

CENTRO UNIVERSITARIO BRASILEIRO - UNIBRA CURSO DE
GRADUAÇÃO TECNÓLOGO EM REDES DE COMPUTADORES

Lucas Justo de Souza
Saulo de Tarso Ramos Alves

Gerenciamento de redes e sua gestão de qualidade

RECIFE/2022

Lucas Justo de Souza
Saulo de Tarso Ramos Alves

Gerenciamento de redes e sua gestão de qualidade

Trabalho de Conclusão de Curso
Apresentado ao Centro Universitário
Brasileiro - UNIBRA, como requisito
parcial para obtenção do título de
Tecnólogo em Redes de Computadores.
Prof^ª. Orientadora: **Ameliara Freire.**

RECIFE/2022

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 2338/ O.

S719g Souza, Lucas Justo de.
Gerenciamento de redes e sua gestão de qualidade / Lucas Justo de Souza; Saulo de Tarso Ramos Alves. - Recife: O Autor, 2022.
11 p.

Orientador(a): MSc. Ameliara Freire Santos de Miranda.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro - UNIBRA. Tecnólogo em Redes de Computadores, 2022.

Inclui Referências.

1. Gerência de redes. 2. Infra-estrutura. 3. SNMP. 4. Sistema. 5. Dados. I. Alves, Saulo de Tarso Ramos. II. Centro Universitário Brasileiro. - UNIBRA. III. Título.

CDU: 004

AGRADECIMENTOS

Dedicamos esse trabalho primeiramente a Deus por ter dado saúde mesmo em meio a pandemia que vivemos e ter dado condições para pudéssemos continuar, agradecemos também aos professores que se esforçaram para nos ensinar em um formato de aula completamente diferente do comum, e principalmente a nós estudantes por nos esforçarmos e buscarmos nosso melhor diante de tantas situações complicadas que vivemos nesse período .

RESUMO

O estudo que está sendo feito trará e abordará a *gestão de redes e sua qualidade*, no cenário atual podemos sim ver e achar falha na gestão de redes tanto da montagem e estruturação física, até mesmo nas questões lógicas de um sistema implantado. O ambiente de TI vem crescendo muito atualmente e em toda empresa é necessário um responsável pelo setor de TI, onde o mesmo tem que saber identificar os problemas e resolver os mesmos. Partindo deste ponto temos softwares de coleta de dados e monitoramento de dados e também protocolos que ajudam no processo de administração da rede maneira de identificar o problema, a melhor forma de aplicar o protocolo SNMP e como utilizar o mesmo no ambiente de gerenciamento de redes. A gerência de redes pode manter sua empresa em quesitos de TI muito bem mantida e sem preocupações futuras, prover um ambiente de TI bem estruturado e organizado é importante para que a empresa não pare de faturar e assim possa se sustentar no mercado e sem problemas deixando a mesma parada.

Palavra chave: Gerência de redes, infra-estrutura, SNMP, sistema, dados.

