Mário Amisse Algema

Implementação de Listas de Controle de Acesso (ACL) como mecanismos de Segurança em Redes de Computadores.
Caso de Estudo -Águas da Região de Maputo.

Licenciatura em Informática

Universidade Pedagógica de Maputo

Maputo

2023

Mário Amisse Algema

Implementação de Listas de Controle de Acesso (ACL) como mecanismos de Segurança em Redes Computadores.
Caso de Estudo -Águas da Região de Maputo.

Licenciatura em Informática

Monografia do final do curso, apresentado no departamento pedagógico, na Faculdade de Engenharia e Tecnologias da (UPM), Em cumprimento aos requisitos para a obtenção do grau académico de licenciatura em informática.

Supervisor:
Dr. Xadreque Macamo

Universidade Pedagógica de Maputo
Maputo
2023

ÍNDICE

ÍNDICE DE TABELAS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

ACL- Access Control List

AdeM- Águas da Região de Maputo

DHCP- Dynamic Host Configuration Protocol

DoS -Denial of Service

DUAL - Diffusing Update Algorithm

EIGRP- Enhanced Interior Gateway Routing Protocol

FET- Faculdade de Engenharia e Tecnologias

FTP File Transfer Protocol

ICMP- Internet Control Message Protocol

IEEE- Instituto de Engenheiros Electricistas e Electrónico

IETF- Internet Engineering Task Force

IGP- Interior Gate Protocol

IOS- Internetwork Operating System

IP- Internet Protocol

LAN- Local Area Network

MAC -Media Acess Control

NAT- Network Address Translation

OSPF- Open Shortest Path First

QoS- Quality of Service

RH- Recursos-Humanos

RIP- Routing Information Protocol

SNMP -Simple Network Management Protocol

TCP- Transmission Control Protocol

TI- Tecnologia e Informação

UDP- User Datagram Protocol

UPM- Universidade Pedagógica de Maputo

VLAN- Virtual Local Area Network

VPN-Virtual Private Network

VTP- Vlan Trunking Protocol

WAN- Wide Area Network

DECLARAÇÃO

Declaro que esta Monografia é resultado da minha investigação pessoal e orientação do meu Supervisor, o seu conteúdo é original e todas as fontes consultadas estão devidamente mencionadas no texto, nas notas e na bibliografia final.

Declaro ainda que este trabalho não foi apresentado em nenhuma outra instituição para obtenção de qualquer grau académico.

Maputo,____de_____de_____

_____

(Mário Amisse Algema)

DEDICATÓRIA

Dedico este trabalho a minha Mãe, Clarinha Mussa. Que foi incansável na tentativa de proporcionar aos seus filhos a melhor educação.

Aos meus irmãos Zacarias Mussama, Anastácia Mussama, Erlinda José e Antoninho José que sempre me apoiaram e depositaram confiança.

AGRADECIMENTOS

Em primeiro lugar agradeço o meu supervisor dr. Xadreque Macamo, pela dedicação e conselhos que foram de grande ajuda na realização deste trabalho.

Aos meus pais, pelos conselhos e por me tornarem no homem que sou hoje, mostrando que através do conhecimento se ganha a vida, mas que com a sabedoria se constrói uma história.

A todos docentes e funcionários da Universidade Pedagógica de Maputo (UPM) que contribuíram directa e indirectamente para minha formação.

A todos os amigos e colegas que estudaram comigo na Universidade Pedagógica de Maputo.

Muito Obrigado!

RESUMO

Este trabalho consiste na implementação de mecanismos de segurança em redes de dados nas Águas da Região de Maputo, O trabalho tem como finalidade implementar políticas de controle de acesso mais robustas baseada em Access Control Lists (ACLs) nos três (3) departamentos, departamentos de Vendas, Recursos Humanos e Contabilidade, O objectivo concreto deste trabalho é aplicar políticas de controle de acesso baseada em filtros de pacotes para proteger o acesso não autorizado de recursos na rede. Espera-se com este trabalho mostrar a necessidade de manter segurança usando ACLs como ferramenta poderosa para evitar ataques internos e externos na rede de dado, controlar e tornar seguro o tráfego na rede.

Palavras-chaves: ACLs, Segurança de rede, Filtros de pacotes.

ABSTRACT

This work consists of the implementation of security mechanisms in data networks in Maputo Region Waters, The work aims to implement more robust access control policies based on Access Control Lists (ACLs) in the three (3) departments, Sales, Human Resources and Accounting, The concrete objective of this work is to apply access control policies based on packet filters to protect unauthorized access to network resources. wait with this work to show the need to maintain security using ACLs as a powerful tool to prevent internal and external attacks on the data network, control and secure network traffic.

Key-words: ACLs, Network security, Packet filters.

1. Capítulo I-Introdução

Com o aumento da utilização das redes de computadores e da internet, em várias instituições é acompanhado também com aumento de números de invasões e infecções por vírus, tai surgiu então à necessidade primária de investimento na área de segurança de redes.

Hoje em dia em debates públicos sobre tecnologias de informação e comunicação que acontecem na área tecnológica em Moçambique, assim como no mundo fora é comum falarem sobre a segurança das tecnologias de informação e comunicação, o facto que exige maior segurança das redes de computadores.

A segurança possui muitas faces e uma das mais importantes é a capacidade de controlar o fluxo de pacotes em uma rede, com o objectivo de proteger nossas redes de falhas, degradação dos serviços, roubo ou comprometimento dos dados resultantes de uma acção intencional ou de um erro provocado por usuários.

Actualmente, um dos grandes desafios dos administradores de redes de uma empresa é sem dúvida alguma manter seu ambiente seguro e principalmente estabelecer um controle de tráfego de pacotes nesta rede, daí a necessidade de utilizarmos as Listas de Controle de Acesso.

A segurança das redes informáticas é hoje um ponto de extrema relevância no que respeita à transmissão de dados entre experiências dentro da rede local e entre redes com localizações geográficas diferentes.

O foco principal da Segurança da Informação é proteger o activo mais importante para o negócio da empresa, as informações devendo assim ser colocado em prática os requisitos responsáveis pela segurança que conforme a NBR/ISO/IEC 27002, são eles: confidencialidade, integridade e disponibilidade; apesar de não ser os únicos pontos importantes da segurança, ao atender os critérios necessários aos pilares da segurança, grande parte da protecção estará garantida (LAURENO, 2005).

Fazendo o bom uso da Segurança da Informação a empresa terá muitos benefícios e com isso poderá dar continuidade a seus trabalhos. Com a evolução tecnológica o mundo pode-se conectar com mais facilidade e assim fazer a troca de informações. Porém o risco de perdê-las é maior, já que há muita gente com capacidade de invadir sistemas e roubar ou alterar tais informações.

LYRA (2008) enfatiza que a segurança da informação é obtida com a implementação de um conjunto de controle adequados que inclui políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles, além de implementados, precisam de ser estabelecidos, monitorados, analisados criticamente e melhorados onde for necessário, para garantir que os objectivos do negócio e da segurança da organização sejam atendidos.

1.1 Problematização

Durante o período de estágio nas Águas da Região de Maputo, um dos problemas identificados tem a ver com ataques internos e falta de mecanismos de controle de tráfego broadcast na rede de computadores. Todos colaboradores têm acesso a todos recursos da rede, servidor de ficheiro e tem acesso a porta 80 através de servidor Web da empresa, como consequência regista falhas constante na rede e lentidão principalmente no acesso a internet porque todos funcionários querem acessar a internet numa rede que funciona com 4Mbps.

Os funcionários passam muito tempo nas redes sócias deixando para mais tarde as suas tarefas diárias ou acaba por não cumprir as suas metas diárias, regista se muito tráfego na rede de forma desnecessária e fazem download de vídeos que não agrega valor no funcionamento da empresa, e a instituição queixa se com a vulnerabilidade da rede.

O link que vai para servidor Web e servidor de ficheiros (FTP) ficam congestionados com maior tráfegos de dados que fluem no link não oferecendo maior largura de banda para uma rede de 4 Mbps. Como consequências disso, não há qualidades de serviços (QoS) na rede e dificulta o troubleshoot dos administradores de rede

Água da região de Maputo (AdeM) tem falta de um sistema de segurança interna no acesso a recursos da rede, falta de sistemas de permissão ou negação para acesso a um certo sistema como forma de optimizar o tráfego dentro da rede.

Portanto, a actual organização da rede impossibilita o fluxo adequado de dados, controle e o monitoramento das operações, o acesso aos servidores não é apropriada e o uso indevido de largura de banda da rede tem consequências desagradável para o bom funcionamento da rede. O problema de pesquisa é garantir maior qualidade de serviço (QoS) e maior segurança no acesso a recursos da rede das águas da região de Maputo e controlar o tráfego de dados e melhor gestão de recursos da rede e dar permissão ou negação para certos grupos de usuários dentro da rede.

Com base nessas evidências formula-se o seguinte problema de investigação até que ponto a rede das Águas da Região de Maputo pode implementar um sistema de segurança baseada em filtros de pacotes na rede?

Segundo (FILIPPETTI, 2008) Listas de controle de acesso (ACLs) são os filtros de pacotes de uma rede. Listas de Controle de Acesso (ACL) podem restringir, permitir ou negar o tráfego que é essencial para a segurança., Uma ACL permite que você controle o fluxo de pacotes para um único ou grupo de endereço IP ou diferente para protocolos, tais como TCP, UDP, ICMP, etc.

Definindo um contexto especifico, O presente trabalho pretende abordar conceitos teóricos e práticos referente a implementação de Listas de controle de Acesso (ACLs) na AdeM.

1.2 Justificativa

O que levou me a escolha do tema deve-se ao facto de Águas da Região de Maputo registar constante anomalias relacionada com ataques internos e externos, ataques causados por próprios colaboradores de forma tensional e intencional, tai surgiu a necessidade de implementar políticas de controle de acesso para solucionar esses tipos de ataque, permitir maior controle de acesso a recursos da rede. As medidas de controle de acesso para ameaças externas deve ser proporcional as medidas de ataque internas, por este razão as listas de controle de acesso deve ser os primeiros mecanismos de seguranças em rede para evitar ataques internos e externos. A razão da escolha do tema deve também o facto de Listas de Controle de Acesso ser mecanismos que não envolve muito custo para a sua implementação. Hoje em dia não basta ter uma rede de dados, mas sim é necessário investir na segurança da rede para garantir a segurança da informação, dos recursos e melhorar o tráfego de dados e acesso a recursos da rede. Manter a conectividade é muito importante, mas também precisamos manter a segurança, manter a robustez da rede, e seguir as políticas de negócio de nossa empresa.

1.3 Objectivos

1.3.1 Objectivo Geral

- ✓ Implementação de Listas de controle de Acesso (ACLs) na Águas da Região de Maputo para solucionar problemas de vulnerabilidades na rede.

1.3.2 Objectivos Específicos

- ✓ Efectuar o diagnóstico do estado actual da rede;
- ✓ Identificar os departamentos a implementar as Listas;
- ✓ Escolher melhor Listas de Control de Acesso (ACLs) a ser aplicada.

1.4 Questões de Pesquisa

- ➢ Qual é o melhor política de controle de acesso para aplicar na AdeM?
- ➢ Como tornar a rede de dados da AdeM efectivamente fiável e segura?
- ➢ Qual será o impacto com implementação de ACL na AdeM?

1.5 Hipóteses

Hipótese 1: Listas de Controle de Acesso (ACLs) é a melhor política de controle de acesso para resolver os problemas identificados na AdeM;

Hipótese 2: Para tornar a rede de AdeM efectivamente fiável e segura é preciso criar politicas, normas e procedimentos de gestão que vai de acordo com a necessidade da empresa;

Hipótese 3: implementação de Listas de controle de acesso (ACL), na águas da região de Maputo espera se reduzir ataques internos e sobrecarga dos equipamentos, e proporcionar maior segurança da rede.

1.6 Metodologia

A metodologia de investigação refere-se as fases ou procedimentos que se seguem em determinada investigação, e tem como finalidade determinar as regras de investigação e a prova da veracidade científica (Vilelas, 2009).

Com vista a alcançar os objectivos do presente trabalho, adoptou-se o método de abordagem qualitativo, como também as técnicas de recolha de dados tais como revisão bibliográfica e entrevistas.

Para a realização deste trabalho foi realizado uma grande pesquisa por meio de livros, artigos científicos e sites na internet sobre o tema do projecto. Também foi necessário um estudo de como implementar e configurar ACL para solucionar os problemas identificados, prevenir e identificar novos problemas causados por essas vulnerabilidades.

Quanto ao trabalho de campo, ele consistiu na recolha de dados no terreno, com entrevistas dos técnicos de redes de computadores da empresa, fazendo anotações num diário de campo que serviram posteriormente para a redacção do trabalho final.

Revisão bibliográfica: esta etapa consistiu na análise de literaturas publicadas em forma de livros, revistas, artigos e outras fontes disponíveis na *internet* como forma de compreender e verificar aspectos similares abordados por diferentes autores sobre a segurança baseada em ACLs e os protocolos a ele associado. Após a revisão bibliográfica realizou-se a pesquisa de campo com o objectivo de avaliar o estudo de caso.

Entrevista: para a obtenção da informação inerente a segurança em rede naquela Instituição foram realizadas entrevistas com técnicos de rede e funcionários das Águas da região de Maputo com o objectivo de recolher dados para fazer uma posterior análise das combinações sobre a vida dos funcionários e suas funções dentro da instituição, Questionando aspectos relativos a Segurança em redes de computadores, e o porquê da necessidade da implementação de listas de controle de Acesso para uma empresa corporativa.

Escolha de ACL Estendidas: Após diagnóstico feito na rede então existente, verificou-se a necessidade de implementar ACL Estendida. A razão mais importante para escolher Listas de Controle de Acesso (ACLs) estendidas é o facto de fornecer maior segurança na rede, uma vez que as Listas de Controle Acesso Estendida verificam os endereços de origem e de destino dos pacotes. Elas podem também verificar protocolos específicos, números de portas, e outros parâmetros, que permitem maior flexibilidade e controlo por parte de administradores.

Após a implementação de Listas de Controle de acesso (ACL), verificou-se um relevante salto de qualidade da rede e segurança, com aumento da largura de banda para tráfego de dados.

1.7 Estrutura do Trabalho

O presente trabalho está organizado em 5 capítulos:

Capítulo I- (Introdução): Refere-se a introdução, onde dá-se a conhecer o estado da arte e faz-se, também, o enquadramento contextual do tema. Ainda neste capítulo mencionam-se os objectivos do estudo e a metodologia usada para a materialização do estudo.

