de TI”, Rio de Janeiro: Brasport.