AM - Agente Móvel

SNMP- Simple Network Management Protocol

CMIP - Common Management Information Protocol

NMS - Network Management Station

WWW - World Wide Web

Qos - Qualidade de Serviço

SMI - Structure of Management Information

NE - Network Element

MIB - Management Information Base

SUMÁRIO

1. INTRODUÇÃO

1.2 Problemática

1.3 Justificativa

1.2 Objetivo

1.5 Objetivos específicos

2. REFERENCIAL TEÓRICO

2.1 Gerências de redes

2.2 O protocolo SNMP

2.3 Implementação do SNMP

2.4 Gerências de redes centralizadas e a análise dos dados

2.5 Implementação de softwares para controle de dados

1. INTRODUÇÃO

A evolução das tecnologias cresceu de forma diligente nas últimas décadas. No ano de 1962 o engenheiro Joseph Licklider já pensava na criação de uma rede mundial de computadores. Porém foi na década de 90 que surgiu o WWW (World Wide Web) juntamente com o HTTPS. Até o ano de 2000 que foi o ano da real popularização da internet utilizava-se a internet discada que o fornecimento da conexão era realizado por provedor que dependia de uma linha telefônica para o funcionamento. Hoje em dia o serviço de internet se tornou de fácil acesso para grande parcela da população mundial. Com esse grande avanço tecnológico a internet deixou de ser um serviço exclusivo para computador, mas passou a estar presente em vários dispositivos. Todo esse avanço tecnológico foi possível também graças ao surgimento de várias empresas que com as suas diversidades de dispositivos fabricados por várias empresas, cada uma com sua diversidade de funcionalidade. Tendo em conta o valor das redes para as empresas, o controle/gerenciamento ganhou muita importância. Assegurar com qualidade o funcionamento da rede passou a ser uma tarefa nada fácil para a área de TI das empresas. Por esse fator de não ser uma tarefa fácil a ser cumprida foram criados alguns softwares que dão suporte para esse gerenciamento. Atualmente esses sistemas vêm com a finalidade de auxiliar os profissionais da área de TI na melhor forma para gerenciar os recursos. Alguns desses sistemas são oferecidos pelas próprias empresas ou são adquiridos outros softwares dependendo da necessidade de cada empresa.

Falando sobre um protocolo imprescindível para a gestão de redes seria o protocolo SNMP (Simple Network Management Protocol) um protocolo desenvolvido para que dispositivos de rede que utilizam um protocolo que possam ser gerenciados de maneira remota. CMIP (Common Management Information Protocol – referência OSI) porém vale lembrar que o mais utilizado ainda sim é o SNMP. Também temos alguns softwares para uma melhor gestão aqui estão alguns deles, GotsiteMonitor, Sparrow IQ, Netrounds, Zabbix, Freshdesk.

1.2 Problemática

Visto que a aplicação do protocolo SNMP (Simple Network Management Protocol) para a realização da parametrização da rede ainda sim tem alguns paradigmas e inseguranças vêm que o mesmo pode ser utilizado. Se implantado de maneira correta podemos atingir um ótimo dimensionamento da rede num geral, o mesmo é

atribuído a outros protocolos, o SNMP trabalha em conjunto com CIMIP (Common Management Information Protocol). Aplicando de maneira correta a parametrização da rede fica excelente e temos um ambiente de TI mais controlado e seguro. (ARANTES; ARANTES, 2001)

1.3 Objetivos : Neste tópico serão apresentados objetivos do trabalho, sendo divididos em objetivo geral e objetivo específicos

1.3.1 Objetivo geral : Realizar um estudo sobre o monitoramento de rede voltado aos protocolos ICMP e SNMP utilizando a ferramenta Wireshark

1.3.2 Objetivo Específico :

colocaria aquelas 04 pontos que tu pois sem o texto

só adicionaria algo tipo uso de tal ferramenta

Com base nas pesquisas realizadas e mostrar as soluções e possíveis soluções e maneiras de identificar os problemas e como resolver de acordo com os níveis de problemas assim gerando uma tratativa mais assertiva, assim vindo a otimizar o tempo de trabalho dando espaço para que possamos resolver outros problemas ou realizar uma vistoria em todo o ambiente de rede.

2. REFERENCIAL TEÓRICO

2.1 Contextualização

A gerência de redes é algo muito amplo quando falamos de gerência, temos que ter em mente que vamos precisar realizar um projeto, colocar as configurações do mesmo em prática, manter o projeto em observação e corrigir os erros o mais rápido possível. Para que a estação de TI não pare com isso podemos dizer e afirmar que se tratando de gerência de redes temos que ter um conhecimento vasto, porém saber dividir e focar nossa gama de conhecimento no problema ou objetivo necessário para que não ocorra um desperdício de tempo.

Os modelos de gerência adotados atualmente são baseados na arquitetura cliente/servidor ou gerente/agente Arantes (2001). Neste modelo todo o sistema é controlado pela estação de gerenciamento que a mesma é responsável pela total gestão da rede, ela pede para os elementos de rede para que realize as operações (ARANTES, 2001).

Podemos descrever e separar em quatro partes o gerenciamento centralizado que são:

- Estação de Gerenciadora (NMS - Network Management Station) basicamente o sistema central onde é ele que controla tudo e faz o contato com os elementos de rede (ARANTES, 2001).
- Elemento de Rede (NE - Network Element) conhecido como nó o mesmo é um elemento gerenciável ou um recurso gerenciável. O nó ou NE trabalha diretamente ligado ao MIB, onde o mesmo responde ou envia informações ao NMS o gerente da rede.
- Base de Informação de Gerenciamento (MIB - Management Information Base) uma base de dados onde é armazenado os dados dos elementos gerenciáveis.
- Estrutura de Gerenciamento de Informação (SMI - Structure of Management Information) O SMI diz os parâmetros de configuração para acesso ao protocolo de suporte dos elementos gerenciados e a definição dos mesmos de

maneira

Com toda essa estrutura o gerente de rede consegue ter um controle porém o mesmo ainda sim fica sobrecarregado, com o excesso de informações por isso foi pensado sobre a implementação do protocolo SNMP assim simplificando os meios e ainda sim mantendo uma gerência organizada.