Capítulo II - (Revisões literárias): Refere-se a parte do trabalho onde se aborda conceitos teóricos, de modo a correlacionar a pesquisa com o universo teórico. Aqui são mencionadas as definições essenciais para a consubstanciação do estudo, é feita a revisão bibliográfica.

Capítulo III- (Apresentação e discussão do Resultado): será feito um levantamento da situação da rede actual, mostrando os problemas que foram identificados e as possíveis soluções.

Capítulo IV- (Conclusão e recomendações): Refere-se a parte onde são apresentadas as conclusões do trabalho, levantadas recomendações e possíveis melhorias.

Capítulo V- (Referencias Bibliográficas): Refere-se os livros e sites consultados para a produção do trabalho.

2 Capítulo II- Referencial Teórico

2.1 Listas de Controle de Acesso ou Access Control Lists (ACLs).

Segundo (ROVERE, 2018),Uma lista de controle de acesso (ACL) é uma lista de regras que especifica quais usuários ou sistemas têm acesso concedido ou negado a um determinado objecto ou recurso do sistema. As listas de controle de acesso também são instaladas em roteadores ou switches, onde actuam como filtros, gerenciando qual tráfego pode acessar a rede.

Já (FILIPPETTI, 2008), ressalta que ACL: São listas de controle de acesso são aplicadas na interface do roteador, que filtram o tráfego na rede. Essas listas contem informações sobre os tipos de pacotes que o roteador deve aceitar ou recusar. Elas gerenciam o tráfego aumentando a segurança na rede.

Uma das habilidades mais importantes das quais um administrador de rede precisa é dominar as listas de controle de acesso (ACLs). Os administradores utilizam as ACLs a fim de parar o tráfego ou permitir apenas o tráfego especificado enquanto interrompe todo o restante do tráfego em suas redes.

A razão mais importante para configurar as ACLs é fornecer segurança para a sua rede e utiliza-las para outros parâmetros (QoS, validação de tráfego, etc).

Para que um servidor forneça acesso a um recurso, ele antes consulta a lista para verificar se o dispositivo que o está requisitando possui permissão para utilizá-lo. As listas de controle de acesso normalmente definem suas permissões com base em atributos do requisitante e do recurso solicitado. (ROUSE MARGARET, 2009).

O objectivo do controle de acesso físico não é proibir ou dificultar o acesso, mas controlá-lo. Um bom sistema de controle de acesso físico deve ser capaz de assegurar a entrada fácil e simplificada das pessoas devidamente autorizadas, e detectar e/ou impedir o acesso de pessoas não autorizadas (ODOM, 2003).

Segundo **(**FERREIRA**,** 2002), Uma ACL, no contexto dos produtos Cisco é um recurso que permite filtrar determinados pacotes, exactamente como um firewall faria, porém de uma maneira muito mais simplificada e com menos recursos. A utilização de ACLs permite filtrar tentativas de conexões indo/vindo de/para hosts específicos.

2.2 Aplicação de Listas de Controle de Acesso (ACLs)

Conforme ROVERE (2018), as ACLs são instruções que faz o controle dos acessos que são aplicadas a endereços ou protocolos de camada superior. ACLs tem uma forma eficaz de controle de tráfego dentro e fora da rede. Podendo fazer configurações para todos os protocolos de rede roteados. Um dos pontos mais importantes de usar o ACL é fornecer segurança para a rede, para validação de tráfegos, etc.

Os cenários para a utilização de Listas de Controle de Acesso são quase ilimitados. Você poderá permitir somente um host da sua rede a realizar certas tarefas ou transmitir certos protocolos, enquanto negando todo o resto na rede.

Assim como qualquer outro componente em uma rede, o emprego de Access Control Lists deverá ser planejado, criteriosamente. Onde se fizer necessário, uma ACL será sempre bem-vinda. Caso você necessite bloquear um determinado host para o acesso à segmentos específicos da sua rede, o posicionamento correto de uma Access-List oferecerá a solução mais rápida, e provavelmente a menos custosa **(**MAYRA, 2011).

Caso você possua um pool de endereços IP que precisam ser traduzidos aleatoriamente em um determinado perímetro de segurança, o posicionamento de uma Access List, em conjunto com os parâmetros do NAT, oferecerá uma solução completa.

Normalmente as ACLs são utilizadas em roteadores compondo o perímetro de segurança dentro da sua rede. Por mais que você disponha de *firewalls* dedicados, a inserção de *Access Control Lists* em um roteador Cisco oferecerá uma nível de segurança adicional, garantindo ainda mais a integridade da sua rede.

A utilização de Access Controle Lists (ACL), será sempre necessária quando você pretende manipular o tráfego utilizando recursos do Cisco e prover a segurança básica do seu roteador ou perímetro de segurança.

2.2.1 Benefícios de uma ACL

Segundo o (ODOM, 2003), "A implementação de listas de acesso pode ter um impacto positivo na rede na medida em que pode reduzir de forma bastante significativa a carga dos dispositivos de rede, Particularmente Routers, através da redução do tráfego devido a filtragem de pacotes.

De acordo com (ROVERE, 2012), As ACLs podem permitir ou negar o tráfego para certo endereço ou tipo de trafego e podem restringir a utilização da rede para um serviço e/ou dispositivo. As ACLs fornecem uma forma eficiente de controlar o tráfego dentro e fora da sua rede. Você pode configurar as ACLs para todos os protocolos de rede roteados. A razão mais importante para configurar as ACLs é fornecer segurança para a sua rede e utiliza-las para outro parâmetros (QoS, validação de tráfego, etc).

De acordo com SADAYAO e FILIPPETTI, dizem, os principais benefícios do uso de listas de acesso são os seguintes:

Bloquear tráfego indesejado ou usuários - As listas de acesso podem filtrar pacotes de entrada ou de saída em uma interface, controlando assim o acesso a uma rede com base em endereços de origem, endereços de destino ou autenticação de usuário. Pode-se também usar as listas de acesso para determinar os tipos de tráfego encaminhados ou bloqueados nas interfaces do dispositivo. Por exemplo, pode-se usar listas de acesso para permitir que o tráfego de e-mail seja encaminhado através de uma rede e para bloquear a entrada de todo o tráfego *Telnet* numa rede.

Controlar o acesso para *vty* - As listas de acesso em um *vty* de entrada (*Telnet*) podem controlar quem pode aceder as linhas para um dispositivo. As listas de acesso em um *vty* de saída podem controlar os destinos que as linhas de um dispositivo podem alcançar.

Fornecer controlo de largura de banda - As listas de acesso em um *link* lento podem impedir o excesso de tráfego em uma rede.

Fornecer controlo NAT - as listas de acesso podem controlar quais endereços são traduzidos pelo *Network Address Translation* (NAT).

Reduzir a probabilidade de ataques DoS - As listas de acesso reduzem a probabilidade de ataques de negação de serviço (DoS). É possível especificar os endereços IP de origem para controlar o tráfego de *hosts*, redes ou usuários que tencionam aceder à rede. É possível configurar o recurso TCP *Intercept* para impedir que os servidores sejam inundados com pedidos de conexão.

2.2.2 Finalidade das ACL

Segundo (FILIPPETTI, 2008), A filtragem de pacote, às vezes chamada de filtragem de pacote estática, controla acesso a uma rede analisando os pacotes de entrada e saída e transmitindo-os ou eliminando-os com base em critérios, como o endereço IP de origem, o Endereço IP de destino e o protocolo transportado no pacote. Um roteador actua como um filtro de pacote ao encaminhar ou

recusar pacotes de acordo com as regras de filtragem. Uma ACL é uma lista sequencial de instruções de permissão ou de negação, conhecidas como entradas de controle de acesso (ACEs).

De acordo com **(**ODOM, 2003), quando configuradas, as ACLs executam as seguintes tarefas:

Limitar o tráfego e aumentam o desempenho da rede. Por exemplo, se a política corporativa não permite tráfego de vídeo na rede, as ACLs que bloqueiam tráfego de vídeo podem ser configuradas e aplicadas. Isso reduziria significativamente a carga da rede e aumentaria o desempenho da rede.

Fornecer controle de fluxo de tráfego. As ACLs podem restringir a entrega de actualizações de roteamento. Se as actualizações não forem necessárias devido às condições da rede, a largura de banda é preservada.

2.2.3 Tipos de Listas de controle de acesso (ACLs)

Existem vários tipos de listas de controle de acesso e a maioria é definida para um propósito ou protocolo distinto. Em roteadores Cisco, existem dois tipos principais: padrão e estendido. Esses dois tipos são os ACLs mais amplamente usados, (FILIPPETTI, 2008, pág. 28).

2.2.4 Access list Standard (Padrão)

Access lists Standard chamado também de lista Normal - A lista de acesso Standard verifica o IP de origem de um pacote que pode ser roteado. Baseada na rede/sub-rede/ endereço do hosts é permitido ou bloqueado o envio do pacote, ou seja, que o mesmo saia por outra interface.

2.2.5 Listas de controle de Acesso Estendida

Para (FILIPPETTI, 2008, pág. 29), ACL Estendida é utilizada para filtrar pacotes baseados na origem e no destino através de protocolo (IP, TCP, ICMP, etc.) e número de porta. Devem estar mais próximos da origem para evitar o uso desnecessário da rede e permitem maior flexibilidade e controlo por parte de administradores.

De acordo com (FILIPPETTI, 2008, pág. 30), É usado o comando *access-list* no modo de configuração global para criar uma entrada numa ACL estendida IPv4. Deve ser atribuído um valor para a ACL que varia de 100 à 199 ou de 2000 à 1699. Os comandos Permit/Deny determinam a permissão ou negação de tráfego de uma determinada origem. Em seguida deve-se colocar o endereço IP e a máscara *wildcard* da origem e do destino.

Quando se deseja permitir ou negar um serviço específico ou conjuntos de serviços, torna-se necessário o uso de um operador que pode ser lt (*less than*), gt (*greater than*), eq (*equal*), neq (*not equal*), range (*inclusive range*). O comando port especifica o número da porta ou das portas TCP ou UDP que se deseja permitir ou negar o tráfego. **Access-list** <#> <Permit> any any

É usado quando é feita uma lista com base em negações para evitar a negação de todos os outros pacotes por causa da declaração de negação implícita no final da lista de acesso

2.2.6 Listas de controle de acesso (ACLs) Numeradas

As ACLs podem ser identificadas utilizando números ou nomes. Nas ACLs numeradas o número é atribuído com base no protocolo que será filtrado, de 1 a 99 e 1300 a 1999 para ACL Padrão e de 100 a 199 e 2000 a 2699 para ACL Estendida.

As listas de acesso tem grande importância para o controle, entretanto, em grandes redes as listas numeradas não são a melhor opção, levando em consideração o gerenciamento das listas existentes e o facto de que elas não podem ser editadas. Para resolver tais problemas, foram criadas as listas de acesso nomeadas, facilitando o gerenciamento através de nomes intuitivos definidos pelo administrador e facilitando as modificações, permitindo a exclusão ou inserção de uma nova linha. (FILIPPETTI, 2008).

2.2.7 Listas de controle de Acesso (ACLs) Nomeadas

ACLs nomeadas podem ser usadas para comparar os mesmos pacotes, com os mesmos parâmetros, que você pode comparar com as ACLs IP numeradas - padrão e estendida. A mais óbvia diferença entre as ACLs numeradas e nomeadas é que o IOS identifica ACLs nomeadas usando nomes, ficando mais fácil gerenciá-las. ACLs nomeadas têm também outra característica muito importante, que as ACLs numeradas não têm: você pode deletar uma linha individual, sem necessidade de deletar toda a ACL.

Em uma ACL numerada a exclusão de uma linha apaga toda a ACL criada. Uma óptima dica, que serve para os dois casos, é escrever toda ACL em um editor de textos, e aplicá-la depois de revisada em seu equipamento. Além disso, existe outra diferença importante de configuração entre ACLs numeradas e nomeadas. ACLs nomeadas usam uma configuração global que coloca o usuário em um sub modo de configuração, onde são configuradas as permissões e negações lógicas (permit / deny) (FILIPPETTI, 2008).

2.2.8 Diferença entre Firewall e ACLs

Uma ACL é o mesmo que um *Firewall* sem estado, que apenas restringe, bloqueia ou permite os pacotes que estão fluindo da origem para o destino. As ACLs são usadas em redes internas, ou seja, um provedor não aplicar Regras de ACL para a saída ou entrada de pacotes dos clientes (FILIPPETTI, 2008).

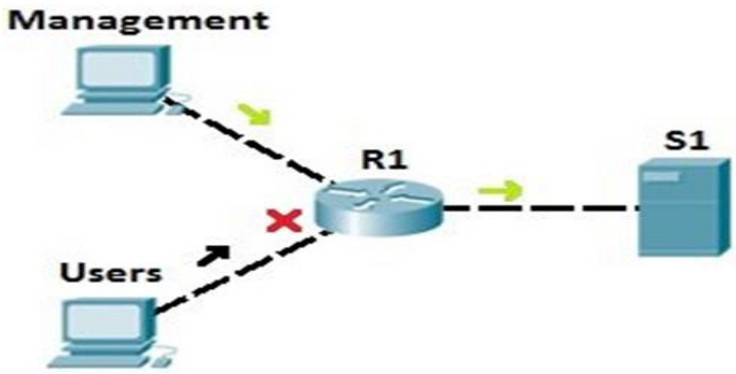

Figura1: Topologia de Rede com ACL
Fonte: (Filippetti, 2008)

Ao contrário da maioria dos Firewalls, ACLs comportam-se de maneira *stateless*, ou seja, todo o tráfego entrando o saindo é verificado pacote por pacote e comparado à ACL para que sejam tomadas as decisões de aceitar ou rejeitar o pacote, de acordo com as ações que o administrador determinou.

2.2.9 Firewall

É um sistema ou grupo de sistemas que aplicam politicas de seguranças de controle de acesso entre duas (2) redes, rede interna e rede externa, ou seja serve para proteger a rede interna de ataques externos (MARCOS, 2006)

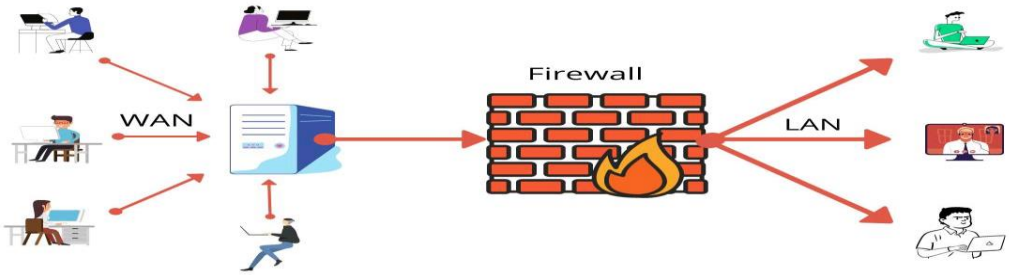

Figura 2: Topologia de Rede com firewall.
Fonte: (FOROUZAN, 2006)

Segundo (FOROUZAN, 2006), Ao contrário do que muitos pensam, um *firewall* não é um dispositivo único, mas sim um conjunto de ferramentas de segurança instaladas e configuradas de modo a trabalharem em conjunto, garantindo assim a aplicação dos parâmetros implementados pelo administrador de segurança para tratamento dos pacotes que trafegam pelas redes.