2.1 O protocolo SNMP

O protocolo SNMP foi projetado para ser um padrão de gerenciamento de redes e monitoramento e foi descrito na RFC 1067. Portanto com ele é possível que diferentes dispositivos compartilhem informações entre si dentro de uma rede.

O SNMP possui suas ferramentas específicas para gerenciamento de dispositivos e monitorar o desempenho. Com ele é possível acompanhar oscilações na rede e ver qual o status dos dispositivos em tempo real.

O Desenvolvimento do SNMP foi com base com o propósito de ter uma solução leve já que a maioria dos equipamentos a serem monitorados é de ponta (Roteadores, servidores, switches) possuindo um processamento baixo. Lembrando que o SNMP não é orientado a conexão e não tem ações prévias ou posteriores após o envio de uma mensagem (ROCHA, 2017).

Ele possui uma fácil implantação visto que ele não precisa de nenhum arquivo executável para a instalação ele já vem instalado de fábrica o usuário apenas irá o habilitar.

Na abordagem em relação às suas características o SNMP consome poucos recursos tanto de processamento quanto de custo. Abaixo listamos informações que são monitoradas pelo protocolo:

- Quantidade de processos que estão sendo executados em cada dispositivo; ● Estatísticas de tráfego;
- Informações atualizadas sobre a quantidade de toner nas impressoras; ● Informações sobre uso da memória dos dispositivos.

O modelo SNMP ainda sim é um modelo de gerência centralizada, porém mais fluido, gerando menos erros. O modelo SNMP consiste em três operações de gerenciamento:

- GET: a NMS recuperar uma informação específica do NE Arantes (2001);
- SET: a NMS altera uma informação específica no NE Arantes (2001);
- TRAP: um agente de um NE reporta um evento para a NMS Arantes (2001);

2.3 Implementação do SNMP

O primeiro passo é implementar comunicação por TCP/IP, geralmente dando a cada nó da rede um endereço IP diferente. O passo seguinte é adquirir ou programar softwares para o agente e o gerente, onde ambos geralmente já devem vir com interface gráfica para facilitar a configuração e a visualização dos dados.

Os agentes devem ser instalados em cada nó da rede, enquanto o gerente deve ser instalado em máquinas das quais se deseja monitorar a rede. Daí geralmente é só seguir as instruções dos programas para configurar a rede SNMP, especificando as MIBs (ROCHA, 2017).

2.4 Configuração do protocolo SNMP

- Passo 1: Editar > Preferências > Protocolos > SNMP > Editar
- Passo 2: Clique na opção adicionar
- Passo 3: Conforme a figura 2.2 preencha os campos Engine ID, Username, Autenticação (MD5 ou SHA1), Privacidade (DES, AES, AES192 ou AES256) e a senha
- Passo 4: Escolher a interface que deseja ser Capturado
- Passo 5: No filtro escolha a opção SNMP ou pelas portas 161 e 162 (UDP)

SNMP Users



Engine ID	Username	Authentication model	Password	Privacy protocol	Privacy password
8a45c74544	admin	MD5	123abc	DES	123bcd



C:\Users\adoni\AppData\Roaming\Wireshark\snmp_users

OK

Copy from

Cancel

Help

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.31.19.54	172.31.19.73	SNMP	82	get-request 1...
2	0.000673	172.31.19.73	172.31.19.54	SNMP	100	get-response ...
3	0.003623	172.31.19.54	172.31.19.73	SNMP	96	get-request 1...
4	0.009495	172.31.19.73	172.31.19.54	SNMP	115	get-response ...
5	0.012212	172.31.19.54	172.31.19.73	SNMP	84	get-request 1...
6	0.012966	172.31.19.73	172.31.19.54	SNMP	90	get-response ...
7	0.016247	172.31.19.54	172.31.19.73	SNMP	140	get-request 1...
8	0.022827	172.31.19.73	172.31.19.54	SNMP	165	get-response ...
9	0.025662	172.31.19.54	172.31.19.73	SNMP	86	get-request 1...
10	0.026500	172.31.19.73	172.31.19.54	SNMP	87	get-response ...
11	0.029169	172.31.19.54	172.31.19.73	SNMP	92	get-request 1...
12	0.031899	172.31.19.73	172.31.19.54	SNMP	93	get-response ...

> Frame 7: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits)
> Ethernet II, Src: Dell_4a:33:d2 (00:12:3f:4a:33:d2), Dst: FUJIFILM_15:e6:bc (08:00:37:15:e6:bc)
> Internet Protocol Version 4, Src: 172.31.19.54, Dst: 172.31.19.73
> User Datagram Protocol, Src Port: 15919, Dst Port: 161
> Simple Network Management Protocol

```

0000  08 00 37 15 e6 bc 00 12 3f 4a 33 d2 08 00 45 00  ..7....?J3...E.
0010  00 7e aa 1c 00 00 80 11 11 95 ac 1f 13 36 ac 1f  ~.....-6...
0020  13 49 3e 2f 00 a1 00 6a f5 06 30 60 02 01 00 04  I>/...j..0'....
0030  06 70 75 62 6c 69 63 a0 53 02 01 29 02 01 00 02  public.S...
0040  01 00 30 48 30 16 06 12 2b 06 01 04 01 81 7d 08  .0H0...+...}
0050  40 04 02 01 07 0a 86 de b7 38 05 00 30 16 06 12  @.....8..0...
0060  2b 06 01 04 01 81 7d 08 40 04 02 01 07 0a 86 de  +...}-@.....
0070  b7 36 05 00 30 16 06 12 2b 06 01 04 01 81 7d 08  .6..0...+...}
0080  40 04 02 01 05 0a 86 de b9 60 05 00  @.....:..

```

2.4 Gerências de redes centralizadas e a análise dos dados

Na gestão de redes centralizada, os nós ou (NEs) onde os mesmos estão espalhados pela rede eles por possuir os MIBs a base de dados os NEs, ajudam na coleta de dado para realizar o processo de análise de dados com isso podemos entender que pode ocasionar uma grande demanda de tráfego de dados das NEs para a NMS assim ocasionando uma limitação de flexibilidade, escalabilidade, desempenho, eficiência além de gerar o congestionamento nos meio de transmissões fazendo assim com que a rede fique instável.

De acordo com (ARANTES, 2001), essas limitações podem ser percebidas pela execução de tarefas simples como em empresas de pequeno porte. Isso vem se intensificando com o crescimento atual do ambiente de TI e também a maior implementação de sistemas mais complexos, conforme o tempo passa a tecnologia muda e automaticamente novos sistemas são implementados e daí vem também a exigência de QoS (Qualidade de Serviço) esses serviços que muitos deles são

exigidos pelo cliente e até mesmo gama da rede exige uma melhor qualidade e automaticamente uma melhor maneira de ser gerenciada.