Um Firewall *stateful*, por outro lado, verifica o tráfego que entra e compara a uma política (que é actualmente muito similar ao formato de uma ACL) e cria um registo da conexão se o tráfego for permitido.

Os pacotes subsequentes que pertencem a esta conexão são permitidos automaticamente sem verificar novamente a regra criada, ou seja, a regra não é consultada de novo. Embora isto permita

conseguir relatórios e *logs* detalhados (por exemplo, um Firewall permite de forma fácil fornecer o acesso e arquivos de log baseado por conexão), também pode nos trazer certas desvantagens. Imagine este cenário: um ataque que consiste em emitir um grande número de pacotes do Internet Control Message Protocol (ICMP). A última coisa que você quer neste caso é encher a tabela de conexões do Firewall do perímetro, ou borda. Neste cenário destaca-se uma característica específica dos Firewalls:

Eles são *stateful*, mantêm o estado – o estado das conexões. Não é uma característica desejável manter o estado da conexão nestes casos, porque equipamentos *stateful* têm um limite de conexões simultâneas que podem lidar. Depois que a tabela de conexões estiverem cheia, o tráfego que chega de forma legítima é negada devido ao dano causado pelo ataque. Este ataque é conhecido como Negação de Serviço (DoS). Este é um ponto onde os Firewalls perdem quando comparados a dispositivos *stateless*, tais como os roteadores e switches processando ACLs. A escolha entre ACLs ou Firewalls nem sempre é necessária, na maioria dos casos um complementa o outro (NETO, 2004)

2.3 Regras de criação de uma ACL

Para (PADILLA, 2010) ACL são uma colecção de condições de permissão e negação, chamadas de regras, que fornecem segurança bloqueando usuários não autorizados e permitindo que usuários autorizados acessem recursos específicos. As ACLs podem bloquear qualquer tentativa injustificada de acessar os recursos da rede.

(PADILLA, 2010), As regras de uma ACL são criadas para permitir PERMIT ou para negar DENY o tráfego. Tudo o que não for permitido estará implicitamente negado (IMPLICIT DENY). Todas as listas de acesso precisam de, pelo menos, uma declaração de permissão. Caso contrário, todos os pacotes são negados e nenhum tráfego passa.

Para (FILIPPETTI, 2008, pág. 923) sublinhou que use o comando permit any any caso, queira permitir que todos os outros pacotes não sejam negados. O uso do comando permit any any tem efeito de evitar a negação de todos os outros pacotes por causa da declaração de negação implícita no final de uma lista de acesso. Não se deve fazer a primeira entrada na lista de acesso com o comando permit any, porque todo o tráfego irá passar e nenhum pacote atingirá a linha subsequente. Na verdade, uma vez que é especificado o comando permit any, todo o tráfego que ainda não tenha sido negado irá passar.

Embora todas as listas de acesso terminem com uma declaração de negação implícita, recomenda-se o uso de uma declaração de negação explícita (por exemplo, deny any any).

Crie a lista de acesso antes de aplicá-la a uma interface (ou em outro lugar), porque se se aplicar uma lista de acesso inexistente a uma interface e, em seguida, proceder à configuração da lista de acesso, a primeira instrução é implementada e a declaração de negação implícita que se segue poderia causar problemas de acesso imediato.

Outra razão para configurar uma lista de acesso antes de aplicá-la é porque uma interface com uma lista de acesso vazia aplicada a ela permite todo o tráfego.

2.3.1 Processo de ACL

Segundo (FILIPPETTI, 2008) O tráfego que entra no Router é comparado às entradas da ACL com base na ordem em que as entradas foram adicionadas no Router. Novas declarações são adicionadas ao final da lista. O Router continua a procurar até que encontre uma correspondência, se correspondências são forem encontradas até ao final da lista, o tráfego é negado. Por este motivo, é aconselhável que as entradas frequentemente atingidas estejam no topo da lista.

Uma ACL de entrada única com apenas uma entrada de negação tem o efeito de negar todo o tráfego, pois há uma negação implícita para o tráfego que não é permitido. Deve-se ter pelo menos uma declaração de permissão em uma ACL, caso contrário, todo o tráfego será bloqueado.

2.3.2 Máscara curinga (*Wildcard Mask*)

Segundo (SISCO, 1999) As mascaras curiga ou wildcard masks são muito utilizadas em configurações de listas de controlo de acesso e também em protocolos de roteamento como OSPF. Serve para aplicações onde as mascaras de sub-rede não são possíveis de se aplicar.

Uma coisa muito importante que deve ser lembrada quando queremos especificar um grupo de *hosts* em uma rede, ou uma rede inteira, são as máscaras curingas, ou *wildcard mask*, usadas pelas ACL. O conceito de máscara curinga é muito similares aqueles de máscara de sub-rede, com uma pequena mas muito significante diferença na lógica. Uma máscara de sub-rede é uma sequência de binário 1s e 0s que são utilizados para determinar qual parte de um endereço IP é associado com o endereço de rede. Com uma máscara de sub-rede, se um bit em particular em um endereço IP é parte de um endereço de rede, o correspondente bit na máscara de sub-rede é cedido para 1. Uma máscara curinga é muito similar, porém a lógica é inversa.

Um binário na máscara curinga significa “não se preocupe”. É o dígito binário 0 na máscara curinga que distingue os bits importantes, que devem ser comparados. Em outras palavras pegamos a máscara de sub-rede (em decimal), convertemos para binário e invertemos os 0s e 1s, depois convertemos de novo para decimal.

Uma rede classe 192.168.10.0/24, portanto tem a máscara de rede 255.255.255.0 (ou em binário 11111111.11111111.11111111.00000000). Para chegarmos à máscara curinga temos que inverter os 0’s e 1’s, dessa forma temos em binário – 00000000.00000000.00000000.11111111. Quando

convertido novamente em decimal temos: 0.0.0.255. Esta é a mascara curinga *(wildcard)* para rede 192.168.10.0/24.

Da mesma forma podemos obter a máscara curinga para um determinado grupo *(range)* de host, e não somente para uma rede inteira. Por exemplo, para sub-rede 172.16.10.4/30. Serão testados os endereços 172.16.10.4 até 172.16.10.7.

Tabela1: Ilustração de Wildcard Mask

Endereço da sub-rede	Máscara de sub-rede	Mascara curing	
Decimal	172.16.10.4/30	255.255.255.252	0.0.0.3
Decimal	192.168.100.8/29	255.255.255.248	0.0.0.7
Decimal	192.168.0.0/24	255.255.255.0	0.0.0.255

Fonte: Autoria própria, 2022

Suponha que você queira permitir o acesso de qualquer pacote que se origine na sub-rede 192.168.0.100 com máscara 255.255.255.240. Para encontrar a máscara curinga para esta máscara de sub-rede 255.255.255.240 basta fazer o seguinte:

- ✓ Onde na máscara se lê “255”, escreva “0”
- ✓ Onde na máscara se lê “0”, escreva “255”

2.3.3 Port-Security

De acordo com (CHRISTOPHER e MARCELO) O port-security é uma tecnologia que aumenta a robustez da rede utilizando a infra-estrutura já existente no ambiente sem a necessidade da compra de qualquer dispositivo adicional.

Essa tecnologia permite um controle mais rígido dos dispositivos que se conectam a sua rede, devido ao fato de somente permitir endereços físicos (endereços MAC) devidamente cadastrados no switch (que neste caso, realiza o papel de autenticador).

O port-security possui as seguintes características:

Descarta todo fluxo de dados até que o dispositivo transmissor tenha seu endereço físico (MAC) validado na interface onde o port-security está habilitado.

Para que o equipamento (*switch*) possa aplicar a segurança de portas provida pela tecnologia, necessitamos configurar os endereços físicos que podem autenticar- se na interface em questão.

E podemos realizar isto de duas maneiras:

- ❖ **Manualmente** - Um método que permite uma maior confiabilidade nos endereços. Cadastrados no switch, uma vez que para adicionar novos endereços seria necessário a intervenção do administrador de rede.
- ❖ **Automático** - Alternativamente, pode configurar a segurança das portas utilizando o processo chamado “sticky learning” no qual o switch verifica o endereço físico de todos os equipamentos conectados às respectivas portas do equipamento no momento da sua configuração. Ao utilizar este método deve atentar-se ao fato de que somente computadores “confiáveis” deverão

estar conectados ao switch no momento da configuração deste serviço automático. Ao configurarmos a segurança de portas, devemos atentar ao fato de que esse serviço só pode ser habilitado em portas de acesso, e devemos alterar o modo da interface que irá receber este serviço para que a mesma fique no modo correcto.

2.3.4 Configuração de Port-Security

O objectivo do Port-Security é impedir que hosts não autorizados acessem a rede, restringindo a porta a um número máximo de endereços MAC

Caso haja uma violação da regra uma acção é tomada conforme configuração. Existem três tipos de configuração:

- Endereços MAC seguros estáticos (Static): Configurados manualmente usando o comando Switchport de segurança, dentro da configuração de interface e armazenados na tabela de endereços
- Endereços MAC seguros dinâmicos (Dynamic): Estes são configurados dinamicamente, armazenados apenas na tabela de endereços na RAM, e removidos na reinicialização do Switch.
- Endereços MAC seguros fixos (Sticky): Podem ser aprendidos dinamicamente ou configurados manualmente, são armazenados na tabela de endereços. Se os endereços estão salvos na NVRAM, quando o Switch é rebotado, a interface não tem necessidade de ser reconfigurada dinamicamente, mas para isso você deve especificar o MAC.

Para o (MARCELO, 2008) Existem três regras para o caso de violação: Protect, Restrict e Shutdown.

- **Protect (Proteger):** Quando o número de endereços MAC seguros atinge o limite permitido na porta, pacotes com endereços de origem desconhecidos são ignorados até que você remova um número suficiente de endereços MAC seguros ou aumente o número máximo de endereços permitidos. Você não é notificado de que houve uma violação de segurança
- **Restrict (Restringir):** Quando o número de endereços MAC seguros atinge o limite permitido na porta, pacotes com endereços de origem desconhecidos são ignorados até que você remova um número suficiente de endereços MAC seguros ou aumente o número máximo de endereços permitidos. Nesse modo, você é notificado de que houve uma violação de segurança. Especificamente, um Trap SNMP é enviado, uma mensagem Syslog é registada em log e o contador de violação é incrementado.
- **Shutdown (Desligado):** Nesse modo, uma violação de segurança de porta faz com que a interface seja desabilitada para erro imediatamente e apaga o LED da porta. Ele também envia um Trap para o SNMP, registra em log uma mensagem syslog e incrementa o contador de violação. Quando uma porta segura estiver no estado desabilitado para o erro, será possível tira-la desse estado digitando-se os comandos de configuração da interface Shutdown e No Shutdown. Este é o modo padrão.

2.3.5 VLAN – Redes Locais Virtuais

Uma das tecnologias que contribuem com a excelência do desempenho da rede é a separação dos grandes domínios de broadcast em domínios menores com VLANs, limitando assim o número de dispositivos que participam de broadcast (CISCO, 2015).

Para (TANENBAUM 2011) as VLANs permitem que a topologia física seja dividida em diferentes topologias lógicas.

Segundo (KUROSE E ROSS 2010), a utilização de VLANs auxilia na solução das seguintes dificuldades:

• Falta de isolamento do tráfego: o tráfego broadcast percorre toda a rede, limitar o escopo desse tráfego de broadcast aprimoraria o desempenho da LAN. A limitação do tráfego de broadcast também é importante por razões de segurança e privacidade, evitando que um grupo de funcionários, por exemplo, analise o tráfego do grupo de gerência.

• Uso ineficiente de comutadores: se uma instituição tivesse 10 grupos, seriam necessários 10 comutadores. Se cada grupo fosse com menos de 10 pessoas, um único comutador de 96 pontos seria suficiente para atender a todos, mas esse comutador não fornece isolamento de tráfego.

• Gerenciamento de usuários: se um funcionário se locomove entre os grupos o cabeamento físico deve ser mudado para conectar o funcionário a um comutador diferente.

Para (CISCO 2015) os principais benefícios de usar VLANs são:

• Segurança – Grupos que tem dados confidenciais são separados do restante da rede, diminuindo as chances de acesso sem permissão a informações confidenciais.

• Redução de custo – Menor necessidade das actualizações de rede e uso mais eficiente da largura de banda.

• Melhor desempenho – Dividir a rede em vários grupos de trabalhos lógicos reduz tráfego desnecessário na rede e aumenta o desempenho.

• Atenuação da tempestade de broadcast – Dividir a rede em VLANs diminui o número de dispositivos que podem participar de uma situação de descontrole por excesso de broadcast.

• Maior eficiência do pessoal de TI (Tecnologia e Informação) – VLANs simplifica o gerenciamento da rede, além da facilidade de identificar a função de uma VLAN, dando a ela um nome apropriado, “Financeiro”, por exemplo.

• Projecto mais simples ou gerenciamento de aplicativo – Simplifica o gerenciamento de um projecto ou trabalho com um aplicativo especializado.