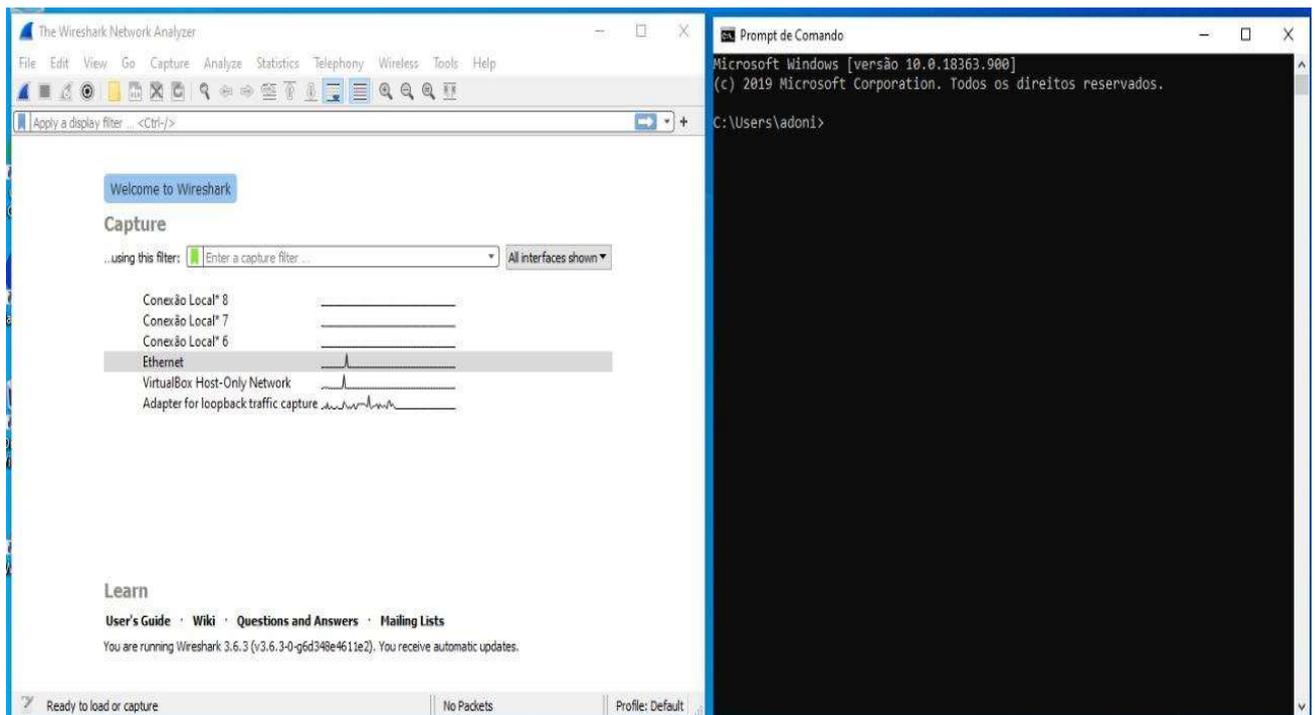
Na gestão de redes a arquitetura centralizada se mostra ainda mais ineficiente em períodos de congestionamento, um exemplo disso que podemos mostrar é um horário onde a loja ou empresa começa a ter muitos acessos simultâneos, isso vai gerar uma grande demanda gestão para estabilizar a situação e voltar a rede ao normal. Basicamente esse congestionamento acontece porque a NMS fica atuando mais com os elementos de rede para a busca de dados, assim as NEs começam a mandar notificações para a NMS o que vai intensificar o congestionamento.

2.5 Protocolo ICMP

O protocolo ICMP (Internet Control Message Protocol) pertence ao nicho do TCP/IP e permite a comunicação entre gateway e hosts. O mesmo é responsável por mandar uma mensagem ao gerente relatando o funcionamento da rede (GUGELMIN, 2012).