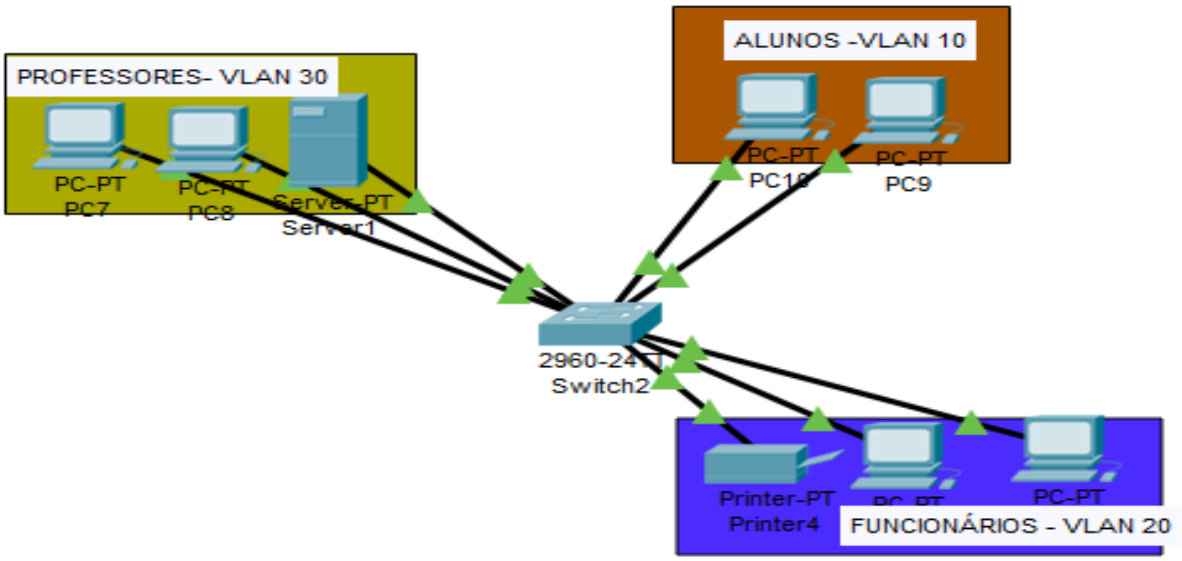

Figura3: Ilustração de VLAN

Fonte: Autoria Própria, 2022

2.3.6 VTP (VLAN Trunking Protocol)

De acordo com (TANENBAUM, 2003, Pág.108), Para manter a conectividade das VLANs em todas a estrutura de swich, as VLANs deve ser configurada em cada Switch. O protocolo VTP (VLAN Trunking Protocol) da CISCO garante um método mais fácil para manutenção de uma configuração de VLAN consistente em toda a rede comutada.

Usado para distribuir e sincronizar informações de identificação das Vlans configuradas em toda a rede comutada. As configurações estabelecidas em um único servidor VTP são propagadas através do enlace tronco para todos os switches conectados na rede.

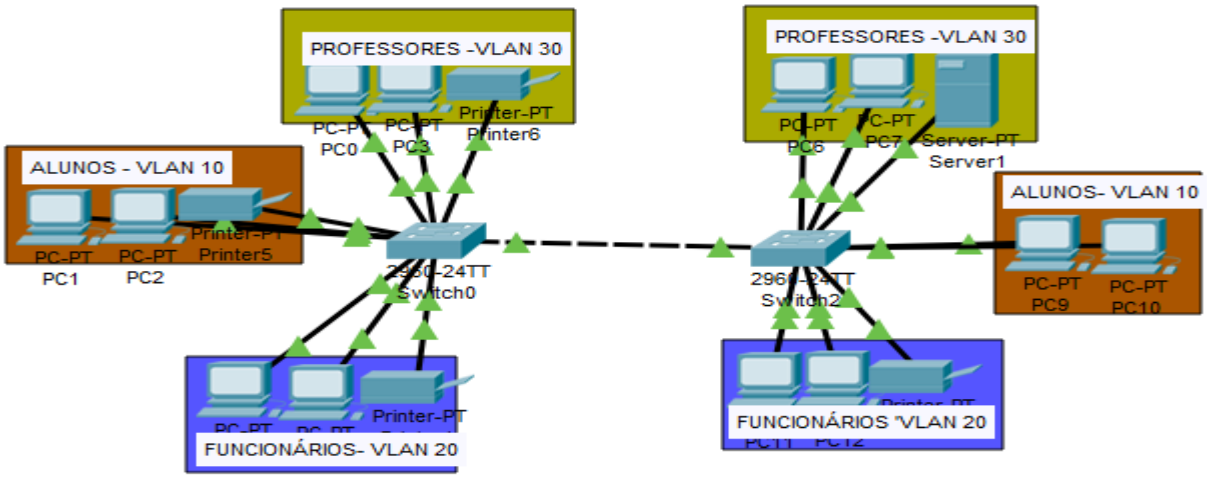

Figura4: Ilustração de VTP (VLAN Trunking Protocol)

Fonte: Autoria Própria,2022

2.3.7 Roteadores

Segundo (DOYLE, 1997), Roteadores são equipamentos utilizados para ligar redes distintas mesmo sendo de arquitecturas diferentes, operando na camada de rede (camada três do modelo OSI).

Capazes de ler os pacotes de dados, a cessar as informações ali presentes, incluindo o endereço IP de origem e destino.

2.3.8 Funções de Router

O mesmo (DOYLE, 1997, pág. 95), sublinhou que Roteadores possuem duas funções básicas: permitir a conexão de duas redes distintas e escolher um caminho a ser usado para o data grama chegar até o seu destino.

2.3.9 Encaminhamento de pacotes

Para (HUBERT, 2001), Os Routers usam as tabelas de roteamento para determinar para onde encaminhar pacotes. Cada linha da tabela de roteamento indica qual interface de rede é usada para encaminhar um pacote. O endereço IP do destino no pacote define o destino do pacote.

Os Routers usam a sua própria tabela de roteamento e comparam as entradas com o endereço IP de destino do pacote. O resultado é a decisão de qual interface de saída será usada para enviar o pacote. Se o Router não tiver uma entrada correspondente na sua tabela de roteamento, o pacote é descartado.

Um Router deve ser capaz de determinar que protocolo de roteamento deve usar se tiver duas rotas idênticas de dois protocolos de roteamento diferentes para uma rede. Esta determinação é feita com base num recurso chamada distância administrativa.

2.4 Roteamento Inter-VLAN

Segundo (DOOLEY, 2006), Computadores em VLANs diferentes são, por defeito, incapazes de se comunicar. A forma de permitir que esses computadores se comuniquem é usar uma solução chamada roteamento inter-VLAN (Router on a Stick). O roteamento inter-VLAN ocorre entre domínios de *broadcast* diferentes com recurso a um dispositivo da camada 3.

2.4.1 Router-on-a-Stick

Para (DOOLEY, 2006), Alguns *software* de Routers permitem a configuração de interfaces de Routers como *link* trunk fazendo com que um única interface física roteie tráfego entre múltiplas VLANs na rede. A configuração ente um Router e um Switch *core* é as vezes referida como um *router on a stick*. Para executar funções de roteamento inter-VLAN, o Router deve saber como alcançar todas VLANs que estão sendo interconectadas. No Router devem haver conexões lógicas separadas para cada VLAN, e entroncamento VLAN (tal como o IEEE 802.1Q) deve ser habilitado nestas conexões.

O Router então envia um tráfego de VLAN roteado que é etiquetado para a VLAN de destino fora da mesma interface física. Estas subinterfaces são configuradas no *software* e cada uma é configurada de forma independente com o seu próprio endereço IP e uma é atribuída a um VLAN específica.

As subinterfaces são configuradas para diferentes sub-redes correspondentes as VLANs a elas atribuídas para facilitar o roteamento lógico antes que os *frames* de dados sejam etiquetados por VLANs e enviados de volta para a interface física.

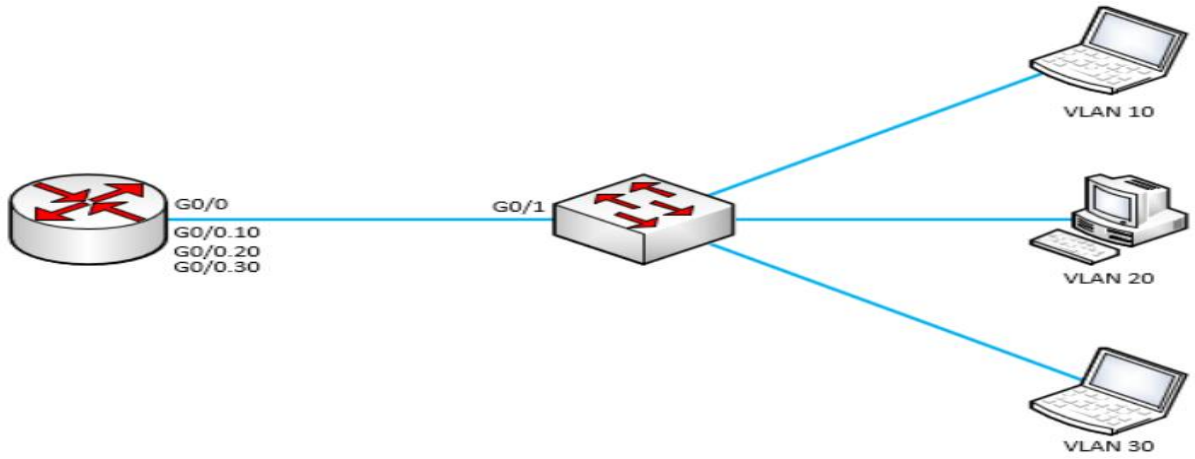

Figura5: Ilustação de de Router on a Stick
Fonte: CISCO, 2010

2.4.2 Protocolos de roteamento dinâmicos

Segundo (SISCO, 2010), Roteamento é o processo de determinação do caminho para onde enviar pacotes de dados que são destinados para endereços fora da rede local.

Os Routers podem usar protocolos de roteamento dinâmicos para criar e manter a tabela de roteamento dinamicamente, acomodando assim as mudanças na rede, onde quer que elas ocorram. Protocolos de roteamento dinâmicos são conjuntos de processos, algoritmos, e mensagens que são usados para compartilhar informações de roteamento.

Esses protocolos definem as regras que um Router usa quando está a comunicar-se com um Router vizinho para determinar caminhos para redes remotas e manter estas redes na sua tabela de roteamento.

2.4.3 Protocolo de roteamento RIP

Segundo a (HUBERT, 2001, pág. 78), RIP *(Routing Information Protocol*) é um protocolo de roteamento, baseado no algoritmo Vector-Distância, projectado para ser usado como um *Interior Gate Protocol* em redes de tamanho moderado com diâmetro máximo de 15 saltos.

2.4.4 Características básicas de protocolo RIP

- ✓ Projectado como um protocolo intra-domínio (IGP).
- ✓ Utiliza um algoritmo do tipo Vector de Distância (Bellman-Ford)
- ✓ A métrica utilizada é a distância da origem até o destino em número de enlaces que devem ser percorridos.
- ✓ Não permite o balanceamento do tráfego.
- ✓ A rota inatingível apresenta uma métrica igual a 16.
- ✓ Realiza actualizações a cada 30 segundos.

2.4.5 Protocolo de roteamento OSPF IPv4

De acordo com (HUBERT, 2001), OSPF (*Open Shortest Path First*) é um protocolo de roteamento *link-state* que é geralmente usado em redes devido à escalabilidade, convergência rápida, e suporte a ambientes com dispositivos de diferentes fabricantes. Este protocolo é um IGP que foi desenvolvido pela IETF. Por ser padronizado, este protocolo é amplamente implementado, o que torna essencial o conhecimento da sua configuração e manutenção.

2.4.6 Vantagens de Protocolo OSPF

Por ser um protocolo de roteamento *link-state*, o OSPF possui as seguintes vantagens em relação aos protocolos de roteamento Vector Distância:

•Maior escalabilidade – protocolos *link-state* usam uma estrutura hierárquica e podem escalar para redes muito grandes, se correctamente projectados.

•Visão geral da topologia – porque cada Router contém informação total acerca de todos os Routers e *links* na rede, cada Router é capaz de seleccionar independentemente um caminho eficiente e livre de *loops*, baseando-se no custo para alcançar todos os vizinhos na rede.

•Actualizações sempre que há mudanças na topologia e actualizações periódicas – protocolos link-state enviam actualizações da topologia mudada.

Por usar actualizações etiquetadas, é preservada largura de banda.

Adicionalmente, actualizações são feitas periodicamente, por defeito a cada 30 minutos.

Resposta rápida a mudanças na topologia **–protocolos** *link-state* estabelece relações de vizinhança com Routers adjacentes. A falha de um vizinho é detectada rapidamente, e esta falha é comunicada usando actualizações etiquetadas para todos os Routers da rede. Este reporte imediato geralmente conduz para um tempo de convergência rápido.

Maior volume de informação transmitida entre Routers–Routers que usam um protocolo link-state tem uma visão comum da rede. Isto significa que cada Router tem toda informação acerca de outros Routers e *links* entre eles, incluindo a métrica em cada *link*.

2.4.7 Adjacências OSPF

Segundo **(**HUBERT, 2001), Os Routers vizinhos OSPF devem reconhecer um ao outro na rede antes de partilharem informações porque o roteamento OSPF depende do estado do *link* entre dois Routers. Os Routers reconhecem um ao outro usando o protocolo *Hello.* Para fazer esse reconhecimento, determinando se há algum vizinho ligado ao *link*, pacotes *hello* são enviados em todas interfaces OSPF habilitadas.

2.4.8 Estrutura de área OSPF

O mesmo **(**HUBERT, 2006), ressaltou que protocolos de roteamento *Link-state* usam uma hierarquia de duas camadas:

❖ Área *Backbone* ou área de trânsito: Áreas *backbone* interconectam áreas OSPF diferentes. A estrutura hierárquica das áreas OSPF exige que todas as áreas estejam directamente conectadas a uma área *backbone*.

❖ Área normal ou área não-*backbone*: Áreas normais são normalmente configuradas de acordo com o agrupamento funcional ou geográfico. Por padrão, áreas normais não permitem que tráfego de uma determinada área use os seus *links* para alcançar uma outra área. Todo o tráfego de outras áreas deve atravessar uma área de trânsito.

2.4.9 Adjacências OSPF

Segundo (HUBERT, 2006), Os Routers vizinhos OSPF devem reconhecer um ao outro na rede antes de partilharem informações porque o roteamento OSPF depende do estado do *link* entre dois Routers. Os Routers reconhecem um ao outro usando o protocolo *Hello.* Para fazer esse reconhecimento, determinando se há algum vizinho ligado ao *link*, pacotes *hello* são enviados em todas interfaces OSPF habilitadas.

2.5 Estrutura de área OSPF

(HUBERT, 2006) sublinhou que Protocolos de roteamento *Link-state* usam uma hierarquia de duas camadas:

• Área *Backbone* ou área de trânsito: áreas *backbone* interconectam áreas OSPF diferentes.

A estrutura hierárquica das áreas OSPF exige que todas as áreas estejam directamente conectadas a uma área *backbone*.

• Área normal ou área não-*backbone*: áreas normais são normalmente configuradas de acordo com o agrupamento funcional ou geográfico. Por padrão, áreas normais não permitem que tráfego de uma determinada área use os seus *links* para alcançar uma outra área. Todo o tráfego de outras áreas deve atravessar uma área de trânsito.

2.5.1 Protocolo de roteamento EIGRP

Segundo (NGUYEN, 2013), define que, EIGRP (*Enhanced Interior Gateway Routing Protocol*) é um protocolo de roteamento baseado no algoritmo vector distância avançado que foi desenvolvido pela Cisco. Este protocolo de roteamento é aplicável em diferentes topologias. Numa rede bem projectada, o EIGRP é escalável e provê tempo convergência rápida com um mínimo de sobrecarga. Por todas vantagens que a ele são agregadas, o EIGRP é uma escolha bastante popular quando se trata de um protocolo de roteamento em dispositivos Cisco.

2.5.2 Recursos do EIGRP

Para (NGUYEN, 2013) EIGRP é um protocolo de roteamento que combina as vantagens dos protocolos *linkstate* e vector distância. Esta combinação permite-lhe possuir os seguintes recursos:

•Convergência Rápida: o EIGRP usa DUAL (*Diffusing Update Algorithm*) para activar convergência rápida. O DUAL reside no centro do protocolo de roteamento**,** garantindo assim caminhos livre de *loops* e caminhos de *backup* ao longo do domínio de roteamento.

Um Router que usa EIGRP guarda todas as rotas de *backup* disponíveis, e assim sendo, pode adaptar-se rapidamente para rotas alternativas. Se a rota primária na tabela de roteamento falha, a melhor rota de *backup* é imediatamente adicionada a tabela de roteamento. Se não existir nenhuma rota apropriada ou rota de *backup* na tabela de roteamento local, o EIGRP consulta os seus vizinhos para descobrir uma rota alternativa.

• Balanceamento de carga: o EIGRP suporta melhor a métrica de balanceamento de carga desigual do que a métrica de balanceamento de carga igual. Isto permite distribuir melhor o controlo de tráfego nas suas redes.

• Roteamento *classless* e livre de *loops*: porque o EIGRP é um protocolo de roteamento *classless*, ele anuncia uma máscara de roteamento para cada rede de destino.

2.5.3 Selecção de caminho EIGRP

Cada Router EIGRP mantém uma tabela de vizinhos. Esta tabela inclui uma lista de Routers EIGRP directamente conectados que têm uma adjacência com o Router em questão. Relacionamentos de vizinhança são usados para rastrear o estado desses vizinhos. O EIGRP usa um protocolo de peso leve *Hello* para monitorar o estado de conexão com seus vizinhos.

Cada Router EIGRP mantém também uma tabela de topologia para cada configuração do protocolo roteado. A tabela de topologia inclui entrada de rotas para todos destinos que o Router aprende a partir dos seus vizinhos EIGRP directamente conectados.

O EIGRP escolhe as melhores rotas para um destino a partir da tabela de topologia e coloca essas rotas na sua tabela de roteamento. Essa escolha é feita com base na métrica mais baixa. Depois de escolher a melhor rota, o Router escolhe a rota de *backup*.

2.5.4 DHCP- (Dynamic Host Configuration Protocol)

O DHCP surgiu da necessidade de atribuição de endereços IP a grandes redes, o seu antecessor (Bootstrap Protocol) fazia com que fosse necessária a configuração manual das tabelas de mapeamento. Com o avanço para o DHCP esta dificuldade foi sanada pois ele trabalha com atribuição manual e automática. Quando um equipamento é adicionado à rede, a ele é atribuído um endereço IP (TANEMBAUM, 2011).

Se um host deixar a rede e não retornar seu endereço IP ao servidor DHCP, esse endereço será permanentemente perdido. Depois de um certo período, muitos endereços poderão se perder. Para evitar que isso aconteça, a atribuição de endereços IP pode se referir a um período fixo, uma técnica chamada arrendamento (leasing). Pouco antes de expirar o prazo de arrendamento, o host deve solicitar ao DHCP uma renovação. Se ele deixar de fazer uma solicitação ou se a solicitação for negada, o host não poderá mais usar o endereço IP que recebeu antes (TANEMBAUM, 2011).

2.5.5 Sub-redes de uma rede

(TANEMBAUM, 1996) disse, Sub-redes de uma rede significa usar a máscara de sub-rede para dividir a rede e quebrar uma grande rede em segmentos menores, mais eficientes e gerenciáveis, ou sub-redes.

Com sub-redes, a rede não está limitado ao padrão de classe A, B, C ou máscaras de rede e não há mais flexibilidade na concepção da rede.

Endereços de sub-rede incluem a parte da rede, além de um campo de sub-rede e um campo de host. A capacidade de decidir como dividir a parte do host original para o novo campo de acolhimento de sub-rede e fornece flexibilidade para abordar o administrador da rede (TANENBAUM, 2003).

2.5.6 Vantagens de Sub-Redes

O mesmo (TANEMBAUM, 1996), Uma das vantagens de criar sub-redes de uma rede é simplificar a administração. Normalmente, uma organização possui departamentos diferentes que exigem acesso a diferentes tipos de recursos. Se os departamentos de contabilidade e limpeza estiverem na mesma sub-rede, por exemplo, as restrições de acesso deverão ser controladas nó a nó. Mas quando os dois departamentos são colocados em sub-redes separadas, as opções de segurança podem ser aplicadas com base nessas sub-redes.

2.5.7 Protocolo ICMP – Internet Control Message Protocol

O Protocolo ICMP, cuja sigla significa “Protocolo de Controle de Mensagens da Internet”, é um protocolo que comunica mensagens de erro e outras condições que requeiram atenção em uma rede. O protocolo IP, que fornece o mecanismo para entrega de data gramas entre dispositivos, carece dessa funcionalidade, e por isso o ICMP foi criado, sendo um protocolo extremamente importante por conta dessas capacidades. Geralmente as mensagens ICMP são tratadas na camada de Internet (IP) ou então na camada de Transporte (TCP ou UDP) **(**TORRES, 2001)**.**

2.6 Classes de Mensagens ICMP

As mensagens ICMP podem ser divididas em duas grandes classes:

- Mensagens de Erro: Usadas para informar a um dispositivo transmissor que um erro ocorreu durante a transmissão do datagrama. Geralmente os erros são relacionados à estrutura do datagrama em si, ou problemas encontrados durante o tráfego dos pacotes através da rede.
- Mensagens de Informação (Consultas / Query): São mensagens que permitem aos dispositivos trocarem informações entre si e realizarem determinados tipos de testes e diagnósticos.

2.6.1 Protocolo TCP (Protocolo de controlo de transmissão)

Segundo (TORRES,2001,pag.101), O Protocolo TCP, que pertence à camada de Transporte juntamente com o UDP, fornece um serviço de entrega de pacotes confiável e orientado a conexão.

2.6.2 Protocolo UDP (User Datagram Protocol)

Para (TORRES, 2001, pág.107**)** O Protocolo UDP, que pertence à camada de transporte juntamente com o protocolo TCP, é um protocolo simples, orientado a data grama. Ele não fornece confiabilidade na transmissão, pois envia os data gramas requisitados pela aplicação sem nenhuma garanta de que eles chegarão ao seu destino.

O protocolo UDP é o protocolo orientado a data gramas. Isso ocorre porque não há sobrecarga para abrir, manter e encerrar uma conexão. O UDP é eficiente para o tipo de transmissão de rede de broadcast e multicast.

2.6.3 Packet Tracer

Segundo (STALLINGS, 2005), É um simulador de redes de computadores criado pela empresa Cisco Systems Inc, com a finalidade de preparar profissionais de informática para projectar, configurar e solucionar problemas de redes e o uso dos equipamentos desenvolvidos pela empresa dentro do Networking Academy, Cisco no programa de desenvolvimento de habilidades em redes.

O software Packet Tracer foi desenvolvido por uma das maiores empresas de equipamentos de infra-estrutura do mundo, a CISCO SYSTEM. Tem como finalidade criar e simular comportamentos reais em ambientes de rede LANs e WANs, permitindo realizar diversas situações de roteamentos, VLANs, desde layouts de redes simples até complexas.

É uma ferramenta de simulação de configuração de rede inovadora utilizada para o ensino, jogos e avaliação. Packet Tracer incentiva os alunos a explorar todas as suas perguntas," (CISCO, 2015). Além de ser gratuito, o software conta com um ambiente gráfico de fácil configuração e elaboração de layout. Com a possibilidade de simulação, criação e avaliação de diversos conceitos extremamente complexos de tecnologia de redes e telecomunicações.

De acordo com (SHEIKH, 2014), O simulador oferece um ambiente totalmente visual, com animações gratuitas que modelam cenários complexos, sem a necessidade de equipamentos físicos. Trata-se de um simulador com a finalidade de ensino e a aprendizagem, é fácil de trabalhar e faz com que o usuário ganhe mais confiança no ambiente de trabalho.

O programa possibilita ao estudante de redes:

A visualização do ambiente de rede para a criação, configuração e solução de problemas;

A criação e visualização da transmissão de pacotes virtuais através da rede criada em tempo real desenvolver habilidades para solução de problemas potenciais criar e configurar complexas topologias de redes que estão muito além aos seus equipamentos disponíveis encoraja o estudante a desafiar seus conhecimentos em uma grande variedade de protocolos.

3 Capítulo III- Apresentação e discussão de Resultados

3.1 Acesso a Rede Actual

A Rede de dados da Águas da Região de Maputo foi criada em 2009, com o propósito de partilhar recursos da rede e troca de informações.

Com o crescimento constante da Rede da Águas de região de Maputo (AdeM), faz com que mais dispositivos sejam conectados na rede, causando crescimento desordenado da infra-estrutura dos activos e passivos de rede.

Actualmente a Rede da Águas da Região de Maputo regista maior número de usuários que acessam a internet e serviços de impressão, e por este facto registam maior tráfego na rede que afecta negativamente o desempenho da rede e de várias tarefas da instituição.

O acesso a Recursos da rede é através de senhas que permite também o acesso ao servidor FTP e outros equipamentos protegidos da Rede, e muitos funcionários da Águas de Região de Maputo tem acesso a senha, mesmos sendo secreta.

O uso de Senhas não resolve os problemas de Cibe criminosos, porque os criminosos aprimoram as suas técnicas constantemente para garantir invasões bem-sucedidas e gerar receita e lucro consistentes.

O acesso através da senha acontece para todos os equipamentos da rede, até agora acesso através da senha e um dos mecanismos que funciona somente na Águas da Região de Maputo, e criptografia de senhas deve ser acompanhadas através de outros mecanismos de seguranças em Redes como Listas de \Controle de Acesso (ACLs).

Toda essa forma de acesso da rede mencionada acima não oferece segurança interna e nem externa da rede, quaisquer funcionários daquela instituição que usar uma engenharia social pode ter acesso aos recursos protegidos da Rede.

Actualmente quem tem acesso a recursos protegidos da Rede são os administradores e técnicos da rede. Porque nem todo usuário deve ter acesso à rede. Para impedir possíveis invasores, Os técnicos de informática de Águas da Região de Maputo precisam reconhecer cada usuário e cada dispositivo. Em seguida, aplicar as listas de controle de Acesso (ACLs). Para poder bloquear endereço ip dos funcionários não autorizados ou conceder a eles apenas acesso limitado. Esse processo é um controle de acesso à rede (ACLs).

3.2 Diagnóstico de estado da Rede Actual

Na fase prévia de diagnóstico da rede existente, foram identificados algumas falhas. As falhas encontradas são enumeradas a seguir:

1- Sobrecarga de dispositivos (Servidores WEB, FTP e Impressoras) da rede com maior fluxo de dados e não há mecanismos de redução de tráfego através de filtragens de pacotes.

2- Falta de políticas de prioridade de trafego: O tráfego de dados na rede deve ser priorizando de acordo com as suas necessidades. Em alguns casos, o congestionamento pode ser reduzido, priorizando as necessidades de tráfego de redes de acordo com os usuários da rede das águas da região de Maputo da rede.

3- Excesso de tráfego para Internet (Servidor Web): Há ainda outras causas, como grandes *downloads* de filmes, vídeos e músicas feitos pelos funcionários que diminui a largura de banda na rede, o que pode causar indisponibilidade ou lentidão para alguns usuários.

4-Falta de segurança de roteador: Actualmente os administradores da rede de AdeM não conseguem controlar os pacotes que entra e sai do roteador.

5- Dificuldade para controlar o tráfego: Actualmente os administradores da rede têm dificuldade de controlar o tráfego de dados que flui na rede devido aumento de números de usuários na rede.

6-Falta de links de redundâncias nos departamentos de Recursos Humanos (RH) e departamentos de contabilidade, para reduzir constante desconexão e falta de comunicação com outros departamentos.

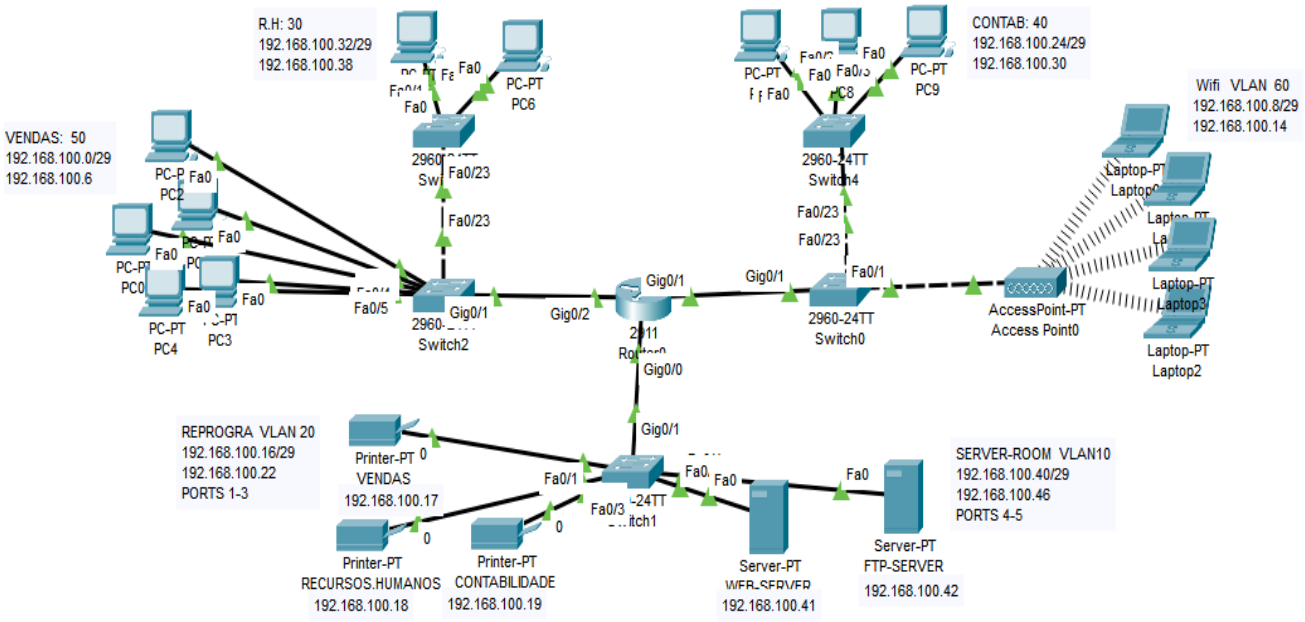

Figura 6: Topologia da Rede Actual sem Listas
Fonte: Autoria própria, 2022.