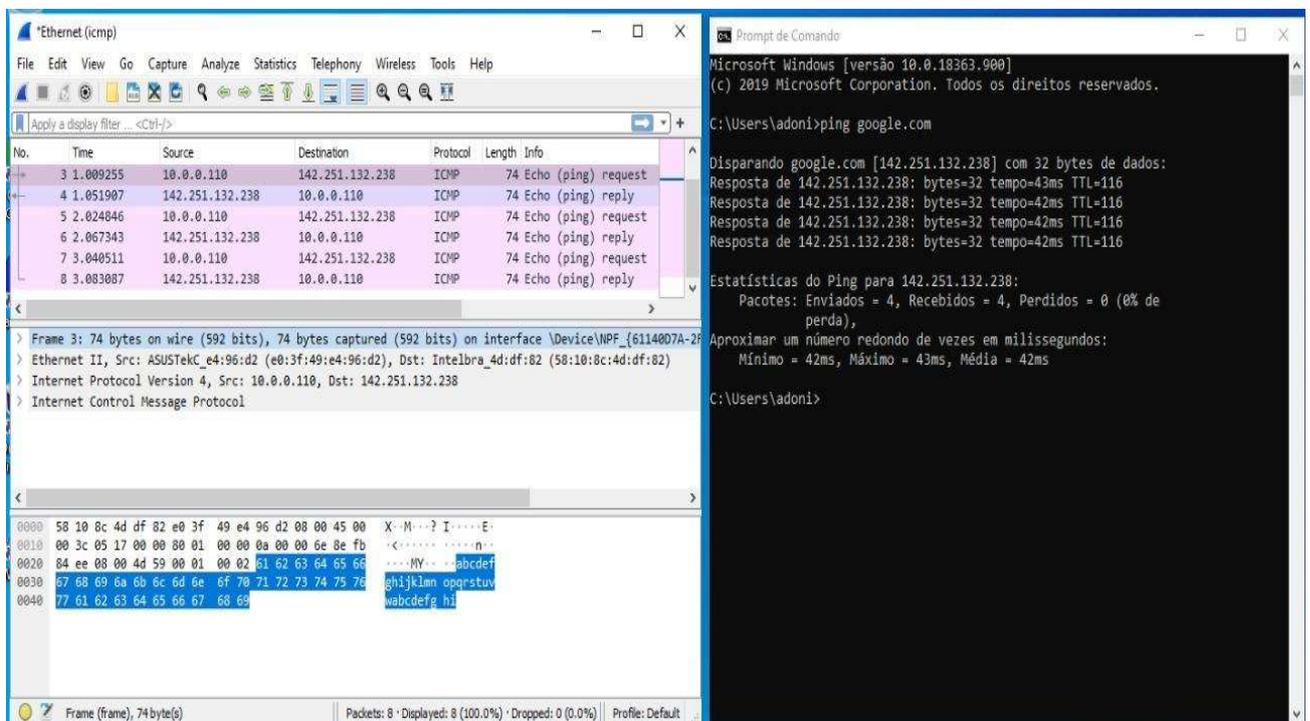
O mesmo é uma ferramenta que é aplicada na maioria dos ambientes de TI para buscar a melhora e o monitoramento da rede de maneira constante, assim podemos identificar os erros e os estados para o requisitante, neste caso o responsável de TI da empresa. O protocolo IP em si já possui um mecanismo de detecção de erros em que através de um checksum de cabeçalho de cada datagrama que é criado pelo host de origem e verificado pelo host de destino GUGELMIN (2012), essas mensagens são datagramas que se não conforme como o que é pedido são descartadas sem que ocorra uma avaliação deste datagrama, não ocorre uma análise. (GUGELMIN, 2012).