3.2.1 Os departamentos Identificados para implementar Listas de controle de Acesso (ACLs)

A empresa Águas da Região de Maputo (AdeM), assume a responsabilidade de prestação de serviços de captação, tratamento, transporte e distribuição de água na região metropolitana de Maputo, isto é, na cidade de Maputo, cidade da Matola e Vila de Boane.

O caso em estudo são três (3) departamentos que funcionam no mesmo compartimento, que são os seguintes: departamentos de Vendas, RH e Contabilidade. Departamento de Vendas localiza-se no rés-do-chão que funciona para pagamentos de facturas e assinatura de contratos, o sector de vendas ocupa posição de destaque para o sucesso da empresa.

Departamentos de RH localizados no rés-do-chão, que trata questões de gerenciamento de recursos humanos.

Departamento de contabilidades localiza-se no mesmo piso de Vendas e RH, que trata de questões de contas da empresa das águas da região de Maputo.

O facto de todos os departamentos funcionar no mesmo piso a partilha de recursos não e organizado.

3.2.2 Proposta de implementação de Listas de controle de Acesso (ACLs)

Depois de efectuar os diagnósticos da rede existente na Águas da região de Maputo e identificar os departamentos para implementar as politicas de controle de ACLs.

Agora é a fase de implementação de listas de controle de acesso para solucionar os problemas nos departamentos identificados para optimizar o tráfego e serviços de impressão e acesso a internet de forma segura sem criar loops na rede. Depois da implementação de listas de controle de Acesso (ACLs):

1- Apenas os computadores dos chefes de departamentos (computadores simbolizados por um circulo em volta), devem poder enviar pacotes para qualquer impressora na rede, devendo os demais computadores poder enviar pacotes apenas para as impressoras dos seus respectivos departamentos.

2- O acesso a Internet, através do *Web-Server* localizado na *ServerRoom*, deve ser permitido apenas para os chefes de departamento (computadores simbolizados por um circulo em volta).

3- Para os visitantes (wifi), todos os visitantes que chegar na empresa terá acesso a internet a partir do servidor Web localizado na *ServerRoom.*

Com estas políticas de segurança a empresa pode reduzir o custo de manutenção da rede e melhorar o tráfego de dados dentro da rede.

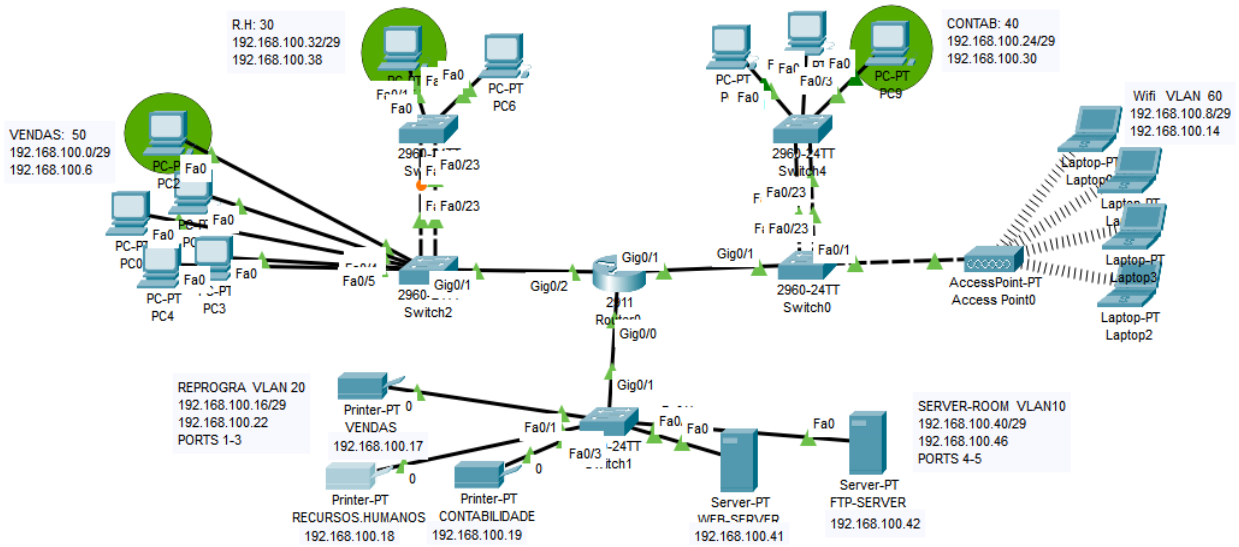

Figura7: Topologia da rede proposta com Listas.
Fonte**:** Autoria Própria,2022.

3.2.3 Comandos de configuração da Topologia Proposta

Para o bom funcionamento da nova topologia da rede proposta foram executados os seguintes comandos:

A figura abaixo ilustra os comandos de configuração de DHCP Pool para o departamento de Vendas, isto é, estou atribuir todos computadores de vendas com ip dinâmico para evitar perdas de endereço IP.

```
Router(config)#
Router(config)#ip DHCP pool Vendas
Router(dhcp-config)#ne
Router(dhcp-config)#network 192.168.100.0 255.255.255.248
Router(dhcp-config)#de
Router(dhcp-config)#default-router 192.168.100.6
Router(dhcp-config)#exit
Router(config)#
```

Figura 8: Comandos de configuração de DHCP para Vendas

Fonte: Fonte**:** Autoria Própria,2022.

A figura abaixo ilustra os comandos de configuração de DHCP Pool para todos computadores do departamento de Recursos Humanos (RH), isto é, estou atribuir os computadores com ip dinâmico para evitar perdas de IP.

```
Router(config)#ip DHCP pool RH
Router(dhcp-config)#network 192.168.100.32 255.255.255.248
Router(dhcp-config)#default-router 192.168.100.38
Router(dhcp-config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figura 9: Comando de configuração de DHCP para RH

Fonte: Fonte**:** Autoria Própria,2022.

A figura abaixo ilustra os comandos de configuração de DHCP Pool para todos computadores do departamento da Rede Externa (WiFi), isto é, estou atribuir os computadores com ip dinâmico para evitar perdas de endereço IP.

Router>enable

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip DHCP pool WIFI
Router(dhcp-config)#network 192.168.100.8 255.255.255.248
Router(dhcp-config)#default-router 192.168.100.14
Router(dhcp-config)#EXIT
Router(config)#EXIT
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figura10: Comandos de configuração de DHCP para Rede Externa

Fonte: Fonte**:** Autoria Própria,2022.

A Figura abaixo ilustra a configuração de DHCP Pool para todos computadores do departamento de Contabilidades, isto é, estou atribuir os computadores com ip dinâmico para evitar perdas de endereço IP.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip DHCP pool CONTABILIDADE
Router(dhcp-config)#network 192.168.100.24 255.255.255.248
Router(dhcp-config)#default-router 192.168.100.30
Router(dhcp-config)#EXIT
Router(config)#EXIT
```

Figura11: Comando de configuração de DHCP para Contabilidade

Fonte: Fonte**:** Autoria Própria,2022.

A figura abaixo ilustra o comando de configuração de listas de controle de acesso (ACLs), onde cada departamento imprime na sua própria impressora, isto, é, todos os elementos do departamentos de vendas com a rede 192.168.100.0/29 imprime na impressora do departamento venda com ip 192.168.100.17. A rede de RH com ip rede 192.168.100.32/29 imprime na sua própria impressora com ip 192.168.100.18, e todos os elementos do departamentos de contabilidade com a rede 192.168.100.24/29 imprime na sua própria impressora com ip 192.168.100.19 respectivamente.

Com excepção dos chefes de cada departamentos onde o ip 192.168.100.1 identifica ip do computador do chefe de vendas, 192.168.100.33 identifica computador do chefe de RH e ip 192.168.100.25 identifica o ip do computador do chefe de contabilidades respectivamente acessando qualquer impressora que esta na rede 192.168.100.16/29 localizada no reprografia.

```
Router(config)#
Router(config)#access-list 100 permit ip host 192.168.100.1 192.168.100.16 0.0.0.7
Router(config)#access-list 100 permit ip host 192.168.100.33 192.168.100.16 0.0.0.7
Router(config)#access-list 100 permit ip host 192.168.100.25 192.168.100.16 0.0.0.7
Router(config)#acc
Router(config)#access-list 100 permit ip 192.168.100.0 0.0.0.7 host 192.168.100.17
Router(config)#access-list 100 permit ip 192.168.100.32 0.0.0.7 host 192.168.100.18
Router(config)#access-list 100 permit ip 192.168.100.24 0.0.0.7 host 192.168.100.19
Router(config)#acc
Router(config)#access-list 100 den
Router(config)#access-list 100 deny ip an
Router(config)#access-list 100 deny ip any an
Router(config)#access-list 100 deny ip any any
Router(config)#int
Router(config)#interface gi
Router(config)#interface gigabitEthernet 0/0.20
Router(config-subif)#ip acc
Router(config-subif)#ip access-group 100 out
Router(config-subif)#exit
Router(config)#exit
```

Figura12: Comando de configuração de Listas para acesso a impressora

Fonte: Fonte**:** Autoria Própria,2022.

A figura abaixo ilustra os comandos de configuração de Listas de controle de Acesso (ACLs), aplicando politicas de controle de acesso ao Servidor FTP, O chefe de vendas identificado com ip 192.168.100.1 tem acesso ao servido Web de acordo com as politicas de Listas, o chefe de Recursos Humanos (RH) com ip 192.168.100.33/29, tem acesso ao servidor de ficheiros identificado com ip 192.168.100.42/29, através de listas de controle de acesso.

```
Router(config)#
Router(config)#access-list 120 permit ip host 192.168.100.1 host 192.168.100.42
Router(config)#access-list 120 permit ip host 192.168.100.33 host 192.168.100.42
Router(config)#access-list 120 permit ip host 192.168.100.25 host 192.168.100.42
Router(config)#acc
Router(config)#access-list 120 deny ip an
Router(config)#access-list 120 deny ip any an
Router(config)#access-list 120 deny ip any any
Router(config)#int
Router(config)#interface g0/0.10
Router(config-subif)#ip acc
Router(config-subif)#ip access-group 120 out
Router(config-subif)#exit
Router(config)#exit
Router#
```

Figura13: Comando de configuração de Listas para acesso a servidor FTP

Fonte: Fonte**:** Autoria Própria,2022.

A figura abaixo ilustra os comandos de configuração de Listas de controle de Acesso (ACLs) onde os chefes dos departamentos tem acesso a porta 80 traves do Servidor Web. O chefe de departamentos de vendas com ip 192.168.100.1 tem acesso a internet através do servidor Web, e o chefe de departamentos de RH com ip 192.168.100.33, tem acesso a internet através do servidor

Web co ip 192.168.100.41/29, o mesmo acontece com o chefe de departamentos de contabilidades identificado com ip 192.168.100.25 tem acesso a internet do servido Web com ip 192.168.100.41/29 Servidor localizado no Server-Room.

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#acc
Router(config)#access-list 170 permit tcp host 192.168.100.1 host 192.168.100.41 eq 80
Router(config)#access-list 170 permit tcp host 192.168.100.33 host 192.168.100.41 eq 80
Router(config)#access-list 170 permit tcp host 192.168.100.25 host 192.168.100.41 eq 80
Router(config)#acc
Router(config)#access-list 170 permit tcp 192.168.100.8 0.0.0.7 host 192.168.100.41 eq 80
Router(config)#acc
Router(config)#access-list 170 de
Router(config)#access-list 170 deny tcp an
Router(config)#access-list 170 deny tcp any an
Router(config)#access-list 170 deny tcp any any
Router(config)#int
Router(config)#interface g0/0.10
Router(config-subif)#ip acc
Router(config-subif)#ip access-group 170 out
Router(config-subif)#exit
Router(config)#exit
Router#
```

Figura14: Comando de configuração de Listas para acesso a Servidor Web

Fonte: Fonte**:** Autoria Própria,2022.

4 Capítulo IV- Conclusão & Recomendações

Listas de controle de acesso é um recurso muito útil em termos de segurança interna e externas da rede, e têm um papel fundamental no que se diz respeito à filtro de pacotes na rede. E ajuda os administradores a proteger a rede de ameaças internas e externas, pois elas podem servir como peça fundamental na política de segurança da rede.

Com implementação de Listas de controle de acesso (ACL), Águas da Região de Maputo vai melhorar a sua segurança interna e externa, vai aliviar a sobrecarga dispositivos da rede vai receber pacotes necessários fornecendo segurança e bloqueando usuários não autorizados e permitindo que usuários autorizados acessem recursos específicos. As ACLs podem bloquear qualquer tentativa injustificada de acessar os recursos da rede.

Com a implementação de listas de acesso nas Águas da Região de Maputo é fundamental porque haverá aumento da produção porque os funcionários vão se concentrar nas tarefas da empresa, isto é haverá poucos tráfegos na rede, os funcionários não vão fazer download dos filmes que é uma das causas do consumo dos recursos da rede.

Listas de controle de Acesso é um mecanismo encontrado pelos administradores para fazer uma gestão sã da rede sem gastar muito dinheiro na aquisição de equipamentos adicionais.

É muito importante ressaltar que as listas de acesso só terão seu melhor funcionamento se forem devidamente configuradas. E para isso é necessário que o administrador da rede ou a pessoa encarregada da segurança tenha um bom domínio sobre as mesmas. Isto se faz necessário, pois qualquer erro na configuração ou aplicação das listas de acesso pode acarretar que o objectivo traçado para ela não seja alcançado.

4.1 Recomendações

As recomendações do trabalho são referências a assuntos que foram identificados no decorrer da elaboração do trabalho. Entretanto, são assuntos pertinentes interessantes para a resolução adequada ou precisa desse problema. São eles:

- Uniformização do equipamento – Assim com o mesmo tipo de tecnologia ou tecnologias do mesmo fabricante
- Implementação de Virtual Private Network (VPN), que vai ajudar os funcionários de Águas da Região de Maputo (AdeM) a trabalhar a partir de casa com maior segurança possível na criptografia de dados.

5 CAPITULO V- REFERÊNCIAS BIBLIOGRÁFICAS

- CCNA Certification – Routing Basics for CISCO Certified Network Associates Exam 640-407", R. N. Myher, Prentice-Hall, ISBN: 0-13-086185-5, 1999.
- ANDREW S. TANENBAUM. Redes de Computadores. 4. ed. São Paulo: Campus, 2003.
- BLOG CCNA – Cisco Certified, Disponível em: <http://blog.ccna.com.br>. Acesso em: fev. 2010.
- Cisco, *"Cisco Active Network Abstraction 3.7 Reference Guide"*. Chapter 10. Retrieved on Feb 1, 2010. Internet:
- Cisco, "Cisco Active Network Abstraction 3.7 Reference Guide". Chapter 10. Retrieved on Feb 1, 2010
- CISCO. CCNA EXPLORATION 4.0. 2015. Disponível em http://www.pb.utfpr.edu.br/redes/cisco/. Acesso em 19 de agosto de 2015.
- CISCO.COM – Cisco Systems, Disponível em: <http://www.cisco.com>. Acesso em: mar. 2010.
- DOOLEY, Kevin; BROWN, Ian. *Cisco Cookbook*, 2nd Ed. O'Reilly, 2006. GLOBALKNOWLEDGE.COM – Global Knowledge, Disponível em: <http://www. globalknowledge.com>. A cesso em: mar. 2010.
- FILIPPETTI, Marcos A., CCNA 4.1: Guia Completo de Estudos. Florianópolis: Visual Books, 2008.
- FILTRADO DE PAQUETES DE DADOS A TRAVÉS DE LISTAS DE CONTROL DE ACCESO (ACL). Por Santiago Jácome / Mayra Salazar (Mayo de 2011). Disponible en: http://santiagojacome.wordpress.com/2011/05/25/filtrado-de-paquetes-de-datos-a-traves-de-listas de-control-de-acceso-acl/
- GALLO, M. A.; HANCOCK, W. M. Comunicação entre Computadores e Tecnologias de Rede. Sao Paulo: Thomson Learning, 2003.
- HUBERT Pun, "Convergence Behavior of RIP and OSPF Network Protocols". Retrieved in Dec 2001. Internet:
- JEFF Doyle, "*Routing TCP/IP (Volume I)*", Cisco Systems Press. Chapter 5-9. Published in 1997. Internet:K.Mirzahossein, M.Nguyen and S.Elmasry, "*Analysis of RIP, OSPF, and EIGRP Routing Protocols using OPNET*". Retrieved in 2013. Internet: http://www.sfu.ca/mtn9/427_Report.pdf.
- KUROSE, J. F. Redes de Computadores e a Internet: Uma Nova Abordagem. São Paulo: Addison-Wesley, 2004.

- KUROSE, James F.; ROSS, Keith W. Redes de computadores e a Internet: uma abordagem topdown. 5 ed. São Paulo:AddisonWesley, 2010. ϒ TANENBAUM, Andrew S. Redes de computadores. 4. ed. Rio de Janeiro: Elsevier, 2003. ϒ FROSSARD, Vera. Arquitetura e protocolos de rede TCP/IP. Rio de Janeiro: Rede Nacional de Ensino e Pesquisa, 2005.
- LISTA DE CONTROL DE ACCESO. Por Ing. JAVIER PADILLA (Diciembre de 2011). Disponible en: http://ing.javierpadilla.over-blog.es/article-lista-de-control-de-acceso-93373625.html
- Monográfico: Listas de control de acceso (ACLs)-Utilización de ACLs en router. Por Elvira Mifsu (Septiembre de 2012).
- MORAES, Igor M. VLANs – Redes Locais Virtuais. 2002. Disponível em http://www.gta.ufrj.br/grad/02_2/vlans/. Acesso em 21 de agosto de 2015.
- SADAYAO, Jeff. Cisco *IOS Access List.* First Ed. O'Reilly, 2001.
- SANTOS, Omar; STUPPI, John. CCNA Security 210-260 Official Cert Guide. Cisco Press, 2015.
- Seméria, C.; Understanding IP Addressing: Everthing You Ever Wanted to know. 3ComCorporation, 1996.
- STALLINGS, W. Redes e Sistemas de Comunicação de Dados: Teoria e Aplicações Corporativas. 5. ed. Rio de Janeiro: Elsevier, 2005.
- TANENBAUM, Andrew S.; Computer Networks; 3ª Edição; Prentice-Hall, New Jersey 1996.
- TECHREPUBLIC – TechRepublic Blogs, Disponível em:<http://blogs.techrepublic.com.com/>. Acesso em: fev. 2010.
- TORRES, Gabriel. Redes de computadores: curso completo. Rio de Janeiro: Axcel Books, 2001.

APÊNDICE

A figura abaixo ilustra o computador do chefe de departamento de venda (computadores simbolizados por um circulo em volta) com IP: 192.168.100.1 a cessando internet através do servidor Web de IP: 192.168.100.41

Figura15: Teste de Acesso a internet ou Servidor Web
Fonte: Autoria própria,2022.

O computador do chefe de departamento de venda (computador simbolizado por um circulo em volta) com IP: 192.168.100.1 enviando dados para todas as impressoras de vendas, RH e contabilidade conforme a figura a baixo.