Figura 2.5



Referente à ferramenta Wireshark que é utilizada para realizar a captura de pacotes ICMP e a janela do prompt comando;

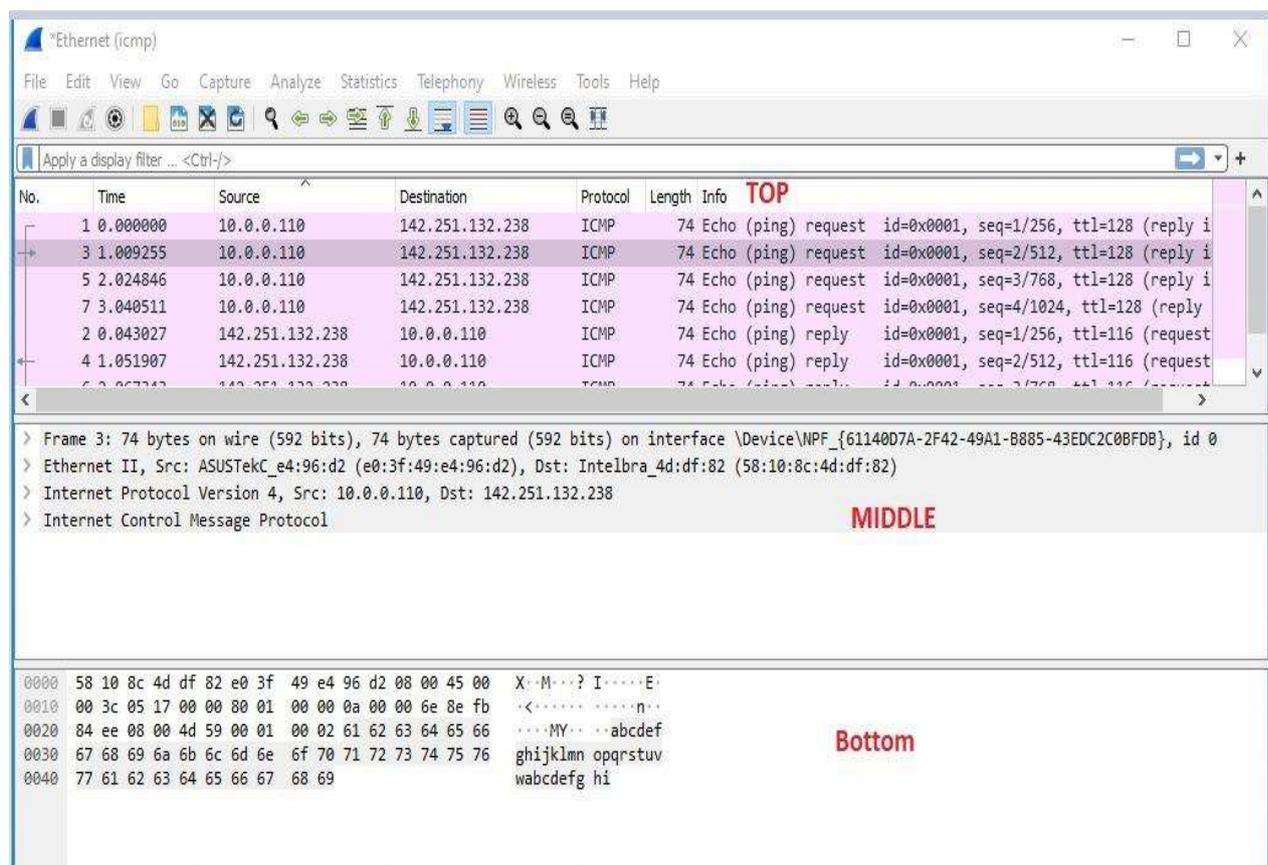
Figura 2.6



Foi realizado um ping para o goole.com para ser dado Inicio a captura dos pacotes do

ICMP. O ICMP também é filtrado utilizando o comando traceroute.

Figura 2.7



Campo TOP é o tráfego de pacotes ICMP. MIDDLE é referente às informações do cabeçalho do pacote solicitado para a análise. BOTTOM Neste campo são as informações em binário

2.9 Implementação de softwares para controle de dados

Os softwares de monitoramento/controle de dados servem para realizar uma preventiva na rede onde vai fazer que as mesmas não fiquem paradas para ser realizada uma manutenção corretiva, assim gerando uma perda na produtividade ou até mesmo se for um setor de vendas gerar uma perda monetária para as empresas. Com tudo sabemos que é difícil realizar um controle de uma ambiente de TI mesmo

que pequeno, por isso podemos realizar a implantação desses softwares:

GotsiteMonitor : É um serviço de monitoramento de sites, hosts e serviços que permite observar os tempos de resposta para seus serviços a partir de 12 pontos espalhados pelo mundo. Muito útil para empresas que têm clientes e/ou filiais espalhadas pelo mundo.

Sparrow IQ: É uma ferramenta para monitoramento de banda, com detalhes sobre o volume de tráfego e identificação de protocolos e aplicações.

Netrounds: É um software de monitoramento de rede baseado em probes, o que significa que ele gera tráfego na sua rede, fazendo monitoramento tanto ativo como passivo, com o objetivo de medir latência, jitter e outros indicadores importantes para qualquer sysadmin.

Zabbix: é uma ferramenta de monitoramento de redes ou já estão onde ela a mesma monitora servidores serviços foi desenvolvida para monitorar a disponibilidade e a experiência do usuário com os serviços oferecidos ou com o seu servidor de busca ou de sua empresa a mesma consegue oferecer o monitoramento pela internet a mesma também atribui o protocolo SNMP muito utilizado na gestão de redes

Wireshark: Um software que analisa os protocolos, porém voltado mais para a segurança da rede também chamado de Sniffer ou (farejador em português) ele é utilizado para monitorar a rede, detectar problemas ou até mesmo identificar conexões suspeitas ele pode também testar as senhas utilizadas na rede para saber se as mesmas estão criptografadas. O mesmo pode ser utilizado por pessoas leigas e também oferece mais informações técnicas para quem já tem prática na área de atuação mas o que podemos dizer é que esse software pode ajudar no monitoramento do tráfego da rede.

3.0 Conclusão

O estudo apresentado neste trabalho teve como objetivo informar ao leitor sobre o funcionamento e qual seria a aplicação dos protocolos SNMP e ICMP. Uma parte relevante desta pesquisa foram as formas as quais as aplicações foram realizadas

para demonstrar ao leitor do texto da configuração até o momento em que ocorre a captura de pacotes para sua análise diante da ferramenta escolhida pelos autores. Diante deste cenário fica claro que o bom uso da ferramenta aliado com o conhecimento sobre determinado protocolo irá conseguir de modo geral um ótimo gerenciamento de rede.

O trabalho em si nos contribuiu para um alto desenvolvimento pessoal dado que ampliou o nosso conhecimento por meio do trabalho multidisciplinar implementando e aplicando os protocolos citados ao longo deste trabalho. O atual estudo ainda poderá auxiliar os leitores que buscam conhecimentos em relação ao uso do wireshark para os protocolos que foram analisados.