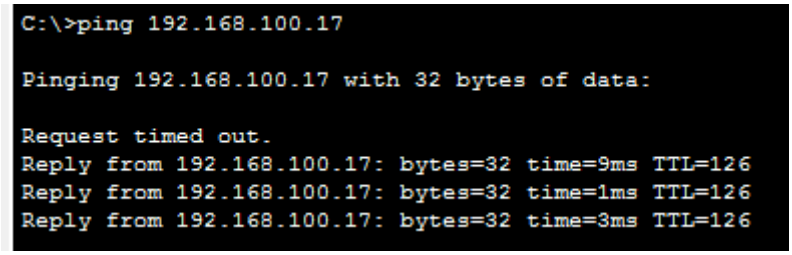

Figura16:Teste de ping para impressora de Venas.
Fonte: Autoria própria,2022.

A imagem abaixo ilustra o teste de ping onde o computador do chefe de venda faz ping para a impressora do departamento de RH.

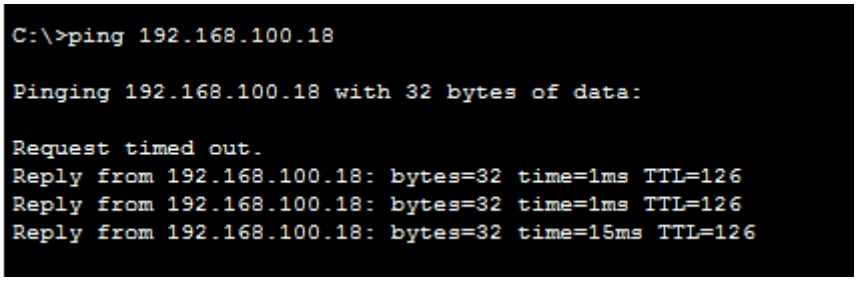

Figura17: Teste de Ping para impressora de Recursos Humanos RH
Fonte: Autoria própria,2022.

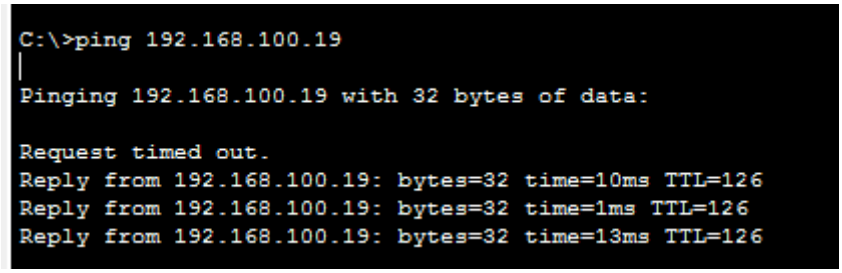

Figura18: Teste de ping para impressora de Contabilidade
Fonte: Autoria própria,2022.

E por sua vez através de listas de controle de acesso (ACL), todos computadores dos funcionários normais que se localizam no departamento de vendas não tem acesso a internet através do servidor Web localizado na *ServerRoom* e os mesmos só pode imprimir na sua respectiva impressora com IP: 192.160.100.17 como ilustra a figura a baixo.

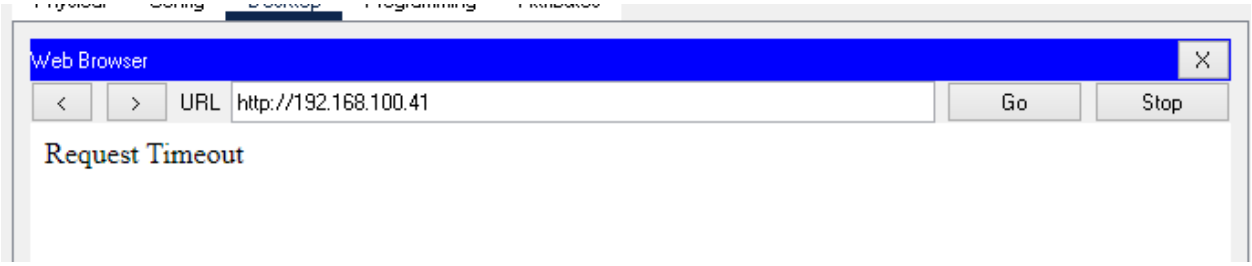

Figura19:Teste de acesso a Servidor Web pelos funcionários de Vendas
Fonte: Autoria própria,2022.

A imagem a baixo mostra os funcionários de departamentos de Vendas acessando impressora de RH sem sucesso, como mostra na imagem abaixo.

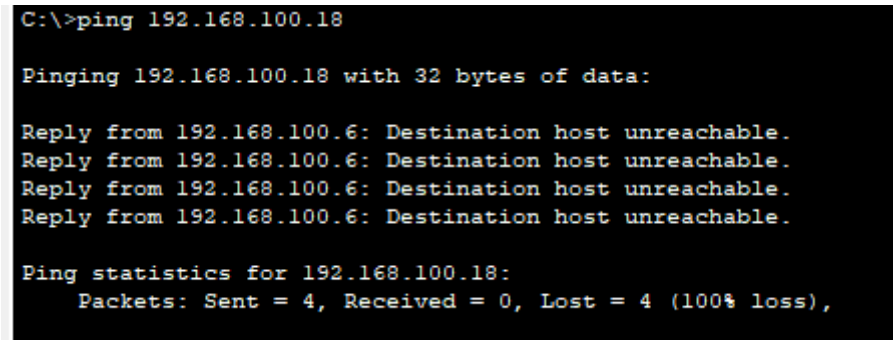

Figura20: Teste de Ping da impressora de RH pelos funcionarios
Fonte: Autoria própria, 2022.

5.1 Simulação de ACL no departamento de RH

Para o departamento de RH, segundo mecanismo de segurança em rede ACL e política da empresa, apena o chefe de departamento de recursos humanos (computador simbolizado por um circulo em

volta) de IP: 192.168.100.33 pode acessar o servidor Web de IP: 192.168.100.41 e enviar dados para qualquer impressora (Vendas, RH e contabilidade), só para chefe, os demais deve imprimir na sua própria impressora, como ilustra na figura abaixo:

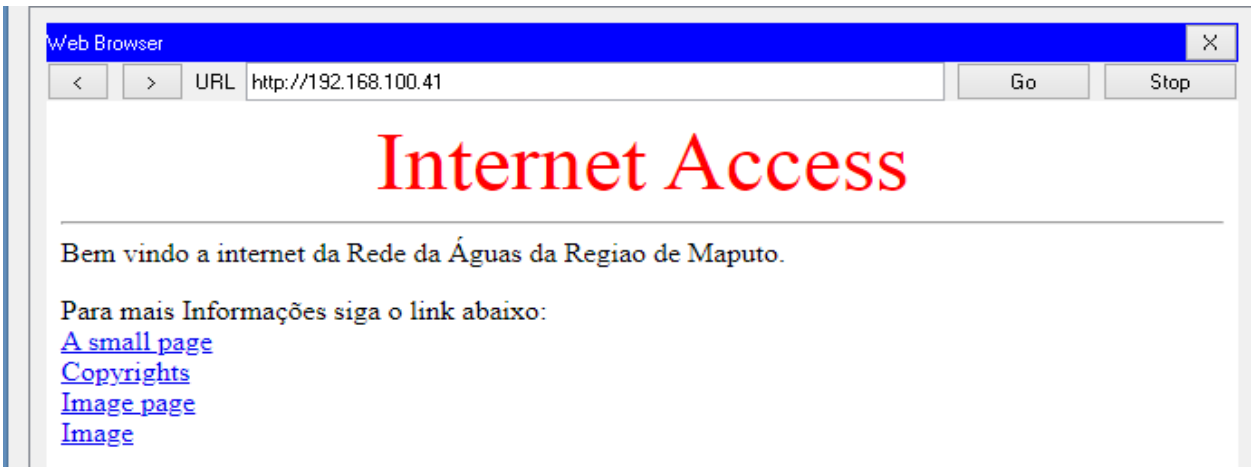

Figura21: Teste de Acesso a Servidor Web pelo chefe de RH
Fonte: Autoria própria,2022.

A figura abaixo mostra o teste de ping, onde o chefe dos departamentos de RH imprime na impressora de departamentos de vendas com sucesso

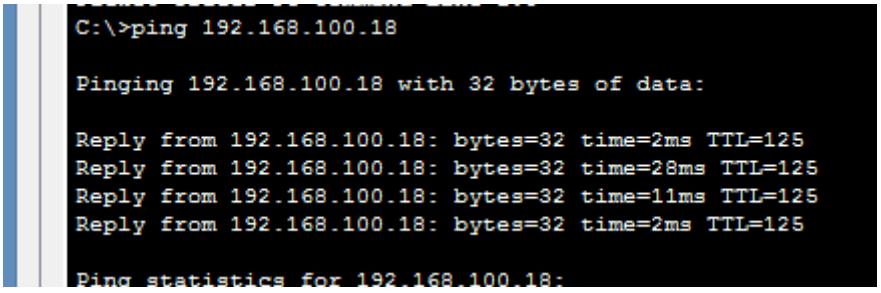

Figura22: Teste de Ping na impressora de RH pelos funcionários.
Fonte: Autoria própria,2022.

A Figura abaixo ilustra o chefe de departamentos Recursos Humanos imprimindo na impressora de contabilidades com sucesso.

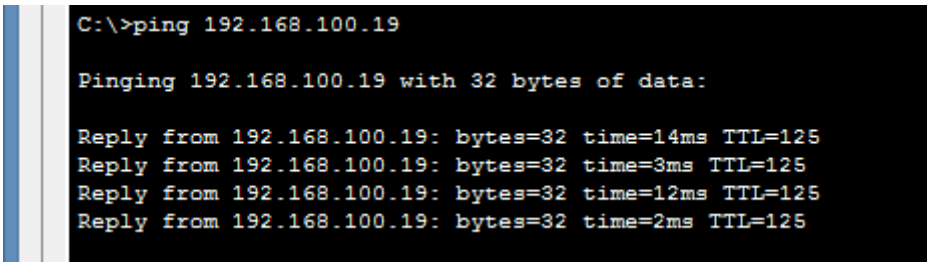

Figura23:Teste de Ping na impressora de contabilidade.
Fonte: Autoria própria,2022.

Mas os demais funcionários do departamento de RH, não tem acesso a internet através do servidor Web, e apena deve imprimir na sua respectiva impressora por questões de segurança da empresa.

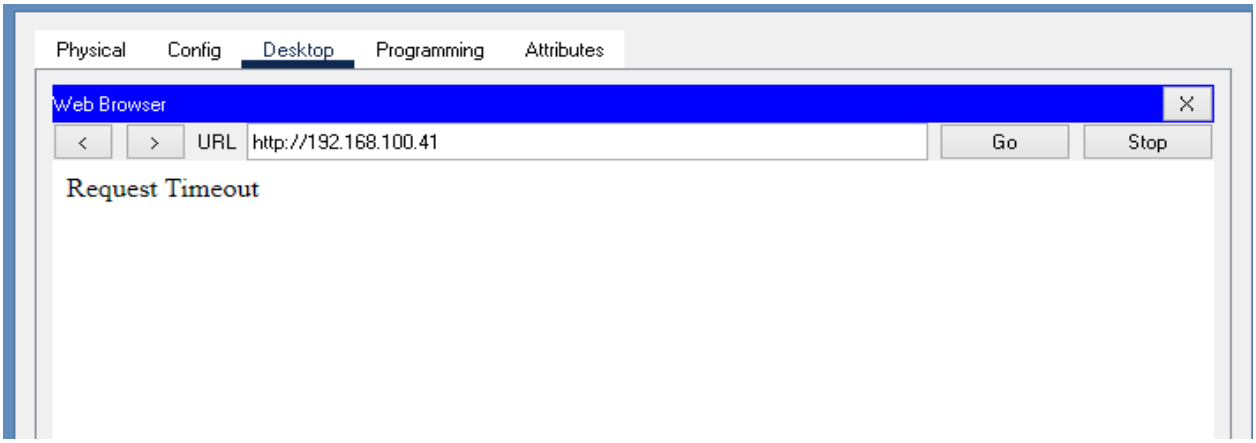

Figura24: Teste de Acesso a Servidor Web pelos funcionários de RH
Fonte: Autoria própria,2022.

A Figura abaixo ilustra os funcionários normais de RH acessando na impressora de Vendas e Contabilidade, isto é, impressora dos outros departamentos

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.17

Pinging 192.168.100.17 with 32 bytes of data:

Reply from 192.168.100.38: Destination host unreachable.
Reply from 192.168.100.38: Destination host unreachable.
Reply from 192.168.100.38: Destination host unreachable.
Reply from 192.168.100.38: Destination host unreachable.

Ping statistics for 192.168.100.17:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.100.19

Pinging 192.168.100.19 with 32 bytes of data:

Reply from 192.168.100.38: Destination host unreachable.
Reply from 192.168.100.38: Destination host unreachable.
Reply from 192.168.100.38: Destination host unreachable.
Reply from 192.168.100.38: Destination host unreachable.

Ping statistics for 192.168.100.19:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura25: Teste de Ping sem sucesso sem sucesso pelos funcionários de RH
Fonte: Autoria própria,2022.

5.2 Simulação de ACL no departamento de contabilidade

Para o departamento de contabilidade também obedece o mesmo mecanismo de segurança da rede interna da empresa usando listas de controle de acesso (ACL), nesta senda apena o chefe de contabilidade é que deve ter acesso a internet e deve imprimir em todas a impressoras de Vendas, RH e contabilidade conforme a política da empresa, como ilustra a figura abaixo.

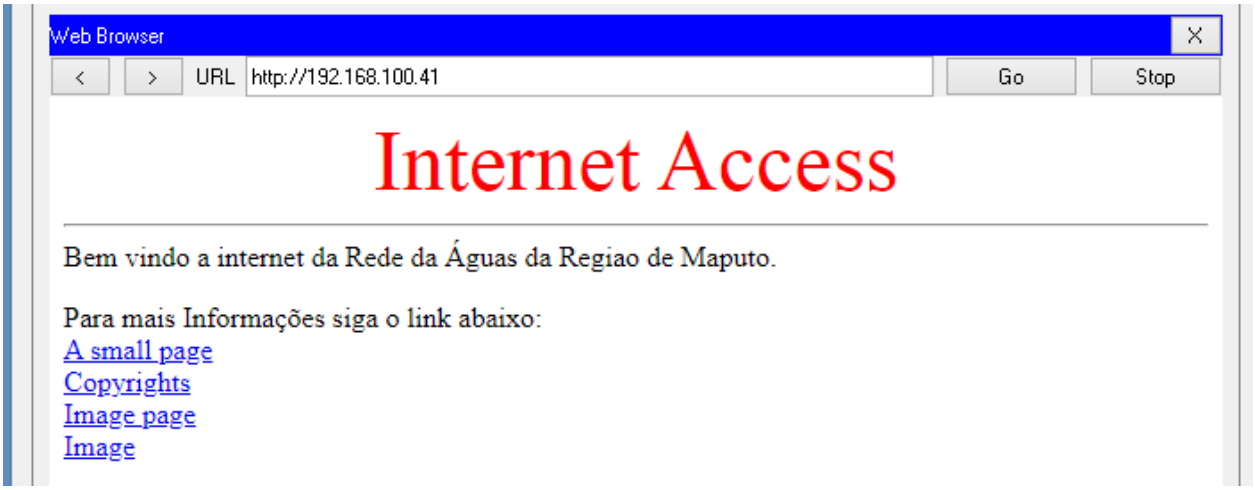

Figura26: Teste de acesso a Servidor Web pelo chefe de Contabilidade
Fonte: Autoria própria, 2022.

A Figura abaixo ilustra o Chefe de contabilidade imprimindo na impressora de Venda e RH com sucesso, devido as politicas de Listas de Controle de Acesso (ACLs).

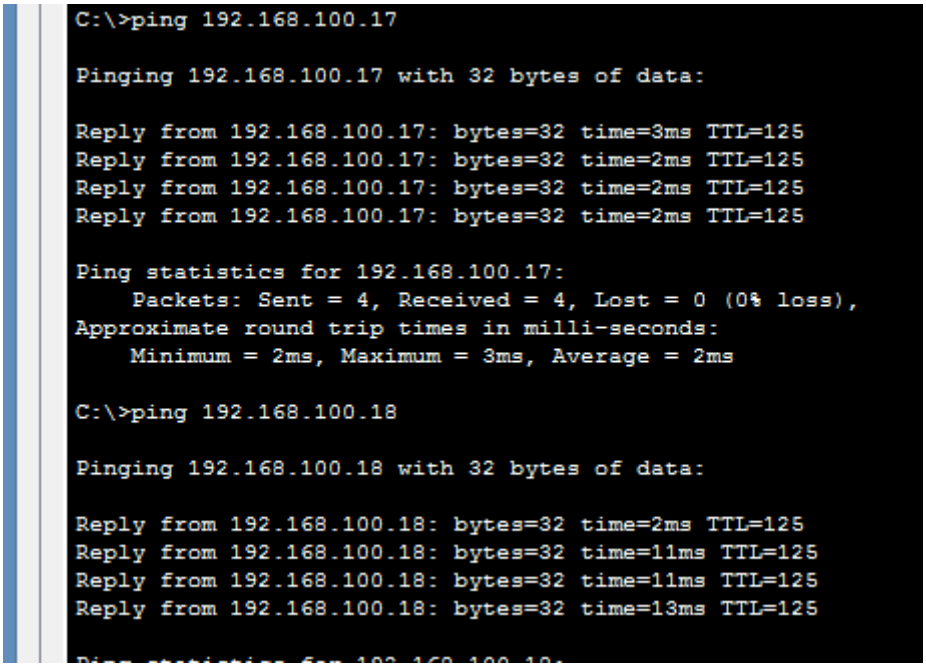

Figura27: Teste de Ping na impressora de Vendas e RH
Fonte: Autoria própria,2022.

A Figura a baixo ilustra os Funcionários normais da contabilidade tentando acessar a internet através do servidor Web sem sucesso, através de Listas de controle de acesso, devido as politicas de Listas de Controle de Acesso (ACLs).

Figura28: Teste de acesso a Servidor Web pelos funcionários de contabilidade

Fonte: Autoria própria,2022.

A figura abaixo ilustra os funcionários normais de Contabilidade tentando acessar as impressoras de Vendas e RH sem sucesso devido as Listas de controle de Acesso (ACLs)

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.17

Pinging 192.168.100.17 with 32 bytes of data:

Reply from 192.168.100.30: Destination host unreachable.
Reply from 192.168.100.30: Destination host unreachable.
Reply from 192.168.100.30: Destination host unreachable.
Reply from 192.168.100.30: Destination host unreachable.

Ping statistics for 192.168.100.17:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.100.18

Pinging 192.168.100.18 with 32 bytes of data:

Reply from 192.168.100.30: Destination host unreachable.
Reply from 192.168.100.30: Destination host unreachable.
Reply from 192.168.100.30: Destination host unreachable.
Reply from 192.168.100.30: Destination host unreachable.

Ping statistics for 192.168.100.18:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura29: Teste de ping sem sucesso na impressora de RH e Vendas

Fonte: Autoria própria,2022.

5.2.1 Comandos de Configuração de ACL Padrão

Router(config)#access-list *<1-199> <Permit/Deny> <source_ipaddress> <source-wildcard-mask>*

Router(config)#access-list *<acl#>* Permit any

Router(config)# interface gigabitethernet #/#

Router(config-if)#ip access-group *<acl#> <in/out>*

5.2.2 Comandos de Configuração de lista Estendida

Router(config)#access-list *<100-199> <Permit/Deny> <protocol><source_ip-address>*

<soure_wildcard-mask> <destination_ip-address> <destination_wildcardmask> <eq> <port>

Router(config)#**access-**list *<acl#>* permit *<protocol>* any any

Router(config)#interface fastethernet #/#

Router(config-if)#ip access-group *<acl#> <in/out>*

Router(config-if)#end.

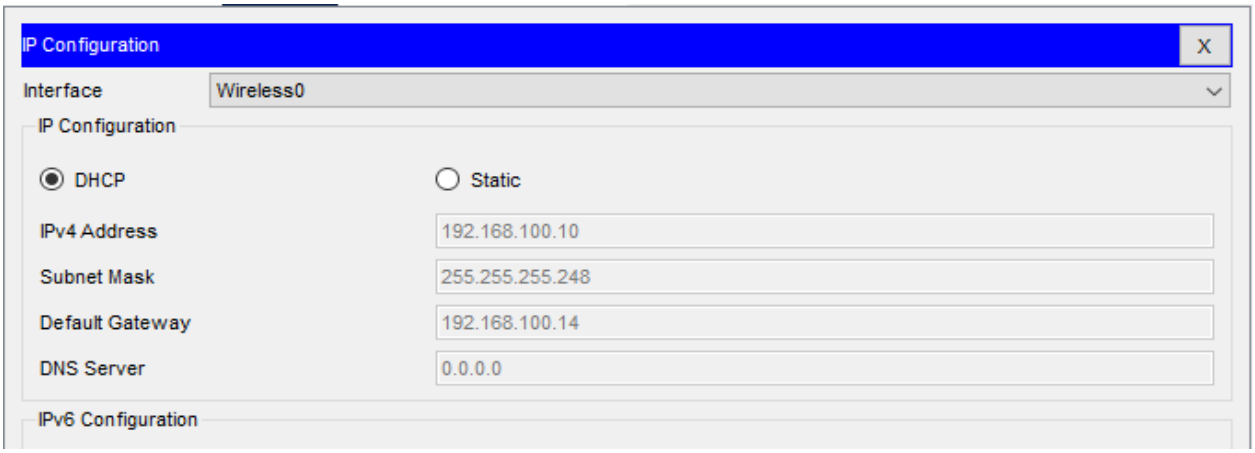

Figura 30: O computador recebe IP através de DHCP

Fonte: Autoria Própria,2022.

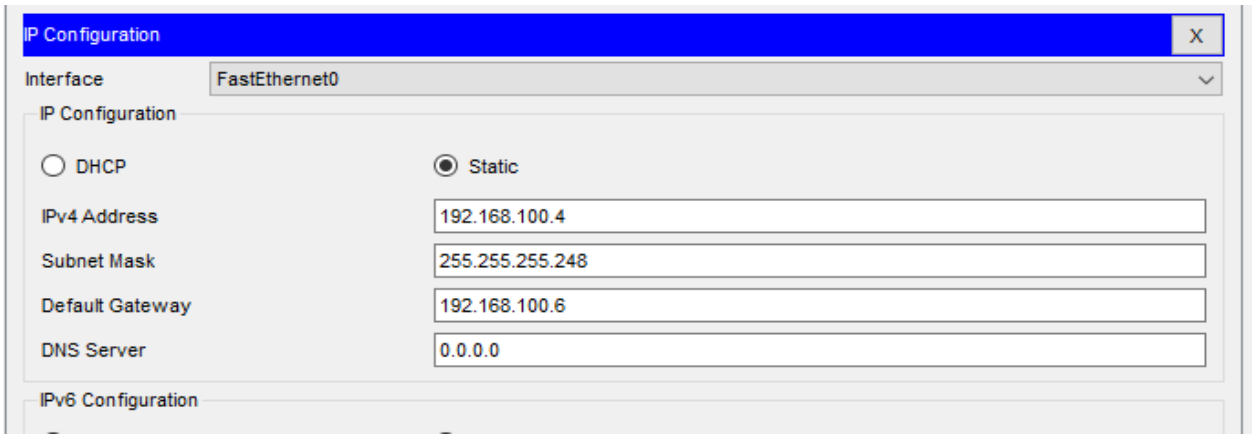

Figura31: Computador com ip estático

Fonte: Autoria Própria,2022.